1Z0-997-22 Q&As

Oracle Cloud Infrastructure 2022 Architect Professional

Pass Oracle 1Z0-997-22 Exam with 100% Guarantee

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

https://www.pass2lead.com/1z0-997-22.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Oracle Official Exam Center

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.

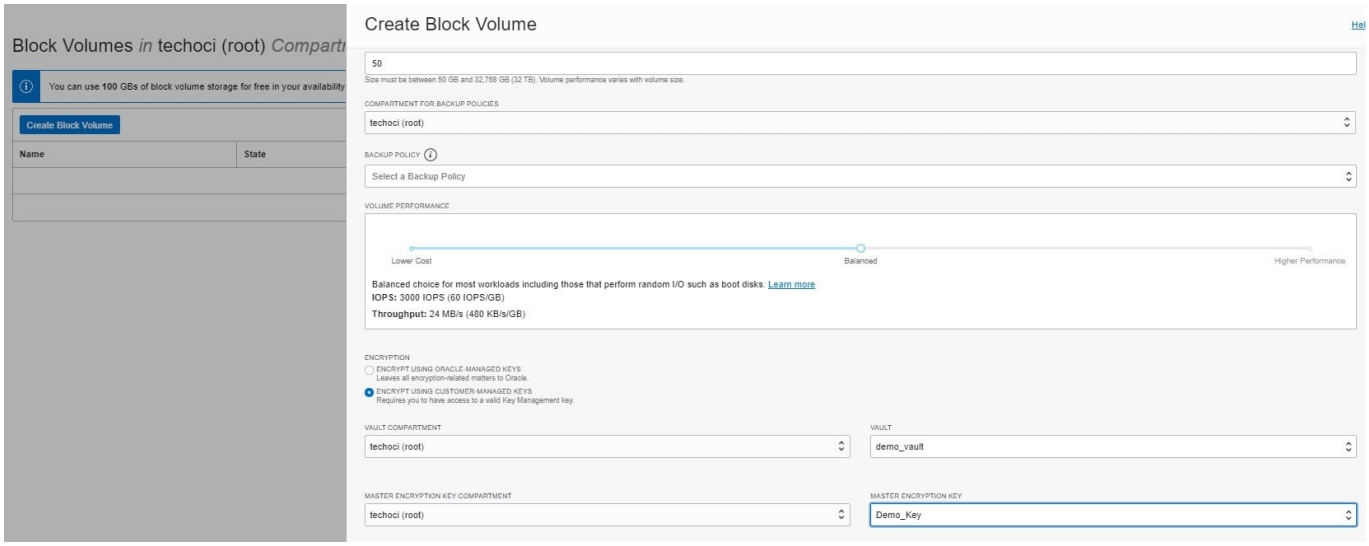
Correct Answer: BD

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.

