KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

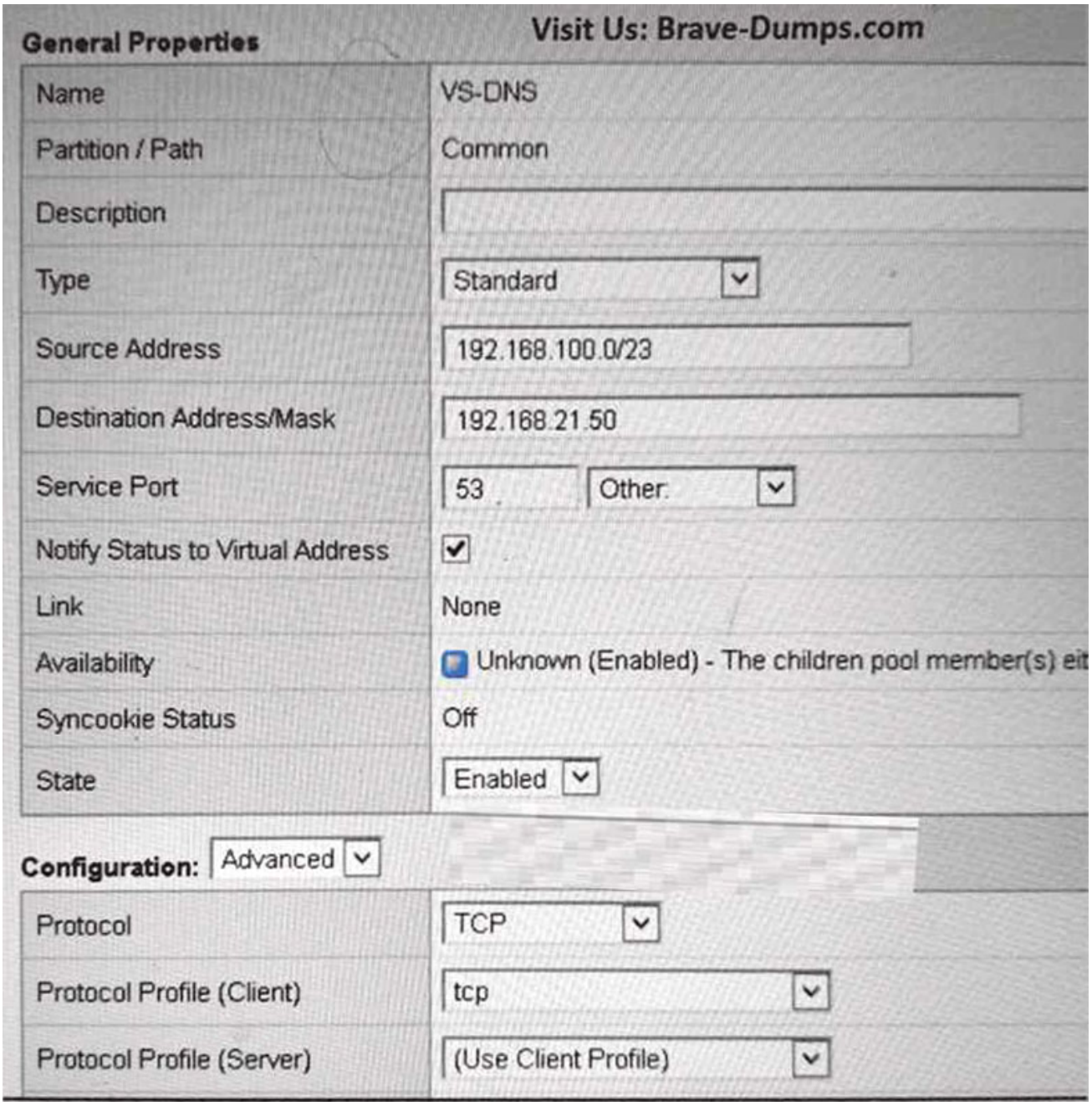
www.kaozhengpro.com

Exam : **F5CAB3**

Title : BIG-IP Administration Data Plane Configuration

Version : DEMO

1.Refer to the exhibit.



DNS queries from two internal DNS servers are being load-balanced to external DNS servers via a virtual server on a BIG-IP device.
The DNS queries originate from:
192.168.10.100
192.168.10.200
and target:
192.168.2.150
All DNS queries destined for the external DNS servers fail.
Which property change should the BIG-IP Administrator make in the Virtual Server to resolve this issue? (Choose one answer)
A. Protocol profile (Client) to DNS_OPTIMIZED

