DUMPSARENA

VMware Avi Load 30.x Administrator

VMware 6V0-22.25

Version Demo

Total Demo Questions: 6

Total Premium Questions: 61

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Technologies	18
Topic 2, Products and Solutions	3
Topic 3, Planning and Designing	1
Topic 4, Installing, Configuring, and Setup	20
Topic 5, Performance-tuning, Optimization, and Upgrades	2
Topic 6, Troubleshooting and Repairing	13
Topic 7, Administrative and Operational Tasks	4
Total	61

QUESTION NO: 1

The Avi Controller becomes temporarily unreachable from all Service Engines, but the Service Engines and pool members remain operational. What is the most likely immediate effect on an existing Virtual Service?

A. The Virtual Service immediately stops accepting client connections

B. The Virtual Service continues processing traffic with its last known configuration

C. Pool health monitoring immediately stops on all Service Engines

D. All Service Engines automatically restart to elect a new Controller

ANSWER: B

Explanation:

The Virtual Service continues to process existing client traffic because Service Engines are the Avi data plane. They retain the configuration already distributed by the Controller and continue to perform functions such as traffic forwarding, load balancing, and pool health monitoring.

Controller unavailability prevents centralized management operations such as publishing new configuration changes and can affect analytics visibility, but it does not immediately stop correctly configured Service Engines from serving an existing Virtual Service. The Controller does not proxy each client transaction.

QUESTION NO: 2

A Virtual Service must preserve the original client source IP address when forwarding traffic to pool members. Which two design requirements must be considered? Choose two.

A. Enable Preserve Client IP Address in the Virtual Service Network Service settings

B. Ensure that return traffic from pool members is routed through the Service Engine

C. Enable X-Forwarded-For header insertion in the HTTP Application Profile

D. Use Elastic Active-Active high availability mode

E. Configure HTTP Cookie Persistence on the Virtual Service

ANSWER: A B

Explanation:

Enable Preserve Client IP Address on the Virtual Service and **ensure that return traffic from the pool members is routed through the Service Engine** are correct. The Virtual Service setting disables SNAT for the applicable traffic, allowing the backend server to receive the original client address.

Without SNAT, the backend server must return traffic through the Service Engine to preserve a symmetric connection path. X-Forwarded-For is an HTTP header mechanism and does not preserve the Layer 3 source address. Cookie persistence is unrelated to source-address preservation, while Elastic Active-Active is not the required HA design for this non-SNAT use case.

QUESTION NO: 3

Which three functions are performed by the Avi Load Balancer data plane? Choose three.

A. Terminate and process client application traffic

B. Execute pool health monitors

C. Select eligible pool members for requests

D. Index client logs for centralized search

E. Manage configuration backups

ANSWER: A B C

Explanation:

Terminate and process client application traffic, **execute pool health monitors**, and **select eligible pool members for requests** are data-plane functions performed by Service Engines. Service Engines process Virtual Service traffic locally and make immediate forwarding decisions using the configuration distributed by the Controller.

The Controller provides centralized management and analytics functions. It indexes client logs and manages configuration backups, but it does not process production client traffic or execute the active health-monitor probes sent to pool members.

QUESTION NO: 4

Which configuration results in a Virtual Service being marked down by the Service Engine?

A. The Pool is configured with the wrong health monitor

B. The HTTP Policy is configured to send a local response

C. The DataScript is attached to the Virtual Service without a default pool

D. The HTTP Redirect policy is attached to the Virtual Service, and the pool is marked down by health check

ANSWER: C

Explanation:

The DataScript is attached to the Virtual Service without a default pool is the configuration that can cause the Service Engine to mark the Virtual Service down. A Virtual Service normally needs a usable forwarding destination for requests that reach it. The default pool supplies that destination when policy or DataScript logic does not explicitly select a different pool. When a DataScript is attached but the Virtual Service has no default pool, the script must provide valid pool-selection behavior for the applicable traffic path. Otherwise, the Service Engine has no eligible backend destination to which it can forward the request. This creates an invalid traffic-processing path for the Virtual Service and can result in its operational state being reported as down.

DataScript is evaluated by the Service Engine during request processing and can influence pool selection. Consequently, a DataScript design must ensure that matching requests reach a valid selected pool, or that a default pool is available as the fallback. This requirement is especially important when a script contains conditional logic, because requests that do not meet a pool-selection condition still require a valid forwarding path. Broadcom's Avi Load Balancer documentation describes Virtual Service pool configuration and DataScript capabilities in the Avi Load Balancer documentation and the Avi DataScript and automation documentation.

QUESTION NO: 5

Which three statements are true for Connection Multiplexing? Choose three.

A. Multiplexing does not support UDP

B. Multiplexing is not compatible with NTLM authentication

C. Multiplexing results in a higher number of server-side connections

D. Multiplexing reduces the number of server-side connections

E. Multiplexing causes unbalanced distribution of HTTP requests across servers

ANSWER: A B D

Explanation:

Connection multiplexing is an HTTP application-profile capability in Avi Load Balancer that decouples client-side connections from server-side connections. Avi can accept requests on many client TCP connections while reusing a smaller pool of persistent TCP connections to backend servers. Consequently, *Multiplexing reduces the number of server-side connections*, which lowers TCP handshake, teardown, and associated resource overhead on the application servers. The feature operates in the HTTP request-processing path, including HTTP/1.0 and HTTP/1.1 request switching, rather than for generic Layer-4 traffic; therefore, *Multiplexing does not support UDP*. UDP is connectionless and has no server-side TCP connection that could be reused. *Multiplexing is not compatible with NTLM authentication* because NTLM uses connection-oriented authentication behavior. Maintaining the expected association between an authenticated client and a backend connection is essential for that authentication flow, whereas multiplexing intentionally allows backend TCP connections to be shared across requests. These characteristics should be considered when configuring an HTTP application profile, particularly for applications that use connection-bound authentication or require dedicated server connections. See the Avi Load Balancer documentation at HTTP Application Profiles and the Broadcom VMware Tanzu documentation portal.

QUESTION NO: 6

Where are application traffic log messages specific to WAF found for a Virtual Service?

A. Alerts tab of the Operations screen

B. Logs tab of the Virtual Service detail screen

C. Analytics tab of the Virtual Service detail screen

D. Security tab of the Virtual Service detail screen

ANSWER: D

Explanation:

Security tab of the Virtual Service detail screen is the correct location because Avi Load Balancer presents WAF-specific request events in the Virtual Service's security context. When a WAF policy is attached to a Virtual Service, the system evaluates incoming HTTP/S requests against configured rules and signatures. The resulting security event records include useful investigation details such as the matched rule or signature, the action taken, request attributes, and client context. Administrators use these WAF log entries to investigate detected attacks, validate enforcement behavior, tune WAF policy settings, and distinguish legitimate traffic from requests that trigger security protections. This placement keeps security inspection workflows associated with the protected application itself: open the applicable Virtual Service and use its Security view to review WAF-related application traffic messages. Avi documentation describes WAF as a Virtual Service security capability and documents the associated operational monitoring and logging information in the administration guidance. See the VMware Avi Load Balancer documentation portal and the Avi Load Balancer Administration Guide for WAF configuration and monitoring details.