ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Oracle

Code: 1Z0-1104-25

Exam: Oracle Cloud Infrastructure 2025 Security Professional

https://www.examsnest.com/exam/1z0-1104-25/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Topic 1, Labs / Hands-on Performance Based

Question: 1

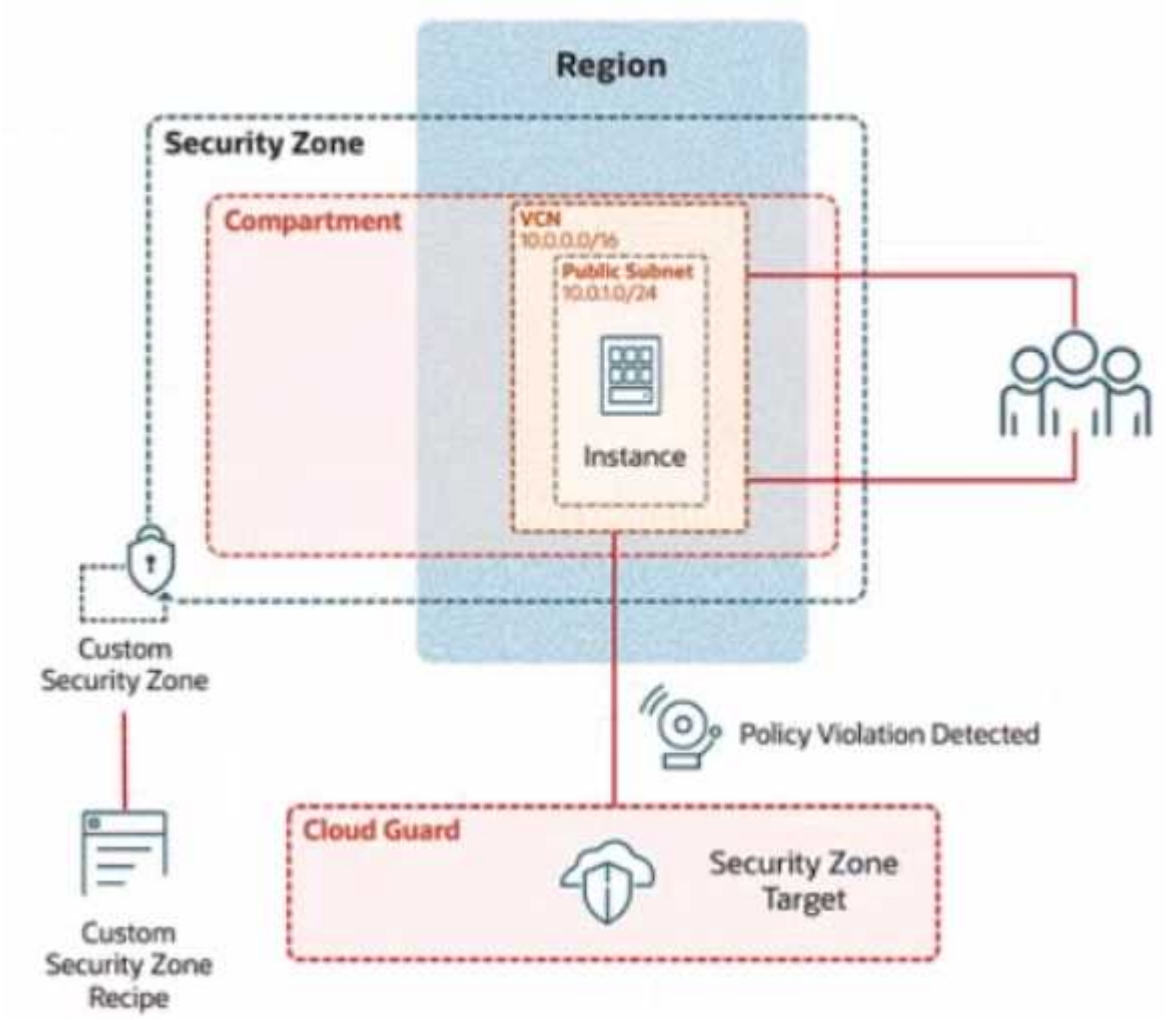
SIMULATION

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

Task 1: Create a Custom Security Zone Recipe

Create a Custom Security Zone Recipe named IAD-SP-PBT-CSP-01 that allows the provisioning of compute instances in the public subnet.

