

Google

Exam Questions Associate-Cloud-Engineer

Google Cloud Certified - Associate Cloud Engineer



NEW QUESTION 1

Your company is moving its entire workload to Compute Engine. Some servers should be accessible through the Internet, and other servers should only be accessible over the internal network. All servers need to be able to talk to each other over specific ports and protocols. The current on-premises network relies on a demilitarized zone (DMZ) for the public servers and a Local Area Network (LAN) for the private servers. You need to design the networking infrastructure on Google Cloud to match these requirements. What should you do?

- A. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LA
- B. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.
- C. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LA
- D. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public egress traffic for the DMZ.
- E. 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LA
- F. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.
- G. 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LA
- H. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public egress traffic for the DMZ.

Answer: C

Explanation:

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

NEW QUESTION 2

Your company has multiple projects linked to a single billing account in Google Cloud. You need to visualize the costs with specific metrics that should be dynamically calculated based on company-specific criteria. You want to automate the process. What should you do?

- A. In the Google Cloud console, visualize the costs related to the projects in the Reports section.
- B. In the Google Cloud console, visualize the costs related to the projects in the Cost breakdown section.
- C. In the Google Cloud console, use the export functionality of the Cost tab
- D. Create a Looker Studio dashboard on top of the CSV export.
- E. Configure Cloud Billing data export to BigQuery for the billing account
- F. Create a Looker Studio dashboard on top of the BigQuery export.

Answer: D

NEW QUESTION 3

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 4

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 5

Your company's security vulnerability management policy wants 3 member of the security team to have visibility into vulnerabilities and other OS metadata for a specific Compute Engine instance. This Compute Engine instance hosts a critical application in your Google Cloud project. You need to implement your company's security vulnerability management policy. What should you do?

- A. • Ensure that the Ops Agent is installed on the Compute Engine instance. • Create a custom metric in the Cloud Monitoring dashboard. • Provide the security team member with access to this dashboard.
- B. • Ensure that the Ops Agent is installed on the Compute Engine instance. • Provide the security team member roles/configure.inventoryViewer permission.
- C. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Provide the security team member roles/configure.vulnerabilityViewer permission.
- D. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Create a log sink to a BigQuery dataset. • Provide the security team member with access to this dataset.

Answer: C

NEW QUESTION 6

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: A

NEW QUESTION 7

Your application is running on Google Cloud in a managed instance group (MIG). You see errors in Cloud Logging for one VM that one of the processes is not responsive. You want to replace this VM in the MIG quickly. What should you do?

- A. Select the MIG from the Compute Engine console and, in the menu, select Replace VMs.
- B. Use the `gcloud compute instance-groups managed recreate-instances` command to recreate the VM.
- C. Use the `gcloud compute instances update` command with a REFRESH action for the VM.
- D. Update and apply the instance template of the MIG.

Answer: A

NEW QUESTION 8

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: B

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 9

You are building a data lake on Google Cloud for your Internet of Things (IoT) application. The IoT application has millions of sensors that are constantly streaming structured and unstructured data to your backend in the cloud. You want to build a highly available and resilient architecture based on Google-recommended practices. What should you do?

- A. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage
- B. Stream data to Pub/Su
- C. and use Storage Transfer Service to send data to BigQuery.
- D. Stream data to Dataflow, and use Storage Transfer Service to send data to BigQuery.
- E. Stream data to Dataflow, and use Dataprep by Trifacta to send data to Bigtable.

Answer: B

NEW QUESTION 10

Your company is using Google Workspace to manage employee accounts. Anticipated growth will increase the number of personnel from 100 employees to 1.000 employees within 2 years. Most employees will need access to your company's Google Cloud account. The systems and processes will need to support 10x growth without performance degradation, unnecessary complexity, or security issues. What should you do?

- A. Migrate the users to Active Director
- B. Connect the Human Resources system to Active Director
- C. Turn on Google Cloud Directory Sync (GCDS) for Cloud Identit
- D. Turn on Identity Federation from Cloud Identity to Active Directory.
- E. Organize the users in Cloud Identity into group
- F. Enforce multi-factor authentication in Cloud Identity.
- G. Turn on identity federation between Cloud Identity and Google Workspac
- H. Enforce multi-factor authentication for domain wide delegation.
- I. Use a third-party identity provider service through federatio
- J. Synchronize the users from Google Workplace to the third-party provider in real time.

Answer: B

NEW QUESTION 10

You have created an application that is packaged into a Docker image. You want to deploy the Docker image as a workload on Google Kubernetes Engine. What should you do?

- A. Upload the image to Cloud Storage and create a Kubernetes Service referencing the image.
- B. Upload the image to Cloud Storage and create a Kubernetes Deployment referencing the image.
- C. Upload the image to Container Registry and create a Kubernetes Service referencing the image.
- D. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

Answer: D

Explanation:

A deployment is responsible for keeping a set of pods running. A service is responsible for enabling network access to a set of pods.

NEW QUESTION 13

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 18

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 22

You need to manage a Cloud Spanner Instance for best query performance. Your instance in production runs in a single Google Cloud region. You need to improve performance in the shortest amount of time. You want to follow Google best practices for service configuration. What should you do?

