Google Cloud

Professional Cloud Architect Sample Questions

The Cloud Architect sample questions will familiarize you with the format of exam questions and example content that may be covered on the exam.

The sample questions do not represent the range of topics or level of difficulty of questions presented on the exam. Performance on the sample questions should not be used to predict your Cloud Architect exam result.

Registration

First Name *

Hiroko

Last Name *

Yamaji

Primary Email *

hiroko@hirokoymj.com

Recovery Email

hiroko@hirokoymj.com

Organization (Employer or School) *

na

Organization email (an email associated with your current organization)

____

Country *

Japan ▾

Primary Relationship to Google *

Other ▾

Send me offers, updates and useful tips for getting the most out of Google Cloud training and certification products and services. *

No ▾

For this question, refer to the EHR Healthcare case study.
https://services.google.com/fh/files/blogs/master_case_study_ehr_healthcare.pdf

✕ Anonymous users from all over the world access a public health information website hosted in an on-premises EHR data center. The servers that host this website are older, and users are complaining about sluggish response times. There has also been a recent increase of distributed denial-of-service attacks toward the website. The attacks always come from the same IP address ranges. EHR management has identified the public health information website as an easy, low risk application to migrate to Google Cloud. You need to improve access latency and provide a security solution that will prevent the denial-of-service traffic from entering your Virtual Private Cloud (VPC) network. What should you do?

○ A. Deploy an external HTTP(S) load balancer, configure VPC firewall rules, and move the applications onto Compute Engine virtual machines.

○ B. Deploy an external HTTP(S) load balancer, configure Google Cloud Armor, and move the application onto Compute Engine virtual machines.

○ C. Containerize the application and move it into Google Kubernetes Engine (GKE). Create a GKE service to expose the pods within the cluster, and set up a GKE network policy.

● D. Containerize the application and move it into Google Kubernetes Engine (GKE). Create an internal load balancer to expose the pods outside the cluster, and configure Identity-Aware Proxy (IAP) for access. ✕

Correct answer

● B. Deploy an external HTTP(S) load balancer, configure Google Cloud Armor, and move the application onto Compute Engine virtual machines.

Feedback

A is not correct because firewall rules do not block malicious traffic into a VPC but rather block it at the VM level.

B is correct because the external HTTP(s) load balancer will improve access latency and Cloud Armor can be configured to block the Distributed Denial-of-Service (DDoS) attack.

C is not correct because a GKE service does not expose a set of pods outside of a cluster and a GKE network policy only filters traffic between pods and services.

D is not correct because a GKE internal load balancer will not load balance external traffic and anonymous users need access to the website so IAP is not a fit.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

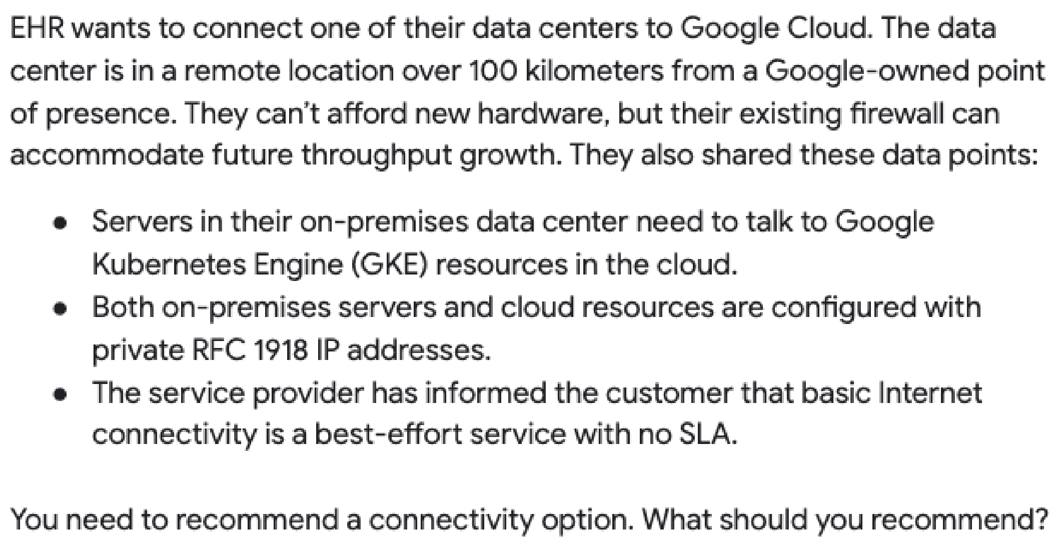
https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

