Exam : **1z0-1104-23**

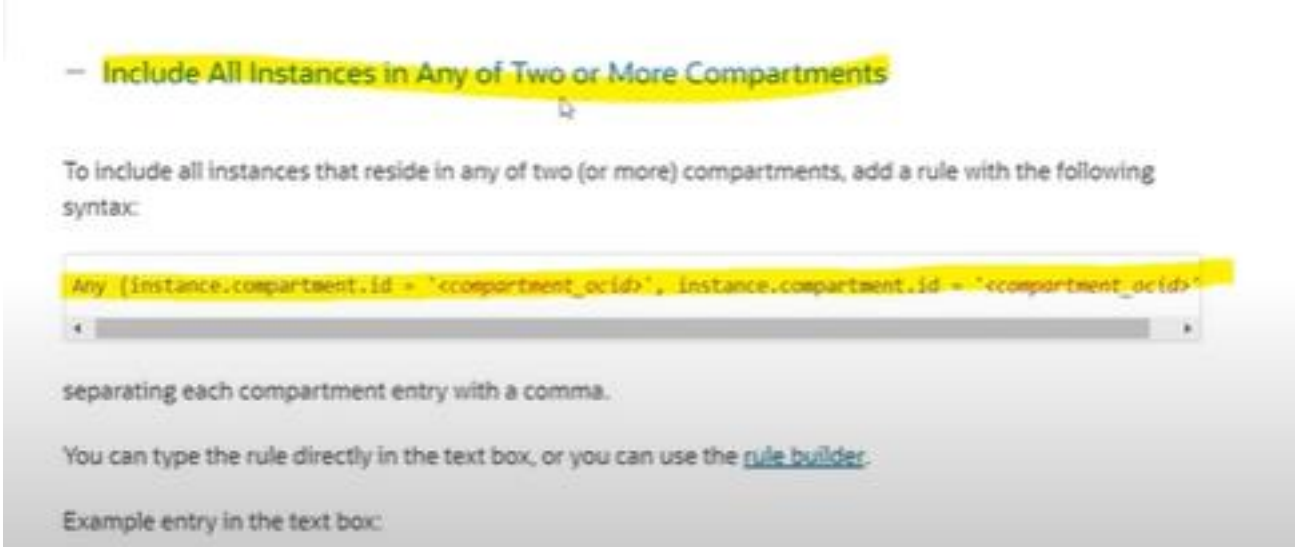
Title : Oracle Cloud Infrastructure 2023 Security Professional

