DUMPSBOSS.

BIG-IP Administration Control Plane Administration () exam

F5 F5CAB4

Version Demo

Total Demo Questions: 8

Total Premium Questions: 88

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A BIG-IP system does not have Internet access and must be licensed by using the manual activation process.

Which two actions are required to complete manual license activation? (Choose two answers)

A. Generate a license dossier from the BIG-IP system

B. Install the license file returned by the F5 licensing service

C. Create a UCS archive and upload it to the F5 licensing service

D. Synchronize the license from a peer device through ConfigSync

E. Install a BIG-IP software image before submitting a dossier

ANSWER: A B

Explanation:

Manual activation requires the administrator to generate a license dossier from the BIG-IP system and submit that dossier to the F5 licensing service by using a system with Internet access. F5 returns a license file, which the administrator then installs on the BIG-IP system to complete activation.

Creating a UCS archive does not activate a license, and a software-image installation does not provide a license dossier or license file. ConfigSync is also unrelated to licensing and should not be used to distribute a device license.

QUESTION NO: 2

A BIG-IP Administrator has created a Self IP on an administrative VLAN. Administrators must be able to use SSH and the Configuration Utility through this Self IP, but no other management services should be exposed on that address.

Which configuration should the administrator use? (Choose one answer)

A. Set Port Lockdown to Allow Custom and allow TCP ports 22 and 443

B. Set Port Lockdown to Allow Default

C. Configure a management route for the administrative VLAN

D. Assign the Self IP to a new traffic group

ANSWER: A

Explanation:

The administrator should configure the Self IP **Port Lockdown** setting to **Allow Custom** and allow only the required services, such as TCP port 22 for SSH and TCP port 443 for HTTPS. Port Lockdown controls which services can be reached through a Self IP address.

The management-port SSH allow list applies to the dedicated management interface and does not by itself control services exposed through a traffic VLAN Self IP. A traffic group controls floating ownership and failover behavior, not service access permissions.

QUESTION NO: 3

A BIG-IP Administrator needs to export system configuration for migration purposes. Which file type should be used?

A. SCF

B. QKView

C. UCS

D. ISO

ANSWER: C

Explanation:

UCS is the appropriate file type for exporting a BIG-IP system configuration for migration. A User Configuration Set archive, typically saved with a `.ucs` extension, packages the BIG-IP configuration and important associated system files into one portable archive. Administrators create it with `tmsh save /sys ucs` and can transfer it to another BIG-IP system for restoration with `tmsh load /sys ucs`. This makes UCS the standard mechanism for moving an existing configuration to replacement hardware or another compatible BIG-IP instance while retaining the configuration elements needed to re-create the system's operational state. Depending on the migration scenario, administrators should still review platform-specific settings, network interface mappings, licenses, and the destination version before loading the archive. F5 documents UCS archives as the mechanism to save and restore BIG-IP configuration data and associated files; this is distinct from a diagnostic collection or installation image. For guidance on managing archives in the BIG-IP Configuration utility and from the command line, see the F5 tmsh sys ucs reference. F5 migration documentation also describes creating and loading UCS archives when transferring a configuration between BIG-IP systems: K12278: Transferring a UCS archive to a different BIG-IP system.

QUESTION NO: 4

A BIG-IP Administrator plans to perform maintenance on the active device in a synchronized active/standby pair. The administrator wants the peer device to continue handling traffic during the maintenance activity.

Which two actions should the administrator perform before taking the active device out of service? (Choose two answers)

A. Verify that the peer device is healthy and the device group is In Sync

B. Force the active device to standby

C. Force the standby device offline

D. Delete the traffic group from the active device

E. Reboot both devices at the same time

ANSWER: A B

Explanation:

The administrator should first **verify that the peer device is healthy and that the device group is In Sync**. This confirms that the standby device has a current configuration and is available to assume ownership of the traffic groups.

The administrator should then **force the active device to standby**. This initiates a controlled failover so that the peer can become active before maintenance begins. Rebooting the active device without confirming synchronization can create avoidable risk, while forcing the healthy standby device offline would remove the intended failover target.

