# Exam Questions F5CAB1

BIG-IP Administration Install, Initial Configuration, and Upgrade

**https://www.2passeasy.com/dumps/F5CAB1/**

**NEW QUESTION 1**
Given thatBIGIP-<version>.isoandHotfix-BIGIP-<version>-ENG.isohave been uploaded to/shared/images on an F5 device, what is the appropriatetmsh command to prepare and update the BIG-IP device with the hotfixof a software version on a new volume HD1.2?
(Choose one.)

A. tmsh install /sys software hotfix Hotfix-BIGIP-<version>-ENG.iso create-volume HD1.2
B. tmsh install /sys software BIGIP-<version>.iso hotfix Hotfix-BIGIP-<version>-ENG.iso create-volume HD1.2
C. tmsh create /sys software hotfix Hotfix-BIGIP-<version>-ENG.iso volume HD1.2
D. tmsh copy /sys software hotfix Hotfix-BIGIP-<version>-ENG.iso volume HD1.2

**Answer:** B

**Explanation:**
When installing a BIG-IP software versionwith a HotFixon anew boot volume, F5 requires that both thebase TMOS imageand theHotFix imagebe installed together as part of the same installation workflow.
The correct process is:

- Specify thebase TMOS ISO
- Specify theHotFix ISOthat corresponds to that base version
- Instruct the system tocreate a new boot volume
- Install both images into that new volume

This is achieved with the following tmsh syntax:
tmsh install /sys software BIGIP-<version>.iso hotfix Hotfix-BIGIP-<version>-ENG.iso create-volume HD1.2 This command:

- Installs the base image first
- Applies the HotFix on top of the base image
- Creates and installs everything onHD1.2
- Leaves the currently active volume untouched for rollback

Why the other options are incorrect
* A. Installing only the hotfix
A HotFix cannot be installed by itself on a new volume. A base image must already be present.
* C. Using create instead of install
The create keyword is not valid for software installation operations.
* D. Using copy
The copy command does not install software images or hotfixes.

**NEW QUESTION 2**
For an upgrade of a standalone BIG-IP, a maintenance window is available in which brief interruptions are allowed.
Actions with no impact can be done outside the maintenance window.
When should a license reactivation be performed?

A. During the maintenance window.
B. Before the maintenance window.
C. After the maintenance window.

**Answer:** B

**Explanation:**
License reactivation updates the BIG-IP device??s license file to ensure:

- TheService Check Dateis current
- The device is eligible to install the intended TMOS version
- Any module entitlement updates are received

Reactivationdoes not interrupt trafficand does not require a reboot, making it safe to performbeforethe maintenance window.
F5 best practices state:

- Performall non-impact tasks priorto the scheduled maintenance window
- Leave the window available for activities that require rebooting, such as the software installation itself Since license reactivation isnon-disruptive, it should be donebeforethe upgrade window starts.

**NEW QUESTION 3**
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:**

(Paraphrased from F5 BIG-IP Administration / Installation / Initial Configuration concepts)
Within the BIG-IP Traffic Management Shell (tmsh), system configuration objects—including the management IP—are organized under the/syshierarchy. The management IP address is a configurable property stored in the system configuration and can be viewed using the tmshlistcommand, which displays configuration objects and their currently assigned values.
Why ??list /sys management-ip?? is correct

- The list command in tmsh is used todisplay configured system values, not runtime statistics.
- The object that holds the management IP settings on BIG-IP systems is located at:/sys management-ip
- Running the command:list /sys management-ipwill reveal the settings for the management IP interface, including the address, netmask, and any associated attributes.
- This is the standard method used during system setup and verification to confirm the management IP configuration.

This behavior aligns with BIG-IP administration procedures, where configuration information is retrieved usinglist, while operational data is retrieved usingshow.
Why the other options are incorrect
* A. run /util bash ifconfig mgmt

- This command enters the Bash shell, then runs ifconfig to display the management interface.
- While this can show the management interface address, it isnot a tmsh-native command, and the question specifically asks for a tmsh command.
- Administrators use tmsh directly for configuration display rather than leaving the shell.

* C. show /sys management-ip

- The show command displaysstatistics or operational data, not configuration values.
- The management-ip object does not maintain statistics; therefore show does not return the configuration details required.
- Only thelistcommand reveals stored configuration data such as IP address and netmask.

