Associate-Cloud-Engineer合格受験記、Associate-Cloud-Engineer問題集

P.S. CertShikenがGoogle Driveで共有している無料かつ新しいAssociate-Cloud-Engineerダンプ：https://drive.google.com/open?id=1L7o5D_DWgMLxCqedOaYJx1RxlACWd0Rk

当社GoogleのAssociate-Cloud-Engineerガイド急流は、過去の試験論文と業界での人気の傾向に基づいて、厳密な分析と要約を行っており、改訂および更新されています。 Associate-Cloud-Engineer試験問題により、洗練された概念が簡素化されました。このソフトウェアは、さまざまな自己学習および自己評価機能を強化して、学習結果を確認します。 Associate-Cloud-Engineerテストトレントのソフトウェアは、統計レポート機能を提供し、学生が脆弱なリンクを見つけて対処するのに役立ちます。 Associate-Cloud-Engineer試験問題のこのバージョンを使用すると、試験に簡単に合格することができます。

Google Associate-Cloud-Engineer認定は、GCPのスキルと知識を示すための優れた方法です。この認定は、グローバルに認知され、クラウドコンピューティングのキャリアを始めたり、進歩させたりするための貴重な資産です。適切な準備とトレーニングを行えば、誰でもこの試験に合格し、GCPプロフェッショナルの成長するコミュニティに参加できます。

Google Associate-Cloud-Engineer 認定試験は、クラウドコンピューティングにおけるスキルと知識を検証するための優れた機会です。この資格は、IT業界でキャリアアップしたい個人や、Google Cloudテクノロジーの専門知識を認められたい個人にとって、価値のある資格です。クラウドコンピューティングのプロフェッショナルの需要が高まる中、この認定試験に合格することで、新しいキャリアの機会を得たり、求人市場で競争力を維持することができます。

>> Associate-Cloud-Engineer合格受験記 <<

高品質なAssociate-Cloud-Engineer合格受験記試験-試験の準備方法-効率的なAssociate-Cloud-Engineer問題集

空想は人間が素晴らしいアイデアをたくさん思い付くことができますが、行動しなければ何の役に立たないのです。GoogleのAssociate-Cloud-Engineer認定試験に合格のにどうしたらいいかと困っているより、パソコンを起動して、CertShikenをクリックしたほうがいいです。CertShikenのトレーニング資料は１００パーセントの合格率を保証しますから、あなたのニーズを満たすことができます。

Google Associate-Cloud-Engineer試験は、クラウドコンピューティングに関する知識とスキルをテストするGoogleが提供する認定試験です。この試験は、試験受験者がコンピューティング、ストレージ、ネットワーキング、セキュリティを含むGoogle Cloud Platform（GCP）サービスを展開および管理する能力を評価するように設計されています。この試験は、クラウドコンピューティングの経験があり、自分のスキルと知識を確認したい個人を対象としています。

Google Associate Cloud Engineer Exam 認定 Associate-Cloud-Engineer 試験問題 (Q220-Q225):

質問 # 220
You are the team lead of a group of 10 developers. You provided each developer with an individual Google Cloud Project that they can use as their personal sandbox to experiment with different Google Cloud solutions. You want to be notified if any of the developers are spending above $500 per month on their sandbox environment. What should you do?

- A. Create a separate billing account per sandbox project and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per billing account.
- B. Create a budget per project and configure budget alerts on all of these budgets.
- C. Create a single billing account for all sandbox projects and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per project.
- D. Create a single budget for all projects and configure budget alerts on this budget.

正解：B

解説：
Key is anyone goes above $500 means it requires project level.
https://cloud.google.com/billing/docs/how-to/budgets

質問 # 221
You've deployed a microservice called myapp1 to a Google Kubernetes Engine cluster using the YAML file specified below:
You need to refactor this configuration so that the database password is not stored in plain text. You want to follow Google-recommended practices. What should you do?

- A. Store the database password in a file inside a Kubernetes persistent volume, and use a persistent volume claim to mount the volume to the container.
- B. Store the database password inside the Docker image of the container, not in the YAML file.
- C. Store the database password inside a ConfigMap object. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap.
- D. Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.

正解：D

解説：
https://cloud.google.com/config-connector/docs/how-to/secrets#gcloud

質問 # 222
Your team is building a website that handles votes from a large user population. The incoming votes will arrive at various rates. You want to optimize the storage and processing of the votes. What should you do?

- A. Save the incoming votes to Firestore. Use Cloud Scheduler to trigger a Cloud Functions instance to periodically process the votes.
- B. Save the incoming votes to Pub/Sub. Use the Pub/Sub topic to trigger a Cloud Functions instance to process the votes.
- C. Save the incoming votes to a JSON file on Cloud Storage. Process the votes in a batch at the end of the day.
- D. Use a dedicated instance to process the incoming votes. Send the votes directly to this instance.