QUESTION NO: 5

What can the BIG-IP Administrator do when restoring BIG-IP configuration files with a UCS archive? (Choose two answers)

A. The BIG-IP Administrator can only restore the UCS archive to the same system from which it was saved.

B. The BIG-IP Administrator can restore a UCS archive on a BIG-IP system running a later software version than the version of software the UCS archive was created on.

C. The BIG-IP Administrator can restore a UCS archive on a BIG-IP system on a different platform.

D. The BIG-IP Administrator can only restore a UCS archive on a BIG-IP system running the same version.

ANSWER: B C

Explanation:

A UCS archive packages BIG-IP configuration data and related system files so that an administrator can restore a saved configuration during recovery, replacement, upgrade, or migration work. A UCS created on an earlier TMOS release can be loaded on a system running a later compatible TMOS release. During the load, BIG-IP processes the configuration using the target release's configuration format, which supports the normal upgrade path from an older release to a newer one. Administrators should still validate the restored configuration, licenses, provisioning, and feature support after an upgrade because the target system's software capabilities determine what can run.

A UCS can also be restored to a different BIG-IP platform. This supports scenarios such as replacing an appliance, moving between hardware models, or migrating to a BIG-IP Virtual Edition deployment. For a cross-platform migration, F5 documents use of the `platform-migrate` option when loading the UCS. This omits platform-specific files that should not be transferred and allows the destination system to retain its own platform identity and relevant local settings. The archive is therefore portable when the restore procedure and migration options are selected appropriately. See F5's tmsh sys ucs reference and BIG-IP UCS restore documentation.

QUESTION NO: 6

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

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:

The IP address of the device used to access the management interface is NOT included in the " httpd Allow " list in the CLI. BIG-IP serves the Configuration utility's HTTPS management interface through the `httpd` service. The `sys httpd allow` setting is an access-control list that limits which source IP addresses or networks may establish connections to that service. Therefore, when the administrator's workstation address is absent from the configured allow list, its HTTPS request to the management IP can be rejected even when the device, management IP address, and HTTPS service are otherwise reachable. An administrator can inspect the active setting with `tmsh list sys httpd allow` and, where authorized, update it to include the required trusted host or subnet. Care is required when changing this setting remotely: the current administration host should be retained in the list so the active management session is not unintentionally blocked. F5 documents the `allow` property and its role in restricting access to the HTTPD service in the tmsh sys httpd reference. Additional management-plane security context is available in the F5 security training documentation.

QUESTION NO: 7

A BIG-IP Administrator is reviewing a sync-failover device group before initiating ConfigSync. Which two settings are device-specific and are not synchronized between members through ConfigSync? (Choose two answers)

A. The device hostname

B. The management IP address

C. A virtual server configuration

D. A pool configuration

E. An iRule assigned to a virtual server

ANSWER: A B

Explanation:

The device hostname and the management IP address are device-specific settings. Each BIG-IP device requires its own identity and dedicated management connectivity, so these values are maintained locally rather than synchronized through a device group.

ConfigSync is intended to synchronize shared configuration objects, such as virtual servers, pools, and many traffic-management settings. Synchronizing a hostname or management IP address would cause an operational conflict between devices in the device service cluster.

QUESTION NO: 8

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)

A. /var/log/pam/tallylog

B. /var/log/secure

C. /var/log/ltm

D. /var/log/httpd

ANSWER: B

Explanation:

/var/log/secure is the appropriate log to review because BIG-IP records administrative authentication activity through the system authentication and authorization services in this file. This includes attempts to authenticate to the BIG-IP management interfaces, such as the Configuration Utility, and commonly provides details needed to investigate a particular user's activity: the user name, authentication result, source information where available, and relevant authentication-service messages. An administrator can search this file for the user name or for authentication-related events to establish whether an attempt occurred and assess its outcome. On BIG-IP, this is also the central log that is useful when correlating local authentication with external authentication configurations, such as LDAP, Active Directory, RADIUS, or TACACS+. F5 documents the system log locations and identifies the secure log as the location for authentication-related messages. Because the question concerns a named administrator's attempted access to the Configuration Utility rather than application traffic or virtual-server processing, reviewing **/var/log/secure** directly addresses the required audit evidence. See F5's Overview of system logs and the log files and the BIG-IP logging documentation for related log-location guidance.