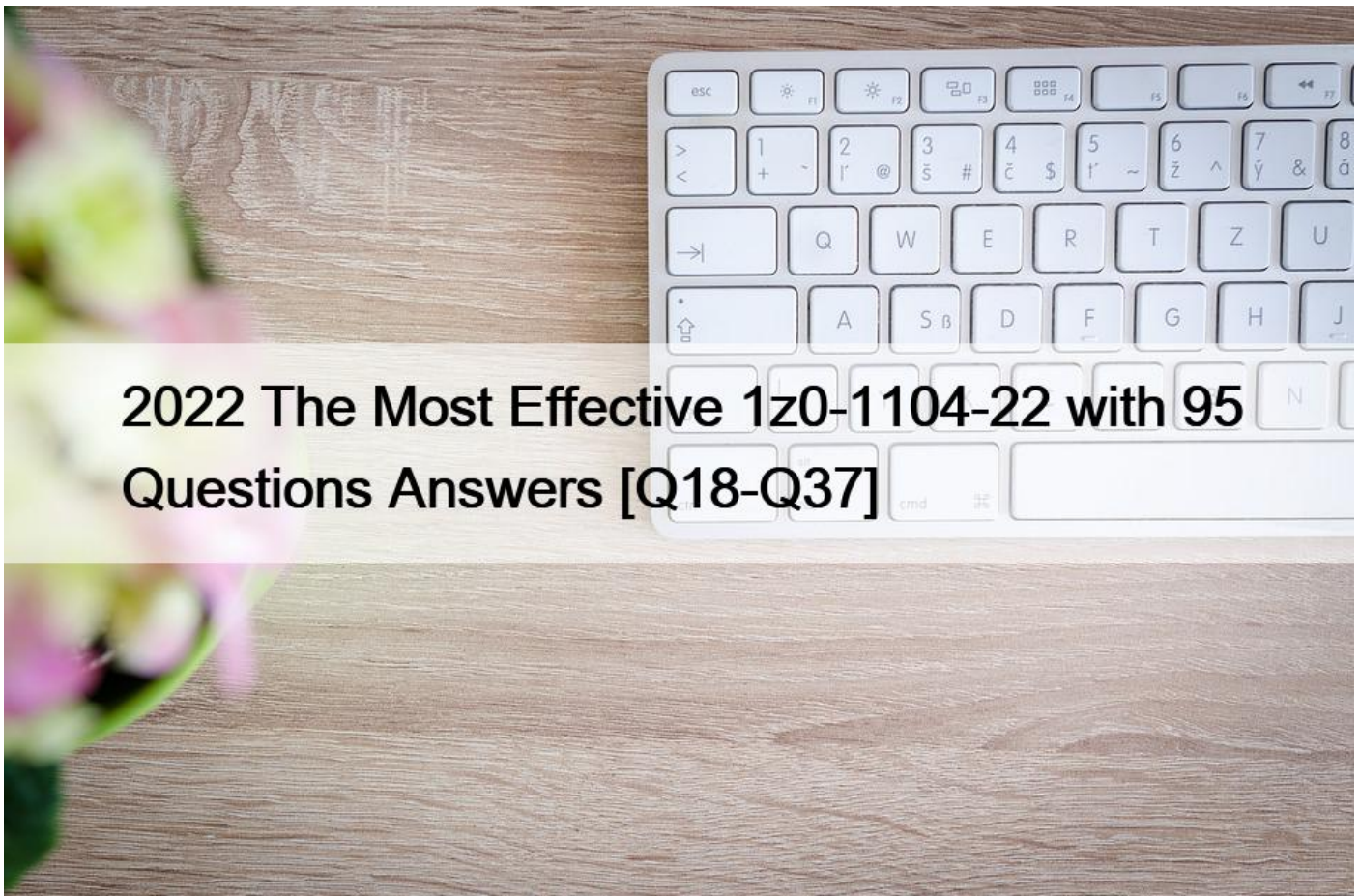


## 2022 The Most Effective 1z0-1104-22 with 95 Questions Answers [Q18-Q37]



### 2022 The Most Effective 1z0-1104-22 with 95 Questions Answers Try Free and Start Using Realistic Verified 1z0-1104-22 Dumps Instantly. QUESTION 18

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

- \* Policies
- \* Users
- \* Dynamic groups
- \* Groups

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 19

You want to make API calls against other OCI services from your instance without configuring user credentials. How would you achieve this?

