Question 1: Correct

You want to monitor resource utilization (RAM, Disk, Network, CPU etc.) for all applications in development, test and production GCP projects in a single dashboard. What should you do?

​

Enable Stackdriver Monitoring API, create a workspace under production project, and then add development and test projects.

(Correct)

​

Enable Stackdriver Monitoring API and then use default dashboards to view all projects in sequence.

​

Enable Stackdriver Monitoring API and then share charts from development, test and production GCP projects.

​

Enable Stackdriver Monitoring API and then give the metrics.reader role to development, test and production GCP projects.

Explanation

Enable Stackdriver Monitoring API and then share charts from development, test and production GCP projects. is not right.

This involves a lot of work. You can share charts from project A, B, and C by enabling Cloud Monitoring as a data source for Grafana

Ref: https://cloud.google.com/monitoring/charts/sharing-charts

and then follow the instructions at https://grafana.com/docs/grafana/latest/features/datasources/cloudmonitoring/

to build grafana dashboards.

Enable Stackdriver Monitoring API and then give the metrics.reader role to development, test and production GCP projects. is not right.

There isn't any metrics.reader role.

Rer: https://cloud.google.com/monitoring/access-control

Enable Stackdriver Monitoring API and then use default dashboards to view all projects in sequence. is not right.

Possibly, but this doesn't satisfy the requirement "single pane of glass".

Enable Stackdriver Monitoring API, create a workspace under production project, and then add development and test projects. is the right answer.

A Workspace is a tool for monitoring resources contained in one or more Google Cloud projects or AWS accounts. A Workspace accesses metric data from its monitored projects, but the metric data remains in those projects. You can configure Project A to be the host project and Projects B and C as the monitored projects. You can now build dashboards in the stackdriver workspace and view monitoring information for all projects in a "single pane of glass".

Ref: https://cloud.google.com/monitoring/workspaces

Bottom of Form

Top of Form

Question 2: Incorrect

You run a batch job monthly in your on-premises data centre that downloads clickstream logs from Google Cloud Storage bucket, enriches the data and stores them in Cloud BigTable. The job runs for 32 hours on average, can be restarted if interrupted, and must complete. You want to migrate this batch job onto a cost-efficient GCP compute service. What should you do?

​

Create an Instance Template with Preemptible VMs. Create a Managed Instance Group from the template and adjust Target CPU Utilization. Migrate the workload.

​

Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes.

(Correct)

​

Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

​

Migrate the workload to a Compute Engine Preemptible VM.

(Incorrect)

Explanation

Migrate the workload to a Compute Engine Preemptible VM. is not right.

A preemptible VM is an instance that 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 are excess Compute Engine capacity, so their availability varies with usage. Since our batch process must be restarted if interrupted, a preemptible VM by itself is not sufficient.

https://cloud.google.com/compute/docs/instances/preemptible#what\_is\_a\_preemptible\_instance

Migrate the workload to a Compute Engine VM. Start and stop the instance as needed. is not right.

Stopping and starting instances as needed is a manual activity and incurs operational expenditure. Since our requirement is to minimize cost, we shouldn't do this.

Create an Instance Template with Preemptible VMs. Create a Managed Instance Group from the template and adjust Target CPU Utilization. Migrate the workload. is not right.

Our requirement is not to scale up or scale down based on target CPU utilization.

Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes. is the right answer.

Preemptible VMs are Compute Engine VM instances that last a maximum of 24 hours and provide no availability guarantees. Preemptible VMs are priced lower than standard Compute Engine VMs and offer the same machine types and options. You can use preemptible VMs in your GKE clusters or node pools to run batch or fault-tolerant jobs that are less sensitive to the ephemeral, non-guaranteed nature of preemptible VMs.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/preemptible-vms

Ref: https://cloud.google.com/blog/products/containers-kubernetes/cutting-costs-with-google-kubernetes-engine-using-the-cluster-autoscaler-and-preemptible-vms

Bottom of Form

Top of Form

Question 3: Incorrect

You plan to deploy an application to Google Compute Engine instance, and it relies on making connections to a Cloud SQL database for retrieving book publications. To minimize costs, you are developing this application on your local workstation, and you want it to connect to a Cloud SQL instance. Your colleague suggested setting up Application Default Credentials on your workstation to make the transition to Google Cloud easier. You are now ready to move the application to Google Compute Engine instance. You want to follow Google recommended practices to enable secure IAM access. What should you do?

​

Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application.

​

Assign appropriate access for Google services to the service account used by the Compute Engine VM.

(Correct)

​

Store credentials for your user account with appropriate access for Google services in a config file, and deploy this config file with your application.

​

Create a service account with appropriate access for Google services, and configure the application to use this account.

(Incorrect)

Explanation

Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application. is not right.

To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. Since our application is running inside Google Cloud, Google's recommendation is to assign the required permissions to the service account and not use the service account keys.

Ref: https://cloud.google.com/iam/docs/creating-managing-service-account-keys

Store credentials for your user account with appropriate access for Google services in a config file, and deploy this config file with your application. is not right.

For application to application interaction, Google recommends use of service accounts. A service account is an account for an application instead of an individual end user. When you run code that's hosted on Google Cloud, the code runs as the account you specify. You can create as many service accounts as needed to represent the different logical components of your application.

Ref: https://cloud.google.com/iam/docs/overview#service\_account

Create a service account with appropriate access for Google services, and configure the application to use this account. is not right.

Using Application Default Credentials ensures that the service account works seamlessly; when testing on your local machine, it uses a locally-stored service account key, but when running on Compute Engine, it uses the project's default Compute Engine service account. So we have to provide access to the service account used by the compute engine VM and not the service account used by the application..

Ref: https://cloud.google.com/iam/docs/service-accounts#application\_default\_credentials

Assign appropriate access for Google services to the service account used by the Compute Engine VM. is the right answer.

Using Application Default Credentials ensures that the service account works seamlessly; when testing on your local machine, it uses a locally-stored service account key, but when running on Compute Engine, it uses the project's default Compute Engine service account. So we have to provide access to the service account used by the compute engine VM.

Ref: https://cloud.google.com/iam/docs/service-accounts#application\_default\_credentials

Bottom of Form

Top of Form

Question 4: Correct

You work for a multinational delivery services company that uses Apache Cassandra DB as the backend store for its delivery track and trace system. The existing on-premises data centre is out of space. To cope with an anticipated increase in requests in the run-up to Christmas, you want to move this application rapidly to Google Cloud whilst ensuring you can spin up multiple stacks (development, test, production) and isolate them from each other. How can you do this?

​

1. Build a Cassandra Compute Engine instance and take a snapshot of it.

2. Use the snapshot to create instances for your developers.

​

1. Advise your developers to go to Cloud Marketplace.

2. Ask the developers to launch a Cassandra image for their development work.

(Correct)

​

1. Build an instruction guide to install Cassandra on GCP.

2. Make the instruction guide accessible to your developers.

​

1. Build a Cassandra Compute Engine instance and take a snapshot of it.

2. Upload the snapshot to Cloud Storage and make it accessible to your developers.

3. Build instructions to create a Compute Engine instance from the snapshot so that developers can do it themselves.

Explanation

1. Build an instruction guide to install Cassandra on GCP.

2. Make the instruction guide accessible to your developers. is not right.

There is a very simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to come up with an installation guide and ask your developers to do it.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

1. Build a Cassandra Compute Engine instance and take a snapshot of it.

2. Use the snapshot to create instances for your developers. is not right.

Like above, there is a very simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to do this in a convoluted way.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

1. Build a Cassandra Compute Engine instance and take a snapshot of it.

2. Upload the snapshot to Cloud Storage and make it accessible to your developers.

3. Build instructions to create a Compute Engine instance from the snapshot so that developers can do it themselves. is not right.

Like above, there is a very simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to do this in a convoluted way.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

1. Advise your developers to go to Cloud Marketplace.

2. Ask the developers to launch a Cassandra image for their development work. is the right answer.

You can deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. Not only do you get a unified bill for all GCP services, your Developers can now create Cassandra clusters on Google Cloud in minutes and build applications with Cassandra as a database as a service without the operational overhead of managing Cassandra. Each instance is deployed to a separate set of VM instances (at the time of writing this, 3 x VM instance: 4 vCPUs + 26 GB memory (n1-highmem-4) + 10-GB Boot Disk) which are all isolated from the VM instances for other Cassandra deployments.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

Bottom of Form

Top of Form

Question 5: Correct

You are migrating a Python code snippet (API) from the on-premises data centre to Google Cloud Platform. The Python API is triggered when a new file is created or updated in a NAS share. Your manager suggested replacing NAS share with Cloud Storage. What GCP compute service should you use for the API?

​

Use Dataflow as a batch job, and configure the bucket as a data source.

​

Use Cloud Functions and configure the bucket as a trigger resource.

(Correct)

​

Use Google Kubernetes Engine and configure a CronJob to trigger the application using Pub/Sub.

​

Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub.

Explanation

Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub. is not right.

Cloud Scheduler lets you run your batch and big data jobs on a recurring schedule. Since it doesn't work real time, you can't execute a code snippet whenever a new file is uploaded to a Cloud Storage bucket.

https://cloud.google.com/scheduler

Use Google Kubernetes Engine and configure a CronJob to trigger the application using Pub/Sub. is not right.

You can use CronJobs to run tasks at a specific time or interval. Since it doesn't work real time, you can't execute a code snippet whenever a new file is uploaded to a Cloud Storage bucket.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/cronjobs

Use Dataflow as a batch job, and configure the bucket as a data source. is not right.

Dataflow is Unified stream and batch data processing that's serverless, fast, and cost-effective. Batch processing is not real time, so you can't execute a code snippet whenever a new file is uploaded to a Cloud Storage bucket.

Ref: https://cloud.google.com/dataflow

Use Cloud Functions and configure the bucket as a trigger resource. is the right answer.

Cloud Functions can respond to change notifications emerging from Google Cloud Storage. These notifications can be configured to trigger in response to various events inside a bucket—object creation, deletion, archiving and metadata updates.

Ref: https://cloud.google.com/functions/docs/calling/storage

Bottom of Form

Top of Form

Question 6: Correct

Your production applications are distributed across several Google Cloud Platform (GCP) projects, and your operations team want to efficiently manage all the production projects and applications using gcloud SDK on Cloud Shell. What should you recommend they do to achieve this in the fewest possible steps?

​

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.

​

1. Create a configuration for each project you need to manage.

2. Activate the appropriate configuration when you work with each of your assigned GCP projects.

(Correct)

​

1. Use the default configuration for one project you need to manage.

2. Activate the appropriate configuration when you work with each of your assigned GCP projects.

​

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

Explanation

1. Create a configuration for each project you need to manage.

2. Activate the appropriate configuration when you work with each of your assigned GCP projects. is the right answer.

gcloud configurations enable you to manage multiple projects in gcloud cli using the fewest possible steps,

Ref: https://cloud.google.com/sdk/gcloud/reference/config

For example, we have two projects

$ gcloud projects list

PROJECT\_ID NAME PROJECT\_NUMBER

project-1-278333 project-1-278333 85524215451

project-2-278333 project-2-278333 25349885274

We create configuration for each project. For project-2-278333,

$ gcloud config configurations create project-1-config

$ gcloud config set project project-1-278333

And for project-2-278333,

$ gcloud config configurations create project-2-config

$ gcloud config set project project-2-278333

We now have two configurations, one for each project.

