[Jan-2024 Updated Oracle 1z0-1072-23 Dumps - PDF & Online Engine [Q24-Q41

[Jan-2024] Updated Oracle 1z0-1072-23 Dumps -
PDF & Online Engine [Q24-Q41]

[Jan-2024] Updated Oracle 1z0-1072-23 Dumps &ndash; PDF & Online Engine
1z0-1072-23.pdf - Questions Answers PDF Sample Questions Reliable

NO.24 You have a high-demand web application running on Oracle Cloud Infrastructure (OCI). Your tenancy administrator has set up a schedule-based autoscaling policy on instance pool with an initial size of 5 instances for the application.

Policy 1:

Target pool size:10 instances

Execution time:8:30 a.m. on every Monday through Friday, in every month, in every year Cron expression:0 30 8 ? * MON-FRI *
Which statement accurately explains the goal of this policy?
* Goal: A one-time schedule with only one scaling out event. At 8:30 a.m., on December 31, 2021, scale the instance pool to 10 instances from 5.
* Goal: A recurring monthly schedule. On all days of the month, set the initial pool size to 5 instances. At

8.30 a.m., on every day of the month, scale out to 10 instances.
* Goal: A recurring daily schedule. On weekday mornings at 8.30 a.m., scale out to 10 instances.

* Goal: A recurring weekly schedule. On all days of the week at 8.30 a.m., scale out the pool to 10 instances from the initial size of 5

The explanation is that a schedule-based autoscaling policy allows you to adjust the size of your instance pool based on a cron expression that specifies the date and time of the scaling action. The cron expression consists of six fields: seconds, minutes, hours, day of month, month, and day of week. In this case, the cron expression is 0 30 8 ? * MON-FRI *, which means that the scaling action will occur at 8:30 a.m. on every Monday through Friday, regardless of the day of month or month. Therefore, the goal of this policy is to scale out the instance pool to 10 instances on weekday mornings at 8:30 a.m.

NO.25 You need to set up instance principals so that an application running on aninstance can call Oracle CloudInfrastructure (OCI) public services, without the need to configure user credentials.

A developer in your team has already configured the application built using an OCISDK to authenticate using theinstance principals provider.

Which is NOTa necessary step to complete this set up?

* Create a dynamic group with matching rules to specify which instances can make API calls against services.
* Generate Auth Tokens to enable instances in the dynamic group to authenticate with APIs.
* Create a policy granting permissions to the dynamic group to access services in your compartment or tenancy.
* Deploy the application and the SDK to all the instances that belong to the dynamic group.

Explanation

Generating Auth Tokens to enable instances in the dynamic group to authenticate with APIs is not a necessary step to complete this set up. This is because Auth Tokens are used to authenticate users, not instances, when making API calls to OCI services. Instance principals are a feature that allows instances to authenticate themselves using certificates, without requiring user credentials or Auth Tokens. The other options are necessary steps to complete this set up, as they enable instances in the dynamic group to make API calls against services using instance principals and IAM policies. References: [Instance Principals], [Auth Tokens]

NO.26 You are part of a team that manages a set of workload instances running in an on-premises environment. The Architect team is tasked with designing and configuring Oracle Cloud Infrastructure (OCI) Logging service to collect logs from these instances. There is a requirement to archive Info-level logging data of these instances into the OCI Object Storage.

Which TWO features of OCI can help you achieve this?

* Cloud Agent Plugin
* Grouping Function
* Service Connectors
* Agent Configuration
* ObjectCollectionRule

Cloud Agent Plugin and Service Connectors are two features of OCI that can help collect logs from on-premises instances and archive them into OCI Object Storage. Cloud Agent Plugin is a component of the OCI Logging service that can be installed on any Linux or Windows instance to collect logs and send them to OCI. Service Connectors are components of the OCI Service Connector Hub that can transfer data between different OCI services, such as Logging and Object Storage. The other options are not relevant for this requirement. Reference: [Cloud Agent Plugin], [Service Connectors]

NO.27 Which is NOT a valid option for an Oracle Cloud Infrastructure (OCI) compute shape?

* Bare Metal
* Dedicated Virtual Machine Host
* Virtual Machine
* Exadata Virtual Machine

Explanation

Exadata Virtual Machine is not a valid option for an OCI compute shape. Exadata Virtual Machine is a deployment option for Exadata Cloud Service or Exadata Cloud@Customer, which are services that provide dedicated Exadata infrastructure for running Oracle databases in OCI. Exadata Virtual Machine allows you to create multiple virtual machines on each Exadata compute node and isolate them from each other using Oracle VM technology. The valid options for OCI compute shapes are:

Bare Metal: A bare metal instance is a physical server that gives you direct access to the underlying hardware and full isolation from other tenants.

Dedicated Virtual Machine Host: A dedicated virtual machine host is a physical server that hosts only your virtual machine instances and no other tenant&#8217;s instances.

Virtual Machine: A virtual machine instance is a virtual server that runs on a shared physical server with other tenants&#8217; instances.

Burstable: A burstable instance is a virtual machine instance that has a baseline utilization of either 12% or 50% of each CPU core and can burst above the baseline when needed.

NO.28 Which tool provides a diagram of the implemented topology of all Virtual Cloud Networks (VCNs) in a selected region and tenancy?
* Network Watcher
* Traffic Analytics
* VCN Flow Logs
* Network Visualizer
Network Visualizer is the tool that provides a diagram of the implemented topology of all VCNs in a selected region and tenancy. Network Visualizer is a feature of the OCI Networking service that allows users to view and manage their network resources in a graphical interface. It can help users understand their network topology, troubleshoot issues, and optimize performance. The other options are not tools that provide a diagram of the VCN topology, but rather other features or services of OCI Networking.
Reference: [Network Visualizer]

NO.29 You are using the Oracle Cloud Infrastructure (OCI) Vault service to create and manage Secrets. For your databasepassword, you have created a secret and rotated the secret one time. The secret versions are as follows:

Version Number | Status

&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8212;&#8211;

2 (latest) | Current

1 | Previous

You later realize that you have made a mistake in updating the secret content for version 2 and want to rollback to version 1.

What should you do to rollback to version 1?
* Deprecate version 2 (latest). Create new Secret version 3. Create soft link from version 3 to version 1.
* Create a new secret version 3 and set to Pending. Copy the content of version 1 into version 3.
* From the version 2 (latest) menu, select &#8220;Rollback&#8221; and select version 1 when given the option.
* From the version 1 menu on the OCI console, select &#8220;Promote to Current&#8221;.
Explanation

From the version 1 menu on the OCI console, select &#8220;Promote to Current&#8221;. The explanation is that when you promote a secret version to current, it becomes the latest version of the secret and is used by default when you access the secret. This way, you can rollback to a previous version of the secret without creating a new version.

NO.30 In which two ways can Oracle Security Zones assist with the cloud security shared responsibility model?
* Encrypt storage resources with a customer-managed key.
* Allow access to an unsecured compartment, which is moved from a standard compartment.
* Deny public access to Oracle Cloud Infrastructure resources, such as databases and object storage buckets.
* Add or move a standard compartment to a highly secured security zone compartment.

Oracle Security Zones is a service that helps you enforce best practices and prevent misconfigurations on your OCI resources by applying predefined policies and controls. Some of the benefits of using Security Zones are:

Encrypt storage resources with a customer-managed key: Security Zones require that all storage resources, such as block volumes, boot volumes, file systems, and object storage buckets, are encrypted with a customer-managed key from Vault. This ensures that you have full control over the encryption and decryption of your data at rest.

Deny public access to OCI resources, such as databases and object storage buckets: Security Zones prevent you from creating or updating OCI resources that have public access enabled, such as databases and object storage buckets that are accessible from the internet. This reduces the risk of unauthorized access or data leakage.

NO.31 Which is NOT a valid Oracle Cloud Infrastructure (OCI) Virtual Cloud Network (VCN) approach?
* Ensure not all IP addresses are allocated at once within a VCN or subnet; instead reserve some IP addresses for future use.
* Use OCI tags to tag VCN resources so that all resources follow organizational tagging/naming conventions.
* Private subnets should ideally have individual route tables to control the flow of traffic within and outside of VCN.
* Ensure VCN CIDR prefix overlaps with other VCNs in your tenancy or with your organizations private IP network ranges.

Ensure VCN CIDR prefix overlaps with other VCNs in your tenancy or with your organizations private IP network ranges. The explanation is that a VCN CIDR prefix is the range of IPv4 addresses that can be used within the VCN and its subnets. The VCN CIDR prefix should not overlap with other VCNs in your tenancy or with your organization&#8217;s private IP network ranges, as this can cause routing conflicts and connectivity issues. You should choose a VCN CIDR prefix that is large enough to accommodate your current and future needs, but not too large to waste IP addresses. You can use any of the private IPv4 address ranges specified in RFC 1918 for your VCN CIDR prefix.

NO.32 Your DevOps team needs to interconnect the on-premises network to the Oracle Cloud Infrastructure (OCI) resources, such as a managed database that resides in a private subnet. They indicate that they have a low budget and their bandwidth requirements are minimal, so you decide that a site-to-site VPN is the best option.

They provide you with their router public IP address. You need to create an object in OCI that represents this router. Which object would you create?
* Internet Gateway
* Dynamic Routing Gateway (DRG)
* Customer Premises Equipment (CPE)
* Virtual Network Interface Card (vNIC)
* IPSec Tunnel
* Bastion Host

Customer Premises Equipment (CPE). The explanation is that CPE is an object in OCI that represents your on-premises router or VPN device that connects to your VCN via a site-to-site VPN. A site-to-site VPN is a secure and encrypted connection between your on-premises network and your VCN over the public internet. To set up a site-to-site VPN, you need to create a CPE object with your router&#8217;s public IP address and other information, such as vendor and platform. You also need to create a Dynamic Routing Gateway (DRG) object in your VCN and attach it to your VCN. Then, you need to create an IPSec connection between your CPE and DRG, which will create two redundant VPN tunnels for high availability.

NO.33 Which TWO are key benefits of setting up Site-to-Site VPN on Oracle Cloud Infrastructure (OCI)?
* When setting up Site-to-Site VPN, it creates a private connection that provides consistent network experience.
* When setting up Site-to-Site VPN, customers can configure it to use static or dynamic routing (BGP).
* When setting up Site-to-Site VPN, OCI provisions redundant VPN tunnels.
* When setting up Site-to-Site VPN, customers can expect bandwidth above 2 Gbps.
Explanation

When setting up Site-to-Site VPN, customers can configure it to use static or dynamic routing (BGP). When setting up Site-to-Site VPN, OCI provisions redundant VPN tunnels. The explanation is that Site-to-Site VPN is a secure and encrypted connection between your on-premises network and your Virtual Cloud Network (VCN) in OCI over the public internet. When setting up Site-to-Site VPN, you can choose to use static routing or dynamic routing (Border Gateway Protocol or BGP) to exchange routes between your network and OCI.

OCI also provisions two redundant VPN tunnels for each Site-to-Site VPN connection to provide high availability and failover.

NO.34 You are a security administrator for your company&#8217;s Oracle Cloud Infrastructure (OCI) tenancy. Your storage administrator informs you that she cannot associate an encryption key from an existing Vault to a new Object Storage bucket.

What could be a possible reason for this behavior?
* The Object Storage bucket policy lacks the necessary Access Control List (ACL).
* The storage administrator forgot to select &#8220;Encrypt using Oracle managed keys&#8221; while creating the bucket.
* There is no Identity and Access Management (IAM) policy that allows the Object Storage service to use the key.
* The secret for the key was not created beforehand
There is no Identity and Access Management (IAM) policy that allows the Object Storage service to use the key. The explanation is that when you create an Object Storage bucket with encryption using a customer-managed key from Vault, you need to have an IAM policy that allows the Object Storage service to use the key on your behalf. The policy should look like this:

allow service objectstorage-<region> to use key in compartment <compartment-name> where <region> is the region where your bucket resides and <compartment-name> is the compartment where your key resides.

NO.35 You plan to launch a VM instance with the VM.Standard2.24 shape and Oracle Linux 8 platform image. You want to protect your VM instance from low-level threats, such as rootkits and bootkits that can infect the firmware and operating system and are difficult to detect.

What should you do?
* Use in-transit encryption.
* Use Vulnerability Scanning Service.
* Create a burstable instance.
* Create a shielded instance.
The explanation is that shielded instances are VM instances that have additional security features to protect them from low-level threats, such as rootkits and bootkits that can infect the firmware and operating system and are difficult to detect. Shielded instances use verified boot, which ensures that only trusted software components are executed during the boot process. Shielded instances also use virtual trusted platform module (vTPM), which provides a secure storage for encryption keys and certificates. Shielded instances are available for Oracle Linux 8 platform images with VM.Standard2.* shapes.

NO.36 You plan to upload a large file (3 TiB) to Oracle Cloud Infrastructure (OCI) Object Storage. You would like tominimize the impact of network failures while uploading, and therefore you decide to use the multipart upload capability.

Which TWO statements are true about performing a multipart upload using the Multipart Upload API?
* You do not need to split the object into parts. Object Storage splits the object into parts and uploads all ofthe parts automatically.

* While a multipart upload is still active, you can keep adding parts as long asthe total number is less than10,000.
* You do not have to commit the upload after you have uploaded all the object parts.
* When you split the object into individual parts, each part can be as large as 50 GiB.
Explanation

While a multipart upload is still active, you can keep adding parts as long as the total number is less than

10,000. When you split the object into individual parts, each part can be as large as 50 GiB. The explanation is that a multipart upload allows you to upload a large object in parts, which can improve performance and reliability. You need to split the object into parts yourself and upload each part separately using the Multipart Upload API. You can add parts to an active multipart upload until you reach the maximum number of 10,000 parts per upload. Each part can range from 10 MiB to 50 GiB in size, except for the last part, which can be any size.

NO.37 You are a system administrator of your company and you are managing a complex environment consisting of compute instances running Oracle Linux on Oracle Cloud Infrastructure (OCI). It&#8217;s your task to apply all the latest kernel security updates to all instances.

Which OCI service will allow you to complete this task?
* OCI Streaming service
* OS Management service
* OCI Registry
* OCI Security Zones to achieve automatic security updates
* OCI Cloud Guard to monitor and install the security updates
OS Management service is the OCI service that will allow you to complete this task. OS Management service is a service that helps users automate patching and package management for Oracle Linux and Windows instances in OCI. It can also help users monitor and manage system configuration and compliance across their instances. The other options are not suitable for this task, as they do not provide the functionality of OS Management service. Reference: [OS Management Service]

NO.38 Which Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) policy is invalid?
* Allow dynamic-group FrontEnd to manage instance-family in compartment Project-A
* Allow any-user to inspect users in tenancy
* Allow group A-Developers to create volumes in compartment Project-A
* Allow group A-Admins to manage all-resources in compartment Project-A
Allow group A-Developers to create volumes in compartment Project-A is an invalid IAM policy. This is because create is not a valid verb for volumes. The correct verb for creating volumes is attach. The other options are valid IAM policies that use correct verbs and syntax. Reference: [IAM Policies], [Verbs]

NO.39 You created a virtual cloud network (VCN) with three private subnets. Two of the subnets contain application servers and the third subnet contains a DB System. The application requires a shared file system, therefore you have provisioned one using the file storage service (FSS).

You have also created the corresponding mount target in one of the application subnets. The VCN security lists are properly configured so that the application servers can access FSS. The security team changed the settings for the DB System to have read-only access to the file system. However when they test it, they are unable to access FSS.

How would you allow access to FSS?
* Create an NFS export option that allows READ_ONLY access where the source is the CIDR range of the DB System subnet.
* Create an instance principal for the DB System. Write an Identity and Access Management (IAM) policy that allows the instance principal read-only access to the file storage service.
* Modify the security list associated with the subnet where the mount target resides. Change the ingress rules corresponding to the

DB System subnet to be stateless.
* Modify the security list associated with the subnet where the mount target resides.
* Change the ingress rules corresponding to the DB System subnet to be stateful.
Creating an NFS export option that allows READ_ONLY access where the source is the CIDR range of the DB System subnet is the correct answer. This is because NFS export options are used to control the level of access that clients have to file systems. By creating an NFS export option with READ_ONLY access for the DB System subnet, you can allow the DB System to read data from the file system, but not write or modify it. The other options are not correct, as they do not address the requirement of read-only access for the DB System. Reference: [NFS Export Options]

NO.40 Which THREE protocols are supported by the Oracle Cloud Infrastructure (OCI) Network Load Balancer?
* HTTP
* UDP
* BGP
* TCP
* ICMP
* iSCSI
The explanation is that the OCI Network Load Balancer supports three protocols: UDP, TCP, and ICMP. These protocols are used to distribute traffic across multiple backend servers based on different criteria, such as source and destination IP addresses, ports, and ICMP types and codes.

NO.41 You have a block volume created in the US West (Phoenix) region. You enabled Cross Region Replication for thevolume and selected US West (San Jose) as the destination region. Now, you would like to create a new volumefrom the volume replica in the US West (San Jose) region.

What should you do?
* Activate the replica.
* Trigger the replica.
* No action required. By default, the replica is available as a block volume.
* Initiate the replica.
Explanation

The explanation is that when you enable Cross Region Replication for a block volume, Object Storage creates a replica of the volume in another region of your choice. The replica is not available as a block volume until you activate it. To activate a replica, you need to select the replica from the Block Storage console and click Activate Replica. This will create a new block volume from the replica in the destination region.

Oracle 1z0-1072-23 Dumps PDF Are going to be The Best Score:
https://www.actualtests4sure.com/1z0-1072-23-test-questions.html]