# Mountkirk case study

1. topic question.

For this question, refer to MountKirk Games case study. MountKirk Games wants to migrate from their current analytics and statistics reporting model to one that meets their technical requirements on Google Cloud Platform.

Which two steps should be part of their migration plan?

A. Evaluate the impact of migrating their current batch ETL code to Cloud Dataflow.

B. Write a schema migration plan to denormalize data for better performance in BigQuery.

C. Draw an architecture diagram that show how to move from a single MySQL database to a MySQL cluster.

D. Load 10 TB of analytics data from a previous game into a Cloud SQL instance, and run test queries against the full dataset to confirm that they complete successfully.

E. Integrate Cloud Armor to defend against possible SQL injection attacks in analytics files uploaded to Cloud Storage.

Answer: AB

* denormalize tables definitely will enable better query performance later in BQ.
* https://cloud.google.com/bigquery/docs/loading-data#loading\_denormalized\_nested\_and\_repeated\_data
* C-E seems to be totally unrelated

1. topic question.

For this question, refer to MountKirk Games case study. You need to analyze and define the technical architecture for the database workloads for your company, MountKirk Games. Considering the business and technical requirements, what should you do?

A. Use Cloud SQL for time series data, and use Cloud Bigtable for historical data queries.

B. Use Cloud SQL for to replace MySQL, and use Cloud Spanner for historical data queries.

C. Use Cloud Bigtable to replace MySQL, and use BigQuery for historical data queries.

D. Use Cloud Bigtable for time series data, use Cloud Spanner for transactional data, and use BigQuery for historical data queries.

Answer: D

Time series analytics plus low-latency update ==> BigTable

Transactional data ==> Spanner

Data analytics (without frequent update) 🡺 BQ

1. topic question.

For this question, refer to MountKirk Games case study. MountKirk Games wants you to design a way to test the analytics platform's resilience to changes in mobile network latency. What should you do?

A. Deploy failure injection software to the game analytics platform that can inject additional latency to mobile client analytics traffic.

B. Build a test client that can be run from a mobile phone emulator on a Compute Engine virtual machine, and run multiple copies in Google Cloud Platform regions all over the world to generate realistic traffic.

C. Add the ability to introduce a random amount of delay before beginning to process analytics files uploaded from mobile devices.

D. Create an opt-in beta of the games that runs on player's mobile devices and collect response times from analytics endpoints running in Google Cloud Platform regions all over the world.

Answer: A

Real time test is the ideal test. testing it on emulator, or using random delay will not be suffice

1. topic question.

You are implementing Firestore for Mountkirk Games. Mountkirk Games wants to give a new game programmatic access to a legacy game’s Firestore database.  
Access should be as restricted as possible. What should you do?

A. Create a service account (SA) in the legacy game's Google Cloud project, add a second SA in the new game's IAM page, and then give the Organization Admin role to both SAs.

B. Create a service account (SA) in the legacy game's Google Cloud project, give the SA the Organization Admin role, and then give it the Firebase Admin role in both projects.

C. Create a service account (SA) in the legacy game's Google Cloud project, add this SA in the new game's IAM page, and then give it the Firebase Admin role in both projects.

D. Create a service account (SA) in the legacy game's Google Cloud project, give it the Firebase Admin role, and then migrate the new game to the legacy game's project.

Answer: C

Giving SA the Org. Admin role is overkilled. Remember access should be as restricted as possible

1. topic question.

Mountkirk Games wants to limit the physical location of resources to their operating Google Cloud regions. What should you do?

A. Configure an organizational policy which constrains where resources can be deployed.

B. Configure IAM conditions to limit what resources can be configured.

C. Configure the quotas for resources in the regions not being used to 0.

D. Configure a custom alert in Cloud Monitoring so you can disable resources as they are created in other regions.

Answer: A

Use of org. policy to control resources deployment location. IAM to control access to resource lifecycle(delete,create,shutdown,startup). Quotas is like limit resource capacity/rate. Alert for notification

1. topic question.

You need to implement a network ingress for a new game that meets the defined business and technical requirements. Mountkirk Games wants each regional game instance to be located in multiple Google Cloud regions. What should you do?

A. Configure a global load balancer connected to a managed instance group running Compute Engine instances.

B. Configure kubemci with a global load balancer and Google Kubernetes Engine.

C. Configure a global load balancer with Google Kubernetes Engine.

D. Configure Ingress for Anthos with a global load balancer and Google Kubernetes Engine.

Answer: D

GKE is definitely better choice compares to GCE

Anthos is only required if it’s a case of hybrid environments

1. topic question.

Mountkirk Games' gaming servers are not automatically scaling properly. Last month, they rolled out a new feature, which suddenly became very popular. A record number of users are trying to use the service, but many of them are getting 503 errors and very slow response times. What should they investigate first?

A. Verify that the database is online.

B. Verify that the project quota hasn't been exceeded

C. Verify that the new feature code did not introduce any performance bugs

D. Verify that the load-testing team is not running their tool against production

Answer: B

Explanation: 503 means the server is currently unable to handle the request due to a temporary overloading or maintenance of the server.. If database was offline, everyone would get the 503 error.

1. topic question.

Mountkirk Games wants you to design their new testing strategy. How should the test coverage differ from their existing backends on the other platforms?

A. Tests should scale well beyond the prior approaches

B. Unit tests are no longer required, only end-to-end tests

C. Tests should be applied after the release is in the production environment

D. Tests should include directly testing the Google Cloud Platform (GCP) infrastructure

Answer: A

1. topic 5 question 2

Mountkirk Games has deployed their new backend on Google Cloud. 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 Google Cloud for simulating production load

B. Use the existing infrastructure to test the Google Cloud-based backend at scale

C. Build stress tests into each component of your application using resources internal to Google Cloud to simulate load

D. Create a set of static environment in Google Cloud to test different levels of load - for example, high, medium and low

Answer: A

Best to create the environment in GC instead of using existing environment

1. topic 5 question 3

Mountkirk Games wants to set up a continuous delivery pipeline. Their architecture includes many small services that they want to be able to update and roll back quickly. Mountkirk Games has the following requirements:

* Services are deployed redundantly across multiple regions in the US and Europe
* Only frontend services are exposed on the public internet
* They can provide a single frontend IP for their fleet of services
* Deployment artifacts are immutable

Which set of products should they use?

A. Google Cloud Storage, Google Cloud Dataflow, Google Compute Engine

B. Google Cloud Storage, Google App Engine, Cloud Load Balancer

C. Google Container Registry, Google Container Engine, Google HTTP(S) Load Balancer

D. Google Cloud Functions, Google Cloud Pub/Sub, Google Cloud Deployment Manager

Answer: C

K8s with containers are best combo to deploying small services. Bcos they can be updated quickly and rollback quickly

Container Registry is a place to store built docker images

1. topic 5 question 4

Mountkirk Games’ gaming servers are not automatically scaling properly. Last month, they rolled out a new feature, which suddenly became very popular. A record number of users are trying to use the service, but many of them are getting 503 errors and very slow response times. What should they investigate first?

A. Verify that the database is online

B. Verify that the project quota hasn't been exceeded

C. Verify that the new feature code did not introduce any performance bugs

D. Verify that the load-testing team is not running their tool against production

Answer: B

Keyword “Investigate first?” on why autoscaling not working. after then investigate 503 error and slow response times.

Q14.

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. Kubernetes Engine, Cloud Pub/Sub, and Cloud SQL

B. Cloud Dataflow, Cloud Storage, Cloud Pub/Sub, and BigQuery

C. Cloud SQL, Cloud Storage, Cloud Pub/Sub, and Cloud Dataflow

D. Cloud Dataproc, Cloud Pub/Sub, Cloud SQL, and Cloud Dataflow

E. Cloud Pub/Sub, Compute Engine, Cloud Storage, and Cloud Dataproc

Answer: B

Explanations:

real-time analytics platform ==> BigQuery

real-time low latency update ==> Bigtable

regional with lots of limitation RDBMS ==> Cloud SQL

Q15.

For this question, refer to the Mountkirk Games case study. You are in charge of the new Game Backend Platform architecture. The game communicates with the backend over a REST API.  
You want to follow Google-recommended practices. How should you design the backend?

A. Create an instance template for the backend. For every region, deploy it on a multi-zone managed instance group. Use an L4 load balancer.

B. Create an instance template for the backend. For every region, deploy it on a single-zone managed instance group. Use an L4 load balancer.

C. Create an instance template for the backend. For every region, deploy it on a multi-zone managed instance group. Use an L7 load balancer.

D. Create an instance template for the backend. For every region, deploy it on a single-zone managed instance group. Use an L7 load balancer.

Answer: C

Multi-zone managed instance group with global L7 load balancer

Q16.

You need to optimize batch file transfers into Cloud Storage for Mountkirk Games’ new Google Cloud solution. The batch files contain game statistics that need to be staged in Cloud Storage and be processed by an extract transform load (ETL) tool. What should you do?

A. Use gsutil to batch move files in sequence.

B. Use gsutil to batch copy the files in parallel.

C. Use gsutil to extract the files as the first part of ETL.

D. Use gsutil to load the files as the last part of ETL.

Answer: B

Main objective – optimize batch file transfers into CS

1. topic 5 question 5

Mountkirk Games needs to create a repeatable and configurable mechanism for deploying isolated application environments. Developers and testers can access each other's environments and resources, but they cannot access staging or production resources. The staging environment needs access to some services from production.

What should you do to isolate development environments from staging and production?

A. Create a project for development and test and another for staging and production

B. Create a network for development and test and another for staging and production

C. Create a subnetwork for development and another for staging and production

D. Create one project for development a second staging and a third for production

Answer: D

According to Google best/recommended practice - [link](https://cloud.google.com/appengine/docs/legacy/standard/php/creating-separate-dev-environments)

1. topic 6 question 2

For this question, refer to MountKirk Games case study. You need to analyze and define the technical architecture for the compute workloads for your company, MountKirk Games. Considering the Mo Games business and technical requirements, what should you do?

A. Create network load balancers. Use preemptible Compute Engine instances.

B. Create network load balancers. Use non-preemptible Compute Engine instances.

C. Create a global load balancers with managed instance groups and autoscaling policies. Use preemptible Compute Engine instances.

D. Create global load balancer with managed instance groups and autoscaling policies. Use non-preemptible Compute Engine instances.

Answer-: D

Autoscaler will shutdown instance when there is no traffic. There is no need for preemptible options

1. topic 6 question 3

For this question, refer to the MountKirk Games case study. MountKirk Games wants to design their solution for the future in order to take advantage of cloud and technology improvements as they become available.

Which two steps should they take? Choose 2 answers

A. Store as much analytics and game activity data as financially feasible today so it can be used to train machine learning models to predict user behavior in the future.

B. Begin packaging their game backend artifacts in container images and running them on Google Kubernetes Engine to improve the ability to scale up or down based on game activity

C. Set up a CI/CD pipeline using Jenkins and Spinnaker to automate canary deployments and improve development velocity.

D. Adopt a schema versioning tool to reduce downtime when adding new game features that require storing additional player data in the database.

E. Implement a weekly rolling maintenance process for the Linux virtual machine so they can apply critical kernel patches and package updates and reduce the risk of 0-day vulnerabilities.

Answer: AB

* use ML to predict user’s behaviour
* containerized is better tool compares to source code versioning

1. topic 6 question 6

For this question, refer to the MountKirk case study. Which managed storage option meets MountKirk's technical requirement for storing game activity in a time series database service?

A. Cloud Bigtable

B. Cloud Spanner

C. BigQuery

D. Cloud Datasto

Answer: A

Natural fit for time series data ==> Bigtable

1. topic 7 question 5

Your development teams release new versions of games running on Google Kubernetes Engine (GKE) daily. You want to create service level indicators (SLIs) to evaluate the quality of the new versions from the user’s perspective. What should you do?

A. Create CPU Utilization and Request Latency as service level indicators.

B. Create GKE CPU Utilization and Memory Utilization as service level indicators.

C. Create Request Latency and Error Rate as service level indicators.

D. Create Server Uptime and Error Rate as service level indicators.

Answer: C

Keyword “from user perspective” typically leads to lowest latency requirements

Error rate is better SLI compares to CPU utilization (too general)

1. topic 7 question 6

Mountkirk Games wants you to secure the connectivity from the new gaming application platform to Google Cloud. You want to streamline the process and follow  
Google-recommended practices.

What should you do?

A. Configure Workload Identity and service accounts to be used by the application platform.

B. Use Kubernetes Secrets, which are obfuscated by default. Configure these Secrets to be used by the application platform.

C. Configure Kubernetes Secrets to store the secret, enable Application-Layer Secrets Encryption, and use Cloud Key Management Service (Cloud KMS) to manage the encryption keys. Configure these Secrets to be used by the application platform.

D. Configure HashiCorp Vault on Compute Engine, and use customer managed encryption keys and Cloud Key Management Service (Cloud KMS) to manage the encryption keys. Configure these Secrets to be used by the application platform.

Answer: A

If follow google-recommended practices, that would be to use workload identity and SA to enable Google cloud service from accessing applications in google cloud platform (GCE, GKE)

1. topic 7 question 7

Your development team has created a mobile game app. You want to test the new mobile app on Android and iOS devices with a variety of configurations. You need to ensure that testing is efficient and cost-effective. What should you do?

A. Upload your mobile app to the Firebase Test Lab, and test the mobile app on Android and iOS devices.

B. Create Android and iOS VMs on Google Cloud, install the mobile app on the VMs, and test the mobile app.

C. Create Android and iOS containers on Google Kubernetes Engine (GKE), install the mobile app on the containers, and test the mobile app.

D. Upload your mobile app with different configurations to Firebase Hosting and test each configuration.

Answer: A

Most efficient method to test mobile app is via Firebase

Firebase is merely database solution so it can’t run application

\*\*\*\* MountKirk case questions ended \*\*\*\*

# TerramEarth case study

1. topic question.

For this question, refer to the TerramEarth case study. You start to build a new application that uses a few Cloud Functions for the backend. One use case requires a Cloud Function func\_display to invoke another Cloud Function func\_query. You want func\_query only to accept invocations from func\_display. You also want to follow Google’s recommended best practices. What should you do?

A. Create a token and pass it in as an environment variable to func\_display. When invoking func\_query, include the token in the request. Pass the same token to func\_query and reject the invocation if the tokens are different.

B. Make func\_query 'Require authentication.' Create a unique service account and associate it to func\_display. Grant the service account invoker role for func\_query. Create an id token in func\_display and include the token to the request when invoking func\_query.

C. Make func\_query 'Require authentication' and only accept internal traffic. Create those two functions in the same VPC. Create an ingress firewall rule for func\_query to only allow traffic from func\_display.

D. Create those two functions in the same project and VPC. Make func\_query only accept internal traffic. Create an ingress firewall for func\_query to only allow traffic from func\_display. Also, make sure both functions use the same service account.

Answer: B

Again, according to Google recommended best practices in integrating two services/functions would be using service account.

1. topic question.

For this question, refer to the TerramEarth case study. You are building a microservice-based application for TerramEarth. The application is based on Docker containers. You want to follow Google-recommended practices to build the application continuously and store the build artifacts. What should you do?

A. Configure a trigger in Cloud Build for new source changes. Invoke Cloud Build to build container images for each microservice, and tag them using the code commit hash. Push the images to the Container Registry.

B. Configure a trigger in Cloud Build for new source changes. The trigger invokes build jobs and build container images for the microservices. Tag the images with a version number, and push them to Cloud Storage.

C. Create a Scheduler job to check the repo every minute. For any new change, invoke Cloud Build to build container images for the microservices. Tag the images using the current timestamp, and push them to the Container Registry.

D. Configure a trigger in Cloud Build for new source changes. Invoke Cloud Build to build one container image, and tag the image with the label 'latest.' Push the image to the Container Registry.

Answer: A

Microservice-based ==> Multi-containers.

Build container images ==> Cloud Build

Container registry ==> Stores container images

\*\*\*\* TerramEarth case questions ended \*\*\*\*

1. topic question.

For this question, refer to the TerramEarth case study. You are migrating a Linux-based application from your private data center to Google Cloud. The TerramEarth security team sent you several recent Linux vulnerabilities published by Common Vulnerabilities and Exposures (CVE). You need assistance in understanding how these vulnerabilities could impact your migration. What should you do? (Choose two.)

A. Open a support case regarding the CVE and chat with the support engineer.

B. Read the CVEs from the Google Cloud Status Dashboard to understand the impact.

C. Read the CVEs from the Google Cloud Platform Security Bulletins to understand the impact.

D. Post a question regarding the CVE in Stack Overflow to get an explanation.

E. Post a question regarding the CVE in a Google Cloud discussion group to get an explanation.

Answer: AC

Google Security Bulletins provides detailed reports that describe identified vulnerabilities or weaknesses within GCP services or components. Customer can’t get assistance…

1. topic question.

Today, TerramEarth maintenance workers receive interactive performance graphs for the last 24 hours (86,400 events) by plugging their maintenance tablets into the vehicle. The support group wants support technicians to view this data remotely to help troubleshoot problems. You want to minimize the latency of graph loads.

How should you provide this functionality?

A. Execute queries against data stored in a Cloud SQL.

B. Execute queries against data indexed by vehicle\_id.timestamp in Cloud Bigtable.

C. Execute queries against data stored on daily partitioned BigQuery tables.

D. Execute queries against BigQuery with data stored in Cloud Storage via BigQuery federation.

Answer: B

Bigtable ofc, for low latency update and analytics

1. topic question.

You analyzed TerramEarth’s business requirement to reduce downtime, and found that they can achieve a majority of time saving by reducing customer’s wait time for parts. You decided to focus on reduction of the 3 weeks aggregate reporting time.

Which modifications to the company’s processes should you recommend?

A. Migrate from CSV to binary format, migrate from FTP to SFTP transport, and develop machine learning analysis of metrics

B. Migrate from FTP to streaming transport, migrate from CSV to binary format, and develop machine learning analysis of metrics

C. Increase fleet cellular connectivity to 80%, migrate from FTP to streaming transport, and develop machine learning analysis of metrics

D. Migrate from FTP to SFTP transport, develop machine learning analysis of metrics, and increase dealer local inventory by a fixed factor

Answer: C

Migrate to another transport/format will definitely increases the reporting time. Why not stream straight.

1. topic 8 question.

For this question, refer to the TerramEarth case study. To be compliant with European GDPR regulation, TerramEarth is required to delete data generated from its European Customers after a period of 36 months when it contains personal data. In the new architecture, this data will be stored in both Cloud Storage and BigQuery. What should you do?

A. Create a BigQuery table for the European data, and set the table retention period to 36 months. For Cloud Storage, use gsutil to enable lifecycle management using a DELETE action with an Age condition of 36 months.

B. Create a BigQuery table for the European data, and set the table retention period to 36 months. For Cloud Storage, use gsutil to create SetStorageClass to NON action with an Age condition of 36 months.

C. Create a BigQuery time-partitioned table for the European data, and set the partition expiration period to 36 months. For Cloud Storage, use gsutil to enable lifecycle management using a DELETE action with an Age condition of 36 months.

D. Create a BigQuery time-partitioned table for the European data, and set the partition expiration period to 36 months. For Cloud Storage, use gsutil to create SetStorageClass to NON action with an Age condition of 36 months.

Answer: C

Best answer - Use partitioned table in BQ with expiration date and use lifecycle policies on bucket to delete data after 36 months

1. topic 8 question

For this question, refer to the TerramEarth case study. You need to implement a reliable, scalable Google Cloud solution for the data warehouse for your company, TerramEarth. Considering the TerramEarth business and technical requirements, what should you do?

A. Replace the existing data warehouse with BigQuery. Use table partitioning.

B. Replace the existing data warehouse with a Compute Engine instance with 96 CPUs.

C. Replace the existing data warehouse with BigQuery. Use federated data sources.

D. Replace the existing data warehouse with a Compute Engine instance with 96 CPUs. Add an additional Compute Engine preemptible instance with 32 CPUs.

Answer: A

From case requirements:

Warehouse currently has following:

A single PostgreSQL server

- Redhat Linux

- 64 CPUs

- 128 GB of RAM

- 4x 6TB HDD in RAID 0

Data warehousing for querying or data analytic purposes only - best practice use BigQuery. cheap, fast, scalable

Table partitioning improves query performance and control costs by deleting/reduce number of rows. More informatin on partitioning - <https://cloud.google.com/bigquery/docs/partitioned-tables#when_to_use_partitioning>

Federated data sources is also known as external data source .

1. topic 8 question

Because you do not know every possible future use for the data TerramEarth collects, you have decided to build a system that captures and stores all raw data in case you need it later.

How can you most cost-effectively accomplish this goal?

A. Have the vehicles in the field stream the data directly into BigQuery.

B. Have the vehicles in the field pass the data to Cloud Pub/Sub and dump it into a Cloud Dataproc cluster that stores data in Apache Hadoop Distributed File System (HDFS) on persistent disks.

C. Have the vehicles in the field continue to dump data via FTP, adjust the existing Linux machines, and use a collector to upload them into Cloud Dataproc HDFS for storage.

D. Have the vehicles in the field continue to dump data via FTP, and adjust the existing Linux machines to immediately upload it to Cloud Storage with gsutil.

Answer: D

Why not BQ? Due to Quota , max rows per second per project . hence can’t handle 120 fields/sec. (see technical requirement of TerramEarth)

Options with Dataproc is wrong due to costing on long running and larget amount of HDFS storage

1. topic 8 question 2

The TerramEarth development team wants to create an API to meet the company’s business requirements. You want the development team to focus their development effort on business value versus creating a custom framework.  
Which method should they use?

