F5CAB5: Preparing for BIG-IP Administration and Troubleshooting

For F5 BIG-IP configuration interviews, disciplined reasoning is what matters. Reciting commands or knowing every answer will not substitute for it. State what you observed, name the affected layer, identify the exact tool or change, and explain your verification.

> The mistake that changed how I work: I changed a live object before proving where the fault was.

F5 BIG-IP Configuration and BIG-IP Administration

1. What is BIG-IP TMOS?

Tests: Platform role. **Answer:** "I described BIG-IP TMOS as the operating layer that loads configuration, processes traffic, and repor health." **Loses marks:** Describing only the graphical interface.

2. How do virtual servers, pools, and members relate?

Tests: Object model. **Answer:** "I traced the virtual server to its pool, then to an eligible member. Monitoring controlled eligibility." **Loses marks:** Assuming that every pool uses round-robin selection.

3. How do you make a safe configuration change?

Tests: Change control. **Answer:** "I captured `tmsh show running-config`, then backed up the configuration and made one scoped change. Finally, I verified traffic." **Loses marks:** Skipping the backup or verification after the change.

4. How should administrative access be managed?

Tests: Least privilege. **Answer:** "I used named accounts, least-privilege roles, partition assignments, and audit trails." **Loses marks:** Recommending shared root access.

Traffic, Monitors, and Evidence in F5 BIG-IP Troubleshooting

5. How do you configure an HTTP-monitored pool member?

Tests: Object relationships. **Answer:** "I set the address and port, attached an HTTP monitor, and defined its send and receive expectations Then I checked the reason for the marked-down state." **Loses marks:** Using an unreliable application URL as the health endpoint.

6. Why does a passing member remain down?

Tests: Source-aware diagnosis. **Answer:** "I compared the monitor strings, headers, source address, and port against a packet capture taken from BIG-IP." **Loses marks:** Assuming that my workstation and TMOS follow the same network path.

7. What evidence do you collect first?

Tests: Structured triage. **Answer:** "I recorded the time, virtual server, pool, member, and status. Then I inspected `/var/log/ltm` and the relevant access logs." **Loses marks:** Restarting services before preserving the evidence.

8. When should you use `tcpdump`?

Tests: Packet-level reasoning. **Answer:** "I filtered by interface, host, and port to determine whether TCP, TLS, or HTTP had failed. **Loses marks:** Capturing the wrong interface or collecting unnecessary traffic.

BIG-IP iRules and HTTP Diagnosis

9. How do you distinguish 502 from 503?

Tests: HTTP semantics. **Answer:** "I identified who generated it. A generated 503 usually means no eligible member, while a 502 suggests invalid upstream HTTP." **Loses marks:** Treating both codes as proof that the member is down.

10. How do you investigate a 502?

Tests: End-to-end diagnosis. **Answer:** "I correlated the logs and packets, then inspected the member's response. I also checked the headers and connection reuse." **Loses marks:** Changing pool settings before identifying the faulty response.

11. How do you create a useful iRule?

Tests: BIG-IP iRules logic**Answer:** "I matched `HTTP::host`, preserved `HTTP::uri`, and issued `HTTP::redirect`. I attached it narrowly and verified the response." **Loses marks:** Applying an unvalidated rule globally.

12. How do you debug an iRule?

Tests: Controlled diagnosis. **Answer:** "I reviewed the rule priority, conditions, variables, and `/var/log/ltm`. Before changing anything, I reproduced one request." **Loses marks:** Editing the application before examining the rule.

Operational Judgment: Where Strong Candidates Separate

13. How do you diagnose a TLS failure?

Tests: TLS diagnosis.**Answer:** "I used `openssl s_client` to check SNI, the cipher, the protocol, the certificate chain, and expiry."**Loses marks:** Changing ciphers before proving a mismatch.

14. What do you verify during failover?

Tests: HA awareness. **Answer:** "I checked the traffic state, configuration synchronisation, address and route ownership, and the logs around failover." **Loses marks:** Confusing a reboot with a failover event.

15. What if you do not know the answer?

Tests: Honest escalation. **Answer:** "During BIG-IP support, I said, 'I don't know yet.' I stated what I had ruled out and requested missin evidence. Then I escalated the impact, timing, and reversible steps." **Loses marks:** Bluffing or presenting a guess as fact.

