

Learn from Home | Flat 50% OFF SITEWIDE | Use Coupon - WHIZSITE50



[Home](#) > My Courses > Google Cloud Certified Professional Cloud Architect > Practice Test I > Report

Search Courses



Practice Test I

Completed on 26-July-2020



Congratulations, you passed. Keep it up



Attempt

01



Marks Obtained

44 / 50



Your score

88%



Time Taken

N/A



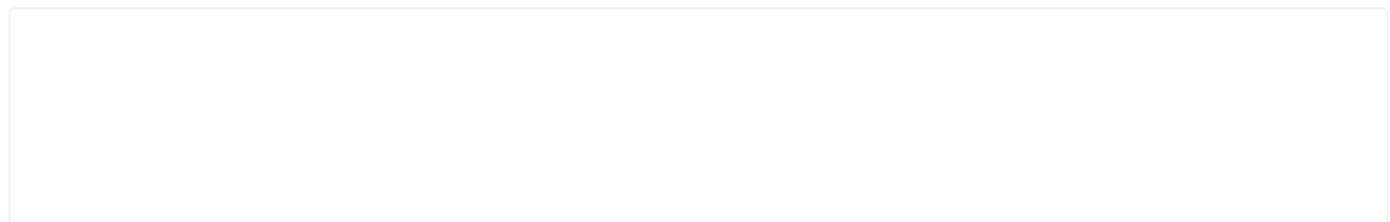
Result

Congratulations! Passed

Share your Result with your friends



Domains wise Quiz Performance Report



No	1
Domain	Other
Total Question	50
Correct	44
Incorrect	6
Unattempted	0
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	50
Correct	44
Incorrect	6
Unattempted	0
Marked for review	0

Review the Answers

Sorting by

All

Question 1

Correct

Domain : Other

For this question, refer to the [Dress4Win](#) case study.

You want to ensure Dress4Win's sales and tax records remain available for infrequent viewing by auditors for at least 10 years. Cost optimization is your top priority. Which cloud services should you choose?

- A. Google Bigtable with US or EU as location to store the data, and gcloud to access the data.
- B. BigQuery to store the data, and a web server cluster in a managed instance group to access the data. Google Cloud SQL mirrored across two distinct regions to store the data, and a Redis cluster in a managed instance group to access the data.
- C. Google Cloud Storage Nearline to store the data, and gsutil to access the data.
- ✓ D. Google Cloud Storage Coldline to store the data, and gsutil to access the data.

Explanation:

Correct Answer D

Feedback

A and B are not suitable for this type of task "infrequent viewing by auditors for at least 10 years" and they are not cost-effective, either

D (Correct answer) - "for infrequent viewing by auditors" and "for at least 10 years" fit the usage pattern for Coldline and qualify Answer D for meeting the requirements "Cost optimization is your top priority" due to its lowest storage cost.

Explanation

This is about chose storage solution for backup or archieving, depending the required access frequency which in turn impact the cost, you have the option between Nearline and Coldline

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

Storage solutions for any workload



High-performance object storage

Backup and archival storage

HIGH FREQUENCY ACCESS



Multi-Regional

Most projects start with Multi-regional Storage, which is optimized for **geo redundancy** and **end-user latency**



Regional

Use Regional Storage when your project requires **higher performance local access** to computing resources - for example, when you need to support **high-frequency analytics workloads**.

LOW FREQUENCY ACCESS



Nearline

Nearline Storage is fast, highly durable storage for data accessed less than **once a month**.

LOWEST FREQUENCY ACCESS



Coldline

Coldline Storage is fast, highly durable storage for data accessed less than **once a year**.

Ask our Experts

Rate this Question?

[View Queries](#)

open

Question 2

Correct

Domain : Other

For this question, refer to the [Mountkirk Games](#) case study.

Mountkirk Games has deployed their new backend on Google Cloud Platform (GCP). You want to create a thorough testing process for new versions of the backend before they are released to the public. You want the testing environment to scale in an economical way.

How should you design the process?

- ✓ A. Create a scalable environment in GCP for simulating production load.
- B. Build stress tests into each component of your application using resources internal to GCP to simulate load.
- C. Use the existing infrastructure to test the GCP-based backend at scale.
- D. Create a set of static environments in GCP to test different levels of load – for example, high, medium, and low.

Explanation:

Correct Answer A

Feedback

A (Correct answer) – Create a scalable environment in GCP for simulating production load.

With this disposable and repeatable testing resources, you can do load test whenever needed. Shutdown or stop the services or simplify delete and recreate it based on the test plans, to keep the cost low.

It meets the requirements "create a thorough testing process for new versions of the backend before they are released to the public" and "testing environment to scale in an economical way". Doing thorough testing on production infrastructure is risky to other running application, not feasible, not scale in economical way.

B – Build stress tests into each component of your application using resources internal to GCP to simulate load.

This is not scale nor economical and too complicated to implement.

C – Use the existing infrastructure to test the GCP-based backend at scale.

At first glance, reuse exiting environments so it'll be scalable, economical, and in the real situation. If we read the case study again, we know that Mountkirk games is a popular game platform targeting to global users with very high traffic and heavy load. Doing a load test on the production is no longer an option, nor is it necessarily a scale in an economical way if you mix the production and testing load. Comparing to the solution creating disposable and reputable testing environment simulating production load and execute test plans on demanding, Answer A is the winner.

D – Create a set of static environments in GCP to test different levels of load – for example, high, medium, and low.

This is nor scale nor economical

[Ask our Experts](#)Rate this Question?  [View Queries](#)open 

Question 3

Correct

Domain : Other

You have been asked to select the storage system for the click-data of your company's large portfolio of websites. This data is streamed in from a custom website analytics package at a typical rate of 6,000 clicks per minute, with bursts of up to 8,500 clicks per second. It must be stored for future analysis by your data science and user experience teams.

Which storage infrastructure should you choose?

- A. Google cloud Datastore
- B. Google Cloud SQL
- C. Google Cloud Bigtable 
- D. Google Cloud Storage

Explanation:

Correct Answer C

Feedback

A - Google cloud Datastore. Doesn't meet this requirement "It must be stored for future analysis by your data science and user experience teams." Google Cloud Datastore is a NoSQL document database built for automatic scaling, high performance, and ease of application development and integrating well with App Engine.

Datastore: A scalable, fully-managed NoSQL document database for your web and mobile applications.

Good for:

Semi-structured application data

Hierarchical data

Durable key-value data

Workload:

User profiles

Product catalogs

Game state

B - Google Cloud SQL. Cloud SQL is mainly for OLTP (Transactional, CRUD) not for taking and storing streaming data. It does not have the scalability and elasticity to absorb this amount of data in real time.

C (Correct Answer) - Google Cloud Bigtable. The reason is that data is in IoT nature and it will be used for analytics.

Bigtable: A scalable, fully-managed NoSQL wide-column database that is suitable for both real-time access and analytics workloads. Bigtable is ideal for very large NoSQL datasets and is useful for high-speed transactions and analysis. It integrates well with ML, Dataproc, and analytics

Good for

Low-latency read/write access

High-throughput analytics

Native time series support

Work load

IoT, finance, adtech

Personalization, recommendations

Monitoring

Geospatial datasets

Graphs

Although both Datastore and Bigtable are NoSQL databases, Bigtable is able to support over a petabyte of data and is useful for high speed analytics as well, whereas Datastore is not.

D - Google Cloud Storage. GCS is ideally for Object storage purpose although it has pretty good scalability. It's not suitable for IoT kind of spiky streaming data. Its buckets initially support roughly 1000 writes per second and then scale as needed. As the request rate for a given bucket grows, Cloud

Storage automatically increases the IO capacity for that bucket by distributing the request load across multiple servers. Especially considering the click stream rate of 6,000 clicks per minute, with bursts of up to 8,500 clicks per second, the way GCS handle and absorb this kind high and low data stream by scale up and down make it not suitable for this task.

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 4

Correct

Domain : Other

Over time, you've created 5 snapshots of a single instance. To save space, you delete snapshots number 3 and 4. What has happened to the fifth snapshot?

- A. The data from both snapshots 3 and 4 necessary for continuance are transferred to snapshot 5. 
- B. It is no longer useable and cannot restore data.
- C. All later snapshots, including 5, are automatically deleted as well.
- D. The data from snapshot 4 necessary for continuance was transferred to snapshot 5, however snapshot 3's contents were transferred to snapshot 2.

Explanation:

Correct Answer A

Explanation

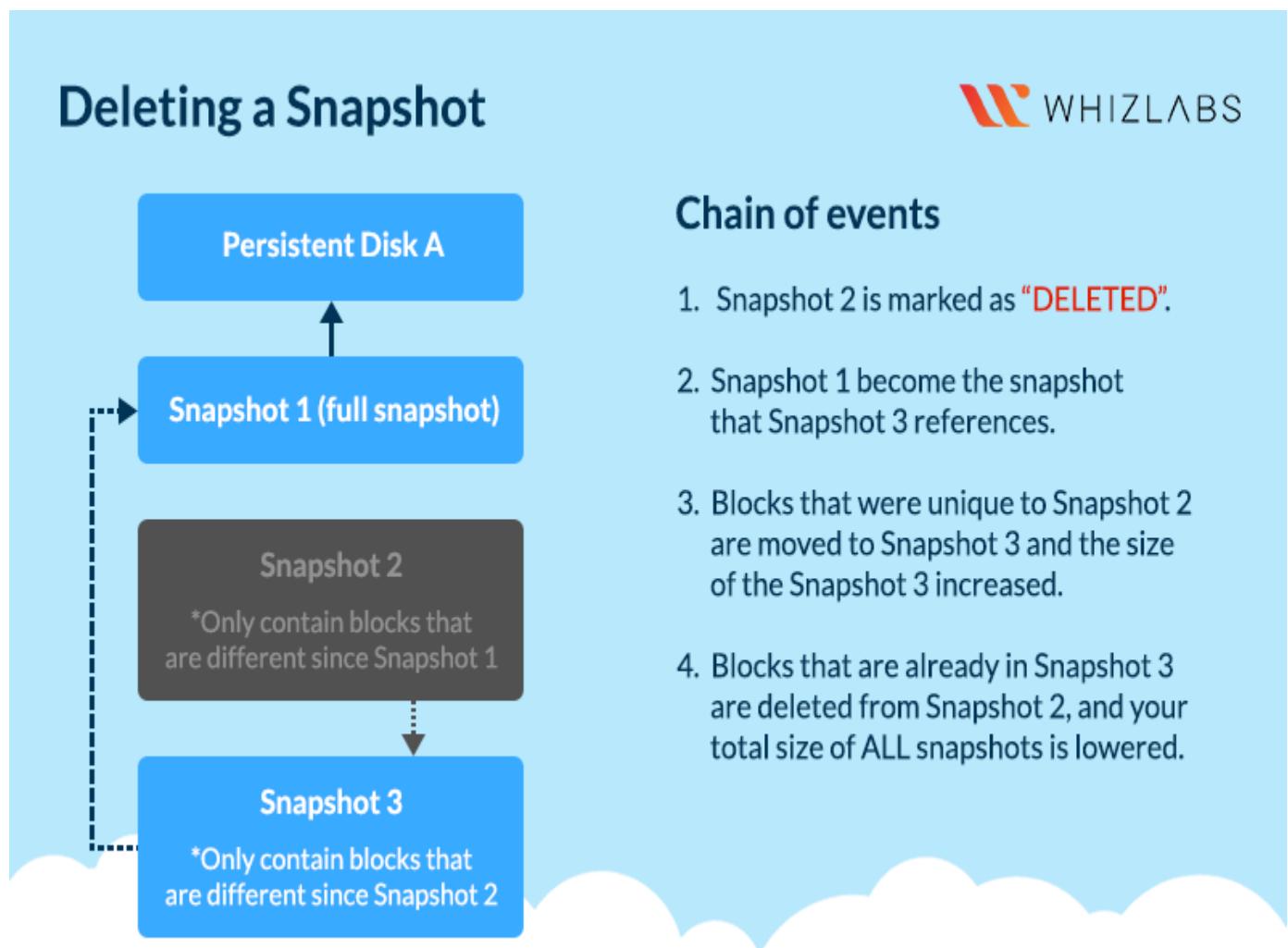
Deleting a snapshot: <https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots>

When you delete a snapshot, Compute Engine immediately marks the snapshot as DELETED in the system. If the snapshot has no dependent snapshots, it is deleted outright. However, if the snapshot does have dependent snapshots:

- 1) Any data that is required for restoring other snapshots is moved into the next snapshot, increasing its size.
- 2) Any data that is not required for restoring other snapshots is deleted. This lowers the total size of all your snapshots.
- 3) The next snapshot no longer references the snapshot marked for deletion, and instead references the snapshot before it.

Because subsequent snapshots might require information stored in a previous snapshot, keep in mind that deleting a snapshot does not necessarily delete all the data on the snapshot. As mentioned in the first bullet above, if any data on a snapshot that is marked for deletion is needed for restoring subsequent snapshots, that data is moved into the next corresponding snapshot. To definitively delete data from your snapshots, you should delete all snapshots.

The diagram below illustrates the process described above:



[Ask our Experts](#)Rate this Question?  [View Queries](#)open 

Question 5

Incorrect

Domain : Other

A small number of API requests to your microservices-based application take a very long time. You know that each request to the API can traverse many services. You want to know which service takes the longest in those cases. What should you do?

- A. Set timeouts on your application so that you can fail requests faster.
- B. Instrument your application with StackDriver Trace to break down the request latencies at each microservice. 
- ✓ C. Send custom metrics for each of your requests to Stackdriver Monitoring. 
- D. Use Stackdriver Monitoring to look for insights that show when your API latencies are high.

Explanation:

Correct Answer B

Explanation

A - Set timeouts on your application so that you can fail requests faster - This won't be able to tell you directly where the bottleneck is.

B (Correct Answer) - Instrument your application with StackDriver Trace to break down the request latencies at each microservice. This is exactly StackDriver Trace comes to play.

C - Send custom metrics for each of your requests to Stackdriver Monitoring – without knowing where the bottleneck is beforehand, it's not easy, if not impossible, to setup custom metrics to capture the latency causes. Besides, the question itself is about to find where the latency/bottleneck exists.

