OCI Foundations Associate Certification Notes

Oracle Cloud Infrastructure Global Locations
March 2023
41 regions; 9 more planned
12 Azure Interconnect Regions
Types of regions:
Commercial
Commercial Planned
Sovereign Planned
Government
Microsoft Interconnect Azure

OCI has over 80 services currently available in OCI

7 Major services of OCI: [Cloud regions | Cloud@Customer | Hybrid Cloud | Multi-cloud]
Applications
Analytics
Developer Services
Data & AI
Databases
Infrastructure
Governance and Administration

Core Infrastructure:
Compute: Bare metal, VM, CPUs, GPUs, HPC
Containers: Containers, Kuberetes, Service Mesh, Registry
OS, Vmware: Autonomous Linux,
OS Mgmt Service, Marketplace
Storage: NVMe, Block, File, Object, Archive, Data Transfer
Networking: VCN, LB, Service Gateway, FC, VPN, Cluster Networking

Applications:
Serverless: Events, Functions, API Gateway
App Integration: Integration Cloud, Workflow, Notifications, Email Delivery
Business & industry Saas: ERP, HCM, SCM. Sales, Marketing, Service, Vertical Industry

Analytics:
Business Analytics: Analytics Cloud, Fusion Analytics

Governance & Administration:
Cloud Ops:

IAM, Compartments, Tagging, Console, Cost Advisor
Security:
Cloud Guard, Security Zones, Vault. KMS, Data Safe, DDoS, WAF
Observability:
Monitoring. Logging. Logging Analytics, Notifications, Events, Operations Insights, APM, Management Cloud

Data & AI:
Big Data: Big Data, Data Flow, Data Integration, Data Catalog, Golden Gate
AI services: Data Science, Digital Assistant
Messaging: Streaming. Queueing, Service, Connector

Databases:
Oracle Databases:
ATP, ADW, DBCS VM/BM, JSON, Dedicated, Exadata, Exadata C@C
Distributed & OSS Databases:
NoSQL, MySQL

Developer Services:
Low Code: APEX
AppDev: Visual Builder Studio, GraalVM, Helidon, SOL Developer, Shell, APIs/ CLI/ SDKs/Docs
Infrastructure as Code: Resource Manager, Terraform, Ansible

[penny per core hr]

OCI Architecture:
Regions -> AD -> FD

Choosing a Region:
Location:
Choose a region closest to your users for lowest latency and highest performance!
Data Residency & Compliance:
Many countries have strict data residency requirements.
Service Availability:
New cloud services are made available based on regional demand, regulatory compliance, resource availability, and other factors.

Availability Domains:
Isolated from each other, fault tolerant, unlikely to fail simultaneously.
Physical infrastructure not shared

Fault Domains:
Each Availability Domain has three Fault Domains (FD).

Logical data center within an AD
Resources placed in different FDs will not share single points of hardware failure
In any region, resources in at most ONE fault domain are being actively changed at any point in time. This means that availability problems caused by change procedures are isolated at the fault domain level.
You can control the placement of your compute or database instances to fault domains at instance "launch" time.

Oracle Cloud ID (OCID)
ocid1. <RESOURCE TYPE>. <REAIM>. [REGION] [. FUTURE USE]. <UNIQUE ID>

Compartments
Six levels of Nesting allowed

Policies - Human readable statements to define granular permissions:
Allow group <group name> to ‹verb> <resource-type> in tenancy
Allow group <group name> to ‹verb> <resource-type> in compartment ‹compartment name> [where <conditions>1]
Policy Attachment - To a compartment or the tenancy
Policies are only applied to groups but not users

Verb: manage, use, read, inspect

Aggregate resource-type:
all-resources
database-family
instance-family
object-family
virtual-network-family
volume-family

Best practice: Don't Use the Tenancy Administrator Account for Day-to-Day Operations
Best practice: Create dedicated compartments to isolate resources
Best practice: Enforce the use of Multi-Factor Authentication (MA)

AM resources do not have an aggregate resource type: True

Policies - OCI Admin: Least Amount of Policies:
Allow group OCI-admin-group to manage all-resources in tenancy
Allow group OCI-admin-group to manage domains in tenancy
Allow group OCI-admin-group to manage users in tenancy
Allow group OCI-admin-group to manage groups in tenancy
Allow group OCI-admin-group to manage dynamic-groups in tenancy

Allow group OCI-admin-group to manage policies in tenancy
Allow group OCI-admin-group to manage compartments in tenancy

VCN:
VCN is a regional service
No entry in route table needed for routing data between public and private subnets. VCN takes care of that.
Longest specific match gets more priority for routing
SAME OCI Region: networks talk to each through "local peering" using local peering gateway (LPG)
Different OCI regions: networks communicate with each other through Remote peering using dynamic routing gateways
Dynamic routing gateway v2: for more networks within the OCI region to communicate with each other, (maybe 300 + networks), instead of local peering, DRG v2 can be used.
Security Lists: firewall Rules associated to a subnet and applied to all instances in the subnet
Stateful: if traffic is allowing in through a port, it is always allowed out as well

Route Table

VCN uses virtual route tables to send traffic out of the VCN (for example, to the internet, to your on-premises network, or to a peered VCN). These route tables have route rules that provide mapping for traffic from subnet via gateways to other subnets or destinations outside VCN
Each rule specifies a destination CIDR block and the target (the next hop) for any traffic that matches that CIDR.

Security List

Security List is a common set of firewall rules associated with a subnet and applied to all compute instances in that subnet. Security List specifies two types of traffic allowed:

- Ingress: Incoming Traffic
- Egress: Outgoing Traffic

Firewall rules in OCI are defined at the subnet level and not at compute instance level.

Network Security Group

Network Security Groups are another method for implementing security rules. NSGs provides a virtual firewall for a set of Cloud resources that have the same security posture.
Read our blog to know more about **Network Security Groups Vs. Security List: When to use What?**

Gateways

There are 5 gateways in OCI Networking:
1) Internet Gateway (IG): It provides a path for network traffic between the

internet and OCI VCN. Compute Instance in Public Subnet by default won't be able to connect to the internet without IG.
2) NAT Gateway: It gives resources without public IP addresses access to the internet without allowing incoming traffic from the internet to that resources.
3) Service Gateway: It allows OCI resources to access public OCI services without the use of the Internet or NAT Gateway Eg: Object Storage.
4) Dynamic Routing Gateway (DRG): DRG provides a single point of entry for remote network paths coming into VCN. It provides a path for VCNs to communicate across regions or outside the region to On-premise. Each VCN can have a single DRG.
5) Local Peering Gateway (LPG): Used to establish communication between resources of different VCNs within a Region.
Read our blog to know more in detail about **Gateways in OCI: Internet Gateway, NAT Gateway, Service Gateway, Dynamic Routing Gateway**

VCN Peering

- VCN Peering is the process of connecting multiple virtual cloud networks (VCN)
- With peering, instances in two VCNs communicate as if they are in the same network
- VCN Peering can be of two types **Local VCN Peering (within Region)** using **LPG & Remote VCN Peering (across Regions)** using DRG.
  - **Local VCN Peering(LPG)**: The process of creating a path between VCNs for communication in a single region.
  - **Remote Peering Connection:** The process of creating a path between VCNs communication across regions.
- Local VCN Peering is supported in all OCI Regions.

Security List: A set of firewall rules that apply to all resources in a subnet
Network Security Group: A set of firewall rules that apply to any set of resources in a VCN that you specify
[port 80: web servers on compute instances]
[port 1521: ?]