Enter the OCID of the created custom security zone recipe in the text box below.

Answer: See the solution below in

Explanation.

Explanation:

To create a Custom Security Zone Recipe named IAD-SP-PBT-CSP-01 that allows the provisioning of compute instances in a public subnet, we will follow the steps outlined in the Oracle Cloud Infrastructure (OCI) Security Zones documentation. These steps are based on verified procedures from the OCI Security Zone Guide and related resources.

Step-by-Step Solution for Task 1: Create a Custom Security Zone Recipe

Log in to the OCI Console:

Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.com).

Ensure you have access to the assigned compartment provided in the tenancy.

Navigate to Security Zones:

From the OCI Console, go to the navigation menu (hamburger icon) on the top left.

Under Governance and Administration, select Security Zones.

Create a New Security Zone Recipe:

In the Security Zones dashboard, click on the Recipes tab.

Click the Create Recipe button.

Configure the Recipe Details:

Name: Enter IAD-SP-PBT-CSP-01.

Description: (Optional) Add a description, e.g., "Custom recipe to allow compute instances in public subnet."

Leave the Compartment as the assigned compartment provided.

Define the Security Zone Policy:

In the policy editor, start with a base policy. Since the Maximum Security Zone recipe restricts public subnet usage, you need to customize it.

Add the following policy statement to allow compute instances in a public subnet:

Allow service compute to use virtual-network-family in compartment <compartment-name> where ALL {

target.resource.type = 'Instance',

target.vcn.cidr_block = '10.0.0.0/16',

target.subnet.cidr_block = '10.0.10.0/24'

}

Replace <compartment-name> with the name of your assigned compartment.

This policy allows the Compute service to provision instances in the public subnet (10.0.10.0/24) within the VCN (10.0.0.0/16).

Adjust Restrictions:

Ensure the recipe does not inherit the Maximum Security Zone recipe's default restrictions that block public subnet usage. Explicitly allow the public subnet by including the subnet CIDR block (10.0.10.0/24) in the policy.

Remove or modify any conflicting default rules that prohibit public subnet usage (e.g., rules blocking internet access or public IP assignment).

Save the Recipe:

Click Create to save the custom security zone recipe.

Once created, note the OCID of the recipe from the recipe details page. The OCID will be a unique identifier starting with ocid1.securityzonerecipe.

Verify the Recipe:

Go to the Recipes tab and locate IAD-SP-PBT-CSP-01.

Ensure the policy reflects the allowance for compute instances in the public subnet by reviewing the policy statement.

OCID of the Created Custom Security Zone Recipe

The exact OCID will be generated upon creation (e.g., ocid1.securityzonerecipe.oc1..unique_string). Please enter the OCID displayed in the OCI Console after completing Step 7.

Notes

Ensure IAM policies are correctly configured to grant you permissions to create and manage security zone recipes in the compartment.

The policy assumes the public subnet CIDR (10.0.10.0/24) matches the diagram. Adjust if the actual subnet CIDR differs.

Test the recipe by associating it with a security zone and attempting to launch a compute instance to confirm compliance.

