



1Z0-1084-20^{Q&As}

Oracle Cloud Infrastructure Developer 2020 Associate

Pass Oracle 1Z0-1084-20 Exam with 100% Guarantee

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

<https://www.geekcert.com/1z0-1084-20.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

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 2

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>

QUESTION 3

You need to execute a script on a remote instance through Oracle Cloud Infrastructure Resource Manager. Which option can you use?

- A. Use `/bin/sh` with the full path to the location of the script to execute the script.
- B. It cannot be done.
- C. Download the script to a local desktop and execute the script.
- D. Use `remote-exec`

Correct Answer: D

Resource Manager is an Oracle Cloud Infrastructure service that allows you to automate the process of provisioning your Oracle Cloud Infrastructure resources. Using Terraform, Resource Manager helps you install, configure, and manage resources through the "infrastructure-as-code" model. With Resource Manager, you can use Terraform's remote exec functionality to execute scripts or commands on a remote computer. You can also use this technique for other provisioners that require access to the remote resource.

QUESTION 4

You have deployed a Python application on Oracle Cloud Infrastructure Container Engine for Kubernetes. However, during testing you found a bug that you rectified and created a new Docker image. You need to make sure that if this new Image doesn't work then you can roll back to the previous version. Using `kubectl`, which deployment strategies should you choose?

- A. Rolling Update
- B. Canary Deployment
- C. Blue/Green Deployment
- D. A/B Testing

Correct Answer: C

Canary deployments are a pattern for rolling out releases to a subset of users or servers. The idea is to first deploy the change to a small subset of servers, test it, and then roll the change out to the rest of the servers. The canary deployment serves as an early warning indicator with less impact on downtime: if the canary deployment fails, the rest of the servers aren't impacted. Blue-green deployment is a technique that reduces downtime and risk by running two identical production environments called Blue and Green. At any time, only one of the environments is live, with the live environment serving all production traffic. For this example, Blue is currently live and Green is idle. A/B testing is a way to compare two versions of a single variable, typically by testing a subject's response to variant A against variant B, and determining which of the two variants is more effective. A rolling update offers a way to deploy the new version of



your application gradually across your cluster.

QUESTION 5

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/gettingstarted-with-microservices-part-three>

[Latest 1Z0-1084-20 Dumps](#)

[1Z0-1084-20 PDF Dumps](#)

[1Z0-1084-20 Practice Test](#)