1Z0-1104-22Q&As

Oracle Cloud Infrastructure 2022 Security Professional

Pass Oracle 1Z0-1104-22 Exam with 100% Guarantee

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

https://www.passapply.com/1z0-1104-22.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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\\'

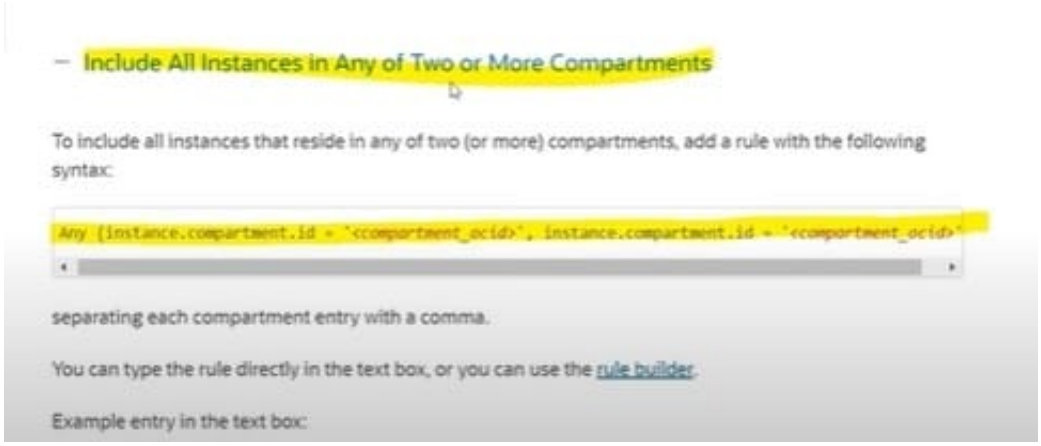
A. Any { instance in compartment `Prod\\' and Compartment \\'SIT\\' }

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\\' }

Correct Answer: B



QUESTION 2

When creating an OCI Vault, which factors may lead to select the Virtual Private Vault? Select TWO correct answers

A. Need for more than 9211 key versions

B. Greater degree of isolation

C. To mask Pll data for non-production environment

D. Ability to back up the vault

Correct Answer: BD

VAULTS

Vaults are logical entities where the Vault service creates and durably stores keys and secrets. The type of vault you have determines features and functionality such as degrees of storage isolation, access to management and encryption, scalability, and the ability to back up. The type of vault you have also affects pricing. You cannot change a vault's type after you create the vault.

The Vault service offers different vault types to accommodate your organization's needs and budget. All vault types ensure the security and integrity of the encryption keys and secrets that vaults store. A virtual private vault is an isolated partition on a hardware security module (HSM). Vaults otherwise share partitions on the HSM with other vaults.

Virtual private vaults include 1000 key versions by default. If you don't require the greater degree of isolation or the ability to back up the vault, you don't need a virtual private vault. Without a virtual private vault, you can manage costs by paying for key versions individually, as you need them. (Key versions count toward your key limit and costs. A key always contains at least one active key version. Similarly, a secret always has at least one secret version. However, limits on secrets apply to the tenancy, rather than a vault.)

The Vault service designates vaults as an Oracle Cloud Infrastructure resource.

QUESTION 3

As a solutions architect, you need to assist operations team to write an I AM policy to give users in group-uat1 and group- uat2 access to manage all resources in the compartment Uat. Which is the CORRECT IAM policy ?

A. Allow any-user to manage all resources in tenancy where target.compartment= Uat

B. Allow any-user to manage all resources in compartment Uat where request.group=/group-uat/*

C. Allow group /group-uat*/ to manage all resources in compartment Uat

D. Allow group group-uat1 group-uat2 tomanage all resources in compartment Uat

Correct Answer: D

QUESTION 4

Which storage type is most effective when you want to move some unstructured data, consisting of images and videos, to cloud storage?

