DUMPSBOSS.

Oracle Cloud Infrastructure 2026 Security Professional

Oracle 1z0-1104-25

Version Demo

Total Demo Questions: 5

Total Premium Questions: 56

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A company has implemented OCI IAM policies with multiple levels of compartments. A policy attached to a parent compartment grants "manage virtual-network-family" permissions. A policy attached to a child compartment grants "use virtual-network-family" permissions.

According to OCI IAM policy inheritance, how does the OCI IAM policy engine resolve the permissions for a user attempting to perform an operation that requires 'manage' permissions in the child compartment?

A. The operation is denied due to conflicting policies.

B. The policy in the parent compartment takes precedence, and the user is granted "manage" permissions.

C. The policy in the child compartment takes precedence, and the user is granted "use" permissions only.

ANSWER: B

Explanation:

The policy in the parent compartment takes precedence, and the user is granted "manage" permissions. In OCI, a policy that grants access within a compartment applies to that compartment and to all of its child compartments in the hierarchy. Therefore, the parent-compartment statement granting `manage virtual-network-family` is effective for virtual networking resources and operations in the child compartment as well. The child-compartment statement granting `use virtual-network-family` does not reduce, override, or otherwise constrain the permission already granted through the parent scope. OCI IAM evaluates applicable policy statements cumulatively to determine whether the requesting principal has the permission required for the requested operation; OCI policies are allow statements and do not provide an explicit deny mechanism that could negate an inherited grant. Since `manage` includes the permissions needed for management operations on the virtual-network resource family, the operation requiring manage-level access in the child compartment is authorized. This inheritance behavior enables administrators to establish broad access at a parent level while adding further grants at more specific compartment levels when needed. See Oracle's IAM Policies documentation and its guidance on compartments and access control.

QUESTION NO: 2 - (SIMULATION)

Task 2: Create a Compute Instance and Install the Web Server

Create a compute instance, where:

Name: PBT-CERT-VM-01

Image: Oracle Linux 8

Shape: VM.Standard.A1.Flex

Subnet: Compute-Subnet-PBT-CERT

Install and configure Apache web server:

a.

Install Apache

sudo yum -y install httpd

b.

Enable and start Apache

sudo systemctl enable httpd

sudo systemctl restart httpd

2. Install and configure Apache web server:

a. Install Apache

sudo yum -y install httpd

b. Enable and start Apache

sudo systemctl enable httpd

sudo systemctl restart httpd

c. Configure firewall to allow HTTP traffic (port 80)

sudo firewall-cmd --permanent --add-port=80/tcp

sudo firewall-cmd --reload

d. Create an index.html file

sudo bash -c 'echo You are visiting Web Server 1 >> /var/www/html/index.html'

Enter the OCID of the created compute instance PBT-CERT-VM-01 in the text box below.

ANSWER: Check the explanation for the answer

Explanation:

Create the instance with the required configuration:

Name: `PBT-CERT-VM-01`
Image: Oracle Linux 8
Shape: `VM.Standard.A1.Flex`
Subnet: `Compute-Subnet-PBT-CERT`

After it reaches **Running**, connect as `opc` and run:

```
sudo yum -y install httpd
sudo systemctl enable httpd
sudo systemctl restart httpd
sudo firewall-cmd --permanent --add-port=80/tcp
sudo firewall-cmd --reload
sudo bash -c 'echo You are visiting Web Server 1 >> /var/www/html/index.html'
```

Answer to enter: Copy and paste the actual OCID shown on the details page of the newly created `PBT-CERT-VM-01` instance. It has the format:

```
ocid1.instance.oc1.<region-identifier>.<unique-instance-id>
```

The exact OCID is generated uniquely in the simulation tenancy and cannot be determined before the instance is created. In the OCI Console, open **Compute > Instances > PBT-CERT-VM-01**, click **Copy** beside **OCID**, and enter that full value in the text box.

Also ensure that the subnet security list or NSG permits inbound TCP port `80`; the OS firewall command alone does not open OCI network ingress.