A. Use Google App Engine with Google Cloud Endpoints. Focus on an API for dealers and partners

B. Use Google App Engine with a JAX-RS Jersey Java-based framework. Focus on an API for the public

C. Use Google App Engine with the Swagger (Open API Specification) framework. Focus on an API for the public

D. Use Google Container Engine with a Django Python container. Focus on an API for the public

E. Use Google Container Engine with a Tomcat container with the Swagger (Open API Specification) framework. Focus on an API for dealers and partners

Answer: A

Keyword “API” ==> Google Cloud Endpoint. It is used to develop, deploy and manage APIs on any google cloud backend. Also with endpoint, you do no need to deploy third-party web server or framework for API lifecycles

1. topic 8 question 3

Your development team has created a structured API to retrieve vehicle data. They want to allow third parties to develop tools for dealerships that use this vehicle event data. You want to support delegated authorization against this data.  
What should you do?

A. Build or leverage an OAuth-compatible access control system

B. Build SAML 2.0 SSO compatibility into your authentication system

C. Restrict data access based on the source IP address of the partner systems

D. Create secondary credentials for each dealer that can be given to the trusted third party

Answer: A

SAML ==>for authentication

OAuth 🡺for authorization

1. topic 8 question 4

TerramEarth plans to connect all 20 million vehicles in the field to the cloud. This increases the volume to 20 million 600 byte records a second for 40 TB an hour.

How should you design the data ingestion?

A. Vehicle write data directly to GCS

B. Vehicle write data directly to Google Cloud Pub/Sub

C. Vehicle stream data directly to Google BigQuery

D. Vehicles continue to write data using existing system (FTP)

Answer: B

Cloud Pub/Sub - Streaming of rather huge amount of data

BQ ==> Data analytics

BigTable ==>Data analytics with low latency updates (time series)

1. topic 8 question 5

You analyzed TerramEarth’s business requirement to reduce downtime and found that they can achieve a majority of time saving by reducing customers’ wait time for parts. You decided to focus on reduction of the 3 weeks’ aggregate reporting time.

Which modifications to the company’s processes should you recommend?

A. Migrate from CSV to binary format, migrate from FTP to SFTP transport, and develop machine learning analysis of metrics.

B. Migrate from FTP to streaming transport, migrate from CSV to binary format, and develop machine learning analysis of metrics.

C. Increase fleet cellular connectivity to 80%, migrate from FTP to streaming transport, and develop machine learning analysis of metrics.

D. Migrate from FTP to SFTP transport, develop machine learning analysis of metrics, and increase dealer local inventory by a fixed factor.

Answer: C

Cell connectivity is important to IoT devices

Machine learning is ideal for predictive maintenance workloads.

1. topic 8 question 6

Which of TerramEarth’s legacy enterprise processes will experience significant change as a result of increased Google Cloud Platform adoption?

A. Opex/capex allocation, LAN changes, capacity planning

B. Capacity planning, TCO calculations, opex/capex allocation

C. Capacity planning, utilization measurement, data center expansion

D. Data Center expansion, TCO calculations, utilization measurement

Answer: B

TCO, Opex and Capex will experience significant change due to cloud adoption

1. topic 8 question 7

To speed up data retrieval, more vehicles will be upgraded to cellular connections and be able to transmit data to the ETL process. The current FTP process is error-prone and restarts the data transfer from the start of the file when connections fail, which happens often. You want to improve the reliability of the solution and minimize data transfer time on the cellular connections.  
What should you do?

A. Use one Google Container Engine cluster of FTP servers. Save the data to a Multi-Regional bucket. Run the ETL process using data in the bucket

B. Use multiple Google Container Engine clusters running FTP servers located in different regions. Save the data to Multi-Regional buckets in US, EU, and Asia. Run the ETL process using the data in the bucket

C. Directly transfer the files to different Google Cloud Multi-Regional Storage bucket locations in US, EU, and Asia using Google APIs over HTTP(S). Run the ETL process using the data in the bucket

D. Directly transfer the files to a different Google Cloud Regional Storage bucket location in US, EU, and Asia using Google APIs over HTTP(S). Run the ETL process to retrieve the data from each Regional bucket

Answer: C

Leveraging multi-regional storage bucket would make more sense

1. topic 8 question 8

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. Move all the data into 1 zone, then launch a Cloud Dataproc cluster to run 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. Launch a cluster in each region to preprocess and compress the raw data, then move the data into a region bucket and use a Cloud Dataproc cluster to finish the job

Answer: D

A&B move all (question says after 100k miles vehicles will breaks down, so no point move all datas)

C is wrong, due to fact Dataproc and the bucket is regional-based

1. topic 8 question 9

TerramEarth has equipped all connected trucks with servers and sensors to collect telemetry data. Next year they want to use the data to train machine learning models. They want to store this data in the cloud while reducing costs.  
What should they do?

A. Have the vehicle's computer compress the data in hourly snapshots, and store it in a Google Cloud Storage (GCS) Nearline bucket

B. Push the telemetry data in real-time to a streaming dataflow job that compresses the data, and store it in Google BigQuery

C. Push the telemetry data in real-time to a streaming dataflow job that compresses the data, and store it in Cloud Bigtable

D. Have the vehicle's computer compress the data in hourly snapshots, and store it in a GCS Coldline bucket

Answer: D

Most cost effective…

1. topic 8 question 10

Your agricultural division is experimenting with fully autonomous vehicles. You want your architecture to promote strong security during vehicle operation.

Which two architecture should you consider? Choose two

A. Treats every micro service call between modules on the vehicle as untrusted

B. Requires IPv6 for connectivity to ensure a secure address space.

C. Use a trusted platform module (TPM) and verify firmware and binaries on boot

D. Use a functional programming language to isolate code execution cycles

E. Use multiple connectivity subsystems for redundancy

F. Enclose the vehicle's drive electronic in a Faraday cage to isolate chips

Answer: AC

Prevent man in the middle attacks between modules

TPM prevent rootkis or other corruptions on root disk

1. topic 8 question 11

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?

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

B. Capture all operating data, train machine learning models that identify ideal operations, and run locally to make operational adjustments automatically

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

D. 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

Answer: B

A – not efficient

C – GCM already been deprecated in 2018

D – not all vehicles are connected in the field.

1. topic 9 question 2

For this question, refer to the TerramEarth case study. TerramEarth has decided to store data files in Cloud Storage. You need to configure Cloud Storage lifecycle rules to store 1 year of data and minimize file storage cost. Which two actions should you take?

A. Create a Cloud Storage lifecycle rule with Age: "30," Storage Class: "Standard," and Action: "Set to Coldline," and create a second Cloud Storage life-cycle rule with Age: "365" Storage Class: "Coldline," and Action: "Delete."

B. Create a Cloud Storage lifecycle rule with Age: "30," Storage Class: "Coldline," and Action: "Set to Nearline," and create a second Cloud Storage life-cycle rule with Age: "91" Storage Class: "Coldline," and Action: "Set to Nearline."

C. Create a Cloud Storage lifecycle rule with Age: "30," Storage Class: "Standard," and Action: "Set to Nearline," and create a second Cloud Storage life-cycle rule with Age: "91" Storage Class: "Nearline," and Action: "Set to Coldline."

D. Create a Cloud Storage lifecycle rule with Age: "30," Storage Class: "Standard," and Action: "Set to Coldline," and create a second Cloud Storage life-cycle rule with Age: "365" Storage Class: "Nearline," and Action: "Delete."

Answer: A

We need to delete data after 1 year. Only option A and D delete data. however option D set to nearline instead of coldline. nearline is 30-days, coldline 90-days, archive 365-days. there is no option to use archive 😉

1. topic 9 question 4

For this question, refer to the TerramEarth case study. A new architecture that writes all incoming data to BigQuery has been introduced. You notice that the data is dirty, and want to ensure data quality on an automated daily basis while managing cost.  
What should you do?

A. Set up a streaming Cloud Dataflow job, receiving data by the ingestion process. Clean the data in a Cloud Dataflow pipeline.

B. Create a Cloud Function that reads data from BigQuery and cleans it. Trigger the Cloud Function from a Compute Engine instance.

C. Create a SQL statement on the data in BigQuery, and save it as a view. Run the view daily, and save the result to a new table.

D. Use Cloud Dataprep and configure the BigQuery tables as the source. Schedule a daily job to clean the data.

Answer: D

A or D can do the job. However to do it on daily while managing costs 🡺dataprep

1. topic 9 question 5

For this question, refer to the TerramEarth case study. Considering the technical requirements, how should you reduce the unplanned vehicle downtime in GCP?

A. Use BigQuery as the data warehouse. Connect all vehicles to the network and stream data into BigQuery using Cloud Pub/Sub and Cloud Dataflow. Use Google Data Studio for analysis and reporting.

B. Use BigQuery as the data warehouse. Connect all vehicles to the network and upload gzip files to a Multi-Regional Cloud Storage bucket using gcloud. Use Google Data Studio for analysis and reporting.

C. Use Cloud Dataproc Hive as the data warehouse. Upload gzip files to a Multi-Regional Cloud Storage bucket. Upload this data into BigQuery using gcloud. Use Google Data Studio for analysis and reporting.

D. Use Cloud Dataproc Hive as the data warehouse. Directly stream data into partitioned Hive tables. Use Pig scripts to analyze data.

Answer: A

Keywords “Connect all vehicles and stream data”

BigQuery ==> data warehouse + data analytic solution

Dataproc ==> purely analytic solution only

1. topic 9 question 6

For this question, refer to the TerramEarth case study. You are asked to design a new architecture for the ingestion of the data of the 200,000 vehicles that are connected to a cellular network. You want to follow Google-recommended practices.  
Considering the technical requirements, which components should you use for the ingestion of the data?

A. Google Kubernetes Engine with an SSL Ingress

B. Cloud IoT Core with public/private key pairs

C. Compute Engine with project-wide SSH keys

D. Compute Engine with specific SSH keys

Answer: B

Ingest data directly from IoT devices on vehicles to IoT core

1. topic 10 question 2

For this question, refer to the TerramEarth case study. You have broken down a legacy monolithic application into a few containerized RESTful microservices.  
You want to run those microservices on Cloud Run. You also want to make sure the services are highly available with low latency to your customers. What should you do?

A. Deploy Cloud Run services to multiple availability zones. Create Cloud Endpoints that point to the services. Create a global HTTP(S) Load Balancing instance and attach the Cloud Endpoints to its backend.

B. Deploy Cloud Run services to multiple regions. Create serverless network endpoint groups pointing to the services. Add the serverless NEGs to a backend service that is used by a global HTTP(S) Load Balancing instance.

C. Deploy Cloud Run services to multiple regions. In Cloud DNS, create a latency-based DNS name that points to the services.

D. Deploy Cloud Run services to multiple availability zones. Create a TCP/IP global load balancer. Add the Cloud Run Endpoints to its backend service.

Answer: B

Cloud Run is regional service. Hence we cannot use global LB or multiple regions directly. they must be placed as NEGS as backend service to global LB.

1. topic 10 question 4

For this question, refer to the TerramEarth case study. TerramEarth has a legacy web application that you cannot migrate to cloud. However, you still want to build a cloud-native way to monitor the application. If the application goes down, you want the URL to point to a “Site is unavailable” page as soon as possible. You also want your Ops team to receive a notification for the issue. You need to build a reliable solution for minimum cost. What should you do?

A. Create a scheduled job in Cloud Run to invoke a container every minute. The container will check the application URL. If the application is down, switch the URL to the "Site is unavailable" page, and notify the Ops team.

B. Create a cron job on a Compute Engine VM that runs every minute. The cron job invokes a Python program to check the application URL. If the application is down, switch the URL to the "Site is unavailable" page, and notify the Ops team.

C. Create a Cloud Monitoring uptime check to validate the application URL. If it fails, put a message in a Pub/Sub queue that triggers a Cloud Function to switch the URL to the "Site is unavailable" page, and notify the Ops team.

D. Use Cloud Error Reporting to check the application URL. If the application is down, switch the URL to the "Site is unavailable" page, and notify the Ops team.

Answer: C

For all the monitoring/notifications – ofc go for google cloud monitoring solution

Other option will just create too much works and hence too costly

1. topic 10 question 6

For this question, refer to the TerramEarth case study. TerramEarth has about 1 petabyte (PB) of vehicle testing data in a private data center. You want to move the data to Cloud Storage for your machine learning team. Currently, a 1-Gbps interconnect link is available for you. The machine learning team wants to start using the data in a month. What should you do?

A. Request Transfer Appliances from Google Cloud, export the data to appliances, and return the appliances to Google Cloud.

B. Configure the Storage Transfer service from Google Cloud to send the data from your data center to Cloud Storage.

C. Make sure there are no other users consuming the 1Gbps link, and use multi-thread transfer to upload the data to Cloud Storage.

D. Export files to an encrypted USB device, send the device to Google Cloud, and request an import of the data to Cloud Storage.

Answer: A

Main concern, huge amount of data 1TB, and very small link 1GBps. That will takes forever to move data.

Dress4win case study

Q1.

The current Dress4win system architecture has high latency to some customers because it is located in one data center. As of a future evaluation and optimizing for performance in the cloud, Dresss4win wants to distribute it's system

architecture to multiple locations within Google Cloud. Which approach should they use?

A. Use regional managed instance groups and a global load balancer to increase performance because the regional managed instance group can grow instances in each region separately based on traffic.

B. Use a global load balancer with a set of virtual machines that forward the requests to a closer group of virtual machines managed by your operations team.

C. Use regional managed instance groups and a global load balancer to increase reliability by providing automatic failover between zones in different regions.

D. Use a global load balancer with a set of virtual machines that forward the requests to a closer group of virtual machines as part of a separate managed instance groups.

Answer: A

Q2.

Dress4Win has asked you to recommend machine types they should deploy their application servers to.

How should you proceed?

A. Perform a mapping of the on-premises physical hardware cores and RAM to the nearest machine types in the cloud.

B. Recommend that Dress4Win deploy application servers to machine types that offer the highest RAM to CPU ratio available.

C. Recommend that Dress4Win deploy into production with the smallest instances available, monitor them over time, and scale the machine type up until the desired performance is reached.

D. Identify the number of virtual cores and RAM associate with the application server VM align them to a custom machine type in the cloud, monitor performance, and scale the machine type up until the desired performance is reached.

Answer: C

Q3.

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

B. In the Cloud Platform Console download the list of the uptime servers' IP addresses and create an inbound firewall rules

C. Configure their load balancer to pass through the User-Agent HTTP header when the value matches GoogleStackdriverMonitoring-UptimeChecks

D. Configure their legacy web servers to allow requests that contain user-Agent HTTP header when the value matches GoogleStackdriverMonitoring-UptimeChecks

Answer: B

Configure rules into firewall

Q4.

The Dress4Win security team has disabled external SSH access into production virtual machines (VMs) on Google Cloud.

The operations team needs to remotely manage the VMs, build and push Docker containers, and manage Google Cloud Storage objects.

What can they do?

A. Grant the operation engineer access to use Google Cloud Shell

B. Configure a VPN connection to Google Cloud to allow SSH access to the cloud VMs.

C. Develop a new access request process that grants temporary SSH access to cloud VMs when an operations engineer needs to perform a task.

D. Have the development team build an API service that allows the operations team to execute specific remote procedure calls to accomplish their tasks.

Answer: A

# JencoMart case study

1. topic question

A few days after JencoMart migrates the user credentials database to Google Cloud Platform and shuts down the old server, the new database server stops responding to SSH connections. It is still serving database requests to the application servers correctly.  
What three steps should you take to diagnose the problem? (Choose three.)

A. Delete the virtual machine (VM) and disks and create a new one

B. Delete the instance, attach the disk to a new VM, and investigate

C. Take a snapshot of the disk and connect to a new machine to investigate

D. Check inbound firewall rules for the network the machine is connected to

E. Connect the machine to another network with very simple firewall rules and investigate

F. Print the Serial Console output for the instance for troubleshooting, activate the interactive console, and investigate

Answer: CDF

Option A&B is wrong - VM still serving database requests, hence cannot delete

Option E – reconnect to another network. this needs to remove the VM from old network and readd to new network.

1. topic 4 question 1

The JencoMart security team requires that all Google Cloud Platform infrastructure is deployed using a least privilege model with separation of duties for administration between production and development resources.  
What Google domain and project structure should you recommend?

A. Create two G Suite accounts to manage users: one for development/test/staging and one for production. Each account should contain one project for every application

B. Create two G Suite accounts to manage users: one with a single project for all development applications and one with a single project for all production applications

C. Create a single G Suite account to manage users with each stage of each application in its own project

D. Create a single G Suite account to manage users with one project for the development/test/staging environment and one project for the production environment

Answer: C

According to Google best practice. General recommendation is to have one project per application per environment. For example, if you have two applications: app1 and app2; each having development and production environments. You will have four projects: app1-dev, app1-prod, app2-dev and app2-prod. This isolates environments from each other, so changes to one do not accidentally impact other. Besides, this setup enables better access control.

1. topic 2 question

JencoMart has built a version of their application on Google Cloud Platform that serves traffic to Asia. You want to measure success against their business and technical goals.  
Which metrics should you track?

A. Error rates for requests from Asia

B. Latency difference between US and Asia

C. Total visits, error rates, and latency from Asia

D. Total visits and average latency for users from Asia

E. The number of character sets present in the database

Answer: C

1. topic 2 question 3

JencoMart has decided to migrate user profile storage to Google Cloud Datastore and the application servers to Google Compute Engine (GCE). During the migration, the existing infrastructure will need access to Datastore to upload the data.  
What service account key-management strategy should you recommend?

A. Provision service account keys for the on-premises infrastructure and for the GCE virtual machines (VMs)

B. Authenticate the on-premises infrastructure with a user account and provision service account keys for the VMs

C. Provision service account keys for the on-premises infrastructure and use Google Cloud Platform (GCP) managed keys for the VMs

D. Deploy a custom authentication service on GCE/Google Kubernetes Engine (GKE) for the on-premises infrastructure and use GCP managed keys for the VMs

Answer: C

Best-practices uses service accounts and managed services as much as possible when migrating data/application to GCP

1. topic 2 question 6

JencoMart wants to move their User Profiles database to Google Cloud Platform.

Which Google Database should they use?

A. Cloud Spanner

B. Google BigQuery

C. Google Cloud SQL

D. Google Cloud Datastore

Answer: D

100%! refer to “*topic 2 question 3”*. Answer in the question xD

\*\*\*\* JencoMart case questions ended \*\*\*\*

# Helicopter Racing League (HRL) case study

1. topic 3 question 1

For this question, refer to the Helicopter Racing League (HRL) case study. Your team is in charge of creating a payment card data vault for card numbers used to bill tens of thousands of viewers, merchandise consumers, and season ticket holders. You need to implement a custom card tokenization service that meets the following requirements:  
\* It must provide low latency at minimal cost.  
\* It must be able to identify duplicate credit cards and must not store plaintext card numbers.  
\* It should support annual key rotation.

Which storage approach should you adopt for your tokenization service?

A. Store the card data in Secret Manager after running a query to identify duplicates.

B. Encrypt the card data with a deterministic algorithm stored in Firestore using Datastore mode.

C. Encrypt the card data with a deterministic algorithm and shard it across multiple Memorystore instances.

D. Use column-level encryption to store the data in Cloud SQL.

Answer: B

Must not store plaintext – encrypt data

minimal cost – Firestore . Multiple memorystore instances is way too expensive

1. topic 3 question 2

For this question, refer to the Helicopter Racing League (HRL) case study. Recently HRL started a new regional racing league in Cape Town, South Africa. In an effort to give customers in Cape Town a better user experience, HRL has partnered with the Content Delivery Network provider, Fastly. HRL needs to allow traffic coming from all of the Fastly IP address ranges into their Virtual Private Cloud network (VPC network). You are a member of the HRL security team and you need to configure the update that will allow only the Fastly IP address ranges through the External HTTP(S) load balancer. Which command should you use?  
A.  
gcloud compute security-policies rules update 1000 \  
–security-policy from-fastly \  
–src-ip-ranges \* \  
–action “allow”

B.  
gcloud compute firewall rules update sourceiplist-fastly \  
–priority 1000 \  
–allow tcp:443

C.  
gcloud compute firewall rules update hlr-policy \  
–priority 1000 \  
–target-tags=sourceiplist-fastly \  
–allow tcp:443

D.  
gcloud compute security-policies rules update 1000 \  
–security-policy hlr-policy \  
–expression “evaluatePreconfiguredExpr(‘sourceiplist-fastly’)” \  
–action “allow”

Answer: D

Firewall rules to restrict between VPC internal networks

Security policies to restrict external networks, must use “evaluatePreconfiguredExpr()”

1. topic 3 question 3

For this question, refer to the Helicopter Racing League (HRL) case study. The HRL development team releases a new version of their predictive capability application every Tuesday evening at 3 a.m. UTC to a repository. The security team at HRL has developed an in-house penetration test Cloud Function called Airwolf. The security team wants to run Airwolf against the predictive capability application as soon as it is released every Tuesday. You need to set up Airwolf to run at the recurring weekly cadence. What should you do?

A. Set up Cloud Tasks and a Cloud Storage bucket that triggers a Cloud Function.

B. Set up a Cloud Logging sink and a Cloud Storage bucket that triggers a Cloud Function.

C. Configure the deployment job to notify a Pub/Sub queue that triggers a Cloud Function.

D. Set up Identity and Access Management (IAM) and Confidential Computing to trigger a Cloud Function.

Answer: C

Triggering Pub/Sub to invoke Cloud Functions seems to be relevant. Cloud Storage doesn't make any sense

<https://cloud.google.com/scheduler/docs/tut-pub-sub>

1. topic 3 question 4

For this question, refer to the Helicopter Racing League (HRL) case study. HRL wants better prediction accuracy from their ML prediction models. They want you to use Google's AI Platform so HRL can understand and interpret the predictions. What should you do?

