
**Vendor:**Oracle

**Exam Code:**1Z0-1085-20

**Exam Name:**Oracle Cloud Infrastructure Foundations 2020 Associate

**Version:**Demo

**QUESTION 1**

Which three services Integrate with Oracle Cloud Infrastructure (OCI) Key Management?

A. Functions

B. Block Volume

C. Object Storage

D. Auto Scaling

E. Identity and Access Management

F. File Storage

Correct Answer: BCF

DATA ENCRYPTION

Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements for cryptographic algorithms and key management The Oracle Cloud Infrastructure Block Volume service always encrypts all block volumes, boot volumes, and volume backups at rest by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. By default all volumes and their backups are encrypted using the Oracle- provided encryption keys. Each time a volume is cloned or restored from a backup the volume is assigned a new unique encryption key.

The File Storage service encrypts all file system and snapshot data at rest. By default all file systems are encrypted using Oracle-managed encryption keys. You have the option to encrypt all of your file systems using the keys that you own and manage using the Vault service. Object Storage employs 256-bit Advanced Encryption Standard (AES-256) to encrypt object data on the server. Each object is encrypted with its own data encryption key. Data encryption keys are always encrypted with a master encryption key that is assigned to the bucket. Encryption is enabled by default and cannot be turned off. By default, Oracle manages the master encryption key.

Reference:

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Concepts/overview.htm https://docs.cloud.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm https://docs.cloud.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm

Oracle Cloud Infrastructure Key Management is a managed service that enables you to encrypt your data

using keys that you control.IAM, Autoscaling and functions cannot be used with Key Management and hence are incorrect options.

Reference:

https://docs.cloud.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm

---

**QUESTION 2**

Which is NOT required to register and log support requests in My Oracle Support (MOS)?

A. Your Customer Support Identifier (CSI)

B. Your account password

C. Your tenancy OCID (Oracle Cloud Identifier)

D. Your resource OCID (Oracle Cloud Identifier)

Correct Answer: D

You can open a support service request with Oracle Support To create a service request:

Go to My Oracle Support and sign in.

If you are not signed in to Oracle Cloud Support, click Switch to Cloud Support at the top of the page.

Click Create Service Request.

Select the following from the displayed menus:

Service Type: Select Oracle Cloud Infrastructure from the list. Service Name: Select the appropriate option for your organization. Problem Type: Select your problem type from the list.

Enter your contact information.

Enter a Description, and then enter the required fields specific to your issue. For most Oracle Cloud Infrastructure issues you need to include the OCID (Oracle Cloud Identifier) for each resource you need help with. See Locating Oracle Cloud Infrastructure IDs for instructions on locating these.

Reference:

https://www.zerowait-state.com/blog/create-sr/

---

**QUESTION 3**

Which statement about the Oracle Cloud Infrastructure (OCI) shared-security model is true?

A. You are responsible for securing all data that you place in OCI

B. You are not responsible for any aspect of security in OCI

C. You are responsible for securing the hypervisor within OCI compute service

D. You are responsible for managing security controls within the physical OCI network

Correct Answer: A

Oracle Cloud Infrastructure offers best-in-class security technology and operational processes to secure its enterprise cloud services. However, for you to securely run your workloads in Oracle Cloud Infrastructure, you must be aware of your security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), and you are responsible for securely configuring your cloud resources. Security in the cloud is a shared responsibility between you and Oracle. In a shared, multi-tenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data-center facilities, and hardware and software systems) and you are responsible for securing your workloads and configuring your services (such as compute, network, storage, and database) securely. In a fully isolated, single-tenant, bare metal server with no Oracle software on it, your responsibility increases as you bring the entire software stack (operating systems and above) on which you deploy your applications. In this environment, you are responsible for securing your workloads, and configuring your services (compute, network, storage, database) securely, and ensuring that the software components that you run on the bare metal servers are configured, deployed, and managed securely. The responsibilities can be divided as: Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm

- **Identity and Access Management (IAM):** As with all Oracle cloud services, you should protect your cloud access credentials and set up individual user accounts. You are responsible for managing and reviewing access for your own employee accounts and for all activities that occur under your tenancy. Oracle is responsible for providing effective IAM services such as identity management, authentication, authorization, and auditing.
- **Workload Security:** You are responsible for protecting and securing the operating system and application layers of your compute instances from attacks and compromises. This protection includes patching applications and operating systems, operating system configuration, and protection against malware and network attacks. Oracle is responsible for providing secure images that are hardened and have the latest patches. Also, Oracle makes it simple for you to bring the same third-party security solutions that you use today.
- **Data Classification and Compliance:** You are responsible for correctly classifying and labeling your data and meeting any compliance obligations. Also, you are responsible for auditing your solutions to ensure that they meet your compliance obligations.
- **Host Infrastructure Security:** You are responsible for securely configuring and managing your compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform (database configuration) services. Oracle has a shared responsibility with you to ensure that the service is optimally configured and secured. This responsibility includes hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices.
- **Network Security:** You are responsible for securely configuring network elements such as virtual networking, load balancing, DNS, and gateways. Oracle is responsible for providing a secure network infrastructure.
- **Client and Endpoint Protection:** Your enterprise uses various hardware and software systems, such as mobile devices and browsers, to access your cloud resources. You are responsible for securing all clients and endpoints that you allow to access Oracle Cloud Infrastructure services.

---

**QUESTION 4**

Your company has deployed a business critical application in Oracle Cloud Infrastructure. What should you

do to ensure that your application has the highest level of resilience and availability?

A. Deploy the application across multiple Availability Domains and Subnets

B. Deploy the application across multiple Virtual Cloud Networks

C. Deploy the application across multiple Regions and Availability Domains

D. Deploy the application across multiple Availability Domains and Fault Domains

Correct Answer: C

To design a high availability architecture, three key elements should be considered-- redundancy, monitoring, and failover: 1) Redundancy means that multiple components can perform the same task. The problem of a single point of failure is eliminated because redundant components can take over a task performed by a component that has failed. 2) Monitoring means checking whether or not a component is working properly. 3) Failover is the process by which a secondary component becomes primary when the primary component fails. The best practices introduced here focus on these three key elements. Although high availability can be achieved at many different levels, including the application level and the cloud infrastructure level, here we will focus on the cloud infrastructure level. An Oracle Cloud Infrastructure region is a localized geographic area composed of one or more availability domains, each composed of three fault domains. High availability is ensured by a redundancy of fault domains within the availability domains. An availability domain is one or more data centers located within a region. Availability domains are isolated from each other, fault tolerant, and unlikely to fail simultaneously. Because availability domains do not share physical infrastructure, such as power or cooling, or the internal availability domain network, a failure that impacts one availability domain is unlikely to impact the availability of others. A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains let you distribute your instances so that they are not on the same physical hardware within a single availability domain. As a result, an unexpected hardware failure or a Compute hardware maintenance that affects one fault domain does not affect instances in other fault domains. You can optionally specify the fault domain for a new instance at launch time, or you can let the system select one for you. All the availability domains in a region are connected to each other by a low-latency, high bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability and disaster recovery. Reference: https://docs.oracle.com/en/solutions/design-ha/index.html#GUID-76ECDDB4-4CB1-4D93-9A6DA8B620F72369

---

**QUESTION 5**

You are analyzing your Oracle Cloud Infrastructure (OCI) usage with Cost Analysis tool in the OCI console. Which of the following is NOT a default feature of the tool?

A. Filter costs by applications

B. Filter costs by tags

C. Filter costs by compartments

D. Filter costs by date

Correct Answer: A

Cost Analysis is an easy-to-use visualization tool to help you track and optimize your Oracle Cloud Infrastructure spending, allows you to generate charts, and download accurate, reliable tabular reports of aggregated cost data on your Oracle Cloud Infrastructure consumption. Use the tool for spot checks of spending trends and for generating reports

| | |
|---|---|
| Filters | Allows filtering on the following:<br>• Availability Domain<br>• Compartment<br>**Note**<br>Filtering by compartment displays usage and costs attributed to all resources in the selected compartments, and their child compartments.<br>◦ By OCID<br>◦ By Name<br>◦ By Path (for example, root/compartmentname /compartmentname)<br>• Platform (Gen-1 are services which are not OCI native. Gen-2 includes all OCI native services)<br>• Tag<br>◦ By Tag Namespace<br>◦ By TagKey + Value<br>• Region<br>• Service<br>• Product description (the human-readable corresponding name) |


Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Billing/Concepts/costanalysisoverview.htm

---

**QUESTION 6**

A new customer has logged into Oracle Cloud Infrastructure (OCI) as an administrator for the first time. The admin would like to deploy Infrastructure into a region other then their home region. What is the first Stop they must take in order to accomplish this task?

