

Câu hỏi 1Đã bỏ qua

Your app-building company has several projects under its umbrella. Different teams at your enterprise have different cloud Budgets and their GCP billing is managed by different billing accounts. Your company has a centralized finance team that needs a single visual representation of all costs incurred. New cost data should be included in the reports as soon as it's available. What should you do?

Correct answer

A. Export the billing data to BigQuery using Billing data export and create a Data Studio dashboard for visualization.

B. Export the costs to CSV from the Costs table and visualize it using Data Studio.

C. Use the pricing calculator to get the pricing on a per-resource basis.

D. Go to the Cloud Billing Console Reports view to view the desired cost information.

Giải thích tổng thể

A is correct because you can run an analysis on Bigquery after exporting the billing reports from all projects to the same dataset. It suggests using Billing data export to export the billing data to BigQuery and then create a Data Studio dashboard for visualization. This option allows for the centralization of all costs incurred from different teams and billing accounts, providing a single visual representation for the finance team.

B is incorrect because CSV export is a manual process and not very efficient and scalable. It suggests exporting the costs to CSV from the Costs table. This option may not provide real-time data updates and would require manual efforts to export and visualize the data in Data Studio. It does not fulfill the requirement of including new costs data as soon as it's available.

C is incorrect because we need actual prices and not just estimates. It suggests using the pricing calculator to get pricing on a per-resource basis. The pricing calculator is useful for estimating costs but not for visualizing the actual costs incurred across different projects and billing accounts. It does not fulfill the requirement of providing a single visual representation for the finance team.

D is incorrect because the reports view will not show billing information of all projects in the same window as the billing accounts are different. It suggests going to the Cloud Billing Console Reports view. While the Cloud Billing Console provides some reporting capabilities, it may not provide the flexibility and customization options required to create a comprehensive visual representation of all costs incurred. It

does not fulfill the requirement of creating a single visual representation for the finance team.

Links:

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

Câu hỏi 2Đã bỏ qua

You work at a billion-dollar RPG game development company. You are running your Gaming server on GKE on multiple pods running on four n1-standard-2 nodes on a GKE cluster. Additional pods need to be deployed on the same cluster requiring an n2-highmem-16 type of node. Your app is live in production and cannot afford downtime. What should you do?

A. Run `gcloud container clusters upgrade` before deploying the new services.

Correct answer

B.

1. Create a new Node Pool with n2-highmem-16 machine type.

2. Deploy the new pods.

C.

1. Create a new cluster with n2-highmem-16 nodes.

2. Delete the old cluster and redeploy the pods in the new cluster.

D.

1. Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes.

2. Delete the old cluster and redeploy the pods.

Giải thích tổng thể

A is incorrect because you need to create a new node pool for the new pods as they require different types of instances. Running "gcloud container clusters upgrade" would upgrade the existing nodes in the cluster to a different machine type. This would not meet the requirement of deploying new pods on nodes with the n2-highmem-16 machine type.

B is correct because you can add new types of instances to the GKE cluster by adding node pools. It will not cause any downtime to the existing cluster. Creating a new Node Pool with the n2-highmem-16 machine type allows for the deployment of new pods on the same cluster. This option does not involve any downtime as the existing pods can continue running on the current nodes while the new pods are deployed on the new Node Pool.

C is incorrect because there is no need to create a new cluster for it. Creating a new cluster with n2-highmem-16 nodes and deleting the old cluster would result in downtime during the redeployment of the pods. The app being live in production cannot afford downtime.

D is incorrect because there is no need to create a new cluster for it. Creating a new cluster with both n1-standard-2 and n2-highmem-16 nodes and deleting the old cluster would also result in downtime during the redeployment of the pods.

Additionally, it would require managing and maintaining two different node types in the cluster, which may not be necessary or efficient.

Links:

<https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools>

Câu hỏi 3Đã bỏ qua

You work as a data scientist in an e-commerce shoe-selling company. Your website uses Cloud Spanner as its database backend to keep current state information about users. All events triggered by the users are logged in Cloud Bigtable. The Cloud Spanner data is exported every day to Cloud Storage for backup purposes. Your Datascience team is training an ML model on the user data and they need to join data from Cloud Spanner and Bigtable together. How can you fulfill this requirement as efficiently as possible?

A. Copy data from Cloud Storage and Cloud Bigtable for specific users using a dataflow job.

B. Create a dataflow job that copies data from Cloud Bigtable and Cloud Spanner for specific users.

C. Write a Spark job that runs on a Dataproc cluster to extract data from Cloud Bigtable and Cloud Storage for specific users.

Correct answer

D.

1. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable.

2. Join these tables through user fields using the BigQuery console and apply appropriate filters.

Giải thích tổng thể

A is incorrect because creating a dataflow job can require significant effort. It suggests copying data from Cloud Storage and Cloud Bigtable for specific users

using a dataflow job. This approach involves unnecessary data movement and processing, as it requires copying data from two separate sources and then filtering it based on specific users.

B is incorrect because creating a dataflow job can require significant effort. It suggests creating a dataflow job that copies data from Cloud Bigtable and Cloud Spanner for specific users. Similar to option A, this approach involves unnecessary data movement and processing, as it requires copying data from two separate sources and then filtering it based on specific users.

C is incorrect because using Dataproc and Spark can require significant effort and time. It suggests writing a Spark job that runs on a Dataproc cluster to extract data from Cloud Bigtable and Cloud Storage for specific users. This approach also involves unnecessary data movement and processing, as it requires extracting data from two separate sources and then filtering it based on specific users.

D is correct because BigQuery supports analytics on data through external tables from Cloud Storage and Bigtable. It is perfect for this use case. It suggests creating two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. By doing so, the data from both sources can be directly queried and joined in BigQuery without the need for additional data movement or processing. The join can be performed using the user fields, and appropriate filters can be applied to retrieve the required data efficiently. This approach minimizes data movement, reduces processing overhead, and provides an efficient way to join data from both Cloud Spanner and Cloud Bigtable.

Links:

<https://cloud.google.com/bigquery/external-data-sources>

NOTE:

An external data source is a data source that you can query directly from BigQuery, even though the data is not stored in BigQuery storage. For example, you might have data in a different Google Cloud database, in files in Cloud Storage, or in a different cloud product altogether that you would like to analyze in BigQuery, but that you aren't prepared to migrate.

Use cases for external data sources include the following:

- For extract-load-transform (ELT) workloads, loading and cleaning your data in one pass and writing the cleaned result into BigQuery storage, by using a `CREATE TABLE ... AS SELECT` query.
- Joining BigQuery tables with frequently changing data from an external data source. By querying the external data source directly, you don't need to reload the data into BigQuery storage every time it changes.

Câu hỏi 4Đã bỏ qua

*You work at a large logistics and shipment company. The shipment tracking application is hosted on Compute Engine VMs in the us-central1-a zone. You want to make sure that the app does not go down in case of a zonal failure on GCP. How should you do it with minimum costs?

Correct answer

A.

1. Create Compute Engine resources in us-central1-b.
2. Set up a load balancer to balance the load across both us-central1-a and us-central1-b.

B.

1. Create a Managed Instance Group with the zone specified as us-central1-a.
2. Configure Health Check with a short Health Interval.

C.

1. Create an HTTP(S) Load Balancer.
2. Direct traffic to your VMs using one or more Global Forwarding rules.

D.

1. Back-up your application regularly.
2. Create a Cloud Monitoring Alert to be notified in case your application becomes unavailable.
3. Restore from backups when you receive a notification.

Giải thích tổng thể

A is correct because, in order to remediate the problem of a single point of failure, we have to replicate VMs within multiple zones. It leverages the concept of geographical redundancy by creating resources in a different zone, us-central1-b, which ensures that the app does not go down in case of zonal failure. By setting up a load balancer, the traffic can be balanced across both zones, providing high availability at minimum costs.

B is incorrect because a health check will not be helpful if the zone goes down. Creating a Managed Instance Group with the zone specified as us-central1-a does not provide redundancy in case of zonal failure. It only ensures that the instances within the us-central1-a zone are managed efficiently. Without resources in a different zone, the app will still go down in case of zonal failure.

C is incorrect because creating a load balancer does not automatically provide high availability. Creating an HTTP(S) Load Balancer and directing traffic to VMs using Global Forwarding rules does not provide redundancy in case of zonal failure. It only allows for load balancing across instances within the same zone. In case of zonal failure, the app will still go down.

D is incorrect because backing up is a good practice but it does not help in case of zone failure. Backing up the application regularly and creating Cloud Monitoring Alerts to be notified of unavailability does not provide immediate high availability in case of zonal failure. It focuses on restoring from backups, which may take time and lead to downtime for the app.

NOTE: (Source - GCP docs)

- Choose regions that make sense for your scenario. For example, if you only have customers in the US, or if you have specific needs that require your data to live in the US, it makes sense to store your resources in zones in the `us-central1` region or zones in the `us-east1` region.
- A *zone* is a deployment area within a region. The fully-qualified name for a zone is made up of `<region>-<zone>`. For example, the fully qualified name for zone `a` in region `us-central1` is `us-central1-a`.

Links:

https://cloud.google.com/compute/docs/regions-zones#choosing_a_region_and_zone

Random GCP Concept (optional read)

Google Cloud CDN leverages Google's globally distributed edge network to accelerate content delivery for applications served from Google Cloud. It integrates with Google Cloud Load Balancing and Google Cloud Storage, sophisticated caching to reduce server load, automatic HTTPS encryption, and fine-tuned cache controls. It utilizes Anycast IP addresses to route user requests to the nearest edge location,

enhancing speed and reliability. Additionally, Google Cloud CDN supports origin fetch optimization, real-time logging, and monitoring through Google Cloud Monitoring, and is equipped with robust security features like Google-managed SSL certificates and integration with Google Cloud Armor for enhanced protection. These capabilities make Google Cloud CDN an effective solution for optimizing the performance and security of web applications and services.

Câu hỏi 5Đã bỏ qua

You have recently joined the security team at a big enterprise. Your first task is to inspect who has the project owner role in a certain GCP project. What should you do?

A. Go to the Google Cloud console and validate which SSH keys are stored as project-wide keys.

B. Navigate to Identity-Aware Proxy and check who has permission for these resources.

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

Correct answer

D. View the current role assignments by running the command `gcloud projects get-iam-policy`.

Giải thích tổng thể

A is incorrect because SSH keys and IAM roles have no connection between them. It involves validating SSH keys, which is not directly related to project owner roles. It is not directly related to determining who has the project owner role in a GCP project. Validating SSH keys stored as project-wide keys does not provide information about the project owner role.

B is incorrect because IAP roles and project owner roles are two different types of roles. Identity-Aware Proxy (IAP) is not specifically used for managing roles and permissions in a GCP project. IAP is primarily used for controlling access to web applications running on App Engine flexible environment or Compute Engine.

C is incorrect because the requirement is to see who currently has the owner role and Audit logs will show historical data. Enabling Audit Logs on the IAM & admin page for all resources does not directly provide information about the project owner role. Audit Logs primarily capture actions taken on resources but do not specifically indicate role assignments.

D is correct because viewing the role assignments in the command line is the fastest and easiest way to check who has what role. Running the command `"gcloud`

projects get-iam-policy" provides a comprehensive view of the current role assignments within a GCP project. This command retrieves the IAM policy for a project and displays all the role assignments, which include the project owner role. This allows the security team to inspect and determine who has the project owner role in the GCP project.

Links:

<https://groups.google.com/g/google-cloud-dev/c/Z6sZs7TvygQ?pli=1>

Câu hỏi 6Đã bỏ qua

You work at a large credit card company that offers loans and credits to its customers. The company's app is hosted on GCP. There are 35 distributed backend microservices that your app requires. All the distributed microservices need to connect to a non-relational database using credentials. As the chief of DevSecOps, you want to make sure that the credentials are stored securely. Where should you store these credentials?

A. In the source code files

B. In an environment variable

Correct answer

C. In Secret Manager

D. In ACLs restricted config file

Giải thích tổng thể

A is incorrect because storing credentials in source code is not secure as it is easily discoverable in plain text by anyone with access to the source code. Storing credentials in the source code files is not a secure practice. Source code files are often accessible to multiple developers and can be easily compromised, leading to a potential security breach.

B is incorrect because credentials would be available in plain text and hence not secure. Storing credentials in an environment variable is also not a recommended practice. Environment variables are accessible to applications running on the server and can be easily accessed by anyone with access to the server, including other applications or users.

C is correct because the secret manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager is a secure and dedicated storage service provided by Google Cloud. It is designed specifically for storing and managing sensitive data such as API keys, passwords, and other credentials. Secret Manager provides fine-grained access

control and encryption, ensuring that the credentials are securely stored and accessed only by authorized services or users.

D is incorrect because access to the config file needs to be managed manually and there is an increased risk if the config file contains the credentials in plain text. Storing credentials in ACLs (Access Control Lists) restricted config file is not a best practice. While ACLs can restrict access to the config file, the file itself may still be accessible to unauthorized individuals or applications. Additionally, managing and maintaining ACLs for multiple distributed microservices can become complex and cumbersome.

Links:

<https://cloud.google.com/kubernetes-engine/docs/concepts/secret>

<https://cloud.google.com/secret-manager>

Câu hỏi 7Đã bỏ qua

You work in an app development startup as a cloud engineer. Your company extensively uses Kubernetes on GKE. Several applications are deployed on separate VPC-native Google Kubernetes Engine clusters in the same subnet. There are no more IPs available in the subnet. How can you ensure that the clusters can grow in nodes when needed?

- A. Create a new subnet in the same region as the subnet being used.**
- B. Add an alias IP range to the subnet used by the GKE clusters.**
- C. Create a new VPC, and set up VPC peering with the existing VPC.**

Correct answer

- D. Expand the CIDR range of the relevant subnet for the cluster.**

Giải thích tổng thể

A is incorrect because there is no need to create a new subnet and migrate all nodes to it as subnet IP ranges can be expanded. Creating a new subnet in the same region will not solve the issue of running out of IP addresses in the current subnet. The new subnet will have its own limited number of IP addresses and will not be able to support the growth of the existing clusters.

