Exam : **1z0-1124-25**

Title : Oracle Cloud Infrastructure 2025 Networking Professional

Vendor : Oracle

Version : DEMO

NO.1 Which OCI service facilitates the creation of a private connection between two VCNs located in different tenancies, without traversing the public internet?

A. Internet Gateway

B. Service Gateway

C. Remote Peering Connection (RPC)

D. Dynamic Routing Gateway (DRG) with Local Peering Gateway (LPG)

Answer: C

Explanation:
* Requirement:Private VCN connection across tenancies.
* Services:
* Internet Gateway:Public access; incorrect.
* Service Gateway:OCI services, not VCNs; incorrect.
* RPC:Cross-tenancy private peering; correct.
* DRG with LPG:LPG is intra-region, not cross-tenancy; incorrect.
* Evaluate Options:
* A:Public; incorrect.
* B:Service-focused; incorrect.
* C:Designed for this scenario; correct.
* D:Misaligned components; incorrect.
* Conclusion:RPC is the right service.

RPC enables cross-tenancy peering. The Oracle Networking Professional study guide notes, "Remote Peering Connections (RPCs) establish private connectivity between VCNs in different tenancies over OCI's private backbone" (OCI Networking Documentation, Section: Remote Peering Connections). This ensures no public internet traversal.

NO.2 You are setting up a Site-to-Site VPN connection between your on-premises network and OCI. You have generated the IKE pre-shared key and configured the VPN connection in OCI. You now need to configure your on-premises Customer Premises Equipment (CPE). Which information from the OCI console is ESSENTIAL for configuring your on-premises CPE to establish the VPN connection?

A. The OCI region and availability domain.

B. The public IP address of the OCI Dynamic Routing Gateway (DRG) and the IKE pre-shared key.

C. The OCID (Oracle Cloud Identifier) of the VPN connection and the compartment ID.

D. The subnet CIDR blocks within your OCI VCN.

Answer: B

Explanation:
* Objective: Identify essential info for CPE to establish a Site-to-Site VPN with OCI.
* Option A: Region and availability domain are for OCI resource placement, not CPE config-incorrect.
* Option B: The DRG's public IP is the VPN endpoint, and the IKE pre-shared key authenticates the tunnel-essential and correct.
* Option C: OCID and compartment ID are for OCI management, not CPE setup-incorrect.
* Option D: Subnet CIDRs are for routing, configured later, not for tunnel establishment-incorrect.
* Conclusion: Option B provides the critical VPN connection details.

Oracle documentation states:
* "To configure your CPE for Site-to-Site VPN, you need the public IP address of the DRG (VPN headend) and the IKE pre-shared key from the OCI console."This confirms Option B.

Reference:Setting Up IPSec VPN - Oracle Help Center(docs.oracle.com/en
-us/iaas/Content/Network/Tasks
/settingupIPSec.htm).

NO.3 Your organization is migrating workloads to a multicloud environment using OCI, AWS, and Azure. You have applications that require access to on-premises resources and must maintain high security standards.
Which connectivity configuration would provide the MOST secure and reliable access while adhering to best practices for a hybrid multicloud architecture?

A. Establishing IPSec VPN tunnels from the on-premises network directly to each cloud provider (OCI, AWS, and Azure), terminating on the respective cloud provider's virtual network gateways

B. Using public internet connectivity for all cloud providers and relying on application-level security measures

C. Creating a private network connection to OCI using FastConnect, then extending the network to AWS and Azure using a software-defined WAN (SD-WAN) solution that supports end-to-end encryption and policy-based routing

D. Connecting on-premises to OCI using FastConnect and building VPN tunnels from OCI to Azure and AWS

Answer: C

Explanation:
* Needs: Secure, reliable hybrid multicloud access.
* Option A: Multiple VPNs are secure but complex and less reliable over internet-less optimal.
* Option B: Public internet with app security is insecure-incorrect.
* Option C: FastConnect to OCI provides a private base; SD-WAN extends securely to AWS/Azure with encryption and HA-correct.
* Option D: FastConnect to OCI with VPNs to others risks OCI as a single point of failure-less reliable.
* Conclusion: Option C is the most secure and reliable.
Oracle advises:
* "For hybrid multicloud, use FastConnect for primary connectivity and SD-WAN to extend securely to other clouds with encryption and policy control."This supports Option C. Reference:Multicloud Best Practices - Oracle Help Center(docs.oracle.com/en-us/iaas/Content/Network/Concepts/multicloud.htm#bestpractices).

