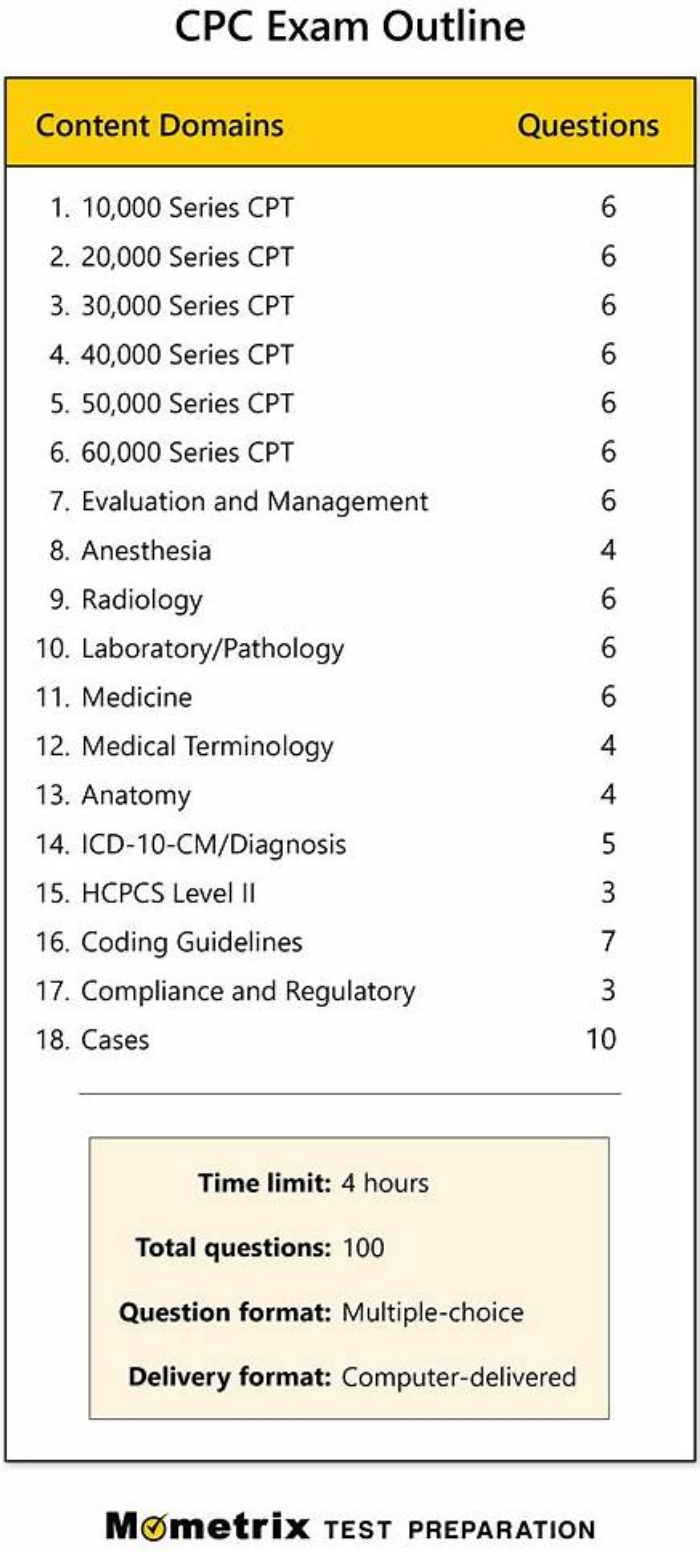
2026 Efficient F5CAB5–100% Free Test Practice | Exam Topics F5CAB5 Pdf



CPC Exam Outline

Content Domains	Questions
1. 10,000 Series CPT	6
2. 20,000 Series CPT	6
3. 30,000 Series CPT	6
4. 40,000 Series CPT	6
5. 50,000 Series CPT	6
6. 60,000 Series CPT	6
7. Evaluation and Management	6
8. Anesthesia	4
9. Radiology	6
10. Laboratory/Pathology	6
11. Medicine	6
12. Medical Terminology	4
13. Anatomy	4
14. ICD-10-CM/Diagnosis	5
15. HCPCS Level II	3
16. Coding Guidelines	7
17. Compliance and Regulatory	3
18. Cases	10

Time limit: 4 hours

Total questions: 100

Question format: Multiple-choice

Delivery format: Computer-delivered

Mometrix TEST PREPARATION

Can you imagine that you only need to review twenty hours to successfully obtain the F5 certification? Can you imagine that you don’t have to stay up late to learn and get your boss’s favor? With F5CAB5 study materials, passing exams is no longer a dream. If

you are an office worker, F5CAB5 Study Materials can help you make better use of the scattered time to review. Just a mobile phone can let you do questions at any time.