D - Use Stackdriver Monitoring to look for insights that show when your API latencies are high – this could tell you when the API call latency reaching to certain threshold/criteria but can hardly tell

where the root causes is without additional setup and analysis.

Reference Resources

Stackdriver Trace can help you answer the following questions:

<https://cloud.google.com/trace/docs/overview>

- How long does it take my application to handle a given request?
- Why is it taking my application so long to handle a request?
- Why do some of my requests take longer than others?
- What is the overall latency of requests to my application?
- Has latency for my application increased or decreased over time?
- What can I do to reduce application latency?

"As micro-services become more popular, the cross-application tracing provided by Stackdriver Trace becomes essential in pinpointing the root cause of latency issues."

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 6

Correct

Domain : Other

One of your clients is using customer –managed encryption, which of the following statements are true when you are applying customer-managed encryption key to an object.[Select any 3]

- ✓ A. the encryption key is used to encrypt the object's data 
- ✓ B. the encryption key is used to encrypt the object's CRC32C checksum 
- C. the encryption key is used to encrypt the object's name
- ✓ D. the encryption key is used to encrypt the object's MD5 hash 

Explanation:

Answer: Option A, B, D are the CORRECT choice because, When you apply a customer-managed encryption key to an object, the encryption key is used to encrypt the object, its CRC32C checksum, and its MD5 hash. The remaining **metadata** for the object, including the object's name, is encrypted using standard server-side keys. This allows you to always read and update metadata, as well as list and delete objects, provided you have **permission** to do so.

<https://cloud.google.com/storage/docs/encryption/customer-managed-keys>

Ask our Experts

Rate this Question?  

View Queries

open 

Question 7

Correct

Domain : Other

For this question, refer to the **TerramEarth** case study.

TerramEarth's 20 million vehicles are scattered around the world. Based on the vehicle's location its telemetry data is stored in a Google Cloud Storage (GCS) regional bucket (US, Europe, or Asia). The CTO has asked you to run a report on the raw telemetry data to determine why vehicles are breaking down after 100 K miles. You want to run this job on all the data. What is the most cost-effective way to run this job?

- ✓ A. Launch a cluster in each region to preprocess and compress the raw data, then move the data into a regional bucket and use a Cloud Dataproc cluster to finish the job. 
- B. Move all the data into 1 region, then launch a Google Cloud Dataproc cluster to run the job.
- C. Launch a cluster in each region to preprocess and compress the raw data, then move the data into a multi-region bucket and use a Dataproc cluster to finish the job.
- D. Move all the data into 1 zone, then launch a Cloud Dataproc cluster to run the job.

Explanation:

The correct answer is Option A.

A (Correct answer) - Launch a cluster in each region to preprocess and compress the raw data, then move the data into a regional bucket and use a Cloud Dataproc cluster to finish the job.

Since the raw data are saved based on the vehicle's location all over the world, most likely they'll scatter in many different regions and eventually they need to move to a centralized location for final processing.

Preprocessing raw data and compressing them from each location to reduce the size so to save the between-region data egress cost.

Dataproc is Zone-specific resources and since you want to run this job on all data and you or your group probably are the only consumers for the data, moving the data into a regional bucket same or closest to the DataProc cluster zone's region for final analysis is most cost effective.

Use a regional location to help optimize latency, availability, and network bandwidth for data consumers grouped in the same region.

Use a multi-regional location when you want to serve content to data consumers that are outside of the Google network and distributed across large geographic areas.

- Store frequently accessed data, or data that needs to be geo-redundant as Multi-Regional Storage.

B - Move all the data into 1 region, then launch a Google Cloud Dataproc cluster to run the job.

Since the raw data are save based on the vehicles' location all over the world, moving them to a centralized region without preprocessing and compressing would incur additional between-region data egress cost

C - Launch a cluster in each region to preprocess and compress the raw data, then move the data into a multi-region bucket and use a Dataproc cluster to finish the job.

Dataproc is Zone-specific resources and since you want to run this job on all data and data consumption occurs in a centralized location, then moving the data into a multi-region bucket for Dataproc cluster jobs is not most cost effective.

Use a multi-regional location when you want to serve content to data consumers that are outside of the Google network and distributed across large geographic areas.

- Store frequently accessed data, or data that needs to be geo-redundant as Multi-Regional Storage.

D - Move all the data into 1 zone, then launch a Cloud Dataproc cluster to run the job. GCS is either Regional or Multi-Regional not Zonal Resources

[Ask our Experts](#)Rate this Question?  [View Queries](#)open 

Question 8

Correct

Domain : Other

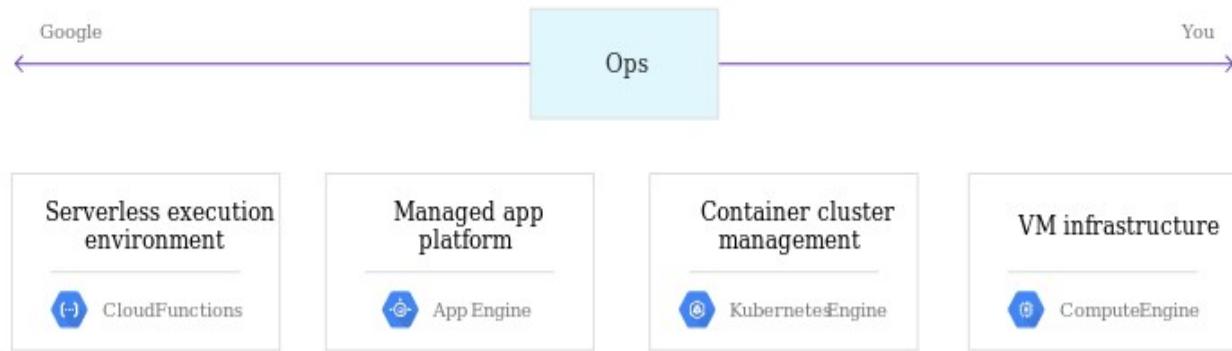
Your company just finished a rapid lift and shift to Google Compute Engine for your compute needs. You have another 9 months to design and deploy a more cloud-native solution. The business team is looking for services with lesser responsibility and easy manageability. Please select the order of services with lesser responsibility to more responsibility

- A. Google Container Engine with containers > Google App Engine Standard Environment >Cloud Functions >Compute Engine with containers >Compute Engine
- B. Cloud Functions >Google App Engine Standard Environment>Google Container Engine with containers >Compute Engine with containers > Compute Engine 
- C. Cloud Functions >Google Container Engine with containers >Google App Engine Standard Environment >Compute Engine >Compute Engine with containers
- D. Google App Engine Standard Environment > Cloud Functions>Compute Engine with containers>Google Container Engine with containers>Compute Engine

Explanation:

Answer: B is the CORRECT choice, Cloud Functions is the least no-Ops, then App Engine, then followed by Google Container Engine with containers(kubernetes) and then Compute Engine with containers and at last Compute Engine.

You can imagine a spectrum where, at one end, you have most of the responsibilities for resource management and, at the other end, Google has most of those responsibilities:



Ask our Experts

Rate this Question?

[View Queries](#)

open

Question 9

Correct

Domain : Other

Your company's test suite is a custom C++ application that runs tests throughout each day on Linux virtual machines. The full test suite takes several hours to complete, running on a limited number of on premises servers reserved for testing. Your company wants to move the testing infrastructure to the cloud, to reduce the amount of time it takes to fully test a change to the system, while changing the tests as little as possible. Which cloud infrastructure should you recommend?

- A. Google Cloud Dataproc to run Apache Hadoop jobs to process each test
- B. Google App Engine with Google Stackdriver for logging
- C. Google Compute Engine managed instance groups with auto-scaling
- D. Google Compute Engine unmanaged instance groups and Network Load Balancer

Explanation:

Correct Answer C

Feedback

A - Google Cloud Dataproc to run Apache Hadoop jobs to process each test

Apache Hadoop runs Java not C++; If the questions meant to use Hadoop to manage and process the test, it's overkill and also need significant changes to the testing infrastructure to integrate with Dataproc.

B - Google App Engine with Google Stackdriver for logging

App Engine did not natively support C++, also it's probably hard to port their "runs tests throughout each day on Linux virtual machines" to App Engine "while changing the tests as little as possible"; StackDriver logging won't help porting the test to GCP, either.

Between C and D, the main difference is managed or unmanaged instance group

Unmanaged instance groups are groups of dissimilar instances that you can arbitrarily add and remove from the group. Unmanaged instance groups do not offer autoscaling, rolling update support, or the use of instance templates so Google recommends creating managed instance groups whenever possible. Use unmanaged instance groups only if you need to apply load balancing to your pre-existing configurations or to groups of dissimilar instances.

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

From the question there is no such requirement for unmanaged instance group and not mention that dissimilar Linux machine types are required.

In addition, judging from what they suffered "The full test suite takes several hours to complete, running on a limited number of on-premises servers", it seems they simply need more computation power – bigger and/or more instances for the testing. So the managed instance group with autoscaling is the preferred.

Ask our Experts

Rate this Question?  

View Queries

open 

Question 10

Correct

For this question refer to the [TerramEarth](#) case study

Operational parameters such as oil pressure are adjustable on each of TerramEarth's vehicles to increase their efficiency, depending on their environmental conditions. Your primary goal is to increase the operating efficiency of all 20 million cellular and unconnected vehicles in the field. How can you accomplish this goal?

Select one:

- A. Have your engineers inspect the data for patterns, and then create an algorithm with rules that make operational adjustments automatically.
- B. Implement a Google Cloud Dataflow streaming job with a sliding window and use Google Cloud Messaging (GCM) to make operational adjustments automatically.
- C. Capture all operating data, train machine learning models that identify ideal operations, and host in Google Cloud Machine Learning (ML) Platform to make operational adjustments automatically.
- D. Capture all operating data, train machine learning models that identify ideal operations, and run locally to make operational adjustments automatically.



Explanation:

Correct Answer D

Feedback

A - Have your engineers inspect the data for patterns, and then create an algorithm with rules that make operational adjustments automatically.

This won't work – the engineer simply won't be able just to inspect the data for patterns for 20 million vehicles whether the algorithm created run local or in-cloud

B - Implement a Google Cloud Dataflow streaming job with a sliding window and use Google Cloud Messaging (GCM) to make operational adjustments automatically.

Without data analytics and machine learning, the two technologies just won't create meaningful algorithm for operational adjustments automatically. Besides, majority (99%) of the 20M vehicles are unconnected and the two technologies have to run on GCP for scalability so there is no way to communicate between local and GCP for adjustments automatically.

C - Capture all operating data, train machine learning models that identify ideal operations, and host in Google Cloud Machine Learning (ML) Platform to make operational adjustments automatically.

Again, majority (99%) of the 20M vehicles are unconnected and if the trained model was host in Google Cloud Machine Learning (ML) Platform then there is no way to use the model generated parameters to command the field vehicles to make operational adjustments automatically.

D (Correct Answer) - Capture all operating data, train machine learning models that identify ideal operations, and run locally to make operational adjustments automatically.

After creating good ML model by "Capture all operating data, train machine learning models that identify ideal operations", you can run the model in the vehicle to make operational adjustments automatically based on each specific vehicle's parameters. Probably run the model in the onboard computer or computer connected to the maintenance port.

TerramEarth connection related Information in the Case Study

There are 20 million TerramEarth vehicles in operation that collect 120 fields of data per second. Data is stored locally on the vehicle and can be accessed for analysis when a vehicle is serviced. The data is downloaded via a maintenance port. This same port can be used to adjust operational parameters, allowing the vehicles to be upgraded in the field with new computing modules.

Approximately 200,000 vehicles are connected to a cellular network, allowing TerramEarth to collect data directly.

Ask our Experts

Rate this Question?  

View Queries

open 

Question 11

Correct

Domain : Other

You need to regularly create disk level backups of the root disk of a critical instance. These backups need to be able to be converted into new instances that can be used in different projects. How should you do this? Select 2 possible way to accomplish this.

- A. Create snapshots, turn the snapshot into a custom image, and share the image across projects. 

- B. Use the VM migration tools in Compute Engine to copy a VM to a different project.
- ✓ C. Create snapshots and share them to other projects. 
- D. Stream your VM's data into Cloud Storage and share the exported data in the storage bucket with another project.

Explanation:

Correct Answers: A and C

Explanation

B – is for migration not for "regularly create disk level backups of the root disk of a critical instance". There are tools allowing copying (importing) on-premises virtual disk to Compute engine but you cannot copy GCP VM.

C(Correct Answer) - Sharing storage resources across projects and organizations

You can share access to images, disks, and snapshots using the following IAM roles or permissions:

Images: The **roles/compute.imageUser** role or the **compute.images.useReadOnly** permission.

Snapshots: The **roles/compute.storageAdmin** role or the **compute.snapshots.useReadOnly** permission.

Disks: The **roles/compute.storageAdmin** role or the **compute.disks.useReadOnly** permission.

These roles and permissions allow you to share each resource type independently with other team members outside of your projects. For example, your company might have a specific project with qualified images that the rest of your company can use. You can assign a group to the project that is explicitly responsible for creating and maintaining images. Then, you can grant the **roles/compute.imageUser** role to other team members so that team members can use these images in their own projects.

Note: These roles allows users to use your storage resources in any project, including projects outside of your organization. To restrict image use to specific organizations or specific projects, **set the 'constraints/compute.storageResourceUseRestrictions' constraint** as an organization policy

<https://cloud.google.com/compute/docs/images/sharing-images-across-projects>

A (Correct answer) - The proper method is to create a custom image either from an existing, stopped instance, or snapshots of a boot disk, which can then be shared across projects and used to create additional instances.

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

D- doesn't meet the requirement "regularly create disk level backups of the root disk of a critical instance" nor is it easy to convert into new instance.

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 12

Correct

Domain : Other

Your company has decided to build a backup replica of their on-premises user authentication PostgreSQL database on Google Cloud Platform. The database is 4 TB, and large updates are frequent. Replication requires RFC1918 private address space. Which networking approach would be the best choice?

- A. Create two VPN tunnels within the same Cloud VPN gateway to the same destination VPN gateway.
- B. Direct Peering.
- C. Google Cloud Dedicated Interconnect or Google Cloud Partner Interconnect 
- D. Google Cloud VPN connected to the data center network.

Explanation:

The correct answer is Option C.

