Download Oracle 1Z0-1124-25 Exam Dumps Free

Shared by Landry on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When migrating workloads requiring high availability and redundancy for on-premises connectivity to OCI, which approach is recommended?

Options:

A- Single FastConnect connection
B- Site-to-Site VPN over a single internet connection
C- Dual FastConnect connections with diverse paths
D- Internet Gateway with multiple public IPs

Answer:

C

Explanation:

Requirements: HA and redundancy for on-premises-to-OCI connectivity.

Option A: Single FastConnect lacks redundancy---incorrect.

Option B: Single VPN over internet has no redundancy and poor performance---incorrect.

Option C: Dual FastConnect with diverse paths ensures HA and redundancy via separate routes---correct.

Option D: Internet Gateway with public IPs isn't dedicated or redundant---incorrect.

Conclusion: Option C is the recommended approach.

Oracle advises:

'For high availability, use dual FastConnect connections with diverse paths to eliminate single points of failure in hybrid connectivity.'

This supports Option C. Reference: FastConnect High Availability - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/fastconnect.htm#ha).

Question 2

Question Type: MultipleChoice

Your security policy mandates that all communication between your compute instances in a private subnet and OCI Object Storage must be authenticated and authorized using IAM policies and not rely on public IP addresses. Which OCI networking feature is the most appropriate to satisfy this requirement?

Options:

A- Public Subnet with an Internet Gateway and IAM rules.
B- Private Subnet with a NAT Gateway and IAM rules.
C- Private Subnet with a Service Gateway and IAM rules.
D- Public Subnet with a Network Firewall and IAM rules.

Answer:

C

Explanation:

Requirement: Private, IAM-secured access to Object Storage.

Option A: Public subnet with Internet Gateway uses public IPs---violates policy.

Option B: NAT Gateway is for internet access, not private OCI services---incorrect.

Option C: Service Gateway enables private access to Object Storage, paired with IAM for auth---correct.

Option D: Public subnet with firewall still relies on public IPs---incorrect.

Conclusion: Option C meets all requirements.

Oracle states:

'Use a Service Gateway for private access to OCI Object Storage from a private subnet, with IAM policies for authentication and authorization.'

This supports Option C. Reference: Service Gateway Overview - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/servicegateway.htm).

Question 3

Question Type: MultipleChoice

You are designing a hybrid cloud solution where sensitive data must be transferred between your on-premises data center and an OCI VCN. You require a dedicated, private connection with guaranteed bandwidth and low latency. In addition to FastConnect, what additional product would you implement to achieve encryption of the traffic traversing the FastConnect link and to ensure data confidentiality?

Options:

A- IPSec VPN
B- Oracle Cloud Infrastructure Vault
C- MACsec
D- OCI Bastion

Answer:

C

Explanation:

Requirement Analysis: The solution needs a private, high-bandwidth, low-latency connection (provided by FastConnect) with encryption for data confidentiality.

Option A (IPSec VPN): IPSec encrypts traffic at Layer 3 over public or private networks. While feasible over FastConnect, it's redundant since FastConnect is already private, adding unnecessary overhead and complexity.

Option B (OCI Vault): Vault manages encryption keys and secrets but doesn't encrypt traffic itself---only supports application-level encryption, not link-level---incorrect.

Option C (MACsec): MACsec (Media Access Control Security) provides Layer 2 encryption for Ethernet traffic, ideal for securing FastConnect's dedicated link directly between devices, ensuring confidentiality without higher-layer overhead---correct.

Option D (OCI Bastion): Bastion secures remote access to VCN resources, not link encryption---incorrect.

Conclusion: MACsec enhances FastConnect with efficient, link-level encryption, meeting all requirements.

Oracle documentation states:

'MACsec provides Layer 2 encryption for FastConnect, securing Ethernet traffic between on-premises and OCI infrastructure. It's ideal for ensuring confidentiality over dedicated connections.'

This supports Option C as the best additional product. Reference: FastConnect Security Options - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/fastconnect.htm#security).

Question 4

Question Type: MultipleChoice

You are configuring a VCN with multiple subnets for a customer. The security team requires that all instances have IPv6 addresses. You configure the VCN with an IPv6 ULA CIDR block of fc00:1:1::/48 and create two private subnets. After launching instances in the two private subnets, you notice that they only have IPv4 addresses assigned. You have not manually configured any IPv6 addresses on the instances themselves. What steps are necessary to ensure the instances automatically receive IPv6 addresses?