$ gcloud config configurations list

NAME IS\_ACTIVE ACCOUNT PROJECT COMPUTE\_DEFAULT\_ZONE COMPUTE\_DEFAULT\_REGION

cloudshell-4453 False

project-1-config False project-1-278333

project-2-config True project-2-278333

To activate configuration for project-1,

$ gcloud config configurations activate project-1-config

Activated [project-1-config].

$ gcloud config get-value project

Your active configuration is: [project-1-config]

project-1-278333

To activate configuration for project-2,

$ gcloud config configurations activate project-2-config

Activated [project-2-config].

$ gcloud config get-value project

Your active configuration is: [project-2-config]

project-2-278333

Bottom of Form

Top of Form

Question 7: Incorrect

Your company runs most of its compute workloads in Google Compute Engine in the europe-west1-b zone. Your operations team use Cloud Shell and Bastion Hosts with Cloud SDK installed to manage these instances. They want to know if it is possible to designate a default compute zone and not supply the zone parameter when running each command in the CLI. What should you do?

​

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

(Incorrect)

​

In the CLI installation directory, create a file called default.conf containing zone=europe-west1-b.

​

Create a Metadata entry on the Compute Engine page with key compute/zone and value europe-west1-b.

​

In the Settings page for Compute Engine under Default location, set the zone to europe-west1-b.

(Correct)

Explanation

In the CLI installation directory, create a file called default.conf containing zone=europe-west1-b. is not right.

gcloud does not read configurations from default.conf

Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations

Ref: https://cloud.google.com/sdk/docs/configurations

Set the europe-west1-b zone as the default zone using the gcloud config subcommand. is not right.

Using gcloud config set, you can set the zone in your active configuration only. This does not apply to other gcloud configurations and does not become the default for the project.

Ref: https://cloud.google.com/sdk/gcloud/reference/config/set

gcloud config set compute/zone europe-west1-b

Create a Metadata entry on the Compute Engine page with key compute/zone and value europe-west1-b. is not right.

You could achieve this behaviour by running the following in gcloud.

https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region#gcloud

gcloud compute project-info add-metadata \

--metadata google-compute-default-region=europe-west1,google-compute-default-zone=europe-west1-b

As shown above, the key to be used is google-compute-default-zone and not compute/zone.

In the Settings page for Compute Engine under Default location, set the zone to europe-west1-b. is the right answer.

Ref: https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region#gcloud

The default region and zone settings affect only client tools, such as the gcloud command-line tool and the Google Cloud Console. When you use these tools to construct your requests, the tools help you manage resources by automatically selecting the default region and zone. When you use the Cloud Console to create regional or zonal resources like addresses and instances, Compute Engine sets the region and zone fields for you. You can accept the pre-populated values, or explicitly change one or both of the values. When you use the gcloud tool, omit setting the --region and --zone flags to use the default region and zone properties for the new project. You can always change the default region and zone settings in the metadata server, override the default region and zone locally for the gcloud tool, or override the settings manually for each request in either the gcloud tool and the Cloud Console.

You could also achieve this behaviour by running the following in gcloud.

https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region#gcloud

gcloud compute project-info add-metadata \

--metadata google-compute-default-region=europe-west1,google-compute-default-zone=europe-west1-b

After you update the default metadata by using any method, run the gcloud init command to reinitialize your default configuration. The gcloud tool refreshes the default region and zone settings only after you run the gcloud init command.

Bottom of Form

Top of Form

Question 8: Correct

Your company’s compute workloads are split between the on-premises data centre and Google Cloud Platform. The on-premises data centre is connected to Google Cloud network by Cloud VPN. You have a requirement to deploy a new non-publicly-reachable compute engine instance on a c2-standard-8 machine type in australia-southeast1-b zone. What should you do?

​

Create a route on the VPC to route all traffic to the instance over the VPN tunnel.

​

Create the instance with Private Google Access enabled.

​

Create the instance without a public IP address.

(Correct)

​

Create a deny-all egress firewall rule on the VPC network.

Explanation

Create the instance with Private Google Access enabled. is not right.

VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access to external IP addresses of Google APIs and services. Private Google Access has no effect on instances with Public IPs as they are always publicly reachable irrespective of the private google access setting.

Ref: https://cloud.google.com/vpc/docs/private-access-options#pga

Create a deny-all egress firewall rule on the VPC network. is not right.

An egress firewall rule prevents traffic from leaving the VPC network but does not prevent traffic coming in. If the instance has a public IP address, then the instance is still publicly reachable despite creating a deny-all egress firewall rule.

Create a route on the VPC to route all traffic to the instance over the VPN tunnel. is not right.

You can not create routes for public IP addresses. Routes within the VPC are applicable only to traffic on the internal IP range.

Ref: https://cloud.google.com/vpc/docs/routes

Create the instance without a public IP address. is the right answer.

Public IP addresses are internet routable. But Private IP addresses are internal and cannot be internet routable, such as RFC 1918 addresses. So creating the instance without a public IP address ensures that no internet traffic can reach it.

Ref: https://cloud.google.com/vpc/docs/ip-addresses

Bottom of Form

Top of Form

Question 9: Correct

You want to run an application in Google Compute Engine in the app-tier GCP project and have it export data from Cloud Bigtable to daily-us-customer-export Cloud Storage bucket in data-warehousing project. You plan to run a Cloud Dataflow job in the data-warehousing project to pick up data from this bucket for further processing. How should you design the IAM access to enable the compute instance push objects to daily-us-customer-export Cloud Storage bucket in data-warehousing project?

​

Make daily-us-customer-export public and create a folder with a pseudo-randomized suffix name. Share the folder with the IoT team.

​

Move both projects under the same folder.

​

Create a Shared VPC network between both projects. Grant the VM Service Account the role Storage Object Creator on app-tier.

​

Grant the VM Service Account the role Storage Object Creator on daily-us-customer-export.

(Correct)

Explanation

Move both projects under the same folder. is not right.

Folder resources provide an additional grouping mechanism and isolation boundaries between projects. They can be seen as sub-organizations within the Organization. Folders can be used to model different legal entities, departments, and teams within a company. For example, a first level of folders could be used to represent the main departments in your organization. Since folders can contain projects and other folders, each folder could then include other sub-folders, to represent different teams. Each team folder could contain additional sub-folders to represent different applications.

Ref: https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy

Although it is possible to move both projects under the same folder, unless the relevant permissions are assigned to the VM service account, it can't push the exports to the cloud storage bucket in a different project.

Create a Shared VPC network between both projects. Grant the VM Service Account the role Storage Object Creator on app-tier. is not right.

The bucket daily-us-customer-export is in the data-warehousing so the VMs service account must the assigned the role on data-warehousing and not app-tier.

Make daily-us-customer-export public and create a folder with a pseudo-randomized suffix name. Share the folder with the IoT team. is not right.

Making the report public compromises security. It doesn't matter that the folder has a pseudo-randomized suffix name. Anyone can check the contents of a public bucket.

Grant the VM Service Account the role Storage Object Creator on daily-us-customer-export. is the right answer.

Since the VM needs to access the bucket daily-us-customer-export which is in the data-warehousing, its service account needs to be granted the required permissions (Storage Object Creator) on the bucket daily-us-customer-export in the data-warehousing.

Bottom of Form

Top of Form

Question 10: Correct

Your company uses Google Cloud for all its compute workloads. One of the applications that you developed has passed unit testing, and you want to use Jenkins to deploy the application in User Acceptance Testing (UAT) environment. Your manager has asked you to automate Jenkins installation quickly and as easily as possible. What should you do

​

Create a new Kubernetes Engine cluster. Create a deployment for the Jenkins image.

​

Create an instance template with the Jenkins executable. Create a managed instance group with this template.

​

Create a new Compute Engine instance. Run the Jenkins executable.

​

Deploy Jenkins through the Google Cloud Marketplace.

(Correct)

Explanation

Create a new Compute Engine instance. Run the Jenkins executable. is not right.

While this can be done, this involves a lot more work than installing the Jenkins server through GCP Marketplace.

Create a new Kubernetes Engine cluster. Create a deployment for the Jenkins image. is not right.

While this can be done, this involves a lot more work than installing the Jenkins server through GCP Marketplace.

Create an instance template with the Jenkins executable. Create a managed instance group with this template. is not right.

Like the above options, this can be done but it involves a lot more work than installing the Jenkins server through GCP Marketplace.

Deploy Jenkins through the Google Cloud Marketplace. is the right answer.

The simplest way to launch a Jenkins server is from GCP Market place. GCP market place has a number of builds available for Jenkins: https://console.cloud.google.com/marketplace/browse?q=jenkins. All you need to do is spin up an instance from a suitable market place build and you have a Jenkins server in a few minutes with just a few clicks.

Bottom of Form

Top of Form

Question 11: Incorrect

EU GDPR requires you to respond to a Subject Access Request (SAR) within one month. To be compliant, your company deployed an application that uses Apache WebServer to provide SAR archive (tar) files back to customers requesting them. Your compliance team has asked you to set up an email notification when the network egress charges for this server exceeds 250 dollars. What should you do?

​

Use the Stackdriver Logging Agent to export the Apache web server logs to Stackdriver Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Stackdriver for the current month and sends an email if the size of all HTTP responses, multiplied by current GCP egress prices, totals over 250 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

​

Set up a budget alert on the billing account with an amount of 250 dollars, a threshold of 100%, and notification type of email.

​

Set up a budget alert on the project with an amount of 250 dollars, a threshold of 100%, and notification type of email.

(Incorrect)

​

Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 250 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

(Correct)

Explanation

Set up a budget alert on the project with an amount of 250 dollars, a threshold of 100%, and notification type of email. is not right.

This budget alert is defined for the project which means it includes all costs and not just the egress network costs - which goes against our requirements; and it also contains costs across all applications and not just the Compute Engine instance containing the Apache web server. While it is possible to set budget scope to include the Product (i.e. Google Compute Engine) and a label that uniquely identifies the specific compute engine instance, the option doesn't mention this.

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

Set up a budget alert on the billing account with an amount of 250 dollars, a threshold of 100%, and notification type of email. is not right.

Like above, but worse as this budget alert includes costs from all projects linked to the billing account. And like above, while it is possible to scope an alert down to Project/Product/Labels, the option doesn't mention this.

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

Use the Stackdriver Logging Agent to export the Apache web server logs to Stackdriver Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Stackdriver for the current month and sends an email if the size of all HTTP responses, multiplied by current GCP egress prices, totals over 250 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly. is not right.

You can't arrive at the exact egress costs with this approach. You can configure apache logs to include the response object size.

