



**Vendor:** VMware

**Exam Code:** 6V0-22.25

**Exam Name:** VMware Avi Load Balancer 30.x Administrator

**Version:** DEMO

### QUESTION 1

Which functionality cannot be configured via a Network Security Policy?

- A. IP Reputation
- B. Botnet Detection
- C. Rate Limit
- D. Block selected countries

**Answer: B**

**Explanation:**

Avi Network Security Policies are evaluated at the network-security layer and can be used for actions such as allowing, dropping, denying, rate limiting, and applying rules based on client characteristics such as IP reputation or geolocation. Blocking selected countries is supported through geolocation- based matching, and IP reputation is also a supported security capability in Avi. Rate limiting is a valid Network Security Policy action. Botnet Detection, however, is not configured through a Network Security Policy. Bot detection and bot management are part of Avi's WAF and bot- management security features, associated with application-layer HTTP security rather than the network security policy object. Therefore, the function that cannot be configured through a Network Security Policy is Botnet Detection.

### QUESTION 2

An application had an outage during an Avi upgrade. The Service Engine Group assigned to the Virtual Service is using the default configuration. What is the likely reason for this outage?

- A. There was a global internet outage
- B. The Virtual Service was not scaled out
- C. Firewall rules were not configured for the failover Service Engine
- D. This is by design since Service Engine upgrades are disruptive

**Answer: B**

**Explanation:**

Avi upgrades can be performed with minimal disruption when Virtual Services have sufficient Service Engine redundancy. VMware Avi documentation for upgrades explains that upgrades are disruptive for Virtual Services running in Elastic HA N+M Buffer mode when the Virtual Service is placed on only one Service Engine and is not scaled out. The default Service Engine Group configuration commonly results in a Virtual Service being placed on a single active Service Engine unless it is manually or automatically scaled out. During a Service Engine upgrade, traffic can be interrupted if there is no additional active Service Engine already carrying that Virtual Service. Therefore, the most likely cause of the outage is that the Virtual Service was not scaled out.

### QUESTION 3

Which metrics graph in the Virtual Service Analytics page will show the rate of 5xx errors?

- A. Conns
- B. Requests
- C. HTTP Errors
- D. End-to-End Timing

**Answer: B**

**Explanation:**

The Virtual Service Analytics page provides different graph categories for traffic, connection,

timing, and error visibility. VMware Avi documentation states that the Requests chart shows the number of responses to requests per second and breaks down successful requests versus errors, including 4xx and 5xx errors. This makes the Requests graph the appropriate place to view the rate of HTTP 5xx errors for a Virtual Service. The Conns graph is focused on connection counts and rates, while End-to-End Timing shows timing components such as client RTT, server RTT, application response, and data transfer. "HTTP Errors" may sound plausible, but in the Avi Virtual Service Analytics graph naming described here, 5xx rate visibility is included under Requests.

#### QUESTION 4

The "N" in N+M Elastic HA refers to which Service Engine Group parameter?

- A. Minimum scale per Virtual Service
- B. Maximum number of Service Engines
- C. Number of buffer Service Engines
- D. Maximum number of Virtual Services per Service Engine

**Answer: A**

**Explanation:**

In Avi Load Balancer Elastic HA N+M mode, the Service Engine Group maintains a defined active scale and buffer capacity for redundancy and placement flexibility. VMware Avi documentation explains that in N+M mode, N represents the minimum number of Service Engines required for a Virtual Service, while M represents the spare or buffer capacity that Avi attempts to maintain across the Service Engine Group. This means N is related to the minimum active scale for the Virtual Service, not the total maximum number of Service Engines in the group, not the number of buffer Service Engines, and not the maximum number of Virtual Services per Service Engine. Therefore, the correct parameter for N is Minimum scale per Virtual Service.

#### QUESTION 5

Which WAF inspection method is the most computationally expensive?

- A. Signature
- B. Allow List
- C. Mode Delegation
- D. Positive Security

**Answer: D**

**Explanation:**

Avi WAF supports several inspection methods, including signature-based protection, allow-list style controls, and Positive Security. Positive Security is more computationally expensive because it validates application behavior against learned or configured rules that define what is explicitly allowed. This requires deeper inspection and more rule evaluation than simply matching known attack signatures. Signature inspection generally compares requests against known malicious patterns, while Positive Security evaluates whether requests conform to permitted application behavior. VMware Avi WAF documentation describes Positive Security and learning as a deeper application security method. Because it performs more detailed validation of acceptable behavior, it consumes more processing resources than the other listed methods. Therefore, the most computationally expensive inspection method is Positive Security.

#### QUESTION 6

What is a valid reason to configure the Custom mode for the TCP Proxy Profile?