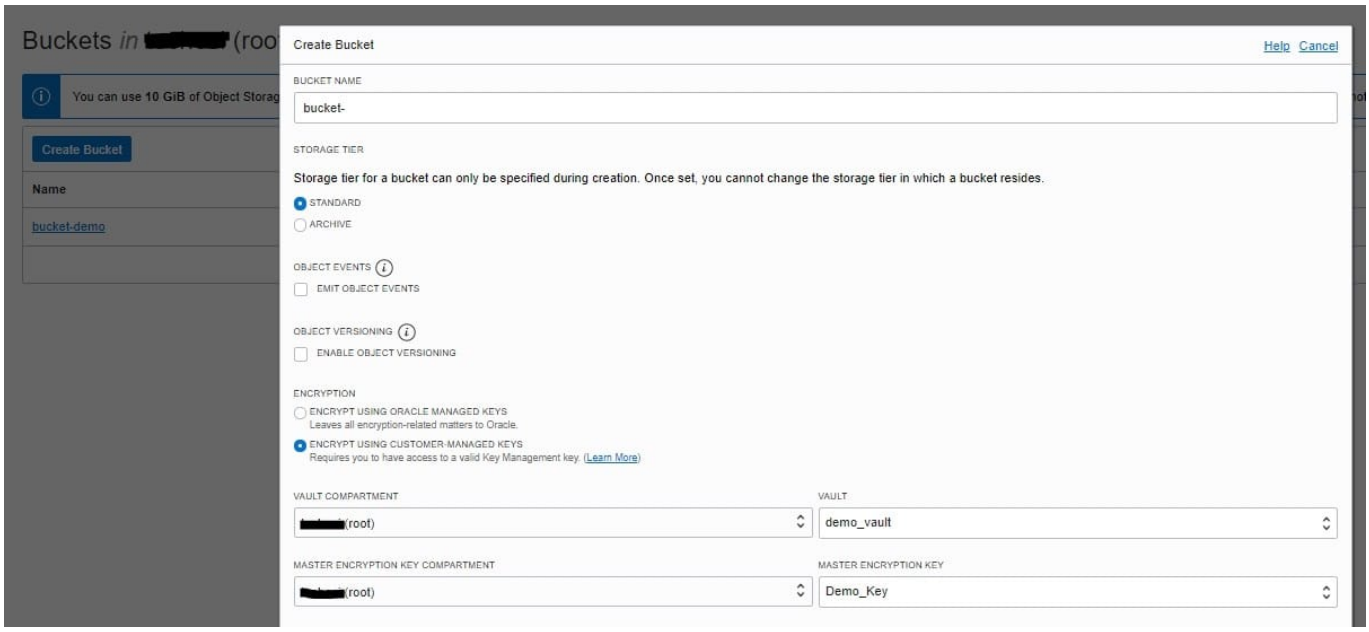
You have the option to encrypt all of your volumes and their backups using the keys that you own and manage using the Vault service.If you do not configure a volume to use the Vault service or you later

unassign a key from the volume, the Block Volume service uses the Oracle-provided encryption key instead.



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.



QUESTION 2

An organization has its IT infrastructure in a hybrid setup with an on-premises environment and an Oracle Cloud Infrastructure (OCI) Virtual Cloud Network (VCN) in the us-phonix-1 region. The on-premise applications communications with compute instances inside the VPN over a hardware VPN connection. They are looking to implement an Intrusion detected and Prevention (IDS/IPS) system for their OCI environment. This platform should have the ability to scale to thousands of compute of instances running inside the VCN. How should they architect their solution on OCI to achieve this goal?

A. Set up an OCI Private Load Balance! and configure IDS/IPS related health checks at TCP and/or HTTP level to inspect traffic

B. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform to inspection

C. There Is no need to implement an IPS/IDS system as traffic coming over IPSec VPN tunnels Is already encrypt

D. Configure autoscaling on a compute Instance pool and set vNIC to promiscuous mode to called traffic across the vcn and send it IDS/IPS platform for inspection.

Correct Answer: B

in Transit routing through a private IP in the VCN you set up an instance in the VCN to act as a firewall or intrusion detection system to filter or inspect the traffic between the on- premises network and Oracle Services Network.

The Networking service lets you implement network security functions such as intrusion detection,

application-level firewalls In fact, the IDS model can be host-based IDS (HIDS) or network- based IDS (NIDS). HIDS is installed at a host to periodically monitor specific system logs for patterns of intrusions. In contrast, an NIDS sniffs the

traffic to analyze suspicious behaviors. A signature-based NIDS (SNIDS) examines the traffic for patterns of known intrusions. SNIDS can quickly and reliably diagnose the attacking techniques and security holes without generating an overwhelming number of false alarms because SNIDS relies on known signatures.

However, anomaly-based NIDS (ANIDS) detects unusual behaviors based on statistical methods. ANIDS

could detect symptoms of attacks without specific knowledge of details. However, if the training data of the

normal traffic are inadequate, ANIDS may generate a large number of false alarms.

QUESTION 3

You are the security architect for a medium sized e-commerce company that runs all of their applications in Oracle Cloud Infrastructure (OCI). Currently, there are 14 unique applications, each deployed and secured in their own compartment. The Operations team has procured a new monitoring tool that will be deployed throughout the OCI ecosystem. Their requirement is to deploy one management node into each compartment.

Currently, the Operations team Identity and Access Management (IAM) group has the following policy: allow group OpsTeam to READ all-resources in tenancy

Once the new monitoring nodes are deployed, the Operations team may need to stop, start, or reboot them occasionally.

What is the most efficient solution to allow the Operations team to fully manage the monitoring nodes, without allowing them to alter other resources across the tenancy?