For this question, refer to the EHR Healthcare case study.
https://services.google.com/fh/files/blogs/master_case_study_ehr_healthcare.pdf

✗



EHR wants to connect one of their data centers to Google Cloud. The data center is in a remote location over 100 kilometers from a Google-owned point of presence. They can't afford new hardware, but their existing firewall can accommodate future throughput growth. They also shared these data points:

- Servers in their on-premises data center need to talk to Google Kubernetes Engine (GKE) resources in the cloud.
- Both on-premises servers and cloud resources are configured with private RFC 1918 IP addresses.
- The service provider has informed the customer that basic Internet connectivity is a best-effort service with no SLA.

You need to recommend a connectivity option. What should you recommend?

○ A. Provision Carrier Peering.

○ B. Provision a new Internet connection.

○ C. Provision a Partner Interconnect connection.

● D. Provision a Dedicated Interconnect connection. ✗

Correct answer

● C. Provision a Partner Interconnect connection.

Feedback

A is not correct because it does not give private IP addressing across the connection.

B is not correct because an additional Internet connection will not provide RFC1918 communications by itself.

C is correct because it allows the customer to lower latency by connecting directly to a partner network that is directly connected to Google. This option will also allow the customer to use the lower bandwidth interfaces that they have on their current firewall.

D is not correct because Dedicated Interconnect would require the customer to buy new hardware to get a 10 gig interface for their firewall.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

For this question, refer to the EHR Healthcare case study.
https://services.google.com/fh/files/blogs/master_case_study_ehr_healthcare.pdf

✓ One of EHR's healthcare customers is an internationally renowned research and hospital facility. Many of their patients are well-known public personalities. Sources both inside and outside have tried many times to obtain health information on these patients for malicious purposes. The hospital requires that patient information stored in Cloud Storage buckets not leave the geographic areas in which the buckets are hosted. You need to ensure that information stored in Cloud Storage buckets in the "europe-west2" region does not leave that area. What should you do?

○ A. Encrypt the data in the application on-premises before the data is stored in the "europe-west2" region.

● B. Enable Virtual Private Cloud Service Controls, and create a service perimeter around the Cloud Storage resources. ✓

○ C. Assign the Identity and Access Management (IAM) "storage.objectViewer" role only to users and service accounts that need to use the data.

○ D. Create an access control list (ACL) that limits access to the bucket to authorized users only, and apply it to the buckets in the "europe-west2" region.

Feedback

A is not correct because encrypting the data does not stop data exfiltration.

B is correct because VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google Cloud services.

C is not correct because IAM roles deal with identity-based access control, not context-aware perimeter security.

D is not correct because Cloud Storage ACLs are a mechanism you can use to define who has access to your buckets and objects, as well as their level of access. ACLs do not stop data exfiltration.

https://cloud.google.com/...

https://cloud.google.com/...

For this question, refer to the EHR Healthcare case study.
https://services.google.com/fh/files/blogs/master_case_study_ehr_healthcare.pdf

✗ The EHR sales employees are a remote-based workforce that travels to different locations to do their jobs. Regardless of their location, the sales employees need to access web-based sales tools located in the EHR data center. EHR is retiring their current Virtual Private Network (VPN) infrastructure, and you need to move the web-based sales tools to a BeyondCorp access model. Each sales employee has a Google Workspace account and uses that account for single sign-on (SSO). What should you do?

○ A. Create an Identity-Aware Proxy (IAP) connector that points to the sales tool application.

○ B. Create a Google group for the sales tool application, and upgrade that group to a security group.

● C. Deploy an external HTTP(S) load balancer and create a custom Cloud Armor policy for the sales tool application. ✗

○ D. For every sales employee who needs access to the sales tool application, give their Google Workspace user account the predefined AppEngine Viewer role.

Correct answer

● A. Create an Identity-Aware Proxy (IAP) connector that points to the sales tool application.

Feedback

A is correct because Identity-Aware Proxy (IAP) connector allows you to manage access to HTTP-based apps outside of Google Cloud.

B is not correct because Google groups by themselves do not grant access to an application nor do they move an application to a beyond corp model.

C is not correct because Cloud Armor does not authenticate or authorize application access.

D is not correct because the application is installed in the datacenter, not in the AppEngine environment.

https://cloud.google.com/...

