

Exam Questions Associate-Cloud-Engineer

Google Cloud Certified - Associate Cloud Engineer

<https://www.2passeasy.com/dumps/Associate-Cloud-Engineer/>



NEW QUESTION 1

You significantly changed a complex Deployment Manager template and want to confirm that the dependencies of all defined resources are properly met before committing it to the project. You want the most rapid feedback on your changes. What should you do?

- A. Use granular logging statements within a Deployment Manager template authored in Python.
- B. Monitor activity of the Deployment Manager execution on the Stackdriver Logging page of the GCP Console.
- C. Execute the Deployment Manager template against a separate project with the same configuration, and monitor for failures.
- D. Execute the Deployment Manager template using the `--preview` option in the same project, and observe the state of interdependent resources.

Answer: D

NEW QUESTION 2

You have developed an application that consists of multiple microservices, with each microservice packaged in its own Docker container image. You want to deploy the entire application on Google Kubernetes Engine so that each microservice can be scaled individually. What should you do?

- A. Create and deploy a Custom Resource Definition per microservice.
- B. Create and deploy a Docker Compose File.
- C. Create and deploy a Job per microservice.
- D. Create and deploy a Deployment per microservice.

Answer: D

NEW QUESTION 3

You are working for a hospital that stores its medical images in an on-premises data room. The hospital wants to use Cloud Storage for archival storage of these images. The hospital wants an automated process to upload any new medical images to Cloud Storage. You need to design and implement a solution. What should you do?

- A. Deploy a Dataflow job from the batch template "Datastore to Cloud Storage" Schedule the batch job on the desired interval
- B. In the Cloud Console, go to Cloud Storage Upload the relevant images to the appropriate bucket
- C. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage Schedule the script as a cron job
- D. Create a Pub/Sub topic, and enable a Cloud Storage trigger for the Pub/Sub topic
- E. Create an application that sends all medical images to the Pub/Sub topic

Answer: C

Explanation:

they require cloud storage for archival and they want to automate the process to upload new medical images to cloud storage, hence we go for gsutil to copy on-prem images to cloud storage and automate the process via cron job. whereas Pub/Sub listens to the changes in the Cloud Storage bucket and triggers the pub/sub topic, which is not required.

NEW QUESTION 4

You have a single binary application that you want to run on Google Cloud Platform. You decided to automatically scale the application based on underlying infrastructure CPU usage. Your organizational policies require you to use virtual machines directly. You need to ensure that the application scaling is operationally efficient and completed as quickly as possible. What should you do?

- A. Create a Google Kubernetes Engine cluster, and use horizontal pod autoscaling to scale the application.
- B. Create an instance template, and use the template in a managed instance group with autoscaling configured.
- C. Create an instance template, and use the template in a managed instance group that scales up and down based on the time of day.
- D. Use a set of third-party tools to build automation around scaling the application up and down, based on Stackdriver CPU usage monitoring.

Answer: B

Explanation:

Managed instance groups offer autoscaling capabilities that let you automatically add or delete instances from a managed instance group based on increases or decreases in load (CPU Utilization in this case). Autoscaling helps your apps gracefully handle increases in traffic and reduce costs when the need for resources is lower. You define the autoscaling policy and the autoscaler performs automatic scaling based on the measured load (CPU Utilization in this case). Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling). Ref: <https://cloud.google.com/compute/docs/autoscaler>

NEW QUESTION 5

You received a JSON file that contained a private key of a Service Account in order to get access to several resources in a Google Cloud project. You downloaded and installed the Cloud SDK and want to use this private key for authentication and authorization when performing gcloud commands. What should you do?

- A. Use the command `gcloud auth login` and point it to the private key
- B. Use the command `gcloud auth activate-service-account` and point it to the private key
- C. Place the private key file in the installation directory of the Cloud SDK and rename it to "credentials.json"
- D. Place the private key file in your home directory and rename it to "GOOGLE_APPLICATION_CREDENTIALS".

Answer: B

Explanation:

Authorizing with a service account

`gcloud auth activate-service-account` authorizes access using a service account. As with `gcloud init` and `gcloud auth login`, this command saves the service account credentials to the local system on successful completion and sets the specified account as the active account in your Cloud SDK configuration.

https://cloud.google.com/sdk/docs/authorizing#authorizing_with_a_service_account

NEW QUESTION 6

You are operating a Google Kubernetes Engine (GKE) cluster for your company where different teams can run non-production workloads. Your Machine Learning (ML) team needs access to Nvidia Tesla P100 GPUs to train their models. You want to minimize effort and cost. What should you do?

- A. Ask your ML team to add the "accelerator: gpu" annotation to their pod specification.
- B. Recreate all the nodes of the GKE cluster to enable GPUs on all of them.
- C. Create your own Kubernetes cluster on top of Compute Engine with nodes that have GPU
- D. Dedicate this cluster to your ML team.
- E. Add a new, GPU-enabled, node pool to the GKE cluster
- F. Ask your ML team to add the cloud.google.com/gke -accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

Answer: D

Explanation:

This is the most optimal solution. Rather than recreating all nodes, you create a new node pool with GPU enabled. You then modify the pod specification to target particular GPU types by adding node selector to your workloads Pod specification. You still have a single cluster so you pay Kubernetes cluster management fee for just one cluster thus minimizing the

cost. Ref: <https://cloud.google.com/kubernetes-engine/docs/how-to/gpus> Ref: <https://cloud.google.com/kubern>

Example:

```
> apiVersion: v1
> kind: Pod
> metadata:
> name: my-gpu-pod
> spec:
> containers:
> name: my-gpu-container
> image: nvidia/cuda:10.0-runtime-ubuntu18.04
> command: ["/bin/bash"]
> resources:
> limits:
> nvidia.com/gpu: 2
> nodeSelector:
> cloud.google.com/gke-accelerator: nvidia-tesla-k80 # or nvidia-tesla-p100 or nvidia-tesla-p4 or nvidia-tesla-v100 or nvidia-tesla-t4
```

NEW QUESTION 7

You have just created a new project which will be used to deploy a globally distributed application. You will use Cloud Spanner for data storage. You want to create a Cloud Spanner instance. You want to perform the first step in preparation of creating the instance. What should you do?

- A. Grant yourself the IAM role of Cloud Spanner Admin
- B. Create a new VPC network with subnetworks in all desired regions
- C. Configure your Cloud Spanner instance to be multi-regional
- D. Enable the Cloud Spanner API

Answer: D

Explanation:

<https://cloud.google.com/spanner/docs/getting-started/set-up>

NEW QUESTION 8

You need to create a copy of a custom Compute Engine virtual machine (VM) to facilitate an expected increase in application traffic due to a business acquisition. What should you do?

- A. Create a Compute Engine snapshot of your base V
- B. Create your images from that snapshot.
- C. Create a Compute Engine snapshot of your base V
- D. Create your instances from that snapshot.
- E. Create a custom Compute Engine image from a snapshot
- F. Create your images from that image.
- G. Create a custom Compute Engine image from a snapshot
- H. Create your instances from that image.

Answer: D

Explanation:

A custom image belongs only to your project. To create an instance with a custom image, you must first have a custom image.

NEW QUESTION 9

You need to create a custom VPC with a single subnet. The subnet's range must be as large as possible. Which range should you use?

- A. .00.0.0/0
- B. 10.0.0.0/8
- C. 172.16.0.0/12
- D. 192.168.0.0/16

Answer: B

Explanation:

https://cloud.google.com/vpc/docs/vpc#manually_created_subnet_ip_ranges

NEW QUESTION 10

You are deploying a production application on Compute Engine. You want to prevent anyone from accidentally destroying the instance by clicking the wrong button. What should you do?

- A. Disable the flag "Delete boot disk when instance is deleted."
- B. Enable delete protection on the instance.
- C. Disable Automatic restart on the instance.
- D. Enable Preemptibility on the instance.

Answer: B

Explanation:

Preventing Accidental VM Deletion This document describes how to protect specific VM instances from deletion by setting the deletionProtection property on an Instance resource. To learn more about VM instances, read the Instances documentation. As part of your workload, there might be certain VM instances that are critical to running your application or services, such as an instance running a SQL server, a server used as a license manager, and so on. These VM instances might need to stay running indefinitely so you need a way to protect these VMs from being deleted. By setting the deletionProtection flag, a VM instance can be protected from accidental deletion. If a user attempts to delete a VM instance for which you have set the deletionProtection flag, the request fails. Only a user that has been granted a role with compute.instances.create permission can reset the flag to allow the resource to be deleted.

<https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion>

NEW QUESTION 10

You need to set up permissions for a set of Compute Engine instances to enable them to write data into a particular Cloud Storage bucket. You want to follow Google-recommended practices. What should you do?

- A. Create a service account with an access scop
- B. Use the access scope 'https://www.googleapis.com/auth/devstorage.write_only'.
- C. Create a service account with an access scop
- D. Use the access scope 'https://www.googleapis.com/auth/cloud-platform'.
- E. Create a service account and add it to the IAM role 'storage.objectCreator' for that bucket.
- F. Create a service account and add it to the IAM role 'storage.objectAdmin' for that bucket.

Answer: C

Explanation:

https://cloud.google.com/iam/docs/understanding-service-accounts#using_service_accounts_with_compute_eng <https://cloud.google.com/storage/docs/access-control/iam-roles>

NEW QUESTION 15

You are running a data warehouse on BigQuery. A partner company is offering a recommendation engine based on the data in your data warehouse. The partner company is also running their application on Google Cloud. They manage the resources in their own project, but they need access to the BigQuery dataset in your project. You want to provide the partner company with access to the dataset What should you do?

- A. Create a Service Account in your own project, and grant this Service Account access to BigQuery in your project
- B. Create a Service Account in your own project, and ask the partner to grant this Service Account access to BigQuery in their project
- C. Ask the partner to create a Service Account in their project, and have them give the Service Account access to BigQuery in their project
- D. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project

Answer: D

Explanation:

<https://gtseres.medium.com/using-service-accounts-across-projects-in-gcp-cf9473fef8f0#:~:text=Go%20to%20t>

NEW QUESTION 16

Your management has asked an external auditor to review all the resources in a specific project. The security team has enabled the Organization Policy called Domain Restricted Sharing on the organization node by specifying only your Cloud Identity domain. You want the auditor to only be able to view, but not modify, the resources in that project. What should you do?

- A. Ask the auditor for their Google account, and give them the Viewer role on the project.
- B. Ask the auditor for their Google account, and give them the Security Reviewer role on the project.
- C. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.
- D. Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project.

Answer: C

Explanation:

Using primitive roles The following table lists the primitive roles that you can grant to access a project, the description of what the role does, and the permissions bundled within that role. Avoid using primitive roles except when absolutely necessary. These roles are very powerful, and include a large number of permissions across all Google Cloud services. For more details on when you should use primitive roles, see the Identity and Access Management FAQ. IAM predefined roles are much more granular, and allow you to carefully manage the set of permissions that your users have access to. See Understanding Roles for a list of roles that can be granted at the project level. Creating custom roles can further increase the control you have over user permissions. https://cloud.google.com/resource-manager/docs/access-control-proj#using_primitive_roles

<https://cloud.google.com/iam/docs/understanding-custom-roles>

NEW QUESTION 19

You need to select and configure compute resources for a set of batch processing jobs. These jobs take around 2 hours to complete and are run nightly. You want to minimize service costs. What should you do?

- A. Select Google Kubernetes Engine
- B. Use a single-node cluster with a small instance type.
- C. Select Google Kubernetes Engine
- D. Use a three-node cluster with micro instance types.
- E. Select Compute Engine
- F. Use preemptible VM instances of the appropriate standard machine type.
- G. Select Compute Engine
- H. Use VM instance types that support micro bursting.

Answer: C

Explanation:

If your apps are fault-tolerant and can withstand possible instance preemptions, then preemptible instances can reduce your Compute Engine costs significantly. For example, batch processing jobs can run on preemptible instances. If some of those instances stop during processing, the job slows but does not completely stop. Preemptible instances complete your batch processing tasks without placing additional workload on your existing instances and without requiring you to pay full price for additional normal instances.

<https://cloud.google.com/compute/docs/instances/preemptible>

NEW QUESTION 24

You need to manage a third-party application that will run on a Compute Engine instance. Other Compute Engine instances are already running with default configuration. Application installation files are hosted on Cloud Storage. You need to access these files from the new instance without allowing other virtual machines (VMs) to access these files. What should you do?

- A. Create the instance with the default Compute Engine service account Grant the service account permissions on Cloud Storage.
- B. Create the instance with the default Compute Engine service account Add metadata to the objects on Cloud Storage that matches the metadata on the new instance.
- C. Create a new service account and assign this service account to the new instance Grant the service account permissions on Cloud Storage.
- D. Create a new service account and assign this service account to the new instance Add metadata to the objects on Cloud Storage that matches the metadata on the new instance.

Answer: C

Explanation:

<https://cloud.google.com/iam/docs/best-practices-for-using-and-managing-service-accounts>

If an application uses third-party or custom identities and needs to access a resource, such as a BigQuery dataset or a Cloud Storage bucket, it must perform a transition between principals. Because Google Cloud APIs don't recognize third-party or custom identities, the application can't propagate the end-user's identity to BigQuery or Cloud Storage. Instead, the application has to perform the access by using a different Google identity.

NEW QUESTION 29

You host a static website on Cloud Storage. Recently, you began to include links to PDF files on this site. Currently, when users click on the links to these PDF files, their browsers prompt them to save the file onto their local system. Instead, you want the clicked PDF files to be displayed within the browser window directly, without prompting the user to save the file locally. What should you do?

- A. Enable Cloud CDN on the website frontend.
- B. Enable 'Share publicly' on the PDF file objects.
- C. Set Content-Type metadata to application/pdf on the PDF file objects.
- D. Add a label to the storage bucket with a key of Content-Type and value of application/pdf.

Answer: C

Explanation:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_Types#importance_of_setting_t

NEW QUESTION 34

You are building an application that stores relational data from users. Users across the globe will use this application. Your CTO is concerned about the scaling requirements because the size of the user base is unknown. You need to implement a database solution that can scale with your user growth with minimum configuration changes. Which storage solution should you use?

- A. Cloud SQL
- B. Cloud Spanner
- C. Cloud Firestore
- D. Cloud Datastore

Answer: B

Explanation:

Cloud Spanner is a relational database and is highly scalable. Cloud Spanner is a highly scalable, enterprise-grade, globally-distributed, and strongly consistent database service built for the cloud specifically to combine the benefits of relational database structure with a non-relational horizontal scale. This combination delivers high-performance transactions and strong consistency across rows, regions, and continents with an industry-leading 99.999% availability SLA, no planned downtime, and enterprise-grade security

Ref: <https://cloud.google.com/spanner>

Graphical user interface, application, Teams Description automatically generated

	CLOUD SPANNER	TRADITIONAL RELATIONAL	TRADITIONAL NON-RELATIONAL
Schema	✓ Yes	✓ Yes	✗ No
SQL	✓ Yes	✓ Yes	✗ No
Consistency	✓ Strong	✓ Strong	✗ Eventual
Availability	✓ High	✗ Failover	✓ High
Scalability	✓ Horizontal	✗ Vertical	✓ Horizontal
Replication	✓ Automatic	⚙️ Configurable	⚙️ Configurable

NEW QUESTION 39

You are asked to set up application performance monitoring on Google Cloud projects A, B, and C as a single pane of glass. You want to monitor CPU, memory, and disk. What should you do?

- A. Enable API and then share charts from project A, B, and C.
- B. Enable API and then give the metrics.reader role to projects A, B, and C.
- C. Enable API and then use default dashboards to view all projects in sequence.
- D. Enable API, create a workspace under project A, and then add project B and C.

Answer: D

Explanation:

<https://cloud.google.com/monitoring/settings/multiple-projects> <https://cloud.google.com/monitoring/workspaces>

NEW QUESTION 43

You have an application that uses Cloud Spanner as a database backend to keep current state information about users. Cloud Bigtable logs all events triggered by users. You export Cloud Spanner data to Cloud Storage during daily backups. One of your analysts asks you to join data from Cloud Spanner and Cloud Bigtable for specific users. You want to complete this ad hoc request as efficiently as possible. What should you do?

- A. Create a dataflow job that copies data from Cloud Bigtable and Cloud Storage for specific users.
- B. Create a dataflow job that copies data from Cloud Bigtable and Cloud Spanner for specific users.
- C. Create a Cloud Dataproc cluster that runs a Spark job to extract data from Cloud Bigtable and Cloud Storage for specific users.
- D. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable.
- E. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

Answer: D

Explanation:

"The Cloud Spanner to Cloud Storage Text template is a batch pipeline that reads in data from a Cloud Spanner table, optionally transforms the data via a JavaScript User Defined Function (UDF) that you provide, and writes it to Cloud Storage as CSV text files."

<https://cloud.google.com/dataflow/docs/guides/templates/provided-batch#cloudspannertogcstext>

"The Dataflow connector for Cloud Spanner lets you read data from and write data to Cloud Spanner in a Dataflow pipeline"

<https://cloud.google.com/spanner/docs/dataflow-connector> <https://cloud.google.com/bigquery/external-data-sources>

NEW QUESTION 48

You manage three Google Cloud projects with the Cloud Monitoring API enabled. You want to follow Google-recommended practices to visualize CPU and network metrics for all three projects together. What should you do?

- A. * 1. Create a Cloud Monitoring Dashboard* 2. Collect metrics and publish them into the Pub/Sub topics 3. Add CPU and network Charts (or each of the three projects)
- B. * 1. Create a Cloud Monitoring Dashboard.* 2. Select the CPU and Network metrics from the three projects.* 3. Add CPU and network Charts for each of the three projects.
- C. * 1 Create a Service Account and apply roles/viewer on the three projects* 2. Collect metrics and publish them to the Cloud Monitoring API* 3. Add CPU and network Charts for each of the three projects.
- D. * 1. Create a fourth Google Cloud project* 2 Create a Cloud Workspace from the fourth project and add the other three projects

Answer: B

NEW QUESTION 51

You have been asked to set up the billing configuration for a new Google Cloud customer. Your customer wants to group resources that share common IAM policies. What should you do?

- A. Use labels to group resources that share common IAM policies
- B. Use folders to group resources that share common IAM policies
- C. Set up a proper billing account structure to group IAM policies
- D. Set up a proper project naming structure to group IAM policies

Answer: B

Explanation:

Folders are nodes in the Cloud Platform Resource Hierarchy. A folder can contain projects, other folders, or a combination of both. Organizations can use folders to group projects under the organization node in a hierarchy. For example, your organization might contain multiple departments, each with its own set of Google Cloud resources. Folders allow you to group these resources on a per-department basis. Folders are used to group resources that share common IAM policies. While a folder can contain multiple folders or resources, a given folder or resource can have exactly one parent.
<https://cloud.google.com/resource-manager/docs/creating-managing-folders>

NEW QUESTION 56

You have a Dockerfile that you need to deploy on Kubernetes Engine. What should you do?

- A. Use `kubectl app deploy <dockerfilename>`.
- B. Use `gcloud app deploy <dockerfilename>`.
- C. Create a docker image from the Dockerfile and upload it to Container Registry
- D. Create a Deployment YAML file to point to that image
- E. Use `kubectl` to create the deployment with that file.
- F. Create a docker image from the Dockerfile and upload it to Cloud Storage
- G. Create a Deployment YAML file to point to that image
- H. Use `kubectl` to create the deployment with that file.

Answer: C

NEW QUESTION 60

You are hosting an application on bare-metal servers in your own data center. The application needs access to Cloud Storage. However, security policies prevent the servers hosting the application from having public IP addresses or access to the internet. You want to follow Google-recommended practices to provide the application with access to Cloud Storage. What should you do?

- A. 1. Use `nslookup` to get the IP address for `storage.googleapis.com`.2. Negotiate with the security team to be able to give a public IP address to the servers.3. Only allow egress traffic from those servers to the IP addresses for `storage.googleapis.com`.
- B. 1. Using Cloud VPN, create a VPN tunnel to a Virtual Private Cloud (VPC) in Google Cloud Platform (GCP).2. In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance.3. Configure your servers to use that instance as a proxy to access Cloud Storage.
- C. 1. Use Migrate for Compute Engine (formerly known as Velostrata) to migrate those servers to Compute Engine.2. Create an internal load balancer (ILB) that uses `storage.googleapis.com` as backend.3. Configure your new instances to use this ILB as proxy.
- D. 1. Using Cloud VPN or Interconnect, create a tunnel to a VPC in GCP.2. Use Cloud Router to create a custom route advertisement for `199.36.153.4/30`. Announce that network to your on-premises network through the VPN tunnel.3. In your on-premises network, configure your DNS server to resolve `*.googleapis.com` as a CNAME to `restricted.googleapis.com`.

Answer: D

Explanation:

Our requirement is to follow Google recommended practices to achieve the end result. Configuring Private Google Access for On-Premises Hosts is best achieved by VPN/Interconnect + Advertise Routes + Use restricted Google IP Range.

- Using Cloud VPN or Interconnect, create a tunnel to a VPC in GCP
- Using Cloud Router to create a custom route advertisement for `199.36.153.4/30`. Announce that network to your on-premises network through the VPN tunnel.
- In your on-premises network, configure your DNS server to resolve `*.googleapis.com` as a CNAME to `restricted.googleapis.com` is the right answer right, and it is what Google recommends.

Ref: <https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid>

- You must configure routes so that Google API traffic is forwarded through your Cloud VPN or Cloud Interconnect connection, firewall rules on your on-premises firewall to allow the outgoing traffic, and DNS so that traffic to Google APIs resolves to the IP range you've added to your routes.

- You can use Cloud Router Custom Route Advertisement to announce the Restricted Google APIs IP addresses through Cloud Router to your on-premises network.

The Restricted Google APIs IP range is `199.36.153.4/30`. While this is technically a public IP range, Google does not announce it publicly. This IP range is only accessible to hosts that can reach your Google Cloud projects through internal IP ranges, such as through a Cloud VPN or Cloud Interconnect connection. Without having a public IP address or access to the internet, the only way you could connect to cloud storage is if you have an internal route to it.

- So Negotiate with the security team to be able to give public IP addresses to the servers is not right.

Following Google recommended practices is synonymous with using Google's services (Not quite, but it is at least for the exam !!).

- So In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance is not right.
- Migrating the VM to Compute Engine is a bit drastic when Google says it is perfectly fine to have Hybrid Connectivity architectures

<https://cloud.google.com/hybrid-connectivity>.

So,

- Use Migrate for Compute Engine (formerly known as Velostrata) to migrate these servers to Compute Engine is not right.

NEW QUESTION 65

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

Answer: C

Explanation:

Set budgets and budget alerts Overview Avoid surprises on your bill by creating Cloud Billing budgets to monitor all of your Google Cloud charges in one place. A budget enables you to track your actual Google Cloud spend against your planned spend. After you've set a budget amount, you set budget alert threshold rules

that are used to trigger email notifications. Budget alert emails help you stay informed about how your spend is tracking against your budget. 2. Set budget scope Set the budget Scope and then click Next. In the Projects field, select one or more projects that you want to apply the budget alert to. To apply the budget alert to all the projects in the Cloud Billing account, choose Select all.

<https://cloud.google.com/billing/docs/how-to/budgets#budget-scope>

NEW QUESTION 69

Your VMs are running in a subnet that has a subnet mask of 255.255.255.240. The current subnet has no more free IP addresses and you require an additional 10 IP addresses for new VMs. The existing and new VMs should all be able to reach each other without additional routes. What should you do?

- A. Use gcloud to expand the IP range of the current subnet.
- B. Delete the subnet, and recreate it using a wider range of IP addresses.
- C. Create a new project
- D. Use Shared VPC to share the current network with the new project.
- E. Create a new subnet with the same starting IP but a wider range to overwrite the current subnet.

Answer: A

Explanation:

<https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range>

gcloud compute networks subnets expand-ip-range - expand the IP range of a Compute Engine subnetwork gcloud compute networks subnets expand-ip-range

NAME --prefix-length=PREFIX_LENGTH

[--region=REGION] [GLOUD_WIDE_FLAG ...]

NEW QUESTION 73

You need to immediately change the storage class of an existing Google Cloud bucket. You need to reduce service cost for infrequently accessed files stored in that bucket and for all files that will be added to that bucket in the future. What should you do?

- A. Use the gsutil to rewrite the storage class for the bucket Change the default storage class for the bucket
- B. Use the gsutil to rewrite the storage class for the bucket Set up Object Lifecycle management on the bucket
- C. Create a new bucket and change the default storage class for the bucket Set up Object Lifecycle management on lite bucket
- D. Create a new bucket and change the default storage class for the bucket import the files from the previous bucket into the new bucket

Answer: B

NEW QUESTION 76

Your organization has three existing Google Cloud projects. You need to bill the Marketing department for only their Google Cloud services for a new initiative within their group. What should you do?

- A. * 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud Project for the Marketing department* 2. Link the new project to a Marketing Billing Account
- B. * 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud account* 2. Create a new Google Cloud Project for the Marketing department* 3. Set the default key-value project labels to department marketing for all services in this project
- C. * 1. Verify that you are assigned the Organization Administrator IAM role for your organization's Google Cloud account* 2. Create a new Google Cloud Project for the Marketing department 3. Link the new project to a Marketing Billing Account.
- D. * 1. Verify that you are assigned the Organization Administrator IAM role for your organization's Google Cloud account* 2. Create a new Google Cloud Project for the Marketing department* 3. Set the default key value project labels to department marketing for all services in this project

Answer: A

NEW QUESTION 79

You created a Kubernetes deployment by running `kubectl run nginx image=nginx labels=app=prod`. Your Kubernetes cluster is also used by a number of other deployments. How can you find the identifier of the pods for this nginx deployment?

- A. `kubectl get deployments --output=pods`
- B. `gcloud get pods --selector="app=prod"`
- C. `kubectl get pods -l "app=prod"`
- D. `gcloud list gke-deployments -filter={pod }`

Answer: C

Explanation:

This command correctly lists pods that have the label `app=prod`. When creating the deployment, we used the label `app=prod` so listing pods that have this label retrieve the pods belonging to nginx deployments. You can list pods by using Kubernetes CLI `kubectl get pods`.

Ref: <https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/>

Ref: <https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/#list-containe>

NEW QUESTION 81

An employee was terminated, but their access to Google Cloud Platform (GCP) was not removed until 2 weeks later. You need to find out this employee accessed any sensitive customer information after their termination. What should you do?

- A. View System Event Logs in Stackdrive
- B. Search for the user's email as the principal.
- C. View System Event Logs in Stackdrive
- D. Search for the service account associated with the user.
- E. View Data Access audit logs in Stackdrive
- F. Search for the user's email as the principal.
- G. View the Admin Activity log in Stackdrive
- H. Search for the service account associated with the user.

Answer: C

Explanation:

<https://cloud.google.com/logging/docs/audit>

Data Access audit logs Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data.

<https://cloud.google.com/logging/docs/audit#data-access>

NEW QUESTION 82

You deployed an LDAP server on Compute Engine that is reachable via TLS through port 636 using UDP. You want to make sure it is reachable by clients over that port. What should you do?

- A. Add the network tag allow-udp-636 to the VM instance running the LDAP server.
- B. Create a route called allow-udp-636 and set the next hop to be the VM instance running the LDAP server.
- C. Add a network tag of your choice to the instance
- D. Create a firewall rule to allow ingress on UDP port 636 for that network tag.
- E. Add a network tag of your choice to the instance running the LDAP server
- F. Create a firewall rule to allow egress on UDP port 636 for that network tag.

Answer: C

Explanation:

A tag is simply a character string added to a tags field in a resource, such as Compute Engine virtual machine (VM) instances or instance templates. A tag is not a separate resource, so you cannot create it separately. All resources with that string are considered to have that tag. Tags enable you to make firewall rules and routes applicable to specific VM instances.

NEW QUESTION 85

You are monitoring an application and receive user feedback that a specific error is spiking. You notice that the error is caused by a Service Account having insufficient permissions. You are able to solve the problem but want to be notified if the problem recurs. What should you do?

- A. In the Log Viewer, filter the logs on severity 'Error' and the name of the Service Account.
- B. Create a sink to BigQuery to export all the log
- C. Create a Data Studio dashboard on the exported logs.
- D. Create a custom log-based metric for the specific error to be used in an Alerting Policy.
- E. Grant Project Owner access to the Service Account.

Answer: C

NEW QUESTION 89

You have a virtual machine that is currently configured with 2 vCPUs and 4 GB of memory. It is running out of memory. You want to upgrade the virtual machine to have 8 GB of memory. What should you do?

- A. Rely on live migration to move the workload to a machine with more memory.
- B. Use gcloud to add metadata to the VM
- C. Set the key to required-memory-size and the value to 8 GB.
- D. Stop the VM, change the machine type to n1-standard-8, and start the VM.
- E. Stop the VM, increase the memory to 8 GB, and start the VM.

Answer: D

Explanation:

In Google compute engine, if predefined machine types don't meet your needs, you can create an instance with custom virtualized hardware settings. Specifically, you can create an instance with a custom number of vCPUs and custom memory, effectively using a custom machine type. Custom machine types are ideal for the following scenarios: 1. Workloads that aren't a good fit for the predefined machine types that are available you. 2. Workloads that require more processing power or more memory but don't need all of the upgrades that are provided by the next machine type level. In our scenario, we only need a memory upgrade. Moving to a bigger instance would also bump up the CPU which we don't need so we have to use a custom machine type. It is not possible to change memory while the instance is running so you need to first stop the instance, change the memory and then start it again. See below a screenshot that shows how CPU/Memory can be customized for an instance that has been

stopped. Ref: <https://cloud.google.com/compute/docs/instances/creating-instance-with-custom-machine-type>

NEW QUESTION 91

Your company has an internal application for managing transactional orders. The application is used exclusively by employees in a single physical location. The application requires strong consistency, fast queries, and ACID guarantees for multi-table transactional updates. The first version of the application is implemented in PostgreSQL, and you want to deploy it to the cloud with minimal code changes. Which database is most appropriate for this application?

- A. BigQuery
- B. Cloud SQL
- C. Cloud Spanner
- D. Cloud Datastore

Answer: B

Explanation:

<https://cloud.google.com/sql/docs/postgres>

NEW QUESTION 95

You have been asked to set up Object Lifecycle Management for objects stored in storage buckets. The objects are written once and accessed frequently for 30

days. After 30 days, the objects are not read again unless there is a special need. The object should be kept for three years, and you need to minimize cost. What should you do?

- A. Set up a policy that uses Nearline storage for 30 days and then moves to Archive storage for three years.
- B. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.
- C. Set up a policy that uses Nearline storage for 30 days, then moves the Coldline for one year, and then moves to Archive storage for two years.
- D. Set up a policy that uses Standard storage for 30 days, then moves to Coldline for one year, and then moves to Archive storage for two years.

Answer: B

Explanation:

The key to understand the requirement is : "The objects are written once and accessed frequently for 30 days" Standard Storage

Standard Storage is best for data that is frequently accessed ("hot" data) and/or stored for only brief periods of time.

Archive Storage

Archive Storage is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Unlike the "coldest" storage services offered by other Cloud providers, your data is available within milliseconds, not hours or days. Archive Storage is the best choice for data that you plan to access less than once a year.

<https://cloud.google.com/storage/docs/storage-classes#standard>

NEW QUESTION 97

Your company's infrastructure is on-premises, but all machines are running at maximum capacity. You want to burst to Google Cloud. The workloads on Google Cloud must be able to directly communicate to the workloads on-premises using a private IP range. What should you do?

- A. In Google Cloud, configure the VPC as a host for Shared VPC.
- B. In Google Cloud, configure the VPC for VPC Network Peering.
- C. Create bastion hosts both in your on-premises environment and on Google Cloud
- D. Configure both as proxy servers using their public IP addresses.
- E. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Answer: D

Explanation:

"Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization."

<https://cloud.google.com/vpc/docs/vpc-peering> while

"Cloud Interconnect provides low latency, high availability connections that enable you to reliably transfer data between your on-premises and Google Cloud Virtual Private Cloud (VPC) networks."

<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview>

and "HA VPN is a high-availability (HA) Cloud VPN solution that lets you securely connect your on-premises network to your VPC network through an IPsec VPN connection in a single region."

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview>

NEW QUESTION 98

You are storing sensitive information in a Cloud Storage bucket. For legal reasons, you need to be able to record all requests that read any of the stored data. You want to make sure you comply with these requirements. What should you do?

- A. Enable the Identity Aware Proxy API on the project.
- B. Scan the bucket using the Data Loss Prevention API.
- C. Allow only a single Service Account access to read the data.
- D. Enable Data Access audit logs for the Cloud Storage API.

Answer: D

Explanation:

Logged information Within Cloud Audit Logs, there are two types of logs: Admin Activity logs: Entries for operations that modify the configuration or metadata of a project, bucket, or object. Data Access logs: Entries for operations that modify objects or read a project, bucket, or object. There are several sub-types of data access logs: ADMIN_READ: Entries for operations that read the configuration or metadata of a project, bucket, or object. DATA_READ: Entries for operations that read an object. DATA_WRITE: Entries for operations that create or modify an object. <https://cloud.google.com/storage/docs/audit-logs#types>

NEW QUESTION 101

You manage an App Engine Service that aggregates and visualizes data from BigQuery. The application is deployed with the default App Engine Service account. The data that needs to be visualized resides in a different project managed by another team. You do not have access to this project, but you want your application to be able to read data from the BigQuery dataset. What should you do?

- A. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.
- B. Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.
- C. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.
- D. In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project.

Answer: B

Explanation:

The resource that you need to get access is in the other project. roles/bigquery.dataViewer BigQuery Data Viewer

When applied to a table or view, this role provides permissions to: Read data and metadata from the table or view.

This role cannot be applied to individual models or routines.

When applied to a dataset, this role provides permissions to: Read the dataset's metadata and list tables in the dataset. Read data and metadata from the dataset's tables.

When applied at the project or organization level, this role can also enumerate all datasets in the project. Additional roles, however, are necessary to allow the running of jobs.

NEW QUESTION 106

You have a web application deployed as a managed instance group. You have a new version of the application to gradually deploy. Your web application is currently receiving live web traffic. You want to ensure that the available capacity does not decrease during the deployment. What should you do?

- A. Perform a rolling-action start-update with maxSurge set to 0 and maxUnavailable set to 1.
- B. Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.
- C. Create a new managed instance group with an updated instance template
- D. Add the group to the backend service for the load balance
- E. When all instances in the new managed instance group are healthy, delete the old managed instance group.
- F. Create a new instance template with the new application versio
- G. Update the existing managed instance group with the new instance template
- H. Delete the instances in the managed instance group to allow the managed instance group to recreate the instance using the new instance template.

Answer: B

Explanation:

https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max_

NEW QUESTION 111

You have deployed multiple Linux instances on Compute Engine. You plan on adding more instances in the coming weeks. You want to be able to access all of these instances through your SSH client over the Internet without having to configure specific access on the existing and new instances. You do not want the Compute Engine instances to have a public IP. What should you do?

- A. Configure Cloud Identity-Aware Proxy (or HTTPS resources)
- B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.
- C. Create an SSH keypair and store the public key as a project-wide SSH Key
- D. Create an SSH keypair and store the private key as a project-wide SSH Key

Answer: B

Explanation:

<https://cloud.google.com/iap/docs/using-tcp-forwarding>

NEW QUESTION 113

You need to grant access for three users so that they can view and edit table data on a Cloud Spanner instance. What should you do?

- A. Run `gcloud iam roles describe roles/spanner.databaseUser`
- B. Add the users to the role.
- C. Run `gcloud iam roles describe roles/spanner.databaseUser`
- D. Add the users to a new group
- E. Add the group to the role.
- F. Run `gcloud iam roles describe roles/spanner.viewer --project my-projec`
- G. Add the users to the role.
- H. Run `gcloud iam roles describe roles/spanner.viewer --project my-projec`
- I. Add the users to a new group. Add the group to the role.

Answer: B

Explanation:

<https://cloud.google.com/spanner/docs/iam#spanner.databaseUser>

Using the `gcloud` tool, execute the `gcloud iam roles describe roles/spanner.databaseUser` command on Cloud Shell. Attach the users to a newly created Google group and add the group to the role.

NEW QUESTION 115

You built an application on your development laptop that uses Google Cloud services. Your application uses Application Default Credentials for authentication and works fine on your development laptop. You want to migrate this application to a Compute Engine virtual machine (VM) and set up authentication using Google-recommended practices and minimal changes. What should you do?

- A. Assign appropriate access for Google services to the service account used by the Compute Engine VM.
- B. Create a service account with appropriate access for Google services, and configure the application to use this account.
- C. Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application.
- D. Store credentials for your user account with appropriate access for Google services in a config file, and deploy this config file with your application.

Answer: B

Explanation:

In general, Google recommends that each instance that needs to call a Google API should run as a service account with the minimum permissions necessary for that instance to do its job. In practice, this means you should configure service accounts for your instances with the following process: Create a new service account rather than using the Compute Engine default service account. Grant IAM roles to that service account for only the resources that it needs. Configure the instance to run as that service account. Grant the instance the <https://www.googleapis.com/auth/cloud-platform> scope to allow full access to all Google Cloud APIs, so that the IAM permissions of the instance are completely determined by the IAM roles of the service account. Avoid granting more access than necessary and regularly check your service account permissions to make sure they are up-to-date.

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#best_practices

NEW QUESTION 117

You have been asked to migrate a Docker application from datacenter to cloud. Your solution architect has suggested uploading Docker images to GCR in one project and running an application in a GKE cluster in a separate project. You want to store images in the project `img-278322` and run the application in the project `prod-278986`. You want to tag the image as `acme_track_n_trace:v1`. You want to follow Google-recommended practices. What should you do?

- A. Run `gcloud builds submit --tag gcr.io/img-278322/acme_track_n_trace`
- B. Run `gcloud builds submit --tag gcr.io/img-278322/acme_track_n_trace:v1`
- C. Run `gcloud builds submit --tag gcr.io/prod-278986/acme_track_n_trace`
- D. Run `gcloud builds submit --tag gcr.io/prod-278986/acme_track_n_trace:v1`

Answer: B

Explanation:

➤ Run `gcloud builds submit tag gcr.io/img-278322/acme_track_n_trace:v1`. is the right answer.
This command correctly tags the image as `acme_track_n_trace:v1` and uploads the image to the `img-278322` project.
Ref: <https://cloud.google.com/sdk/gcloud/reference/builds/submit>

NEW QUESTION 120

You need to create a Compute Engine instance in a new project that doesn't exist yet. What should you do?

- A. Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.
- B. Enable the Compute Engine API in the Cloud Console, use the Cloud SDK to create the instance, and then use the `—project` flag to specify a new project.
- C. Using the Cloud SDK, create the new instance, and use the `—project` flag to specify the new project. Answer yes when prompted by Cloud SDK to enable the Compute Engine API.
- D. Enable the Compute Engine API in the Cloud Console
- E. Go to the Compute Engine section of the Console to create a new instance, and look for the Create In A New Project option in the creation form.

Answer: A

Explanation:

<https://cloud.google.com/sdk/gcloud/reference/projects/create> Quickstart: Creating a New Instance Using the Command Line Before you begin

- * 1. In the Cloud Console, on the project selector page, select or create a Cloud project.
- * 2. Make sure that billing is enabled for your Google Cloud project. Learn how to confirm billing is enabled for your project.

To use the `gcloud` command-line tool for this quickstart, you must first install and initialize the Cloud SDK:

- * 1. Download and install the Cloud SDK using the instructions given on Installing Google Cloud SDK.
- * 2. Initialize the SDK using the instructions given on Initializing Cloud SDK.

To use `gcloud` in Cloud Shell for this quickstart, first activate Cloud Shell using the instructions given on Starting Cloud Shell.
<https://cloud.google.com/ai-platform/deep-learning-vm/docs/quickstart-cli#before-you-begin>

NEW QUESTION 124

You have an application that uses Cloud Spanner as a backend database. The application has a very predictable traffic pattern. You want to automatically scale up or down the number of Spanner nodes depending on traffic. What should you do?

- A. Create a cron job that runs on a scheduled basis to review stackdriver monitoring metrics, and then resize the Spanner instance accordingly.
- B. Create a Stackdriver alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold
- C. SREs would scale resources up or down accordingly.
- D. Create a Stackdriver alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold
- E. Google support would scale resources up or down accordingly.
- F. Create a Stackdriver alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold
- G. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

Answer: D

Explanation:

As to `mexblood1`'s point, CPU utilization is a recommended proxy for traffic when it comes to Cloud Spanner. See: Alerts for high CPU utilization The following table specifies our recommendations for maximum CPU usage for both single-region and multi-region instances. These numbers are to ensure that your instance has enough compute capacity to continue to serve your traffic in the event of the loss of an entire zone (for single-region instances) or an entire region (for multi-region instances). - <https://cloud.google.com/spanner/docs/cpu-utilization>

NEW QUESTION 126

You have an instance group that you want to load balance. You want the load balancer to terminate the client SSL session. The instance group is used to serve a public web application over HTTPS. You want to follow Google-recommended practices. What should you do?

- A. Configure an HTTP(S) load balancer.
- B. Configure an internal TCP load balancer.
- C. Configure an external SSL proxy load balancer.
- D. Configure an external TCP proxy load balancer.

Answer: A

NEW QUESTION 129

You created a cluster.YAML file containing

- `resources:`
- `name: cluster`
- `type: container.v1.cluster`
- `properties:`
- `zone: europe-west1-b`
- `cluster:`
- `description: My GCP ACE cluster`
- `initialNodeCount: 2`

You want to use Cloud Deployment Manager to create this cluster in GKE.

What should you do?

- A. gcloud deployment-manager deployments create my-gcp-ace-cluster --config cluster.yaml
- B. gcloud deployment-manager deployments create my-gcp-ace-cluster --type container.v1.cluster --config cluster.yaml
- C. gcloud deployment-manager deployments apply my-gcp-ace-cluster --type container.v1.cluster --config cluster.yaml
- D. gcloud deployment-manager deployments apply my-gcp-ace-cluster --config cluster.yaml

Answer: D

Explanation:

gcloud deployment-manager deployments create creates deployments based on the configuration file. (Infrastructure as code). All the configuration related to the artifacts is in the configuration file. This command correctly creates a cluster based on the provided cluster.yaml configuration file.

Ref: <https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/create>

NEW QUESTION 130

You are given a project with a single virtual private cloud (VPC) and a single subnetwork in the us-central1 region. There is a Compute Engine instance hosting an application in this subnetwork. You need to deploy a new instance in the same project in the europe-west1 region. This new instance needs access to the application. You want to follow Google-recommended practices. What should you do?

- A. 1. Create a subnetwork in the same VPC, in europe-west1.2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.
- B. 1. Create a VPC and a subnetwork in europe-west1.2. Expose the application with an internal load balancer.3. Create the new instance in the new subnetwork and use the load balancer's address as the endpoint.
- C. 1. Create a subnetwork in the same VPC, in europe-west1.2. Use Cloud VPN to connect the two subnetworks.3. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.
- D. 1. Create a VPC and a subnetwork in europe-west1.2. Peer the 2 VPCs.3. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

Answer: C

Explanation:

➤ Given that the new instance wants to access the application on the existing compute engine instance, these applications seem to be related so they should be within the same VPC. It is possible to have them in different VPCs and peer the VPCs but this is a lot of additional work and we can simplify this by choosing the option below (which is the answer)

* 1. Create a subnet in the same VPC, in europe-west1.

* 2. Create the new instance in the new subnet and use the first instance subnets private address as the endpoint. is the right answer.

➤ We can create another subnet in the same VPC and this subnet is located in europe-west1. We can then spin up a new instance in this subnet. We also have to set up a firewall rule to allow communication between the two subnets. All instances in the two subnets with the same VPC can communicate through the internal IP Address

Ref: <https://cloud.google.com/vpc>

NEW QUESTION 135

You are building a product on top of Google Kubernetes Engine (GKE). You have a single GKE cluster. For each of your customers, a Pod is running in that cluster, and your customers can run arbitrary code inside their Pod. You want to maximize the isolation between your customers' Pods. What should you do?

- A. Use Binary Authorization and whitelist only the container images used by your customers' Pods.
- B. Use the Container Analysis API to detect vulnerabilities in the containers used by your customers' Pods.
- C. Create a GKE node pool with a sandbox type configured to gvisor
- D. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.
- E. Use the cos_containerd image for your GKE node
- F. Add a nodeSelector with the value cloud.google.com/gke-os-distribution: cos_containerd to the specification of your customers' Pods.