- A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 45% If you exceed this threshold, add nodes to your instance.
- B. Create an alert in Cloud Monitoring to alert when the percentage to high priority CPU utilization reaches 45% Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage
- C. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65% If you exceed this threshold, add nodes to your instance
- D. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. Use database query statistics to identity queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

Answer: B

Explanation:

<https://cloud.google.com/spanner/docs/cpu-utilization#recommended-max>

NEW QUESTION 26

You are running multiple VPC-native Google Kubernetes Engine clusters in the same subnet. The IPs available for the nodes are exhausted, and you want to ensure that the clusters can grow in nodes when needed. What should you do?

- A. Create a new subnet in the same region as the subnet being used.

- B. Add an alias IP range to the subnet used by the GKE clusters.
- C. Create a new VPC, and set up VPC peering with the existing VPC.
- D. Expand the CIDR range of the relevant subnet for the cluster.

Answer: D

Explanation:

gcloud compute networks subnets expand-ip-range NAME gcloud compute networks subnets expand-ip-range

- expand the IP range of a Compute Engine subnetwork <https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range>

NEW QUESTION 31

You need to run an important query in BigQuery but expect it to return a lot of records. You want to find out how much it will cost to run the query. You are using on-demand pricing. What should you do?

- A. Arrange to switch to Flat-Rate pricing for this query, then move back to on-demand.
- B. Use the command line to run a dry run query to estimate the number of bytes read.
- C. Then convert that bytes estimate to dollars using the Pricing Calculator.
- D. Use the command line to run a dry run query to estimate the number of bytes returned.
- E. Then convert that bytes estimate to dollars using the Pricing Calculator.
- F. Run a select count (*) to get an idea of how many records your query will look through.
- G. Then convert that number of rows to dollars using the Pricing Calculator.

Answer: B

NEW QUESTION 33

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 38

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 objec
- C. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.
- D. Store the database password inside a ConfigMap objec
- 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 42

Your team is running an on-premises ecommerce application. The application contains a complex set of microservices written in Python, and each microservice is running on Docker containers. Configurations are injected by using environment variables. You need to deploy your current application to a serverless Google Cloud cloud solution. What should you do?

- A. Use your existing CI/CD pipeline Use the generated Docker images and deploy them to Cloud Run.Update the configurations and the required endpoints.
- B. Use your existing continuous integration and delivery (CI/CD) pipelin
- C. Use the generated Docker images and deploy them to Cloud Functio
- D. Use the same configuration as on-premises.
- E. Use the existing codebase and deploy each service as a separate Cloud Function Update the configurations and the required endpoints.
- F. Use your existing codebase and deploy each service as a separate Cloud Run Use the same configurations as on-premises.

Answer: A

NEW QUESTION 45

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 snapsho
- F. Create your images from that image.
- G. Create a custom Compute Engine image from a snapsho
- 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 50

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 53

Your managed instance group raised an alert stating that new instance creation has failed to create new instances. You need to maintain the number of running instances specified by the template to be able to process expected application traffic. What should you do?

- A. Create an instance template that contains valid syntax which will be used by the instance grou
- B. Delete any persistent disks with the same name as instance names.
- C. Create an instance template that contains valid syntax that will be used by the instance grou
- D. Verify that the instance name and persistent disk name values are not the same in the template.
- E. Verify that the instance template being used by the instance group contains valid synta
- F. Delete any persistent disks with the same name as instance name
- G. Set the disks.autoDelete property to true in the instance template.
- H. Delete the current instance template and replace it with a new instance templat
- I. Verify that the instance name and persistent disk name values are not the same in the templat
- J. Set the disks.autoDelete property to true in the instance template.

Answer: A

Explanation:

<https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-migs> https://cloud.google.com/compute/docs/instance-templates#how_to_update_instance_templates

NEW QUESTION 55

You need to configure IAM access audit logging in BigQuery for external auditors. You want to follow Google-recommended practices. What should you do?

- A. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.
- B. Add the auditors group to two new custom IAM roles.
- C. Add the auditor user accounts to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.
- D. Add the auditor user accounts to two new custom IAM roles.

Answer: A

Explanation:

https://cloud.google.com/iam/docs/job-functions/auditing#scenario_external_auditors

Because if you directly add users to the IAM roles, then if any users left the organization then you have to remove the users from multiple places and need to revoke his/her access from multiple places. But, if you put a user into a group then its very easy to manage these type of situations. Now, if any user left then you just need to remove the user from the group and all the access got revoked

The organization creates a Google group for these external auditors and adds the current auditor to the group. This group is monitored and is typically granted access to the dashboard application. During normal access, the auditors' Google group is only granted access to view the historic logs stored in BigQuery. If any anomalies are discovered, the group is granted permission to view the actual Cloud Logging Admin Activity logs via the dashboard's elevated access mode. At the end of each audit period, the group's access is then revoked. Data is redacted using Cloud DLP before being made accessible for viewing via the dashboard application. The table below explains IAM logging roles that an Organization Administrator can grant to the service account used by the dashboard, as well as the resource level at which the role is granted.

NEW QUESTION 56

You need to enable traffic between multiple groups of Compute Engine instances that are currently running two different GCP projects. Each group of Compute Engine instances is running in its own VPC. What should you do?

- A. Verify that both projects are in a GCP Organizatio
- B. Create a new VPC and add all instances.
- C. Verify that both projects are in a GCP Organizatio
- D. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.
- E. Verify that you are the Project Administrator of both project
- F. Create two new VPCs and add all instances.
- G. Verify that you are the Project Administrator of both project
- H. Create a new VPC and add all instances.

Answer: B

Explanation:

Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network, so that they can communicate with each other securely and efficiently using internal IPs from that network. When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. The VPC networks in the host project are called Shared VPC networks. Eligible resources from service projects can use subnets in the Shared VPC network

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

"For example, an existing instance in a service project cannot be reconfigured to use a Shared VPC network, but a new instance can be created to use available subnets in a Shared VPC network."

NEW QUESTION 58

Your company developed an application to deploy on Google Kubernetes Engine. Certain parts of the application are not fault-tolerant and are allowed to have downtime Other parts of the application are critical and must always be available. You need to configure a Goorj e Kubernfl:es Engine duster while optimizing for cost. What should you do?

- A. Create a cluster with a single node-pool by using standard VM
- B. Label the fault-tolerant Deployments as spot-true.
- C. Create a cluster with a single node-pool by using Spot VM
- D. Label the critical Deployments as spot-false.
- E. Create a cluster with both a Spot W node pool and a rode pool by using standard VMs Deploy the critica
- F. deployments on the Spot VM node pool and the fault; tolerant deployments on the node pool by using standard VMs.
- G. Create a cluster with both a Spot VM node pool and by using standard VM
- H. Deploy the critical deployments on the mode pool by using standard VMs and the fault-tolerant deployments on the Spot VM node pool.

Answer: C

NEW QUESTION 59

You have a Google Cloud Platform account with access to both production and development projects. You need to create an automated process to list all compute instances in development and production projects on a daily basis. What should you do?

- A. Create two configurations using gcloud confi
- B. Write a script that sets configurations as active, individuall
- C. For each configuration, use gcloud compute instances list to get a list of compute resources.
- D. Create two configurations using gsutil confi
- E. Write a script that sets configurations as active, individuall
- F. For each configuration, use gsutil compute instances list to get a list of compute resources.
- G. Go to Cloud Shell and export this information to Cloud Storage on a daily basis.
- H. Go to GCP Console and export this information to Cloud SQL on a daily basis.

Answer: A

Explanation:

You can create two configurations – one for the development project and another for the production project. And you do that by running “gcloud config configurations create” command.<https://cloud.google.com/sdk/gcloud/reference/config/configurations/create>In your custom script, you can load these configurations one at a time and execute gcloud compute instances list to list Google Compute Engine instances in the project that is active in the gcloud configuration.Ref: <https://cloud.google.com/sdk/gcloud/reference/compute/instances/list>Once you have this information, you can export it in a suitable format to a suitable target e.g. export as CSV or export to Cloud Storage/BigQuery/SQL, etc

NEW QUESTION 62

You are configuring Cloud DNS. You want to create DNS records to point home.mydomain.com, mydomain.com. and www.mydomain.com to the IP address of your Google Cloud load balancer. What should you do?

- A. Create one CNAME record to point mydomain.com to the load balancer, and create two A records to point WWW and HOME to mydomain.com respectively.
- B. Create one CNAME record to point mydomain.com to the load balancer, and create two AAAA records to point WWW and HOME to mydomain.com respectively.
- C. Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.
- D. Create one A record to point mydomain.com to the load balancer, and create two NS records to point WWW and HOME to mydomain.com respectively.

Answer: C

NEW QUESTION 63

You want to run a single caching HTTP reverse proxy on GCP for a latency-sensitive website. This specific reverse proxy consumes almost no CPU. You want to have a 30-GB in-memory cache, and need an additional 2 GB of memory for the rest of the processes. You want to minimize cost. How should you run this reverse proxy?

- A. Create a Cloud Memorystore for Redis instance with 32-GB capacity.
- B. Run it on Compute Engine, and choose a custom instance type with 6 vCPUs and 32 GB of memory.
- C. Package it in a container image, and run it on Kubernetes Engine, using n1-standard-32 instances as nodes.
- D. Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB.

Answer: A

Explanation:

What is Google Cloud Memorystore?

Overview. Cloud Memorystore for Redis is a fully managed Redis service for Google Cloud Platform. Applications running on Google Cloud Platform can achieve extreme performance by leveraging the highly scalable, highly available, and secure Redis service without the burden of managing complex Redis deployments.

NEW QUESTION 67

You need to provide a cost estimate for a Kubernetes cluster using the GCP pricing calculator for Kubernetes. Your workload requires high IOPs, and you will also be using disk snapshots. You start by entering the number of nodes, average hours, and average days. What should you do next?

