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.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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which is NOT covered by Oracle Cloud Infrastructure (OCI) Service Level Agreement (SLA)?

A. Manageability

B. Performance

C. Reliability

D. Availability

Correct Answer: C

https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf Enterprises demand more than just availability from their cloud infrastructure. Mission-critical workloads also require consistent performance, and the ability to manage, monitor, and modify resources running in the cloud at any time. Only Oracle offers end-to-end SLAs covering performance, availability, manageability of services.

Availability

Rest assured that your cloud workloads are in continual operation with Oracle's commitments to uptime and connectivity.

Manageability

The elasticity and configurability of infrastructure is part of why people move applications to the cloud. Your services need to be manageable all the time to deliver this benefit. Oracle provides manageability SLAs to ensure your ability to manage, monitor, and modify resources.

Performance

It's not enough for your IaaS resources to be merely accessible. They should consistently perform the way you expect them to. Oracle is the first cloud vendor to guarantee performance, so you can rely on your infrastructure for enterprise applications.

Reference: https://www.oracle.com/in/cloud/iaas/sla.html

QUESTION 2

According to Shared security model, which two are a customer\\'s responsibilities in Oracle Cloud Infrastructure (OCI)?

A. Physical security of OCI data center facilities

B. Virtual Machine hypervisor

C. Local NVMe data persistence

D. Customer data

E. Object Storage data durability

Correct Answer: DE

Customer and Oracle\\'s responsibilities can be divided into the following areas: 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. 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.

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

QUESTION 3

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 4

_____ is a fully-managed, scalable, and highly available service that you can use to deploy your containerized applications to the cloud.

A. Oracle Cloud Infrastructure Container Engine for Kubernetes

B. Oracle Cloud Infrastructure Container Engine for Containerization

C. Oracle Cloud Infrastructure Container Engine for Deployment

D. Oracle Cloud Infrastructure Container Engine for Docker

Correct Answer: A

Oracle Cloud Infrastructure Container Engine for Kubernetes is a fully-managed, scalable, and highly available service that you can use to deploy your containerized applications to the cloud. Use Container Engine for Kubernetes (sometimes abbreviated to just OKE) when your development team wants to reliably build, deploy, and manage cloud-

native applications. You specify the compute resources that your applications require, and Container Engine for Kubernetes provisions them on Oracle Cloud Infrastructure in an existing OCI tenancy. You can access Container Engine for Kubernetes to define and create Kubernetes clusters using the Console and the REST API. You can access the clusters you create using the Kubernetes command line (kubectl), the Kubernetes Dashboard, and the Kubernetes API. Container Engine for Kubernetes is integrated with Oracle Cloud Infrastructure Identity and Access Management (IAM), which provides easy authentication with native Oracle Cloud Infrastructure identity functionality. Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/ContEng/Concepts/contengoverview.htm

QUESTION 5

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