DUMPSBOSS.

Oracle Cloud Infrastructure 2022 Security Professional

Oracle 1z0-1104-22

Version Demo

Total Demo Questions: 10

Total Premium Questions: 94

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Cloud Guard detected a risk score of zero in the dashboard, what does this mean ?

A. Risk score doesn't say anything. These are just numbers

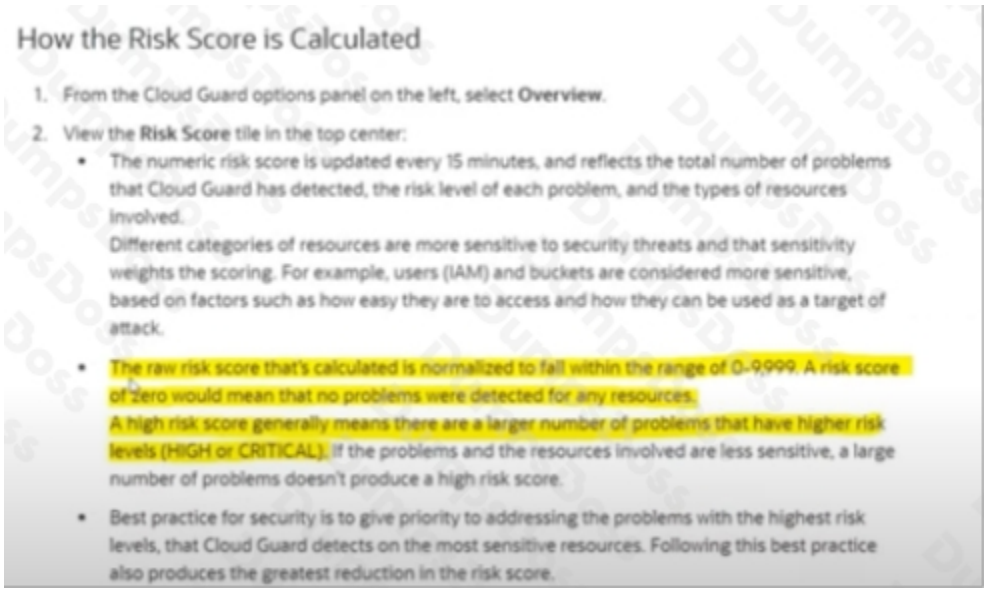
B. LOW or MINOR issues

C. Larger number of problems that have high risk levels (HIGH or CRITICAL)

D. No problem detected for any resource

ANSWER: D

Explanation:



How the Risk Score is Calculated

1. From the Cloud Guard options panel on the left, select **Overview**.
2. View the **Risk Score** tile in the top center:
   - The numeric risk score is updated every 15 minutes, and reflects the total number of problems that Cloud Guard has detected, the risk level of each problem, and the types of resources involved.
     Different categories of resources are more sensitive to security threats and that sensitivity weights the scoring. For example, users (IAM) and buckets are considered more sensitive, based on factors such as how easy they are to access and how they can be used as a target of attack.
   - The raw risk score that's calculated is normalized to fall within the range of 0-9999. A risk score of zero would mean that no problems were detected for any resources.
     A high risk score generally means there are a larger number of problems that have higher risk levels (HIGH or CRITICAL). If the problems and the resources involved are less sensitive, a large number of problems doesn't produce a high risk score.
   - Best practice for security is to give priority to addressing the problems with the highest risk levels, that Cloud Guard detects on the most sensitive resources. Following this best practice also produces the greatest reduction in the risk score.