For this question, refer to the Mountkirk Games case study.
https://services.google.com/fh/files/blogs/master_case_study_mountkirk_games.pdf

✗ You are the data compliance officer for Mountkirk Games and must protect customers' personally identifiable information (PII). Mountkirk Games wants to make sure they can generate anonymized usage reports about their new game and delete PII data after a specific period of time. The solution should have minimal cost. You need to ensure compliance while meeting business and technical requirements. What should you do?

○ A. Archive audit logs in Cloud Storage, and manually generate reports.

● B. Write a Cloud Logging filter to export specific date ranges to Pub/Sub. ✗

○ C. Archive audit logs in BigQuery, and generate reports using Google Data Studio.

○ D. Archive user logs on a locally attached persistent disk, and cat them to a text file for auditing.

Correct answer

● C. Archive audit logs in BigQuery, and generate reports using Google Data Studio.

Feedback

A is not correct because Cloud Storage is an object store with no query language access for report generation.

B is not correct because it does not address log storage for data retention.

C is correct because BigQuery allows easy querying for report generation, with low storage costs.

D is not correct because long term storage in persistent disks is expensive.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

For this question, refer to the Mountkirk Games case study.
https://services.google.com/fh/files/blogs/master_case_study_mountkirk_games.pdf

✗ Mountkirk Games wants you to make sure their new gaming platform is being operated according to Google best practices. You want to verify that Google-recommended security best practices are being met while also providing the operations teams with the metrics they need. What should you do? (Choose two)

☑ A. Ensure that you aren’t running privileged containers. ✓

☑ B. Ensure that you are using obfuscated Tags on workloads. ✗

□ C. Ensure that you are using the native logging mechanisms.

□ D. Ensure that workloads are not using securityContext to run as a group.

□ E. Ensure that each cluster is running GKE metering so each team can be charged for their usage.

Correct answer

☑ A. Ensure that you aren’t running privileged containers.

☑ C. Ensure that you are using the native logging mechanisms.

Feedback

A is correct because this is High Priority according to Google best practices.

B is not correct because tags should be readable and useful to the operations teams when they are working on the clusters.

C is correct because this is High Priority according to Google best practices.

D is not correct because this may be required for some workloads.

E is not correct because although from a business process this may be useful it won’t impact the operations or security of the cluster.

https://cloud.google.com/...

For this question, refer to the Mountkirk Games case study.
https://services.google.com/fh/files/blogs/master_case_study_mountkirk_games.pdf

✗ You need to implement Virtual Private Cloud (VPC) Service Controls for Mountkirk Games. Mountkirk Games wants to allow Cloud Shell usage by its developers. Developers should not have full access to managed services. You need to balance these conflicting goals with Mountkirk Games' business requirements. What should you do?

○ A. Use VPC Service Controls for the entire platform.

○ B. Prioritize VPC Service Controls implementation over Cloud Shell usage for the entire platform.

● C. Include all developers in an access level associated with the service perimeter, and allow them to use Cloud Shell. ✗

○ D. Create a service perimeter around only the projects that handle sensitive data, and do not grant your developers access to it.

Correct answer

● D. Create a service perimeter around only the projects that handle sensitive data, and do not grant your developers access to it.

Feedback

A is not correct because VPC Service Controls do not directly affect scaling of Google Cloud architecture.

B is not correct because a security perimeter is not a business requirement, but rapid iteration is.

C is not correct because it works but does not scale, and we do not want to give users this much access.

D is correct because VPC Service Controls protects data, and Cloud Shell facilitates rapid iteration of Google Cloud architecture changes.

https://cloud.google.com/...

https://cloud.google.com/...

For this question, refer to the Mountkirk Games case study.
https://services.google.com/fh/files/blogs/master_case_study_mountkirk_games.pdf

✗ Your new game running on Google Cloud is in public beta, and you want to design meaningful service level objectives (SLOs) before the game becomes generally available. What should you do?

● A. Define one SLO as 99.9% game server availability. Define the other SLO as less than 100-ms latency. ✗

○ B. Define one SLO as service availability that is the same as Google Cloud's availability. Define the other SLO as 100-ms latency.

○ C. Define one SLO as 99% HTTP requests return the 2xx status code. Define the other SLO as 99% requests return within 100 ms.

○ D. Define one SLO as total uptime of the game server within a week. Define the other SLO as the mean response time of all HTTP requests that are less than 100 ms.

Correct answer

● C. Define one SLO as 99% HTTP requests return the 2xx status code. Define the other SLO as 99% requests return within 100 ms.

Feedback

A is incorrect because it doesn't clearly define how to measure both the availability and latency.

B is incorrect because Google Cloud availability has an impact on customer availability but it is only one factor. Also, for different Google Cloud products, the availability could be different.

C is correct because it clearly defines the service level indicators and how to measure them.

D is incorrect because there is no objective for the server uptime.

https://landing.google.co...

For this question, refer to the Helicopter Racing League (HRL) case study. https://services.google.com/fh/files/blogs/master_case_study_helicopter_racing_league.pdf

✓ HRL wants you to help them bring existing recorded video content to new fans in emerging regions. Considering the HRL business and technical requirements, what should you do?

○ A. Serve the video content directly from a multi-region Cloud Storage bucket.

● B. Use Cloud CDN to cache the video content from HRL's existing public cloud provider. ✓

○ C. Use Apigee Edge to cache the video content from HRL's existing public cloud provider.

○ D. Replicate the video content in Google Kubernetes Engine clusters in regions close to the fans.

Feedback

A is not correct because a multi-region bucket does not serve all global areas with similar latency.

B is correct because Cloud CDN can be used to cache data hosted on other cloud providers and supports large objects such as video.

C is not correct because Apigee Edge is not designed to cache data larger than 512 KB.

D is not correct because replicating the video content introduces unnecessary complexity.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://docs.apigee.com/...

https://cloud.google.com/...

For this question, refer to the TerramEarth case study.
https://services.google.com/fh/files/blogs/master_case_study_terramearth.pdf

✓ You are the data compliance officer for TerramEarth and must protect customers' personally identifiable information (PII), like credit card information. TerramEarth wants to personalize product recommendations for its large industrial customers. You need to respect data privacy and deliver a solution. What should you do?

○ A. Use AutoML to provide data to the recommendation service.

○ B. Process PII data on-premises to keep the private information more secure.

● C. Use the Cloud Data Loss Prevention (DLP) API to provide data to the recommendation service. ✓

○ D. Manually build, train, and test machine learning models to provide product recommendations anonymously.

Feedback

A is not correct because AutoML does not inherently provide data de-identification.

B is not correct because TerramEarth's requirements are to go into the cloud, not stay on-premises.

C is correct because Cloud DLP was specifically designed for this use case.

D is not correct because developing machine learning models is an excessive way to de-identify data.

https://cloud.google.com/…

https://cloud.google.com/…

✓ You are designing a future-proof hybrid environment that will require network connectivity between Google Cloud and your on-premises environment. You want to ensure that the Google Cloud environment you are designing is compatible with your on-premises networking environment. What should you do?

○ A. Use the default VPC in your Google Cloud project. Use a Cloud VPN connection between your on-premises environment and Google Cloud.

○ B. Create a custom VPC in Google Cloud in auto mode. Use a Cloud VPN connection between your on-premises environment and Google Cloud.

○ C. Create a network plan for your VPC in Google Cloud that uses CIDR ranges that overlap with your on-premises environment. Use a Cloud Interconnect connection between your on-premises environment and Google Cloud.

● D. Create a network plan for your VPC in Google Cloud that uses non-overlapping CIDR ranges with your on-premises environment. Use a Cloud Interconnect connection between your on-premises environment and Google Cloud. ✓

Feedback

A is not correct because the default VPC is a VPC with Auto Mode IP ranges, which has the same problem as answer C.

B is not correct because with Auto Mode IP Ranges there is no guarantee that the IP ranges will not overlap with your on premises environment, either now or in the future.

C is not correct because to ensure correct routing, ranges cannot overlap between environments.

D is correct because this ensures your on premises network is compatible with your Google Cloud VPC.

https://cloud.google.com/…

✓ Your company wants to track whether someone is present in a meeting room reserved for a scheduled meeting. There are 1000 meeting rooms across 5 offices on 3 continents. Each room is equipped with a motion sensor that reports its status every second. You want to support the data ingestion needs of this sensor network. The receiving infrastructure needs to account for the possibility that the devices may have inconsistent connectivity. Which solution should you design?

○ A. Have each device create a persistent connection to a Compute Engine instance and write messages to a custom application.

○ B. Have devices poll for connectivity to Cloud SQL and insert the latest messages on a regular interval to a device specific table.