B is incorrect because adding an alias IP range does not expand the subnet. Adding an alias IP range to the current subnet will only provide additional IP addresses for the subnet, but it will not address the issue of running out of IPs. The alias IP range will be limited and may not be sufficient to support the desired growth of the clusters.

C is incorrect because there is no need to create a new VPC. Creating a new VPC and setting up VPC peering with the existing VPC will not solve the problem of running out of IP addresses in the current subnet. VPC peering allows communication between VPCs, but it does not provide additional IP addresses for the existing subnet.

D is correct because, in this scenario, the main issue is the depletion of available IP addresses in the subnet used by the Google Kubernetes Engine (GKE) clusters. By expanding the CIDR range of the subnet, you're essentially increasing the pool of available IP addresses within that subnet. This expansion allows for accommodating additional nodes in the existing GKE clusters without requiring the complexity of creating new subnets or VPCs. This solution ensures scalability within the current setup. As the company grows and requires more resources within the GKE clusters, having an expanded CIDR range provides the flexibility to add more nodes without hitting IP address limitations.

Links:

<https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips>

Câu hỏi 8Đã bỏ qua

Every night at 1 AM, a batch job runs on your GCP project that uses a large number of VMs. The batch job is fault-tolerant and it can still run properly if some of the VMs get destroyed. Your goal is to reduce the cost of this job. What should you do?

Correct answer

A.

1. Run the batch job in a simulation of maintenance events.

2. If the test succeeds use preemptible N1 Standard VMs for future jobs.

B.

1. Run the batch job in a simulation of maintenance events.

2. If the test succeeds, use N1 Standard VMs for future jobs.

C.

1. Run the batch job in a managed instance group.

2. If the test succeeds, use N1 Standard VMs in the managed instance group for future jobs.

D.

1. Run the batch job using N1 standard VMs instead of N2.

2. If the test succeeds, use N1 Standard VMs for future jobs.

Giải thích tổng thể

A is correct because preemptible VMs can provide up to 80% discount over normal VMs if the workloads are fault-tolerant. It proposes running the batch job in a simulation of maintenance events. This allows for testing if the job can still run properly even if some VMs get destroyed. If the test is successful, preemptible N1 Standard VMs can be used for future jobs. Preemptible VMs are significantly cheaper than regular VMs, helping to reduce costs.

B is incorrect because N1-standard VMs do not save cost as much as preemptible VMs. It suggests running the batch job in a simulation of maintenance events but does not provide a plan for reducing costs like option A. It does not mention using preemptible VMs or any other cost-saving measures.

C is incorrect because a managed instance group does not provide cost savings as much as preemptible VMs. It suggests running the batch job in a managed instance group, but it does not mention any cost-saving measures. Using a managed instance group may provide better fault tolerance and ease of management, but it does not directly address reducing costs.

D is incorrect because N1-standard VMs do not save cost as much as preemptible VMs. It suggests running the batch job using N1 standard VMs instead of N2, but it does not mention any cost-saving measures. Switching between N1 and N2 standard VMs may provide different performance characteristics, but it does not directly address reducing costs.

Links:

<https://cloud.google.com/preemptible-vm>

Câu hỏi 9Đã bỏ qua

You work as a site reliability engineer in a firm with multiple GCP projects. You are building a customer-facing website on Compute Engine. Your GCP project is used by other teams to host their apps as well. How can you prevent other teams from accidentally causing downtime to your application?

A. Use a Shielded VM.

B. Use a Preemptible VM.

C. Use a sole-tenant node.

Correct answer

D. Enable deletion protection on the instance.

Giải thích tổng thể

A is incorrect because a shielded VM does not prevent the instance to be deleted.

Using a Shielded VM does not specifically address the issue of preventing other teams from accidentally causing downtime to the application. Shielded VMs provide advanced security features, such as secure boot and virtual trusted platform module (vTPM), but they do not have any direct impact on preventing downtime caused by other teams' actions.

B is incorrect because a preemptible VM may be shut down at any time and cause downtime. Using a Preemptible VM also does not address the issue of preventing other teams from accidentally causing downtime to the application. Preemptible VMs are cost-effective, short-lived instances that can be interrupted by Compute Engine at any time, but they do not provide any specific measures to protect against actions or activities from other teams that could potentially cause downtime.

C is incorrect because a sole-tenant node does not prevent the instance to be deleted. Using a sole-tenant node solves a different problem. Sole-tenant nodes provide physical isolation for workloads that require it, ensuring that your instances run on a dedicated host system. While this can enhance security and performance, it does not specifically prevent other teams from accidentally causing downtime to the application.

D is correct because you can protect specific VM instances from deletion by setting the `deletionProtection` property on an Instance resource. Enabling deletion protection on the instance addresses the specific concern of preventing other teams from accidentally causing downtime. When deletion protection is enabled, it adds an additional confirmation step to the deletion process, preventing accidental deletion of the instance by other teams. This helps safeguard the compute resources hosting the customer-facing website from accidental disruptions or downtime caused by other teams' actions.

NOTE:

Enabling deletion protection on a Compute Engine instance ensures that the instance cannot be deleted accidentally. This feature can be useful in a shared project where multiple teams have access to the Compute Engine instances, as it

prevents other teams from mistakenly deleting the instance and causing downtime to the application running on it.

Option-C, using a sole-tenant node, provides dedicated physical resources to a project, which ensures that resources on that server are only used by your project and not by any other project in the same project. However, it does not prevent other teams from accidentally causing downtime on the application. Also, it is important to note that sole-tenant is applicable project-wise and in this case, everyone is on the same project and hence it makes sense to use **Enable detection protection on the instance**.

While using a sole-tenant node provides added security benefits such as reducing the risk of noisy neighbors, it does not directly address the issue of accidental deletion of the instance, which is the concern in this scenario.

Therefore, the correct answer is D. Enable deletion protection on the instance.

Links:

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

Câu hỏi 10Đã bỏ qua

There are thousands of employees in your company working from all over the globe. All users in your organization have an Active Directory account. Your organization wants to control and manage all of the Google's and Google Cloud Platform accounts of employees through Active Directory. What should you do?

Correct answer

- A. Synchronize users into Cloud Identity using Google Cloud Directory Sync (GCDS).**
- B. Write a script using Cloud Identity APIs to synchronize users to Cloud Identity.
- C. Upload a csv containing an export of all Active Directory users in Google Admin Console.
- D. Ask each employee to sign up for a Google account and require them to use their company email address and password.

Giải thích tổng thể

A is correct because Google Cloud Directory Sync enables administrators to synchronize users, groups, and other data from an Active Directory/LDAP service to their Google Cloud domain directory. Using Google Cloud Directory Sync (GCDS) allows for the synchronization of users from an organization's Active Directory into Cloud Identity. This ensures that all users in the organization, regardless of their location, will have their accounts managed and controlled through Active Directory.

B is incorrect because there is no need to write custom scripts as a ready-made solution already exists. Writing a script using Cloud Identity APIs to synchronize users to Cloud Identity would require significant coding and development expertise. It would be a more complex and time-consuming approach compared to using GCDS, which provides a user-friendly interface for managing user synchronization.

C is incorrect because manually exporting and importing user data is time-consuming and error-prone. Uploading a CSV containing an export of all Active Directory users in the Google Admin Console would not provide continuous synchronization. This method would require manual updates each time there are changes in the Active Directory, making it less efficient for managing a large number of employees globally.

D is incorrect because asking each employee to create their own account does not provide central management of identities. Asking each employee to sign up for a Google account and requiring them to use their company email address and password would not provide centralized control and management through Active Directory. It would create individual Google accounts for each employee, leading to difficulties in standardizing access and permissions across the organization.

Links:

<https://tools.google.com/dlpage/dirsync/>

<https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction>

Câu hỏi 11Đã bỏ qua

*You are part of the Data Engineering team at an e-commerce company. You are managing the BigQuery dataset that contains user activity data. Another team has requested access to the BigQuery Dataset but you need to make sure they do not

accidentally delete any datasets. What are some of the recommended best practices to grant access?

A. Provide users with roles/bigquery user role only, instead of roles/bigquery dataOwner.

B. Provide users with roles/bigquery dataEditor role only, instead of roles/bigquery dataOwner.

C.

1. Create a custom role by removing delete permissions

2. Add users to that role only.

Correct answer

D.

1. Create a custom role by removing delete permissions.

2. Add users to the group

3. Then, add the group to the custom role.

Giải thích tổng thể

A is incorrect because it allows the creation of new datasets within the project; the creator is granted the BigQuery Data Owner role (roles/bigquery.dataOwner) on these new datasets. Providing users with the roles/bigquery user role only would not prevent them from accidentally deleting datasets. The roles/bigquery user role only provides basic access to execute queries and read data.

B is incorrect because the dataEditor role will allow the users to update or even delete the data. Providing users with the roles/bigquery dataEditor role only would still allow them to delete datasets. The roles/bigquery dataEditor role has permission to edit and delete data within datasets.

C is incorrect because the best practice is to grant roles to groups and not users. Creating a custom role by removing delete permissions and adding users to that role would still require individual user management and could be time-consuming and error-prone.

D is correct because a custom role with no delete permissions is the best option for this use case. Granting the role to groups is considered best practice. Creating a custom role by removing delete permissions and adding users to a group, and then adding the group to the custom role, allows for easier and more efficient management of user access. By adding users to a group, you can easily add or remove multiple users from the custom role without having to individually manage


each user's access permissions. Additionally, by removing delete permissions from the custom role, you can ensure that users in the group cannot accidentally delete datasets.

Links:

<https://cloud.google.com/bigquery/docs/access-control>

NOTE:

The GCP team officially has recommended minimizing the use of **BigQuery's dataset-level basic roles**. In the production environment, it's been recommended to use predefined IAM roles. If the predefined role doesn't have the required permission then we can always use create a custom role.

 **Caution:** BigQuery's dataset-level basic roles existed prior to the introduction of IAM. We recommend that you minimize the use of basic roles. In production environments, don't grant basic roles unless there is no alternative. Instead, use [predefined IAM roles](#).

Link: <https://cloud.google.com/bigquery/docs/access-control-basic-roles#overview>

Random GCP Concept (optional read)

Google Cloud Vertex AI is a managed machine learning platform that enables data scientists and developers to build, deploy, and scale ML models more efficiently. Key features include AutoML for automating model selection and training, a unified user interface for managing the entire ML lifecycle, integration with Google Cloud services like BigQuery and Cloud Storage, and support for custom and pre-trained models. Vertex AI supports multiple ML frameworks, including TensorFlow, PyTorch, and scikit-learn, and offers tools for experiment tracking, model monitoring, and prediction. It also provides MLOps features to streamline model deployment, versioning, and maintenance and the ability to deploy models to Google's globally distributed edge network for faster predictions. Vertex AI is designed to enhance productivity and ensure robust, scalable deployments, making it a comprehensive solution for enterprise AI development.

Câu hỏi 12Đã bỏ qua

You are using Ubuntu for developing HRMS software on GCP. You installed the Google Cloud SDK using the Google Cloud Ubuntu package repository. Your

application uses Cloud Datastore as its database. How can you test this app locally without deploying it to GCP?

A. Use `gcloud datastore export` to export Cloud Datastore data.

B. Use `gcloud datastore indexes create` to create a Cloud Datastore index.

Correct answer

C. Install the `google-cloud-sdk-datastore-emulator` component using the `apt-get install` command.

D. Install the `cloud-datastore-emulator` component using the `gcloud components install` command.

Giải thích tổng thể

A is incorrect because exporting the data from the datastore does not enable you to test the datastore locally. `"gcloud datastore export"` is used to export data from Cloud Datastore, not to test an application locally. It is primarily used to export data from Cloud Datastore, not to set up a local testing environment.

B is incorrect because creating indexes does not enable you to test the datastore locally. `"gcloud datastore indexes create"` is used to create indexes for Cloud Datastore, not to test an application locally.

C is correct because the datastore emulator is installed using `apt` and not `gcloud`. When you install SDK using `apt` Cloud SDK Component Manager is disabled and you need to install extra packages again using `apt`.

- The `google-cloud-sdk-datastore-emulator` component provides a local emulator for Cloud Datastore. By installing this component using the `apt-get install` command, you can set up a local testing environment that emulates Cloud Datastore. This way, you can test your HRMS software locally without the need to deploy it to GCP. The emulator simulates Cloud Datastore behavior, allowing you to perform data operations locally during development and testing.

- `"google-cloud-sdk-datastore-emulator"` component allows you to run a local emulator for Cloud Datastore, which can be used to test the application without deploying it to GCP.

- As per the question, the Cloud SDK was installed from the Google Cloud Ubuntu package repository; hence, to install the datastore emulator, we should use the command in Option-C.

- When you install SDK using `apt` Cloud the sdk component manager is disabled and we need to install extra packages again using the `apt` command.

D is incorrect because the datastore emulator is installed using apt and not gcloud. The "cloud-datastore-emulator" component is a legacy component and is not recommended for use. The correct component to install is "google-cloud-sdk-datastore-emulator". Moreover, this option appears to be confusing the component names. There is no specific component named "cloud-datastore-emulator" in the Google Cloud SDK.

Links:

<https://cloud.google.com/datastore/docs/tools/datastore-emulator>

https://cloud.google.com/sdk/docs/components#additional_components

https://cloud.google.com/sdk/docs/components#managing_cloud_sdk_components

<https://cloud.google.com/sdk/docs/install#deb>

Note:

- Why Option-D is incorrect?

1. If you installed the SDK from the Ubuntu repo and try to do the following:

```
$ gcloud components install cloud-datastore-emulator
```

You will receive this message:

```
ERROR: (gcloud.components.install)
```

You cannot perform this action because the Cloud SDK component manager

is disabled for this installation. You can run the following command

to achieve the same result for this installation:

```
sudo apt-get install google-cloud-sdk-datastore-emulator
```

2. Add google repo, update and then install:

`apt-get install google-cloud-sdk-datastore-emulator`

if you try to install with gcloud you will get the error:

ERROR: (gcloud.components.install) You cannot perform this action because this Cloud SDK installation is managed by an external package manager.

Please consider using a separate installation of the Cloud SDK created through the default mechanism described at: <https://cloud.google.com/sdk/>

- What is the difference between these two commands?

1. `google-cloud-cli-datastore-emulator`
2. `google-cloud-sdk-datastore-emulator`

Both `google-cloud-cli-datastore-emulator` and `google-cloud-sdk-datastore-emulator` are commands that start the Cloud Datastore emulator, which is a local environment for testing and developing applications that use the Cloud Datastore service.

The difference between these two commands is the version of the Google Cloud SDK that they are associated with.

- The "google-cloud-cli-datastore-emulator" command is associated with version 236.0.0 and earlier of the Google Cloud SDK. This command is deprecated and should not be used in newer versions of the SDK.
- The "google-cloud-sdk-datastore-emulator" command is associated with version 237.0.0 and later of the Google Cloud SDK. This is the current command to use for starting the Cloud Datastore emulator.

In summary, "google-cloud-cli-datastore-emulator" is an older command that should not be used in newer versions of the Google Cloud SDK.

"google-cloud-sdk-datastore-emulator" is the current command to use for starting the Cloud Datastore emulator in the latest version of the SDK.

Câu hỏi 13 **Đã bỏ qua**

Your company extensively uses the Google Cloud Platform for all its government-related projects. The projects are distributed in a complex hierarchical structure with hundreds of folders and projects. Only the Cloud Governance team is allowed to view the full hierarchical structure. What minimum permission (Google-recommended practices) should be given to the Governance team to perform their duties?

A. Add the users to roles/browser role.

B. Add the users to roles/iam.roleViewer role.

Correct answer

C.

1. Add the users to a group

2. Add this group to roles/browser.

D.

1. Add the users to a group

2. Add this group to roles/iam.roleViewer role.

Giải thích tổng thể

A is incorrect because granting users the roles/browser role does not provide sufficient permissions for viewing the full hierarchical structure of projects and folders in Google Cloud Platform (GCP). The roles/browser role only grants permissions to view resources within a single project, not across the entire hierarchy. Since the company's projects are distributed in a complex hierarchical structure with hundreds of folders and projects, this permission would be inadequate for the Cloud Governance team to fulfill their duties effectively.

B is incorrect because assigning users the roles/iam.roleViewer role also does not grant the necessary permissions for the Cloud Governance team to view the entire hierarchical structure. Similar to the roles/browser role, roles/iam.roleViewer provides read-only access to IAM policies and permissions for a specific project, not for the entire hierarchy of projects and folders. Consequently, this permission level would not meet the requirements for the Governance team to perform their duties.

C is correct because it aligns with Google-recommended practices for managing permissions in GCP. By adding the users to a group and assigning that group the roles/browser role, the Cloud Governance team will have the necessary permissions to view the full hierarchical structure of projects and folders. This approach ensures

efficient management of permissions, as permissions can be easily managed at the group level, allowing for streamlined access control and auditability.

D is incorrect because while adding users to a group and assigning that group the roles/iam.roleViewer role would grant them read-only access to IAM policies and permissions, it still wouldn't provide the comprehensive view of the entire hierarchical structure needed by the Cloud Governance team. As with option B, this permission level is limited to individual projects and does not extend to the entire hierarchy, making it insufficient for the Governance team's requirements.

Links:

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

Câu hỏi 14Đã bỏ qua

You are the head of data and security in a space research organization. Your company uses Active Directory Federation Service as a Security Assertion Markup Language (SAML) identity provider and integrates it to perform Single Sign On (SSO) with supported service providers. Your company uses Cloud Identity for using GCP. What should you do to allow users to log in to Cloud Identity using Active Directory credentials?

A. Set up SSO with Google as an identity provider in Cloud Identity to access custom SAML apps.

Correct answer

B. Set up SSO with a third-party identity provider in Cloud Identity with Google as a service provider.

C.

1. Obtain OAuth 2.0 credentials

2. Configure the user consent screen

3. Set up OAuth 2.0 for Mobile & Desktop Apps.

D.

1. Obtain OAuth 2.0 credentials

2. Configure the user consent screen

3. Set up OAuth 2.0 for Web Server Applications.

Giải thích tổng thể

A is incorrect because Google needs to be an SSO service provider as the company already has an SSO identity provider. It suggests setting up SSO with Google as an

identity provider in Cloud Identity to access custom SAML apps. However, the question states that the company is using Active Directory Federation Service as its SAML identity provider, not Google. Therefore, setting up SSO with Google would not allow users to log in to Cloud Identity using Active Directory credentials.

B is correct because setting Google as the SSO Service provider will enable users to log in to their GSuite account with their SSO credentials. It suggests setting up SSO with a third-party identity provider in Cloud Identity with Google as a service provider. This option aligns with the scenario described in the question, where the company is using Active Directory Federation Service as its SAML identity provider. By setting up SSO with a third-party identity provider (such as Active Directory Federation Service) and configuring Google as the service provider, users would be able to log in to Cloud Identity using their Active Directory credentials.

C is incorrect because OAuth2 is not the right protocol for this. It suggests obtaining OAuth 2.0 credentials and configuring the user consent screen for Mobile & Desktop Apps. However, the question does not mention the need for OAuth 2.0 credentials or the use of Mobile & Desktop Apps. This option is not relevant to the scenario described.

D is incorrect because OAuth2 is not the right protocol for this. It suggests obtaining OAuth 2.0 credentials and configuring the user consent screen for Web Server Applications. Similar to option C, this option does not align with the scenario described in the question. There is no mention of the need for OAuth 2.0 credentials or the use of Web Server Applications.

Links:

<https://developer.okta.com/docs/concepts/saml/>

<https://support.google.com/a/answer/60224?hl=en>

Câu hỏi 15Đã bỏ qua

You are working at a startup that specializes in creating digital simulations of chemicals. You are working in a small team responsible for maintaining the uptime of 3 different projects: A, B, and C. You want to monitor the CPU, memory, and disk of these projects in a single dashboard. What should you do?

A. Share charts from projects A, B, and C.

B. Assign the metrics.reader role to projects A, B, and C.

C. Use default dashboards to view all projects in sequence.

Correct answer

D. Create a workspace under project A, and then add projects B and C.

Giải thích tổng thể

A is incorrect because sharing charts from different projects is not efficient and safe. Sharing charts from each project would require manually updating the charts and would not provide a centralized and real-time monitoring solution.

B is incorrect because the metrics will reside in different projects and it will be difficult to show them in a single dashboard. Assigning the metrics.reader role would only give you the ability to view the metrics of each project separately, but would not provide a single dashboard to monitor all projects together.

C is incorrect because monitoring separate projects separately is not scalable. Using default dashboards would still not allow you to monitor all projects together in a single dashboard. Default dashboards are project-specific and cannot be combined.

D is correct because workspaces is made for monitoring multiple projects. Creating a workspace under project A would allow you to have a centralized dashboard where you can monitor the CPU, memory, and disk of all three projects (A, B, and C) together. This option provides a single dashboard solution for monitoring and analysis of all projects.

Links:

<https://cloud.google.com/blog/products/management-tools/using-stackdriver-workspaces-help-manage-your-hybrid-and-multicloud-environment>

<https://cloud.google.com/monitoring/settings>

Câu hỏi 16Đã bỏ qua

You are the Owner of a fast-growing financial services startup. You have recently hired a person to manage all service accounts for Google Cloud Projects. What is the minimum permission you should grant this person to allow him to perform his duties?

A. Provide the user with roles/iam.roleAdmin role.

B. Provide the user with roles/iam.securityAdmin role.

C. Provide the user with roles/iam.serviceAccountUser role.

Correct answer

D. Provide the user with roles/iam.serviceAccountAdmin role.

Giải thích tổng thể

A is incorrect because roleAdmin is a much broader role than what is required here. The roles/iam.roleAdmin role is not necessary for managing service accounts in Google Cloud Projects. This role grants full control over IAM policies and bindings, including the ability to create, update, and delete roles, but it is not specific to managing service accounts.

B is incorrect because the securityAdmin role does not allow the management of service accounts. The roles/iam.securityAdmin role is also not specifically focused on managing service accounts. This role grants permissions to view and manage IAM policies, but it does not provide the necessary permissions for managing service accounts.

C is incorrect because serviceAccountUser does not allow the creation and management of service accounts. The roles/iam.serviceAccountUser role only provides the user with the ability to use service accounts, but it does not grant permissions to manage or administer service accounts. It is a more limited role compared to the roles mentioned in the other options.

D is correct because serviceAccountAdmin (roles/iam.serviceAccountAdmin): Includes permissions to list service accounts and get details about a service account. Also includes permissions to create, update, and delete service accounts and view or change the IAM policy on a service account. The roles/iam.serviceAccountAdmin role provides the minimum set of permissions required to manage all service accounts for Google Cloud Projects. This role grants the user the ability to create, update, and delete service accounts, as well as manage IAM policies for the service accounts. It is specifically designed for managing service accounts within Google Cloud.

Links:

<https://cloud.google.com/iam/docs/creating-managing-service-accounts>

Câu hỏi 17Đã bỏ qua

You are running a free static website showcasing some high-quality 3D renders of an under-construction real-estate property. The renders are stored as large files on an Apache web server running on a Compute Engine instance. Several other applications are also running on the same GCP project. You want to be notified by email when the egress network costs for the server exceed 100 dollars for the current month as measured by Google Cloud. What should you do?

A.

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

B.

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

Correct answer

C.

1. Export the billing data to BigQuery.

2. Write a Python-based Cloud Function that queries the BigQuery table to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars.

3. Set up Cloud Scheduler to trigger the function hourly.

D.

1. Install the Cloud Logging Agent on the Compute Engine instance and export the Apache web server logs to Cloud Logging.

2. Write a Python-based Cloud Function that queries the BigQuery tables to parse the HTTP response log data in Cloud Logging for the current month and sends an email if the size of all HTTP responses, multiplied by current Google Cloud egress prices, exceeds 100 dollars.

3. Set up Cloud Scheduler to trigger the function hourly.

Giải thích tổng thể

A is incorrect because the billing alert gets triggered on the project's total cost and not just the egress cost. It suggests creating a budget alert on the project level instead of a specific resource or service. This would provide a notification for overall project spending but not specifically for the egress network costs of the Apache web server.

B is incorrect because the billing alert gets triggered on the project's total cost and not just the egress cost. It suggests creating a budget alert on the billing account level instead of a specific resource or service. This would provide a notification for overall billing account spending but not specifically for the egress network costs of the Apache web server.

C is correct because exporting the billing data to bigquery and analyzing the charges incurred by egress is the best option for this use case. It exports the billing

data to BigQuery, allowing for more advanced querying and analysis. By writing a Python-based Cloud Function that queries the BigQuery table to sum the egress network costs for the Apache web server for the current month, it can send an email notification if the cost exceeds \$100. Setting up Cloud Scheduler to trigger the function hourly ensures real-time monitoring and timely notifications.

D is incorrect because Cloud Logging does not provide billing information. It suggests installing the Cloud Logging Agent on the Compute Engine instance and exporting the Apache web server logs to Cloud Logging. While this can provide log data, it does not directly address the egress network costs. Additionally, parsing the HTTP response log data in Cloud Logging and calculating the costs based on current Google Cloud egress prices adds unnecessary complexity compared to utilizing billing data and BigQuery for cost calculations.

NOTE:

As per the GCP docs, 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 Looker Studio to visualize your data. You can also use this export method to export data to a JSON file.

Links:

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

Câu hỏi 18Đã bỏ qua

Your firm generates hundreds of GB of user data per week. You are planning to store backups of your on-premise application data to Cloud Storage. The backup data is expected to be accessed once a quarter in case of a disaster. Which storage option is most cost-efficient for this use case?

Correct answer

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

Giải thích tổng thể

A is correct because Coldline storage is ideal for data you plan to read or modify at most once a quarter. Coldline is the most suitable storage class for this use case.

Coldline Storage is the most cost-efficient option for storing backups that are accessed infrequently. Coldline Storage offers the lowest cost per gigabyte compared to the other options. It is designed for data that is accessed once a quarter or less and provides lower availability and higher retrieval costs compared to other storage options.

B is incorrect because a nearline storage bucket is the most optimal storage option for data you plan to read or modify on average once per month or less. Nearline Storage is designed for data that is accessed less frequently but still requires faster access compared to Coldline Storage. While it might be suitable for storing backups, it has a higher cost per gigabyte compared to Coldline Storage and, therefore, is not the most cost-efficient option for this use case.

C is incorrect because there is no mention of regional or multi-regional data availability. Regional Storage is designed for higher availability and is suitable for storing frequently accessed data within a specific region. It has a higher cost per gigabyte compared to both Coldline Storage and Nearline Storage and is not the most cost-efficient option for storing backups that are accessed once a quarter.

D is incorrect because there is no mention of regional or multi-regional data availability. Multi-Regional Storage is designed for maximum availability and is suitable for storing data that needs to be accessed frequently across different regions. It has the highest cost per gigabyte compared to the other options and is not the most cost-efficient option for storing backups that are accessed infrequently.

Links:

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

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

Câu hỏi 19Đã bỏ qua

Your e-commerce webapp is currently self-hosted. You realized that it takes lots of server and data maintenance on your part. As part of your company's plan to migrate the on-premise workload to Google Cloud, you have decided to migrate the development environments of a few non-critical applications first. The apps use Cassandra as their database. Cassandra instances for different apps need to be isolated from each other. How can you move them to Google Cloud quickly?

A.

1. Write an instruction guide to install Cassandra on Google Cloud.

2. Provide the instruction guide to your developers.

Correct answer

B.

1. Ask the developers to launch a Cassandra image for their development work using Google Cloud Marketplace.

C.

1. Create a Cassandra Compute Engine instance and take its snapshot.

2. Create instances for your developers using the snapshot.

D.

1. Create a Cassandra Compute Engine instance and take its snapshot.

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

3. write instructions to create a Compute Engine instance from the snapshot and ask the developers to do it themselves.

Giải thích tổng thể

A is incorrect because building a guide does not mean the effort will be minimum and the developers might not have experience working with infrastructure. It involves manually installing Cassandra on Google Cloud, which can be time-consuming and requires server and data maintenance.