A. Use Explainable AI.

B. Use Vision AI.

C. Use Google Cloud's operations suite.

D. Use Jupyter Notebooks.

Answer: A

AI Explanations helps you understand your model's outputs for classification and regression tasks. Whenever you request a prediction on AI Platform, AI Explanations tells you how much each feature in the data contributed to the predicted result ([link](https://cloud.google.com/ai-platform/prediction/docs/ai-explanations/overview))

\*\*\*\* Helicopter Racing League (HRL) case questions ended \*\*\*\*

# EHR Healthcare case study

1. topic 4 question 1

For this question, refer to the EHR Healthcare case study. You are responsible for ensuring that EHR’s use of Google Cloud will pass an upcoming privacy compliance audit. What should you do? (Choose two.)

A. Verify EHR's product usage against the list of compliant products on the Google Cloud compliance page.

B. Advise EHR to execute a Business Associate Agreement (BAA) with Google Cloud.

C. Use Firebase Authentication for EHR's user facing applications.

D. Implement Prometheus to detect and prevent security breaches on EHR's web-based applications.

E. Use GKE private clusters for all Kubernetes workloads.

Answer: AB

Google Cloud compliance page present comprehensive list of compliance requirements

BAA means HIPAA. It’s a solid agreement between Google and healthcare industry

1. topic 4 question 2.

For this question, refer to the EHR Healthcare case study. You need to define the technical architecture for securely deploying workloads to Google Cloud. You also need to ensure that only verified containers are deployed using Google Cloud services. What should you do? (Choose two.)

A. Enable Binary Authorization on GKE, and sign containers as part of a CI/CD pipeline.

B. Configure Jenkins to utilize Kritis to cryptographically sign a container as part of a CI/CD pipeline.

C. Configure Container Registry to only allow trusted service accounts to create and deploy containers from the registry.

D. Configure Container Registry to use vulnerability scanning to confirm that there are no vulnerabilities before deploying the workload.

Answer: AD

Binary Authorization – verify deployed container

Vulnerability scanning – scan container for CVE packages/setup

1. topic 4 question 3

You need to upgrade the EHR connection to comply with their requirements. The new connection design must support business-critical needs and meet the same network and security policy requirements. What should you do?

A. Add a new Dedicated Interconnect connection.

B. Upgrade the bandwidth on the Dedicated Interconnect connection to 100 G.

C. Add three new Cloud VPN connections.

D. Add a new Carrier Peering connection.

Answer: A

Best practice to support business-critical needs ==> Dedicated interconnect

Option BCD are all wrong bcos you simply cannot upgrade/add connections to on Dedicated Inteconnect

1. topic 4 question 4

For this question, refer to the EHR Healthcare case study. You need to define the technical architecture for hybrid connectivity between EHR’s on-premises systems and Google Cloud. You want to follow Google’s recommended practices for production-level applications. Considering the EHR Healthcare business and technical requirements, what should you do?

A. Configure two Partner Interconnect connections in one metro (City), and make sure the Interconnect connections are placed in different metro zones.

B. Configure two VPN connections from on-premises to Google Cloud, and make sure the VPN devices on-premises are in separate racks.

C. Configure Direct Peering between EHR Healthcare and Google Cloud, and make sure you are peering at least two Google locations.

D. Configure two Dedicated Interconnect connections in one metro (City) and two connections in another metro, and make sure the Interconnect connections are placed in different metro zones.

Answer: D

One of the technical requirements for connectivity: provide secure and high-performance connection between legacy file- and API-based applications (on-premises) systems and google cloud

1. topic 4 question 5

For this question, refer to the EHR Healthcare case study. You are a developer on the EHR customer portal team. Your team recently migrated the customer portal application to Google Cloud. The load has increased on the application servers, and now the application is logging many timeout errors. You recently incorporated Pub/Sub into the application architecture, and the application is not logging any Pub/Sub publishing errors. You want to improve publishing latency.  
What should you do?

A. Increase the Pub/Sub Total Timeout retry value.

B. Move from a Pub/Sub subscriber pull model to a push model.

C. Turn off Pub/Sub message batching.

D. Create a backup Pub/Sub message queue.

Answer: C

To minimize latency in Pub/Sb, turn off message batching

1. topic 4 question 6

For this question, refer to the EHR Healthcare case study. In the past, configuration errors put public IP addresses on backend servers that should not have been accessible from the Internet. You need to ensure that no one can put external IP addresses on backend Compute Engine instances and that external IP addresses can only be configured on frontend Compute Engine instances. What should you do?

A. Create an Organizational Policy with a constraint to allow external IP addresses only on the frontend Compute Engine instances.

B. Revoke the compute.networkAdmin role from all users in the project with front end instances.

C. Create an Identity and Access Management (IAM) policy that maps the IT staff to the compute.networkAdmin role for the organization.

D. Create a custom Identity and Access Management (IAM) role named GCE\_FRONTEND with the compute.addresses.create permission.

Answer: A

General concept. To set a global policy about configuration - do it with organization policy

1. topic 4 question 7

For this question, refer to the EHR Healthcare case study. You are responsible for designing the Google Cloud network architecture for Google Kubernetes  
Engine. You want to follow Google best practices. Considering the EHR Healthcare business and technical requirements, what should you do to reduce the attack surface?

A. Use a private cluster with a private endpoint with master authorized networks configured.

B. Use a public cluster with firewall rules and Virtual Private Cloud (VPC) routes.

C. Use a private cluster with a public endpoint with master authorized networks configured.

D. Use a public cluster with master authorized networks enabled and firewall rules.

Answer: A

For best security – use private k8s cluster & private endpoint

And according to EHR technical requirements, dedicated interconnection will be used – hence enabling hybrid connection between EHR on-prem and Google VPC networks

\*\*\*\* EHR Healthcare case questions ended \*\*\*\*

# Dress4win case study

1. topic 11 question 1

As part of their new application experience, Dress4Win allows customers to upload images of themselves. The customers has exclusive control over who may view these images.

Customers should be able to upload images with minimal latency and also be shown their images quickly on the main application page when they log in.

Which configuration should Dress4Win use?

A. Store image files in a Google Cloud Storage bucket. Use Google Cloud Datastore to maintain metadata that maps each customer's ID and their image files.

B. Store image files in a Google Cloud Storage bucket. Add custom metadata to the uploaded images in Cloud Storage that contains the customer's unique ID.

C. Use a distributed file system to store customers' images. As storage needs increase, add more persistent disks and/or nodes. Assign each customer a unique I, which sets each file's owner attribute, ensuring privacy of images.

D. Use a distributed file system to store customers' images. As storage needs increase, add more persistent disks and/or nodes. Use a Google Cloud SQL database to maintain metadata that maps each customer's ID to their image files.

Answer: A

Use Datastore to store user's profile data

1. topic 11 question 3

Dress4Win has asked you to recommend machine types they should deploy their application servers to.

How should you proceed?

A. Perform a mapping of the on-premises physical hardware cores and RAM to the nearest machine types in the cloud.

B. Recommend that Dress4Win deploy application servers to machine types that offer the highest RAM to CPU ratio available.

C. Recommend that Dress4Win deploy into production with the smallest instances available, monitor them over time, and scale the machine type up until the desired performance is reached.

D. Identify the number of virtual cores and RAM associated with the application server virtual machines align them to a custom machine type in the cloud, monitor performance, and scale the machine types up until the desired performance is reached.

Answer: D

Option A&B definitely not best practices

Option C will cause user’s connection issue at start

1. topic 11 question 4

For this question, refer to the Dress4Win case study. As part of Dress4Win's plans to migrate to the cloud, they want to be able to set up a managed logging and monitoring system so they can handle spikes in their traffic load. They want to ensure that:

The infrastructure can be notified when it needs to scale up and down to handle the traffic and flow of usage throughout the day.

Their administrators are notified automatically when their application reports errors.

They can filter their aggregated logs down in order to debug one piece of the application across many hosts.

Which Google StackDriver features should they use?

A. Logging, Alerts, Insights, Debug

B. Monitoring, Trace, Debug, Logging

C. Monitoring, Logging, Alerts, Error Reporting

D. Monitoring, Logging, Debug, Error Report

Answer: D

Explanations

Alert to notify!

1. topic 11 question 5

Dress4Win would like to become familiar with deploying applications to the cloud by successfully deploying some applications quickly, as is. They have asked for your recommendation.

What should you advice?

A. Identify self-contained applications with external dependencies as a first move to the cloud.

B. Identify enterprise applications with internal dependencies and recommend these as a first move to the cloud.

C. Suggest moving their in-house databases to the cloud and continue serving requests to on-premise applications.

D. Recommend moving their message queuing servers to the cloud and continue handling requests to on premise applications.

Answer: C

\*\*\*\* Dress4win case questions ended \*\*\*\*

1. topic 11 question 9

For this question, refer to the Dress4Win case study. Dress4Win has end-to-end tests covering 100% of their endpoints. They want to ensure that the move to the cloud does not introduce any new bugs. Which additional testing methods should the developers employ to prevent an outage?

A. They should enable Google Stackdriver Debugger on the application code to show errors in the code.

B. They should add additional unit tests and production scale load tests on their cloud staging environment.

C. They should run the end-to-end tests in the cloud staging environment to determine if the code is working as intended.

D. They should add canary tests so developers can measure how much of an impact the new release causes to latency.

Answer: A

Debugging, code checking on the fly (live application)

1. topic 12 question 1

For this question, refer to the Dress4Win case study, Dress4Win is expecting to grow to 10 times its size in 1 year with a corresponding growth in data and traffic that mirrors the existing patterns of usage. The CIO has set the target of migrating production infrastructure to the cloud within the next 6 months. How will you configure the solution to scale for this growth without making major application changes and still maximize the ROI?

A. Migrate the web application layer to App Engine, and MySQL to Cloud Datastore, and NAS to Cloud Storage, Deploy RabbitMQ, and deploy Hadoop servers using Deployment Manager.

B. Migrate RabbitMQ to Cloud Pub/Sub, Hadoop to BigQuery, and NAS to Compute Engine with Persistent Disk storage. Deploy Tomcat, and deploy Nginx using Deployment Manager.

C. Implement managed instance groups for Tomcat and Nginx. Migrate MySQL to Cloud SQL, RabbitMQ to Cloud Pub/Sub, Hadoop to Cloud Dataproc, and NAS to compute Engine with Persistent Disk storage.

D. Implement managed instance groups for Tomcat and Nginx. Migrate MySQL to Cloud SQL, RabbitMQ to Cloud Pub/Sub, hadoop to Cloud Dataproc, and NAS to Cloud Storage.

Answer: D

Use Managed Instance Group for auto-scaling purpose

Nas to GCE with PD

1. topic 12 question 2

For this question, refer to the Dress4Win case study. Considering the given business requirements, how would you automate the deployment of web and transactional data layers?

A. Deploy Nginx and Tomcat using Cloud Deployment Manager to Compute Engine. Deploy a Cloud SQL server to replace MySQL. Deploy Jenkins using Cloud Deployment Manager.

B. Deploy Nginx and Tomcat using Cloud Launcher. Deploy a MySQL server using Cloud Launcher. Deploy Jenkins to Compute Engine using Cloud Deployment Manager scripts.

C. Migrate Nginx and Tomcat to App Engine. Deploy a Cloud Datastore server to replace the MySQL server in a high-availability configuration. Deploy Jenkins to Compute Engine using Cloud Launcher.

D. Migrate Nginx and Tomcat to App Engine. Deploy a MySQL server using Cloud Launcher. Deploy Jenkins to Compute Engine using Cloud Launcher.

Answer: A

60% on A, 40% on D

Cloud launcher is now known as Marketplace.

1. topic 12 question 3

For this question, refer to the Dress4Win case study. Which of the compute services should be migrated as-is and would still be an optimized architecture for performance in the cloud?

A. Web application deployed using App Engine standard environment.

B. RabbitMQ deployed using an unmanaged instance group.

C. Hadoop/Spark deployed using Cloud Dataproc Regional in High Availability mode.

D. Jenkins, monitoring, bastion hosts, security scanners services deployed on custom machine types.

Answer: A

1. topic 12 question 4

For this question, refer to the Dress4Win case study. Considering the given business requirements, how would you automate the deployment of web and transactional data layers?

A. Deploy Nginx and Tomcat using Deployment Manager to Compute Engine. Deploy a Cloud SQL server to replace MySQL. Deploy Jenkins using Cloud Deployment Manager.

B. Deploy Nginx and Tomcat using Cloud Marketplace . Deploy a MySQL server using Cloud Marketplace. Deploy Jenkins to Compute Engine using Cloud Deployment Manager scripts.

C. Deploy Nginx and Tomcat to App Engine. Deploy a Cloud Datastore server to replace MySQL server in a high-availability configuration. Deploy Jenkins to Compute Engine using Cloud Marketplace.

D. Deploy Nginx and Tomcat to App Engine. Deploy a MySQL server using Cloud Marketplace. Deploy Jenkins to Compute Engine using Cloud Marketplace.

Answer: D

1. topic 12 question 6

For this question, refer to the Dress4Win case study. You want to ensure that your on-premises architecture meets business requirements before you migrate your solution.

What change in the on-premises architecture should you make?

A. Replace RabbitMQ with Google Pub/Sub.

B. Downgrade MySQL to v5.7, which is supported by Cloud SQL for MySQL.

C. Resize compute resources to match predefined Compute Engine machine types.

D. Containerize the micro-services and host them in Google Kubernetes Engine.

Answer: D

# General Qs

1. topic question.

You want to create a private connection between your instances on Compute Engine and your on-premises data center. You require a connection of at least 20 Gpbs. You want to follow Google-recommended practices. How should you set up the connection?

A. Create a VPC and connect it to your on-premises data center using Dedicated Interconnect.

B. Create a VPC and connect it to your on-premises data center using a single Cloud VPN.

C. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises data center using Dedicated Interconnect.

D. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises data center using a single Cloud VPN.

Answer: A

Dedicated Interconnect: provides direct physical connection between your on-premises network and Google's network.

Cloud VPN: securely connects your on-premises network to Google Cloud VPC network thru IPSEC. Traffic travelling between two networks is encrypted by one VPN gateway, then decrypted by another VPN gateway.

Each cloud VPN tunnel can support up to 3 GBs when traffic is traversing a direct peering link or 1.5 GBps when traversing thru public internet.

CDN : leverages Google globally distributed edged points of presence to accelerate content delivery for website and application served out of GCE and GCS. CDN lowers network latency , offloads origins, and reduces serving costs. Caching content at the edges of Google's network provides faster delivery of content to your users while reducing serving costs. CDN interconnect is about egress from the VPC

1. topic 1 question

Your company is using BigQuery as its enterprise data warehouse. Data is distributed over several Google Cloud projects. All queries on BigQuery need to be billed on a single project. You want to make sure that no query costs are incurred on the projects that contains the data. Users should be able to query the datasets, but not edit them. How should you configure users's access roles?

A. Add all users to a group. Grant the group the roles of BigQuery user on the billing project and BigQuery dataViewer on the projects that contain the data.

B. Add all users to a group. Grant the group the roles of BigQuery dataViewer on the billing project and BigQuery user on the projects that contain the data.

C. Add all users to a group. Grant the group the roles of BigQuery jobUser on the billing project and BigQuery dataViewer on the projects that contain the data.

D. Add all users to a group. Grant the group the roles of BigQuery dataViewer on the billing project and BigQuery jobUser on the projects that contain the data.

Answer: A

user roles in BigQuery still able to self-create datasets;

JobUser mainly used to manage job in BigQuery, so they cant list and query data

restarting instances

1. topic question.

A recent audit revealed that a new network was created in your Google Cloud project. In this network, a GCE instance has an SSH port open to the world. You want to discover this network's origin.

What should you do?

A. Search for Create VM entry in the Stackdriver alerting console

B. Navigate to the Activity page in the Home section. Set category to Data Access and search for Create VM entry

C. In the Logging section of the console, specify GCE Network as the logging section. Search for the Create Insert entry

D. Connect to the GCE instance using project SSH keys. Identify previous logins in system logs, and match these with the project owners list

Answer: C

1. topic question.

You want to optimize the performance of an accurate, real-time, weather-charting application. The data comes from 50,000 sensors sending 10 readings a second, in the format of a timestamp and sensor reading.

Where should you store the data?

A. Google BigQuery

B. Google Cloud SQL

C. Google Cloud Bigtable

D. Google Cloud Storage

Answer: C

Keyword “real-time, sensor, huge amount of data per second”

1. topic 1 question

Your organization has 5 TB of private data on premises. You need to migrate the data to Cloud Storage. You want to maximize the data transfer speed. How should you migrate the data?

A. Use gsutil.

B. Use gcloud.

C. Use GCS REST API.

D. Use Transfer Service.

Answer: D

Storage Transfer Service performs online transfer from AWS, another bucket or an HTTP/HTTPS as well as on-prem .

1. topic 1 question 1

Your company has decided to make a major revision of their API in order to create better experiences for their developers. They need to keep the old version of the API available and deployable, while allowing new customers and testers to try out the new API. They want to keep the same SSL and DNS records in place to serve both APIs.

What should they do?

A. Configure a new load balancer for the new version of the API

B. Reconfigure old clients to use a new endpoint for the new API

C. Have the old API forward traffic to the new API based on the path

D. Use separate backend pools for each API path behind the load balancer

Answer: D

100% Keyword is LB with separate backend target pools to route traffic

1. topic 1 question 2

Your company plans to migrate a multi-petabyte data set to the cloud. The data set must be available 24hrs a day. Your business analysts have experience only with using SQL interface.

How should you store the data to optimize it for ease of analysis?

A. Load data into Google BigQuery

B. Insert data into Google Cloud SQL

C. Put flat files into Google Cloud Storage

D. Stream data into Google Cloud Datastore

Answer: A

Analytics with SQL interface

Confirm!

1. topic 1 question 3.

The operations manager asks you for a list of recommended practices that she should consider when migrating a J2EE application to the cloud.

Which three practices should you recommended? Choose 3 answers

A. Port the application code to run on Google App Engine

B. Integrate Cloud Dataflow into the application to capture real-time metrics

C. Select an automation framework to reliably provision the cloud infrastructure

D. Instrument the application with a monitoring tool like Stackdriver Debugger

E. Deploy a continuous integration tool with automated testing in a staging environment

F. Migrate from MySQL to a managed NoSQL database like Google Cloud Datastore or Bigtable

Answer: ADE

The focus Is on the application not the infra on cloud.

Between B and D, capturing telemetry best go with Debugger

Between A and C, App engine already provides the fully managed framework

E is definitely must to test

F no mention about DB.

1. topic 1 question 4

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?  
A screenshot of a computer program

AI-generated content may be incorrect.

A. The session variable is local to just a single instance

B. The session variable is being overwritten in Cloud Datastore

C. The URL to the API needs to be modified to prevent caching

D. The HTTP Expire headers needs to be set to -1 stop caching

Answer: A

100%.

AppEngine spins up new containers automatically according to the load. During peak traffic, HTTP requests originated by the same user could be served by different containers. Given that the variable `sessions` is recreated for each container, it might store different data. The problem here is that this Flask app is stateful. The `sessions` variable is the state of this app. And stateful variables in AppEngine / Cloud Run / Cloud Functions are problematic. A solution would be to store the session in some database (e.g. Firestore, Memorystore) and retrieve it from there. This way the app would fetch the session from a single place and would be stateless.

1. topic 1 question 5

An application development team believes their current logging tool will not meet their needs for their new cloud-based product. They want a better tool to capture errors and help them analyze their historical log data. You want to help them find a solution that meets their needs.

What should you do?

A. Direct them to download and install the Google StackDriver logging agent.

B. Send them a list of online resource about logging best practices

C. Help them define their requirements and assess viable logging tools

D. Help them upgrade their current tool to take advantage of any new features

Answer: A

Definitely use Google Stackdriver Logging

1. topic 1 question 6

You need to reduce the number of unplanned rollbacks of erroneous production deployments in your company's web hosting platform. Improvements to the QA Test processes accomplished an 80% reduction.

Which additional two approaches can you take to further reduce the rollbacks? Choose 2 answers.

A. Introduce a green-blue deployment model

B. Replace the QA environments with canary releases

C. Fragment the monolithic platform into microservices

D. Reduce the platform's dependency on relational database systems

E. Replace the platform's relational database systems with a NoSQL database

Answer: AC

Explanations: Blue-green deployment is a technique that reduces downtime and risk by running two identical production environments called Blue and Green.At any time, only one of the environments is live, with the live environment serving all production traffic. For this example, Blue is currently live and Green is idle.

Canary releases  is a technique to reduce the risk of introducing a new software version in production by slowly rolling out the change to a small subset of users, before rolling it out to the entire infrastructure and making it available to everybody

1. topic 1 question 7

To reduce costs, the Director of Engineering has required all developers to move their development infrastructure resources from on-premises vm to Google Cloud. These resources go through multiple start/stop events during the day and require state to persist. You have been asked to design the process of running a development environment in Google Cloud while providing cost visibility to the finance department.

Which two steps should you take? Choose 2 answer.

A. Use persistent disks to store the state. Start and stop the VM

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

F. Store all state in Google Cloud Storage, snapshot the persistent disks, and terminate the VM

Answer: AD

100%.

B is wrong because requirement is for state to persist.

C no needed.

EF too costly or too much works..

1. topic 1 question 8

Your company wants to track whether someone is present in a meeting room reserved for a scheduled meeting. There are 1000 meeting rooms across 5 offices on 3 continents. Each room is equipped with a motion sensor that reports its status every second. The data from the motion detector includes only a sensor ID and several different discrete items of information. Analysts will use this data, together with information about account owners and office locations.

Which database type should you use?

