



F5 Networks F5CAB5 Practice Questions

Shared by Page on 09-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

A gateway_icmp health monitor is configured on a pool. The BIG-IP Administrator is investigating why the pool is reported as down while the server is online. Other pools with servers in the same subnet are correctly monitored.

What can cause this behavior? (Choose one answer)

Options:

- A- The admin user is logged on the server.
- B- The latest patches have not been installed on the server.
- C- The host-based firewall is active on the server.
- D- The HTTP service is not started on the server.

Answer:

C

Explanation:

A gateway_icmp monitor checks basic network reachability by sending ICMP echo requests (pings) to the pool member or its gateway. If the pool is marked DOWN while the server is confirmed to be online, the most likely cause is that ICMP traffic is being blocked.

A host-based firewall active on the server (Option C) can block ICMP echo requests or replies, preventing BIG-IP from receiving a successful response to the health check. This results in the monitor failing and the pool member being marked down, even though the server and application are otherwise functioning normally. This explanation is consistent with the scenario where other servers in the same subnet work correctly, indicating that routing and BIG-IP configuration are not the issue.

The other options are unrelated to ICMP monitoring. Logged-in users (Option A), missing patches (Option B), and stopped HTTP services (Option D) do not affect a gateway_icmp monitor. BIG-IP troubleshooting best practices recommend verifying ICMP reachability and firewall policies when diagnosing ICMP-based monitor failures.

Question 2

Question Type: MultipleChoice

A BIG-IP Administrator suspects that one of the BIG-IP device power supplies is experiencing power outages.

Which log file should the BIG-IP Administrator check to verify the suspicion? (Choose one answer)

Options:

- A- /var/log/daemon.log
- B- /var/log/kern.log
- C- /var/log/ltn
- D- /var/log/audit

Answer:

C

Explanation:

According to official F5 documentation (K52015891 -- Troubleshooting BIG-IP power supply issues), hardware-related alerts for power supplies, fans, and chassis components are logged in /var/log/ltn.

When a BIG-IP device experiences a power supply issue---such as failure, intermittent outages, or fan-related faults---the system generates alerts through internal platform monitoring services. These alerts are written to the /var/log/ltn file and often appear with messages similar to:

Chassis power supply 2 has experienced an issue. Status is as follows: FAN=bad; STATUS=bad.

This makes /var/log/ltn the authoritative log file for identifying and verifying power supply and chassis-related problems on BIG-IP systems.

The other log files are not appropriate for this purpose:

/var/log/daemon.log contains general daemon messages but is not the primary source for chassis hardware alerts.

/var/log/kern.log logs kernel-level events, not platform power status.

/var/log/audit records administrative actions and configuration changes.

Conclusion:

Per F5-supported guidance, when suspecting power supply outages or chassis hardware issues, the BIG-IP Administrator should always check /var/log/ltn first.

Question 3

Question Type: MultipleChoice

A set of servers is used for an FTP application as well as an HTTP website via separate BIG-IP Pools. The server support team reports that some servers are receiving a lot more traffic than others. Which Load Balancing Method should the BIG-IP Administrator apply to even out the connection count?

Options:

- A- Ratio (Member)
- B- Least Connections (Member)
- C- Least Connections (Node)
- D- Ratio (Node)

Answer:

C

Explanation:

When load balancing is not working as expected across hardware hosting multiple services, the administrator must distinguish between 'member' and 'node' level algorithms. A 'member' is a specific IP and port (e.g., 10.1.1.1:80), while a 'node' is the physical server's IP (10.1.1.1) regardless of the port. If servers host both FTP and HTTP services in separate pools, using 'Least Connections (Member)' only balances connections within each individual pool. This can lead to a skewed distribution where one server is selected for a new HTTP connection because it has the fewest HTTP connections, even if it is currently overloaded with hundreds of FTP connections. By applying 'Least Connections (Node),' the BIG-IP tracks the total number of connections to the physical hardware across all ports and pools. This ensures that the administrator can maintain an even distribution of the total workload across the server fleet, resolving the reports of uneven traffic distribution reported by the server support team.

Question 4

Question Type: MultipleChoice

Without decrypting, what portion of an HTTPS session is visible with a packet capture? (Select one answer)

Options:

- A- HTTP Response Headers
- B- Source IP Address
- C- HTTP Request Headers
- D- Cookies

Answer:

B

Explanation:

In an HTTPS session, the application-layer payload—including HTTP request headers, response headers, cookies, and body content—is encrypted using SSL/TLS. Without decrypting the traffic (for example, without SSL offloading on BIG-IP or access to the private keys), a packet capture cannot reveal any HTTP-level details.

However, network-layer and transport-layer information remains visible, even when encryption is used. This includes source and destination IP addresses, source and destination ports, TCP flags, sequence numbers, and TLS handshake metadata. Therefore, the source IP address (Option B) is visible in a packet capture of HTTPS traffic without decryption.

