Oracle 1Z0-1072-25 Practice Questions

Shared by Graves on 10-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How would you allow access to FSS for a DB System with read-only permissions?

Options:

A- Create an NFS export option that allows READ_ONLY access.
B- Modify the security list to allow stateful ingress rules.
C- Modify the security list to allow stateless ingress rules.
D- Create an instance principal for the DB System.

Answer:

A

Explanation:

To allow access to Oracle Cloud Infrastructure (OCI) File Storage Service (FSS) for a Database (DB) System with read-only permissions, you should create an NFS export option that specifies READ_ONLY access.

NFS Export Options: These options define the access permissions (read/write or read-only) for clients connecting to the file system. By setting the export option to READ_ONLY, you ensure that the DB System can only read from the FSS and cannot modify or delete files.

Oracle Cloud Infrastructure Documentation: File Storage Service Export Options

Question 2

Question Type: MultipleChoice

Which statement accurately describes the key features and benefits of OCI Confidential Computing?

Options:

A- It optimizes network performance through advanced routing algorithms.

B- It provides automatic scalability and load balancing capabilities.
C- It encrypts and isolates in-use data and the applications processing that data.
D- It enables users to securely store and retrieve data by using distributed file systems.

Answer:

C

Explanation:

OCI Confidential Computing is a security feature designed to protect data in use. This is particularly important for sensitive workloads where data must be secured not only when at rest or in transit but also while being processed.

Encrypts and Isolates In-Use Data: OCI Confidential Computing ensures that data and the applications processing it are isolated from the underlying infrastructure. This means that even if the infrastructure is compromised, the in-use data remains secure. The technology typically leverages secure enclaves or other hardware-based isolation mechanisms to achieve this.

Other Options:

Optimizing Network Performance (A), Automatic Scalability and Load Balancing (B), and Secure Data Storage (D) are important features, but they are not related to the core capabilities of Confidential Computing, which focuses on in-use data protection.

Relevant OCI Documentation:

OCI Confidential Computing Overview

This documentation provides a detailed explanation of how OCI Confidential Computing works and its benefits for securing sensitive data during processing.

Question 3

Question Type: MultipleChoice

Why was SSH still possible after port 22 was removed from the Security Lists?

Options:

A- The VCN where that compute instance resides still has an Internet Gateway.
B- The VNIC of that compute instance is attached to a Cluster Network.
C- The VCN where that compute instance resides still has a route rule.
D- The VNIC of that compute instance is attached to a Network Security Group (NSG).

Answer:

D

Explanation:

Even after removing port 22 from the Security Lists, SSH was still possible because the Virtual Network Interface Card (VNIC) of the compute instance is attached to a Network Security Group (NSG).

NSGs: NSGs provide a more flexible and granular way to manage security rules compared to Security Lists. They allow you to apply security rules directly to VNICs associated with resources such as compute instances. If an NSG allows traffic on port 22, SSH will still be possible, regardless of the Security List settings.

Oracle Cloud Infrastructure Documentation: Security Lists and Network Security Groups

Question 4

Question Type: MultipleChoice

Which components are required for establishing remote peering between two Virtual Cloud Networks (VCNs) in Oracle Cloud Infrastructure (OCI)?

Options:

A- A single VCN with nonoverlapping CIDRS in each region, a dynamic routing gateway (DRG) attached to each VCN, and a direct connection between the DRGS.
B- Two VCNs with overlapping CIDRS in different regions, a virtual private network (VPN) gateway attached to each VCN, and a direct connection between the VPN gateways.
C- Two VCNs with nonoverlapping CIDRS in the same region, a dynamic routing gateway (DRG) attached to each VCN, and a direct connection between the DRGs.
D- Two VCNs with nonoverlapping CIDRS in different regions, a dynamic routing gateway (DRG) attached to each VCN, a remote peering connection (RPC) on each DRG, and a connection established between the RPCs.

Answer:

D

Explanation:

Remote peering in Oracle Cloud Infrastructure allows two VCNs in different regions to communicate securely. To establish remote peering, the following components are required:

Two VCNs with Nonoverlapping CIDRs:

The CIDR blocks of the two VCNs must not overlap. This is crucial to avoid routing conflicts and ensure that traffic is correctly routed between the VCNs.

