Leads4Pass

1Z0-1085-20^{Q&As}

Oracle Cloud Infrastructure Foundations 2020 Associate

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

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

https://www.leads4pass.com/1z0-1085-20.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which feature is NOT a component of Oracle Cloud Infrastructure (OCI) Identity and Access management service?

A. User Credentials

B. Network Security Group

C. Federation

D. Policies

Correct Answer: C

QUESTION 2

Which two situations incur costs in Oracle Cloud Infrastructure (OCI)?

A. Data ingress from the internet

B. Transferring data across regions

C. Transferring data from one instance to another in the same Availibility Domain

D. Data egress to the internet E. Transferring data from one instance to another across different Availibility Domains in a Region

Correct Answer: BD

QUESTION 3

Which kind of scaling is supported by virtual machines in Oracle Cloud Infrastructure Compute service?

A. Only scaling up or down

B. Only scaling out

C. Scaling up or down, and scaling in or out

D. Only scaling in

Correct Answer: C

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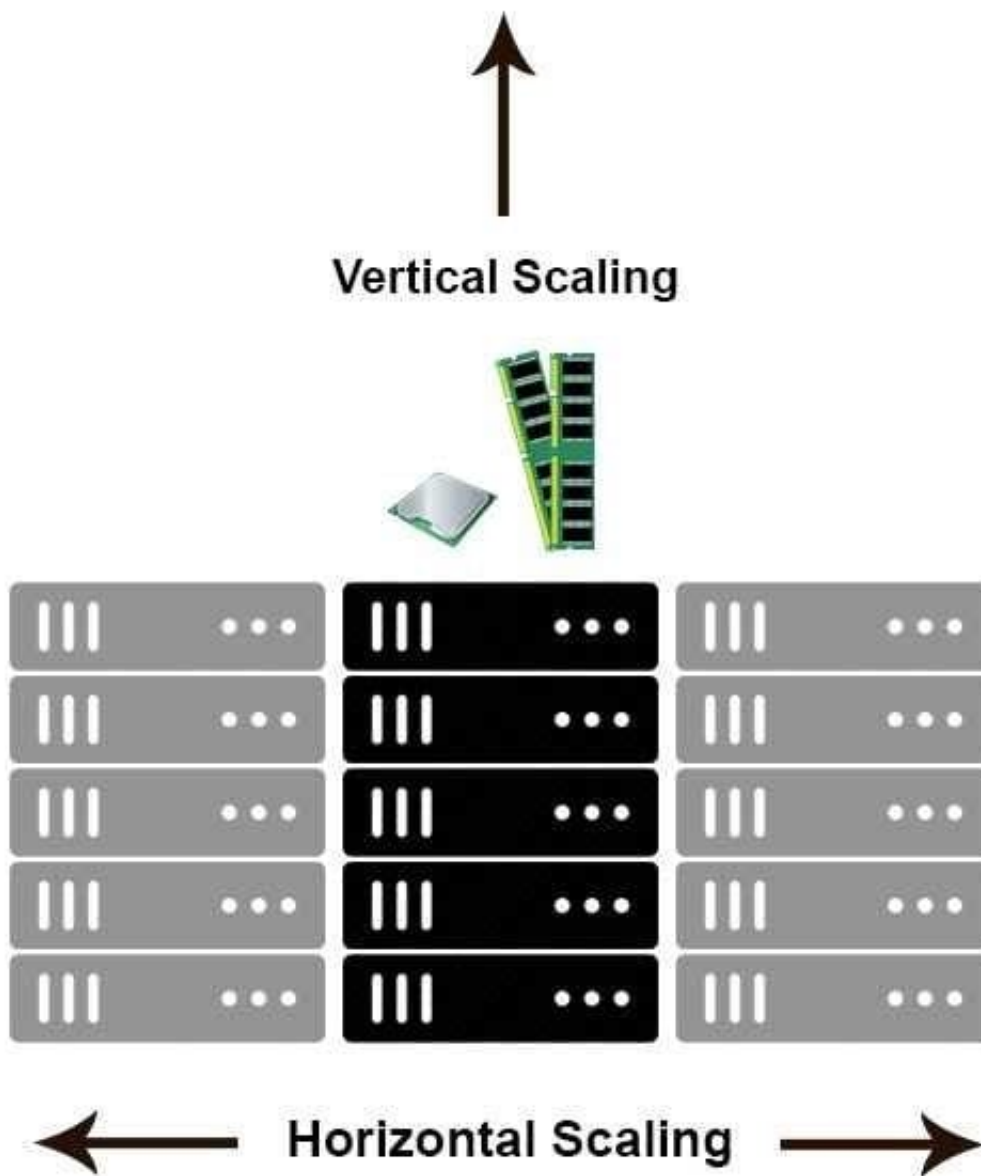
With horizontal-scaling it is often easier to scale dynamically by adding more machines into the existing pool -- Vertical-scaling is often limited to the capacity of a single machine, scaling beyond that capacity often involves downtime and comes with an upper limit. Reference: https://medium.com/@abhinavkorpal/scaling-horizontally-and-vertically-for-databases-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

QUESTION 4

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 5

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

https://www.leads4pass.com/1z0-1085-20.html
2024 Latest leads4pass 1Z0-1085-20 PDF and VCE dumps Download

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
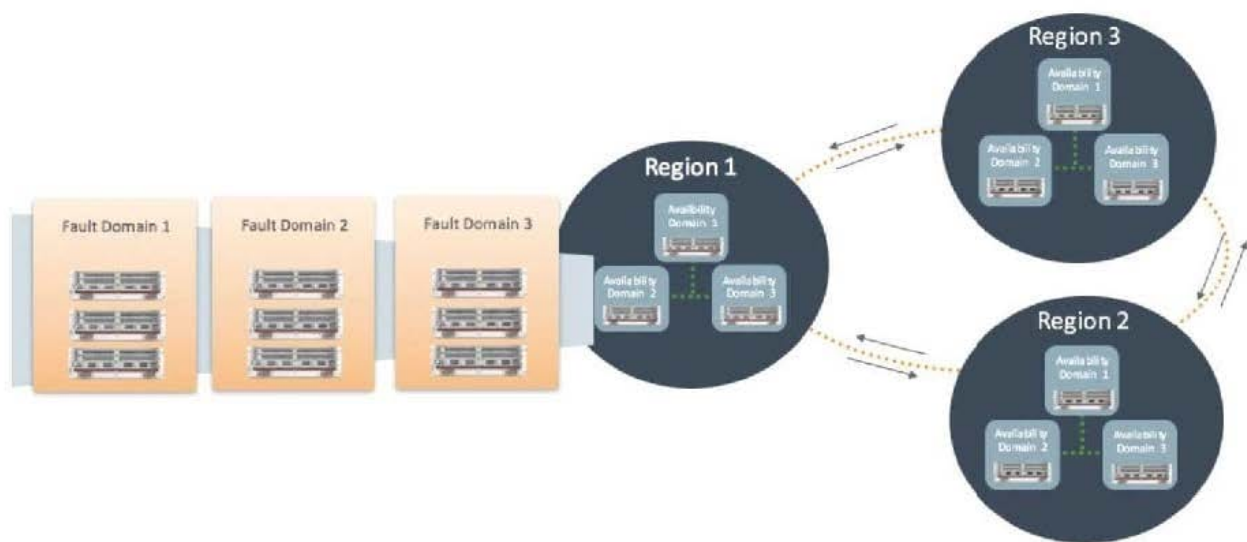
1Z0-1085-20 PDF Dumps   1Z0-1085-20 VCE Dumps   1Z0-1085-20 Study Guide