1Z0-1072-22 Q&As

Oracle Cloud Infrastructure 2022 Architect Associate

Pass Oracle 1Z0-1072-22 Exam with 100% Guarantee

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

https://www.geekcert.com/1z0-1072-22.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

Which two resources reside exclusively in a single Oracle Cloud Infrastructure Availability Domain?

A. Identity and Access Management Groups

B. Web Application Firewall policy

C. Block volume

D. Compute Instance

E. Object Storage

Correct Answer: CD

https://docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm#one

QUESTION 2

You have been asked to create an Identity and Access Management (IAM) user that will authenticate to

Oracle Cloud Infrastructure (OCI) API endpoints. This user must not be given credentials that would allow

them to log into the OCI console.

Which two authentication options can you use? (Choose two.)

A. SSL certificate

B. API signing key

C. SSH key pair

D. PEM Certificate file

E. Auth token

Correct Answer: BE

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcredentials.htm

QUESTION 3

You work for a health insurance company that stores a large number of patient health records in an Oracle Cloud Infrastructure (OCI) Object Storage bucket named "HealthRecords". Each record needs to be securely stored for a period of 5 years for regulatory compliance purposes and cannot be modified, overwritten or deleted during this time period. What can you do to meet this requirement?

A. Create an OCI Object Storage Lifecycle Policies rule to archive objects in the HealthRecords bucket for five years.

B. Create an OCI Object Storage time-bound Retention Rule on the HealthRecords bucket for five years. Enable Retention Rule Lock on this bucket.

C. Enable encryption on the HealthRecords bucket using your own vault master encryption keys.

D. Enable versioning on the HealthRecords bucket.

Correct Answer: B

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Object/Tasks/usingretentionrules.htm

QUESTION 4

Which of the following statement is true regarding Oracle Cloud Infrastructure Object Storage Pre-Authenticated Requests?

A. It Is not possible to create pre-authenticated requests for "archive" storage tier

B. Changing the bucket visibility does not change existing pre-authenticated requests

C. It is not possible to create pre-authenticated requests for the buckets, but only for the objects

D. Pre-authenticated requests don\\'t have an expiration

Correct Answer: B

Pre-authenticated requests provide a way to let users access a bucket or an object without having their own credentials, as long as the request creator has permissions to access those objects. For example, you can create a request that lets an operations support user upload backups to a bucket without owning API keys. Or, you can create a request that lets a business partner update shared data in a bucket without owning API keys. When you create a pre-authenticated request, a unique URL is generated. Anyone you provide this URL to can access the Object Storage resources identified in the pre-authenticated request, using standard HTTP tools like curl and wget. Understand the following scope and constraints regarding pre-authenticated requests: Users can\\'t list bucket contents. You can create an unlimited number of pre-authenticated requests. There is no time limit to the expiration date that you can set. You can\\'t edit a pre-authenticated request. If you want to change user access options in response to changing requirements, you must create a new pre-authenticated request. The target and actions for a pre-authenticated request are based on the creator\\'s permissions. The request is not, however, bound to the creator\\'s account login credentials. If the creator\\'s login credentials change, a pre-authenticated request is not affected. You cannot delete a bucket that has a pre-authenticated request associated with that bucket or with an object in that bucket. Understand the following scope and constraints regarding public access: Changing the type of access is bi-directional. You can change a bucket\\'s access from public to private or from private to public. Changing the type of access doesn\\'t affect existing pre-authenticated requests. Existing pre- authenticated requests still work.

QUESTION 5

You are a network architect of an application running on Oracle Cloud Infrastructure (OCI). Your security team has informed you about a security patch that needs to be applied immediately to one of the backend web servers. What should you do to ensure that the OCI load balancer does not forward traffic to this backend server during maintenance?

A. Drain all existing connections to this backend server and mark the backend web server offline

B. Create another OCI load balancer for the backend web servers, which are active and handling traffic

C. Edit the security list associated with the subnet to avoid traffic connectivity to this backend serve

D. Stop the load balancer for maintenance and restart the load balancer after the maintenance is finished

Correct Answer: A

A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability. You can configure multiple load balancing policies and application-specific health checks to ensure that the load balancer directs traffic only to healthy instances. The load balancer can reduce your maintenance window by draining traffic from an unhealthy application server before you remove it from service for maintenance. The Load Balancing service considers a server marked drain available for existing persisted sessions. New requests that are not part of an existing persisted session are not sent to that server. Edit Drain State: Opens a dialog box in which you can change the drain state. If you set the server\\'s drain status to true, the load balancer stops forwarding new TCP connections and new non-sticky HTTP requests to this backend server. This setting allows an administrator to take the server out of rotation for maintenance purposes.

e. Edit Offline State: Opens a dialog box in which you can change the offline status.

If you set the server\\'s offline status to true, the load balance forwards no ingress traffic to this backend

server.