- A. Fill in local SS
- B. Fill in persistent disk storage and snapshot storage.
- C. Fill in local SS
- D. Add estimated cost for cluster management.
- E. Select Add GPU
- F. Fill in persistent disk storage and snapshot storage.
- G. Select Add GPU
- H. Add estimated cost for cluster management.

Answer: A

Explanation:

<https://cloud.google.com/compute/docs/disks/local-ssd>

NEW QUESTION 69

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 storage class
- D. Configure dual-regional storage for the dual region closest to the users Configure a Standard storage class

Answer: B

Explanation:

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

NEW QUESTION 74

You have an application running in Google Kubernetes Engine (GKE) with cluster autoscaling enabled. The application exposes a TCP endpoint. There are several replicas of this application. You have a Compute Engine instance in the same region, but in another Virtual Private Cloud (VPC), called gce-network, that has no overlapping IP ranges with the first VPC. This instance needs to connect to the application on GKE. You want to minimize effort. What should you do?

- A. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.2. Set the service's externalTrafficPolicy to Cluster.3. Configure the Compute Engine instance to use the address of the load balancer that has been created.
- B. 1. In GKE, create a Service of type NodePort that uses the application's Pods as backend.2. Create a Compute Engine instance called proxy with 2 network interfaces, one in each VPC.3. Use iptables on this instance to forward traffic from gce-network to the GKE nodes.4. Configure the Compute Engine instance to use the address of proxy in gce-network as endpoint.
- C. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.2. Add an annotation to this service: cloud.google.com/load-balancer-type: Internal3. Peer the two VPCs together.4. Configure the Compute Engine instance to use the address of the load balancer that has been created.
- D. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.2. Add a Cloud Armor Security Policy to the load balancer that whitelists the internal IPs of the MIG's instances.3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

Answer: A

Explanation:

performs a peering between the two VPC's (the statement makes sure that this option is feasible since it clearly specifies that there is no overlapping between the ip ranges of both vpc's), deploy the LoadBalancer as internal with the annotation, and configure the endpoint so that the compute engine instance can access the application internally, that is, without the need to have a public ip at any time and therefore, without the need to go outside the google network. The traffic, therefore, never crosses the public internet.

<https://medium.com/pablo-perez/k8s-externaltrafficpolicy-local-or-cluster-40b259a19404> <https://cloud.google.com/kubernetes-engine/docs/how-to/internal-load-balancing>

clients in a VPC network connected to the LoadBalancer network using VPC Network Peering can also access the Service
<https://cloud.google.com/kubernetes-engine/docs/how-to/service-parameters>

NEW QUESTION 78

You are building a new version of an application hosted in an App Engine environment. You want to test the new version with 1% of users before you completely switch your application over to the new version. What should you do?

- A. Deploy a new version of your application in Google Kubernetes Engine instead of App Engine and then use GCP Console to split traffic.
- B. Deploy a new version of your application in a Compute Engine instance instead of App Engine and then use GCP Console to split traffic.
- C. Deploy a new version as a separate app in App Engin
- D. Then configure App Engine using GCP Console to split traffic between the two apps.
- E. Deploy a new version of your application in App Engin
- F. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

Answer: D

Explanation:

GCP App Engine natively offers traffic splitting functionality between versions. You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitting traffic allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.

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

NEW QUESTION 80

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 84

Your company runs one batch process in an on-premises server that takes around 30 hours to complete. The task runs monthly, can be performed offline, and must be restarted if interrupted. You want to migrate this workload to the cloud while minimizing cost. What should you do?

- A. Migrate the workload to a Compute Engine Preemptible VM.
- B. Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes.
- C. Migrate the workload to a Compute Engine V
- D. Start and stop the instance as needed.
- E. Create an Instance Template with Preemptible VMs O
- F. Create a Managed Instance Group from the template and adjust Target CPU Utilizatio
- G. Migrate the workload.

Answer: D

Explanation:

Install the workload in a compute engine VM, start and stop the instance as needed, because as per the question the VM runs for 30 hours, process can be performed offline and should not be interrupted, if interrupted we need to restart the batch process again. Preemptible VMs are cheaper, but they will not be available beyond 24hrs, and if the process gets interrupted the preemptible VM will restart.

NEW QUESTION 89

You created a Kubernetes deployment by running `kubectl run nginx image=nginx replicas=1`. After a few days, you decided you no longer want this deployment. You identified the pod and deleted it by running `kubectl delete pod`. You noticed the pod got recreated.

```
> $ kubectl get pods
NAME READY STATUS RESTARTS AGE
nginx-84748895c4-nqqmt 1/1 Running 0 9m41s
> $ kubectl delete pod nginx-84748895c4-nqqmt
pod nginx-84748895c4-nqqmt deleted
> $ kubectl get pods
NAME READY STATUS RESTARTS AGE
nginx-84748895c4-k6bzl 1/1 Running 0 25s
```

What should you do to delete the deployment and avoid pod getting recreated?

