Oracle 1Z0-1124-25 Practice Questions

Shared by Baldwin on 10-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are designing a microservices-based application on OCI. Each microservice is deployed as a container in Oracle Container Engine for Kubernetes (OKE). You want to expose these microservices through a single entry point using a Layer 7 load balancer and route traffic based on the request path. Which OCI load balancing integration method with OKE is the MOST appropriate and efficient?

Options:

A- Manually create a Regional Load Balancer and configure backend sets with the private IP addresses of the Kubernetes worker nodes hosting the microservices.
B- Deploy a Kubernetes LoadBalancer service, which automatically provisions an OCI Regional Load Balancer to distribute traffic to the microservice pods.
C- Deploy a Kubernetes NodePort service for each microservice and configure an OCI Network Load Balancer to forward traffic to the NodePort services on the worker nodes.
D- Deploy a Kubernetes Ingress controller that leverages an OCI Regional Load Balancer to route traffic to the microservice pods based on Ingress rules.

Answer:

D

Explanation:

Goal: Layer 7 routing for OKE microservices via a single entry point.

Option A: Manual configuration is inefficient and doesn't support path-based routing---incorrect.

Option B: LoadBalancer service provisions a Layer 4 balancer, not Layer 7 path routing---incorrect.

Option C: NodePort with NLB is Layer 4, less secure, and lacks path routing---incorrect.

Option D: Ingress controller with Regional Load Balancer (Application LB) provides Layer 7 routing based on paths---correct and efficient.

Conclusion: Option D is the best integration method.

Oracle states:

'Use a Kubernetes Ingress controller with OCI Regional Load Balancer for Layer 7 routing to OKE microservices based on request paths.'

This supports Option D. Reference: OKE Networking - Oracle Help Center (docs.oracle.com/en-

us/iaas/Content/ContEng/Tasks/contengnetworking.htm).

Question 2

Question Type: MultipleChoice

In a Zero Trust network architecture, what is the primary purpose of implementing micro-segmentation within OCI VCNs?

Options:

A- To increase network bandwidth.
B- To reduce the number of required route tables.
C- To limit the blast radius of potential security breaches.
D- To simplify inter-region connectivity.

Answer:

C

Explanation:

Context: Zero Trust assumes no trust, requiring strict isolation (micro-segmentation).

Option A: Bandwidth isn't increased by segmentation---incorrect.

Option B: Segmentation may increase route tables for granularity, not reduce them---incorrect.

Option C: Micro-segmentation isolates workloads, limiting breach impact (blast radius)---core Zero Trust goal and correct.

Option D: Inter-region connectivity isn't simplified by micro-segmentation---incorrect.

Conclusion: Option C aligns with Zero Trust principles.

Oracle notes:

'Micro-segmentation in OCI VCNs, using NSGs and security lists, limits the blast radius of breaches by isolating resources, a key Zero Trust principle.'

This supports Option C. Reference: Zero Trust in OCI - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Concepts/zerotrust.htm).

Question 3

Question Type: MultipleChoice

Your company utilizes a hybrid cloud architecture, connecting its on-premises network to an OCI VCN using a FastConnect private peering connection. You need to ensure that instances within a specific subnet in the VCN can only communicate with resources in a designated IP address range within the on-premises network. What is the MOST effective way to achieve this specific network isolation?

Options:

A- Configure an Internet Gateway for the subnet with a route rule to the on-premises network.
B- Modify the VCN's default security list to restrict traffic to the on-premises IP address range.
C- Create a custom route table for the subnet with a route rule pointing to the Dynamic Routing Gateway (DRG) and configure network security groups (NSGs) to limit traffic to the specified on-premises IP address range.
D- Configure a Local Peering Gateway (LPG) for the subnet to route traffic to the on-premises network.

Answer:

C

Explanation:

Goal: Restrict subnet traffic to a specific on-premises IP range via FastConnect.

Option A: Internet Gateway is for public access, not FastConnect---incorrect.

Option B: Default security list applies broadly, lacking granularity; NSGs are more effective---less optimal.

Option C: Custom route table with DRG ensures FastConnect routing; NSGs provide precise, instance-level traffic restriction---correct.

Option D: LPG is for same-region VCN peering, not on-premises---incorrect.

Conclusion: Option C is the most effective method.

Oracle notes:

'Use a custom route table with a DRG route rule for FastConnect traffic. NSGs offer granular control to restrict traffic to specific IP ranges.'

This supports Option C. Reference: FastConnect and NSG Overview - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/fastconnect.htm & docs.oracle.com/en-us/iaas/Content/Network/Concepts/NSGs.htm).

