1Z0-1085-20 Q&As

Oracle Cloud Infrastructure Foundations 2020 Associate

Pass Oracle 1Z0-1085-20 Exam with 100% Guarantee

QUESTION 1

Which three components are part of Oracle Cloud Infrastructure Identity and Access Management service?

A. Virtual Cloud Networks

B. Policies

C. Regional Subnets

D. Dynamic Groups

E. Roles

F. Compute Instances

G. Users

Correct Answer: BDG

IAM components are 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). 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. 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. 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. Reference:

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

QUESTION 2

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

A. Tenancy

B. Identity and Access Management Groups

C. Compartments

D. Availability Domain

Correct Answer: C

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.

User Group can use some resources in the compartment like network resources also they can\\'t create it

depend on the policy that assigned Remember, a compartment is a logical grouping, not a physical one

Reference:

https://docs.cloud.oracle.com/en-us/iaas/tools/oci-cli/2.9.8/oci_cli_docs/cmdref/iam/compartment.html

QUESTION 3

Which resource do you manage in an Infrastructure-as-a-services (IAAS) offering?

A. Operating system

B. Network

C. Storage

D. Servers

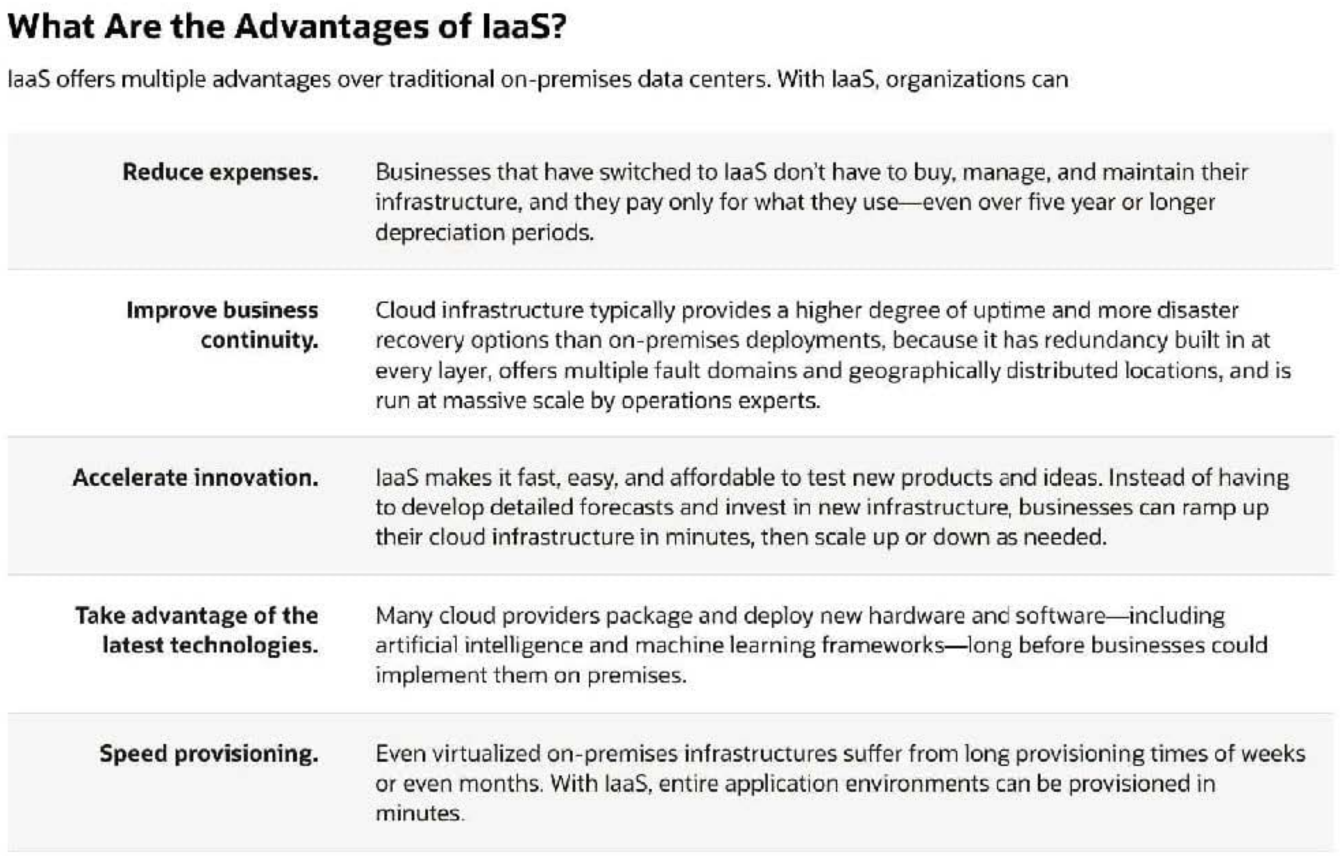
Correct Answer: A

Infrastructure as a service (IaaS) is a type of cloud service model in which computing resources are hosted in the cloud. Businesses can use the IaaS model to shift some or all of their use of on- premises or colocated data center infrastructure to the cloud, where it is owned and managed by a cloud provider. These infrastructure elements can include compute, network, and storage hardware as well as other components and software.

How Does IaaS Work?

