F5CAB4 Free Dumps & Valid F5CAB4 Test Pdf


Score Report

certified

F5CAB4 - BIG-IP Administration Control Plane Administration

Exam Score Report

Date Tested: 12/10/2025
Candidate: [redacted]

Thank you for completing the F5CAB4 - BIG-IP Administration Control Plane Administration exam. Based on preliminary exam scoring, you have **Passed**.

This is a preliminary result. Your exam results can be found in the Education Services Portal within 24 hours.

Looking at the experiences of our loyal customers, you will find with the help of our excellent F5CAB4 exam questions, to achieve the desired certification is no long a unreached dream. And i believe that you will definitely be more determined to pass the F5CAB4 Exam. At the same time, you will also believe that our F5CAB4 learning questions can really help you. We can claim that as long as you study with our F5CAB4 praparation engine for 20 to 30 hours, you will pass the exam easily.

If you want to enjoy the real exam environment, the software version of our F5CAB4 exam questions will help you solve your problem, because the software version of our F5CAB4 test torrent can simulate the real exam environment. The F5CAB4 study materials from our company can help you get your certification easily, and if you use our F5CAB4 Study Materials, it will be very easy for you to save a lot of time, we believe our F5CAB4 learning guide will be the most suitable choice for you,

>> F5CAB4 Free Dumps <<

Marvelous F5CAB4 Free Dumps - Win Your F5 Certificate with Top Score

The F5 F5CAB4 practice tests have customizable time and F5CAB4 exam questions feature so that the students can set the time and F5CAB4 exam questions according to their needs. The F5 F5CAB4 practice test questions are getting updated on the daily basis and there are also up to 1 year of free updates. Earning the F5 F5CAB4 Certification Exam is the way to grow in the modern era with high-paying jobs. The 24/7 support system is available for the customers so that they can get the solution to every problem they face and pass BIG-IP Administration Control Plane Administration (F5CAB4) exam. You can also evaluate the F5CAB4 prep material with a free demo.

F5 F5CAB4 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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 3	• Identify configured system services: This domain covers verifying proper configuration of essential services including DNS, NTP, SNMP, and syslog.
Topic 4	• 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 5	• Explain config sync: This section focuses on configuration synchronization procedures, identifying sync errors, determining sync necessity, checking sync status, and comparing configuration timestamps.
Topic 6	• Explain authentication methods: This section focuses on user management including creating • modifying users, configuring remote authentication providers, and implementing group-based access control.

Topic 7	• Given a scenario, interpret Service status: This section teaches interpreting service states, analyzing netstat output, and determining whether services are listening on specific ports.

F5 BIG-IP Administration Control Plane Administration Sample Questions (Q49-Q54):

NEW QUESTION # 49
Which TMSH command initiates a manual configuration synchronization to the specified device group? (Choose one answer)

- A. tmsh load sys config to-group <device_group>
- B. tmsh modify sys failover auto-sync enable
- C. tmsh run cm config-sync to-group <device_group>
- D. tmsh run sys device-group update-config

Answer: C

Explanation:
Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents:
In a BIG-IP Device Service Cluster (DSC), manual configuration synchronization is performed using the ConfigSync framework.
The supported and documented command to manually push the local configuration to a specific device group is:
tmsh run cm config-sync to-group <device_group>
This command:
Initiates a one-time manual ConfigSync
Pushes the local device's configuration to all members of the specified device group Is commonly used when auto-sync is disabled or when the administrator wants explicit control over synchronization timing Why the other options are incorrect:
A is not a valid TMSH command for ConfigSync.
B enables auto-sync but does not perform an immediate synchronization.
D is not a valid or supported TMSH command for device group configuration synchronization.
Therefore, the correct command to manually synchronize configuration to a device group is C.

NEW QUESTION # 50
What is the tmsh command to list the IP ranges that can access the management interface via SSH?
(Choose one answer)

- A. tmsh list /sys sshd /etc/hosts.allow
- B. tmsh show /sys sshd /etc/hosts.allow
- C. tmsh list /sys sshd allow
- D. tmsh show /sys sshd allow

Answer: C

Explanation:
On BIG-IP systems, SSH access restrictions are configured under the /sys sshd object. The allow property defines the IP addresses or networks permitted to connect to the management interface using SSH.
* The list command is used to display the current configuration settings.
* Therefore, tmsh list /sys sshd allow correctly displays the configured allowed IP ranges.
Why the other options are incorrect:
* A (show) displays runtime or statistical information, not configuration values.
* C and D incorrectly reference /etc/hosts.allow; BIG-IP manages SSH access through TMSH objects, not by directly listing host files in this context.

