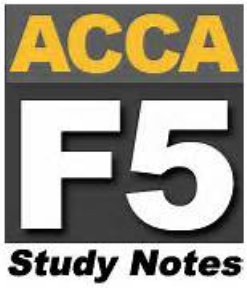
F5 F5CAB3 Valid Study Notes & Latest F5CAB3 Version



Our F5CAB3 practice quiz will be the optimum resource. Many customers claimed that our study materials made them at once enlightened after using them for review. If you are still tentative about our F5CAB3 exam dumps, and some exam candidate remain ambivalent to the decision of whether to choose our F5CAB3 Training Materials, there are free demos for your reference for we understand your hesitation.

F5 F5CAB3 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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.

>> F5 F5CAB3 Valid Study Notes <<

Latest F5CAB3 Version & Latest F5CAB3 Exam Materials

Our professional experts are very excellent on the compiling the content of the F5CAB3 exam questions and design the displays. Moreover, they impart you information in the format of the F5CAB3 questions and answers that is actually the format of your real certification test. Hence not only you get the required knowledge, but also you find the opportunity to practice real exam scenario. We have three versions of the F5CAB3 Training Materials: the PDF, Software and APP online. And the Software version can simulate the real exam.

F5 BIG-IP Administration Data Plane Configuration Sample Questions (Q56-Q61):

NEW QUESTION # 56
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 a curl
- B. Run an ssldump
- C. Run a qkview
- D. Run a tcpdump

Answer: D

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 # 57
Refer to the exhibit.
A BIG-IP Administrator needs to configure health monitors for a newly configured server pool named Pool_B.
Which health monitor settings will ensure that all pool members will be accurately marked as available or unavailable? (Choose one answer)

- A. HTTP, HTTPS, FTP, and ICMP with the Availability Requirement of at least one health monitor
- B. HTTPS, HTTP, FTP, and SSH with the Availability Requirement of all health monitors
- C. HTTPS, HTTP, FTP, and SSH with the Availability Requirement of at least one health monitor
- D. HTTPS, HTTP, FTP, and SSH with the Availability Requirement of all health monitors

Answer: C

Explanation:
From the exhibit, the pool contains different applications on different service ports (for example, HTTP/80, FTP/21, HTTPS/443, SSH/22). To mark pool members correctly, BIG-IP must be able to verify the actual service running on each member's port.
In BIG-IP Administration: Data Plane Configuration, monitor behavior is described as follows:
* When multiple monitors are assigned to a pool, the Availability Requirement controls how monitor results are evaluated:
* At least one = the pool member is marked up if any one of the assigned monitors succeeds.
* All = the pool member is marked up only if every assigned monitor succeeds.
* For pools containing members with different services/ports, using All can incorrectly mark members down because monitors intended for other services will fail on the wrong port.
Why C is correct:
* Assigning HTTPS, HTTP, FTP, and SSH covers the actual services shown in the pool.
* Setting the Availability Requirement to at least one ensures that each pool member is considered available when its appropriate service monitor succeeds, without being forced to pass unrelated service monitors.
Why the other options are incorrect:
* A / D (Availability Requirement = all): would cause members to be marked down when unrelated monitors fail (e.g., SSH monitor

against an HTTP member).
* B (includes ICMP): ICMP can indicate the host is reachable even if the application service is down, which does not "accurately" reflect service availability.
Therefore, the best choice is HTTPS, HTTP, FTP, and SSH with Availability Requirement of at least one health monitor.

NEW QUESTION # 58
Refer to the exhibit.
A BIG-IP Administrator configures a new VLAN on an HA pair of devices that does NOT yet have any traffic. This action causes the assigned traffic group to fail over to the standby device. Which VLAN setting should be changed to prevent this issue?

- A. Auto Last Hop
- B. Source Check
- C. Fail-safe
- D. Customer Tag

Answer: C

Explanation:
The exhibit shows the advanced configuration of a VLAN where the Fail-safe option is checked. VLAN Fail- safe is a high-availability feature used to monitor network connectivity on a specific VLAN. When enabled, the BIG-IP system monitors the VLAN for network traffic. If the system does not detect any "useful" traffic on the VLAN within the specified Fail-safe Timeout (which is 90 seconds in the exhibit), it attempts to generate traffic by pinging the default gateway or other devices. If it still detects no traffic, the BIG-IP concludes that the VLAN is unreachable or the network interface has failed, and it triggers a "Fail-safe Action"-in this case, "Reboot" or a failover to the peer device in the HA group.
Because the administrator has just created a new VLAN that "does NOT yet have any traffic," the Fail-safe mechanism triggers immediately after the 90-second timeout period. Since no devices are yet communicating on this VLAN, the BIG-IP incorrectly assumes there is a hardware or cabling failure and forces a failover to ensure the standby device (which might have better connectivity) takes over. To prevent this unwanted failover, the administrator should uncheck the Fail-safe box for that specific VLAN until the VLAN is fully populated with active nodes and regular traffic. Once the application is live and traffic is flowing, Fail-safe can be re-enabled to provide an additional layer of redundancy. Auto Last Hop (Option A) and Source Check (Option B) are routing and security features that do not trigger HA failover events.

NEW QUESTION # 59
A BIG-IP Administrator is setting up a new BIG-IP device. The network administrator reports that the interface has an incompatible media speed. The BIG-IP Administrator needs to change this setting manually.
From which location should the BIG-IP Administrator perform this task?

