Exam F5 F5CAB1 Preparation, F5CAB1 Questions

Many candidates may think that it will take a long time to prapare for the F5CAB1 exam. Actually, it only takes you about twenty to thirty hours to practice our F5CAB1 exam simulation. We believe that the professional guidance will help you absorb the knowledge quickly. You will have a wide range of chance after obtaining the F5CAB1 certificate. You need to have a brave attempt. Our F5CAB1 training engine will help you realize your dreams.

F5 F5CAB1 Exam Syllabus Topics:

Topic	Details
Topic 1	• BIG IP Administration Data Plane Configuration: This section of the exam measures skills of System Administrators and covers configuring BIG IP objects that control data plane behavior. It focuses on setting up virtual servers, pools, nodes, monitors, and profiles so that applications are delivered reliably and efficiently according to design requirements.
Topic 2	• BIG IP Administration Install Initial Configuration and Upgrade: This section of the exam measures skills of System Administrators and covers the lifecycle tasks for deploying and maintaining a BIG IP system. It includes installing the platform, performing initial setup, applying licenses, configuring basic networking, and planning and executing software upgrades and hotfixes.
Topic 3	• BIG IP Administration Control Plane Administration: This section of the exam measures skills of System Administrators and covers managing the control plane where BIG IP is configured and administered. It includes working with user accounts, roles, device settings, configuration management, and using the graphical interface and command line for daily administrative tasks.
Topic 4	• BIG IP Administration Support and Troubleshooting: This section of the exam measures skills of Network Administrators and covers identifying and resolving common issues that affect BIG IP operation. It focuses on using logs, statistics, diagnostic tools, and basic troubleshooting methods to restore normal traffic flow and maintain stable application delivery.

Topic 5	• BIG IP Administration Data Plane Concepts: This section of the exam measures skills of Network Administrators and covers how BIG IP handles application traffic on the data plane. It includes understanding flow of traffic, key data path components, basic concepts of load balancing, and how security and performance features affect user traffic.

>> Exam F5 F5CAB1 Preparation <<

F5CAB1 Questions - Test F5CAB1 Guide Online

Our team of experts updates actual F5 F5CAB1 questions regularly so you can prepare for the F5CAB1 exam according to the latest syllabus. Additionally, we also offer up to 1 year of free F5CAB1 exam questions updates. We have a 24/7 customer service team available for your assistance if you get stuck somewhere. Buy F5CAB1 Latest Questions of Exams4sures now and get ready to crack the F5CAB1 certification exam in a single attempt.

F5 BIG-IP Administration Install, Initial Configuration, and Upgrade Sample Questions (Q14-Q19):

NEW QUESTION # 14
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.
Whatport lockdownsettings 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 Management
- B. The Self-IP port lockdown behavior could be adjusted toAllow Mgmt
- C. The Self-IP port lockdown behavior could be adjusted toAllow All
- D. The Self-IP port lockdown behavior could be adjusted toAllow Default

Answer: A,B

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
* This allows only a minimal set of system-required ports (e.g., failover, config sync), not SSH or HTTPS.
* 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 # 15
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 both nodes in the HA pair, then reboot both nodes simultaneously to ensure they run the same software version.
- B. 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.
- C. Reset the Device Trust, apply the update to each node separately, reboot both nodes, then re-establish the Device Trust.
- D. 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.

Answer: B

Explanation:
For BIG-IP high-availability (HA) pairs, F5's recommended upgrade workflow prioritizesservice continuity, predictable failover, andminimal 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
OptionCexactly matches F5's documented production-safe upgrade method:
* Upgrade thestandbynode first
* Reboot into new image
* Failover to upgraded device
* Validate
* Upgrade the remaining (now-standby) device
This procedure minimizes risk and traffic disruption.
Why the other options are incorrect:
A). Upgrade the active node first
* Upgrading the active device requires removing it from service and failing over abruptly. This is not recommended and increases service disruption risk.
B). Resetting device trust
* Resetting trust is unnecessary and can disrupt configuration sync, peer communication, and cluster operation. It is not part of any standard upgrade workflow.
D). Upgrading and rebooting both nodes simultaneously
* This would causetotal outage, because both HA members would be unavailable at the same time.

NEW QUESTION # 16
When is theLicense Service Check Dateenforced on a BIG-IP system?

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

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 # 17
An F5 BIG-IP Administrator is asked to report which modules areprovisionedon the BIG-IP.
In which two ways can this be done?
(Choose two.)

- A. Via TMSH withshow /sys provision
- B. Via TMSH withlist /sys provision
- C. Via the GUI atStatistics # Module Statistics # System
- D. Via the GUI atSystem # Resource Provisioning # Module Allocation

Answer: B,D

Explanation:
Provisioning determines:
* Which BIG-IP modules are enabled (LTM, ASM, APM, AFM, DNS, etc.)
* Their provisioning levels (None, Minimal, Nominal, Dedicated)
Two accurate ways to view provisioning settings are:
A). GUI - System # Resource Provisioning # Module Allocation
This is the primary GUI screen showing:
* All modules
* Their provisioning level
* System resource distribution impact
Administrators commonly use this page to confirm or change module provisioning.
D). TMSH - list /sys provision
This tmsh command displays each module and its provisioning level:
sys provision ltm { level nominal }
sys provision asm { level none }
This is the authoritative CLI method for checking module provisioning configurations.
Why the other options are incorrect:
B). show /sys provision
* Showsruntimeinformation butnot the actual configuration levels.
* list is the correct command for configuration details.
C). Statistics # Module Statistics
* Shows performance statistics, NOT provisioning status.
Therefore, the correct responses areAandD.

NEW QUESTION # 18
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 power supply is NOT operating properly
- D. A warning-level alarm condition is present

Answer: D

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 # 19
.....

Desktop F5 F5CAB1 Practice Exam Software is a one-of-a-kind and very effective software developed to assist applicants in preparing for the F5 F5CAB1 certification test. The Desktop F5 F5CAB1 Practice Exam Software that we provide includes a self-assessment feature that enables you to test your knowledge by taking simulated tests and evaluating the results.