B is correct because launching Cassandra from the marketplace is the fastest and safest way. It allows the developers to quickly launch a pre-configured Cassandra image from the Google Cloud Marketplace. This eliminates the need for manual installation and ensures that the Cassandra instances are properly set up.

C is incorrect because it is not the quickest way. It only creates a single Cassandra Compute Engine instance and takes its snapshot. It does not provide a way to isolate the Cassandra instances for different apps or migrate them to Google Cloud quickly.

D is incorrect because it is not the quickest way. It involves creating a single Cassandra Compute Engine instance, taking its snapshot, uploading the snapshot to Cloud Storage, and providing instructions to the developers to create their own instances from the snapshot. This process can be time-consuming and does not provide a straightforward way to isolate the Cassandra instances for different apps.

Links:

<https://medium.com/google-cloud/how-to-deploy-cassandra-and-connect-on-google-cloud-platform-with-a-few-clicks-11ee3d7001d1>

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

Câu hỏi 20Đã bỏ qua

Your company sells beauty products globally via a web-based application. You have recently started using the Google Cloud Platform. You downloaded and installed the gcloud command line interface (CLI) and authenticated it with your Google Account. There are several Compute Engine instances in your GCP projects that you want to manage through the command line. The instances are located in the europe-west1-d zone. How can you avoid having to specify the zone with each CLI command when managing these instances?

Correct answer

A. Use the gcloud config subcommand to set the europe-west1-d zone as the default zone.

B. Go to the Settings page for Compute Engine and set the zone to europe-west1-d under Default location.

C. Create a file called default.conf in the CLI installation directory. The file contains the text: zone=europe-west1-d.

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

Giải thích tổng thể

A is correct because setting the default zone will enable gcloud to use the same zone for all gcloud services without having to specify it every time a command is run. The gcloud config subcommand allows you to set various configurations for the gcloud CLI tool. By using the command "gcloud config set compute/zone europe-west1-d", you can set the europe-west1-d zone as the default zone for all CLI commands. This way, you do not have to specify the zone with each command when managing instances, saving time and effort.

B is incorrect because changing the settings in the GCP console does not affect the gcloud command-line tool. The Settings page for Compute Engine does not have an option to set the default zone. It primarily allows you to configure the default project, enable APIs, manage SSH keys, and customize quota.

C is incorrect because the default zone is set through the command line. There is no such functionality in the gcloud CLI tool to create a default.conf file in the installation directory. The gcloud CLI tool primarily relies on configurations set through the gcloud config command.

D is incorrect because changing the compute engine metadata does not change the gcloud command-line config. Creating a Metadata entry on the Compute Engine page with key compute/zone will not affect the CLI commands. Metadata entries are primarily used to add custom key-value pairs to instances for various purposes, but they do not override the default zone used by the gcloud CLI tool.

Links:

<https://cloud.google.com/compute/docs/gcloud-compute#set-default-region-zone-environment-variables>

Note:

- The default region and zone set in environment variables override the default region and zone set in your local client and in the metadata server.
- To make these environment variables permanent, include these commands in your `~/.bashrc` file and restart your terminal.
- You can override environment variables by including the `--zone` or `--region` flag in your commands.

Câu hỏi 21Đã bỏ qua

You work as a cloud engineer at a social media app company. This app is using a hybrid cloud environment with some workloads on-premises and some on GCP Compute Engine VMs. The on-premise network communicates with the GCP VPC using Cloud VPN over private IPs. A new internal service needs to be deployed on Compute Engine such that no traffic from the public internet can be routed to it. What should create such a VM?

Correct answer

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

Giải thích tổng thể

A is correct because an instance without a public IP address is not accessible through the internet. Creating the instance without a public IP address ensures that no traffic from the public internet can be routed to it. By not assigning a public IP address, the VM can only be accessed through private IP addresses within the network.

B is incorrect because enabling Private Google Access does not prevent internet traffic from entering the VM. Enabling Private Google Access allows instances to reach Google APIs and services using internal IP addresses, but it does not prevent traffic from the public internet from being routed to the VM. It is mainly used for instances that do not have public IP addresses but still require access to Google services.

C is incorrect because we need an ingress rule in this case and not an egress rule. Creating a deny-all egress firewall rule on the VPC network would block all outgoing traffic from the VM, including legitimate internal traffic. This would prevent the necessary communication within the hybrid cloud environment and the desired deployment of the new internal service.

D is incorrect because this is way too invasive and doesn't explicitly address the issue of preventing public internet traffic from reaching your instance. Routing all traffic to the instance over the VPN tunnel would still allow traffic from the public internet to reach the instance. The VPN tunnel is used for secure communication between the on-premises network and the GCP VPC, but it does not restrict access from the public internet.

Links:

<https://medium.com/google-cloud/how-to-ssh-into-your-gce-machine-without-a-public-ip-4d78bd23309e>

Câu hỏi 22Đã bỏ qua

You are part of the infrastructure governance team at your digital ad agency. One of the apps is going through a revamp and requires changes in infrastructure as well. You need to get the proposed changes reviewed by your team. What is Google's recommended practice for it?

A.

- 1. Describe the proposed changes using Deployment Manager**
- 2. Store them in a Cloud Storage bucket.**

Correct answer

B.

1. Describe the proposed changes using Deployment Manager

2. Store them in Cloud Source Repositories.

C.

1. Apply the changes in a development environment

2. Save the output of the gcloud instances list command in a shared Storage bucket.

D.

1. Apply the changes in a development environment

2. Save the output of the gcloud instances list command in Cloud Source Repositories.

Giải thích tổng thể

A is incorrect because while using Deployment Manager templates to describe the proposed changes is a good practice, storing them in a Cloud Storage bucket is not the recommended approach. Cloud Storage is primarily designed for storing and accessing files and objects, but it is not the ideal solution for managing infrastructure configuration files like Deployment Manager templates.

B is correct because:

- It aligns with Google's recommended best practices for managing infrastructure changes. Deployment Manager templates allow you to define and describe your infrastructure changes in a declarative manner. Storing these templates in Cloud Source Repositories provides version control, collaboration, and a centralized location for managing the changes.
- Cloud Source Repositories are specifically designed for hosting and versioning source code. While Deployment Manager templates are not traditional source code, they are configuration files that define the desired state of the infrastructure. Storing them in a source code repository allows you to track changes, manage different versions, and collaborate with the rest of the team effectively.

C is incorrect because applying changes before the review is not a best practice. It suggests applying the changes in a development environment and saving the output

of the `gcloud instances list` command in a shared Storage bucket. This does not provide a clear and concise description of the proposed changes, making it difficult for the infrastructure governance team to review and provide feedback.

D is incorrect because applying changes before the review is not a best practice. It suggests saving the output of the `gcloud instances list` command in Cloud Source Repositories instead of describing the proposed changes using Deployment Manager. Just saving the output of the command does not provide enough information for the infrastructure governance team to review and understand the changes being made to the infrastructure.

Links:

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

<https://github.com/GoogleCloudPlatform/deploymentmanager-samples>

<https://cloud.google.com/compute/docs/disks/gcs-buckets>

<https://cloud.google.com/source-repositories/docs/features>

https://cloud.google.com/source-repositories/docs/configure-access-control#granting_member_access

https://cloud.google.com/deployment-manager/docs/configuration/templates/hosting-templates-externally#hosting_external_templates

Câu hỏi 23 **Đã bỏ qua**

Your data science team uses Google Kubernetes Engine for running their machine learning pipelines. These pipelines mostly train image processing models. Some of the long-running, non-restartable jobs in a few pipelines require the use of GPU. How can you fulfill the request at an optimal cost?

Correct answer

A. Use the GKE cluster's node auto-provisioning feature.

B. Add a VerticalPodAutoscaler to those workloads.

C. Add a node pool with preemptible VMs and GPUs attached to those VMs.

D. Add a node pool of instances with GPUs, and enable autoscaling on this node pool with a minimum size of 1.

Giải thích tổng thể

A is correct because Node auto-provisioning is a mechanism of the cluster autoscaler, which scales on a per-node pool basis. With node auto-provisioning enabled, the cluster autoscaler can extend node pools automatically based on the specifications of unschedulable Pods. Using the GKE cluster's node auto-provisioning feature allows for dynamically provisioning nodes with GPUs only when they are needed. This helps optimize cost as resources are only allocated as necessary.

B is incorrect because VerticalPodAutoscaler does not work with GPU. Adding a VerticalPodAutoscaler would not fulfill the requirement of using GPUs. The VerticalPodAutoscaler is used for optimizing resource allocation within pods, not for provisioning GPUs.

C is incorrect because preemptible VMs are not a good choice for long-running and non-restartable VMs. Adding a node pool with preemptible VMs and GPUs would not be optimal for long-running, non-restartable jobs. Preemptible VMs have a maximum lifespan of 24 hours and can be terminated at any time. This would not be suitable for jobs that need to run continuously.

D is incorrect because, for infrequent access, you don't want to have a permanent homogeneous cluster. Enabling autoscaling on a node pool with a minimum size of 1 would not optimize cost. This means that there would always be at least 1 GPU-enabled instance running, even if it's not currently being utilized. This could lead to unnecessary costs when the GPU is not needed.

NOTE:

The question mentions "You want to minimize the cost". D is clearly not ideal because 1 instance with GPUs running all the time for an incidental job is too expensive and is not recommended here.

Using auto-provisioning (Option-A) new node pools are created and deleted automatically.

--> In this question, none of the given options are 100% correct. It is just that only Option-A is **NOT incorrect**.

Links:

<https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-provisioning>

Câu hỏi 24Đã bỏ qua

You are building a stock trading app using Compute Engine and Cloud SQL. The app is deployed in a development environment and you are planning to release it to the general public soon. You need to create a production environment for the release. Your security team has given a list of recommendations to be implemented for the production environment. One of the non-negotiable requirements is that network routes should not exist between the two environments. What is the Google-recommended way of fulfilling this requirement?

Correct answer

A.

1. Create a new GCP project
2. Enable the Compute Engine and Cloud SQL APIs
3. Replicate the development environment setup in the new project.

B.

1. Create a new subnet in the existing VPC and name it production.
2. Create a new Cloud SQL instance for production in the same project
3. Deploy the application using those resources.

C.

1. Create a new project
2. Update your existing VPC to be a Shared VPC
3. Share that VPC with your new project, and replicate the development environment setup in that new project in the Shared VPC.

D.

1. Request your security team to grant you the Project Editor role in one of the production projects used by another team
2. Replicate the development environment setup in that project.

Giải thích tổng thể

A is correct because keeping the development and production environments separate is a best practice as it is the best way to isolate the environments. It suggests creating a new GCP project and replicating the development environment setup in the new project. By doing this, the production environment is completely isolated from the development environment, ensuring that there are no network routes between the two environments.

B is incorrect because it is not a best practice as it allows communication between the two environments. It suggests creating a new subnet in the existing VPC and deploying the application using the same project resources. This does not fulfill the requirement of having no network routes between the two environments as they would still be sharing the same VPC.

C is incorrect because While this is best practice to create a new project for a different environment, it explicitly breaks the security team's rule of having no path between environments by the nature of the shared VPC. The shared VPC allows entities in both VPCs to communicate as if they were in the same VPC. That's wrong. It suggests updating the existing VPC to be a Shared VPC and replicating the development environment setup in a new project within the Shared VPC. While this does create some level of isolation between the development and production environments, it does not completely eliminate network routes between them.

D is incorrect because it is not best practice to replicate the setup in that project. It suggests requesting the security team to grant the Project Editor role in one of the production projects used by another team and replicating the development environment setup in that project. This does not fulfill the requirement of having no network routes between the two environments as they would still be within the same project.

Links:

<https://cloud.google.com/solutions/best-practices-vpc-design>

Câu hỏi 25Đã bỏ qua

The production environment of your Cryptocurrency trading website is going through an external security audit. The Organization Policy called Domain Restricted Sharing is applied on the organization node, preventing users other than the organization's Cloud Identity domain from gaining access to the GCP organization. The auditor

needs to view the resources in the project but not edit anything. How can you enable this access?

A. Give the Auditor's Google account the Viewer role on the project.

B. Give the auditor's Google account the Security Reviewer role on the project.

Correct answer

C.

1. Create a temporary account for the auditor in Cloud Identity

2. Give that account the Viewer role on the project.

D.

1. Create a temporary account for the auditor in Cloud Identity

2. Give that account the Security Reviewer role on the project.

Giải thích tổng thể

A is incorrect because it suggests giving the auditor's existing Google account the Viewer role on the project. This approach does not work due to the Domain Restricted Sharing policy, which prevents users outside of the organization's Cloud Identity domain from accessing resources within the GCP organization. Since the auditor's account is presumably outside of this domain, they would not be able to access the project despite having the Viewer role.

B is incorrect because the domain restriction policy will not allow the auditor to use their own Google account. Giving the auditor's Google account the Security Reviewer role on the project would also provide them with more access than necessary. The Security Reviewer role allows the user to not only view resources but also review security configuration and settings within the project, which is not required for the audit.

C is correct because it involves creating a temporary account for the auditor within the organization's Cloud Identity domain, thus complying with the Domain Restricted Sharing policy. By giving this account the Viewer role on the project, the auditor will be able to view all resources in the project without the ability to edit them. This method adheres to the policy constraints and fulfills the audit requirements by enabling read-only access to the auditor who is now considered part of the organization's domain.

D is incorrect because the security reviewer role is over-permissive and against the best practices. Creating a temporary account for the auditor in Cloud Identity and

giving that account the Security Reviewer role on the project would provide the auditor with more access than necessary, as explained in option B.

Links:

<https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>

Câu hỏi 26Đã bỏ qua

You are running a Social Media Platform on Compute Engine. You cannot afford to lose any user data and you need to back up the VM's boot disk regularly. You also need to make sure the data can be restored quickly in case of a disaster. Older backups should be deleted automatically to save costs. What is the Google Recommended approach for it?

A. Create an instance template using a Cloud Function.

Correct answer

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

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

D. Use Cloud Tasks to create an image and export it to Cloud Storage.

Giải thích tổng thể

A is incorrect because there is no need for a cloud function for regular backups. Creating an instance template using a Cloud Function does not directly address the requirement of backing up the VM's boot disk regularly and restoring data quickly in case of a disaster. Instance templates and Cloud Functions serve different purposes and do not provide the specific backup and restore functionalities required in this scenario.

B is correct because Snapshots and disks are independent objects on GCP, you could create a snapshot from the disk and then delete the disk, and the snapshot will stay in place. Actually, you could use this snapshot to create a new disk, assign to another VM, mount it, and use it (all the information that the original disk had at the time of the snapshot will still be there). Creating a snapshot schedule for the disk using the desired interval is the recommended approach for backing up the VM's boot disk. Snapshots are point-in-time copies of the disk, and by creating a schedule, you can ensure regular backups are taken. Snapshots are efficient for backup and restore operations, and by using them, you can quickly restore the data in case of a disaster. Additionally, with a snapshot schedule, you can also configure the retention policy to automatically delete older backups, helping to save costs.

C is incorrect because there is no need to create a CRON job. Creating a cron job to create a new disk from the disk using gcloud does not directly address the requirement of backing up the VM's boot disk regularly and restoring data quickly in case of a disaster. This approach involves manually creating new disks, and it may not be efficient or suitable for regular backups and disaster recovery.

D is incorrect because there is no need to create a cloud task. Using Cloud Tasks to create an image and export it to Cloud Storage is not the recommended approach for this scenario. Cloud Tasks is a task queue service and is primarily used for distributed task processing. It is not designed specifically for disk backup and restore operations. While it is possible to use Cloud Tasks along with other services to create an image and export it to Cloud Storage, it may not provide the necessary functionalities and efficiency required for regular backups and quick data restoration.

Links:

<https://cloud.google.com/compute/docs/disks/snapshot-best-practices>

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

Câu hỏi 27Đã bỏ qua

You have been assigned to facilitate an external audit of your travel booking application hosted on GCP. The Auditor has requested for permissions to review your GCP Audit Logs and also to review your Data Access logs. What Cloud Identity and Access Management (Cloud IAM) should you provide to the Auditor?

A.

1. Provide the auditor with the IAM role `roles/logging.privateLogViewer`.

2. Export logs to Cloud Storage.

Correct answer

B.

1. Provide the auditor with the IAM role `roles/logging.privateLogViewer`.

2. Direct the auditor to also review the logs for changes to Cloud IAM policy.

C.

1. Provide the auditor with a custom role that has `logging.privateLogEntries.list` permission.

2. Export logs to Cloud Storage.

D.

1. Provide the auditor with a custom role that has `logging.privateLogEntries.list` permission.

2. Direct the auditor to also review the logs for changes to Cloud IAM policy.

Giải thích tổng thể

A is incorrect because there is no need to export the logs to Cloud Storage for the Auditor to access them. It only provides the auditors with the IAM role for private log viewing and exporting logs to Cloud Storage. It does not include permissions to review data access logs or logs for changes to the Cloud IAM policy.

B is correct because the role `roles/logging.privateLogViewer` is required to view data access logs and the logs can be accessed from the logs console. It provides the auditors with the IAM role for private log viewing. Additionally, it directs the auditors to also review the logs for changes to Cloud IAM policy. This ensures that the auditors have access to the necessary logs for their review.

C is incorrect because there is no need for a custom role for this. It provides a custom role with the permission to list private log entries, but it does not include permissions to review data access logs or logs for changes to Cloud IAM policy.

D is incorrect because there is no need for a custom role for this. It provides a custom role with the permission to list private log entries, but it does not include permissions to review data access logs or logs for changes to Cloud IAM policy. Additionally, it does not direct the auditors to review the logs for changes to Cloud IAM policy.

Links:

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

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

Câu hỏi 28Đã bỏ qua

Your company runs multiple websites on different GCP projects for selling groceries, medicines, liquor, etc. Your security team is developing an anomaly detection tool that will be used to analyze all logs from all projects over the last 60 days. To facilitate the development of the tool, you need to enable the security team to quickly explore and analyze the log contents. What is the Google recommended practice to obtain combined logs of all projects?

Note: Stackdriver is now called 'Google Cloud's Operation Suite'.

A. Select `resource.labels.project_id=""` in Stackdriver logging.

Correct answer

B.

1. Export the logs using a Stackdriver Logging Export with a Sink destination to a BigQuery dataset.

2. Configure the table partitioning in BigQuery based on the log timestamp and set up a lifecycle policy to delete partitions older than 60 days.

C.

1. Export the logs using a Stackdriver Logging Export with a Sink destination to Cloud Storage.

2. Create a lifecycle rule to delete objects after 60 days.

D.

1. Read from Stackdriver and store the logs in BigQuery using a Cloud Scheduler job.

2. Configure the table expiration to 60 days.

Giải thích tổng thể

A is incorrect because you cannot view logs of multiple projects at the same time in Stackdriver logging. Selecting `resource.labels.project_id=""` in Stackdriver logging will only filter the logs based on `project_id`, but it will not combine the logs from all projects into one single view.

B is correct because:

- This option involves exporting logs from Stackdriver Logging to BigQuery, which is a robust data warehousing solution capable of handling large datasets efficiently. By configuring table partitioning based on log timestamps in BigQuery and setting up a lifecycle policy to delete older partitions, it ensures that only logs within the last 60 days are retained for analysis. This aligns perfectly with the requirement of analyzing logs for the last 60 days while managing data retention effectively.

- This way, logs are segmented into partitions based on timestamps, ensuring that only the necessary data (logs within the last 60 days) is retained for the security team's anomaly detection tool. Old data beyond the required timeframe is automatically managed and deleted as per the defined lifecycle policy.

C is incorrect because Cloud Storage does not allow performing analysis on the logs. Exporting the logs to Cloud Storage with a lifecycle rule to delete objects after 60 days will store the logs in Cloud Storage, but it will not combine the logs from all projects into one dataset. Additionally, it requires the security team to perform additional analysis on logs stored in Cloud Storage instead of providing a more convenient way to explore and analyze the log contents.

D is incorrect because there is no need to create a Cloud Scheduler job for this. Using a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery does not provide a direct way to combine logs from all projects into one dataset. Additionally, it requires additional configuration and management of the Cloud Scheduler job.

Links:

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

Note: Stackdriver is now called 'Google Cloud's Operation Suite'.

Câu hỏi 29 **Đã bỏ qua**

Your company is a well-reputed firm in the food delivery sector. Your company has hosted its web and mobile applications on GCP. You are responsible for managing GCP costs for your organization. You have identified that a certain division of your company has several services configured but they are not using them. What should you do to turn off all configured services in the GCP project?

Correct answer

A.

1. Make sure you have the Project Owner IAM role for this project.
2. Navigate to the project in the GCP console, click Shut down, and then enter the project ID.

B.

1. Make sure you have the Project Owner IAM role for this project.
2. Navigate to the project in the GCP console, locate the resources and delete them.

C.

1. Make sure you have the **Organizational Administrator IAM** role for this project.

2. Navigate to the project in the **GCP console**, enter the project ID, and then click **Shut down**.

D.

1. Make sure that you have the **Organizational Administrator IAM** role for this project.

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

Giải thích tổng thể

A is correct because an owner of a GCP project can shut it down. It outlines the correct steps to turn off all configured services in the GCP project. First, the person should have the Project Owner IAM role for this project, which gives them the necessary permissions. Then, they need to navigate to the project in the GCP console and click on the "Shut down" option. Finally, they should enter the project ID to confirm the shutdown.

B is incorrect because manually locating and deleting the resources can be error-prone and time-consuming. It suggests deleting the resources instead of shutting them down. Deleting the resources would permanently remove them from the project and may result in loss of data or configurations, which may not be desired in this scenario where the services are not currently being used.

C is incorrect because the Organizational Administrator IAM role does not include the permissions necessary to delete a project or its resources in the Google Cloud Platform. This role is focused on broader organizational management and lacks specific permissions like `resourcemanager.projects.delete`, which are essential for project deletion. Therefore, someone with the Organizational Administrator role would be unable to execute the steps in Option C for shutting down a GCP project, as they cannot directly delete the project or its resources. The Project Owner IAM role, in contrast, has the required permissions for such actions.

D is incorrect because there is no need for an Organization Admin role for this. It suggests deleting the resources instead of shutting them down. Similar to option B, this may not be the desired action when the objective is to turn off configured services rather than permanently removing them. Additionally, it suggests needing the Organizational Administrator IAM role for this project, which is not necessary.

Links:

<https://cloud.google.com/resource-manager/docs/creating-managing-projects>

NOTE: (Source GCP docs)

Warning: You can recover most resources if you restore a project within the 30-day period. Some services have delays in restoring and you might need to wait some time for services to be restored. Some resources, such as Cloud Storage or Pub/Sub resources, are deleted much sooner. These resources might not be fully recoverable even if you restore the project within the 30-day period. Billing accounts are disconnected from the project within one day, an asynchronous process that could happen in a few or several hours. The billing account must be manually linked again after the project is restored.

Câu hỏi 30Đã bỏ qua

You are responsible for maintaining all Service Accounts for your Logistics application that is distributed over multiple projects. Some activity data is stored in a bigquery dataset in the em-databases-app project and it needs to be accessed by VMs in a web-applications project. How can you enable this access to service accounts using Google's recommended practices?

- A. Grant project owner for web-applications appropriate roles to em-databases-app.
- B. Grant project owner role to em-databases-app and the web-applications project.
- C. Grant project owner role to em-databases-app and bigquery.dataViewer role to web applications.

Correct answer

- D. Grant bigquery.dataViewer role to em-databases-app and appropriate roles to web-applications.

Giải thích tổng thể

A is incorrect because IAM roles are given to users and service accounts and not projects. Granting the project owner for web-applications does not ensure that the service account in the web-applications project has access to the bigquery dataset in the em-databases-app project. The project owner role only provides permissions for managing the project itself, not accessing resources in other projects.

B is incorrect because the project owner is too broad of a scope for this. Granting the project owner role to both projects does not specifically grant access to the service account in the web-applications project to access the bigquery dataset in the em-databases-app project. It gives full control over both projects but does not specify the necessary roles for accessing the bigquery dataset.

C is incorrect because granting the project owner role to em-databases-app and bigquery.dataViewer role to web-applications still does not grant access to the service account in web-applications project to access the bigquery dataset in the em-databases-app project. The bigquery.dataViewer role only allows viewing data in BigQuery but does not grant access to the specific dataset in another project.

D is correct because granting the bigquery.dataViewer role to em-databases-app ensures that the service account in the em-databases-app project has the necessary permissions to view the data in the bigquery dataset. Additionally, granting appropriate roles (such as the necessary permissions or roles for accessing the dataset or resources) to the web-applications project ensures that the service account in the web-applications project also has the necessary permissions to access the dataset in the em-databases-app project. This combination of granting roles to both projects ensures that the service account can access the dataset as recommended by Google's practices.

NOTE:

The question doesn't specify what kind of access is to be given (i.e. Owner or Data Viewer role). But the question does mention "... **Google-recommended practices to give access to the service account ...**".

Hence, we can (/should) follow the principle of **least privilege** to provide only **read** access. So the most correct answer in the given scenario is **Option-D** (i.e. bigquery.dataViewer role).

Links:

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

Câu hỏi 31Đã bỏ qua

One of your key employees received a job offer from another cloud company. S/he left the Organization without giving notice. His Google Account was kept active for 3 weeks. How can you find out if the employee accessed any sensitive data after s/he left?

A.

1. Visit Cloud Logging to view System Event logs.

2. Search for the user's email as the principal.

B.

1. Visit Cloud Logging to view System Event log.

2. Search for the service account associated with the user.

Correct answer

C.

1. Visit Cloud Logging to view Data Access audit logs.

2. Search for the user's email as the principal.

D.

1. Visit Cloud Logging to view Admin activity logs.

2. Search for the service account associated with the user.

Giải thích tổng thể

A is incorrect because System event logs do not provide data access-related information. It suggests visiting Cloud Logging to view System Event logs, which may not provide relevant information about the employee accessing sensitive data after leaving the organization. Additionally, searching for the user's email as the principal may not accurately capture the employee's activity after leaving.

B is incorrect because System event logs do not provide data access-related information. It also suggests visiting Cloud Logging to view System Event logs and searching for the service account associated with the user. However, this may not provide the necessary information about the employee's access to sensitive data after leaving.

C is correct because the data access logs show if the user tried to access any sensitive data. It suggests visiting Cloud Logging to view Data Access audit logs, which can provide a detailed record of data access activities. By searching for the user's email as the principal, it is possible to identify if the employee accessed any sensitive data.

D is incorrect because Admin Activity logs do not provide data access related information. It suggests visiting Cloud Logging to view Admin activity logs and searching for the service account associated with the user. While this may provide information about administrative activities, it may not directly indicate if the employee accessed sensitive data after leaving.

Links:

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

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

Câu hỏi 32Đã bỏ qua

You work at a top tech firm that provides CRM solutions to its clients around the globe. One of the CRM projects is hosted on GCP. One of the use cases for a GCP service in your project requires a custom IAM role. The permissions in the role must be suitable for production use. Your security team needs to keep track of the status of this custom role. This will be the first version of the custom role, but it may get new versions in the future. What should you do?

Correct answer

A.

1. Make sure all permissions in your role have a 'supported' support level for role permissions.

2. Set the role stage to ALPHA while testing the role permissions.

B.

1. Make sure all permissions in your role have a 'supported' support level for role permissions.

2. Set the role stage to BETA while testing the role permissions.

C.

1. Make sure all permissions in your role have a 'testing' support level for role permissions.

2. Set the role stage to ALPHA while testing the role permissions.

D.

1. Make sure all permissions in your role have a 'testing' support level for role permissions.

2. Set the role stage to BETA while testing the role permissions

Giải thích tổng thể

A is correct because Custom roles include a launch stage, which is stored in the stage property for the role. The launch stage is informational; it helps you keep track of whether each role is ready for widespread use. ALPHA means the role is still

being developed or tested, or it includes permissions for Google Cloud services or features that are not yet public. It is not ready for widespread use.

B is incorrect because while this option maintains the requirement for permissions with a 'supported' level, setting the role stage to BETA might imply that the role is still in a testing or pre-production phase, potentially conflicting with the need to have permissions ready for production. Using BETA might suggest an ongoing evaluation phase rather than indicating that the permissions are considered production-ready.

C is incorrect because the permissions that have status TESTING may not be yet fully supported to be used with custom roles. Thus, they are not fit for production use. It suggests using a 'testing' support level for role permissions, which may not provide the necessary level of confidence in the stability and suitability of the permissions for production use. Additionally, setting the role stage to ALPHA does not guarantee that all permissions in the role have a 'supported' support level.

D is incorrect because the permissions that have status TESTING may not be yet fully supported to be used with custom roles. Thus, they are not fit for production use. It suggests using a 'testing' support level for role permissions, which may not provide the necessary level of confidence in the stability and suitability of the permissions for production use. Additionally, setting the role stage to BETA does not guarantee that all permissions in the role have a 'supported' support level.

Links:

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

Support level	Description
SUPPORTED	The permission is fully supported in custom roles.
TESTING	Google is testing the permission 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.
NOT_SUPPORTED	The permission is not supported in custom roles.

Câu hỏi 33Đã bỏ qua

You have created a UI on the App engine that queries BigQuery and aggregates the data to create beautiful visualizations. The application uses the default App Engine Service Account. The BigQuery dataset is managed by another team in a different GCP project. You don't need access to the GCP project but your app needs to create the visualizations by reading the data from BigQuery. What should you do?

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

Correct answer

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

C. Provide the default App Engine service account with the role of BigQuery Data Viewer in your GCP project.

D. Provide the role of BigQuery Job User in your project to a newly created service account from the other team.

Giải thích tổng thể

A is incorrect because the Bigquery job user role Provides permissions to run jobs, including queries, within the project, it is not suitable to read data. The BigQuery Job User role only allows the user to submit jobs to BigQuery, but it does not grant the necessary permissions to read data from BigQuery or create visualizations.

B is correct because the Bigquery data viewer role allows users to read data and metadata from the table or view. The BigQuery Data Viewer role grants the necessary permissions to read data from BigQuery. By granting this role to the default App Engine Service account, the application will be able to create visualizations by querying and aggregating the data from BigQuery.

C is incorrect because the data is in another project and thus, the role needs to be given in the other project and not in the current project. Providing the default App Engine service account with the BigQuery Data Viewer role in your GCP project does not give the necessary permissions to read data from the BigQuery dataset managed by the other team in their GCP project.

D is incorrect because the data is in another project and thus, the role needs to be given in the other project and not in the current project. Providing the role of BigQuery Job User to a newly created service account from the other team does not grant the necessary permissions to read data from BigQuery or create visualizations.

NOTE:

- As per the question the application needs to create visualizations by **reading** data from bigquery.

- On your end, you do not need to run queries directly in BigQuery on another team's project. Running and execution of the job will be done by another team where they have required permission to perform this job.

- Hence, B is the correct answer, as we need only DataViewer permission to complete the job as per the **principle of the least privilege**.

Links:

<https://cloud.google.com/bigquery/docs/access-control>

Câu hỏi 34Đã bỏ qua

Your QA team has provided a signoff to deploy a new application in a new production environment. The application will be deployed on a Compute Engine instance on a new GCP project that is not created yet. What should you do?

Correct answer

A.

1. Use the Cloud SDK to create a new project
2. Enable the Compute Engine API in that project
2. Create the instance specifying your new project.

B.

1. Use the Cloud Console to enable Compute Engine API
2. Use the Cloud SDK to create the instance
3. Use the --project flag to specify a new project.

C.

1. Use the Cloud SDK to create a new instance
2. Use the --project flag to specify the new project.
3. When Cloud SDK prompts you to enable the Compute Engine API, answer YES.

D.

1. Use the Cloud Console to enable Compute Engine API.
2. Navigate to the Compute Engine section of the Console and create a new instance.
3. Look for the Create In A New Project option in the creation form.

Giải thích tổng thể

A is correct because you need to create a new project, then enable the compute engine API on that project and then you can create the compute engine instance on that project. It follows the correct sequence of steps. It first creates a new project using the Cloud SDK, enables the Compute Engine API in that project, and then creates the instance specifying the new project.

B is incorrect because the `--project` flag does not create a new project. It enables the Compute Engine API first using the Cloud Console and then uses the Cloud SDK to create the instance. The correct sequence requires enabling the API after creating the project.

C is incorrect because the `--project` flag does not create a new project. It creates a new instance using the Cloud SDK but doesn't mention anything about creating the project. The correct sequence requires creating the project first before creating the instance.

D is incorrect because you need to create a new project first. It enables the Compute Engine API using the Cloud Console but doesn't provide any information about creating a new project. The correct sequence requires creating a new project before enabling the API and creating the instance.

Links:

<https://cloud.google.com/ai-platform/deep-learning-vm/docs/quickstart-cli#before-you-begin>

Câu hỏi 35Đã bỏ qua

Your Motorcycle company is going through a Digitization phase. There are a lot of unstructured files in different file formats. ETL transformations on the data will be performed using Cloud Dataflow. What should you do to make the data accessible on Google Cloud?

A. Use the `bq` command line tool to upload the data to BigQuery.

Correct answer

B. Use the `gsutil` command line tool to upload the data to Cloud Storage.

C. Use the import function in the console to upload the data into Cloud SQL.

D. Use the import function in the console to upload the data into Cloud Spanner.

Giải thích tổng thể

A is incorrect because Bigquery only supports a limited number of structured file formats. The `bq` command line tool is used to interact with BigQuery, which is a data

warehousing and analytics solution. It is not designed for uploading unstructured files or performing ETL transformations.

B is correct because Cloud Storage is object storage and can store files of any type. The gsutil command line tool is used to interact with Cloud Storage, which provides a scalable and durable object storage solution. It is well-suited for storing and accessing unstructured files. By using gsutil, you can upload the unstructured files to Cloud Storage and make them accessible on Google Cloud.

C is incorrect because Cloud SQL only supports structured file formats. The import function in the console is used for uploading data into Cloud SQL, which is a fully managed relational database service. It is not specifically designed for handling unstructured files or performing ETL transformations.

D is incorrect because Cloud Spanner can only store structured data. The import function in the console is used for uploading data into Cloud Spanner, which is a globally distributed and strongly consistent relational database service. It is not specifically designed for handling unstructured files or performing ETL transformations.

Links:

<https://cloud.google.com/products/storage>

Câu hỏi 36Đã bỏ qua

You are part of the Google Cloud operations team at the Digital vertical of your retail stores' chain. You are managing multiple projects. How can you configure the Google Cloud SDK to easily manage multiple projects?

Correct answer

A.

- 1. Make a separate configuration for each project you need to manage.**
- 2. Activate the appropriate configuration for each of your assigned Google Cloud projects as required.**

B.

- 1. Make a separate configuration for each project you need to manage.**
- 2. Update the configuration values using gcloud init whenever you need to work with a non-default project.**

C.

1. Use the default configuration for one project you need to manage.
2. Activate the appropriate configuration for each of your assigned Google Cloud projects as required.

D.

1. Use the default configuration for one project you need to manage.
2. Update the configuration values using `gcloud init` whenever you need to work with a non-default project.

Giải thích tổng thể

A is correct because it is considered best practice to create separate configurations for separate projects and switch between them as needed. It suggests making a separate configuration for each project that needs to be managed. This allows for better organization and separation of settings for each project. Additionally, activating the appropriate configuration for each assigned project ensures that the correct settings are used when working on a specific project.

B is incorrect because if the configurations are created, then you don't need to run `gcloud init` to switch to a different config. It also suggests making a separate configuration for each project, which is correct. However, it suggests updating the configuration values using `gcloud init` whenever a non-default project needs to be worked on. This method can be time-consuming and inefficient when managing multiple projects, as it requires manually updating configurations each time.

C is incorrect because it is considered best practice to create separate configurations for separate projects and switch between them as needed. It suggests using the default configuration for one project that needs to be managed. This can lead to confusion and potential errors when working on multiple projects, as the default configuration may not have the correct settings for each project. It is better to create separate configurations for each project.

D is incorrect because it is considered best practice to create separate configurations for separate projects and switch between them as needed. It suggests using the default configuration for one project and updating the configuration values using `gcloud init` whenever a non-default project needs to be worked on. This method suffers from the same issues as option B, as it requires manual updating of configurations each time a different project needs to be worked on. Separating configurations for each project is a better approach.

Links:

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

Note:

gcloud config set sets the specified property in your active configuration only. A property governs the behavior of a specific aspect of Google Cloud CLI such as the service account to use or the verbosity level of logs. To set the property across all configurations, use the `--installation` flag.

Câu hỏi 37Đã bỏ qua

You are part of the production support team for a global e-commerce app. You received an alert that a new instance creation failed to create new instances on a managed instance group used by the app. The app requires the number of active instances specified in the template to serve its users properly. What should you do in such a scenario?

A.

1. Make sure the instance template has valid syntax.
2. Delete any persistent disks with the same name as instance names.

B.

1. Make sure the instance template used by the instance group has valid syntax.
2. Verify that the instance name and persistent disk name values are not the same in the template.

Correct answer

C.

1. Create a new instance template with a valid syntax and set `disks.autoDelete=true`
2. Delete existing persistent disks with the same name as instance names
3. Make rolling update (to switch to a new template)

D.

1. Delete the current one and create a new instance template.
2. Make sure that the instance name and persistent disk name values are different in the template.
3. Set the `disks.autoDelete` property to true in the instance template.

Giải thích tổng thể

A is incorrect because it is not the root cause of the issue. This is also a temporary solution. It suggests checking the syntax of the instance template and deleting any persistent disks with the same name as instance names. However, this does not address the issue of new instance creation failure on the managed instance group.

B is incorrect because it is not the root cause of the issue. It suggests checking the syntax of the instance template and verifying that the instance name and persistent disk name values are not the same in the template. While this could be a valid step to ensure proper instance creation, it does not address the issue of the failed instance creation on the managed instance group.

C is correct because we cannot update an existing template hence our best option is to create a new instance template and set `disks.autoDelete=true`. Also, we need to make a rolling update in order to switch to a new instance. It provides a sequence of steps to resolve the issue. It suggests creating a new instance template with a valid syntax, and setting the `disks.autoDelete` property to true, deleting existing persistent disks with the same name as instance names, and performing a rolling update to switch to the new template. This sequence of steps helps in resolving the issue and ensuring proper instance creation on the managed instance group.

NOTE: When auto-delete is on, the persistent disk is deleted when the instance it is attached to is deleted.

D is incorrect because we cannot delete an existing instance template when it's in use. We need a rolling update. It suggests creating a new instance template to replace the existing one and ensuring that the instance name and persistent disk name values are different in the template. However, it does not address the issue of new instance creation failure on the managed instance group or provide any steps to resolve the issue.

Links:

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

<https://cloud.google.com/sdk/gcloud/reference/compute/instances/set-disk-auto-delete>

How to update instance template:

https://cloud.google.com/compute/docs/instance-templates#how_to_update_instance_templates

How to update instance templates

Instance templates are designed to create instances with identical configurations. So you cannot update an existing instance template or change an instance template after you create it.

If you need to make changes to the configuration, [create a new instance template](#). You can create a template based on an existing instance template, or based on an existing instance. You can also [override instance template fields](#) when creating a VM instance from an instance template.

Câu hỏi 38Đã bỏ qua

You are part of the SRE team responsible for maintaining the site reliability for an e-commerce application in production on Compute Engine. You want to be proactive about monitoring the environment and want to be notified by email if the Compute Engine Instance's CPU utilization goes above 90%. What Google Services can you use to achieve this?

Note: Stackdriver is now called 'Google Cloud's Operation Suite'.

A.

1. Create a consumer Gmail account.
2. Write a script that uses GCP APIs to monitor CPU usage.
3. Have that script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server whenever the CPU utilization exceeds the threshold.

Correct answer

B.

1. Go to Stackdriver Monitoring and a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it.
2. Create a Cloud Monitoring Alerting Policy that uses the threshold as a trigger condition.
3. Configure your email address in the notification channel.

C.

1. Go to Stackdriver Monitoring and a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it.
 2. Write a script that uses GCP APIs to monitor the CPU usage and sends it as a custom metric to Cloud Monitoring.
 3. Create an uptime check for the instance in Cloud Monitoring.
- D.

1. Go to Cloud Logging and create a logs-based metric by using this regular expression: CPU Usage: ([0-9] {1,3})% to extract the CPU usage
2. Create an Alerting Policy in Cloud Monitoring based on this metric.
3. Configure your email address in the notification channel.

Giải thích tổng thể

A is incorrect because using consumer Gmail accounts for GCP is very difficult to manage and GSuite accounts are recommended. It involves creating a consumer Gmail account and writing a script to monitor CPU usage using GCP APIs. This approach is not recommended as it requires manual setup and maintenance of the script, and also relies on a consumer Gmail account for sending emails.

B is correct because Stackdriver Alerting gives timely awareness to problems in your cloud applications so you can resolve the problems quickly. It suggests using Stackdriver Monitoring and Cloud Monitoring Workspace to monitor the CPU utilization. By associating the GCP project with Stackdriver Monitoring, you can create a Cloud Monitoring Alerting Policy that triggers when the CPU utilization exceeds the threshold. The email notification can be configured with the desired email address.

C is incorrect because stackdriver supports alerting by email by default and does not require you to write a script. It also involves using Stackdriver Monitoring and a Cloud Monitoring Workspace but suggests sending the CPU usage as a custom metric to Cloud Monitoring. However, it does not mention creating an alerting policy or configuring email notifications for CPU utilization exceeding the threshold.

D is incorrect because the service required for monitoring the CPU is Stackdriver Monitoring and not logging. It suggests using Cloud Logging to create a logs-based metric for CPU usage. Although it creates an alerting policy based on this metric, it does not mention using Stackdriver Monitoring or Cloud Monitoring Workspace. Additionally, it does not specify how to configure email notifications for the alert.

Links:

<https://cloud.google.com/monitoring/alerts>

Note: Stackdriver is now called 'Google Cloud's Operation Suite'.