A. Flat file

B. NoSQL

C. Relational

D. Blobstore

Answer: B

motion sensor is of IoT devices. typically they produced non-sql information

1. topic 1 question 9

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 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 rules exists to allow source traffic on HTTP / HTTPS to reach the load balancer.

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

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

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

Answer: C

100% as VM are being restarted due to health probe carried by LB. For health probes to be carried by LB successfully the firewall must be configured correctly.

1. topic 1 question 10

You write a Python script to connect to Google BigQuery from a Google Compute Engine virtual machine. The script is printing errors that it cannot connect to BigQuery.

What should you do to fix the script?

A. Install the latest BigQuery API client library for Python.

B. Run your script on a new vm with the BigQuery access scope enabled.

C. Create a new service account with BigQuery access and execute your script with that user.

D. Install the bq component for gcloud with the command gcloud components install bq.

Answer: C

Explanation:

Best practice, always use of IAM with service accounts

1. topic 1 question 11

Your customer is moving an existing corporate application to Google Cloud from an on-premises data center. The business owners require minimal user disruption. There are strict security team requirements for storing passwords.

What authentication strategy should they use?

A. Use G Suite Password Sync to replicate passwords into Google.

B. Federate authentication via SAML 2.0 to the existing Identity Provider.

C. Provision users in Google using the Google Cloud Directory Sync tool.

D. Ask users to set their Google password to match their corporate password.

Answer: B

GCDS tool only copies the usernames, not the passwords. Clients need to provide a new password for accessing Google Cloud after GCDS sync. that itself causes much user disruption

1. topic 1 question 12

Your company has successfully migrated to the cloud and wants to analyze their data stream to optimize operations. They do not have any existing code for this analysis, so they are exploring all their options. These options include a mix of batch and stream processing, as they are running some hourly jobs and live-processing some data as it comes in.

Which technology should they use for this?

A. Google Cloud Dataproc

B. Google Cloud Dataflow

C. Google Container Engine with Bigtable

D. Google Compute Engine with Google BigQuery

Answer: B

100%

1. topic 1 question 13

Your customer is receiving reports that their recent 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

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

Answer: C

Keywords “recently updated, and the current behavior was not reported before update”

Trace can identify where is the lag

1. topic 1 question 14

A production database virtual machine on Google Compute Engine has an ext4-formatted persistent disk for data files. The database is about to run out of storage space.

How can you remediate the problem with the least amount of downtime?

A. In the Cloud Platform Console, increase the size of the persistent disk and use the resize2fs command in linux

B. Shut down the virtual machine, use the Cloud Platform Console to increase the persistent disk size, then restart the virtual machine

C. In the Cloud Platform Console, increase the persistent disk size, and verify the new space is ready to use with the fdisk command in Linux

D. In the Cloud Platform Console, create a snapshot of the persistent disk restore the snapshot to a new larger disk, unmount the old disk, mount the new disk and restart the database service

Answer: A

Keyword “resize2fs in linux”

1. topic 1 question 15

Your application needs to process credit card transactions. You want the smallest scope of Payment Card Industry (PCI) compliance without compromising the ability to analyze transactional data and trends relating to which payment methods are used.

How should you design your architecture?

A. Create a tokenizer service and store only tokenized data

B. Create separate projects that only process credit card data

C. Create separate subnetworks and isolate the components that process credit card data

D. Streamline the audit recovery phase by labeling all of the VMs that process PCI data

Answer: A

1. topic 1 question 16

You have been asked to select the storage system for the click-data of your company's large porfolio 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 have been stored for future analysis by your data science and user experience teams.

Which storage infra should you choose?

A. Google Cloud SQL

B. Goolge Cloud Bigtable

C. Google Cloud Storage

D. Google Cloud Datastore

Answer: B

Real-time update

1. topic 1 question 17

You are creating a solution to remove backup files older than 90 days from your backup Cloud Storage bucket. You want to optimize ongoing Cloud Storage spend.

What should you do?

A. Write a lifecycle management rule in XML and push it to the bucket with gsutil

B. Write a lifecycle management rule in JSON and push it to the bucket with gsutil

C. Schedule a cron script using gsutil ls -lr gs://backups/\*\* to find and remove items older than 90 days

D. Schedule a cron script using gsutil ls -l gs://backups/\*\* to find and remove items older than 90 days and schedule it with cron

Answer: B

Using JSON is much more efficient than XML or cron script

1. topic 1 question 18

Your company is forecasting a sharp increase in the number and size of Apache Spark and Hadoop jobs being run on your local datacenter. You want to utilize the cloud to help you scale this upcoming demand with the least amount of operations work and code change.

Which product should you use?

A. Google Cloud Dataflow

B. Google Cloud Dataproc

C. Google Compute Engine

D. Google Container Engine

Answer: B

Explanation:

Dataproc Google platform implementation of Hadoop and Apache Spark

1. topic 1 question 19

The database administration team has asked you to help them improve the performance of their new database server running on Google Compute Engine. The database is for importing and normalizing their performance statistics and is built with MySQL running on Debian Linux. They have an n1-standard-8 virtual machine with 80 GB of SSD persistent disk.

What should they change to get better performance from this system?

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

B. Create a new virtual machine running PostgreSQL

C. Dynamically resize the SSD persistent disk to 500 GB

D. Migrate their performance metrics warehouse to BigQuery

E. Modify all of their batch jobs to use bulk inserts into the database

Answer: C

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

1. topic 1 question 20

You want to optimize the performance of an accurate, real-time, weather-charting application. The data comes from 50,000 sensors sending 10 readings a second, in the format of a timestamp and sensor reading.

Where should you store the data?

A. Google BigQuery

B. Google Cloud SQL

C. Google Cloud Bigtable

D. Google Cloud Storage

Answer: C

100% Natural fit for time series data ==> Bigtable

1. topic 1 question 21

Your company's user-feedback portal comprises a standard LAMP stack replicated across two zones. It is deployed in the US-Central1 region and uses autoscaled managed instance groups on all layers, except the database. Currently only a small group of select customers have access to the portal. The portal meets 99.99% availability SLA under these conditions. However next quarter, you company will be making the portal availability to all users, including unauthorised users. You need to develop a resiliency testing strategy to ensure the system maintains the SLA once they introduce additional user load.

What should you do?

A. Capture existing users input, and replay captured user load until autoscaled is triggered on all layers. At the same time, terminate all resources in one of the zones

B. Create synthetic random user input, replay synthetic load until autoscale logic is triggered on at least one layer, and introduce "chaos" to the system by terminating random resources on both zones

C. Exposes the new system to a larger group of users, and increase group size each day until autoscale logic is triggered on all layers. At the same time, terminate random resources on both zones

D. Capture existing users input, and replay captured user load until resource utilization crosses 80%. Also derive estimated number of users based on existing user's usage of the app, and deploy enough resources to handle 200% of expected load

Answer: B

The best for resilience in to introduce chaos in the infrastructure. ([link](https://cloud.google.com/solutions/scalable-and-resilient-apps#test_your_resilience))

1. topic 1 question 22

One of the developers on your team deployed their application in Google Container Engine with the Dockerfile below. They report that their application deployments are taking too long.

FROM ubuntu:16.04

COPY . /src

RUN apt-get update && apt-get install -y python python-pip

RUN pip install -r requirements.txt

You want to optimize this Dockerfile for faster deployment times without adversely affecting the app's functionality.

Which two actions should you take? Choose 2 answers.

A. Remove Python after running pip

B. Remove dependencies from requirements.txt

C. Use a slimmed-down base image like Alpine Linux

D. Use larger machine types for your Google Container Engine node pools

E. Copy the source after the package dependencies (Python and pip) are installed

Answer:CE

Explanations: Alphine Linux is a minimal docker image with a complete package index and only 5mb in size, and it can fit into RAM

Copy only **after** all packages specified in requirements.txt had installed and running

1. topic 1 question 23

Your solution is producing performance bugs in production that you did not see in staging and test environments. You wants to adjust your test and deployment procedures to avoid this problem in the future.

What should you do?

A. Deploy fewer changes to production

B. Deploy smaller changes to production

C. Increase the load on your test and staging environments

D. Deploy changes to a small subset of users before rolling out to production

Answer: C

Question Statement: You want to adjust your test and deployment procedures to avoid this problem in the future So based on this, I think the option "C" is correct, since it is the only one talking about doing changes in the test environment.

1. topic 1 question 24

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. Send custom metrics for each of your request to Stackdriver Monitoring

C. Use Stackdriver Monitoring to look for insights that show when your API latencies are high

D. Instrument your application with Stackdriver Trace in order to break down the request latencies at each microservice.

Answer: D

Keyword “trace” – for latencies/request take long time and etc

1. topic 1 question 25

During a high traffic portion of the day, one of your relational databases crashes, but the replica is never promoted to a master. You want to avoid this in the future.

What should you do?

A. Use a different database

B. Choose larger instances for your database

C. Create snapshots of your database more regularly

D. Implement routinely scheduled failovers of your databases

Answer: D

Increases the instance size would help prevent the need for failover during high traffic times. However, routinely scheduled failovers would allow the team to test the failover when it is not required. This would make sure it is working when it is required.

1. topic 1 question 26

Your organization requires that metrics from all applications be retained for 5 years for future analysis in possible legal proceedings.

Which approach should you use?

A. Grant the security team access to the logs in each Project

B. Configure Stackdriver Monitoring for all Projects, and export to BigQuery

C. Configure Stackdriver Monitoring for all Projects with default retention policies

D. Configure Stackdriver Monitoring for all Projects, and export to Google Cloud Storage

Answer: D

Explanations:

Monitoring metrics can be exported to BigQuery or Cloud Storage. retention period of 5 years is cost-effective if stored in CS

1. topic 1 question 27

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 private address space communication.

Which networking approach should you use?

A. Google Cloud Dedicated Interconnect

B. Google Cloud VPN connected to the data center network

C. A NAT and TLS translation gateway installed on-premises

D. A Google Compute Engine instance with a VPN server installed connected to the data center network

Answer: A

Keywords “4 TB, large updates are frequent, private address space”

1. topic 1 question 28

Auditors visit your teams every 12 months and ask to review all the Google Cloud Identity and Access Management (Cloud IAM) policy changes in the previous 12 months. You want to streamline and expedite the analysis and audit process.

What should you do?

A. Create custom Google Stackdriver alerts and send them to the auditor

B. Enable logging export to Google BigQuery and use ACLs and views to scope the data shared with the auditor

C. Use cloud functions to transfer log entries to Google Cloud SQL and use ACLs and views to limit an auditor's view

D. Enable Google Cloud Storage (GCS) log export to audit logs into a GCS bucket and delegates access to the bucket

Answer: B

([link](https://cloud.google.com/iam/docs/roles-audit-logging#scenario_external_auditors)) – due to recommended practices

1. topic 1 question 29

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 credential securely.

Where should you store the credentials?

A. In the source code

B. In an environment variable

C. In a secret management system

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

Answer: C

credential = encryption keys

1. topic 1 question 30

A lead engineer wrote a custom tool that deploys vm in the legacy data center. He wants to migrate the custom tool to the new cloud environment. You want to advocate for the adoption of Google Cloud Deployment Manager.

What are two business risks of migrating to Cloud Deployment Manager? Choose 2 answers.

A. Cloud Deployment Manager uses Python

B. Cloud Deployment Manager APIs could be deprecated in the future

C. Cloud Deployment Manager is unfamiliar to the company's engineers

D. Cloud Deployment Manager requires a Google APIs service account to run

E. Cloud Deployment Manager can be used to permanently delete cloud resources

F. Cloud Deployment Manager only supports automation of Google Cloud resources

Answer: CF

Deployment Manager is based on YAML – hence option A-C is not applicable

1. topic 1 question 31

A development manager is building a new application. He asks you to review his requirements and identify what cloud technology he can use to meet them. The application must:

- Be based on open-source technology for cloud portability

- Dynamically scale compute capacity based on demand

- Support continuous software delivery

- Run multiple segregate copies of the same application stack

- Deploy app bundles using dynamic templates

- Route network traffic to specific services based on URL

Which combination of tech will meet all his requirements?

A. Google Kubernetes Engine, Jenkins, and Helm

B. Google Kubernetes Engine, and Cloud Load Balancing

C. Google Kubernetes Engine, and Cloud Deployment Manager

D. Google Kubernetes Engine, Jenkins, and Cloud Load Balancing

Answer: A

Explanations:

to support continous software delivery ==>Jenkins

run multiple segregated copies, dynamic templatest ==>Helm charts

1. topic 1 question 32

You have created several pre-emptible 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 named k99.shutdown in the /etc/rc.6.d/ directory

B. Create a shutdown script registered as a xinetd service in Linux and configure a Stackdriver endpoint check to call the service

C. 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

D. 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

Answer: C

VM’s setting with metadata entry will provide shutdown/startup-script

1. topic 1 question 33

Your organization has a 3-tier web application deployed in the same network on Google Cloud. Each tier (web, API, and database) scales independently of the others Network traffic should flow through the web to the API tier and then on to the database tier. Traffic should not flow between the web and the database tier.

How should you configure the network?

A. Add each tier to a different subnetwork.

B. Set up software based firewalls on individual VMs.

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

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

Answer: D

100%

1. topic 1 question 34

Your development team has installed a new Linux kernel module on the batch servers in Google Compute Engine (GCE) virtual machines (VMs) to speed up the nightly batch process. Two days after the installation, 50% of the batch servers failed the nightly batch run. You want to collect details on the failure to pass back to the development team.

Which three actions should you take? (Choose three.)

A. Use Stackdriver Logging to search for the module log entries

B. Read the debug GCE Activity log using the API or Cloud Console

C. Use gcloud or Cloud Console to connect to the serial console and observe the logs

D. Identify whether a live migration event of the failed server occurred, using in the activity log

E. Adjust the Google Stackdriver timeline to match the failure time, and observe the batch server metrics

F. Export a debug VM into an image, and run the image on a local server where kernel log messages will be displayed on the native screen

Answer: ACE

Option A: definitely must

Option B: Activity log to see Admin activity on GCE. nothing to do with that particular instance

Option C: open console to observe further

Option D: doesn’t make sense

Option E: Adjust timeline, zoom into specific timeline to dig further

Option F: doesn’t make sense

1. topic 1 question 35

Your company wants to try out the cloud with low risk. They want to archive approximately 100 TB of their log data to the cloud and test the analytics features available to them there, while also retaining that data as a long-term disaster recovery backup.

Which two steps should you take? (Choose two.)

A. Load logs into Google BigQuery

B. Load logs into Google Cloud SQL

C. Import logs into Google Stackdriver

D. Insert logs into Google Cloud Bigtable

E. Upload log files into Google Cloud Storage

Answer: AE

archive huge log data = Cloud Storage, analytics = BQ

1. topic 1 question 36

You created a pipeline that can deploy your source code changes to your infrastructure in instance groups for self healing. One of the changes negatively affects your key performance indicator. You are not sure how to fix it and investigation could take up to a week.

What should you do?

A. Log in to a server, and iterate a fix locally.

B. Change the instance group template to the previous one, and delete all instances.

C. Revert the source code change and rerun the deployment pipeline.

D. Log into the servers with the bad code change, and swap in the previous code.

Answer: C

Option A&D – too slow

Option B – too manual/too much works. Furthermore, why delete all instances?

1. topic 1 question 37

Your organization wants to control IAM policies for different departments independently, but centrally. Which approach should you take?

A. Multiple Organizations with multiple Folders.

B. Multiple Organizations, one for each department.

C. A single Organization with Folder for each department.

D. A single Organization with multiple projects, each with a central owner.

Answer: C

Explanations:

Centrally = Single Organization

Folders to contain resources that belong to different dept and assign admin roles on folders to delegate admin privilege

1. topic 1 question 38

You deploy your custom Java application to Google App Engine. It fails to deploy and gives you the following stack trace.

" starting of error message "

java.lang.SecurityException: SHA1 digest error for co/Altostrat/CloakedServlet.class

at com.ggoel.appengine.runtime.Request.process

-d36f818a24b8cf1d (Request.java)

at sun.security.util.ManifestEntryVerifier.verify (ManifestEntryVerifier.java:210)

at java.util.jar.JarVerifier.processEntry (JarVerifier.java:218)

at java.util.jar.JarVerified.update (JarVerifier.java:205)

at java.util.jar.JarVerifiersVerifierStream.read (JarVerifier.java:428)

at java.util.jar.JarVerified.update (JarVerifier.java:205)

at java.net.URL.ClassLoader.defineClass (URLClassLoader.java:273)

at sun.reflect.GenerateMethodAccessor5.invoke (Unknown Source)

...

...

...

" ending of error message "

What should you do?

A. Upload missing JAR files and redeploy your application.

B. Digitally sign all of your JAR files and redeploy your application.

C. Recompile the CloakedServlet class using and MD5 hash instead of SHA1.

D. Change to BigQuery database system.

Answer: C

1. topic 1 question 39

You are designing a mobile chat application. You want to ensure people cannot spoof chat messages, by providing a message that were sent by a specific user.

What should you do

A. Tag messages client side with the originating user identifier and the destination user.

B. Encrypt the message client side using block-based encryption with a shared key.

C. Use public key infrastructure (PKI) to encrypt the message client side using the originating user's private key.

D. Use a trusted certificate authority to enable SSL connectivity between the client application and the server.

Answer: C

Explanations:

block-based encryption refers to disk/raw disk that were zoned thru SAN-based protocol

SSL requires server to have signed cert and does not validate client

1. topic 1 question 41

Your customer support tool logs all email and chat conversations to Cloud Bigtable for retention and analysis. What is the recommended approach for sanitizing this data of personality identifiable information or payment card information before initial storage?

A. Hash all data using SHA256.

B. Encrypt all data using elliptic curve cryptography.

C. De-identify the data with the Cloud Data Loss Prevention API.

D. Use regular expression to find and redact phone numbers, email addresses, and credit card numbers.

Answer: C

1. topic 1 question 42

You are using Cloud Shell and need to install a custom utility for use in a few weeks. Where can you store the file so it is in the default execution path and persists across sessions?

A. ~/bin

B. Cloud Storage

C. /google/scripts

D. /usr/local/bin

Answer: A

Cloud Shell provisions 5 GB of free persistent disk storage mounted as your $HOME directory on the virtual machine instance. This storage is on a per-user basis and is available across projects.

1. topic 1 question 43

You want to create a private connection between your instances on Compute Engine and your on-premises data center. You require a connection of at least 20

Gbps. You want to follow Google-recommended practices. How should you set up the connection?

A. Create a VPC and connect it to your on-premises data center using Dedicated Interconnect.

B. Create a VPC and connect it to your on-premises data center using a single Cloud VPN.

C. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises data center using Dedicated Interconnect.

D. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises datacenter using a single Cloud VPN.

Answer: A

100% Cloud VPN can only offers upto 5Gps

1. topic 1 question 44

You are analyzing and defining business processes to support your startup's trial usage of Google Cloud, and you don't yet know what consumer demand for your product will be. Your manager requires you to minimize Google Cloud service costs and adhere to Google best practices. What should you do?

A. Utilize free tier and sustained use discounts. Provision a staff position for service cost management.

B. Utilize free tier and sustained use discounts. Provides training to the team about service cost management.

C. Utilize free tier and committed use discounts. Provision a staff position for service cost management.

D. Utilize free tier and committed use discounts. Provides training to the team about service cost management.

Answer: B

Committed(CD) vs Sustained(SD)

- CD is best for stable and predictable workloads. commited to pay regardless whether resource are utilized or not!

- CD periods are 1 or 3yrs

- SD is like incremental discount when you kept using the resources. Discount increases with usage and get up to 30% for instance that run the entire month.

- SD useful with Esp. VMs created by GKE and GCE. Not usefull with GAE or GC Dataflow.

- Retaining staff is more cost effective than hiring new staff based on general practices

1. topic 1 question 45

You are building a continuous deployment pipeline for a project stored in Git source repository and want to ensure that code changes can be verified before deploying to production. What should you do?

A. Use Spinnaker to deploy builds to production using the red/black deployment strategy so that changes can easily be rolled back.

B. Use Spinnaker to deploy builds to production and run tests on production deployments.

C. Use Jenkins to build the staging branches and the master branch. Build and deploy changes to production for 10% of users before doing a complete rollout.

D. Use Jenkins to monitor tags in the repository. Deploy staging tags to a staging environment for testing. After testing, tag the repository for production and deploy that to the production environment.

Answer: D

tagging is a best practice that is recommended on Jenkins/Spinnaker to deploy the right code and prevent accidentally (or intentionally) push of wrong code to production environments.

1. topic 1 question 46

A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places.

Which Storage solution are they allowed to use?

A. Cloud Bigtable

B. Cloud BigQuery

C. Compute Engine SSD Disk

D. Compute Engine Persistent Disk

Answer: B

Keyword “automatically replicate” --> BigQuery transparently and automatically provides highly durable, replicated storage in multiple locations and high availability with no extra charge and no additional setup.

<https://cloud.google.com/bigquery-transfer/docs/locations>

1. topic 1 question 47

Your company is migrating its on-premises data center into the cloud. As part of the migration, you want to integrate Google Kubernetes Engine (GKE) for workload orchestration. Parts of your architecture must also be PCI DSS-compliant. Which of the following is most accurate?

A. App Engine is the only compute platform on Google Cloud that is certified for PCI DSS hosting.

B. GKE cannot be used under PCI DSS because it is considered shared hosting.

C. GKE and Google Cloud provide the tools you need to build a PCI DSS-compliant environment.

D. All Google Cloud services are usable because Google Cloud is certified PCI-compliant.

Answer: D

All GC services are certified!

