Vendor: Oracle

Exam Code:1Z0-1104-22

Exam Name: Oracle Cloud Infrastructure 2022 Security Professional

Version: Demo

QUESTION 1

Which is NOT a part of Observability and Management Services?

A. Event Services

B. OCI Management Service

C. Logging Analytics

D. Logging

Correct Answer: B

https://www.oracle.com/in/manageability/

QUESTION 2

How can you restrict access to OCI console from unknown IP addresses?

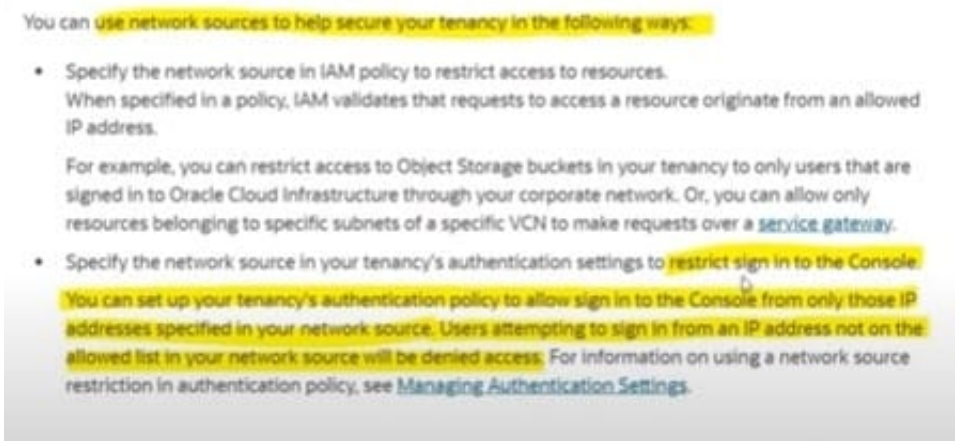
A. Create tenancy\\'s authentication policy and create WAF rules

B. Create tenancy\\'s authentication 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



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.
- Specify the network source in your tenancy's authentication settings to restrict sign in to the Console.
  You can set up your tenancy's authentication policy to allow sign in to the Console from only those IP addresses specified in your network source. Users attempting to sign in from an IP address not on the allowed list in your network source will be denied access. For information on using a network source restriction in authentication policy, see Managing Authentication Settings.

QUESTION 3

Which component helps move logging data to other services, such as archiving log data in object storage?

A. Agent Configuration

B. Unified Monitoring Agent

C. Service Connector Hub

D. Service Log Category

Correct Answer: C

Service Connector Hub Service Connector Hub moves logging data to other services in Oracle Cloud Infrastructure. For example, use Service Connector Hub to alarm on log data, send log data to databases, and archive log data to Object Storage. For more information, see Service Connector Hub. https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm

---

QUESTION 4

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

QUESTION 5

VCN Flow log record details about the traffic that has been denied or approved is based on which of the following statements?

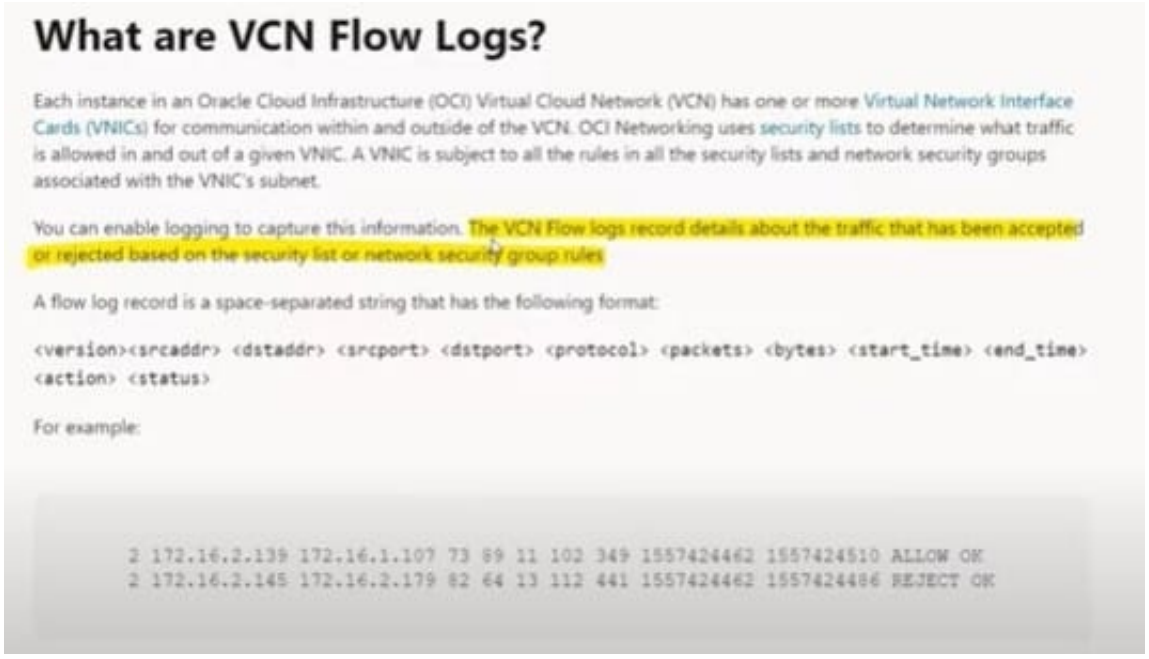
A. Configuration of route table

B. Security Lists orNetwork Security Group Rules

C. Web Application Firewall (WAF)

D. Auth tokens

Correct Answer: B



QUESTION 6

As a security architect, how can you preventunwanted bots while desirable bots are allowed to enter?

A. Data Guard

B. Vault

C. Compartments

D. Web Application Firewall (WAF)

Correct Answer: D

QUESTION 7

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

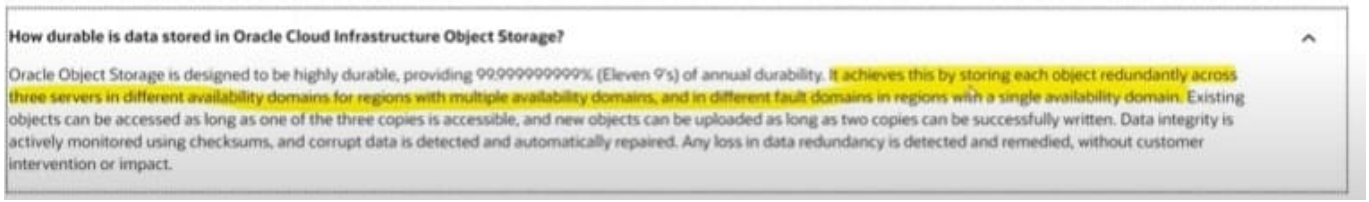
A. Service Gateway

B. Redundant Storage across availability domains

C. Redundant Array of IndependentDisks

D. Object Versioning

Correct Answer: BD



QUESTION 8

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

Correct Answer: C

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

---

QUESTION 9

With regard to vulnerability and cloud penetration testing, which rules of engagement apply? Select TWO correct answers.

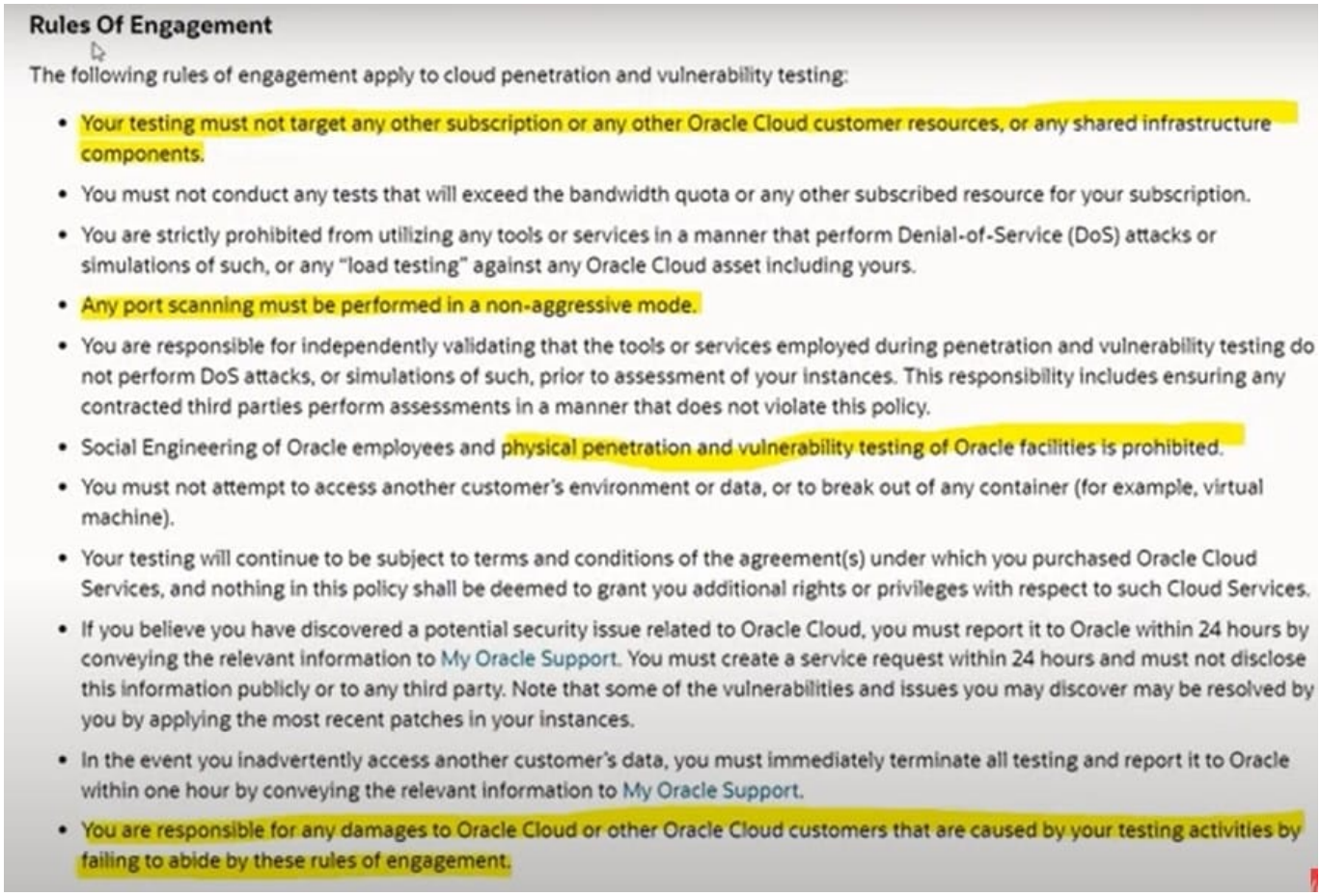
A. Any port scanning must be performed in an aggressive mode

B. Physical penetration and vulnerability testing of Oraclefacilities is prohibited

C. Testing should target any other subscription or any other Oracle Cloud customer resources

D. You are responsible for any damages to Oracle Cloud customers that are caused by your testing activities

Correct Answer: BD



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.
- If you believe you have discovered a potential security issue related to Oracle Cloud, you must report it to Oracle within 24 hours by conveying the relevant information to My Oracle Support. You must create a service request within 24 hours and must not disclose this information publicly or to any third party. Note that some of the vulnerabilities and issues you may discover may be resolved by you by applying the most recent patches in your instances.
- In the event you inadvertently access another customer's data, you must immediately terminate all testing and report it to Oracle within one hour by conveying the relevant information to My Oracle Support.
- You are responsible for any damages to Oracle Cloud or other Oracle Cloud customers that are caused by your testing activities by failing to abide by these rules of engagement.

QUESTION 10

Which type of software do you use to centrally distributeand monitor the patch level of systems throughout the enterprise?

A. Network Monitor software

B. Web Application Firewall

C. Patch Management software

D. Recovery Manager software

Correct Answer: C

https://docs.oracle.com/cd/E11857_01/em.111/e18710/T531901T535649.htm

---

QUESTION 11

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

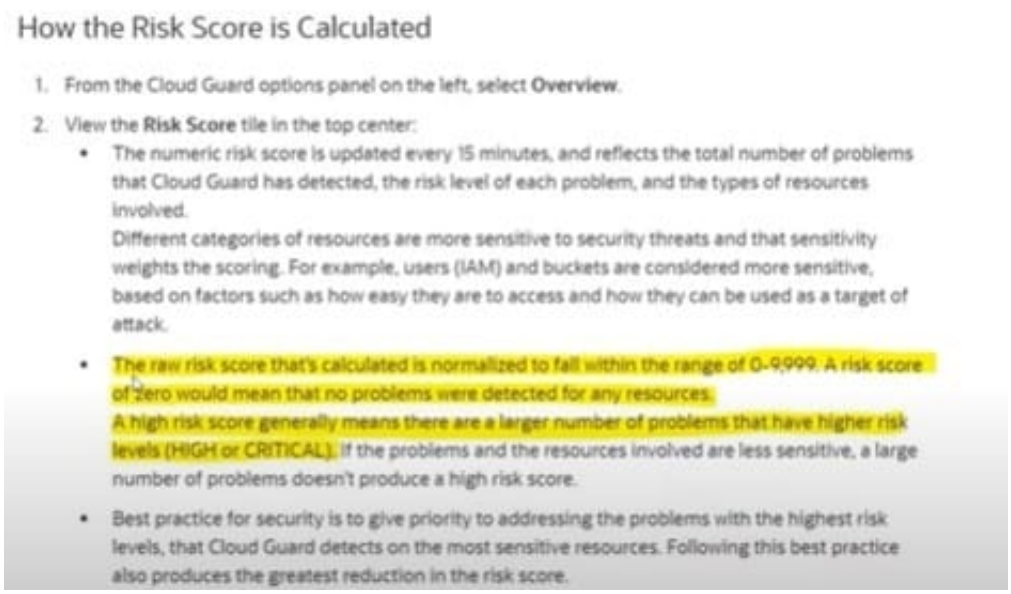
A. Risk score doesn\\'t say anything. These are just numbers

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

Correct Answer: D



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 12

How can you convert a fixed load balancer to a flexible load balancer?

A. There is no way to covert the load balancer.

B. Use Update Shape workflows.

C. Delete the fixed load balancer and create a new one.

D. Using the Edit Listener option.

Correct Answer: B