- A. In the Configuration Utility, System > Configuration
- B. On the Front Console
- C. In the Configuration Utility, Network > Interface
- D. In the TMOS Shell Command line

Answer: C

Explanation:
Standard BIG-IP administration dictates that hardware-level physical attributes are managed within the Network section of the configuration. When a network switch and a BIG-IP fail to successfully negotiate speed and duplex settings (Auto-Negotiation), it can result in CRC errors, late collisions, or a total lack of link. To resolve this manually, the administrator must navigate to the Configuration Utility (GUI) and go to Network > Interfaces.
Within the Interfaces list, the administrator can select the specific physical port (e.g., 1.1 or 1.2) and modify its properties. By default, the media speed is set to "Auto," but the drop-down menu allows for manual selection of specific speeds (e.g., 100Mb/s, 1Gb/s, 10Gb/s) and duplex settings (Full or Half). While these changes can also be made via the TMOS Shell (TMSH) (Option B) using the modify net interface command, the question asks for the standard location, which in most administrative contexts refers to the primary GUI path. System > Configuration (Option D) is used for global device settings like NTP, DNS, and licensing, not for interface-specific physical layer parameters. The Front Console (Option A), referring to the LCD panel on physical appliances, is primarily used for initial management IP setup and viewing system alerts, but does not provide the granular interface configuration required for media speed adjustments.

NEW QUESTION # 60
Refer to the exhibit.
DNS queries from two internal DNS servers are being load-balanced to external DNS servers via a virtual server on a BIG-IP device. The DNS queries originate from:
192.168.10.100
192.168.10.200
and target:
192.168.2.150
All DNS queries destined for the external DNS servers fail.
Which property change should the BIG-IP Administrator make in the Virtual Server to resolve this issue?
(Choose one answer)

- A. Protocol profile (Client) to DNS_OPTIMIZED
- B. Type to Performance (HTTP)
- C. Source Address to 192.168.10.0/24
- D. Protocol to UDP

Answer: D

Explanation:
DNS traffic is primarily transported using UDP port 53. In the exhibit, the Virtual Server is configured with the Protocol set to TCP, which prevents standard DNS queries from being processed correctly. BIG-IP Virtual Servers must be configured with the correct Layer 4 protocol to match the application traffic they are handling.
According to the BIG-IP Administration: Data Plane Configuration documentation:
* The Protocol setting on a Virtual Server defines whether traffic is processed as TCP, UDP, or another supported transport protocol.
* Standard DNS queries and responses use UDP, while TCP is only required for DNS zone transfers (AXFR) or exceptionally large responses.
* When a DNS Virtual Server is incorrectly configured with TCP, UDP-based DNS queries are dropped, causing all requests to fail.
Why the other options are incorrect:
* A. Protocol profile (Client) to DNS_OPTIMIZEDA DNS profile enhances DNS functionality but does not correct an incorrect transport protocol configuration.
* B. Type to Performance (HTTP)Performance (HTTP) Virtual Servers are designed for HTTP traffic and are not suitable for DNS services.
* C. Source Address to 192.168.10.0/24The existing source IPs already fall within the allowed range, so this setting does not address the failure.
Correct Resolution:
Changing the Protocol to UDP aligns the Virtual Server with standard DNS transport requirements, allowing DNS queries to be successfully processed and load-balanced.

NEW QUESTION # 61
.....

www.pdfvce.com 】 open and search for （ F5CAB3 ） to download for free □F5CAB3 Hottest Certification

- BIG-IP Administration Data Plane Configuration Exam Questions - F5CAB3 Torrent Prep - F5CAB3 Test Guide □ Immediately open ⇛ www.testkingpass.com ⇚ and search for ➥ F5CAB3 □ to obtain a free download □F5CAB3 Latest Dumps Free
- Valid Study F5CAB3 Questions □ F5CAB3 Latest Dumps Free □ Reliable F5CAB3 Braindumps □ Search on ➡ www.pdfvce.com □□□ for " F5CAB3 " to obtain exam materials for free download □Valid Dumps F5CAB3 Pdf
- Prominent Features of {F5} F5 F5CAB3 Exam Questions ⤴ Search for □ F5CAB3 □ on ➢ www.troytecdumps.com □ immediately to obtain a free download □F5CAB3 Latest Test Report
- Pdf F5CAB3 Files □ New F5CAB3 Test Answers □ Pdf F5CAB3 Files □ Immediately open ➠ www.pdfvce.com □ □ and search for ▸ F5CAB3 ◂ to obtain a free download □F5CAB3 Latest Test Report
- Reliable F5CAB3 Braindumps □ Exam F5CAB3 Experience □ F5CAB3 Latest Test Cost □ Go to website □ www.pass4test.com □ open and search for ➥ F5CAB3 □ to download for free □F5CAB3 Hottest Certification
- F5CAB3 Dumps Save Your Money with Up to one year of Free Updates □ Go to website 「 www.pdfvce.com 」 open and search for □ F5CAB3 □ to download for free □F5CAB3 Valid Study Notes
- F5CAB3 Latest Test Cost □ Exam F5CAB3 Experience □ F5CAB3 Valid Dumps □ Search for ➽ F5CAB3 □ and download it for free immediately on □ www.testkingpass.com □ □F5CAB3 Reliable Test Forum
- myportal.utt.edu.tt, sanqizhi.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes