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.pass4itsure.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 statements are true about Oracle Cloud Infrastructure (OCI) DB Systems?

A. Customers have no control over database patching.

B. The database and backups are encrypted by default.

C. Customers can consolidate multiple database homes on a single virtual machine database host.

D. Customers can manage the TDE Wallet after DB Systems is provisioned.

Correct Answer: BD

All databases created in Oracle Cloud Infrastructure are encrypted using transparent data encryption (TDE). Oracle Cloud Infrastructure encrypts all managed backups in the object store. Oracle uses the Database Transparent Encryption feature by default for encrypting the backups. and the customers can manage the TDE Wallet after DB Systems are provisioned.

QUESTION 2

Your company has been running several small applications in Oracle Cloud Infrastructure and is planning a proof-of-concept (POC) to deploy PeopleSoft. If your existing resources are being maintained in the root compartment, what is the recommended approach for defining security for the upcoming POC?

A. Create a new compartment for the POC and grant appropriate permissions to create and manage resources within the compartment.

B. Provision all new resources into the root compartment. Grant permissions that only allow for creation and management of resources specific to the POC.

C. Provision all new resources into the root compartment. Use defined tags to separate resources that belong to different applications.

D. Create a new tenancy for the POC. Provision all new resources into the root compartment. Grant appropriate permissions to create and manage resources within the root compartment.

Correct Answer: A

If your organization is small, or if you are still in the proof-of-concept stage of evaluating Oracle Cloud Infrastructure, consider placing all of your resources in the root compartment (tenancy). This approach makes it easy for you to quickly view and manage all your resources. You can still write policies and create groups to restrict permissions on specific resources to only the users who need access. If you plan to maintain all your resources in the root compartment, we recommend setting up a separate sandbox compartment to give users a dedicated space to try out features. In the sandbox compartment, you can grant users permissions to create and manage resources, while maintaining stricter permissions on the resources in your tenancy (root) compartment. https://www.oracle.com/a/ocom/docs/best-practicesfor-iam-on-oci.pdf

QUESTION 3

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 4

You are a system administrator of your company and you are asked to manage updates and patches across all your compute instances running Oracle Linux in Oracle Cloud Infrastructure (OCI). As part of your task, you need to apply all the latest kernel security updates to all instances. Which OCI service will allow you to complete this task?

A. Resource Manager

B. OS Management

C. Storage Gateway

D. Streaming E. Registry

Correct Answer: B

Reference: https://blogs.oracle.com/cloud-infrastructure/os-management-with-oracle-cloud-infrastructure

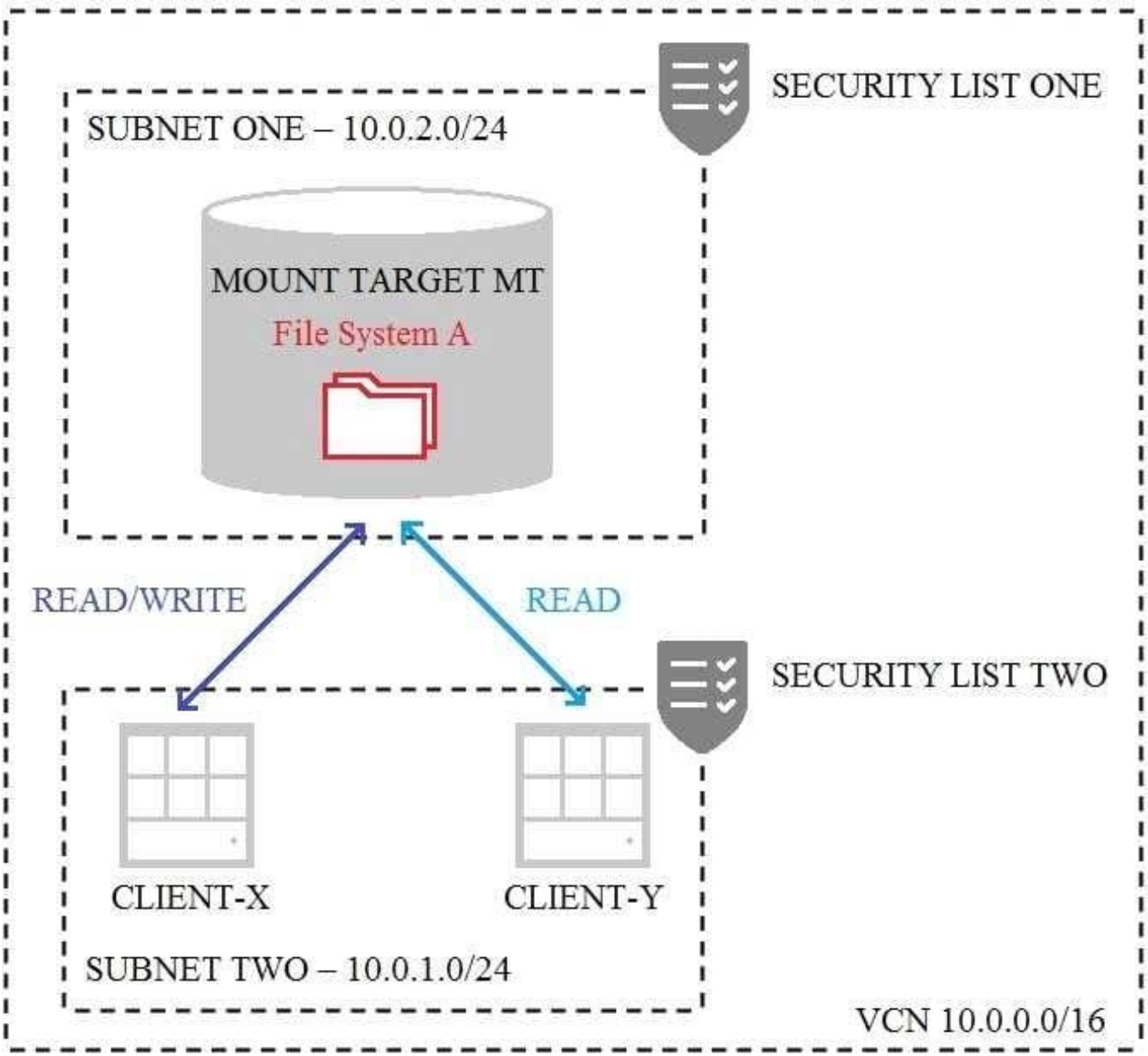
QUESTION 5

You have setup your environment as shown below with the Mount Target "MT" successfully mounted on

both compute instances CLIENT-X and CLIENT-Y.

For security reasons you want to control the access to the File System A in such a way that CLIENT-X has

READ/WRITE and CLIENT-Y has READ only permission.



What you should do?

A. Update the OS firewall in CLIENT-X to allow READ/WRITE access.

B. Update the security list TWO to restrict CLIENT-Y access to read-only.

C. Update the mount target export options to restrict CLIENT-Y access to read-only.

D. Update the security list ONE to restrict CLIENT-Y access to read only.

Correct Answer: D