



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

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





QUESTION 1

You subscribe to a PaaS service that follows the Shared Responsibility model. Which type of security is your responsibility?

- A. Network
- B. Infrastructure
- C. Data
- D. Guest OS

Correct Answer: C

<https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf>

QUESTION 2

What is the matching rule syntax for a single condition?

- A. any| all { <condition>,<condition>,... }
- B. instance.compartment.id = '<compartment_ocid>'
- C. variable =|!= 'value'
- D. Any {instance.compartment.id = '<compartment_ocid>', instance.compartment.id = '<compartment_ocid>'}

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: C



Writing Matching Rules to Define Dynamic Groups

Matching rules define the resources that belong to the dynamic group. In the Console, you can either enter the rule manually in the provided text box, or you can use the [rule builder](#). The rule builder lets you make selections and entries in a dialog, then writes the rule for you, based on your entries.

You can define the members of the dynamic group based on the following:

- compartment ID - include (or exclude) the instances that reside in that compartment based on compartment OCID
- instance ID - include (or exclude) an instance based on its instance OCID
- tag namespace and tag key - include (or exclude) instances tagged with a specific tag namespace and tag key. All tag values are included. For example, include all instances tagged the with tag namespace `department` and the tag key `operations`.
- tag namespace, tag key, and tag value - include (or exclude) instances tagged with a specific value for the tag namespace and tag key. For example include all instances tagged with the tag namespace `department` and the tag key `operations` and with the value `'45'`.

A matching rule has the following syntax:

For a single condition:

```
variable ==|!= 'value'
```

QUESTION 3

On which option do you set Oracle Cloud Infrastructure Budget?

- A. Compartments
- B. Instances
- C. Free-form tags
- D. Tenancy

Correct Answer: A

How Budgets Work

Budgets are set on cost-tracking tags or on compartments (including theroot compartment) to track all spending in that cost-tracking tag or for that compartment and its children.

<https://docs.oracle.com/en-us/iaas/Content/Billing/Concepts/budgetsoverview.htm>



QUESTION 4

When creating an OCI Vault, which factors may lead to select the Virtual Private Vault? Select TWO correct answers

- A. Need for more than 9211 key versions
- B. Greater degree of isolation
- C. To mask PII data for non-production environment
- D. Ability to back up the vault

Correct Answer: BD

VAULTS

Vaults are logical entities where the Vault service creates and durably stores keys and secrets. The type of vault you have determines features and functionality such as degrees of storage isolation, access to management and encryption, scalability, and the ability to back up. The type of vault you have also affects pricing. You cannot change a vault's type after you create the vault.

The Vault service offers different vault types to accommodate your organization's needs and budget. All vault types ensure the security and integrity of the encryption keys and secrets that vaults store. A virtual private vault is an isolated partition on a hardware security module (HSM). Vaults otherwise share partitions on the HSM with other vaults.

Virtual private vaults include 1000 key versions by default. If you don't require the greater degree of isolation or the ability to back up the vault, you don't need a virtual private vault. Without a virtual private vault, you can manage costs by paying for key versions individually, as you need them. (Key versions count toward your key limit and costs. A key always contains at least one active key version. Similarly, a secret always has at least one secret version. However, limits on secrets apply to the tenancy, rather than a vault.)

The Vault service designates vaults as an Oracle Cloud Infrastructure resource.

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.

[1Z0-1104-22 VCE Dumps](#)

[1Z0-1104-22 Practice Test](#)

[1Z0-1104-22 Study Guide](#)