Question: 2

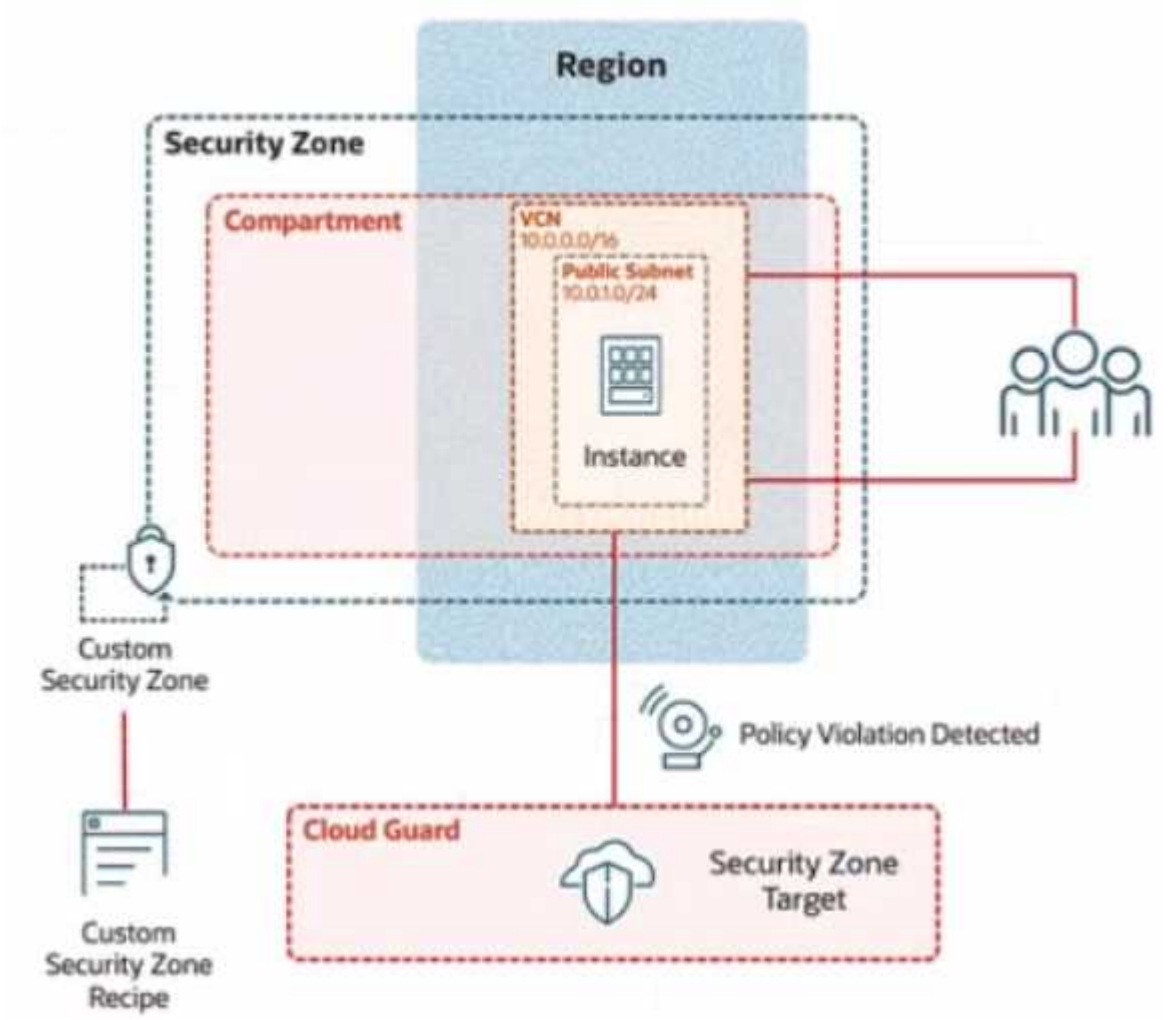
SIMULATION

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

Task 2: Create a Security Zone

Create a security Zone named IAD_SAP-PBT-CSZ-01 in your assigned compartement and associate it with the Custom Security Zone Recipe (IAD-SAP-PBT-CSP-01) created in the previous task.

Enter the OCID of the created Security zone in the box below.

Security Zone name: IAD-SP-PBT-CSZ--01
Associated Recipe: IAD-SP-PBT-CSP-01
Compartment: 98815992-C01
Purpose: Allow compute in Public Subnet

Answer: See the solution below in Explanation.

Explanation:

To create a Security Zone named IAD_SAP-PBT-CSZ-01 in your assigned compartment and associate it with the Custom Security Zone Recipe IAD-SP-PBT-CSP-01 created in the previous task, follow these steps based on the Oracle Cloud Infrastructure (OCI) Security Zones documentation.

Step-by-Step Solution for Task 2: Create a Security Zone

Log in to the OCI Console:

Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.com).

Ensure you have access to the assigned compartment.

Navigate to Security Zones:

From the OCI Console, click the navigation menu (hamburger icon) on the top left.

Under Governance and Administration, select Security Zones.

Create a New Security Zone:

In the Security Zones dashboard, click the Create Security Zone button.

Configure the Security Zone Details:

Name: Enter IAD_SAP-PBT-CSZ-01.

Compartment: Select the assigned compartment provided.

Description: (Optional) Add a description, e.g., "Security Zone for public subnet compute instances."

Associate the Custom Security Zone Recipe:

In the Recipe section, select the custom recipe IAD-SP-PBT-CSP-01 created in Task 1 from the dropdown list.