Question 4

Question Type: MultipleChoice

Your company has established a hybrid cloud environment using FastConnect to connect your on-premises network to your OCI VCN. You are advertising on-premises network prefixes to OCI via BGP. You want to ensure that OCI only learns routes from your on-premises network that are within a specific range, and that any other prefixes advertised are rejected to prevent routing conflicts. Which BGP attribute and configuration on the OCI side should you use to achieve this?

Options:

A- AS Path Prepending: Configure AS Path Prepending on the FastConnect virtual circuit to discourage OCI from selecting routes outside the desired range.
B- MED (Multi-Exit Discriminator): Configure MED values on the on-premises BGP router to influence OCI's route selection based on preferred exit points.
C- Route Filtering using Route Distinguisher (RD) and Route Target (RT): Configure RDs and RTs on the FastConnect virtual circuit to filter routes based on tenant isolation.
D- Route Filtering using Prefix Lists: Configure Prefix Lists on the FastConnect virtual circuit to accept only the desired prefix ranges and reject all others.

Answer:

D

Explanation:

Objective: Filter BGP routes on OCI to accept only specific on-premises prefixes.

BGP Attributes Overview:

AS Path Prepending: Lengthens AS path to influence route preference, not filtering.

MED: Influences exit point selection, not route acceptance.

RD/RT: Used in MPLS VPNs for tenant isolation, not simple prefix filtering.

Prefix Lists: Directly filter prefixes based on IP ranges.

Evaluate Options:

A: AS Path Prepending affects preference, not filtering; unsuitable.

B: MED influences path selection, not route rejection; incorrect.

C: RD/RT is for VPN contexts, not applicable here.

D: Prefix Lists explicitly allow/deny prefixes, meeting the requirement.

Conclusion: Prefix Lists on the FastConnect virtual circuit provide precise control over accepted routes.

Prefix Lists are the most effective BGP tool for filtering routes in OCI. The Oracle Networking Professional study guide notes, 'Prefix Lists can be applied to FastConnect virtual circuits to filter BGP advertisements, ensuring only approved prefixes are learned by OCI' (OCI Networking Documentation, Section: FastConnect and BGP). This prevents routing conflicts by rejecting unwanted prefixes, aligning with the security and control requirements.

Question 5

Question Type: MultipleChoice

Your security team has mandated that all traffic to Oracle Cloud Infrastructure Object Storage must be encrypted end-to-end and must not be routed over the public internet. You are designing a solution where compute instances within a private subnet will frequently upload and download data from Object Storage. Which option best options provides the most secure and compliant solution?

Options:

A- Configure a Service Gateway to Object Storage and enable encryption at rest on the Object Storage bucket.
B- Configure a NAT Gateway for the instances and enable encryption in transit using HTTPS for all Object Storage API calls.
C- Configure a Service Gateway to Object Storage and ensure all API calls to Object Storage are made over HTTPS.
D- Configure a Private Endpoint to Object Storage and ensure all API calls to Object Storage are made over HTTPS.

Answer:

C

Explanation:

Requirements: End-to-end encryption, no public internet for Object Storage access.

Options Analysis:

Service Gateway: Private access to Object Storage.

NAT Gateway: Public internet access; unsuitable.

Private Endpoint: Alternative private access, but newer feature.

HTTPS: Ensures in-transit encryption.

Evaluate Options:

A: Encryption at rest doesn't cover transit; incomplete.

B: NAT uses public internet; violates policy; incorrect.

C: Service Gateway with HTTPS ensures full encryption and privacy; correct.

D: Private Endpoint with HTTPS is valid but less common than Service Gateway; slightly less optimal historically.

Conclusion: Service Gateway with HTTPS is most secure and compliant.

Service Gateway is standard for private Object Storage access. The Oracle Networking Professional study guide states, 'A Service Gateway with HTTPS API calls ensures end-to-end encrypted traffic to Object Storage without public internet traversal' (OCI Networking Documentation, Section: Service Gateway). This meets security mandates effectively.

Question 6

Question Type: MultipleChoice

When migrating workloads from AWS to OCI, which connectivity option generally offers the LOWEST latency and HIGHEST bandwidth for data transfer, assuming a direct, dedicated connection is financially viable?

Options:

A- Establishing an IPSec VPN tunnel over the public internet between the AWS Virtual Private Cloud (VPC) and the OCI Virtual Cloud Network (VCN).
B- Utilizing a third-party cloud exchange provider to create a private network interconnect between AWS Direct Connect and OCI FastConnect.
C- Leveraging AWS Storage Gateway to replicate data to OCI Object Storage over the internet.
D- Employing AWS Transit Gateway to connect to a VPN Gateway on OCI via a public IP address.