Load Balancer: Used for high availability and high scalability; higher level of routing intelligence (looks at packets)
Layer 7 load balancer: HTTP/HTTPS;
2 types if shapes for LB:
-> Scalable - Flexible/ Dynamic shapes: define min, max and range, LB supports any traffic in that range: 10 mbps - 8 gbps
-> Predefined Shape: Small , med and large; no warmup required; automatically scales
LB can be public or private

Network Load Balancer: Much faster and lower latency: used for high performance
OCI Network Load Balancer operates at layer 4 (transport layer) of the OS model. It distributes traffic among instances within its backend set based on TCP or UDP protocols.

Specify a load balancing policy:
Weighted round robin: This policy distributes incoming traffic sequentially to each server in a backend set list.
IP hash: This policy ensures that requests from a particular client are always directed to the same backend server.
Least connections: This policy routes incoming request traffic to the backend server with the fewest active connections.

Configure listener for a load balancer:
A listener is a logical entity that checks for incoming traffic on the load balancer's IP address. To handle TCP, HTTP and HTTPS traffic, you must configure at least one listener per traffic type. You can configure additional listeners after you create your load balancer.

COMPUTE:
- types: VM [shared, multi-tenant], Bare meter servers [dedicated servers/ machine, not shared], Dedicated host [dedicated BM machine + VM on top of that, not shared]
- offers scalability, high performance, lower pricing
- Flexible shapes: OCPUs, Memory
- AMD, intel, ampere (arm - based, and best if the bunch, higher performance and lower cost)
- pricing model: pay as you go, Universal Credits
- Preemptive VMS: Low Cost, Short lived VMs, Batch Jobs, Fault tolerant workloads, 50% cheaper

Launching a compute instance Steps:
VCN [wizard, cidr block] > subnet [cidr block, route table] > internet gateway > add route rules > security list [port 80 for web servers] > create instance [cloose AD, capacity type, fault domain (leave it to oracle to choose), image (OS) and shape (VM or BM, cpu, memory, flex means flexible shapes), VCN, subnet, ssh keys (public key)]
You can now SSH to this instance.

Scaling:
Vertical:
Scale-up and scale-down instance shape supported
New shape must have same hardware architecture

Downtime required
Stop instance before vertical scaling

Horizontal or Auto scaling:
for high availability
Enables large-scale deployment of VMs
Scale-out or scale-in
One VM fails, others keep working
Match traffic demand by adding/removing VMs automatically

To Autoscale:
Running instance > Config [OS image, metadata, shapes, VNICs, Storage, subnets] > instance pool [Put in different Availability Domains, Manage all together (stop, start, terminate)] > scaling rules [min and max size]

OKE [Oracle containers using kubernetes]:
VM: hardware > hyperviser > VMs [app, libs, OS]
Containers: Hardware > OS > Container runtime [docker] > Container [app, lib]

Disadvantages of VMs:
Higher Utilization of Resources Compared to On-Premises
Multiple VMs
Multiple OS
Higher Disk Space
Longer Boot Time

Advantages of containers:
Faster Boot Time
Lightweight
Portable

Container Orchestration:
Deploy, Connect, Manage, Scale Up-Down.

Kubernetes, an open source platform:
Can run containerized applications of any scale without any down time
Can self-heal containerized applications
Can auto-scale containerized applications
Greatly simplifies deployment operations

Docker is used to manage and build the containers.
Docker as a container runtime is no longer supported after Kubernetes v1.20
(other runtimes like CRI-O are used instead)
Kubernetes links containers running on multiple hosts and orchestrates them.

Containers communicate with each other via Kubernetes.

OKE Overview:
Core :
> Fully managed, scalable, and highly available service
Engine :
> Uses the open-source system: Kubernetes
Developer :
> One click cluster creation
> CLI/API support
> Support for Arm and GPU instances
DevOps :
> Autoscaling support
> Automatic Kubernetes upgrade
> Self-healing cluster nodes

Components of a cluster:
pods [groups of node pools [group pf nodes]][customer managed worker nodes], control plane nodes [oracle manages, scaling, manages worker nodes, HA, no pay, make cluster decisions]

Types of OKE clusters:
Basic Clusters:
> Basic clusters support all the core functionality provided by Kubernetes and Container Engine for Kubernetes
> Basic clusters come with a Service Level Obiective (SLO) but not a financially-backed Service Level Agreement (SLA)
Enhanced Clusters:
> Enhanced clusters support all available features, including features not supported by basic clusters

Types of node pools:
Managed Nodes:
You are responsible for managing managed nodes (can configure them to meet your specific requirements).
You are responsible for upgrading Kubernetes on managed nodes, and for managing cluster capacity.
You can create managed nodes and node pools in both basic clusters and enhanced clusters.
Virtual Nodes:
Virtual nodes provide a 'serverless'
Kubernetes experience, enabling you to run containerized applications at scale
The Kubernetes software is upgraded, and security patches are applied while respecting application availability requirements.

You can only create virtual nodes and virtual node pools in enhanced clusters.

OCI Container Instances: [serverless, fully managed, w/o Kubernetes]
OCI Container Instances eliminate operational complexities for users
OCI Container Instances take care of the underlying container runtime and compute resources
The compute infrastructure provides robust workload isolation for enhanced security

Oracle Functions: [Function as a service]
Charged for function runtime
Event Driven Architecture
Oracle Cloud Integrated
Container Native
Open Source

Push container to registry > function trigger > code runs > pay for code execution

Storage:
> local NVMe
> block volume
> file storage
> object storage

Data migration services:
> data transfer disk
> Data transfer appliance
> storage gateway

Object Storage:
Internet-scale, high-performance storage platform
Data managed as objects
Ideal for unstructured data
Regional, Public service
Multiple storage tiers
Private access from OCI resources (e.g. compute)
Advanced capabilities

OCI Object Storage Scenarios:
Content Repository
Unstructured and semi-structured data
Big Data/Spark/ Hadoop/Data Analytics
Archive/Backup

Object storage Resources:
Object: [key value pair, Object's metadata]
Bucket: [Stored in a bucket, Unique name in a tenancy, Flat hierarchy]
Namespace: [Logical entity; top-level container for all buckets/objects, Global unique name]

Objects Storage Tiers:
Standard Storage Tier [hot] :
Fast, immediate, and frequent access
Most recent copy of the data
Instantaneous retrieval
Can't be downgraded

Infrequent Access Storage Tier: [cool]
Ideal for data that you access infrequently
Storage costs lower than the Standard Storage Tier
Minimum retention requirement for Infrequent Access: 31 days
Retrieval fees

Archive Storage Tier: [cold]
Seldom or rarely accessed data
Minimum retention requirement for Archive Storage: 90 days
Objects need to be restored before download
Restore time: 1 Hour
Download time: 24 Hours
Archive Bucket can't be upgraded

> auto tiering; versioning; rules can be applied for lifecycle; data encryption by default; access through API calls

Block volume:
Compute instance > block volume
Advantages:
Create and Attach Disks
Detach and Delete Disks
Keep Data Even After You Delete The Instance
Durable and persist

Block volume tiers:
Lower Cost: Large Sequential 1/O Workloads, 2 10PS/GB
Balanced: Balanced Choice for Random I/O, 60 IOPS/GB
Higher Performance: Most I/O-demanding Workloads, 75 IOPS/GB
Ultra High Performance: Highest I/O-demanding Workloads, 90-225 IOPS/GB

> Auto-tune Performance
> encrypted [at rest, in-transit]
> read/write sharable
> Resizing while instance running
> replications between regions [DR, migration, Expansion]
> volume groups [for time consistent backups]
> attachment type: ISCSI [no vm?] , Paravirtualized [virtualize volume in hypervisor and then attach to instance]

File Storage:
> Hierarchical Collection of Documents Organized into Named Directories
> Distributed File System [Linux: NFS; Windows: SMB]
- Supported by UNIX and Windows
- Allows Creation, Deletion, Reading, Writing, Sharing, and Locking
- Supported by All Major OSes and Hypervisors
- (Typically) No Extra Client Software Needed
- Provides Access Over Networks

OCI File Storage Service:
> Shared storage for compute instances
> Supports NFSv3 distributed file system
> Data protection: Snapshots
> Security: Data-at-rest and in-transit encryption

DATABASES:
Oracle public cloud:
> base db service
> Exacta db service on dedicated infrastructure [customer manages db; infra by oracle]
> autonomous db [shared and dedicated exadata]
Cloud @customer
> exadata
> autonomous

Autonomous DB:
> uses ML to automate db activities, infrastructure [scaling, patching, fault tolerance, provisioning, tuning]
> shared [autonomous transaction processing and data warehouse]
> dedicated [atp and adw]
> ATP, ADW, autonous JSON db , APEX service
> avoid repetitive db tasks
> The self-driving feature of Oracle Autonomous Database enables automatic database optimizations without manual intervention. It uses machine learning and

automation to perform tasks such as provisioning, patching, tuning, and backup, which helps reduce the need for manual database administration and maintenance.
> Oracle Autonomous Database supports various workload types like Autonomous Data Warehouse (ADW) for high-performance analytics, Autonomous Transaction Processing (ATP) for high-performance transactional workloads, APEX for low-code application development, and JSON for JSON document storage and querying. However, MySQL is a different type of database system and not a workload type supported within Oracle Autonomous Database. Oracle does provide a separate managed service for MySQL in the Oracle Cloud, but it is not a workload type under the Autonomous Database offering.

Choose network access type: [ADW]
Secure access from everywhere: Allow users with database credentials to access the database from the internet.
Secure access from allowed IPs and VCNs only: Restrict access to specified IP addresses and VCNs.
Private endpoint access only: Restrict access to a private endpoint within an OCI VCN.

MySQL Database Service:
> High Availability
> Fault-tolerant system with automatic failover and zero data loss
> increased uptime
> standalone ; high availability

MySQL Database Service with HeatWave:
> Easily run high performance analytics against your MySQL database, no ETL required
> OLTP [InnoDB] and OLAP applications [Heatwave]
> Single MySQL database for OLTP & analytics applications
> All existing applications work without any changes
> MySQL HeatWave uses an in-memory data storage mechanism to provide high-performance query execution. It achieves this by storing the data in a columnar format in-memory, which allows for faster access and processing of data during query execution, especially for OLAP workloads.

Oracle NoSQL Database Cloud Service:
Features overview:
> Fully managed: Database operation, maintenance, tuning are managed by Oracle
> Data model flexibility: Document, fixed-schema, key/value models supported with a single application interface
> Developer friendly: Easy-to-use APIs and integrated with different developer tools

> Elastic: Dynamically change throughput and storage capacities based on workloads
> Access control: Enterprise grade security with roles and privileges
> Always available: Built-in high availability to ensure business continuity
> High performance: Predictable single-digit millisecond latencies with high workloads
> Low operating cost: Pay only for the throughput and storage capacities provisioned
> Hybrid cloud: Interoperate with Oracle NoSQL on-premise solution using a single application interface
> used for applications with high volume requirement

SECURITY:
> in OCI, Oracle is responsible for the cloud, and users are responsible for security in the cloud.
> security is implemented at various layers of the stack
> Security layers: Services and Use cases:

Infrastructure Protection:DDoS, Protection, Web Application Firewall, Security Lists / NSG, Network Firewall
• DDoS protection
• Network security controls
• Virtual firewalls
• Filter malicious web traffic

Identity and Access Management: IAM,MFA,Federation,Audit
• Manage user access and policies
• Manage multi-factor authentication
• Single sign-on to identity providers
• Record API calls automatically

OS and Workload Protection: Shielded Instances, Dedicated Host, Bastion, OS Management
• Secure Boot, Measured Boot, TPM
• Workload isolation
• Managed Bastion
• OS patch and package management

Data Protection: Vault Key Management, Vault Secrets, Management, Data Safe, Certificates
• Encryption for data at rest and in transit
• Centralized key storage and management
• Rotate, manage, and retrieve secrets
• Discover, classify, and protect data