Câu hỏi 39 **Đã bỏ qua**

Your Online multi-player RPG game uses Cloud Spanner as its Database to store, update, and retrieve player points. The game receives traffic in a very predictable manner. How can you automatically scale up and scale down the number of Spanner nodes depending on traffic?

A.

1. Create a cron job that runs periodically and reviews Cloud Monitoring metrics

2. Then resizes the Spanner instance accordingly.

B.

1. Create a Cloud Monitoring alerting policy that sends an email alert to the oncall SRE team when Cloud Spanner CPU exceeds the threshold.

2. Ask the SREs to scale resources up or down accordingly.

C.

1. Create a Cloud Monitoring alerting policy that sends an alert to Google Cloud Support email when Cloud Spanner CPU exceeds the threshold.

2. Ask Google support to scale resources up or down accordingly.

Correct answer

D.

1. Create a Cloud Monitoring alerting policy that sends an alert to a webhook when the Cloud Spanner CPU is over or under the threshold.

2. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

Giải thích tổng thể

A is incorrect because a CRON job is not very effective as we want to scale up or down based on load and not periodically. It suggests using a cron job to periodically review Cloud Monitoring metrics and resize the Spanner instance accordingly.

However, this approach would not be able to dynamically scale the number of Spanner nodes based on real-time traffic. It would only allow for manual resizing based on periodic metric reviews.

B is incorrect because involving the SRE team increases the manual effort required in scaling up and down and since this process is repeatable, it should be automated if possible. It proposes creating a Cloud Monitoring alerting policy that sends an email alert to the oncall SRE team when Cloud Spanner CPU exceeds the threshold. While this would allow for manual scaling of resources up or down, it would require human intervention and may result in delays in responding to traffic changes.

C is incorrect because alerting Google Cloud support will not do anything as you have to maintain your infrastructure yourself. It suggests creating a Cloud Monitoring alerting policy that sends an alert to Google Cloud Support email when Cloud Spanner CPU exceeds the threshold. This approach would introduce additional steps and dependencies as it requires involving Google Cloud Support to manually scale the resources. It would not offer an automated and immediate response to changing traffic patterns.

D is correct because alerting policy is the most proactive approach to auto-scaling and a cloud function is a good candidate for the backend service responsible for scaling spanner nodes up or down. It recommends creating a Cloud Monitoring alerting policy that sends an alert to a webhook when the Cloud Spanner CPU is over or under the threshold. Additionally, it proposes creating a Cloud Function that listens to HTTP and automatically resizes the Spanner resources accordingly. This solution enables real-time scaling by utilizing automation and the capabilities of Cloud Functions to respond to alerts and trigger resizing actions. It eliminates the need for manual intervention and minimizes delays in scaling up or down based on traffic changes.

Links:

There's an official repository that does something similar to provide autoscaling to Cloud Spanner: <https://github.com/cloudspannerecosystem/autoscaler>

Câu hỏi 40 **Đã bỏ qua**

You have designed a PDF processing application that uses multiple GCP products. Your company's finance team has asked you to provide them with an estimate of the monthly cost of running the application. What should you do?

Correct answer

A.

1. Find out the pricing for each product in the solution by visiting its pricing page.

2. Use the pricing calculator to find out the total monthly costs for each Google Cloud product.

B.

1. Find out the pricing for each product in the solution by visiting its pricing page.

2. Create a Google Sheet that summarizes the expected monthly costs for each product.

C.

1. Provision the solution on Google Cloud for 1 week.

2. Visit the Billing Report page in the Cloud Console.

3. Multiply the 1-week cost to determine the monthly costs.

D.

1. Provision the solution on Google Cloud for 1 week.

2. Use Cloud Monitoring to determine the provisioned and used resource amounts.

3. Multiply the 1-week cost to determine the monthly costs.

Giải thích tổng thể

A is correct because the pricing calculator is the fastest and most accurate way to calculate pricing for GCP. It is the recommended approach for estimating the monthly cost of running the application. Option A suggests finding out the pricing for each product in the solution by visiting its pricing page, which allows the user to get accurate and up-to-date pricing information for each Google Cloud product. The pricing calculator can then be used to calculate the total monthly costs by inputting the usage details for each product. This approach ensures that the estimate is based on the specific usage and pricing of each product in the solution.

B is incorrect because a ready tool is available for pricing calculation and prices of cloud services change with time. It suggests creating a Google Sheet to summarize the expected monthly costs for each product. While creating a spreadsheet can be a useful tool for organizing and analyzing data, it may not provide accurate and up-to-date pricing information. This approach may require manually updating the

spreadsheet with any changes in pricing or usage, making it less reliable and potentially leading to inaccurate cost estimates.

C is incorrect because there is no need to keep the infrastructure provisioned and incur charges on it for calculating the price. It suggests provisioning the solution on Google Cloud for only 1 week and then multiplying the 1-week cost to determine the monthly costs. This approach may not provide an accurate estimate of the monthly costs as it is based on the usage and costs incurred for just 1 week. It does not take into account any variations in usage or costs that may occur over a longer period of time. Additionally, this approach may require repeatedly provisioning and de-provisioning the solution in order to get the cost estimate, which can be time-consuming and inconvenient.

D is incorrect because there is no need to keep the infrastructure provisioned and incur charges on it for calculating the price. It suggests provisioning the solution on Google Cloud for 1 week and using Cloud Monitoring to determine the provisioned and used resource amounts, and then multiplying the 1-week cost to determine the monthly costs. While using Cloud Monitoring can provide valuable insights into resource usage, it may not accurately reflect the usage and costs over a longer period of time. Similar to option C, this approach may require repeatedly provisioning and de-provisioning the solution in order to get the cost estimate, which can be inefficient and impractical.

Links:

<https://cloud.google.com/products/calculator>

Câu hỏi 41Đã bỏ qua

You are a software engineer at a startup. You have built an image search API service that is used by users from all over the world. The application receives SSL-encrypted TCP traffic on port 443. Which load balancing option should you use to minimize latency for the clients?

- A. HTTPS Load Balancer**
- B. Network Load Balancer**

Correct answer

- C. SSL Proxy Load Balancer**
- D. Internal TCP/UDP Load Balancer**

Giải thích tổng thể

A is incorrect because if the question mentioned 'HTTPS on 443' then A would be correct. But in this case, it is not. The HTTPS Load Balancer is designed for

HTTP/HTTPS traffic and not specifically for SSL-encrypted TCP traffic on port 443. It is more suitable for web applications where HTTP/HTTPS traffic needs to be load balanced.

B is incorrect because a Network load balancer is a generic type. The Network Load Balancer is designed for forwarding traffic at the Transport Layer (Layer 4) by operating at the connection level and routing traffic based on IP protocol data. It is not specifically designed for SSL-encrypted TCP traffic on port 443 and may not provide the same level of performance optimization for image search API service.

C is correct.

- SSL Proxy Load Balancing is a reverse proxy load balancer that distributes SSL traffic coming from the internet to virtual machine (VM) instances in your Google Cloud VPC network.

- Minimize latency for global users means SSL offloading close to those users while sending the traffic as much through the Google network as possible as opposed to over the internet. This means we need to use SSL Load Balancer.

- Moreover, SSL Proxy Load Balancing support for the following ports: 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, 3389, 5222, 5432, 5671, 5672, 5900, 5901, 6379, 8085, 8099, 9092, 9200, and 9300.

D is incorrect because we need external traffic and the internal load balancer is for internal traffic. The Internal TCP/UDP Load Balancer is designed for internal TCP/UDP traffic within a VPC network and not for SSL-encrypted TCP traffic over the internet. Furthermore, adding a firewall rule allowing ingress traffic from 0.0.0.0/0 on the target instances would open up the instances to all traffic and may not be secure or appropriate for the image search API service.

Links:

<https://cloud.google.com/load-balancing/docs/load-balancing-overview#types-of-cloud-load-balancing>

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

<https://tools.ietf.org/html/rfc2818>

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

Câu hỏi 42Đã bỏ qua

You work at a software solutions company and you have hosted your HRMS software on a general-purpose Compute Engine instance. Your application is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk. The disk size is currently 350 GB. The application primarily reads large files from disk. How can you provide a maximum amount of throughput with an optimal cost?

- A. Increase the size of the disk to 1 TB.**
- B. Increase the allocated CPU to the instance.**

Correct answer

- C. Use a Local SSD on the instance instead.**
- D. Use a Regional SSD on the instance instead.**

Giải thích tổng thể

A is incorrect because increasing the disk size will improve performance but it will increase the overall cost. Hence not recommended. Increasing the size of the disk will not necessarily improve the disk read throughput. The issue is with disk read throttling, not the disk capacity. Increasing the size of the disk may only provide more storage space but will not address the performance issue.

B is incorrect because increasing the CPU allocation does not affect disk IO performance. Increasing the allocated CPU to the instance will not directly impact the disk read throughput. The issue is with disk read throttling, not the CPU capacity. Increasing the CPU allocation may only help with CPU-intensive tasks but will not address the performance issue related to excessive disk read throttling.

C is correct

- Local SSD has more IOPS (Input/Output Operations Per Second). Moreover, SSD persistent disks are designed for single-digit millisecond latencies. Observed latency is application-specific.

- 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.

- Here are the calculations (taken from GCP when creating an instance):

350 Gb SSD Persistent disk: 59.50\$/month, read IOPS: 10 500 with n1-standard-1

1000 Gb SSD Persistent disk: 170.00\$/month, read IOPS: 15 000 with n1-standard-1

375 Gb Local SSD (NVMe): 30.00\$/month, read IOPS: 170 000 with n1-standard-1

These values prove that switching to a local SSD makes it cheaper and faster. Adding CPUs will make it more expensive than the old price.

D is incorrect because it will not improve performance. Using a Regional SSD on the instance will not necessarily address the excessive disk read throttling issue.

Regional SSDs are network-attached storage options that provide higher durability and availability but may not offer the same level of performance as Local SSDs.


Therefore, using a Regional SSD may not provide the maximum amount of throughput needed to optimize the cost and address the performance issue related to excessive disk read throttling.

Links:

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

<https://cloud.google.com/compute/docs/disks#performance>

Note: (Source: Google Docs)

 **Warning:** 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. For more information, see [Local SSD data persistence](#).

Câu hỏi 43Đã bỏ qua

One of your Machine Learning pipelines at your AI services company uses Dataproc. The Dataproc cluster runs in a single VPC network in a single subnet with range 10.0.2.0/25. The VPC network does not have any more private IP addresses left.

You need to add a few more VMs to communicate with the cluster. How can you do it with the minimum number of steps?

Correct answer

A. Modify the existing subnet range to 10.0.2.0/24.

B.

1. Add a new Secondary IP Range in the VPC.

2. Configure the VMs to use that range.

C.

1. Create a new VPC network.

2. Provision the VMs in the new VPC. Enable VPC Peering between the new VPC network and the Dataproc cluster VPC network.

D.

1. Create a new VPC network for the VMs with a subnet of 10.0.2.0/16.

2. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network.

3. Configure a custom Route exchange.

Giải thích tổng thể

A is correct because it is possible to increase the IP range of a subnet after creation. This option allows for expanding the available IP address range within the same VPC network, providing additional addresses for the new VMs. By modifying the subnet range from /25 to /24, the subnet size is increased, which allows for more IP addresses to be assigned. This can be done without the need to create additional VPC networks or establish VPC peering. We can increase the CIDR range with a minimum number of steps.

- `gcloud compute networks subnets expand-ip-range` expands the IP range of a VPC subnetwork.

B is incorrect because subnets can be expanded in size, there is no need to create a new subnet. Adding a new Secondary IP Range in the VPC and configuring the VMs to use that range would not solve the problem of running out of available private IP addresses in the subnet. The Secondary IP Range is used to assign additional IP addresses to existing VM instances within the same subnet, but it does not increase the total number of available private IP addresses in the subnet.

C is incorrect because there is no need to create a separate VPC for the VMs. Creating a new VPC network and provisioning the VMs in the new VPC network would require setting up VPC peering between the new VPC network and the existing Dataproc cluster VPC network. This would involve additional configuration and steps, which are not necessary to solve the problem of running out of available private IP addresses in the existing VPC network subnet.

D is incorrect because there is no need to create a separate VPC. Creating a new VPC network for the VMs with a subnet of 10.0.2.0/16 would result in a much larger address range than needed. This would consume more IP addresses than necessary and could potentially lead to IP address wastage. Additionally, VPC network peering and custom route exchange would add complexity and additional steps, which are not needed to solve the problem at hand.

Links:

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

Câu hỏi 44 **Đã bỏ qua**

Your startup recently got acquired by a large E-commerce company and it has significantly increased the traffic to your website. Your website is hosted on a custom Compute Engine instance. You need to create a copy of your VM to facilitate the increase in demand (NOTE: A custom image already exists). What should you do?

A.

1. Create a Compute Engine snapshot from the base VM.

2. Use the snapshot to create the images.

B.

1. Create a Compute Engine snapshot from the base VM.

2. Use the snapshot to create the instances.

C.

1. Create a Compute Engine snapshot from the base VM.

2. Create a custom Compute Engine image from this snapshot.

3. Use the image to create new images.

Correct answer

D.

1. Create a Compute Engine snapshot from the base VM.
2. Create a custom Compute Engine image from this snapshot.
3. Use the image to launch new instances.

Giải thích tổng thể

A is incorrect because we need to create a VM and not just its image. Creating a snapshot from the base VM would only create a backup of the VM disk and not a template that can be used to create new instances.

B is incorrect because even though it is possible to create a VM from a snapshot, usually snapshots are used for backup purposes, and images are used for scaling VMs. Using a snapshot to directly create instances would result in multiple instances with the same configuration and data, instead of creating a template that can be used to launch multiple instances.

C is incorrect because the option proposes creating a snapshot from the base VM and then creating a custom image from that snapshot. However, the subsequent use of the created image to "create new images" seems to be an incorrect step. It's not standard practice to directly create new images from an existing image in GCP. This will not be able to handle the increase in demand.

D is correct because this option follows a more standard and recommended process in GCP. It suggests creating a snapshot from the base VM, which captures the current state of the disk. From this snapshot, a custom image is created. This custom image serves as a template from which new instances can be launched. This method allows scalability by creating multiple instances from the custom image to handle the increased demand, aligning with best practices in GCP.

