DUMPSBOSS.

Oracle Cloud Infrastructure Foundations 2021 Associate

Oracle 1z0-1085-21

Version Demo

Total Demo Questions: 10

Total Premium Questions: 98

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which two security capabilities are offered by Oracle Cloud Infrastructure?

A. Always on data encryption for data-at-rest.

B. Certificate Management service

C. Captcha

D. Key Management service

E. Managed Active Directory service

ANSWER: A D

Explanation:

Oracle Cloud Infrastructure's security approach is based on seven core pillars. Each pillar has multiple solutions designed to maximizethe security and compliance of the platform and to help customers to improve their security posture.

High Availability: Offer fault-independent data centers that enable high-availability scale-out architectures and are resilient against network attacks,ensuring constant uptime in the face of disaster and security attack.

Customer Isolation: Allow customers to deploy their application and data assets in an environment that commits full isolation from other tenants and Oracle's staff.

Data Encryption: Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements with respect to cryptographic algorithms and key management.

Security Controls: Offer customers effective and easy-to-use application, platform, and network security solutions that allow them to protect their workloads, have a secure application delivery using a global edge network, constrain access to their services, and segregate operational responsibilities to reduce the risk associated with malicious and accidental user actions.

Visibility: Offer customers comprehensive log data and security analytics that they can use to audit and monitor actions on their resources, allowing them to meet their audit requirements and reduce securityand operational risk.

Secure Hybrid Cloud: Enable customers to use their existing security assets, such as user accounts and policies, as well as third-party security solutions, when accessing their cloud resources and securing their data and application assets in the cloud.

Verifiably Secure Infrastructure: Follow rigorous processes and use effective security controls in all phases of cloud service development and operation. Demonstrate adherence to Oracle's strict security standards through third-partyaudits, certifications, and attestations. Help customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors, and regulators.

QUESTION NO: 2

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 largescale events such as earthquakes

D. Build replicated systems for disaster recovery

E. Protect against planned hardware maintenance

ANSWER: A E

Explanation:

A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availabilitydomain 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.

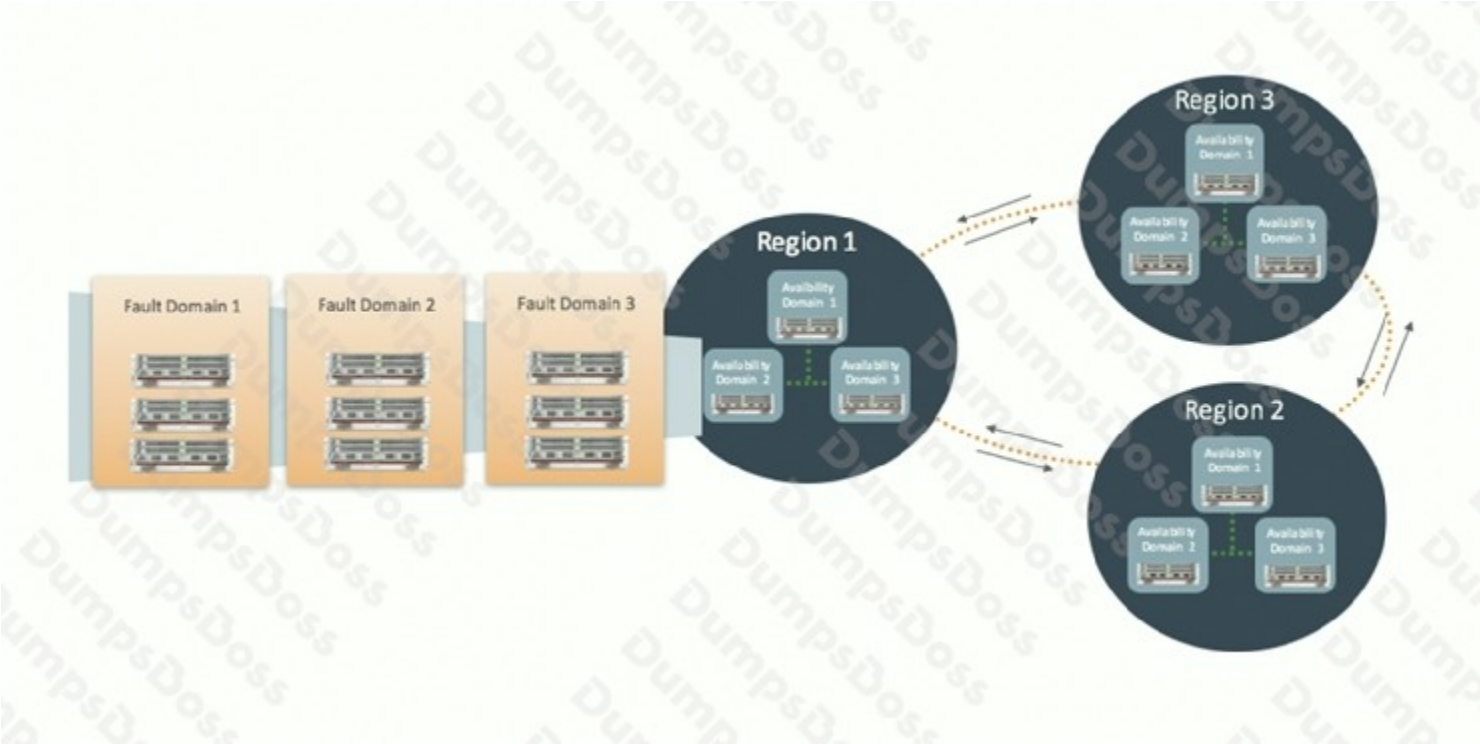
To control the placement of your compute instances, bare metal DB system instances, or virtual machine DB system instances, you can optionally specify the fault domain for a new instance or instance pool at launch time. If you don't specify the fault domain, the system selects one for you. Oracle Cloud 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 plannedoutages 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



QUESTION NO: 3

A company has developed an eCommerce web application In Oracle CloudInfrastructure.