● C. Have devices poll for connectivity to Pub/Sub and publish the latest messages on a regular interval to a shared topic for all devices. ✓

○ D. Have devices create a persistent connection to an App Engine application fronted by Cloud Endpoints, which ingest messages and write them to Datastore.

Feedback

A is not correct because having a persistent connection does not handle the case where the device is disconnected.

B is not correct because Cloud SQL is a regional, relational database and not the best fit for sensor data. Additionally, the frequency of the writes has the potential to exceed the supported number of concurrent connections.

C is correct because Pub/Sub can handle the frequency of this data, and consumers of the data can pull from the shared topic for further processing.

D is not correct because having a persistent connection does not handle the case where the device is disconnected.

https://cloud.google.com/…

https://cloud.google.com/…

✓ Your company wants to try out the cloud with low risk. They want to archive approximately 100 TB of their log data to the cloud and test the serverless analytics features available to them there, while also retaining that data as a long-term disaster recovery backup. Which two steps should they take? (Choose two)

☑ A. Load logs into BigQuery. ✓

□ B. Load logs into Cloud SQL.

□ C. Import logs into Cloud Logging.

□ D. Insert logs into Cloud Bigtable.

☑ E. Upload log files into Cloud Storage. ✓

Feedback

A is correct because BigQuery is a serverless cloud data warehouse for analytics and supports the volume and analytics requirement.

B is not correct because Cloud SQL does not support the expected 100 TB. Additionally, Cloud SQL is a relational database and not the best fit for time-series log data formats.

C is not correct because Cloud Logging is optimized for monitoring, error reporting, and debugging instead of analytics queries.

D is not correct because Cloud Bigtable is optimized for read-write latency and analytics throughput, not analytics querying and reporting.

E is correct because Cloud Storage provides the Coldline and Archive storage classes to support long-term storage with infrequent access, which would support the long-term disaster recovery backup requirement.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✓ You set up an autoscaling managed instance group to serve web traffic for an upcoming launch. After configuring the instance group as a backend service to an HTTP(S) load balancer, you notice that virtual machine (VM) instances are being terminated and re-launched every minute. The instances do not have a public IP address. You have verified that the appropriate web response is coming from each instance using the curl command. You want to ensure that the backend is configured correctly. What should you do?

○ A. Ensure that a firewall rule exists to allow source traffic on HTTP/HTTPS to reach the load balancer.

○ B. Assign a public IP to each instance, and configure a firewall rule to allow the load balancer to reach the instance public IP.

● C. Ensure that a firewall rule exists to allow load balancer health checks to reach the instances in the instance group. ✓

○ D. Create a tag on each instance with the name of the load balancer. Configure a firewall rule with the name of the load balancer as the source and the instance tag as the destination.

Feedback

A is not correct because the issue to resolve is the VMs being terminated, not access to the load balancer.

B is not correct because this introduces a security vulnerability without addressing the primary concern of the VM termination.

C is correct because health check failures lead to a VM being marked unhealthy and can result in termination if the health check continues to fail. Because you have already verified that the instances are functioning properly, the next step would be to determine why the health check is continuously failing.

D is not correct because the source of the firewall rule that allows load balancer and health check access to instances is defined IP ranges, and not a named load balancer. Tagging the instances for the purpose of firewall rules is appropriate but would probably be a descriptor of the application, and not the load balancer.

https://cloud.google.com/…

https://cloud.google.com/…

✗ Your organization has a 3-tier web application deployed in the same Google Cloud Virtual Private Cloud (VPC). Each tier (web, API, and database) scales independently of the others. Network traffic should flow through the web to the API tier, and then on to the database tier. Traffic should not flow between the web and the database tier. How should you configure the network with minimal steps?

○ A. Add each tier to a different subnetwork.

○ B. Set up software-based firewalls on individual VMs.

● C. Add tags to each tier and set up routes to allow the desired traffic flow. ✗

○ D. Add tags to each tier and set up firewall rules to allow the desired traffic flow.

Correct answer

● D. Add tags to each tier and set up firewall rules to allow the desired traffic flow.

Feedback

A is not correct because the subnetwork alone will not allow and restrict traffic as required without firewall rules.

B is not correct because this adds complexity to the architecture and the instance configuration.

C is not correct because routes still require firewall rules to allow traffic as requests. Additionally, the tags are used for defining the instances the route applies to, and not for identifying the next hop. The next hop is either an IP range or instance name, but in the proposed solution the tiers are only identified by tags.

