Prepare Smart for Success Free Oracle 1Z0-1104-25 Exam Questions and Answers

Ready to pass faster? Grab free and updated Oracle Cloud Infrastructure 2025 Security Professional exam PDF questions now. Get authentic 1Z0-1104-25 dumps packed with verified answers and secure your certification success with PrepBolt 1Z0-1104-25 exam pdf questions and answers.

Thank you for Downloading 1Z0-1104-25 exam PDF Demo

https://prepbolt.com/1Z0-1104-25.html

Question 1

Question Type: MultipleChoice

In Oracle Cloud Infrastructure (OCI), bare metal instances provide customers with direct access to the underlying hardware. To mitigate security risks when a customer terminates a bare metal instance, OCI utilizes Root-of-Trust hardware.

What is the primary function of the Root-of-Trust hardware in this context?

Options:

A- It automatically encrypts data at rest on the bare metal instance.
B- It ensures all non-volatile memory on the terminated instance is securely wiped before reuse.
C- It guarantees complete isolation between customer workloads on different instances.
D- It eliminates the need for hypervisors, reducing the potential attack surface.

Answer:

B

Question 2

Question Type: MultipleChoice

"Your company is in the process of migrating its sensitive data to Oracle Cloud Infrastructure (OCI) and is prioritizing the strongest possible security measures. Encryption is a key part of this strategy, but you are particularly concerned about the physical security of the hardware where your encryption keys will be stored.

Which characteristic of OCI Key Management Service (KMS) helps ensure the physical security of your encryption keys?

Options:

A- Granular customer control over key access permissions
B- Centralized key management for simplified administration
C- Seamless integration with other OCI services for streamlined workflows
D- Utilization of FIPS 140-2 validated Hardware Security Modules (HSMs)'

Answer:

D

Question 3

Question Type: MultipleChoice

An OCI administrator notices that a compute instance running in the production compartment is unable to create Object Storage buckets using the OCI CLI command:

oci os bucket create --name mybucket --compartment-id --auth instance_principal

The error message returned states:

"NotAuthorizedOrNotFound: You are not authorized to perform this action."

The administrator verifies that the instance has Internet access and can reach OCI endpoints.

What then could be causing the issue?

Options:

A- The instance is using the wrong OCI CLI authentication method.
B- The bucket name is already in use, causing a conflict.
C- The policy is written at the root compartment instead of the production compartment.
D- The instance is not part of any Dynamic Group or the matching rule is incorrect.

Answer:

D

Question 4

Question Type: MultipleChoice

SIMULATION

Challenge 1 - Task 1

Integrate TLS Certificate Issued by the OCI Certificates Service with Load Balancer

You are a cloud engineer at a tech company that is migrating its services to Oracle Cloud Infrastructure (OCI). You are required to set up secure communication for your web application using

OCI's Certificate service. You need to create a Certificate Authority (CA), issue a TLS/SSL server certificate, and configure a load balancer to use this certificate to ensure encrypted traffic between clients and the backend servers.

Review the architecture diagram, which outlines the resources 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

OCI Vault to store the secret required by the program, which is created in the root compartment as PBI_Vault_SP

Task 1: Create and Configure a Virtual Cloud Network (VCN)

Create a Virtual Cloud Network (VCN) named PBT-CERT-VCN-01 with the following specifications:

VCN with a CIDR block of 10.0.0.0/16

Subnet 1 (Compute Instance):

Name: Compute-Subnet-PBT-CERT

CIDR Block: 10.0.1.0/24

Subnet 2 (Load Balancer):

Name: LB-Subnet-PBT-CERT-SNET-02

CIDR Block: 10.0.2.0/24

Internet Gateway for external connectivity

Route table and security lists:

Security List named PBT-CERT-CS-SL-01 for Subnet 1 (Compute-Subnet-PBT-CERT) to allow SSH (port 22) traffic

Security List named PBT-CERT-LB-SL-01 for Subnet 2 (LB-Subnet-PBT-CERT) to allow HTTPS (port 443) traffic

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

Options:

A- See the solution below in Explanation

Answer:

A

Explanation:

Challenge 1: Integrate TLS Certificate Issued by the OCI Certificates Service with Load Balancer

Task 1: Create and Configure a Virtual Cloud Network (VCN)

Step 1: Create the Virtual Cloud Network (VCN)

Log in to the OCI Console.

Navigate to Networking > Virtual Cloud Networks.

Click Create Virtual Cloud Network.

Select VCN with Internet Connectivity (to include an Internet Gateway by default).

Enter the following details:

Name: PBT-CERT-VCN-01

Compartment: Select your assigned compartment.

VCN CIDR Block: 10.0.0.0/16

Leave other settings as default (e.g., create a new public subnet and route table).

Click Create Virtual Cloud Network. Wait for the VCN to be created.

Step 2: Create Subnet 1 (Compute-Subnet-PBT-CERT)

In the VCN details page for PBT-CERT-VCN-01, click Subnets under Resources.

Click Create Subnet.

Enter the following details:

Name: Compute-Subnet-PBT-CERT

Subnet Type: Regional

CIDR Block: 10.0.1.0/24

Route Table: Select the default route table created with the VCN.

Subnet Access: Public Subnet (to allow internet access).

DNS Resolution: Enabled.

Click Create.

