1Z0-997$^{\text{Q\&As}}$

Oracle Cloud Infrastructure 2019 Architect Professional

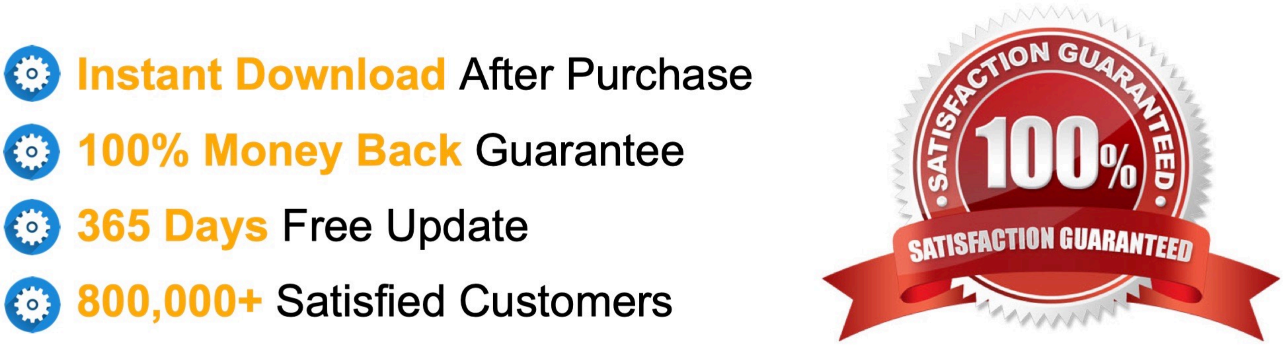
Pass Oracle 1Z0-997 Exam with 100% Guarantee

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

https://www.geekcert.com/1z0-997.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Your company will soon start moving critical systems Into Oracle Cloud Infrastructure (OCI) platform.

These systems will reside in the us-phoenix-1and us-ashburn 1 regions. As part of the migration planning,

you are reviewing the company\\'s existing security policies and written guidelines for the OCI platform

usage within the company. you have to work with the company managed key.

Which two options ensure compliance with this policy?

A. When you create a new compute instance through OCI console, you use the default options for "configure boot volume" to speed up the process to create this compute instance.

B. When you create a new block volume through OCI console, select Encrypt using Key Management checkbox and use encryption keys generated and stored in OCI Key Management Service.

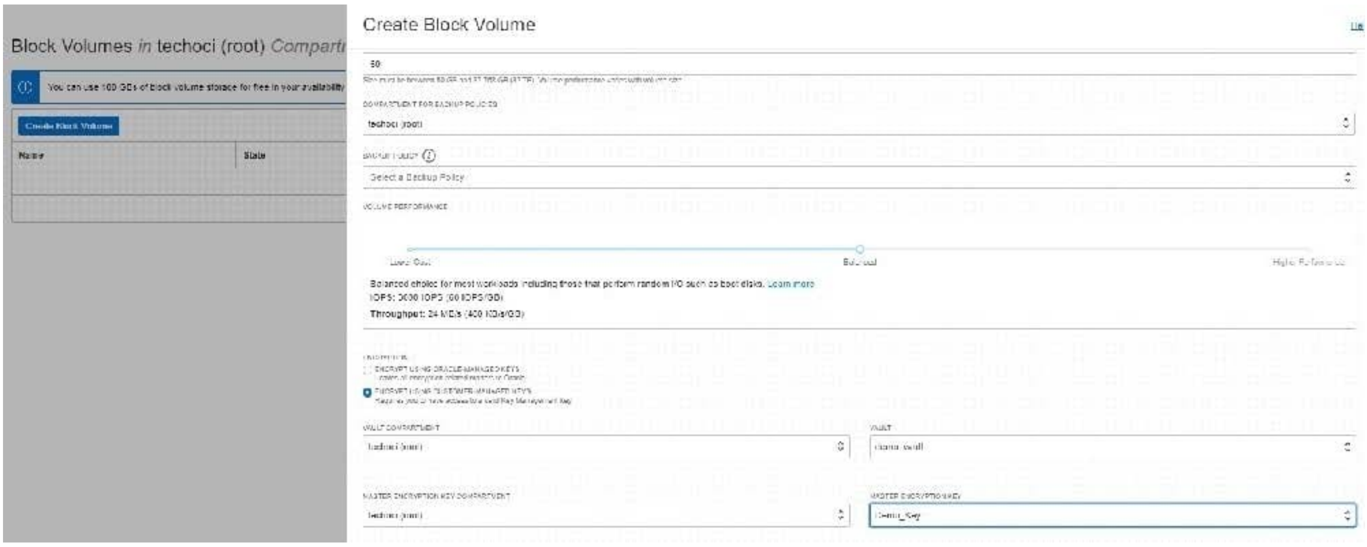
C. When you create a new compute instance through OCI console, you use the default shape to speed up the process to create this compute instance.