NO.4 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?

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).

NO.5 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?

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).

NO.6 A large financial institution is migrating its on-premises trading platform to OCI. The platform requires low latency and high bandwidth connectivity to the on-premises data center. You have established an Oracle Cloud Infrastructure FastConnect circuit. You now need to connect multiple VCNs in different regions to the on-premises data center via this FastConnect circuit, optimizing for cost and management overhead. Which DRG configuration would be the most efficient and recommended approach?

A. Create a separate DRG in each region and attach each VCN to its regional DRG. Then, create a separate FastConnect attachment to each regional DRG. Finally, configure static routes on each DRG to direct traffic appropriately.

B. Create a single DRG in one region and attach all VCNs in all regions to this single DRG using remote peering connections. Attach the FastConnect circuit to this single DRG. Configure static routes on the DRG to direct traffic to the appropriate VCNs.

C. Create a single DRG in one region. Attach all VCNs in all regions to this single DRG using DRG attachments with remote peering. Attach the FastConnect circuit to the single DRG.

D. Create a single DRG in one region and attach all VCNs in all regions to this single DRG using local peering gateways (LPGs). Attach the FastConnect circuit to this single DRG. Configure static routes on the DRG to direct traffic to the appropriate VCNs.

Answer: C

Explanation:

* Requirements:Low latency, high bandwidth, multi-region VCNs via one FastConnect, minimal cost /overhead.
* DRG Strategy:
* Multiple DRGs:Increases cost and complexity.
* Single DRG:Centralizes management, reduces FastConnect attachments.
* Evaluate Options:
* A:Multiple DRGs and FastConnects; costly and complex; incorrect.
* B:Remote peering connections imply RPC, not standard DRG attachments; less precise.
* C:Single DRG with remote peering attachments; efficient and correct terminology; optimal.
* D:LPGs are intra-region, not cross-region; incorrect.
* Conclusion:Single DRG with remote peering attachments is most efficient.

A single DRG optimizes multi-region setups. The Oracle Networking Professional study guide notes, "For connecting multiple VCNs across regions to a single FastConnect, use one DRG with remote peering attachments to minimize cost and management overhead" (OCI Networking Documentation, Section: DRG with FastConnect). Option C aligns with OCI's recommended architecture.

NO.7 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?

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).

NO.8 Your company needs to connect an on-premises data center to an OCI Virtual Cloud Network (VCN) to extend their existing infrastructure to the cloud. The connection MUST be secure, reliable, and provide consistent, low-latency access to resources in both environments. Resources in the OCI VCN need access to the on-premises servers, and resources in the on-premises data center need to access the compute instances located in a private subnet within the OCI VCN. Which is the MOST appropriate architectural design for establishing connectivity in this hybrid cloud environment, considering the available endpoints and gateway options in OCI?

A. Implement a Site-to-Site VPN connection between the on-premises network and the OCI VCN, utilizing a Dynamic Routing Gateway (DRG) in OCI.

B. Establish a FastConnect connection between the on-premises network and the OCI VCN, utilizing a Dynamic Routing Gateway (DRG) in OCI.

C. Configure a public endpoint for each resource in the OCI VCN that needs to be accessed from the on- premises network.

D. Implement a FastConnect connection from the on-premises network to the OCI VCN utilizing a Dynamic Routing Gateway (DRG) in OCI and implement a Site-to-Site VPN connection as backup.

Answer: D

Explanation:
* Requirements: Secure, reliable, low-latency, bidirectional access with redundancy.
* Option A: VPN via DRG is secure but lacks low latency and redundancy-insufficient.
* Option B: FastConnect via DRG offers low latency and security but no redundancy-partial fit.
* Option C: Public endpoints are insecure and high-latency-incorrect.
* Option D: FastConnect for primary low-latency access, VPN as backup for redundancy-correct and most appropriate.
* Conclusion: Option D meets all criteria.
Oracle states:
* "FastConnect with DRG provides secure, low-latency hybrid connectivity. Add a Site-to-Site VPN for redundancy to ensure reliability."This supports Option D. Reference:Hybrid Cloud Connectivity - Oracle Help Center(docs.oracle.com/en-us/iaas/Content/Network/Tasks/hybridcloud.htm).