正解：B

解説：
Pub/Sub is a fully managed, real-time messaging service that allows you to send and receive messages between independent applications. Pub/Sub can handle fluctuating and high-volume data streams, such as votes from a large user population. You can use Pub/Sub to save the incoming votes to a topic, which is a named resource that represents the stream of messages. You can also use Pub/Sub to trigger a Cloud Functions instance to process the votes. Cloud Functions is a serverless platform that runs single-purpose functions in response to events. Cloud Functions can scale automatically based on the demand, and you only pay for the resources you use. You can use Cloud Functions to perform any logic or computation on the votes, such as counting, filtering,

aggregating, or storing them.
This option is the best choice for optimizing the storage and processing of the votes, as it provides high scalability, low latency, and low cost. It also requires minimal operational and infrastructure management, as both Pub/Sub and Cloud Functions are fully managed services.
The other options are not correct because they either do not provide the required scalability, performance, or functionality. Option A is not correct because using a dedicated instance to process the incoming votes, and sending the votes directly to this instance, is not scalable, as the instance may not be able to handle the variable and high load of the votes. It is also not efficient, as the instance may be underutilized or overutilized at different times. Saving the incoming votes to a JSON file on Cloud Storage, and processing the votes in a batch at the end of the day, is not optimal, as it introduces latency and complexity in the processing. Option B is not correct because saving the incoming votes to Firestore, and using Cloud Scheduler to trigger a Cloud Functions instance to periodically process the votes, is not suitable for high-volume and real-time data streams, such as votes. Firestore is a serverless, NoSQL database that is designed for structured and hierarchical data, not for unstructured and flat data, such as votes. Cloud Scheduler is a fully managed cron job service that allows you to schedule tasks at fixed intervals, not in response to events. Using Cloud Scheduler to trigger Cloud Functions may introduce unnecessary delays and overhead in the processing.
Reference:
Pub/Sub documentation
Cloud Functions documentation
Choosing a storage option
Choosing an event-driven compute platform

質問 # 223
After a recent security incident, your startup company wants better insight into what is happening in the Google Cloud environment. You need to monitor unexpected firewall changes and instance creation. Your company prefers simple solutions. What should you do?

- A. Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.
- B. Install Kibana on a compute Instance. Create a log sink to forward Cloud Audit Logs filtered for firewalls and compute instances to Pub/Sub. Target the Pub/Sub topic to push messages to the Kibana instance. Analyze the logs on Kibana in real time.
- C. Create a log sink to forward Cloud Audit Logs filtered for firewalls and compute instances to Cloud Storage.Use BigQuery to periodically analyze log events in the storage bucket.
- D. Turn on Google Cloud firewall rules logging, and set up alerts for any insert, update, or delete events.

正解：A

解説：
This answer is the simplest and most effective way to monitor unexpected firewall changes and instance creation in Google Cloud. Cloud Logging filters allow you to specify the criteria for the log entries that you want to view or export. You can use the Logging query language to write filters based on the LogEntry fields, such as resource.type, severity, or protoPayload.methodName. For example, you can filter for firewall-related events by using the following query:
resource.type="gce_subnetwork" logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall" You can filter for instance-related events by using the following query:
resource.type="gce_instance" logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Factivity_log" You can create log-based metrics from these filters to measure the rate or count of log entries that match the filter. Log-based metrics can be used to create charts and dashboards in Cloud Monitoring, or to set up alerts based on the metric values. For example, you can create an alert policy that triggers when the log-based metric for firewall changes exceeds a certain threshold in a given time interval. This way, you can get notified of any unexpected or malicious changes to your firewall rules.
Option B is incorrect because it is unnecessarily complex and costly. Installing Kibana on a compute instance requires additional configuration and maintenance. Creating a log sink to forward Cloud Audit Logs to Pub/Sub also incurs additional charges for the Pub/Sub service. Analyzing the logs on Kibana in real time may not be feasible or efficient, as it requires constant monitoring and manual intervention.
Option C is incorrect because Google Cloud firewall rules logging is a different feature from Cloud Audit Logs. Firewall rules logging allows you to audit, verify, and analyze the effects of your firewall rules by creating connection records for each rule that applies to traffic. However, firewall rules logging does not log the insert, update, or delete events for the firewall rules themselves. Those events are logged by Cloud Audit Logs, which record the administrative activities in your Google Cloud project.
Option D is incorrect because it is not a real-time solution. Creating a log sink to forward Cloud Audit Logs to Cloud Storage requires additional storage space and charges. Using BigQuery to periodically analyze log events in the storage bucket also incurs additional costs for the BigQuery service. Moreover, this option does not provide any alerting mechanism to notify you of any unexpected or malicious changes to your firewall rules or instances.

質問 # 224
You need to create an autoscaling managed instance group for an HTTPS web application. You want to make sure that unhealthy VMs are recreated. What should you do?

- A. In the Instance Template, add the label 'health-check'.
- B. In the Instance Template, add a startup script that sends a heartbeat to the metadata server.
- C. Select Multi-Zone instead of Single-Zone when creating the Managed Instance Group.
- D. Create a health check on port 443 and use that when creating the Managed Instance Group.

正解：A

質問 # 225
.....