- A. `kubectl delete deployment nginx`
- B. `kubectl delete --deployment=nginx`
- C. `kubectl delete pod nginx-84748895c4-k6bz1 --no-restart 2`
- D. `kubectl delete inginx`

Answer: A

Explanation:

This command correctly deletes the deployment. Pods are managed by kubernetes workloads (deployments). When a pod is deleted, the deployment detects the pod is unavailable and brings up another pod to maintain the replica count. The only way to delete the workload is by deleting the deployment itself using the `kubectl delete deployment` command.

- `$ kubectl delete deployment nginx`
- `deployment.apps/nginx deleted`

Ref: <https://kubernetes.io/docs/reference/kubectl/cheatsheet/#deleting-resources>

NEW QUESTION 92

You just installed the Google Cloud CLI on your new corporate laptop. You need to list the existing instances of your company on Google Cloud. What must you do before you run the `gcloud compute instances list` command?

Choose 2 answers

- A. Run `gcloud auth login`, enter your login credentials in the dialog window, and paste the received login token to `gcloud CLI`.
- B. Create a Google Cloud service account, and download the service account key
- C. Place the key file in a folder on your machine where `gcloud CLI` can find it.
- D. Download your Cloud Identity user account key
- E. Place the key file in a folder on your machine where `gcloud CLI` can find it.
- F. Run `gcloud config set compute/zone $my_zone` to set the default zone for `gcloud CLI`.
- G. Run `gcloud config set project $my_project` to set the default project for `gcloud CLI`.

Answer: AE

Explanation:

Before you run the `gcloud compute instances list` command, you need to do two things: authenticate with your user account and set the default project for `gcloud CLI`.

To authenticate with your user account, you need to run `gcloud auth login`, enter your login credentials in the dialog window, and paste the received login token to `gcloud CLI`. This will authorize the `gcloud CLI` to access Google Cloud resources on your behalf¹.

To set the default project for `gcloud CLI`, you need to run `gcloud config set project $my_project`, where

`$my_project` is the ID of the project that contains the instances you want to list. This will save you from having to specify the project flag for every `gcloud` command².

Option B is not recommended, because using a service account key increases the risk of credential leakage and misuse. It is also not necessary, because you can use your user account to authenticate to the `gcloud CLI`³. Option C is not correct, because there is no such thing as a Cloud Identity user account key. Cloud Identity is a service that provides identity and access management for Google Cloud users and groups⁴. Option D is not required, because the `gcloud compute instances list` command does not depend on the default zone. You can list instances from all zones or filter by a specific zone using the `--filter` flag.

References:

- 1: <https://cloud.google.com/sdk/docs/authorizing>
- 2: <https://cloud.google.com/sdk/gcloud/reference/config/set>
- 3: <https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys>
- 4: <https://cloud.google.com/identity/docs/overview>
- : <https://cloud.google.com/sdk/gcloud/reference/compute/instances/list>

NEW QUESTION 97

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 on
- C. Set the 'On-host maintenance' to Migrate VM instance
- D. Add the instance template to an instance group.
- E. Create an instance template for the instance
- F. Set 'Automatic Restart' to off
- 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 instance
- 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 so 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 99

You are working in a team that has developed a new application that needs to be deployed on Kubernetes. The production application is business critical and should be optimized for reliability. You need to provision a Kubernetes cluster and want to follow Google-recommended practices. What should you do?

- A. Create a GKE Autopilot cluste
- B. Enroll the cluster in the rapid release channel.
- C. Create a GKE Autopilot cluste
- D. Enroll the cluster in the stable release channel.
- E. Create a zonal GKE standard cluste
- F. Enroll the cluster in the stable release channel.
- G. Create a regional GKE standard cluste
- H. Enroll the cluster in the rapid release channel.

Answer: B

Explanation:

Autopilot is more reliable and stable release gives more time to fix issues in new version of GKE

NEW QUESTION 103

You are planning to migrate your on-premises data to Google Cloud. The data includes:

- 200 TB of video files in SAN storage
- Data warehouse data stored on Amazon Redshift
- 20 GB of PNG files stored on an S3 bucket

You need to load the video files into a Cloud Storage bucket, transfer the data warehouse data into BigQuery, and load the PNG files into a second Cloud Storage bucket. You want to follow Google-recommended practices and avoid writing any code for the migration. What should you do?

- A. Use gcloud storage for the video file
- B. Dataflow for the data warehouse data, and Storage Transfer Service for the PNG files.
- C. Use Transfer Appliance for the video
- D. BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.
- E. Use Storage Transfer Service for the video files, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.
- F. Use Cloud Data Fusion for the video files, Dataflow for the data warehouse data, and Storage Transfer Service for the PNG files.

Answer: C

NEW QUESTION 107

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 older microservices
- B. Create a node pool with compute-optimized machine type nodes for the image rendering microservice Use the node pool with general-purposemachine 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 imagerendering microservice deployment Keep the resource requests for the other microservices at the default

Answer: B

NEW QUESTION 109

You created an instance of SQL Server 2017 on Compute Engine to test features in the new version. You want to connect to this instance using the fewest number of steps. What should you do?