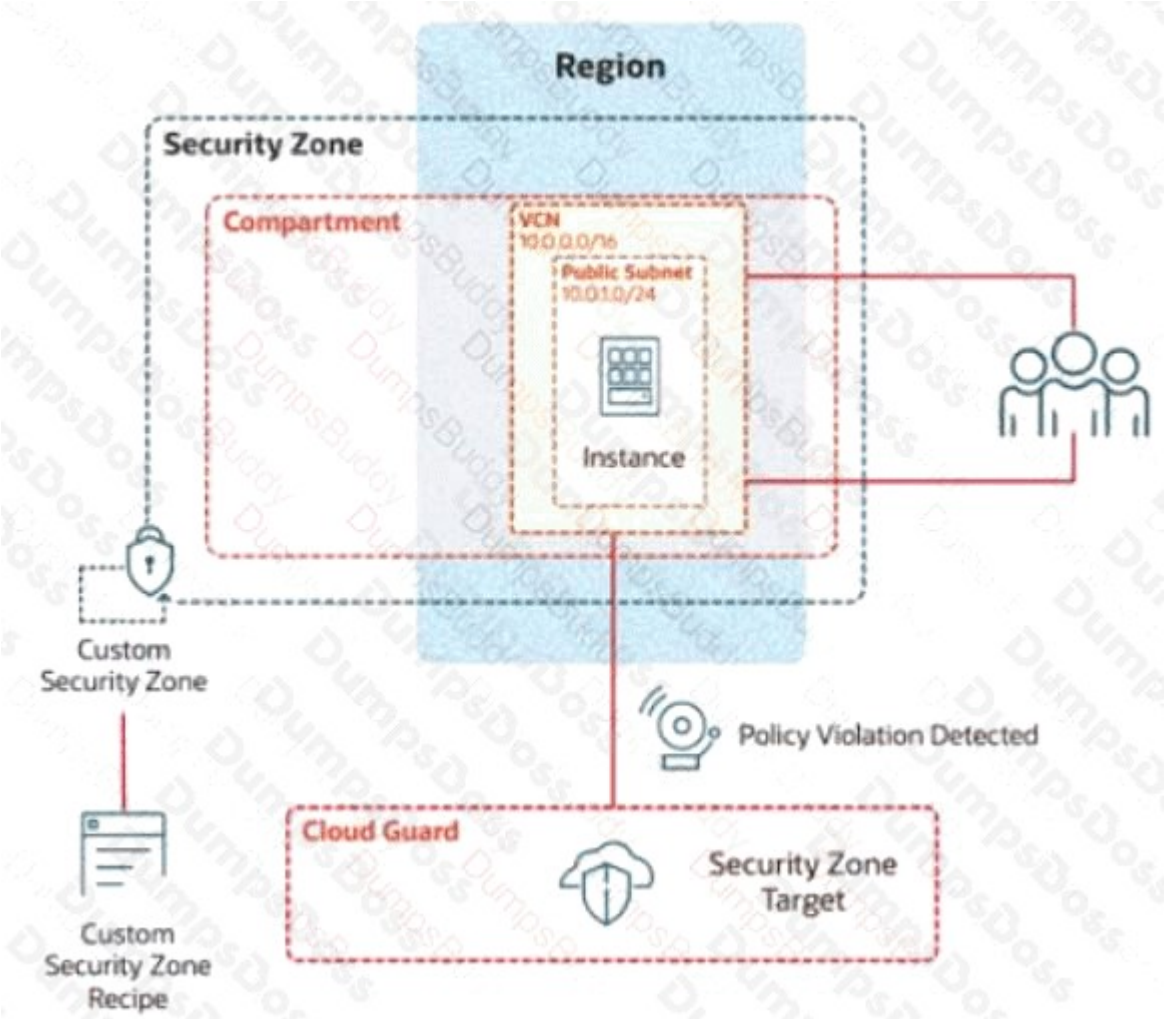
QUESTION NO: 3 - (SIMULATION)

Challenge 2 -Task 1

In deploying a new application, a cloud customer needs to reflect different security postures. If a security zone is enabled with the Maximum Security Zone recipe, the customer will be unable to create or update a resource in the security zone if the action violates the attached Maximum Security Zone policy.

As an application requirement, the customer requires a compute instance in the public subnet. You therefore, need to configure Custom Security Zones that allow the creation of compute instances in the public subnet.

Review the architecture diagram, which outlines the resoures you'll need to address the requirement:



Preconfigured

To complete this requirement, you are provided with the following:

Access to an OCI tenancy, an assigned compartment, and OCI credentials

Required IAM policies

Task3: Create and configure a Virtual Cloud Network and Private Subnet

Createand configure virtual cloud Network (VCN) named IAD SP-PBT-VCN-01, with an internet Gateway and configure appropriate route rules to allow external connectivity.