Option C is correct - Google Cloud Dedicated Interconnect or Google Cloud partner Interconnect

Both VPN and Dedicated Interconnect/Partner Interconnect provide private address space communication. 'The database is 4 TB, and large updates are frequent' makes the Dedicated Interconnect/Partner Interconnect a suitable solution due to its bandwidth capability and SLA

A single interconnect can be a single 10G link or a link bundle, connected to a single Google router

Option D is incorrect because Google Cloud VPN connected to the data center network

Option A is incorrect because you cannot create two VPN tunnels within the same Cloud VPN gateway to the same destination VPN gateway.

Option B is incorrect because Direct Peering exists outside of the Google Cloud Platform.

INTERCONNECT	PEERING
Direct access to RFC1918 IPs in your VPC – with SLA	Access to Google public IPs only – without SLA
Includes: <ul style="list-style-type: none"> • Dedicated Interconnect • Partner Interconnect • IPsec VPN 	Includes: <ul style="list-style-type: none"> • Direct Peering • Carrier Peering

<https://cloud.google.com/hybrid-connectivity/>

Dedicated Interconnect Overview:

<https://cloud.google.com/interconnect/docs/concepts/dedicated-overview>

Ask our Experts

Rate this Question?  

View Queries

open 

Question 13

Correct

Domain : Other

One of your clients are storing highly sensitive data on Google Cloud Storage, they strictly adhere to their compliance, hence they do not want their keys to be stored in a cloud, please suggest them the right choice of encryption.

- ✓ A. You provide a raw CSEK as part of an API call 

- B. All objects on Google Storage are encrypted by default hence additional encryption isn't required
 - C. Give your Cloud Storage service account access to an encryption key, that service account encrypts
 - D. Google recommends the usage of cloud KMS for storing CMEK.
-

Explanation:

The correct answer is Option A.

Option A is the correct choice because the client doesn't want to store the encryption keys on Google Cloud. Supplying your own encryption key is best suited in this scenario. Google uses your key to protect the Google-generated keys used to encrypt and decrypt your data.

Option B is incorrect because, even though All objects on Google Storage are encrypted by default, the client is storing sensitive data and hence default encryption isn't the best option.

<https://cloud.google.com/security/encryption-at-rest/>

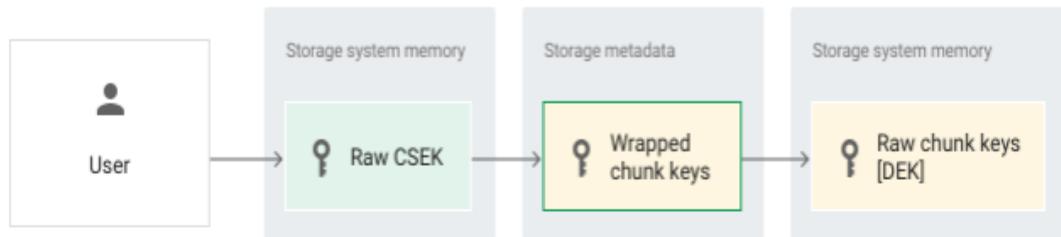
Option C is incorrect because giving your Cloud Storage service account access to an encryption key, that service account encrypts comes under Customer-Managed Encryption Keys, these keys are stored in Google cloud, hence not the correct choice here.

Option D is incorrect because in customer-managed encryption key, your encryption keys are stored within Cloud KMS. The client doesn't want to store keys on the Cloud.

When you use Customer-Supplied Encryption Keys in Cloud Storage

You provide a raw CSEK as part of an API call. This key is transmitted from the Google front end to the storage system's memory. This key is used as the key encryption key in Google Cloud Storage for your data.

The raw CSEK is used to unwrap wrapped chunk keys, to create raw chunk keys in memory. These are used to decrypt data chunks stored in the storage systems. These keys are used as the data encryption keys (DEK) in Google Cloud Storage for your data.



Key(s)	Stored in	Purpose	Accessible until
Raw CSEK	Storage system memory	Provided by the customer. <i>Key encryption key (KEK)</i> for chunk keys. Wraps the chunk keys.	Customer-requested operation (e.g., <code>insertObject</code> or <code>getObject</code>) is complete
Wrapped chunk keys	Storage devices	Protect chunk keys stored at rest	Storage object is deleted
Raw chunk keys	Storage devices' memory	<i>Data encryption key (DEK)</i> for the data. Read/write data to the disk.	Customer-requested operation is complete

Reference:

<https://cloud.google.com/storage/docs/encryption/customer-managed-keys>

Ask our Experts

Rate this Question?

[View Queries](#)

open

Question 14

Correct

Domain : Other

You are using DataFlow to ingest a large amount of data and later you send the data to Bigquery for Analysis, but you realize the data is dirty, what would be the best choice to use to clean the data in stream with serverless approach?

- A. Fetch data from Bigquery and clean data from DataPrep and send it back to Bigquery

- Fetch the data from Bigquery and create one more pipeline, clean data from
✓ B. DataFlow and send it back to Bigquery 

Fetch the data from Bigquery and clean data from DataProc and send it back to
C. Bigquery

D. Send the data to Data Storage and use BigTable to clean the data.

Explanation:

Answer: Option B is CORRECT because Data Flow can be used to customize the data cleaning process unlike in Data Prep. Using Data Flow, it would involve coding when correcting errors, omissions, or inconsistencies. Also It ask for the data in stream with serverless approach.

Option A is INCORRECT because DataPrep is one of the options to clean the data. But the functionalities of DataPrep is limited and doesn't provide customized rules for data cleaning process. DataFlow provides customizable data cleaning process. Question asks for the best choice and hence DataFlow.

Option C is INCORRECT because Cloud Dataproc is a fully-managed cloud service for running Apache Spark and Apache Hadoop clusters not for cleaning data.

Option D is INCORRECT because Cloud Bigtable is Google's NoSQL Big Data database service it is not used to clean data.

Google Doc and Explanation:

Google has given an example of this problem.

Please refer to <https://cloud.google.com/community/tutorials/data-science-preprocessing>

Cleaning data in a data processing pipeline

Author(s): [@jerjou](#) Published: May 22, 2017

Google Cloud Platform Community tutorials submitted from the community do not represent official Google Cloud Platform product documentation.

When gathering information from the real world, the data will often contain errors, omissions, or inconsistencies that should be corrected before you can analyze it effectively. Instead of doing it by hand, or performing a separate cleansing step, [Google Cloud Dataflow](#) allows you to define simple functions that can cleanse your data in a pipeline, which you can plug into your data ingestion pipeline for automatic cleansing.

In this tutorial, you'll write functions to perform various data cleansing tasks, which you'll then string together into a pipeline to be run in series on [Cloud Dataflow](#). Note that you could also plug arbitrary functions - such as those from the [data extraction](#) tutorial - into this pipeline as well. We leave as an exercise for the reader.

For this example, you'll define a series of simple filters on a sample dirty dataset. The dataset used in this tutorial is [Meteorite Landing data](#) from [data.gov](#), which catalogs, among other things, the location and year of all known meteorite landings. You'll run the following filters on the raw json data:

Filtering out records without location or year filled in

Converting the strings into their native types

Removing redundant and bad data

You'll then tie all the filters together in a pipeline that can be run both locally (for ease of experimentation, and for small datasets), and on the [Google Cloud Dataflow](#) service, for large datasets and streaming datasets that are continuously being updated. To accomplish this, you'll add a function for sourcing the data, and one for saving it:

Chunk the json array into its individual elements

Save the results in a queryable format

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 15

Correct

Domain : Other

You have a long-running job that one of your employees has permissions to start. You don't want that job to be terminated when the employee who last started that job leaves the company. What would be the best way to address the concern in this scenario?

A. Create many IAMusers and give them the permission.

- ✓ B. Create a service account. Grant the Service Account User permission to the employees who needs to start the job. Also, provide "Compute Instance Admin" permission to that service account.



- C. Give full permissions to the Service Account and give permission to the employee to access this service account.
- D. Use Google-managed service accounts in this scenario.

Explanation:

Answer: Option B is the CORRECT because, creating service accounts for each service with only the permissions required for that service is the best practice, even if the employee leaves the organization other employees can use the service account .

Option A is INCORRECT because Service Account is used to give permission to Application or VMs.

A service account is a special type of Google account that belongs to your application or a virtual machine (VM), instead of to an individual end user. Your application assumes the identity of the service account to call Google APIs so that the users aren't directly involved. With Admin access, the employees will be able to create Compute Engine instances which runs the service account, connect to them, and use the service account to start the job. So in nutshell, admin empowers to effectively run code as the service accounts used to run these instances, and indirectly gain access to all the resources for which the service accounts has access.

Option C is INCORRECT because Granting the service account only the minimum set of permissions required to achieve their goal is the best practice.

Option D is INCORRECT because Google Managed service accounts are created and owned by Google. These accounts represent different Google services and each account is automatically granted IAM roles to access your GCP project. This service account is designed specifically to run internal Google processes on your behalf and is not listed in the Service Accounts section of GCP Console.

More reading at <https://cloud.google.com/iam/docs/understanding-service-accounts>

Ask our Experts

Rate this Question?  

View Queries

open 

Question 16

Correct

Domain : Other

You have created several preemptible Linux virtual machine instances using Google Compute Engine. You want to properly shut down your application before the virtual machines are preempted. What

should you do?

- A. Create a shutdown script registered as a xinetd service in Linux and configure a StackDriver endpoint check to call the service.
- B. Create a shutdown script, registered as a xinetd service in Linux, and use the gcloud compute instances add-metadata command to specify the service URL as the value for a new metadata entry with the key shutdown-script-url
- C. Create a shutdown script named k99.shutdown in the /etc/rc.6.d/ directory.
- ✓ D. Create a shutdown script and use it as the value for a new metadata entry with the key shutdown-script in the Cloud Platform Console when you create the new virtual machine instance. 

Explanation:

Correct Answer D

Feedback

Running Shutdown Scripts: Create and run shutdown scripts that execute commands right before an instance is terminated or restarted, on a best-effort basis. This is useful if you rely on automated scripts to start up and shut down instances, allowing instances time to clean up or perform tasks, such as exporting logs, or syncing with other systems.

<https://cloud.google.com/compute/docs/shutdownscript>

To setup Shutdown Scripts, go to GCP console and follow the steps:

Compute Engine -> VM instance -> Create Instance -> (Expand) Management, disks, networking, SSH keys

Enter the key "shutdown-script" and proper value

Metadata (Optional)

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. [Learn more](#)

Key	Value	X
-----	-------	---

[Ask our Experts](#)Rate this Question?  [View Queries](#)

open ▾

Question 17

Correct

Domain : Other

You need to allow traffic from specific virtual machines in 'subnet-a' network access to machines in 'subnet-b' without giving the entirety of subnet-a access. How can you accomplish this?

- ✓ A. Create a firewall rule to allow traffic from resources with specific network tags, then assign the machines in subnet-a the same tags. 
- B. Relocate the subnet-a machines to a different subnet and give the new subnet the needed access.
- C. Create a rule to deny all traffic to the entire subnet, then create a second rule with higher priority giving access to tagged VM's in subnet-a.
- D. You can only grant firewall access to an entire subnet and not individual VM's inside.

Explanation:

Correct Answer A

A (Correct answer) - Create a firewall rule to allow traffic from resources with specific network tags, then assign the machines in subnet-a the same tags.

Network tags allow more granular access based on individually tagged instances - Instances by target tags: The firewall rule is applicable only to VMs if they have a matching network tag.

B - Relocate the subnet-a machines to a different subnet and give the new subnet the needed access.

This would give the entire subnet access which is against the requirements: allow traffic from specific virtual machines in 'subnet-a' network access to machines in 'subnet-b' without giving the entirety of subnet-a access.

C - Create a rule to deny all traffic to the entire subnet, then create a second rule with higher priority giving access to tagged VM's in subnet-a.

Creating overlapping rules with higher priority might technically work, but since traffic defaults to denied if no rule is in place, this is unnecessary. Assigning rules and instances by tags is the best answer.

D - You can only grant firewall access to an entire subnet and not individual VM's inside.

This is not true per answer A

Ask our Experts

Rate this Question?

[View Queries](#)

open ▾

Question 18

Correct

Domain : Other

A news feed web service has the following code running on Google App Engine. During peak load, users report that they can see news articles they already viewed. What is the most likely cause of this problem?

```
1. import news
2. from flask import Flask, redirect, request
3. from flask.ext.api import status
4. from google.appengine.apl import users

5. app = Flask (__name__)
6. sessions = {}
7. @app. Route ("/")
8. def homepage () :
9.     user = users.get current_user ()
10.    if not user:
11.        return "Invalid login", Status.HTTP_401_UNAUTHORIZED
12.    if user not in sessions:
13.        sessions [user] = {"viewed": []}

14. news_articles = news.get_new_news (user, sessions [user] {"viewed"})
15. sessions [user] {"viewed"} += [n["Id"] for n in news_articles]

16. return news, render (news_articles)

17. if __name__ == "__main__":
18.     app.run()
```

- ✓ A. The session variable is local to just a single instance. 
 - B. The session variable is being overwritten in Cloud Datastore.
 - C. The URL of the API needs to be modified to prevent caching.
 - D. The HTTP Expires header needs to be set to -1 to stop caching.
-

Explanation:

Correct Answer : A

Answer A is the correct – The session variable is local to just a single instance.

The question described “users report that they can see news articles they already viewed”, which means the correct behavior is, user should only be able to read article they did not reviewed before.

Here is how:

Line 6 declared new session variable: sessions = {}, initially is empty

Then the code somehow gets the all user, and somehow get the article

Line 13, 14, 15: basically, save the article(s) the current specific user viewed in session variable. The sessions variable is key value pair data type, key is “viewed”, value is a list VIEWED [article 1, article 2...]. Of course, if THE user just started or never viewed any article, the list would be empty

Remember that session variable host list articles only if they viewed by that user.

Then you deploy and run the app in AppEngine. “During peak load” most likely means you have many instances run the same codebase independently from each other. If a user hit instance #9, read an article A, then made another request, most likely he'd hit another instance, say #1000. The session variable in the code running in instance #1000 would not have had that information and the article A might be displayed again treated as not viewed before.

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 19

Correct

One of the microservices in your application has an intermittent performance problem. You have not observed the problem when it occurs but when it does, it triggers a particular burst of log lines. You want to debug a machine while the problem is occurring. What should you do?

