1Z0-997 Q&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.pass4itsure.com/1z0-997.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Your team is conducting a root analysis (RCA) following a recent, unplanned outage. One of the block volumes attached to your production WebLogic server was deleted and you have tasked with identifying the source of the action. You search the Audit logs and find several Delete actions that occurred in the previous 24 hours. Given the sample of this event.


```
"event":{
"tenantId":"ocid1.tenancy.oc1..aaaaaaaaymp6934bqkimnbuciaaslaaaaa"
"compartmentId":"ocid1.compartment.oc1..aaaaaaaav4x6wimindk7zngnAlaaa"
"compartmentName":"Production"
"eventId":"14a87512 db1rille),A06-041027d191f9"
"eventName":"DeleteVolume"
"eventSource":"BlockVolames"
"eventType":"ServiceAPI"
"principalId":"ocid1.user.oc1..aaaaaaaaiglSkkeib62pz3ualqwxy6olzd7daagaaaaa"
"credentialId":"
"requestAction":"DELETE"
"requestId":"csid06406dob4a7999cecId516C4ce52/f79253t181thilb36blad34bM51040/?A112B6BFFOK3011165P6SUM0C"
"requestAgent":"Mozilia/5.° (Windows NT 10.0; •Win64; x64) AppleWebKit/o31.36 WM, like Gecko) Chrome/15.0.377.14..."
"requestHeaders":{...
}
"requestOrigin":"129.254.11.219"
"request Resource":"/20160918/volumes/ociA1.volume.oc1.iad.abuwc1jtxksq424tohccipilbzzl3w)rr1j2ezissSes105125kzxlic"
"responseStatus":"204"
```


Which item from the event log helps you identify the individual or service that initiated the DeleteVolume API call?

A. requestAgent

B. eventource

C. principalId

D. requestOrigin

E. eventId

Correct Answer: C

The Oracle Cloud Infrastructure Audit service automatically records calls to all supported Oracle Cloud

Infrastructure public application programming interface (API) endpoints as log events.

Currently, all services support logging by Audit.

Every audit log event includes two main parts:

Envelopes that act as a container for all event messages Payloads that contain data from the resource

emitting the event message The identity object contains the following attributes. data.identity.authType The

type of authentication used.

data.identity.principalId The OCID of the principal.

data.identity.principalName The name of the user or service. This value is the friendly name associated

with principalId .

QUESTION 2

A civil engineering company is running an online portal In which engineers can upload there constructions photos, videos, and other digital files. There is a new requirement for you to implement: the online portal must offload the digital content to an Object Storage bucket for a period of 72 hours. After the provided time limit has elapsed, the portal will hold all the digital content locally and wait for the next offload period. Which option fulfills this requirement?

A. Create a pre-authenticated URL for the entire Object Storage bucket to read and list the content with an expiration of 72 hours.

B. Create a pre authenticated URL lot each object that Is uploaded to the Object Storage bucket with an expiration of 72 hours.

C. Create a Dynamic Group with matching rule for the portal compute Instance and grant access to the Object Storage bucket for 72 hours.

D. Create a pre authenticated URL for the entire Object Storage bucket to write content with an expiration of 72 hours.

Correct Answer: D

Pre-authenticated requests provide a way to let users access a bucket or an object without having their own credentials, as long as the request creator has permission to access those objects. For example, you can create a request that lets operations support user upload backups to a bucket without owning API keys. Or, you can create a request that lets a business partner update shared data in a bucket without owning API keys. When creating a pre-authenticated request, you have the following options: You can specify the name of a bucket that a pre-authenticated request user has write access to and can upload one or more objects to. You can specify the name of an object that a pre-authenticated request user can read from, write to, or read from and write to. Scope and Constraints Understand the following scope and constraints regarding pre-authenticated requests: Users can\\'t list bucket contents. You can create an unlimited number of pre-authenticated requests. There is no time limit to the expiration date that you can set. You can\\'t edit a pre-authenticated request. If you want to change user access options in response to changing requirements, you must create a new pre-authenticated request. The target and actions for a pre-authenticated request are based on the creator\\'s permissions. The request is not, however, bound to the creator\\'s account login credentials. If the creator\\'s login credentials change, a pre-authenticated request is not affected.

You cannot delete a bucket that has a pre-authenticated request associated with that bucket or with an object in that bucket.

QUESTION 3

Your organization is planning on using Oracle Cloud Infrastructure (OCI) File Storage Service (FSS). You will be deploying multiple compute instance in Oracle Cloud Infrastructure (OCI) and mounting the file system to these compute instances. The file system will hold payment data processed by a Database instance and utilized by compute instances to create a overall inventory report. You need to restrict access to this data for specific compute instances and must be allowed/blocked per compute instance\\'s CIDR block. Which option can you use to secure access?

A. Use stateless Security List rule to restrict access from known IP addresses only.

B. Create a new VCN security list, choose SOURCE TYPE as Service and SOURCE SERVICE as FSS. Add stateless ingress and egress rules for specific P address and CIDR blocks.

C. Use \\'Export option\\' feature of FSS to restrict access to the mounted file systems.

D. Create and configure OCI Web Application Firewall service with built in DNS based intelligent routing.

Correct Answer: C

NFS export options enable you to create more granular access control than is possible using just security list rules to limit VCN access. You can use NFS export options to specify access levels for IP addresses or CIDR blocks connecting to file systems through exports in a mount target. Access can be restricted so that each client\\'s file system is inaccessible and invisible to the other, providing better security controls in multi-tenant environments. Using NFS export option access controls, you can limit clients\\' ability to connect to the file system and view or write data. For example, if you want to allow clients to consume but not update resources in your file system, you can set access to Read Only. You can also reduce client root access to your file systems and map specified User IDs (UIDs) and Group IDs (GIDs) to an anonymous UID/GID of your choice. For more information about how NFS export options work with other security layers

QUESTION 4

All three Data Guard Configuration are fully supported on Oracle Cloud infrastructure (OCI). You want to deploy a maximum availability architecture (MAA) for database workload. Which option should you consider while designing your Data Guard configuration to ensure best RTO and PRO without causing any data loss?

A. Configure "Maximum Protection" mode which provides zero data loss If the primary database fails.

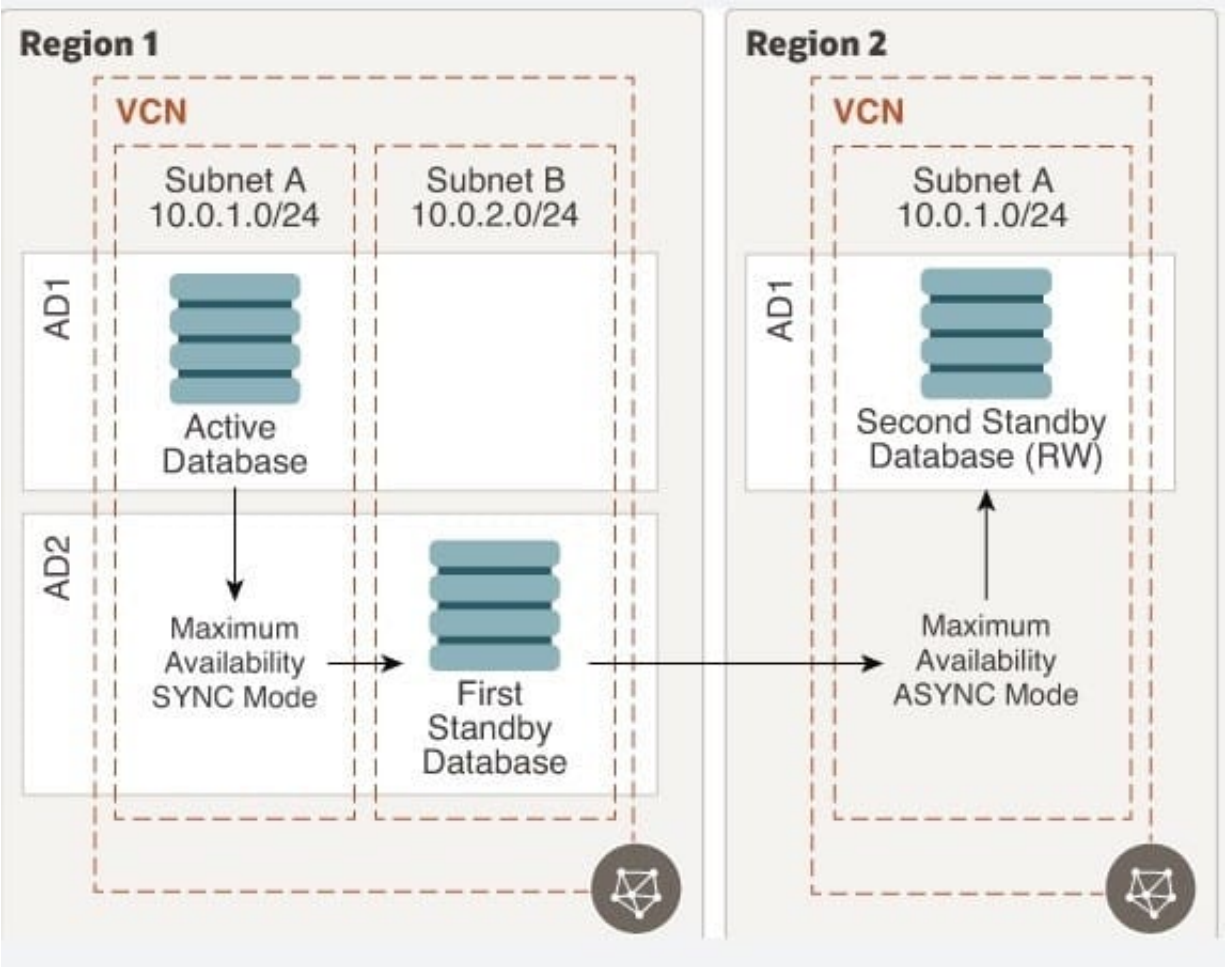
B. Configure "Maximum Performance" mode In SYNC mode between two availability domains (same region) which provides, the highest level of data protection that is possible without affecting the performance of the primary database.

C. Configure \\'\\'Maximum Scalability" mode which provides the highest level of scalability without compromising the availability of the primary database.

D. Configure \\'\\'Maximum Availability" mode in SYNC mode between two availability domains (same

Correct Answer: D

https://docs.cloud.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/best-practices- for-dr-onoci.pdf All three Data Guard configurations are fully supported on Oracle Cloud Infrastructure. However, because of a high risk of production outage, we don\\'t recommend using the maximum protection mode for your Data Guard configuration. We recommend using the maximum availability mode in SYNC mode between two availability domains (same region), and using the maximum availability mode in ASYNC mode between two regions. This architecture provides you the best RTO and RPO without causing any data loss. We recommend building this architecture in daisy-chain mode: the primary database ships redo logs to the first standby database in another availability domain in SYNC mode, and then the first standby database ships the redo logs to another region in ASYNC mode. This method ensures that your primary database is not doing the double work of shipping redo logs, which can cause performance impact on a production workload.



This configuration offers the following benefits: No data loss within a region. No overhead on the production database to maintain standbys in another region. Option to configure lagging on the DR site if needed for business reasons. Option to configure multiple standbys in different regions without any additional overhead on the

production database. A typical use case is a CDN application Bottom of Form

QUESTION 5

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.