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.

ANSWER: A

Explanation:

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

QUESTION NO: 4

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

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

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.

ANSWER: C

Explanation:

Oracle Cloud Infrastructureoffers 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 isresponsible 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 hardenedand 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 anycompliance 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.

QUESTION NO: 5

You are setting up a proof of concept (POC) and need to quickly establish a secure between an on-premises data center andOracle Cloud Infrastructure (OCI).

Which OCI service should you implement?

A. VCN Peering

B. FastConnect

C. Internet Gateway

D. IPSec VPN

ANSWER: D

Explanation:

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

QUESTION NO: 6

Oracle CloudInfrastructure Budgets can be set on which two options?

A. Free-form tags

B. Compartments

C. Tenancy

D. Virtual Cloud Network

E. Cost-tracking tags

ANSWER: B E

Explanation:

A budget can be used to set soft limits on your Oracle Cloud Infrastructure spending. Youcan set alerts on your budget to let you know when you might exceed your budget, and you can view all of your budgets and spending from one single place in the Oracle Cloud Infrastructure console.

How Budgets Work:

Budgets are set on cost-tracking tags or on compartments (including the root compartment) to track all spending in that cost-tracking tag or for that compartment and its children.

All budgets alerts are evaluated every 15 minutes. To see the last time a budget was evaluated, open the details for a budget. You will see fields that show the current spend, the forecast and the "Spent in period" field which shows you the time period over which the budget was evaluated. When a budget alert fires, the email recipients configured in the budget alert receive an email.

QUESTION NO: 7

Which CANNOT be used with My Oracle Support (MOS)?

A. Add or change a tenancy administrator

B. Request a Service Limit increase

C. Reset the password or unlock the account for the tenancy administrator

D. Troubleshoot your resources in an Oracle Cloud Infrastructure Free Trial account

ANSWER: D

Explanation:

Open a support service requestwith MOS option is available to paid accounts. Customers using only Always Free resources are not eligible for Oracle Support. Limited support is available to Free Tier accounts with Free Trial credits. After you use all of your credits or after your trialperiod ends (whichever comes first), you must upgrade to a paid account to access Oracle Support. If you choose not to upgrade and continue to use Always Free Services, you will not be eligible to raise a service request in My Oracle Support.

In additionto support for technical issues, use My Oracle Support if you need to:

· Reset the password or unlock the account for the tenancy administrator

· Add or change a tenancy administrator

· Request a service limit increase

QUESTION NO: 8

In what two ways does Oracle Cloud Infrastructure (OCI) offer industry leadingprice-performance?

A. OCI leverages advanced encryption that results In fast performance

B. With OCI, pricing Is low and predictable across all regions and services.

C. OCI hypervisor provides Industry loading performance.

D. OCI backs performance claimswith Service Level Agreements.

E. OCI does not over subscribe CPU, but only memory.

ANSWER: B D

Explanation:

OCI leverages advanced encryption that leads to fast performance, OCI does not over subscribe CPU, but only memory, and OCI hypervisor provides industry leadingperformance are WRONG.

However, OCI does back claims with SLAs and offers predictable pricing for all services.

QUESTION NO: 9

You wererecently assigned to manage a project to deploy Oracle E-Business Suite on Oracle Cloud Infrastructure (OCI). The application will require a database, several servers, and a shared file system.

Which three OCI services are best suited for this project?

A. OCI virtual or Bare Metal DB Systems

B. OCI Streaming Service

C. Object Storage Service

D. Virtual Machine (VM) or Bare Metal (BM) compute Instances

E. File Storage Service

F. Oracle Container Engine for Kubernetes

ANSWER: A D E

Explanation:

https://docs.oracle.com/en/solutions/deploy-ebusiness-suite-oci/index.html#GUID-0CA881FD-D96F-4885-BC7

QUESTION NO: 10

After Signing up for a new Oracle cloud Infrastructure tenancy, what wouldyou subscribe to in order to deploy infrastructure and services in different parts of the world?

A. Availability Domain

B. Fault Domains

C. Pay as you go pricing

D. Region

ANSWER: D

Explanation:

Oracle Cloud Infrastructure is hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Most Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance. Traffic between availability domains and between regions is encrypted. Availability domains are isolated from each other, fault tolerant, and very unlikely to failsimultaneously. Because availability domains do not share infrastructure such as power or cooling, or the internal availability domain network, a failure at one availability domain within a region is unlikely to impact the availability of the others withinthe same region.

The availability domains within the same region are connected to each other by a low latency, high bandwidth network, which makes it possible for you to provide high-availability connectivity to the internet and

on-premises, and to buildreplicated systems in multiple availability domains for both high-availability and disaster recovery.

Oracle is adding multiple cloud regions around the world to provide local access to cloud resources for our customers. To accomplish this quickly, we’vechosen to launch regions in new geographies with one availability domain.

As regions require expansion, we have the option to add capacity to existing availability domains, to add additional availability domains to an existing region, or to build a new region. The expansion approach in a particular scenario is based on customer requirements as well as considerations of regional demand patterns and resource availability.

For any region with one availability domain, a second availability domain or region in the same country or geo-political area will be made available within a year to enable further options for disaster recovery that support customer requirements for data residency where they exist.