Vendor : Oracle

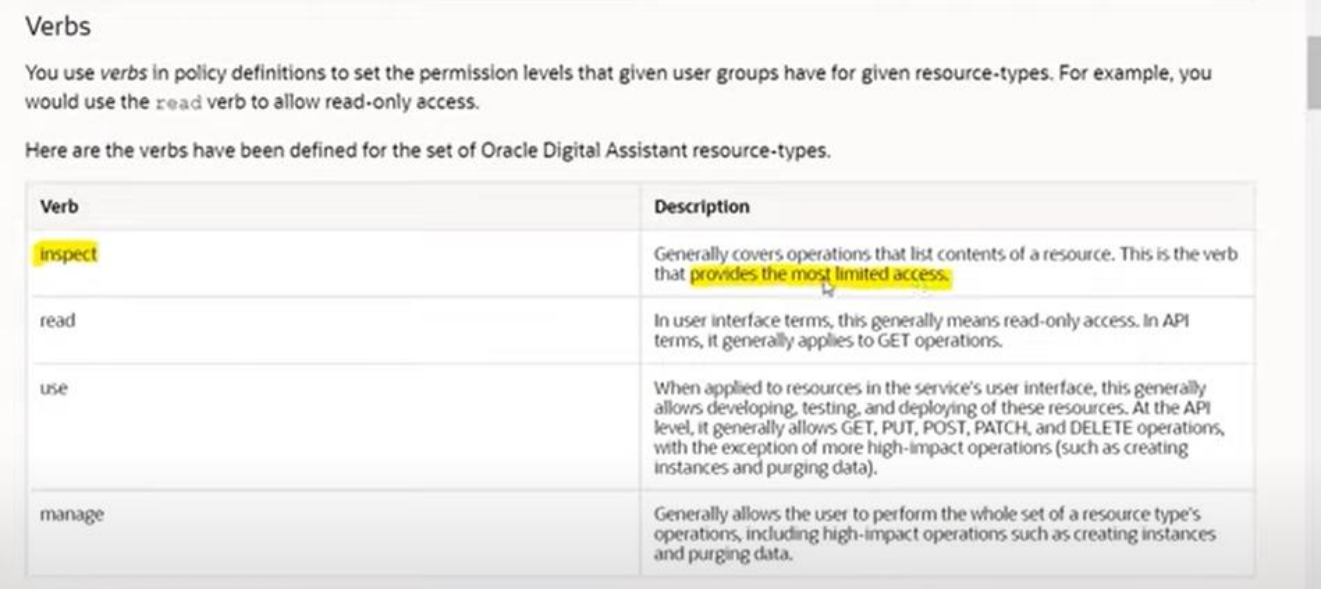
Version : DEMO

NO.1 Which three Oracle Cloud Infrastructure (OCI) services are covered by Cloud Guard? (Choose three.)
A. Oracle Integration Osud (OIC)
B. Blockchain
C. Object Storage
D. Database Cloud Service
E. Identity and Access Management (IAM)
Answer: C,D,E

NO.2 You want to include all instances in any of two or morecompartments, which syntax should you use for dynamic policy you want to create for "Prod" compartment and "SIT" compartment?
Prod OCID : 'JON.Prod'
SIT OCID : 'JON.SIT'
A. Any { instance in compartment 'Prod' and Compartment 'SIT' }
B. Any { instance.compartment.id = 'JON.Prod', instance.compartment.id = 'JON.SIT'
C. All { instance.compartment.id = 'JON.Prod', instance.compartment.id = 'JON.SIT'
D. All { instance in compartment 'Prod' and Compartment 'SIT' }
Answer: B
Explanation:



NO.3 Which IAM policy should be created to give XYZ the ability to list contents of a resource excluding the fneeds to authenticatein prod compartment ? Principle of least priviledge should be used.
A. Allow group XYZ to manage all resources in compartment != prod
B. Allow group XYZ to use all resources in compartment != prod
C. Allow group XYZ to inspect all resources in tenancy where target.compartment.name != prod
D. Allow group XYZ to read all resources in tenancy where target.compartment.name != prod
Answer: C
Explanation:



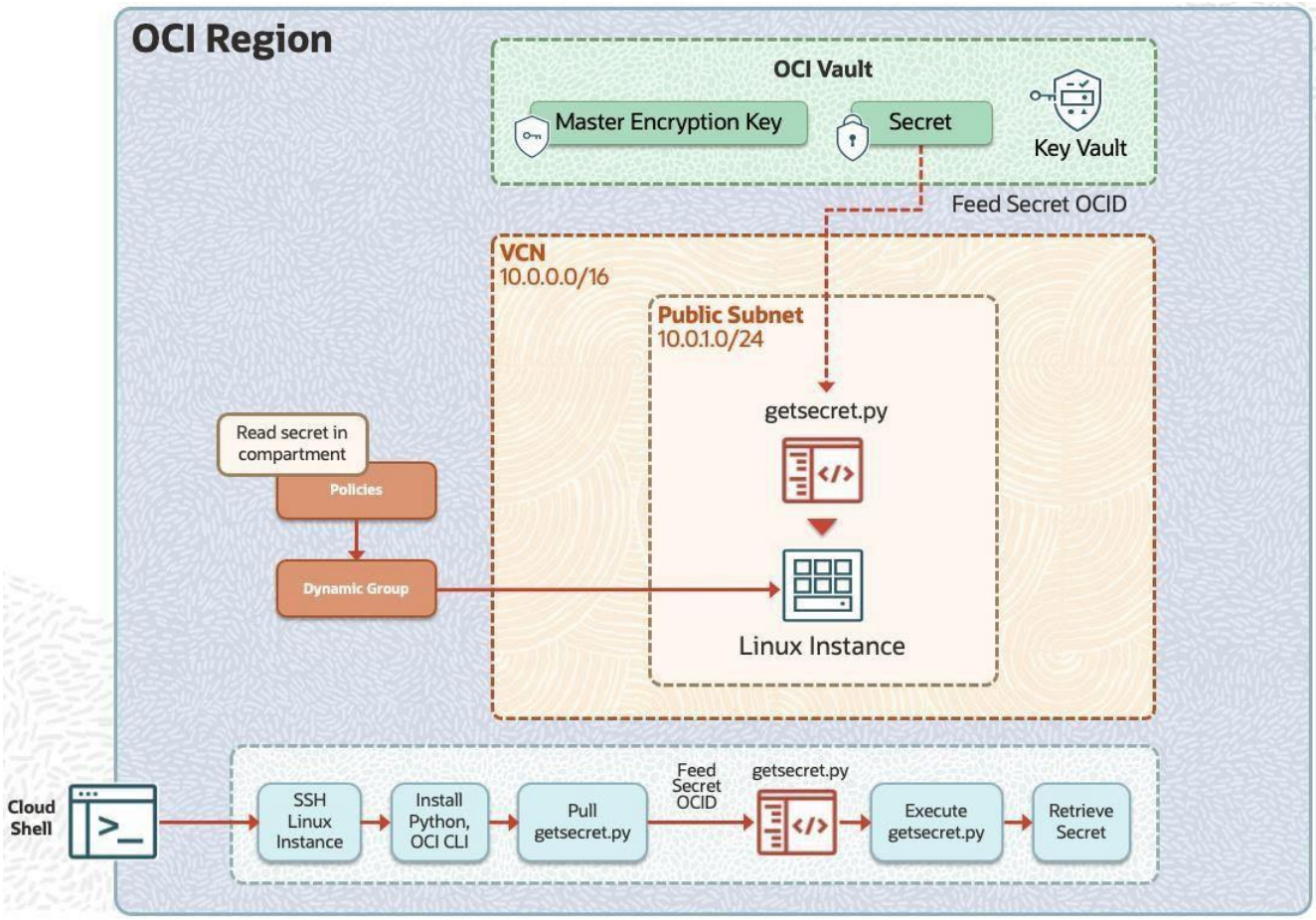
Verbs

You use *verbs* in policy definitions to set the permission levels that given user groups have for given resource-types. For example, you would use the `read` verb to allow read-only access.

Here are the verbs have been defined for the set of Oracle Digital Assistant resource-types.

Verb	Description
inspect	Generally covers operations that list contents of a resource. This is the verb that provides the most limited access.
read	In user interface terms, this generally means read-only access. In API terms, it generally applies to GET operations.
use	When applied to resources in the service's user interface, this generally allows developing, testing, and deploying of these resources. At the API level, it generally allows GET, PUT, POST, PATCH, and DELETE operations, with the exception of more high-impact operations (such as creating instances and purging data).
manage	Generally allows the user to perform the whole set of a resource type's operations, including high-impact operations such as creating instances and purging data.

NO.4 Challenge 1 - Task 5 of 5
Authorize OCI Resources to Retrieve the Secret from the Vault
Scenario
You are working on a Python program running on a compute instance that needs to access an external service. To access the external service, the program needs credentials (password). Given that it is not a best security practice, you decide not to hard code the credential in the program. Instead, you store the password (secret) in a vault using the OCI Vault service. The requirement now is to authorize the compute instance so that the Python program can retrieve the password (secret) by making an API call to the OCI Vault.



Preconfigured
To complete this requirement, you are provided with:
An OCI Vault to store the secret required by the program, which is created in the root compartment as PBT_Vault_SP.
An instance principal IAM service, which enables instances to be authorized actors (principals) that can retrieve the secret from the OCI Vault.
A dynamic group named PBT_Dynamic_Group_SP with permissions to access the OCI Vault. This dynamic group includes all of the instances in your compartment.
Access to Cloud Shell.
Permissions to perform only the tasks within the challenge.
Note: You are provided with access to an OCI Tenancy, an assigned compartment, and OCI credentials. Throughout your exam, ensure to use the assigned Compartment 99234021-C01 and Region us-ashburn-1.