NEW QUESTION # 51
A BIG-IP administrator is troubleshooting inconsistent configuration objects on devices in a device group. The administrator uses the command:
tmsh run /cm watch-devicegroup-device
and observes the following output:

devices <devgroup> device clu_id cl_orig cl_time last_sync
20:21 sync_test bigip_a 3273 bigip_a 14:27:00
20:21 sync_test bigip_b 1745 bigip_b 13:52:34 13:42:04
20:21 sync_test bigip_c 1745 bigip_a 13:52:34 13:42:04
What two conclusions can be made about this output? (Choose two answers)

- A. Two of the devices in the device group have a configuration that is out of date.
- B. bigip_a has the latest configuration.
- C. The correct configuration exists on bigip_a and bigip_c because their cluster times match.
- D. The config from bigip_c was synced to the other devices in the device group during the most recent ConfigSync.
- E. The correct configuration exists on bigip_b and bigip_c because their cluster times match.

Answer: A,B

Explanation:
Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents:
watch-devicegroup-device shows (among other columns) the commit ID (cid.id / shown here as clu_id), the originating device for that commit (cid-orig / shown here as cl_orig), and the time the configuration change was made (cid.time / shown here as cl_time). The highest/newest commit ID and its time represent the most recent configuration change seen among the devices. (clouddocs.f5.com) bigip_a has the latest configuration (A) because it shows commit ID 3273 at 14:27:00, which is newer than commit ID 1745 at 13:52:34 on bigip_b and bigip_c. (clouddocs.f5.com) Two devices are out of date (B) because bigip_b and bigip_c are still on the older commit ID 1745, so they do not match the latest commit shown on bigip_a. (clouddocs.f5.com) Why the other options are not supported by this output:
C is not supported: bigip_c is not showing a newer commit than the others; it's on the older commit (1745), so it's not the source of the most recent change. The output's cid-orig column is what tells you where the change was made. (clouddocs.f5.com) D/E are incorrect logic: matching cid.time between two devices only indicates they share the same change timestamp/commit, not that it is the correct or latest configuration. The "latest" is indicated by the newest commit ID/time (here, bigip_a). (clouddocs.f5.com)

NEW QUESTION # 52
A BIG-IP Administrator must determine if a Virtual Address is configured to fail over to the standby member of a device group. In which area of the Configuration Utility can this be confirmed?

- A. Device Management > Traffic Groups
- B. Local Traffic > Virtual Servers
- C. Device Management > Devices
- D. Device Management > Overview

Answer: B

Explanation:
Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: To re27port the current status of high availability for specific traffic, an administrator must verify the Traffic Group association28. In the Configuration Utility, Virtual Server properties include the Virtual Address settings where the 'Traffic Group' is assigned29292929. If the Virtual Address is assigned to a floating traffic group (like traffic-group-1), it is configured to fail over to the standby member30303030.

NEW QUESTION # 53
As an organization grows, more people have to log into the BIG-IP. Instead of adding more local users, the BIG-IP Administrator is asked to configure remote authentication against a central authentication server.
Which two types of remote server can be used here? (Choose two answers)

- A. OAUTH
- B. LDAP
- C. SAML
- D. RADIUS

Answer: B,D

Explanation:
Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents:

BIG-IP supports remote authentication by integrating with centralized authentication services through its AAA framework. The supported and commonly used remote authentication servers include:
LDAP (A)
Used to authenticate users against directory services such as Active Directory or other LDAP-compliant directories.
RADIUS (C)
Commonly used for centralized authentication, authorization, and accounting, especially in network and security environments.
Why the other options are incorrect:
OAUTH (B) is an authorization framework, not supported as a direct administrative authentication backend for BIG-IP management access.
SAML (D) is primarily used for single sign-on (SSO) in application authentication scenarios, not for BIG-IP administrative login authentication.
Thus, the correct remote authentication server types are LDAP and RADIUS.

NEW QUESTION # 54
.....