Answer: C

NEW QUESTION 140

Your company has workloads running on Compute Engine and on-premises. The Google Cloud Virtual Private Cloud (VPC) is connected to your WAN over a Virtual Private Network (VPN). You need to deploy a new Compute Engine instance and ensure that no public Internet traffic can be routed to it. What should you do?

- A. Create the instance without a public IP address.
- B. Create the instance with Private Google Access enabled.
- C. Create a deny-all egress firewall rule on the VPC network.
- D. Create a route on the VPC to route all traffic to the instance over the VPN tunnel.

Answer: A

Explanation:

VMs cannot communicate over the internet without a public IP address. Private Google Access permits access to Google APIs and services in Google's production infrastructure.

<https://cloud.google.com/vpc/docs/private-google-access>

NEW QUESTION 144

Your coworker has helped you set up several configurations for gcloud. You've noticed that you're running commands against the wrong project. Being new to the company, you haven't yet memorized any of the projects. With the fewest steps possible, what's the fastest way to switch to the correct configuration?

- A. Run gcloud configurations list followed by gcloud configurations activate .
- B. Run gcloud config list followed by gcloud config activate.
- C. Run gcloud config configurations list followed by gcloud config configurations activate.

D. Re-authenticate with the gcloud auth login command and select the correct configurations on login.

Answer: C

Explanation:

as gcloud config configurations list can help check for the existing configurations and activate can help switch to the configuration.

gcloud config configurations list lists existing named configurations

gcloud config configurations activate activates an existing named configuration

Obtains access credentials for your user account via a web-based authorization flow. When this command completes successfully, it sets the active account in the current configuration to the account specified. If no configuration exists, it creates a configuration named default.

NEW QUESTION 145

You create a Deployment with 2 replicas in a Google Kubernetes Engine cluster that has a single preemptible node pool. After a few minutes, you use kubectl to examine the status of your Pod and observe that one of them is still in Pending status:

```
$ kubectl get pods -l app=myapp
NAME                                READY   STATUS    RESTART  AGE
myapp-deployment-58ddb995-1p86m    0/1     Pending  0        9m
myapp-deployment-58ddb995-qjpkg    1/1     Running  0        9m
```

What is the most likely cause?

- A. The pending Pod's resource requests are too large to fit on a single node of the cluster.
- B. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.
- C. The node pool is configured with a service account that does not have permission to pull the container image used by the pending Pod.
- D. The pending Pod was originally scheduled on a node that has been preempted between the creation of the Deployment and your verification of the Pods' status.
- E. It is currently being rescheduled on a new node.

Answer: B

Explanation:

> The pending Pods resource requests are too large to fit on a single node of the cluster. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod. is the right answer.

> When you have a deployment with some pods in running and other pods in the pending state, more often than not it is a problem with resources on the nodes. Heres a sample output of this use case. We see that the problem is with insufficient CPU on the Kubernetes nodes so we have to either enable auto-scaling or manually scale up the nodes.

NEW QUESTION 146

Your organization has a dedicated person who creates and manages all service accounts for Google Cloud projects. You need to assign this person the minimum role for projects. What should you do?

- A. Add the user to roles/iam.roleAdmin role.
- B. Add the user to roles/iam.securityAdmin role.
- C. Add the user to roles/iam.serviceAccountUser role.
- D. Add the user to roles/iam.serviceAccountAdmin role.

Answer: D

NEW QUESTION 150

You have one GCP account running in your default region and zone and another account running in a non-default region and zone. You want to start a new Compute Engine instance in these two Google Cloud Platform accounts using the command line interface. What should you do?

- A. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.
- B. Create two configurations using gcloud config configurations create [NAME]. Run gcloud configurations list to start the Compute Engine instances.
- C. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud config list to start the Compute Engine instances.
- D. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud configurations list to start the Compute Engine instances.

Answer: A

Explanation:

"Run gcloud configurations list to start the Compute Engine instances". How the heck are you expecting to "start" GCE instances doing "configuration list". Each gcloud configuration has a 1 to 1 relationship with the region (if a region is defined). Since we have two different regions, we would need to create two separate configurations using gcloud config configurations createRef: <https://cloud.google.com/sdk/gcloud/reference/config/configurations/create> Secondly, you can activate each configuration independently by running gcloud config configurations activate [NAME]Ref: <https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate> Finally, while each configuration is active, you can run the gcloud compute instances start [NAME] command to start the instance in the configurations region.<https://cloud.google.com/sdk/gcloud/reference/compute/instances/start>

NEW QUESTION 153

You want to send and consume Cloud Pub/Sub messages from your App Engine application. The Cloud Pub/Sub API is currently disabled. You will use a service account to authenticate your application to the API. You want to make sure your application can use Cloud Pub/Sub. What should you do?

- A. Enable the Cloud Pub/Sub API in the API Library on the GCP Console.
- B. Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it.

- C. Use Deployment Manager to deploy your applicatio
- D. Rely on the automatic enablement of all APIs used by the application being deployed.
- E. Grant the App Engine Default service account the role of Cloud Pub/Sub Admi
- F. Have your application enable the API on the first connection to Cloud Pub/Sub.

Answer: A

Explanation:

Quickstart: using the Google Cloud Console

This page shows you how to perform basic tasks in Pub/Sub using the Google Cloud Console. Note: If you are new to Pub/Sub, we recommend that you start with the interactive tutorial. Before you begin

Set up a Cloud Console project. Set up a project

Click to:

Create or select a project.

Enable the Pub/Sub API for that project.

You can view and manage these resources at any time in the Cloud Console. Install and initialize the Cloud SDK.

Note: You can run the gcloud tool in the Cloud Console without installing the Cloud SDK. To run the gcloud tool in the Cloud Console, use Cloud Shell .

<https://cloud.google.com/pubsub/docs/quickstart-console>

NEW QUESTION 158

You are managing several Google Cloud Platform (GCP) projects and need access to all logs for the past 60 days. You want to be able to explore and quickly analyze the log contents. You want to follow Google- recommended practices to obtain the combined logs for all projects. What should you do?

- A. Navigate to Stackdriver Logging and select resource.labels.project_id=""
- B. Create a Stackdriver Logging Export with a Sink destination to a BigQuery datase
- C. Configure the table expiration to 60 days.
- D. Create a Stackdriver Logging Export with a Sink destination to Cloud Storag
- E. Create a lifecycle rule to delete objects after 60 days.
- F. Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuer
- G. Configure the table expiration to 60 days.

Answer: B

Explanation:

➤ Navigate to Stackdriver Logging and select resource.labels.project_id=*. is not right.

Log entries are held in Stackdriver Logging for a limited time known as the retention period which is 30 days (default configuration). After that, the entries are deleted. To keep log entries longer, you need to export them outside of Stackdriver Logging by configuring log sinks.

Ref: <https://cloud.google.com/blog/products/gcp/best-practices-for-working-with-google-cloud-audit-logging> ➤ Configure a Cloud Scheduler job to read from

Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days. is not right.

While this works, it makes no sense to use Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery when Google provides a feature (export sinks) that does exactly the same thing and works out of the box. Ref: https://cloud.google.com/logging/docs/export/configure_export_v2

➤ Create a Stackdriver Logging Export with a Sink destination to Cloud Storage. Create a lifecycle rule to delete objects after 60 days. is not right.

You can export logs by creating one or more sinks that include a logs query and an export destination. Supported destinations for exported log entries are Cloud Storage, BigQuery, and

Pub/Sub. Ref: https://cloud.google.com/logging/docs/export/configure_export_v2

Sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account. If it makes it easier to exporting from all projects of an organization, you can create an aggregated sink that can export log entries from all the projects, folders, and billing accounts of a Google Cloud

organization. Ref: https://cloud.google.com/logging/docs/export/aggregated_sinks

Either way, we now have the data in Cloud Storage, but querying logs information from Cloud Storage is harder than Querying information from BigQuery dataset. For this reason, we should prefer Big Query over Cloud Storage.

➤ Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days. is the right answer.

You can export logs by creating one or more sinks that include a logs query and an export destination. Supported destinations for exported log entries are Cloud Storage, BigQuery, and

Pub/Sub. Ref: https://cloud.google.com/logging/docs/export/configure_export_v2

Sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account. If it makes it easier to exporting from all projects of an organization, you can create an aggregated sink that can export log entries from all the projects, folders, and billing accounts of a Google Cloud

organization. Ref: https://cloud.google.com/logging/docs/export/aggregated_sinks

Either way, we now have the data in a BigQuery Dataset. Querying information from a Big Query dataset is easier and quicker than analyzing contents in Cloud Storage bucket. As our requirement is to Quickly analyze the log contents, we should prefer Big Query over Cloud Storage.

Also, You can control storage costs and optimize storage usage by setting the default table expiration for newly created tables in a dataset. If you set the property when the dataset is created, any table created in the dataset is deleted after the expiration period. If you set the property after the dataset is created, only new tables are deleted after the expiration period. For example, if you set the default table expiration to 7 days, older data is automatically deleted after 1 week. Ref: <https://cloud.google.com/bigquery/docs/best-practices-storage>

NEW QUESTION 161

Your team maintains the infrastructure for your organization. The current infrastructure requires changes. You need to share your proposed changes with the rest of the team. You want to follow Google's recommended best practices. What should you do?

- A. Use Deployment Manager templates to describe the proposed changes and store them in a Cloud Storage bucket.
- B. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.
- C. Apply the change in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.
- D. Apply the change in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

Answer: B

Explanation:

Showing Deployment Manager templates to your team will allow you to define the changes you want to implement in your cloud infrastructure. You can use Cloud

Source Repositories to store Deployment Manager templates and collaborate with your team. Cloud Source Repositories are fully-featured, scalable, and private Git repositories you can use to store, manage and track changes to your code.
<https://cloud.google.com/source-repositories/docs/features>

NEW QUESTION 163

You have deployed an application on a single Compute Engine instance. The application writes logs to disk. Users start reporting errors with the application. You want to diagnose the problem. What should you do?

- A. Navigate to Cloud Logging and view the application logs.
- B. Connect to the instance's serial console and read the application logs.
- C. Configure a Health Check on the instance and set a Low Healthy Threshold value.
- D. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

Answer: D

NEW QUESTION 167

Your company runs its Linux workloads on Compute Engine instances. Your company will be working with a new operations partner that does not use Google Accounts. You need to grant access to the instances to your operations partner so they can maintain the installed tooling. What should you do?

- A. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.
- B. Tag all the instances with the same network tag.
- C. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag.
- D. Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.
- E. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

Answer: A

Explanation:

IAP controls access to your App Engine apps and Compute Engine VMs running on Google Cloud. It leverages user identity and the context of a request to determine if a user should be allowed access. IAP is a building block toward BeyondCorp, an enterprise security model that enables employees to work from untrusted networks without using a VPN.

By default, IAP uses Google identities and IAM. By leveraging Identity Platform instead, you can authenticate users with a wide range of external identity providers, such as:

- Email/password
- OAuth (Google, Facebook, Twitter, GitHub, Microsoft, etc.) SAML
- OIDC
- Phone number Custom Anonymous

This is useful if your application is already using an external authentication system, and migrating your users to Google accounts is impractical.

<https://cloud.google.com/iap/docs/using-tcp-forwarding#grant-permission>

NEW QUESTION 172

You want to verify the IAM users and roles assigned within a GCP project named my-project. What should you do?

- A. Run `gcloud iam roles list`
- B. Review the output section.
- C. Run `gcloud iam service-accounts list`
- D. Review the output section.
- E. Navigate to the project and then to the IAM section in the GCP Console.
- F. Review the members and roles.
- G. Navigate to the project and then to the Roles section in the GCP Console.
- H. Review the roles and status.

Answer: C

Explanation:

Logged onto console and followed the steps and was able to see all the assigned users and roles.

NEW QUESTION 173

Your organization has strict requirements to control access to Google Cloud projects. You need to enable your Site Reliability Engineers (SREs) to approve requests from the Google Cloud support team when an SRE opens a support case. You want to follow Google-recommended practices. What should you do?

- A. Add your SREs to roles/iam.roleAdmin role.
- B. Add your SREs to roles/accessapproval approver role.
- C. Add your SREs to a group and then add this group to roles/iam roleAdmin role.
- D. Add your SREs to a group and then add this group to roles/accessapproval approver role.

Answer: D

NEW QUESTION 174

You are deploying an application to a Compute Engine VM in a managed instance group. The application must be running at all times, but only a single instance of the VM should run per GCP project. How should you configure the instance group?

- A. Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 1.
- B. Set autoscaling to Off, set the minimum number of instances to 1, and then set the maximum number of instances to 1.
- C. Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 2.
- D. Set autoscaling to Off, set the minimum number of instances to 1, and then set the maximum number of instances to 2.

Answer: A

Explanation:

<https://cloud.google.com/compute/docs/autoscaler#specifications>

Autoscaling works independently from autohealing. If you configure autohealing for your group and an instance fails the health check, the autohealer attempts to recreate the instance. Recreating an instance can cause the number of instances in the group to fall below the autoscaling threshold (minNumReplicas) that you specify.

- > Since we need the application running at all times, we need a minimum 1 instance.
- > Only a single instance of the VM should run, we need a maximum 1 instance.
- > We want the application running at all times. If the VM crashes due to any underlying hardware failure, we want another instance to be added to MIG so that application can continue to serve requests. We can achieve this by enabling autoscaling. The only option that satisfies these three is Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 1.

Ref: <https://cloud.google.com/compute/docs/autoscaler>

NEW QUESTION 178

You are performing a monthly security check of your Google Cloud environment and want to know who has access to view data stored in your Google Cloud Project. What should you do?

- A. Enable Audit Logs for all APIs that are related to data storage.
- B. Review the IAM permissions for any role that allows for data access
- C. Most Voted
- D. Review the Identity-Aware Proxy settings for each resource.
- E. Create a Data Loss Prevention job.

Answer: B

Explanation:

<https://cloud.google.com/logging/docs/audit>

NEW QUESTION 182

You have a Compute Engine instance hosting a production application. You want to receive an email if the instance consumes more than 90% of its CPU resources for more than 15 minutes. You want to use Google services. What should you do?

- A. * 1. Create a consumer Gmail account.* 2. Write a script that monitors the CPU usage.* 3. When the CPU usage exceeds the threshold, have that script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server.
- B. * 1. Create a Stackdriver Workspace, and associate your Google Cloud Platform (GCP) project with it.* 2.Create an Alerting Policy in Stackdriver that uses the threshold as a trigger condition
- C. 3.Configure your email address in the notification channel.
- D. * 1. Create a Stackdriver Workspace, and associate your GCP project with it.* 2.Write a script that monitors the CPU usage and sends it as a custom metric to Stackdriver
- E. 3.Create an uptime check for the instance in Stackdriver.
- F. * 1. In Stackdriver Logging, create a logs-based metric to extract the CPU usage by using this regular expression: CPU Usage: ([0-9]{1,3})%* 2.In Stackdriver Monitoring, create an Alerting Policy based on this metric
- G. 3.Configure your email address in the notification channel.

Answer: B

Explanation:

Specifying conditions for alerting policies This page describes how to specify conditions for alerting policies. The conditions for an alerting policy define what is monitored and when to trigger an alert. For example, suppose you want to define an alerting policy that emails you if the CPU utilization of a Compute Engine VM instance is above 80% for more than 3 minutes. You use the conditions dialog to specify that you want to monitor the CPU utilization of a Compute Engine VM instance, and that you want an alerting policy to trigger when that utilization is above 80% for 3 minutes. <https://cloud.google.com/monitoring/alerts/ui-conditions-ga>
<https://cloud.google.com/monitoring/alerts/using-alerting-ui> <https://cloud.google.com/monitoring/support/notification-options>

NEW QUESTION 187

You have 32 GB of data in a single file that you need to upload to a Nearline Storage bucket. The WAN connection you are using is rated at 1 Gbps, and you are the only one on the connection. You want to use as much of the rated 1 Gbps as possible to transfer the file rapidly. How should you upload the file?

- A. Use the GCP Console to transfer the file instead of gsutil.
- B. Enable parallel composite uploads using gsutil on the file transfer.
- C. Decrease the TCP window size on the machine initiating the transfer.
- D. Change the storage class of the bucket from Nearline to Multi-Regional.

Answer: B

Explanation:

<https://cloud.google.com/storage/docs/parallel-composite-uploads> <https://cloud.google.com/storage/docs/uploads-downloads#parallel-composite-uploads>

NEW QUESTION 191

You want to select and configure a solution for storing and archiving data on Google Cloud Platform. You need to support compliance objectives for data from one geographic location. This data is archived after 30 days and needs to be accessed annually. What should you do?

- A. Select Multi-Regional Storage
- B. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.
- C. Select Multi-Regional Storage
- D. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage.
- E. Select Regional Storage
- F. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage.
- G. Select Regional Storage
- H. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

Answer: D

Explanation:

Google Cloud Coldline is a new cold-tier storage for archival data with access frequency of less than once per year. Unlike other cold storage options, Nearline has no delays prior to data access, so now it is the leading solution among competitors.

The Real description is about Coldline storage Class: Coldline Storage

Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs.

Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Note, however, that for data being kept entirely for backup or archiving purposes, Archive Storage is more cost-effective, as it offers the lowest storage costs.

<https://cloud.google.com/storage/docs/storage-classes#coldline>

NEW QUESTION 195

Your auditor wants to view your organization's use of data in Google Cloud. The auditor is most interested in auditing who accessed data in Cloud Storage buckets. You need to help the auditor access the data they need. What should you do?

- A. Assign the appropriate permissions, and then use Cloud Monitoring to review metrics
- B. Use the export logs API to provide the Admin Activity Audit Logs in the format they want
- C. Turn on Data Access Logs for the buckets they want to audit, and Then build a query in the log viewer that filters on Cloud Storage
- D. Assign the appropriate permissions, and then create a Data Studio report on Admin Activity Audit Logs

Answer: C

Explanation:

Types of audit logs Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization: Admin Activity audit logs Data Access audit logs System Event audit logs Policy Denied audit logs ***Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. <https://cloud.google.com/logging/docs/audit#types>

<https://cloud.google.com/logging/docs/audit#data-access> Cloud Storage: When Cloud Storage usage logs are enabled, Cloud Storage writes usage data to the Cloud Storage bucket, which generates Data Access audit logs for the bucket. The generated Data Access audit log has its caller identity redacted.

NEW QUESTION 198

You are using Container Registry to centrally store your company's container images in a separate project. In another project, you want to create a Google Kubernetes Engine (GKE) cluster. You want to ensure that Kubernetes can download images from Container Registry. What should you do?

- A. In the project where the images are stored, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.
- B. When you create the GKE cluster, choose the Allow full access to all Cloud APIs option under 'Access scopes'.
- C. Create a service account, and give it access to Cloud Storage
- D. Create a P12 key for this service account and use it as an imagePullSecrets in Kubernetes.
- E. Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account.

Answer: A

Explanation:

Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account. is not right.As mentioned above, Container Registry ignores permissions set on individual objects within the storage bucket so this isnt going to work.

Ref: <https://cloud.google.com/container-registry/docs/access-control>

NEW QUESTION 200

You need to configure optimal data storage for files stored in Cloud Storage for minimal cost. The files are used in a mission-critical analytics pipeline that is used continually. The users are in Boston, MA (United States). What should you do?

- A. Configure regional storage for the region closest to the users Configure a Nearline storage class
- B. Configure regional storage for the region closest to the users Configure a Standard storage class
- C. Configure dual-regional storage for the dual region closest to the users Configure a Nearline storageclass
- D. Configure dual-regional storage for the dual region closest to the users Configure a Standard storage class

Answer: D

Explanation:

Keywords: - continually -> Standard - mission-critical analytics -> dual-regional

NEW QUESTION 201

You have a project for your App Engine application that serves a development environment. The required testing has succeeded and you want to create a new project to serve as your production environment. What should you do?

- A. Use gcloud to create the new project, and then deploy your application to the new project.
- B. Use gcloud to create the new project and to copy the deployed application to the new project.
- C. Create a Deployment Manager configuration file that copies the current App Engine deployment into a new project.
- D. Deploy your application again using gcloud and specify the project parameter with the new project name to create the new project.

Answer: A

Explanation:

You can deploy to a different project by using `--project` flag.

By default, the service is deployed the current project configured via:

```
$ gcloud config set core/project PROJECT
```

To override this value for a single deployment, use the `--project` flag:

```
$ gcloud app deploy ~/my_app/app.yaml --project=PROJECT Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy
```

NEW QUESTION 202

You have a website hosted on App Engine standard environment. You want 1% of your users to see a new test version of the website. You want to minimize complexity. What should you do?

- A. Deploy the new version in the same application and use the --migrate option.
- B. Deploy the new version in the same application and use the --splits option to give a weight of 99 to the current version and a weight of 1 to the new version.
- C. Create a new App Engine application in the same project
- D. Deploy the new version in that application. Use the App Engine library to proxy 1% of the requests to the new version.
- E. Create a new App Engine application in the same project
- F. Deploy the new version in that application. Configure your network load balancer to send 1% of the traffic to that new application.

Answer: B

Explanation:

<https://cloud.google.com/appengine/docs/standard/python/splitting-traffic#gcloud>

NEW QUESTION 203

You need a dynamic way of provisioning VMs on Compute Engine. The exact specifications will be in a dedicated configuration file. You want to follow Google's recommended practices. Which method should you use?