Ensure the recipe is correctly associated to enforce the policy allowing compute instances in the public subnet.

Define the Security Zone Scope:

Under Resources to Protect, select the compartment or specific resources (e.g., the VCN with CIDR 10.0.0.0/16 and public subnet 10.0.10.0/24) to apply the security zone.

Check the box to include all resources in the selected compartment if applicable.

Create the Security Zone:

Click Create to finalize the security zone creation.

Once created, note the OCID of the security zone from the security zone details page. The OCID will be a unique identifier starting with ocid1.securityzone.

Verify the Security Zone:

Go to the Security Zones tab and locate IAD_SAP-PBT-CSZ-01.

Confirm the associated recipe (IAD-SP-PBT-CSP-01) and the applied policies.

OCID of the Created Security Zone

The exact OCID will be generated upon creation (e.g., ocid1.securityzone.oc1..<unique_string>). Please enter the OCID displayed in the OCI Console after completing Step 7.

Question: 3

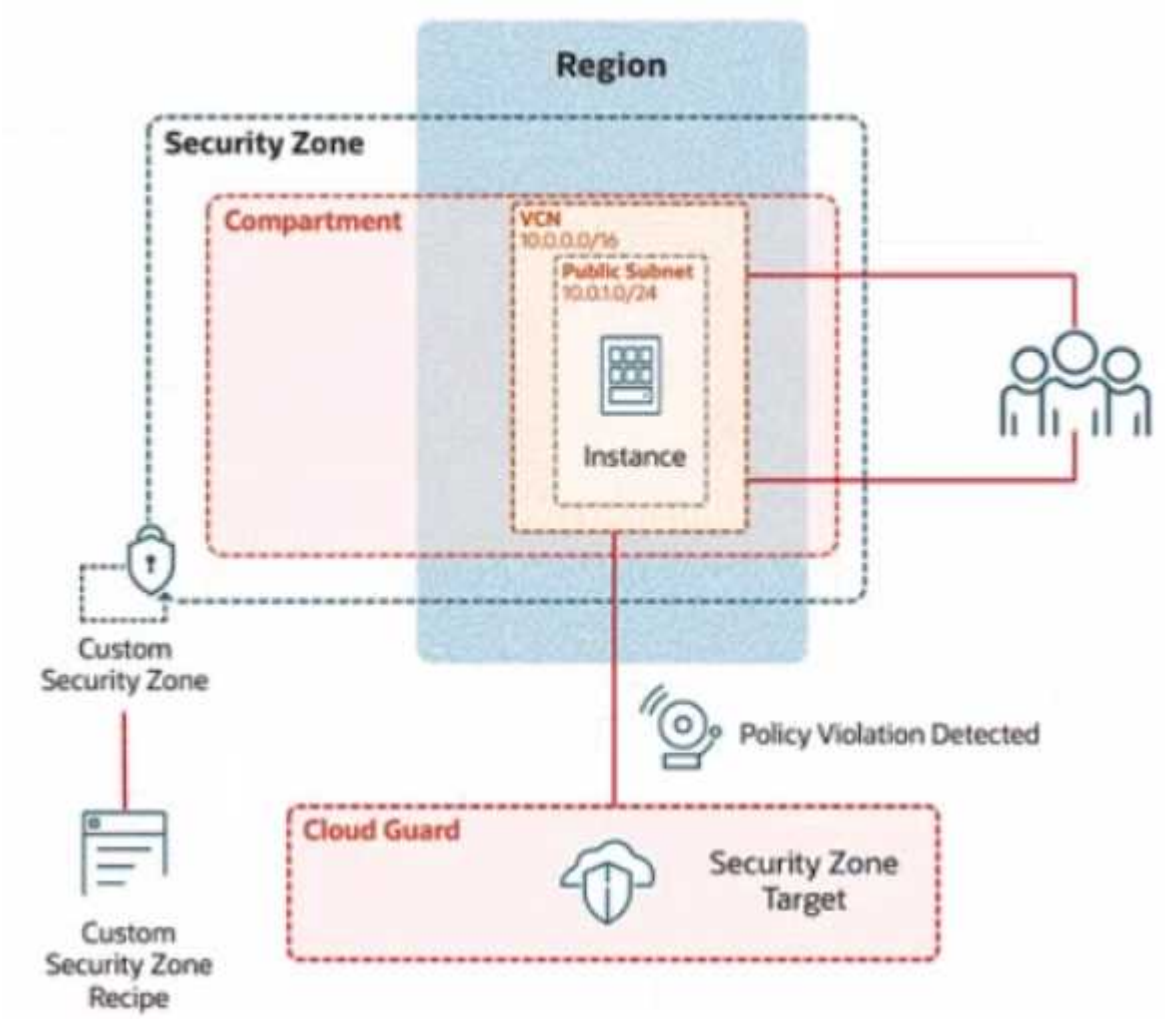
SIMULATION

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

Create and 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: See the

solution below in Explanation.

Explanation:

To create and configure a Virtual Cloud Network (VCN) named IAD-SP-PBT-VCN-01 with an Internet Gateway and appropriate route rules for external connectivity, follow these steps based on the Oracle Cloud Infrastructure (OCI) Networking documentation.

Step-by-Step Solution for Task 3: Create and Configure a VCN and Private Subnet

Log in to the OCI Console:

Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.com).

Ensure you have access to the assigned compartment.

Navigate to Virtual Cloud Networks:

From the OCI Console, click the navigation menu (hamburger icon) on the top left.