Conclusion: Close with Evidence and Ownership

Close by asking which failures dominate the team, how changes are approved and rolled back, and what evidence escalation requires. Within a day, I sent a thank-you note that named one relevant diagnosis, the logs I would request, and my verification plan. It showec disciplined F5 BIG-IP configuration and F5 BIG-IP troubleshooting without turning into a lecture.

FAQ

- **Must I memorise every command?** No. Master the object model, evidence path, and safe workflow, then verify syntax in the lab.
- **What if my hands-on experience is limited?** Describe what you actually contributed. Keep observed evidence separate from assumptions.

F5 Networks

F5CAB5 Exam

BIG-IP Administration Support and Troubleshooting

Thank you for Downloading F5CAB5 exam PDF Demo

You can also try our F5CAB5 Full Version Download

https://www.certkillers.net/Exam/F5CAB5

Version: 6.2

Question: 1

A BIG-IP Administrator needs to determine why only one pool member is showing connections from the virtual server, resulting in uneven load balancing.

What two reasons would cause uneven load balancing? (Choose two answers)

A. The virtual server is marked down.

B. Monitors have marked down multiple pool members.

C. The pool has a persistence profile configured.

D. All pool members are marked down.

Answer: B,C

Explanation:

Uneven load balancing on a BIG-IP system typically occurs when traffic is not distributed evenly across all available pool members. One common reason is thatmonitors have marked down multiple pool members (Option B). When health monitors fail for specific pool members, BIG-IP automatically removes those members from load-balancing decisions. As a result, traffic is sent only to the remaining healthy member, creating the appearance that load balancing is not functioning correctly. This behavior is expected and aligns with BIG-IP's design to ensure traffic is sent only to healthy resources.

Another frequent cause isthe presence of a persistence profile on the pool or virtual server (Option C).

Persistence (such as source address or cookie persistence) forces subsequent client connections to be sent to the same pool member for session continuity. While persistence is critical for certain applications, it can override the load-balancing algorithm and cause most or all traffic to be directed to a single pool member, especially during low traffic volumes or testing scenarios.

The other options are incorrect because avirtual server marked down (Option A)would not pass traffic at all, andall pool members marked down (Option D)would result in no connections rather than uneven distribution. This analysis follows standard BIG-IP troubleshooting methodology using pool status, monitor results, and persistence configuration review.

Question: 2

A BIG-IP Administrator plans to upgrade a BIG-IP device to the latest TMOS version.

Which two tools could the administrator leverage to verify known issues for the target versions? (Choose two answers)

A. F5 End User Diagnostics (EUD)

B. F5 Bug Tracker

C. F5 University

D. F5 iHealth

E. F5 Downloads

Answer: B,D

Explanation:

Before upgrading a BIG-IP system to a newer TMOS version, it is critical to review known issues to avoid introducing instability or regressions.F5 Bug Tracker (Option B)is a primary resource for this purpose. It allows administrators to search for documented software defects by TMOS version, module, symptom, or bug ID. Using Bug Tracker, an administrator can identify unresolvedissues, fixed bugs, and behavioral changes that may affect their specific deployment, such as traffic handling, high availability, or module-

specific functionality. This directly supports proactive troubleshooting and informed upgrade planning.

F5 iHealth (Option D)is another essential tool used during upgrade preparation. iHealth analyzes uploaded UCS or QKView files and correlates the device configuration and software version with F5's known issues database. It provides actionable reports highlighting critical defects, upgrade risks, interoperability concerns, and recommended target versions. iHealth is especially valuable because it contextualizes known issues based on the actual configuration running on the device.

The other options are not appropriate for verifying known software issues.F5 End User Diagnostics (Option A)is a client-side troubleshooting tool,F5 University (Option C)is a training platform, andF5 Downloads (Option E)is primarily used to obtain software images and release notes, not to analyze known defects in depth.

Question: 3

A BIG-IP Administrator needs to collect HTTP status code and HTTP method for traffic flowing through a virtual server.

