1Z0-1085-22$^{\text{Q\&As}}$

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.passapply.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

Which two should be considered when designing a fault tolerant solution in Oracle Cloud Infrastructure (OCI)?

A. ensuring your solution components are distributed across OCI Fault Domains

B. performing data integrity check when using OCI File Storage Service

C. writing custom scripts that will monitor your solution

D. using multiple OCI Availability Domains (AD), where available, to deploy your solution

E. creating a manual cluster of compute instances

Correct Answer: AD

Creating a manual cluster of compute instances, and Writing custom scripts that will monitor your solution are not valid ways to ensure fault tolerance at all. Also, Performing Data Integrity check when using OCI File Storage Service is not valid since OCI takes care of it. Therefore, we are left with: 1) Using multiple OCI Availibility Domains (AD), where available, to deploy your solution - Which is excellent because we have multiple AD\\'s so that if one fails, we have a backup AD! 2) Ensuring your solution components are distributed across OCI Fault Domains - So that we can protect our deployment against unexpected power failures, AD failure etc. Reference: https://blogs.oracle.com/cloud-infrastructure/using-availibility-domains-and-fault-domains-to- improveapplication-resiliency

QUESTION 2

What does Oracle\\'s Payment Card Industry Data Security Standard (PCI DSS) attestation of compliance provide to customers?

A. Customers can use these services for workloads that provides validation of card holder transaction but only as 3rd party

B. Customers can use these services for workloads that process, or transmit cardholder data but not store it.

C. Customers can use these services for workloads to process applications for credit card approval securely.

D. Customers can use these services for workloads that store, process, or transmit cardholder data.

Correct Answer: D

The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security standard designed to encourage and enhance cardholder data security and promote the adoption of consistent data security measures around the technical and operational components related to cardholder data. Oracle has successfully completed a Payment Card Industry Data Security Standard (PCI DSS) audit and received an Attestation of Compliance (AoC) covering several Oracle Cloud Infrastructure services and the Oracle RightNow Service Cloud Service. As a PCI Level 1 Service Provider, customers can now use these services for workloads that store, process or transmit cardholder data.

Reference: https://www.oracle.com/cloud/cloud-infrastructure-compliance/

QUESTION 3

You run 5 Oracle Cloud Infrastructure (OCI) Virtual Machine instances on an OCI dedicated virtual host. How will this deployment be billed?

A. Only the dedicated virtual machine host will be billed

B. The dedicated virtual machine host and the boot volumes of each instance will be billed

C. The dedicated virtual machine host all 5 instances, and the boot volume of each instance will be billed

D. All 5 instances will be billed on the basis of the number of OCPUs

Correct Answer: B

You must create a dedicated virtual machine host before you can place any instances on it. When creating the dedicated virtual machine host, you select an availability domain and fault domain to launch it in. All the VM instances that you place on the host will subsequently be created in this availability domain and fault domain. You also select a compartment when you create the dedicated virtual machine host, but you can move the host to a new compartment later without impacting any of the instances placed on it. You can also create the instances in a different compartment than the dedicated virtual machine host, or move them to difference compartments after they have been launched. You are billed for the dedicated virtual machine host as soon as you create it, but you are not billed for any of the individual VM instances you place on it. You will still be billed for image licensing costs if they apply to the image you are using for the VM instances.

Read more: https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm

QUESTION 4

Which offers the lowest pricing for storage (per GB)?

A. Oracle Cloud Infrastructure Object Storage (standard tier)

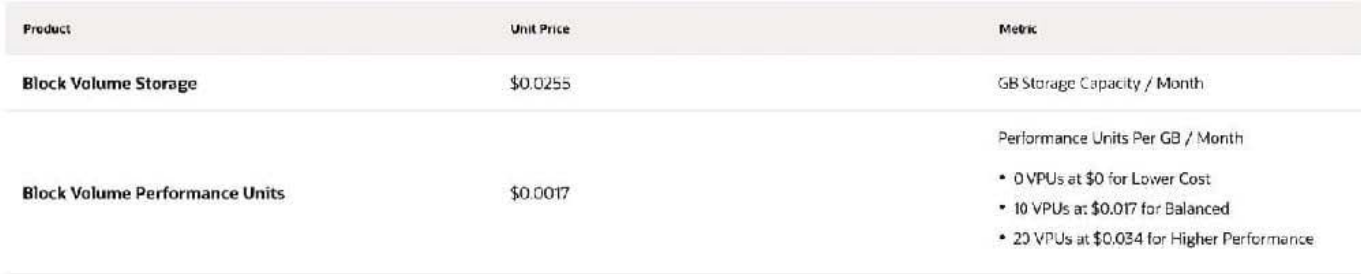
B. Oracle Cloud Infrastructure Block Volume

