Free Questions for Professional-Cloud-DevOps-Engineer by certscare

Shared by Wilder on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are configuring Cloud Logging for a new application that runs on a Compute Engine instance with a public IP address. A user-managed service account is attached to the instance. You confirmed that the necessary agents are running on the instance but you cannot see any log entries from the instance in Cloud Logging. You want to resolve the issue by following Google-recommended practices. What should you do?

Options:

A) Add the Logs Writer role to the service account.

B) Enable Private Google Access on the subnet that the instance is in.

C) Update the instance to use the default Compute Engine service account.

D) Export the service account key and configure the agents to use the key.

Answer:

A

Explanation:

The correct answer is

A) Add the Logs Writer role to the service account.

To use Cloud Logging, the service account attached to the Compute Engine instance must have the necessary permissions to write log entries. The Logs Writer role (roles/logging.logWriter) provides this permission. You can grant this role to the user-managed service account at the project, folder, or organization level1.

Private Google Access is not required for Cloud Logging, as it allows instances without external IP addresses to access Google APIs and services2. The default Compute Engine service account already has the Logs Writer role, but it is not a recommended practice to use it for user applications3. Exporting the service account key and configuring the agents to use the key is not a secure way of authenticating the service account, as it exposes the key to potential compromise4.

1: Access control with IAM | Cloud Logging | Google Cloud

2: Private Google Access overview | VPC | Google Cloud

3: Service accounts | Compute Engine Documentation | Google Cloud

4: Best practices for securing service accounts | IAM Documentation | Google Cloud

Question 2

Question Type: **MultipleChoice**

Your product is currently deployed in three Google Cloud Platform (GCP) zones with your users divided between the zones. You can fail over from one zone to another, but it causes a 10-minute service disruption for the affected users. You typically experience a database failure once per quarter and can detect it within five minutes. You are cataloging the reliability risks of a new real-time chat feature for your product. You catalog the following information for each risk:

* Mean Time to Detect (MUD} in minutes

* Mean Time to Repair (MTTR) in minutes

* Mean Time Between Failure (MTBF) in days

* User Impact Percentage

The chat feature requires a new database system that takes twice as long to successfully fail over between zones. You want to account for the risk of the new database failing in one zone. What would be the values for the risk of database failover with the new system?

A.

MTTD: 5

MTTR: 10

MTBF: 90

Impact: 33%

B.

MTTD:5

MTTR: 20

MTBF: 90

Impact: 33%

Options:

C) MTTD:5
MTTR: 10
MTBF: 90
Impact 50%
D.
MTTD:5
MTTR: 20
MTBF: 90
Impact: 50%

Answer:

C

Question 3

Question Type: MultipleChoice

You are part of an organization that follows SRE practices and principles. You are taking over the management of a new service from the Development Team, and you conduct a Production Readiness Review (PRR). After the PRR analysis phase, you determine that the service cannot currently meet its Service Level Objectives (SLOs). You want to ensure that the service can meet its SLOs in production. What should you do next?

Adjust the SLO targets to be achievable by the service so you can bring it into production.

Options:

B) Notify the development team that they will have to provide production support for the service.

C) Identify recommended reliability improvements to the service to be completed before handover.

D) Bring the service into production with no SLOs and build them when you have collected operational data.

Answer:

C

Question 4

Question Type: MultipleChoice

You are configuring Cloud Logging for a new application that runs on a Compute Engine instance with a public IP address. A user-managed service account is attached to the instance. You confirmed that the necessary agents are running on the instance but you cannot see any log entries from the instance in Cloud Logging. You want to resolve the issue by following Google-recommended practices. What should you do?

Options:

A) Add the Logs Writer role to the service account.

B) Enable Private Google Access on the subnet that the instance is in.

C) Update the instance to use the default Compute Engine service account.

D) Export the service account key and configure the agents to use the key.

Answer:

A

Explanation:

The correct answer is

A) Add the Logs Writer role to the service account.

To use Cloud Logging, the service account attached to the Compute Engine instance must have the necessary permissions to write log entries. The Logs Writer role (roles/logging.logWriter) provides this permission. You can grant this role to the user-managed service account at the project, folder, or organization level1.

Private Google Access is not required for Cloud Logging, as it allows instances without external IP addresses to access Google APIs and services2. The default Compute Engine service account already has the Logs Writer role, but it is not a recommended practice to use it for user applications3. Exporting the service account key and configuring the agents to use the key is not a secure way of authenticating the service account, as it exposes the key to potential compromise4.

1: Access control with IAM | Cloud Logging | Google Cloud

2: Private Google Access overview | VPC | Google Cloud

3: Service accounts | Compute Engine Documentation | Google Cloud

4: Best practices for securing service accounts | IAM Documentation | Google Cloud