1Z0-1084-25 Passleader Review & Test 1Z0-1084-25 Preparation

2025 Latest Dumpleader 1Z0-1084-25 PDF Dumps and 1Z0-1084-25 Exam Engine Free Share: https://drive.google.com/open?id=1N91v7sLAzNEfEwCf1AA-VYNUgNpotce8

Furthermore, Dumpleader is a very responsible and trustworthy platform dedicated to certifying you as a Ariba specialist. We provide a free sample before purchasing Oracle 1Z0-1084-25 valid questions so that you may try and be happy with its varied quality features. Learn for your Oracle certification with confidence by utilizing the Dumpleader 1Z0-1084-25 Study Guide, which is always forward-thinking, convenient, current, and dependable.

No doubt the Oracle Cloud Infrastructure 2025 Developer Professional (1Z0-1084-25) certification is one of the most challenging certification exams in the market. This 1Z0-1084-25 certification exam gives always a tough time to Oracle Cloud Infrastructure 2025 Developer Professional (1Z0-1084-25) exam candidates. The Dumpleader understands this hurdle and offers recommended and real 1Z0-1084-25 Exam Practice questions in three different formats. These formats hold high demand in the market and offer a great solution for quick and complete Oracle Cloud Infrastructure 2025 Developer Professional (1Z0-1084-25) exam preparation.

>> 1Z0-1084-25 Passleader Review <<

1Z0-1084-25 Passleader Review - Pass Guaranteed 2026 1Z0-1084-25: Oracle Cloud Infrastructure 2025 Developer Professional First-grade Test Preparation

Many people may have different ways and focus of study to pass 1Z0-1084-25 exam in the different time intervals, but we will find that in real life, can take quite a long time to learn 1Z0-1084-25 learning questions to be extremely difficult. You may be taken up with all kind of affairs, and sometimes you have to put down something and deal with the other matters for the latter is more urgent and need to be done immediately. With the help of our 1Z0-1084-25 training guide, your dream won't be delayed anymore.

Oracle 1Z0-1084-25 Exam Syllabus Topics:

Topic	Details
Topic 1	• Monitoring & Troubleshooting Cloud-Native Applications: This section of the exam focuses on monitoring and troubleshooting cloud-native applications. It covers using OCI Monitoring to track metrics, OCI Logging for managing logs and performing tasks related to monitoring, logging, and tracing for better observability and issue resolution.

Topic 2	• Cloud Native Fundamentals: This section of the exam measures the skills of target audience and covers the essential principles of cloud-native development. It explains the core concepts, key pillars, and advantages of cloud-native applications. The section also focuses on microservices architecture, including its design methodology and how it supports scalable, distributed applications.
Topic 3	• Testing and Securing Cloud-Native Applications: This section focuses on testing strategies and security for cloud-native applications. It discusses different testing methodologies, securing sensitive information using OCI Vault, and implementing security measures to address cloud-native development challenges.
Topic 4	• Leveraging Serverless Technologies for Cloud Native Development: This section of the exam measures the skills of professionals in serverless development within OCI. It covers creating serverless applications using Oracle Functions, building API gateways for routing traffic, and integrating systems through OCI Streaming Service. Additionally, it explores event-driven architectures using OCI Event Service and how OCI Queue enables asynchronous messaging between microservices.
Topic 5	• Cloud Native Applications and Containerization: This section of the exam covers containerization technologies for cloud-native applications. It explains Docker architecture, its components, and the process of pulling and pushing container images using Oracle Cloud Infrastructure Registry (OCIR). It also explores container orchestration, deploying applications on Oracle Kubernetes Engine (OKE), and using OCI Service Mesh for Kubernetes deployments.

Oracle Cloud Infrastructure 2025 Developer Professional Sample Questions (Q68-Q73):

NEW QUESTION # 68
Your team has chosen to use master encryption key (MEK) within an Oracle Cloud Infrastructure (OCI) Vault for encrypting Kubernetes secrets associated with your microservice deployments in OCI Container Engine for Kubernetes (OKE) clusters so that you can easily manage key rotation. Which of the following is NOT valid about rotating keys in the OCI Vault service?

- A. Each key version is tracked internally with separate unique OCIDS.
- B. Both software and HSM-protected MEKS can be rotated.
- C. When you rotate an MEK, a new key version is automatically generated.
- D. Once rotated, older key versions can be used for encryption until they are deleted.