Answer:

B

Explanation:

Goal: Lowest latency, highest bandwidth for AWS-to-OCI migration.

Option A: IPSec VPN over public internet has variable latency and limited bandwidth---incorrect.

Option B: Third-party cloud exchange with Direct Connect and FastConnect offers a private, dedicated link, minimizing latency and maximizing bandwidth---correct.

Option C: Storage Gateway over internet is slow and not dedicated---incorrect.

Option D: Transit Gateway with VPN uses public internet, lacking performance---incorrect.

Conclusion: Option B provides the best performance.

Oracle documentation notes:

'A third-party cloud exchange provider can interconnect AWS Direct Connect and OCI FastConnect, delivering a private, high-bandwidth, low-latency connection.'

This validates Option B. Reference: Multicloud Connectivity - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Concepts/multicloud.htm).

Question 7

Question Type: MultipleChoice

You are working as an OCI Network Specialist. Your company is migrating its on-premises IPv6 network to OCI. As part of the migration, you need to enable communication between the on-premises network and a VCN in OCI using FastConnect. Your company utilizes global unicast IPv6 addresses on-premises and wants to continue utilizing those addresses in OCI. However, you have a restriction that compute instance traffic must be limited to IPv6 only. After assigning IPv6 addresses from the prefix to the instance, they cannot ping external IPv6 addresses. What configuration most likely addresses this issue?

Options:

A- You can't use your own IPv6 address space in OCI. You must use OCI's provided ULA.
B- Ensure that there are IPv6 default routes (::/0) pointing to a NAT Gateway in your VCN route

tables.
C- Ensure that there is an Internet Gateway (IGW) attached to the VCN with a default route (::/0) in your subnet route table.
D- Ensure that there is a Service Gateway attached to the VCN with a default route (::/0) in your subnet route table.

Answer:

C

Explanation:

Problem: Instances with IPv6-only traffic can't ping external IPv6 addresses despite FastConnect and IPv6 prefixes.

Option A: OCI supports Bring Your Own IP (BYOIP) for IPv6, including global unicast addresses, so this is incorrect.

Option B: NAT Gateways are for IPv4 outbound traffic, not IPv6---irrelevant here.

Option C: For IPv6-only instances to reach external IPv6 addresses (beyond FastConnect), an Internet Gateway (IGW) is required with a default route (::/0) in the subnet route table. This enables public IPv6 connectivity---correct.

Option D: Service Gateway is for OCI services, not general IPv6 internet access---incorrect.

Conclusion: Option C fixes the issue by enabling IPv6 internet access.

Oracle states:

'To enable IPv6 traffic to the internet, attach an Internet Gateway to the VCN and add a route rule for ::/0. OCI supports BYOIP for public IPv6 prefixes.'

This aligns with Option C. Reference: IPv6 in OCI - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIPv6.htm).

Question 8

Question Type: MultipleChoice

You are designing a solution to implement IPSec encryption over a FastConnect circuit between your on-premises network and OCI. You are concerned about the overhead of IPSec impacting the maximum MTU (Maximum Transmission Unit) size that can be supported. What is the most important factor to consider when determining the MTU size for the IPSec tunnel interfaces in this scenario?

Options:

A- The available bandwidth of the FastConnect circuit. A larger MTU requires a higher bandwidth connection.
B- The smallest MTU supported by any device along the entire network path between your on-premises network and OCI, including the FastConnect provider's network.
C- The MTU size of the underlying Ethernet frames used by the FastConnect circuit.
D- The fragmentation settings on the DRG in OCI.

Answer:

B

Explanation:

Concern: IPSec overhead reduces effective MTU.

MTU Impact: Must avoid fragmentation, which degrades performance.

Evaluate Factors:

A: Bandwidth doesn't dictate MTU; incorrect.

B: Smallest MTU in path (path MTU) prevents fragmentation; most critical.

C: Ethernet MTU is a factor but not the limiting one; incomplete.

D: DRG fragmentation settings are secondary to path MTU; incorrect.

Conclusion: Path MTU is the key determinant to avoid fragmentation.

IPSec reduces MTU due to headers. The Oracle Networking Professional study guide explains, 'When configuring IPSec over FastConnect, the most important factor is the smallest MTU supported along the entire path to prevent fragmentation and ensure efficient traffic flow' (OCI Networking Documentation, Section: IPSec over FastConnect). Path MTU discovery is critical.