Ref: https://httpd.apache.org/docs/1.3/logs.html#common

And you can then do what this option says to arrive at the combined size of all the responses but this is not 100% accurate as it does not include header sizes. Even if we assume the header size is insignificant compare to the large files published on apache web server, our question asks us to do this the Google way "as measured by Google Cloud Platform (GCP)". GCP does not look at the response sizes in the Apache log files to determine the egress costs. The GCP egress calculator takes into consideration the source and destination (source = the region that hosts the Compute Engine instance running Apache Web Server; and the destination is the destination region of the packet). The egress cost is different for different destinations as shown in this pricing reference.

Ref: https://cloud.google.com/vpc/network-pricing#internet\_egress

The Apache logs do not give you the destination information and without this information, you can't accurately calculate the egress costs.

Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 250 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly. is the right answer.

This is the only option that satisfies our requirement. We do it the Google way by (re)using the Billing Data that GCP uses. And we scope down the costs to just egress network costs for the apache web server. Finally, we schedule this to run hourly and send an email if the costs exceed 250 dollars.

Bottom of Form

Top of Form

Question 12: Incorrect

You want to migrate a legacy application from your on-premises data centre to Google Cloud Platform. The application serves SSL traffic from worldwide clients on TCP port 443. What GCP Loadbalancing service should you use?

​

Network Load Balancer

​

Internal TCP/UDP Load Balancer. Add a firewall rule allowing ingress traffic from 0.0.0.0/0 on the target instances.

​

SSL Proxy Load Balancer

(Correct)

​

HTTPS Load Balancer

(Incorrect)

Explanation

Internal TCP/UDP Load Balancer. Add a firewall rule allowing ingress traffic from 0.0.0.0/0 on the target instances. is not right.

Internal TCP Load Balancing is a regional load balancer that enables you to run and scale your services behind an internal load balancing IP address that is accessible only to your internal virtual machine (VM) instances. Since we need to serve public traffic, this load balancer is not suitable for us.

Ref: https://cloud.google.com/load-balancing/docs/internal

Network Load Balancer. is not right.

Google Cloud external TCP/UDP Network Load Balancing is a regional, non-proxied load balancer. Since this is a regional load balancer, its endpoint is regional and this means that the traffic for this load balancer must traverse through the internet to reach the regional endpoint. Not a problem for clients located closer to this region but traversing through the internet can add a lot of latency to connections from other regions. In this scenario, clients are located all over the world, therefore Network Load Balancer is not a suitable option.

Ref: https://cloud.google.com/load-balancing/docs/network

HTTPS Load Balancer. is not right.

External HTTP(S) Load Balancer is a layer 7 load balancer suitable for HTTP/HTTPS traffic and is not suited for TCP traffic.

Ref: https://cloud.google.com/load-balancing/docs/choosing-load-balancer#summary-of-google-cloud-load-balancers

SSL Proxy Load Balancer. is the right answer.

By using Google Cloud SSL Proxy Load Balancing for your SSL traffic, you can terminate user SSL (TLS) connections at the load balancing layer, and then balance the connections across your backend instances by using the SSL (recommended) or TCP protocols. The SSL proxy load balancer terminates TLS in locations that are distributed globally, so as to minimize latency between clients and the load balancer.

Ref: https://cloud.google.com/load-balancing/docs/ssl

Ref: https://cloud.google.com/load-balancing/docs/choosing-load-balancer

Bottom of Form

Top of Form

Question 13: Correct

You are deploying an application on the Google Compute Engine, and you want to minimize network egress costs. The organization has a policy that requires you to block all but essential egress traffic. What should you do?

​

Set up a high-priority (1000) rule to allow the appropriate ports.

​

Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

(Correct)

​

Set up a high-priority (1000) rule that pairs both ingress and egress ports.

​

Set up a high-priority (1000) rule that blocks all egress and a low-priority (65534) rule that allows only the appropriate ports.

Explanation

Set up a high-priority (1000) rule to allow the appropriate ports. is not right.

This would enable all egress traffic. Every VPC network has two implied firewall rules one of which is the implied allow egress rule. This egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud. Since we want to restrict egress on all but required traffic, you can't rely on just the high priority rules to allow specific traffic.

Ref: https://cloud.google.com/vpc/docs/firewalls#default\_firewall\_rules

Set up a high-priority (1000) rule that pairs both ingress and egress ports. is not right.

There is no relation between ingress and egress and they both work differently. Like above, this would enable all egress traffic. Every VPC network has two implied firewall rules one of which is the implied allow egress rule. This egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud. Since we want to restrict egress on all but required traffic, you can't rely on just the high priority rules to allow specific traffic.

Ref: https://cloud.google.com/vpc/docs/firewalls#default\_firewall\_rules

Set up a high-priority (1000) rule that blocks all egress and a low-priority (65534) rule that allows only the appropriate ports. is not right.

The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. The highest priority rule applicable for a given protocol and port definition takes precedence over others. In this scenario, having a deny all traffic at priority 1000 takes effect over all other egress rules that allow traffic at a lower priority resulting in all outgoing traffic being blocked.

Ref: https://cloud.google.com/vpc/docs/firewalls#priority\_order\_for\_firewall\_rules

Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports. is the right answer.

The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. The highest priority rule applicable for a given protocol and port definition takes precedence over others. The relative priority of a firewall rule determines whether it is applicable when evaluated against others. In this scenario, the allow rule at priority 1000 is evaluated first and this allows the required egress traffic. The deny rule at 65534 priority is executed last and denies all other traffic that is not allowed by previous allow rules. This is exactly what we want.

Ref: https://cloud.google.com/vpc/docs/firewalls#priority\_order\_for\_firewall\_rules

Bottom of Form

Top of Form

Question 14: Incorrect

You are running a business-critical application in a fleet of compute engine instances behind an autoscaled Managed Instances Group (MIG). The MIG initiated a scale-up event to keep up with the increasing incoming traffic, but the compute engine instance failed to create. How should you debug this issue?

​

Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template.

(Correct)

​

Create an instance template that contains valid syntax that will be used by the instance group. Delete any persistent disks with the same name as instance names.

​

Create an instance template that contains valid syntax that will be used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

​

Delete the current instance template and replace it with a new instance template. Verify that the instance name and persistent disk name values are not the same in the template. Set the disks.autoDelete property to true in the instance template.

(Incorrect)

Explanation

Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template. is the right answer.

As described in this article, "My managed instance group keeps failing to create a VM. What's going on?"

https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances#troubleshooting

The likely causes are

1. A persistent disk already exists with the same name as VM Instance

2. disks.autoDelete option is set to false

3. instance template might be invalid

Therefore, we need to ensure that instance template is valid, disks.autoDelete is turned on, and that there are no existing persistent disks with the same name as VM instance.

Bottom of Form

Top of Form

Question 15: Incorrect

You deployed the Finance teams’ Payroll application to Google Cloud Compute Engine, and this application is used by staff during regular business hours. The operations team want to backup the VMs daily outside the business hours and delete images older than 30 days to save costs. They need an automated solution with the least operational overhead. What should they do?

​

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.

(Incorrect)

​

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 - 2:00 AM - Autodelete snapshots after 30 days

(Correct)

​

1. Update your instance metadata to add the following value: snapshot-schedule: 0 1 \* \* \*

2. Update your instance metadata to add the following value: snapshot-retention: 30

​

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.

Explanation

1. Update your instance metadata to add the following value: snapshot-schedule: 0 1 \* \* \*

2. Update your instance metadata to add the following value: snapshot-retention: 30. is not right.

Adding these metadata tags on the instance has no effect on snapshot creation/automation.

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. is not right.

You want to fulfill this requirement by using the least number of services. While this works, it involves the use of Cloud Functions and Cloud Scheduler and we should look at doing this using the least number of services.

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. is not right.

Bash scripts and crontabs add a lot of operational overhead. You want to fulfill this requirement with the least management overhead so you should avoid this.

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 - 2:00 AM - Autodelete snapshots after 30 days. is the right answer.

Google recommends you use Use snapshot schedules as a best practice to back up your Compute Engine workloads.

Ref: https://cloud.google.com/compute/docs/disks/scheduled-snapshots

Bottom of Form

Top of Form

Question 16: Incorrect

You run a business-critical application in a Google Cloud Compute Engine instance, and you want to set up a cost-efficient solution for backing up the data on the boot disk. You want a solution that:

· minimizes operational overhead

· backs up boot disks daily

· allows quick restore of the backups when needed

· deletes backups older than a month automatically.

What should you do?

​

Create a snapshot schedule for the disk using the desired interval.

(Correct)

​

Create a cron job to create a new disk from the disk using gcloud.

​

Create a Cloud Task to create an image and export it to Cloud Storage.

(Incorrect)

​

Create a Cloud Function to create an instance template.

Explanation

Create a Cloud Function to create an instance template. is not right.

This does not fulfil our requirement of backing up data on boot disk 'regularly'.

Create a cron job to create a new disk from the disk using gcloud. is not right.

Like above, this does not fulfil our requirement of backing up data on boot disk 'regularly'.

Create a Cloud Task to create an image and export it to Cloud Storage. is not right.

Like above, this does not fulfil our requirement of backing up data on boot disk 'regularly'.

Create a snapshot schedule for the disk using the desired interval. is the right answer.

Create snapshots to periodically back up data from your zonal persistent disks or regional persistent disks. To reduce the risk of unexpected data loss, consider the best practice of setting up a snapshot schedule to ensure your data is backed up on a regular schedule.

Ref: https://cloud.google.com/compute/docs/disks/create-snapshots

You can also delete snapshots on a schedule by defining a snapshot retention policy. A snapshot retention policy defines how long you want to keep your snapshots. If you choose to set up a snapshot retention policy, you must do so as part of your snapshot schedule.

Ref: https://cloud.google.com/compute/docs/disks/scheduled-snapshots#retention\_policy

Bottom of Form

Top of Form

Question 17: Correct

Your company plans to migrate all applications from the on-premise data centre to Google Cloud Platform and requires a monthly estimate of the cost of running these applications in GCP. How can you provide this estimate?

​

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

​

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

(Correct)

​

Provision the solution on GCP. Leave the solution provisioned for 1 week. Use Stackdriver to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs.

​

For each GCP 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.

Explanation

Provision the solution on GCP. Leave the solution provisioned for 1 week. Use Stackdriver to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs. is not right.

By provisioning the solution on GCP, you are going to incur costs. Our requirement is to just estimate the costs and this can be done by using Google Cloud Pricing Calculator.

Ref: https://cloud.google.com/products/calculator

Provision the solution on GCP. Leave the solution provisioned for 1 week. Use Stackdriver to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs. is not right.

By provisioning the solution on GCP, you are going to incur costs. Our requirement is to just estimate the costs and this can be done by using Google Cloud Pricing Calculator.

Ref: https://cloud.google.com/products/calculator

For each GCP 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. is not right.

This would certainly work but is a manual task. Why use this when you can use Google Cloud Pricing Calculator to achieve the save?

Ref: https://cloud.google.com/products/calculator

For each GCP product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each GCP product. is the right answer.

You can use the Google Cloud Pricing Calculator to total the estimated monthly costs for each GCP product. You don't incur any charges for doing so.