- A. Log into one of the machines running the microservice and wait for the log storm.
- B. In the Stackdriver Error Reporting dashboard, look for a pattern in the times the problem occurs.
- C. Configure your microservice to send traces to Stackdriver Trace so you can find what is taking so long.
- D. Set up a log metric in Stackdriver Logging, and then set up an alert to notify you when the number of log lines increases past a threshold. 

Explanation:

Correct Answer D

Feedback

D (Correct Answer) - Since you know that there is a burst of log lines you can set up a metric that identifies those lines. Stackdriver will also allow you to set up a text, email or messaging alert that can notify promptly when the error is detected so you can hop onto the system to debug.

A - Logging into an individual machine may not see the specific performance problem as multiple machines may be in the configuration and reducing the chances of interacting with an intermittent performance problem.

B - Error reporting won't necessarily catch the log lines unless they are stack traces in the proper format. Additionally, just because there is a pattern doesn't mean you will know exactly when and where to log in to debug.

C - Trace may tell you where time is being spent but won't let you know in on the exact host that the problem is occurring on because you generally only send samples of traces. There is also no alerting on traces to notify exactly when the problem is happening.

Additional Resource

<https://cloud.google.com/logging/docs/logs-based-metrics/>

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 20

Correct

Domain : Other

To ensure that your application will handle the load even if an entire zone fails, what should you do?
Select all correct options.

- A. Don't select the 'Multizone' option when creating your managed instance group.
- B. Spread your managed instance group over two zones and overprovision by 100%. (for Two Zone) 
- C. Create a regional unmanaged instance group and spread your instances across multiple zones.
- D. Overprovision your regional managed instance group by at least 50%. (for Three Zones) 

Explanation:

Correct answer B and D

Feedback

B is correct if one zone fails you still have 100% desired capacity in another zone

C is incorrect because it won't be able to handle the full load since, it's unmanaged group and won't auto scale accordingly.

D is correct since you have at least total 150% desired capacity spread over 3 zones, each zone has 50% capacity. You'll have 100% desired capacity in two zones if any single zone failed at given time.

Reference Resources

<https://cloud.google.com/compute/docs/instance-groups/distributing-instances-with-regional-instance-groups>

If you are creating a regional managed instance group in a region with at least three zones, Google recommends overprovisioning your instance group by at least 50%.

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 21

Correct

Domain : Other

You are creating a single preemptible VM instance named "preempt" to be used as scratch space for a single workload. If your VM is preempted, you need to ensure that disk contents can be re-used. Which gcloud command would you use to create this instance?

- ✓ A. gcloud compute instances create "preempt" --preemptible --no-boot-disk-auto-delete 
- B. gcloud compute instances create "preempt" --preemptible --boot-disk-auto-delete=no
- C. gcloud compute instances create 'preempt' --preemptible
- D. gcloud compute instances create "preempt" --no-auto-delete

Explanation:

Correct Answer A

Explanation

A (Correct answer) – Specifying '--no-boot-disk-auto-delete' preserves the disk. This flag is not enabled by default so if not specify, it causes the disk to be auto-deleted.

B – The default is boot disk automatically delete and no flag needed, also the syntax is incorrect for this type of flags

C – if you don't specify '--no-boot-disk-auto-delete'. The default would be boot disk automatically delete

Here is the corresponding console setting displaying the default option

The screenshot shows a navigation bar with tabs: Management, Security, Disks (which is highlighted in blue), and Networking. Below the tabs, under the heading 'Boot disk', there is a section titled 'Deletion rule'. A checkbox labeled 'Delete boot disk when instance is deleted' is checked. The entire interface has a light gray background with dark gray text and blue highlights for selected tabs.

D – when instance created without this flag: --preemptible, it'll be standard instance

Here is the corresponding console setting in "Availability Policy" when you create instance with --preemptible flag

Availability policy

Preemptibility

A preemptible VM costs much less, but lasts only 24 hours. It can be terminated sooner due to system demands. [Learn more](#)

On

Ask our Experts

Rate this Question?

View Queries

open

Question 22

Correct

Domain : Other

You want to make a copy of a production Linux virtual machine in the US-Central region. You want to manage and replace the copy easily if there are changes in the production virtual machine. You will deploy the copy as a new instance in a different project in the US-East region. What steps must you take? Select 2 options

- A. Use the Linux dd and netcat commands to copy and stream the root disk contents to a new virtual machine instance in the US-East region.
- B. Create a snapshot of the root disk and select the snapshot as the root disk when you create a new virtual machine instance in the US-East region. 
- C. Create an image file from the root disk with Linux dd command, create a new disk from the image file, and use it to create a new virtual machine instance in the US-East region.
- D. Create a snapshot of the root disk, create an image file in Google Cloud Storage from the snapshot, and create a new virtual machine instance in the US-East region using the image file for the root disk. 

Explanation:

Correct Answer: B & D

Explanation:

D (Correct Answer) - This approach meets all of the requirements, it is easy to do and works cross project and cross region.

A - This approach affects the performance of the existing machine and incurs significant network costs.

B(Correct Answer) - We can share the snapshots of boot dist across the project and region.

C - dd will not work correctly on a mounted disk.

Reference Resources

<https://cloud.google.com/compute/docs/images/sharing-images-across-projects> Sharing Images Across Projects

Ask our Experts

Rate this Question?  

Question 23

Correct

Domain : Other

A lead software engineer tells you that his new application design uses websockets and HTTP sessions that are not distributed across the web servers. You want to help him ensure his application will run properly on Google Cloud Platform. What should you do?

- A. Help the engineer to convert his websocket code to use HTTP streaming.
- B. Review the encryption requirements for websocket connections with the security team.
- C. Meet with the cloud operations team and the engineer to discuss load balancer options. 
- D. Help the engineer redesign the application to use a distributed user session service that does not rely on websockets and HTTP sessions.

Explanation:

Correct Answer C

Feedback

C (Correct Answer) - The HTTP(S) load balancer in GCP handles websocket traffic natively. Backends that use WebSocket to communicate with clients can use the HTTP(S) load balancer as a front end, for scale and availability.

A - There is no compelling reason to move away from websockets as part of a move to GCP.

B - This may be a good exercise anyway, but it doesn't really have any bearing on the GCP migration.

D - There is no compelling reason to move away from websockets as part of a move to GCP.

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 24

Correct

Domain : Other

Which of the following are the best practices recommended by Google Cloud when dealing with service Accounts. Select 3 relevant options

- A. Grant the service account full set of permissions
- B. Do not delete service accounts that are in use by running instances on Google App Engine or Google Compute Engine 
- C. Grant serviceAccountUser role to all the users in the organization.
- D. Use the display name of a service account to keep track of the service accounts. When you create a service account, populate its display name with the purpose of the service account. 
- E. Create service accounts for each service with only the permissions required for that service. 

Explanation:

Answer: Option B, D & E are the CORRECT choices.

Option A is INCORRECT because always grant the service account only the minimum set of permissions required to achieve their goal.

Option C is INCORRECT because always restrict who can act as service accounts. Users who are Service Account Users for a service account can indirectly access all the resources the service account has access to. Therefore, be cautious when granting the serviceAccountUser role to a user.

Best practices

- Restrict who can act as service accounts. Users who are [Service Account Users](#) for a service account can indirectly access all the resources the service account has access to. Therefore, be cautious when granting the `serviceAccountUser` role to a user.
- Grant the service account only the minimum set of permissions required to achieve their goal. Learn about [Granting roles to a service account for specific resources](#).
- Create service accounts for each service with only the permissions required for that service.
- Use the display name of a service account to keep track of the service accounts. When you create a service account, populate its display name with the purpose of the service account.
- Define a naming convention for your service accounts.
- [Implement processes to automate the rotation of user-managed service account keys](#).
- Take advantage of the [IAM service account API](#) to implement key rotation.
- Audit service accounts and keys using either the `serviceAccount.keys.list()` method or the [Logs Viewer](#) page in the console.
- Do not delete service accounts that are in use by running instances on Google App Engine or Google Compute Engine.

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 25

Correct

Domain : Other

You have been delegated Access to XYZ Organization, you want to create Shared VPC, even with the delegated access you aren't able to create the Shared VPC, what solution would resolve the issue?

- A. With Delegated Access, you don't need any other extra permission.
- B. Give yourself Compute Shared VPC Admin role 
- C. Give yourself Compute Admin Access
- D. Add your member and give them a Shared Network Admin Role.

Explanation:

Answer: Option B is the CORRECT choice because Compute Shared VPC Admin role gives you the permission to set up Shared VPC.

Option A is INCORRECT because even with delegated access you need to give yourself Compute Shared Admin role.

Option C is INCORRECT because giving Compute Admin Access role doesn't give you permission to set up Shared VPC.

Option D is INCORRECT because there is NO Shared Network Admin Role in GCP

Read More at <https://cloud.google.com/vpc/docs/provisioning-shared-vpc>

The screenshot shows a dropdown menu titled "Select a role". At the top left is a blue bracket icon. To its right is a search bar with the placeholder "Type to filter". On the far right is a trash can icon. The main area contains two columns of roles. The left column lists service accounts: Cloud Trace, Codelab API Keys, Compute Engine, Container Analysis, Dataflow, Dataprep, and Dataproc. The right column lists Compute-related roles under the heading "COMPUTE NETWORK VIEWER": Compute OS Admin Login, Compute OS Login, Compute OS Login External ..., Compute Security Admin, Compute Storage Admin, Compute Viewer, and Compute Shared VPC Admin. The "Compute Engine" row is highlighted with a blue background. At the bottom of the dropdown is a blue button labeled "MANAGE ROLES".

Ask our Experts

Rate this Question?

[View Queries](#)

[open](#) ▾

Question 26

Correct

You set up an autoscaling 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 the appropriate web response is coming from each instance using the curl command. You want to ensure 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. 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.
- C. Ensure that a firewall rule exists to allow load balancer health checks to reach the instances in the instance group. ✓
- D. Assign a public IP to each instance and configure a firewall rule to allow the load balancer to reach the instance public IP.

Explanation:

Correct Answer C

Feedback

C (correct answer) - Ensure that a firewall rule exists to allow load balancer health checks to reach the instances in the instance group.

HTTP health check probes are sent from the IP ranges depending on LB types used. These are IP address ranges that the load balancer uses to connect to backend instances. You must create firewall rules that allows traffic from those ranges to reach your instances

For Network load balancing

When a health check is used with Network load balancing, the health check probes come from addresses in the ranges 209.85.152.0/22, 209.85.204.0/22, and 35.191.0.0/16.

For HTTP(S), SSL proxy, TCP proxy, and Internal load balancing

When a health check is used with HTTP(S), SSL proxy, TCP proxy, or Internal load balancing, the health check probes come from addresses in the ranges 130.211.0.0/22 and 35.191.0.0/16.

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

Firewall controls access at instance level, not load balancer. Must allow load balancer traffic to connect backend instance allowing health check

B - 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.

At this moment it is not possible to set firewall rules over the GCE Load Balancers. You need to create firewall rules that at subnet or instances level allowing specific health check IP ranges (See Answer A above), not the LB tags, to connect to all your load balanced instances.

D - Assign a public IP to each instance and configure a firewall rule to allow the load balancer to reach the instance public IP.

This is not mandatory since your LB could be Internal load balancing so instances' external IPs may be removed

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 27

Correct

Domain : Other

You are working on a project with two compliance requirements. The first requirement states that your developers should be able to see the Google Cloud Platform billing charges for only their own projects. The second requirement states that your finance team members can set budgets and view the current charges for all projects in the organization. The finance team should not be able to view the project contents. You want to set permissions. What should you do?

- A. Add the finance team members to the default IAM Owner role. Add the developers to a custom role that allows them to see their own spend only.
- B. Add the finance team members to the Billing Administrator role for each of the billing accounts that they need to manage. Add the developers to the Viewer role for the Project. 
- C. Add the developers and finance managers to the Viewer role for the Project.

- D. Add the finance team to the Viewer role for the Project. Add the developers to the Security Reviewer role for each of the billing accounts.

Explanation:

Correct answer B

Feedback

B (Correct Answer) - B is correct because it uses the principle of least privilege for IAM roles; use the Billing Administrator IAM role for that job function.

A, C, and D are not correct because it is a Google best practice to use pre-defined IAM roles when they exist and match your business scenario; see the link below.

Reference

IAM for Billing: <https://cloud.google.com/iam/docs/job-functions/billing>

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

Question 28

Correct

Domain : Other

For this question, refer to the [Dress4Win](#) case study.

Dress4Win has configured a new uptime check with Google Stackdriver for several of their legacy services. The Stackdriver dashboard is not reporting the services as healthy. What should they do?

- ✓ A. In the Cloud Platform Console download the list of the uptime servers' IP addresses and create an inbound firewall rule 
- B. Install the Stackdriver agent on all of the legacy web servers.

- Configure their legacy web servers to allow requests that contain user-Agent HTTP header when the value matches GoogleStackdriverMonitoring-UptimeChecks (<https://cloud.google.com/monitoring>)
- Configure their load balancer to pass through the User-Agent HTTP header when the value matches GoogleStackdriverMonitoring-UptimeChecks (<https://cloud.google.com/monitoring>)

Explanation:

Correct Answer A

Explanation

A (Correct Answer) - In the Cloud Platform Console download the list of the uptime servers' IP addresses and create an inbound firewall rule.

"If you are checking a service that is behind a firewall, you can configure your service's firewall to accept traffic from the current set of IP addresses used for uptime checking (Getting uptime-check IP addresses https://cloud.google.com/monitoring/uptime-checks/#monitoring_uptime_check_list_ips-console).

The returned information typically contains about 20 IP addresses. Uptime checks can come from any of the IP addresses, but only one address from each geographic location is used for each time interval. The geographic locations are listed in the uptime checks dashboard, shown in the previous section. You can also use free, web-based services to identify the registered locations of the IP addresses you downloaded.

The IP addresses used by uptime checking might change, but typically not more than once per quarter and not without an announcement.

B - Install the Stackdriver agent on all of the legacy web servers.

Uptime checks work by making HTTP requests and monitors the returned HTTP status code. There is no specific StackDriver agent needed for uptime check to work.

