F5 Networks

F5CAB1

BIG-IP Administration Install, Initial Configuration, and Upgrade

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.2

Question: 1

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: B, D

Explanation:
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:
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 for known bugs by TMOS version, module, severity, or defect ID.
Review the status 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 for hardware diagnostics (ports, memory, fans). It does not provide software-related issue verification and is not used for upgrade planning.
C . F5 University
This is a training 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 is not a tool for identifying known bugs. Release notes summarize general fixes and features, but systematic bug verification requires iHealth or the Bug Tracker.

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:
Within the BIG-IP Traffic Management Shell (tmsh), system configuration objects—including the management IP—are organized under the /sys hierarchy. The management IP address is a configurable property stored in the system configuration and can be viewed using the tmsh list command, which displays configuration objects and their currently assigned values.
Why “list /sys management-ip” is correct
The list command in tmsh is used to display 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-ip
will 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 using list, while operational data is retrieved using show.
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 is not 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 displays statistics or operational data, not configuration values.
The management-ip object does not maintain statistics; therefore show does not return the configuration details required.
Only the list command reveals stored configuration data such as IP address and netmask.

Question: 3

The BIG-IP Administrator received a ticket that an authorized user is attempting to connect to the Configuration Utility from a jump host and is being denied.
The HTTPD allow list is configured as:
sys httpd {
allow { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }
}
The jump host IP is 172.28.32.22.
What command should the BIG-IP Administrator use to allow HTTPD access for this jump host?

A. modify /sys httpd allow replace-all-with { 172.28.32.22 }
B. modify /sys httpd allow delete { 172.28.31.0/255.255.255.0 172.28.65.0/255.255.255.0 }
C. modify /sys httpd allow add { 172.28.32.22 }

Answer: C

Explanation:
The HTTPD allow list controls which IP addresses or subnets may access the Configuration Utility (TMUI) on the BIG-IP system. The Administrator already has two subnets allowed and needs to add a single host IP to the existing list.
The object /sys httpd allow supports actions such as add, delete, and replace-all-with.
Because the goal is to add one more entry without removing the existing permitted subnets, the correct command is:
modify /sys httpd allow add { 172.28.32.22 }
This appends the new host to the existing list while preserving the previously configured networks.
Why the other options are incorrect:
Option A (replace-all-with) would overwrite the entire allow list, removing existing permitted subnets—unacceptable.
Option B (delete) would remove the existing networks and not add the required host.
Therefore, the correct administrative action is to add the jump host's IP.

Question: 4

The Configuration Utility of a BIG-IP device is currently accessible via its management IP 10.53.1.245 from all VLANs.

The BIG-IP Administrator needs to restrict access so only hosts from the 10.0.0.0/24 subnet can access the Configuration Utility.
Which TMSH command accomplishes this?

A. (tmos)# create /net acl MGMT.HTTP rule add { (permit tcp 10.0.0.0 0.0.0.255 host 10.53.1.245 http) }
B. (tmos)# modify /ltm httpd allow replace-all-with {10.0.0.0/24}
C. (tmos)# create /net acl MGMT.HTTP rule add { (permit tcp 10.0.0.0/24 10.53.1.245 http) (deny ip any any http) }
D. (tmos)# modify /sys httpd allow replace-all-with {10.0.0.0/24}

Answer: D

Explanation:
BIG-IP controls access to the web-based Configuration Utility (TMUI) through the /sys httpd allow list. This parameter specifies which client IPs or subnets may initiate HTTP/HTTPS connections to the management interface.
To restrict TMUI access to only the 10.0.0.0/24 subnet:
The correct method is to modify the HTTPD allow list so that it contains only this subnet.
This requires replacing the entire current list with the new subnet using:
modify /sys httpd allow replace-all-with {10.0.0.0/24}
This ensures that only clients within 10.0.0.0/24 can reach the Configuration Utility.
Why the other options are incorrect:
Options A and C create network ACL objects under /net acl, which apply to data-plane traffic, not management-plane TMUI access. TMUI access is not controlled by LTM ACLs but by the HTTPD allow directive.
Option B is incorrect syntax and references /ltm httpd, which is not the proper object; the correct hierarchy is /sys httpd.
Thus, only modifying the /sys httpd allow list achieves the required restriction.

Question: 5

modification]
An organization is planning to upgrade a BIG-IP system from 16.1.x to 17.1.x.
For a successful upgrade, the Service Check Date must 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 the Service 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
The Service Check Date determines 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.conf stores BIG-IP configuration objects, not license metadata.
/config/svc_chk_date.dat is not a valid file in the licensing system; it does not contain license parameters.
/config/BigDB.dat stores internal database values, not licensing attributes.
Thus, only the bigip.license file contains the correct licensing information required for verifying upgrade eligibility.

Visit us at: https://www.examsempire.com/f5cab1

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/