Free PDF Quiz 2026 F5 F5CAB3: BIG-IP Administration Data Plane Configuration Perfect Study Group

P.S. Free 2026 F5 F5CAB3 dumps are available on Google Drive shared by DumpsActual: https://drive.google.com/open?id=1L5PmXRmi_0X7ImoriEmmAKwlmMJ1fFG_

You can enjoy the instant download of F5CAB3 exam dumps after purchase so you can start studying with no time wasted. You can install our F5CAB3 study file on your computer or other device as you like without any doubts. Because our F5CAB3 test engine is virus-free, you can rest assured to use. What's more, the F5CAB3 Questions and answers are the best valid and latest, which can ensure 100% pass. Our 24/7 customer service is available and you can contact us for any questions about F5 practice dumps.

You can learn F5CAB3 quiz torrent skills and theory at your own pace, and you are not necessary to waste your time on some useless books or materials and you will save more time and energy that you can complete other thing. We also provide every candidate who wants to get certification with free Demo to check our materials. No other F5CAB3 Study Materials or study dumps can bring you the knowledge and preparation that you will get from the F5CAB3 study materials available only from DumpsActual.

>> F5CAB3 Study Group <<

Exam F5CAB3 Study Guide | Test F5CAB3 Simulator

All these F5CAB3 exam questions formats contain the real BIG-IP Administration Data Plane Configuration (F5CAB3) exam practice test questions that assist you in preparation and you will feel condiment to pass the final F5 F5CAB3 exam easily. The F5 F5CAB3 desktop practice test software and web-based practice test software, both are the mock BIG-IP Administration Data Plane Configuration (F5CAB3) exam that provides you real-time F5CAB3 exam environment for quick and complete preparation.

F5 F5CAB3 Exam Syllabus Topics:

Topic	Details

Topic 1	• Apply procedural concepts required to modify and manage virtual servers: This domain covers managing virtual servers including applying persistence, encryption, and protocol profiles, identifying iApp objects, reporting iRules, and showing pool configurations.
Topic 2	• Apply procedural concepts required to modify and manage pools: This domain addresses managing server pools including health monitors, load balancing methods, priority groups, and service port configurations.

F5 BIG-IP Administration Data Plane Configuration Sample Questions (Q63-Q68):

NEW QUESTION # 63
Due to a change in application requirements, a BIG-IP Administrator needs to modify the configuration of a Virtual Server to include a Fallback Persistence Profile.
Which persistence profile type should the BIG-IP Administrator use?

- A. Hash
- B. SSL
- C. Source Address Affinity
- D. Universal

Answer: C

Explanation:
Fallback persistence is used when the primary persistence method fails. Source Address Affinity is a Layer 4 persistence method and is fully supported as a fallback option for most virtual server types.

NEW QUESTION # 64
A virtual server is configured to offload SSL from a pool of backend servers. When users connect to the virtual server, they successfully establish an SSL connection but no content is displayed. A packet trace performed on the server shows that the server receives and responds to the request. What should a BIG-IP Administrator do to resolve the problem?

- A. disable SNAT
- B. enable SNAT
- C. disable Server SSL profile
- D. enable Server SSL profile

Answer: B

Explanation:
This scenario describes a classic routing issue often encountered during SSL offload deployments. The fact that an SSL connection is established indicates the Client SSL profile is working correctly. The packet trace showing the server "receives and responds" to the request is the most critical diagnostic clue.
When a BIG-IP receives traffic, it typically passes the client's original source IP address to the backend server. If the backend server's default gateway is not the BIG-IP (a common "one-arm" network topology), the server will attempt to send its response directly back to the client's IP via its own default router. The client's browser will reject this response because it expects traffic to come from the Virtual Server's IP, not the backend server's IP.
To resolve this, the administrator must enable SNAT (Source Address Translation), typically using SNAT Automap. When SNAT is enabled, the BIG-IP replaces the client's original source IP with one of its own Self IPs before forwarding the request to the server. Because the source of the packet is now the BIG-IP, the backend server is forced to send its response back to the BIG-IP. The BIG-IP then receives the response, translates it back, and delivers the content to the user. Option A is unnecessary if the servers are expecting plain-text traffic after the BIG-IP performs offload. Option D would only worsen the existing routing discrepancy.

