1Z0-1085-22 Q&As

Oracle Cloud Infrastructure 2022 Foundations Associate

Pass Oracle 1Z0-1085-22 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/1z0-1085-22.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Oracle Official Exam Center

QUESTION 1

What does compute instance horizonal scaling mean?

A. stopping/starting the instance

B. backing up data to object storage

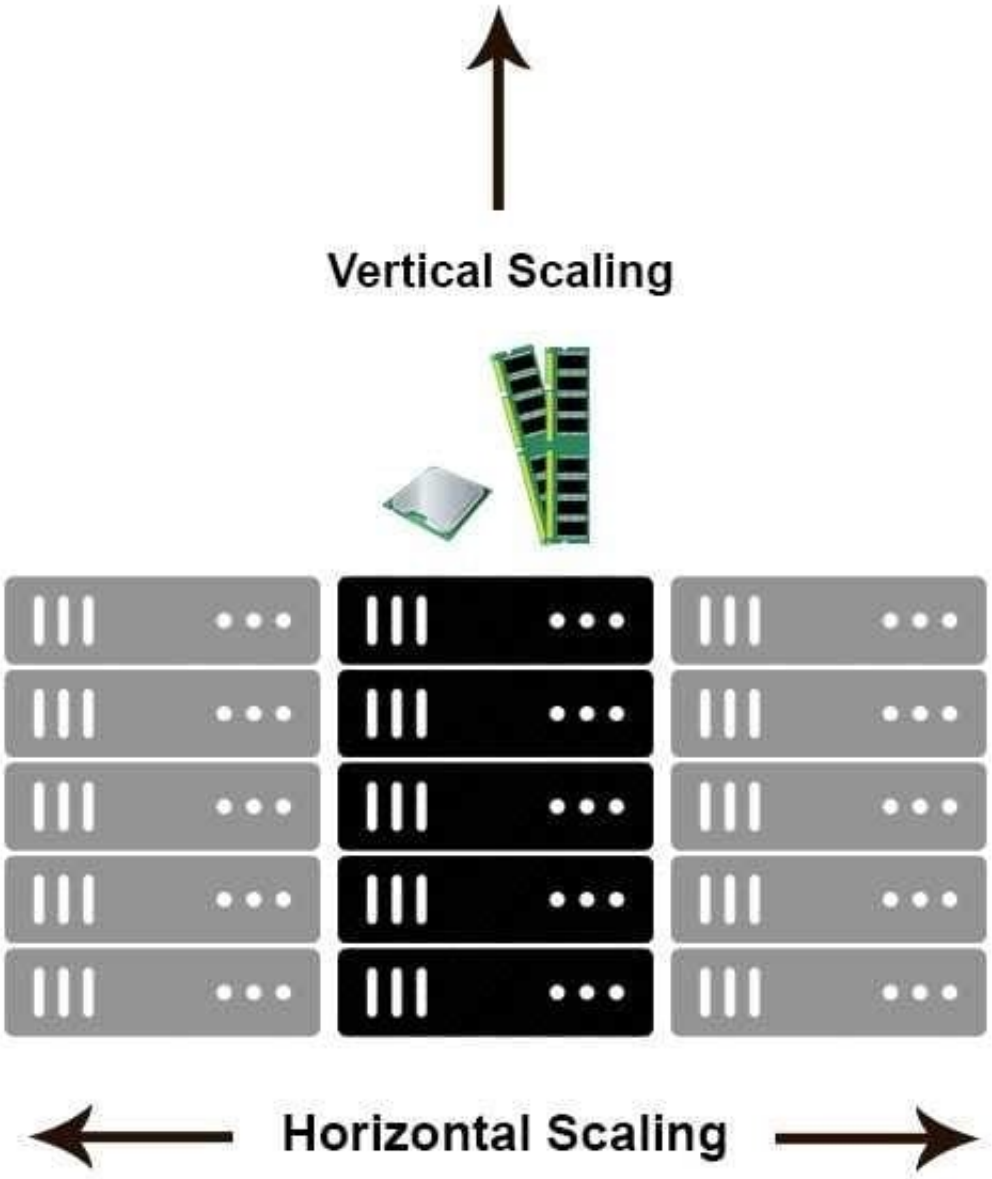
C. adding additional compute instances

D. changing compute instance size

Correct Answer: C

Cloud Horizontal Scaling refers to provisioning additional servers to meet your needs, often splitting workloads between servers to limit the number of requests any individual server is getting. In a cloud-based environment, this would mean adding additional instances instead of moving to a larger instance size. Cloud Vertical Scaling refers to adding more CPU or memory to an existing server, or replacing one server with a more powerful server.

Reference: https://cloudcheckr.com/cloud-cost-management/cloud-vs-data-center-what-is-scalability-in-cloudcomputing/ Horizontal scaling means that you scale by adding more machines into your pool of resources whereas Vertical scaling means that you scale by adding more power (CPU, RAM) to an existing machine. An easy way to remember this is to think of a machine on a server rack, we add more machines across the horizontal direction and add more resources to a machine in the vertical direction.



With horizontal-scaling it is often easier to scale dynamically by adding more machines into the existing pool -- Vertical-scaling is often limited to the capacity of a single machine, scaling beyond that capacity often involves downtime and comes with an upper limit. Reference: https://medium.com/@abhinavkorpal/scaling-horizontally-and-vertically-for-databases- a2aef778610c

QUESTION 2

Which statement below is not true for Oracle Cloud infrastructure Compartments?

A. Resources can be moved from one compartment to another

B. Compartments cannot be nested

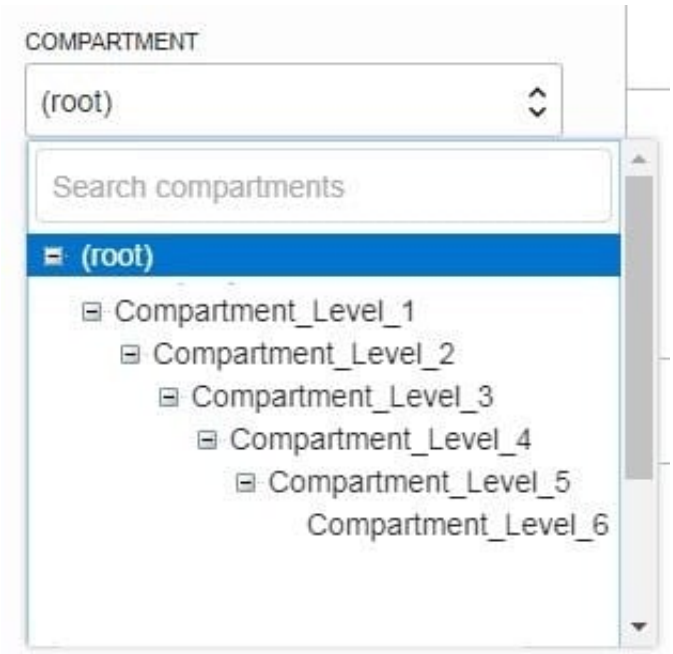
C. Each OCI resource belongs to a single compartment

D. Resources and compartments can be added and deleted anytime

Correct Answer: B

When creating a compartment, you must provide a name for it (maximum 100 characters, including letters, numbers, periods, hyphens, and underscores) that is unique within its parent compartment. You must also provide a description, which is a non-unique, changeable description for the compartment, from 1 through 400 characters. Oracle will also assign the compartment a unique ID called an Oracle Cloud ID. You can create subcompartments in compartments to create hierarchies that are six levels deep.

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm When you first start working with Oracle Cloud Infrastructure, you need to think carefully about how you want to use compartments to organize and isolate your cloud resources. Compartments are fundamental to that process. Most resources can be moved between compartments. However, it\\'s important to think through your compartment design for your organization up front, before implementing anything. For more information, see Setting Up Your Tenancy. The Console is designed to display your resources by compartment within the current region. When you work with your resources in the Console, you must choose which compartment to work in from a list on the page. That list is filtered to show only the compartments in the tenancy that you have permission to access. If you\\'re an administrator, you\\'ll have permission to view all compartments and work with any compartment\\'s resources, but if you\\'re a user with limited access, you probably won\\'t. Compartments are tenancy-wide, across regions. When you create a compartment, it is available in every region that your tenancy is subscribed to. You can get a cross-region view of your resources in a specific compartment with the compartment explorer. See Viewing All Resources in a Compartment. You can create subcompartments in compartments to create hierarchies that are six levels deep.



Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

QUESTION 3

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 4

Which Oracle Cloud Infrastructure compute shapes does not incur instance billing in a STOPPED state?

A. Dense I/O

B. Standard

C. GPU

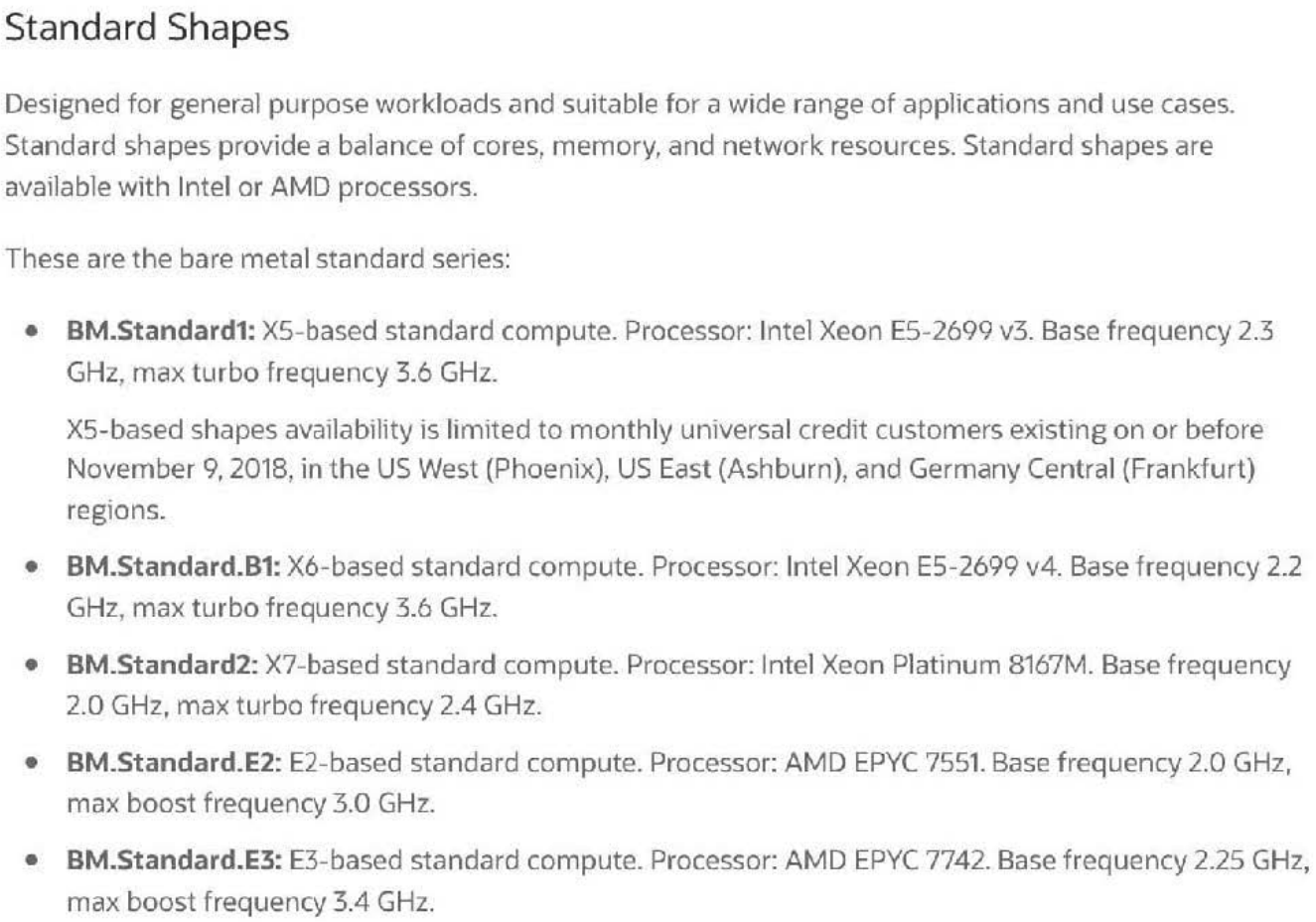
D. HPC

Correct Answer: B

A shape is a template that determines the number of CPUs, amount of memory, and other resources that

are allocated to an instance.

Standard shapes don\\'t incur costs in a STOPPED state.



Standard Shapes

Designed for general purpose workloads and suitable for a wide range of applications and use cases. Standard shapes provide a balance of cores, memory, and network resources. Standard shapes are available with Intel or AMD processors.

These are the bare metal standard series:

- **BM.Standard1:** X5-based standard compute. Processor: Intel Xeon E5-2699 v3. Base frequency 2.3 GHz, max turbo frequency 3.6 GHz.

  X5-based shapes availability is limited to monthly universal credit customers existing on or before November 9, 2018, in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.
- **BM.Standard.B1:** X6-based standard compute. Processor: Intel Xeon E5-2699 v4. Base frequency 2.2 GHz, max turbo frequency 3.6 GHz.
- **BM.Standard2:** X7-based standard compute. Processor: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.
- **BM.Standard.E2:** E2-based standard compute. Processor: AMD EPYC 7551. Base frequency 2.0 GHz, max boost frequency 3.0 GHz.
- **BM.Standard.E3:** E3-based standard compute. Processor: AMD EPYC 7742. Base frequency 2.25 GHz, max boost frequency 3.4 GHz.

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm#baremetalshapes__bm-standard

QUESTION 5

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 6

Which is a key benefit of using oracle cloud infrastructure autonomous data warehouse?

A. No username and password required

B. Scale both CPU and Storage without downtime

C. Apply database patches as they become available D. Maintain root level acress to the underlying operating system

Correct Answer: B

Oracle Autonomous Data Warehouse is a cloud data warehouse service that eliminates virtually all the complexities of operating a data warehouse and securing data. It automates provisioning, configuring, securing, tuning, scaling, patching, backing up, and repairing of the data warehouse. Unlike other "fully managed" cloud data warehouse solutions that only patch and update the service, it also features elastic, automated scaling, performance tuning, security, and a broad set of built-in capabilities that enable machine learning analysis, simple data loading, and data visualizations. Data Warehouse uses continuous query optimization, table indexing, data summaries, and auto- tuning to ensure consistent high performance even as data volume and number of users grows. Autonomous scaling can temporarily increase compute and I/O by a factor of three to maintain performance. Unlike other cloud services which require downtime to scale, Autonomous Data Warehouse scales while the service continues to run. Reference: https://www.oracle.com/autonomous-database/autonomous-data-warehouse/

QUESTION 7

Which statement is true for an oracle cloud Infrastructure (OCI) compute instance?

A. Compute instance always get a public IP address

B. Compute instance does not use a boot volume

C. Compute instance cannot leverage auto scaling feature

D. Compute instance always get a private IP address

Correct Answer: D

When you create an instance, the instance is automatically attached to a virtual network interface card (VNIC) in the cloud network\\'s subnet and given a private IP address from the subnet\\'s CIDR. You can let the IP address be automatically assigned, or you can specify a particular address of your choice. The private IP address lets instances within the cloud network communicate with each other.

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/launchinginstance.htm Instances use IP addresses for communication. Each instance has at least one private IP address and optionally one or more public IP addresses. A private IP address enables the instance to communicate with other instances inside the VCN, or with hosts in your on-premises network (via an IPSec VPN or Oracle Cloud Infrastructure FastConnect). A public IP address enables the instance to communicate with hosts on the internet. Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/managingIPaddresses.htm

QUESTION 8

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

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

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

C. You are responsible for securing all data that you place in OCI D. You are responsible for securing the hypervisor within OCI Compute service.

Correct Answer: C

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. More specifically, your and Oracle\\'s responsibilities can be divided into the following areas: 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. 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.

Reference: https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

QUESTION 9

What service is NOT available as part of Oracle Cloud Free Tier?

A. Oracle Cloud Infrastructure Monitoring

B. Oracle Cloud Infrastructure Exadata DB Systems

C. Oracle Cloud Infrastructure Autonomous Data Warehouse

D. Oracle Cloud Infrastructure Compute

Correct Answer: B

For more information on Oracle Cloud Infrastructure Free Tier refer below official documentation https://docs.cloud.oracle.com/en-us/iaas/Content/FreeTier/freetier.htm?Highlight=Free%20Tier Exadata DB Systems aren\\'t a part of the free tier: Reference: https://www.oracle.com/in/cloud/free/

QUESTION 10

What is Oracle\\'s responsibility according to the Oracle Cloud Infrastructure (OCI) shared-security model?

A. Configuring OCI services securely

B. Data classification and compliance

C. Securing application workloads

D. Security of data center facilities

Correct Answer: D

Oracle\\'s mission is to build cloud infrastructure and platform services for your business to have effective and manageable security to run your mission-critical workloads and store your data with confidence. 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. More specifically, your and Oracle\\'s responsibilities can be divided into the following areas:

- **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.

- **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.
- **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.

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

QUESTION 11

Which statement is correct regarding the oracle cloud infrastructure Compute services?

A. When you stop a compute instance, all data on the boot volume is lost

B. You can attach a maximum of one public to each compute instance

C. You can launch either virtual machines or bare metal instances

D. You cannot attach a block volume to a compute instance

Correct Answer: C

Oracle Cloud Infrastructure Compute lets you provision and manage compute hosts, known as instances You can launch instances as needed to meet your compute and application requirements. After you launch an instance, you can access it securely from your computer, restart it, attach and detach volumes, and terminate it when you\\'re done with it. Any changes made to the instance\\'s local drives are lost when you terminate it. Any saved changes to volumes attached to the instance are retained. Oracle Cloud Infrastructure offers both bare metal and virtual machine instances: 1) Bare Metal: A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation. 2) Virtual Machine: A virtual machine (VM) is an independent computing environment that runs on top of physical bare metal hardware. The virtualization makes it possible to run multiple VMs that are isolated from each other. VMs are ideal for running applications that do not require the performance and resources (CPU, memory, network bandwidth, storage) of an entire physical machine. An Oracle Cloud Infrastructure VM compute instance runs on the same hardware as a bare metal instance, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure. Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Concepts/computeoverview.htm

QUESTION 12

Which OCI Identity and access management capability helps you to organize multiple users into teams?

