



# 1Z0-997<sup>Q&As</sup>

Oracle Cloud Infrastructure 2019 Architect Professional

## Pass Oracle 1Z0-997 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/1z0-997.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Oracle  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

You are building a highly available and fault tolerant web application deployment for your company. Similar application delayed by competitors experienced web site attack including DDoS which resulted in web server failing. You have decided to use Oracle Web Application Firewall (WAF) to implement an architecture which will provide protection against such attacks and ensure additional configuration will you need to implement to make sure WAF is protecting my web application 24?. Which additional configuration will you need to Implement to make sure WAF Is protecting my web application 24??

- A. Configure auto scaling policy and it to WAF instance.
- B. Configure Control Rules to send traffic to multiple web servers
- C. Configure multiple origin servers
- D. Configure new rules based on now vulnerabilities and mitigations

Correct Answer: C

**Origin Management** An origin is an endpoint (typically an IP address) of the application protected by the WAF. An origin can be an Oracle Cloud Infrastructure load balancer public IP address. A load balancer IP address can be used for high availability to an origin. Multiple origins can be defined, but only a single origin can be active for a WAF. You can set HTTP headers for outbound traffic from the WAF to the origin server. These name value pairs are then available to the application. Oracle Cloud Infrastructure Web Application Firewall (WAF) is a cloud-based, Payment Card Industry (PCI) compliant, global security service that protects applications from malicious and unwanted internet traffic. WAF can protect any internet facing endpoint, providing consistent rule enforcement across a customer's applications. WAF provides you with the ability to create and manage rules for internet threats including Cross-Site Scripting (XSS), SQL Injection and other OWASP-defined vulnerabilities. Unwanted bots can be mitigated while tactically allowed desirable bots to enter. Access rules can limit based on geography or the signature of the request. Distributed Denial of Service (DDoS) A DDoS attack is an often intentional attack that consumes an entity's resources, usually using a large number of distributed sources. DDoS can be categorized into either Layer 7 or Layer 3/4 (L3/4) A layer 7 DDoS attack is a DDoS attack that sends HTTP/S traffic to consume resources and hamper a website's ability to delivery content or to harm the owner of the site. The Web Application Firewall (WAF) service can protect layer 7 HTTP-based resources from layer 7 DDoS and other web application attack vectors.