Under Networking, select Virtual Cloud Networks.

Create a New VCN:

Click Start VCN Wizard and select Create VCN with Internet Connectivity.

VCN Name: Enter IAD-SP-PBT-VCN-01.

Compartment: Select the assigned compartment.

VCN CIDR Block: Enter 10.0.0.0/16 (matches the diagram's VCN CIDR).

Public Subnet CIDR Block: Enter 10.0.10.0/24 (matches the diagram's public subnet).

Accept the default settings for the public subnet and Internet Gateway creation.

Click Create to provision the VCN, Internet Gateway, and public subnet.

Verify the Internet Gateway:

After creation, go to the VCN details page for IAD-SP-PBT-VCN-01.

Under Resources, select Internet Gateways.

Ensure the Internet Gateway is attached and enabled.

Configure Route Rules:

In the VCN details page, under Resources, select Route Tables.

Select the default route table associated with the public subnet (10.0.10.0/24).

Click Add Route Rules.

Target Type: Select Internet Gateway.

Destination CIDR Block: Enter 0.0.0.0/0.

Target Internet Gateway: Select the Internet Gateway created with the VCN.

Click Add Route Rule to save.

Update Security List (if needed):

Under Resources, select Security Lists.

Edit the default security list for the public subnet.

Add an ingress rule:

Source CIDR: 0.0.0.0/0

IP Protocol: TCP

Source Port Range: All

Destination Port Range: 22 (for SSH) or as required by your application.

Add an egress rule:

Destination CIDR: 0.0.0.0/0

IP Protocol: All

Save the changes.

Note the VCN OCID:

Return to the VCN details page for IAD-SP-PBT-VCN-01.

Copy the OCID displayed (e.g., ocid1.vcn.oc1..<unique_string>).

OCID of the Created VCN

Enter the OCID of the created VCN (IAD-SP-PBT-VCN-01) into the text box. The exact OCID will be available after Step 3 (e.g., ocid1.vcn.oc1..<unique_string>).