C. Oracle Cloud Infrastructure Archive Storage

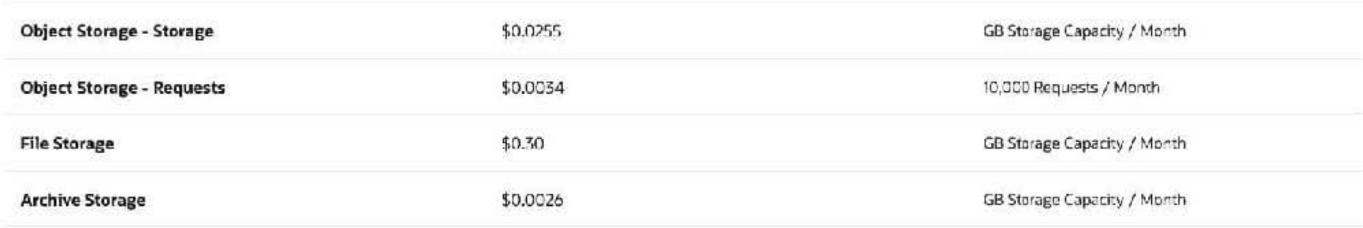
D. Oracle Cloud Infrastructure File Storage

Correct Answer: C

Oracle Cloud Infrastructure Archive Storage is the lowest pricing for storage (per GB) Reference: https://www.oracle.com/cloud/storage/pricing.html



Product	Unit Price	Metric
Block Volume Storage	$0.0255	GB Storage Capacity / Month
Block Volume Performance Units	$0.0017	Performance Units Per GB / Month • 0 VPUs at $0 for Lower Cost • 10 VPUs at $0.017 for Balanced • 20 VPUs at $0.034 for Higher Performance



Object Storage - Storage	$0.0255	GB Storage Capacity / Month
Object Storage - Requests	$0.0034	10,000 Requests / Month
File Storage	$0.30	GB Storage Capacity / Month
Archive Storage	$0.0026	GB Storage Capacity / Month

Archive storage as seen above is the cheapest! Reference: https://www.oracle.com/cloud/storage/pricing.html

QUESTION 5

A customer wants to use Oracle Cloud Infrastructure (OCI) storing application backups which can be stored for months, but retrieved immediately based on business needs. Which OCI storage service can be used to meet this requirement?

A. Archive Storage

B. Block Volume

C. Object Storage (standard)

D. File Storage

Correct Answer: C

Oracle Cloud Infrastructure offers two distinct storage class tiers to address the need for both performant, frequently accessed "hot" storage, and less frequently accessed "cold" storage. Storage tiers help you maximize performance where appropriate and minimize costs where possible. Use Object Storage for data to which you need fast, immediate, and frequent access. Data accessibility and performance justifies a higher price to store data in the Object Storage tier. Use Archive Storage for data to which you seldom or rarely access, but that must be retained and preserved for long periods of time. The cost efficiency of the Archive Storage tier offsets the long lead time required to access the data. Unlike Object Storage, Archive Storage data retrieval is not instantaneous.

Reference: https://oracledbwr.com/oracle-cloud-infrastructure-object-storage-service/

QUESTION 6

Which service is the most effective for moving large amounts of data from your on-premises to OCI?

A. Data Transfer appliance

B. Data Safe

C. Internal Gateway

D. Dynamic Routing Gateway

Correct Answer: A

QUESTION 7

You are setting up a proof of concept (POC) and need to quickly establish a secure between an on-

premises data center and Oracle Cloud Infrastructure (OCI).