Ref: https://cloud.google.com/products/calculator

Bottom of Form

Top of Form

Question 18: Correct

Your company has a massive quantity of unstructured data in Apache AVRO and PARQUET files in the on-premise data centre and wants to transform this data using a Dataflow job and migrate cleansed/enriched data to BigQuery. How should you make the on-premise files accessible to Cloud Dataflow?

​

Upload the data into Cloud SQL using the import function in the console.

​

Upload the data into Cloud Spanner using the import function in the console.

​

Upload the data to Cloud Storage using the gsutil command line tool.

(Correct)

​

Upload the data to BigQuery using the bq command line tool.

Explanation

The key to answering this question is "unstructured data".

Upload the data to BigQuery using the bq command line tool. is not right.

The bq load command is used to load data in BigQuery from a local data source i.e. local file but the data has to be in a structured format.

bq --location=LOCATION load \

--source\_format=FORMAT \

PROJECT\_ID:DATASET.TABLE \

PATH\_TO\_SOURCE \

SCHEMA

where

schema: a valid schema. The schema can be a local JSON file, or it can be typed inline as part of the command. You can also use the --autodetect flag instead of supplying a schema definition.

Ref: https://cloud.google.com/bigquery/docs/loading-data-local#bq

Upload the data into Cloud SQL using the import function in the console. is not right.

Fully managed relational database service for MySQL, PostgreSQL, and SQL Server. As this is relational database, it is for structured data and not fit for unstructured data.

Ref: https://cloud.google.com/sql

Upload the data into Cloud Spanner using the import function in the console. is not right.

Cloud Spanner is the first scalable, enterprise-grade, globally-distributed, and strongly consistent database service built for the cloud specifically to combine the benefits of relational database structure with non-relational horizontal scale. Although Google claims Cloud Spanner is the best of the relational and non-relational worlds, it also says "With Cloud Spanner, you get the best of relational database structure and non-relational database scale and performance with external strong consistency across rows, regions, and continents.". Cloud spanner is for structured data and not fit for unstructured data.

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

Upload the data to Cloud Storage using the gsutil command line tool. is the right answer.

Cloud storage imposes no such restrictions, you can store large quantities of unstructured data in different file formats. Cloud Storage provides globally unified, scalable, and highly durable object storage for developers and enterprises. In addition, Dataflow can query Cloud Storage filesets as described in this article Ref: https://cloud.google.com/dataflow/docs/guides/sql/data-sources-destinations#querying-gcs-filesets

Bottom of Form

Top of Form

Question 19: Correct

You manage an overnight batch job that uses 20 VMs to transfer customer information from a CRM system to BigQuery dataset. The job can tolerate some VMs going down. The current high cost of the VMs make the overnight job not viable, and you want to reduce the costs. What should you do?

​

Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

(Correct)

​

Run a test using simulated maintenance events. If the test is successful, use N1 Standard VMs when running future jobs.

​

Run a test using a managed instance group. If the test is successful, use N1 Standard VMs in the managed instance group when running future jobs.

​

Run a test using N1 standard VMs instead of N2. If the test is successful, use N1 Standard VMs when running future jobs.

Explanation

Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs. is the right answer.

Since the batch workload is fault-tolerant i.e. can tolerate some of the VMs being terminated, you should use preemptible VMs. A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might stop (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage. If your apps are fault-tolerant and can withstand possible instance preemptions, then preemptible instances can reduce your Compute Engine costs significantly. For example, batch processing jobs can run on preemptible instances. If some of those instances stop during processing, the job slows but does not completely stop. Preemptible instances complete your batch processing tasks without placing additional workload on your existing instances and without requiring you to pay full price for additional normal instances.

Ref: https://cloud.google.com/compute/docs/instances/preemptible#what\_is\_a\_preemptible\_instance

Bottom of Form

Top of Form

Question 20: Incorrect

An auditor requires specific access on certain GCP services in your Cloud project. You have started working on the first version of a customer role to enable this access. You are currently testing this role in a test GCP project. The compliance team requires this role to be production-ready, and want you to share with them the lifecycle stage. What should you do?

​

Use permissions in your role that use the TESTING support level for role permissions. Set the role stage to BETA while testing the role permissions.

​

Use permissions in your role that use the SUPPORTED support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

(Correct)

​

Use permissions in your role that use the TESTING support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

(Incorrect)

​

Use permissions in your role that use the SUPPORTED support level for role permissions. Set the role stage to BETA while testing the role permissions.

Explanation

When setting support levels for permissions in custom roles, you can set to one of SUPPORTED, TESTING or NOT\_SUPPORTED.

SUPPORTED -The permission is fully supported in custom roles.

TESTING - The permission is being tested to check its compatibility with custom roles. You can include the permission in custom roles, but you might see unexpected behavior. Not recommended for production use.

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

Since we want the role to be suitable for production use, we need "SUPPORTED" and not "TESTING".

In terms of role stage, the stage transitions from ALPHA --> BETA --> GA

Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#testing\_and\_deploying

Since this is the first version of custom role, we start with "ALPHA".

The only option that satisfies "ALPHA" stage with "SUPPORTED" support level is

Use permissions in your role that use the SUPPORTED support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

Bottom of Form

Top of Form

Question 21: Incorrect

Your company wants to migrate all compute workloads from the on-premises data centre to Google Cloud Compute Engine. A third-party team provides operational support for your production applications outside business hours. Everyone at your company has a Gsuite account, but the support team do not. How should you grant them access to the VMs?

​

Tag all the instances with the same network tag. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag.

(Incorrect)

​

Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

(Correct)

​

Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.

​

Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

Explanation

Tag all the instances with the same network tag. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag. is not right.

This a terrible way to enable access - the SSH connections may be happening over untrusted networks i.e. no encryption and you can't SSH to the instances without adding an SSH public key.

Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner. is not right.

A step forward but you can't SSH without adding SSH public keys to the instances and opening the firewall ports to allow traffic from the operations partner IP range.

Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances. is not right.

Like above, you haven't opened the firewall to allow traffic from the operations partner IP range and the SSH connections may be happening over untrusted networks i.e. no encryption.

Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User. is the right answer.

This is the preferred approach given that the operations partner does not use Google accounts. IAP lets you

- Control access to your cloud-based and on-premises applications and VMs running on Google Cloud

- Verify user identity and use context to determine if a user should be granted access

- Work from untrusted networks without the use of a VPN

- Implement a zero-trust access model

This is how you would go about setting up SSH tunnels using IAP: https://cloud.google.com/iap/docs/using-tcp-forwarding#tunneling\_ssh\_connections

Bottom of Form

Top of Form

Question 22: Correct

Your company is building a mobile application that enables users to upload and share images with their friends. Your company places a high value on security, prefers minimal maintenance (no-op), and wants to optimize costs where possible. You are designing the backend for the app based on these requirements:

- Enable users to upload images for 30 minutes,

- Enable users to retrieve and share their images,

- Delete images older than 45 days.

You have very little time to design the solution and take it to production. What should you do?

​

Use signed URLs to allow suppliers limited time access to store their objects.

(Correct)

​

Build a lifecycle policy to delete Cloud Storage objects after 45 days.

(Correct)

​

Build a Cloud function that triggers a timer of 45 days to delete objects that have expired.

​

Set up an SFTP server for your application, and create a separate user for each supplier.

​

Develop a script that loops through all Cloud Storage buckets and deletes any buckets that are older than 45 days.

Explanation

Set up an SFTP server for your application, and create a separate user for each supplier. is not right.

It is possible to set up an SFTP server so that your suppliers can upload files but building an SFTP solution is not something you would do when the development cycle is short. You should instead look for off the shelf solutions that work with minimal configuration. Moreover, this option doesn't specify where the uploaded files are stored, how the files are secured and how the expiration is handled.

Build a Cloud function that triggers a timer of 45 days to delete objects that have expired. is not right.

Sure can be done but this is unnecessary when GCP already provides lifecycle management for the same. You are unnecessarily adding cost and complexity by doing this using Cloud functions.

Develop a script that loops through all Cloud Storage buckets and deletes any buckets that are older than 45 days. is not right.

Like above, sure can be done but this is unnecessary when GCP already provides lifecycle management for the same. You are unnecessarily adding cost and complexity by doing it this way.

Use signed URLs to allow suppliers limited time access to store their objects. is the right answer.

When we generate a signed URL, we can specify an expiry (30 mins) and users can only upload for the specified time "30 minutes". In addition, only users with the signed URL can view/download the objects so we share individual signed URLs so that "suppliers can access only their own data". Finally, all objects in Google Cloud Storage are encrypted which takes care of one of the primary goal "data security".

Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

Build a lifecycle policy to delete Cloud Storage objects after 45 days. is the right answer.

Since you don't need data older than 45 days, deleting such data is the right approach. You can set a lifecycle policy to automatically delete objects older than 45 days. The policy is valid on current as well as future objects and doesn't need any human intervention. This takes care of the other primary goal "expiration of aged data" and ensures that we "Delete data that is over 45 days old.".

Ref: https://cloud.google.com/storage/docs/lifecycle

Bottom of Form

Top of Form

Question 23: Incorrect

You company updated its business operating model recently and no longer need the applications deployed in the data-analytics-v1 GCP project. You want to turn off all GCP services and APIs in this project. You want to do this efficiently using the least number of steps. What should you do?

​

1. Verify that you are assigned the Project Owners IAM role for this project.

2. Switch to the project in the GCP console, locate the resources and delete them.

​

1. Verify that you are assigned the Organization Administrator IAM role for this project.

2. Switch to the project in the GCP console, locate the resources and delete them.

​

1. Verify that you are assigned the Organization Administrator IAM role for this project.

2. Locate the project in the GCP console, enter the project ID and then click Shut down.

(Incorrect)

​

1. Verify that you are assigned the Project Owners IAM role for this project.

2. Locate the project in the GCP console, click Shut down and then enter the project ID.

(Correct)

Explanation

1. Verify that you are assigned the Organization Administrator IAM role for this project.

2. Locate the project in the GCP console, enter the project ID and then click Shut down. is not right.

Organization Admin role provides permissions to get and list projects but not shutdown projects.

Ref: https://cloud.google.com/iam/docs/understanding-roles#resource-manager-roles

1. Verify that you are assigned the Organization Administrator IAM role for this project.

2. Switch to the project in the GCP console, locate the resources and delete them. is not right.

Organization Admin role provides permissions to get and list projects but not delete projects.

Ref: https://cloud.google.com/iam/docs/understanding-roles#resource-manager-roles

1. Verify that you are assigned the Project Owner IAM role for this project.

2. Switch to the project in the GCP console, locate the resources and delete them. is not right.

The primitive Project Owner role provides permissionst to delete project

https://cloud.google.com/iam/docs/understanding-roles#primitive\_roles

But locating all the resources and deleting them is a manual task, time consuming and error prone. Our goal is to accomplish the same but with fewest possible steps

1. Verify that you are assigned the Project Owner IAM role for this project.

2. Locate the project in the GCP console, click Shut down and then enter the project ID. is the right answer.

The primitive Project Owner role provides permissionst to delete project

https://cloud.google.com/iam/docs/understanding-roles#primitive\_roles

You can shut down projects using the Cloud Console. When you shut down a project, this immediately happens: All billing and traffic serving stops, You lose access to the project, The owners of the project will be notified and can stop the deletion within 30 days, The project will be scheduled to be deleted after 30 days. However, some resources may be deleted much earlier.