Question 9

Question Type: MultipleChoice

You are designing a highly available web application in OCI. You've created a VCN with two public subnets across different Availability Domains (ADs). You need to enable IPv6 support for the application to cater to a growing number of IPv6-only clients. You plan to use a Load Balancer to distribute traffic to backend compute instances in the public subnets. Which option

best approaches ensures the highest level of resilience and IPv6 connectivity for your application?

Options:

A- Configure the VCN with a /48 IPv6 ULA prefix. Configure the Load Balancer to listen on IPv4 only, and the compute instances to listen on both IPv4 and IPv6, relying on NAT for IPv6 clients.
B- Configure the VCN with a /48 IPv6 ULA prefix. Configure the Load Balancer to listen on both IPv4 and IPv6 addresses. Ensure the backend compute instances also listen on both IPv4 and IPv6 addresses. Route traffic accordingly using NSGs.
C- Configure the VCN with a public IPv6 CIDR block obtained from Oracle. Configure the Load Balancer to listen on IPv4 only, while backend compute instances listen on both IPv4 and IPv6, relying on NAT for IPv6 clients.
D- Configure the VCN with a public IPv6 CIDR block obtained from Oracle. Configure the Load Balancer to listen on both IPv4 and IPv6 addresses. Ensure the backend compute instances also listen on both IPv4 and IPv6 addresses.

Answer:

D

Explanation:

Requirements: HA and IPv6 support for public web app.

Option A: ULA is private, not routable; NAT for IPv6 is inefficient---incorrect.

Option B: ULA doesn't support public IPv6 clients---incorrect.

Option C: Public IPv6 CIDR is correct, but IPv4-only LB with NAT lacks direct IPv6---less resilient.

Option D: Public IPv6 CIDR with dual-stack LB and instances ensures full IPv6 support and HA across ADs---correct.

Conclusion: Option D maximizes resilience and connectivity.

Oracle states:

'For public IPv6 applications, use a public IPv6 CIDR block and configure Load Balancers and instances for both IPv4 and IPv6 to ensure resilience.'

This supports Option D. Reference: IPv6 in OCI - Oracle Help Center (docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIPv6.htm).

Question 10

Question Type: MultipleChoice

You are designing a hybrid cloud environment where multiple VCNs in OCI need to communicate with your on-premises network. You are using a single Dynamic Routing Gateway (DRG) to connect to your on-premises network via FastConnect. You want to ensure that each VCN is isolated from the others and that traffic between VCNs must pass through your on-premises security appliances for inspection. How should you configure the DRG attachments and route tables to enforce this security policy?

Options:

A- Attach all VCNs and the FastConnect to the DRG. Configure the DRG route table associated with each VCN attachment to route all traffic destined for other VCNs to the FastConnect attachment. Configure the FastConnect DRG route table to route traffic destined to each VCN to the corresponding VCN attachment.
B- Attach all VCNs and the FastConnect to the DRG. Configure static routes on each VCN's route table pointing to the DRG for any subnet not within the VCN. Enable the 'Transit Routing' feature on the DRG to allow inter-VCN communication.
C- Attach each VCN directly to the FastConnect using IPSec VPN tunnels, bypassing the DRG entirely to ensure all traffic flows through the on-premises security appliances.
D- Attach each VCN to the DRG using a Local Peering Gateway (LPG) and then attach one VCN to FastConnect. Configure routes so that traffic traverses from LPG to LPG through the on-premises network.

Answer:

A

Explanation:

Requirements: VCN isolation, inter-VCN traffic via on-premises appliances.

DRG Role: Central hub for VCN and FastConnect connectivity.

Evaluate Options:

A: DRG routes inter-VCN traffic via FastConnect to on-premises; meets isolation and inspection needs.

B: Transit Routing allows direct VCN-to-VCN communication, bypassing on-premises; incorrect.

C: Bypassing DRG with VPNs is complex and unsupported; incorrect.

D: LPG is for intra-region peering, not DRG-to-FastConnect; incorrect.

Conclusion: Option A enforces the policy via DRG route tables.

DRG route tables control traffic flow. The Oracle Networking Professional study guide states, 'To force inter-VCN traffic through an on-premises network via FastConnect, configure DRG route tables to route VCN-destined traffic to the FastConnect attachment, ensuring isolation and inspection' (OCI Networking Documentation, Section: DRG Routing). This setup leverages a single DRG effectively.

P2P exams

P2P exams

To Get Premium Files for 1Z0-1124-25 Visit

https://www.p2pexams.com/products/1z0-1124-25

For More Free Questions Visit

https://www.p2pexams.com/oracle/pdf/1z0-1124-25

