

# 1Z0-1104-22<sup>Q&As</sup>

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.leads4pass.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**

For how long are API calls audited and available?

- A. 30days
- B. 90 days
- C. 365 days
- D. 60 days

Correct Answer: B

---

**QUESTION 2**

As a security administrator, you found out that there are users outside your co network who are accessing OCI Object Storage Bucket. How can you prevent these users from accessing OCI resources in corporate network?

- A. Create an IAM policy and create WAF rules
- B. Create an IAM policy and add a network source
- C. Make OCI resources private instead of public
- D. Create PAR to restrict access the access

Correct Answer: B

## Introduction to Network Sources

A network source is a set of defined IP addresses. The IP addresses can be public IP addresses or IP addresses from VCNs within your tenancy. After you create the network source, you can reference it in policy or in your tenancy's authentication settings to control access based on the originating IP address.

Network resources can only be created in the tenancy (or root compartment) and, like other Identity resources, reside in the [home region](#). For information about the number of network sources you can have, see [IAM Without Identity Domains Limits](#).

You can use [network sources](#) to help secure your tenancy in the following ways:

- Specify the network source in IAM policy to restrict access to resources. When specified in a policy, IAM validates that requests to access a resource originate from an allowed IP address. For example, you can restrict access to Object Storage buckets in your tenancy to only users that are signed in to Oracle Cloud Infrastructure through your corporate network. Or, you can allow only resources belonging to specific subnets of a specific VCN to make requests over a [service gateway](#).
- 

**QUESTION 3**

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 4

You want software that can automatically collect and aggregate log data generated throughout your organization's infrastructure, analyze it, and send alerts if it detects a deviation from the norm. Which software must you use?

- A. Security Information Management (SIM)
- B. SecurityEvent Management (SEM)
- C. Security Integration Management (SIM)
- D. Security Information and Event Management (SIEM)

Correct Answer: D

---

#### QUESTION 5

Which OCI cloud service lets you centrally manage the encryption keys that protect your data and the secret credentials that you use to securely access resources?

- A. Data Safe
- B. Cloud Guard
- C. Data Guard
- D. Vault

Correct Answer: D

---

Oracle Cloud Infrastructure Vault is a managed service that lets you centrally manage the encryption keys that protect your data and the secret credentials that you use to securely access resources. Vaults securely store master encryption keys and secrets that you might otherwise store in configuration files or in code. Specifically, depending on the protection mode, keys are either stored on the server or they are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification.

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

---

## QUESTION 6

Which statement is not true about Cloud Security Posture?

- A. Problems contain data about the specific type of issue that was found.
- B. Problems can be resolved, dismissed, or remediated.
- C. Problems are defined by the type of detector that creates them: activity or configuration.
- D. Problems are created when Cloud Guard discovers a deviation from a responder rule.

Correct Answer: D

<https://www.oracle.com/security/cloud-security/what-is-cspm/>

---

## QUESTION 7

You are using a custom application with third-party APIs to manage application and data hosted in an Oracle Cloud Infrastructure (OCI) tenancy. Although your third-party APIs don't support OCI's signature-based authentication, you want them to communicate with OCI resources. Which authentication option must you use to ensure this?

- A. OCI username and Password
- B. API Signing Key
- C. SSH Key Pair with 2048-bit algorithm
- D. Auth Token

Correct Answer: D

---

## QUESTION 8

Which resources can be used to create and manage from Vault Service ? Select TWO correct answers

- A. Secret
- B. IAM

C. Keys

D. Cloud Guard

Correct Answer: AC



**Vault**

You can use the Vault service to create and manage the following resources:

- Vaults
- Keys
- Secrets

A vault includes the encryption keys and secret credentials that you use to protect your data and connect to secured resources. As customer-managed resources, you have complete control over who has access to your vaults, keys, and secrets. You also control what authorized users and services can do with Vault resources. Levels of access might range from something as granular as whether an individual key can be used by a particular service to more broadly impactful lifecycle management activities, like whether a user can delete a key from a vault to prevent its use altogether.

Keys are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. Secrets and secret versions are base64-encoded and encrypted with master encryption keys, but do not reside within the HSM.

---

### QUESTION 9

You want to create a stateless rule for SSH in security list and the ingress rule has already been properly configured what combination should you use on the egress rule what combination should you use on the egress rule?