Which default profile provides this information? (Choose one answer)

A. Request Adapt

B. HTTP

C. Analytics

D. Statistics

Answer: C

Explanation:

To collect application-layer details such asHTTP status codes(200, 404, 500, etc.) andHTTP methods(GET, POST, PUT, DELETE), the BIG-IP system must use a profile designed for traffic visibility and reporting rather than basic traffic handling. TheAnalytics profile (Option C)is the correct choice because it is specifically designed to collect, store, and present detailed statistics about HTTP and TCP traffic passing

through a virtual server.

When an Analytics profile is attached to a virtual server, BIG-IP can record metrics such as HTTP response codes, request methods, URI paths, latency, throughput, and client-side/server-side performance data. These statistics are then accessible through the BIG-IP GUI underStatistics → Analytics, allowing administrators to validate application behavior and troubleshoot performance or functional issues.

TheHTTP profile (Option B)enables HTTP protocol awareness and features like header insertion and compression, but it does not provide historical or statistical reporting of HTTP methods and response codes.Request Adapt (Option A)is used for ICAP-based content adaptation, not visibility.Statistics (Option D)is not a standalone profile and does not provide HTTP-level insight.

Therefore, the Analytics profile is the only default profile that fulfills this requirement.

Question: 4

Which two methods should the BIG-IP Administrator use to troubleshoot a pool member that has been markedDOWNby its health monitor? (Choose two answers)

A. Review the BIG-IP routing table using netstat -rn to show all routes.

B. Enable monitor logging for the pool member that isDOWN.

C. Review the pool and pool-member statistics table for error data.

D. Collect a TCPdump packet capture for theDOWNpool member.

Answer: B,D

Explanation:

When a pool member is markedDOWN, it indicates that the configured health monitor is failing. The most effective troubleshooting approach is to focus on the monitor behavior and the actual traffic between BIG-IP and the pool member.

Enabling monitor logging (Option B)is a recommended first step. Monitor logging provides detailed

information about why the health check is failing, such as timeouts, connection refusals, incorrect responses, or unexpected status codes. This directly correlates with BIG-IP troubleshooting best practices and allows administrators to confirm whether the failure is due to application behavior, incorrect monitor configuration, or network reachability.

Collecting a TCPdump packet capture (Option D)is also a highly effective method. A packet capture allows the administrator to verify whether the monitor probes are being sent, whether responses are received, and whether packets are being dropped, reset, or malformed. This is especially valuable when diagnosing firewall issues, SSL problems, or application-level failures.

Reviewing pool statistics (Option C) is useful for general monitoring but does not explainwhya health monitor is failing. Reviewing the routing table (Option A) is typically unnecessary unless there is evidence of a broader routing issue affecting multiple destinations.

Question: 5

A BIG-IP Administrator observes the following pool member status message:

Pool /Common/testpool member /Common/10.120.0.5:8090 monitor status down

[/Common/http: up, /Common/http2: down; last error:]

Why is this pool member being marked down? (Choose one answer)

A. The pool member is currently only serving HTTP traffic.

B. The pool member is currently only serving TCP traffic.

C. The pool member is currently only serving UDP traffic.

D. The pool member is currently only serving HTTPS traffic.

Answer: A

Explanation:

The pool member is markedDOWNbecause it is monitored bymultiple health monitors, specifically anHTTPmonitor and anHTTP/2monitor. The status message clearly shows that theHTTP monitor is UP, while theHTTP/2 monitor is DOWN. In BIG-IP, when multiple monitors are assigned to a pool member, the default behavior isAND logic, meaningall assigned monitors must succeedfor the pool member to be considered healthy.

In this scenario, the server is responding successfully to standard HTTP (likely HTTP/1.1) requests but does not support or respond correctly to HTTP/2 requests. As a result, the HTTP/2 monitor fails, which causes the overall monitor status to beDOWN, even though HTTP traffic itself is working.

This behavior is expected and documented in BIG-IP monitoring logic. Unless the monitor rule is explicitly changed to“at least one of”, a single failing monitor will mark the pool member down. Therefore, the correct conclusion is that the pool member isonly serving HTTP traffic, not HTTP/2.

The resolution would be to either remove the HTTP/2 monitor, correct the application to support HTTP/2, or adjust the monitor rule to match the intended health-check logic.

Thank You for trying F5CAB5 PDF Demo

To try our F5CAB5 Full Version Download visit link below

https://www.certkillers.net/Exam/F5CAB5

Start Your F5CAB5 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your F5CAB5 preparation with actual exam questions.