In a typical IaaS model, a business--which can be of any size--consumes services like compute, storage, and databases from a cloud provider. The cloud provider offers those services by hosting hardware and software in the cloud. The business will no longer need to purchase and manage its own equipment, or space to host the equipment, and the cost will shift to a pay-as-you-go model.

When the business needs less, it pays for less. And when it grows, it can provision additional computing resources and other technologies in minutes.



What Are the Advantages of IaaS?

IaaS offers multiple advantages over traditional on-premises data centers. With IaaS, organizations can

Reduce expenses.	Businesses that have switched to IaaS don't have to buy, manage, and maintain their infrastructure, and they pay only for what they use—even over five year or longer depreciation periods.
Improve business continuity.	Cloud infrastructure typically provides a higher degree of uptime and more disaster recovery options than on-premises deployments, because it has redundancy built in at every layer, offers multiple fault domains and geographically distributed locations, and is run at massive scale by operations experts.
Accelerate innovation.	IaaS makes it fast, easy, and affordable to test new products and ideas. Instead of having to develop detailed forecasts and invest in new infrastructure, businesses can ramp up their cloud infrastructure in minutes, then scale up or down as needed.
Take advantage of the latest technologies.	Many cloud providers package and deploy new hardware and software—including artificial intelligence and machine learning frameworks—long before businesses could implement them on premises.
Speed provisioning.	Even virtualized on-premises infrastructures suffer from long provisioning times of weeks or even months. With IaaS, entire application environments can be provisioned in minutes.

Reference: https://www.oracle.com/in/cloud/what-is-iaas/

QUESTION 4

Which capability can be used to protect against unexpected hardware or power supply failures within an availability domain?