- A. Deployment Manager
- B. Cloud Composer
- C. Managed Instance Group
- D. Unmanaged Instance Group

Answer: A

Explanation:

<https://cloud.google.com/deployment-manager/docs/configuration/create-basic-configuration>

NEW QUESTION 206

You've deployed a microservice called myapp1 to a Google Kubernetes Engine cluster using the YAML file specified below:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: myapp1-deployment
spec:
  selector:
    matchLabels:
      app: myapp1
  replicas: 2
  template:
    metadata:
      labels:
        app: myapp1
    spec:
      containers:
      - name: main-container
        image: gcr.io/my-company-repo/myapp1:1.4
        env:
        - name: DB_PASSWORD
          value: "t0ugh2guess!"
        ports:
        - containerPort: 8080
```

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 inside the Docker image of the container, not in the YAML file.
- B. Store the database password inside a Secret object
- C. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.
- D. Store the database password inside a ConfigMap object
- E. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap.
- F. 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.

Answer: B

Explanation:

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

NEW QUESTION 211

Your company publishes large files on an Apache web server that runs on a Compute Engine instance. The Apache web server is not the only application running in the project. You want to receive an email when the egress network costs for the server exceed 100 dollars for the current month as measured by Google Cloud Platform (GCP). What should you do?

- A. Set up a budget alert on the project with an amount of 100 dollars, a threshold of 100%, and notification type of "email."
- B. Set up a budget alert on the billing account with an amount of 100 dollars, a threshold of 100%, and notification type of "email."
- C. Export the billing data to BigQuery
- D. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollar
- E. Schedule the Cloud Function using Cloud Scheduler to run hourly.
- F. Use the Stackdriver Logging Agent to export the Apache web server logs to Stackdriver Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Stackdriver for the current month and sends an email if the size of all HTTP responses, multiplied by current GCP egress prices, totals over 100 dollar
- G. Schedule the Cloud Function using Cloud Scheduler to run hourly.

Answer: C

Explanation:

<https://blog.doit-intl.com/the-truth-behind-google-cloud-egress-traffic-6e8f57b5c2f8>

NEW QUESTION 215

An application generates daily reports in a Compute Engine virtual machine (VM). The VM is in the project corp-iot-insights. Your team operates only in the project corp-aggregate-reports and needs a copy of the daily exports in the bucket corp-aggregate-reports-storage. You want to configure access so that the daily reports from the VM are available in the bucket corp-aggregate-reports-storage and use as few steps as possible while following Google-recommended practices. What should you do?

- A. Move both projects under the same folder.
- B. Grant the VM Service Account the role Storage Object Creator on corp-aggregate-reports-storage.
- C. Create a Shared VPC network between both project
- D. Grant the VM Service Account the role Storage Object Creator on corp-iot-insights.
- E. Make corp-aggregate-reports-storage public and create a folder with a pseudo-randomized suffix name. Share the folder with the IoT team.

Answer: B

Explanation:

Predefined roles

The following table describes Identity and Access Management (IAM) roles that are associated with Cloud Storage and lists the permissions that are contained in each role. Unless otherwise noted, these roles can be applied either to entire projects or specific buckets.

Storage Object Creator (roles/storage.objectCreator) Allows users to create objects. Does not give permission to view, delete, or overwrite objects.

<https://cloud.google.com/storage/docs/access-control/iam-roles#standard-roles>

NEW QUESTION 216

You have an application on a general-purpose Compute Engine instance that is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk. The application primarily reads large files from disk. The disk size is currently 350 GB. You want to provide the maximum amount of throughput while minimizing costs. What should you do?

- A. Increase the size of the disk to 1 TB.
- B. Increase the allocated CPU to the instance.
- C. Migrate to use a Local SSD on the instance.
- D. Migrate to use a Regional SSD on the instance.

Answer: C

Explanation:

Standard persistent disks are efficient and economical for handling sequential read/write operations, but they aren't optimized to handle high rates of random input/output operations per second (IOPS). If your apps require high rates of random IOPS, use SSD persistent disks. SSD persistent disks are designed for single-digit millisecond latencies. Observed latency is application specific.

NEW QUESTION 219

Your company has a large quantity of unstructured data in different file formats. You want to perform ETL transformations on the data. You need to make the data accessible on Google Cloud so it can be processed by a Dataflow job. What should you do?

- A. Upload the data to BigQuery using the bq command line tool.
- B. Upload the data to Cloud Storage using the gsutil command line tool.
- C. Upload the data into Cloud SQL using the import function in the console.
- D. Upload the data into Cloud Spanner using the import function in the console.

Answer: B

Explanation:

"large quantity" : Cloud Storage or BigQuery "files" a file is nothing but an Object

NEW QUESTION 221

You are configuring service accounts for an application that spans multiple projects. Virtual machines (VMs) running in the web-applications project need access to BigQuery datasets in crm-databases-proj. You want to follow Google-recommended practices to give access to the service account in the web-applications project. What should you do?

- A. Give "project owner" for web-applications appropriate roles to crm-databases- proj
- B. Give "project owner" role to crm-databases-proj and the web-applications project.
- C. Give "project owner" role to crm-databases-proj and bigquery.dataViewer role to web-applications.
- D. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

Answer: D

NEW QUESTION 225

You have a number of compute instances belonging to an unmanaged instances group. You need to SSH to one of the Compute Engine instances to run an ad hoc script. You've already authenticated gcloud, however, you don't have an SSH key deployed yet. In the fewest steps possible, what's the easiest way to SSH to the instance?

- A. Run `gcloud compute instances list` to get the IP address of the instance, then use the `ssh` command.
- B. Use the `gcloud compute ssh` command.
- C. Create a key with the `ssh-keygen` command.
- D. Then use the `gcloud compute ssh` command.
- E. Create a key with the `ssh-keygen` command.
- F. Upload the key to the instance.
- G. Run `gcloud compute instances list` to get the IP address of the instance, then use the `ssh` command.

Answer: B

Explanation:

`gcloud compute ssh` ensures that the user's public SSH key is present in the project's metadata. If the user does not have a public SSH key, one is generated using `ssh-keygen` and added to the project's metadata. This is similar to the other option where we copy the key explicitly to the project's metadata but here it is done automatically for us. There are also security benefits with this approach. When we use `gcloud compute ssh` to connect to Linux instances, we are adding a layer of security by storing your host keys as guest attributes. Storing SSH host keys as guest attributes improve the security of your connections by helping to protect against vulnerabilities such as man-in-the-middle (MITM) attacks. On the initial boot of a VM instance, if guest attributes are enabled, Compute Engine stores your generated host keys as guest attributes.

Compute Engine then uses these host keys that were stored during the initial boot to verify all subsequent connections to the VM instance.

Ref: <https://cloud.google.com/compute/docs/instances/connecting-to-instance> Ref: <https://cloud.google.com/s>

NEW QUESTION 227

You need to manage multiple Google Cloud Platform (GCP) projects in the fewest steps possible. You want to configure the Google Cloud SDK command line interface (CLI) so that you can easily manage multiple GCP projects. What should you do?

- A. * 1. Create a configuration for each project you need to manage.* 2. Activate the appropriate configuration when you work with each of your assigned GCP projects.
- B. * 1. Create a configuration for each project you need to manage.* 2. Use `gcloud init` to update the configuration values when you need to work with a non-default project.
- C. * 1. Use the default configuration for one project you need to manage.* 2. Activate the appropriate configuration when you work with each of your assigned GCP projects.
- D. * 1. Use the default configuration for one project you need to manage.* 2. Use `gcloud init` to update the configuration values when you need to work with a non-default project.

Answer: A

Explanation:

<https://cloud.google.com/sdk/gcloud> https://cloud.google.com/sdk/docs/configurations#multiple_configurations

NEW QUESTION 230

Your organization has user identities in Active Directory. Your organization wants to use Active Directory as their source of truth for identities. Your organization wants to have full control over the Google accounts used by employees for all Google services, including your Google Cloud Platform (GCP) organization. What should you do?

- A. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.
- B. Use the Cloud Identity APIs and write a script to synchronize users to Cloud Identity.
- C. Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console.
- D. Ask each employee to create a Google account using self sign-up.
- E. Require that each employee use their company email address and password.

Answer: A

NEW QUESTION 233

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

Answer: A

Explanation:

https://cloud.google.com/compute/docs/instance-groups/autohealing-instances-in-migs#setting_up_an_autohealing_instance_group

NEW QUESTION 234

Your development team needs a new Jenkins server for their project. You need to deploy the server using the fewest steps possible. What should you do?

- A. Download and deploy the Jenkins Java WAR to App Engine Standard.
- B. Create a new Compute Engine instance and install Jenkins through the command line interface.
- C. Create a Kubernetes cluster on Compute Engine and create a deployment with the Jenkins Docker image.
- D. Use GCP Marketplace to launch the Jenkins solution.

Answer: D

NEW QUESTION 237

You have a workload running on Compute Engine that is critical to your business. You want to ensure that the data on the boot disk of this workload is backed up regularly. You need to be able to restore a backup as quickly as possible in case of disaster. You also want older backups to be cleaned automatically to save on cost. You want to follow Google-recommended practices. What should you do?

- A. Create a Cloud Function to create an instance template.
- B. Create a snapshot schedule for the disk using the desired interval.
- C. Create a cron job to create a new disk from the disk using gcloud.
- D. Create a Cloud Task to create an image and export it to Cloud Storage.

Answer: B

Explanation:

Best practices for persistent disk snapshots

You can create persistent disk snapshots at any time, but you can create snapshots more quickly and with greater reliability if you use the following best practices.

Creating frequent snapshots efficiently

Use snapshots to manage your data efficiently.

Create a snapshot of your data on a regular schedule to minimize data loss due to unexpected failure. Improve performance by eliminating excessive snapshot downloads and by creating an image and reusing it. Set your snapshot schedule to off-peak hours to reduce snapshot time.

Snapshot frequency limits

Creating snapshots from persistent disks

You can snapshot your disks at most once every 10 minutes. If you want to issue a burst of requests to snapshot your disks, you can issue at most 6 requests in 60 minutes.

If the limit is exceeded, the operation fails and returns the following error: <https://cloud.google.com/compute/docs/disks/snapshot-best-practices>

NEW QUESTION 241

You want to configure 10 Compute Engine instances for availability when maintenance occurs. Your requirements state that these instances should attempt to automatically restart if they crash. Also, the instances should be highly available including during system maintenance. What should you do?

- A. Create an instance template for the instance
- B. Set the 'Automatic Restart' to o
- C. Set the 'On-host maintenance' to Migrate VM instanc
- D. Add the instance template to an instance group.
- E. Create an instance template for the instance
- F. Set 'Automatic Restart' to of
- G. Set 'On-host maintenance' to Terminate VM instance
- H. Add the instance template to an instance group.
- I. Create an instance group for the instance
- J. Set the 'Autohealing' health check to healthy (HTTP).
- K. Create an instance group for the instanc
- L. Verify that the 'Advanced creation options' setting for 'do not retry machine creation' is set to off.

Answer: A

Explanation:

Create an instance template for the instances so VMs have same specs. Set the "'Automatic Restart' to on to VM automatically restarts upon crash. Set the "'On-host maintenance' to Migrate VM instance. This will take care of VM during maintenance window. It will migrate VM instance making it highly available Add the instance template to an instance group so instances can be managed.

- onHostMaintenance: Determines the behavior when a maintenance event occurs that might cause your instance to reboot.
- [Default] MIGRATE, which causes Compute Engine to live migrate an instance when there is a maintenance event.
- TERMINATE, which stops an instance instead of migrating it.
- automaticRestart: Determines the behavior when an instance crashes or is stopped by the system.