Options:

A- No further steps are needed. Instances will automatically receive IPv6 addresses within the configured subnets upon launch.
B- Ensure that SLAAC (Stateless Address Autoconfiguration) is enabled on the operating system of the instances within the two subnets.
C- IPv6 address assignment is only supported on instances launched in public subnets.
D- Make sure the 'Assign public IPv4 address' option is not selected during instance creation. This will force the instance to default to IPv6 allocation.

Answer:

B

Explanation:

Problem: Instances lack IPv6 addresses despite VCN IPv6 configuration.

OCI IPv6 Behavior: IPv6 requires subnet enablement and OS support via SLAAC.

Evaluate Options:

A: Incorrect. OCI doesn't auto-assign IPv6 without OS configuration.

B: Correct. SLAAC must be enabled on the instance OS for auto-assignment.

C: Incorrect. IPv6 works in both public and private subnets.

D: Incorrect. IPv4 and IPv6 assignments are independent.

Conclusion: Enabling SLAAC on the OS ensures automatic IPv6 assignment.

IPv6 in OCI relies on SLAAC for automatic address assignment. The Oracle Networking Professional study guide states, 'To enable IPv6 on instances, the VCN and subnet must have IPv6 CIDR blocks, and the instance OS must support SLAAC to automatically configure IPv6 addresses' (OCI Networking Documentation, Section: IPv6 Configuration). Without SLAAC, instances default to IPv4 only.

Question 5

Question Type: MultipleChoice

Your company is setting up a FastConnect connection with a provider. You have purchased a port from the provider, and they are requesting information to set up the connection to Oracle Cloud Infrastructure. They specifically require information to configure the VLANs. What information regarding VLAN configuration is ESSENTIAL for them to successfully establish the FastConnect circuit?

Options:

A- The list of all VCN CIDR blocks and their associated tags.
B- A single unused VLAN ID, your BGP ASN, and the BGP peering IP addresses you want to use.
C- The MTU (Maximum Transmission Unit) size for all VNICs in your OCI tenancy.
D- Your Oracle Cloud Identifier (OCID) and compartment ID.

Answer:

B

Explanation:

Requirement: Provide VLAN config info for FastConnect setup.

Option A: CIDR blocks are for routing, not VLAN setup---incorrect.

Option B: VLAN ID defines the circuit, BGP ASN and peering IPs establish routing---essential and correct.

Option C: MTU is a performance setting, not required for VLAN config---incorrect.

Option D: OCID and compartment ID are for OCI management, not provider setup---incorrect.

Conclusion: Option B provides the necessary VLAN configuration details.

Oracle states:

'For FastConnect, provide the provider with a VLAN ID, your BGP ASN, and BGP peering IPs to configure the virtual circuit.'

This confirms Option B. Reference: FastConnect Configuration - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/fastconnect.htm#providerconfig).

Question 6

Question Type: MultipleChoice

You are designing a multicloud architecture where your customer wants to leverage OCI for its cost-effective compute and storage, while utilizing Microsoft Azure's AI/ML services and AWS's extensive serverless capabilities. The application requires low latency and high bandwidth between the clouds. Which of the following approaches provides the LEAST optimal solution for interconnecting these three cloud providers for production workloads?

Options:

A- Establishing a dedicated, low-latency connection between each cloud provider's nearest peering location using a third-party network provider for maximum bandwidth and minimizing network hops
B- Creating IPSec VPN tunnels between OCI, Azure, and AWS, utilizing the native VPN gateways offered by each respective cloud provider for secure, encrypted communication
C- Utilizing OCI FastConnect to establish private peering with Azure and AWS through supported FastConnect partners to ensure dedicated bandwidth and consistent performance
D- Connecting OCI to Azure via OCI Azure Interconnect, then establishing an IPSec VPN tunnel from Azure to AWS using Azure's VPN Gateway

Answer:

B

Explanation:

Requirements: Low latency, high bandwidth for multicloud production.

Option A: Dedicated peering via third-party provider offers high performance---optimal.