- \* Create a dynamic group and add a policy.
- \* Create a dynamic group and add your instance.
- \* Create a group and add a policy.
- \* No configuration is required for making API calls.

#### DYNAMIC GROUP

Dynamic groups allow you to group Oracle Cloud Infrastructure instances as principal actors, similar to user groups. You can then create policies to permit instances in these groups to make API calls against Oracle Cloud Infrastructure services. Membership in the group is determined by a set of criteria you define, called matching rules.

<https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/calling-services-from-instances.htm>

### QUESTION 20

Logical isolation for resources is provided by which OCI feature?

- \* Tenancy
- \* Availability Zone
- \* Region
- \* Compartments

### QUESTION 21

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?

- \* service connector hub
- \* management agent log integration
- \* objectcollectionrule
- \* audit analysis dashboard

### QUESTION 22

How can you convert a fixed load balancer to a flexible load balancer?

- \* There is no way to convert the load balancer.
- \* Use Update Shape workflows.
- \* Delete the fixed load balancer and create a new one.
- \* Using the Edit Listener option.

### QUESTION 23

Which is NOT a part of Observability and Management Services?

- \* Event Services
- \* OCI Management Service
- \* Logging Analytics
- \* Logging

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

#### QUESTION 24

Which of these protects customer data at rest and in transit in a way that allows customers to meet their security and compliance requirements for cryptographic algorithms and key management?

- \* Security controls
- \* Customer isolation
- \* Data encryption
- \* Identity Federation

DATA ENCRYPTION

Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements for cryptographic algorithms and key management.

[https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security\\_overview.htm](https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm)

#### QUESTION 25

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 tenant 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?

- \* allow group orgauditgrp to read all-resources in tenancy where target.compartment.name !=dev
- \* allow group orgauditgrp to read all-resources in compartment !=dev
- \* allow group orgauditgrp to inspect all-resources in tenancy where target compartment.name !=dev
- \* allow group orgauditgrp to inspect all-resources in compartment !=dev

#### QUESTION 26

With regard to vulnerability and cloud penetration testing, which rules of engagement apply? Select TWO correct answers.

- \* Any port scanning must be performed in an aggressive mode
- \* Physical penetration and vulnerability testing of Oracle facilities is prohibited
- \* Testing should target any other subscription or any other Oracle Cloud customer resources
- \* You are responsible for any damages to Oracle Cloud customers that are caused by your testing activities

## Rules Of Engagement

The following rules of engagement apply to cloud penetration and vulnerability testing:

- Your testing must not target any other subscription or any other Oracle Cloud customer resources, or any shared infrastructure components.
- You must not conduct any tests that will exceed the bandwidth quota or any other subscribed resource for your subscription.
- You are strictly prohibited from utilizing any tools or services in a manner that perform Denial of Service (DoS) attacks or simulations of such, or any "load testing" against any Oracle Cloud asset including yours.
- Any port scanning must be performed in a non-aggressive mode.
- You are responsible for independently validating that the tools or services employed during penetration and vulnerability testing do not perform DoS attacks, or simulations of such, prior to assessment of your instances. This responsibility includes ensuring any contracted third parties perform assessments in a manner that does not violate this policy.
- Social Engineering of Oracle employees and physical penetration and vulnerability testing of Oracle facilities is prohibited.
- You must not attempt to access another customer's environment or data, or to break out of any container (for example, virtual machine).
- Your testing will continue to be subject to terms and conditions of the agreement(s) under which you purchased Oracle Cloud Services, and nothing in this policy shall be deemed to grant you additional rights or privileges with respect to such Cloud Services.
- If you believe you have discovered a potential security issue related to Oracle Cloud, you must report it to Oracle within 24 hours by conveying the relevant information to [My Oracle Support](#). You must create a service request within 24 hours and must not disclose this information publicly or to any third party. Note that some of the vulnerabilities and issues you may discover may be resolved by you by applying the most recent patches in your instances.
- In the event you inadvertently access another customer's data, you must immediately terminate all testing and report it to Oracle within one hour by conveying the relevant information to [My Oracle Support](#).
- You are responsible for any damages to Oracle Cloud or other Oracle Cloud customers that are caused by your testing activities by falling to abide by these rules of engagement.