Step 3: Create Subnet 2 (LB-Subnet-PBT-CERT-SNET-02)

In the VCN details page, click Subnets under Resources.

Click Create Subnet.

Enter the following details:

Name: LB-Subnet-PBT-CERT-SNET-02

Subnet Type: Regional

CIDR Block: 10.0.2.0/24

Route Table: Select the default route table created with the VCN.

Subnet Access: Public Subnet (to allow internet access for the load balancer).

DNS Resolution: Enabled.

Click Create.

Step 4: Verify Internet Gateway

In the VCN details page, under Resources, click Internet Gateways.

Ensure an Internet Gateway is listed and attached to PBT-CERT-VCN-01. If not created, click Create Internet Gateway, name it (e.g., PBT-CERT-IGW), and attach it.

Step 5: Configure Route Table

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

Select the default route table or create a new one named PBT-CERT-RT-01.

Click Add Route Rule. 4 - Destination CIDR Block: 0.0.0.0/0

Target Type: Internet Gateway

Target: Select the Internet Gateway created (e.g., PBT-CERT-IGW).

Click Add Route Rule and save.

Step 6: Create Security List for Subnet 1 (Compute-Subnet-PBT-CERT)

In the VCN details page, under Resources, click Security Lists.

Click Create Security List.

Enter the following:

Name: PBT-CERT-CS-SL-01

Compartment: Your assigned compartment.

Add the following ingress rule:

Source CIDR: 0.0.0.0/0 (allow from any source, adjust as per security needs)

IP Protocol: TCP

Source Port Range: All

Destination Port Range: 22 (for SSH)

Allows: Traffic

Click Create.

Step 7: Create Security List for Subnet 2 (LB-Subnet-PBT-CERT-SNET-02)

In the VCN details page, under Resources, click Security Lists.

Click Create Security List.

Enter the following:

Name: PBT-CERT-LB-SL-01

Compartment: Your assigned compartment.

Add the following ingress rule:

Source CIDR: 0.0.0.0/0 (allow from any source, adjust as per security needs)

IP Protocol: TCP

Source Port Range: All

Destination Port Range: 443 (for HTTPS)

Allows: Traffic

Click Create.

Step 8: Retrieve and Enter VCN OCID

Go to the VCN details page for PBT-CERT-VCN-01.

Copy the OCID from the VCN information section.

Enter the OCID in the provided text box.

Question 5

Question Type: MultipleChoice

"You are part of the security operations of an organization with thousands of users accessing Oracle Cloud Infrastructure (OCI). It is reported that an unknown user action was executed resulting in configuration errors. You are tasked with identifying the details of all users who were active in the last

six hours along with any REST API calls that were executed.

Which OCI feature should you use?

Options:

A- Audit Analysis Dashboard
B- Management Agent Log Ingestion
C- Object Collection Rule
D- Service Connector Hub'

Answer:

A

Question 6

Question Type: MultipleChoice

SIMULATION

Task 7: Verify the OCI Certificate with Load Balancer

Verify HTTPS connection to the load balancer by running the following command in Cloud Shell

curl -k https://

Enter the following URL in the web browser:

https://

If prompted with a certificate error, accept the risk and continue.

Verify web page content by ensuring the text, "You are visiting Web Server 1" from the index.html file is displayed in the browser

Options:

A- See the solution below in Explanation

Answer:

A

Explanation:

Task 7: Verify the OCI Certificate with Load Balancer

Step 1: Obtain the Public IP of the Load Balancer

Log in to the OCI Console.

Navigate to Networking > Load Balancers.

Click on PBT-CERT-LB-01.

Note the Public IP Address from the load balancer details page.

Step 2: Verify HTTPS Connection Using Cloud Shell

Open the OCI Cloud Shell from the top-right corner of the OCI Console.

Run the following command, replacing <Public IP of PBT-CERT-LB-01> with the public IP you noted:

curl -k https://<Public IP of PBT-CERT-LB-01>

Expected output: You should see the text 'You are visiting Web Server 1' if the connection is successful. The -k flag ignores certificate validation errors (common during initial testing with self-signed or newly issued certificates).

If you encounter an error, ensure the load balancer is active, the listener is configured correctly, and the backend server (PBT-CERT-VM-01) is reachable.

Step 3: Verify in a Web Browser

Open a web browser.

Enter the following URL, replacing <Public IP of PBT-CERT-LB-01> with the public IP you noted:

https://<Public IP of PBT-CERT-LB-01>

If prompted with a certificate warning (e.g., due to a self-signed certificate or untrusted CA), accept the risk and proceed (click 'Advanced' and 'Proceed' or similar, depending on your browser).

Verify that the web page displays the text 'You are visiting Web Server 1' from the index.html file created on PBT-CERT-VM-01.

Step 4: Troubleshoot (if needed)

If the text is not displayed:

Check the load balancer health status under Backend Sets > Health in the OCI Console.

Ensure the security list PBT-CERT-LB-SL-01 allows port 443 and the compute instance security list allows port 80.

Verify the Apache service is running on PBT-CERT-VM-01 by SSHing in and running sudo systemctl status httpd.

Topic 2, Misc. Questions

Thank You for trying 1Z0-1104-25 PDF Demo

To try our 1Z0-1104-25 practice exam software visit link below

https://prepbolt.com/1Z0-1104-25.html

Start Your 1Z0-1104-25 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your 1Z0-1104-25 preparation with actual exam questions.