1. topic 1 question 48

Your company has multiple on-premises systems that serve as sources for reporting. The data has not been maintained well and has become degraded over time. You want to use Google-recommended practices to detect anomalies in your company data. What should you do?

A. Upload your files into Cloud Storage. Use Cloud Datalab to explore and clean your data.

B. Upload your files into Cloud Storage. Use Cloud Dataprep to explore and clean your data.

C. Connect Cloud Datalab to your on-premises systems. Use Cloud Datalab to explore and clean your data.

D. Connect Cloud Dataprep to your on-premises systems. Use Cloud Dataprep to explore and clean your data.

Answer: B

Datalab tool is like NOTEBOOK in the CLOUD. provides user to write down notes, charting, and etc

Dataprep tool is for transforming, preparing data , clean data for further data analysis. Unfortunately both can’t connect directly to systems on-premises

1. topic 1 question 49

Google Cloud Platform resources are managed hierarchically using organization, folders, and projects. When Cloud Identity and Access management (IAM) policies exist at these different levels, what is the effective policy at a particular node of the hierarchical??

A. The effective policy is determined only by the policy set at the node.

B. The effective policy is the policy set at the node and restricted by the policies of its ancestors.

C. The effective policy is the union of the policy set at the node and policies inherited from its ancestors.

D. The effective policy is the intersection of the policy set at the node and policies inherited from its ancestors.

Answer: C

Reference: <https://cloud.google.com/iam/docs/resource-hierarchy-access-control>

1. topic 1 question 50

You are migrating your on-premises solution to Google Cloud in several phases. You will use Cloud VPN to maintain a connection between your on-premises systems and Google Cloud until the migration is completed. You want to make sure all your on-premises systems remain reachable during this period. How should you organize your networking in Google Cloud?

A. Use the same IP range on Google Cloud as you use on-premises.

B. Use the same IP range on Google Cloud as you use on-premises for your primary IP range and use a secondary range that does not overlap with the range you use on-premises.

C. Use an IP range on Google Cloud that does not overlap with the range you use on-premises.

D. Use an IP range on Google Cloud that does not overlap with the range you use on-premises for your primary IP range and use a secondary range with the same IP range as you use on-premises.

Answer: C

Primary IP address range: are used for VM primary internal IP addresses, VM alias IP addresses, and internal load balancers

Secondary IP address range: are used only for alias IP addresses. Can define up to 5 secondary IP address ranges.

1. topic 1 question 51

You have found an error in your App Engine application caused by missing Cloud Datastore indexes. You have created a YAML file with the required indexes and want to deploy these new indexes to Cloud Datastore. What should you do?

A. Point gcloud datastore create-indexes to your configuration file.

B. Upload the configuration file to App Engine's default Cloud Storage bucket, and have App Engine detect the new indexes.

C. In the Google Cloud Console, use Datastore admin to delete the current indexes and upload the new configuration file.

D. Create an HTTP request to the built-in python module to send the index configuration file to your application.

Answer: A

Reference :<https://cloud.google.com/sdk/gcloud/reference/datastore/create-indexes>

1. topic 1 question 52

You have an application that will run on Compute Engine. You need to design an architecture that takes into account a disaster recovery plan that requires your application to fail over to another region in case of a regional outage. What should you do?

A. Deploy the application on two Compute Engine instances in the same project but in different region.

Use the first instance to serve traffic, and use the HTTP load balancing service to fail over to the standby instance in a case of a disaster.

B. Deploy the application on a Compute Engine instance. Use the instance to serve traffic, and use HTTP load balancing service to fail over to an instance on your premises in case of a disaster.

C. Deploy the application on two Compute Engine instance groups, each in the same project but in a different region.

Use the first instance group to serve traffic, and use the HTTP load balancing service to fail over to the standby instance group in case of a disaster.

D. Deploy the application on two Compute Engine instance groups, each in a separate project and a different region.

Uses the first instance group to server traffic, and use the HTTP load balancing service to fail over to the standby instance group in case of a disaster.

Answer: C

Explanations:

LB with IG is the best practices .

1. topic 1 question 53

You are deploying an application on App Engine that needs to integrate with an on-premises database. For security purposes, your on-premises database must not be accessible through the public internet. What should you do?

A. Deploy your application on App Engine standard environment and use App Engine firewall rules to limit access to the on-premises database.

B. Deploy your application on App Engine standard environment and use Cloud VPN to limit access to the on-premises database.

C. Deploy your application on App Engine flexible environment and use App Engine firewall rules to limit access to the on-premises database.

D. Deploy your application on App Engine flexible environment and use Cloud VPN to limit access to the on-premises database.

Answer: D

To customize App engine, must use flexible environment.

Firewall in Google Cloud generally used to control incoming but not outgoing.

1. topic 1 question 54

You're working in a highly secured environment where public internet access from the Compute Engine VMs is not allowed. You do not yet have a VPN connection to access an on-premises file server. You need to install specific software on a Compute Engine instance. How should you install the software?

A. Upload the required installation files to Cloud Storage. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gsutil.

B. Upload the required installation files to Cloud Storage and use firewall rules to block all traffic except the IP address range for Cloud Storage. Download the files to the VM using gsutil.

C. Upload the required installation files to Cloud Source Repositories. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gcloud.

D. Upload the required installation files to Cloud Source Repositories and use use firewall rules to block all traffic except the IP address range for Cloud Storage. Download the files to the VM using gsutil.

Answer: A

Explanations :

Without Public IP - no problem - use Private Google Access options

1. topic 1 question 55

Your company is moving 75 TB of data into Google Cloud. You want to use Cloud Storage and follow Google-recommended practices. What should you do?

A. Move your data onto a Transfer Appliance. Use a Transfer Appliance Rehydrator to decrypt the data into Cloud Storage.

B. Move your data onto a Transfer Appliance. Use Cloud Dataprep to decrypt the data into Cloud Storage.

C. Install gsutil on each server that contains data. Use resumable transfers to upload the data into Cloud Storage.

D. Install gsutil on each server containing data. Use Streaming transfers to upload the data into Cloud Storage.

Answer: A

Anytime requires large amount of data to be transfer into Google Cloud ==> Use Transfer Appliance

1. topic 1 question 56

You have an application deployed on Google Kubernetes Engine using a Deployment named echo-deployment. The deployment is exposed using a Service called echo-service. You need to perform an update to the application with minimal downtime to the application. What should you do?

A. Use kubectl set image deployment/echo-deployment <new-image>.

B. Use the rolling update functionality of the Instance Group behind the Kubernetes cluster.

C. Update the deployment yaml file with the new container image. Use kubectl delete deployment/echo-deployment and kubectl create -f <yaml-file>.

D. Update the service yaml file with the new container image. Use kubectl delete service/echo-service and kubectl create -f <yaml-file>.

Answer: A

Only option A make sense. by set image to new image/tag, k8s will perform rolling update onto the deployment.

1. topic 1 question 57

Your company is using BigQuery as its enterprise data warehouse. Data is distributed over several Google Cloud projects. All queries on BigQuery need to be billed on a single project. You want to make sure that no query costs are incurred on the projects that contain the data. Users should be able to query the datasets, but not edit them.

How should you configure users' access roles?

A. Add all users to a group. Grant the group the role of BigQuery user on the billing project and BigQuery dataViewer on the projects that contain the data.

B. Add all users to a group. Grant the group the roles of BigQuery dataViewer on the billing project and BigQuery user on the projects that contain the data.

C. Add all users to a group. Grant the group the roles of BigQuery jobUser on the billing project and BigQuery dataViewer on the projects that contain the data.

D. Add all users to a group. Grant the group the roles of BigQuery dataViewer on the billing project and BigQuery jobUser on the projects that contain the data.

Answer: C

100% using the principle of least privileges

1. topic 1 question 58

You have developed an application using Cloud ML Engine that recognizes famous paintings from uploaded images. You want to test the application and allow specific people to upload images for the next 24 hours. Not all users have a Google Account. How should you have users upload images?

A. Have users upload the images to Cloud Storage. Protect the bucket with a password that expires after 24 hours.

B. Have users upload the images to Cloud Storage using a signed URL that expires after 24 hours.

C. Create an App Engine web application where users can upload images. Configure App Engine to disable the application after 24 hours. Authenticate users via Cloud Identity.

D. Create an App Engine web application where users can upload images for the next 24 hours. Authenticate users via Cloud Identity.

Answer: B

Signed URL : <https://cloud.google.com/storage/docs/access-control/signed-urls>

it provides a way to give time-limited read or write access to anyone in possession of the URL, regardless of whether they have google account.

1. topic 1 question 59

Your web application must comply with the requirements of the EU's General Data Protection Regulation (GDPR). You are responsible for the technical architecture of your web application. What should you do?

A. Ensure that your web application only uses native features and services of Google Cloud, because Google already has various certifications and provides "pass-on" compliance when you use native features.

B. Enable the relevant GDPR compatibility setting within the Google Cloud Console for each of the services in use within your application.

C. Ensure that Cloud Security Scanner is part of your test planning strategy in order to pick up any compliance gaps.

D. Define a design for the security of data in your web application that meets GDPR requirements.

Answer: D

<https://cloud.google.com/security/gdpr>

1. topic 1 question 60.

You need to set up Microsoft SQL Server on GCP. Management requires that there's no downtime in case of a data center outage in any of the zones within a Google Cloud region. What should you do?

A. Configure a Cloud SQL instance with high-availability enabled.

B. Configure a Cloud Spanner instance with a regional instance configuration.

C. Set up SQL Server on Compute Engine, using Always On Availability Groups using Windows Failover Clustering. Place nodes in different subnets.

D. Set up SQL Server Always On Availability Groups using Windows Failover Clustering. Place nodes in different zones.

Answer: A

Option A is solid fully managed and support additional replica for HA design. Cloud SQL is regional resource. However HA configuration supports secondary zeon within configured region.

Option D is possible too. But too much works, customized and configured manually by customer.

1. topic 1 question 61

The development team has provided you with a kubernetes Deployment file. You have no infrastructure yet and need to deploy the application. What should you do?

A. Use gcloud to create a kubernetes cluster. Use Deployment Manager to create the deployment.

B. Use gcloud to create a kubernetes cluster. Use kubectl to create the deployment.

C. Use kubectl to create a kubernetes cluster. Use Deployment Manager to create the deployment.

D. Use kubectl to create a kubernetes cluster. Use kubectl to create the deployment.

Answer: B

Explanation:

Definitely need to use gcloud to first create the kubernetes cluster

1. topic 1 question 62

You need to evaluate your team readiness for a new Google Cloud project. You must perform the evaluation and create a skills gap plan which incorporates the business goal of cost optimization. Your team has deployed two Google Cloud projects successfully to date. What should you do?

A. Allocate budget for team training. Set a deadline for the new Google Cloud project.

B. Allocate budget for team training. Create a roadmap for your teammate to achieve GC certification based on job role.

C. Allocate budget to hire skilled external consultants. Set a deadline for the new Google Cloud project.

D. Allocate budget to hire skilled external consultants. Create a roadmap for your teammate to achieve GC certification based on job role.

Answer: B

Keyword – certification

1. topic 1 question 63

You are designing an application for use only during business hours. For the minimum viable product release, you'd like to use a managed product that automatically "scales to zero" so you don't incur costs when there is no activity. Which primary compute resource should you choose?

A. Cloud Functions

B. Compute Engine

C. Google Kubernetes Engine

D. AppEngine flexible environment

Answer: A

Managed product and scales to zero = Cloud Functions

1. topic 1 question 64

You are creating an App Engine application that uses Cloud Datastore as its persistence layer. You need to retrieve several root entities for which you have the identifiers. You want to minimize the overhead in operations performed by Cloud Datastore. What should you do?

A. Create the key object for each Entity and run a batch get operation.

B. Create the key object for each Entity and run multiple get operations, one operation for each entity.

C. Use the identifiers to create a query filter and run a batch query operation.

D. Use the identifiers to create a query filter and run multiple query operations, one operation for each entity.

Answer: A

100% Batch operations instead of single operations . They are more efficient bcos they perform multiple operations with same overhead as a single operaiton

1. topic 1 question 65

You need to upload files from your on-premises environment to Cloud Storage. You want the files to be encrypted on Cloud Storage using customer-supplied encryption keys. What should you do?

A. Supply the encryption key in a .boto configuration file. Use gsutil to upload the files.

B. Supply the encryption key in using gcloud config. Use gsutil to upload the files to that bucket.

C. Use gsutil to upload the files, and use the flag --encryption-key to supply the encryption key.

D. Use gsutil to create a bucket, and use the flag --encryption-key to supply the encryption key. Use gsutil to upload the files to that bucket.

Answer: A

gsutil accepts customer-supplied encryption keys (CSEK) for interacting with GC Storage using JSON API. The keys are provided via .boto configuration file

1. topic 1 question 66

Your customer wants to capture multiple GBs of aggregate real-time key performance indicators (KPIs) from their game servers running on Google Cloud and monitor the KPIs with low latency. How should they capture the KPIs?

A. Store time-series data from the game servers in Google Bigtable, and view it using Google Data Studio

B. Output custom metrics to Stackdriver from the game servers, and create a Dashboard in Stackdriver Monitoring Console to view them.

C. Schedule BigQuery load jobs to ingest analytics files uploaded to Cloud Storage every ten minutes, and visualize the results in Google Data Studio.

D. Insert the KPIs into Cloud Datastore entities, and run ad hoc analysis and visualization of them in Cloud Datalab.

Answer:A

Explanations:

- Bigtable & Datastore: NoSQL , unstructural and best use with real-time data analytics

- BigQuery: SQL similar , best with structural data

- Stackdrivers :meant to monitor/logging of Google Cloud services/components not user's data

1. topic 1 question 67

You have a Python web application with many dependencies that requires 0.1 CPU cores and 128 MB of memory to operate in production. You want to monitor and maximize machine utilization. You also want to reliably deploy new versions of the application. Which set of steps should you take?

A. Perform the following:

1. Create a managed instance group with f1-micro type machines.

2. Use a startup script to clone the repository, check out the production branch, install the dependencies, and start the Python app.

3. Restart the instances to automatically deploy new production releases.

B. Perform the following:

1. Create a a managed instance group with n1-standard-1 type machines.

2. Build a Compute Engine image from the production branch that contains all of the dependencies and automatically starts the Python app.

3. Rebuild the Compute Engine image, and update the instance template to deploy new production releases.

C. Perform the following:

1. Create a Google Kubernetes Engine (GKE) cluster with n1-standard-1 type machines.

2. Build a Docker image from the production branch with all of the dependencies, and tag it with the version number.

3. Create a Kubernetes Deployment with the imagePullPolicy set to "IFNotPresent" in the staging namespace, and then promote it to the production namespace after testing.

D. Perform the following:

1. Create a GKE cluster with n1-standard-4 type machines.

2. Build a Docker image from the master branch with all of the dependencies, and tag it with "latest.

3. Create a kubernetes Deployment in the default namespace with the imagePullPolicy set to "Always". Restart the pods to automatically deploy new production releases.

Answer: A

1. topic 1 question 68

Your company wants to start using Google Cloud resources but wants to retain their on-premises Active Directory domain controller for identity management. What should you do?

A. Use the Admin Directory API to authenticate against the AD DC.

B. Use Google Cloud Directory Sync to synchronize AD usernames with cloud identities and configure SAML SSO.

C. Use Cloud Identity-Aware Proxy configured to use the on-premises AD DC as an identity provider.

D. Use Compute Engine to create an AD DC that is a replica of the on-premises AD DC using Google Cloud Directory Sync.

Answer: B

easiest to sync credentials (identity) from on-prem

1. topic 1 question 69

You are running a cluster on Google Kubernetes Engine (GKE) to serve a web application. Users are reporting that a specific part of the application is not responding anymore. You notice that all pods of your deployment keep restarting after 2 seconds. The application writes logs to standard outputs. You want to inspect the logs to find the cause of the issue. Which approach can you take?

A. Review the Stackdriver logs for each Compute Engine instance that is serving as a node in the cluster.

B. Review the Stackdriver logs for the specific GKE container that is serving the unresponsive part of the application.

C. Connect to the cluster using gcloud credentials and connect to a container in one of the pods to read the logs.

D. Review the Serial Port logs for each Compute Engine instance that is serving as a node in the cluster.

Answer: B

1. topic 1 question 70

You are using a single Cloud SQL instance to serve your application from a specific zone. You want to introduce high availability. What should you do?

A. Create a read replica instance in a different region.

B. Create a failover replica instance in a different region.

C. Create a read replica instance in the same region, but in a different zone.

D. Create a failover replica instance in the same region, but in a different zone.

Answer: D

Failover replica must be in same region, but can be in different zone

refer to <https://cloud.google.com/sql/docs/mysql/high-availability>

1. topic 1 question 71

Your company is running a stateless application on a Compute Engine instance. The application is used heavily during regular business hours and lightly outside of business hours. Users are reporting that the application is slow during peak hours. You need to optimize the application's performance. What should you do?

A. Create a snapshot of the existing disk. Create an instance template from the snapshot. Create an autoscaled managed instance group from the instance template.

B. Create a snapshot of the existing disk. Create a custom image from the snapshot. Create an autoscaled managed instance group from the custom image.

C. Create a custom image from the existing disk. Create an instance template from the custom image. Create an autoscaled managed instance group from the instance template.

D. Create an instance template from the existing disk. Create a custom image from the instance template. Create an autoscaled managed instance group from the custom image.

Answer: C

Explanations:

Snapshots are primarily used for backup and disaster recovery

Existing disks > Custom image > Instance Template > Instance Group

1. topic 1 question 72

Your web application has several VM instances running within a VPC. You want to restrict communications between instances to only the paths and ports you authorize, but you don't want to rely on static IP addresses or subnets because the application can autoscale. How should you restrict communication?

A. Use separate VPCs to restrict traffic.

B. Use firewall rules based on network tags attached to the compute instance.

C. Use Cloud DNS and only allow connections from authorized hostnames.

D. Use service accounts and configure the web application to authorize particular service accounts to have access.

Answer: B

1. topic 1 question 73

You are using Cloud SQL as the database backend for a large CRM deployment. You want to scale as usage increases and ensure that you don't run off out of storage, maintain 75% CPU usage cores, and keep replication lag below 60 seconds. What are the correct steps to meet your requirements?

A.

1. Enable automatic storage increase for the instance.

2. Create a Stackdriver alert when CPU usage exceeds 75%, and change the instance type to reduce CPU usage.

3. Create a Stackdriver alert for replication lag, and shard the database to reduce replication time.

B.

1. Enable automatic storage increase for the instance.

2. Change the instance type to a 32-core machine type to keep CPU usage below 75%.

3. Create a Stackdriver alert for replication lag, and deploy memcache to reduce load on the master.

C.

1. Create a Stackdriver alert when storage exceeds 75%, and increase the available storage on the instance to create more space.

2. Deploy memcached to reduce CPU load.

3. Change the instance type to a 32-core machine type to reduce replication lag.

D.

1. Create a Stackdriver alert when storage exceeds 75%, and increase the available storage on the instance to create more space.

2. Deploy memcached to reduce CPU load.

3. Create a Stackdriver alert for replication lag, and change the instance type to a 32-core machine type to reduce replication lag.

Answer: A

Sharding is a type of db partitionoing that separates very large db into smaller faster, more easily managed parts called data shards

1. topic 1 question 74

You are tasked with building an online analytical processing (OLAP) marketing analytics and reporting tool. This requires a relational database that can operate on hundreds of terabytes of data. What is the Google recommended tool for such applications?

A. Cloud Spanner, because it is globally distributed

B. Cloud SQL, because it is a fully managed relational database.

C. Cloud Firebase, because it offers real-time synchronization across devices.

D. BigQuery, because it is designed for large-scale processing of tabular data.

Answer: D

Keywords: relational db means Cloud SQL or Spanner. Spanner for horizontal scalability

Cloud SQL storage is limited to 30TB

Cloud Spanner 2tb/node , max of 25 nodes

1. topic 1 question 77

You want to establish a Compute Engine application in a single VPC across two regions. The application must communicate over VPN to an on-premises network. How should you deploy the VPN?

A. Use VPC Network Peering between the VPC and the on-premises network.

B. Explore the VPC to the on-premises network using IAM and VPC Sharing.

C. Create a global Cloud VPN Gateway with VPN tunnels from each region to the on-premises peer gateway.

D. Deploy Cloud VPN Gateway in each region. Ensure that each region has at least one VPN tunnel to the on-premises peer gateway.

Answer: C

1. topic 1 question 75

You have deployed an application to Google Kubernetes Engine (GKE), and are using the Cloud SQL proxy container to make the Cloud SQL database available to the services running on Kubernetes. You are notified that the application is reporting database connection issues. Your company policies require a post-mortem. What should you do?

A. Use gcloud sql instances restart.

B. Validate that the Service Account used by the Cloud SQL proxy container still has the Cloud Build Editor role.

C. In the Google Cloud Console, navigate to Stackdriver Logging. Consult logs for GKE and Cloud SQL.

D. In the Google Cloud Console, navigate to Cloud SQL. Restore the latest backup. Use kubectl to restart all pods.

Answer: C

Explanation: require post-mortem means further investigation. checking logs would be the logical step

1. topic 1 question 76

Your company pushes batches of sensitive transaction data from its application server VMs to cloud Pub/Sub for processing and storage. What is Google-recommended way for your application to authenticate to the required Google Cloud Services?

A. Ensure that VM service accounts are granted the appropriate Cloud Pub/Sub IAM roles.

B. Ensure that VM service accounts do not have access to Cloud Pub/Sub, and use VM access scopes to grant the appropriate Cloud Pub/Sub IAM roles.

C. Generate an OAuth2 access token for accessing Cloud Pub/Sub, encrypt it, and store it in Cloud Storage for access from each VM.

