



F5 Networks F5CAB4 Practice Questions

Shared by Noel on 09-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

A BIG-IP Administrator needs to view the CPU utilization of a particular Virtual Server. Which section of the Configuration Utility should the administrator use for this purpose?

Options:

- A- Statistics > Module Statistics > Local Traffic > Virtual Addresses
- B- Statistics > Module Statistics > Traffic Summary1
- C- Statistics > Analytics > Process CPU Utilization234
- D- Statistics > Module Statistics > Local Traffic > Virtual Servers567

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: Monitoring specific object health is a core function of the Control Plane. While the dashboard provides a global overview, granular performance data---such as the CPU overhead a specific Virtual Server is placing on the Traffic Management Microkernel (TMM)---is found under the Module Statistics. Navigating to Statistics > Module Statistics > Local Traffic > Virtual Servers allows an administrator to report on the current status and resource consumption of individual traffic objects.

Question 2

Question Type: MultipleChoice

What are the recommended methods for forcing a BIG-IP system to standby mode? (Select two answers)

Options:

- A- Active BIG-IP: CLI > tmsh run /sys failover device standby
- B- Active BIG-IP: Configuration Utility > Device Management > Devices > Local Device (Self) > Force to Standby

C- Active BIG-IP: Configuration Utility > Device Management > Traffic Groups > Local Device (Self) > Force to Standby

D- Active BIG-IP: CLI > tmsh run /sys failover standby

Answer:

A, B

Explanation:

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

BIG-IP provides two supported and documented methods to manually force a device into standby state in a high-availability (HA) configuration:

CLI method (A):

```
tmsh run /sys failover device standby
```

This is the correct and supported TMSH command to force the local device to transition from active to standby.

Configuration Utility method (B):

Navigating to Device Management > Devices > Local Device (Self) and selecting Force to Standby performs the same operation through the GUI and is fully supported.

Why the other options are incorrect:

C is incorrect: Traffic Groups do not provide a "Force to Standby" option for the local device; traffic groups are used to manage which device owns specific traffic, not to force device-level failover.

D is incorrect: tmsh run /sys failover standby is not a valid TMSH command. The correct syntax requires device standby.

Thus, the correct answers are A and B.

Question 3

Question Type: MultipleChoice

Which method is recommended for creating a new user from the CLI? (Choose one answer)

Options:

- A- Run tmsh create auth user username prompt-for-password from bash
- B- Edit bigip.conf to add the new user and the user's clear-text password
- C- Run f5adduser 'username' then f5passwd username from bash or tmsh
- D- Run useradd 'username' then passwd username from bash or tmsh

Answer:

A

Explanation:

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

The recommended and supported method for creating BIG-IP users from the CLI is through TMSH, using the authentication subsystem.

tmsh create auth user <username> prompt-for-password:

Properly creates the user within BIG-IP's AAA/authentication framework

Encrypts the password securely

Ensures the user is stored and managed correctly in the BIG-IP configuration database

Is fully supported and documented

Why the other options are incorrect:

B is unsafe and unsupported because editing bigip.conf directly and storing clear-text passwords violates security and configuration management best practices.

C (f5adduser / f5passwd) is deprecated and not recommended for modern BIG-IP versions.

D creates a Linux system user only, not a BIG-IP administrative user, and will not allow access to the Configuration Utility or TMSH roles.

Question 4

Question Type: MultipleChoice

A BIG-IP Administrator needs to fall over the active device. The administrator logs into the Configuration Utility and navigates to Device Management > Traffic Group. However, "Force to Standby" is greyed out. What is causing this issue?

Options:

- A- The BIG-IP Administrator is NOT logged into command line to tail over
- B- The BIG-IP Administrator is on the Standby Device
- C- The BIG-IP Administrator is logged in as root
- D- The BIG-IP Administrator is logged in as administrator

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: In a High Availability pair, the 'Force to Standby' action is a Control Plane command used to trigger a manual failover. This option is only logical and available on the device that is currently in the Active state. If the button is greyed out, it indicates that the administrator is already logged into the Standby unit, which has no active traffic groups to relinquish.

Question 5

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

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 assigned292929. 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.

Question 6

Question Type: MultipleChoice

One of the two members of a device group has been decommissioned. The BIG-IP Administrator tries to delete the device group, but is unsuccessful. Prior to removing the device group, which action should be performed?

