



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.geekcert.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

Given a service deployed on Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE), which annotation should you add in the sample manifest file below to specify a 400 Mbps load balancer?

```
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    <Fill in>
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: nginx
```

- A. service.beta.kubernetes.io/oci-load-balancer-value: 400Mbps
- B. service.beta.kubernetes.io/oci-load-balancer-size: 400Mbps
- C. service.beta.kubernetes.io/oci-load-balancer-shape: 400Mbps
- D. service, beta, kubernetes . io/oci-load-balancer-kind: 400Mbps

Correct Answer: C

QUESTION 2

Which pattern can help you minimize the probability of cascading failures in your system during partial loss of connectivity or a complete service failure?

- A. Retry pattern
- B. Anti-corruption layer pattern
- C. Circuit breaker pattern
- D. Compensating transaction pattern

Correct Answer: C

A cascading failure is a failure that grows over time as a result of positive feedback. It can occur when a portion of an overall system fails, increasing the probability that other portions of the system fail. The circuit breaker pattern prevents the service from performing an operation that is likely to fail. For example, a client service can use a circuit breaker to prevent further remote calls over the network when a downstream service is not functioning properly. This can also prevent the network from becoming congested by a sudden spike in failed retries by one service to another, and it can



also prevent cascading failures. Self-healing circuit breakers check the downstream service at regular intervals and reset the circuit breaker when the downstream service starts functioning properly.
<https://blogs.oracle.com/developers/getting-started-with-microservices-part-three>

QUESTION 3

A developer using Oracle Cloud Infrastructure (OCI) API Gateway must authenticate the API requests to their web application. The authentication process must be implemented using a custom scheme which accepts string parameters from the API caller. Which method can the developer use In this scenario?

- A. Create an authorizer function using request header authorization.
- B. Create an authorizer function using token-based authorization.
- C. Create a cross account functions authorizer.
- D. Create an authorizer function using OCI Identity and Access Management based authentication

Correct Answer: B

Having deployed the authorizer function, you enable authentication and authorization for an API deployment by including two different kinds of request policy in the API deployment specification:

An authentication request policy for the entire API deployment that specifies: The OCID of the authorizer function that you deployed to Oracle Functions that will perform authentication and authorization. The request attributes to pass to the

authorizer function. Whether unauthenticated callers can access routes in the API deployment.

An authorization request policy for each route that specifies the operations a caller is allowed to perform, based on the caller's access scopes as returned by the authorizer function. Using the Console to Add Authentication and Authorization

Request Policies To add authentication and authorization request policies to an API deployment specification using the Console:

Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page. For more information, see [Deploying an API on an API Gateway by Creating an API Deployment](#) and

[Updating API Gateways and API Deployments](#). In the API Request Policies section of the Basic Information page, click the Add button beside Authentication and specify:

Application in : The name of the application in Oracle Functions that contains the authorizer function. You can select an application from a different compartment. Function Name: The name of the authorizer function in

Oracle Functions. Authentication Token: Whether the access token is contained in a request header or a query parameter.

Authentication Token Value: Depending on whether the access token is contained in a request header or a query parameter, specify:

Header Name: If the access token is contained in a request header, enter the name of the header. Parameter Name: If the access token is contained in a query parameter, enter the name of the query parameter.

<https://docs.cloud.oracle.com/en-us/iaas/Content/APIGateway/Tasks/apigatewayaddingauthzauthn.htm>



QUESTION 4

A programmer is developing a Node.js application which will run in a Linux server on their on-premises data center. This application will access various Oracle Cloud Infrastructure (OCI) services using OCI SDKs. What is the secure way to access OCI services with OCI Identity and Access Management (IAM)?

- A. Create a new OCI IAM user associated with a dynamic group and a policy that grants the desired permissions to OCI services. Add the on-premises Linux server in the dynamic group.
- B. Create an OCI IAM policy with the appropriate permissions to access the required OCI services and assign the policy to the on-premises Linux server.
- C. Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, generate the keypair used for signing API requests and upload the public key to the IAM user.
- D. Create a new OCI IAM user, add the user to a group associated with a policy that grants the desired permissions to OCI services. In the on-premises Linux server, add the user name and password to a file used by Node.js authentication.

Correct Answer: C

Before using Oracle Functions, you have to set up an Oracle Cloud Infrastructure API signing key. The instructions in this topic assume:

-

you are using Linux

-

you are following Oracle's recommendation to provide a passphrase to encrypt the private key For more Details Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions

<https://docs.cloud.oracle.com/en-us/iaas/Content/Functions/Tasks/functionssetupapikey.htm>

QUESTION 5

You are implementing logging in your services that will be running in Oracle Cloud Infrastructure Container Engine for Kubernetes. Which statement describes the appropriate logging approach?

- A. Each service logs to its own log file.
- B. All services log to an external logging system.
- C. All services log to standard output only.
- D. All services log to a shared log file.

Correct Answer: C

Application and systems logs can help you understand what is happening inside your cluster. The logs are particularly useful for debugging problems and monitoring cluster activity. Most modern applications have some kind of logging



mechanism; as such, most container engines are likewise designed to support some kind of logging. The easiest and most embraced logging method for containerized applications is to write to the standard output and standard error streams.

<https://kubernetes.io/docs/concepts/cluster-administration/logging/> <https://blogs.oracle.com/developers/5-best-practices-for-kubernetes-security>

[Latest 1Z0-1084-22 Dumps](#)

[1Z0-1084-22 VCE Dumps](#)

[1Z0-1084-22 Exam Questions](#)