A. Policies

B. Groups

C. Dynamic Groups

D. Users

Correct Answer: B

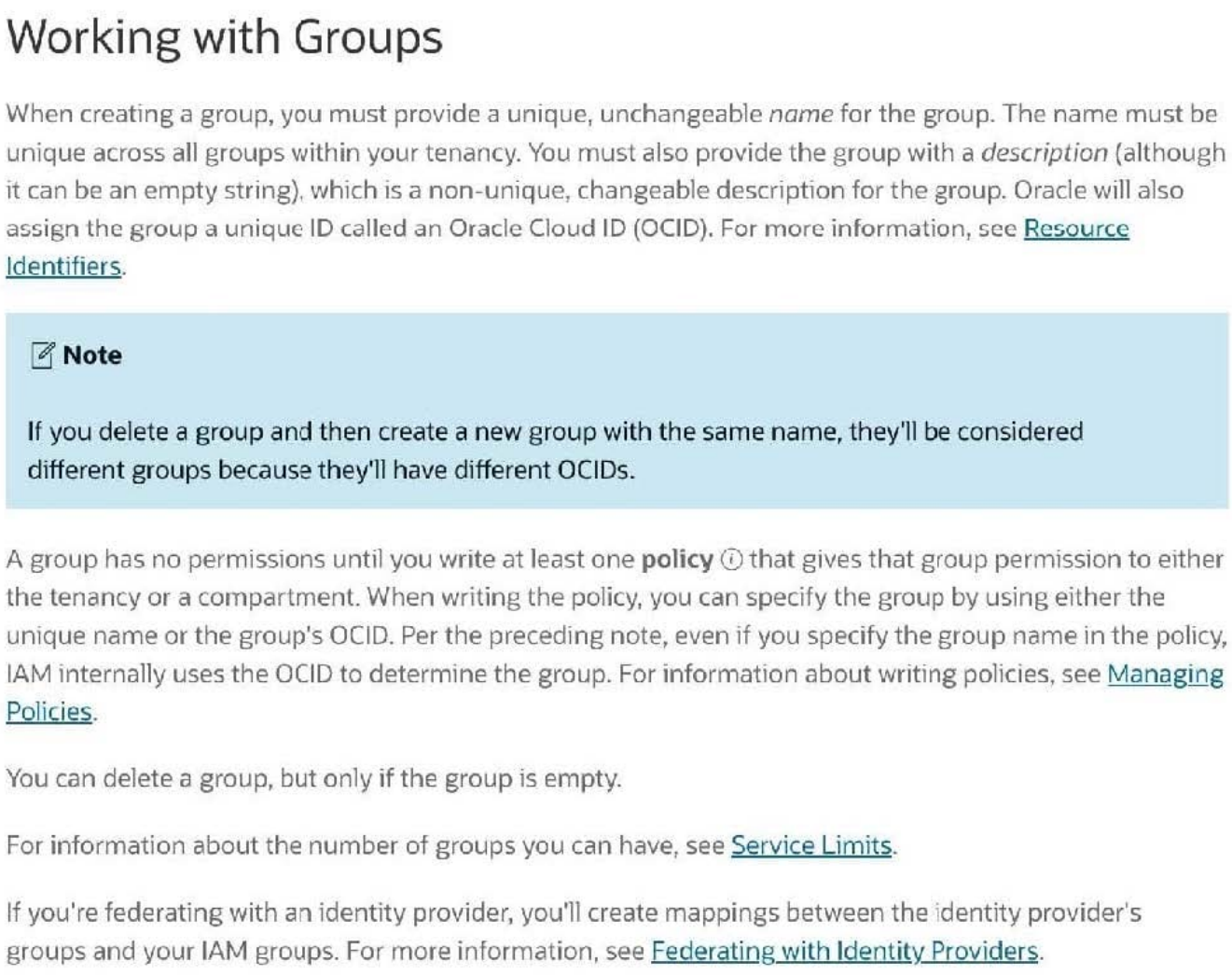
IAM Group is A collection of users who all need the same type of access to a particular set of resources or compartment.

IAM DYNAMIC GROUP is 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.

Reference:

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

A collection of users who all need the same type of access to a particular set of resources or compartment.



