F5-Networks

Exam Questions F5CAB1

BIG-IP Administration Install, Initial Configuration, and Upgrade

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A secondary administrator has been granted access to a BIG-IP device through itsManagement Interface, but is unable to access the Configuration Utility (WebUI).
What command can be run from the CLI to capture the network traffic on the management interface and troubleshoot the issue?
(Choose two.)

A. tcpdump -i eth0 -n port 443
B. tcpdump -i mgmt -n port 443
C. tcpdump -i 0.0 -n port 443
D. tcpdump -i tun0 -n port 443
E. tcpdump -i management -n port 443

Answer: AB

Explanation:
The BIG-IP has two distinct planes:
- Management-plane# handled entirely by the management interface (MGMT)
- Data-plane (TMM)# handles Self IPs, VLAN interfaces, and traffic processing

To capture traffic on the management interface, only the management-side NICs may be used:
- mgmt# Logical name for the management interface
- eth0# Physical Linux interface mapped to the management port on most BIG-IP platforms

Both of these correctly capture inbound/outbound WebUI (HTTPS/443) traffic on the management port.
Why the correct answers are A and B
* A. tcpdump -i eth0 -n port 443
  - On BIG-IP appliances and VMs, the management port maps toeth0at the Linux OS level.
  - Capturing on eth0 correctly shows HTTPS traffic to the WebUI.
* B. tcpdump -i mgmt -n port 443
  - mgmtis the BIG-IP alias for the management interface.
  - This is thepreferredand most explicit capture interface for management-plane packet captures.

Why the other options are incorrect:
* C. tcpdump -i 0.0
  - Interface0.0is the TMM switch interface used for data-plane packet captures.
  - Itdoes NOTcapture management-plane traffic.
* D. tcpdump -i tun0
  - Used for tunnel interfaces (IPsec, VXLAN, etc.)
  - Not related to management access.
* E. tcpdump -i management
  - There isnointerface named management on BIG-IP.
  - The correct names are mgmt or eth0.

NEW QUESTION 2
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 3
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 4
A BIG-IP device will be dedicated to functioning as a WAF, requiring only theASMmodule to be provisioned.
What provisioning level will ensure that the system allocatesall CPU, memory, and disk resourcesto this module exclusively?

A. Dedicated
B. Comprehensive
C. Maximal
D. Nominal

Answer: A

Explanation:
Provisioning defines how BIG-IP allocates system resources to modules. The provisioning levels include:

- Dedicated– allocatesallCPU, memory, and disk resources to a single module
- Nominal– standard resource allocation balanced with other modules
- Minimal– lowest level, used for basic utility needs
- None– module disabled
- Comprehensive / Maximal– not valid TMOS provisioning levels

Why ??Dedicated?? is correct
When a BIG-IP device is intended to runonly ASM(Web Application Firewall), the recommended way to maximize performance is to provision the module atDedicatedlevel.
WithASM: Dedicated:

- ASM receives theentire hardware capacity
- No other modules can or should be provisioned
- This is explicitly recommended when a device is used solely as a WAF platform

Why other options are incorrect
* B. Comprehensive / C. Maximal

- These arenot valid provisioning modesin BIG-IP.

- TMOS supports: Nominal, Minimal, Large (module-specific), and Dedicated.

* D. Nominal

- Shares resources with other modules
- Does not provide full system performance
- Not suitable when exclusive resource allocation is required Thus,Dedicatedis the correct provisioning choice.

NEW QUESTION 5
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 6
The BIG-IP Administrator uses Secure Copy Protocol (SCP) to upload a TMOS image to the/shared/images/ directory in preparation for an upgrade.
After the upload is complete, what will the system dobeforethe image appears in the GUI under:
System » Software Management » Image List?

A. The system performs a reboot into the new partition
B. The system verifies the internal checksum
C. The system copies the image to /var/local/images/

Answer: B

Explanation:
When a TMOS ISO file is transferred to/shared/images/, the BIG-IP automatically performs a validation step:
Checksum Verification

- Before the image becomes visible in the GUI, the systemverifies the internal checksumembedded inside the ISO.