Options:

- A- Disable the device group
- B- Remove all members from the device group
- C- Remove the decommissioned device from the device group
- D- Make sure all members of the device group are in sync

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: To maintain integrity in a High Availability environment, TMOS prevents the deletion of active Devic28e Groups. Procedurally, a device group is a container for synchronization; the Control Plane requires that you first strip the group of all associated members (devices) before the group object itself can be removed from the configuration.

Question 7

Question Type: MultipleChoice

Which log file should the BIG-IP Administrator check to determine if a specific user tried to log in to the BIG-IP Configuration Utility? (Choose one answer)

Options:

- A- /var/log/pam/tallylog
- B- /var/log/secure
- C- /var/log/ltn
- D- /var/log/httpd

Answer:

B

Explanation:

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

On BIG-IP systems, all authentication attempts for administrative access---including logins to the Configuration Utility (GUI)---are logged in /var/log/secure. This log file records:

Successful and failed login attempts

The username used

The authentication method (local, LDAP, RADIUS, etc.)

Access denials and PAM authentication errors

Why the other options are incorrect:

/var/log/pam/tallylog tracks account lockouts and failed attempt counters, not detailed login attempts.

/var/log/ltn logs traffic management events, not administrative authentication.

/var/log/httpd logs web server activity but does not record authentication success or failure for BIG-IP administrative users.

Therefore, the correct log file to verify whether a user attempted to log in to the BIG-IP Configuration Utility is /var/log/secure.

=====

Question 8

Question Type: MultipleChoice

Users are unable to reach an application. The BIG-IP Administrator checks the Configuration Utility and observes that the Virtual Server has a red diamond in front of the status.

What is causing this issue? (Choose one answer)

Options:

- A- The Virtual Server is receiving HTTPS traffic over an HTTP virtual
- B- All pool members are down
- C- All pool members have been disabled
- D- The Virtual Server is disabled

Answer:

D

Explanation:

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

In the BIG-IP Configuration Utility, status icons provide immediate health information. A red diamond specifically indicates that the object itself is administratively disabled. When a virtual server is disabled, BIG-IP will not accept or process traffic for that virtual server, regardless of pool or node state.

If all pool members were down, the virtual server would typically show a yellow triangle (available but no resources).

If all pool members were disabled, the virtual server would usually still be enabled but unavailable due to pool status, not shown as a red diamond.

Protocol mismatch (HTTPS sent to HTTP) does not change the administrative status icon of the virtual server.

Therefore, the red diamond clearly indicates the virtual server is disabled, making D the correct answer.

Question 9

Question Type: MultipleChoice

The BIG-IP Administrator generates a qkview using "qkview -s0" and needs to transfer the output file via SCP. Which directory contains the output file?

Options:

- A- /var/log
- B- /var/tmp
- C- /var/local
- D- /var/config

P2P
exams

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: A QKView is a comprehensive snapshot of the device's Control Plane state, configuration, and logs used for troubleshooting. By default, the qkview utility stores its generated output file in the /var/tmp/ directory. Administrators must know this path to retrieve the file for upload to F5 iHealth or Support.

Question 10

Question Type: MultipleChoice

An LTM device has a virtual server mapped to www.f5.com. Users report that when they connect to /resources/201.1.2h.l_l.com they are unable to receive content. What is the likely cause of the issue?

Options:

- A- The pool associated with the virtual server does not have priority group activation enabled.
- B- The virtual address does not have ARP enabled.
- C- The virtual address does not have route advertising enabled.
- D- The pool associated with the virtual server is failing its health check.

P2P
exams

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: The Control Plane is responsible for ARP (Address Resolution Protocol) management for Virtual Addresses. For a Virtual Server to be reachable, the BIG-IP must respond to ARP requests for that IP. If the 'ARP' setting is disabled on the Virtual Address properties, upstream routers cannot resolve the MAC address of the BIG-IP, leading to connectivity failure even if the service itself is 'Available.'



To Get Premium Files for F5CAB4 Visit

<https://www.p2pexams.com/products/f5cab4>

For More Free Questions Visit

<https://www.p2pexams.com/f5-networks/pdf/f5cab4>

20%
DISCOUNT

P2P
exams