Options A, C, and D are incorrect because HTTP headers and cookies are part of the encrypted payload once HTTPS is established. BIG-IP troubleshooting documentation emphasizes this distinction when analyzing encrypted traffic flows using tcpdump, as administrators must rely on IP, port, and timing information unless SSL inspection or decryption is configured.

Question 5

Question Type: MultipleChoice

A BIG-IP Administrator makes a configuration change to the BIG-IP device. Which file logs the message regarding the configuration change?

Options:

- A- /var/log/messages
- B- /var/log/audit
- C- /var/log/user.log
- D- /var/log/secure

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Support and Troubleshooting documents: Troubleshooting configuration-related issues requires a clear trail of what was changed and by whom. The BIG-IP system includes a dedicated audit logging feature for this purpose²⁸. Whenever a system object---such as a virtual server, pool, or iRule---is created, modified, or deleted, the system records the event in /var/log/audit²⁹. These logs provide critical context during troubleshooting by showing if a performance drop or traffic failure coincided with a specific administrative action³⁰. Unlike /var/log/ltn, which focuses on local traffic events like pool member status changes, or /var/log/secure, which handles authentication attempts, the audit log specifically tracks the 'how' and 'when' of configuration changes³¹. This is a vital resource for administrators to determine if a virtual server is not working as expected due to a recent manual change or an automated system action, allowing for a rapid 'rollback' or correction of the configuration.

Question 6

Question Type: MultipleChoice

resume is enabled and a health check first fails and then passes?

Options:

- A- Offline (Disabled)
- B- Offline (Enabled)
- C- Available (Disabled)
- D- Available (Enabled)

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Support and Troubleshooting documents: The 'Manual Resume' feature is a safety mechanism used when a pool is not working as expected due to flapping services or unstable backend applications.

Normally, when a health monitor fails, the pool member is marked 'Offline' (Red), and when the monitor passes, it automatically returns to 'Available' (Green)⁴⁷. However, if 'Manual Resume' is enabled, the BIG-IP will not automatically put the member back into rotation after a failure⁴⁸. Even if the health check begins to pass again, the member remains in an 'Offline (Disabled)' state⁴⁹. This requires an administrator to manually intervene and re-enable the member. This is a common point of confusion when troubleshooting; a member may show passing health checks but still not receive traffic because it is waiting for a manual administrative 'resume' command. This feature is intended to prevent 'unhealthy' servers from receiving traffic until an engineer has confirmed the root cause of the initial failure was resolved.

Question 7

Question Type: MultipleChoice

A Virtual Server uses an iRule to send traffic to pool members depending on the URI. The BIG-IP Administrator needs to modify the pool member in the iRule. Which event declaration does the BIG-IP Administrator need to change to accomplish this?

Options:

- A- CLIENT_ACCEPTED
- B- HTTP_RESPONSE
- C- HTTP_REQUEST
- D- SERVER_CONNECTED

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From BIG-IP Administration Support and Troubleshooting documents: In F5 TMOS administration, the traffic flow is processed through specific event huddles w3ithin iRules. To troubleshoot or m4odify traffic based on a URI (Uniform Resource Identifier), the BIG-IP system must first parse the application-layer data. The HTTP_REQUEST event is triggered when the system has fully received and parsed the HTTP request headers from the client⁵. This is the correct point to implement logic that selects a pool or pool member based on the path or file requested (e.g., /images or /api). Using CLIENT_ACCEPTED would be too early in the troubleshooting process because that event triggers at the L4 (TCP) connection establishment phase, before any URI information is available⁶. Conversely, HTTP_RESPONSE occurs during the return traffic from the server, which is too late to make a load balancing decision⁷. For troubleshooting virtual server behavior where URIs are involved, ensuring the iRule is attached to a Virtual Server with an HTTP profile

and using the HTTP_REQUEST event is essential for proper traffic steering and inspection.

Question 8

Question Type: MultipleChoice

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? (Select one answer)

Options:

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

Question 9

Question Type: MultipleChoice

A BIG-IP Administrator creates a new Virtual Server. The end user is unable to access the page. During troubleshooting, the administrator learns that the connection between the BIG-IP system and server is NOT set up correctly. What should the administrator do to solve this issue?

Options:

A- Disable Address Translation

B- Set Address Translation to Auto Map, configure a SNAT pool, and have pool members in the same subnet of the servers

C- Set Address Translation to SNAT and configure a specific translation address

D- Set Address Translation to SNAT and have self-IP configured in the same subnet of servers

Answer:

C

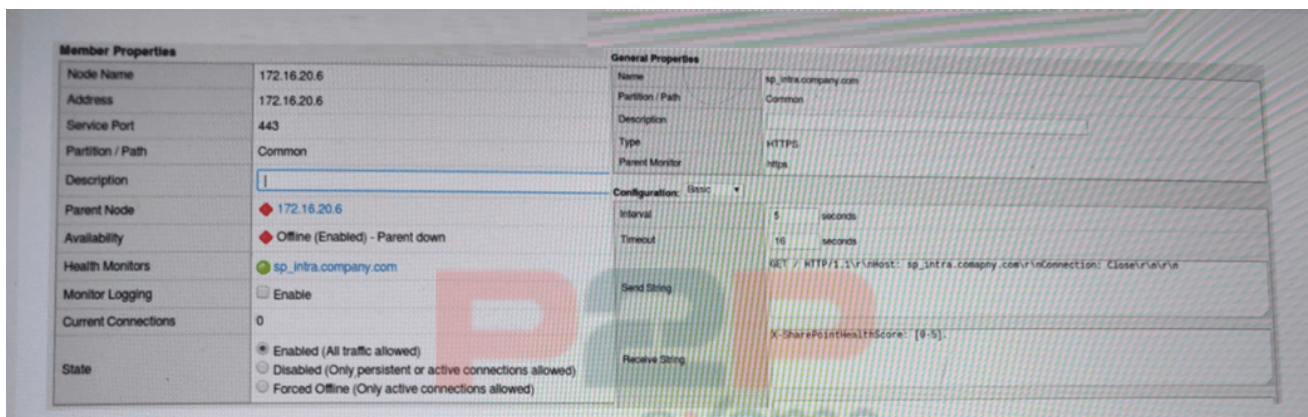
Explanation:

When a virtual server is not working as expected despite the pool members being marked 'UP' (Green), the issue is frequently a return-path routing failure. If the BIG-IP forwards a request with the original client's source IP address, the backend server will try to respond directly to that client. If the server does not have its default gateway pointed back to the BIG-IP, the response packet will be routed elsewhere (or dropped), resulting in a connection timeout for the user. To resolve this, the administrator must configure 'Source Address Translation' (SNAT). By setting SNAT to 'Automap' or a specific SNAT address, the BIG-IP replaces the client's IP with its own internal self-IP. The backend server then sees the BIG-IP as the source and sends the response back to it locally. This troubleshooting step ensures a functional, symmetric traffic flow. Identifying the need for SNAT is one of the most common troubleshooting tasks for new virtual server deployments where the BIG-IP is not the default gateway for the backend servers.

Question 10

Question Type: MultipleChoice

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)

Options:

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

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.

Question 11

Question Type: MultipleChoice

In the BIG-IP Configuration Utility, a user requests a single screen view to determine the status of all Virtual Servers and associated pool members, as well as any iRules in use. Where should the BIG-IP Administrator instruct the user to find this view?

Options:

- A- Local Traffic > Monitors
- B- Local Traffic > Virtual Servers
- C- Local Traffic > Network Map
- D- Statistics

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From BIG-IP A41dministration Support and Troubleshooting documents: To confirm functionality across a complex environment, the 'Network Map' is the most efficient troubleshooting tool in the Configuration Utility⁴³. It provides a hierarchical, visual representation of the traffic management objects⁴⁴. A single glance allows the administrator to see the status of a Virtual Server (Green/Red/Yellow), the status of its associated pool, the health of individual pool members, and which iRules are currently attached⁴⁵. This view is superior to the standard 'Virtual Server List' for troubleshooting because it maps the dependencies between objects⁴⁶. For example, if a Virtual Server is 'Red,' the Network Map will show if that status is inherited from a failed pool or a specific monitor failing on a pool member. Reviewing these basic stats in the Network Map helps the administrator quickly isolate whether a failure is at the service level (Virtual Server), the logic level (iRule), or the hardware level (Pool Member).

Question 12

Question Type: MultipleChoice

A BIG-IP Administrator needs to view the CPU utilization of a particular Virtual Server. Which section of the Configuration Utility should the administrator use for this purpose?

Options:

- A- Statistics > Module Statistics > Local Traffic > Virtual Addresses
- B- Statistics > Module Statistics > Traffic Summary
- C- Statistics > Analytics > Process CPU Utilization
- D- Statistics > Module Statistics > Local Traffic > Virtual Servers

Answer:

D

Explanation:

When a BIG-IP system experiences high overall CPU usage, troubleshooting requires identifying which specific application or service is the primary consumer of resources. While the system-wide performance graphs provide a global view, the granular data necessary to isolate a 'top talker' is found in the 'Local Traffic' statistics. Navigating to Statistics > Module Statistics > Local Traffic > Virtual Servers allows the administrator to see specific metrics for each configured virtual server, including the number of packets processed, current connections, and critical CPU cycles consumed. This is essential for troubleshooting performance issues where an

inefficient iRule, high SSL handshake volume, or complex L7 profiles (like Compression or ASM) might be overtaxing the Traffic Management Microkernel (TMM) for one specific application. By reviewing these basic stats, an administrator can determine if a performance bottle-neck is a system-wide hardware issue or if it is isolated to a single virtual server, enabling targeted remediation such as optimizing iRule logic or moving the high-load virtual server to a dedicated device.



To Get Premium Files for F5CAB5 Visit

<https://www.p2pexams.com/products/f5cab5>

For More Free Questions Visit

<https://www.p2pexams.com/f5-networks/pdf/f5cab5>

20%
DISCOUNT

P2P
exams