D. When you create a new OCI Object Storage bucket through OCI console, you need to choose "ENCRYPT USING CUSTOMER-MANAGED KEYS" option.

E. You do not need to perform any additional actions because the OCI Block Volume service always encrypts all block volumes, boot volumes, and volume backups at rest by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption.

Correct Answer: BD

Block Volume Encryption By default all volumes and their backups are encrypted using the Oracle-provided encryption keys. Each time a volume is cloned or restored from a backup the volume is assigned a new unique encryption key. You have the option to encrypt all of your volumes and their backups using the keys that you own and manage using the Vault service.If you do not configure a volume to use the Vault service or you later unassign a key from the volume, the Block Volume service uses the Oracle-provided encryption key instead.



Block Volumes *in* techoci (root) Comparti

You can use 100 GBs of block volume storage for free in your availability

Create Block Volume

50

COMPARTMENT FOR BACKUP POLICIES: techoci (root)

BACKUP POLICY: Select a Backup Policy

VOLUME PERFORMANCE: Balanced

Balanced choice for most workloads including those that perform random I/O such as boot disks. Learn more
IOPS: 3000 IOPS (60 IOPS/GB)
Throughput: 24 MB/s (480 KB/s/GB)

ENCRYPTION
○ ENCRYPT USING ORACLE-MANAGED KEYS
● ENCRYPT USING CUSTOMER-MANAGED KEYS

VAULT COMPARTMENT: techoci (root)

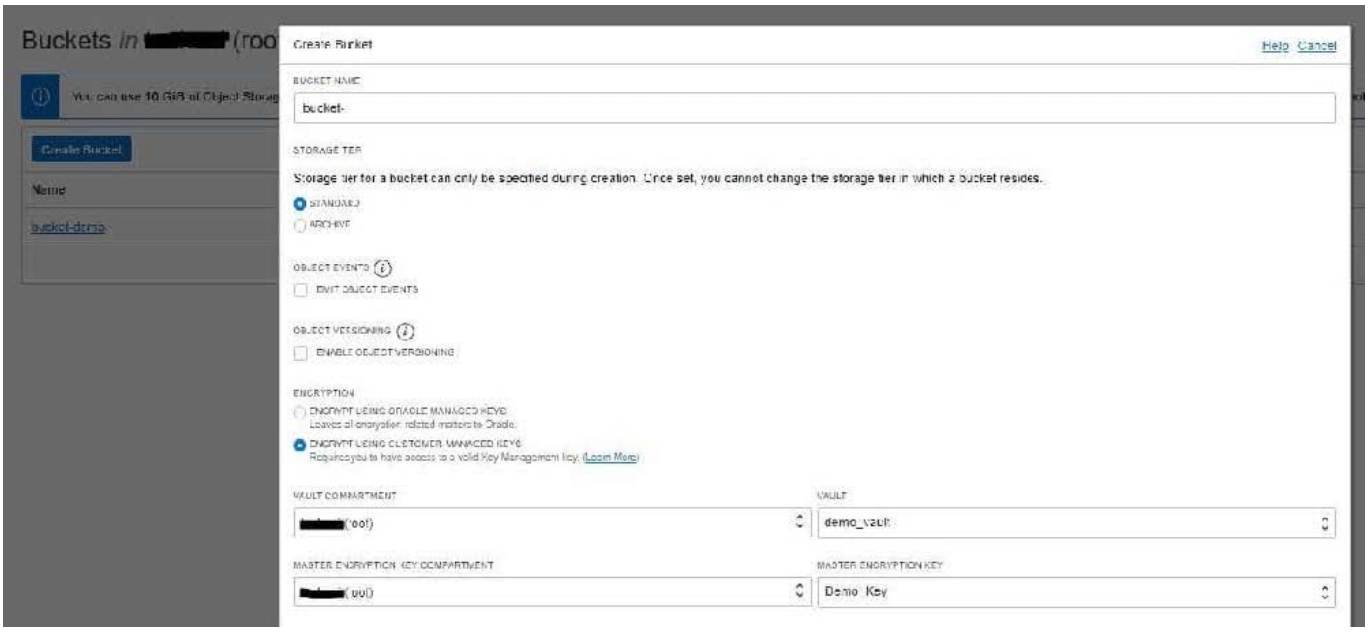
VAULT: demo_vault

MASTER ENCRYPTION KEY COMPARTMENT: techoci (root)

MASTER ENCRYPTION KEY: Demo_Key

This applies to both encryption at-rest and in-transit encryption. Object Storage Encryption Object Storage employs

256-bit Advanced Encryption Standard (AES-256) to encrypt object data on the server. Each object is encrypted with its own data encryption key. Data encryption keys are always encrypted with a master encryption key that is assigned to the bucket. Encryption is enabled by default and cannot be turned off. By default, Oracle manages the master encryption key. However, you can optionally configure a bucket so that it\\'s assigned an Oracle Cloud Infrastructure Vault master encryption key that you control and rotate on your own schedule. Encryption: Buckets are encrypted with keys managed by Oracle by default, but you can optionally encrypt the data in this bucket using your own Vault encryption key. To use Vault for your encryption needs, select Encrypt Using Customer-Managed Keys. Then, select the Vault Compartment and Vault that contain the master encryption key you want to use. Also select the Master Encryption Key Compartment and Master Encryption Key.