A. Standard storage

B. File storage

C. Archivestorage

D. Block volume

Correct Answer: A

Use Oracle Cloud Infrastructure Object Storage for data to which you need fast, immediate, and frequent access. Data accessibility and performance justifies a higher price point to store data in the Object Storage tier. The Object Storage service can store an unlimited amount of unstructured data of any content type, including analytic data and rich content,

like images and videos.

https://docs.oracle.com/en/solutions/learn-migrate-app-data-to-cloud/considerations-object- storage.html#GUID-AC192B08-5160-4DA7-B43E-001753D99CF1

QUESTION 5

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

Correct Answer: C

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

QUESTION 6

Which statements are CORRECT about Multi-Factor Authentication in OCI ? Select TWO correct answers

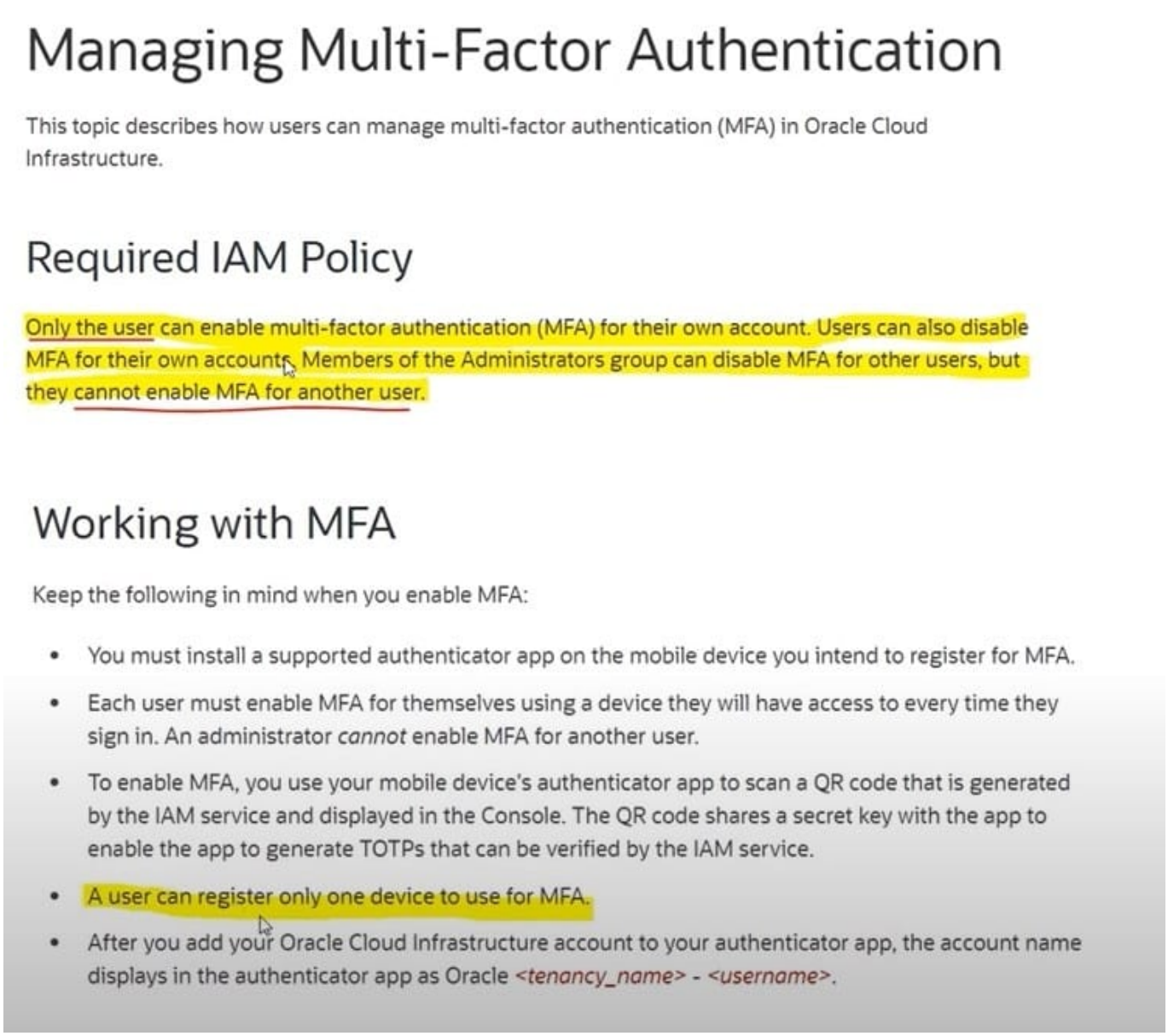
A. Members of the Administrators group can disable MFA for other users

B. Users cannot enable MFA for themselves

C. A user can registermultiple devices to use for MFA.

D. Members of the Administrators group cannot enable MFA for another user

Correct Answer: AD



Managing Multi-Factor Authentication

This topic describes how users can manage multi-factor authentication (MFA) in Oracle Cloud Infrastructure.

