1Z0-1104-22 Q&As

Oracle Cloud Infrastructure 2022 Security Professional

Pass Oracle 1Z0-1104-22 Exam with 100% Guarantee

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

https://www.passapply.com/1z0-1104-22.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which component helps move logging data to other services, such as archiving log data in object storage?

A. Agent Configuration

B. Unified Monitoring Agent

C. Service Connector Hub

D. Service Log Category

Correct Answer: C

Service Connector Hub Service Connector Hub moves logging data to other services in Oracle Cloud Infrastructure. For example, use Service Connector Hub to alarm on log data, send log data to databases, and archive log data to Object Storage. For more information, see Service Connector Hub. https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm

QUESTION 2

A company has OCI tenancy which has mount target associated with two File Systems, CG_1 and CG_2. These FileSystems are accessed by IP-based clients AB_1 and AB_2 respectively. As a security administrator, how can you provide access to both clients such that CGI has Read only access on AB1 and CG_2 has Read/Write access on AB_2?

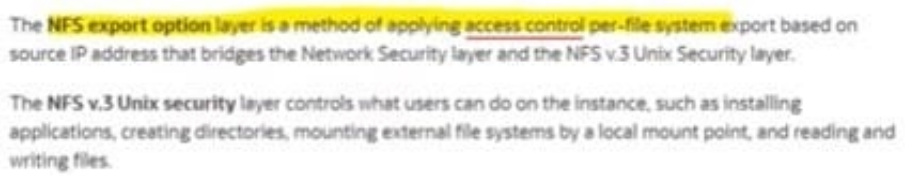
A. NFS Export Option

B. Access Control Lists

C. NFS v3 Unix Security

D. Vault

Correct Answer: AC


The **NFS export option** layer is a method of applying access control per-file system export based on source IP address that bridges the Network Security layer and the NFS v.3 Unix Security layer.

The **NFS v.3 Unix security** layer controls what users can do on the instance, such as installing applications, creating directories, mounting external file systems by a local mount point, and reading and writing files.

QUESTION 3

In which two ways can you improve data durability in Oracle Cloud Infrastructure Object Storage?

A. Setup volumes in a RAID1 configuration

B. Enable server-sideencryption

C. Enable Versioning

D. Limit delete permissions

E. Enable client-side encryption

Correct Answer: A

QUESTION 4

Which Oracle Cloud Service provides restricted accessto target resources?

A. Bastion

B. Internet Gateway

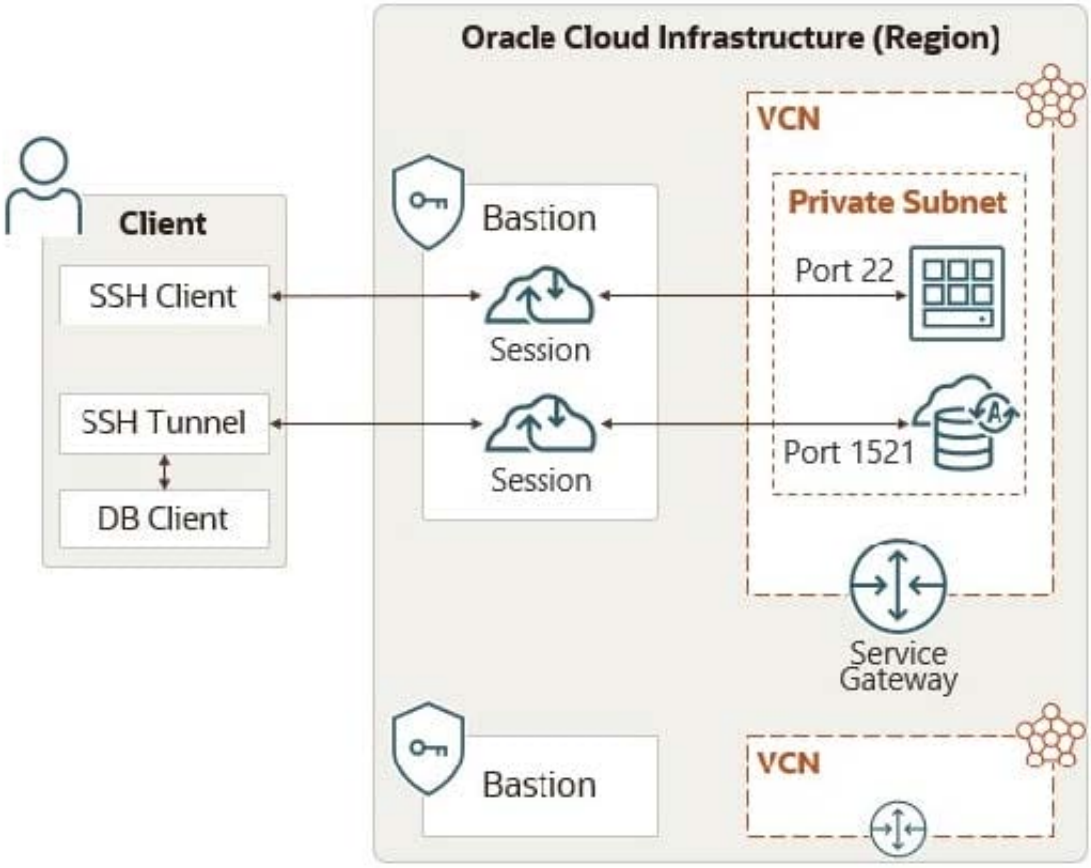
C. Load balancer

D. SSL certificate

Correct Answer: A

Bastion

Oracle Cloud Infrastructure Bastion provides restricted and time-limited access to target resources that don\\'t have public endpoints.



https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_features.htm

QUESTION 5

A member of operations team has set Pre-Authenticated Request (PAR) associated with a bucket to an incorrect date and now wants to edit the PARrequest. How can this be achieved?

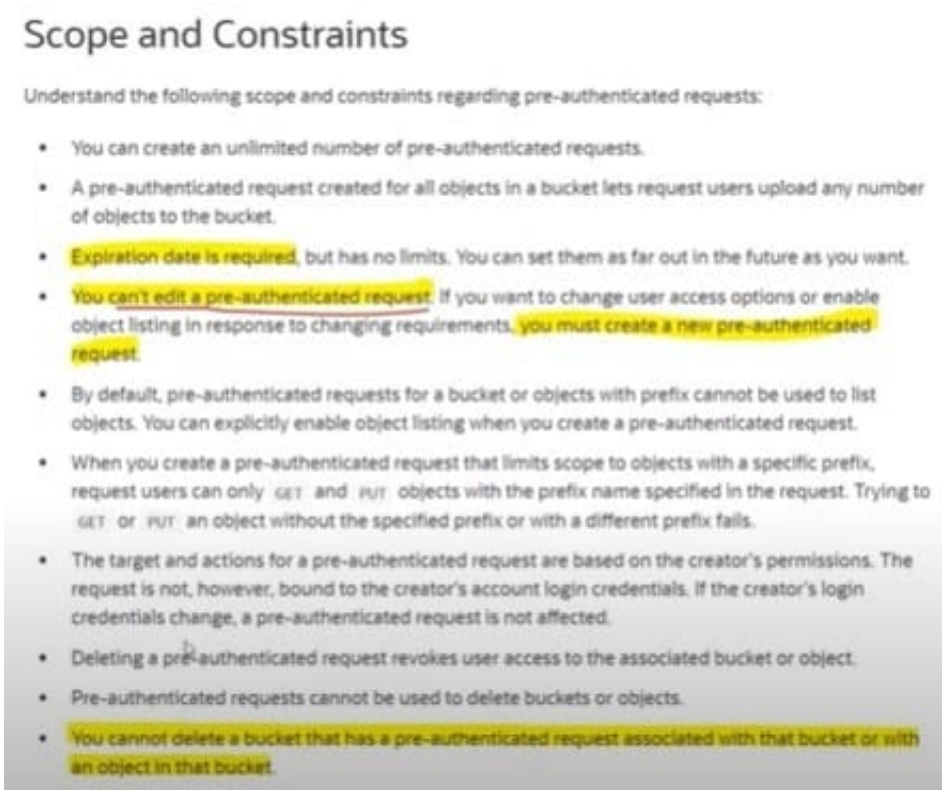
A. Don\\'t set an expiration time for PAR

B. Delete the bucket associated with PAR and recreate it

C. Delete the PAR and recreate it with the required date

D. Delete both PAR as well as the bucket then recreate both

Correct Answer: C



Scope and Constraints

Understand the following scope and constraints regarding pre-authenticated requests:

- You can create an unlimited number of pre-authenticated requests.
- A pre-authenticated request created for all objects in a bucket lets request users upload any number of objects to the bucket.
- Expiration date is required, but has no limits. You can set them as far out in the future as you want.
- You can't edit a pre-authenticated request. If you want to change user access options or enable object listing in response to changing requirements, you must create a new pre-authenticated request.
- By default, pre-authenticated requests for a bucket or objects with prefix cannot be used to list objects. You can explicitly enable object listing when you create a pre-authenticated request.
- When you create a pre-authenticated request that limits scope to objects with a specific prefix, request users can only GET and PUT objects with the prefix name specified in the request. Trying to GET or PUT an object without the specified prefix or with a different prefix fails.
- 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.
- Deleting a pre-authenticated request revokes user access to the associated bucket or object.
- Pre-authenticated requests cannot be used to delete buckets or objects.
- You cannot delete a bucket that has a pre-authenticated request associated with that bucket or with an object in that bucket.