B. Type to Performance (HTTP)
C. Source Address to 192.168.10.0/24
D. Protocol to UDP
Answer: D
Explanation:
DNS traffic is primarily transported using UDP port 53. In the exhibit, the Virtual Server is configured with the Protocol set to TCP, which prevents standard DNS queries from being processed correctly. BIG-IP Virtual Servers must be configured with the correct Layer 4 protocol to match the application traffic they are handling.
According to the BIG-IP Administration: Data Plane Configuration documentation:
The Protocol setting on a Virtual Server defines whether traffic is processed as TCP, UDP, or another supported transport protocol.
Standard DNS queries and responses use UDP, while TCP is only required for DNS zone transfers (AXFR) or exceptionally large responses.
When a DNS Virtual Server is incorrectly configured with TCP, UDP-based DNS queries are dropped, causing all requests to fail.
Why the other options are incorrect:
A. Protocol profile (Client) to DNS_OPTIMIZEDA DNS profile enhances DNS functionality but does not correct an incorrect transport protocol configuration.
B. Type to Performance (HTTP)Performance (HTTP) Virtual Servers are designed for HTTP traffic and are not suitable for DNS services.
C. Source Address to 192.168.10.0/24The existing source IPs already fall within the allowed range, so this setting does not address the failure.
Correct Resolution:
Changing the Protocol to UDP aligns the Virtual Server with standard DNS transport requirements, allowing DNS queries to be successfully processed and load-balanced.

2.A BIG-IP Administrator finds the following log entry after a report of user issues connecting to a virtual server:
01010201: Intercept exhaustion on 10.70.110.112 to 192.28.123.250:80 (proto 6)
How should the BIG-IP Administrator modify the SNAT pool that is associated with the virtual server? (Choose one answer)
A. Increase the timeout of the SNAT addresses
B. Remove the SNAT pool and apply SNAT Automap
C. Remove an IP address from the SNAT pool
D. Add an IP address to the SNAT pool
Answer: D
Explanation:
The log message “Intercept exhaustion” indicates that the BIG-IP system has exhausted the available source port translations for one or more SNAT addresses. This occurs when too many concurrent client connections are being translated through a limited number of SNAT IP addresses, and all ephemeral source ports (typically ~64,000 per SNAT IP) are in use.
According to the BIG-IP Administration: Data Plane Configuration documentation:
Each SNAT IP address provides a finite number of available source ports.

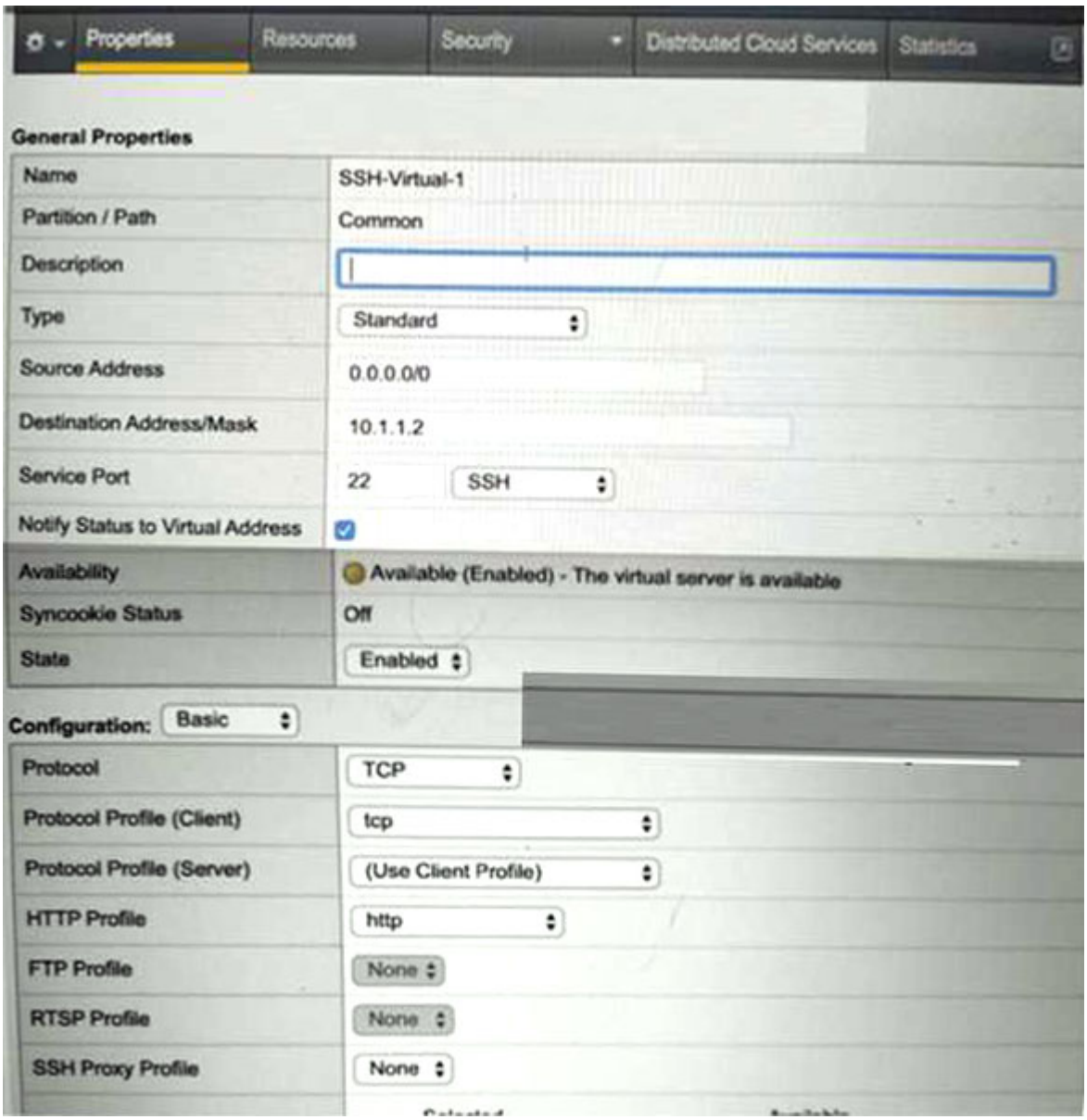
When the number of concurrent connections exceeds the available port space, the BIG-IP logs an Intercept exhaustion error and new connections fail.
The recommended resolution is to increase the available SNAT resources by adding additional IP addresses to the SNAT pool.
Why the other options are incorrect:
A. Increase the timeout of the SNAT addresses Increasing timeouts may actually worsen the problem by keeping ports allocated longer, accelerating port exhaustion.
B. Remove the SNAT pool and apply SNAT Automap SNAT Automap uses the Self IP addresses on the egress VLAN, which may not provide additional capacity and can introduce routing or design issues. This is not a direct or recommended fix for SNAT exhaustion.
C. Remove an IP address from the SNAT pool This would reduce the number of available source ports and further exacerbate the intercept exhaustion condition.
Correct Resolution:
By adding an IP address to the SNAT pool, the BIG-IP increases the total number of available source ports, alleviating intercept exhaustion and restoring successful client connections.