**NEW QUESTION 4**
A BIG-IP Administrator discovers malicious brute-force attempts to access the BIG-IP device on the management interfacevia 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:** C

**Explanation:**
The BIG-IPmanagement interface (MGMT port)is controlled throughSystem settings, not through the Network menu.
SSH access on the management interface is configured here:
System # Configuration # Device # General # SSH Access / SSH IP Allow
This section allows the administrator to:

- Enable or disable SSH service
- Restrict SSH access to specific IP addresses or subnets
- Apply security policies to the management interface

Why the other options are incorrect:
* A. Network > Interfaces

- Used for data-plane physical interface settings, not management plane SSH restrictions.

* B. Network > Self IPs

- Controls in-band management or data-plane access, not the dedicated management port.

* D. System > Platform

- Used for hostname, time zone, LCD contrast, hardware settings — not SSH security on the management port.

Therefore, restricting SSH access to themanagement interfacemust be done under:
#System # Configuration # Device # General
Which corresponds toOption C.

**NEW QUESTION 5**
An organization is planning to upgrade a BIG-IP system from16.1.xto17.1.x.
For a successful upgrade, theService Check Datemust be equal to or newer than the License Check Date required for 17.1.x.
Which command will show the Service Check Date on the BIG-IP system being upgraded?

A. grep "Service check date" /config/bigip.license
B. grep "Service check date" /config/bigip.conf
C. grep "Service check date" /config/svc_chk_date.dat
D. grep "Service check date" /config/BigDB.dat

**Answer:** A

**Explanation:**

BIG-IP licensing information, including theService Check Date, is stored in the file:
/config/bigip.license
This file contains all license attributes downloaded from the F5 licensing server, including:
License key
Licensed modules
Useful life date
Service check date
TheService Check Datedetermines whether the system is eligible for upgrades to specific TMOS versions. When reviewing upgrade readiness, administrators extract this value directly from the license file with:
grep "Service check date" /config/bigip.license
Why the other options are incorrect:
/config/bigip.confstores BIG-IP configuration objects, not license metadata.
/config/svc_chk_date.datisnota valid file in the licensing system; it does not contain license parameters.
/config/BigDB.datstores internal database values, not licensing attributes.
Thus, only thebigip.licensefile contains the correct licensing information required for verifying upgrade eligibility.

**NEW QUESTION 6**
A BIG-IP Administrator plans to upgrade a BIG-IP device to the latest TMOS version.
Which two tools could the administrator leverage to verify known issues for the target versions? (Choose two.)

A. F5 End User Diagnostics (EUD)
B. F5 iHealth
C. F5 University
D. F5 Bug Tracker
E. F5 Downloads

**Answer:** BD

**Explanation:**
Comprehensive and Detailed Explanation (Paraphrased from F5 BIG-IP Administration Install, Initial Configuration, and Upgrade concepts)
When performing a TMOS upgrade, F5 recommends validating the target software version to ensure that the release does not contain defects that may impact system behavior. The upgrade preparation process includes checking for known issues, validating compatibility, and reviewing advisory information for the intended version. Two primary F5 tools serve this purpose:
* B. F5 iHealth
iHealth is a cloud-based diagnostic and analysis platform used to evaluate the operational state of a BIG-IP system.
Administrators upload a QKView file to iHealth to receive an automated assessment of the system. As part of upgrade planning, iHealth provides:
Version-specific issue analysis, comparing the system??s configuration and hardware against F5??s internal catalog of published issues.
Upgrade advisories, identifying potential risks such as deprecated features, module compatibility concerns, or changes in behavior between TMOS versions.
Checks against known defects, allowing administrators to determine whether the target TMOS version contains issues relevant to their deployment.
This aligns with F5??s recommended upgrade workflow, where iHealth is used before upgrading to confirm system readiness and detect software-level concerns.
* D. F5 Bug Tracker
The Bug Tracker is F5??s dedicated interface for reviewing software defects across TMOS releases.
It enables administrators to:
Search forknown bugs by TMOS version, module, severity, or defect ID.
Review thestatus of defects(open, resolved, fixed in later releases).
Identify whether high-impact or security-related issues are associated with the target upgrade version.
F5 documentation emphasizes reviewing known defects prior to installation of new software images, making the Bug Tracker a critical resource for upgrade validation.
Why the other options are not correct
* A. F5 End User Diagnostics (EUD)
EUD is used exclusively forhardware diagnostics(ports, memory, fans). It does not provide software-related issue verification and is not used for upgrade planning.
* C. F5 University
This is atraining platform, not an operational tool. It does not provide defect listings or upgrade-specific warnings.
* E. F5 Downloads
Although it provides access to software images and release notes, it isnot a tool for identifying known bugs. Release notes summarize general fixes and features, but systematic bug verification requires iHealth or the Bug Tracker.