Ref: https://cloud.google.com/resource-manager/docs/creating-managing-projects#shutting\_down\_projects

Bottom of Form

Top of Form

Question 24: Correct

Your company deployed its applications across hundreds of GCP projects that use different billing accounts. The finance team is struggling to add up all production Cloud Opex costs and has requested your assistance for enabling/providing a single pane of glass for all costs incurred by all applications in Google Cloud. You want to include new costs as soon as they become available. What should you do?

​

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

​

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

(Correct)

​

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

​

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

Explanation

Fill all resources in the Pricing Calculator to get an estimate of the monthly cost. is not right.

We are interested in the costs incurred, not estimates.

Visit the Cost Table page to get a CSV export and visualize it using Data Studio. is not right.

The question states "You want to include new costs as soon as they become available" but exporting CSV is a manual process i.e. not automated so you don't get new cost data as soon as it becomes available.

Use the Reports view in the Cloud Billing Console to view the desired cost information. is not right.

If all projects are linked to the same billing account, then the billing report would have provided this information in a single screen with a visual representation that can be customized based on different parameters, however, in this scenario, projects are linked to different billing accounts and viewing the billing information of all these projects in a single visual representation is not possible in Reports view in Cloud Billing Console.

Ref: https://cloud.google.com/billing/docs/how-to/reports

Configure Billing Data Export to BigQuery and visualize the data in Data Studio. is the right answer.

Cloud Billing export to BigQuery enables you to export detailed Google Cloud billing data (such as usage, cost estimates, and pricing data) automatically throughout the day to a BigQuery dataset that you specify. Then you can access your Cloud Billing data from BigQuery for detailed analysis, or use a tool like Google Data Studio to visualize your data and provide cost visibility to the finance department. All projects can be configured to export their data to the same billing dataset and since the export happens automatically throughout the day, this satisfies our "as soon as possible" requirement.

Ref: https://cloud.google.com/billing/docs/how-to/export-data-bigquery

Bottom of Form

Top of Form

Question 25: Incorrect

You migrated a mission-critical application from the on-premises data centre to Google Kubernetes Engine (GKE). The default node pool uses e2-standard-2 machine types and is struggling to handle all the requests. You want to run the application on c2-standard-16 machine types. How can you do this without causing application downtime?

​

Create a new cluster with n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

​

Use gcloud container clusters upgrade. Deploy the new services.

(Incorrect)

​

Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

​

Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

(Correct)

Explanation

Create a new cluster with n2-highmem-16 nodes. Redeploy the pods and delete the old cluster. is not right.

This option results in the extra cost of running two clusters in parallel until the cutover happens. In addition, creating a single node pool with just n2-highmem-16 nodes might result in inefficient use of resources and subsequently extra costs.

Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes. Redeploy the pods and delete the old cluster. is not right.

Having two node pools - one based on n1-standard-2 and the other based on n2-highmem-16 is the right idea. The relevant pods can be deployed to the respective node pools. However, you are incurring the extra cost of running two clusters in parallel while the cutover happens.

Use gcloud container clusters upgrade. Deploy the new services. is not right.

gcloud container clusters upgrade - is used to upgrade the Kubernetes version of an existing container cluster.

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/upgrade

Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods. is the right answer.

This is the easiest and most practical of all options. Having two node pools - one based on n1-standard-2 and the other based on n2-highmem-16 is the right idea. In addition, adding the node pools to the existing cluster does not affect the existing node pool and therefore no downtime.

Bottom of Form

Top of Form

Question 26: Correct

You deployed a mission-critical application on Google Compute Engine. Your operations team have asked you to enable measures to prevent engineers from accidentally destroying the instance. What should you do?

​

Enable Preemptibility on the instance.

​

Enable delete protection on the instance.

(Correct)

​

Disable the flag "Delete boot disk when instance is deleted."

​

Disable Automatic restart on the instance.

Explanation

Enable Preemptibility on the instance. is not right.

A preemptible VM is an instance that 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 are excess Compute Engine capacity, so their availability varies with usage. This wouldn't help with our requirement - to prevent anyone from accidentally destroying the instance.

Ref: https://cloud.google.com/compute/docs/instances/preemptible

Disable the flag "Delete boot disk when instance is deleted." is not right.

You can automatically delete read/write zonal persistent disks when the associated VM instance is deleted. Disabling the flag would prevent the disk deletion but not the instance termination.

Ref: https://cloud.google.com/compute/docs/disks/add-persistent-disk#updateautodelete

Disable Automatic restart on the instance. is not right.

The restart behavior determines whether the instance automatically restarts if it crashes or gets terminated. This does not prevent anyone from accidentally destroying the instance.

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

Enable delete protection on the instance. is the right answer.

By setting the deletionProtection flag, a VM instance can be protected from accidental deletion. If a user attempts to delete a VM instance for which you have set the deletionProtection flag, the request fails.

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

Bottom of Form

Top of Form

Question 27: Correct

Your company migrated a custom VM from its on-premises data centre to a single Google Cloud Compute Engine. You forecast an increase in the requests and want to create another copy of the custom VM to handle the burst in traffic. What should you do?

​

Create a Compute Engine snapshot of your base VM. Create your instances from that snapshot.

​

Create a custom Compute Engine image from a snapshot. Create your images from that image.

​

Create a Compute Engine snapshot of your base VM. Create your images from that snapshot.

​

Create a custom Compute Engine image from a snapshot. Create your instances from that image.

(Correct)

Explanation

Create a Compute Engine snapshot of your base VM. Create your images from that snapshot. is not right.

You can't process additional traffic with images. You need to spin up new compute engine VM instances.

Ref: https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots

Create a custom Compute Engine image from a snapshot. Create your images from that image. is not right.

You can't process additional traffic with images. You need to spin up new compute engine VM instances.

Ref: https://cloud.google.com/compute/docs/images

Create a Compute Engine snapshot of your base VM. Create your instances from that snapshot. is not right.

You can’t create an instance with a custom image from a snapshot. A custom image belongs only to your project. To create an instance with a custom image, you must first have a custom image.

Ref: <https://cloud.google.com/compute/docs/instances/create-start-instance#creating_a_vm_from_a_custom_image>

Create a custom Compute Engine image from a snapshot. Create your instances from that image. is the right answer.

To create an instance with a custom image, you must first have a custom image. You can create custom images from source disks, images, snapshots, or images stored in Cloud Storage. You can then use the custom image to create one or more instances as needed.

Ref: <https://cloud.google.com/compute/docs/instances/create-start-instance#creating_a_vm_from_a_custom_image>

Ref: https://cloud.google.com/compute/docs/images

These additional instances can be used to process the additional application traffic.

Bottom of Form

Top of Form

Question 28: Incorrect

Your company stores an export of its Customer PII data in a multi-regional Google Cloud storage bucket. Your legal and compliance department needs to provide an external auditor every year with a report of all operations/requests on the data in this bucket. What should you do?

​

Scan the bucker using the Data Loss Prevention API.

​

Allow only a single Service Account access to read the data.

(Incorrect)

​

Enable the Identity Aware Proxy API on the project.

​

Enable Data Access audit logs for the Cloud Storage API.

(Correct)

Explanation

Enable the Identity Aware Proxy API on the project. is not right.

Identity Aware Proxy is for controlling access to your cloud-based and on-premises applications and VMs running on Google Cloud. It can't be used to record/monitor data access in Cloud Storage bucket.

Ref: https://cloud.google.com/iap

Scan the bucker using the Data Loss Prevention API. is not right.

Cloud Data Loss Prevention is a fully managed service designed to help you discover, classify, and protect your most sensitive data.. It can't be used to record/monitor data access in Cloud Storage bucket.

Ref: https://cloud.google.com/dlp

Allow only a single Service Account access to read the data. is not right.

Doing so would restrict the functionality and moreover, unless data access logs are enabled you can record all requests that read any of the stored data

Ref: https://cloud.google.com/storage/docs/access-logs

Enable Data Access audit logs for the Cloud Storage API. is the right answer.

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

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

You can enable data access audit logs at multiple levels as described here

Ref: https://cloud.google.com/logging/docs/audit/configure-data-access#configuration\_overview

Bottom of Form

Top of Form

Question 29: Incorrect

All departments at your company have their own Google Cloud Projects. You got transferred into a new department that doesn’t have a project yet, and you are ready to deploy a new application onto a Compute Engine Instance. What should you do?

​

Enable the Compute Engine API in the Cloud Console. 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.

​

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.

​

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.

(Correct)

​

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.

(Incorrect)

Explanation

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. is not right.

You can't create the instance without first creating the project. The --project flag in gcloud compute create instances command is used to specify an existing project.

https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

--project=PROJECT\_ID

The Google Cloud Platform project ID to use for this invocation. If omitted, then the current project is assumed; the current project can be listed using gcloud config list --format='text(core.project)' and can be set using gcloud config set project PROJECTID.

Ref: https://cloud.google.com/sdk/gcloud/reference#--project

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. is not right.

You can't create the instance without first creating the project. The --project flag in gcloud compute create instances command is used to specify an existing project.

https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

--project=PROJECT\_ID

The Google Cloud Platform project ID to use for this invocation. If omitted, then the current project is assumed; the current project can be listed using gcloud config list --format='text(core.project)' and can be set using gcloud config set project PROJECTID.

Ref: https://cloud.google.com/sdk/gcloud/reference#--project

Enable the Compute Engine API in the Cloud Console. 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. is not right.

In Cloud Console, when you create a new instance you don't get an option to select the project. The compute engine instance is always created in the current active project.

Ref: https://cloud.google.com/compute/docs/instances/create-start-instance

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. is the right answer.

This does it all in the correct order. You first create a project using gcloud projects create, then enable the compute engine api and finally create the VM instance in this project by using the --project flag or by creating an instance in this project in Cloud console.

https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

--project=PROJECT\_ID

The Google Cloud Platform project ID to use for this invocation. If omitted, then the current project is assumed; the current project can be listed using gcloud config list --format='text(core.project)' and can be set using gcloud config set project PROJECTID.

Ref: https://cloud.google.com/sdk/gcloud/reference#--project

Bottom of Form

Top of Form

Question 30: Correct

You work for a multinational car insurance company that specializes in rewarding safer drivers with cheaper premiums. Your company does this by installing black box IoT devices in its 2 million insured drivers’ cars. These devices capture driving behaviours such as acceleration/deceleration, speed compared to speed limits, and types of driving, such as commuting on freeway compared to commuting on surface streets etc. You expect to receive hundreds of events per minute from every device. You need to store this data and retrieve data consistently based on the event time, and both operations should be atomic. Where should you store this data?

​

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

​

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

​

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

​

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

(Correct)

Explanation

Create a file in Cloud Storage per device and append new data to that file. is not right.