A. Fault Domains

B. Compartments

C. Top of Rack Switches

D. Power Distribution Units

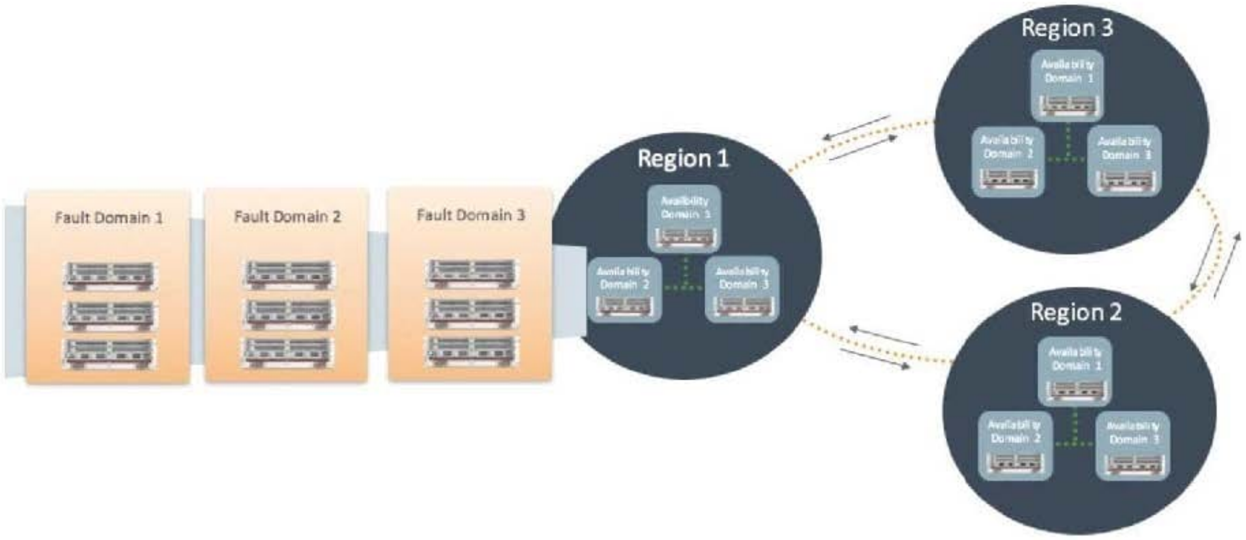
Correct Answer: A

A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains provide anti-affinity: they let you distribute your instances so that the instances are not on the same physical hardware within a single availability domain. A hardware failure or Compute hardware maintenance event that affects one fault domain does not affect instances in other fault domains. In addition, the physical hardware in a fault domain has independent and redundant power supplies, which prevents a failure in the power supply hardware within one fault domain from affecting other fault domains.

Usually fault domains to do the following things:

1) Protect against unexpected hardware failures or power supply failures.

2) Protect against planned outages because of Compute hardware maintenance.



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

QUESTION 5

Which of the following services can you control access to via IAM?