Detection and Remediation: Cloud Guard, Security, Zones, Threat, Intelligence, Vulnerability, Scanning
• Security posture management
• Secure Enclave
• Security Advisor
• Vulnerability and exposure scanning

Oracle Cloud Guard: [cloud security and posture management]
> you can automate detecting and applying fixes
> Detectors [public instances, bucket, suspicious IP] > Problems [notifications] > Responders [stop instance, disable bucket, suspend users or any corrective actions]

Security Zones and Security Advisor:
> security zone: Refers to a cloud compartment in which you cannot disable security
> Security Advisor: Refers to a cloud service that unifies security zone, cloud guard, and other cloud capabilities
> Security Zone Recipe: policies ; a compartment can be assigned as security zone

Encryption:
> plain to cipher text; decryption is reverse process
> A key is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encrypt or decrypt data.
> Encryption key/key pair is generated for a specific algorithm that can be used for encryption or digital signing.
> encryption at rest: stored data is un-readable without key needed to decrypt
> encryption in transit: client -> in-transit encryption > server
> Symmetric-key cryptography is where a single key is used for encryption and decryption [AES encryption keys]
> Asymmetric encryption is where different keys are used for encryption and decryption. [public and private keys used to encrypt and decrypt respectively] [RSA encryption keys]
> ECDSA encryption keys: for digital signing only and NOT to encrypt or decrypt

> Hardware Security Module (HSM):
HSM is a physical computing device.
Tamper-evident hardware
Used to manage digital keys
Performs cryptographic functions

> OCI uses HSM on the backend:
OCI Vault service uses HSMs that meet the Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification.
Tamper-resistant
Requires identity-based authentication
Deletes keys from the device when it detects tampering

Vault:
> AES, RSA, ECDSA algorithm support
> integrated with OCI services
> key rotation
> its works using Envelope Encryption: 2 tier [master key, data keys]; easier to manage; limits blast radius; rotate master key
>> if master key is deleted, no way to recover data
>> soft delete keys with 7 days GAP
>> you can schedule vault deletion with wait 7 - 30 day period

GOVERNANCE AND ADMINISTRATION:
> Pricing:
Pay as you go (PAYG):
Charged only for the resource consumed
No upfront commitment
No minimum service period
Usage metered

Annual Universal Credits:
Commit to an annual pool of funds
Significant savings
Must use credits within 12 months
Discounts based on size of deal and term of deal

Bring Your Own License (BYOL):
Apply your current on-premises Oracle licenses to equivalent, highly automated Oracle IaaS & PaaS services in the cloud
Complete license mobility with on-premises

> Factors that affect pricing:
>> Resource Size:
Bigger resources cost more!
>> Resource Type:
VMs v/s BMs
VMs v/s Functions
BYOL v/s managed DBs

>> Data Transfer:
No Ingress cost
Careful with Egress cost
Between ADs, ingress and egress is free
>> All OCI regions have the same pricing!

> Cost management Tools:
>> budgets
>> Cost Analysis
>> Cost and Usage Reports
>> Limits, Quotas and Usage
>> Compartment Quotas [set, unset, or zero resources]

> Service limits are the upper bounds placed by Oracle on the number of resources you can create in a region or tenancy, while compartment quotas are the upper bounds defined by the users for resource usage within specific compartments. The distinction is that service limits are set by Oracle and apply to a tenancy in a region, while compartment quotas are set by the users and apply to specific compartments.