Enter the OCID of the created VCN in the text box below.

ANSWER: Check the explanation for the answer

Explanation:

Create the following networking resources in the assigned Security Zone compartment:

VCN name: `IAD SP-PBT-VCN-01`
VCN IPv4 CIDR: `10.0.0.0/16`
Public subnet IPv4 CIDR (per the architecture): `10.0.1.0/24`

The diagram identifies the subnet as a **Public Subnet**, despite the task heading referring to a private subnet. Configure the subnet so that it can use an Internet Gateway, as required for the public-instance use case and permitted by the custom Security Zone recipe.

Console steps

1. Open **Networking > Virtual Cloud Networks**, select the assigned compartment, and select **Create VCN**.
2. Create the VCN with name `IAD SP-PBT-VCN-01` and CIDR block `10.0.0.0/16`.
3. From the new VCN's **Internet Gateways** resource, select **Create Internet Gateway**. Create it in the same compartment and ensure it is **enabled**.
4. From **Route Tables**, create or edit the route table that will be associated with the public subnet. Add this rule:

```
Destination CIDR: 0.0.0.0/0
Target type: Internet Gateway
Target: the Internet Gateway created for IAD SP-PBT-VCN-01
```

5. Create the subnet using CIDR `10.0.1.0/24`, associate it with that route table, and configure it as a public subnet (do not prohibit public IPv4 addresses on VNICs). The custom Security Zone recipe must be the one that permits this public-subnet configuration.

Answer to enter: On the VCN details page, copy the OCID for `IAD SP-PBT-VCN-01` and paste that exact generated value into the simulation text box. It will have this form:

`ocid1.vcn.oc1.<region-identifier>.<unique-id>`

The precise OCID cannot be predetermined; it is generated by OCI when the VCN is created.

QUESTION NO: 4

An application tier consists of Compute instances distributed across several subnets. The security team wants one set of ingress and egress rules to follow the application instances even when an instance is moved to another subnet or when additional subnets are introduced.

Which OCI networking security control should be used?

A. A network security group

B. A security list

C. A route table

D. A Network Load Balancer

ANSWER: A

Explanation:

A network security group (NSG) is the appropriate control because its security rules are associated with selected virtual network interface cards (VNICs), rather than with an entire subnet. This allows the same application-tier rules to be applied consistently to instances across multiple subnets.

Security lists apply to every VNIC in the associated subnet, so they are less suitable when the policy must follow a specific application tier across changing subnet placement. Route tables control traffic paths, and a Network Load Balancer does not provide instance-level ingress and egress rule enforcement.

QUESTION NO: 5

"A programmer is developing a Node.js application which will run on a Linux server on their on-premises data center. This application will access various Oracle Cloud Infrastructure (OCI) services using OCI SDKs.

What is the secure way to access OCI services with OCI Identity and Access Management (IAM)?

A. Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, add the user name and password to a file used by Node.js authentication.

B. Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, generate the keypair used for signing API requests and upload the public key to the IAM user.

C. Create a new OCI IAM user associated with a dynamic group and a policy that grants the desired permissions to OCI services. Add the on-premises Linux server in the dynamic group.

D. Create an OCI IAM policy with appropriate permissions to access the required OCI services and assign the policy to the on-premises Linux server."

ANSWER: B

Explanation:

Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, generate the keypair used for signing API requests and upload the public key to the IAM user. This is the appropriate authentication model for an application running outside OCI because the OCI SDK can use API-signing key credentials for an IAM user. The application retains the private key securely on the on-premises host and uses it to cryptographically sign each OCI API request. OCI validates that signature against the public key registered for the IAM user, while IAM policies granted through the user's group control exactly which actions and resources the application can access.

For the Node.js SDK, the application's configuration supplies values such as the tenancy OCID, user OCID, API-key fingerprint, region, and the path to the private signing key. The private key must be protected with restrictive file permissions and should not be committed to source control or embedded in application code. This approach provides strong, non-password-based authentication and enables administrators to rotate or revoke the API signing key when necessary. Oracle documents this SDK configuration and signing-key workflow at SDK and CLI Configuration File and How to Generate an API Signing Key.