**NEW QUESTION 7**
The BIG-IP Administrator needs to update access to the Configuration Utility to include the 172.28.31.0/24and172.28.65.0/24networks.
From the TMOS Shell (tmsh), which command should the BIG-IP Administrator use to complete this task?

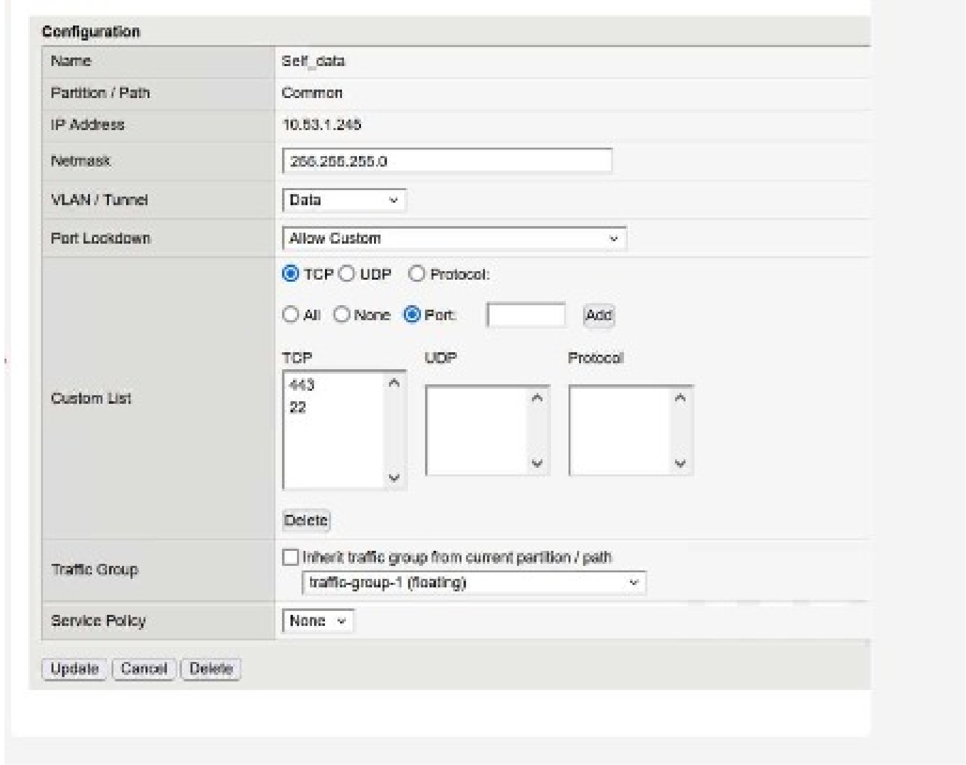
A. modify /sys httpd allow add { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }
B. modify /sys httpd allow add { 172.28.31.0 172.28.65.0 }
C. modify /sys httpd permit add { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }

**Answer:** A

**Explanation:**
Access to the BIG-IP Configuration Utility (TMUI) is controlled through the/sys httpd allowlist.
This list defines which IP addresses or subnets are allowed to connect to the management web interface.
To allow two new subnets—172.28.31.0/24and172.28.65.0/24—the administrator mustaddboth subnets to the existing list without removing current entries.
In tmsh, subnet entries must be specified innetwork/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 }
Why the other options are incorrect:
Option B:
IPs are listed without masks, which is invalid for subnet-based access control.
The system requiresnetwork/netmaskformat.
Option C:
The command uses permit instead of allow, which is not a valid attribute of /sys httpd.
The correct keyword must beallow.

Thus, onlyOption Acorrectly adds both permitted subnets in the proper tmsh format.

