

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.pass2lead.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 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 2

What does the following identity policy do?

Allow group my-group to use fn-invocation in compartment ABC where target.function.id = `\\`

- A. Enables users in a group to create, update, and delete ALL applications and functions in a compartment
- B. Enables users to invoke all the functions in a specific application
- C. Enables users to invoke just one specific function
- D. Enables users to invoke all the functions in a compartment except for one specific function

Correct Answer: C

QUESTION 3

As a security architect, how can you prevent unwanted bots while desirable bots are allowed to enter?

- A. Data Guard
- B. Vault
- C. Compartments
- D. Web Application Firewall (WAF)

Correct Answer: D

QUESTION 4

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 5

Which security issues can be identified by Oracle Vulnerability Scanning Service? Select TWO correct answers

- A. Distributed Denial of Service (DDoS)
- B. Ports that are unintentionally left open can be a potential attack vector for cloud resources
- C. SQL Injection
- D. CIS published Industry-standard benchmarks

Correct Answer: BD

Scanning Overview

Oracle Vulnerability Scanning Service helps improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. The service generates reports with metrics and details about these vulnerabilities.

The Scanning service can identify several types of security issues in your compute instances ⓘ:

- Ports that are unintentionally left open might be a potential attack vector to your cloud resources, or enable hackers to exploit other vulnerabilities.
- OS packages that require updates and patches to address vulnerabilities
- OS configurations that hackers might exploit
- Industry-standard benchmarks published by the [Center for Internet Security](#) (CIS).

The Scanning service checks hosts for compliance with the section 5 (Access, Authentication, and Authorization) benchmarks defined for [Distribution Independent Linux](#).

QUESTION 6

As a security administrator, you want to create cloud resources that align with Oracle's security principles and best practices. Which security service should you use?

- A. Identity and Access Management
- B. Cloud Guard
- C. Security Advisor
- D. Web Application Firewall (WAF)

Correct Answer: C

QUESTION 7

You are part of security operation of an organization with thousand of your users accessing Oracle cloud infrastructure it was reported that an unknown user action was executed resulting in configuration error you are tasked to quickly identify

the details of all users who were active in the last six hours also with any rest API call that were executed. Which oci feature should you use?

- A. service connector hub
- B. management agent log integration
- C. objectcollectionrule
- D. audit analysis dashboard

Correct Answer: D

QUESTION 8

Oracle Object Storage achieves data durability by which of the mechanisms ? Select TWO correct answers

- A. Service Gateway
- B. Redundant Storage across availability domains
- C. Redundant Array of Independent Disks
- D. Object Versioning

Correct Answer: BD

How durable is data stored in Oracle Cloud Infrastructure Object Storage?

Oracle Object Storage is designed to be highly durable, providing 99.999999999% (Eleven 9's) of annual durability. It achieves this by storing each object redundantly across three servers in different availability domains for regions with multiple availability domains, and in different fault domains in regions with a single availability domain. Existing objects can be accessed as long as one of the three copies is accessible, and new objects can be uploaded as long as two copies can be successfully written. Data integrity is actively monitored using checksums, and corrupt data is detected and automatically repaired. Any loss in data redundancy is detected and remedied, without customer intervention or impact.

QUESTION 9

Security Advisor

Security Advisor helps you create cloud resources that align with Oracle's security principles and best practices. It also ensures that your resources meet the requirements enforced by security zone policies. For example, you can quickly create resources that are encrypted with a customer-managed master encryption key using the Vault service.

For example, you can use Security Advisor to create the following resources:

- Object Storage bucket
- File Storage file system
- Compute instance (Compute) (and associated boot volume)
- Block Volume block storage volume

Which OCI service can index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor data?

- A. Data Guard
- B. Data Safe
- C. WAF
- D. Logging Analytics

Correct Answer: D

About Logging Analytics

Oracle Cloud Logging Analytics is a cloud solution in Oracle Cloud Infrastructure that lets you index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor all log data from your applications and system infrastructure on cloud or on-premises.

QUESTION 10

What do the features of OS Management Service do?

- A. Add complexity in using multiple tools to manage mixed-OS environments.
- B. Provide paid service and support to OCI subscribers for fixes on priority.

- C. Increase security and reliability by regular bug fixes.
- D. Encourage manual setup to avoid machine-induced errors.

Correct Answer: C

<https://docs.oracle.com/en/solutions/oci-best-practices/manage-your-operating-systems1.html>

QUESTION 11

You create a new compartment, "apps," to host some production apps and you create an apps_group and added users to it. What would you do to ensure the users have access to the apps compartment?

- A. Add an IAM policy for the individual users to access the apps compartment.
- B. Add an IAM policy for apps_group granting access to the apps compartment.
- C. Add an IAM policy to attach tenancy to the apps group.
- D. No action is required.

Correct Answer: B

QUESTION 12

Your company has hired a consulting firm to audit your oracle cloud infrastructure activity and configuration you have created a set of users who will be performing the audit, you assigned these user to the orgauditgrp group. the auditor required the ability to see the configuration of all resources within tenancy and you have agreed to exempt the dev compartment from the audit.

Which IAM policy should be created to grant the orgauditgrp the ability to look at configuration for all resources except for those resources inside the dev compartment?

- A. allow group orgauditgrp to read all-resources in tenancy where target.compartment.name !=dev
- B. allow group orgauditgrp to read all-resources in compartment !=dev
- C. allow group orgauditgrp to inspect all-resources in tenancy where target compartment.name !=dev
- D. allow group orgauditgrp to inspect all-resources in compartment !=dev

Correct Answer: C

QUESTION 13

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 14

Which parameters customers need to configure while reading secrets by name using CL1 or API? Select TWO correct answers.

- A. Certificates
- B. Secret Name
- C. ASCII Value
- D. Vault Id

Correct Answer: BD



QUESTION 15

Operations team has made a mistake in updating the secret contents and immediately need to resume using older secret contents in OCI Secret Management within a Vault. As a Security Administrator, what step should you perform to rollback to last version? Select TWO correct answers.

- A. Mark the secret version as `'deprecated'`
- B. Mark the secret version as `'Previous'`
- C. Mark the secret version as `'Rewind'`
- D. Upload new secret and mark as `'Pending'`. Promote this secret version as `'Current'`

Correct Answer: BD

Rotation States

Secret versions can have more than one rotation state at a time. Where only one secret version exists, such as when you first create a secret, the secret version is automatically marked as both `'current'` and the `'latest'`. The `'latest'` version of a secret contains the secret contents that were last uploaded to the vault, in case you want to keep track of that.

When you rotate a secret to upload new secret contents, you can mark it as `'pending'`. Marking a secret version's rotation state as `'pending'` lets you upload the secret contents to the vault without immediately putting them into active use. You can continue using the `'current'` secret version until you're ready to promote a pending secret version to `'current'` status. This typically happens after you've rotated credentials on the target resource or service first. You don't want to unexpectedly change a secret version. Changing what secret version is current prevents the application that needs it from retrieving the expected secret version from the vault.

For the purposes of rolling back to a previous version easily, such as when you've made a mistake in updating the secret contents or when you've restored a backup of an older resource and need to resume using older secret contents, secret versions can also be marked as `'previous'`. A secret version marked as `'previous'` was previously a secret version marked as `'current'`. To roll back to a previous version, you update the secret to specify the secret version number you want.