A. In each of the 14 compartments, create a new policy with the following statement: allow group OpsTeam to manage instance-family in compartment XXX where XXX is the name of the compartment where you are creating the policy.

B. Create a new policy in the root compartment with the following policy statement: allow group OpsTeam to manage instance-family in tenancy where ANY (request.operation ?`UpdateInstance\\', request.operation ?`InstanceAction\\')

C. Tag all the monitoring nodes with the defined tag AllPolicy:AllowAccess:OpsTeam and write the following IAM policy: allow group OpsTeam to manage instance-family in tenancy where target.resource.tag.AllPolicy.AllowAccess ? `OpsTeam\\'

D. Tag all the monitoring nodes with the free-form tag AllowAccess:OpsTeam and write the following IAM policy: allow group OpsTeam to manage instance-family in tenancy where target.resource.tag.AllowAccess = `OpsTeam\\'

Correct Answer: A

QUESTION 4

An online registration system Is currently hosted on one large Oracle Cloud Infrastructure (OCT) Bare metal compute Instance with attached block volume to store of the users\\' data. The registration system accepts the Information from

the user, Including documents and photos then performs automated verification and processing to check it the user is eligible for registration.

The registration system becomes unavailable at tunes when there is a surge of users using the system the existing architecture needs improvement as it takes a long time for the system to complete the processing and the attached block volumes are not large enough to use data being uploaded by the users.

Which Is the most effective option to achieve a highly scalable solution?

A. Attach more Block volumes as the data volume increase, use Oracle Notification Service (ONS) to distribute tasks to a pool of compute instances working In parallel, and Auto Scaling to dynamically size the pool of Instances depending on the number of notifications received from the Notification Service. Use Resource Manager stacks to replicate your architecture to another region.

B. Change your architecture to use an OCI Object Storage standard tier bucket, replace the single bare metal instance with a Oracle Streaming Service (OSS) to ingest the Incoming requests and distribute the tasks to a group of compute Instances with Auto Scaling

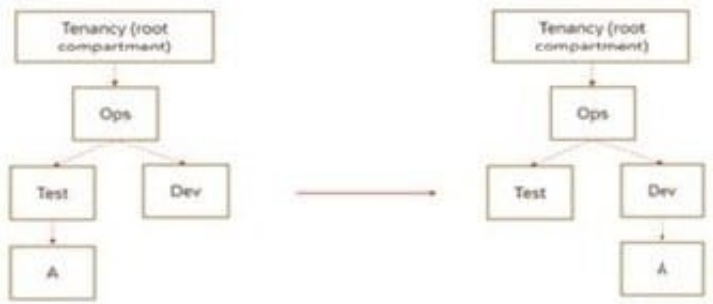
C. Upgrade your architecture to use a pool of Bare metal servers and configure them to use their local SSDs for faster data access Set up Oracle Streaming Service (OSS) to distribute the tasks to the pool of Bare metal Instances with Auto Scaling to dynamically increase or decrease the pool of compute instances depending on the length of the Streaming queue.

D. Upgrade your architecture to use more Block volumes as the data volume Increases. Replace the single bare metal instance with a group of compute instances with Auto Scaling to dynamically increase or decrease the compute instance pools depending on the traffic.

Correct Answer: D

QUESTION 5

Your customer has gone through a recent reorganization. As part of this change, they are organizing their Oracle Cloud Infrastructure (OCI) compartment structure to align with the company\\'s new organizational structure. (Refer to the exhibit)



They have made the following change:

Compartment A is moved, and its new parent compartment is compartment Dev.

Policy defined in compartment A: Allow group G1 to manage instance-family in compartment A

Policy defined in root compartment: Allow group admins to manage instance-family in compartment Ops: Test: A

After the compartment move, which action will provide users of group G1 and admins with similar privileges as before

the move?

A. Define the following policy in compartment Dev: Allow group G1 to manage instance-family in compartment A

B. Define the following policies in compartment Dev: Allow group G1 to manage instance-family in compartment A Allow group admins to manage instance-family in compartment Ops: Dev: A

C. Define the following policy in compartment: Dev: Allow group admins to manage instance-family in compartment Ops: Dev: A

D. Mo change in any policy statement is required as all the policies associated with a compartment being moved is automatically updated

Correct Answer: A