Terrible idea!! Cloud Storage Objects are immutable, which means that an uploaded object cannot change throughout its storage lifetime. In practice, this means that you cannot make incremental changes to objects, such as append operations. However, it is possible to overwrite objects that are stored in Cloud Storage, and doing so happens atomically — until the new upload completes the old version of the object will be served to the readers, and after the upload completes the new version of the object will be served to readers. So for each update, the clients (construction equipments)) will have to read the full object, append a single row and upload the full object again. With the high frequency of IOT data here, it is possible that different clients (construction equipments) read different data while the updates happen and this can mess things up big time.

Ref: https://cloud.google.com/storage/docs/key-terms#immutability

Create a file in Cloud Filestore per device and append new data to that file. is not right.

Like above, there is no easy way to append data to a file in Cloud Filestore. For each update, the clients (construction equipments)) will have to read the full file, append a single row and upload the full file again. A client has to lock the file before updating and this prevents other clients from modifying the file. With the high frequency of IOT data here, this design is impracticle.

Ref: https://cloud.google.com/filestore/docs/limits#file\_locks

Ingest the data into Datastore. Store data in an entity group based on the device. is not right.

Cloud Datastore isn't suitable for ingesting IoT data. It is more suitable for Gaming leaderboard/player profile data, or where direct client access and real time sync to clients is required.

Ref: https://cloud.google.com/products/databases

In addition, storing data in an entity group based on the device means that in order to retrieve data based on the time of the event, the query has to iterate through all entities and look at the timestamp value in order to arrive at the result which isn't the best design.

Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp. is the right answer.

Cloud Bigtable provides a scalable NoSQL database service with consistent low latency and high throughput, making it an ideal choice for storing and processing time-series vehicle data.

Ref: https://cloud.google.com/solutions/designing-connected-vehicle-platform#data\_ingestion

By creating a row key based on the event timestamp, you can easily/fetch data based on the time of the event which is our requirement.

Ref: https://cloud.google.com/bigtable/docs/schema-design-time-series

Bottom of Form

Top of Form

Question 31: Correct

Your business-critical application deployed on a compute engine instance in us-west1-a zone suffered an outage due to GCP zone failure. You want to modify the application to be immune to zone failures while minimizing costs. What should you do?

​

1. Perform regular backups of your application.

2. Create a Cloud Monitoring Alert and be notified if your application becomes unavailable.

3. Restore from backups when notified.

​

1. Create Compute Engine resources in us-west1-b.

2. Balance the load across both us-west1-a and us-west1-b.

(Correct)

​

1. Create an HTTP(S) Load Balancer.

2. Create one or more global forwarding rules to direct traffic to your VMs.

​

1. Create a Managed Instance Group and specify us-west1-a as the zone.

2. Configure the Health Check with a short Health Interval.

Explanation

1. Perform regular backups of your application.

2. Create a Cloud Monitoring Alert and be notified if your application becomes unavailable.

3. Restore from backups when notified. is not right.

This wouldn't eliminate downtime, the solution doesn't support the failure of a single Compute Engine zone and the solution involves manual intervention which adds to the overall cost.

1. Create an HTTP(S) Load Balancer.

2. Create one or more global forwarding rules to direct traffic to your VMs. is not right.

The VMs are still in a single zone so this solution doesn't support the failure of a single Compute Engine zone.

1. Create a Managed Instance Group and specify us-west1-a as the zone.

2. Configure the Health Check with a short Health Interval. is not right.

The VMs are still in a single zone so this solution doesn't support the failure of a single Compute Engine zone.

1. Create Compute Engine resources in us-west1-b.

2. Balance the load across both us-west1-a and us-west1-b. is the right answer.

Creating Compute Engine resources in us-west1-b and balancing the load across both zones ensures that the solution supports the failure of a single Compute Engine zone and eliminates downtime. Even if one zone goes down, the application can continue to serve requests from the other zone.

Bottom of Form

Top of Form

Question 32: Incorrect

A finance analyst at your company is suspended pending an investigation into alleged financial misconduct. However, their Gsuite account was not disabled immediately. Your compliance team has asked you to find out if the suspended employee has accessed any audit logs or BigQuery datasets after their suspension. What should you do?

​

View System Event Logs in Stackdriver. Search for the service account associated with the user.

​

View the Admin Activity log in Stackdriver. Search for the service account associated with the user.

​

View System Event Logs in Stackdriver. Search for the user's email as the principal.

(Incorrect)

​

View Data Access audit logs in Stackdriver. Search for the user's email as the principal.

(Correct)

Explanation

View the Admin Activity log in Stackdriver. Search for the service account associated with the user. is not right.

Admin Activity logs do not contain log entries for reading resource data. Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources.

Ref: https://cloud.google.com/logging/docs/audit#admin-activity

View System Event Logs in Stackdriver. Search for the user's email as the principal. is not right.

System Event audit logs do not contain log entries for reading resource data. System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources. System Event audit logs are generated by Google systems; they are not driven by direct user action.

Ref: https://cloud.google.com/logging/docs/audit#system-event

View System Event Logs in Stackdriver. Search for the service account associated with the user. is not right.

System Event audit logs do not contain log entries for reading resource data. System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources. System Event audit logs are generated by Google systems; they are not driven by direct user action.

Ref: https://cloud.google.com/logging/docs/audit#system-event

View Data Access audit logs in Stackdriver. Search for the user's email as the principal. is the right answer.

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

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

Bottom of Form

Top of Form

Question 33: Correct

You are running a business-critical application in a GKE cluster in a subnet with cluster autoscaling enabled. A massive surge in demand for your company’s products has seen the GKE cluster node pool scale-up until there were no more free IP addresses available for new VMs. What should you do to fix this issue?

​

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

​

Expand the CIDR range of the relevant subnet for the cluster.

(Correct)

​

Create a new VPC, and set up VPC peering with the existing VPC.

​

Add an alias IP range to the subnet used by the GKE clusters.

Explanation

Create a new subnet in the same region as the subnet being used. is not right.

When you create a regional (private) GKE cluster, it automatically creates a private cluster subnet and you can't change this/add a second subnet.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#view\_subnet

Add an alias IP range to the subnet used by the GKE clusters. is not right.

Since there are no more primary IP Address available in the VPC, it is not possible to provision new VMs. You cannot create a VM with just a secondary (alias) IP. All subnets have a primary CIDR range, which is the range of internal IP addresses that define the subnet. Each VM instance gets its primary internal IP address from this range. You can also allocate alias IP ranges from that primary range, or you can add a secondary range to the subnet and allocate alias IP ranges from the secondary range.

Ref: https://cloud.google.com/vpc/docs/alias-ip#subnet\_primary\_and\_secondary\_cidr\_ranges

Create a new VPC, and set up VPC peering with the existing VPC. is not right.

You can't split a GKE cluster across two VPCs. You can't use shared VPC either as Google Kubernetes Engine does not support converting existing clusters to the Shared VPC model.

https://cloud.google.com/kubernetes-engine/docs/how-to/cluster-shared-vpc#overview

Expand the CIDR range of the relevant subnet for the cluster. is the right answer.

Since there are no more IPs available in the IP range, you need to expand the primary IP range of an existing subnet by modifying its subnet mask, setting the prefix length to a smaller number. This adds more IP addresses to the subnet IP range and lets the GKE cluster spin up more nodes as needed.

Ref: https://cloud.google.com/vpc/docs/using-vpc#expand-subnet

Bottom of Form

Top of Form

Question 34: Incorrect

You developed an application on App Engine Service to read data from a BigQuery dataset and convert the data to PARQUET format. The application is using the default App Engine service account in the app-tier GCP project. The data team owns the BigQuery dataset in the data-warehousing project. What IAM Access should you grant to the default App Engine service account in app-tier GCP project?

​

Ask data team to grant your default App Engine Service account the role of BigQuery Job User.

​

In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.

(Incorrect)

​

In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project.

​

Ask data team to grant your default App Engine Service account the role of BigQuery Data Viewer.

(Correct)

Explanation

Ask data team to grant your default App Engine Service account the role of BigQuery Job User. is not right.

Granting jobUser IAM role lets your App engine service create and run jobs including "query jobs" but doesn't give access to read data i.e. query the data directly from the datasets. The role that you need for reading data from datasets is dataViewer!!

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

In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project. is not right.

If you grant the role from your project, you are granting the permissions for BigQuery instance in your project. Since the requirement is for the app engine service to read data from the BigQuery dataset in a different project, this wouldn't work. Moreover, granting jobUser IAM role lets you run jobs including "query jobs" but doesn't give access to read data i.e. query the data directly from the datasets. The role that you need for reading data from datasets is dataViewer!!

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

In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer. is not right.

If you grant the role from your project, you are granting the permissions for BigQuery instance in your project. Since the requirement is for the app engine service to read data from the BigQuery dataset in a different project, these permissions are insufficient.

Ask data team to grant your default App Engine Service account the role of BigQuery Data Viewer. is the right answer.

SInce the data resides in the other project, the role must be granted in the other project to the App Engine service account. And since you want to read the data from BigQuery datasets, you need dataViewer role.

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

Bottom of Form

Top of Form

Question 35: Correct

Your compliance team has asked you to set up an external auditor access to logs from all GCP projects for the last 60 days. The auditor wants to explore and analyze the contents of the records quickly and efficiently. What should you do?

​

Create a Stackdriver Logging Export with a Sink destination to Cloud Storage. Create a lifecycle rule to delete objects after 60 days.

​

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

(Correct)

​

Navigate to Stackdriver Logging and select resource.labels.project\_id="\*"

​

Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days.

Explanation

Navigate to Stackdriver Logging and select resource.labels.project\_id="\*". is not right.

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

https://cloud.google.com/blog/products/gcp/best-practices-for-working-with-google-cloud-audit-logging

Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days. is not right.

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

Ref: https://cloud.google.com/logging/docs/export/configure\_export\_v2

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

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

Ref: https://cloud.google.com/logging/docs/export/configure\_export\_v2

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

https://cloud.google.com/logging/docs/export/aggregated\_sinks

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

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

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

Ref: https://cloud.google.com/logging/docs/export/configure\_export\_v2

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

https://cloud.google.com/logging/docs/export/aggregated\_sinks

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

Also, You can control storage costs and optimize storage usage by setting the default table expiration for newly created tables in a dataset. If you set the property when the dataset is created, any table created in the dataset is deleted after the expiration period. If you set the property after the dataset is created, only new tables are deleted after the expiration period.

For example, if you set the default table expiration to 7 days, older data is automatically deleted after 1 week.

Ref: <https://cloud.google.com/bigquery/docs/best-practices-storage>

Bottom of Form

Top of Form

Question 36: Incorrect

Your production Compute workloads are running in a subnet with a range 192.168.20.128/25. A recent surge in traffic has seen the production VMs struggle, and you want to add more VMs, but there are no free IP addresses for the Managed Instances Group (MIG) to autoscale. All new and old VMs need to communicate with each other. How can you do this with the fewest steps?

​

Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

(Correct)

​

Create a new Secondary IP Range in the VPC and configure the VMs to use that range.

(Incorrect)

​

Create a new VPC network for the VMs with a subnet of 192.168.21.0/24. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

​

Modify the existing subnet range to 192.168.20.0/24.

Explanation

Modify the existing subnet range to 192.168.20.0/24. is not right.

