DUMPSBOSS.

Oracle Cloud Infrastructure 2020 Cloud Operations Associate

Oracle 1z0-1067-20

Version Demo

Total Demo Questions: 10

Total Premium Questions: 73

Buy Premium PDF

https://dumpsboss.co

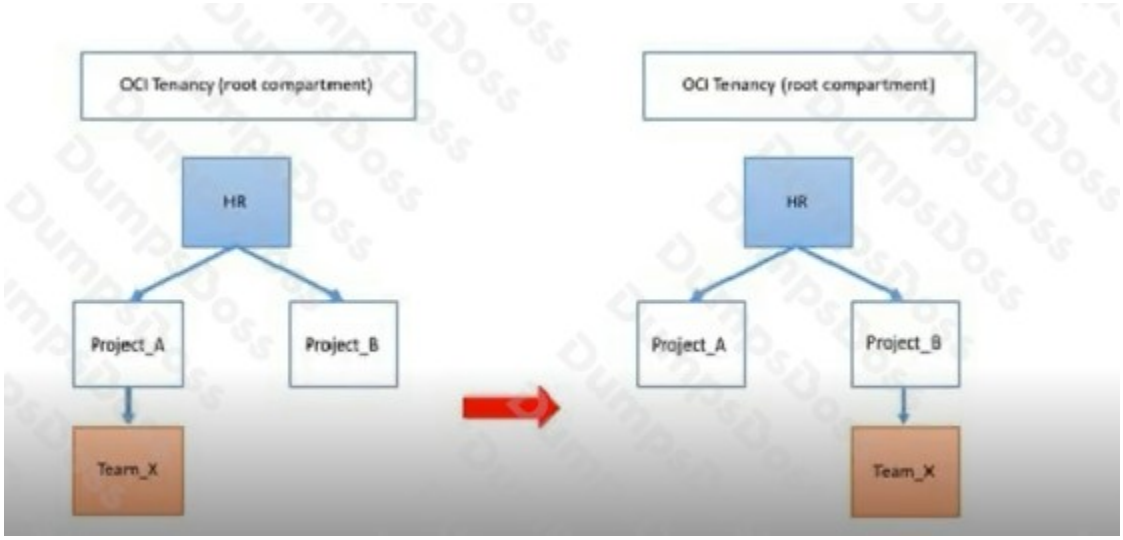
support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Your company has restructured its HR departments. As part of this change, you also need to re-organize compartments within Oracle Cloud Infrastructure (OCI) to align them to the company's new organizational structure. The following change is required:

Comportment Team_x needs to be moved under a new parent compartment, Project_B



The tenancy has the following policies defined for compartments Project_A and Project_B: Policy1 Allow group G1 to manage instance-family in compartment HR:Project_A

Policy2 Allow group G2 to manage instance-family in compartment HR:Project_B Which two statements describe the impacts after the compartment Team_x is moved?

A. Group G2 can now manage instance-families in compartment Project_B compartment Project_A and compartment Team_x

B. Group G1 can now manage instance-families in compartment Project_A but not in compartment Team_x

C. Group G1 can now manage instance-families in compartment project_A,compartment project_B and compartment Team_x

D. Group G2 can now manage instance-families in compartment Project_B and compartment Team_x

E. Group G2 can now manage instance-families in compartment Project_A but not in compartment Team_x

ANSWER: B D

Explanation:

Understanding the Policy Implications When You Move a Compartment

After you move a compartment to a new parent compartment, the access policies of the new parent take effect and the policies of the previous parent no longer apply. Before you move a compartment, ensure that:

- You are aware of the policies that govern access to the compartment in its current position.

- You are aware of the polices in the new parent compartment that will take effect when you move the compartment.

Groups with Permissions in the Current Compartment Lose Access; Groups with Permissions in the Destination Compartment Gain Access

QUESTION NO: 2

Security testing Policy describes when and how you may conduct certain types of security testing of Oracle Cloud Services, Including vulnerability and penetration tests, as well as tests Involving data scraping tools.

What does Oracle allow as part of this testing?

A. Customers can simulate DoS attack scenarios as long as Its restricted to the customer's own environment.

B. Customers are allowed to test Oracle Cloud Infrastructure (OCI) hardware related to resources in their tenancy.

C. Customers are allowed to use their own testing and monitoring tools.

D. Customers can validate that their network resources are isolated from other customer resources.

ANSWER: C

Explanation:

Penetration and Vulnerability Testing

Oracle regularly performs penetration and vulnerability testing and security assessments against the Oracle cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle Cloud Services.

However, Oracle does not assess or test any components (including, non-Oracle applications, non-Oracle databases or other non-Oracle software, code or data, as may be applicable) that you manage through or introduce into – including introduction through your development in or creation in - the Oracle Cloud Services (the “Customer Components”). This policy does not address or provide any right to conduct testing of any third party materials included in the Customer Components.

Except as otherwise permitted or restricted in your Oracle Cloud Services agreements, your service administrator who has system level access to your Oracle Cloud Services may run penetration and vulnerability tests for the Customer Components included in certain of your Oracle Cloud Services in accordance with the following rules and restrictions.

Permitted Cloud Penetration and Vulnerability Testing

The following explains where penetration and vulnerability testing of Customer Components is permitted:

IaaS: Using your own monitoring and testing tools, you may conduct penetration and vulnerability tests of your acquired single-tenant Oracle Infrastructure as a Service (IaaS) offerings. You must notify Oracle prior to conducting any such penetration and vulnerability tests in accordance with the process set forth below.

Pursuant to such penetration and vulnerability tests, you may assess the security of the Customer Components; however, you may not assess any other aspects or components of these Oracle Cloud Services including the facilities, hardware, software, and networks owned or managed by Oracle or its agents and licensors.

PaaS: Using your own monitoring and testing tools, you may conduct penetration and vulnerability tests of your acquired single-tenant PaaS offerings. You must notify Oracle prior to conducting any such penetration

and vulnerability tests in accordance with the process set forth below. Pursuant to such penetration and vulnerability tests, you may assess the security of the Customer Components; however, you may not assess any other aspects or components of these Oracle Cloud Services including the facilities, hardware, networks, applications, and software owned or managed by Oracle or its agents and licensors. To be clear, you may not assess any Oracle applications that are installed on top of the PaaS service.

SaaS: Penetration and vulnerability testing is not permitted for Oracle Software as a Service (SaaS) offerings. Rules of Engagement

The following rules of engagement apply to cloud penetration and vulnerability testing:

Your testing must not target any other subscription or any other Oracle Cloud customer resources, or any shared infrastructure components.

You must not conduct any tests that will exceed the bandwidth quota or any other subscribed resource for your subscription.

You are strictly prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such, or any “load testing” against any Oracle Cloud asset including yours.

Any port scanning must be performed in a non-aggressive mode.

You are responsible for independently validating that the tools or services employed during penetration and vulnerability testing do not perform DoS attacks, or simulations of such, prior to assessment of your instances. This responsibility includes ensuring any contracted third parties perform assessments in a manner that does not violate this policy.

Social Engineering of Oracle employees and physical penetration and vulnerability testing of Oracle facilities is prohibited.

You must not attempt to access another customer’s environment or data, or to break out of any container (for example, virtual machine).

Your testing will continue to be subject to terms and conditions of the agreement(s) under which you purchased Oracle Cloud Services, and nothing in this policy shall be deemed to grant you additional rights or privileges with respect to such Cloud Services.

QUESTION NO: 3

You have set up threshold alarm for CPU Utilization metric for a value greater than 80 percent. You get a notification email about this alarm.

Which of the following action will help you respond to this notification?

A. Modify the alarm to route notifications to Oracle Cloud Infrastructure Streaming Service (OSS) for later Investigation.

B. Modify the alarm to route notifications to an Oracle Cloud Infrastructure Object Storage bucket for later investigation.

C. Change at-risk threshold for the CPU utilization metric to a lower number.

D. Suppress the alarm notifications temporarily.

ANSWER: D

Explanation:

A typical at-risk threshold for the CpuUtilization metric is any value greater than 80 percent. A Compute instance breaching this threshold is at risk of becoming inoperable. Often the cause of this behavior is one or more applications consuming a high percentage of the CPU.

In this example, you decide to notify the operations team immediately, setting the severity of the alarm as “Critical” because repair is required to bring the instances back to optimal operational levels. You configure alarm notifications to the responsible team by both PagerDuty and email, requesting an investigation and appropriate fixes before the instances go into an inoperable state. You set repeat notifications every minute. When someone responds to the alarm notifications, you temporarily stop notifications using the best practice of suppressing the alarm . Once metrics return to optimal values, you remove the suppression

Suppress Alarms During Investigations

Once a team member responds to an alarm, suppress notifications during the effort to investigate or mitigate the issue. Temporarily stopping notifications helps to avoid distractions during the investigation and mitigation. Remove the suppression when the issue has been resolved.

This topic describes best practices for working with alarms .

https://docs.cloud.oracle.com/en-us/iaas/Content/Monitoring/Concepts/alarmsbestpractices.htm

QUESTION NO: 4

Which two statements are true about Oracle Cloud Infrastructure Compute Service? (Choose two.)

A. You cannot launch a bare metal server in Oracle Cloud Infrastructure Compute Service

B. You can attach a block volume in an Availability Domain other than your compute instance

C. You can share custom images across tenancies and regions

D. You can launch a virtual or bare metal instance by using the same LaunchInstance API

ANSWER: C D

Explanation:

Regions and Availability Domains Volumes are only accessible to instances in the same availability domain . You cannot move a volume between availability domains or regions.

QUESTION NO: 5

One of your development teams has asked for your help to standardize the creation of several compute instances that must be provisioned each day of the week. You initially write several Command Line Interface (CLI) commands with all appropriate configuration parameters to achieve this task later determining this method lacks flexibility.

Which command generates a JSON-based template that Oracle Cloud Infrastructure (OCI) CLI can use to provision these Instances on a regular basis?

A. oci compute provision-Instance — generate-full-command-Json-Input

B. oci compute instance create --generate-cll-skeleton

C. oci compute instance launch --generate-cll-skeleton

D. oci compute instance launch --generate-full-command-json-input

ANSWER: D

Explanation:

Use --generate-full-command-json-input. To generate the JSON for launching an instance, run the following command.

oci compute instance launch --generate-full-command-json-input https://docs.cloud.oracle.com/en-us/iaas/Content/API/SDKDocs/cliusing.htm

QUESTION NO: 6

You are using Oracle Cloud Infrastructure (OCI) console to set up an alarm on a budget to track your OCI spending. Which two are valid targets for creating a budget In OCI?

A. Select Tenancy as the type of target for your budget.

B. Select Cost-Tracking Tags as the type of target for your budget.

C. Select Compartment as the type of target for your budget.

D. Select group as the type of target for your budget.

E. Select user as the type of target for your budget.

ANSWER: B C

Explanation:

The following concepts are essential to working with budgets:

BUDGET

A monthly threshold you define for your Oracle Cloud Infrastructure spending. Budgets are set on

cost-tracking tags or compartments and track all spending in the cost-tracking tag or compartment and any child compartments. Note: the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.

ALERT

You can define email alerts that get sent out for your budget. You can send a customized email message body with these alerts. Alerts are evaluated every 15 minutes, and can be triggered when your actual or your forecasted spending hits either a percentage of your budget or a specified set amount

Select the target for your budget

For budgets targeting a compartment: Select a target compartment for your budget from the Target Compartment drop-down list. Note that while the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.

For budgets targeting a cost-tracking tag: Select a tag namespaceSelect a target cost-tracking tag key.Enter a value for the cost-tracking tag.

QUESTION NO: 7

You have the following compartment structure within your company's Oracle Cloud Infrastructure (OCI) tenancy:

You want to create a policy in the root compartment to allow SystemAdmins to manage VCNs only In CompartmentC.

Which policy is correct?

A. Allow group SystemAdmins to manage virtual-network-family in compartment CompartmentC

B. Allow group SystemAdmins to manage virtual-network-family in compartment CompartmentB:CompartmentC

C. Allow group SystemAdmins to manage virtual-network-family in compartment CompartmentA:CompartmentB:CompartmentC

D. Allow group SystemAdmins to manage virtual-network-family in compartment Root

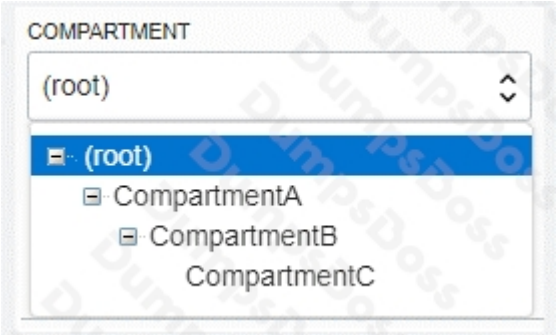
ANSWER: C

Explanation:

a policy statement must specify the compartment for which access is being granted (or the tenancy). Where you create the policy determines who can update the policy. If you attach the policy to the compartment or its

parent, you can simply specify the compartment name. If you attach the policy further up the hierarchy, you must specify the path. The format of the path is each compartment name (or OCID) in the path, separated by a colon:

:: . . . For example, assume you have a three-level compartment hierarchy, shown here:



You want to create a policy to allow NetworkAdmins to manage VCNs in CompartmentC. If you want to attach this policy to CompartmentC or to its parent, CompartmentB, write this policy statement:

Allow group NewtworkAdmins to manage virtual-network-family in compartment CompartmentC

However, if you want to attach this policy to CompartmentA (so that only administrators of CompartmentA can modify it), write this policy statement that specifies the path:

Allow group NewtworkAdmins to manage virtual-network-family in compartment CompartmentB:CompartmentC

To attach this policy to the tenancy, write this policy statement that specifies the path from CompartmentA to CompartmentC:

Allow group NewtworkAdmins to manage virtual-network-family in compartment CompartmentA:CompartmentB:CompartmentC

QUESTION NO: 8

Which five are the required parameters to launch an instance in Oracle Cloud Infrastructure? (Choose five.)

A. private IPaddress

B. Virtual Cloud Network

C. host name

D. instance shape

E. image operating system

F. subnet

G. Availability Domain

ANSWER: B D E F G

Explanation:

https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Concepts/computeoverview.htm

QUESTION NO: 9

Which three statements are true about Object Storage data security and encryption in Oracle Cloud Infrastructure (OCI)?

A. OCI Key Management is used by default to provide data security.

B. Server side encryption uses per-object keys which are managed by Oracle.

C. All traffic to and from Object Storage service is encrypted using TLS.

D. A VPN connection to OCI is required to ensure security data transfer to an object storage bucket.

E. Client-side encryption is managed by the customer.

ANSWER: B C E

Explanation:

All data in Object Storage is encrypted at rest by using AES-256. Encryption is on by default and cannot be turned off. Each object is encrypted with its encryption key, and the object encryption keys are encrypted with a master encryption key. In addition, customers can use client-side encryption to encrypt objects with their encryption keys before storing them in Object Storage buckets. An available option for customers is to use the Amazon S3 Compatibility API, along with client-side object encryption support available in AWS SDK for Java.

Data in transit between customer clients (for example, SDKs and CLIs) and Object Storage public endpoints is encrypted with TLS 1.2 by default. FastConnect public peering allows on-premises access to Object Storage to go over a private network, rather than the public internet.

Oracle Cloud Infrastructure Key Management is a managed service the enables you, the customer, to manage and control AES symmetric keys used to encrypt your data-at-rest. Keys are stored in a FIPS 140-2, Level

3- certified, Hardware Security Module (HSM) that is durable and highly available. The Key Management service is integrated with many Oracle Cloud Infrastructure services, including Block Volumes, File Storage, Oracle Container Engine for Kubernetes, and Object Storage.

Use the Key Management service if you need to store your Master Encryption Keys in an HSM to meet governance and regulatory compliance requirements or when you want more control over the cryptoperiod of the encryption keys used for your data.

When you store your data with Oracle Cloud Infrastructure Block Volumes, File Storage Service, and Object Storage and don’t use Key Management, your data is protected using encryption keys that are securely stored and controlled by Oracle.

QUESTION NO: 10

You are tasked with creating a group called volumeBackcupAdmins to manage only block volume backups.

Which of the following set of policy/policies would you need to write to meet this requirement? A)

```
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
```

B)

```
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to use volume-attachments in tenancy
Allow group VolumeBackupAdmins to use instances in tenancy
```

C)

```
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
```

D)

```
Allow group VolumeBackupAdmins to use volumes in tenancy
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to use volume-attachments in tenancy
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: A

Explanation:

Let volume backup admins manage only backups

Type of access: Ability to do all things with volume backups, but not create and manage volumes themselves. This makes sense if you want to have a single set of volume backup admins manage all the volume backups in all the compartments. The first statement gives the required access to the volume that is being backed up; the second statement enables creation of the backup (and the ability to delete backups). The third statement enables the creation and management of user defined backup policies; the fourth statement enables assignment and removal of assignment of backup policies.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes and backups in a particular compartment, specify that compartment instead of the tenancy.

Allow group VolumeBackupAdmins to use volumes in tenancy

Allow group VolumeBackupAdmins to manage volume-backups in tenancy

If the group will be using the Console, the following policy gives a better user experience:

Allow group VolumeBackupAdmins to use volumes in tenancy

Allow group VolumeBackupAdmins to manage volume-backups in tenancy Allow group VolumeBackupAdmins to inspect volume-attachments in tenancy Allow group VolumeBackupAdmins to inspect instances in tenancy