PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **F5CAB3**

Title : BIG-IP Administration Data Plane Configuration

Vendor : F5

Version : DEMO

NO.1 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? (Choose one answer)

A. Disable Address Translation

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

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

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

Answer: D

Explanation:

The issue described is a classic symptom of asymmetric routing, which frequently occurs when the BIG-IP system and the back-end servers reside on the same subnet (often referred to as a " one-arm " deployment).

The Routing Problem: By default, the BIG-IP system preserves the original client source IP address when forwarding traffic to a pool member. If the server is in the same subnet as the client or if the server ' s default gateway is not the BIG-IP, the server will attempt to send its response directly back to the client's IP address, bypassing the BIG-IP.

Stateful Failure: Since the BIG-IP is a Full Proxy, it maintains a state table. Because the response packet never returns through the BIG-IP, the system cannot complete the three-way handshake or manage the application session, resulting in a connection failure for the user.

The Solution (SNAT): Enabling Source Network Address Translation (SNAT) solves this by changing the source IP address of the request to an IP address owned by the BIG-IP (typically a self-IP).

Requirement for Subnet Alignment: To ensure the server sends the response back to the BIG-IP, the translation address must be reachable. By using a self-IP configured in the same subnet as the servers, the BIG-IP ensures that the server sees the request coming from a local " neighbor. " The server will then naturally send the response back to that self-IP, allowing the BIG-IP to translate the packet back and forward it to the client.

Why other options are incorrect:

A: Disabling address translation would ensure the server-side traffic uses the client IP, making asymmetric routing inevitable in this scenario.

B: This is technically contradictory; " Auto Map " specifically uses existing self-IPs and does not require or use a " SNAT pool " configuration.

C: While using a specific translation address can work, it does not inherently guarantee the Layer 2/Layer 3 reachability mentioned in the scenario as effectively as ensuring the self-IP is correctly placed in the server ' s subnet.

NO.2 During high-demand traffic events, the BIG-IP Administrator needs to limit new connections per second.

What should be applied?

A. HTTP Compression profile

B. Connection rate limit

C. Connection limit

D. OneConnect profile

Answer: B

Explanation:
Connection rate limiting controls how many new connections per second are accepted, protecting backend resources.

NO.3 A BIG-IP Administrator is configuring an SSH Pool with five members. Which Health Monitor should be applied to ensure that available pool members are monitored accordingly?