A. Networking components

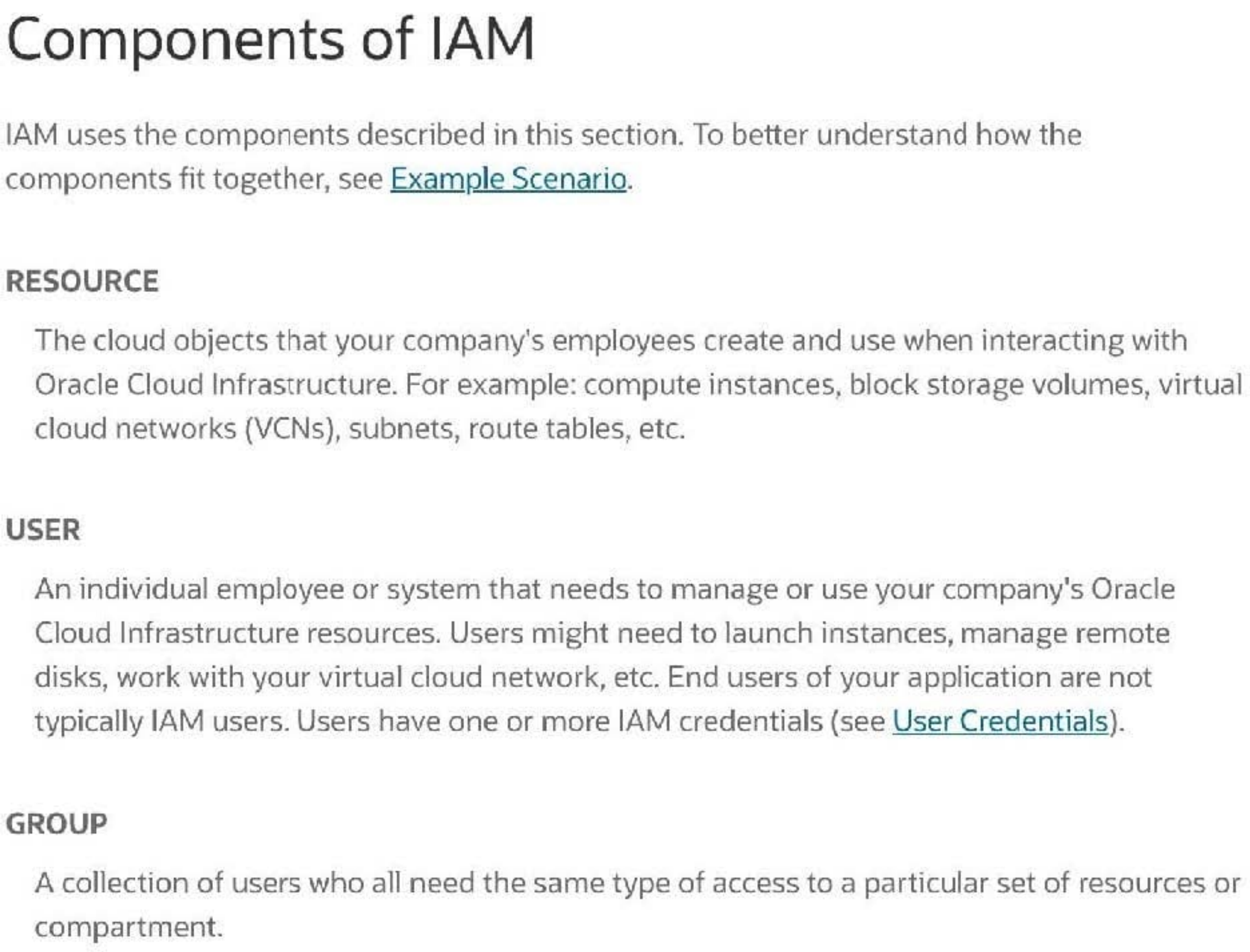
B. Compute Instances

C. All services including IAM

D. DB systems

Correct Answer: C

Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who has access to your cloud resources. You can control what type of access a group of users have and to which specific resources. This section gives you an overview of IAM components and an example scenario to help you understand how they work together.



Components of IAM

IAM uses the components described in this section. To better understand how the components fit together, see Example Scenario.