Since there are no private IP addresses available in the VPC network, it is not possible to expand the existing subnet range to use /24.

Create a new Secondary IP Range in the VPC and configure the VMs to use that range. is not right.

Since there are no more primary IP Address available in the VPC, it is not possible to provision new VMs. You cannot create a VM with just a secondary (alias) IP. All subnets have a primary CIDR range, which is the range of internal IP addresses that define the subnet. Each VM instance gets its primary internal IP address from this range. You can also allocate alias IP ranges from that primary range, or you can add a secondary range to the subnet and allocate alias IP ranges from the secondary range.

Ref: https://cloud.google.com/vpc/docs/alias-ip#subnet\_primary\_and\_secondary\_cidr\_ranges

Create a new VPC network for the VMs with a subnet of 192.168.21.0/24. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange. is not right.

Subnet routes that don't use privately reused public IP addresses are always exchanged between peered networks. You can also exchange custom routes, which include static and dynamic routes, and routes for subnets that use privately reused public IP addresses if network administrators in both networks have the appropriate peering configurations. But in this case, there is no requirement to exchange custom routes.

Ref: https://cloud.google.com/vpc/docs/vpc-peering?&\_ga=2.257174475.-1345429276.1592757751#importing-exporting-routes

Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network. is the right answer.

By creating a new VPC network, you have a new IP address range in the underlying subnets and you can spin up VMs in this new VPC. In addition, by peering this with the Dataproc cluster VPC, the VMs can communicate on their private IP address range. (Assuming all firewall rules are set up to allow traffic). You can create a new VPC with a non overlapping range and enable peering between the two VPCs and this enables the new VMs in the new VPC to communicate with the Dataproc cluster in the existing VPC. The routes for the non-reused primary IP addresses are automatically exchanged between peered networks so you don’t need to exchange custom routes.

Ref: https://cloud.google.com/vpc/docs/vpc-peering

Bottom of Form

Top of Form

Question 37: Incorrect

Your team creates/updates the infrastructure for all production requirements. You need to implement a new change to the current infrastructure and want to preview the update to the rest of your team before committing the changes. You want to follow Google-recommended practices. What should you?

​

Apply the change in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.

​

Use Deployment Manager templates to describe the proposed changes and store them in a Cloud Storage bucket.

(Correct)

​

Apply the change in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

​

Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

(Incorrect)

Explanation

Apply the change in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket. is not right.

gcloud compute instances list - lists Google Compute Engine instances. The infrastructure changes may include much more than just compute engine instances e.g. firewall rules, vpc, subnets, databases etc. The output of this command is not sufficient to describe the proposed changes. Moreover, you want to share the proposed changes, not the changes after applying them.

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

Apply the change in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories. is not right.

gcloud compute instances list - lists Google Compute Engine instances. The infrastructure changes may include much more than just compute engine instances e.g. firewall rules, vpc, subnets, databases etc. The output of this command is not sufficient to describe the proposed changes. Moreover, you want to share the proposed changes, not the changes after applying them.

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories. is not right.

With deployment manager, you can preview the update you want to make before committing any changes, with the gcloud command-line tool or the API. The Deployment Manager service previews the configuration by expanding the full configuration and creating "shell" resources. Deployment Manager does not instantiate any actual resources when you preview a configuration, giving you the opportunity to see the deployment before committing to it.

Ref: https://cloud.google.com/deployment-manager

However, saving the proposed changes to Cloud Source Repositories is not a great idea. Cloud source repositories is a private Git repository in GCP and is not a suitable place for such content.

Ref: https://cloud.google.com/source-repositories

Use Deployment Manager templates to describe the proposed changes and store them in a Cloud Storage bucket. is the right answer.

With deployment manager, you can preview the update you want to make before committing any changes, with the gcloud command-line tool or the API. The Deployment Manager service previews the configuration by expanding the full configuration and creating "shell" resources. Deployment Manager does not instantiate any actual resources when you preview a configuration, giving you the opportunity to see the deployment before committing to it.

Ref: https://cloud.google.com/deployment-manager

Cloud Storage bucket is an ideal place to upload the information and share it with the rest of the team.

Bottom of Form

Top of Form

Question 38: Incorrect

Your compliance team has asked you to set up an external auditor access to audit logs and data access logs in the production GCP project. You want to follow Google recommended practices. What should you do?

​

Assign the auditor the IAM role roles/logging.privateLogViewer. Perform the export of logs to Cloud Storage.

(Incorrect)

​

Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

(Correct)

​

Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Perform the export of logs to Cloud Storage.

​

Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy.

Explanation

Google Cloud provides Cloud Audit Logs, which is an integral part of Cloud Logging. It consists of two log streams for each project: Admin Activity and Data Access, which are generated by Google Cloud services to help you answer the question of "who did what, where, and when?" within your Google Cloud projects.

Ref: https://cloud.google.com/iam/docs/job-functions/auditing#scenario\_external\_auditors

To view Admin Activity audit logs, you must have one of the following Cloud IAM roles in the project that contains your audit logs:

- Project Owner, Project Editor, or Project Viewer.

- The Logging Logs Viewer role.

- A custom Cloud IAM role with the logging.logEntries.list Cloud IAM permission.

https://cloud.google.com/iam/docs/audit-logging#audit\_log\_permissions

To view Data Access audit logs, you must have one of the following roles in the project that contains your audit logs:

- Project Owner.

- Logging's Private Logs Viewer role.

- A custom Cloud IAM role with the logging.privateLogEntries.list Cloud IAM permission.

https://cloud.google.com/iam/docs/audit-logging#audit\_log\_permissions

---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Perform the export of logs to Cloud Storage. is not right.

logging.privateLogEntries.list provides permissions to view Data Access audit logs but this does not grant permissions to view Admin activity logs.

Ref: https://cloud.google.com/logging/docs/access-control#console\_permissions

Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy. is not right.

logging.privateLogEntries.list provides permissions to view Data Access audit logs but this does not grant permissions to view Admin activity logs.

Ref: https://cloud.google.com/logging/docs/access-control#console\_permissions

Assign the auditor the IAM role roles/logging.privateLogViewer. Perform the export of logs to Cloud Storage. is not right.

roles/logging.privateLogViewer is the right role and lets the auditor review admin activity and data access logs but exporting logs to Cloud Storage indicates that we want the auditor to review logs from Cloud Storage and not the logs within Cloud Logging console. In this scenario, unless the auditor is assigned a role that lets them access the relevant cloud storage buckets, they wouldn't be able to view log information in the buckets.

Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy. is the right answer.

roles/logging.privateLogViewer (Private Logs Viewer) includes everything from roles/logging.viewer, plus the ability to read Access Transparency logs and Data Access audit logs. This lets the auditor review the admin activity and data access logs in Cloud Logging console.

Ref: https://cloud.google.com/logging/docs/access-control

Bottom of Form

Top of Form

Question 39: Correct

You are migrating a complex on-premises data warehousing solution to Google Cloud. You plan to create a fleet of Google Compute Engine instances behind a Managed Instances Group (MIG) in the app-tier project, and BigQuery in the data-warehousing project. How should you configure the service accounts used by Compute Engine instances to allow them query access to BigQuery datasets?

​

Grant project owner role on data-warehousing project to the service account in app-tier project.

​

Grant project owner role on data-warehousing project and bigquery.dataViewer role to the service account in app-tier.

​

Grant bigquery.dataViewer role on data-warehousing project to the service account in app-tier.

(Correct)

​

Grant project owner role on app-tier project to the service account in data-warehousing project.

Explanation

Grant project owner role on app-tier project to the service account in data-warehousing project. is not right.

Our requirement is to identify the access needed for service account in the app-tier project, not the service account in data-warehousing project

Grant project owner role on data-warehousing project to the service account in app-tier project. is not right.

The primitive project owner role provides permissions to manage all resources within the project. For this scenario, the service account in the app-tier project needs access to BigQuery datasets in data-warehousing project. Granting the project owner role would fall foul of least privilege principle.

Ref: https://cloud.google.com/iam/docs/recommender-overview

Grant project owner role on data-warehousing project and bigquery.dataViewer role to the service account in app-tier. is not right.

The primitive project owner role provides permissions to manage all resources within the project. For this scenario, the service account in the app-tier project needs access to BigQuery datasets in data-warehousing project. Granting the project owner role would fall foul of least privilege principle.

Ref: https://cloud.google.com/iam/docs/recommender-overview

Grant bigquery.dataViewer role on data-warehousing project to the service account in app-tier. is the right answer.

bigquery.dataViewer role provides permissions to read the dataset's metadata and list tables in the dataset as well as Read data and metadata from the dataset's tables. This is exactly what we need to fulfil this requirement and follows the least privilege principle.

Ref: https://cloud.google.com/iam/docs/understanding-roles#bigquery-roles

Bottom of Form

Top of Form

Question 40: Incorrect

Your company has deployed all its production applications in a single Google Cloud Project. The operations team requires access to all production services in this project to debug live issues and deploy enhancements. Your security team prevents the creation of IAM roles that automatically broaden to include new permissions/services in future. How should you design the IAM role for operations team?

​

Grant all members of the DevOps team the role of Project Editor on the production project.

(Incorrect)

​

Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

(Correct)

​

Grant all members of the DevOps team the role of Project Editor on the organization level.

​

Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the organization level.

Explanation

Grant all members of the DevOps team the role of Project Editor on the production project. is not right.

You want to prevent Google Cloud product changes from broadening their permissions in the future. So you shouldn't use predefined roles e.g. Project Editor. Predefined roles are created and maintained by Google. Their permissions are automatically updated as necessary, such as when new features or services are added to Google Cloud.

Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#basic\_concepts

Grant all members of the DevOps team the role of Project Editor on the organization level. is not right.

You want to prevent Google Cloud product changes from broadening their permissions in the future. So you shouldn't use predefined roles e.g. Project Editor. Predefined roles are created and maintained by Google. Their permissions are automatically updated as necessary, such as when new features or services are added to Google Cloud.

Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#basic\_concepts

Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the organization level. is not right.

Unlike predefined roles, the permissions in custom roles are not automatically updated when Google adds new features or services. So the custom role is the right choice.

Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#basic\_concepts

However, granting the custom role at the organization level grants the DevOps team access to not just the production project but also testing and development projects which go against the principle of least privilege and should be avoided.

Ref: https://cloud.google.com/iam/docs/understanding-roles

Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project. is the right answer.

Unlike predefined roles, the permissions in custom roles are not automatically updated when Google adds new features or services. So the custom role is the right choice.

Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#basic\_concepts

Granting the custom role at the production project level grants the DevOps team access to just the production project and not testing and development projects which aligns with the principle of least privilege and should be preferred.

Ref: https://cloud.google.com/iam/docs/understanding-roles

Bottom of Form

Top of Form

Question 41: Correct

You deployed an application on a general-purpose Google Cloud Compute Engine instance that uses a persistent zonal SSD of 300 GB. The application downloads large Apache AVRO files from Cloud Storage, read all them to retrieve customer details and outputs a text file on local disk for each customer before pushing all the text files to aq Google Storage Bucket. These operations require high disk I/O, but you find that the read and write operations on the disk are always throttled. What should you do to improve the throughput?

