F5CAB5 Valid Test Format, Free F5CAB5 Download

Web-based F5CAB5 practice test of Lead2Passed is accessible from any place. You merely need an active internet connection to take this F5 F5CAB5 practice exam. Browsers including MS Edge, Internet Explorer, Safari, Opera, Chrome, and Firefox support this F5CAB5 Practice Exam. Additionally, this BIG-IP Administration Support and Troubleshooting (F5CAB5) test is supported by operating systems including Android, Mac, iOS, Windows, and Linux.

F5 F5CAB5 Exam Syllabus Topics:

Topic	Details
Topic 1	• Identify the reason a pool is not working as expected: This domain focuses on troubleshooting pools including health monitor failures, priority group membership, and configured versus availability status of pools and members.
Topic 2	• 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.
Topic 3	• Given a scenario, review basic stats to confirm functionality: This section involves interpreting traffic object statistics and network configuration statistics to validate system functionality.
Topic 4	• 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.

>> F5CAB5 Valid Test Format <<

Free F5CAB5 Download | Reliable F5CAB5 Exam Bootcamp

You will not only get familiar with the BIG-IP Administration Support and Troubleshooting (F5CAB5) exam environment but also

enhance your time management skills which will be quite helpful in the final F5CAB5 certification exam. The F5CAB5 desktop practice test software will install on your Windows-based computer and laptop. Very easy to install and provide a user-friendly interface to F5CAB5 Exam candidates. Whereas the F5CAB5 web-based practice test software is concerned, it is a browser-based application that works with all the latest browsers.

F5 BIG-IP Administration Support and Troubleshooting Sample Questions (Q22-Q27):

NEW QUESTION # 22
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. HTTP
- B. Statistics
- C. Request Adapt
- D. Analytics

Answer: D

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.

NEW QUESTION # 23
A BIG-IP Administrator receives reports from users that SSL connections to the BIG-IP device are failing.
Upon checking the log files, the administrator notices: SSL transaction (TPS) rate limit reached. stats show a maximum of 1200 client-side SSL TPS and 800 server-side SSL TPS. What is the minimum SSL license limit required to handle this peak?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

Explanation:
Troubleshooting failed SSL handshakes involves interpreting the resource limits defined by the system's license8888. The log message SSL transaction (TPS) rate limit reached indicates the BIG-IP is dropping SSL connections because it has exceeded its licensed "Transactions Per Second" capacity. When analyzing stats to determine the correct license level, the administrator must focus on "Client-side" SSL TPS. This represents the initial encrypted handshakes between users and the BIG-IP virtual servers91.
In this scenario, the peak client-side demand is 1200 TPS. While the 800 server-side transactions represent re-encryption toward the backend, F5's primary SSL TPS license limits typically apply to the client-facing side of the traffic flow.
Therefore, to resolve the intermittent connectivity issues and ensure the virtual server works reliably during peaks, the license must be upgraded to at least 1200 TPS949596969696.9798Confirming this peak via statistics andcomparing it to the current license is a standard troubleshooting step for SSL performance issues.

NEW QUESTION # 24

Refer to Exhibit:
An organization is reporting slow performance accessing their Intranet website, hosted in a public cloud. All employees use a single Proxy Server with the public IP of 104.219.110.168 to connect to the Internet. What should the BIG-IP Administrator of the Intranet website do to fix this issue?

- A. Change Source Address to 104.219.110.168/32
- B. Change Default Persistence Profile to cookie
- C. Change Fallback Persistence Profile to source_addr
- D. Change Load Balancing Method to Least Connection

Answer: B

Explanation:
This scenario describes a classic network performance issue known as the "Mega-Proxy" problem. When an organization routes all employee traffic through a single proxy server, the BIG-IP sees thousands of unique users as having the exact same source IP address. If the administrator has configured "Source Address Affinity" persistence, the BIG-IP will correctly follow the rule but incorrectly route all users to the same single backend pool member. This creates a severe load imbalance where one server is overwhelmed while others remain idle, leading to poor application response times. To resolve this, the administrator must change the persistence profile to "HTTP Cookie". Cookie-based persistence allows the BIG-IP to place a unique identifier in each user's browser, allowing the system to distinguish between individual sessions even if they share the same source IP. This fix ensures that traffic is distributed evenly across the pool members, restoring4 the expect5ed load balancing functionality and resolving the slow performance reported by users behind the corporate proxy.

NEW QUESTION # 25
Without decrypting, what portion of an HTTPS session is visible with a packet capture? (Choose one answer)

- A. HTTP Response Headers
- B. HTTP Request Headers
- C. Source IP Address
- D. Cookies

Answer: C

Explanation:
In an HTTPS session, the application-layer payload-including HTTP request headers, response headers, cookies, and body content-is encrypted using SSL/TLS. Without decrypting the traffic (for example, without SSL offloading on BIG-IP or access to the private keys), a packet capture cannot reveal any HTTP-level details.
However, network-layer and transport-layer information remains visible, even when encryption is used. This includes source and destination IP addresses, source and destination ports, TCP flags, sequence numbers, and TLS handshake metadata. Therefore, the source IP address (Option B) is visible in a packet capture of HTTPS traffic without decryption.
Options A, C, and D are incorrect because HTTP headers and cookies are part of the encrypted payload once HTTPS is established. BIG-IP troubleshooting documentation emphasizes this distinction when analyzing encrypted traffic flows using tcpdump, as administrators must rely on IP, port, and timing information unless SSL inspection or decryption is configured.

NEW QUESTION # 26
The BIG-IP appliance fails to boot. The BIG-IP Administrator needs to run the End User Diagnostics (EUD) utility to collect data to send to F5 Support. Where can the BIG-IP Administrator access this utility?

- A. External VLAN interface
- B. Console Port
- C. Management Port
- D. Internal VLAN interface

Answer: B

Explanation:
The End User Diagnostics (EUD) utility is a hardware-level testing suite used to verify the integrity of the physical components of a BIG-IP appliance.
* Access Requirements: Because the EUD must be run while the TMOS operating system is not loaded (typically when the device

cannot boot or requires hardware validation), it cannot be accessed via network-based interfaces like the Management Port or VLANs.
* Console Connection: The administrator must connect a terminal to the physical Console Port (using a serial cable) to interact with the boot menu.
* Execution Process: Upon restarting the appliance, the administrator must intercept the boot process at the GRUB menu and select the "End User Diagnostics" option. All output and menu selections are then handled through the serial console session.

NEW QUESTION # 27
......

If you try to get the BIG-IP Administration Support and Troubleshooting certification that you will find there are so many chances wait for you. You can get a better job; you can get more salary. But if you are trouble with the difficult of F5CAB5 exam, you can consider choose our F5CAB5 Exam Questions to improve your knowledge to pass F5CAB5 exam, which is your testimony of competence. Now we are going to introduce our F5CAB5 test guide to you, please read it carefully.