



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.passapply.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

Which IAM policy should be created to give XYZ the ability to list contents of a resource excluding the needs to authenticate in prod compartment ? Principle of least privilege should be used.

- A. Allow group XYZ to manage all resources in compartment != prod
- B. Allow group XYZ to use all resources in compartment != prod
- C. Allow group XYZ to inspect all resources in tenancy where target.compartment.name != prod
- D. Allow group XYZ to read all resources in tenancy where target.compartment.name != prod

Correct Answer: C

Verbs

You use *verbs* in policy definitions to set the permission levels that given user groups have for given resource-types. For example, you would use the `read` verb to allow read-only access.

Here are the verbs have been defined for the set of Oracle Digital Assistant resource-types.

Verb	Description
inspect	Generally covers operations that list contents of a resource. This is the verb that provides the most limited access.
read	In user interface terms, this generally means read-only access. In API terms, it generally applies to GET operations.
use	When applied to resources in the service's user interface, this generally allows developing, testing, and deploying of these resources. At the API level, it generally allows GET, PUT, POST, PATCH, and DELETE operations, with the exception of more high-impact operations (such as creating instances and purging data).
manage	Generally allows the user to perform the whole set of a resource type's operations, including high-impact operations such as creating instances and purging data.

QUESTION 2

Select the component that encompasses the overall configuration of your WAF service on OCI.

- A. Protection rules
- B. Bot Management
- C. Web Application Firewall policy
- D. Origin

Correct Answer: C

WAF Policy Management



Provides an overview of web application firewall (WAF) policies, including their creation, updating, and deletion.

WAF policies encompass the overall configuration of your WAF service, including access rules, rate limiting rules, and protection rules.

https://docs.oracle.com/en-us/iaas/Content/WAF/Policies/waf-policy_management.htm

QUESTION 3

As a lead Security Architect, you have tasked to restrict access to and from the worker nodes in pods running in Oracle Container Engine for Kubernetes?

- A. Cloud Guard
- B. Vulnerability Scanning
- C. Security Lists
- D. Identity and Access Management

Correct Answer: C

Node Pool Security Lists

Network administrators can define security list rules on node pool subnets to restrict access to and from worker nodes. Defining security list rules allows administrators to enforce network restrictions that cannot be overridden on the hosts in your cluster.

Because all pod-to-pod communication occurs in a VXLAN overlay network on the worker nodes, you are cannot use security list rules to restrict pod-to-pod communication. However, you can use security lists to restrict access to and from your worker nodes.

Important: There is a minimum set of security list rules that must exist on node pool subnets to ensure that the cluster can function. See [Example Network Resource Configurations](#) for information on the minimum set of security list rules before making any changes to your security list rules.

QUESTION 4

Which Security Zone policy is NOT valid?

- A. A boot volume can be moved from a security zone to a standard compartment.
- B. A compute instance cannot be moved from a security zone to a standard compartment.
- C. Resources in a security zone should not be accessible from the public internet.
- D. Resources in a security zone must be automatically backed up regularly.



Correct Answer: A

QUESTION 5

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>

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

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

[1Z0-1104-22 Exam Questions](#)