C and D are incorrect - uptime-check servers are configured its User-Agent header value (Identifying uptime check traffic https://cloud.google.com/monitoring/uptime-checks/#identifying_uptime_check_traffic):

GoogleStackdriverMonitoring-UptimeChecks (<https://cloud.google.com/monitoring>):

Regardless on instance or LoadBalancer level, as long as the firewall allowed, this user-agent can pass through; also, there is no feature supporting User-Agent header value associated firewall rule configuration.

Additional Resource

For your quick reference, here are the part of [Dress4win](#) existing Application servers in a single data center location:

- Tomcat - Java micro-services
- Nginx - static content

Apache Beam - Batch processing

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 29

Correct

Domain : Other

Your company is using Bigquery for data analysis, many users have access to this service and the data set, you would want to know which user has run what query, what would be the best way to get the required information?

- A. Go to job history, it has information about which user has run what query.
- B. Query the Stackdriver logs

- C. Check the Audit logs for the user ID.
- ✓ D. Go to Query history it has information about which user has run what query. 

Explanation:

Answer: Option D is the correct choice because Query history has the required information.

Option A is incorrect because it has information about export, load, copy etc.



The screenshot shows a 'Query history' section with the following data:

Time	User	Query	Action
1:47 PM	[REDACTED]	select * from [REDACTED]	[REDACTED]
1:44 PM	[REDACTED]	select * from [REDACTED]	[REDACTED]
1:42 PM	[REDACTED]	select * from [REDACTED]	[REDACTED]
1:42 PM	[REDACTED]	select * from [REDACTED]	[REDACTED]

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 30

Incorrect

Domain : Other

For this question, refer to the [Mountkirk Games](#) case study.

Mountkirk Games wants to set up a real-time analytics platform for their new game. The new platform must meet their technical requirements. Which combination of Google technologies will meet all of their requirements?

- A. Cloud Dataflow, Cloud Storage, Cloud Pub/Sub, and BigQuery 
- B. Cloud SQL, Cloud Storage, Cloud Pub/Sub, and Cloud Dataflow

- C. Container Engine, Cloud Pub/Sub, and Cloud SQL
- ✓ D. Cloud Pub/Sub, Compute Engine, Cloud Storage, and Cloud Dataproc 
- E. Cloud Dataproc, Cloud Pub/Sub, Cloud SQL, and Cloud Dataflow

Explanation:

Correct Answer A

Feedback

(see [Mountkirk Games](#) case study for details or below for briefing summary)

For requirements: Process incoming data on the fly directly from the game servers - Cloud Dataflow (Both Stream and Batch), reference architect component ?, we can eliminate C and D since they don't have DataFlow

C - Container Engine, Cloud Pub/Sub, and Cloud SQL

D - Cloud Pub/Sub, Compute Engine, Cloud Storage, and Cloud Dataproc

For requirements: Allow SQL queries to access at least 10 TB of historical data - BigQuery, reference architect component?, we can eliminate B and E since they don't have BigQuery

B - Cloud SQL, Cloud Storage, Cloud Pub/Sub, and Cloud Dataflow

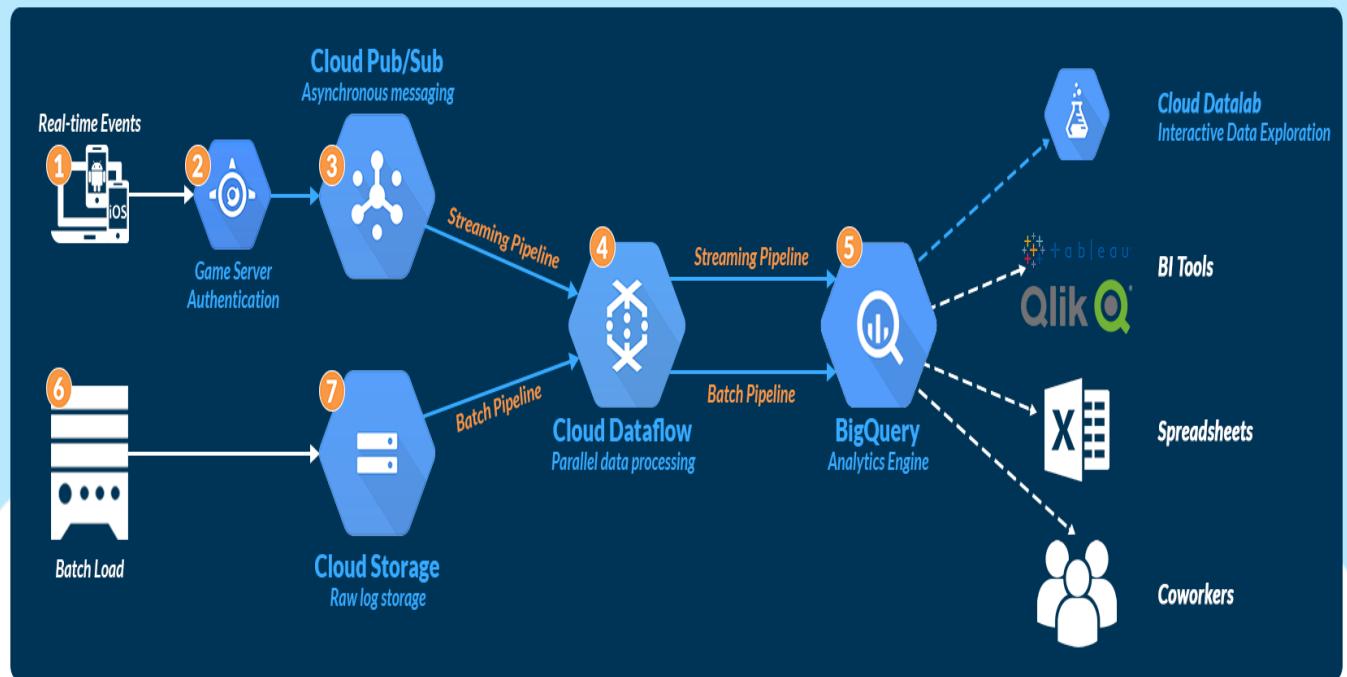
E - Cloud Dataproc, Cloud Pub/Sub, Cloud SQL, and Cloud Dataflow

The only correct answer left is A, which meets all of their requirements

A - Cloud Dataflow, Cloud Storage, Cloud Pub/Sub, and BigQuery

Below is a reference architect Google recommending for similar scenario in data collection and analysis <https://cloud.google.com/solutions/mobile/mobile-gaming-analysis-telemetry>

Building a Mobile Gaming Analytics Platform - a Reference Architecture



Mountkirk Games real-time analytics platform

Solution Concept

Mountkirk Games is building a new game, which they expect to be very popular. They plan to deploy the game's backend on Google Compute Engine so they can capture streaming metrics, run intensive analytics, and take advantage of its autoscaling server environment and integrate with a managed NoSQL database.

Technical Requirements

Requirements for Game Analytics Platform

- Dynamically scale up or down based on game activity – Compute engine, container engine, Cloud Storage
- Process incoming data on the fly directly from the game servers - Cloud Dataflow (Both Stream and Batch)
- Process data that arrives late because of slow mobile networks - Cloud Pub/Sub
- Allow SQL queries to access at least 10 TB of historical data - BigQuery
- Process files that are regularly uploaded by users' mobile devices - Cloud Pub/Sub

Use only fully managed services – BigQuery, DataFlow, Cloud SQL

Ask our Experts

Rate this Question?  

View Queries

open 

Question 31

Correct

Domain : Other

You are managing the GCP Account of a client, the client raises a request to attach 9 local SSDs and launch a VM instance in us-east1 Region, as a Cloud Architect what would be your response to the above request?

- A. You can always attach maximum of ten local SSD devices to a VM instance
- ✓ B. If a resource is not available, you won't be able to create new resources of that type, even if you still have remaining quota in your region or project and you can attach up to eight local SSD devices for 3 TB of total local SSD storage space per instance 
- C. Launch the instance first and add the local SSD drives later for optimal performance.
- D. Request changes to quota from the Quotas page in the GCP Console

Explanation:

Answer: Option B is the CORRECT because, Each local SSD is 375 GB in size, but you can attach up to eight local SSD devices for 3 TB of total local SSD storage space per instance. If a resource is not available, you won't be able to create new resources of that type, even if you still have remaining quota in your region or project.

Option A is INCORRECT because you can only attach up to 8 local SSD devices to a VM instance also if the resource isn't available you can't create the resource.

Option C is INCORRECT because you can attach the local SSD devices to an Instance while launching a VM instance.

Option D is INCORRECT because you can only attach up to 8 local SSD devices to a VM instance that is the limit.

Read more about it here: <https://cloud.google.com/compute/docs/disks/local-ssd>

<https://cloud.google.com/compute/quotas>

Ask our Experts

Rate this Question?

[View Queries](#)

open

Question 32

Correct

Domain : Other

Your customer is receiving reports that their recently updated Google App Engine application is taking approximately 30 seconds to load for some of their users. This behavior was not reported before the update. What strategy should you take?

- A. Work with your ISP to diagnose the problem.
- B. Open a support ticket to ask for network capture and flow data to diagnose the problem, then roll back your application.
- C. Roll back to an earlier known good release initially, then use Stackdriver Trace and logging to diagnose the problem in a development/test/staging environment.
- D. Roll back to an earlier known good release, then push the release again at a quieter period to investigate. Then use Stackdriver Trace and logging to diagnose the problem.

Explanation:

Correct Answer C

Explanation

A – You ISP normally won't help in this level. Also, the problem most likely is caused by recent update. The good approach is to rollback first and then investigate later. Similarly, this also applies to answer B.

To investigate this kind of issue, use Stackdriver Trace and logging to diagnose the bottleneck

C and D have something in common for both "use Stackdriver Trace and logging", either in test/dev or in production environment and "Roll back to an earlier known good release". At this moment, only the "earlier known good release" version starts receiving traffic.

The difference lies between C's "to diagnose the problem in a development/test/staging environment." and D's "then push the release again at a quieter period to investigate".

If you want to debug in production environments, "then push the release again at a quieter period to investigate" is not necessary - you can simply switch "default" version or split the traffic between the "earlier known good release" version and the new problem version.

Essentially D's "then push the release again at a quieter period to investigate" disqualifies itself as good answer – the default would be the new pushed version (the one with problem) starts receiving traffic "at a quieter period", and the slow loading users may not present. But with answer C in development/test/staging environment, you can arbitrarily load those suffering users if you know them or simulate production load to reveal the problem users and then do further investigation.

So, C is the correct answer: First, rollback to "the earlier known good release" and then use the test/dev/staging envs to investigate.

Additional Resource

<https://cloud.google.com/appengine/docs/flexible/python/testing-and-deploying-your-app>

Testing and Deploying your Application

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 33

Correct

Domain : Other

A power generation company is looking to use Google cloud platform to monitor a power station. They have installed several IOT sensors in the power station like temperature sensors, smoke detectors, motion detectors etc. Sensor data will be continuously streamed to the cloud. There it has to be handled by different components for real-time monitoring and alerts, analysis and performance improvement. What Google Cloud Architecture would serve their purpose?

- Cloud IoT Core receives data from IOT devices, Cloud IOT core transforms and redirects requests to a Cloud Pub/Subtopic. After the data is stored in Cloud Pub/Sub, it is retrieved by a streaming job running in Cloud Dataflow that transforms the data and sends it to Big Query for analysis ✓
- ✓ A. Send IOT devices data to Cloud Storage, load data from cloud storage to Big Query
 - B. Cloud IOT core receives data from IOT sensors, then sends the data to cloud storage, transform the data using Cloud Dataflow and send the data to Big Query for Analysis
 - C. Cloud IOT core receives the data from IOT devices, Cloud IOT core transforms and redirects the request to Pub/Sub, use data proc to transform the data and send it to BigQuery for Analysis

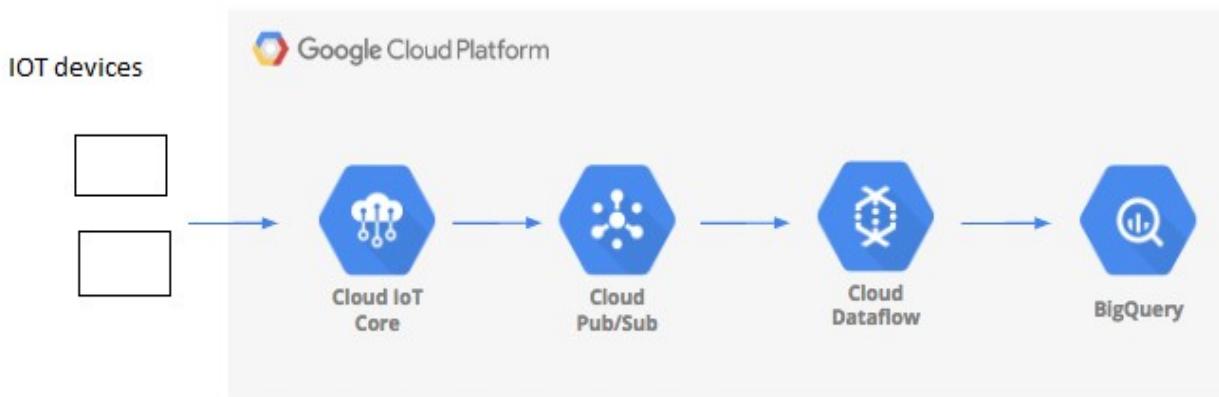
Explanation:

Answer: Option A is the CORRECT choice because Cloud IoT core can accept data from IOT devices and Cloud Pub/Sub acts as a connector service and sends the data to Cloud Data Flow for transformation. Data Flow transforms the data and sends it to Big Query for analysis.

Option B is INCORRECT because, Cloud Storage isn't the right choice for streaming data, using Cloud Pub/Sub is the best choice.

Option C is INCORRECT because cloud IoT core can stream the data directly to Cloud Pub/Sub .(use Cloud Storage for Batch Upload)

Option D is INCORRECT because data proc is a fully managed cloud service for running Apache Spark and Apache Hadoop clusters.



<https://cloud.google.com/community/tutorials/cloud-iot-rtdp>

[Ask our Experts](#)Rate this Question?  [View Queries](#)open 

Question 34

Correct

Domain : Other

A digital Media company has recently moved its infrastructure from On-premise to Google Cloud, they have several instances under a Global HTTPS load balancer, a few days ago the Application and Infrastructure were subjected to DDOS attacks, they are looking for a service that would provide a defense mechanism against the DDOS attacks. Please select the relevant service.