Option B: IPSec VPNs over public internet have variable latency and limited bandwidth---least optimal.

Option C: FastConnect peering with partners ensures dedicated performance---optimal.

Option D: OCI-Azure Interconnect is fast, but VPN to AWS adds latency---less optimal than A or C but better than B.

Conclusion: Option B is the least optimal due to performance constraints.

Oracle notes:

'IPSec VPNs over public internet provide security but lack the bandwidth and latency consistency of dedicated connections like FastConnect for production workloads.''

This supports Option B as least optimal. Reference: Multicloud Connectivity Options - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Concepts/multicloud.htm#options).

Question 7

Question Type: MultipleChoice

Your company has a FastConnect circuit established between your on-premises data center and OCI. However, you have a specific regulatory requirement to encrypt all traffic, even over dedicated connections like FastConnect. You need to implement IPSec encryption without significantly impacting the available bandwidth of your FastConnect circuit. Which is the most effective approach to implement IPSec encryption over your existing FastConnect circuit, while maintaining high bandwidth?

Options:

A- Configure a Site-to-Site VPN using the OCI Dynamic Routing Gateway (DRG) over the FastConnect virtual circuit. Use a low-overhead encryption algorithm like AES-GCM.
B- Deploy virtual firewall appliances within OCI and your on-premises network and configure IPSec tunnels between them, routing all traffic through the firewalls. Use a high-security encryption algorithm like AES-256.
C- Terminate IPSec VPN on compute instances in a public subnet on the OCI side.
D- Establish a second, separate Site-to-Site VPN connection to OCI over the public internet, and route all sensitive traffic over this VPN, while routing non-sensitive traffic over the FastConnect circuit.

Answer:

A

Explanation:

Requirements: Encrypt FastConnect traffic with minimal bandwidth impact.

IPSec Options:

DRG VPN: Native OCI solution over FastConnect.

Firewall Appliances: Adds overhead and complexity.

Compute Instances: Resource-intensive, not scalable.

Internet VPN: Uses public internet, against requirements.

Evaluate Options:

A: DRG VPN with AES-GCM (low-overhead encryption) leverages FastConnect; optimal.

B: Firewalls with AES-256 add overhead, reducing bandwidth; less effective.

C: Compute-based VPN is inefficient and public-facing; unsuitable.

D: Public internet VPN violates privacy requirement; incorrect.

Conclusion: DRG VPN with AES-GCM is the most effective solution.

OCI supports IPSec over FastConnect via DRG. The Oracle Networking Professional study guide explains, 'A Site-to-Site VPN over FastConnect using the DRG provides encrypted traffic with low-overhead algorithms like AES-GCM, maintaining high bandwidth' (OCI Networking Documentation, Section: FastConnect with VPN). This meets regulatory and performance needs efficiently.

Question 8

Question Type: MultipleChoice

You are configuring a FastConnect connection between your on-premises network and OCI. You need to establish a BGP (Border Gateway Protocol) session to exchange routing information. You want to use private peering to securely connect to your private resources within OCI. What are the MINIMUM requirements for configuring BGP for private peering over FastConnect?

Options:

A- A public AS number and a valid ASN for the OCI side.
B- A private AS number for the on-premises side and a valid ASN for the OCI side.
C- A public IP address range for BGP peering on the on-premises side and OCI side and an established DRG.
D- A valid ASN for the on-premises side and the OCI side and a non-overlapping IP address range for BGP peering on both the on-premises and OCI side.

Answer:

D

Explanation:

Goal: Minimum BGP setup for private FastConnect peering.

Option A: Public ASN isn't required; private ASNs work---incorrect.

Option B: Private ASN is allowed, but doesn't specify IPs---insufficient.

Option C: Public IPs aren't needed for private peering---incorrect.

Option D: Valid ASNs (public or private) and non-overlapping private IPs are the minimum for BGP---correct.

Conclusion: Option D meets the requirements.

Oracle notes:

'For BGP over FastConnect private peering, provide a valid ASN (public or private) and a non-overlapping IP range for peering.'

This confirms Option D. Reference: FastConnect BGP Configuration - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/fastconnect.htm#BGP).