Question: 4

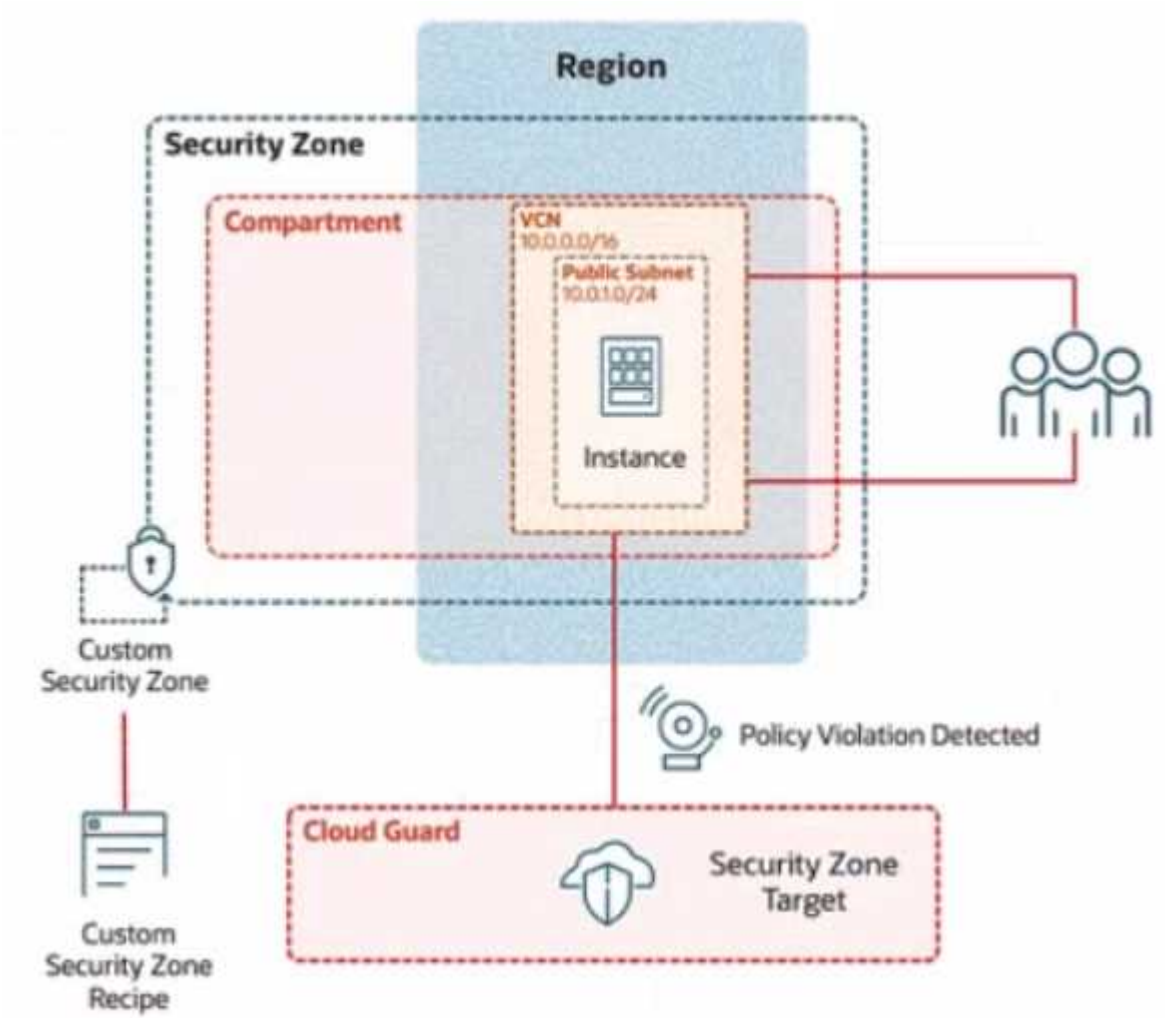
SIMULATION

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

Task 4: Create a Public Subnet

Create a public subnet named IAD-SP-PBT-PUBSNET-01, within the VCN IAD-SP-PBT-VCN-01

use a CIDR block of 10.0.1.0/24 and configure the subnet to use the internet Gateway

Answer: See the solution below in Explanation.

Explanation:

To create a public subnet named IAD-SP-PBT-PUBSNET-01 within the VCN IAD-SP-PBT-VCN-01 using a CIDR block of 10.0.1.0/24 and configure it to use the Internet Gateway, follow these steps based on the Oracle Cloud Infrastructure (OCI) Networking documentation.

Step-by-Step Solution for Task 4: Create a Public Subnet

Log in to the OCI Console:

Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.com).

Ensure you have access to the assigned compartment.

Navigate to Virtual Cloud Networks:

From the OCI Console, click the navigation menu (hamburger icon) on the top left.

Under Networking, select Virtual Cloud Networks.

Select the VCN:

Locate and click on the VCN named IAD-SP-PBT-VCN-01 created in Task 3.

Under Resources, select Subnets.

Create a New Subnet:

Click the Create Subnet button.

Configure the Subnet Details:

Name: Enter IAD-SP-PBT-PUBSNET-01.

Compartment: Ensure it is set to the assigned compartment.

Subnet Type: Select Public Subnet.

CIDR Block: Enter 10.0.1.0/24.

Route Table: Select the default route table associated with the VCN (ensure it includes a route to the Internet Gateway with destination 0.0.0.0/0).