A. Use API endpoints to create resources in the desired region.

B. Navigate to the desired region and begin creating resources.

C. Subscribe to the desired region.

D. File a service request for access to each additional region.

Correct Answer: C

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your home region. Your home region is where your IAM resources are defined. When you subscribe to another region, your IAM resources are available in the new region, however, the master definitions reside in your home region and can only be changed there. When you subscribe your tenancy to a new region, all the policies from your home region are enforced in the new region. If you want to limit access for groups of users to specific regions, you can write policies to grant access to specific regions only. Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingregions.htm

To create an instance in another region, perform these preliminary steps:

1.

Extend your subscription to another region.

2.

Federate Oracle Identity Cloud Service (IDCS) from the new region with Oracle Cloud Infrastructure

(OCI).

Also, when you purchase these services or sign up for a free promotion, you typically choose the data

region closest to your location to access them. This becomes your primary data region. However, if

required, you can extend your subscription to other geographical regions (within the same cloud account)

and use the services there.

Reference:

https://docs.oracle.com/en/cloud/paas/content-cloud/administer/create-instance-oracle-cloud- console.html

---

**QUESTION 7**

Which capability enables you to search, purchase, and start using software in your Oracle Cloud Infrastructure (OCI) tenancy?

A. OCI Marketplace

B. OCI OS Management

C. OCI Resource Manager

D. OCI Registry

Correct Answer: A

Oracle Cloud Infrastructure Marketplace is an online store that offers solutions specifically for customers of Oracle Cloud Infrastructure. In the Oracle Cloud Infrastructure Marketplace catalog, you can find listings for two types of solutions from Oracle and trusted partners: images and stacks. These listing types include different categories of applications. Also, some listings are free and others require payment. Images are templates of virtual hard drives that determine the operating system and software to run on an instance. You can deploy image listings on an Oracle Cloud Infrastructure Compute instance. Marketplace also offers stack listings. Stacks represent definitions of groups of Oracle Cloud Infrastructure resources that you can act on as a group. Each stack has a configuration consisting of one or more declarative configuration files. With an image or a stack, you have a customized, more streamlined way of getting started with a publisher\\'s software.

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Marketplace/Concepts/marketoverview.htm

---

**QUESTION 8**

A company has developed an eCommerce web application In Oracle Cloud Infrastructure. What should they do to ensure that the application has the highest level of resilience?

A. Deploy the application across multiple Regions and Availability Domains.

B. Deploy the application across multiple Availability Domains and subnet.

C. Deploy the application across multiple Virtual Cloud Networks.

D. Deploy the application across multiple Availability Domains and Fault Domains.

Correct Answer: A

For highest level of resilience you can deploy the application between regions and distribute on availability domain and fault domains.

Reference: https://www.oracle.com/cloud/iaas/faq.html

---

**QUESTION 9**

Which three components are part of Oracle Cloud Infrastructure (OCI) identity and access management service?

A. Regional Subnets

B. Policies

C. Users

D. Compute Instances

E. Dynamic Groups

F. Roles

G. Virtual Cloud Networks

Correct Answer: BCE

Components of IAM IAM uses the components described in this section. To better understand how the components fit together, see Example Scenario. RESOURCE The cloud objects that your company\\'s employees create and use when interacting with Oracle Cloud Infrastructure. For example: compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, route tables, etc. USER An individual employee or system that needs to manage or use your company\\'s Oracle Cloud Infrastructure resources. Users might need to launch instances, manage remote disks, work with your virtual cloud network, etc. End users of your application are not typically IAM users. Users have one or more IAM credentials (see User Credentials). GROUP A collection of users who all need the same type of access to a particular set of resources or compartment. DYNAMIC GROUP A special type of group that contains resources (such as compute instances) that match rules that you define (thus the membership can change dynamically as matching resources are created or deleted). These instances act as "principal" actors and can make API calls to services according to policies that you write for the dynamic group. NETWORK SOURCE A group of IP addresses that are allowed to access resources in your tenancy. The IP addresses can be public IP addresses or IP addresses from a VCN within your tenancy. After you create the network source, you use policy to restrict access to only requests that originate from the IPs in the network source. COMPARTMENT A collection of related resources. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources. You use them to clearly separate resources for the purposes of measuring usage and billing, access (through the use of policies), and isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of your organization. For more information, see Setting Up Your Tenancy. TENANCY The root compartment that contains all of your organization\\'s Oracle Cloud Infrastructure resources. Oracle automatically creates your company\\'s tenancy for you. Directly within the tenancy are your IAM entities (users, groups, compartments, and some policies; you can also put policies into compartments inside the tenancy). You place the other types of cloud resources (e.g., instances, virtual networks, block storage volumes, etc.) inside the compartments that you create. POLICY A document that specifies who can access which resources, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. For more information, see Example Scenario and How Policies Work. The word "policy" is used by people in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources. HOME REGION The region where your IAM resources reside. All IAM resources are global and available across all regions, but the master set of definitions reside in a single region, the home region. You must make changes to your IAM resources in your home region. The changes will be automatically propagated to all regions. For more information, see Managing Regions. FEDERATION A relationship that an administrator configures between an identity provider and a service provider. When you federate Oracle Cloud Infrastructure with an identity provider, you manage users and groups in the identity provider. You manage authorization in Oracle Cloud Infrastructure\\'s IAM service. Oracle Cloud Infrastructure tenancies are federated with Oracle Identity Cloud Service by default.

