



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.pass4itsure.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

You have created a repository in Oracle Cloud Infrastructure Registry in the us-ashburn-1 (iad) region in your tenancy with a namespace called "heyoci. Which three are valid tags for an image named "myapp"?

- A. iad.ocir.io/heyoci/myproject/myapp:0.0.1
- B. us-ashburn-1.ocir.io/heyoci/myapp:0.0.2-beta
- C. us-ashburn-1.ocir.io/heyoci/myproject/myapp:0.0.2-beta
- D. us-ashburn-1.ocir.io/myproject/heyoci/myapp:latest
- E. iad.ocir.io/myproject/heyoci/myapp:latest
- F. iad.ocir.io/heyoci/myapp:0.0.2-beta
- G. iad.ocir.io/heyoci/myapp:latest

Correct Answer: AFG

Give a tag to the image that you're going to push to Oracle Cloud Infrastructure Registry by entering:

docker tag

where:

uniquely identifies the image, either using the image's id (for example, 8e0506e14874), or the image's name and tag separated by a colon (for example, acme-web-app:latest).

is in the format .ocir.io/: where:

is the key for the Oracle Cloud Infrastructure Registry region you're using. For example, iad. See Availability by Region. ocir.io is the Oracle Cloud Infrastructure Registry name. is the auto-generated

Object Storage namespace string of the tenancy that owns the repository to which you want to push the image (as shown on the Tenancy Information page). For example, the namespace of the acme-dev tenancy might be ansh81vru1zp.

Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, acme-dev). Note also that your user must have access to the tenancy.

(if specified) is the name of a repository to which you want to push the image (for example, project01). Note that specifying a repository is optional (see About Repositories). is the name you want to give the

image in Oracle Cloud Infrastructure Registry (for example, acme-web-app).

is an image tag you want to give the image in Oracle Cloud Infrastructure Registry (for example, version2.0.test).

For example, for convenience you might want to group together multiple versions of the acme-web-app image in the acme-dev tenancy in the Ashburn region into a repository called project01. You do this by including the name of the

repository in the image name when you push the image, in the format .ocir.io/:. For example, iad.ocir.io/ansh81vru1zp/project01/acme-web-app:4.6.3. Subsequently,



when you use the docker push command, the presence of the repository in the image's name ensures the image is pushed to the intended repository. If you push an image and include the name of a repository that doesn't already exist, a new

private repository is created automatically. For example, if you enter a command like docker push iad.ocir.io/ansh81vru1zp/project02/acme-web-app:7.5.2 and the project02 repository doesn't exist, a private repository called project02 is

created automatically. If you push an image and don't include a repository name, the image's name is used as the name of the repository. For example, if you enter a command like docker push iad.ocir.io/ansh81vru1zp/acme-web-app:7.5.2

that doesn't contain a repository name, the image's name (acme-web-app) is used as the name of a private repository. [https:// docs.cloud.oracle.com/en-us/iaas/Content/Registry/Concepts/registrywhatisarepository.htm](https://docs.cloud.oracle.com/en-us/iaas/Content/Registry/Concepts/registrywhatisarepository.htm)

QUESTION 2

Per CAP theorem, in which scenario do you NOT need to make any trade-off between the guarantees?

- A. when there are no network partitions
- B. when the system is running in the cloud
- C. when the system is running on-premise
- D. when you are using load balancers

Correct Answer: A

CAP THEOREM

"CONSISTENCY, AVAILABILITY and PARTITION TOLERANCE are the features that we want in our distributed system together"

Of three properties of shared-data systems (Consistency, Availability and tolerance to network Partitions) only two can be achieved at any given moment in time.

QUESTION 3

Which one of the following is NOT a valid backend-type supported by Oracle Cloud Infrastructure (OCI) API Gateway?

- A. STOCK_RESPONSE_BACKEND
- B. ORACLE_FUNCTIONS_BACKEND
- C. ORACLE_STREAMS_BACKEND
- D. HTTP_BACKEND

Correct Answer: C

In the API Gateway service, a back end is the means by which a gateway routes requests to the back- end services that implement APIs. If you add a private endpoint back end to an API gateway, you give the API gateway access to the



VCN associated with that private endpoint. You can also grant an API gateway access to other Oracle Cloud Infrastructure services as back ends. For example, you could grant an API gateway access to Oracle Functions, so you can create and deploy an API that is backed by a serverless function. API Gateway service to create an API gateway, you can create an API deployment to access HTTP and HTTPS URLs. <https://docs.cloud.oracle.com/en-us/iaas/Content/APIGateway/Tasks/apigatewayusinghttpbackend.htm> API Gateway service to create an API gateway, you can create an API deployment that invokes serverless functions defined in Oracle Functions. <https://docs.cloud.oracle.com/en-us/iaas/Content/APIGateway/Tasks/apigatewayusingfunctionsbackend.htm> API Gateway service, you can define a path to a stock response back end <https://docs.cloud.oracle.com/en-us/iaas/Content/APIGateway/Tasks/apigatewayaddingstockresponses.htm>

QUESTION 4

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 5

In the sample Kubernetes manifest file below, what annotations should you add to create a private load balancer In oracle Cloud infrastructure Container Engine for Kubernetes?

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

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

A. service.beta.kubernetes.io/oci-load-balancer-private:"true"



B. service.beta.kubernetes.io/oci-load-balancer-private: "true" service.beta.kubernetes.io/oci-load-balancer-subnet1: "ocid1.subnet.oc1..aaaaa....vdfw"

C. service.beta.kubernetes.io/oci-load-balancer-internal: "true"

D. service.beta.kubernetes.io/oci-load-balancer-internal: "true" service.beta.kubernetes.io/oci-load-balancer-subnet1: "ocid1.subnet.oc1..aaaaa....vdfw"

Correct Answer: D

https://docs.cloud.oracle.com/en-us/iaas/Content/ContEng/Tasks/contengcreatingloadbalancer.htm?TocPath=Services%7CExample%20Network%20Resource%20Configuration%7CUpgrading%20the%20Version%20of%20Kubernetes%20Running%20on%20a%20Master%20Node%7C_____2

0Running%20on%20a%20Master%20Node%7C_____2

Creating Internal Load Balancers in Public and Private Subnets You can create Oracle Cloud Infrastructure load balancers to control access to services running on a cluster:

When you create a `custom` cluster, you select an existing VCN that contains the network resources to be used by the new cluster. If you want to use load balancers to control traffic into the VCN, you select existing public or private subnets in

that VCN to host the load balancers. When you create a `quick cluster`, the VCN that's automatically created contains a public regional subnet to host a load balancer. If you want to host load balancers in private subnets, you can add private

subnets to the VCN later.

Alternatively, you can create an internal load balancer service in a cluster to enable other programs running in the same VCN as the cluster to access services in the cluster. You can host internal load balancers in public subnets and private

subnets.

To create an internal load balancer hosted on a public subnet, add the following annotation in the metadata section of the manifest file:

```
service.beta.kubernetes.io/oci-load-balancer-internal: "true"
```

To create an internal load balancer hosted on a private subnet, add both following annotations in the metadata section of the manifest file:

```
service.beta.kubernetes.io/oci-load-balancer-internal: "true" service.beta.kubernetes.io/oci-load-balancer-subnet1: "ocid1.subnet.oc1..aaaaa....vdfw" where ocid1.subnet.oc1..aaaaa....vdfw is the OCID of the private subnet.
```

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

[1Z0-1084-22 Practice Test](#)

[1Z0-1084-22 Braindumps](#)