**NEW QUESTION 8**
Refer to the exhibit.



**Configuration**

| | |
|---|---|
| Name | Self_data |
| Partition / Path | Common |
| IP Address | 10.53.1.245 |
| Netmask | 255.255.255.0 |
| VLAN / Tunnel | Data |
| Port Lockdown | Allow Custom |
| Custom List | ● TCP ○ UDP ○ Protocol:<br>○ All ○ None ● Port: Add<br>TCP: 443, 22 · UDP: · Protocol:<br>Delete |
| Traffic Group | □ Inherit traffic group from current partition / path<br>traffic-group-1 (floating) |
| Service Policy | None |

What traffic will be permitted to reach the BIG-IP?

A. FTP
B. SSH
C. Telnet

**Answer:** B

**Explanation:**
The exhibit shows the configuration of aSelf IPwith:
Port Lockdown: Allow Custom
ACustom Listthat includes the following TCP ports:
443
22
Meaning of these ports:
TCP 443?? HTTPS (TMUI — web-based management)
TCP 22?? SSH (command-line remote access)
No other TCP, UDP, or protocol entries are listed; therefore, only these two services are allowed to reach the BIG-IP via this Self IP.
Evaluating the answer choices:
Option
Service
Port
Allowed?
FTP
TCP 21
Not listed
Not allowed
SSH
TCP 22
Listed
Allowed
Telnet
TCP 23
Not listed
Not allowed
Thus,SSHis the only traffic permitted through this Self IP configuration.

**NEW QUESTION 9**
Which two items demonstrate the creation of a new volumefor software images?
(Choose two.)

A. tmsh install software image /shared/images/BIGIP-.iso volume HD1.5 create-volume
B. tmsh install /sys software image BIGIP-.iso volume HD1.5 create-volume
C. Using the GUI, go toSystem>Disk Management, selectNew Volum
D. In the pop-up window, type the name or number of the new volume and clickApply.
E. tmsh install sys software image /shared/images/BIGIP-.iso volume HD1.5 create-volume
F. Using the GUI, go toSystem>Software Management>Available Images>Install, and in the Install Software Image pop-up window, type the new volume name or number and clickInstall.

**Answer:** AC

**Explanation:**
In BIG-IP, software images are installed onboot volumes(for example, HD1.1, HD1.2, HD1.3, etc.).
To install software on anew volume, the administrator must instruct the system to create a new boot location before installation.
There are two correct ways to create a new volume:

* A. tmsh command (with correct syntax)
tmsh install software image /shared/images/BIGIP-.iso volume HD1.5 create-volume
This syntax correctly includes:
install software image
full path to ISO (/shared/images/...)
volume name (HD1.5)
create-volumekeyword
This instructs BIG-IP to create the new boot volume as part of the installation.
* C. Using the GUI ?? System>Disk Management
From the Disk Management menu, the administrator can:
Select ??New Volume??
Enter the volume identifier (e.g., HD1.5)
Apply changes
This GUI method is officially supported and explicitly creates a new boot volume before installing the software.
Why the other options are incorrect:
* B. Incorrect tmsh syntax
Missing /shared/images/ path
Incorrect command structure
* D. Incorrect command structure
Missing required keywords and correct command hierarchy
* E. Software Management ?? Install does NOT create volumes
This installs to anexistingvolume only
The GUI install dialog does not create new boot volumes
Thus, onlyOption AandOption Cproperly create a new software volume.

**NEW QUESTION 10**
A BIG-IP Administrator needs to install a HotFix on a standalone BIG-IP device, which hasHD1.1as the Active Boot Location.
The administrator has already re-activated the license and created a UCS archive. In which sequence should the administrator perform the remaining steps?

A. Install HotFix in HD1.2, Install base Image in HD1.2, Activate HD1.2
B. Install HotFix in HD1.1, Reboot the BIG-IP device, Install UCS Archive
C. Install base Image in HD1.2, Install HotFix in HD1.2, Activate HD1.2
D. Activate HD1.2, Install base Image in HD1.2, Install HotFix in HD1.2

**Answer:** C

**Explanation:**
When installing a HotFix on a BIG-IP device, F5 best practices require:

- Installing the base TMOS image on a new, unused boot volume (HD1.2)
- This ensures the upgrade happens on a clean volume.
- The existing active boot location remains untouched for rollback.
- Installing the HotFix onto the SAME new boot volume (HD1.2)
- HotFixes must be applied on top of a base version.
- They cannot be installed on an empty volume.
- They must match the base image version.
- Activating the new boot volume (HD1.2)
- The system reboots into the updated software stack.
- Activation happensafterbase + HotFix installation is complete.