D is correct because as instances scale, they will all have the same tag to identify the tier. These tags can then be leveraged in firewall rules to allow and restrict traffic as required, because tags can be used for both the target and source.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✓ You are designing a large distributed application with 30 microservices. Each of your distributed microservices needs to connect to a database backend. You want to store the credentials securely. Where should you store the credentials?

○ A. In the source code

○ B. In an environment variable

● C. In a secret management system ✓

○ D. In a config file that has restricted access through ACLs

Feedback

A is not correct because storing credentials in source code and source control is discoverable, in plain text, by anyone with access to the source code. This also introduces the requirement to update code and do a deployment each time the credentials are rotated.

B is not correct because consistently populating environment variables would require the credentials to be available, in plain text, when the session is started.

C is correct because a secret management system such as Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud.

D is not correct because instead of managing access to the config file and updating manually as keys are rotated, it would be better to leverage a key management system. Additionally, there is increased risk if the config file contains the credentials in plain text.

https://cloud.google.com/...

https://cloud.google.com/...

✓ Your customer is moving their corporate applications to Google Cloud. The security team wants detailed visibility of all resources in the organization. You use Resource Manager to set yourself up as the Organization Administrator. Which Identity and Access Management (IAM) roles should you give to the security team while following Google recommended practices?

○ A. Organization viewer, Project owner

● B. Organization viewer, Project viewer ✓

○ C. Organization administrator, Project browser

○ D. Project owner, Network administrator

Feedback

A is not correct because Project owner is too broad. The security team does not need to be able to make changes to projects.

B is correct because:
- Organization viewer grants the security team permissions to view the organization's display name.
- Project viewer grants the security team permissions to see the resources within projects.

C is not correct because Organization Administrator is too broad. The security team does not need to be able to make changes to the organization.

D is not correct because Project Owner is too broad. The security team does not need to be able to make changes to projects.

https://cloud.google.com/...

✓ To reduce costs, the Director of Engineering has required all developers to move their development infrastructure resources from on-premises virtual machines (VMs) to Google Cloud. These resources go through multiple start/stop events during the day and require state to persist. You have been asked to design the process of running a development environment in Google Cloud while providing cost visibility to the finance department. Which two steps should you take? (Choose two)

☑ A. Use persistent disks to store the state. Start and stop the VM as needed. ✓

□ B. Use the "gcloud --auto-delete" flag on all persistent disks before stopping the VM.

□ C. Apply VM CPU utilization label and include it in the BigQuery billing export.

☑ D. Use BigQuery billing export and labels to relate cost to groups. ✓

□ E. Store all state in a Local SSD, snapshot the persistent disks, and terminate the VM.

Feedback

A is correct because persistent disks will not be deleted when an instance is stopped.

B is not correct because the --auto-delete flag has no effect unless the instance is deleted. Stopping an instance does not delete the instance or the attached persistent disks.

C is not correct because labels are used to organize instances, not to monitor metrics.

D is correct because exporting daily usage and cost estimates automatically throughout the day to a BigQuery dataset is a good way of providing visibility to the finance department. Labels can then be used to group the costs based on team or cost center.

E is not correct because the state stored in local SSDs will be lost when the instance is stopped.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✓ The database administration team has asked you to help them improve the performance of their new database server running on Compute Engine. The database is used for importing and normalizing the company's performance statistics. It is built with MySQL running on Debian Linux. They have an n1-standard-8 virtual machine with 80 GB of SSD zonal persistent disk which they can't restart until the next maintenance event. What should they change to get better performance from this system as soon as possible and in a cost-effective manner?

○ A. Increase the virtual machine's memory to 64 GB.

○ B. Create a new virtual machine running PostgreSQL.

● C. Dynamically resize the SSD persistent disk to 500 GB. ✓

○ D. Migrate their performance metrics warehouse to BigQuery.

Feedback

A is not correct because increasing the memory size requires a VM restart.

B is not correct because the DB administration team is requesting help with their MySQL instance. Migration to a different product should not be the solution when other optimization techniques can still be applied first.

C is correct because persistent disk performance is based on the total persistent disk capacity attached to an instance and the number of vCPUs that the instance has. Incrementing the persistent disk capacity will increment its throughput and IOPS, which in turn improve the performance of MySQL.

D is not correct because the DB administration team is requesting help with their MySQL instance. Migration to a different product should not be the solution when other optimization techniques can still be applied first.

https://cloud.google.com/...   https://cloud.google.com/...