NOTE:

- In summary, an image is a template used to create new VM instances, while a snapshot is a copy of a persistent disk used for backup and recovery purposes. Images are used to create instances with the same configuration, while snapshots are used to create new disks or restore existing ones.
- Options A and B propose using snapshots directly to create images or instances, which isn't standard in GCP. Option C involves creating a custom image from a snapshot, which is valid, but the subsequent mention of "creating new images" could

be inaccurate. Option D, however, correctly suggests creating a custom image from a snapshot and then using instances from that image, aligning with recommended practices in GCP to handle increased demand.

Links:

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

Câu hỏi 45Đã bỏ qua

You are running a website to sell products made by local artisans on a single Compute Engine instance. Some of your users have reported that they are getting errors while using the application. The application writes logs to the disk. How can you diagnose the problem?

- A. View the application logs in Cloud Logging.
- B. Read the application logs by connecting to the instance's serial console.
- C. Create a Health Check for the instance with a Low Healthy Threshold value.

Correct answer

D. Install and configure the Cloud Logging Agent on the VM and view the logs from Cloud Logging.

Giải thích tổng thể

A is incorrect because VM logs don't show up in cloud logging by default. Viewing the application logs in Cloud Logging would require the application to send the logs to Cloud Logging. In this scenario, the application is writing logs to the disk and not sending them directly to Cloud Logging.

B is incorrect because reading the logs from the instance's serial console is not convenient and scalable. Reading the application logs by connecting to the instance's serial console would require manual intervention and may not provide real-time access to the logs. It is not an efficient or scalable solution for diagnosing problems with the application.

C is incorrect because setting up a health check does not enable logging automatically. Creating a Health Check for the instance with a Low Healthy Threshold value is used for monitoring the health and availability of the instance, not for diagnosing application errors or issues. It does not provide access to the application logs.

D is correct because the Cloud Logging agent needs to be installed in the VM so that the logs can be collected and sent to Cloud Logging for analysis. Installing and configuring the Cloud Logging Agent on the VM allows the application logs written to

the disk to be automatically collected and sent to Cloud Logging. This enables real-time access to the logs, making it easier to diagnose and troubleshoot any errors or issues with the application.

Links:

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

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

Câu hỏi 46 **Đã bỏ qua**

You work in the business intelligence engineering department in your company. You are collaborating with another team at your organization to build a Business Intelligence Dashboard for the directors of the company. The other team owns the data which they use to generate reports on a daily basis using a CRON job on a VM in a corp-data-analysis project. Your team is working on the frontend of the dashboard and they need a copy of the daily exports in the bucket corp-total-analysis-storage in the corp-total-analysis project. You are asked to configure access for the daily exports from the VM to be made available in the bucket corp-total-analysis-storage in as few steps as possible using Google's recommended practices. What should you do?

A. Move both projects under the same folder.

Correct answer

B. Assign Storage Object Creator to the VM Service Account on corp-total-analysis-storage.

C.

1. Create a Shared VPC network between both projects.

2. Assign the Storage Object Creator role to the VM Service Account on corp-data-analysis.

D.

1. Make the bucket corp-total-analysis-storage public and create a folder with a pseudo-randomized suffix name.

2. Share the folder with the IoT team.

Giải thích tổng thể

A is incorrect because moving the two projects requires migration efforts and it may not be possible. Moving both projects under the same folder is not necessary for

configuring access for the daily exports. It does not directly address the requirement of making the daily exports available in the bucket.

B is correct because granting the service account access to create objects in the other project is the fastest and the recommended way to achieve this. Assigning the Storage Object Creator role to the VM Service Account on corp-total-analysis-storage allows the VM to create and write objects (daily exports) to the specified bucket. This aligns with the requirement of making the daily exports available in the bucket.

C is incorrect because creating a VPC network between the two projects will not do anything as Cloud Storage is not part of the VPC. Creating a Shared VPC network between both projects and assigning the Storage Object Creator role to the VM Service Account on corp-data-analysis does not directly address the requirement of making the daily exports available in the specific bucket.

D is incorrect because making the bucket public is a security risk and should not be done. Making the bucket corp-total-analysis-storage public and sharing a folder with the IoT team is not the recommended approach for configuring access to the daily exports. It introduces potential security risks by making the data publicly accessible and involving additional teams that may not be relevant to the requirement.

Links:

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

Câu hỏi 47Đã bỏ qua

*You are building an API using Python. The API internally uses several Google Cloud Services using Application Default credentials. You have tested the API locally and it works correctly. As a next step, you want to deploy the API on a Compute Engine Instance. How can you set up authentication using Google-recommended practices and minimal changes?

Correct answer

A.

1. Provide necessary IAM permissions for Google services to the Compute Engine VM's service account.

B.

1. Create a new service account and provide it with appropriate IAM permissions

2. Configure the application to use this account.

C.

1. Create a config file containing the Service account credentials.

2. Deploy this config file with your application.

D.

1. Create a config file containing the User account credentials.

2. Deploy this config file with your application.

Giải thích tổng thể

A is correct because you can attach service accounts to resources for many different Google Cloud services, including Compute Engine, Google Kubernetes Engine, App Engine, Cloud Run, and Cloud Functions. We recommend using this strategy because it is more convenient and secure than manually passing credentials. It is recommended to provide necessary IAM permissions for Google services to the Compute Engine VM's service account. By granting the required IAM permissions to the service account, the API deployed on the Compute Engine Instance will have the necessary access to the Google Cloud services it needs to interact with.

B is incorrect because there is no need to create another service account. Creating a new service account and configuring the application to use this account would require additional changes and configurations to be made. It is not the minimal approach recommended by Google

C is incorrect because storing credentials in a config file is not safe and should be avoided. Creating a config file containing the Service account credentials and deploying it with the application would not be the recommended practice. Service account credentials should be managed and used securely, and deploying them with the application could expose sensitive information.

D is incorrect because storing credentials in a config file is not safe and should be avoided. Creating a config file containing the User account credentials and deploying it with the application is not recommended. User account credentials are not meant to be used by applications running on VM instances. The recommended practice is to use service account credentials for application authentication with Google Cloud services.

NOTE 1: Why Option-A is correct over Option-B

1. As per the question we need minimal changes and in Option-A we just need to provide the required IAM permissions to achieve this. **(Minimal changes)**

2. In Option-B we need to do multiple settings i.e. create a new service account, assign appropriate IAM permissions, and then configure it to suit our application needs (again this step requires multiple settings). I found Option-B to be tedious. **(NOT minimal changes)**

NOTE 2:

If we closely read Option-B it states that "..... configure the **application to use this account**".

We **never/don't** add a service account to the application. Instead, we always assign appropriate access for Google services to the service account. So there is no need to create a new service account.

[Option-A & Option-B are the mere play of words :)]

Hence, the most correct and appropriate answer is Option-A :)

Links:

<https://cloud.google.com/docs/authentication/production>

Random GCP Concept (optional read)

Google Kubernetes Engine (GKE) is a managed, production-ready environment for deploying containerized applications using Google Cloud infrastructure. Key features of GKE include automatic scaling, node auto-repair, and auto-upgrade functionalities, ensuring the Kubernetes clusters are always available, scalable, and up-to-date. GKE supports hybrid and multi-cloud deployments through its Anthos integration, offering flexibility in where applications are deployed. It also provides integrated logging and monitoring with Google Cloud operations (formerly Stackdriver) for enhanced visibility into the application's performance and health. Security is a priority with GKE, offering features like role-based access control (RBAC), Google-managed SSL certificates for load balancers, and integration with Google's security model. Moreover, GKE simplifies Kubernetes operations by providing a fully managed master node, network policies configuration, and built-in container networking.

Câu hỏi 48Đã bỏ qua

You are working at a steel company that aims to transform its digital processes by moving to the Google Cloud Platform. You have identified a monthly running Batch job (that takes 40 hours to complete) on your on-premises data center as a candidate for cloud migration. The job process can be performed offline, and it must be restarted if interrupted. What is the best approach for migrating this workload to GCP?

- A. Migrate the workload to a Compute Engine Preemptible VM.
- B. Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes.

Correct answer

C.

1. Migrate the workload to a Compute Engine VM.

2. Start and stop the instance as needed.

D.

1. Create an Instance Template with Preemptible VMs On.

2. Create a Managed Instance Group from the template and adjust Target CPU Utilization.

3. Migrate the workload.

Giải thích tổng thể

A is incorrect because a preemptible VM is not fit for long-running tasks as it can be terminated anytime. Migrating the workload to a Compute Engine Preemptible VM is not the best approach in this scenario. Preemptible VMs are primarily designed for short-lived, fault-tolerant workloads and may be terminated at any time without notice. Since the Batch job must be restarted if interrupted, using Preemptible VMs could result in data loss or inconsistent results.

B is incorrect because similar to Preemptible VMs, Preemptible nodes can be terminated at any time without notice. This can lead to the interruption of the Batch job and potential data loss or inconsistent results.

C is correct because migrating the workload to a standard Compute Engine VM and starting/stopping the instance as needed offer the most reliability and control for a long-running, offline batch job that requires 40 hours to complete and must be restarted if interrupted. Compute Engine VMs provide persistent, on-demand

compute capacity that can be tailored to the job's requirements, including custom machine types and the ability to stop and start the instance, thus optimizing costs when the resources are not in use. This approach avoids the risk of preemption and ensures that the job can run to completion without interruption, aligning with the workload's requirements.

D is incorrect because a preemptible VM is not fit for long-running tasks as it can be terminated anytime. Creating an Instance Template with Preemptible VMs and a Managed Instance Group might not be the best approach for this scenario. While it could provide some level of fault tolerance with the ability to automatically recreate terminated instances, it may not guarantee data integrity or consistent job execution if the instance is terminated before the workload is completed. Additionally, adjusting the Target CPU Utilization might not address the requirement of restarting the job if interrupted.

NOTE:

If the task is stopped it is needed to restart AND it takes 40 hours. Preemptible will stop in 24 hours and restart will happen which means JOB will never finish. Be it VM or K8s. Hence, the correct answer is C.

Links:

<https://cloud.google.com/compute/docs/instances/preemptible#testing-preemption-settings>

<https://cloud.google.com/compute/all-pricing>

<https://cloud.google.com/preemptible-vms>

Câu hỏi 49 **Đã bỏ qua**

Your team wants to experiment with CI/CD for their app using Jenkins on the Google Cloud Platform. What should you do to quickly and easily install Jenkins on GCP?

Correct answer

A. Deploy Jenkins through the Google Cloud Marketplace.

B.

1. Create a new Compute Engine instance.

2. Download the Jenkins Executable on the instance and run it.

C.

1. Create a new GKE cluster.

2. Use the Jenkins image to create a deployment.

D.

1. Use the Jenkins executable to create an instance template.

2. Use the template to create a managed instance group.

Giải thích tổng thể

A is correct because deploying Jenkins through the GCP marketplace is the best way to deploy Jenkins quickly. Deploying Jenkins through the Google Cloud Marketplace is the recommended and easiest method to install Jenkins on the Google Cloud Platform. It provides a simple and automated way to install and configure Jenkins with all the necessary dependencies and settings.

B is incorrect because it is not the fastest and most secure way. Manually downloading the Jenkins executable on a Compute Engine instance and running it can be time-consuming and may require additional configuration and setup steps. It does not utilize the built-in capabilities of the Google Cloud Platform for managing and scaling applications.

C is incorrect because it is not the fastest and most secure way. Creating a new GKE cluster and using the Jenkins image to create a deployment is more suitable for running Jenkins in a containerized environment using Kubernetes. While it provides advantages such as scalability and container orchestration, it may require additional configuration and setup for Jenkins to work correctly.

D is incorrect because it is not the fastest and most secure way. Using the Jenkins executable to create an instance template and managed instance group is not the recommended method for installing Jenkins on the Google Cloud Platform. It does not provide the automated deployment and management capabilities offered by other options like using the Google Cloud Marketplace or running Jenkins in a containerized environment.

Links:

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

Câu hỏi 50Đã bỏ qua

You are running a new-age business of commercial vehicle renting business. Sensors on the vehicles monitor signals like engine status, distance traveled, fuel level, and more. The customers are billed based on these metrics. The devices can emit a very high amount of data, up to thousands of events per hour per device. The system needs to store the individual signals atomically and data retrieval should be consistent based on the time of the event. What should you do?

A.

1. For every device, create a file in Cloud Storage.

2. Append new data to that file.

B.

1. For every device, create a file in Cloud Filestore.

2. Append new data to that file.

C.

1. Load the data into Datastore.

2. Create entity groups based on the device and store data in them.

Correct answer

D.

1. Load the data into Cloud Bigtable.

2. Use the event timestamp to create a row key based event.

Giải thích tổng thể

A is incorrect because Cloud Storage is not the right choice for such a high frequency of data. Creating a file in Cloud Storage for every device and appending new data to that file can quickly become inefficient and difficult to manage when dealing with a high amount of data. Cloud Storage is designed for storing and retrieving large, unstructured objects, not for atomic updates and consistent data retrieval based on event time.

B is incorrect because Cloud Firestore will not handle such a large amount of time-series data. Cloud Filestore is a managed file storage service for applications that require high-performance file storage. Similar to Cloud Storage, it is not designed for atomic updates and consistent data retrieval based on event time. It is more suitable for storing and accessing shared files in a network file system manner.

C is incorrect because Datastore is not the right choice for such a high frequency of data. Datastore (now known as Firestore) is a NoSQL document database. While it

can handle high read and write loads, it is not a good choice for atomic updates and consistent data retrieval based on event time. Entity groups can be used for data hierarchy, but it does not guarantee efficient and consistent queries based on event time.

D is correct because Cloud Bigtable is a petabyte-scale no-SQL database that is very good at storing and analyzing time-series data. Cloud Bigtable is a scalable, fully managed NoSQL wide-column database. It is designed for storing and retrieving large amounts of data with low latency. By using the event timestamp to create a row key, you can ensure consistent data retrieval based on event time. Bigtable can handle the high data ingestion rate and provide efficient queries for analyzing the signals from commercial vehicles.

Links:

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