---

**QUESTION 2**

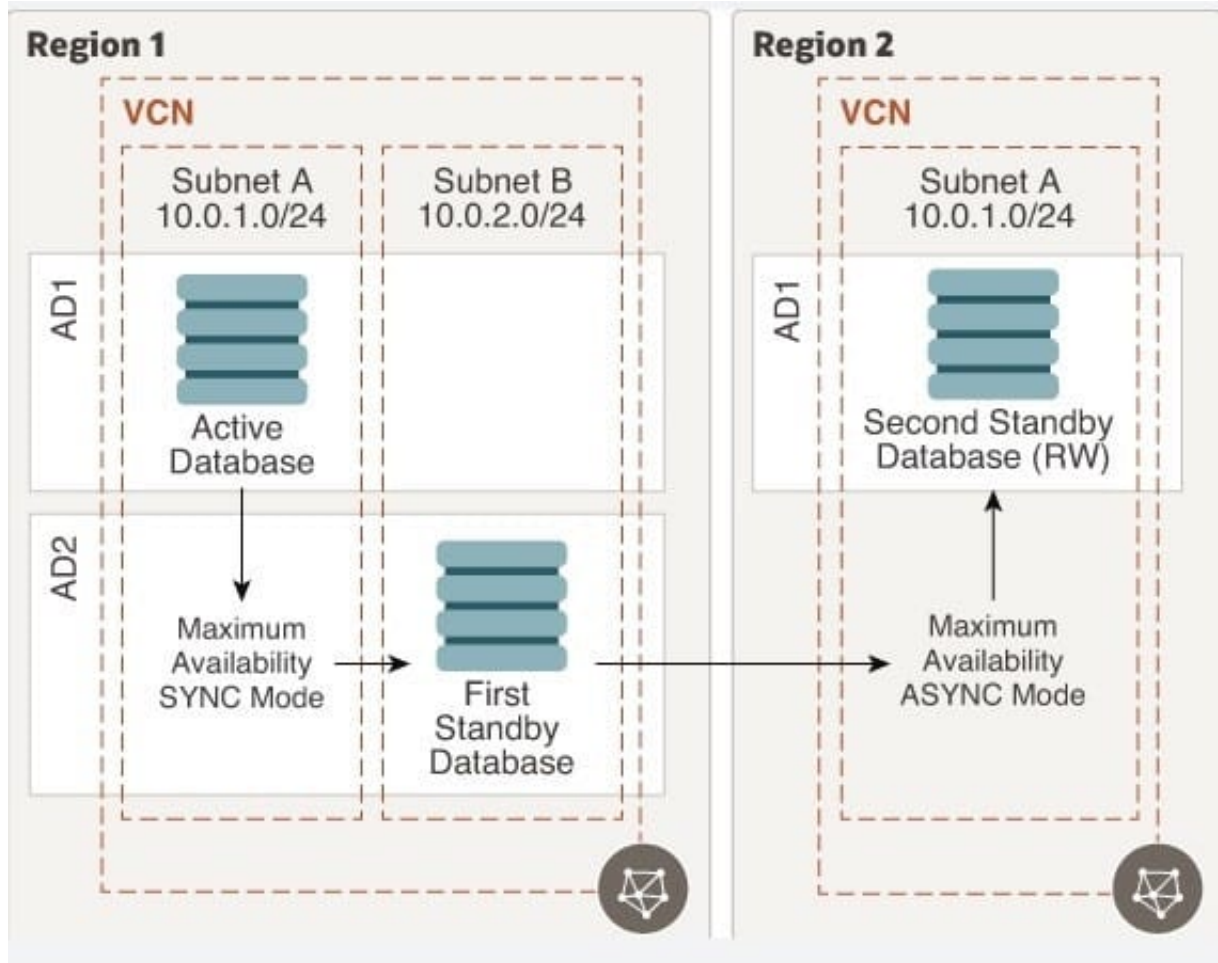
All three Data Guard Configuration are fully supported on Oracle Cloud infrastructure (OCI). You want to deploy a maximum availability architecture (MAA) for database workload. Which option should you consider while designing your Data Guard configuration to ensure best RTO and PRO without causing any data loss?

- A. Configure "Maximum Protection" mode which provides zero data loss If the primary database fails.
- B. Configure "Maximum Performance" mode In SYNC mode between two availability domains (same region) which provides, the highest level of data protection that is possible without affecting the performance of the primary database.
- C. Configure "Maximum Scalability" mode which provides the highest level of scalability without compromising the availability of the primary database.
- D. Configure "Maximum Availability" mode in SYNC mode between two availability domains (same

Correct Answer: D



<https://docs.cloud.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/best-practices-for-dr-onoci.pdf> All three Data Guard configurations are fully supported on Oracle Cloud Infrastructure. However, because of a high risk of production outage, we don't recommend using the maximum protection mode for your Data Guard configuration. We recommend using the maximum availability mode in SYNC mode between two availability domains (same region), and using the maximum availability mode in ASYNC mode between two regions. This architecture provides you the best RTO and RPO without causing any data loss. We recommend building this architecture in daisy-chain mode: the primary database ships redo logs to the first standby database in another availability domain in SYNC mode, and then the first standby database ships the redo logs to another region in ASYNC mode. This method ensures that your primary database is not doing the double work of shipping redo logs, which can cause performance impact on a production workload.