3.A BIG-IP Administrator uses backend servers to host multiple services per server. There are multiple virtual servers and pools defined, referencing the same backend servers.
Which load balancing algorithm is most appropriate to have an equal number of connections on each backend server? (Choose one answer)
A. Least Connections (node)
B. Predictive (member)
C. Least Connections (member)
D. Predictive (node)
Answer: A
Explanation:
In this scenario, each backend node (server) hosts multiple services and is referenced by multiple pools and virtual servers. The goal is to ensure an equal number of total connections per backend server, regardless of how many pool members (services/ports) exist on that server.
According to the BIG-IP Administration: Data Plane Configuration documentation:
Least Connections (node) tracks the total number of active connections to a node across all pool members and services.
This algorithm ensures load distribution is balanced at the server level, not just at the individual service (member) level.
It is specifically recommended when:
Multiple pool members exist on the same backend server
Multiple virtual servers reference the same backend servers
Why the other options are incorrect:
B. Predictive (member)Predictive algorithms are advanced and traffic-pattern based, but they operate at the member level and do not guarantee equal connections per server.
C. Least Connections (member)This balances connections per pool member, which can overload a server hosting multiple members while still appearing “balanced” per member.
D. Predictive (node)Although node-aware, predictive algorithms are less deterministic and not the best choice when strict equality of connections is required.

Correct Resolution:
Using Least Connections (node) ensures that each backend server carries an equal connection load across all services and pools.

4.The BIG-IP Administrator is investigating whether better TCP performance is possible for a virtual server.
Which built-in profile should be tried first? (Choose one answer)
A. f5-tcp-legacy
B. f5-tcp-progressive
C. f5-tcp-mobile
D. No option
Answer: B
Explanation:
BIG-IP provides several built-in TCP profiles optimized for different traffic patterns and network conditions. When attempting to improve general TCP performance, the recommended starting point is f5-tcp-progressive.
According to the BIG-IP Administration: Data Plane Configuration documentation:
f5-tcp-progressive is designed as a balanced, general-purpose TCP optimization profile.
It dynamically adjusts TCP behavior to improve throughput and latency for most enterprise applications.
It is the recommended first-choice profile when tuning TCP performance before moving to more specialized profiles.
Why the other options are incorrect:
A. f5-tcp-legacyThis profile exists for backward compatibility and does not include modern TCP optimizations.
C. f5-tcp-mobileThis profile is optimized specifically for high-latency, lossy mobile networks and is not suitable for general-purpose environments.
D. No option B IG-IP explicitly provides built-in TCP profiles for performance tuning; using none would forgo optimization opportunities.
Correct Resolution:
The administrator should first apply f5-tcp-progressive to evaluate potential TCP performance improvements before considering more specialized profiles.

5.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.