Dynamic Routing Gateway (DRG) Attached to Each VCN:

A DRG is a virtual router that provides a path for traffic between the VCN and networks outside the VCN, such as other VCNs via remote peering, on-premises networks, or other cloud services. Each VCN needs its own DRG.

Remote Peering Connection (RPC):

An RPC is a specialized connection on the DRG used specifically for remote peering. You need to create an RPC on each DRG associated with the VCNs you wish to peer.

Connection Between RPCs:

Finally, a connection must be established between the RPCs of the two DRGs. This connection facilitates the secure and private exchange of traffic between the VCNs over Oracle's backbone network.

Incorrect Options:

Option A involves a single VCN, which does not fulfill the requirement of remote peering between two VCNs.

Option B involves overlapping CIDRs and VPN gateways, which are incorrect for remote peering.

Option C suggests peering within the same region, which would be considered local peering rather than remote peering.

Relevant OCI Documentation:

OCI Remote VCN Peering

Dynamic Routing Gateway (DRG) Overview

These resources provide a detailed guide on configuring remote peering in OCI, ensuring secure and effective communication between VCNs across regions.

Question 5

Question Type: MultipleChoice

What are the two types of capture filters that can be created for network monitoring?

Options:

A- Flow control capture filters and traffic capture filters
B- Flow log capture filters and packet capture filters
C- VTAP capture filters and network capture filters
D- Flow log capture filters and VTAP capture filters

Answer:

D

Explanation:

In Oracle Cloud Infrastructure (OCI), there are two primary types of capture filters used for network monitoring:

Flow Log Capture Filters: These filters are used to capture and log network flow information (e.g., source and destination IP addresses, ports, protocols). Flow logs provide insights into the traffic patterns within your VCN.

VTAP Capture Filters: Virtual Test Access Point (VTAP) capture filters allow you to capture and inspect traffic from specific network interfaces or subnets without affecting the flow of traffic. This is particularly useful for deep packet inspection and monitoring purposes.

Oracle Cloud Infrastructure Documentation: Flow Logs

Oracle Cloud Infrastructure Documentation: VTAP

Question 6

Question Type: MultipleChoice

Which statement accurately describes ephemeral principals?

Options:

A- Ephemeral principals are temporary credentials granted to resources.
B- Ephemeral principals are another term for dynamic groups.
C- Ephemeral principals are user accounts with limited lifespans.
D- Ephemeral principals represent long-lived service accounts.

Answer:

A

Explanation:

Ephemeral principals in Oracle Cloud Infrastructure (OCI) refer to temporary security credentials granted to resources, such as compute instances, to enable them to interact with OCI services securely. These credentials have a limited lifespan and are typically used in situations where resources need to authenticate temporarily without the need for long-lived credentials.

Use Case: Ephemeral principals are often used for instance principals, allowing compute instances to make API calls without the need to manage long-term keys or credentials.

Oracle Cloud Infrastructure Documentation: Using Instance Principals

Question 7

Question Type: MultipleChoice

Which statement is NOT true about the Oracle Cloud Infrastructure (OCI) Object Storage service?

Options:

A- Immutable option for data stored in Object Storage can be set via retention rules.
B- Object Storage resources can be shared across tenancies.
C- Object lifecycle rules can be used to archive or delete objects.
D- Object Versioning is enabled at the namespace level.

Answer:

B

Explanation:

Oracle Cloud Infrastructure (OCI) Object Storage is a scalable, highly durable service that allows you to store any type of data in a secure and cost-effective manner. The correct and incorrect statements regarding OCI Object Storage are as follows:

A . Immutable Option: You can indeed set an immutable option for data in Object Storage using retention rules. This feature ensures that once data is written, it cannot be modified or deleted until the retention period expires, making it ideal for regulatory compliance.

C . Object Lifecycle Rules: Object lifecycle policies allow you to automate the archiving or deletion of objects based on their age or other criteria, helping manage storage costs and data retention efficiently.

D . Object Versioning: Versioning is enabled at the bucket level, not the namespace level. However, once enabled for a bucket, it helps retain, retrieve, and restore every version of every object stored in that bucket.

B . Object Storage Sharing Across Tenancies: This statement is not true. OCI Object Storage buckets and objects are specific to a tenancy and cannot be shared across different tenancies directly. Access to Object Storage resources is controlled within a single tenancy through IAM policies.

Relevant OCI Documentation:

OCI Object Storage Overview

Object Lifecycle Management

These references provide details on how Object Storage functions and the features available.

