



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.geekcert.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**

What is a key benefit of Oracle Cloud Infrastructure (OCI) Virtual Machine DB Systems?

- A. Support for RAC DB systems
- B. No need to create database Indices
- C. Automated backups to OCI Block Volume
- D. Automated disaster recovery

Correct Answer: A

There are two types of DB systems on virtual machines: A 1-node virtual machine DB system consists of one virtual machine. A 2-node virtual machine DB system consists of two virtual machines. (RAC) A virtual machine DB system database uses Oracle Cloud Infrastructure block storage instead of local storage. You specify a storage size when you launch the DB system, and you can scale up the storage as needed at any time. For 1-node virtual machine DB systems, Oracle Cloud Infrastructure provides have a "fast provisioning" option that allows you to create your DB system using Logical Volume Manager as your storage management software. Oracle Cloud Infrastructure offers single-node DB systems on either bare metal or virtual machines, and 2-node RAC DB systems on virtual machines. If you need to provision a DB system for development or testing purposes, then a special fast provisioning single-node virtual machine system is available. You can manage these systems by using the Console, the API, the Oracle Cloud Infrastructure CLI, the Database CLI (DBCLI), Enterprise Manager, Enterprise Manager Express, or SQL Developer.



Supported Database Editions and Versions

All single-node Oracle RAC DB systems support the following Oracle Database editions:

- Standard Edition
- Enterprise Edition
- Enterprise Edition - High Performance
- Enterprise Edition - Extreme Performance

Two-node Oracle RAC DB systems require Oracle Enterprise Edition - Extreme Performance.

For standard provisioning of DB systems (using [Oracle Automatic Storage Management ↗](#) (ASM) as your storage management software), the supported database versions are:

- Oracle Database 19c (19.0)
- Oracle Database 18c (18.0)
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1)
- Oracle Database 11g Release 2 (11.2)

For [fast provisioning](#) of single-node virtual machine database systems (using [Logical Volume Manager ↗](#) as your storage management software), the supported database versions are:

- Oracle Database 20c (20.0) - [Preview version](#) only
- Oracle Database 19c (19.0)
- Oracle Database 18c (18.0)

Reference: <https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Concepts/overview.htm>

QUESTION 2

What does Oracle's Payment Card Industry Data Security Standard (PCI DSS) attestation of compliance provide to customers?

- A. Customers can use these services for workloads that provides validation of card holder transaction but only as 3rd party
- B. Customers can use these services for workloads that process, or transmit cardholder data but not store it.
- C. Customers can use these services for workloads to process applications for credit card approval securely.
- D. Customers can use these services for workloads that store, process, or transmit cardholder data.

Correct Answer: D



The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security standard designed to encourage and enhance cardholder data security and promote the adoption of consistent data security measures around the technical and operational components related to cardholder data. Oracle has successfully completed a Payment Card Industry Data Security Standard (PCI DSS) audit and received an Attestation of Compliance (AoC) covering several Oracle Cloud Infrastructure services and the Oracle RightNow Service Cloud Service. As a PCI Level 1 Service Provider, customers can now use these services for workloads that store, process or transmit cardholder data.

Reference: <https://www.oracle.com/cloud/cloud-infrastructure-compliance/>

QUESTION 3

Oracle cloud Infrastructure is compliant with which three industry standards?

- A. SOC 1 Type 2 and SOC 2 Type 2 attestations
- B. NERC Critical Infrastructure Protection Standards
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. ISO 27001:2013 certification
- E. Health Care Compliance Association (HCCA)

Correct Answer: ACD

Here is the official list of all industry standards that OCI complies with : <https://www.oracle.com/in/cloud/cloud-infrastructure-compliance/>

QUESTION 4

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 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

[1Z0-1085-22 VCE Dumps](#)

[1Z0-1085-22 Study Guide](#)

[1Z0-1085-22 Exam Questions](#)