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 Oracle Cloud Infrastructure service leverages Terraform to configure infrastructure as code?

A. Resource Manager

B. Events

C. Compartment Explorer

D. Oracle Functions

Correct Answer: A

Resource Manager is an Oracle Cloud Infrastructure service that allows you to automate the process of provisioning your Oracle Cloud Infrastructure resources. Using Terraform, Resource Manager helps you install, configure, and manage resources through the "infrastructure-as-code" model. A Terraform configuration codifies your infrastructure in declarative configuration files. Resource Manager allows you to share and manage infrastructure configurations and state files across multiple teams and platforms. This infrastructure management can\\'t be done with local Terraform installations and Oracle Terraform modules alone. For more information about the Oracle Cloud Infrastructure Terraform provider, see Terraform Provider. For a general introduction to Terraform and the "infrastructure-as-code" model, see https:// www.terraform.io. Reference: https://docs.cloud.oracle.com/en-us/iaas/Content/ResourceManager/Concepts/resourcemanager.htm

QUESTION 2

You have a mission-critical application which requires to be globally available at all times. Which deployment strategy should you adopt?

A. Use multiple Fault Domains In each Availability Domain in each Region.

B. Use multiple Availability Domains In one Region.

C. Use multiple Fault Domains In one Region.

D. Use multiple Fault Domains in any Availability Domain in multiple Regions.

Correct Answer: A

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. Regions are independent of other regions and can be separated by vast distances--across countries or even continents.

Availability domains are isolated from each other, fault tolerant, and very unlikely to fail simultaneously. 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 within the same region. 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.

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

QUESTION 3

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

A. Manageability

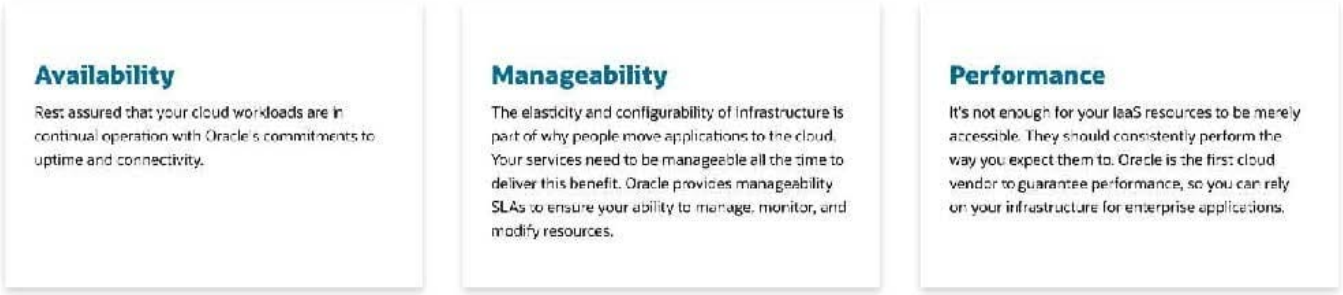
B. Performance

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.



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

QUESTION 4

Which is a key benefit of using oracle cloud infrastructure autonomous data warehouse?

A. No username and password required

B. Scale both CPU and Storage without downtime

C. Apply database patches as they become available D. Maintain root level acress to the underlying operating system

Correct Answer: B

Oracle Autonomous Data Warehouse is a cloud data warehouse service that eliminates virtually all the complexities of operating a data warehouse and securing data. It automates provisioning, configuring, securing, tuning, scaling, patching, backing up, and repairing of the data warehouse. Unlike other "fully managed" cloud data warehouse solutions that only patch and update the service, it also features elastic, automated scaling, performance tuning, security, and a broad set of built-in capabilities that enable machine learning analysis, simple data loading, and data visualizations. Data Warehouse uses continuous query optimization, table indexing, data summaries, and auto- tuning to ensure consistent high performance even as data volume and number of users grows. Autonomous scaling can temporarily

increase compute and I/O by a factor of three to maintain performance. Unlike other cloud services which require downtime to scale, Autonomous Data Warehouse scales while the service continues to run. Reference: https://www.oracle.com/autonomous-database/autonomous-data-warehouse/

QUESTION 5

What is Oracle\\'s responsibility according to the Oracle Cloud Infrastructure (OCI) shared-security model?

A. Configuring OCI services securely

B. Data classification and compliance

C. Securing application workloads

D. Security of data center facilities

Correct Answer: D

Oracle\\'s mission is to build cloud infrastructure and platform services for your business to have effective and manageable security to run your mission-critical workloads and store your data with confidence. 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.

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