Latest Version: 7.0

Question: 1

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

Answer: BD

Explanation:

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.

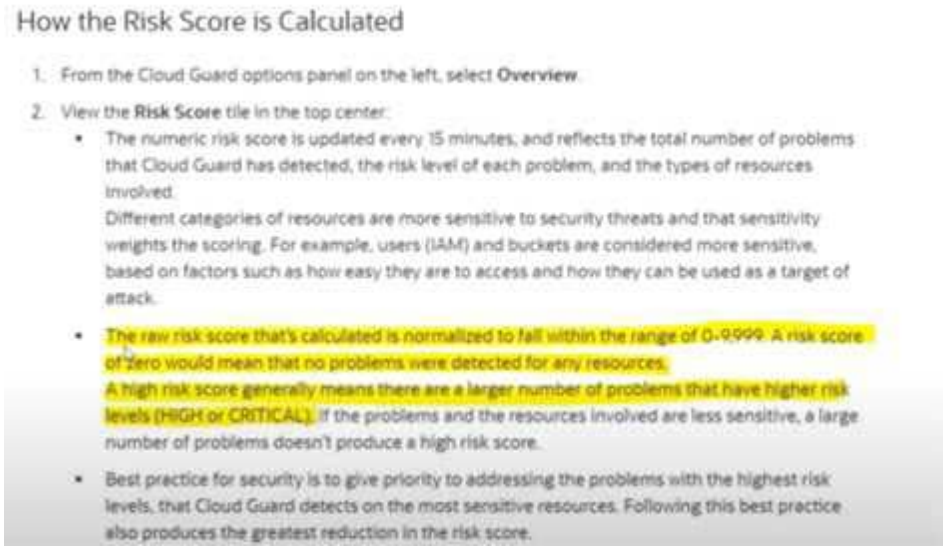
Question: 2

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 0-999. 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.

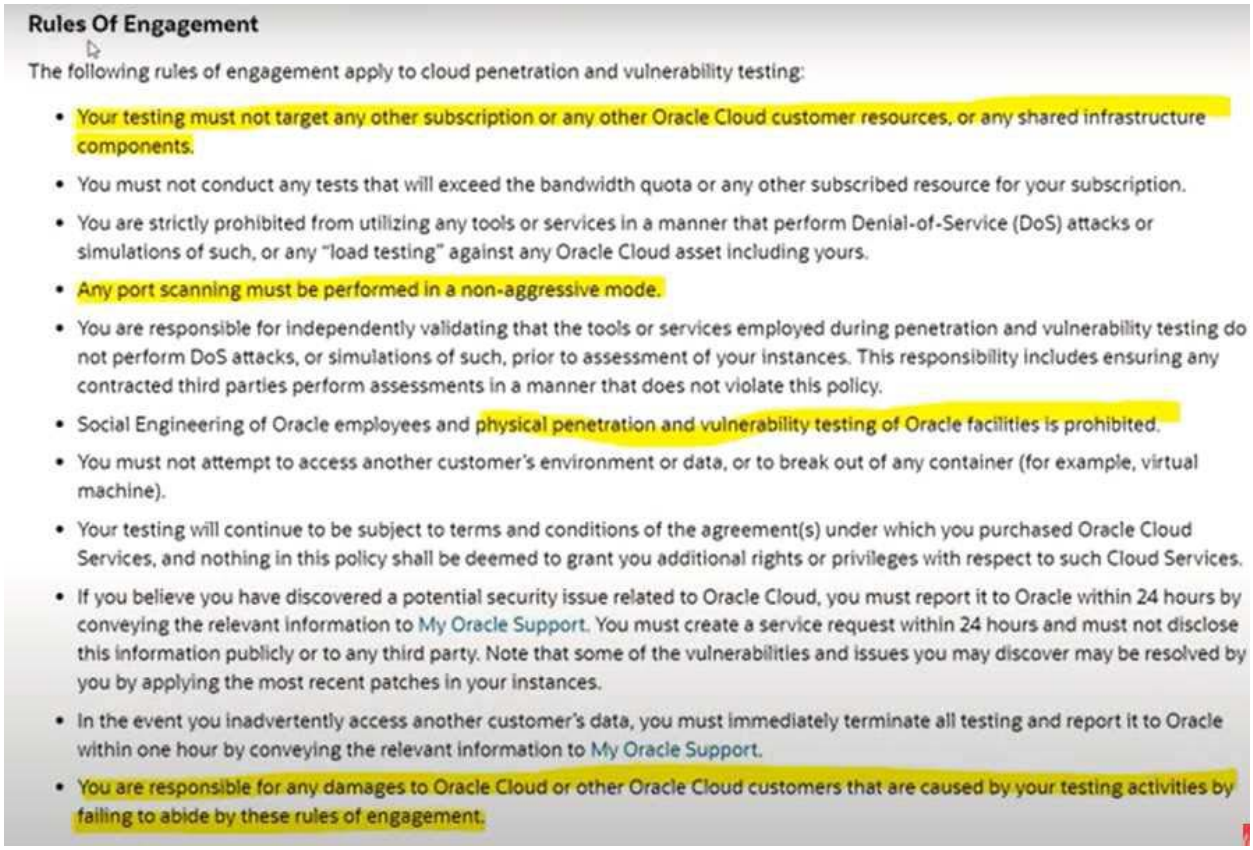
Question: 3

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 Oracle facilities 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

Answer: BD

Explanation:



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: 4

How can you establish private connectivity over two VCN within same OCI region without traversing the traffic over public internet ?

A. NAT Gateway
B. Data Guard
C. Remote VCN Peering
D. Local VCN Peering

Answer: D

Explanation:

- **Local VCN peering**
  Virtual cloud networks (VCNs) within a region can be peered by using local peering gateways (LPG). The resources attached to such peered VCNs can communicate by using private IP addresses without routing the traffic over the public internet. The VCNs can be in the same tenancy or in different tenancies.
- **Remote VCN peering**
  VCNs in different regions can communicate by using private IP addresses without routing the traffic over the public internet. You can set up peering between two VCNs in different regions by configuring a remote peering connection (RPC) on each of the dynamic routing gateways (DRG) attached to the VCNs in the peering relationship. Remote VCN peering is generally used to connect two VCNs across regions in the same tenancy. In certain scenarios, you might need to connect VCNs in two different tenancies across regions.

Question: 5

Which security issues can be identified by Oracle Vulnerability Scanning Service? Select TWO correct answers

A. Distributed Denial of Service (DDoS)
B. Ports that are unintentionally left open can be a potential attack vector for cloud resources
C. SQL Injection
D. CIS published Industry-standard benchmarks

Answer: BD

Explanation:

Scanning Overview

Oracle Vulnerability Scanning Service helps improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. The service generates reports with metrics and details about these vulnerabilities.

The Scanning service can identify several types of security issues in your compute **instances** ⓘ:

- Ports that are unintentionally left open might be a potential attack vector to your cloud resources, or enable hackers to exploit other vulnerabilities.
- OS packages that require updates and patches to address vulnerabilities
- OS configurations that hackers might exploit
- Industry-standard benchmarks published by the Center for Internet Security ↪ (CIS).

  The Scanning service checks hosts for compliance with the section 5 (*Access, Authentication, and Authorization*) benchmarks defined for Distribution Independent Linux ↪.