- A. Cloud Armor 
- B. Cloud-Identity Aware Proxy
- C. GCP Firewalls
- D. IAM policies

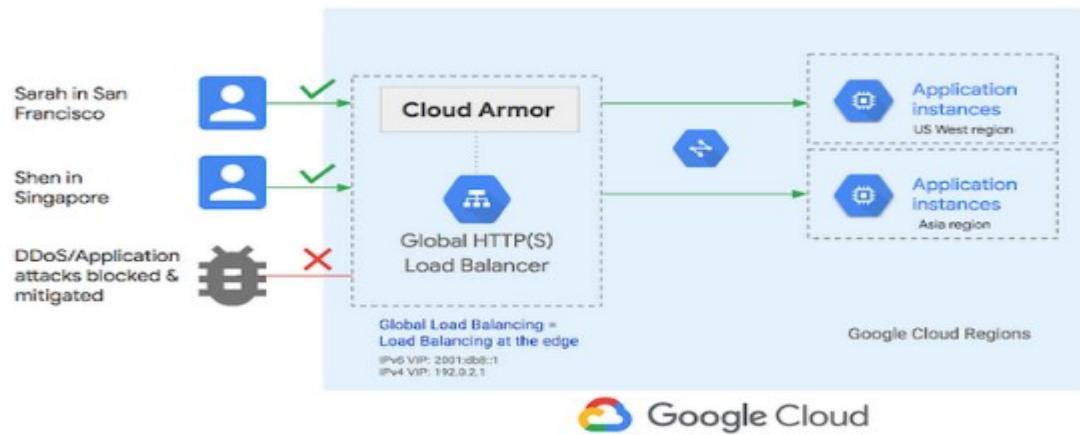
Explanation:

Answer: Option A is the CORRECT choice because Cloud Armor delivers defense at scale against infrastructure and application Distributed Denial of Service (DDoS) attacks using Google's global infrastructure and security systems.

Option B is INCORRECT because, Cloud-Identity Aware Proxy lets you establish a central authorization layer for applications accessed by HTTPS, so you can use an application-level access control model instead of relying on network-level firewalls.

Option C is INCORRECT because GCP firewalls rules don't apply for HTTP(S) Load Balancers, while Cloud Armor is delivered at the edge of Google's network, helping to block attacks close to their source.

Option D.IAM policies doesn't help in mitigating DDOS attacks.



Read more about Cloud Armor at: <https://cloud.google.com/blog/products/gcp/getting-to-know-cloud-armor-defense-at-scale-for-internet-facing-services>

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 35

Correct

Domain : Other

Your office is connected to GCP via a VPN connection. How can you increase the speed of your VPN connection, assuming that your office Internet is not the bottleneck?

- A. Apply for a dedicated interconnect option
- B. Enable high speed routing in your VPN settings
- C. Create an additional VPN tunnel
- D. Submit request to increase bandwidth quota

Explanation:

Correct answer C

Explanation

A - Apply for a dedicated interconnect option. A dedicated interconnect will also increase speeds, however the question asked how to speed up your VPN connection, not create a new type of connection.

C (Correct answer) - Create an additional VPN tunnel. Each VPN tunnel has a max speed of 1.5 Gbps. However, you can create multiple VPN tunnels to increase bandwidth.

Answer B and D either are not applicable or feature doesn't exist.

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

Question 36

Correct

Domain : Other

Using the principle of least privilege and allowing for maximum automation, what steps can you take to store audit logs for long-term access and to allow access for external auditors to view? (Choose two)

- A. Generate a signed URL to the Stackdriver export destination for auditors to access. 
- B. Create an account for auditors to have view access to Stackdriver Logging.
- C. Export audit logs to Cloud Storage via an export sink. 
- D. Export audit logs to BigQuery via an export sink.

Explanation:

Correct Answer A and C

Explanation

C (Correct answer) - Export audit logs to Cloud Storage via an export sink. Cloud Storage is perfect solution for long-term logs storage.

There are 3 type of sink destinations you can export StackDriver Logs to: Cloud Storage, Cloud Pub/Sub, BigQuery. While you could export to BigQuery for low-cost storage, BigQuery is mainly and best for analysis not for long-term storage. Besides, whenever you need to do analysis with BigQuery, you can always easily export the logs from GCS to BigQuery or do query directly against data in GCS bucket.

A (Correct answer) - You could either create a GCP account for auditor ACL object access or signed URL's depending on if they need to have a GCP account or not. Since the requirement is "allow access for external auditors to view", hence signed URL is the right choice

B – Does not meet the "for long-term access" requirement

D – It works but for the "for long-term access" storage consideration, Cloud Storage is better choice over BigQuery

Additional Resources

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

Generate a signed URL to the Stackdriver export destination for auditors to access.

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

Question 37

Correct

Domain : Other

Suppose you have a web server that is working properly, but you can't connect to its instance VM over SSH. Which of these troubleshooting methods can you use without disrupting production traffic?
(Select 3 answers.)

- A. Create a snapshot of the disk and use it to create a new disk; then attach the new disk to a new instance 
- B. Use netcat to try to connect to port 22 
- C. Access the serial console output 

- D. Create a startup script to collect information.

Explanation:

Correct answer A, B, and C

Feedback

Answers A, B, and C are valid methods to diagnose the problem without stop/start the instance. Answer D need to restart the instance for the script to take effect.

Troubleshooting SSH <https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh>

Under certain conditions, it is possible that a Google Compute Engine instance no longer accepts SSH connections. There are many reasons this could happen, from a full disk to an accidental misconfiguration of sshd. This section describes a number of tips and approaches to troubleshoot and resolve common SSH issues.

- 1) Check your firewall rules . . .
- 2) Debug the issue in the serial console

You can enable read-write access to an instance's serial console so you can log into the console and troubleshoot problems with the instance. This is particularly useful when you cannot log in with SSH or if the instance has no connection to the network. The serial console remains accessible in both these conditions.

- 3) Test the network

You can use the netcat tool to connect to your instance on port 22 and see if the network connection is working. If you connect and see an ssh banner (e.g. SSH-2.0-OpenSSH_6.0p1 Debian-4), your network connection is working, and you can rule out firewall problems. First, use the gcloud tool to obtain the external natIP for your instance:

```
gcloud compute instances describe example-instance --  
format='get(networkInterfaces[0].accessConfigs[0].natIP)'
```

198.51.100.8

Use the nc command to connect to your instance:

```
# Check for SSH banner
```

```
user@local:~$ nc [EXTERNAL.IP] 22
```

SSH-2.0-OpenSSH_6.0p1 Debian-4

- 4) Try a new user
- 5) Use your disk on a new instance
- 6) Inspect an instance without shutting it down

You might have an instance you can't connect to that continues to correctly serve production traffic. In this case, you might want to inspect the disk without interrupting the instance's ability to serve users. First, take a snapshot of the instance's boot disk, then create a new disk from that snapshot, create a temporary instance, and finally attach and mount the new persistent disk to your temporary instance to troubleshoot the disk.

- 7) Use a startup script

If none of the above helped, you can create a startup script to collect information right after the instance starts. Follow the instructions for running a startup script.

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 38

Correct

Domain : Other

You have a Kubernetes cluster with 1 node-pool. The cluster receives a lot of traffic and needs to grow. You decide to add a node. What should you do?

- ✓ A. Use "gcloud container clusters resize" with the desired number of nodes. 
- B. Use 'kubectl container clusters resize' with the desired number of nodes.
- C. Edit the managed instance group of the cluster and increase the number of VMs by 1.
- D. Edit the managed instance group of the cluster and enable autoscaling.

Explanation:

Correct answer A

Feedback

A is correct because this resizes the cluster to the desired number of nodes.

B is not correct because you need to use gcloud, not kubectl.

C is not correct because you should not manually manage the MIG behind a cluster.

D is not correct because you should not manually manage the MIG behind a cluster.

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

Question 39

Correct

Domain : Other

One of your client wants to store time series data in Google Cloud Platform. They have found Big Table to be a natural fit for time series data. Choose the best practices suggested by Google Cloud for schema design patterns for storing time series in Cloud Bigtable (Select four).

- ✓ A. For row key design pattern, use tall and narrow tables. 
- B. For row key Always for a row key for a time series includes a timestamp, make sure all your writes will target a single node; fill that node; and then move onto the next node in the cluster .
- ✓ C. Prefer reverse timestamps only where your most common query is for the latest values 
- ✓ D. For patterns for column design , in general ,keep row sizes below approximately 100 MB 
- ✓ E. Design your row key with your queries in mind . 

Explanation:

Answer :A,C,D and E

Option A , C , D, E are the Correct choices , because they are the recommended guidelines for Schema design pattern in Big Table.

Option B is Incorrect because , it will lead to hotspotting. This issue can affect any type of row key that contains a monotonically increasing value. In brief, when a row key for a time series includes a timestamp, all of your writes will target a single node; fill that node; and then move onto the next node in the cluster, resulting in hotspotting. Because Cloud Bigtable stores adjacent row keys on the same server node, all writes will focus only on one node until that node is full, at which point writes will move to the next node in the cluster.

Read more about it here : <https://cloud.google.com/bigtable/docs/schema-design-time-series>

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 40

Incorrect

Domain : Other

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 Platform. 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 2 answers

- A. Store all state in Google Cloud Storage, snapshot the persistent disks, and terminate the VM.
- B. Use the --no-auto-delete flag on all persistent disks and stop the VM. 
- C. Apply VM CPU utilization label and include it in the BigQuery billing export.
- D. Use Google BigQuery billing export and labels to associate cost to groups. 

- E. Use the -auto-delete flag on all persistent disks and terminate the VM.
- F. Store all state into local SSD, snapshot the persistent disks, and terminate the VM. 

Explanation:

Correct answers are B and D

Feedback

B (Correct Answer) - Use the --no-auto-delete flag on all persistent disks and stop the VM – with this flag set, when you terminate the instance, the persistence disk will not be deleted so the disk contents are preserved between start and stop. When the instance is in stop status, you are only charged for very low-cost disk storage

auto-delete for the given disk is enabled by default, use --no-auto-delete to disable.

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

C - Apply VM CPU utilization label and include it in the BigQuery billing export – this is simply not doable

D (Correct Answer) - Use Google BigQuery billing export and labels to associate cost to groups.

Billing export to BigQuery enables you to export your daily usage and cost estimates automatically throughout the day to a BigQuery dataset you specify. You can then access your billing data from BigQuery.

About labels: You'll see columns for labels in your BigQuery dataset, but for the current release some label values will be empty. Label export data will be populated at different times for different services, depending on when each service provides it.

E - Use the -auto-delete flag on all persistent disks and terminate the VM - This is totally against the requirements. Since the instance is terminated and disk is gone when this flag is on, there is no way to restart the same instance and needless to say the disk content are not persisted.

Answer A and F are incorrect, or at least not as good as Answer B – they are not a suitable solution for frequently start/stop and require state to persist.

[Ask our Experts](#)Rate this Question?  [View Queries](#)open 

Question 41

Incorrect

Domain : Other

For this question, refer to the [MountKirk Games](#) case study:

MountKirk Games needs to build out their streaming data analytics pipeline to feed from their game backend application. What GCP services in which order will achieve this?

- A. Cloud Storage - Cloud Dataflow - BigQuery
- B. Cloud Dataproc - Cloud Storage - BigQuery 
- C. Cloud Pub/Sub - Cloud Dataflow - Cloud Bigtable
- D. Cloud Pub/Sub - Cloud Dataflow - BigQuery 

Explanation:

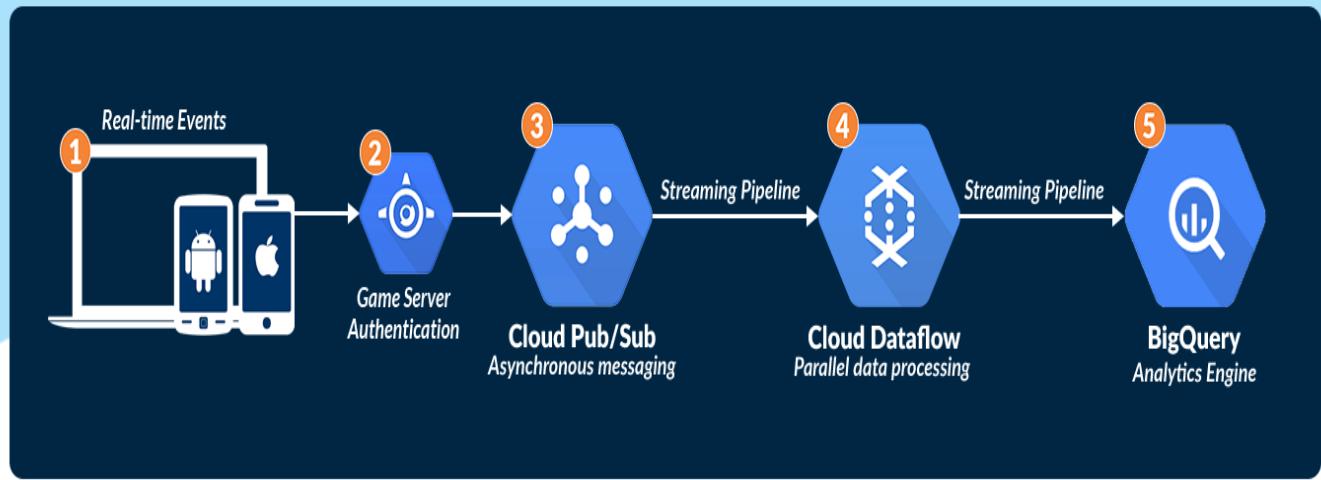
Correct answer D

Explanation

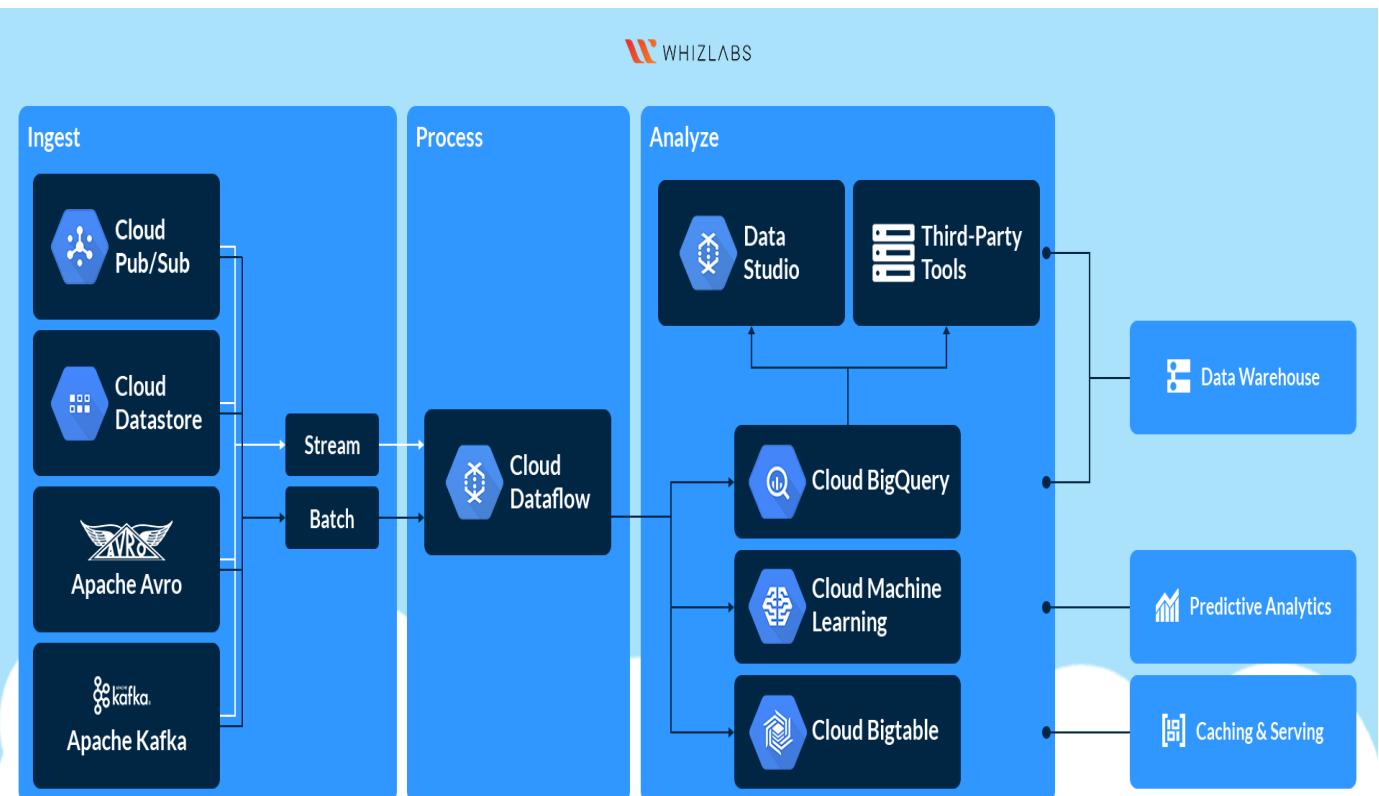
Pub/Sub is kind of 'shock absorber', allowing asynchronous messaging between large numbers of devices. Cloud Dataflow acts as your data processing pipeline for ETL functions on both streaming and batch data. BigQuery is a data warehouse, able to run analysis on petabytes of data using SQL queries.

Below is a reference architect Google recommending for similar scenario in Real-time streaming data collection and analysis <https://cloud.google.com/solutions/mobile/mobile-gaming-analysis-telemetry>

Real-time processing of events from game clients and game servers



Data Transformation with Cloud Dataflow - Dataflow acts as your data processing pipeline for ETL functions on both streaming and batch data.



Ask our Experts

Rate this Question?

View Queries

open ▾

Question 42

Correct

Domain : Other

A Global Media company is configuring a Global load balancer for non-http(s) traffic, they are looking for a service with SSL offloading, as a Cloud Architect what would be your load balancing choice?

- A. HTTPS load balancing
- B. SSL proxy Load balancing. 
- C. TCP proxy Load balancing for all non-http(s) traffic
- D. Network TCP/UDP load balancing

Explanation:

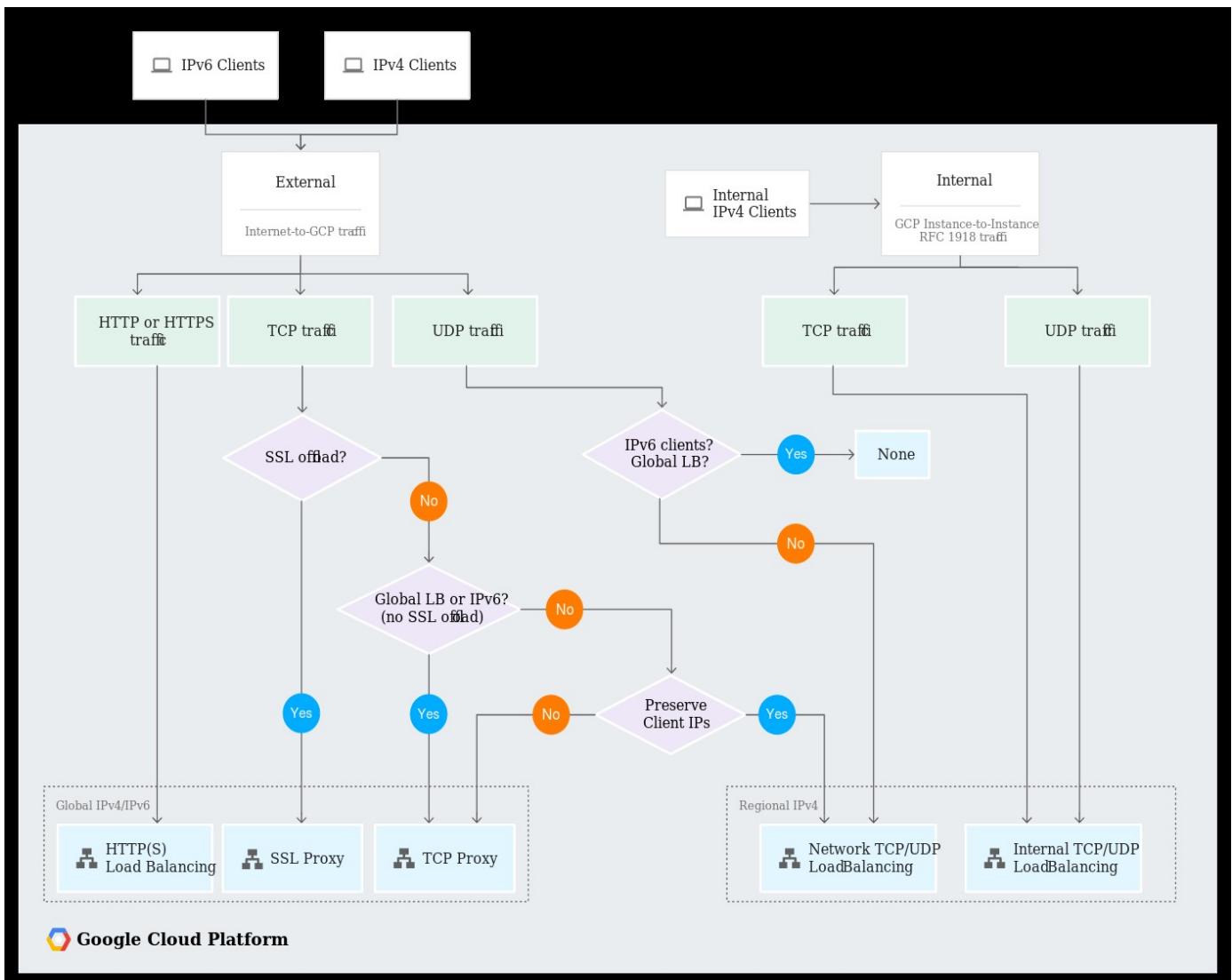
Answer: Option B is the CORRECT choice because SSL proxy Loadbalancing supports SSL offloading and it is availability is Global and it handles non-http(s) traffic.

Option A is INCORRECT because the traffic is non-http(s).

Option C is INCORRECT because TCP proxy can handle non-http(s) traffic but it doesn't come with SSL offloading feature.

Option D is INCORRECT because Network TCP/UDP load balancing is Regional and it doesn't handle SSL offloading.

Google Cloud SSL Proxy Load Balancing terminates user SSL (TLS) connections at the load balancing layer, then balances the connections across your instances using the SSL or TCP protocols. Cloud SSL proxy is intended for non-HTTP(S) traffic.



Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

Question 43

Correct

Domain : Other

You created an update for your application on App Engine. You want to deploy the update without impacting your users. You want to be able to roll back as quickly as possible if it fails. What should you do?

- A. Delete the current version of your application. Deploy the update using the same version identifier as the deleted version.

- B. Notify your users of an upcoming maintenance window. Deploy the update in that maintenance window.
- C. Deploy the update as the same version that is currently running.
- ✓ D. Deploy the update as a new version. Migrate traffic from the current version to the new version. 

Explanation:

Correct answer D

Feedback

A and B are not correct because this will make the application temporarily unavailable to users.

C is not correct because to roll back, you'll need to redeploy the previous deployment because the app was overwritten with the same version number. Therefore this takes longer than a rollback using method D.

D is correct because this makes sure there is no downtime and you can roll back the fastest.

Reference

Migrating and Splitting Traffic <https://cloud.google.com/appengine/docs/admin-api/migrating-splitting-traffic>

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 44

Correct

Domain : Other

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

- ✓ A. In a secret management system 

- B. In the source code
- C. In an environment variable
- D. In a config file that has restricted access through ACLs

Explanation:

Correct Answer A

Feedback

A (Correct answer) - In a secret management system

Applications often require access to small pieces of sensitive data at build or run time. These pieces of data are often referred to as secrets. Secrets are similar in concept to configuration files, but are generally more sensitive, as they may grant access to additional data, such as user data.

<https://cloud.google.com/kms/docs/secret-management>

B - In the source code: This is exactly again the best practice "Do not embed secrets related to authentication in source code, such as API keys, OAuth tokens, and service account credentials." (see below the best practice #1)

C - In an environment variable – you use environment variable to point to the location where the secrets (credentials) are stored other than store the secrete directly (see below the best practice #1)

D - In a configuration file that has restricted access through ACLs - Secrets are similar to but generally more sensitive

than configuration and also, ACLs may not enough for the secrete management. Here is example for Storing secrets <https://cloud.google.com/kms/docs/store-secrets>

Additional Resource

https://cloud.google.com/docs/authentication/production#providing_credentials_to_your_application

Best practices for managing credentials

Credentials provide access to sensitive data. The following practices help protect access to these resources:

- 1) Do not embed secrets related to authentication in source code, such as API keys, OAuth tokens, and service account credentials. You can use an environment variable pointing to credentials outside of the application's source code, such as Cloud Key Management Service.

- 2) Do use different credentials in different contexts, such as in testing and production environments.
- 3) Do transfer credentials only over HTTPS to prevent a third party from intercepting your credentials. Never transfer in clear text or as part of the URL.
- 4) Never embed long-lived credentials into your client-side app. For example, do not embed service account credentials into a mobile app. Client-side apps can be examined, and credentials can easily be found and used by a third party.

Do revoke a token if you no longer need it.

Ask our Experts

Rate this Question?  

View Queries

open 

Question 45

Incorrect

Domain : Other

For this question, refer to the [TerramEarth](#) case study:

Based on TerramEarth's current data flow environment (refer to the image in the case study), what are the direct GCP services needed to replicate the same structure for batch uploads?

- A. Cloud Spanner - Cloud SQL - BigQuery
- B. Cloud Dataflow - Cloud Bigtable - Cloud Dataproc
- C. Cloud Dataproc - Cloud Storage - BigQuery 
- D. Cloud Storage - Cloud Dataflow - BigQuery 

Explanation:

Correct answer D

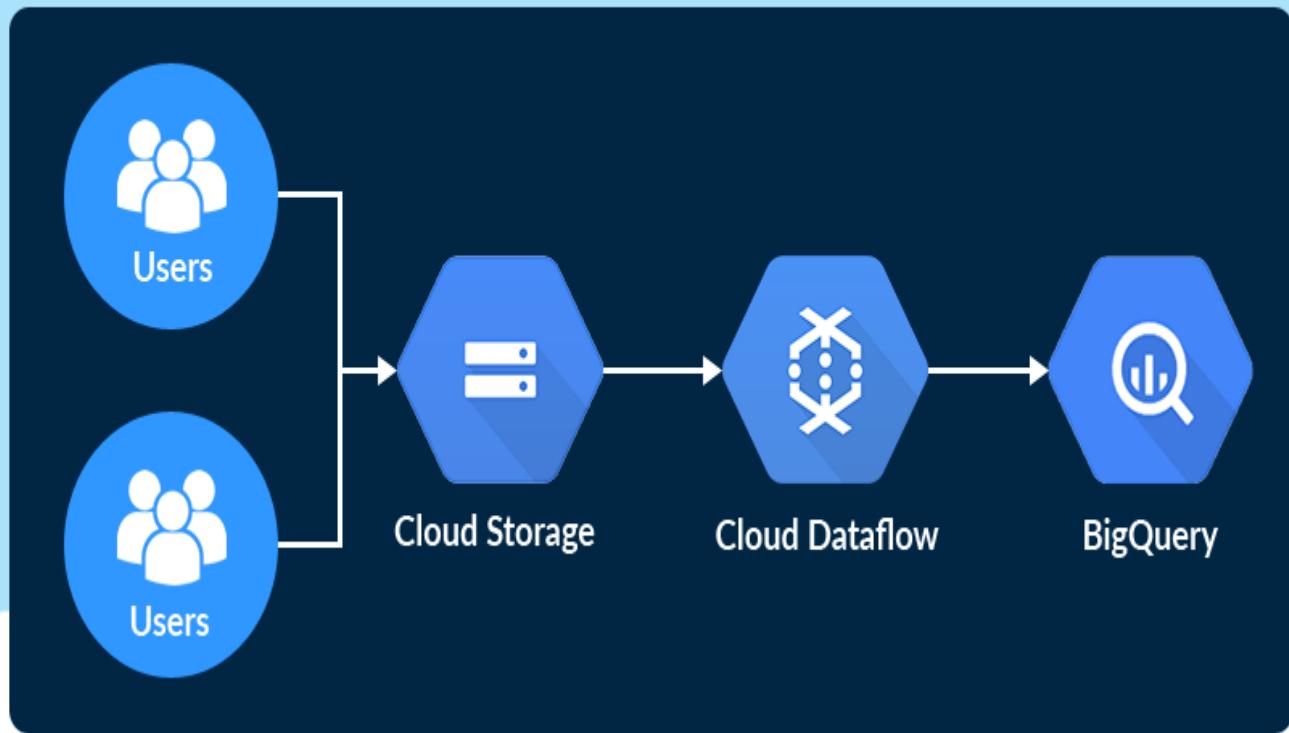
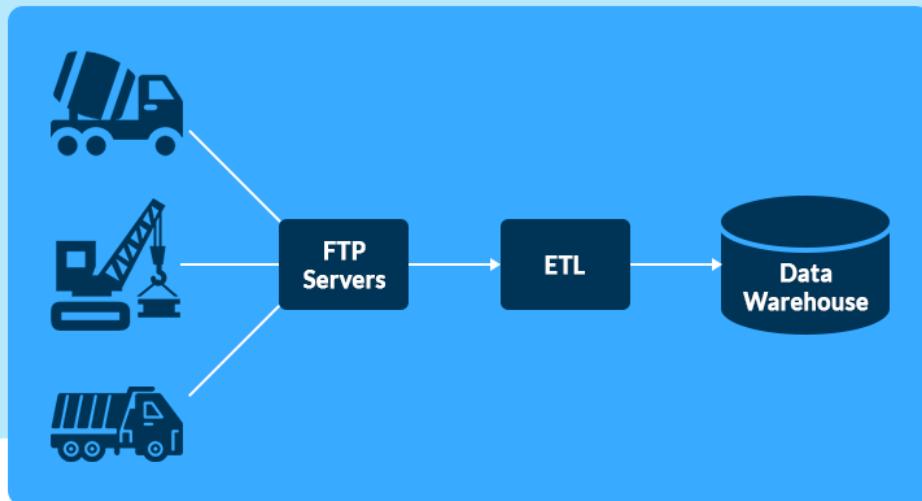
Explanation