Answer:

See the solution below in Explanation
Explanation:
SOLUTION:
Select the Developer Tools icon at the right of the OCI console header and click Cloud Shell to launch your Cloud Shell.
While Cloud Shell is launching, take a moment to locate the public and private keys that you downloaded to your workstation in the previous section.
Example Public Key name: ssh-key-<date>.key.pub
Example Private Key name: ssh-key-<date>.key

Once the Cloud Shell window is open, upload the private key to the Cloud Shell:
Click the Settings icon in the top-right corner of the Cloud Shell window and click Upload.
Navigate to and select the private key. Either drag the private key to the Drop a file window or click Select from your computer, select the private key, and click Upload.
Change the private key permissions by issuing the following command:
chmod 400 <private key name>.key
Retrieve the Public IP address of the instance that you created in the previous section and paste it to connect to the instance using the opc user in the Cloud Shell.
ssh -i <private key name> opc<public IP address of instance>
After connecting to the compute instance, run the following commands to install/verify Python and OCI CLI packages on the Linux Instance.
sudo dnf -y install oraclelinux-developer-release-el8
sudo dnf install python36-oci-cli
After installing Python and the required dependencies, download the Python script to retrieve the secret.
wget https://objectstorage.us-ashburn-1.oraclecloud.com/n/ocuocictrng5/b/PBT_Storage/o/getsecret.py Open a Python file with a nano editor.
nano getsecret.py
In the Python script, replace the secret ID ocid with your secret ID.
Replace secret id value below with the ocid of your secret secret id = <secret id> For example: Secret id = "ocid1.vaultsecret.oci.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx Note: if you have not already copied the secret ID, go to Vault and select the Secret link from the resources. Then, in List Scope, choose <your working compartment>, click your secret key, and copy the OCID.
To save the script hit:
Ctrl+o > Enter [To write/save]
Ctrl+x > Yes > Enter [To exit]
Make the getsecret .py script executable.
chmod +x getsecret.py
Run the following command to retrieve the secret:
python getsecret.py
The secret content created in the vault has been retrieved by the application running on the instance. Instance Principal and the Vault enable you to abstract the difficulty of developing your own security strategy for storing and encrypting passwords and other sensitive information.

NO.5 Which are the three prerequisites for successfully configuring a Bastion managed SSH ses-sion to a compute instance in a private subnet? (Choose three.)

A. The compute instance must have the Bastion cloud agent enabled.

B. The private subnet must have a service or NAT gateway.

C. The private subret must not have any gateway in it

D. The SSH port forwarding feature needs to be enabled

E. The compute instance must have the Bastion cloud agent disabled

F. The route table associated with the subnet needs to have a route rule to a service or NAT gateway.

Answer: A,B,F

NO.6 Which type of FastConnect supports configuring Oracle Cloud Infrastructure (OCI) Site-to-Site

VPN for encryption? (Choose the best Answer.)

A. FastConnect Public Peering

B. FastConnect Cross-Connect group

C. FastConnect Privat Peering

D. FastConnect Partner

Answer: A

NO.7 Which Cloud Guard component identifies issues with resources or user actions and alerts you when an issue is found?

A. Problems

B. Targets

C. Detectors

D. Responders

Answer: C

Explanation:

Detector

Performs checks to identify potential security problems based on activities or configurations. Rules followed to identify problems are the same for allcompartments in a target.

https://docs.oracle.com/en-us/iaas/cloud-guard/using/part-start.htm

NO.8 Select the component that encompasses the overall configuration of your WAF service on OCI.

A. Protection rules

B. Bot Management

C. Web Application Firewall policy

D. Origin

Answer: C

Explanation:

WAF Policy Management

Provides an overview of web application firewall (WAF) policies, including their creation, updating, and deletion.

WAF policies encompass the overall configuration of your WAF service, includingaccess rules, rate limiting rules, and protection rules.

https://docs.oracle.com/en-us/iaas/Content/WAF/Policies/waf-policy_management.htm

NO.9 When configuring inter-tenancy virtual cloud network (VCN) peering using local peering gateways (LPG), which OCID do you need from the other tenancy to properly configure the Requestor and Acceptor identity Access Management (IAM) policies? (Choose the best Answer.)

A. Local Peening Gateway OCID

B. Tenancy OCID

C. Virtual Cloud Network OCID

D. Compartment OCID

E. Local Peering Connection OCIO

Answer: A

NO.10 How do you enable server-side encryption in an Oracle Cloud Infrastructure (OCI) Object Storage bucket? (Choose the best Answer.)

A. By uploading your encryption key to OCI Vault and associating it with the bucket you want to encrypt.

B. By updating the buckets metadata value for encrypted_bucket to "true"

C. By default, server-side encryption is enabled and requires no user action.

D. By uploading encrypted objects will enable the encryption in the objects.

Answer: C

NO.11 Which two responsibilities must be taken care of by a customer while managing Web Application Firewall (WAF)? (Choose two.)

A. Onboard and configure the WAF policy for the web application

B. Import new Open Web Application Security Project (OWASP) Core Rule Sets (CRS) as they are released

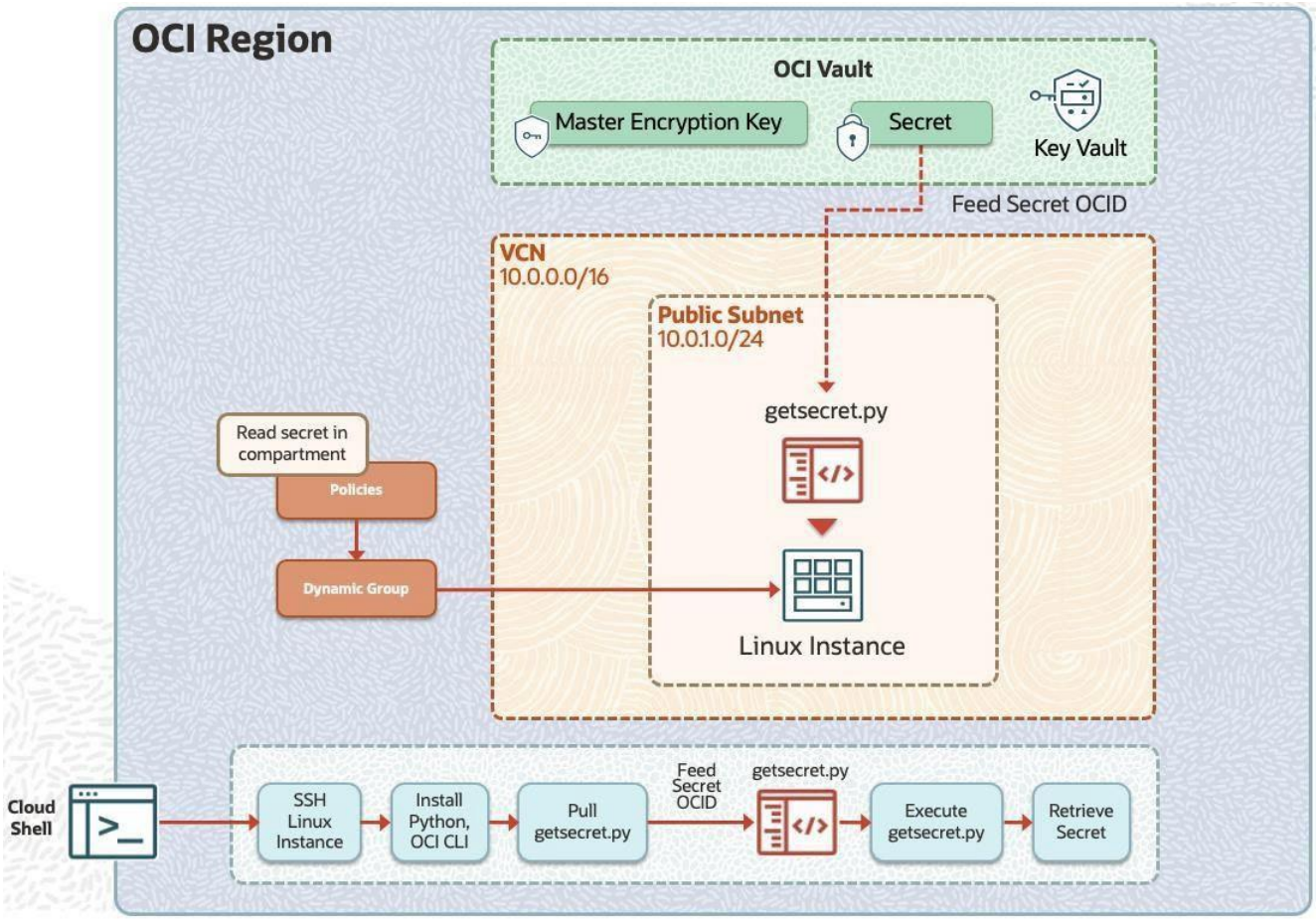
C. Tune WAF's access rules and bot management strategies according to the web application traffic

D. Provide High Availability (HA) for the WAF edge nodes.

E. Patch their WAF instance when Oracle makes faxes available.

Answer: A,C

NO.12 Challenge 1 - Task 2 of 5
Authorize OCI Resources to Retrieve the Secret from the Vault
Scenario
You are working on a Python program running on a compute instance that needs to access an external service. To access the external service, the program needs credentials (password). Given that it is not a good security practice, you decide not to hard code the credential in the program. Instead, you store the password (secret) in a vault using the OCI Vault service. The requirement now is to authorize the compute instance so that the Python program can retrieve the password (secret) by making an API call to the OCI Vault.



Preconfigured:
To complete this requirement, you are provided with:
An OCI Vault to store the secret required by the program, which is created in the root compartment as PBT_Vault_SP.
An instance principal IAM service, which enables instances to be authorized actors (principals) that can retrieve the secret from the OCI Vault.
A dynamic group named PBT_Dynamic_Group_SP with permissions to access the OCI Vault. This dynamic group includes all of the instances in your compartment.
Access to Cloud Shell.
Permissions to perform only the tasks within the challenge.
Note: You are provided with access to an OCI Tenancy, an assigned compartment, and OCI credentials. Throughout your exam, ensure to use the assigned Compartment 99234021-C01 and Region us-ashburn-1.
Complete the following task:
In the field below, write the IAM policy, which allows a program running on a computer instance (principal instance) to retrieve a secret from the OCI Vault.

Answer:

See the solution below in Explanation
Explanation:
ALLOW dynamic-group PBT_Dynamic_Group_SP TO read secret-family IN COMPARTMENT 99234021-C01

NO.13 What does the following identity policy do?

Allow group my-group to use fn-invocation in compartment ABC where target.function.id = '<function-OCID>'

A. Enables users in a group to create, update, and delete ALL applications and functions in a compartment

B. Enables users to invoke all the functions in a specific application

C. Enables users to invoke just one specific function

D. Enables users to invoke all the functions in a compartment except for one specific function

Answer: C

Explanation:

The policy Allow group my-group to use fn-invocation in compartment ABC where target.function.id = '<function-OCID>' gives the group my-group permission to invoke a specific function (identified by its OCID) in the compartment ABC. The fn-invocation verb allows a group to invoke a function, and the condition where target.function.id = '<function-OCID>' ensures that only the specified function can be invoked by this group

NO.14 You have subscribed to a tenancy, in which you want to isolate the OCI resources from different users logically for governance. Which OCI resource will help you achieve logical separation? (Choose the best Answer.)

A. Compartment

B. Dynamic Group

C. Fault Domain

D. Availability Domain

Answer: A

NO.15 A company plans to use Oracle Cloud services for their production and development environments, but they have different security requirements. Their security policy forbids development environment users from having access to the production environment and requires separate administrators to manage each environment. The company has only one tenancy in Oracle Cloud. How can they ensure that their security requirements are met in Oracle Cloud? (Choose the best Answer.)

A. Create multiple identity domains, one for the production environment and another for the development environment.

B. Use a single identity domain for both production and development environments to simplify administration.

C. Assign the same identity domain administrator to both the production and development environments.

D. Create a separate tenancy for the production environment to isolate administrative control.

Answer: A

NO.16 Which tasks can you perform on a dedicated virtual machine host?

A. Manual scaling

B. Creating instance pools

C. Instance configurations

D. Capacity reservations

Answer: A
Explanation:
Supported features: Most of the Compute features for VM instances are supported for instances running on dedicated virtual machine hosts. However, the following features arenot supported:
Autoscaling
Capacity reservations
Instance configurations
Instance pools
Burstable instances
Reboot migration. You can use manual migration instead
https://docs.oracle.com/en-us/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm#Dedicated_Virtual_Machine_Hosts

NO.17 You are a security administrator for your company's Oracle Cloud Infrastructure (OCI) tenancy. Your storage administrator tells you he or she cannot associate an encryption key from OCI Voult to an Object Storage bucket in the new compartment. What is the reason? (Choose the best Answer.)

A. There is no identity and Access Management (IAM) policy that allows the Object Store service to use the key.

B. The secret for the key was not created beforehand.

C. The storage administrator forgot to select "Oracle Managed on the bucket

D. The resource bucket policy lacks the necessary Access Control List (ACL)

Answer: A