F5 F5CAB5 Exam Syllabus Topics:

Topic	Details
Topic 1	• Given a scenario, interpret traffic flow: This domain covers understanding traffic patterns through client-server communication analysis and interpreting traffic graphs and SNMP results.
Topic 2	• Determine resource utilization: This domain covers analyzing system resources including control plane versus data plane usage, CPU statistics per virtual server, interface statistics, and disk and memory utilization.
Topic 3	• Given a scenario, review basic stats to confirm functionality: This section involves interpreting traffic object statistics and network configuration statistics to validate system functionality.

Exam Topics F5CAB5 Pdf & F5CAB5 Hot Spot Questions

Successful people are never satisfying their current achievements. So they never stop challenging themselves. If you refuse to be an ordinary person, come to learn our F5CAB5 preparation questions. Our F5CAB5 study materials will broaden your horizons and knowledge. Many people have benefited from learning our F5CAB5 learning braindumps. Most of them have realized their dreams and became successful.

F5 BIG-IP Administration Support and Troubleshooting Sample Questions (Q19-Q24):

NEW QUESTION # 19
A BIG-IP Administrator makes a configuration change to a Virtual Server on the Standby device of an HA pair. The HA pair is currently configured with Auto-Sync Enabled. What effect will the change have on the HA pair configuration?

- A. The change will be undone when Auto-Sync propagates the config to the HA pair.
- B. The change will take effect when Auto-Sync propagates the config to the HA pair.
- C. The change will be undone next time a configuration change is made on the Active device.
- D. The change will be propagated next time a configuration change is made on the Active device.

Answer: B

Explanation:
Understanding High Availability (HA) synchronization behavior is critical for maintaining a stable environment. In a device group where "Auto-Sync" is enabled, the BIG-IP system monitors the management plane for any configuration updates across all members. While best practices often suggest making changes on the "Active" device, TMOS allows changes on any device within the group. When a change is made on the "Standby" device, the system detects a configuration mismatch and, because Auto-Sync is enabled, it automatically pushes those changes to the other devices in the sync group, including the current Active member. To troubleshoot if this is working correctly, the administrator should review the "Sync Status" stats in the Configuration Utility. If the changes do not propagate, it suggests9 a breakdown i10n the HA trust relationship or network connectivity issues on the failover VLAN. Proper interpretation of this scenario confirms that the HA functionality is operating correctly, ensuring that both devices have a consistent set of virtual servers and pools, which is vital fl1or seamless failover.

NEW QUESTION # 20
Which Virtual Server type prevents the use of a default pool?

- A. Forwarding (IP)
- B. Performance HTTP

- C. Performance (Layer 4)
- D. Standard

Answer: A

Explanation:
In BIG-IP TMOS administration, the "Forwarding (IP)" virtual server type is unique because it is designed to act as a high-performance router rather than a typical load balancer. Unlike a "Standard" virtual server, which terminates a connection and directs it to a specific pool of members, a Forwarding (IP) virtual server is intended to forward packets based on the system's routing table. Consequently, the configuration for this type of virtual server explicitly removes the option to associate a default pool. If an administrator is troubleshooting a scenario where they cannot assign a pool to a virtual server, they must verify if the type was accidentally set to Forwarding (IP). This type is most commonly used for outbound internet traffic (outbound SNAT) or to allow the BIG-IP to serve as a gateway between internal subnets. Identifying this constraint is vital for troubleshooting configuration errors where an administrator expects the system to load balance traffic but finds the pool association settings are grayed out or unavailable in the Configuration Utility.