This sequence is exactly shown in Option C:
Install base Image in HD1.2 Install HotFix in HD1.2 Activate HD1.2
Why the other options are incorrect:
* A. Install HotFix before base image

- Impossible.
- HotFix requires an installed base version first.

* B. Installing HotFix on HD1.1 (active boot volume)

- Not recommended.
- Upgrading in-place removes rollback safety.
- HotFix cannot be applied cleanly without applying base image first.

* D. Activate HD1.2 before installing anything

- You cannot activate an empty boot volume.
- Activation only occurs after the base + HotFix software is installed.

**NEW QUESTION 10**
The device is currently onv15.1.2.1.

The BIG-IP Administrator needs to boot the device back tov13.1.0.6to gather data for troubleshooting.
The system shows: Sys::Software Status
Volume Product Version Build Active Status Allowed HD1.1 BIG-IP 15.1.2.1 0.0.10 yes complete yes HD1.2 BIG-IP 13.1.0.6 0.0.3 no complete yes
Which is the correct command-line sequence to boot the device to version13.1.0.6?

A. Use tmsh to select a new boot volume, tmsh reboot HD1.2
B. switchboot -b HD1.2, then reboot
C. switchboot -I HD1.2, then reboot
D. Use tmsh to select a new boot volume, tmsh switchboot HD1.2

**Answer:** B

**Explanation:**
To change the boot volume on a BIG-IP system from one installed TMOS version to another, the correct CLI tool is:
switchboot
The correct syntax uses the-bflag:
switchboot -b <volume>
This command marks the specified boot location as the one to be used on the next reboot. Thus, to boot intoHD1.2which contains13.1.0.6, the sequence is:

- Mark HD1.2 as the next boot location:
- switchboot -b HD1.2
- Reboot the system:
- reboot

This is the standard and officially supported method for selecting a different installed volume.
Why the other options are incorrect:
* A. "tmsh reboot HD1.2"

- There is no such tmsh syntax.
- Boot volume cannot be selected by adding a parameter to reboot.

* C. switchboot -I HD1.2

- The -I flag is invalid. Only -b is used.

* D. "tmsh switchboot HD1.2"

- switchboot isnota tmsh command; it is a system-level shell utility.

Therefore,Option Bis the correct and valid command sequence.

**NEW QUESTION 12**
The BIG-IP Administrator wants to manage the newly built F5 system through anin-band Self-IP.
The administrator has configured a VLAN and Self-IP and can ping the IP from their workstation, but cannot access the system viaSSHorHTTPS.
What port lock down settings should the BIG-IP Administrator use to allow management access on the Self-IP?
(Choose two.)

A. The Self-IP port lockdown behavior could be adjusted toAllow Default
B. The Self-IP port lockdown behavior could be adjusted toAllow All
C. The Self-IP port lockdown behavior could be adjusted toAllow Mgmt
D. The Self-IP port lockdown behavior could be adjusted toAllow Management

**Answer:** CD

**Explanation:**
Self-IPs include a security feature calledPort Lockdown, which restricts which services respond on that Self- IP.
By default, Self-IPs block management access (SSH and HTTPS/TMUI), meaning an administrator cannot manage the device through in-band Self-IPs unless explicitly allowed.
Allow Mgmt / Allow Management
These settings enable only the management services required for administrative access, specifically:

- SSH (22)
- HTTPS/TMUI (443)

These options allow secure administration without opening unnecessary ports.
Why these are correct:

- They provide only the essential access for management.
- They follow F5 security best practices when using in-band admin access.
- They donotexpose all services, reducing the attack surface.

Why the other options are incorrect:
* A. Allow Default

- Administrator access would still fail.

* B. Allow All

- Opens all ports on the Self-IP, which isnot secure.
- Exposes services that should remain restricted.

Therefore,Allow Mgmt / Allow Managementare the correct choices.

**NEW QUESTION 14**
A BIG-IP Administrator needs to verify the state of equipment in the data center. A BIG-IP appliance has asolid yellow indicatoron 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:**
Explanation
BIG-IP hardware platforms use chassis LEDs to indicate system health states.
Asolid yellow status LEDtypically indicates awarning 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 awarning-level alarm, meaning the unit is operational but requires investigation.
Why the other options are incorrect
* A. Halted or EUD mode

- This is associated with different LED patterns (usually flashing conditions or specific color codes), not a solid yellow status LED.