Question 9

Question Type: MultipleChoice

You are troubleshooting a network connectivity issue between a compute instance in a private subnet within your VCN and a service on the public internet using Cloud Shell. You suspect a problem with the network security group (NSG) rules associated with the instance's VNIC. Which Cloud Shell command and appropriate tool combination allows you to directly inspect the NSG configuration impacting the VNIC?

Options:

A- oci network network-security-group get --nsg-id <NSG_OCID> piped to grep <instance_VNIC_OCID>
B- oci compute instance get --instance-id <instance_OCID> piped to jq '.vnics[].nic_id | oci network vnic get --vnic-id .' piped to jq '.network_security_group_ids[] | oci network network-security-group get --nsg-id .'
C- oci compute instance get --instance-id <instance_OCID> piped to grep NetworkSecurityGroupIds
D- oci network vnic get --vnic-id <instance_VNIC_OCID> piped to awk '/network_security_group_ids/ {print $2}' | xargs oci network network-security-group get --nsg-id

Answer:

B

Explanation:

Goal: Inspect NSG rules for a VNIC from Cloud Shell.

Command Flow:

Get instance Extract VNIC List NSGs Get NSG details.

Evaluate Options:

A: Direct NSG fetch lacks VNIC linkage; incomplete.

B: Full pipeline from instance to NSG details; precise and correct.

C: Grep is too basic, misses structure; incorrect.

D: Awk parsing is fragile, less reliable than jq; less optimal.

Conclusion: Option B provides the most robust inspection.

CLI with jq ensures accurate NSG retrieval. The Oracle Networking Professional study guide notes, 'To troubleshoot NSG rules, use the OCI CLI to fetch instance VNIC details and associated NSG configurations, piping through jq for structured output' (OCI Networking Documentation, Section: CLI Troubleshooting). Option B follows this methodology.

Question 10

Question Type: MultipleChoice

Your organization is migrating a critical three-tier application to OCI. The application requires a highly available and performant database tier. You plan to use Oracle Autonomous Database on Dedicated Exadata Infrastructure. The Autonomous Database subnet must adhere to the organization's security policy, which mandates no direct internet access and private access to other VCN subnets. You need to ensure the proper IP address allocation and routing. Which option best procedural steps is most effective for achieving this?

Options:

A- Create a public subnet for the Autonomous Database and configure a Service Gateway with access to all Oracle Services in OCI. Configure NSG rules allowing only traffic from the application's compute instances.
B- Create a private subnet for the Autonomous Database and configure a Service Gateway with access to only Object Storage and Yum Server Oracle Services in OCI. Configure NSG rules allowing only traffic from the application's compute instances, and configure routing to a Dynamic Routing Gateway (DRG) for access to other VCN subnets.
C- Create a private subnet for the Autonomous Database and configure a Service Gateway with access to Autonomous Database Oracle Services in OCI. Configure NSG rules allowing only traffic from the application's compute instances, and configure routing to a Dynamic Routing Gateway (DRG) for access to other VCN subnets. Reserve a large CIDR block for future database expansion.
D- Create a public subnet for the Autonomous Database, assign it a public IP address, and configure a Service Gateway with access to all Oracle Services in OCI. Configure routing to an Internet Gateway. Secure access using Security Lists allowing traffic only from approved IP ranges.

Answer:

C

Explanation:

Requirements: Private subnet, no internet, access to other VCN subnets, HA database.

Analyze Components:

Public Subnet: Internet-exposed, against policy.

Private Subnet: No internet, aligns with policy.

Service Gateway: For OCI services, not ADB connectivity.

DRG: For inter-VCN routing.

NSGs: Granular traffic control.

Evaluate Options:

A: Public subnet violates no-internet policy; incorrect.

B: Service Gateway for Object Storage/Yum irrelevant to ADB; incomplete.

C: Private subnet, NSGs, DRG, and CIDR planning meet all needs; correct.

D: Public subnet with internet access; violates policy.

Conclusion: Option C is the most effective approach.

Autonomous Database requires private deployment for security. The Oracle Networking Professional study guide notes, 'For Autonomous Database on Dedicated Exadata, use a private subnet with NSGs for access control and a DRG for inter-VCN connectivity, reserving CIDR for scalability' (OCI Networking Documentation, Section: Autonomous Database Networking). Service Gateway isn't used for ADB access, but the private setup ensures compliance.