### QUESTION 27

What does the following identity policy do?

Allow group my-group to use fn-invocation in compartment ABC where target.function.id = `&#8216;<function-OCID>&#8217;`

- \* Enables users in a group to create, update, and delete ALL applications and functions in a compartment
- \* Enables users to invoke all the functions in a specific application
- \* Enables users to invoke just one specific function
- \* Enables users to invoke all the functions in a compartment except for one specific function

### QUESTION 28

In which two ways can you improve data durability in Oracle Cloud Infrastructure Object Storage?

- \* Setup volumes in a RAID1 configuration
- \* Enable server-side encryption
- \* Enable Versioning
- \* Limit delete permissions
- \* Enable client-side encryption

### QUESTION 29

What is the minimum active storage duration for logs used by Logging Analytics to be archived?

- \* 60 days

- \* 10 days
- \* 30 days
- \* 15 days

<https://docs.oracle.com/en-us/iaas/logging-analytics/doc/manage-storage.html#:~:text=The%20minimum%20Active%20Storage%20Duration,be%20archived%20is%2030%20days.>

The minimum Active Storage Duration (Days) for logs before they can be archived is 30 days.

### QUESTION 30

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?

- \* Create an IAM policy and create WAF rules
- \* Create an IAM policy and add a network source
- \* Make OCI resources private instead of public
- \* Create PAR to restrict access the access

#### Introduction to Network Sources

A network source is a set of defined IP addresses. The IP addresses can be public IP addresses or private 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 root 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 With Network Sources 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 31

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

- \* Bad Bot Denylist
- \* CAPTCHA Challenge
- \* IP Prefix Steering
- \* Good Bot Allowlist

# 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 32

What does an audit log event include?

- \* Audit type
- \* Header
- \* Footer
- \* Type of input

The HTTP header fields and values in the request.

<https://docs.oracle.com/en-us/iaas/Content/Audit/Reference/logeventreference.htm>

## QUESTION 33

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

- \* File Storage
- \* NAT Gateway
- \* Block Volumes
- \* Geolocation Steering

### 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. Select 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 also enable 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.

### QUESTION 34

Which type of software do you use to centrally distribute and monitor the patch level of systems throughout the enterprise?

- \* Network Monitor software
- \* Web Application Firewall
- \* Patch Management software
- \* Recovery Manager software

[https://docs.oracle.com/cd/E11857\\_01/em.111/e18710/T531901T535649.htm](https://docs.oracle.com/cd/E11857_01/em.111/e18710/T531901T535649.htm)

### QUESTION 35

What must be configured for a load balancer to accept incoming traffic?

- \* Service Gateway
- \* SSL certificate
- \* Listener
- \* Route table entry pointing to the listener IP address

A listener is an entity that checks for connection requests. The load balancer listener listens for ingress client traffic using the port you specify within the listener and the load balancer's public IP.

<https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/loadbalancing.htm>

To create a listener:

On your Load Balancer Details page, click Listeners.

Click Create Listener.

Enter the following:

Name: Enter a friendly name. Avoid entering confidential information.

Protocol: Select HTTP.

Port: Enter 80 as the port on which to listen for incoming traffic.

Backend Set: Select the backend set you created.

Click Create.

### QUESTION 36

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

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

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

### QUESTION 37

An automobile company needs to configure Bastion Managed SSH session to a compute instance in a private subnet. What are the TWO prerequisites to configure successfully?

- \* NAT or Service Gateway should be attached to the private subnet
- \* There is no need for any gateway in private subnet
- \* SSH port forwarding should be enabled
- \* Route rule to a NAT or Service Gateway should be associated with the subnet of the route table

**Download Free Latest Exam 1z0-1104-22 Certified Sample Questions:**

<https://www.dumpsmaterials.com/1z0-1104-22-real-torrent.html>