- A. Install a RDP client on your deskto
- B. Verify that a firewall rule for port 3389 exists.
- C. Install a RDP client in your deskto
- D. Set a Windows username and password in the GCP Consol
- E. Use the credentials to log in to the instance.
- F. Set a Windows password in the GCP Consol
- G. Verify that a firewall rule for port 22 exist
- H. Click the RDP button in the GCP Console and supply the credentials to log in.
- I. Set a Windows username and password in the GCP Consol
- J. Verify that a firewall rule for port 3389 exist
- K. Click the RDP button in the GCP Console, and supply the credentials to log in.

Answer: D

Explanation:

<https://cloud.google.com/compute/docs/instances/connecting-to-windows#remote-desktop-connection-app>

<https://cloud.google.com/compute/docs/instances/windows/generating-credentials> <https://cloud.google.com/compute/docs/instances/connecting-to-windows#before-you-begin>

NEW QUESTION 114

You want to configure a solution for archiving data in a Cloud Storage bucket. The solution must be cost-effective. Data with multiple versions should be archived after 30 days. Previous versions are accessed once a month for reporting. This archive data is also occasionally updated at month-end. What should you do?

- A. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Coldline Storage.
- B. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.
- C. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Coldline Storage.
- D. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Nearline Storage.

Answer: B

NEW QUESTION 115

Your company wants to migrate their on-premises workloads to Google Cloud. The current on-premises workloads consist of:

- A Flask web application
- A backend API
- A scheduled long-running background job for ETL and reporting.

You need to keep operational costs low. You want to follow Google-recommended practices to migrate these workloads to serverless solutions on Google Cloud. What should you do?

- A. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Compute Engine.
- B. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.
- C. Use Cloud Tasks to run your background job on Cloud Run.
- D. Run the web application on a Cloud Storage bucket and the backend API on Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.
- E. Run the web application on a Cloud Storage bucket and the backend API on Cloud Run.
- F. Use Cloud Tasks to run your background job on Compute Engine.

Answer: B

NEW QUESTION 116

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 121

Users of your application are complaining of slowness when loading the application. You realize the slowness is because the App Engine deployment serving the application is deployed in us-central whereas all users of this application are closest to europe-west3. You want to change the region of the App Engine application to europe-west3 to minimize latency. What's the best way to change the App Engine region?

- A. Create a new project and create an App Engine instance in europe-west3
- B. Use the gcloud app region set command and supply the name of the new region.
- C. From the console, under the App Engine page, click edit, and change the region drop-down.
- D. Contact Google Cloud Support and request the change.

Answer: A

Explanation:

App engine is a regional service, which means the infrastructure that runs your app(s) is located in a specific region and is managed by Google to be redundantly available across all the zones within that region. Once an app engine deployment is created in a region, it cant be changed. The only way is to create a new project and create an App Engine instance in europe-west3, send all user traffic to this instance and delete the app engine instance in us-central.

Ref: <https://cloud.google.com/appengine/docs/locations>

NEW QUESTION 123

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 128

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 129

The storage costs for your application logs have far exceeded the project budget. The logs are currently being retained indefinitely in the Cloud Storage bucket myapp-gcp-ace-logs. You have been asked to remove logs older than 90 days from your Cloud Storage bucket. You want to optimize ongoing Cloud Storage spend. What should you do?

- A. Write a script that runs `gsutil ls -l gs://myapp-gcp-ace-logs/**` to find and remove items older than 90 day
- B. Schedule the script with cron.
- C. Write a lifecycle management rule in JSON and push it to the bucket with `gsutil lifecycle set config-json-file`.
- D. Write a lifecycle management rule in XML and push it to the bucket with `gsutil lifecycle set config-xml-file`.
- E. Write a script that runs `gsutil ls -l gs://myapp-gcp-ace-logs/**` to find and remove items older than 90 day
- F. Repeat this process every morning.

Answer: B

Explanation:

You write a lifecycle management rule in XML and push it to the bucket with `gsutil lifecycle set config-xml-file`. is not right.

`gsutil lifecycle set` enables you to set the lifecycle configuration on one or more buckets based on the configuration file provided. However, XML is not a valid supported type for the configuration file.

Ref: <https://cloud.google.com/storage/docs/gsutil/commands/lifecycle>

➤ Write a script that runs `gsutil ls -l gs://myapp-gcp-ace-logs/**` to find and remove items older than 90 days. Repeat this process every morning. is not right. This manual approach is error-prone, time-consuming and expensive. GCP Cloud Storage provides lifecycle management rules that let you achieve this with minimal effort.

➤ Write a script that runs `gsutil ls -l gs://myapp-gcp-ace-logs/**` to find and remove items older than 90 days. Schedule the script with cron. is not right. This manual approach is error-prone, time-consuming and expensive. GCP Cloud Storage provides lifecycle management rules that let you achieve this with minimal effort.

➤ Write a lifecycle management rule in JSON and push it to the bucket with `gsutil lifecycle set config-json-file`. is the right answer.