A. UDP

B. HTTP

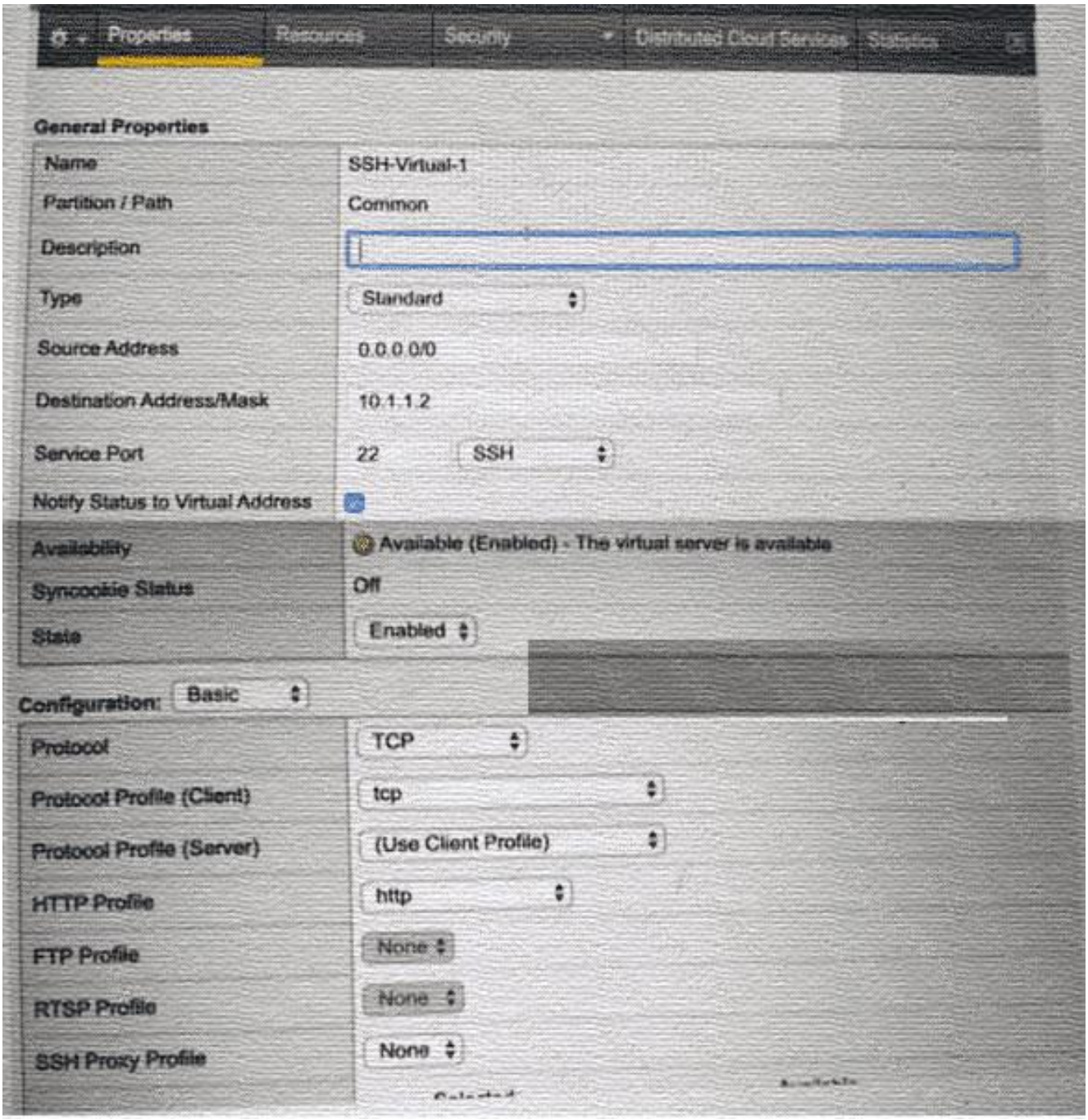
C. HTTPS

D. TCP

Answer: D

Explanation:
SSH (Secure Shell) operates over TCP port 22 , making the TCP health monitor the appropriate and correct choice for monitoring pool members in an SSH pool. The TCP monitor establishes a basic Layer 4 connection to each pool member on the designated port, verifying that the server is reachable and actively accepting TCP connections. A successful three-way handshake confirms the pool member is available; a failure marks it down and removes it from load balancing rotation.
The remaining monitor types are inappropriate for this use case:
* UDP monitor operates at Layer 4 but uses the connectionless UDP protocol, which is incompatible with SSH since SSH exclusively uses TCP as its transport.
* HTTP monitor sends a Layer 7 GET request expecting an HTTP response - irrelevant for an SSH service that does not speak the HTTP protocol.
* HTTPS monitor functions identically to HTTP but over TLS - again, completely misaligned with SSH traffic and port behaviour.
For application-specific SSH validation beyond basic TCP connectivity, an external monitor or custom monitor could be used; however, TCP remains the standard and correct built-in monitor for SSH pool verification within the BIG-IP platform.
Reference: BIG-IP Administration - Data Plane Configuration, Module: Health Monitors - Monito
r Types and Protocol Alignment.

NO.4 Refer to the exhibit.



A BIG-IP Administrator creates a new Virtual Server to load balance SSH traffic. Users are unable to log on to the servers.

What should the BIG-IP Administrator do to resolve the issue? (Choose one answer)

A. Set Protocol to UDP

B. Set Source Address to 10.1.1.2

C. Set Destination Address/Mask to 0.0.0.0/0

D. Set HTTP Profile to None

Answer: D

Explanation:

SSH is a Layer 4 TCP-based protocol that operates on TCP port 22 and does not use HTTP in any capacity. In the exhibit, the Virtual Server is configured with an HTTP Profile applied, which is inappropriate for SSH traffic and causes connection failures.

According to the BIG-IP Administration: Data Plane Configuration documentation:
An HTTP profile must only be applied to Virtual Servers handling HTTP or HTTPS traffic.
When an HTTP profile is attached, BIG-IP expects HTTP headers and attempts to parse application-layer data.
Non-HTTP protocols such as SSH, FTP (control), SMTP, and other raw TCP services will fail if an HTTP profile is enabled.
Why the other options are incorrect:
A). Set Protocol to UDPSSH uses TCP, not UDP. Changing the protocol would break SSH entirely.
B). Set Source Address to 10.1.1.2The source address setting controls client access restrictions and is unrelated to protocol parsing issues.
C). Set Destination Address/Mask to 0.0.0.0/0The destination address is already valid for a specific SSH service and does not impact protocol handling.
Correct Resolution:
The BIG-IP Administrator should remove the HTTP Profile (set it to None) so the Virtual Server functions as a pure Layer 4 TCP service, allowing SSH connections to pass through successfully.

