# 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

**QUESTION 1**

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 2**

You created a pod called "nginx" and its state is set to Pending. Which command can you run to see the reason why the "nginx" pod is in the pending state?

A. kubect2 logs pod nginx

B. kubect2 describe pod nginx

C. kubect2 get pod nginx

D. Through the Oracle Cloud Infrastructure Console

Correct Answer: B

Debugging Pods

The first step in debugging a pod is taking a look at it. Check the current state of the pod and recent events with the following command:

kubectl describe pods ${POD_NAME}

Look at the state of the containers in the pod. Are they all Running? Have there been recent restarts? Continue debugging depending on the state of the pods.

My pod stays pending

If a pod is stuck in Pending it means that it can not be scheduled onto a node. Generally this is because there are insufficient resources of one type or another that prevent scheduling. Look at the output of the kubectl describe ... command

above. There should be messages from the scheduler about why it can not schedule your pod.

https://kubernetes.io/docs/tasks/debug-application-cluster/debug-pod-replication-controller/

**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**

Your organization uses a federated identity provider to login to your Oracle Cloud Infrastructure (OCI) environment. As a developer, you are writing a script to automate some operation and want to use OCI CLI to do that. Your security team

doesn\\'t allow storing private keys on local machines.

How can you authenticate with OCI CLI?

A. Run oci setup keys and provide your credentials

B. Run oci session refresh --profile

C. Run oci session authenticate and provide your credentials

D. Run oci setup oci-cli-rc --file path/to/target/file

Correct Answer: C

Token-based authentication for the CLI allows customers to authenticate their session interactively, then use the CLI for a single session without an API signing key. This enables customers using an identity provider that is not SCIM-

supported to use a federated user account with the CLI and SDKs.

Starting a Token-based CLI Session

To use token-based authentication for the CLI on a computer with a web browser:

In the CLI, run the following command. This will launch a web browser.

oci session authenticate

In the browser, enter your user credentials. This authentication information is saved to the .config file.

**QUESTION 5**

A programmer Is developing a Node is application which will run in a Linux server on their on-premises data center. This application will access various Oracle Cloud Infrastructure (OC1) services using OCI SDKs. What is the secure way to access OCI services with OCI Identity and Access Management (JAM)?

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 Detials 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