You can assign a lifecycle management configuration to a bucket. The configuration contains a set of rules which apply to current and future objects in the bucket. When an object meets the criteria of one of the rules, Cloud Storage automatically performs a specified action on the object. One of the supported actions is to Delete objects. You can set up a lifecycle management to delete objects older than 90 days. `gsutil lifecycle set` enables you to set the lifecycle configuration on the bucket based on the configuration file. JSON is the only supported type for the configuration file. The config-json-file specified on the command line should be a path to a local file containing the lifecycle configuration JSON document.

Ref: <https://cloud.google.com/storage/docs/gsutil/commands/lifecycle> Ref: <https://cloud.google.com/storage/docs/lifecycle>

NEW QUESTION 131

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: A

Explanation:

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

NEW QUESTION 134

You need to track and verify modifications to a set of Google Compute Engine instances in your Google Cloud project. In particular, you want to verify OS system patching events on your virtual machines (VMs). What should you do?

- A. Review the Compute Engine activity logs Select and review the Admin Event logs
- B. Review the Compute Engine activity logs Select and review the System Event logs
- C. Install the Cloud Logging Agent In Cloud Logging review the Compute Engine syslog logs
- D. Install the Cloud Logging Agent In Cloud Logging, review the Compute Engine operation logs

Answer: A

NEW QUESTION 137

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 139

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

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

Answer: A

Explanation:

This answer is the simplest and most effective way to monitor unexpected firewall changes and instance creation in Google Cloud. Cloud Logging filters allow you to specify the criteria for the log entries that you want to view or export. You can use the Logging query language to write filters based on the LogEntry fields, such as `resource.type`, `severity`, or `protoPayload.methodName`. For example, you can filter for firewall-related events by using the following query:

```
resource.type="gce_subnetwork" logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall"
```

You can filter for instance-related events by using the following query: `resource.type="gce_instance"`

```
logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Factivity_log"
```

You can create log-based metrics from these filters to measure the rate or count of log entries that match the filter. Log-based metrics can be used to create charts and dashboards in Cloud Monitoring, or to set up alerts based on the metric values. For example, you can create an alert policy that triggers when the log-based metric for firewall changes exceeds a certain threshold in a given time interval. This way, you can get notified of any unexpected or malicious changes to your firewall rules.

Option B is incorrect because it is unnecessarily complex and costly. Installing Kibana on a compute instance requires additional configuration and maintenance. Creating a log sink to forward Cloud Audit Logs to Pub/Sub also incurs additional charges for the Pub/Sub service. Analyzing the logs on Kibana in real time may not be feasible or efficient, as it requires constant monitoring and manual intervention.

Option C is incorrect because Google Cloud firewall rules logging is a different feature from Cloud Audit Logs. Firewall rules logging allows you to audit, verify, and analyze the effects of your firewall rules by creating connection records for each rule that applies to traffic. However, firewall rules logging does not log the insert, update, or delete events for the firewall rules themselves. Those events are logged by Cloud Audit Logs, which record the administrative activities in your Google Cloud project.

Option D is incorrect because it is not a real-time solution. Creating a log sink to forward Cloud Audit Logs to Cloud Storage requires additional storage space and

charges. Using BigQuery to periodically analyze log events in the storage bucket also incurs additional costs for the BigQuery service. Moreover, this option does not provide any alerting mechanism to notify you of any unexpected or malicious changes to your firewall rules or instances.

NEW QUESTION 143

You are creating an application that will run on Google Kubernetes Engine. You have identified MongoDB as the most suitable database system for your application and want to deploy a managed MongoDB environment that provides a support SLA. What should you do?

- A. Create a Cloud Bigtable cluster and use the HBase API
- B. Deploy MongoDB Alias from the Google Cloud Marketplace
- C. Download a MongoDB installation package and run it on Compute Engine instances
- D. Download a MongoDB installation package, and run it on a Managed Instance Group

Answer: B

Explanation:

<https://console.cloud.google.com/marketplace/details/gc-launcher-for-mongodb-atlas/mongodb-atlas>

NEW QUESTION 145

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 150

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 154

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 155

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-scop>

NEW QUESTION 157

You are assisting a new Google Cloud user who just installed the Google Cloud SDK on their VM. The server needs access to Cloud Storage. The user wants your help to create a new storage bucket. You need to make this change in multiple environments. What should you do?

- A. Use a Deployment Manager script to automate creating storage buckets in an appropriate region
- B. Use a local SSD to improve performance of the VM for the targeted workload
- C. Use the gsutil command to create a storage bucket in the same region as the VM
- D. Use a Persistent Disk SSD in the same zone as the VM to improve performance of the VM

Answer: A

NEW QUESTION 158

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 162

You have a managed instance group comprised of preemptible VM's. All of the VM's keep deleting and recreating themselves every minute. What is a possible cause of this behavior?

- A. Your zonal capacity is limited, causing all preemptible VM's to be shutdown to recover capacity
- B. Try deploying your group to another zone.
- C. You have hit your instance quota for the region.
- D. Your managed instance group's VM's are toggled to only last 1 minute in preemptible settings.
- E. Your managed instance group's health check is repeatedly failing, either to a misconfigured health check or misconfigured firewall rules not allowing the health check to access the instance

Answer: D

Explanation:

as the instances (normal or preemptible) would be terminated and relaunched if the health check fails either due to application not configured properly or the instances firewall do not allow health check to happen.

