100. 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.

Was mit VerticalPodAutscaler und HorizontalPodAutoscaler

116. 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 ג€project ownerג€ for web-applications appropriate roles to crm-databases-proj.

B. Give ג€project ownerג€ role to crm-databases-proj and the web-applications project.

C. Give ג€project ownerג€ 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.

119. 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.

120. You need to manage multiple Google Cloud 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 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 Google Cloud 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 Google Cloud 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.

126. You have designed a solution on Google Cloud that uses multiple Google Cloud 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 Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

B. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Create a Google Sheet that summarizes the expected monthly costs for each product.

C. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Navigate to the Billing Report page in the Cloud Console. Multiply the 1 week cost to determine the monthly costs.

D. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Use Cloud Monitoring to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs.

133. 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 projects. Grant the VM Service Account the role Storage Object Creator on corp-iot-insights.

D. Make corp-aggregate-reports-storage public and create a folder with a pseudo-randomized suffix name. Share the folder with the IoT team.

134. 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.

135? 137?

138. You have downloaded and installed the gcloud command line interface (CLI) and have authenticated with your Google Account. Most of your Compute Engine instances in your project run in the europe-west1-d zone. You want to avoid having to specify this zone with each CLI command when managing these instances. What should you do?

A. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

B. In the Settings page for Compute Engine under Default location, set the zone to europeג€"west1-d.

C. In the CLI installation directory, create a file called default.conf containing zone=europeג€"west1ג€"d.

D. Create a Metadata entry on the Compute Engine page with key compute/zone and value europeג€"west1ג€"d.

139. The core business of your company is to rent out construction equipment at large scale. All the equipment that is being rented out has been equipped with multiple sensors that send event information every few seconds. These signals can vary from engine status, distance traveled, fuel level, and more. Customers are billed based on the consumption monitored by these sensors. You expect high throughput `" up to thousands of events per hour per device `" and need to retrieve consistent data based on the time of the event. Storing and retrieving individual signals should be atomic. What should you do?

A. Create a file in Cloud Storage per device and append new data to that file.

B. Create a file in Cloud Filestore per device and append new data to that file.

C. Ingest the data into Datastore. Store data in an entity group based on the device.

D. Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

144. You have a Compute Engine instance hosting an application used between 9 AM and 6 PM on weekdays. You want to back up this instance daily for disaster recovery purposes. You want to keep the backups for 30 days. You want the Google-recommended solution with the least management overhead and the least number of services. What should you do?

A. 1. Update your instances' metadata to add the following value: snapshotג€"schedule: 0 1 * * * 2. Update your instances' metadata to add the following value: snapshotג€"retention: 30

B. 1. In the Cloud Console, go to the Compute Engine Disks page and select your instance's disk. 2. In the Snapshot Schedule section, select Create Schedule and configure the following parameters: - Schedule frequency: Daily - Start time: 1:00 AM ג€" 2:00 AM - Autodelete snapshots after: 30 days

C. 1. Create a Cloud Function that creates a snapshot of your instance's disk. 2. Create a Cloud Function that deletes snapshots that are older than 30 days. 3. Use Cloud Scheduler to trigger both Cloud Functions daily at 1:00 AM.

D. 1. Create a bash script in the instance that copies the content of the disk to Cloud Storage. 2. Create a bash script in the instance that deletes data older than 30 days in the backup Cloud Storage bucket. 3. Configure the instance's crontab to execute these scripts daily at 1:00 AM.

148. A colleague handed over a Google Cloud Platform project for you to maintain. As part of a security checkup, you want to review who has been granted the Project Owner role. What should you do?

A. In the console, validate which SSH keys have been stored as project-wide keys.

B. Navigate to Identity-Aware Proxy and check the permissions for these resources.

C. Enable Audit Logs on the IAM & admin page for all resources, and validate the results.

D. Use the command gcloud projects get-iam-policy to view the current role assignments.

149. 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.

155. 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.

162. Your company has embraced a hybrid cloud strategy where some of the applications are deployed on Google Cloud. A Virtual Private Network (VPN) tunnel connects your Virtual Private Cloud (VPC) in Google Cloud with your company's on-premises network. Multiple applications in Google Cloud need to connect to an on-premises database server, and you want to avoid having to change the IP configuration in all of your applications when the IP of the database changes. What should you do?

A. Configure Cloud NAT for all subnets of your VPC to be used when egressing from the VM instances.

B. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

C. Configure the IP of the database as custom metadata for each instance, and query the metadata server.

D. Query the Compute Engine internal DNS from the applications to retrieve the IP of the database.

166. Your web application has been running successfully on Cloud Run for Anthos. You want to evaluate an updated version of the application with a specific percentage of your production users (canary deployment). What should you do?

A. Create a new service with the new version of the application. Split traffic between this version and the version that is currently running.

B. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

C. Create a new service with the new version of the application. Add an HTTP Load Balancer in front of both services.

D. Create a new revision with the new version of the application. Add an HTTP Load Balancer in front of both revisions.

Datenbanken für Use Case wählen können

LoadBalancers

IAM roles

Gcloud commands

205. 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.

