PassQueen
a.k.a dumpsqueen.com

BIG-IP Administration Install, Initial Configuration, and Upgrade

F5 F5CAB1

Version Demo

Total Demo Questions: 7

Total Premium Questions: 73

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A BIG-IP Administrator is preparing a **standalone** device for an upgrade to a new TMOS version.

The current software volume must remain available for rollback, and the current configuration must be recoverable if the upgrade is unsuccessful.

Which two actions best meet these requirements?

(Choose two.)

A. Install the target TMOS image to a new boot volume.

B. Create a UCS archive before beginning the installation.

C. Install the target TMOS image directly onto the active boot volume.

D. Delete the existing software image from the active boot volume.

E. Reboot the device before selecting a target boot volume.

ANSWER: A B

Explanation:

Installing the target image to a new boot volume preserves the currently active volume as a rollback option. Creating a UCS archive preserves the current configuration and relevant system files for restoration if needed.

Installing directly onto the active volume removes the intended software rollback point. Deleting the existing image does not protect the active installation, and rebooting before the target volume has been installed does not provide either configuration recovery or software rollback.

QUESTION NO: 2

A newly deployed BIG-IP VE has a management IP address of **192.0.2.10/24**. The management gateway is **192.0.2.1**.

An administrator can access the device from the local management subnet, but management hosts on remote networks cannot reach the device.

Which TMSH command should the administrator use to configure the required management default route?

A. `tmsh create sys management-route default gateway 192.0.2.1`

B. `tmsh create net route default gw 192.0.2.1`

C. `tmsh modify sys management-ip 192.0.2.1/24`

D. `tmsh create net self 192.0.2.10/24 vlan mgmt`

ANSWER: A

Explanation:

`tmsh create sys management-route default gateway 192.0.2.1` creates a default route in the management routing table. The dedicated management interface uses management routes, which are separate from data-plane routes configured under the `net route` hierarchy.

A data-plane default route could cause traffic to use a Self IP rather than the management interface and does not provide the required management-plane return path. The management route allows responses to remote management networks to be sent through the configured management gateway.

QUESTION NO: 3

A BIG-IP device is being prepared for **Automatic Activation**. The device uses a dedicated management interface, and the management network does not provide DHCP options.

Which two configuration items are required for the device to resolve and reach **activate.f5.com** through the management interface?

(Choose two.)

A. A management default route

B. A DNS server configuration

C. A default route in the TMM routing table

D. An Allow All Port Lockdown setting on a Self IP

E. A floating traffic-group address on the management network

ANSWER: A B

Explanation:

A management default route provides the management-plane path to destinations outside the local management subnet. A DNS server configuration is also required to resolve the licensing host name when no static host entry is being used. Together, these settings allow the BIG-IP system to establish the outbound HTTPS connection required for automatic licensing.

A data-plane default route applies to TMM traffic and does not replace management routing. Port Lockdown controls inbound access to a Self IP and is unrelated to outbound management-interface licensing traffic.

QUESTION NO: 4

When using the tmsh shell of a BIG-IP system, which command will display the management-ip address?

A. run /util bash ifconfig mgmt

B. list /sys management-ip

C. show /sys management-ip

ANSWER: B

Explanation:

`list /sys management-ip` is correct because the BIG-IP management address is represented by the `sys management-ip` configuration object in tmsh. The tmsh `list` command reads and displays the configured properties of an object, including the management IP address and its netmask. This is the appropriate tmsh-native method for verifying the persistent management-network configuration that BIG-IP uses for administrative access through the management interface. The leading slash is accepted as an absolute tmsh module path, so `/sys management-ip` identifies the same system configuration object as `sys management-ip`. This command is useful after initial setup, after changing management connectivity, and when validating the configuration before or after an upgrade. F5's tmsh reference documents the `sys management-ip` object and its configuration properties, while the tmsh command reference describes `list` as the command for displaying configuration objects. See the F5 sys management-ip tmsh reference and the F5 tmsh list command reference.