RESOURCE

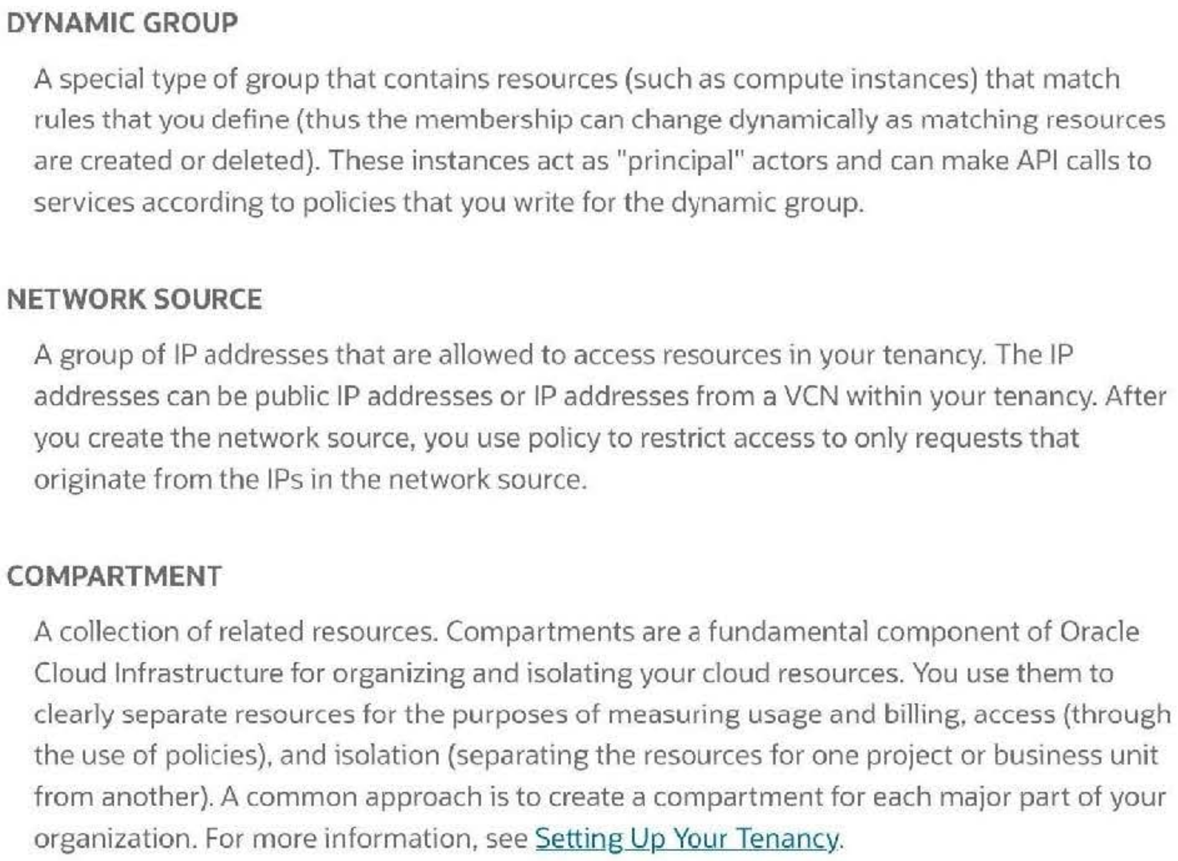
The cloud objects that your company's employees create and use when interacting with Oracle Cloud Infrastructure. For example: compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, route tables, etc.

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

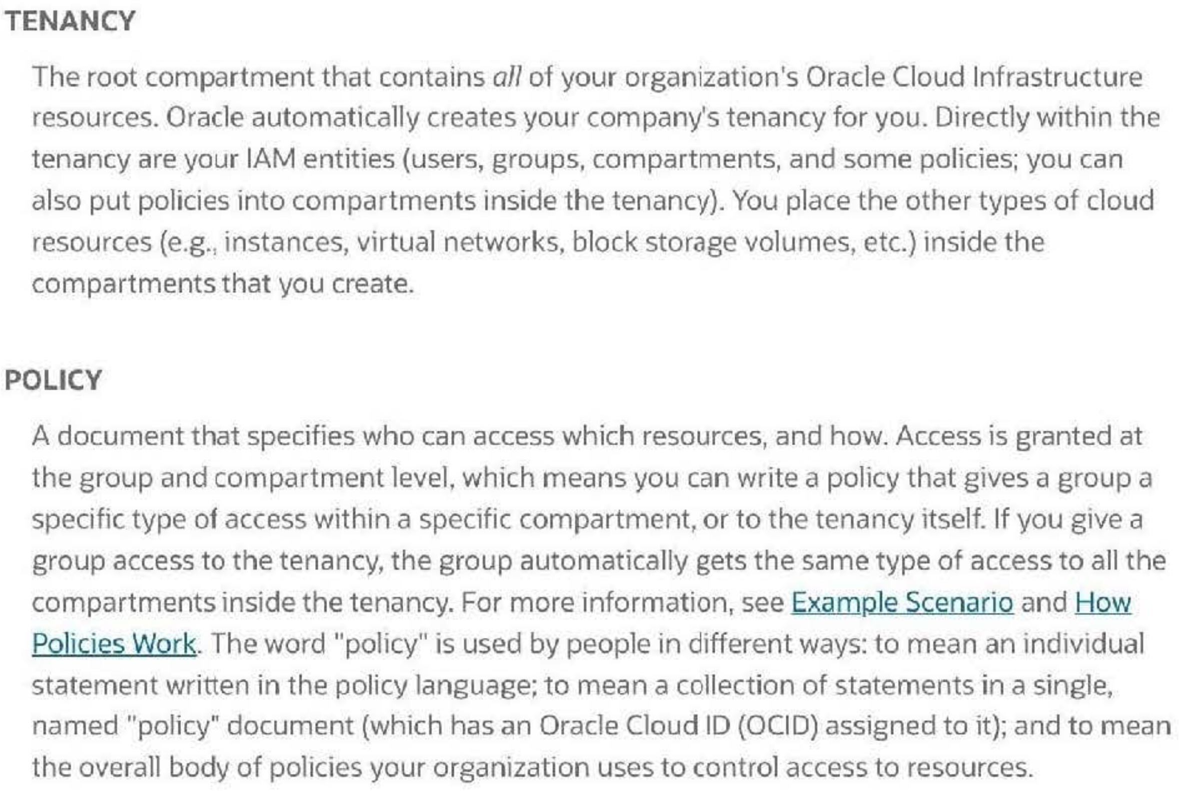
A special type of group that contains resources (such as compute instances) that match rules that you define (thus the membership can change dynamically as matching resources are created or deleted). These instances act as "principal" actors and can make API calls to services according to policies that 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.