Based on their current batch upload model, the direct equivalent would be to use Cloud Storage for storing files, Dataflow for their ETL processing, and BigQuery for their data warehouse needs.

Below illustrates the solution concept.

TerramEarth's Existing Technical Environment

One Possible GCP solution for batch upload flow



[Ask our Experts](#)Rate this Question?  [View Queries](#)open 

Question 46

Correct

Domain : Other

One of the large data Analysis company uses Big Query, Big Table, Data Proc and Cloud Storage services. They use a Hybrid Architecture involving on premise and Google Cloud, Cloud VPN is used to connect to Google Cloud Platform. One of the main challenges for the Organization is mitigating Data exfiltration risks stemming from stolen identities, IAM policy misconfigurations, malicious insiders and compromised virtual machines. What Google Cloud Service can they use to address the challenge?

- A. Shared VPC
- B. Cloud Armour
- C. VPC Service Controls 
- D. Resource Manager

Explanation:

Answer:

Option C is CORRECT because , VPC Service Controls create a security perimeter around data stored in API-based GCP services such as Google Cloud Storage, BigQuery and Bigtable. This helps mitigate data exfiltration risks stemming from stolen identities, IAM policy misconfigurations, malicious insiders and compromised virtual machines.

Option A is INCORRECT because , Shared VPC allows an organization to connect resources from multiple projects to a common VPC network, so that they can communicate with each other securely and efficiently using internal IPs from that network. When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. The VPC networks in the host project are called Shared VPC networks. Eligible resources from service projects can use subnets in the Shared VPC network .Here the challenge is to mitigate Data exfiltration and VPC Service Controls is the right choice.

Option B is INCORRECT because, Cloud Armor is used for delivering defense at scale against infrastructure and application Distributed Denial of Service (DDoS) attacks using Google's global

infrastructure and security systems.

Option D is INCORRECT because .. Resource Manager enables you to programmatically manage these resource containers. Google Cloud Platform provides Resource containers such as Organizations, Folders, and Projects, that allow you to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets you easily manage common aspects of your resources such as access control and configuration settings.

Security benefits of VPC Service Controls

VPC Service Controls helps mitigate the following security risks without sacrificing the performance advantages of direct private access to GCP resources:

1. Access from unauthorized networks using stolen credentials: By allowing private access only from authorized VPC networks, VPC Service Controls protects against theft of OAuth credentials or service account credentials.
2. Data exfiltration by malicious insiders or compromised code: VPC Service Controls complements network egress controls by preventing clients within those networks from accessing the resources of Google-managed services outside the perimeter.

VPC Service Controls also prevents reading data from or copying data to a resource outside the perimeter using service operations such as copying to a public Cloud Storage bucket using the gsutil cp command or to a permanent external BigQuery table using the bq mk command.

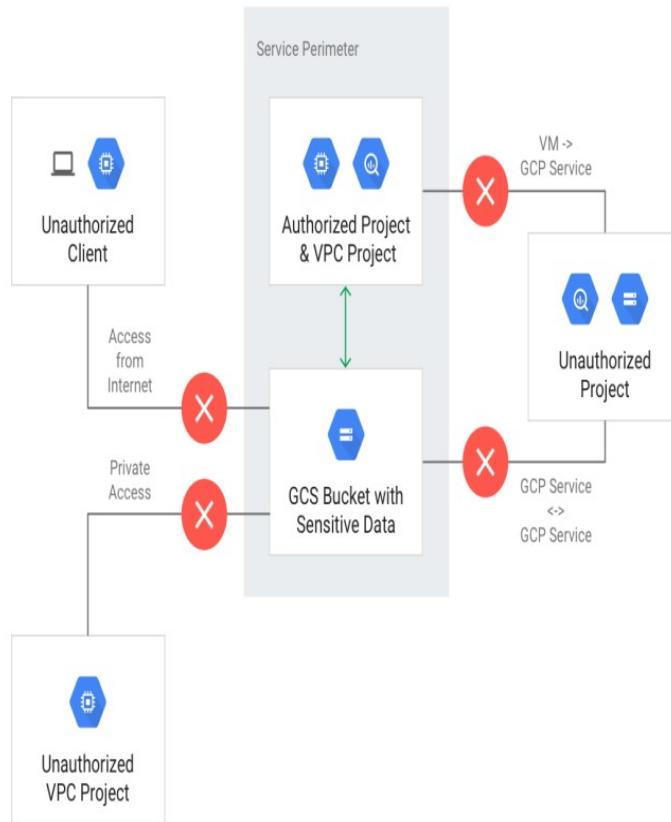
The restricted VIPs feature can be used to prevent access from a trusted network to storage services that are not integrated with VPC Service Controls.

1. Public exposure of private data caused by misconfigured Cloud IAM policies: VPC Service Controls provides an additional layer of security by denying access from unauthorized networks, even if the data is exposed by misconfigured Cloud IAM policies.

By assigning the Access Context Manager Policy Admin role for Cloud IAM, VPC Service Controls can be configured by a user who is not the Cloud IAM policy administrator.

VPC Service Controls is configured for your GCP organization to create a broad, uniform policy that applies consistently to all protected resources within the perimeter. You retain the flexibility to process, transform, and copy data within the perimeter. The security controls automatically apply to all new resources created within a perimeter.

Read more about VPC Service Control here : <https://cloud.google.com/vpc-service-controls/docs/overview>



A service perimeter creates a security boundary around GCP resources. You can configure a service perimeter to control communications from virtual machines (VMs) to a GCP service (API), and between GCP services. A service perimeter allows free communication within the perimeter but, by default, blocks all communication across the perimeter.

For example:

A VM within a Virtual Private Cloud (VPC) network that is part of a service perimeter can read from or write to a Cloud Storage bucket in the same perimeter. However, any attempt to access the bucket from VPC networks that are not inside the perimeter is denied.

A copy operation between two Cloud Storage buckets will succeed if both buckets are in the same service perimeter, but will fail if one of the buckets is outside the perimeter.

A VM within a VPC network that is part of a service perimeter can privately access any Cloud Storage buckets in the same perimeter. However, the VM will be denied access to Cloud Storage buckets that are outside the perimeter.

Ask our Experts

Rate this Question?

[View Queries](#)

open

Question 47

Correct

Domain : Other

You have a definition for an instance template that contains a web application. You are asked to deploy the application so that it can scale based on the HTTP traffic it receives. What should you do?

- A. Create a VM from the instance template. Create a custom image from the VM's disk.
- B. Create a VM from the instance template. Create an App Engine application in Automatic Scaling mode that forwards all traffic to the VM.
- C. Create a managed instance group based on the instance template. Configure autoscaling based on HTTP traffic and configure the instance group as the backend service of an HTTP load balancer. 
- D. Create the necessary amount of instances required for peak user traffic based on the instance template. Create an unmanaged instance group and add the instances to that instance group. Configure the instance group as the Backend Service of an HTTP load balancer.

Explanation:

Correct answer C

Feedback

A Is not correct because the Load Balancer will just load balance access to the uploaded image itself, and not create or autoscale VMs based on that image.

B Is not correct because while the App Engine can scale as a proxy, all requests will still end up on the same Compute Engine instance, which needs to scale itself.

C is correct because a managed instance group can use an instance template to scale based on HTTP traffic.

D is not correct because unmanaged instance groups do not offer autoscaling.

Reference

Managed instance groups and autoscaling

https://cloud.google.com/compute/docs/instance-groups/#managed_instance_groups_and_autoscaling

Exporting an Image <https://cloud.google.com/compute/docs/images/export-image>

Adding a Cloud Storage Bucket to Content-based Load Balancing

<https://cloud.google.com/compute/docs/load-balancing/http/adding-a-backend-bucket-to-content-based-load-balancing>

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

Question 48

Correct

Domain : Other

One of the customers want to redact the sensitive data like credit card numbers , social security numbers that are generated by the application logs .Please select the suitable service that fulfils the necessary requirement .

- ✓ A. Cloud Data Loss Prevention 
- B. Cloud Secure
- C. VPC Service control
- D. Cloud Armour

Explanation:

Answer:A

Option A is the Correct choice because , Cloud DLP helps you better understand and manage sensitive data. It provides fast, scalable classification and redaction for sensitive data elements like credit card numbers, names, social security numbers, US and selected international identifier numbers, phone numbers, and GCP credentials .

Option B is Incorrect because Cloud Secure Service doesn't exist in GCP.

Option C is incorrect because , VPC Service Controls allow users to define a security perimeter around Google Cloud Platform resources such as Cloud Storage buckets, Bigtable instances, and BigQuery datasets to constrain data within a VPC and help mitigate data exfiltration risk but it doesn't help in data redaction .

Option D is Incorrect because ,Cloud Armour Google Cloud Armor delivers defence at scale against infrastructure and application Distributed Denial of Service (DDoS) attacks using Google's global infrastructure and security systems but it doesn't help in data redaction .

Read more about it here : <https://cloud.google.com/dlp/>

Ask our Experts

Rate this Question?  

View Queries

open 

Question 49

Incorrect

Domain : Other

For future phases, Dress4Win is looking at options to deploy data analytics to the Google Cloud. Which option meets their business and technical requirements?

- A. Run current jobs from the current technical environment on Google Cloud Dataproc. 
- B. Review all current data jobs. Identify the most critical jobs and create Google BigQuery tables to storeand query data.
- C. Review all current data jobs. Identify the most critical jobs and develop Google Cloud Data and pipelines to process data.
- ✓ D. Deploy a Hadoop/Spark cluster to Google Compute Engine virtual machines. Move current jobs fromthe current technical environment and run them on the Hadoop/Spark cluster. 

Explanation:

A (Correct Answer) - There is no requirement to migrate the current jobs to a different technology. Using managed services where possible is a requirement. Using Google Cloud Dataproc which direct maps to existing Data analysis allows the current jobs to be executed within Google Cloud Platform on a managed service offering

Please read the case study to draw the conclusion. A quick relevant summary provided below for your reference: Dress4win Existing Technical Environment.

B - Migrating the existing data jobs to a different technology such as Google BigQuery, is not a requirement.

C - Migrating existing data jobs to a different technology such as Google Cloud Dataflow, is not a requirement.

D - Using managed services where possible is a requirement. The current jobs can run on a Hadoop/Spark cluster in Google Compute Engine but it is not a managed services solution.

Both A and D are technically correct but D against one of tech requirements "Use managed services whenever possible."

Dress4win Existing Technical Environment

Apache Hadoop/Spark servers:

Data analysis

Real-time trending calculations

Technical Requirements

Evaluate and choose an automation framework for provisioning resources in cloud.

Support failover of the production environment to cloud during an emergency.

Identify production services that can migrate to cloud to save capacity.

Use managed services whenever possible.

Encrypt data on the wire and at rest.

Support multiple VPN connections between the production data center and cloud environment.

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

Question 50

Correct

Domain : Other

What activity is carried out after the data is transferred to Transfer Appliance to reverse-compression, deduplication, and encryption which are carried out while transferring the data to a transfer appliance?

A. Link Aggregation

✓ B. Data Rehydration 

- C. Data Capture
- D. Data Recapture

Explanation:

Answer: B

Option B is the Correct choice because Data rehydration is the process by which you fully reconstitute the files so you can access and use the transferred data. To rehydrate data, the data is first copied from the Transfer Appliance to your Cloud Storage staging bucket. The data uploaded to your staging bucket is still compressed, deduplicated, and encrypted. Data rehydration reverses this process and restores your data to a usable state.

Option A is Incorrect because Link aggregation is the bundling of multiple network interfaces (NIC) into a single link, which allows maximum data throughput and redundancy in case of a network connection failure.

Option C is Incorrect because Data capture jobs are used to identify data on your network and stream it to Google Transfer Appliance.

Option D is Incorrect because Data Recapture activity doesn't exist.

Read more about it here: <https://cloud.google.com/transfer-appliance/docs/2.0/data-rehydration>

Ask our Experts

Rate this Question?  

[View Queries](#)

open 

[Finish Review](#)

[Certification](#)[Cloud Certification](#)[Java Certification](#)[PM Certification](#)[Big Data Certification](#)[Company](#)[Become Our Instructor](#)[Support](#)[Discussions](#)[Blog](#)[Business](#)

Follow us



© Copyright 2020. Whizlabs Software Pvt. Ltd. All Right Reserved.