QUESTION NO: 2

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

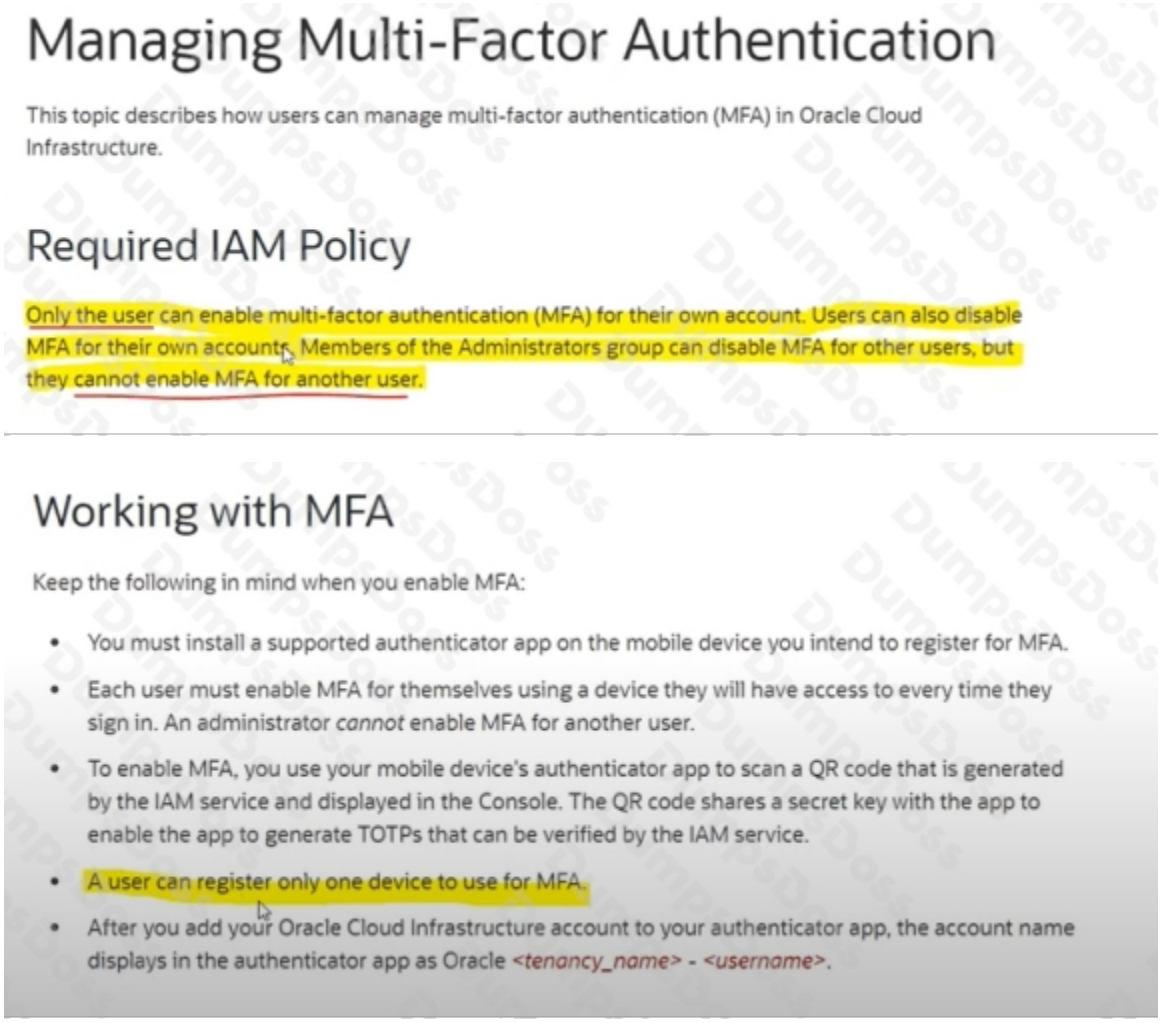
B. Users cannot enable MFA for themselves

C. A user can register multiple devices to use for MFA.

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

ANSWER: A D

Explanation:



QUESTION NO: 3

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

ANSWER: B

Explanation:

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 NO: 4

You create a new compartment, “apps,” to host some production apps and you create an apps_group and added users to it.

What would you do to ensure the users have access to the apps compartment?

A. Add an IAM policy for the individual users to access the apps compartment.

B. Add an IAM policy for apps_group granting access to the apps compartment.

C. Add an IAM policy to attach tenancy to the apps group.

D. No action is required.

ANSWER: B

QUESTION NO: 5

Which resources can be used to create and manage from Vault Service ? Select TWO correct answers

A. Secret

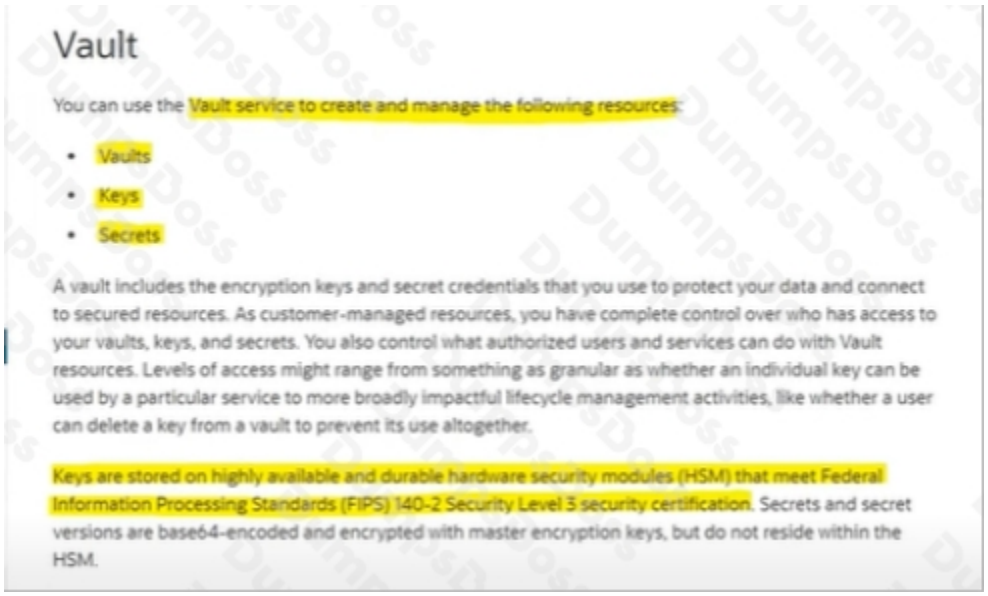
B. IAM

C. Keys

D. Cloud Guard

ANSWER: A C

Explanation:



Vault

You can use the Vault service to create and manage the following resources:

- Vaults
- Keys
- Secrets

A vault includes the encryption keys and secret credentials that you use to protect your data and connect to secured resources. As customer-managed resources, you have complete control over who has access to your vaults, keys, and secrets. You also control what authorized users and services can do with Vault resources. Levels of access might range from something as granular as whether an individual key can be used by a particular service to more broadly impactful lifecycle management activities, like whether a user can delete a key from a vault to prevent its use altogether.

Keys are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. Secrets and secret versions are base64-encoded and encrypted with master encryption keys, but do not reside within the HSM.

QUESTION NO: 6

Oracle Object Storage achieves data durability by which of the mechanisms ? Select TWO correct answers

A. Service Gateway

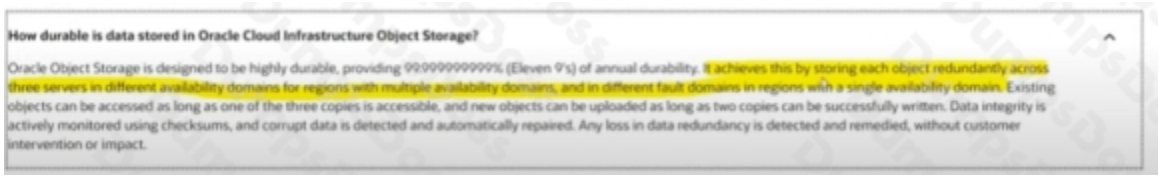
B. Redundant Storage across availability domains

C. Redundant Array of Independent Disks

D. Object Versioning

ANSWER: B D

Explanation:



How durable is data stored in Oracle Cloud Infrastructure Object Storage?

Oracle Object Storage is designed to be highly durable, providing 99.999999999% (Eleven 9's) of annual durability. It achieves this by storing each object redundantly across three servers in different availability domains for regions with multiple availability domains, and in different fault domains in regions with a single availability domain. Existing objects can be accessed as long as one of the three copies is accessible, and new objects can be uploaded as long as two copies can be successfully written. Data integrity is actively monitored using checksums, and corrupt data is detected and automatically repaired. Any loss in data redundancy is detected and remedied, without customer intervention or impact.

QUESTION NO: 7

What must be configured for a load balancer to accept incoming traffic?

A. Service Gateway

B. SSL certificate

C. Listener

D. Route table entry pointing to the listener IP address

ANSWER: C

Explanation:

A listener is an entity that checks for connection requests. The load balancer listener listens for ingress client traffic using the port you specify within the listener and the load balancer's public IP.

https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/loadbalancing.htm

To create a listener:

QUESTION NO: 8

As a Security Admin you want to inspect the metadata and actual data in your Oracle databases to discover sensitive data and provide comprehensive results listing the sensitive columns and related information. Which Data Safe feature will help you to achieve the above requirement ?

A. Data Masking

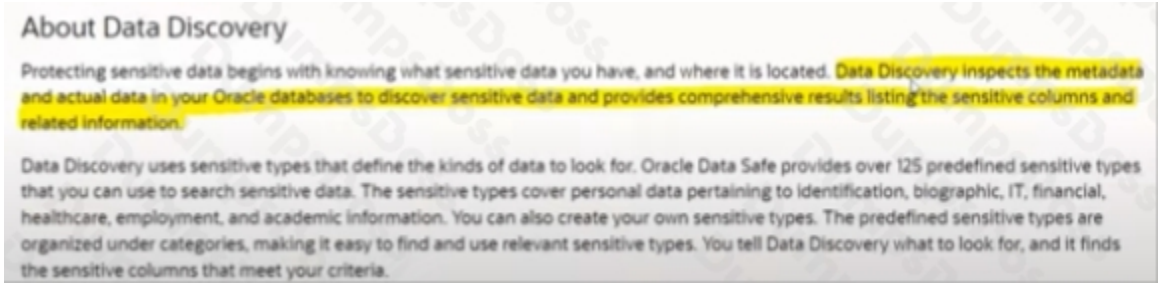
B. Data Discovery

C. Security Assessment

D. User Assessment

ANSWER: B

Explanation:



QUESTION NO: 9

A company has OCI tenancy which has mount target associated with two File Systems, CG_1 and CG_2. These File Systems are accessed by IP-based clients AB_1 and AB_2 respectively. As a security administrator, how can you provide access to both clients such that CGI has Read only access on AB1 and CG_2 has Read/Write access on AB_2?

A. NFS Export Option

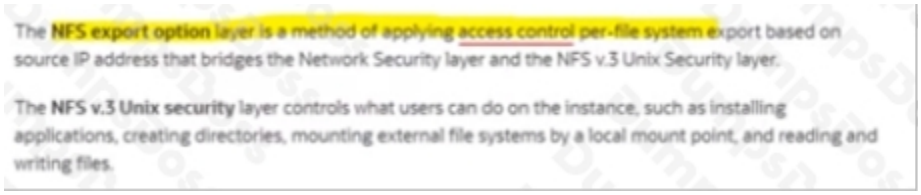
B. Access Control Lists

C. NFS v3 Unix Security

D. Vault

ANSWER: A C

Explanation:


The NFS export option layer is a method of applying access control per-file system export based on source IP address that bridges the Network Security layer and the NFS v.3 Unix Security layer.

The NFS v.3 Unix security layer controls what users can do on the instance, such as installing applications, creating directories, mounting external file systems by a local mount point, and reading and writing files.

QUESTION NO: 10

An automobile company needs to configure Bastion Managed SSH session to a compute

instance in a private subnet. What are the TWO prerequisites to configure successfully?

A. NAT or Service Gateway should be attached to the private subnet

B. There is no need for any gateway in private subnet

C. SSH port forwarding should be enabled

D. Route rule to a NAT or Service Gateway should be associated with the subnet of the route table

ANSWER: A D