Working with Groups

When creating a group, you must provide a unique, unchangeable *name* for the group. The name must be unique across all groups within your tenancy. You must also provide the group with a *description* (although it can be an empty string), which is a non-unique, changeable description for the group. Oracle will also assign the group a unique ID called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

Note

If you delete a group and then create a new group with the same name, they'll be considered different groups because they'll have different OCIDs.

A group has no permissions until you write at least one **policy** that gives that group permission to either the tenancy or a compartment. When writing the policy, you can specify the group by using either the unique name or the group's OCID. Per the preceding note, even if you specify the group name in the policy, IAM internally uses the OCID to determine the group. For information about writing policies, see Managing Policies.

You can delete a group, but only if the group is empty.

For information about the number of groups you can have, see Service Limits.

If you're federating with an identity provider, you'll create mappings between the identity provider's groups and your IAM groups. For more information, see Federating with Identity Providers.

Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managinggroups.htm

QUESTION 13

Which Oracle Cloud Infrastructure service can you use to assess user security of your Oracle databases?

A. Oracle Data Safe

B. Oracle Data Guard

C. Audit Vault and Database Firewall option for Oracle Database Enterprise Edition

D. Audit Service

Correct Answer: A

Oracle Data Safe is a unified control center for your Oracle databases which helps you understand the sensitivity of your data, evaluate risks to data, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, and address data security compliance requirements.

Whether you\\'re using an Autonomous Database or an Oracle DB system, Oracle Data Safe delivers

essential data security capabilities as a service on Oracle Cloud Infrastructure.

Reference:

https://docs.cloud.oracle.com/en-us/iaas/data-safe/doc/oracle-data-safe-overview.html

QUESTION 14

Which describes a key benefit of using Oracle Cloud Infrastructure (OCI)?

A. With OCI, you can only run Java based workloads on bare metal.

B. With OCI, you can run only cloud-native workloads.

C. Only bare metal workloads are supported on OCI.

D. OCI offers consistent performance with a predictable pricing model.

Correct Answer: D

https://www.oracle.com/in/cloud/pricing.html

-

OCI offers consistent performance with a predictable pricing model - is the best suited answer.

-

Only bare metal workloads are supported in OCI - False, since you can work with VMs etc too

-

With OCI, you can run cloud native workloads - False, since you can work with on-premise by connecting it to OCI too.

-

With OCI, you can only run Java based workloads on bare metal - False since Java is not the only programming language supported by OCI.

QUESTION 15

What two statements regarding the Virtual Cloud Network (VCN) are true?

A. A single VCN can contain both private and public Subnets.

B. VCN is a regional resource that span across all the Availability Domains in a Region.

C. You can only create one VCN per region.

D. The VCN is the IPSec-based connection with a remote on premises location.

E. VCN is a global resource that span across all the Regions

Correct Answer: AB

When you work with Oracle Cloud Infrastructure, one of the first steps is to set up a virtual cloud network (VCN) for your cloud resources. VIRTUAL CLOUD NETWORK (VCN) : A virtual, private network that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use. A VCN resides in a single Oracle Cloud Infrastructure region and covers a single, contiguous IPv4 CIDR block of your choice. See Allowed VCN Size and Address Ranges. The terms virtual cloud network, VCN, and cloud network are used interchangeably in this documentation. For more information, see VCNs and Subnets. SUBNETS : Subdivisions you define in a VCN (for example, 10.0.0.0/24 and 10.0.1.0/24). Subnets contain virtual network interface cards (VNICs), which attach to instances. Each subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. You can designate a subnet to exist either in a single availability domainavailability domain or across an entire region (regional subnets are recommended). Subnets act as a unit of configuration within the VCN: All VNICs in a given subnet use the same route table, security lists, and DHCP options (see the definitions that follow). You can designate a subnet as either public or private when you create it. Private means VNICs in the subnet can\\'t have public IP addresses. Public means VNICs in the subnet can have public IP addresses at your discretion. See Access to the Internet.

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