



Vendor: F5

Exam Code: F5CAB1

Exam Name: BIG-IP Administration Install, Initial
Configuration, and Upgrade

Version: DEMO

QUESTION 1

Which configuration file can a BIG-IP administrator use to verify the provisioned modules?

- A. /config/bigip.license
- B. /config/bigip_base.conf
- C. /config/bigip.conf
- D. /var/local/ucs/config.ucs

Answer: C

Explanation:

Provisioning settings define which modules are enabled and how system resources are allocated to them.

These provisioning declarations are stored in:

/config/bigip.conf

This file contains:

Full module provisioning statements

TMSH-equivalent provisioning configurations such as:

```
sys provision ltm { level nominal }
```

```
sys provision asm { level nominal }
```

It is the primary system configuration file that stores all active provisioning details.

QUESTION 2

A BIG-IP Administrator needs to verify the state of equipment in the data center.

A BIG-IP appliance has a solid yellow indicator on the status LED.

How should the administrator interpret this LED indicator?

- A. Appliance is halted or in End-User Diagnostic (EUD) mode
- B. Appliance is a standby member in a device group
- C. A warning-level alarm condition is present
- D. A power supply is NOT operating properly

Answer: C

Explanation:

BIG-IP hardware platforms use chassis LEDs to indicate system health states.

A solid yellow status LED typically indicates a warning condition, such as:

A non-critical hardware alert

A temperature threshold nearing limit

A minor fan or sensor irregularity

Other non-fatal environmental or system conditions

This state reflects a warning-level alarm, meaning the unit is operational but requires investigation.

QUESTION 3

An F5 VE has been deployed into a VMware environment via an OVF file.

An administrator wants to configure the management IP address so the VE can be accessed for further setup.

Which two are valid methods for configuring the management-ip address? (Choose two.)

- A. Log into the remote console and configure the management IP by running the config executable.
- B. Log into the remote console and configure the management IP through TMSH using:
create sys management-ip <ip address>/<mask>
- C. Log into the remote console and configure the management IP through TMSH using:
create ltm management-ip <ip address>/<mask>
- D. Log into the remote console and configure the management IP by running the setup command.

Answer: AB

Explanation:

A newly deployed BIG-IP Virtual Edition (VE) in VMware requires initial configuration of its management-ip address so it can be accessed over the network. F5 provides several valid mechanisms during initial console access:

A. Running the config utility

The config script is available on new BIG-IP installations and VE deployments.

It launches a guided text-based wizard allowing configuration of:

Management IP

Netmask

Default route

This is a standard and recommended method during first-time setup.

B. Using TMSH with create sys management-ip

Administrators can enter TMSH directly from the console and run:

```
create sys management-ip <ip>/<mask>
```

The management-ip object resides under sys, not under ltm or any other module.

This is the correct tmsh method for defining the management interface address.

QUESTION 4

The BIG-IP Administrator needs to update access to the Configuration Utility to include the 172.28.31.0/24 and 172.28.65.0/24 networks. From the TMOS Shell (tmsh), which command should the BIG-IP Administrator use to complete this task?

- A. modify /sys httpd allow add { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }
- B. modify /sys httpd allow add { 172.28.31.0 172.28.65.0 }
- C. modify /sys httpd permit add { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }

Answer: A

Explanation:

Access to the BIG-IP Configuration Utility (TMUI) is controlled through the /sys httpd allow list.

This list defines which IP addresses or subnets are allowed to connect to the management web interface.

To allow two new subnets--172.28.31.0/24 and 172.28.65.0/24--the administrator must add both subnets to the existing list without removing current entries.

In tmsh, subnet entries must be specified in network/netmask format, for example:

```
172.28.31.0/255.255.255.0
```

The correct tmsh command to append these networks is:

```
modify /sys httpd allow add { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }
```

QUESTION 5

A BIG-IP Administrator is responsible for deploying a new software image on an F5 BIG-IP HA pair and has scheduled a one-hour maintenance window. With a focus on minimizing service disruption, which of the following strategies is the most appropriate?

- A. Update the active node first, reboot to the newly updated boot location and verify functionality, then push the update from the active to the standby node and reboot the standby node.
- B. Reset the Device Trust, apply the update to each node separately, reboot both nodes, then re-establish the Device Trust.
- C. Update the standby node first and reboot it to the newly updated boot location, failover to the newly updated node and verify functionality. Repeat the upgrade procedures on the next node, which is now in standby mode.
- D. Update both nodes in the HA pair, then reboot both nodes simultaneously to ensure they run the same software version.