Which OCI service should you implement?

A. VCN Peering

B. FastConnect

C. Internet Gateway

D. IPSec VPN

Correct Answer: D

You can set up a single IPSec VPN with a simple layout that you might use for a proof of concept (POC).

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

It is possible to set up a site-to-site Virtual Private Network (VPN) Connection between your on- premises network (a data center or corporate LAN) and your Oracle virtual cloud network (VCN) over a secure encrypted VPN. The VPN connection uses industry-standard IPSec protocols. The Oracle service that provides site-to-site connectivity is named VPN Connect (also referred to as an IPSec VPN). Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/managingIPsec.htm

QUESTION 8

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 9

Which should you use to distribute Incoming traffic between a set of web servers?

A. Load Balances

B. Internet Gateway

C. Autoscallng

D. Dynamic Routing Gateway

Correct Answer: A

The Oracle Cloud Infrastructure Load Balancing service provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). The service offers a load balancer with your choice of a public or private IP address, and provisioned bandwidth. A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability. You can configure multiple load balancing policies and application-specific health checks to ensure that the load balancer directs traffic only to healthy instances. The load balancer can reduce your maintenance window by draining traffic from an unhealthy application server before you remove it from service for maintenance. HOW LOAD BALANCING WORKS: The Load Balancing service enables you to create a public or private load balancer within your VCN. A public load balancer has a public IP address that is accessible from the internet. A private load balancer has an IP address from the hosting subnet, which is visible only within your VCN. You can configure multiple listeners for an IP address to load balance transport Layer 4 and Layer 7 (TCP and HTTP) traffic. Both public and private load balancers can route data traffic to any backend server that is reachable from the VCN. 1) Public Load Balancer To accept traffic from the internet, you create a public load balancer. The service assigns it a public IP address that serves as the entry point for incoming traffic. You can associate the public IP address with a friendly DNS name through any DNS vendor. A public load balancer is regional in scope. If your region includes multiple availability domains, a public load balancer requires either a regional subnet (recommended) or two availability domain-specific (ADspecific) subnets, each in a separate availability domain. With a regional subnet, the Load Balancing service creates a primary load balancer and a standby load balancer, each in a different availability domain, to ensure accessibility even during an availability domain outage. If you create a load balancer in two AD-specific subnets, one subnet hosts the primary load balancer and the other hosts a standby load balancer. If the primary load balancer fails, the public IP address switches to the secondary load balancer. The service treats the two load balancers as equivalent and you cannot specify which one is "primary". Whether you use regional or AD-specific subnets, each load balancer requires one private IP address from its host subnet. The Load Balancing service supplies a floating public IP address to the primary load balancer. The floating public IP address does not come from your backend subnets. If your region includes only one availability domain, the service requires just one subnet, either regional or AD-specific, to host both the primary and standby load balancers. The primary and standby load balancers each require a private IP address from the host subnet, in addition to the assigned floating public IP address. If there is an availability domain outage, the load balancer has no failover. 2) Private Load Balancer To isolate your load balancer from the internet and simplify your security posture, you can create a private load balancer. The Load Balancing service assigns it a private IP address that serves as the entry point for incoming traffic. When you create a private load balancer, the service requires only one subnet to host both the primary and standby load balancers. The load balancer can be regional or AD-specific, depending on the scope of the host subnet. The load balancer is accessible only from within the VCN that contains the host subnet, or as further restricted by your security rules. The assigned floating private IP address is local to the host subnet. The primary and standby load balancers each require an extra private IP address from the host subnet. If there is an availability domain outage, a private load balancer created in a regional subnet within a multi-AD region provides failover capability. A private load balancer created in an AD-specific subnet, or in a regional subnet within a single availability domain region, has no failover capability in response to an availability domain outage. Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/Balance/Concepts/balanceoverview.htm

QUESTION 10

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 11

Which OCI service is the most cost-effective?

A. File Storage

B. Object Storage (standard)

C. Block Volume

D. Archive Storage

Correct Answer: B

QUESTION 12

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 13

A customer wants a dedicated connection with minimal network latency from their on-premises data center

to Oracle Cloud Infrastructure (OCI).

