2023 Valid 1z0-1104-23 test answers & Oracle Exam PDF [Q54-Q71
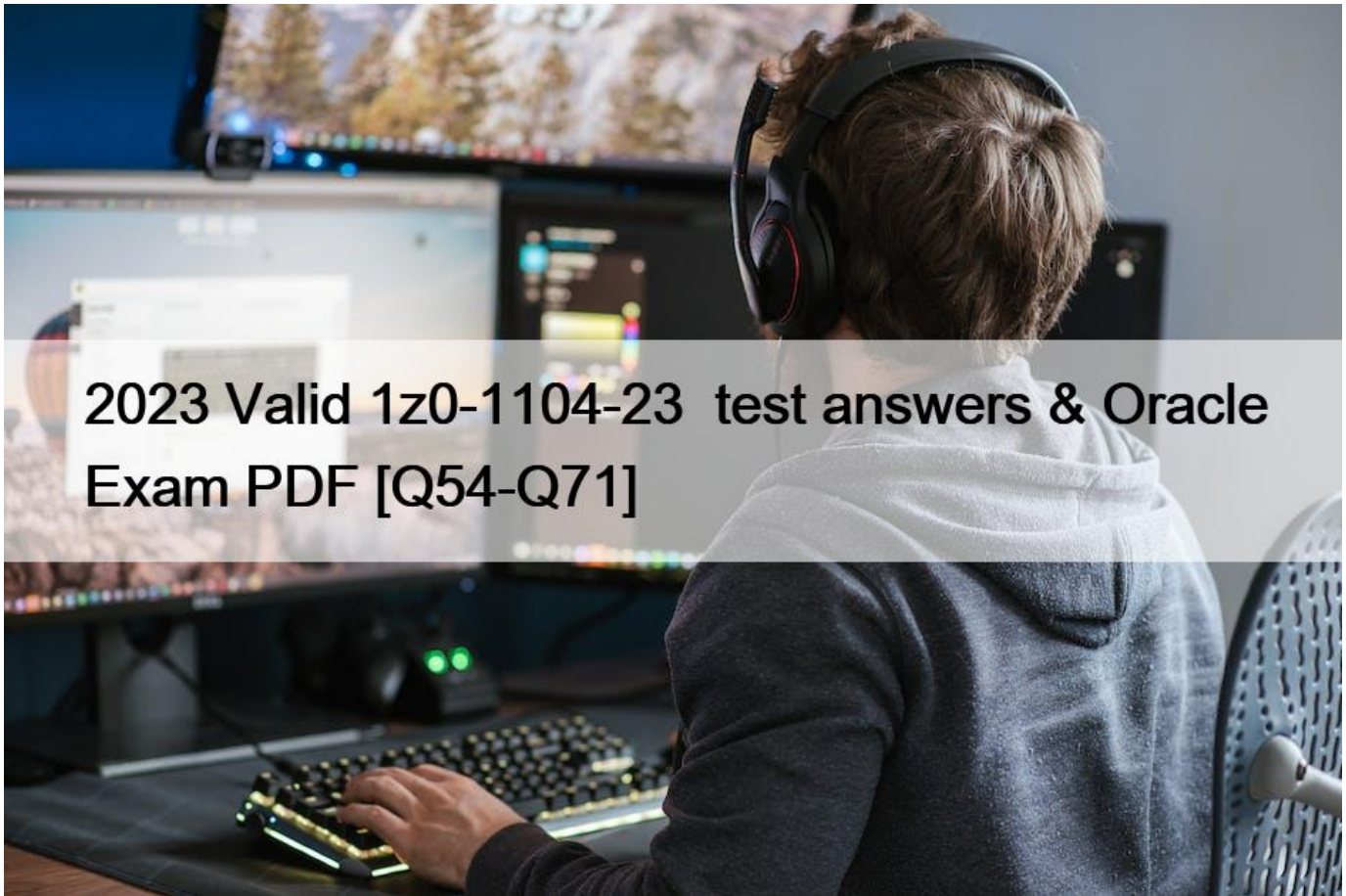

2023 Valid 1z0-1104-23 test answers & Oracle Exam PDF

Free Oracle 1z0-1104-23 Exam Questions and Answer from Training Expert ExamsLabs

Q54. For how long are API calls audited and available?
* 30days
* 90 days
* 365 days
* 60 days
Explanation

https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/Audit/Tasks/settingretentionperiod.

Q55. Which securityissues can be identified by Oracle Vulnerability Scanning Service? Select TWO correct answers
* Distributed Denial of Service (DDoS)
* Ports that are unintentionally left open can be a potential attack vector for cloud resources
* SQL Injection
* CISpublished Industry-standard benchmarks
Explanation

Graphical user interface, text, application, email Description automatically generated

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 ↪.

Q56. Logical isolation for resources is provided by which OCI feature?
* Tenancy
* Availability Zone
* Region
* Compartments
Explanation

Compartments in Oracle Cloud Infrastructure (OCI) are a fundamental component that allows you to create a heterogeneous collection of resources for organization, security isolation, and access control123. They provide a global logical namespace where policies can be enforced, similar to folders in a file system3. By being global, they stretch out to all OCI regions within a given tenancy3.

Q57. Which statement about Oracle Cloud Infrastructure Multi-Factor Authentication (MFA) is NOT valid?
* Users cannot disable MFA for themselves.
* A user can register only one device to use for MFA.
* Users must install a supported authenticator app on the mobile device they intend to register for MFA.
* An administrator can disable MFA for another user.
Explanation

In Oracle Cloud Infrastructure, users can disable Multi-Factor Authentication (MFA) for themselves456. If a user loses their MFA device or wants to register a new one, they can disable MFA for their account and then set it up again with the new device

Q58. An e-commerce company needs to authenticate with third-party API that don’t support OCI’s signature-based authentication.

What can be the solution for the above scenario?
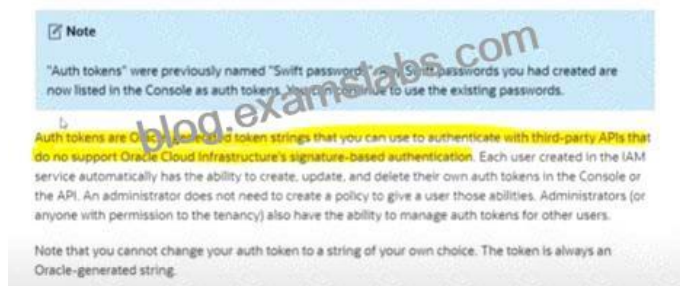* Security Token
* API Key Authentication

* Asymmetric keys
* Auth Token/Swift Password

Explanation

Graphical user interface, text, application, email Description automatically generated

Working with Auth Tokens

> **Note**
>
> "Auth tokens" were previously named "Swift passwords". Any Swift passwords you had created are now listed in the Console as auth tokens. You can continue to use the existing passwords.
>
> Auth tokens are Oracle-generated token strings that you can use to authenticate with third-party APIs that do no support Oracle Cloud Infrastructure's signature-based authentication. Each user created in the IAM service automatically has the ability to create, update, and delete their own auth tokens in the Console or the API. An administrator does not need to create a policy to give a user those abilities. Administrators (or anyone with permission to the tenancy) also have the ability to manage auth tokens for other users.
>
> Note that you cannot change your auth token to a string of your own choice. The token is always an Oracle-generated string.

Q59. A http web server hosted on an Oracle cloud infrastructure compute instance in a public subnet of the vcsl virtual cloudnetwork has a stateless security ingress rule for port 80 access through internet gateway stateful network security group notification for port 80 how will the Oci vcn handle request response traffic to the compute instance for a web page from the http server with port 80?

* network security group would supersede the security utility list and allow both inbound and outbound traffic
* the union of both configuration would happen and allow both inbound and outbound traffic
* due to the conflict in security configuration inbound request traffic would not be allowed
* Because there is no Egress ruled defined in Security List, The Response would not pass through Internet Gateway.

Explanation

In OCI, if there’s a stateless rule in the security list and a stateful rule in the network security group, both rules are evaluated. The union of both configurations would happen, allowing both inbound and outbound traffic. This means that if an incoming packet is allowed by either the security lists or the network security groups, then it’s allowed into the instance. Similarly, if an outgoing packet is allowed by either, then it’s allowed out of the instance

Q60. Which tasks can you perform on a dedicated virtual machine host?

* Manual scaling
* Creating instance pools
* Instance configurations
* Capacity reservations

Explanation

Supported features: Most of the Compute features for VM instances are supported for instances running on dedicated virtual machine hosts. However, the following features arenot supported:

Autoscaling

Capacity reservations

Instance configurations

Instance pools

Burstable instances

Reboot migration. You can use manual migration instead

https://docs.oracle.com/en-us/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm#Dedicated_Virtual_Machi

Q61. What is the minimum active storage duration for logs used by Logging Analytics to be archived?
* 60 days
* 10 days
* 30 days
* 15 days

https://docs.oracle.com/en-us/iaas/logging-analytics/doc/manage-storage.html#:~:text=The%20minimum%20Ac The minimum
Active Storage Duration (Days) for logs before they can be archived is 30 days.

Q62. A company needs to have somebuckets as public in the compartment. You want Cloud Guard to ignore the problem associated
with public bucket. Select TWO correct answers
* Dismiss the issues associated with these resources
* Make the bucket private so that Cloud Guard won’t detectit
* Configure Conditional groups for the detector to fix base line
* First make the bucket private and after few days make the bucket public again

Dismissing the issues associated with these resources in Cloud Guard will prevent these issues from being flagged again. This is
because Cloud Guard allows you to dismiss problems that you don’t want to address, and once dismissed, Cloud Guard does
not raise the problem again unless there is a change in the resource that is associated with the problem. You can find more details
about this in the Oracle Cloud Infrastructure documentation.

Configuring Conditional groups for the detector to fix base line will allow Cloud Guard to understand what is normal for your
infrastructure and not flag these public buckets as issues. Conditional groups in Cloud Guard allow you to modify how detectors
evaluate resources by specifying conditions that a resource must meet for a detector to evaluate it. You can find more details about
this in the Oracle Cloud Infrastructure documentation

Q63. Where are logs stored?
* OCI Object Storage
* OCI File Storage
* OCI Block Storage
* Cloud Agent
Explanation

You can collect log data continuously from Oracle CloudInfrastructure (OCI) Object Storage. To enable the log collection, create
ObjectCollectionRule resource using REST API or CLI. After the successful creation of this resource and having the required IAM
policies, the log collection will be initiated.

https://docs.oracle.com/en-us/iaas/logging-analytics/doc/collect-logs-your-oci-object-storage-bucket.html

Q64. What do the features of OS Management Service do?
* Add complexity in using multiple tools tomanage mixed-OS environments.
* Provide paid service and support to OCI subscribers for fixes on priority.
* Increase security and reliability by regular bug fixes.
* Encourage manual setup to avoid machine-induced errors.
Explanation

https://docs.oracle.com/en/solutions/oci-best-practices/manage-your-operating-systems1.html

Q65. Which of the following is necessary step when creating a secret in vault?

* Vault-managed key is necessary to encrypt the secret
* Digest Hash shouldbe created of the secret value
* Object Storage must be created to run secret service
* Shamir’s secret sharing algorithm should be used to unseal the vault

Explanation

https://docs.oracle.com/en/database/other-databases/essbase/21/essad/create-vault-and-secrets.html

Q66. What does the following identity policy do?

Allow group my-group to use fn-invocation in compartment ABC where target.function.id ='<function-OCID>’

* Enables users in a group to create, update, and delete ALL applications and functions in a compartment
* Enables users to invoke all the functions in a specific application
* Enables users to invoke just one specific function
* Enables users to invoke all the functions in a compartment except for one specific function

Explanation

The policy Allow group my-group to use fn-invocation in compartment ABC where target.function.id ='<function-OCID>’
gives the group my-group permission to invoke a specific function (identified by its OCID) in the compartment ABC. The
fn-invocation verb allows a group to invoke a function, and the condition where target.function.id =
‘<function-OCID>’ ensures that only the specified function can be invoked by this group

Q67. Which is NOT a compliance document?

* Certificate
* Penetration test report
* Attestation
* Bridge letter

Explanation

Types of Compliance Documents

When viewing compliance documents, you can filter onthe following types:

Attestation. A Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Compliance document.

Audit. A general audit report.

Bridge Letter (BridgeLetter). A bridge letter. Bridge letters provide compliance information forthe period of time between the end
date of an SOC report and the date of the release of a new SOC report.

Certificate. A document indicating certification by a particular authority, with regard to certification requirements and examination
results conforming to said requirements.

SOC3. A Service Organization Controls 3 audit report that provides information relating to a service organization’s internal
controls for security, availability, confidentiality, and privacy.

Other. A compliance document that doesn’t fit into any of the preceding, more specific categories.

https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm

Q68. Which OCI service canindex, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor data?

* Data Guard

* Data Safe

* WAF

* Logging Analytics

Explanation

About Logging Analytics

Oracle Cloud Logging Analytics is a cloud solution in Oracle Cloud Infrastructure that lets you index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor all log data from your applications and system infrastructure on cloud or on-premises.

Q69. Which components are a part of the OCI Identity and Access Management service?

* Policies

* Regional subnets

* Compute instances

* VCN

Explanation

https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

Q70. Which statement is true about Oracle Cloud Infrastructure (OCI) Object Storage server-side encryption?

* All the traffic to and from object storage is encrypted by using Transport Layer Security.

* Encryption is not enabled by default.

* Customer-provided encryption keys are never stored in OCI Vault service.

* Each object in a bucket is always encrypted with the same data encryption key.

Oracle Cloud Infrastructure (OCI) Object Storage uses Transport Layer Security (TLS) to encrypt all traffic to and from Object Storage34. This ensures that data is secure during transit.

Q71. A member of operations team has set Pre-Authenticated Request (PAR) associated with a bucket to an incorrect date and now wants to edit the PARrequest. How can this be achieved?

* Don’t set an expiration time for PAR

* Delete the bucket associated with PAR and recreate it

* Delete the PAR and recreate it with the required date

* Delete both PAR as well as the bucket then recreate both

Explanation

Graphical user interface, text, application, email Description automatically generated

Scope and Constraints

Understand the following scope and constraints regarding pre-authenticated requests:

- You can create an unlimited number of pre-authenticated requests.
- A pre-authenticated request created for all objects in a bucket lets request users upload any number of objects to the bucket.
- Expiration date is required, but has no limits. You can set them as far in the future as you want.
- You can't edit a pre-authenticated request. If you want to change user access options or enable object listing in response to changing requirements, you must create a new pre-authenticated request.
- By default, pre-authenticated requests for a bucket or objects with prefix cannot be used to list objects. You can explicitly enable object listing when you create a pre-authenticated request.
- When you create a pre-authenticated request that limits scope to objects with a specific prefix, request users can only GET and PUT objects with the prefix name specified in the request. Trying to GET or PUT an object without the specified prefix or with a different prefix fails.
- 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.
- Deleting a pre-authenticated request revokes user access to the associated bucket or object.
- Pre-authenticated requests cannot be used to delete buckets or objects.
- You cannot delete a bucket that has a pre-authenticated request associated with that bucket or with an object in that bucket.

Top Oracle 1z0-1104-23 Courses Online: https://www.examslabs.com/Oracle/Oracle-Cloud/best-1z0-1104-23-exam-dumps.html]