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.pass4itsure.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

You have an application that requires a shared file system. Which of the following services would you use?

A. File Storage

B. Archive Storage

C. Object Storage

D. Block Volume

Correct Answer: A

Oracle Cloud Infrastructure File Storage service provides a durable, scalable, secure, enterprise-grade network file system. You can connect to a File Storage service file system from any bare metal, virtual machine, or container instance in your Virtual Cloud Network (VCN). You can also access a file system from outside the VCN using Oracle Cloud Infrastructure FastConnect and Internet Protocol security (IPSec) virtual private network (VPN). Large Compute clusters of thousands of instances can use the File Storage service for high-performance shared storage. Storage provisioning is fully managed and automatic as your use scales from a single byte to exabytes without upfront provisioning. The File Storage service supports the Network File System version 3.0 (NFSv3) protocol. The service supports the Network Lock Manager (NLM) protocol for file locking functionality. Oracle Cloud Infrastructure File Storage employs 5way replicated storage, located in different fault domains, to provide redundancy for resilient data protection. Data is protected with erasure encoding. The File Storage service uses the "eventual overwrite" method of data eradication. Files are created in the file system with a unique encryption key. When you delete a single file, its associated encryption key is eradicated, making the file inaccessible. When you delete an entire file system, the file system is marked as inaccessible. The service systematically traverses deleted files and file systems, frees all the used space, and eradicates all residual files. Use the File Storage service when your application or workload includes big data and analytics, media processing, or content management, and you require Portable Operating System Interface (POSIX)-compliant file system access semantics and concurrently accessible storage. The File Storage service is designed to meet the needs of applications and users that need an enterprise file system across a wide range of use cases, including the following:

- **General Purpose File Storage:** Access to an unlimited pool of file systems to manage growth of structured and unstructured data.
- **Big Data and Analytics:** Run analytic workloads and use shared file systems to store persistent data.
- **Lift and Shift of Enterprise Applications:** Migrate existing Oracle applications that need NFS storage, such as Oracle E-Business Suite and PeopleSoft.
- **Databases and Transactional Applications:** Run test and development workloads with Oracle, MySQL, or other databases.
- **Backups, Business Continuity, and Disaster Recovery:** Host a secondary copy of relevant file systems from on premises to the cloud for backup and disaster recovery purposes.
- **MicroServices and Docker:** Deliver stateful persistence for containers. Easily scale as your container-based environments grow.

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

QUESTION 2

Which three components are part of Oracle Cloud Infrastructure (OCI) identity and access management service?

A. Regional Subnets

B. Policies

C. Users

D. Compute Instances

E. Dynamic Groups

F. Roles

G. Virtual Cloud Networks

Correct Answer: BCE

Components of IAM IAM uses the components described in this section. To better understand how the components fit together, see Example Scenario. RESOURCE The cloud objects that your company\\'s employees create and use when interacting with Oracle Cloud Infrastructure. For example: compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, route tables, etc. USER An individual employee or system that needs to manage or use your company\\'s Oracle Cloud Infrastructure resources. Users might need to launch instances, manage remote disks, work with your virtual cloud network, etc. End users of your application are not typically IAM users. Users have one or more IAM credentials (see User Credentials). GROUP A collection of users who all need the same type of access to a particular set of resources or compartment. DYNAMIC GROUP A special type of group that contains resources (such as compute instances) that match rules that you define (thus the membership can change dynamically as matching resources are created or deleted). These instances act as "principal" actors and can make API calls to services according to policies that you write for the dynamic group. NETWORK SOURCE A group of IP addresses that are allowed to access resources in your tenancy. The IP addresses can be public IP addresses or IP addresses from a VCN within your tenancy. After you create the network source, you use policy to restrict access to only requests that originate from the IPs in the network source. COMPARTMENT A collection of related resources. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources. You use them to clearly separate resources for the purposes of measuring usage and billing, access (through the use of policies), and isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of your organization. For more information, see Setting Up Your Tenancy. TENANCY The root compartment that contains all of your organization\\'s Oracle Cloud Infrastructure resources. Oracle automatically creates your company\\'s tenancy for you. Directly within the tenancy are your IAM entities (users, groups, compartments, and some policies; you can also put policies into compartments inside the tenancy). You place the other types of cloud resources (e.g., instances, virtual networks, block storage volumes, etc.) inside the compartments that you create. POLICY A document that specifies who can access which resources, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. For more information, see Example Scenario and How Policies Work. The word "policy" is used by people in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources. HOME REGION The region where your IAM resources reside. All IAM resources are global and available across all regions, but the master set of definitions reside in a single region, the home region. You must make changes to your IAM resources in your home region. The changes will be automatically propagated to all regions. For more information, see Managing Regions. FEDERATION A relationship that an administrator configures between an identity provider and a service provider. When you federate Oracle Cloud Infrastructure with an identity provider, you manage users and groups in the identity provider. You manage authorization in Oracle Cloud Infrastructure\\'s IAM service. Oracle Cloud Infrastructure tenancies are federated with Oracle Identity Cloud Service by default.

https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

QUESTION 3

Which is NOT available to you whenever Oracle Cloud Infrastructure creates or resolves an incident?

A. Twitter notifications

B. Text Message notifications

C. Email notifications

D. Webhook notifications

Correct Answer: A

The Oracle Cloud Infrastructure Notifications service broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency and durable messages for applications hosted on Oracle Cloud Infrastructure and externally. Use Notifications to get notified when event rules are triggered or alarms are breached, or to directly publish a message. Messages sent out as email by the Oracle Cloud Infrastructure Notifications service are processed and delivered through Oracle resources

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

QUESTION 4

Which two Oracle Cloud Infrastructure resources can be used to group/categorize expenses?

A. Policies

B. Tags

C. Users

D. Compartments

E. Groups

Correct Answer: BD

You can do Costs Analysis in OCI and you can group and filter the cost by Tags or compartments To filter costs by dates To filter costs by tags To filter costs by compartments To remove a compartment or tag filter

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