https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

---

**QUESTION 10**

What do the terms OpEx and CapEx refer to?

A. OpEx refers to Operational Excellence and CapEx refers to Capital Excellence

B. OpEx refers to Operational Expenditure and CapEx refers to Capital Expenditure

C. OpEx refers to Operational Expansion and CapEx refers to Capital Expenses

D. OpEx refers to Operational Example and CapEx refers to Capita Example

Correct Answer: B

CapEx is Capital expenditures comprise major purchases that will be used in the future. OpEx Operating expenditures (expenses) represent day-to-day costs that are necessary to keep a business running.

Reference: https://www.10thmagnitude.com/opex-vs-capex-the-real-cloud-computing-cost-advantage/

---

**QUESTION 11**

Which feature allows you to group and logically isolate your Oracle Cloud Infrastructure (OCI) resources?

A. Tenancy

B. Identity and Access Management Groups

C. Availability Domains

D. Compartments

Correct Answer: D

It is collection of related resources. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources. You use them to clearly separate resources for the purposes of measuring usage and billing, access (through the use of IAM Service policies), and isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of your organization. For more information, see Overview of the IAM Service and also Setting Up Your Tenancy. To place a resource in a compartment, simply specify the compartment ID in the "Create" request object when initially creating the resource. For example, to launch an instance into a particular compartment, specify that compartment\\'s OCID in the LaunchInstance request. You can\\'t move an existing resource from one compartment to another. To use any of the API operations, you must be authorized in an IAM policy. If you\\'re not authorized, talk to an administrator. If you\\'re an administrator who needs to write policies to give users access, see Getting Started with Policies. Reference: https://docs.cloud.oracle.com/en-us/iaas/tools/ocicli/2.9.9/oci_cli_docs/cmdref/iam/compartment.html

---

**QUESTION 12**

According to Shared security model, which two are a customer\\'s responsibilities in Oracle Cloud Infrastructure (OCI)?

A. Physical security of OCI data center facilities

B. Virtual Machine hypervisor

C. Local NVMe data persistence

D. Customer data

E. Object Storage data durability

Correct Answer: DE

Customer and Oracle\\'s responsibilities can be divided into the following areas: Physical Security: Oracle is responsible for protecting the global infrastructure that runs all of the services offered in Oracle Cloud Infrastructure. This infrastructure consists of the hardware, software, networking, and facilities that run Oracle Cloud Infrastructure services. Identity and Access Management (IAM): As with all Oracle cloud services, you should protect your cloud access credentials and set up individual user accounts. You are responsible for managing and reviewing access for your own employee accounts and for all activities that occur under your tenancy. Oracle is responsible for providing effective IAM services such as identity management, authentication, authorization, and auditing. Workload Security: You are responsible for protecting and securing the operating system and application layers of your compute instances from attacks and compromises. This protection includes patching applications and operating systems, operating system configuration, and protection against malware and network attacks. Oracle is responsible for providing secure images that are hardened and have the latest patches. Also, Oracle makes it simple for you to bring the same third-party security solutions that you use today. Data Classification and Compliance: You are responsible for correctly classifying and labeling your data and meeting any compliance obligations. Also, you are responsible for auditing your solutions to ensure that they meet your compliance obligations. Host Infrastructure Security: You are responsible for securely configuring and managing your compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform (database configuration) services. Oracle has a shared responsibility with you to ensure that the service is optimally configured and secured. This responsibility includes hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices. Network Security: You are responsible for securely configuring network elements such as virtual networking, load balancing, DNS, and gateways. Oracle is responsible for providing a secure network infrastructure. Client and Endpoint Protection: Your enterprise uses various hardware and software systems, such as mobile devices and browsers, to access your cloud resources. You are responsible for securing all clients and endpoints that you allow to access Oracle Cloud Infrastructure services.

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm