1Z0-1084-22^{Q&As}

Oracle Cloud Infrastructure 2022 Developer Professional

Pass Oracle 1Z0-1084-22 Exam with 100% Guarantee

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

https://www.passapply.com/1z0-1084-22.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

What is the minimum of storage that a persistent volume claim can obtain in Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE)?

A. 50 GB

B. 10 GB

C. 1 GB

D. 1 TB

Correct Answer: A

The minimum amount of persistent storage that a PVC can request is 50 gigabytes. If the request is for less than 50 gigabytes, the request is rounded up to 50 gigabytes. https://docs.cloud.oracle.com/en-us/iaas/Content/ContEng/Tasks/contengcreatingpersistentvolumeclaim.htm

QUESTION 2

As a cloud-native developer, you have written a web service for your company. You have used Oracle Cloud Infrastructure (OCI) API Gateway service to expose the HTTP backend. However, your security team has suggested that your web

service should handle Distributed Denial-of-Service (DDoS) attack. You are time-constrained and you need to make sure that this is implemented as soon as possible.

What should you do in this scenario?

A. Use OCI virtual cloud network (VCN) segregation to control DDoS.

B. Use a third party service integration to implement a DDoS attack mitigation,

C. Use OCI API Gateway service and configure rate limiting.

D. Re-write your web service and implement rate limiting.

Correct Answer: C

Having created an API gateway and deployed one or more APIs on it, you\'ll typically want to limit the rate at which front-end clients can make requests to back-end services. For example, to:

-maintain high availability and fair use of resources by protecting back ends from being overwhelmed by too many requests

-prevent denial-of-service attacks

-constrain costs of resource consumption

- restrict usage of APIs by your customers\' users in order to monetize APIs You apply a rate limit globally to all routes in an API deployment specification. If a request is denied because the rate limit has been exceeded, the response header

specifies when the request can be retried.

You can add a rate-limiting request policy to an API deployment specification by:

using the Console editing a JSON file

QUESTION 3

You are developing a serverless application with Oracle Functions. Your function needs to store state in a database. Your corporate security Standards mandate encryption of secret information like database passwords. As a function developer, which approach should you follow to satisfy this security requirement?

A. Use the Oracle Cloud Infrastructure Console and enter the password in the function configuration section in the provided input field.

B. Use Oracle Cloud Infrastructure Key Management to auto-encrypt the password. It will inject the auto-decrypted password inside your function container.

C. Encrypt the password using Oracle Cloud Infrastructure Key Management. Decrypt this password in your function code with the generated key.

D. All function configuration variables are automatically encrypted by Oracle Functions.

Correct Answer: A

Passing Custom Configuration Parameters to Functions

he code in functions you deploy to Oracle Functions will typically require values for different parameters. Some pre-defined parameters are available to your functions as environment variables. But you\\'ll often want your functions to use

parameters that you\\'ve defined yourself. For example, you might create a function that reads from and writes to a database. The function will require a database connect string, comprising a username, password, and hostname. You\\'ll

probably want to define username, password, and hostname as parameters that are passed to the function when it\\'s invoked.

Using the Console

To specify custom configuration parameters to pass to functions using the Console:

Log in to the Console as a functions developer.

In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Functions.

Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that\\'s specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle

Cloud Infrastructure). Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure). The Applications page shows the applications defined in the

compartment. Click the name of the application containing functions to which you want to pass custom configuration parameters:

To pass one or more custom configuration parameters to every function in the application, click Configuration to see the Configuration section for the application. To pass one or more custom configuration parameters to a particular function,

click the function\\\'s name to see the Configuration section for the function. In the Configuration section, specify details for the first custom configuration parameter:

Key: The name of the custom configuration parameter. The name must only contain alphanumeric characters and underscores, and must not start with a number. For example, username Value: A value for the custom configuration parameter.

The value must only contain printable unicode characters. For example, jdoe

Click the plus button to save the new custom configuration parameter. Oracle Functions combines the key-value pairs for all the custom configuration parameters (both application-wide and function-specific) in the application into a single,

serially-encoded configuration object with a maximum allowable size of 4Kb. You cannot save the new custom configuration parameter if the size of the serially-encoded configuration object would be greater than 4Kb. (Optional) Enter

additional custom configuration parameters as required.

QUESTION 4

A pod security policy (PSP) is implemented in your Oracle Cloud Infrastructure Container Engine for Kubernetes cluster Which rule can you use to prevent a container from running as root using PSP?

A. NoPrivilege

B. RunOnlyAsUser

C. MustRunAsNonRoot

D. forbiddenRoot

Correct Answer: C

Require the container to run without root privileges.

rule: \\\'MustRunAsNonRoot\\\'

Reference: https://kubernetes.io/docs/concepts/policy/pod-security-policy/

QUESTION 5

Which header is NOT required when signing GET requests to Oracle Cloud Infrastructure APIs?

A. date or x-date

B. (request-target)

C. content-type

D. host

Correct Answer: C

For GET and DELETE requests (when there\'s no content in the request body), the signing string must include at least these headers: (request-target) (as described in draft-cavage-http-signatures-08) host date or x-date (if both are included, Oracle uses x-date)

https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/signingrequests.htm

Latest 1Z0-1084-22 Dumps   1Z0-1084-22 PDF Dumps   1Z0-1084-22 Study Guide