NO.9 You are using Terraform to deploy a multi-tier application architecture consisting of a public subnet hosting a load balancer, a private subnet hosting application servers, and another private subnet hosting a database. The Terraform code successfully creates all the required infrastructure, including route tables and security lists.

However, after deployment, you realize that the load balancer cannot reach the application servers in the private subnet. You have verified that the load balancer is healthy and the application servers are running.
What is the most likely cause of this connectivity problem?
A. The security list associated with the application server subnet does not allow ingress traffic from the load balancer's IP address range.
B. The route table associated with the application server subnet has a default route pointing to the Internet Gateway, which is incorrect for a private subnet.
C. The Network Address Translation (NAT) Gateway is misconfigured, preventing the application servers from initiating connections back to the load balancer.
D. The load balancer's security list is not configured to allow egress traffic to the application server subnet on the required ports (e.g., port 8080).
Answer: A
Explanation:
* Problem Scope:Load balancer (public subnet) cannot reach application servers (private subnet).
* Connectivity Flow:Load balancer initiates traffic to application servers; application servers respond.
Key checkpoints: routing and security rules.
* Analyze Routing:Private subnets typically don't route to an Internet Gateway by default; they use NAT or Service Gateways. Misrouting (Option B) would affect outbound traffic, not inbound from the load balancer.
* Security Rules:
* Ingress (App Servers):Must allow traffic from the load balancer's IP range.
* Egress (Load Balancer):Must allow traffic to the application servers.
* Evaluate Options:
* A:Missing ingress rule on application servers' security list blocks load balancer traffic; most likely.
* B:Incorrect default route affects outbound, not inbound; less likely.
* C:NAT misconfiguration impacts outbound, not inbound; incorrect.
* D:Load balancer egress is necessary but secondary to application server ingress.
* Conclusion:Ingress rule absence on the application server subnet is the primary blocker.
Security lists control traffic at the subnet level in OCI. The Oracle Networking Professional study guide explains, "For a load balancer in a public subnet to communicate with instances in a private subnet, the private subnet's security list must include an ingress rule allowing traffic from the load balancer's IP range" (OCI Networking Documentation, Section: Security Lists). Since Terraform deployed the infrastructure, a misconfigured security list is a common oversight.

NO.10 Your company is migrating an on-premises application to OCI. The application requires direct, low-latency access to an on-premises Microsoft SQL Server database. You've established a FastConnect connection between your on-premises network and an OCI VCN via a Dynamic Routing Gateway(DRG). You want to access this database from the OCI VCN. Which type of endpoint, in conjunction with appropriate routing, should you use to facilitate this connection?
A. An Internet Gateway with a public endpoint on the SQL Server.
B. A Service Gateway configured to access the on-premises SQL Server.
C. No specific OCI endpoint is required. The on-premises SQL Server is accessed directly through the DRG and appropriate routing.
D. A Private Endpoint within the VCN configured to connect to the private IP address of the on-

premises SQL Server.
Answer: C
Explanation:
* Requirement: Low-latency, direct access to an on-premises SQL Server via FastConnect.
* Option A: Internet Gateway with a public endpoint exposes the SQL Server to the internet, increasing latency and security risks-incorrect.
* Option B: Service Gateway is for OCI services (e.g., Object Storage), not on-premises resources-incorrect.
* Option C: FastConnect with a DRG provides a private, low-latency link. No additional OCI endpoint is needed; the SQL Server's private IP is accessed directly via DRG routing-correct.
* Option D: Private Endpoints are for OCI services within the VCN (e.g., ADB), not on-premises resources-incorrect.
* Conclusion: Option C leverages FastConnect and DRG for direct, secure access.
Oracle documentation notes:
* "FastConnect with a DRG enables private, low-latency connectivity to on-premises networks. Configure route tables to access on-premises resources directly; no additional endpoints are required." This supports Option C. Reference:FastConnect Overview - Oracle Help Center(docs.oracle.com/en-us
/iaas/Content/Network/Tasks/fastconnect.htm).

NO.11 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?

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).

NO.12 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?

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.