This configuration offers the following benefits: No data loss within a region. No overhead on the production database to maintain standbys in another region. Option to configure lagging on the DR site if needed for business reasons. Option to configure multiple standbys in different regions without any additional overhead on the

production database. A typical use case is a CDN application Bottom of Form

### QUESTION 3

You are designing the network infrastructure for two application servers: appserver-1 and appserver-2 running in two different subnets inside the same Virtual Cloud Network (VCN) Oracle Cloud Infrastructure (OCI). You have a requirement where your end users will access appserver-1 from the internet and appserver-2 from the on-premises network. The on-premises network is connected to your VCN over a FastConnect virtual circuit. How should you design



your routing configuration to meet these requirements?

A. Configure a single routing table (Route Table-1) that has two set of rules. One that has route to internet via the internet Gateway and another that propagate specific routes for the on-premise network via the Dynamic Routing Gateway.

Associate the routing table with all the VCN subnets.

B. Configure a single routing table (Routing Table-1) that has two set of rules: one that has route to internet via the Internet Gateway and another that propagates specific routes for the on-premises network via Dynamic Routing Gateway (DRG). Associate the routing table with the VCN.

C. Configure two routing tables: Route Table-1 that has a route to internet via the Internet gateway. Associate this route table to the subnet containing appserver-1. Route Table-2 that propagate specific routes for the on-premises network via the Dynamic Routing Gateway (DRG) Associate this route table to subnet containing appserver-2.

D. Configure two routing table (Route table-1 Route Table-2) that have rule to route all traffic via the Dynamic Routing Gateway (DRG) Associate the two routing tables with all the VCN subnets.

Correct Answer: C

---

#### QUESTION 4

A retailer bank is currently hosting their mission critical customer application on-premises. The application has a standard 3 tier architecture -4 application servers process the incoming traffic and store application data in an Oracle Exadata Database Server. The bank has recently has service disruption to other inter applications to they are looking to avoid this issue for their mission critical Customer Application. Which Oracle Cloud Infrastructure services should you recommend as part of the DR solution?

A. OCI DNS Service\ Public Load Balancer, Oracle Database Cloud Backup Service, Object Storage Service, Oracle Bare Metal Cloud Service, Oracle Bare Metal Cloud Service with GoldenGate, OCI Container Engines for Kubernetes, Oracle IPSec VPN

B. OCI Traffic Management, Private Load Balancer, Compute instances distributed across multiple Availability Domains and/or Fault Domains, Exadata Cloud Service with Data Guard, Oracle FastConnect, Object Storage, Database Cloud backup module

C. OCI Traffic Management, Public toad Balancer, Compute Instances distributed across multiple

D. OCI DNS Service, Load Balancer as a service using Public Load Balancer distributing traffic Compute Instance across multiple regions, Oracle RAC Database using Virtual Machines, Remote Peering connecting two VCNs in different regions. Exadata Cloud Service with GoldenGate FastConnect, Object Storage, Database Cloud backup module.

Correct Answer: C

OCI Traffic Management Steering Policies can account for health of answers to provide failover capabilities, provide the ability to load balance traffic across multiple resources, and account for the location where the query was initiated to provide a simple, flexible and powerful mechanism to efficiently steer DNS traffic. Public Load Balancer Accepts traffic from the internet using a public IP address that serves as the entry point for incoming traffic. Load balancing service creates a primary load balancer and a standby load balancer, each in a different availability domain

---

#### QUESTION 5



You are tasked with migrating an online shopping website to Oracle Cloud Infrastructure (OCI) and decide to use a Load Balancer. You have configured the backend set with the round robin policy. During the testing phase, you noticed that users are losing items from their shopping carts when they navigate to different pages. How should you implement a solution to this problem?

- A. Set up a Traffic Management Steering Policy to redirect traffic to a different backend set that is deployed exclusively for the purpose of holding all Items placed in the shopping cart.
- B. Configure a set of path route rules that will route to different backend sets based on the URI requested by the customer's browser.
- C. Replace the round robin policy with least connections policy at the backend set.
- D. Set up session persistence at the Load Balancer backend set.

Correct Answer: C

[Latest 1Z0-997 Dumps](#)

[1Z0-997 VCE Dumps](#)

[1Z0-997 Exam Questions](#)