> Cost Advisor: [Cost management, high availability, performance, security]

> Tagging:
>> Customize the organization of your resources
>> Cost Management
>> Tag based Access Control
>> 2 Types of Tags:
>>> Free-form Tags: [key: value]
Basic implementation
Comprises key and value only
No defined schema or access restriction
>>> Defined Tags (recommended): [namespace.Key: Value]
More features and control
Contained in
Namespaces
Defined schema, secured with Policy

> Oracle Support Rewards:
>> Customers can decrease Tech License Support spend to as low as zero by using OCI
>> Earned at the end of each month based on Total Monthly Consumption of OCI Services

————————

SAMPLE QUESTIONS

Q1: Describe OCI Networking Services
Q1: Which component of Oracle Cloud Infrastructure Networking Service provides a private connection between a VCN and an on-premises network?
A. Internet Gateway
B. Network Address Translation (NAT) Gateway
C. Dynamic Routing Gateway (DRG) [A]
D. Service Gateway
Explanation: A Dynamic Routing Gateway (DRG) is a component of OCI Networking Service that provides a private connection between a Virtual Cloud Network (VCN) and an on-premises network. It enables users to establish a secure and reliable connection between their cloud and on-premises resources, facilitating hybrid cloud deployments.

Q2: Describe OCI Networking Services
Q2: What is the primary purpose of a Network Security Group (NSG) in Oracle Cloud
Infrastructure Networking Service?
A. To control routing between VCNs
B. To provide a private connection between a VCN and an on-premises network
C. To control traffic flow between specific resources within a VCN [A]
D. To connect a VCN to the public internet
Explanation: A Network Security Group (NSG) in OCI Networking Service is designed to control traffic flow between specific resources within a VCN. It provides a more granular level of control compared to Security Lists, enabling users to apply security rules to individual resources, such as instances or load balancers.

Q3: Describe OCI Compute Services
Q3: What is the term used to describe the combination of an instance's shape, base image, and metadata in Oracle Cloud Infrastructure Compute service?
A. Instance Configuration [A]
B. Instance Template
C. Instance Profile
D. Instance Specification
Explanation: In OCI Compute Service, an Instance Configuration is a pre-defined configuration that includes the instance's shape, base image, and metadata. It allows users to quickly create new instances with the same configuration, streamlining the deployment process.

Q4: Describe OCI Compute Services
What is the primary purpose of Oracle Cloud Infrastructure Functions?
A. To deploy and manage virtual machines

B. To execute code in response to events or HTTP requests [A]
C. To store and manage files
D. To provide a managed database service
Explanation: The primary purpose of Oracle Cloud Infrastructure Functions is to execute code in response to events or HTTP requests. It is a serverless computing platform that allows developers to build, deploy, and run applications without the need to manage the underling infrastructure.

Q5: Describe OCI Storage Services
Q5: What feature of Oracle Cloud Infrastructure Object Storage Service enables users to automatically move objects between storage tiers based on predefined rules?
A. Object Lifecycle Management [A]
B. Object Versioning
C. Cross-Region Replication
D. Pre-Authenticated Requests
Explanation: Object Lifecycle Management enables users to manage their Object and Archive storage data by taking automated actions based on rules that they define.

Q6: Describe OCI Storage Services
Q6: Which performance level is NOT available in the Oracle Cloud Infrastructure Block
Volume service?
A. Higher Performance
B. Low Performance [A]
C. Balanced
D. Ultra High Performance
Explanation: Block Volume Performance Levels are Lower Cost, Balanced, Higher Performance and Ultra High Performance

Q7: Describe OCI Database Services
Q7: Which workload type is NOT optimized for Oracle Autonomous Database on Shared
Exadata Infrastructure?
A. Data warehousing
B. Transaction processing
C. Mixed workloads
D. High-performance computing [A]
Explanation: Autonomous Database supports different workload types, including: Data Warehouse, Transaction Processing (& mixed workloads). JSON Database, and APEX Service.

Q8: Describe OCI Database Services
Q8: What is the primary purpose of the MySQL Database Service HeatWave option in OCI?
A. To provide a distributed in-memory query accelerator [A]
B. To ensure high availability and fault tolerance
C. To offer a serverless MySQL deployment
D. To enable seamless database migration from on-premises to OCI
Explanation: Oracle MySQL HeatWave is the only MySQL cloud service with a built-in, high performance, in-memory query accelerator-HeatWave. It increases MySQL performance by orders of magnitude for analytics and mixed workloads without any changes to current applications.

