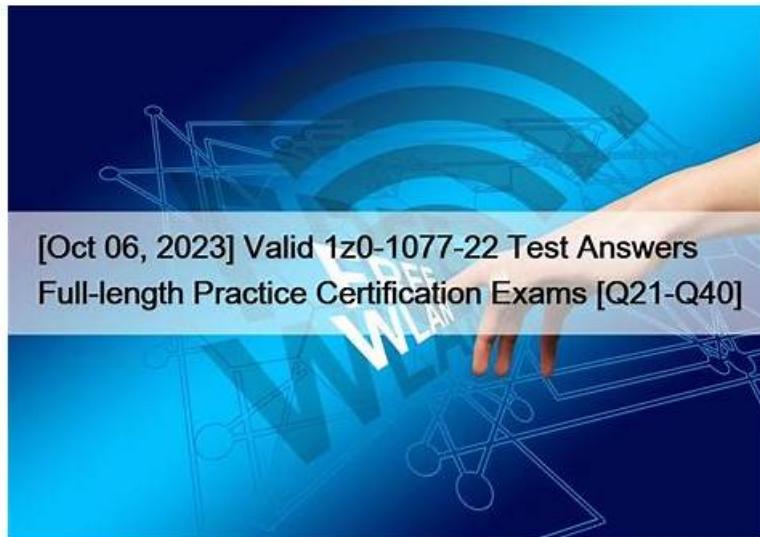


Certification F5CAB4 Cost, F5CAB4 Valid Practice Questions



The appropriate selection of F5CAB4 training is a guarantee of success. However, the choice is very important, FreeCram popularity is well known, there is no reason not to choose it. Of course, Give you the the perfect F5CAB4 training materials, if you do not fit this information that is still not effective. So before using FreeCram training materials, you can download some free questions and answers as a trial, so that you can do the most authentic exam preparation. This is why thousands of candidates depends FreeCram one of the important reason. We provide the best and most affordable, most complete F5CAB4 Exam Training materials to help them pass the exam.

F5 F5CAB4 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Identify and report current device status: This domain covers monitoring BIG-IP operational status through LCD panels, dashboards, Network Map, GUITMSH commands, and checking high availability states.
Topic 2	<ul style="list-style-type: none">Given a scenario, determine device upgrade eligibility: This domain covers determining appropriate timing for software and platform upgrades and strategies to minimize downtime during upgrades.
Topic 3	<ul style="list-style-type: none">Identify configured system services: This domain covers verifying proper configuration of essential services including DNS, NTP, SNMP, and syslog
Topic 4	<ul style="list-style-type: none">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	<ul style="list-style-type: none">List which log files could be used to find events and or hardware issues: This section teaches identification of key log files (var, log, ltm, secure, audit), understanding event severity levels, and interpreting log messages.
Topic 6	<ul style="list-style-type: none">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.

100% Pass Quiz 2026 F5 Efficient F5CAB4: Certification BIG-IP Administration Control Plane Administration Cost

The great advantage of our F5 F5CAB4 study prep is that we offer free updates for one year long. On one hand, these free updates can greatly spare your money since you have the right to free download BIG-IP Administration Control Plane Administration real dumps as long as you need to. On the other hand, we offer this after-sales service to all our customers to ensure that they have plenty of opportunities to successfully pass their F5CAB4 Actual Exam and finally get their desired certification of F5CAB4 practice materials.

