1Z0-997Q&As

Oracle Cloud Infrastructure 2019 Architect Professional

Pass Oracle 1Z0-997 Exam with 100% Guarantee

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

https://www.geekcert.com/1z0-997.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

To serve web traffic for a popular product, your cloud engineer has provisioned four BM.Standard2.52 instances, event spread across two availability domains in the us-asburn-1 region: LoadBalancer is used to deliver the traffic across instances. After several months, the product grows even more popular and you need additional compute capacity. As a result, an engineer provisioned two additional VM.Standard2.8 instances. You register the two VM. Standard2. 8 Instances with your load Balancer Backend sot and quickly find that the VM Standard2.8 Instances running at 100% of CPU utilization but the BM.Standard2 .52 instances have significant CPU capacity that\\'s unused. Which option is the most cost effective and uses instances capacity most effectively?

A. Configure your Load Balance, with weighted round robin policy to distribute traffic to the compute instances, with more weight assigned to bare metal instances.

B. Configure Autoscaling instance pool with LoadBalancer to add up to 3 more BM.Standard2.52 Instances when triggered. Shut off VM.Standard2.8 instances.

C. Route traffic to BM.Standard2.52 and VM Standard2.8 instances directly using DNS and Health Checks. Shut off the load Balances.

D. Configure LoadBalancer with two VM Standard2.8 instances and use Autoscalling Instant pool to add up to two additional VM instances. Shut off BM.Standard2.52 instances.

Correct Answer: A

Customer have 4 BM.Standard2.52 and After several months he need additional compute capacity customer find The VM Standard2.8 Instances running at 100% of CPU utilization but the BM.Standard2 .52 instances have significant CPU capacity that unused. so the customer need to check the Load balance policy to make sure the 4 BM and VM is utilize correctly

QUESTION 2

You are working as a solution architect with a global automotive provider who is looking to create a multi-cloud solution They want to run their application tier in Microsoft Azure while utilizing the Oracle DB Systems In the Oracle Cloud Infrastructure (OCI). What is the most fault tolerant and secure solution for this customer?

A. Create an Oracle database in OCI Virtual Cloud Network (VCN) and connect to the application tier running In Microsoft Azure over the Internet.

B. Create a FastConnect virtual circuit and choose Microsoft Azure from the list of providers available to setup Network connectivity between application tier running in Microsoft Azure Virtual Network and Oracle Databases running In OCI Virtual Cloud (VCN)

C. Use OCI Virtual Cloud Network remote peering connection to create connectivity among application tier running in Microsoft Azure Virtual Network and Oracle Databases running in OCI Virtual Cloud Network (VCN).

D. Create a VPN connection between the application tie, running in Azure Virtual Network and Oracle Databases running In OCI Virtual Cloud Network (VCN).

Correct Answer: C

Oracle and Microsoft have created a cross-cloud connection between Oracle Cloud Infrastructure and Microsoft Azure

in certain regions. This connection lets you set up cross-cloud workloads without the traffic between the clouds going over the internet. you can connect your VNet and VCN so that traffic that uses private IP addresses goes over the crosscloud connection. For example, the following diagram shows a VNet that is connected to a VCN. Resources in the VNet are running a .NET application that access an Oracle database that runs on Database service resources in the VCN. The traffic between the application and database uses a logical circuit that runs on the cross-cloud connection between Azure and Oracle Cloud Infrastructure. The two virtual networks must belong to the same company and not have overlapping CIDRs. The connection requires you to create an Azure ExpressRoute circuit and an Oracle Cloud Infrastructure FastConnect virtual circuit.

QUESTION 3

You are helping a customer troubleshoot a problem. The customer has several Oracle Linux servers in

Based on cost considerations, which option will fix this Issue?

A. Create a Public Load Balancer In front of the servers and add the servers to the Backend Set of the Public Load Balancer.

B. Create another Internet Gateway and configure it as route target for the private subnet.

C. Implement a NAT instance In the public subnet of the VCN and configure the NAT instance as the route target for the private subnet.

D. Create a NAT gateway in the VCN and configure the NAT gateway as the route target for the private subnet.

Correct Answer: A

QUESTION 4

A hospital in Austin has hosted its web based medical records portal entirely In Oracle cloud Infrastructure (OCI) using Compute Instances for its web-tier and DB system database for its data tier. To validate compliance with Health Insurance Portability and Accountability (HIPAA), the security professional to check their systems it was found that there are a lot of unauthorized coming requests coming from a set of IP addresses originating from a country in Southeast Asia. Which option can mitigate this type of attack?

A. Block the attacking IP address by creating by Network Security Group rule to deny access to the compute Instance where the web server Is running

B. Block the attacking IP address by implementing a OCI Web Application Firewall policy using Access Control Rules

C. Mitigate the attack by changing the Route fable to redirect the unauthorized traffic to a dummy Compute instance

D. Block the attacking IP address by creating a Security List rule to deny access to the subnet where the web server Is running

Correct Answer: B

WAF can protect any internet facing endpoint, providing consistent rule enforcement across a customer\\'s applications. WAF provides you with the ability to create and manage rules for internet threats including Cross-Site Scripting (XSS), SQL Injection and other OWASP-defined vulnerabilities. Unwanted bots can be mitigated while tactically allowed desirable bots to enter. Access rules can limit based on geography or the signature of the request. As a WAF administrator you can define explicit actions for requests that meet various conditions. Conditions use various operations and regular expressions. A rule action can be set to log and allow, detect, or block requests

QUESTION 5

You are building a highly available and fault tolerant web application deployment for your company. Similar application delayed by competitors experienced web site attack including DDoS which resulted in web server failing. You have decided to use Oracle Web Application Firewall (WAF) to implement an architecture which will provide protection against such attacks and ensure additional configuration will you need to implement to make sure WAF is protecting my web application 24?. Which additional configuration will you need to Implement to make sure WAF Is protecting my web application 24??

A. Configure auto scaling policy and it to WAF instance.

B. Configure Control Rules to send traffic to multiple web servers

C. Configure multiple origin servers

D. Configure new rules based on now vulnerabilities and mitigations

Correct Answer: C

Origin Management An origin is an endpoint (typically an IP address) of the application protected by the WAF. An origin can be an Oracle Cloud Infrastructure load balancer public IP address. A load balancer IP address can be used for high availability to an origin. Multiple origins can be defined, but only a single origin can be active for a WAF. You can set HTTP headers for outbound traffic from the WAF to the origin server. These name value pairs are then available to the application. Oracle Cloud Infrastructure Web Application Firewall (WAF) is a cloud-based, Payment Card Industry (PCI) compliant, global security service that protects applications from malicious and unwanted internet traffic. WAF can protect any internet facing endpoint, providing consistent rule enforcement across a customer\\'s applications. WAF provides you with the ability to create and manage rules for internet threats including Cross-Site Scripting (XSS), SQL Injection and other OWASP-defined vulnerabilities. Unwanted bots can be mitigated while tactically allowed desirable bots to enter. Access rules can limit based on geography or the signature of the request. Distributed Denial of Service (DDoS) A DDoS attack is an often intentional attack that consumes an entity\\'s resources, usually using a large number of distributed sources. DDoS can be categorized into either Layer 7 or Layer 3/4 (L3/4) A layer 7 DDoS attack is a DDoS attack that sends HTTP/S traffic to consume resources and hamper a website\\'s ability to delivery content or to harm the owner of the site. The Web Application Firewall (WAF) service can protect layer 7 HTTP-based resources from layer 7 DDoS and other web application attack vectors.