- A. Enable Port Address Translation
- B. Configure the default gateway
- C. Statically increase the TCP Receive Window size
- D. Expose client destination TCP port to the application

**Answer: D**

**Explanation:**

The TCP Proxy Profile controls TCP behavior for a Virtual Service. Avi provides system TCP proxy profiles for common use cases, but Custom mode is used when an administrator needs to modify specific TCP proxy behavior beyond the default templates. In this question, the key valid use case is exposing the original client destination TCP port to the application. This is useful when the Virtual Service listens on multiple ports or when the backend application needs awareness of the client-facing destination port. Port Address Translation is handled through Virtual Service and pool port mappings, not as the main reason for TCP Proxy Custom mode. Default gateway configuration is a network routing function, and statically increasing the TCP receive window is not the best Avi-specific answer here. Therefore, the correct choice is D.

**QUESTION 7**

A Virtual Service is configured with an HTTP Security Policy, Network Security Policy, DataScript Response, and an HTTP Request Policy. In which order will these be evaluated?

- A. HTTP Security -> Network Security -> HTTP Request -> DataScript Response
- B. DataScript Response -> Network Security -> HTTP Request -> HTTP Security
- C. Network Security -> HTTP Security -> HTTP Request -> DataScript Response
- D. Network Security -> HTTP Request -> HTTP Security -> DataScript Response

**Answer: C**

**Explanation:**

Avi evaluates traffic according to the processing stage in the packet and HTTP transaction flow. Network Security Policy is evaluated first because it operates at the connection or network-security layer before HTTP request processing. After traffic is allowed through the network-security stage, HTTP security processing is applied to the HTTP transaction. HTTP Request Policies are then evaluated on the request path, where administrators can perform actions such as redirecting, switching pools, modifying headers, or sending a local response. DataScript Response runs later on the response side, after the request has been processed and a response is being handled. This staged order is why the correct sequence is Network Security -> HTTP Security -> HTTP Request DataScript Response.

**QUESTION 8**

Accessing an HTTPS Virtual Service displays an untrusted certificate error. Which option would not cause this issue?

- A. The certificate has expired
- B. The certificate is an RSA certificate instead of an EC certificate
- C. The default self-signed certificate was selected for the Virtual Service
- D. The certificate is signed by a valid internal CA, but it is not trusted by the client

**Answer: B**

**Explanation:**

An HTTPS client shows an untrusted certificate warning when the presented certificate cannot be validated by the client. Common causes include an expired certificate, a self-signed certificate, or a certificate signed by an internal certificate authority that the client does not trust. Avi

documentation distinguishes between RSA and EC certificates as certificate algorithm types that can both be used by Virtual Services. A certificate being RSA instead of EC does not inherently make it untrusted. RSA certificates are still valid and supported when issued by a trusted CA, within their validity period, and matching the requested hostname. Therefore, the certificate algorithm alone is not a cause of an untrusted certificate error. The answer that would not cause the issue is B.

#### QUESTION 9

Which three techniques can improve the performance of a Virtual Service running on a busy Service Engine? Choose three.

- A. Migrate other Virtual Services to different Service Engines
- B. Increase the CPU and memory on all Service Engines in the Service Engine Group
- C. Increase the CPU and memory on all Controllers
- D. Use ECMP to scale the Virtual Service across Service Engines
- E. Move the Virtual Service from EC to RSA certificates and keys

**Answer:** ABD

**Explanation:**

Virtual Service performance is driven primarily by Service Engine data-plane capacity, not Controller resources. If a Service Engine is busy, performance can be improved by reducing the workload on that SE, vertically scaling SE resources, or horizontally scaling traffic across additional Service Engines. Migrating other Virtual Services away reduces contention for CPU, memory, and packet- processing capacity. Increasing CPU and memory on Service Engines increases data-plane capacity, although the SE VM may require reboot depending on the environment. ECMP scale-out can distribute traffic across multiple Service Engines and improve throughput. Increasing Controller CPU and memory helps management or analytics capacity, not Virtual Service data-plane performance. Moving from EC to RSA would usually reduce SSL performance because RSA processing is generally more expensive. Therefore, the correct choices are A, B, and D.

#### QUESTION 10

Which issue or scenario requires elastic scale-out?

- A. Mitigating disruption if a Controller fails
- B. Processing requests across multiple protocols
- C. Managing heavy increases in traffic volume without disruption
- D. Enabling Web Application Firewall

**Answer:** C

**Explanation:**

Elastic scale-out is used to increase data-plane capacity by placing a Virtual Service on additional Service Engines or by increasing Service Engine capacity in response to demand. Avi Elastic HA combines scale-out performance and high availability, and Avi autoscale features are designed to add Service Engine capacity when traffic growth requires more resources. This directly addresses situations where a Virtual Service must handle heavy increases in traffic volume without application disruption. Controller failure protection is handled by Controller clustering, not elastic data-plane scale-out. Processing multiple protocols is a Virtual Service design and profile configuration concern. Enabling WAF is an application security feature and can increase resource needs, but it does not itself define the scenario requiring elastic scale-out. Therefore, the correct answer is C.

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**