- [Default] true, so Compute Engine restarts an instance if the instance crashes or is stopped.
- false, so Compute Engine does not restart an instance if the instance crashes or is stopped.

Enabling automatic restart ensures that compute engine instances are automatically restarted when they crash. And Enabling Migrate VM Instance enables live migrates i.e. compute instances are migrated during system maintenance and remain running during the migration.

Automatic Restart If your instance is set to terminate when there is a maintenance event, or if your instance crashes because of an underlying hardware issue, you can set up Compute Engine to automatically restart the instance by setting the automaticRestart field to true. This setting does not apply if the instance is taken offline through a user action, such as calling sudo shutdown, or during a zone

outage.Ref: <https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options#autorestart>

Enabling the Migrate VM Instance option migrates your instance away from an infrastructure maintenance event, and your instance remains running during the migration. Your instance might experience a short period of decreased performance, although generally, most instances should not notice any difference. This is ideal for instances that require constant uptime and can tolerate a short period of decreased

performance.Ref: https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options#live_

NEW QUESTION 245

You need to deploy an application, which is packaged in a container image, in a new project. The application exposes an HTTP endpoint and receives very few requests per day. You want to minimize costs. What should you do?

- A. Deploy the container on Cloud Run.
- B. Deploy the container on Cloud Run on GKE.
- C. Deploy the container on App Engine Flexible.
- D. Deploy the container on Google Kubernetes Engine, with cluster autoscaling and horizontal pod autoscaling enabled.

Answer: A

Explanation:

Cloud Run takes any container images and pairs great with the container ecosystem: Cloud Build, Artifact Registry, Docker. ... No infrastructure to manage: once

deployed, Cloud Run manages your services so you can sleep well. Fast autoscaling. Cloud Run automatically scales up or down from zero to N depending on traffic.

<https://cloud.google.com/run>

NEW QUESTION 248

You want to add a new auditor to a Google Cloud Platform project. The auditor should be allowed to read, but not modify, all project items. How should you configure the auditor's permissions?

- A. Create a custom role with view-only project permission
- B. Add the user's account to the custom role.
- C. Create a custom role with view-only service permission
- D. Add the user's account to the custom role.
- E. Select the built-in IAM project Viewer rol
- F. Add the user's account to this role.
- G. Select the built-in IAM service Viewer rol
- H. Add the user's account to this role.

Answer: C

NEW QUESTION 249

Your company uses Cloud Storage to store application backup files for disaster recovery purposes. You want to follow Google's recommended practices. Which storage option should you use?

- A. Multi-Regional Storage
- B. Regional Storage
- C. Nearline Storage
- D. Coldline Storage

Answer: D

NEW QUESTION 254

You are running multiple microservices in a Kubernetes Engine cluster. One microservice is rendering images.

The microservice responsible for the image rendering requires a large amount of CPU time compared to the memory it requires. The other microservices are workloads that are optimized for n1-standard machine types. You need to optimize your cluster so that all workloads are using resources as efficiently as possible. What should you do?

- A. Assign the pods of the image rendering microservice a higher pod priority than the other microservices
- B. Create a node pool with compute-optimized machine type nodes for the image rendering microservice Use the node pool with general-purpose machine type nodes for the other microservices
- C. Use the node pool with general-purpose machine type nodes for lite mage rendering microservice Create a nodepool with compute-optimized machine type nodes for the other microservices
- D. Configure the required amount of CPU and memory in the resource requests specification of the image rendering microservice deployment Keep the resource requests for the other microservices at the default

Answer: B

NEW QUESTION 258

You built an application on Google Cloud Platform that uses Cloud Spanner. Your support team needs to monitor the environment but should not have access to table data. You need a streamlined solution to grant the correct permissions to your support team, and you want to follow Google-recommended practices. What should you do?

- A. Add the support team group to the roles/monitoring.viewer role
- B. Add the support team group to the roles/spanner.databaseUser role.
- C. Add the support team group to the roles/spanner.databaseReader role.
- D. Add the support team group to the roles/stackdriver.accounts.viewer role.

Answer: A

Explanation:

➤ roles/monitoring.viewer provides read-only access to get and list information about all monitoring data and configurations. This role provides monitoring access and fits our requirements. roles/monitoring.viewer. is the right answer.

Ref: <https://cloud.google.com/iam/docs/understanding-roles#cloud-spanner-roles>

NEW QUESTION 260

You have a batch workload that runs every night and uses a large number of virtual machines (VMs). It is fault-tolerant and can tolerate some of the VMs being terminated. The current cost of VMs is too high. What should you do?

- A. Run a test using simulated maintenance event
- B. If the test is successful, use preemptible N1 Standard VMs when running future jobs.
- C. Run a test using simulated maintenance event
- D. If the test is successful, use N1 Standard VMs when running future jobs.
- E. Run a test using a managed instance group
- F. If the test is successful, use N1 Standard VMs in the managed instance group when running future jobs.
- G. Run a test using N1 standard VMs instead of N2. If the test is successful, use N1 Standard VMs when running future jobs.

Answer: A

Explanation:

Creating and starting a preemptible VM instance This page explains how to create and use a preemptible virtual machine (VM) instance. A preemptible instance is an instance you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances will always terminate after 24 hours. To learn more about preemptible instances, read the preemptible instances documentation. Preemptible instances are recommended only for fault-tolerant applications that can withstand instance preemptions. Make sure your application can handle preemptions before you decide to create a preemptible instance. To understand the risks and value of preemptible instances, read the preemptible instances documentation. <https://cloud.google.com/compute/docs/instances/create-start-preemptible-instance>

NEW QUESTION 264

Your finance team wants to view the billing report for your projects. You want to make sure that the finance team does not get additional permissions to the project. What should you do?

- A. Add the group for the finance team to roles/billing user role.
- B. Add the group for the finance team to roles/billing admin role.
- C. Add the group for the finance team to roles/billing viewer role.
- D. Add the group for the finance team to roles/billing project/Manager role.

Answer: C

Explanation:

"Billing Account Viewer access would usually be granted to finance teams, it provides access to spend information, but does not confer the right to link or unlink projects or otherwise manage the properties of the billing account." <https://cloud.google.com/billing/docs/how-to/billing-access>

NEW QUESTION 266

Your organization needs to grant users access to query datasets in BigQuery but prevent them from accidentally deleting the datasets. You want a solution that follows Google-recommended practices. What should you do?

- A. Add users to roles/bigquery user role only, instead of roles/bigquery dataOwner.
- B. Add users to roles/bigquery dataEditor role only, instead of roles/bigquery dataOwner.
- C. Create a custom role by removing delete permissions, and add users to that role only.
- D. Create a custom role by removing delete permission
- E. Add users to the group, and then add the group to the custom role.

Answer: D

Explanation:

https://cloud.google.com/bigquery/docs/access-control#custom_roles

Custom roles enable you to enforce the principle of least privilege, ensuring that the user and service accounts in your organization have only the permissions essential to performing their intended functions.

NEW QUESTION 270

You need to create a custom IAM role for use with a GCP service. All permissions in the role must be suitable for production use. You also want to clearly share with your organization the status of the custom role. This will be the first version of the custom role. What should you do?

- A. Use permissions in your role that use the 'supported' support level for role permission
- B. Set the role stage to ALPHA while testing the role permissions.
- C. Use permissions in your role that use the 'supported' support level for role permission
- D. Set the role stage to BETA while testing the role permissions.
- E. Use permissions in your role that use the 'testing' support level for role permission
- F. Set the role stage to ALPHA while testing the role permissions.
- G. Use permissions in your role that use the 'testing' support level for role permission
- H. Set the role stage to BETA while testing the role permissions.

Answer: A

Explanation:

When setting support levels for permissions in custom roles, you can set to one of SUPPORTED, TESTING or NOT_SUPPORTED.

Ref: <https://cloud.google.com/iam/docs/custom-roles-permissions-support>

NEW QUESTION 272

Your organization uses G Suite for communication and collaboration. All users in your organization have a G Suite account. You want to grant some G Suite users access to your Cloud Platform project. What should you do?

- A. Enable Cloud Identity in the GCP Console for your domain.
- B. Grant them the required IAM roles using their G Suite email address.
- C. Create a CSV sheet with all users' email addresses
- D. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.
- E. In the G Suite console, add the users to a special group called cloud-console-users@yourdomain.com. Rely on the default behavior of the Cloud Platform to grant users access if they are members of this group.

Answer: B

NEW QUESTION 273

You have designed a solution on Google Cloud Platform (GCP) that uses multiple GCP products. Your company has asked you to estimate the costs of the solution. You need to provide estimates for the monthly total cost. What should you do?

- A. For each GCP product in the solution, review the pricing details on the products pricing page
- B. Use the pricing calculator to total the monthly costs for each GCP product.

- C. For each GCP product in the solution, review the pricing details on the products pricing pag
- D. Create a Google Sheet that summarizes the expected monthly costs for each product.
- E. Provision the solution on GC
- F. Leave the solution provisioned for 1 wee
- G. Navigate to the Billing Report page in the Google Cloud Platform Consol
- H. Multiply the 1 week cost to determine the monthly costs.
- I. Provision the solution on GC
- J. Leave the solution provisioned for 1 wee
- K. Use Stackdriver to determine the provisioned and used resource amount
- L. Multiply the 1 week cost to determine the monthly costs.

Answer: A

Explanation:

You can use the Google Cloud Pricing Calculator to total the estimated monthly costs for each GCP product. You dont incur any charges for doing so.
Ref: <https://cloud.google.com/products/calculator>

NEW QUESTION 277

You are using multiple configurations for gcloud. You want to review the configured Kubernetes Engine cluster of an inactive configuration using the fewest possible steps. What should you do?

- A. Use gcloud config configurations describe to review the output.
- B. Use gcloud config configurations activate and gcloud config list to review the output.
- C. Use kubectl config get-contexts to review the output.
- D. Use kubectl config use-context and kubectl config view to review the output.

Answer: D

NEW QUESTION 278

Your Dataproc cluster runs in a single Virtual Private Cloud (VPC) network in a single subnet with range 172.16.20.128/25. There are no private IP addresses available in the VPC network. You want to add new VMs to communicate with your cluster using the minimum number of steps. What should you do?

- A. Modify the existing subnet range to 172.16.20.0/24.
- B. Create a new Secondary IP Range in the VPC and configure the VMs to use that range.
- C. Create a new VPC network for the VM
- D. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.
- E. Create a new VPC network for the VMs with a subnet of 172.32.0.0/16. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC networ
- F. Configure a custom Route exchange.

Answer: A

Explanation:

/25:
CIDR to IP Range Result
CIDR Range 172.16.20.128/25 Netmask 255.255.255.128
Wildcard Bits 0.0.0.127
First IP 172.16.20.128
First IP (Decimal) 2886734976 Last IP 172.16.20.255
Last IP (Decimal) 2886735103 Total Host 128
CIDR 172.16.20.128/25
/24:
CIDR to IP Range Result
CIDR Range 172.16.20.128/24 Netmask 255.255.255.0
Wildcard Bits 0.0.0.255
First IP 172.16.20.0
First IP (Decimal) 2886734848 Last IP 172.16.20.255
Last IP (Decimal) 2886735103 Total Host 256
CIDR 172.16.20.128/24

NEW QUESTION 279

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Associate-Cloud-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Associate-Cloud-Engineer Product From:

<https://www.2passeasy.com/dumps/Associate-Cloud-Engineer/>

Money Back Guarantee

Associate-Cloud-Engineer Practice Exam Features:

- * Associate-Cloud-Engineer Questions and Answers Updated Frequently
- * Associate-Cloud-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * Associate-Cloud-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * Associate-Cloud-Engineer Practice Test Questions in Multiple Choice Formats and Updates for 1 Year