F5 Networks

F5CAB4 Exam

BIG-IP Administration Control Plane Administration

Questions & Answers
Demo

Version: 4.0

Question: 1

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 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: 2

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. bigip_a has the latest configuration.

B. Two of the devices in the device group have a configuration that is out of date.

C. The config from bigip_c was synced to the other devices in the device group during the most recent ConfigSync.

D. The correct configuration exists on bigip_b and bigip_c because their cluster times match.

E. The correct configuration exists on bigip_a 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)

Question: 3

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)

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: 4

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

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: 5

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

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.