Download F5 Networks F5CAB4 Exam Dumps Free

Shared by Beard on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A BIG-IP Administrator is conducting maintenance on one BIG-IP appliance in an HA Pair. Why should the BIG-IP Administrator put the appliance into FORCED_OFFLINE state?

Options:

A- To preserve existing connections to Virtual Servers and reduce the CPU load
B- To allow new connections to Virtual Servers and ensure the appliance becomes active
C- To terminate connections to the management IP and decrease persistent connections
D- To terminate existing connections to Virtual Servers and prevent the appliance from becoming active

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Con10trol Plane Administration documents: Placing a device in the FORCED_OFFLINE state is a critical procedural concept for HA maintenance111213. 1415Unlike simply being 'Standby16', the FORCED_OFFLINE state ensures tha17t the Control Plane will not participate in failover selection, effectively preventing the device from becoming 'Active' even if the peer fails18. This state also allows the administrator to terminate existing connections to ensure no traffic is being processed during the maintenance window19.

Question 2

Question Type: MultipleChoice

A configuration change is made on the standby member of a device group. What is displayed as "Recommended Action" on the Device Management Overview screen?

Options:

A- Force active member of device group to standby

B- Activate device with the most recent configuration
C- Synchronize the active member configuration to the group.
D- Synchronize the standby member configuration to the group

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: The BIG-IP Control Plane monitors the 'Commit ID' of the configuration on all group members. When a change is made on the Standby unit, it becomes the member with the most recent configuration. The 'Recommended Action' in the HA status dashboard will be to synchronize that specific device's configuration to the rest of the group to ensure consistency

Question 3

Question Type: MultipleChoice

When looking at this BIG-IP prompt: root@virtual-bigip1] Peer Time Out of Sync

What does the message indicate? (Choose one answer)

Options:

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

Answer:

D

Explanation:

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

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)

Question 4

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

Explanation:

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

Question 5

Question Type: MultipleChoice

The BIG-IP appliance fails to boot. The BIG-IP Administrator needs to run the End User Diagnostics (EUD) utility to collect data to send to F5 Support. Where can the BIG-IP Administrator access this utility?

Options:

A- Console Port
B- Internal VLAN interface
C- External VLAN interface
D- Management Port

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: The EUD is a 33hardware-level diagnostic tool that runs outside of the TMOS operating system. Because it is used when the system cannot boot or is in a pre-boot state, it cannot be accessed via the GUI or management network. The administrator must connect physically via the serial Console Port to interact with the boot menu and initiate the hardware tests.

Question 6

Question Type: MultipleChoice

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

Options:

A- list /cm failover
B- show /sys failover

C- show /cm failover-status

Answer:

C

Explanation:

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

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.

Question 7

Question Type: MultipleChoice

In Which option best log files would log events pertaining to pool members being marked ''UP'' or ''DOWN'' by their Health Monitors be written? (Choose one answer)

Options:

A- /var/log/audit
B- /var/log/ltm
C- /var/log/secure
D- /var/log/monitors

Answer:

B

Explanation:

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

On BIG-IP systems, Local Traffic Manager (LTM) is responsible for:

Pool and pool member management

Health monitor execution

Marking pool members UP or DOWN based on monitor results

Events related to health monitor status changes, including when pool members transition between UP and DOWN, are logged in /var/log/ltm.

Why the other options are incorrect:

/var/log/audit records administrative configuration changes, not runtime health status.

/var/log/secure logs authentication and authorization events.

/var/log/monitors is not a standard BIG-IP log file.

Therefore, the correct log file for pool member health monitor status events is /var/log/ltm.

==========

Question 8

Question Type: MultipleChoice

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)

Options:

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.

Question 9

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? (Choose one answer)

Options:

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

Answer:

C

Explanation:

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

A BIG-IP device group cannot be deleted if it still contains device members, even if one of those devices has already been decommissioned or is unreachable. Before deleting the device group, the administrator must explicitly remove the decommissioned device from the device group configuration.

Once the removed or unreachable device is deleted from the device group membership, the BIG-IP system allows the remaining administrator to successfully delete the device group.

Why the other options are incorrect:

A . Remove all members from the device group

This is not required; the key requirement is removing the decommissioned device, not all members.

B . Make sure all members are in sync

Synchronization status does not prevent device group deletion.

D . Disable the device group

Device groups cannot be disabled; they must be modified or deleted.

Therefore, the correct prerequisite action is to remove the decommissioned device from the device group, making C the correct answer.

==========

Question 10

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 > Devices34
C- Local Traffic > Virtual Servers35
D- Device Management > Overview36

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration do38cuments: While HA state is managed under 'Device Management,' the specific failover behavior of a traffic object is linked to its configuration. A Virtual Address must be associated with a 'Traffic Group' (usually traffic-group-1) to fail over. This association and the resulting floating status can be verified by viewing the Virtual Server or Virtual Address list under Local Traffic > Virtual Servers.

Question 11

Question Type: MultipleChoice

A BIG-IP Administrator needs to restore a UCS file to an F5 device using the Configuration Utility. Which section of the Configuration Utility should the BIG-IP Administrator access to perform this task?

Options:

A- Local Traffic > Virtual Servers
B- Local Traffic > Policies
C- System > Archives
D- System > Configuration

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Control Plane Administration documents: Managing the state of a device often involves restoring configuration backups known as User Configuration Set (UCS) files These archives contain the full system configuration, including licenses and SSL certificates. The Control Plane provides a dedicated management area for these files under System > Archives, where administrators can upload, create, and restore configuration snapshots