D. Create a gateway to Cloud Pub/Sub using a Cloud Function, and grant the Cloud Function service account the appropriate, Cloud Pub/Sub IAM roles.

Answer: A

Best practice to always use IAM to control resources access

1. topic 1 question 78

Your application will be writing their logs to BigQuery for analysis. Each application should have its own table. Any logs older than 45 days should be removed. You want to optimize storage and follow Google-recommended practices. What should you do?

A. Configure the expiration time for your table at 45 days.

B. Make the tables time-partitioned and configure the partition expiration at 45 days.

C. Rely on BigQuery's default behavior to prune application logs older than 45 days.

D. Create a script that uses the BigQuery command line tool (bq) to remove records older than 45 days.

Answer: B

Combine time-partition-table and lifecycle policies will be able to delete older data

1. topic 1 question 79

You want your Google Kubernetes Engine cluster to automatically add or remove nodes based on CPU load.

What should you do?

A. Configure a HorizontalPodAutoscaler with a target CPU usage. Enable the Cluster Autoscaler from the GCP Console.

B. Configure a HorizontalPodAutoscaler with a target CPU usage. Enable autoscaling on the managed instance group for the cluster using the gcloud command.

C. Create a deployment and set the maxUnavailable and maxSurge properties. Enable the Cluster Autoscaler using the gcloud command.

D. Create a deployment and set the maxUnavailable and maxSurge properties. Enable autoscaling on the cluster managed instance group from the GCP Console.

Answer: A

100% HPA!

1. topic 1 question 80

You need to develop procedures to verify resilience of disaster recovery for remote recovery using GCP. Your production environment is hosted on-premises. You need to establish a secure, redundant connection between your on-premises network and the GCP network.

What should you do?

A. Verify that Dedicated Interconnect can replicate files to GCP. Verify that direct peering can establish a secure connection between your networks if Dedicated Interconnect fails.

B. Verify that Dedicated Interconnect can replicate files to GCP. Verify that Cloud VPN can establish a secure connection between your networks if Dedicated Interconnect fails.

C. Verify that the Transfer Appliance can replicate files to GCP. Verify that direct peering can establish a secure connection between your networks if the Transfer Appliance fails.

D. Verify that the Transfer Appliance can replicate files to GCP. Verify that Cloud VPN can establish a secure connection between your networks if the Transfer Appliance fails.

Answer: B

Transfer Applicance is not meant for DR

Option A is wrong bcos peering only works between two VPC networks in GCP

1. topic 1 question 81

Your company operates nationally and plans to use GCP for multiple batch workloads, including some that are not time-critical. You also need to use GCP services that are HIPAA-certified and manage service costs.

How should you design to meet Google best practices?

A. Provision preemptible VMs to reduce cost. Discontinue use of all GCP services and APIs that are not HIPAA-compliant.

B. Provision preemptible VMs to reduce cost. Disable and then discontinue use of all GCP services and APIs that are not HIPAA-compliant.

C. Provision standard VMs in the same region to reduce cost. Discontinue use of all GCP services and APIs that are not HIPAA-compliant.

D. Provision standard VMs to the same region to reduce cost. Disable and then discontinue use of all GCP services and APIs that are not HIPAA-compliant.

Answer: B

Preemptible = save cost

Disable API instead of just discontinue..

1. topic 1 question 82

Your customer wants to do resilience testing of their authentication layer. This consists of a regional managed instance group serving a public REST API that reads from and writes to a Cloud SQL instance.

What should you do?

A. Engage with a security company to run web scrapers that look your for users' authentication data with malicious websites and notify you if any is found.

B. Deploy intrusion detection software to your virtual machines to detect and log unauthorized access.

C. Schedule a disaster simulation exercise during which you can shut off all VMs in a zone to see how your application behaves.

D. Configure a read replica for your Cloud SQL instance in a different zone than the master, and then manually trigger a failover while monitoring KPIs for our REST API.

Answer: C

Option C: answer the resiliency tests for the authentication layer

Option A: to detect malicious websites

Option B: IDS to detect anomalies traffics

Option D: for redundancy design on MS SQL

1. topic 1 question 83

Your BigQuery project has several users. For audit purposes, you need to see how many queries each user ran in the last month. What should you do?

A. Connect Google Data Studio to BigQuery. Create a dimension for the users and a metric for the amount of queries per user.

B. In the BigQuery interface, execute a query on the JOBS table to get the required information.

C. Use 'bq show' to list all jobs. Per job, use 'bq ls' to list job information and get the required information.

D. Use Cloud Audit Logging to view Cloud Audit Logs, and create a filter on the query operation to get the required information.

Answer: D

- Cloud Audit Logs maintains audit logs for admin activity, data access and system events. BIGQUERY is automatically send to cloud audit log functionality.

- In the filter you can filter relevant BigQuery Audit messages, you can express filters as part of the export

1. topic 1 question 84

You want to automate the creation of a managed instance group. The VMs have many OS package dependencies. You want to minimize the startup time for new VMs in the instance group.

What should you do?

A. Use Terraform to create the managed instance group and a startup script to install the OS package dependencies.

B. Create a custom VM image with all OS package dependencies. Use Deployment Manager to create the managed instance group with the VM image.

C. Use Puppet to create the managed instance group and install the OS package dependencies.

D. Use Deployment Manager to create the managed instance group and Ansible to install the OS package dependencies.

Answer: B

100% Google Deployment Manager can do all the automation. no need for other third-party.

1. topic 1 question 85

Your company captures all web traffic data in Google Analytics 360 and stores it in BigQuery. Each country has its own dataset. Each dataset has multiple tables.

You want analysts from each country to be able to see and query only the data for their respective countries.

How should you configure the access rights?

A. Create a group per country. Add analysts to their respective country-groups. Create a single group 'all\_analysts', and add all country-groups as members. Grant the 'all\_analysts' group the IAM role of BigQuery jobUser. Share the appropriate dataset with view access with each respective analyst country-group.

B. Create a group per country. Add analysts to their respective country-groups. Create a single group 'all\_analysts', and add all country-groups as members. Grant the 'all\_analysts' group the IAM role of BigQuery jobUser. Share the appropriate tables with view access with each respective analyst country-group.

C. Create a group per country. Add analysts to their respective country-groups. Create a single group 'all\_analysts', and add all country-groups as members. Grant the 'all\_analysts' group the IAM role of BigQuery dataViewer. Share the appropriate dataset with view access with each respective analyst country- group.

D. Create a group per country. Add analysts to their respective country-groups. Create a single group 'all\_analysts', and add all country-groups as members. Grant the 'all\_analysts' group the IAM role of BigQuery dataViewer. Share the appropriate table with view access with each respective analyst country-group.

Answer: A

Differences between jobUser vs dataViewer ([link](https://cloud.google.com/bigquery/docs/access-control))

* dataViewer can see datas. obviously this against the requirement
* dataset is per country. in each dataset there are many tables.

1. topic 1 question 87

Your web application uses Google Kubernetes Engine to manage several workloads. One workload requires a consistent set of hostnames even after pod scaling and relaunches.

Which feature of Kubernetes should you use to accomplish this?

A. StatefulSets

B. Role-based access control

C. Container environment variables

D. Persistent Volumes

Answer:

100% https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/

1. topic 1 question 88

You are using Cloud CDN to deliver static HTTP(S) website content hosted on a Compute Engine instance group. You want to improve the cache hit ratio.

What should you do?

A. Customize the cache keys to omit the protocol from the key.

B. Shorten the expiration time of the cached objects.

C. Make sure the HTTP(S) header ג€Cache-Regionג€ points to the closest region of your users.

D. Replicate the static content in a Cloud Storage bucket. Point CloudCDN toward a load balancer on that bucket.

Answer: A

<https://cloud.google.com/cdn/docs/caching#cache-keys>

1. topic 1 question 89

Your architecture calls for the centralized collection of all admin activity and VM system logs within your project.

How should you collect these logs from both VMs and services?

A. All admin and VM system logs are automatically collected by Stackdriver.

B. Stackdriver automatically collects admin activity logs for most services. The Stackdriver Logging agent must be installed on each instance to collect system logs.

C. Launch a custom syslogd compute instance and configure your GCP project and VMs to forward all logs to it.

D. Install the Stackdriver Logging agent on a single compute instance and let it collect all audit and access logs for your environment.

Answer: B

indeed admin activity log is pre-configured. To collect each VM system log must have agent install respectively

1. topic 1 question 90

The database administration team has asked you to help them improve the performance of their new database server running on Google Compute Engine. The database is for importing and normalizing their performance statistics and built with MySQL running on Debian Linux. They have an n1-standard-8 virtual machine with 80 GB of SSD persistent disk.

What should they change to get better performance from this system?

A. Increase the virtual machine’s memory to 64 GB

B. Create a new virtual machine running PostgreSQL

C. Dynamically resize the SSD persistent disk to 500 GB

D. Migrate their performance metrics warehouse to BigQuery

E. Modify all of their batch jobs to use bulk inserts into the database

Answer: C

Increase RAM is possible but cant be done dynamically .

Increase size of disk typically increase IOPS and throughtput accesss to the instance

1. topic 1 question 91

All Compute Engine instances in your VPC should be able to connect to an Active Directory server on specific ports. Any other traffic emerging from your instances is not allowed. You want to enforce this using VPC firewall rules.

How should you configure the firewall rules?

A. Create an egress rule with priority 1000 to deny all traffic for all instances. Create another egress rule with priority 100 to allow the Active Directory traffic for all instances.

B. Create an egress rule with priority 100 to deny all traffic for all instances. Create another egress rule with priority 1000 to allow the Active Directory traffic for all instances.

C. Create an egress rule with priority 1000 to allow the Active Directory traffic. Rely on the implied deny egress rule with priority 100 to block all traffic for all instances.

D. Create an egress rule with priority 100 to allow the Active Directory traffic. Rely on the implied deny egress rule with priority 1000 to block all traffic for all instances.

Answer: A

100% Every VPC network has two implied firewall rules:

- egress rule (65535) that allow to destination 0.0.0.0/0 (option C\*D is wrong))

- ingress rule (65535) to deny all from source 0.0.0.0/0

- we need to allow (100) first before deny all traffics (1000). rule with lower priority value processed first

1. topic 1 question 92

Your customer runs a web service used by e-commerce sites to offer product recommendations to users. The company has begun experimenting with a machine learning model on Google Cloud Platform to improve the quality of results.

What should the customer do to improve their model's results over time?

A. Export Cloud Machine Learning Engine performance metrics from Stackdriver to BigQuery, to be used to analyze the efficiency of the model.

B. Build a roadmap to move the machine learning model training from Cloud GPUs to Cloud TPUs, which offer better results.

C. Monitor Compute Engine announcements for availability of newer CPU architectures, and deploy the model to them as soon as they are available for additional performance.

D. Save a history of recommendations and results of the recommendations in BigQuery, to be used as training data.

Answer: D

100% Model performance is generally based on the volume of its training data input. The more the data, the better the model.

TPUs increase performance for all ML processing but not to improve the web service quality of results

1. topic 1 question 93

A development team at your company has created a dockerized HTTPS web application. You need to deploy the application on Google Kubernetes Engine (GKE) and make sure that the application scales automatically.

How should you deploy to GKE?

A. Use the Horizontal Pod Autoscaler and enable cluster autoscaling. Use an Ingress resource to load-balance the HTTPS traffic.

B. Use the Horizontal Pod Autoscaler and enable cluster autoscaling on the Kubernetes cluster. Use a Service resource of type LoadBalancer to load-balance the HTTPS traffic.

C. Enable autoscaling on the Compute Engine instance group. Use an Ingress resource to load-balance the HTTPS traffic.

D. Enable autoscaling on the Compute Engine instance group. Use a Service resource of type LoadBalancer to load-balance the HTTPS traffic.

Answer: A

Service type=Load Balancer doesn’t support L7 load balancing, hence need setup Ingress resource for the LB purposes

1. topic 1 question 94

You need to design a solution for global load balancing based on the URL path being requested. You need to ensure operations reliability and end-to-end in- transit encryption based on Google best practices.

What should you do?

A. Create a cross-region load balancer with URL Maps.

B. Create an HTTPS load balancer with URL Maps.

C. Create appropriate instance groups and instances. Configure SSL proxy load balancing.

D. Create a global forwarding rule. Configure SSL proxy load balancing.

Answer: B

Global = HTTS LB

1. topic 1 question 95

You have an application that makes HTTP requests to Cloud Storage. Occasionally the requests fail with HTTP status codes of 5xx and 429.

How should you handle these types of errors?

A. Use gRPC instead of HTTP for better performance.

B. Implement retry logic using a truncated exponential backoff strategy.

C. Make sure the Cloud Storage bucket is multi-regional for geo-redundancy.

D. Monitor https://status.cloud.google.com/feed.atom and only make requests if Cloud Storage is not reporting an incident.

Answer: B

100% You should use exponential backoff to retry your requests when receiving errors with 5xx or 429 response codes from Cloud Storage.

1. topic 1 question 96

You need to develop procedures to test a disaster plan for a mission-critical application. You want to use Google-recommended practices and native capabilities within GCP.

What should you do?

A. Use Deployment Manager to automate service provisioning. Use Activity Logs to monitor and debug your tests.

B. Use Deployment Manager to automate service provisioning. Use Stackdriver to monitor and debug your tests.

C. Use gcloud scripts to automate service provisioning. Use Activity Logs to monitor and debug your tests.

D. Use gcloud scripts to automate service provisioning. Use Stackdriver to monitor and debug your tests.

Answer: B

[deployment](https://cloud.google.com/solutions/dr-scenarios-planning-guide) manager to automate, stackdriver for application logging/monitoring

activity logs for admin activities logging only

1. topic 1 question 97

Your company creates rendering software which users can download from the company website. Your company has customers all over the world. You want to minimize latency for all your customers. You want to follow Google-recommended practices.

How should you store the files?

A. Save the files in a Multi-Regional Cloud Storage bucket.

B. Save the files in a Regional Cloud Storage bucket, one bucket per zone of the region.

C. Save the files in multiple Regional Cloud Storage buckets, one bucket per zone per region.

D. Save the files in multiple Multi-Regional Cloud Storage buckets, one bucket per multi-region.

Answer: D

A a single bucket in one region. even though its multi-regional its only meant for redundancy.

To improve latency, one multi-region bucket in each region

1. topic 1 question 98

Your company acquired a healthcare startup and must retain its customers' medical information for up to 4 more years, depending on when it was created. Your corporate policy is to securely retain this data, and then delete it as soon as regulations allow.

Which approach should you take?

A. Store the data in Google Drive and manually delete records as they expire.

B. Anonymize the data using the Cloud Data Loss Prevention API and store it indefinitely.

C. Store the data in Cloud Storage and use lifecycle management to delete files when they expire.

D. Store the data in Cloud Storage and run a nightly batch script that deletes all expired data.

Answer: C

4 years is long period. storing it in cloud storage and with lifecycle delete files that obsoletes will reduce costing

1. topic 1 question 99

You are deploying a PHP App Engine Standard service with Cloud SQL as the backend. You want to minimize the number of queries to the database.

What should you do?

A. Set the memcache service level to dedicated. Create a key from the hash of the query, and return database values from memcache before issuing a query to Cloud SQL.

B. Set the memcache service level to dedicated. Create a cron task that runs every minute to populate the cache with keys containing query results.

C. Set the memcache service level to shared. Create a cron task that runs every minute to save all expected queries to a key called ג€cached\_queriesג€.

D. Set the memcache service level to shared. Create a key called ג€cached\_queriesג€, and return database values from the key before using a query to Cloud SQL.

Answer: A

A dedicated memset is always better than shared until cost-effectiveness specify in the exam as objective. So Option C and D are ruled out.

1. topic 1 question 100

You need to ensure reliability for your application and operations by supporting reliable task scheduling for compute on GCP. Leveraging Google best practices, what should you do?

A. Using the Cron service provided by App Engine, publish messages directly to a message-processing utility service running on Compute Engine instances.

B. Using the Cron service provided by App Engine, publish messages to a Cloud Pub/Sub topic. Subscribe to that topic using a message-processing utility service running on Compute Engine instances.

C. Using the Cron service provided by Google Kubernetes Engine (GKE), publish messages directly to a message-processing utility service running on Compute Engine instances.

D. Using the Cron service provided by GKE, publish messages to a Cloud Pub/Sub topic. Subscribe to that topic using a message-processing utility service running on Compute Engine instances.

Answer: B

<https://cloud.google.com/solutions/reliable-task-scheduling-compute-engine>

1. topic 1 question 101

Your company is building a new architecture to support its data-centric business focus. You are responsible for setting up the network. Your company's mobile and web-facing applications will be deployed on-premises, and all data analysis will be conducted in GCP. The plan is to process and load 7 years of archived .csv files totaling 900 TB of data and then continue loading 10 TB of data daily. You currently have an existing 100-MB internet connection.

What actions will meet your company's needs?

A. Compress and upload both archived files and files uploaded daily using the gsutil -m option.

B. Lease a Transfer Appliance, upload archived files to it, and send it to Google to transfer archived data to Cloud Storage. Establish a connection with Google using a Dedicated Interconnect or Direct Peering connection and use it to upload files daily.

C. Lease a Transfer Appliance, upload archived files to it, and send it to Google to transfer archived data to Cloud Storage. Establish one Cloud VPN Tunnel to VPC networks over the public internet, and compress and upload files daily using the gsutil -m option.

D. Lease a Transfer Appliance, upload archived files to it, and send it to Google to transfer archived data to Cloud Storage. Establish a Cloud VPN Tunnel to VPC networks over the public internet, and compress and upload files daily.

Answer: B

Huge amount of 900 TB data, and continue loading 10 TB. ofc we choose dedicated interconnect

1. topic 1 question 102

You are developing a globally scaled frontend for a legacy streaming backend data API. This API expects events in strict chronological order with no repeat data for proper processing.

Which products should you deploy to ensure guaranteed-once FIFO (first-in, first-out) delivery of data?

A. Cloud Pub/Sub alone

B. Cloud Pub/Sub to Cloud Dataflow

C. Cloud Pub/Sub to Stackdriver

D. Cloud Pub/Sub to Cloud SQL

Answer: B

Dataflow enable strict messaging ordering ([link](https://cloud.google.com/solutions/data-lifecycle-cloud-platform))

1. topic 1 question 103

Your company is planning to perform a lift and shift migration of their Linux RHEL 6.5+ virtual machines. The virtual machines are running in an on-premises

VMware environment. You want to migrate them to Compute Engine following Google-recommended practices. What should you do?

A. 1. Define a migration plan based on the list of the applications and their dependencies. 2. Migrate all virtual machines into Compute Engine individually with Migrate for Compute Engine.

B. 1. Perform an assessment of virtual machines running in the current VMware environment. 2. Create images of all disks. Import disks on Compute Engine. 3. Create standard virtual machines where the boot disks are the ones you have imported.

C. 1. Perform an **assessment** of virtual machines running in the current VMware environment. 2. Define a **migration** **plan**, prepare a Migrate for Compute Engine migration RunBook, and execute the migration.

D. 1. Perform an assessment of virtual machines running in the current VMware environment. 2. Install a third-party agent on all selected virtual machines. 3. Migrate all virtual machines into Compute Engine.

Answer: C

Assess current environment and plan for migration.

1. topic 1 question 104

You need to deploy an application to Google Cloud. The application receives traffic via TCP and reads and writes data to the filesystem. The application does not support horizontal scaling. The application process requires full control over the data on the file system because concurrent access causes corruption. The business is willing to accept a downtime when an incident occurs, but the application must be available 24/7 to support their business operations. You need to design the architecture of this application on Google Cloud. What should you do?

A. Use a managed instance group with instances in multiple zones, use Cloud Filestore, and use an HTTP load balancer in front of the instances.

B. Use a managed instance group with instances in multiple zones, use Cloud Filestore, and use a network load balancer in front of the instances.

C. Use an unmanaged instance group with an active and standby instance in different zones, use a regional persistent disk, and use an HTTP load balancer in front of the instances.

D. Use an unmanaged instance group with an active and standby instance in different zones, use a regional persistent disk, and use a network load balancer in front of the instances.

Answer: D

Keywords “TCP” – hence HTTP load balancer can’t be used (Option A & C)

Cloud Filestore – doesn’t allow full control from application

1. topic 1 question 105

Your company has an application running on multiple Compute Engine instances. You need to ensure that the application can communicate with an on-premises service that requires high throughput via internal IPs, while minimizing latency. What should you do?

A. Use OpenVPN to configure a VPN tunnel between the on-premises environment and Google Cloud.

B. Configure a direct peering connection between the on-premises environment and Google Cloud.

C. Use Cloud VPN to configure a VPN tunnel between the on-premises environment and Google Cloud.

D. Configure a Cloud Dedicated Interconnect connection between the on-premises environment and Google Cloud.

Answer: D

100% high throughput via internal IPs plus lowest latency

1. topic 1 question 106

You are managing an application deployed on Cloud Run for Anthos, and you need to define a strategy for deploying new versions of the application. You want to evaluate the new code with a subset of production traffic to decide whether to proceed with the rollout. What should you do?

A. Deploy a new revision to Cloud Run with the new version. Configure traffic percentage between revisions.

B. Deploy a new service to Cloud Run with the new version. Add a Cloud Load Balancing instance in front of both services.

C. In the Google Cloud Console page for Cloud Run, set up continuous deployment using Cloud Build for the development branch. As part of the Cloud Build trigger, configure the substitution variable TRAFFIC\_PERCENTAGE with the percentage of traffic you want directed to a new version.

D. In the Google Cloud Console, configure Traffic Director with a new Service that points to the new version of the application on Cloud Run. Configure Traffic Director to send a small percentage of traffic to the new version of the application.