A. select udp for protocol: enter 22 for source port" and all for destination port

B. select tcp for protocol: enter 22 for source port" and 22 for destination port

C. select tcp for protocol: enter all for source port" and 22 for destination port.

D. select tcp for protocol: enter 22 for source port" and all for destination port

Correct Answer: C

---

### QUESTION 10

Which components are a part of the OCI Identity and Access Management service?

A. Policies

B. Regional subnets

C. Compute instances

D. VCN

Correct Answer: A

QUESTION 11

The following table describes the security zone policies ⓘ that restrict resource movement.

Policy	Services	Description
deny_block_volume_in_security_zone_move_to_compartment_not_in_security_zone	Block Volume	You can't move a <b>block volume</b> ⓘ from a security zone to a standard compartment.
deny_boot_volume_in_security_zone_move_to_compartment_not_in_security_zone	Block Volume	You can't move a <b>boot volume</b> from a security zone to a standard compartment.
deny_instance_in_security_zone_move_to_compartment_not_in_security_zone	Compute	You can't move a <b>compute instance (Compute)</b> ⓘ from a security zone to a standard compartment.
deny_instance_not_in_security_zone_move_to_compartment_in_security_zone	Compute	You can't move a compute instance from a standard compartment to a compartment that is in a security zone.
deny_subnet_in_security_zone_move_to_compartment_not_in_security_zone	Networking	You can't move a <b>subnet</b> ⓘ from a security zone to a standard compartment.
deny_bucket_in_security_zone_move_to_compartment_not_in_security_zone	Object Storage	You can't move a <b>bucket</b> ⓘ from a security zone to a standard compartment.
deny_db_instance_move_to_compartment_not_in_security_zone	Database (all types)	You can't move a <b>database</b> from a security zone to a standard compartment.

Which tasks can you perform on a dedicated virtual machine host?

- A. Manual scaling
- B. Creating instance pools
- C. Instance configurations
- D. Capacity reservations

Correct Answer: A

Supported features: Most of the Compute features for VM instances are supported for instances running on dedicated virtual machine hosts. However, the following features are not supported: Autoscaling Capacity reservations Instance configurations Instance pools Burstable instances Reboot migration. You can use manual migration instead

[https://docs.oracle.com/en-us/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm#Dedicated\\_Virtual\\_Machine\\_Hosts](https://docs.oracle.com/en-us/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm#Dedicated_Virtual_Machine_Hosts)

---

## QUESTION 12

Which of the following services are NOT Security Services in OCI ? Select TWO answers.

- A. Data Guard
- B. Cloud Guard
- C. Vault
- D. Block Volume

Correct Answer: AD

---

## QUESTION 13

What is the use case for Oracle cloud infrastructure logging analytics service?

- A. monitors, aggregates, indexes and analyzes all log data from on-premises.
- B. labels data packets that pass through the internet gateway
- C. automatically create instances to collect logs analysis and send reports
- D. automatically and manage any log based on a subscription model

Correct Answer: A

Oracle Cloud Infrastructure Logging Analytics is a machine learning-based cloud service that monitors, aggregates, indexes, and analyzes all log data from on-premises and multicloud environments. Enabling users to search, explore, and

correlate this data to troubleshoot and resolve problems faster and derive insights to make better operational decisions.

<https://www.oracle.com/manageability/logging-analytics/>

---

## QUESTION 14

A number of malicious requests for a web application is coming from a set of IP addresses originating from Antarctica.

Which of the following statement will help to reduce these types of unauthorized requests ?

- A. Delete NAT Gateway from Virtual Cloud Network
- B. Use WAF policy using Access Control Rules
- C. List specific set of IP addresses then deny rules in Virtual Cloud Network Security Lists
- D. Change your home region in which your resources are currently deployed

Correct Answer: B

---

## QUESTION 15

Which volume type contains the image used to boot a compute instance?

- A. Init 6 volume
- B. Boot volume
- C. Startup volume
- D. Block volume

Correct Answer: B

Boot Volumes When you launch a virtual machine (VM) or bare metal instance based on a platform image or custom image, a new boot volume for the instance is created in the same compartment. That boot volume is associated with that instance until you terminate the instance. When you terminate the instance, you can preserve the boot volume and its data

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

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

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

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