Q9: Describe OCI Security Services
Q9: Which of the following features is NOT provided by Oracle Cloud Infrastructure
Security Zones?
A. Automatically enforcing security best practices
B. Restricting resource creation based on predefined security policies
C. Continuous monitoring of security posture
D. Storing and managing encryption keys and secrets [A]
Explanation: OCI Security Zones provide features like automatically enforcing security best practices, restricting resource creation based on predefined security policies, and continuously monitoring security posture. However, storing and managing encryption keys and secrets is a function of OCI Vault, not Security Zones.

Q1o: Describe OCI Security Services
Q10: Which Oracle Cloud Infrastructure service is responsible for securely storing and managing encryption keys, and secrets?
A. Cloud Guard
B. Security Zones
C. Security Advisor
D. Vault [A]
Explanation: OCI Vault Service is responsible for securely storing and managing encryption keys, secrets, and certificates. Vault Service helps protect sensitive data by providing a secure, centralized repository for managing and controlling access to these critical security assets.

Q11: Describe OCI Pricing Model
Q11: Which factors does NOT impact the cost of running a virtual machine instance in
Oracle Cloud Infrastructure?
A. The number of virtual machines running

B. The size of the VM instance
C. The operating system used by the VM instance
D. The region used by the VM instance [A]
Explanation: The cost of running a virtual machine (VM) instance in OCI can be impacted by multiple factors, including the number of virtual machines running, the size of the VM instance (e.g., number of OCPUs, memory), and the operating system used by the VM instance.
Understanding these factors can help customers better manage their costs.

Q12: Describe OCI Regions and Availability Domains
Q12: Which of the following best describes the relationship between Oracle Cloud Infrastructure Regions and Availability Domains?
A. A region is a part of an Availability Domain
B. Availability Domains exist independently of regions
C. An Availability Domain is a part of a region [A]
D. Regions and Availability Domains are the same thing
Explanation: In OCI, an Availability Domain is a part of a region. A region is a group of geographically close data centers, while an Availability Domain is an isolated, fault-tolerant data center within a region.

———
Additional notes:

The key difference between Security Lists and Network Security Groups in Oracle Cloud Infrastructure is that Security Lists apply to subnets, while Network Security Groups apply to individual instance VNICs. This allows for more granular control of traffic in and out of instances.

A Route Table is a component in Oracle Cloud Infrastructure Networking Service that defines rules for packet forwarding to destinations outside the Virtual Cloud Network (VCN). Route Tables have rules to route traffic from subnets to destinations outside the VCN by way of gateways or specially configured instances.

A Dynamic Routing Gateway (DRG) provides a path for traffic between a VCN and an on-premises network or another VCN in the same or different region.

A Service Gateway in Oracle Cloud Infrastructure networking service enables access to Oracle services within the same region without the traffic going through the public internet. This provides a more secure and reliable connection for accessing Oracle services like Object Storage, Autonomous Database, and others.

Oracle Cloud Infrastructure Web Application Firewall (WAF) is designed to protect your web applications from various types of malicious attacks, such as SQL injection and cross-site scripting. WAF inspects incoming web traffic and filters out any requests that match predefined security rules, ensuring the security and availability of your web applications.

In Oracle Cloud Infrastructure, Security Lists are responsible for controlling traffic between subnets within a virtual cloud network (VCN). They define ingress and egress rules to determine the allowed traffic at the subnet level.

The self-securing feature of Oracle Cloud Infrastructure Autonomous Database provides automatic application of security patches and protection from threats. It ensures that the database is always up-to-date with the latest security updates, helping to safeguard your data and maintain a strong security posture.

In Oracle Cloud Infrastructure, the "Principal" component of an IAM policy statement defines the user or group the policy applies to. It specifies the groups that the policy statement affects, granting them access to resources and actions defined in the policy statement.