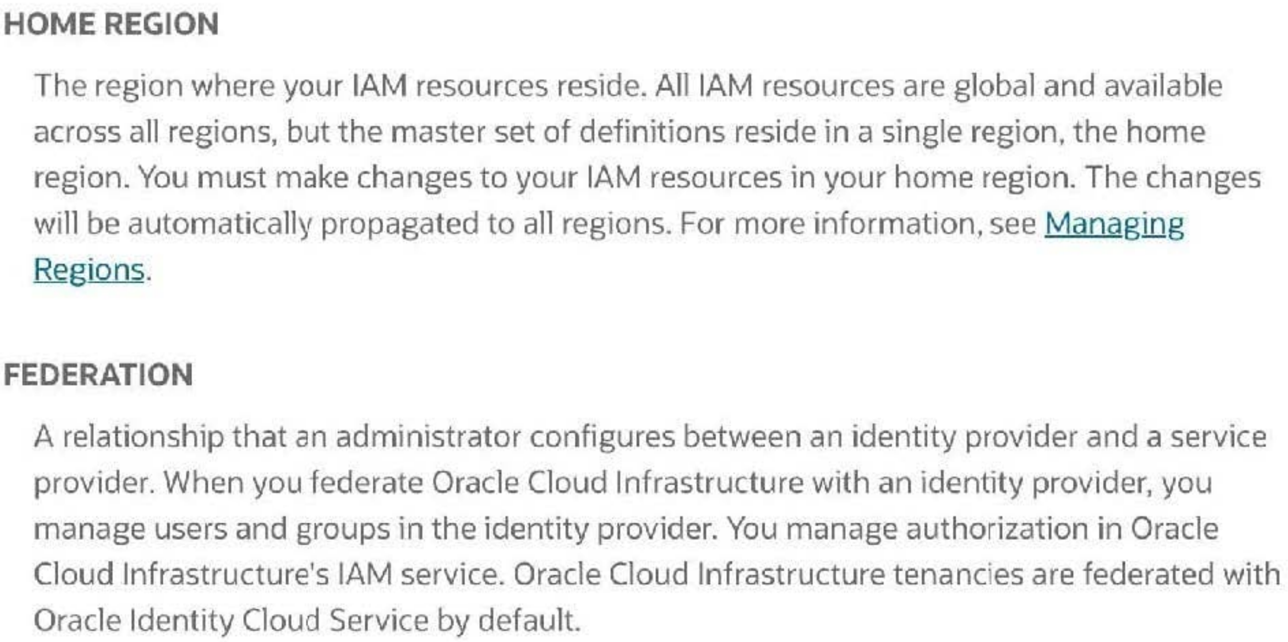


TENANCY

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.

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