Subnet Access: Select Public Subnet and ensure the Internet Gateway is associated.

DHCP Options: Leave as default or customize if required.

Security List: Use the default security list or create a new one with appropriate ingress/egress rules (e.g., allow TCP port 22 for SSH and all egress traffic).

Associate the Internet Gateway:

Verify that the subnet is configured to route traffic through the Internet Gateway. This is automatically handled if you selected the public subnet option and the VCN's route table is correctly set (as configured in Task 3).

If needed, edit the route table for the subnet to ensure a rule exists:

Destination CIDR Block: 0.0.0.0/0

Target Type: Internet Gateway

Target: Select the Internet Gateway associated with IAD-SP-PBT-VCN-01.

Create the Subnet:

Click Create to provision the subnet.

Once created, the subnet will be listed under the VCN's subnets.

Verify the Configuration:

Go to the subnet details page for IAD-SP-PBT-PUBSNET-01.

Confirm the CIDR block is 10.0.1.0/24 and that it is a public subnet with Internet Gateway access.

Notes

Ensure the CIDR block 10.0.1.0/24 does not overlap with existing subnets in the VCN (10.0.0.0/16,

including 10.0.10.0/24 from Task 3).

The Internet Gateway association relies on the route table configuration from Task 3. If it's missing, update the route table as described in Step 6.

Question: 5

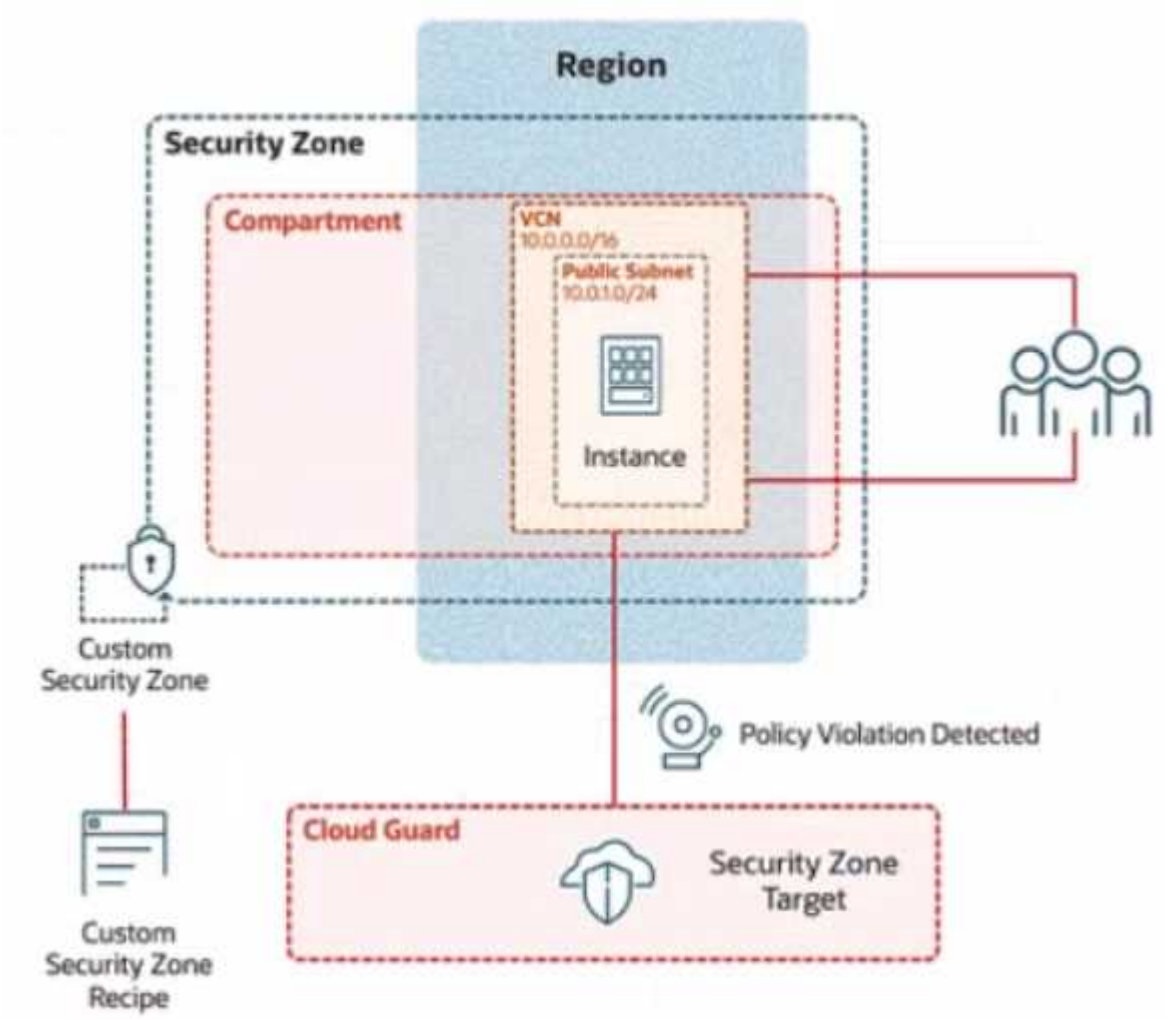
SIMULATION

Challenge 2

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

Task 5: Provision a Compute Instance

Provision a compute instance in the IAD-SP-PBT-PUBSNET-01 public subnet, where:

Name IAD-SP-PBT-1-VM-01

image: Oracle Linux 8

Shape VM: Standard, A1, Flex

Enter the OCID of the created compute instance in the text box below.

Answer: See the solution below in Explanation.

Explanation:

To provision a compute instance named IAD-SP-PBT-1-VM-01 in the IAD-SP-PBT-PUBSNET-01 public subnet with the specified configuration (Oracle Linux 8 image, VM Standard A1 Flex shape), follow these steps based on the Oracle Cloud Infrastructure (OCI) Compute documentation.

Step-by-Step Solution for Task 5: Provision a Compute Instance

Log in to the OCI Console:

Use your OCI credentials to log in to the OCI Console (https://console.us-ashburn-1.oraclecloud.com).

Ensure you have access to the assigned compartment.

Navigate to Compute Instances:

From the OCI Console, click the navigation menu (hamburger icon) on the top left.

Under Compute, select Instances.

Create a New Compute Instance:

Click the Create Instance button.

Configure the Instance Details:

Name: Enter IAD-SP-PBT-1-VM-01.

Compartment: Select the assigned compartment.

Placement: Choose the availability domain (e.g., AD-1) based on your region's availability.

Select the Image:

Under Image and Shape, click Change Image.

Select Oracle Linux 8 from the platform images list.

Click Select Image.

Choose the Shape:

Click Change Shape.

Select VM Standard category.

Choose A1 Flex from the shape options.

Configure the OCPUs (e.g., 1 OCPU) and memory (e.g., 6 GB) as needed for A1 Flex, then click Select Shape.

Configure Networking:

Under Networking, ensure the Virtual Cloud Network is set to IAD-SP-PBT-VCN-01.

Set the Subnet to IAD-SP-PBT-PUBSNET-01 (public subnet with CIDR 10.0.1.0/24).

Enable Assign a public IPv4 address to allow external connectivity.

Leave the default security list or assign a custom one if configured previously.

Set Up SSH Access:

Under Add SSH Keys, either:

Upload your public SSH key file, or

Paste your public SSH key manually.

This ensures you can access the instance via SSH.

Launch the Instance:

Click Create to provision the compute instance.

Wait for the instance to reach the Running state (this may take a few minutes).

Note the Instance OCID:

Once the instance is running, go to the instance details page for IAD-SP-PBT-1-VM-01.

Copy the OCID displayed (e.g., ocid1.instance.oc1..<unique_string>).

OCID of the Created Compute Instance

Enter the OCID of the created compute instance (IAD-SP-PBT-1-VM-01) into the text box. The exact OCID will be available after Step 9 (e.g., ocid1.instance.oc1..<unique_string>).

Notes

Ensure the security zone IAD_SAP-PBT-CSZ-01 and its associated recipe IAD-SP-PBT-CSP-01 allow

compute instance creation in the public subnet (10.0.1.0/24).

Verify network connectivity by testing SSH access using the public IP assigned to the instance.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Oracle

Code: 1Z0-1104-25

Exam: Oracle Cloud Infrastructure 2025 Security Professional

https://www.examsnest.com/exam/1z0-1104-25/

Use Coupon “**SAVE15**” for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation