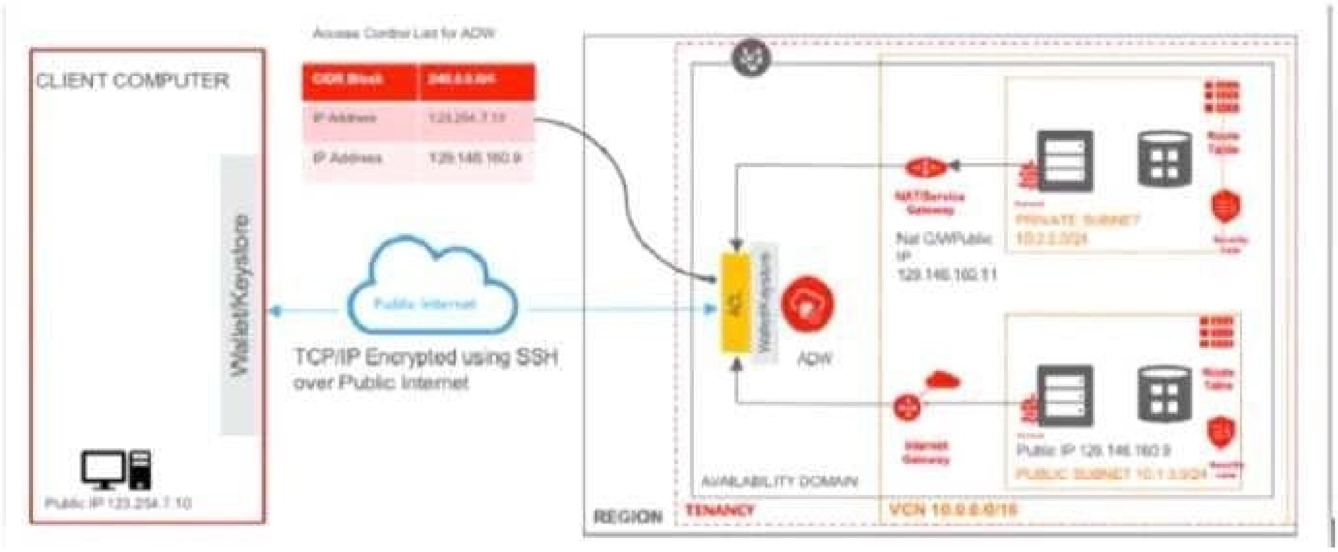
1Z0-997 $^{\text{Q\&As}}$

Oracle Cloud Infrastructure 2019 Architect Professional

Pass Oracle 1Z0-997 Exam with 100% Guarantee

QUESTION 1

You have designed and deployed your Autonomous Data Warehouse (ADW) such that it is accessible from your on-premises data center and servers running on both private and public networks in Oracle Cloud Infrastructure (OCI).



As you are testing the connectivity to your ADW database from the different access paths, you notice that the sewer lunninq on the private network is unable to connect to ADW. Which two steps do you need to take to enable connectivity from the server on the private network to ADW?

A. Add an entry in the Security List of the ADW allowing ingress traffic for C10R block 10.2.2.0/24

B. Add an entry in the route table (associated with the private subnet) with destination of 0.0.0.0/; target type of NAT Gateway, add a stateful egress rule to the security list (associated with the private subnet) with destination of 0.0.0.0./0 and for all IP protocols.

C. Add an entry in the access table list of ASW for CIDR block 10.2.2.0/24.

D. Add an entry in the route table (associated with the private subnet) with destination of 0.0.0.0./0; target type of internet Gateway, add a stateful egress in the security list (associated with the private subnet) with destination of 0.0.0.0/0 and for all IP protocols.

E. Add an entry in the access control list of ADW for IP address 129.146.160.11

Correct Answer: BE

There are 3 connections to ADW 1- Connecting to (ADW) from Public Internet 2- Connecting to ADW (via NAT or Service Gateway) from a server running on a private subnet in OCI (in the same tenancy) 3- Connecting to ADW (via internet Gateway) from a server running on a public subnet in OCI (in the same tenancy

QUESTION 2

You work for a German company as the Lead Oracle Cloud Infrastructure architect. You have designed a highly scalable architecture for your company\\'s business critical application which uses the Load Balancer service auto which uses the Load Balancer service, autoscaling configuration for the application servers and a 2 Node VM Oracle RAC database. During the peak utilization period of the- application yon notice that the application is running slow and customers are complaining. This is resulting in support tickets being created for API timeouts and negative sentiment from the customer base. What are two possible reasons for this application slowness?

A. Autoscaling configuration for the application servers didn\\'t happen due to 1AM policy that\\'s blocking access to the application server compartment

B. The Load Balancer configuration is not sending traffic to the listener of the application servers.

C. Autoscaling configuration for the application servers didn\\'t happen due to compartment quota breach of the VM shapes used by the application servers.

D. Autoscaling configuration for the application servers didn\\'t happen due to service limit breach of the VM shapes used by the application servers E. The Load Balancer doesn\\'t have a Network Security Group to allow traffic to the application servers.

Correct Answer: CD

Autoscaling Autoscaling enables you to automatically adjust the number of Compute instances in an instance pool based on performance metrics such as CPU utilization. This helps you provide consistent performance for your end users during periods of high demand, and helps you reduce your costs during periods of low demand. Prerequisites

-

You have an instance pool. Optionally, you can attach a load balancer to the instance pool. For steps to create an instance pool and attach a load balancer, see Creating an Instance Pool.

-

Monitoring is enabled on the instances in the instance pool. For steps to enable monitoring, see Enabling Monitoring for Compute Instances.

-

The instance pool supports the maximum number of instances that you want to scale to. This limit is determined by your tenancy\\'s service limits. About Service Limits and Usage When you sign up for Oracle Cloud Infrastructure, a set of service limits are configured for your tenancy. The service limit is the quota or allowance set on a resource. For example, your tenancy is allowed a maximum number of compute instances per availability domain. These limits are generally established with your Oracle sales representative when you purchase Oracle Cloud Infrastructure. Compartment Quotas Compartment quotas are similar to service limits; the biggest difference is that service limits are set by Oracle, and compartment quotas are set by administrators, using policies that allow them to

QUESTION 3

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.

QUESTION 4

A large financial company has a web application hosted in their on-premises data center. They are migrating their application to Oracle Cloud Infrastructure (OCI) and require no downtime while the migration is on-going. In order to achieve this, they have decided to divert only 30% of the application works fine, they divert all traffic to OCI. As a solution architect working with this customer, which suggestion should you provide them?

A. Use OCI Traffic management with failover steering policy and distribute the traffic between OC1 and on premises infrastructure.

B. Use OCI Traffic management with Load Balancing steering policy and distribute the traffic between OCI and on premises infrastructure.

C. Use an OCI load Balancer and distribute the traffic between OCI and on premises infrastructure.

D. Use VPN connectivity between on premises Infrastructure and OCI, and create routing tables to distribute the traffic between them.

Correct Answer: B

Traffic Management Steering Policies can account for health of answers to provide failover capabilities, provide the ability to load balance traffic across multiple resources, and account for the location where the query was initiated to provide a simple, flexible and powerful mechanism to efficiently steer DNS traffic.

QUESTION 5

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