Question 8

Question Type: MultipleChoice

How would you allow access to FSS for a DB System with read-only permissions?

Options:

A- Create an NFS export option that allows READ_ONLY access.
B- Modify the security list to allow stateful ingress rules.
C- Modify the security list to allow stateless ingress rules.
D- Create an instance principal for the DB System.

Answer:

A

Explanation:

To allow access to Oracle Cloud Infrastructure (OCI) File Storage Service (FSS) for a Database (DB) System with read-only permissions, you should create an NFS export option that specifies READ_ONLY access.

NFS Export Options: These options define the access permissions (read/write or read-only) for clients connecting to the file system. By setting the export option to READ_ONLY, you ensure that the DB System can only read from the FSS and cannot modify or delete files.

Oracle Cloud Infrastructure Documentation: File Storage Service Export Options

Question 9

Question Type: MultipleChoice

You can attach resources to a Dynamic Routing Gateway (DRG). Choose THREE of these resources.

Options:

A- Virtual Circuits
B- Subnet
C- VNIC
D- Remote Peering Connections
E- IPSec Tunnel
F- Local Peering Connection

Answer:

A, D, E

Explanation:

A Dynamic Routing Gateway (DRG) in Oracle Cloud Infrastructure (OCI) is a virtual router that provides a path for private traffic between your on-premises network and your VCN, or between your VCN and other VCNs. The resources that can be attached to a DRG include:

A . Virtual Circuits: Used to establish a private connection between your on-premises data center and your VCN via Oracle's FastConnect service.

D . Remote Peering Connections: Enables peering between VCNs located in different regions (Remote VCN Peering).

E . IPSec Tunnel: Facilitates secure VPN connections between your on-premises network and your OCI VCN.

Oracle Cloud Infrastructure Documentation: Dynamic Routing Gateway Overview

Question 10

Question Type: MultipleChoice

What would happen if you Select not to proactively reboot the instance before the scheduled maintenance due date?

Options:

A- You will receive another notification to reboot within the next 14 days.
B- The instance will get terminated.
C- The instance is either reboot-migrated or rebuilt in place for you.
D- You will receive another notification to reboot within the next 7 days.

Answer:

C

Explanation:

In OCI, if you choose not to proactively reboot your instance before the scheduled maintenance due date, the system will handle the maintenance automatically to ensure that the instance remains operational.

Reboot-Migration or Rebuild in Place: If you don't reboot the instance yourself, OCI will automatically perform a reboot-migration or rebuild in place for the instance. This ensures that the instance is moved to new hardware or updated without your intervention, maintaining uptime and applying necessary updates or fixes.

Impact on Instance: The exact action taken (reboot-migration or rebuild in place) depends on the type of maintenance required. However, either action will temporarily interrupt the instance, typically involving a reboot, but the instance's data and configuration will be

preserved.

Relevant OCI Documentation:

Instance Maintenance

OCI Maintenance Events

These references discuss the procedures and options available for handling instance maintenance in OCI.

Question 11

Question Type: MultipleChoice

Which TWO statements about the Oracle Cloud Infrastructure (OCI) File Storage Service are accurate?

Options:

A- Communication with file systems in a mount target is encrypted via HTTPS.
B- Customers can encrypt data in their file system using their own Vault encryption key.
C- Customers can encrypt the communication to a mount target via export options.
D- File systems use Oracle-managed keys by default.

Answer:

B, D

Explanation:

Oracle Cloud Infrastructure (OCI) File Storage Service offers robust encryption capabilities to ensure data security.

B . Customer-Managed Encryption: Customers can choose to encrypt their data using their own keys stored in the OCI Vault service. This gives customers control over their encryption keys and enhances data security.

D . Oracle-Managed Encryption: By default, all data stored in OCI File Storage is encrypted using Oracle-managed keys. This ensures that data is encrypted at rest without requiring any action from the customer.

Incorrect Statements:

A . Communication is not encrypted via HTTPS when accessing file systems; instead, encryption in transit is typically managed via NFS over TLS.

C . Encryption of communication to a mount target is handled via network configurations, not through export options.

Oracle Cloud Infrastructure Documentation: File Storage Encryption

To Get Premium Files for 1Z0-1072-25 Visit

https://www.p2pexams.com/products/1z0-1072-25

For More Free Questions Visit

https://www.p2pexams.com/oracle/pdf/1z0-1072-25

