

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.certbus.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

Encrypt Data in Block Volumes

Enterprise Architect, Security Architect, Data Architect

The Oracle Cloud Infrastructure **Block Volumes service always encrypts all block volumes and boot volumes at rest** by using the Advanced Encryption Standard (AES) algorithm with 256-bit keys. Consider the following additional encryption options.

- Encrypt all of your volumes and their backups by using keys that you own, and you can manage the keys by using the Oracle Cloud Infrastructure Vault service.
- Data is transferred between an instance and the attached block volume through an internal and highly secure network. You can enable in-transit encryption for paravirtualized volume attachments on virtual machine instances.

Encrypt Data in File Storage

Enterprise Architect, Security Architect, Data Architect

The Oracle Cloud Infrastructure **File Storage service encrypts all data at rest**. By default, the file systems are encrypted by using Oracle-managed encryption keys.

Encrypt all of your file systems by using keys that you own. You can manage the keys by using the Oracle Cloud Infrastructure Vault service.

With regard to OCI Audit Log Service, which of the statement is INCORRECT?

- A. Retention period for audit events cannot be modified
- B. REST API calls can be recorded by Audit service
- C. Audit Events gets collected when modification within objects stored in an Object Storage bucket
- D. Events logged by the Audit service can be viewed by using the Console, API, or the SDK for Java

Correct Answer: C

QUESTION 2

For how long are API calls audited and available?

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

Correct Answer: B

QUESTION 3

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 destinationport

Correct Answer: C

QUESTION 4

Which is NOT a part of Observability and Management Services?

- A. Event Services
- B. OCI Management Service
- C. Logging Analytics
- D. Logging

Correct Answer: B

<https://www.oracle.com/in/manageability/>

QUESTION 5

A number ofmalicious 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 6

Which OCI cloud service lets you centrally manage the encryption keys thatprotect 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 7

How can you restrict access to OCI console from unknown IP addresses?

- A. Create tenancy's authentication policy and create WAF rules
- B. Create tenancy's authentication 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

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.
- Specify the network source in your tenancy's authentication settings to restrict sign in to the Console.
You can set up your tenancy's authentication policy to allow sign in to the Console from only those IP addresses specified in your network source. Users attempting to sign in from an IP address not on the allowed list in your network source will be denied access. For information on using a network source restriction in authentication policy, see [Managing Authentication Settings](#).

QUESTION 8

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 9

Which type of firewalls are designed to protect against web application attacks, such as SQL injection and cross-site scripting?

- A. Stateful inspection firewall
- B. Web Application Firewall
- C. Incident firewall
- D. Packet filtering firewall

Correct Answer: B

SQL injections. Cross-site scripting. Distributed denial of service(DDoS) attacks. Botnets. These are just some of the cyber-weapons increasingly being used by malicious actors to target web applications, cause data breaches, and expose

sensitive business information.

Oracle WAF uses a multilayered approach to protect web applications from a host of cyberthreats including malicious bots, application layer (L7) DDoS attacks, cross-site scripting, SQL injection, and vulnerabilities defined by the Open Web

Application Security Project (OWASP). When a threat is identified, Oracle WAF automatically blocks it and alerts security operations teams so they can investigate further.

<https://www.oracle.com/a/ocom/docs/security/oci-web-application-firewall.pdf>

QUESTION 10

Bot Management in OCI provides which of the features? Select TWO correct answers.

- A. Bad Bot Denylist
- B. CAPTCHA Challenge
- C. IP Prefix Steering
- D. Good Bot Allowlist

Correct Answer: BD

Bot Management

Bot Management enables you to mitigate undesired bot traffic from your site using CAPTCHA and JavaScript detection tools while enabling known published bot providers to bypass these controls.

Non-human traffic makes up most of the traffic to sites. Bot Manager is designed to detect and block, or otherwise direct, non-human traffic that can interfere with site operations. The Bot Manager features mitigate bots that conduct content and price scraping, vulnerability scanning, comment spam, brute force attacks, and application-layer DDoS attacks. You can also manage the good bot whitelist.

⚠ Caution

When you enable Bot Management, you incur a higher rate on requests to the WAF.

See these topics for more information about Bot Management:

- [JavaScript Challenge](#)
- [Human Interaction Challenge](#)
- [Device Fingerprint Challenge](#)
- [CAPTCHA Challenge](#)
- [Good Bot Allowlist](#)

QUESTION 11

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 12

What would you use to make Oracle Cloud Infrastructure Identity and Access Management govern resources in a tenancy?

- A. Policies
- B. Users
- C. Dynamic groups
- D. Groups

Correct Answer: A

POLICY A document that specifies who can access which resources, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. For more information, see Example Scenario and How Policies Work. The word "policy" is used by people in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources.

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

QUESTION 13

Which storage type is most effective when you want to move some unstructured data, consisting of images and videos, to cloud storage?

- A. Standard storage
- B. File storage
- C. Archivestorage
- D. Block volume

Correct Answer: A

Use Oracle Cloud Infrastructure Object Storage for data to which you need fast, immediate, and frequent access. Data accessibility and performance justifies a higher price point to store data in the Object Storage tier. The Object Storage service can store an unlimited amount of unstructured data of any content type, including analytic data and rich content, like images and videos.

<https://docs.oracle.com/en/solutions/learn-migrate-app-data-to-cloud/considerations-object-storage.html#GUID-AC192B08-5160-4DA7-B43E-001753D99CF1>

QUESTION 14

With regard to WAF in OCI, which of the following statements are NOT customer's responsibility? Select TWO answers.

- A. Configure WAF policies for websites
- B. WAF edge nodes with High Availability
- C. Configure Bot Management strategies for a website traffic

D. Import latest OWASP Core Rule Sets

Correct Answer: BD

QUESTION 15

Which OCI services can encrypt all data-at-rest ? Select TWO correct answers

- A. File Storage
- B. NAT Gateway
- C. Block Volumes
- D. Geolocation Steering

Correct Answer: AC

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

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

[1Z0-1104-22 Braindumps](#)