Buckets *in* [redacted] (roo

You can use 10 GiB of Object Storag

Create Bucket

BUCKET NAME: bucket-

STORAGE TIER

Storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides.

● STANDARD
○ ARCHIVE

OBJECT EVENTS
□ EMIT OBJECT EVENTS

OBJECT VERSIONING
□ ENABLE OBJECT VERSIONING

ENCRYPTION
○ ENCRYPT USING ORACLE MANAGED KEYS
Leaves all encryption related matters to Oracle.
● ENCRYPT USING CUSTOMER MANAGED KEYS
Requires you to have access to a valid Key Management key. (Learn More)

VAULT COMPARTMENT: [redacted] (root)

VAULT: demo_vault

MASTER ENCRYPTION KEY COMPARTMENT: [redacted] (root)

MASTER ENCRYPTION KEY: Demo Key

QUESTION 2

By copying block volume backups to another region at regular intervals, it makes it easier for you to rebuild applications and data in the destination region if a region-wide disaster occurs in the source region. Which IAM Policy statement allows the VolumeAdmins group to copy volume backups between regions?

A. Allow group VolumeAdmins to use volumes in tenancy

B. Allow group VolumeAdmins to copy volume\\' backups in tenancy

C. Allow group VolumeAdmins to manage volume-family In tenancy

D. Allow group VolumeAdmins to inspect volumes in tenancy

Correct Answer: C

The backups feature of the Oracle Cloud Infrastructure Block Volume service lets you make a point- intime snapshot of the data on a block volume.These backups can then be restored to new volumes either immediately after a backup or at a later time that you choose. You can copy block volume backups between regions using the Console, command line interface (CLI), SDKs, or REST APIs. To copy volume backups between regions, you must have permission to read and copy volume backups in the source region, and permission to create volume backups in the destination region. to do all things with block storage volumes, volume backups, and volume groups in all compartments with the exception of copying volume backups across regions. Allow group VolumeAdmins to manage volume-family in tenancy The aggregate resource type volume-family does not include the VOLUME_BACKUP_COPY permission, so to enable copying volume backups across regions you need to ensure that you include the third statement in that policy, which is: Allow group VolumeAdmins to use volume-backups in tenancy where request.permission=\\'VOLUME _BACKUP_COPY\\'

QUESTION 3

You are part of a project team working in the development environment created in OCI. You have realized that the CIDR block specified for one of the subnet in a VCN is not correct and want to delete the subnet. While deleting you are getting an error indicating that there are still resources that you must delete first. The error includes the OCID of the VNIC that is in the subnet. Which of the following action you will take to troubleshoot this issue?

A. Use OCI CLI to call "GetVnic" operation to find out the parent resource of the VNIC

B. Copy and Paste OCID of the VNIC in the search box of the OCI Console to find out the parent resource of the VNIC

C. Use OCI CLI to delete the VNIC first and then delete the subnet

D. Use OCI CLI to delete the subnet using --force option

Correct Answer: A

VCN, it must first be empty and have no related resources or attached gateways To delete a VCN\\'s subnets, they must first be empty. Note: When you create one of the preceding resources, you specify a VCN and subnet for it. The relevant service creates at least one VNIC in the subnet and attaches the VNIC to the resource. The service manages the VNICs on your behalf, so they are not readily apparent to you in the Console. The VNIC enables the resource to communicate with other resources over the network.

Although this documentation commonly talks about the resource itself being in the subnet, it\\'s actually the resource\\'s attached VNIC. If the subnet is not empty, you instead get an error indicating that there are still resources that you must delete first. The error includes the OCID of a VNIC that is in the subnet (there could be more, but the error returns only a single VNIC\\'s OCID). You can use the Oracle Cloud Infrastructure command line interface (CLI) or another SDK or client to call the GetVnic operation with the VNIC OCID. The response includes the VNIC\\'s display name. Depending on the type of parent resource, the display name can indicate which parent resource the VNIC belongs to. You can then delete that parent resource, or you can contact your administrator to determine who owns the resource. When the VNIC\\'s parent resource is deleted, the attached VNIC is also deleted from the subnet. If there are remaining VNICs in the subnet, repeat the process of determining and deleting each parent resource until the subnet is empty. Then you can delete the subnet. For example, if you\\'re using the CLI, use this command to get information about the VNIC. oci network vnic get --vnic-id