QUESTION NO: 5

The BIG-IP Administrator uses Secure Copy Protocol (SCP) to upload a TMOS image to the **/shared/images/** directory in preparation for a TMOS upgrade.

After the upload is completed, what will the system do **before** the image is shown in the GUI under:

System » Software Management » Image List ?

A. The system performs a reboot into a new partition

B. The system verifies the internal checksum

C. The system copies the image to /var/local/images/

ANSWER: B

Explanation:

The system verifies the internal checksum. When a TMOS software image is placed in `/shared/images/`, BIG-IP detects the image and validates it before making it available through the Image List in the Configuration utility. This validation confirms that the uploaded file is a complete, recognizable BIG-IP software image and that its embedded integrity information is consistent. The check is especially important for images transferred with SCP, because a file can exist in the target directory even if a transfer was interrupted or the file was otherwise corrupted. After validation completes successfully, the image becomes available for selection as the source image when installing software to a boot volume. This image-discovery and validation step is separate from installing the software: no boot volume is changed and no reboot occurs merely because an image has been uploaded. F5's software-management documentation describes placing software images in the shared images directory for discovery and management through the Image List. F5 also documents software-image integrity verification as part of safe upgrade preparation. See F5 BIG-IP software update documentation and F5 guidance for verifying BIG-IP software image integrity.

QUESTION NO: 6

Which of the following are resource allocation settings for modules? *(Pick the 2 correct responses below)*

A. Maximum

B. Nominal

C. Limited

D. Dedicated

ANSWER: B D

Explanation:

Nominal and **Dedicated** are valid BIG-IP module provisioning levels, which determine the resources reserved for licensed software modules. Administrators configure these levels through the Resource Provisioning page or with the `tmsh modify sys provision` command. Provisioning is important because enabling a module requires memory, disk space, and related system services; BIG-IP uses the selected level to calculate whether the platform can support the requested module combination.

Nominal is the normal operating provisioning level. It allocates the resources required for a module to run in a standard configuration and is intended for systems running one or more provisioned modules. This is the commonly selected level when the appliance has adequate capacity for the desired module set.

Dedicated is also an official provisioning level. It assigns the maximum available resources to one module, supporting deployments where that module is intended to receive the system's capacity rather than sharing it with other provisioned modules. F5 documents the available provisioning levels, including Nominal and Dedicated, in the BIG-IP `sys provision` reference. See the F5 tmsh sys provision reference and F5 resource provisioning guidance.

QUESTION NO: 7

A BIG-IP Administrator discovers malicious brute-force attempts to access the BIG-IP device on the **management interface** via SSH.

The administrator needs to restrict SSH access to the management interface.

Where should this be accomplished?

A. Network > Interfaces

B. Network > Self IPs

C. System > Configuration

D. System > Platform

ANSWER: D

Explanation:

System > Platform is the correct location because BIG-IP treats the dedicated management port as part of the management plane, and its SSH service access controls are configured through the platform-level SSH settings. In the Configuration area of this page, an administrator can use the SSH Access settings, including the SSH IP Allow list, to limit which source IP addresses or networks may establish SSH sessions to the BIG-IP management interface. Defining only trusted administrative subnets in this allow list directly addresses brute-force attempts by preventing connection attempts from unapproved sources from reaching the management SSH service.

This control corresponds to the BIG-IP `sys sshd` configuration, whose `allow` property specifies the remote IP addresses permitted to access SSH. It is specifically appropriate for protecting out-of-band management access on the MGMT port, independently of traffic and service settings used on the data plane. After making the change, administrators should ensure their own approved management workstation or jump-host subnet is included, then save the configuration so the restriction persists across restart. F5 documents the SSH daemon properties, including the permitted-address configuration, in the tmsh sys sshd reference; the management interface's distinct role is also described in the BIG-IP Systems Getting Started Guide.