NEW QUESTION # 21
A BIG-IP Administrator configured the following virtual server to pass traffic on all addresses and ports.
After configuration is completed, the BIG-IP Administrator notices that the virtual server is unable to pass traffic.
ltm virtual forwarding_any_vs {
destination 0.0.0.0:any
ip-forward
mask 255.255.255.255
profiles {
fastL4 { }
}
serverssl-use-sni disabled
source 0.0.0.0/0
translate-address disabled
translate-port disabled
}
Which part of the configuration is the cause of the issue? (Choose one answer)

- A. Incorrect translate-address configured
- B. Incorrect mask 255.255.255.255
- C. Incorrect destination configured

Answer: B

Explanation:
This virtual server is intended to function as aforwarding (IP-forwarding) virtual server, which is commonly used for routing or firewall-style deployments where BIG-IP forwards traffic transparently without load balancing or address translation. For a forwarding virtual server to match and passall traffic, the destination must be configured as 0.0.0.0:anywith a mask of 0.0.0.0, not 255.255.255.255.
The configured mask 255.255.255.255 represents a/32 host mask, which restricts the virtual server to matching traffic destined only for the exact IP address 0.0.0.0. Since 0.0.0.0 is not a valid routable destination for normal traffic, no packets will ever match the virtual server, causing it to pass no traffic at all.
This is a well-documented BIG-IP behavior:
* destination 0.0.0.0:any
* mask 0.0.0.0
together define acatch-all forwarding virtual server.
The destination itself (Option A) is correct for a forwarding VS, and disabling address translation (Option C) is expected and required for IP-forwarding mode. Therefore, the incorrect subnet mask is the sole reason the virtual server is not functioning as expected.

NEW QUESTION # 22
A BIG-IP Administrator notices that one of the servers that runs an application is NOT receiving any traffic. The BIG-IP Administrator examines the configuration status of the application and observes the displayed monitor configuration and affected pool member status.

What is the possible cause of this issue? (Choose one answer)

- A. The node health monitor is NOT responding.
- B. The application is NOT responding with the expected Receive String.
- C. The BIG-IP device is NOT able to reach the pool.
- D. HTTP 1.1 is NOT appropriate for monitoring purposes.

Answer: A

Explanation:
The key clue in the exhibit is the pool member's availability showing "Offline (Enabled) - Parent down". In BIG-IP terminology, a pool member inherits the status of its parent node. If the node is marked down (for example, by a node-level monitor or a default "node is down" condition), then all pool members using that node IP will also be marked down and will not receive any traffic, even if the application service on the member port might be healthy.
While the HTTPS monitor configuration (send/receive strings) is displayed, the status specifically indicates a node (parent) failure, not a service-level failure. If the problem were the application not matching the receive string, you would typically see the member down due to the member's monitor failing (and the status would reflect monitor failure details), rather than "parent down." Option D is too broad; BIG-IP can generally reach the subnet (other servers work), and this symptom points to a specific node condition. Option C is incorrect because HTTP/1.1 is commonly used for monitoring and is valid when properly formatted (especially with a Host header). Therefore, the most likely cause is that the node health monitor is not responding, causing the node-and consequently the member-to be marked down.

NEW QUESTION # 23
A BIG-IP Administrator configured the following virtual server to pass traffic on all addresses and ports. After configuration is completed, the BIG-IP Administrator notices that the virtual server is unable to pass traffic.
ltm virtual forwarding_any_vs {
destination 0.0.0.0:any
ip-forward
mask 255.255.255.255
profiles {
fastL4 { }
}
serverssl-use-sni disabled
source 0.0.0.0/0
translate-address disabled
translate-port disabled
}
Which part of the configuration is the cause of the issue? (Choose one answer)

- A. Incorrect translate-address configured
- B. Incorrect mask 255.255.255.255
- C. Incorrect destination configured

Answer: B

Explanation:
This virtual server is intended to function as a forwarding (IP-forwarding) virtual server, which is commonly used for routing or firewall-style deployments where BIG-IP forwards traffic transparently without load balancing or address translation. For a

forwarding virtual server to match and pass all traffic, the destination must be configured as 0.0.0.0:any with a mask of 0.0.0.0, not 255.255.255.255.
The configured mask 255.255.255.255 represents a /32 host mask, which restricts the virtual server to matching traffic destined only for the exact IP address 0.0.0.0. Since 0.0.0.0 is not a valid routable destination for normal traffic, no packets will ever match the virtual server, causing it to pass no traffic at all.
This is a well-documented BIG-IP behavior:
destination 0.0.0.0:any
mask 0.0.0.0
together define a catch-all forwarding virtual server.
The destination itself (Option A) is correct for a forwarding VS, and disabling address translation (Option C) is expected and required for IP-forwarding mode. Therefore, the incorrect subnet mask is the sole reason the virtual server is not functioning as expected.

NEW QUESTION # 24
.....