Which service should they choose?

A. Public internet

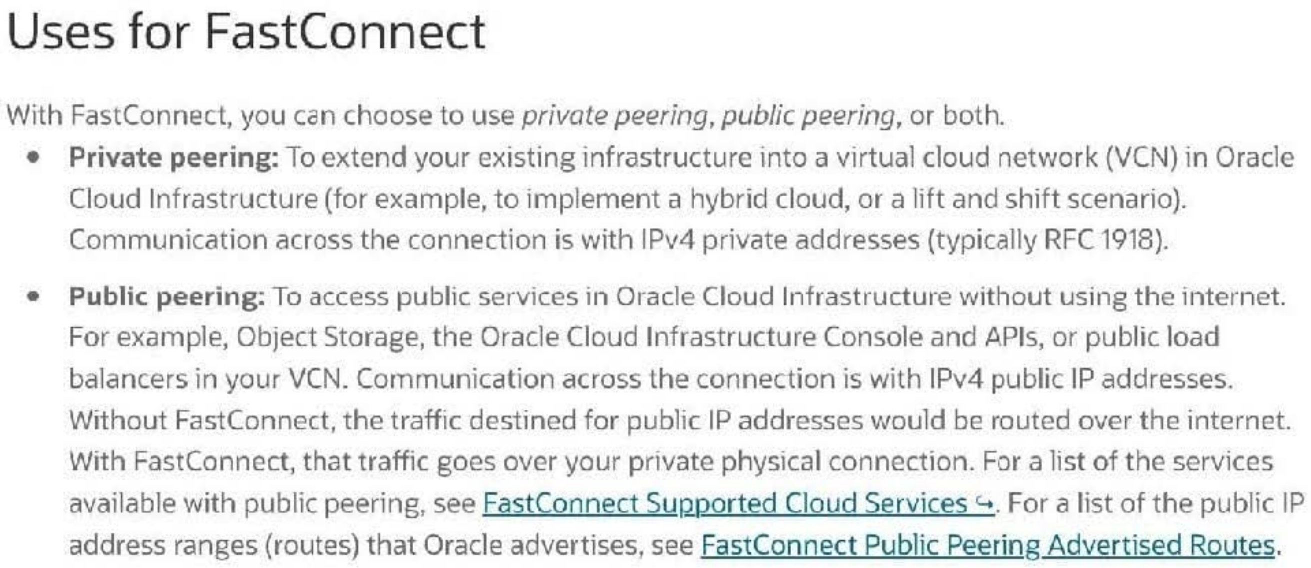
B. Virtual Cloud Network Remote Peering

C. OCI FastConnact

D. IPSec Virtual Private Network (VPN)

Correct Answer: C

Oracle Cloud Infrastructure FastConnect provides an easy way to create a dedicated, private connection between your data center and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet- based connections.



Uses for FastConnect

With FastConnect, you can choose to use *private peering*, *public peering*, or both.

- **Private peering:** To extend your existing infrastructure into a virtual cloud network (VCN) in Oracle Cloud Infrastructure (for example, to implement a hybrid cloud, or a lift and shift scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918).
- **Public peering:** To access public services in Oracle Cloud Infrastructure without using the internet. For example, Object Storage, the Oracle Cloud Infrastructure Console and APIs, or public load balancers in your VCN. Communication across the connection is with IPv4 public IP addresses. Without FastConnect, the traffic destined for public IP addresses would be routed over the internet. With FastConnect, that traffic goes over your private physical connection. For a list of the services available with public peering, see FastConnect Supported Cloud Services ↪. For a list of the public IP address ranges (routes) that Oracle advertises, see FastConnect Public Peering Advertised Routes.

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

QUESTION 14

Which Oracle cloud infrastructure capability can be used to protect against power failures within an availability Domain?