Required IAM Policy

Only the user can enable multi-factor authentication (MFA) for their own account. Users can also disable MFA for their own accounts. Members of the Administrators group can disable MFA for other users, but they cannot enable MFA for another user.

Working with MFA

Keep the following in mind when you enable MFA:

- You must install a supported authenticator app on the mobile device you intend to register for MFA.
- Each user must enable MFA for themselves using a device they will have access to every time they sign in. An administrator *cannot* enable MFA for another user.
- To enable MFA, you use your mobile device's authenticator app to scan a QR code that is generated by the IAM service and displayed in the Console. The QR code shares a secret key with the app to enable the app to generate TOTPs that can be verified by the IAM service.
- A user can register only one device to use for MFA.
- After you add your Oracle Cloud Infrastructure account to your authenticator app, the account name displays in the authenticator app as Oracle *<tenancy_name>* - *<username>*.

QUESTION 7

A member of operations team has set Pre-Authenticated Request (PAR) associated with a bucket to an incorrect date and now wants to edit the PARrequest. How can this be achieved?

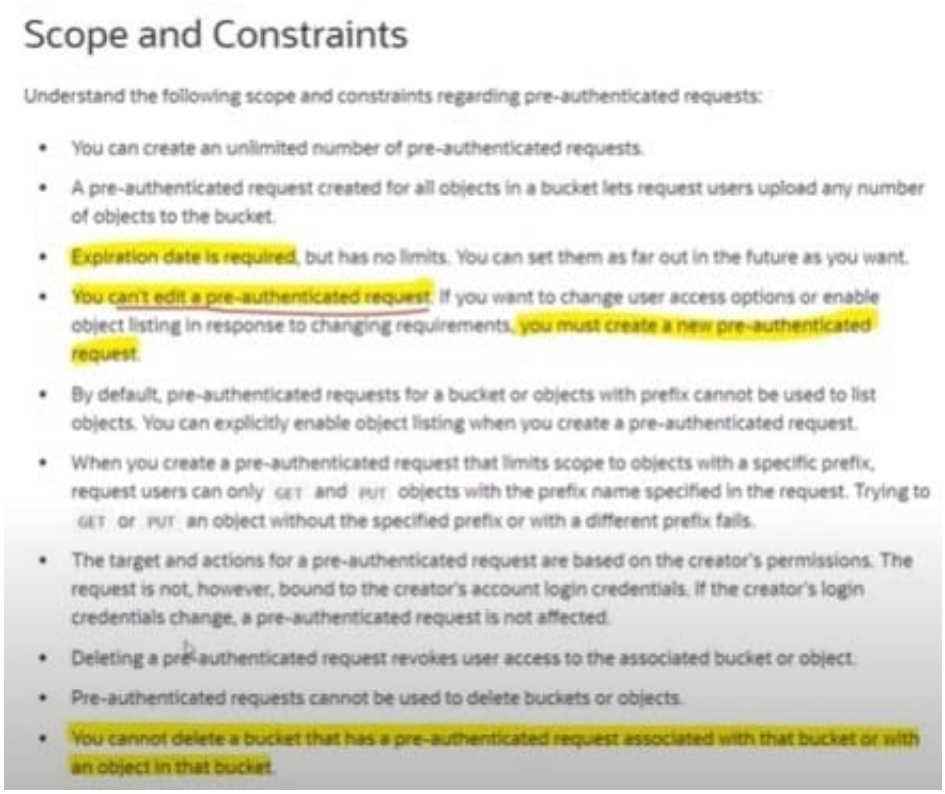
A. Don\\'t set an expiration time for PAR

B. Delete the bucket associated with PAR and recreate it

C. Delete the PAR and recreate it with the required date

D. Delete both PAR as well as the bucket then recreate both

Correct Answer: C



Scope and Constraints

Understand the following scope and constraints regarding pre-authenticated requests:

- You can create an unlimited number of pre-authenticated requests.
- A pre-authenticated request created for all objects in a bucket lets request users upload any number of objects to the bucket.
- Expiration date is required, but has no limits. You can set them as far out in the future as you want.
- You can't edit a pre-authenticated request. If you want to change user access options or enable object listing in response to changing requirements, you must create a new pre-authenticated request.
- By default, pre-authenticated requests for a bucket or objects with prefix cannot be used to list objects. You can explicitly enable object listing when you create a pre-authenticated request.
- When you create a pre-authenticated request that limits scope to objects with a specific prefix, request users can only GET and PUT objects with the prefix name specified in the request. Trying to GET or PUT an object without the specified prefix or with a different prefix fails.
- The target and actions for a pre-authenticated request are based on the creator's permissions. The request is not, however, bound to the creator's account login credentials. If the creator's login credentials change, a pre-authenticated request is not affected.
- Deleting a pre-authenticated request revokes user access to the associated bucket or object.
- Pre-authenticated requests cannot be used to delete buckets or objects.
- You cannot delete a bucket that has a pre-authenticated request associated with that bucket or with an object in that bucket.

QUESTION 8

As a security administrator, you found out that there are users outside your co network who are accessing OCI Object Storage Bucket. How can you prevent these users from accessing OCI resources in corporate network?

A. Create an 1AM policy and create WAF rules

B. Create an 1AM policy and add a network source

C. Make OCI resources private instead of public

D. Create PAR to restrict access the access

Correct Answer: B

Introduction to Network Sources

A network source is a set of defined IP addresses. The IP addresses can be public IP addresses or IP addresses from VCNs within your tenancy. After you create the network source, you can reference it in policy or in your tenancy's authentication settings to control access based on the originating IP address.

Network resources can only be created in the tenancy (or root compartment) and, like other identity resources, reside in the home region. For information about the number of network sources you can have, see IAM Without Identity Domains Limits.

You can use network sources to help secure your tenancy in the following ways:

- Specify the network source in IAM policy to restrict access to resources.
  When specified in a policy, IAM validates that requests to access a resource originate from an allowed IP address.
  For example, you can restrict access to Object Storage buckets in your tenancy to only users that are signed in to Oracle Cloud Infrastructure through your corporate network. Or, you can allow only resources belonging to specific subnets of a specific VCN to make requests over a service gateway.

QUESTION 9

Which statement is not true about Cloud Security Posture?

A. Problems contain data about the specific type of issue that was found.

B. Problems can be resolved, dismissed, or remediated.

C. Problems are defined by the type of detector that creates them: activity or configuration.

D. Problems are created when Cloud Guard discovers a deviation from a responder rule.

Correct Answer: D

https://www.oracle.com/security/cloud-security/what-is-cspm/

QUESTION 10

You have configured the Management Agent on an Oracle Cloud Infrastructure (OCI) Linux instance for log ingestion purposes.

Which is a required configuration for OCI Logging Analytics service to collect data from multiple logs of this Instance?

A. Log - Log Group Association

B. Entity - Log Association

C. Source - Entity Association

D. Log Group - Source Association

Correct Answer: C

QUESTION 11

Bot Management in OCI provides which of the features? Select TWO correct answers.

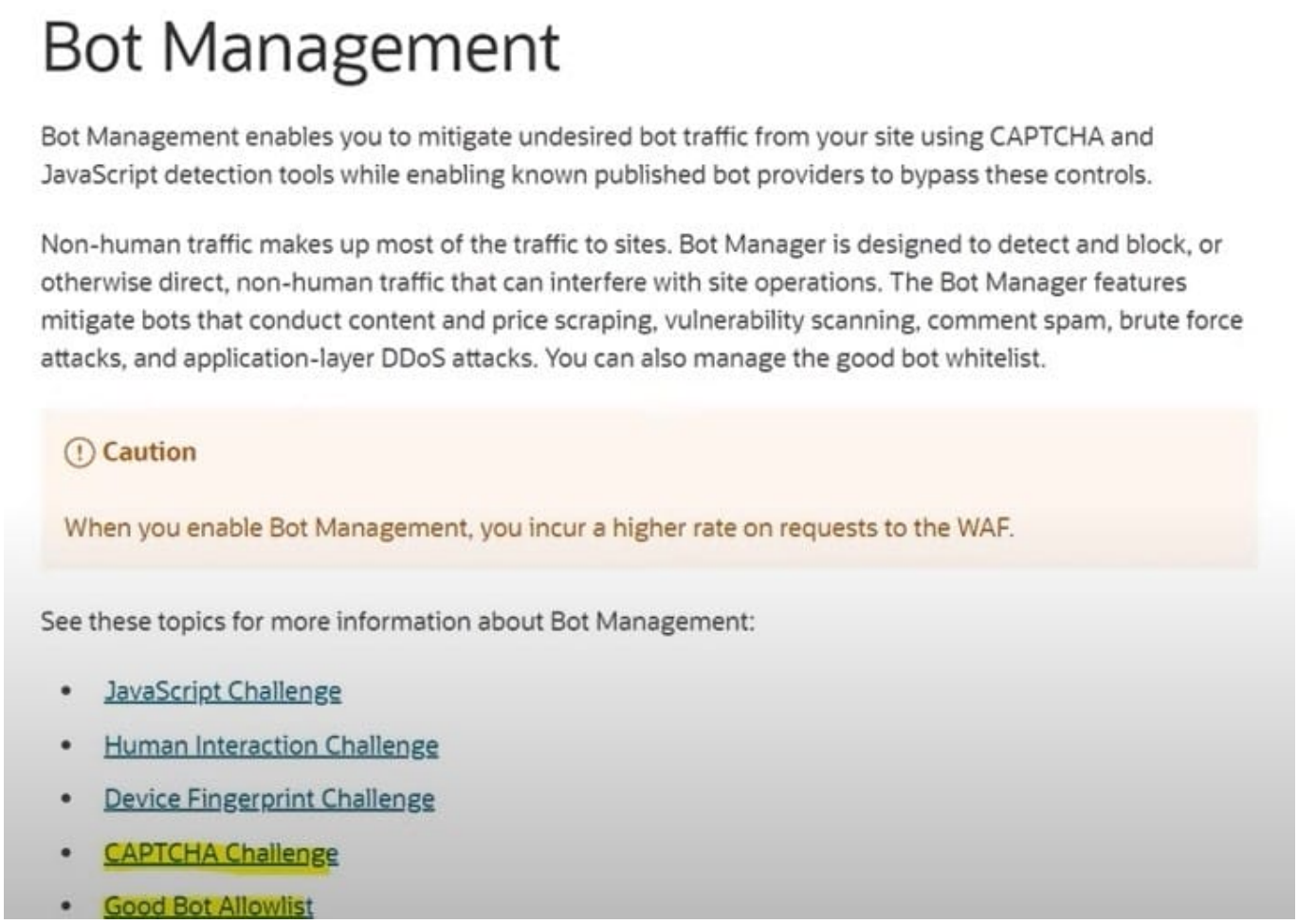
A. Bad Bot Denylist

B. CAPTCHA Challenge

C. IP Prefix Steering

D. Good Bot Allowlist

Correct Answer: BD



QUESTION 12

Which challenge is generally the first level of bot mitigation, but not sufficient with more advanced bot tools?

A. CAPTCHA challenge

B. JavaScript challenge

C. Device fingerprint challenge

D. Human interaction challenge

Correct Answer: B

QUESTION 13

What would you use to make Oracle Cloud Infrastructure Identity and Access Management govern resources in a tenancy?

A. Policies

B. Users

C. Dynamic groups

D. Groups

Correct Answer: A

POLICY A document that specifies who can access which resources, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. For more information, see Example Scenario and How Policies Work. The word "policy" is used by people in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization usesto control access to resources.

https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

QUESTION 14

In which two ways can you improve data durability in Oracle Cloud Infrastructure Object Storage?

A. Setup volumes in a RAID1 configuration

B. Enable server-sideencryption

C. Enable Versioning

D. Limit delete permissions

E. Enable client-side encryption

Correct Answer: A

QUESTION 15

Which components are a part of the OCI Identity and Access Management service?

A. Policies

B. Regional subnets

C. Compute instances

D. VCN

Correct Answer: A