Answer: A

A revision consists of a specific container image, along with environment settings such as environment variables, memory limits, or concurrency value. o Once the new revision is deployed to a Service you can manage the traffic using MANAGE TRAFFIC option inside the revision tab ([link](https://cloud.google.com/run/docs/resource-model))

1. topic 1 question 107

You are monitoring Google Kubernetes Engine (GKE) clusters in a Cloud Monitoring workspace. As a Site Reliability Engineer (SRE), you need to triage incidents quickly. What should you do?

A. Navigate the predefined dashboards in the Cloud Monitoring workspace, and then add metrics and create alert policies.

B. Navigate the predefined dashboards in the Cloud Monitoring workspace, create custom metrics, and install alerting software on a Compute Engine instance.

C. Write a shell script that gathers metrics from GKE nodes, publish these metrics to a Pub/Sub topic, export the data to BigQuery, and make a Data Studio dashboard.

D. Create a custom dashboard in the Cloud Monitoring workspace for each incident, and then add metrics and create alert policies.

Answer: A

Keyword “triage incidents quickly”

1. topic 1 question 108

You are implementing a single Cloud SQL MySQL second-generation database that contains business-critical transaction data. You want to ensure that the minimum amount of data is lost in case of catastrophic failure. Which two features should you implement? (Choose two.)

A. Sharding

B. Read replicas

C. Binary logging

D. Automated backups

E. Semisynchronous replication

Answer: CD

Those features allows you to perform a point-in-time recovery, which restores your database from a backup and recovers it to a fresh Cloud SQL instance

1. topic 1 question 109

You are working at a sports association whose members range in age from 8 to 30. The association collects a large amount of health data, such as sustained injuries. You are storing this data in BigQuery. Current legislation requires you to delete such information upon request of the subject. You want to design a solution that can accommodate such a request. What should you do?

A. Use a unique identifier for each individual. Upon a deletion request, delete all rows from BigQuery with this identifier.

B. When ingesting new data in BigQuery, run the data through the Data Loss Prevention (DLP) API to identify any personal information. As part of the DLP scan, save the result to Data Catalog. Upon a deletion request, query Data Catalog to find the column with personal information.

C. Create a BigQuery view over the table that contains all data. Upon a deletion request, exclude the rows that affect the subject's data from this view. Use this view instead of the source table for all analysis tasks.

D. Use a unique identifier for each individual. Upon a deletion request, overwrite the column with the unique identifier with a salted SHA256 of its value.

Answer: A

The other options doesn’t delete rows

1. topic 1 question 110

Your company has announced that they will be outsourcing operations functions. You want to allow developers to easily stage new versions of a cloud-based application in the production environment and allow the outsourced operations team to autonomously promote staged versions to production. You want to minimize the operational overhead of the solution. Which Google Cloud product should you migrate to?

A. App Engine

B. GKE On-Prem

C. Compute Engine

D. Google Kubernetes Engine

Answer: A

trully PaaS !

1. topic 1 question 111

Your company is running its application workloads on Compute Engine. The applications have been deployed in production, acceptance, and development environments. The production environment is business-critical and is used 24/7, while the acceptance and development environments are only critical during office hours. Your CFO has asked you to optimize these environments to achieve cost savings during idle times. What should you do?

A. Create a shell script that uses the gcloud command to change the machine type of the development and acceptance instances to a smaller machine type outside of office hours. Schedule the shell script on one of the production instances to automate the task.

B. Use Cloud Scheduler to trigger a Cloud Function that will stop the development and acceptance environments after office hours and start them just before office hours.

C. Deploy the development and acceptance applications on a managed instance group and enable autoscaling.

D. Use regular Compute Engine instances for the production environment, and use preemptible VMs for the acceptance and development environments.

Answer: B

Keyword “cost savings during idle time” – Cloud function scales down to zero when there are no requests 🡪 cost nothing

1. topic 1 question 112

You are moving an application that uses MySQL from on-premises to Google Cloud. The application will run on Compute Engine and will use Cloud SQL. You want to cut over to the Compute Engine deployment of the application with minimal downtime and no data loss to your customers. You want to migrate the application with minimal modification. You also need to determine the cutover strategy. What should you do?

A. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. 2. Stop the on-premises application. 3. Create a mysqldump of the on-premises MySQL server. 4. Upload the dump to a Cloud Storage bucket. 5. Import the dump into Cloud SQL. 6. Modify the source code of the application to write queries to both databases and read from its local database. 7. Start the Compute Engine application. 8. Stop the on-premises application.

B. 1. Set up Cloud SQL proxy and MySQL proxy. 2. Create a mysqldump of the on-premises MySQL server. 3. Upload the dump to a Cloud Storage bucket. 4. Import the dump into Cloud SQL. 5. Stop the on-premises application. 6. Start the Compute Engine application.

C. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. 2. Stop the on-premises application. 3. Start the Compute Engine application, configured to read and write to the on-premises MySQL server. 4. Create the replication configuration in Cloud SQL. 5. Configure the source database server to accept connections from the Cloud SQL replica. 6. Finalize the Cloud SQL replica configuration. 7. When replication has been completed, stop the Compute Engine application. 8. Promote the Cloud SQL replica to a standalone instance. 9. Restart the Compute Engine application, configured to read and write to the Cloud SQL standalone instance.

D. 1. Stop the on-premises application. 2. Create a mysqldump of the on-premises MySQL server. 3. Upload the dump to a Cloud Storage bucket. 4. Import the dump into Cloud SQL. 5. Start the application on Compute Engine.

Answer: C

100% Cloud VPN provides hybrid connectivity between on-premises and Google VPC network. Then create replication for the SQL Server

1. topic 1 question 113

Your organization has decided to restrict the use of external IP addresses on instances to only approved instances. You want to enforce this requirement across all of your Virtual Private Clouds (VPCs). What should you do?

A. Remove the default route on all VPCs. Move all approved instances into a new subnet that has a default route to an internet gateway.

B. Create a new VPC in custom mode. Create a new subnet for the approved instances, and set a default route to the internet gateway on this new subnet.

C. Implement a Cloud NAT solution to remove the need for external IP addresses entirely.

D. Set an Organization Policy with a constraint on constraints/compute.vmExternalIpAccess. List the approved instances in the allowedValues list.

Answer: D

100% [link](https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip)

1. topic 1 question 114

Your company uses the Firewall Insights feature in the Google Network Intelligence Center. You have several firewall rules applied to Compute Engine instances.

You need to evaluate the efficiency of the applied firewall ruleset. When you bring up the Firewall Insights page in the Google Cloud Console, you notice that there are no log rows to display. What should you do to troubleshoot the issue?

A. Enable Virtual Private Cloud (VPC) flow logging.

B. Enable Firewall Rules Logging for the firewall rules you want to monitor.

C. Verify that your user account is assigned the compute.networkAdmin Identity and Access Management (IAM) role.

D. Install the Google Cloud SDK, and verify that there are no Firewall logs in the command line output.

Answer: B

100%

1. topic 1 question 115

Your company has sensitive data in Cloud Storage buckets. Data analysts have Identity Access Management (IAM) permissions to read the buckets. You want to prevent data analysts from retrieving the data in the buckets from outside the office network. What should you do?

A. 1. Create a **VPC Service Controls** perimeter that includes the projects with the buckets. 2. Create an access level with the CIDR of the office network.

B. 1. Create a firewall rule for all instances in the Virtual Private Cloud (VPC) network for source range. 2. Use the Classless Inter-domain Routing (CIDR) of the office network.

C. 1. Create a Cloud Function to remove IAM permissions from the buckets, and another Cloud Function to add IAM permissions to the buckets. 2. Schedule the Cloud Functions with Cloud Scheduler to add permissions at the start of business and remove permissions at the end of business.

D. 1. Create a Cloud VPN to the office network. 2. Configure Private Google Access for on-premises hosts.

Answer: A

**VPC Service Controls** help you create a security perimeter around your Google Cloud services (like BigQuery) to reduce the risk of data exfiltration, even if credentials are compromised or insiders attempt to overshare data.

**Private Google Access** for on-premises hosts ensures that on-premises systems can securely access Google APIs and services without going over the public internet, further reducing exposure.

1. topic 1 question 116

You have developed a non-critical update to your application that is running in a managed instance group, and have created a new instance template with the update that you want to release. To prevent any possible impact to the application, you don't want to update any running instances. You want any new instances that are created by the managed instance group to contain the new update. What should you do?

A. Start a new rolling restart operation.

B. Start a new rolling replace operation.

C. Start a new rolling update. Select the Proactive update mode.

D. Start a new rolling update. Select the Opportunistic update mode.

Answer: D

Keywords “requirement is not to update any running instances.” --> opportunitics update mode ([link](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#type))

1. topic 1 question 117

Your company is designing its application landscape on Compute Engine. Whenever a zonal outage occurs, the application should be restored in another zone as quickly as possible with the latest application data. You need to design the solution to meet this requirement. What should you do?

A. Create a snapshot schedule for the disk containing the application data. Whenever a zonal outage occurs, use the latest snapshot to restore the disk in the same zone.

B. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the application data. Whenever a zonal outage occurs, use the instance template to spin up the application in another zone in the same region. Use the regional persistent disk for the application data.

C. Create a snapshot schedule for the disk containing the application data. Whenever a zonal outage occurs, use the latest snapshot to restore the disk in another zone within the same region.

D. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the application data. Whenever a zonal outage occurs, use the instance template to spin up the application in another region. Use the regional persistent disk for the application data.

Answer: B

Regional persistent disk is a storage option that provides synchronous replication of data between two zones in a region. Regional persistent disks can be a good building block to use when you implement HA services in Compute Engine.

1. topic 1 question 118

Your company has just acquired another company, and you have been asked to integrate their existing Google Cloud environment into your company's data center. Upon investigation, you discover that some of the RFC 1918 IP ranges being used in the new company's Virtual Private Cloud (VPC) overlap with your data center IP space. What should you do to enable connectivity and make sure that there are no routing conflicts when connectivity is established?

A. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and apply new IP addresses so there is no overlapping IP space.

B. Create a Cloud VPN connection from the new VPC to the data center, and create a Cloud NAT instance to perform NAT on the overlapping IP space.

C. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and apply a custom route advertisement to block the overlapping IP space.

D. Create a Cloud VPN connection from the new VPC to the data center, and apply a firewall rule that blocks the overlapping IP space.

Answer: A

Definitely will need to apply new IP addresses. By blocking or using NAT doesn’t solve anything, on worst side this doesn’t establish connectivity and routing as required by question.

1. topic 1 question 119

You need to migrate Hadoop jobs for your company's Data Science team without modifying the underlying infrastructure. You want to minimize costs and infrastructure management effort. What should you do?

A. Create a Dataproc cluster using standard worker instances.

B. Create a Dataproc cluster using preemptible worker instances.

C. Manually deploy a Hadoop cluster on Compute Engine using standard instances.

D. Manually deploy a Hadoop cluster on Compute Engine using preemptible instances.

Answer: B

100% Hadoop migrate to Dataproc (GCP)

Minimize cost – enable preemptible

1. topic 1 question 120

Your company has a project in Google Cloud with three Virtual Private Clouds (VPCs). There is a Compute Engine instance on each VPC. Network subnets do not overlap and must remain separated. The network configuration is shown below.

A screenshot of a cloud platform

AI-generated content may be incorrect.

Instance #1 is an exception and must communicate directly with both Instance #2 and Instance #3 via internal IPs. How should you accomplish this?

A. Create a cloud router to advertise subnet #2 and subnet #3 to subnet #1.

B. Add two additional NICs to Instance #1 with the following configuration:

NIC1 -- VPC #2 — SUBNETWORK: subnet #2

NIC2 -- VPC #3 — SUBNETWORK: subnet #3

Update firewall rules to enable traffic between instances.

C. Create two VPN tunnels via CloudVPN: ג€¢ 1 between VPC #1 and VPC #2. ג€¢ 1 between VPC #2 and VPC #3. Update firewall rules to enable traffic between the instances.

D. Peer all three VPCs: ג€¢ Peer VPC #1 with VPC #2. ג€¢ Peer VPC #2 with VPC #3. Update firewall rules to enable traffic between the instances.

Answer: B

If the requirements for all VMs in VPC#1, then peering is needed. however this is an exceptional case just for Instance #1

1. topic 1 question 121

You need to deploy an application on Google Cloud that must run on a Debian Linux environment. The application requires extensive configuration in order to operate correctly. You want to ensure that you can install Debian distribution updates with minimal manual intervention whenever they become available. What should you do?

A. Create a Compute Engine instance template using the most recent Debian image. Create an instance from this template, and install and configure the application as part of the startup script. Repeat this process whenever a new Google-managed Debian image becomes available.

B. Create a Debian-based Compute Engine instance, install and configure the application, and use OS patch management to install available updates.

C. Create an instance with the latest available Debian image. Connect to the instance via SSH, and install and configure the application on the instance. Repeat this process whenever a new Google-managed Debian image becomes available.

D. Create a Docker container with Debian as the base image. Install and configure the application as part of the Docker image creation process. Host the container on Google Kubernetes Engine and restart the container whenever a new update is available.

Answer: B

Option A is not right – instance template meant for instance group

Option C not fitting the “minimal manual intervention” – bcos it says “repeat this process when new image”

Option D not fitting into “requires extensive configuration”

1. topic 1 question 122

You have an application that runs in Google Kubernetes Engine (GKE). Over the last 2 weeks, customers have reported that a specific part of the application returns errors very frequently. You currently have no logging or monitoring solution enabled on your GKE cluster. You want to diagnose the problem, but you have not been able to replicate the issue. You want to cause minimal disruption to the application. What should you do?

A. 1. Update your GKE cluster to use Cloud Operations for GKE. 2. Use the GKE Monitoring dashboard to investigate logs from affected Pods.

B. 1. Create a new GKE cluster with Cloud Operations for GKE enabled. 2. Migrate the affected Pods to the new cluster, and redirect traffic for those Pods to the new cluster. 3. Use the GKE Monitoring dashboard to investigate logs from affected Pods.

C. 1. Update your GKE cluster to use Cloud Operations for GKE, and deploy Prometheus. 2. Set an alert to trigger whenever the application returns an error.

D. 1. Create a new GKE cluster with Cloud Operations for GKE enabled, and deploy Prometheus. 2. Migrate the affected Pods to the new cluster, and redirect traffic for those Pods to the new cluster. 3. Set an alert to trigger whenever the application returns an error.

Answer: A

Diagnose the problem --> GKE monitoring and investigate logs on existing cluster

1. topic 1 question 123

You need to deploy a stateful workload on Google Cloud. The workload can scale horizontally, but each instance needs to read and write to the same POSIX filesystem. At high load, the stateful workload needs to support up to 100 MB/s of writes. What should you do?

A. Use a persistent disk for each instance.

B. Use a regional persistent disk for each instance.

C. Create a Cloud Filestore instance and mount it in each instance.

D. Create a Cloud Storage bucket and mount it in each instance using gcsfuse.

Answer: C

100% Posix = Filestore

1. topic 1 question 124

Your company has an application deployed on Anthos clusters (formerly Anthos GKE) that is running multiple microservices. The cluster has both Anthos Service Mesh and Anthos Config Management configured. End users inform you that the application is responding very slowly. You want to identify the microservice that is causing the delay. What should you do?

A. Use the Service Mesh visualization in the Cloud Console to inspect the telemetry between the microservices.

B. Use Anthos Config Management to create a ClusterSelector selecting the relevant cluster. On the Google Cloud Console page for Google Kubernetes Engine, view the Workloads and filter on the cluster. Inspect the configurations of the filtered workloads.

C. Use Anthos Config Management to create a namespaceSelector selecting the relevant cluster namespace. On the Google Cloud Console page for Google Kubernetes Engine, visit the workloads and filter on the namespace. Inspect the configurations of the filtered workloads.

D. Reinstall istio using the default istio profile in order to collect request latency. Evaluate the telemetry between the microservices in the Cloud Console.

Answer: A

100%. The Anthos Service Mesh pages in the Google Cloud Console provide both summary and in-depth metrics, charts, and graphs that enable you to observe service behavior. You can monitor the overall health of your services, or drill down on a specific service to set a service level objective (SLO) or troubleshoot an issue. ([link](https://cloud.google.com/service-mesh/docs/observability/explore-dashboard))

1. topic 1 question 125

You are working at a financial institution that stores mortgage loan approval documents on Cloud Storage. Any change to these approval documents must be uploaded as a separate approval file, so you want to ensure that these documents cannot be deleted or overwritten for the next 5 years. What should you do?

A. Create a retention policy on the bucket for the duration of 5 years. Create a lock on the retention policy.

B. Create the bucket with uniform bucket-level access, and grant a service account the role of Object Writer. Use the service account to upload new files.

C. Use a customer-managed key for the encryption of the bucket. Rotate the key after 5 years.

D. Create the bucket with fine-grained access control, and grant a service account the role of Object Writer. Use the service account to upload new files.

Answer: A

100%. Bucket lock policy

1. topic 1 question 126

Your team will start developing a new application using microservices architecture on Kubernetes Engine. As part of the development lifecycle, any code change that has been pushed to the remote develop branch on your GitHub repository should be built and tested automatically. When the build and test are successful, the relevant microservice will be deployed automatically in the development environment. You want to ensure that all code deployed in the development environment follows this process. What should you do?

A. Have each developer install a pre-commit hook on their workstation that tests the code and builds the container when committing on the development branch. After a successful commit, have the developer deploy the newly built container image on the development cluster.

B. Install a post-commit hook on the remote git repository that tests the code and builds the container when code is pushed to the development branch. After a successful commit, have the developer deploy the newly built container image on the development cluster.

C. Create a Cloud Build trigger based on the development branch that tests the code, builds the container, and stores it in Container Registry. Create a deployment pipeline that watches for new images and deploys the new image on the development cluster. Ensure only the deployment tool has access to deploy new versions.

D. Create a Cloud Build trigger based on the development branch to build a new container image and store it in Container Registry. Rely on Vulnerability Scanning to ensure the code tests succeed. As the final step of the Cloud Build process, deploy the new container image on the development cluster. Ensure only Cloud Build has access to deploy new versions.

Answer: C

Code changes automatically build image ==> Coud Build

Vulnerability scanning is not a to test, hence no need for it

1. topic 1 question 127

Your operations team has asked you to help diagnose a performance issue in a production application that runs on Compute Engine. The application is dropping requests that reach it when under heavy load. The process list for affected instances shows a single application process that is consuming all available CPU, and autoscaling has reached the upper limit of instances. There is no abnormal load on any other related systems, including the database. You want to allow production traffic to be served again as quickly as possible. Which action should you recommend?

A. Change the autoscaling metric to agent.googleapis.com/memory/percent\_used.

B. Restart the affected instances on a staggered schedule.

C. SSH to each instance and restart the application process.

D. Increase the maximum number of instances in the autoscaling group.

Answer: D

Keywords “serve traffic again quickly as possible”

1. topic 1 question 128

You are implementing the infrastructure for a web service on Google Cloud. The web service needs to receive and store the data from 500,000 requests per second. The data will be queried later in real time, based on exact matches of a known set of attributes. There will be periods where the web service will not receive any requests. The business wants to keep costs low. Which web service platform and database should you use for the application?

A. Cloud Run and BigQuery

B. Cloud Run and Cloud Bigtable

C. A Compute Engine autoscaling managed instance group and BigQuery

D. A Compute Engine autoscaling managed instance group and Cloud Bigtable

Answer: B

Keywords “real time, huge number of requests per second”

1. topic 1 question 129

You are developing an application using different microservices that should remain internal to the cluster. You want to be able to configure each microservice with a specific number of replicas. You also want to be able to address a specific microservice from any other microservice in a uniform way, regardless of the number of replicas the microservice scales to. You need to implement this solution on Google Kubernetes Engine. What should you do?

A. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using a Service, and use the Service DNS name to address it from other microservices within the cluster.

B. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using an Ingress, and use the Ingress IP address to address the Deployment from other microservices within the cluster.

C. Deploy each microservice as a Pod. Expose the Pod in the cluster using a Service, and use the Service DNS name to address the microservice from other microservices within the cluster.

D. Deploy each microservice as a Pod. Expose the Pod in the cluster using an Ingress, and use the Ingress IP address name to address the Pod from other microservices within the cluster.

Answer: A

100% - each microservice to a deployment not pod. deployment can scale to multiple replicas / pods. And expose deployment using service (ingress comes with the service)

1. topic 1 question 130

Your company has a networking team and a development team. The development team runs applications on Compute Engine instances that contain sensitive data. The development team requires administrative permissions for Compute Engine. Your company requires all network resources to be managed by the networking team. The development team does not want the networking team to have access to the sensitive data on the instances. What should you do?

A. 1. Create a project with a standalone VPC and assign the Network Admin role to the networking team. 2. Create a second project with a standalone VPC and assign the Compute Admin role to the development team. 3. Use Cloud VPN to join the two VPCs.

B. 1. Create a project with a standalone Virtual Private Cloud (VPC), assign the Network Admin role to the networking team, and assign the Compute Admin role to the development team.

C. 1. Create a project with a **Shared VPC** and assign the Network Admin role to the networking team. 2. Create a second project without a VPC, configure it as a Shared VPC service project, and assign the Compute Admin role to the development team.

D. 1. Create a project with a standalone VPC and assign the Network Admin role to the networking team. 2. Create a second project with a standalone VPC and assign the Compute Admin role to the development team. 3. Use VPC Peering to join the two VPCs.

Answer: C

Network Admin must not have access to sensitive data on instance ==>isolation by project!

All network managed by the Network team only ==> Shared VPC

1. topic 1 question 131

Your company wants you to build a highly reliable web application with a few public APIs as the backend. You don't expect a lot of user traffic, but traffic could spike occasionally. You want to leverage Cloud Load Balancing, and the solution must be cost-effective for users. What should you do?

