



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.geekcert.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

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 2

What are the security recommendations and best practices for Oracle Functions?

- A. Grant privileges to UID and GID 1000, such that the functions running within a container acquire the default root capabilities.
- B. Add applications to network security groups for fine-grained ingress/egress rules.
- C. Define a policy statement that enables access to functions for requests coming from multiple IP addresses.
- D. Ensure that functions in a VCN have restricted access to resources and services.

Correct Answer: B

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

QUESTION 3

Which is NOT a compliance document?

- A. Certificate



B. Penetration test report

C. Attestation

D. Bridge letter

Correct Answer: B

Types of Compliance Documents

When viewing compliance documents, you can filter on the following types:

Attestation. A Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Compliance document.

Audit. A general audit report.

Bridge Letter (BridgeLetter). A bridge letter. Bridge letters provide compliance information for the period of time between the end date of an SOC report and the date of the release of a new SOC report.

Certificate. A document indicating certification by a particular authority, with regard to certification requirements and examination results conforming to said requirements.

SOC3. A Service Organization Controls 3 audit report that provides information relating to a service organization's internal controls for security, availability, confidentiality, and privacy.

Other. A compliance document that doesn't fit into any of the preceding, more specific categories.

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

QUESTION 4

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 5

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

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

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

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