- This ensures:
- The file was fully transferred
- The image is not corrupted
- It matches the official F5 release signature
- Only after passing this verification does the GUI display the ISO under ??Available Images.??

Why the other options are incorrect:
* A. Reboot into a new partition
- No reboot occurs simply from uploading an image.

* C. Copying into /var/local/images/
- This directory isnotused for ISO storage.
- All valid images remain in/shared/images/.

Thus, the correct system action ischecksum verification.

NEW QUESTION 7
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 8
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 9
When is the License Service Check Date enforced on a BIG-IP system?

A. After editing a virtual server
B. During a software install
C. During system startup

Answer: B

Explanation:
TheService Check Datedetermines whether a particular software version is allowed to run under the device??s license.

- When installing or upgrading TMOS, the installer checks theService Check Datestored in the BIG-IP license file.
- If the license date isolderthan the minimum required for the target version, the software installation is blocked.
- This check happensspecifically during a software install, not during routine device operations.

Editing virtual servers or system startup do not trigger this validation. Thus, the enforcement happensduring software installation.

NEW QUESTION 10
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 10
A BIG-IP Administrator is using Secure Copy Protocol (SCP) to transfer a TMOS image to the BIG-IP system in preparation for an upgrade.
To what directory should the file be transferred?

A. /shared/images/
B. /local/images/
C. /var/images/

Answer: A

Explanation:
BIG-IP systems require all ISO images (base TMOS images and HotFix images) to be stored in a specific directory used for software installation:
/shared/images/
This directory:
Is theonly supported locationfrom which the BIG-IP software installation system validates and installs ISO files
Is accessible by both the GUI and TMSH installers
Has adequate storage space allocated specifically for images
Is part of the shared partition that persists across reboots
When transferring images via SCP, the administrator must copy them directly into/shared/images/so that:
The GUI (System ?? Software Management ?? Available Images) can detect the image
TMSH install software image commands can reference it
Other directories such as/local/images/or/var/images/are not valid storage paths for software images.

NEW QUESTION 11
A new logging solution is being implemented on the network. Policy requires keeping management traffic sent from the BIG-IPout of the management interface. After configuring the BIG-IP to forward messages to the new Syslog server, the BIG-IP Administrator notices that packets are being sentfrom a numbered data-plane Self IP.
What should the BIG-IP Administrator change to send the traffic out of thecorrect interface?

A. Set the Management IP as the source address when configuring a Remote Syslog destination.
B. Create a Management Route for the specific address/subnet of the syslog service via TMSH.
C. Create a new Self IP in the same subnet as the management IP address using a route domain.
D. Modify the port lockdown settings on the Self IP address to allow UDP port 514 traffic.

Answer: B

Explanation:
By default,management-plane trafficuses themanagement routing table, whiledata-plane trafficuses theTMM routing table.
Remote Syslog traffic ismanagement-planetrafficunlessa management route exists.
If noManagement Routematches the Syslog server??s destination IP, the BIG-IP will instead:
UseTMM routes, and
Source the packets from aSelf IP
This is exactly what the administrator is observing.
To force Syslog traffic out the management port:
You must create aManagement Route, which is configured using:
tmsh create /sys management-routegatewaynetwork
This sends syslog traffic:
Out of themanagement interface
Using theManagement IPas the source
Thus,Option Bis correct.
Why the other options are incorrect:
* A. Set the Management IP as the source address
Source address selection is overridden by routing.
Without a management route, traffic still goes out the data plane.
* C. Create a new Self IP using a route domain
Unnecessary and not related to management-plane routing.
Syslog traffic should not rely on data-plane Self IPs.
* D. Modify port lockdown on Self IP to allow UDP/514
This would allow Syslog trafficintothe BIG-IP over a Self IP, not forceoutboundtraffic via management.

NEW QUESTION 12
.....

Relate Links

100% Pass Your F5CAB1 Exam with Exambible Prep Materials

https://www.exambible.com/F5CAB1-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/