F5 BIG-IP Administration Control Plane Administration Sample Questions (Q18-Q23):

NEW QUESTION # 18

When looking at this BIG-IP prompt: root@virtual-bigip1] Peer Time Out of Sync What does the message indicate? (Choose one answer)

- A. That one of the NTP sources has a skewed clock
- B. That the local time is correct, but the remote time is incorrect
- **C. That there was a time synchronization issue between the BIG-IP device and its peer**
- D. That the peer BIG-IP is unreachable for the device group

Answer: C

Explanation:

On BIG-IP systems that participate in a Device Service Cluster (DSC), each device compares the remote device's system time to its own system time. If the difference is outside the ConfigSync time threshold (commonly referenced as 3 seconds by default), BIG-IP updates the shell prompt to show "Peer Time Out of Sync", and ConfigSync operations may fail until time is corrected (typically by fixing NTP reachability

/configuration, or in some cases adjusting the threshold). (cdn.studio.f5.com) This message is specifically about time drift between peers in the trust domain/DSC-not basic reachability (so B is not what it means), and it does not prove which side is "correct" (so C is too specific). It also doesn't directly mean an NTP source is "skewed" (A can be a cause, but the prompt message itself indicates the peer- to-peer time mismatch condition). (cdn.studio.f5.com)

NEW QUESTION # 19

A BIG-IP Administrator plans to resolve a non-critical issue with a BIG-IP device in 2 weeks. What Severity level should be assigned to this type of F5 support ticket?

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

Answer: C

Explanation:

F5 Support uses a specific scale to categorize the urgency of technical issues, which helps the Control Plane management team prioritize resources effectively.

* Severity 1 (Critical): Used for emergency situations where a production site is completely down, or there is a critical impact on business operations with no workaround available.

* Severity 2 (High): Assigned when a system is severely degraded, or a primary function is significantly impacted, but the site remains operational in a degraded state.

* Severity 3 (Medium): Applicable for issues where there is a partial loss of non-critical functionality, or the system is failing intermittently but the core business is not currently impacted.

* Severity 4 (Low): This is the appropriate level for non-critical issues, general "how-to" questions, or maintenance planning. Since the administrator plans to resolve this issue in two weeks, it falls under the category of a low-priority maintenance task that does not require an immediate response from F5 support.

NEW QUESTION # 20

Which command will provide the BIG-IP Administrator with the current device HA status? (Choose one answer)

- A. list /cm failover
- B. show /sys failover
- C. **show /cm failover-status**

Answer: C

Explanation:

To determine the current failover (HA) status of a BIG-IP system using tmsh, F5 documentation explicitly states that the administrator should use the following command:

show /cm failover-status

This command displays:

The current failover state (active, standby, or offline)

Detailed failover status information

The operational HA condition of the device within a device group

According to F5 Knowledge Base Article K08452454, the documented procedure for checking failover status is:

Log in to the TMOS Shell (tmsh)

Run show /cm failover-status

Why the other options are incorrect:

A). list /cm failover shows configuration settings, not operational HA status.

B). show /sys failover is not the documented command for checking current failover status and does not align with F5's recommended procedure.

NEW QUESTION # 21

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

Answer: A,C

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 # 22

The BIG-IP Administrator suspects unauthorized SSH login attempts on the BIG-IP system

Which log file would contain details of these attempts? (Choose one answer)

- A. /var/log/messages

- B. /var/log/audit
- C. /var/log/ltm
- D. /var/log/secure

Answer: D

Explanation:

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

On BIG-IP systems, authentication and authorization events are logged in `/var/log/secure`. This includes:

Successful and failed SSH login attempts

Invalid user authentication attempts

PAM (Pluggable Authentication Module) authentication failures

Access denials related to secure services

Why the other options are incorrect:

/var/log/messages contains general system messages and service events, not detailed authentication failures.

/var/log/audit records administrative configuration changes (who changed what and when), not login attempts.

/var/log/ltm logs traffic-management (TMM) and application-related events.

Therefore, the correct log file for investigating unauthorized SSH login attempts is `/var/log/secure`.

NEW QUESTION # 23

Provided you get the certificate this time with our F5CAB4 training guide, you may have striving and excellent friends and promising colleagues just like you. It is also as obvious magnifications of your major ability of profession, so F5CAB4 Learning Materials may bring underlying influences with positive effects. The promotion or acceptance of our F5CAB4 exam questions will be easy. So it is quite rewarding investment.

F5CAB4 Valid Practice Questions: <https://www.freecram.com/F5-certification/F5CAB4-exam-dumps.html>

