



CertsMania

Free Questions for F5CAB4

Shared by **Brielle** on **Jan 22, 2026**

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

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)

Options:

A.

/var/log/messages

B.

/var/log/secure

C.

/var/log/audit

D.

/var/log/ltn



CertsMania

Answer

B

Explanation

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**.

=====



CertsMania

Questions # 2:

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



CertsMania

Answer

B

Explanation

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.

Questions # 3:

A BIG-IP Administrator runs the initial configuration wizard and learns that the **NTP servers were invalid**.

In which area of the **Configuration Utility** should the BIG-IP Administrator update the list of configured NTP servers? (Choose one answer)

Options:

A.

System > Platform

B.

System > Preferences

C.

System > Services

D.

System > Configuration

Answer

D

Explanation

On a BIG-IP system, **NTP (Network Time Protocol) configuration** is part of the **system-level configuration settings**. In the Configuration Utility, NTP servers are configured under the **System configuration hierarchy**.

The correct navigation path is:

System > Configuration > Device > NTP

This location allows the administrator to:

Add, modify, or remove NTP servers

Ensure accurate system time synchronization

Maintain proper time alignment required for features such as **ConfigSync, HA**

failover, logging, and certificate validation

Why the other options are incorrect:

A. System > Platform is used for hardware-related settings.

B. System > Preferences manages UI and user preferences.

C. System > Services controls system daemons and services, not time configuration.

Therefore, the correct answer is **D. System > Configuration**.

=====

Questions # 4:

A BIG-IP Administrator is setting up a new BIG-IP device. The network administrator reports that the interface has an incompatible media speed. The BIG-IP Administrator needs to change this setting manually. From which location should the BIG-IP Administrator perform this task?¹⁴

Options:

A.

On the Front Console¹⁵

B.

In the TMOS Shell Command line¹⁶

C.

In the Configuration Utility, Network > Interface¹⁷

D.

In the Configuration Utility, System > Configuration¹⁸

Answer

C

Explanation

Comprehensive and Detailed Explanation From BIG-IP Administration20 Control Plane Administration documents: Connectivity management involves ensuring that the physical layer matches the networking environment. Interface properties, including media speed, duplex settings, and MTU, are managed at the Control Plane level under the Network menu. To resolve a mismatch with an upstream switch, the administrator must navigate to Network > Interfaces to manually override auto-negotiation settings.

Questions # 5:

A BIG-IP Administrator is unable to connect to the management interface via HTTPS. What is a possible reason for this issue?

Options:

A.

The port lockdown setting is configured to Allow None.

B.

An incorrect management route is specified.

C.

The IP address of the device used to access the management interface is NOT included in the "P Allow" list in the Configuration Utility.

D.

The IP address of the device used to access the management interface is NOT included in the "httpd Allow" list in the CLI.

Answer

D

Explanation

Management connectivity is protected by an allowed access list for the httpd daemon. Unlike TMM data ports which use 'Port Lockdown' settings, the management port's access is controlled by a specific 'Allow' list. If an administrator's IP is not explicitly included in this list, the Control Plane will reject HTTPS connection attempts to the management utility.

Questions # 6:

A BIG-IP Administrator needs to determine **who changed a Virtual Server configuration**.

In which log file would the BIG-IP Administrator find this data? (Choose one answer)

Options:

A.

/var/log/audit

B.

/var/log/secure

C.

/var/log/ltn

Answer

A

Explanation

The **audit log** (/var/log/audit) records **configuration changes** made on the BIG-IP system, including:

Who made the change (user account)

What was changed (for example, a virtual server modification)

When the change occurred

How it was performed (GUI, TMSH, or API)

Why the other options are incorrect:

/var/log/secure logs authentication events such as login successes and failures, not configuration changes.

/var/log/ltn logs traffic-management and runtime LTM events, not administrative configuration modifications.

Therefore, the correct log file for tracking **who changed a virtual server** is **/var/log/audit**.

Questions # 7:

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? (Choose one answer)

Options:

A.

System > Configuration > Local Traffic

B.

System > Logs > Configuration

C.

System > Logs > Audit

D.

System > Configuration > Device

Answer

B

Explanation

On a BIG-IP system, **remote syslog server configuration** is managed through the logging configuration framework. In the Configuration Utility, this is accessed via:

System > Logs > Configuration

This section allows the administrator to:

Define **remote syslog destinations**

Configure **log publishers**

Control which log types (system, audit, LTM, ASM, etc.) are forwarded to external syslog servers

Why the other options are incorrect:

A. System > Configuration > Local Traffic Used for traffic management settings, not logging.

C. System > Logs > Audit Displays audit log settings and content but does not configure remote syslog destinations.

D. System > Configuration > Device Used for device-level settings such as hostname and platform configuration, not logging.

Therefore, the correct location to reconfigure BIG-IP to send logs to new syslog servers is **System > Logs > Configuration**.

=====

Questions # 8:

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

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.

Questions # 9:

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)

Options:

A.

Create a new Traffic Group and then fail to Standby Unit

B.

Select Traffic Group and then select Failover

C.

Select Traffic Group and then select Force to Standby

D.

Select Traffic Group on Primary Unit and then select Demote

Answer

B

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.

Questions # 10:

The BIG-IP system is provisioned for **LTM only**. The BIG-IP Administrator is tasked with **provisioning ASM**.

What process restarts when the BIG-IP Administrator changes the module provisioning?
(Choose one answer)

Options:

A.

bd

B.

tmm

C.

sshd

○ D.

httpd

Answer

B

Explanation

When a BIG-IP Administrator changes **module provisioning** (for example, enabling **ASM** on a system previously provisioned only for **LTM**), the BIG-IP system must restart the **Traffic Management Microkernel (TMM)** process.

The **TMM process** is responsible for:

Traffic handling

LTM, ASM, and other traffic-processing modules

Enforcing security and application policies

Provisioning changes affect how traffic modules are loaded and integrated into TMM. As a result, **TMM is restarted**, which causes a **temporary interruption of traffic processing**. This is expected behavior and is why module provisioning changes should be planned during a **maintenance window**.

Why the other options are incorrect:

A. bd is related to blade/platform management, not module provisioning.

C. sshd handles SSH access and is not affected by provisioning changes.

D. httpd supports the Configuration Utility (GUI) and does not restart due to module provisioning.

Therefore, the correct answer is **B. tmm**.

=====

To Get Premium Files for F5CAB4 Visit

<https://www.certsmania.com/f5/f5cab4-practice>

For More Free Questions Visit

<https://www.certsmania.com/f5/pdf/f5cab4>



CertsMania