A. Data Plane

B. Fault Domains

C. Services Cells

D. Top of Rack Switch

Correct Answer: B

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. To control the placement of your compute instances, bare metal DB system instances, or virtual machine DB system instances, you can optionally specify the fault domain for a new instance or instance pool at launch time. If you don\\'t specify the fault domain, the system selects one for you. Oracle Cloud Infrastructure makes a best-effort anti-affinity placement across different fault domains, while optimizing for available capacity in the availability domain. To change the fault domain for an instance, terminate it and launch a new instance in the preferred fault domain. Use fault domains to do the following things: Protect against unexpected hardware failures or power supply failures. Protect against planned outages because of Compute hardware maintenance.

Reference: https://blogs.oracle.com/cloud-infrastructure/using-availibility-domains-and-fault-domains-to-improveapplication-resiliency

QUESTION 15

Which two are enabled by Oracle Cloud Infrastructure Fault Domains?

A. Protect against unexpected hardware or power supply failures

B. To meet requirements for legal jurisdictions

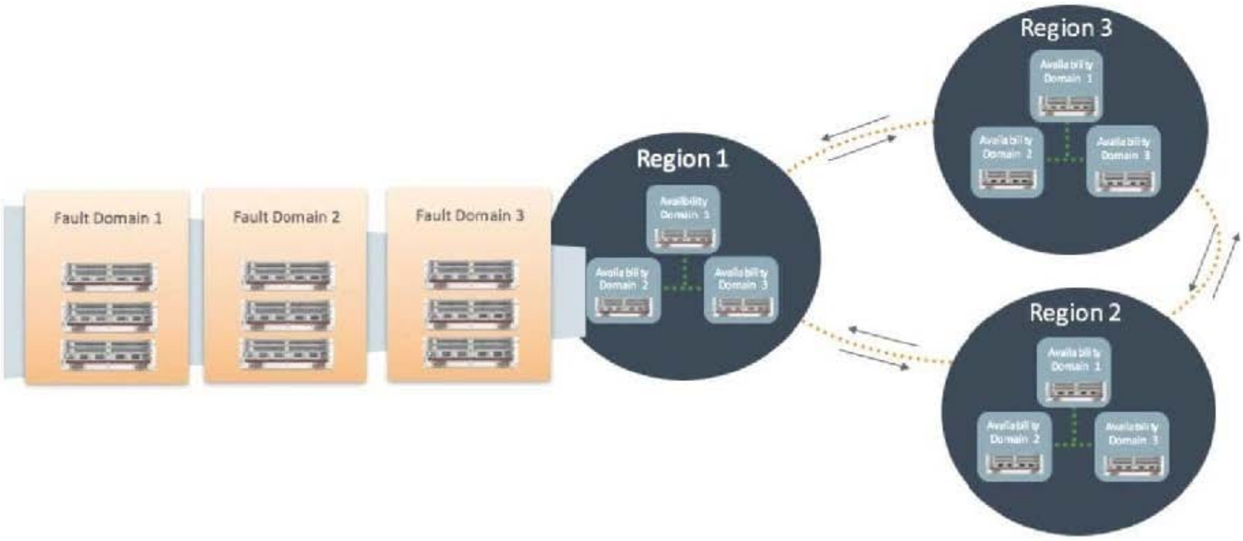
C. To mitigate the risk of large scale events such as earthquakes

D. Build replicated systems for disaster recovery

E. Protect against planned hardware maintenance

Correct Answer: AE

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. To control the placement of your compute instances, bare metal DB system instances, or virtual machine DB system instances, you can optionally specify the fault domain for a new instance or instance pool at launch time. If you don\\'t specify the fault domain, the system selects one for you. Oracle Cloud Infrastructure makes a best-effort anti-affinity placement across different fault domains, while optimizing for available capacity in the availability domain. To change the fault domain for an instance, terminate it and launch a new instance in the preferred fault domain. Use fault domains to do the following things: Protect against unexpected hardware failures or power supply failures. Protect against planned outages because of Compute hardware maintenance. We can use 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


Fault Domain 1
Fault Domain 2
Fault Domain 3
Region 1
Availbility Domain 1
Availability Domain 2
Availability Domain 3
Region 3
Availability Domain 1
Availability Domain 2
Availability Domain 3
Region 2
Availability Domain 1
Availability Domain 2
Availability Domain 3