* B. Standby in device group

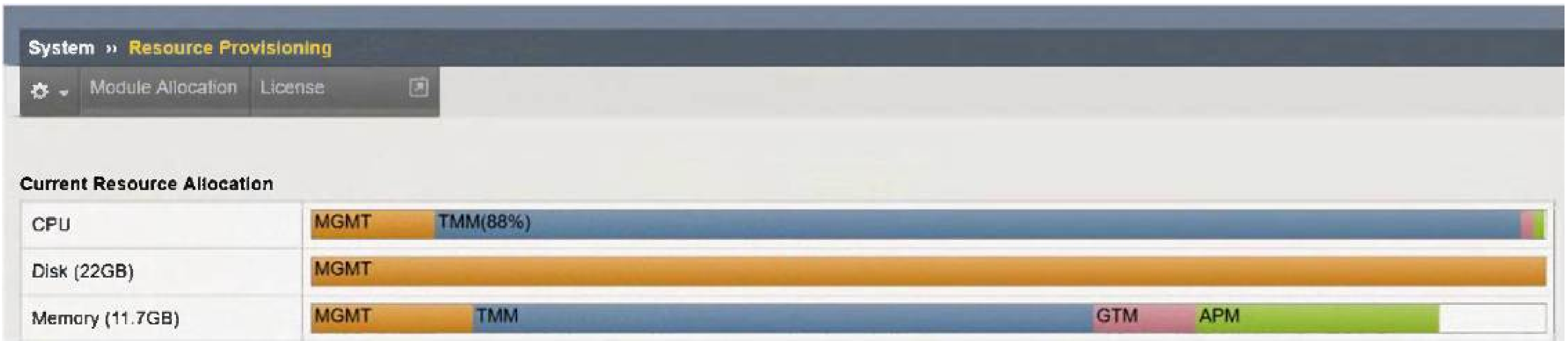
- HA state is not indicated by the chassis status LED.
- Standby status is alogicaldevice state, not a hardware LED state.

* D. Power supply failure

- Power supply indicators use separate LEDs located on each power module (usually flashing amber/red), not the system status LED.

Thus, asolid yellow status indicatorsignifies awarning-level alarm.

**NEW QUESTION 16**
Refer to the exhibit.



System » Resource Provisioning

Module Allocation | License

Current Resource Allocation

| | |
|---|---|
| CPU | MGMT TMM(88%) |
| Disk (22GB) | MGMT |
| Memory (11.7GB) | MGMT TMM GTM APM |

An organization has purchased a BIG-IP license that includes all available modules but has chosen to provision only the modules they require.
The exhibit displays the current resource allocation from theSystem # Resource Provisioningpage.
Based on the information provided, which F5 modules have been provisioned?

A. LTM, APM
B. DNS, APM
C. LTM, DNS, APM
D. TMM, DNS, APS

**Answer:** C

**Explanation:**
The exhibit shows theCurrent Resource Allocationfor:

- CPU
- Disk
- Memory

In particular, theMemory Allocationbar displays the modules that are currently provisioned.
Memory is the most reliable indicator because BIG-IP allocates memoryonlyto modules that are actively provisioned.
From the exhibit:

- MGMT(Management) – always present
- TMM(Traffic Management Microkernel) – indicatesLTM is provisioned
- GTM– this label indicates that theDNS moduleis provisioned (GTM = Global Traffic Manager, now called DNS)

- APM– explicitly shown, indicatingAccess Policy Manageris provisioned

Therefore, the provisioned modules are:

- LTM(implied by TMM allocation)
- DNS/GTM
- APM

This matchesOption C: LTM, DNS, APM.

**NEW QUESTION 21**
Which configuration file can a BIG-IP administrator use to verify theprovisioned 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 theprimary system configuration filethat stores all active provisioning details.
Why the other answers are incorrect
* A. /config/bigip.license
Showslicensedmodules, not provisioned modules.
* B. /config/bigip_base.conf
Stores base networking (VLANs, Self-IPs, routes), not provisioning.
* D. config.ucs
A backup archive, not a live configuration file.
Thus, the correct file to review active module provisioning is/config/bigip.conf.

**NEW QUESTION 22**
......