206. You have two subnets (subnet-a and subnet-b) in the default VPC. Your database servers are running in subnet-a. Your application servers and web servers are running in subnet-b. You want to configure a firewall rule that only allows database traffic from the application servers to the database servers. What should you do?

A. 1. Create service accounts sa-app and sa-db. 2. Associate service account sa-app with the application servers and the service account sa-db with the database servers. 3. Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

B. 1. Create network tags app-server and db-server. 2. Add the app-server tag to the application servers and the db-server tag to the database servers. 3. Create an egress firewall rule to allow network traffic from source network tag app-server to target network tag db-server.

C. 1. Create a service account sa-app and a network tag db-server. 2. Associate the service account sa-app with the application servers and the network tag db-server with the database servers. 3. Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-a IP addresses.

D. 1. Create a network tag app-server and service account sa-db. 2. Add the tag to the application servers and associate the service account with the database servers. 3. Create an egress firewall rule to allow network traffic from source network tag app-server to target service account sa-db.

207. Your team wants to deploy a specific content management system (CMS) solution to Google Cloud. You need a quick and easy way to deploy and install the solution. What should you do?

A. Search for the CMS solution in Google Cloud Marketplace. Use gcloud CLI to deploy the solution.

B. Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace.

C. Search for the CMS solution in Google Cloud Marketplace. Use Terraform and the Cloud Marketplace ID to deploy the solution with the appropriate parameters.

D. Use the installation guide of the CMS provider. Perform the installation through your configuration management system.

208. You are working for a startup that was officially registered as a business 6 months ago. As your customer base grows, your use of Google Cloud increases. You want to allow all engineers to create new projects without asking them for their credit card information. What should you do?

A. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

B. Grant all engineers permission to create their own billing accounts for each new project.

C. Apply for monthly invoiced billing, and have a single invoice for the project paid by the finance team.

D. Create a billing account, associate it with a monthly purchase order (PO), and send the PO to Google Cloud.

209. Your continuous integration and delivery (CI/CD) server can’t execute Google Cloud actions in a specific project because of permission issues. You need to validate whether the used service account has the appropriate roles in the specific project. What should you do?

A. Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

B. Open the Google Cloud console, and check the organization policies.

C. Open the Google Cloud console, and run a query to determine which resources this service account can access.

D. Open the Google Cloud console, and run a query of the audit logs to find permission denied errors for this service account.

212. You are running a web application on Cloud Run for a few hundred users. Some of your users complain that the initial web page of the application takes much longer to load than the following pages. You want to follow Google's recommendations to mitigate the issue. What should you do?

A. Set the minimum number of instances for your Cloud Run service to 3.

B. Set the concurrency number to 1 for your Cloud Run service.

C. Set the maximum number of instances for your Cloud Run service to 100.

D. Update your web application to use the protocol HTTP/2 instead of HTTP/1.1.

213. 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/Sub, and use Storage Transfer Service to send data to BigQuery.

C. Stream data to Dataflow, and use Dataprep by Trifacta to send data to Bigtable.

D. Stream data to Dataflow, and use Storage Transfer Service to send data to BigQuery.

215. Your company requires all developers to have the same permissions, regardless of the Google Cloud project they are working on. Your company's security policy also restricts developer permissions to Compute Engine, Cloud Functions, and Cloud SQL. You want to implement the security policy with minimal effort. What should you do?

A. 1. Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions in one project within the Google Cloud organization. 2. Copy the role across all projects created within the organization with the gcloud iam roles copy command. 3. Assign the role to developers in those projects.

B. 1. Add all developers to a Google group in Google Groups for Workspace. 2. Assign the predefined role of Compute Admin to the Google group at the Google Cloud organization level.

C. 1. Add all developers to a Google group in Cloud Identity. 2. Assign predefined roles for Compute Engine, Cloud Functions, and Cloud SQL permissions to the Google group for each project in the Google Cloud organization.

D. 1. Add all developers to a Google group in Cloud Identity. 2. Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level. 3. Assign the custom role to the Google group.

220. During a recent audit of your existing Google Cloud resources, you discovered several users with email addresses outside of your Google Workspace domain. You want to ensure that your resources are only shared with users whose email addresses match your domain. You need to remove any mismatched users, and you want to avoid having to audit your resources to identify mismatched users. What should you do?

A. Create a Cloud Scheduler task to regularly scan your projects and delete mismatched users.

B. Create a Cloud Scheduler task to regularly scan your resources and delete mismatched users.

C. Set an organizational policy constraint to limit identities by domain to automatically remove mismatched users.

D. Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users

222. You want to permanently delete a Pub/Sub topic managed by Config Connector in your Google Cloud project. What should you do?