NEW QUESTION # 65
A BIG-IP Administrator configures a node with a standard icmp Health Monitor. The Node shows as DOWN although the

Backend Server is configured to answer ICMP requests. Which step should the administrator take next to find the root cause of this issue?

- A. Run an ssldump
- B. Run a qkview
- C. Run a tcpdump
- D. Run a curl

Answer: C

Explanation:
In the F5 BIG-IP ecosystem, a standard ICMP health monitor functions by sending an ICMP echo request to a target node and expecting an ICMP echo reply within a specified timeout period. When a node is marked "DOWN" despite the backend server being configured to respond to ICMP, the issue typically lies in the network path or the specific packet exchange between the BIG-IP's self IP and the node's IP. Running a tcpdump is the most effective next step because it provides a real-time packet capture of the actual monitor traffic leaving the BIG-IP and any return traffic coming back from the server. This allows the administrator to verify if the BIG-IP is actually sending the echo request, if the request is reaching the server, and if the server is indeed replying or if the reply is being dropped by an intermediate firewall or a security policy.
While other tools have their place, they are inappropriate for this specific layer 3/4 connectivity issue. A qkview is a comprehensive diagnostic file used primarily for F5 Support to analyze the entire system's state but is overkill for initial connectivity troubleshooting. An ssldump is used for inspecting SSL/TLS handshakes and encrypted payloads, which is irrelevant for a non-encrypted ICMP monitor. A curl command is a tool for testing HTTP/HTTPS application-level responses; it cannot be used to troubleshoot ICMP (ping) connectivity directly. By using tcpdump -ni <vlan_name> host <node_ip>, the administrator can see the ICMP "type 8" (request) and "type 0" (reply) packets, immediately identifying if the monitor failure is due to a "Destination Unreachable" message or a simple lack of response, thereby pinpointing the root cause in the data plane.

NEW QUESTION # 66
Refer to the exhibit.
A BIG-IP Administrator creates a new Virtual Server to load balance SSH traffic. Users are unable to log on to the servers.
What should the BIG-IP Administrator do to resolve the issue? (Choose one answer)

- A. Set HTTP Profile to None
- B. Set Source Address to 10.1.1.2
- C. Set Destination Address/Mask to 0.0.0.0/0
- D. Set Protocol to UDP

Answer: A

Explanation:
SSH is a Layer 4 TCP-based protocol that operates on TCP port 22 and does not use HTTP in any capacity. In the exhibit, the Virtual Server is configured with an HTTP Profile applied, which is inappropriate for SSH traffic and causes connection failures.
According to the BIG-IP Administration: Data Plane Configuration documentation:
An HTTP profile must only be applied to Virtual Servers handling HTTP or HTTPS traffic.
When an HTTP profile is attached, BIG-IP expects HTTP headers and attempts to parse application-layer data.
Non-HTTP protocols such as SSH, FTP (control), SMTP, and other raw TCP services will fail if an HTTP profile is enabled.
Why the other options are incorrect:
A). Set Protocol to UDPSSH uses TCP, not UDP. Changing the protocol would break SSH entirely.
B). Set Source Address to 10.1.1.2The source address setting controls client access restrictions and is unrelated to protocol parsing issues.
C). Set Destination Address/Mask to 0.0.0.0/0The destination address is already valid for a specific SSH service and does not impact protocol handling.
Correct Resolution:
The BIG-IP Administrator should remove the HTTP Profile (set it to None) so the Virtual Server functions as a pure Layer 4 TCP service, allowing SSH connections to pass through successfully.

NEW QUESTION # 67
Some users who connect to a busy Virtual Server have connections reset by the BIG-IP system. Pool member resources are NOT a factor.
What is a possible cause?

- A. Rewrite profile not configured
- B. Connection Limit is set too low
- C. Server SSL profile not reconfigured
- D. Connection Rate Limit is set too high

Answer: B

Explanation:
When the connection limit is reached, BIG-IP resets new connections, even if pool members are healthy.

NEW QUESTION # 68
......