​

Migrate to use a Local SSD on the instance.

(Correct)

​

Increase the allocated CPU to the instance.

​

Increase the size of the disk to 1 TB.

​

Migrate to use a Regional SSD on the instance.

Explanation

Migrate to use a Regional SSD on the instance. is not right.

Migrating to a regional SSD would actually make it worse. At the time of writing, the Read IOPS for a Zonal standard persistent disks is 7,500 and the Read IOPS reduces to 3000 for a Regional standard persistent disks which reduces the throughput.

Ref: https://cloud.google.com/compute/docs/disks/performance

Increase the size of the disk to 1 TB. is not right.

The performance of SSD persistent disks scales with the size of the disk.

Ref: https://cloud.google.com/compute/docs/disks/performance#cpu\_count\_size

However, there is no guarantee that increasing the disk to 1 TB will increase the throughput in this scenario as disk performance also depends on the number of vCPUs on VM instance.

Ref: https://cloud.google.com/compute/docs/disks/performance#ssd\_persistent\_disk\_performance\_by\_disk\_size

Ref: https://cloud.google.com/compute/docs/disks/performance#machine-type-disk-limits

For example, consider a 1,000 GB SSD persistent disk attached to an instance with an N2 machine type and 4 vCPUs. The read limit based solely on the size of the disk is 30,000 IOPS. However, because the instance has 4 vCPUs, the read limit is restricted to 15,000 IOPS.

Increase the allocated CPU to the instance. is not right.

In Compute Engine, machine types are grouped and curated for different workloads. Each machine type is subject to specific persistent disk limits per vCPU. Increasing the vCPU count increases the Read IOPS

https://cloud.google.com/compute/docs/disks/performance#machine-type-disk-limits

However, there is no guarantee that increasing CPU will definitely increase the throughput in this scenario as disk performance could be limited by disk size.

Ref: https://cloud.google.com/compute/docs/disks/performance#ssd\_persistent\_disk\_performance\_by\_disk\_size

Ref: https://cloud.google.com/compute/docs/disks/performance#machine-type-disk-limits

For example, consider a 1,000 GB SSD persistent disk attached to an instance with an N2 machine type and 48 vCPUs.

The read limit based solely on the vCPU count is 60,000 IOPS. However, because the instance has 1000 GB SSD, the read limit is restricted to 30,000 IOPS.

Migrate to use a Local SSD on the instance. is the right answer.

Local SSDs are physically attached to the server that hosts your VM instance. Local SSDs have higher throughput and lower latency than standard persistent disks or SSD persistent disks. The performance gains from local SSDs require certain trade-offs in availability, durability, and flexibility. Because of these trade-offs, Local SSD storage isn't automatically replicated and all data on the local SSD might be lost if the instance terminates for any reason.

Ref: https://cloud.google.com/compute/docs/disks#localssds

Ref: https://cloud.google.com/compute/docs/disks/performance#type\_comparison

Bottom of Form

Top of Form

Question 42: Incorrect

You deployed an application to the production environment in a GCP Production Project and transitioned it to your operations team. The operations manager wants to identify IAM users with Project Editor role. What should they do?

​

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

(Incorrect)

​

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

​

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

(Correct)

​

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

Explanation

In the console, validate which SSH keys have been stored as project-wide keys. is not right.

Project-wide SSH keys provide the ability to connect to most instances in your project. It can't be used to identify who has been granted the project owner role.

Ref: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#edit-ssh-metadata

Navigate to Identity-Aware Proxy and check the permissions for these resources. is not right.

Identity Aware Proxy is for controlling access to your cloud-based and on-premises applications and VMs running on Google Cloud. It can't be used to gather who has been granted the project owner role.

Ref: https://cloud.google.com/iap

Enable Audit Logs on the IAM & admin page for all resources, and validate the results. is not right.

Once enabled, new users signing in with a project owner role are recorded in logs and you can query this information but these logs don't give you a full list of all users who currently have Project owners role but have not logged in.

Use the command gcloud projects get-iam-policy to view the current role assignments. is the right answer.

gcloud projects get-iam-policy lets you retrieve IAM policy for a project. You can combine this with various flags to retrieve the required information.

e.g.

gcloud projects get-iam-policy $PROJECT\_ID --filter="bindings.role:roles/owner"

Bottom of Form

Top of Form

Question 43: Incorrect

You want to optimize the storage costs for long term archival of logs. Logs are accessed frequently in the first 30 days and only retrieved after that if there is any special requirement in the annual audit. The auditors may look into log entries up to three years old. What should you do?

​

Set up a policy that uses Standard storage for 30 days, then moves to Coldline for one year, and then moves to Archive storage for two years.

(Incorrect)

​

Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

(Correct)

​

Set up a policy that uses Nearline storage for 30 days and then moves to Archive storage for three years.

​

Set up a policy that uses Nearline storage for 30 days, then moves the Coldline for one year, and then moves to Archive storage for two years.

Explanation

Set up a policy that uses Nearline storage for 30 days and then moves to Archive storage for three years. is not right.

Nearline Storage is ideal for data you plan to read or modify on average once per month or less and there are costs associated with data retrieval. Since our requirement is to access data frequently for 30 days, we should avoid Nearline and prefer Standard Storage which is suitable for frequently accessed ("hot" data).

Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

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

Set up a policy that uses Nearline storage for 30 days, then moves the Coldline for one year, and then moves to Archive storage for two years. is not right.

Nearline Storage is ideal for data you plan to read or modify on average once per month or less and there are costs associated with data retrieval. Since our requirement is to access data frequently for 30 days, we should avoid Nearline and prefer Standard Storage which is suitable for frequently accessed ("hot" data).

Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

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

Set up a policy that uses Standard storage for 30 days, then moves to Coldline for one year, and then moves to Archive storage for two years. is not right.

Since our requirement is to access data frequently for 30 days, we should use Standard Storage which is suitable for frequently accessed ("hot" data).

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

However, transitioning to Coldline is unnecessary as there is no requirement to access data thereafter so we might as well transition all data to archival storage which offers the lowest cost option for archiving data.

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

Ref: https://cloud.google.com/storage/docs/storage-classes#archive

Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years. is the right answer.

Since our requirement is to access data frequently for 30 days, we should use Standard Storage which is suitable for frequently accessed ("hot" data).

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

And since there is no requirement to access data thereafter, we can transition all data to archival storage which offers the lowest cost option for archiving data.

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

Ref: https://cloud.google.com/storage/docs/storage-classes#archive

Bottom of Form

Top of Form

Question 44: Correct

You deployed an application using Apache Tomcat server on a single Google Cloud Compute Engine instance (VM). Users are complaining of intermittent issues accessing a specific page in the application, and you want to look at the logs which are on the local disk at /var/log/tomcat/app.log. What should you do?

​

Configure a Health Check on the instance and set a Low Healthy Threshold value.

​

Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

(Correct)

​

Connect to the instance's serial console and read the application logs.

​

Navigate to Cloud Logging and view the application logs.

Explanation

Navigate to Cloud Logging and view the application logs. is not right.

The application writes logs to disk but we don't know if these logs are forwarded to Cloud Logging. Unless you install Cloud logging agent (which this option doesn't talk about) and configured to stream the application logs, the logs don't get to Cloud logging.

Ref: https://cloud.google.com/logging/docs/agent

Connect to the instance's serial console and read the application logs. is not right.

You would interact with instance's serial console to debug boot and networking issues, troubleshoot malfunctioning instances, interact with the GRand Unified Bootloader (GRUB), and perform other troubleshooting tasks. Since the issues being reported are with the application, analysing and debugging in the instances' serial console doesn't help.

Ref: https://cloud.google.com/compute/docs/instances/interacting-with-serial-console

Configure a Health Check on the instance and set a Low Healthy Threshold value. is not right.

Configuring a health check and setting its threshold value doesn't help us diagnose and identify the issue with the application.

Install and configure the Cloud Logging Agent and view the logs from Cloud Logging. is the right answer.

It is a best practice to run the Logging agent on all your VM instances. In its default configuration, the Logging agent streams logs from common third-party applications and system software to Logging; review the list of default logs. You can configure the agent to stream additional logs; go to Configuring the Logging agent for details on agent configuration and operation. As logs are now streamed to Cloud Logging, you can view your logs in Cloud logging and diagnose the problem.

Ref: https://cloud.google.com/logging/docs/agent

Bottom of Form

Top of Form

Question 45: Correct

You work for a startup company where every developer has a dedicated development GCP project linked to a central billing account. Your finance lead is concerned that some developers may leave some services running unnecessarily or may not understand the cost implications of turning on specific services in Google Cloud Platform. They want to be alerted when a developer spends more than 750$ per month in their GCP project. What should you do?

​

Create a single budget for all projects and configure budget alerts on this budget.

​

Create a separate billing account per sandbox project and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per billing account.

​

Create a budget per project and configure budget alerts on all of these budgets.

(Correct)

​

Create a single billing account for all sandbox projects and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per project.

Explanation

Create a single budget for all projects and configure budget alerts on this budget. is not right.

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. But since a single budget is created for all projects, it is not possible to identify if a developers has spent more than $750 per month on their sandbox account.

Ref: https://cloud.google.com/billing/docs/how-to/budgets

Create a separate billing account per sandbox project and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per billing account. is not right.

This does not satisfy our requirement "to be notified" if any of the developers are spending above $750 per month on their sandbox environment.

Create a single billing account for all sandbox projects and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per project. is not right.

This does not satisfy our requirement "to be notified" if any of the developers are spending above $750 per month on their sandbox environment.

Create a budget per project and configure budget alerts on all of these budgets. is the right answer.

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. Since the budget is created per project, the alert triggers when any of the developers have spent more than $750 per month on their sandbox account.

Ref: https://cloud.google.com/billing/docs/how-to/budgets

Bottom of Form

Top of Form

Question 46: Correct

Your gaming backend uses Cloud Spanner to store leaderboard and player profile data. You want to scale the spanner instances based on predictable usage pattern. What should you do?

​

Create a Stackdriver alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly.

​

Create a Stackdriver alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly.

​

Create a Stackdriver alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

(Correct)

​

Create a cron job that runs on a scheduled basis to review stackdriver monitoring metrics, and then resize the Spanner instance accordingly.

Explanation

Create a cron job that runs on a scheduled basis to review stackdriver monitoring metrics, and then resize the Spanner instance accordingly. is not right.

While this works and does it automatically , it does not follow Google's recommended practices.

Ref: https://cloud.google.com/spanner/docs/instances "Note: You can scale the number of nodes in your instance based on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions."

Create a Stackdriver alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly. is not right.

This does not follow Google's recommended practices.

Ref: https://cloud.google.com/spanner/docs/instances "Note: You can scale the number of nodes in your instance based on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions."

Create a Stackdriver alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly. is not right.

This does not follow Google's recommended practices.

Ref: https://cloud.google.com/spanner/docs/instances "Note: You can scale the number of nodes in your instance based on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions."

Create a Stackdriver alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly. is the right answer.

For scaling the number of nodes in Cloud spanner instance, Google recommends implementing this base on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions.

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