Answer: D

Explanation:
The correct answer is: "Once rotated, older key versions can be used for encryption until they are deleted." The statement that is NOT valid about rotating keys in the OCI Vault service is: "Once rotated, older key versions can be used for encryption until they are deleted." In the OCI Vault service, when you rotate a master encryption key (MEK), a new key version is automatically generated. However, once a key is rotated and a new version is created, the older key versions are no longer usable for encryption. The purpose of key rotation is to ensure that the encryption keys are regularly updated and that older keys are no longer used to protect sensitive data. This enhances security by minimizing the impact of potential key compromises. The other statements mentioned are valid: Both software and hardware security module (HSM)-protected MEKs can be rotated. This provides flexibility in choosing the type of MEK and ensures that key rotation can be performed regardless of the encryption method used. Each key version is tracked internally with separate unique OCIDs (Oracle Cloud Identifiers). This allows for easy management and tracking of different key versions within the OCI Vault service. In summary, the statement that is NOT valid is the one suggesting that older key versions can still be used for encryption until they are deleted. Key rotation is designed to ensure the use of the latest key version and to retire older key versions to enhance security.

NEW QUESTION # 69
You are creating an API deployment in Oracle Cloud Infrastructure (OCI) API Gateway and you want to configure request policies to control access. Which is NOT available in OCI API Gateway?

- A. Providing authentication and authorization.
- B. Controlling access to the backend OCI resources.
- C. Limiting the number of requests sent to the backend services.

- D. Enabling Cross-Origin Resource Sharing (CORS) support.

Answer: B

Explanation:
The correct answer is: Controlling access to the backend OCI resources. OCI API Gateway does not provide direct control over access to backend OCI resources. It primarily focuses on managing and securing access to APIs exposed through the gateway. The gateway acts as a front-end for APIs and provides features such as authentication, authorization, rate limiting, and CORS support. While you can configure authentication and authorization policies, limit the number of requests, and enable CORS support in OCI API Gateway, it does not directly control access to backend OCI resources. Access to backend resources is typically managed through other means, such as IAM policies, network security rules, or resource-specific access controls.

NEW QUESTION # 70
What is the maximum execution time of Oracle Functions?

- A. 120 seconds
- B. 240 seconds
- C. 300 seconds
- D. 60 seconds

Answer: C

Explanation:
The maximum execution time of Oracle Functions is 300 seconds, which is equivalent to 5 minutes. This means that a function running within Oracle Functions cannot exceed a runtime of 5 minutes. If a function requires longer execution times, alternative approaches such as invoking external services asynchronously or using long-running processes should be considered. It is important to design functions with this execution time limitation in mind to ensure optimal performance and efficiency within the Oracle Functions platform.

NEW QUESTION # 71
Having created a Container Engine for Kubernetes (OKE) cluster, you can use Oracle Cloud Infrastructure (OCI) Logging to view and search the logs of applications running on the worker node compute instances in the cluster. Which task is NOT required to collect and parse application logs? (Choose the best answer.)

- A. Enable monitoring for all worker nodes in the cluster.
- B. Set the OCI Logging option to Enabled for the cluster.
- C. Create a dynamic group with a rule that includes all worker nodes In the cluster.
- D. Configure a custom log in OCI Logging with the appropriate agent configuration.

Answer: A

Explanation:
The correct answer is: Enable monitoring for all worker nodes in the cluster. Enabling monitoring for all worker nodes in the cluster is not required to collect and parse application logs using Oracle Cloud Infrastructure (OCI) Logging. Monitoring is a separate feature that allows you to collect metrics and monitor the health and performance of the worker nodes. To collect and parse application logs, you need to perform the following tasks: Set the OCI Logging option to Enabled for the cluster: This enables the OCI Logging service for the cluster. Create a dynamic group with a rule that includes all worker nodes in the cluster: This helps in targeting the logs generated by the worker nodes. Configure a custom log in OCI Logging with the appropriate agent configuration: This involves specifying the log source, log path, and log format to parse and collect the application logs. By completing these tasks, you can collect and parse the application logs generated by the applications running on the worker node compute instances in the OKE cluster.

NEW QUESTION # 72
From a DevOps process standpoint, it is a good practice to keep changes to an application under version control. Which of the following allows changes to a Docker image to be stored in a version control system?

- A. Updating docker-compose.yml
- B. Updating Dockerfile

- C. Executing docker commit
- D. Executing docker save

Answer: C

Explanation:
The option that allows changes to a Docker image to be stored in a version control system is: docker commit The docker commit command is used to create a new image from a container's changes. It takes a running container as input, captures the changes made to it, and creates a new image with those changes. This new image can then be tagged and pushed to a registry, or saved locally. By using docker commit, you can effectively capture the changes made to a container as a new image and store it in a version control system along with the Dockerfile and other project files. This allows for reproducibility and traceability of changes to the Docker image over time.

NEW QUESTION # 73

......