Answer: C

Explanation:

For BIG-IP high-availability (HA) pairs, F5's recommended upgrade workflow prioritizes service continuity, predictable failover, and minimal downtime. The established best-practice sequence is:

Upgrade the standby unit first

Because the standby device is not passing traffic, upgrading and rebooting it does not impact production.

Boot the standby unit into the newly installed version

Once online, the administrator verifies basic health, device sync status, cluster communication, and module functionality.

Perform a controlled failover to the upgraded unit

Traffic shifts to the newly upgraded device, allowing validation of the configuration and operational behavior under real traffic loads.

Upgrade the second device (now standby)

The previously active device becomes standby after failover, allowing it to be safely upgraded and rebooted without interruption.

This phased approach ensures only one device is unavailable at a time, allowing continuous traffic flow throughout the upgrade process.

Why the Correct Answer is C

Option C exactly matches F5's documented production-safe upgrade method:

Upgrade the standby node first

Reboot into new image

Failover to upgraded device

Validate

Upgrade the remaining (now-standby) device

This procedure minimizes risk and traffic disruption.

QUESTION 6

What are the two options for securing a BIG-IP's management interface? (Choose two.)

- A. Limiting network access through the management interface to a trusted/secured network VLAN.
- B. Block all management-interface administrative HTTPS and SSH service ports to prevent access.
- C. Use the BIG-IP's Self-IP addresses for administrative access rather than the management interface.
- D. Restrict administrative HTTPS and SSH access to specific IP addresses or IP ranges.

Answer: AD

Explanation:

Securing the BIG-IP management interface is a fundamental administrative responsibility. F5 best practices emphasize restricting who can reach the management port and ensuring that only authorized systems are allowed access.

A. Limiting management access to trusted network segments

F5 recommends placing the management interface on a dedicated, isolated, and secured management network or VLAN, rather than exposing it to production or untrusted networks.

This reduces the attack surface by ensuring only trusted segments have visibility to administrative interfaces.

D. Restricting management access by IP or subnet

F5 BIG-IP uses the `/sys httpd allow list` (for HTTPS) and configuration options in `sshd` (for SSH)

to control which IP addresses or subnets can access the device.

By specifying only known administrative IPs or ranges, unauthorized users cannot reach the login services.

QUESTION 7

Which port is an exception to the Port Lockdown function of Self-IPs if a device-group synchronization cluster is configured?

- A. TCP 443
- B. TCP 4353
- C. UDP 53

Answer: B

Explanation:

Self-IPs implement a security feature known as Port Lockdown, which limits which services are reachable on a Self-IP.

However, certain services required for BIG-IP device-to-device communication bypass Port Lockdown to ensure cluster and HA functionality.

TCP 4353

TCP port 4353 is used by Device Service Clustering (DSC) for:

Device trust establishment

Configuration synchronization

Failover communication

Because BIG-IP devices must always be able to communicate for HA functions to remain operational, port 4353 is exempt from Port Lockdown rules.

QUESTION 8

A BIG-IP device is licensed for LTM, ASM, APM, and AFM.

Currently, it will only be used for load balancing and web application firewalling.

To ensure optimal performance and efficient resource utilization, which of the following module provisioning combinations is the best choice?

- A. LTM: Dedicated
ASM: Dedicated
APM: Minimal
AFM: Minimal
- B. LTM: Dedicated
ASM: Dedicated
APM: None
AFM: None
- C. LTM: Nominal
ASM: Nominal
APM: None

- AFM: None
D. LTM: Nominal
ASM: Nominal
APM: Minimal
AFM: Minimal

Answer: C

Explanation:

BIG-IP provisioning determines how CPU, memory, and disk resources are allocated to each module. The goal is to provision only the modules required and at levels appropriate to their performance needs.

Requirements in the question

The device will be used for:

LTM (Local Traffic Manager) load balancing

ASM (Application Security Manager) WAF

No functions require:

APM (Access Policy Manager)

AFM (Advanced Firewall Manager)

Why Option C is correct

Provisioning both LTM and ASM at Nominal level provides:

Adequate performance for production load

Plentiful system resources while avoiding dedicating the entire system to a single module

Balanced allocation without starving memory or CPU

Setting APM: None and AFM: None ensures unused modules consume zero resources.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14