GCP provides health check systems that connect to virtual machine (VM) instances on a configurable, periodic basis. Each connection attempt is called a probe. GCP records the success or failure of each probe.

Health checks and load balancers work together. Based on a configurable number of sequential successful or failed probes, GCP computes an overall health state for each VM in the load balancer. VMs that respond successfully for the configured number of times are considered healthy. VMs that fail to respond successfully for a separate number of times are unhealthy.

GCP uses the overall health state of each VM to determine its eligibility for receiving new requests. In addition to being able to configure probe frequency and health state thresholds, you can configure the criteria that define a successful probe.

NEW QUESTION 167

You need to set up a policy so that videos stored in a specific Cloud Storage Regional bucket are moved to Coldline after 90 days, and then deleted after one year from their creation. How should you set up the policy?

- A. Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete action
- B. Set the SetStorageClass action to 90 days and the Delete action to 275 days (365 – 90)
- C. Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete action
- D. Set the SetStorageClass action to 90 days and the Delete action to 365 days.
- E. Use gsutil rewrite and set the Delete action to 275 days (365-90).
- F. Use gsutil rewrite and set the Delete action to 365 days.

Answer: A

Explanation:

<https://cloud.google.com/storage/docs/lifecycle#setstorageclass-cost>

The object's time spent set at the original storage class counts towards any minimum storage duration that applies for the new storage class.

NEW QUESTION 170

You want to set up a Google Kubernetes Engine cluster. Verifiable node identity and integrity are required for the cluster, and nodes cannot be accessed from the internet. You want to reduce the operational cost of managing your cluster, and you want to follow Google-recommended practices. What should you do?

- A. Deploy a private autopilot cluster.
- B. Deploy a public autopilot cluster.
- C. Deploy a standard public cluster and enable shielded nodes.
- D. Deploy a standard private cluster and enable shielded nodes.

Answer: D

NEW QUESTION 172

You want to configure autohealing for network load balancing for a group of Compute Engine instances that run in multiple zones, using the fewest possible steps. You need to configure re-creation of VMs if they are unresponsive after 3 attempts of 10 seconds each. What should you do?

- A. Create an HTTP load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (HTTP).
- B. Create an HTTP load balancer with a backend configuration that references an existing instance group. Define a balancing mode and set the maximum RPS to 10.
- C. Create a managed instance group.
- D. Set the Autohealing health check to healthy (HTTP).
- E. Create a managed instance group.
- F. Verify that the autoscaling setting is on.

Answer: C

Explanation:

<https://cloud.google.com/compute/docs/instance-groups>

<https://cloud.google.com/load-balancing/docs/network/transition-to-backend-services#console>

➤ In order to enable auto-healing, you need to group the instances into a managed instance group.

Managed instance groups (MIGs) maintain the high availability of your applications by proactively keeping your virtual machine (VM) instances available. An auto-healing policy on the MIG relies on an application-based health check to verify that an application is responding as expected. If the auto-healer determines that an application isn't responding, the managed instance group automatically recreates that instance.

It is important to use separate health checks for load balancing and for auto-healing. Health checks for load balancing can and should be more aggressive because these health checks determine whether an instance receives user traffic. You want to catch non-responsive instances quickly, so you can redirect traffic if necessary. In contrast, health checking for auto-healing causes Compute Engine to proactively replace failing instances, so this health check should be more conservative than a load balancing health check.

NEW QUESTION 176

Your company set up a complex organizational structure on Google Cloud Platform. The structure includes hundreds of folders and projects. Only a few team members should be able to view the hierarchical structure. You need to assign minimum permissions to these team members and you want to follow Google-recommended practices. What should you do?

- A. Add the users to roles/browser role.
- B. Add the users to roles/iam.roleViewer role.
- C. Add the users to a group, and add this group to roles/browser role.
- D. Add the users to a group, and add this group to roles/iam.roleViewer role.

Answer: C

Explanation:

We need to apply the GCP Best practices. roles/browser Browser Read access to browse the hierarchy for a project, including the folder, organization, and IAM policy. This role doesn't include permission to view resources in the project. <https://cloud.google.com/iam/docs/understanding-roles>

NEW QUESTION 181

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 184

All development (dev) teams in your organization are located in the United States. Each dev team has its own Google Cloud project. You want to restrict access so that each dev team can only create cloud resources in the United States (US). What should you do?

- A. Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations.
- B. Create an organization to contain all the dev projects.
- C. Create an Identity and Access Management (IAM) policy to limit the resources in US regions.
- D. Create an Identity and Access Management (IAM) policy to restrict the resources locations in the U
- E. Apply the policy to all dev projects.

- F. Create an Identity and Access Management (IAM) policy to restrict the resources locations in all dev project
- G. Apply the policy to all dev roles.

Answer: C

NEW QUESTION 187

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The Associate-Cloud-Engineer Practice Test Here](#)