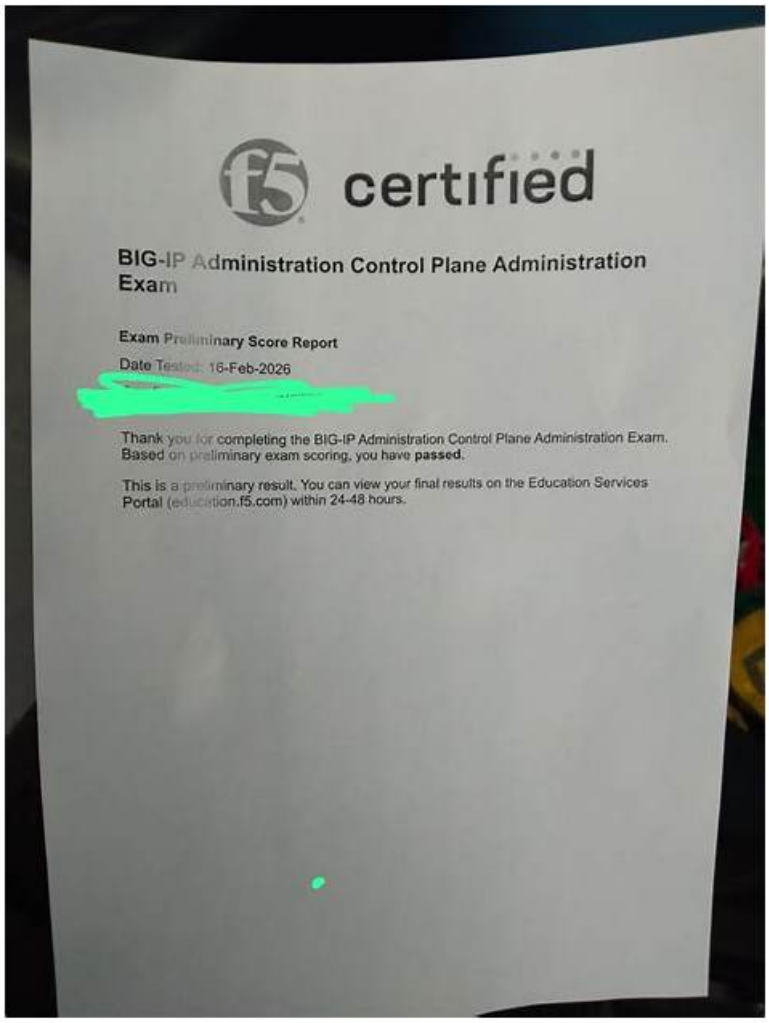
F5CAB4 - Latest BIG-IP Administration Control Plane Administration Latest Exam Tips



BTW, DOWNLOAD part of NewPassLeader F5CAB4 dumps from Cloud Storage: https://drive.google.com/open?id=1JlXq0CpW2WlXcPnzYQprSeaT0-oiuugk

You will also face your doubts and apprehensions related to the F5 BIG-IP Administration Control Plane Administration exam. Our F5 F5CAB4 practice test software is the most distinguished source for the F5 F5CAB4 Exam all over the world because it facilitates your practice in the practical form of the F5 F5CAB4 certification exam.

F5 F5CAB4 Exam Syllabus Topics:

Topic	Details
Topic 1	• Explain config sync: This section focuses on configuration synchronization procedures, identifying sync errors, determining sync necessity, checking sync status, and comparing configuration timestamps.
Topic 2	• Identify management connectivity configurations: This section focuses on understanding management access configurations, including management IP addresses, port lockdown settings, remote connectivity verification, and troubleshooting access issues.
Topic 3	• Apply procedural concepts required to create, manage, and restore a UCS archive: This domain covers UCS backup and restore procedures, understanding backup use cases, proper storage practices, and UCS file contents including private keys.

Topic 4	• Identify and report current device status: This domain covers monitoring BIG-IP operational status through LCD panels, dashboards, Network Map, GUI • TMSH commands, and checking high availability states.
Topic 5	• Explain authentication methods: This section focuses on user management including creating • modifying users, configuring remote authentication providers, and implementing group-based access control.
Topic 6	• Given a scenario, interpret Service status: This section teaches interpreting service states, analyzing netstat output, and determining whether services are listening on specific ports.
Topic 7	• Apply procedural concepts required to manage the state of a high availability pair: This domain covers controlling and monitoring failover states in high availability pairs, including forcing standby • offline modes, reporting failover status, and verifying device trust.

F5CAB4 Latest Braindumps Questions - F5CAB4 Popular Exams

We provide free demo for you to have a try before buying F5CAB4 exam braindumps. Free demo will help you have a better understanding of what you are going to buy, and we also recommend you try the free demo before buying. Moreover, F5CAB4 exam braindumps of us will offer you free update for one year, and you can get the latest version of the exam dumps if you choose us. And the update version for F5CAB4 Exam Dumps will be sent to your email automatically, and you just need to receive them.