A. Use kubectl to create the label deleted-by-cnrm and to change its value to true for the topic resource.

B. Use kubectl to delete the topic resource.

C. Use gcloud CLI to delete the topic.

D. Use gcloud CLI to update the topic label managed-by-cnrm to false.

224. You want to host your video encoding software on Compute Engine. Your user base is growing rapidly, and users need to be able to encode their videos at any time without interruption or CPU limitations. You must ensure that your encoding solution is highly available, and you want to follow Google-recommended practices to automate operations. What should you do?

A. Deploy your solution on multiple standalone Compute Engine instances, and increase the number of existing instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

B. Deploy your solution on multiple standalone Compute Engine instances, and replace existing instances with high-CPU instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

C. Deploy your solution to an instance group, and increase the number of available instances whenever you see high CPU utilization in Cloud Monitoring.

D. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

226. 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 Artifact Registry and create a Kubernetes Service referencing the image.

D. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image.

229. You created several resources in multiple Google Cloud projects. All projects are linked to different billing accounts. To better estimate future charges, you want to have a single visual representation of all costs incurred. You want to include new cost data as soon as possible. What should you do?

A. Fill all resources in the Pricing Calculator to get an estimate of the monthly cost.

B. Use the Reports view in the Cloud Billing Console to view the desired cost information.

C. Visit the Cost Table page to get a CSV export and visualize it using Looker Studio.

D. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

232. You recently received a new Google Cloud project with an attached billing account where you will work. You need to create instances, set firewalls, and store data in Cloud Storage. You want to follow Google-recommended practices. What should you do?

A. Use the gcloud CLI services enable cloudresourcemanager.googleapis.com command to enable all resources.

B. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

C. Open the Google Cloud console and enable all Google Cloud APIs from the API dashboard.

D. Open the Google Cloud console and run gcloud init --project in a Cloud Shell.

233. Your application development team has created Docker images for an application that will be deployed on Google Cloud. Your team does not want to manage the infrastructure associated with this application. You need to ensure that the application can scale automatically as it gains popularity. What should you do?

A. Create an instance template with the container image, and deploy a Managed Instance Group with Autoscaling.

B. Upload Docker images to Artifact Registry, and deploy the application on Google Kubernetes Engine using Standard mode.

C. Upload Docker images to the Cloud Storage, and deploy the application on Google Kubernetes Engine using Standard mode.

D. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

234. You are migrating a business critical application from your local data center into Google Cloud. As part of your high-availability strategy, you want to ensure that any data used by the application will be immediately available if a zonal failure occurs. What should you do?

A. Store the application data on a zonal persistent disk. Create a snapshot schedule for the disk. If an outage occurs, create a new disk from the most recent snapshot and attach it to a new VM in another zone.

B. Store the application data on a zonal persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

C. Store the application data on a regional persistent disk. Create a snapshot schedule for the disk. If an outage occurs, create a new disk from the most recent snapshot and attach it to a new VM in another zone.

D. Store the application data on a regional persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

235. The DevOps group in your organization needs full control of Compute Engine resources in your development project. However, they should not have permission to create or update any other resources in the project. You want to follow Google's recommendations for setting permissions for the DevOps group. What should you do?

A. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

B. Create an IAM policy and grant all compute.instanceAdmin.* permissions to the policy. Attach the policy to the DevOps group.

C. Create a custom role at the folder level and grant all compute.instanceAdmin.* permissions to the role. Grant the custom role to the DevOps group.

D. Grant the basic role roles/editor to the DevOps group.

236. 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) pipeline. Use the generated Docker images and deploy them to Cloud Function. Use the same configuration as on-premises.

C. Use the existing codebase and deploy each service as a separate Cloud Function. Update the configurations and the required endpoints.

D. Use your existing codebase and deploy each service as a separate Cloud Run. Use the same configurations as on-premises.

238. 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 cluster. Enroll the cluster in the rapid release channel.

B. Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

C. Create a zonal GKE standard cluster. Enroll the cluster in the stable release channel.

D. Create a regional GKE standard cluster. Enroll the cluster in the rapid release channel.

239. You are responsible for a web application on Compute Engine. You want your support team to be notified automatically if users experience high latency for at least 5 minutes. You need a Google-recommended solution with no development cost. What should you do?

A. Export Cloud Monitoring metrics to BigQuery and use a Looker Studio dashboard to monitor your web application's latency.

B. Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold.

C. Implement an App Engine service which invokes the Cloud Monitoring API and sends a notification in case of anomalies.

D. Use the Cloud Monitoring dashboard to observe latency and take the necessary actions when the response latency exceeds the specified threshold.

241. You used the gcloud container clusters command to create two Google Cloud Kubernetes (GKE) clusters: prod-cluster and dev-cluster.

- prod-cluster is a standard cluster.
- dev-cluster is an auto-pilot cluster.

When you run the kubectl get nodes command, you only see the nodes from prod-cluster. Which commands should you run to check the node status for dev-cluster?

A. gcloud container clusters get-credentials dev-cluster
kubectl get nodes

B. gcloud container clusters update -generate-password dev-cluster kubectl get nodes

C. kubectl config set-context dev-cluster
kubectl cluster-info

D. kubectl config set-credentials dev-cluster
kubectl cluster-info