NO.5 Local Traffic Network Map: VS_HTTP # POOL_WEB # 192.168.212.30:80 Pool Member | Parent Node
192.168.212.30 Port 80
Why is the virtual server unresponsive to incoming connections?
A. The node monitor failed.
B. The pool member monitor failed.
C. The pool member is disabled.
D. The node is disabled.
Answer: D
Explanation:
In the BIG-IP object hierarchy, a Pool Member is a child object of a Node . A pool member represents a specific IP:Port combination, while the parent node represents the underlying server IP address.
When a node is disabled , all pool members that are children of that node are rendered unavailable - regardless of the individual pool member ' s own health or enabled state.
The Network Map depicted shows the pool member (192.168.212.30:80) with its Parent Node (192.168.212.30) disabled. This parent-child dependency means that even if the pool member itself is healthy and enabled, the disabled node cascades its unavailable state downward, causing the pool to have no available members and rendering VS_HTTP unresponsive to incoming connections.
The other options can be eliminated as follows:
* Pool member monitor failed - the monitor status is not indicated as failed in the Network Map display.
* Pool member is disabled - the pool member itself is not shown as disabled; the parent node is.
* Node monitor failed - no monitor failure is indicated; the node ' s administrative state is explicitly disabled.
Understanding the node-to-member inheritance of availability state is fundamental to accurate BIG-IP traffic troubleshooting.
Reference: BIG-IP Administration - Data Plane Configuration, Module: Pool Members, Nodes, and Availability State Inheritance.

NO.6 The BIG-IP Administrator needs to load balance a pool of web servers. Load balancing should

consider the number of connections that are active on that pool member.
Which load balancing method meets this requirement? (Choose one answer)
A. Least Connections (member)
B. Round Robin
C. Ratio (member)
D. Ratio (node)
Answer: A
Explanation:
The requirement states that load balancing decisions must be based on the number of active connections on each pool member. This directly maps to the Least Connections (member) load balancing method.
According to the BIG-IP Administration: Data Plane Configuration documentation:
Least Connections (member) selects the pool member with the fewest active connections at the time of the request.
This method dynamically adapts to real-time traffic patterns and ensures that more heavily loaded pool members receive fewer new connections.
It is especially effective for web servers where connection duration may vary and equal distribution of active sessions is desired.
Why the other options are incorrect:
B). Round RobinDistributes connections sequentially without considering current load or active connections.
C). Ratio (member)Distributes traffic based on static ratios, not real-time connection counts.
D). Ratio (node)Uses predefined ratios at the node level and does not account for active connection counts.
Correct Resolution:
Using Least Connections (member) ensures that new connections are directed to the pool member currently handling the fewest active connections, meeting the stated requirement.

NO.7 Refer to the exhibit.

A BIG-IP Administrator needs to configure health monitors for a newly configured server pool named Pool_B.

Which health monitor settings will ensure that all pool members will be accurately marked as available or unavailable? (Choose one answer)

A. HTTPS, HTTP, FTP, and SSH with the Availability Requirement of all health monitors

B. HTTP, HTTPS, FTP, and ICMP with the Availability Requirement of at least one health monitor

C. HTTPS, HTTP, FTP, and SSH with the Availability Requirement of at least one health monitor

D. HTTPS, HTTP, FTP, and SSH with the Availability Requirement of all health monitors

Answer: C

Explanation:

From the exhibit, the pool contains different applications on different service ports (for example, HTTP/80, FTP/21, HTTPS/443, SSH/22). To mark pool members correctly, BIG-IP must be able to verify the actual service running on each member's port.

In BIG-IP Administration: Data Plane Configuration, monitor behavior is described as follows:

When multiple monitors are assigned to a pool, the Availability Requirement controls how monitor results are evaluated:

At least one = the pool member is marked up if any one of the assigned monitors succeeds.

All = the pool member is marked up only if every assigned monitor succeeds.

For pools containing members with different services/ports, using All can incorrectly mark members down because monitors intended for other services will fail on the wrong port.

Why C is correct:

Assigning HTTPS, HTTP, FTP, and SSH covers the actual services shown in the pool.

Setting the Availability Requirement to at least one ensures that each pool member is considered available when its appropriate service monitor succeeds, without being forced to pass unrelated service monitors.

Why the other options are incorrect:

A / D (Availability Requirement = all): would cause members to be marked down when unrelated monitors fail (e.g., SSH monitor against an HTTP member).

B (includes ICMP): ICMP can indicate the host is reachable even if the application service is down, which does not "accurately" reflect service availability.
Therefore, the best choice is HTTPS, HTTP, FTP, and SSH with Availability Requirement of at least one health monitor.

NO.8 A Standard Virtual Server for a web application is configured with SNAT Automap. The original client IP must be known by backend servers.
What should the BIG-IP Administrator configure?

A. Performance (HTTP) Virtual Server

B. HTTP profile with X-Forwarded-For

C. HTTP Transparent profile

D. SNAT pool using client IP

Answer: B

Explanation:
X-Forwarded-For inserts the original client IP into HTTP headers while SNAT is enabled.