F5 BIG-IP Administration Control Plane Administration Sample Questions (Q65-Q70):

NEW QUESTION # 65
New Syslog servers have been deployed in an organization. The BIG-IP Administrator must reconfigure the BIG-IP system to send log messages to these servers. In which location in the Configuration Utility can the BIG-IP Administrator make the needed configuration changes to accomplish this?

- A. System > Configuration > Device3
- B. System > Logs > Configuration
- C. System > Logs > Audit2
- D. System > Configuration > Local Traffic

Answer: B

Explanation:
Managing how a BIG-IP communicates with external management services like Syslog is a core Control Plane task. The Configuration Utility organizes these settings under the "System" menu. Specifically, to define remote logging destinations and formats, the administrator must navigate to System > Logs > Configuration to ensure the Control Plane correctly forwards system events to external collectors

NEW QUESTION # 66
A BIG-IP Administrator uses a device group to share the workload and needs to perform service on a BIG-IP device currently active for a traffic group. The administrator needs to enable the traffic group to run on another BIG-IP device in the device group. What should the administrator do to meet the requirement? (Choose one answer)

- A. Select Traffic Group on Primary Unit and then select Demote
- B. Create a new Traffic Group and then fail to Standby Unit
- C. Select Traffic Group and then select Force to Standby
- D. Select Traffic Group and then select Failover

Answer: D

Explanation:
Traffic Groups are the mechanism BIG-IP uses to control which device owns specific application traffic in a high-availability (HA) configuration. When maintenance is required on a device that is currently active for a traffic group, the correct and recommended action is to fail over that traffic group to another device in the device group.
* Failing over the traffic group moves ownership of that traffic group (and the virtual servers associated with it) to another available device without forcing the entire device into standby.
* This allows targeted maintenance while minimizing impact to other traffic groups that may still be active on the device.
Why the other options are incorrect:
* A is unnecessary and incorrect; traffic groups are not recreated for routine maintenance.
* C forces the entire device to standby, which may move more traffic than intended.
* D (Demote) affects device trust/priority behavior and is not the standard or recommended method for moving traffic group ownership.
Therefore, selecting the Traffic Group and choosing Failover is the correct solution.

NEW QUESTION # 67
Users report that traffic is negatively affected every time a BIG-IP device fails over. The traffic becomes stabilized after a few minutes. What should the BIG-IP Administrator do to reduce the impact of future failovers?

- A. Configure MAC Masquerade
- B. Enable Failover Multicast Configuration
- C. Set up Failover Method to HA Order
- D. Configure a global SNAT Listener

Answer: A

Explanation:
When a failover occurs, the newly active device must inform the surrounding network that it now "owns" the shared IP addresses. Without MAC Masquerade, the new device uses its own hardware MAC, requiring upstream routers to update their ARP tables (which causes a delay). MAC Masquerading allows the HA pair to share a "floating" MAC address, ensuring the Control Plane transition is transparent to the network layer

NEW QUESTION # 68
Administrative user accounts have been defined on the remote LDAP server and are unable to log in to the BIG-IP device.
Which log file should the BIG-IP Administrator check to find the related messages? (Choose one answer)

- A. /var/log/user.log
- B. /var/log/ltm
- C. /var/log/messages
- D. /var/log/secure

Answer: D

Explanation:
When BIG-IP is configured to use remote authentication (such as LDAP), all authentication and authorization attempts-including successes and failures-are logged to /var/log/secure.
For LDAP-based administrative login issues, /var/log/secure contains:
* LDAP authentication failures
* PAM authentication errors
* Authorization and access-denied messages
* Details explaining why a remote user could not log in
Why the other options are incorrect:
* /var/log/user.log is not a standard BIG-IP log file for authentication.
* /var/log/ltm logs traffic management events, not user authentication.
* /var/log/messages contains general system messages but not detailed authentication failure information.
Therefore, the correct log file to troubleshoot LDAP administrative login failures is /var/log/secure.

NEW QUESTION # 69

A BIG-IP Administrator wants to allow management access only from a specific subnet. Where should this be configured?

- A. Network > Routes
- B. System > Platform
- C. System > Users
- D. Network > Self IPs (Port Lockdown)

Answer: B

Explanation:
Management access security is a primary Control Plane configuration task3.
* Management Interface Security: The BIG-IP system provides a dedicated management port that is separate from the TMM (Traffic Management Microkernel) data interfaces4444.
* System Platform Settings: Under the System > Platform section of the Configuration Utility, an administrator can define specific IP addresses or subnets that are permitted to access the device via SSH or HTTPS (the GUI).
* Port Lockdown Difference: While "Port Lockdown" settings under Network > Self IPs control access to the device through self-IP addresses on data VLANs, they do not manage the security of the dedicated management port .
* Access Control Lists: For robust security, F5 recommends using the "IP Allow" or "httpd Allow" lists found in the platform settings to prevent malicious brute-force attempts or unauthorized access from non-management networks .

NEW QUESTION # 70
.....

id=1JlXq0CpW2WlXcPnzYQprSeaT0-oiuugk