A. Store static content such as HTML and images in Cloud CDN. Host the APIs on App Engine and store the user data in Cloud SQL.

B. Store static content such as HTML and images in a Cloud Storage bucket. Host the APIs on a zonal Google Kubernetes Engine cluster with worker nodes in multiple zones, and save the user data in Cloud Spanner.

C. Store static content such as HTML and images in Cloud CDN. Use Cloud Run to host the APIs and save the user data in Cloud SQL.

D. Store static content such as HTML and images in a Cloud Storage bucket. Use Cloud Functions to host the APIs and save the user data in Firestore.

Answer: D

Ultimately: store images in cloud storage

Use cloud function (quickly does the job) instead of cloud run (this is for containerized)

1. topic 1 question 132

Your company sends all Google Cloud logs to Cloud Logging. Your security team wants to monitor the logs. You want to ensure that the security team can react quickly if an anomaly such as an unwanted firewall change or server breach is detected. You want to follow Google-recommended practices. What should you do?

A. Schedule a cron job with Cloud Scheduler. The scheduled job queries the logs every minute for the relevant events.

B. Export logs to BigQuery, and trigger a query in BigQuery to process the log data for the relevant events.

C. Export logs to a Pub/Sub topic, and trigger Cloud Function with the relevant log events.

D. Export logs to a Cloud Storage bucket, and trigger Cloud Run with the relevant log events.

Answer: C

100% use of cloud function to react quickly / react to event

1. topic 1 question 133

You have deployed several instances on Compute Engine. As a security requirement, instances cannot have a public IP address. There is no VPN connection between Google Cloud and your office, and you need to connect via SSH into a specific machine without violating the security requirements. What should you do?

A. Configure Cloud NAT on the subnet where the instance is hosted. Create an SSH connection to the Cloud NAT IP address to reach the instance.

B. Add all instances to an unmanaged instance group. Configure TCP Proxy Load Balancing with the instance group as a backend. Connect to the instance using the TCP Proxy IP.

C. Configure Identity-Aware Proxy (IAP) for the instance and ensure that you have the role of IAP-secured Tunnel User. Use the gcloud command line tool to ssh into the instance.

D. Create a bastion host in the network to SSH into the bastion host from your office location. From the bastion host, SSH into the desired instance.

Answer: C

read ([link](https://cloud.google.com/iap/docs/using-tcp-forwarding#tunneling_with_ssh))

1. topic 1 question 134

Your company is using Google Cloud. You have two folders under the Organization: Finance and Shopping. The members of the development team are in a Google Group. The development team group has been assigned the Project Owner role on the Organization. You want to prevent the development team from creating resources in projects in the Finance folder. What should you do?

A. Assign the development team group the Project Viewer role on the Finance folder, and assign the development team group the Project Owner role on the Shopping folder.

B. Assign the development team group only the Project Viewer role on the Finance folder.

C. Assign the development team group the Project Owner role on the Shopping folder, and remove the development team group Project Owner role from the Organization.

D. Assign the development team group only the Project Owner role on the Shopping folder.

Answer: C

100% - Make sure to remove development team from organization

1. topic 1 question 135

You are developing your microservices application on Google Kubernetes Engine. During testing, you want to validate the behavior of your application in case a specific microservice should suddenly crash. What should you do?

A. Add a taint to one of the nodes of the Kubernetes cluster. For the specific microservice, configure a pod anti-affinity label that has the name of the tainted node as a value.

B. Use Istio's fault injection on the particular microservice whose faulty behavior you want to simulate.

C. Destroy one of the nodes of the Kubernetes cluster to observe the behavior.

D. Configure Istio's traffic management features to steer the traffic away from a crashing microservice.

Answer: B

Istio fault injection allows you to simulate application-layer failures in GKE to test your microservices' resilience.

1. topic 1 question 136

Your company is developing a new application that will allow globally distributed users to upload pictures and share them with other selected users. The application will support millions of concurrent users. You want to allow developers to focus on just building code without having to create and maintain the underlying infrastructure. Which service should you use to deploy the application?

A. App Engine

B. Cloud Endpoints

C. Compute Engine

D. Google Kubernetes Engine

Answer: A

Keywords “focus on building code, without care for infra” ==>App Engine (PaaS)

1. topic 1 question 137

Your company provides a recommendation engine for retail customers. You are providing retail customers with an API where they can submit a user ID and the API returns a list of recommendations for that user. You are responsible for the API lifecycle and want to ensure stability for your customers in case the API makes backward-incompatible changes. You want to follow Google-recommended practices. What should you do?

A. Create a distribution list of all customers to inform them of an upcoming backward-incompatible change at least one month before replacing the old API with the new API.

B. Create an automated process to generate API documentation, and update the public API documentation as part of the CI/CD process when deploying an update to the API.

C. Use a versioning strategy for the APIs that increases the version number on every backward-incompatible change.

D. Use a versioning strategy for the APIs that adds the suffix ג€DEPRECATEDג€ to the current API version number on every backward-incompatible change. Use the current version number for the new API.

Answer: C

100% ([link](https://google.aip.dev/185#release-based_versioning))

1. topic 1 question 138

Your company has developed a monolithic, 3-tier application to allow external users to upload and share files. The solution cannot be easily enhanced and lacks reliability. The development team would like to re-architect the application to adopt microservices and a fully managed service approach, but they need to convince their leadership that the effort is worthwhile. Which advantage(s) should they highlight to leadership?

A. The new approach will be significantly less costly, make it easier to manage the underlying infrastructure, and automatically manage the CI/CD pipelines.

B. The monolithic solution can be converted to a container with Docker. The generated container can then be deployed into a Kubernetes cluster.

C. The new approach will make it easier to decouple infrastructure from application, develop and release new features, manage the underlying infrastructure, manage CI/CD pipelines and perform A/B testing, and scale the solution if necessary.

D. The process can be automated with Migrate for Compute Engine.

Answer: C

Keyword “Leadership” 🡪 layman

1. topic 1 question 139

Your team is developing a web application that will be deployed on Google Kubernetes Engine (GKE). Your CTO expects a successful launch and you need to ensure your application can handle the expected load of tens of thousands of users. You want to test the current deployment to ensure the latency of your application stays below a certain threshold. What should you do?

A. Use a load testing tool to simulate the expected number of concurrent users and total requests to your application, and inspect the results.

B. Enable autoscaling on the GKE cluster and enable horizontal pod autoscaling on your application deployments. Send curl requests to your application, and validate if the auto scaling works.

C. Replicate the application over multiple GKE clusters in every Google Cloud region. Configure a global HTTP(S) load balancer to expose the different clusters over a single global IP address.

D. Use Cloud Debugger in the development environment to understand the latency between the different microservices.

Answer: A

1. topic 1 question 140

Your company has a Kubernetes application that pulls messages from Pub/Sub and stores them in Filestore. Because the application is simple, it was deployed as a single pod. The infrastructure team has analyzed Pub/Sub metrics and discovered that the application cannot process the messages in real time. Most of them wait for minutes before being processed. You need to scale the elaboration process that is I/O-intensive. What should you do?

A. Use kubectl autoscale deployment APP\_NAME --max 6 --min 2 --cpu-percent 50 to configure Kubernetes autoscaling deployment.

B. Configure a Kubernetes autoscaling deployment based on the subscription/push\_request\_latencies metric.

C. Use the --enable-autoscaling flag when you create the Kubernetes cluster.

D. Configure a Kubernetes autoscaling deployment based on the subscription/num\_undelivered\_messages metric.

Answer: D

100% <https://cloud.google.com/kubernetes-engine/docs/samples/container-pubsub-horizontal-pod-autoscaler>

1. topic 1 question 141

You are building a CI/CD pipeline that consists of a version control system, Cloud Build, and Container Registry. Each time a new tag is pushed to the repository, a Cloud Build job is triggered, which runs unit tests on the new code builds a new Docker container image, and pushes it into Container Registry. The last step of your pipeline should deploy the new container to your production Google Kubernetes Engine (GKE) cluster. You need to select a tool and deployment strategy that meets the following requirements:

• Zero downtime is incurred

• Testing is fully automated

• Allows for testing before being rolled out to users

• Can quickly rollback if needed

What should you do?

A. Trigger a Spinnaker pipeline configured as an A/B test of your new code and, if it is successful, deploy the container to production.

B. Trigger a Spinnaker pipeline configured as a canary test of your new code and, if it is successful, deploy the container to production.

C. Trigger another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you can perform a canary test.

D. Trigger another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you can perform a shadow test.

Answer: D

Keywords

- “Zero downtime” --> Canary testing allows you to gradually roll out your new container to a small percentage of users while the rest continue using the previous version. This ensures zero downtime during the deployment process.

- “Quickly rollback, build image, automated testing” -->Spinnaker

1. topic 1 question 142

An application development team has come to you for advice. They are planning to write and deploy an HTTP(S) API using Go 1.12. The API will have a very unpredictable workload and must remain reliable during peaks in traffic. They want to minimize operational overhead for this application. Which approach should you recommend?

A. Develop the application with containers, and deploy to Google Kubernetes Engine.

B. Develop the application for App Engine standard environment.

C. Use a Managed Instance Group when deploying to Compute Engine.

D. Develop the application for App Engine flexible environment, using a custom runtime.

Answer: B

Keyword “write and deploy using Go language and minimize operational overhead” --> App Engine; “unpredictable” -->standard

https://cloud.google.com/appengine/docs/the-appengine-environments

1. topic 1 question 143

Your company is designing its data lake on Google Cloud and wants to develop different ingestion pipelines to collect unstructured data from different sources.

After the data is stored in Google Cloud, it will be processed in several data pipelines to build a recommendation engine for end users on the website. The structure of the data retrieved from the source systems can change at any time. The data must be stored exactly as it was retrieved for reprocessing purposes in case the data structure is incompatible with the current processing pipelines. You need to design an architecture to support the use case after you retrieve the data. What should you do?

A. Send the data through the processing pipeline, and then store the processed data in a BigQuery table for reprocessing.

B. Store the data in a BigQuery table. Design the processing pipelines to retrieve the data from the table.

C. Send the data through the processing pipeline, and then store the processed data in a Cloud Storage bucket for reprocessing.

D. Store the data in a Cloud Storage bucket. Design the processing pipelines to retrieve the data from the bucket.

Answer: D

100%. First store unstructured data into Cloud Storage, then use ETL pipelines in Data Lake to process it

1. topic 1 question 144

You are responsible for the Google Cloud environment in your company. Multiple departments need access to their own projects, and the members within each department will have the same project responsibilities. You want to structure your Google Cloud environment for minimal maintenance and maximum overview of

IAM permissions as each department's projects start and end. You want to follow Google-recommended practices. What should you do?

A. Grant all department members the required IAM permissions for their respective projects.

B. Create a Google Group per department and add all department members to their respective groups. Create a folder per department and grant the respective group the required IAM permissions at the folder level. Add the projects under the respective folders.

C. Create a folder per department and grant the respective members of the department the required IAM permissions at the folder level. Structure all projects for each department under the respective folders.

D. Create a Google Group per department and add all department members to their respective groups. Grant each group the required IAM permissions for their respective projects.

Answer: B

100% according to google best practices

1. topic 1 question 145

Your company has an application running as a Deployment in a Google Kubernetes Engine (GKE) cluster. You have separate clusters for development, staging, and production. You have discovered that the team is able to deploy a Docker image to the production cluster without first testing the deployment in development and then staging. You want to allow the team to have autonomy but want to prevent this from happening. You want a Google Cloud solution that can be implemented quickly with minimal effort. What should you do?

A. Configure a Kubernetes lifecycle hook to prevent the container from starting if it is not approved for usage in the given environment.

B. Implement a corporate policy to prevent teams from deploying Docker images to an environment unless the Docker image was tested in an earlier environment.

C. Configure binary authorization policies for the development, staging, and production clusters. Create attestations as part of the continuous integration pipeline.

D. Create a Kubernetes admissions controller to prevent the container from starting if it is not approved for usage in the given environment.

Answer: c

100% USE binary authorization to perform attestation task ([link](https://cloud.google.com/binary-authorization/docs))

1. topic 1 question 146

Your company wants to migrate their 10-TB on-premises database export into Cloud Storage. You want to minimize the time it takes to complete this activity, the overall cost, and database load. The bandwidth between the on-premises environment and Google Cloud is 1 Gbps. You want to follow Google-recommended practices. What should you do?

A. Develop a Dataflow job to read data directly from the database and write it into Cloud Storage.

B. Use the Data Transfer appliance to perform an offline migration.

C. Use a commercial partner ETL solution to extract the data from the on-premises database and upload it into Cloud Storage.

D. Compress the data and upload it with gsutil -m to enable multi-threaded copy.

Answer: B

This question similar to topic 1 question 196. but slightly different answer choice. answer remains the same, use Data Transfer appliance

1. topic 1 question 147

Your company has an enterprise application running on Compute Engine that requires high availability and high performance. The application has been deployed on two instances in two zones in the same region in active-passive mode. The application writes data to a persistent disk. In the case of a single zone outage, that data should be immediately made available to the other instance in the other zone. You want to maximize performance while minimizing downtime and data loss.

What should you do?

A. 1. Attach a persistent SSD disk to the first instance. 2. Create a snapshot every hour. 3. In case of a zone outage, recreate a persistent SSD disk in the second instance where data is coming from the created snapshot.

B. 1. Create a Cloud Storage bucket. 2. Mount the bucket into the first instance with gcs-fuse. 3. In case of a zone outage, mount the Cloud Storage bucket to the second instance with gcs-fuse.

C. 1. Attach a regional SSD persistent disk to the first instance. 2. In case of a zone outage, force-attach the disk to the other instance.

D. 1. Attach a local SSD to the first instance disk. 2. Execute an rsync command every hour where the target is a persistent SSD disk attached to the second instance. 3. In case of a zone outage, use the second instance.

Answer: C

According to [link](https://cloud.google.com/compute/docs/disks/repd-failover)

1. topic 1 question 148

You are designing a Data Warehouse on Google Cloud and want to store sensitive data in BigQuery. Your company requires you to generate the encryption keys outside of Google Cloud. You need to implement a solution. What should you do?

A. Generate a new key in Cloud Key Management Service (Cloud KMS). Store all data in Cloud Storage using the customer-managed key option and select the created key. Set up a Dataflow pipeline to decrypt the data and to store it in a new BigQuery dataset.

B. Generate a new key in Cloud KMS. Create a dataset in BigQuery using the customer-managed key option and select the created key.

C. Import a key in Cloud KMS. Store all data in Cloud Storage using the customer-managed key option and select the created key. Set up a Dataflow pipeline to decrypt the data and to store it in a new BigQuery dataset.

D. Import a key in Cloud KMS. Create a dataset in BigQuery using the customer-supplied key option and select the created key.

Answer: D

Keyword “require generate key outside” ==> after generate, definitely import into KMS. And create dataset straight into BQ.

1. topic 1 question 149

Your organization has stored sensitive data in a Cloud Storage bucket. For regulatory reasons, your company must be able to rotate the encryption key used to encrypt the data in the bucket. The data will be processed in Dataproc. You want to follow Google-recommended practices for security. What should you do?

A. Create a key with Cloud Key Management Service (KMS). Encrypt the data using the encrypt method of Cloud KMS.

B. Create a key with Cloud Key Management Service (KMS). Set the encryption key on the bucket to the Cloud KMS key.

C. Generate a GPG key pair. Encrypt the data using the GPG key. Upload the encrypted data to the bucket.

D. Generate an AES-256 encryption key. Encrypt the data in the bucket using the customer-supplied encryption keys feature.

Answer: B

According to Google recommended practices, then use Google Cloud KMS with encryption set on bucket level

1. topic 1 question 151

Your company has a support ticketing solution that uses App Engine Standard. The project that contains the App Engine application already has a Virtual Private Cloud (VPC) network fully connected to the company's on-premises environment through a Cloud VPN tunnel. You want to enable the App Engine application to communicate with a database that is running in the company's on-premises environment. What should you do?

A. Configure private Google access for on-premises hosts only.

B. Configure private Google access.

C. Configure private services access.

D. Configure serverless VPC access.

Answer: D

Keyword “App engine connected to on-prem via VPN” ==> serverless VPC access

PGA for all VMs (outgoing)

PSA for all VMs (incoming)

1. topic 1 question 152

Your company is planning to upload several important files to Cloud Storage. After the upload is completed, they want to verify that the uploaded content is identical to what they have on-premises. You want to minimize the cost and effort of performing this check. What should you do?

A. 1. Use Linux shasum to compute a digest of files you want to upload. 2. Use gsutil -m to upload all the files to Cloud Storage. 3. Use gsutil cp to download the uploaded files. 4. Use Linux shasum to compute a digest of the downloaded files. 5. Compare the hashes.

B. 1. Use gsutil -m to upload the files to Cloud Storage. 2. Develop a custom Java application that computes CRC32C hashes. 3. Use gsutil ls -L gs://[YOUR\_BUCKET\_NAME] to collect CRC32C hashes of the uploaded files. 4. Compare the hashes.

C. 1. Use gsutil -m to upload all the files to Cloud Storage. 2. Use gsutil cp to download the uploaded files. 3. Use Linux diff to compare the content of the files.

D. 1. Use gsutil -m to upload the files to Cloud Storage. 2. Use gsutil hash -c FILE\_NAME to generate CRC32C hashes of all on-premises files. 3. Use gsutil ls -L gs://[YOUR\_BUCKET\_NAME] to collect CRC32C hashes of the uploaded files. 4. Compare the hashes.

Answer: D

Keywords “minimize cost and effort”

1. topic 1 question 153

You have deployed an application on Anthos clusters (formerly Anthos GKE). According to the SRE practices at your company, you need to be alerted if request latency is above a certain threshold for a specified amount of time. What should you do?

A. Install Anthos Service Mesh on your cluster. Use the Google Cloud Console to define a Service Level Objective (SLO), and create an alerting policy based on this SLO.

B. Enable the Cloud Trace API on your project, and use Cloud Monitoring Alerts to send an alert based on the Cloud Trace metrics.

C. Use Cloud Profiler to follow up the request latency. Create a custom metric in Cloud Monitoring based on the results of Cloud Profiler, and create an Alerting policy in case this metric exceeds the threshold.

D. Configure Anthos Config Management on your cluster, and create a yaml file that defines the SLO and alerting policy you want to deploy in your cluster.

Answer: A

Cloud Service Mesh lets you set SLOs for your services, and monitor and alert on your services in terms of those SLOs. ([link](https://cloud.google.com/service-mesh/docs/observability/slo-overview) )

1. topic 1 question 154

Your company has a stateless web API that performs scientific calculations. The web API runs on a single Google Kubernetes Engine (GKE) cluster. The cluster is currently deployed in us-central1. Your company has expanded to offer your API to customers in Asia. You want to reduce the latency for users in Asia.

What should you do?

A. Create a second GKE cluster in asia-southeast1, and expose both APIs using a Service of type LoadBalancer. Add the public IPs to the Cloud DNS zone.

B. Use a global HTTP(s) load balancer with Cloud CDN enabled.

C. Create a second GKE cluster in asia-southeast1, and use kubemci to create a global HTTP(s) load balancer.

D. Increase the memory and CPU allocated to the application in the cluster.

Answer: C

[link](https://cloud.google.com/blog/products/gcp/how-to-deploy-geographically-distributed-services-on-kubernetes-engine-with-kubemci)

1. topic 1 question 155

You are migrating third-party applications from optimized on-premises virtual machines to Google Cloud. You are unsure about the optimum CPU and memory options. The applications have a consistent usage pattern across multiple weeks. You want to optimize resource usage for the lowest cost. What should you do?

A. Create an instance template with the smallest available machine type, and use an image of the third-party application taken from a current on-premises virtual machine. Create a managed instance group that uses average CPU utilization to autoscale the number of instances in the group. Modify the average CPU utilization threshold to optimize the number of instances running.

B. Create an App Engine flexible environment, and deploy the third-party application using a Dockerfile and a custom runtime. Set CPU and memory options similar to your application's current on-premises virtual machine in the app.yaml file.

C. Create multiple Compute Engine instances with varying CPU and memory options. Install the Cloud Monitoring agent, and deploy the third-party application on each of them. Run a load test with high traffic levels on the application, and use the results to determine the optimal settings.

D. Create a Compute Engine instance with CPU and memory options similar to your application's current on-premises virtual machine. Install the Cloud Monitoring agent, and deploy the third-party application. Run a load test with normal traffic levels on the application, and follow the Rightsizing Recommendations in the Cloud Console.

Answer: D

https://cloud.google.com/migrate/compute-engine/docs/4.9/concepts/planning-a-migration/cloud-instance-rightsizing?hl=en

1. topic 1 question 156

Your company has a Google Cloud project that uses BigQuery for data warehousing. They have a VPN tunnel between the on-premises environment and Google Cloud that is configured with Cloud VPN. The security team wants to avoid data exfiltration by malicious insiders, compromised code, and accidental oversharing.

What should they do?

A. Configure Private Google Access for on-premises only.

B. Perform the following tasks:

1. Create a service account.

2. Give the BigQuery JobUser role and Storage Reader role to the service account.

3. Remove all other IAM access from the project.

C. Configure VPC Service Controls and configure Private Google Access.

D. Configure Private Google Access.

Answer: C

100%

**VPC Service Controls** help you create a security perimeter around your Google Cloud services (like BigQuery) to reduce the risk of data exfiltration, even if credentials are compromised or insiders attempt to overshare data.

**Private Google Access** for on-premises hosts ensures that on-premises systems can securely access Google APIs and services without going over the public internet, further reducing exposure.

1. topic 1 question 157

You are working at an institution that processes medical data. You are migrating several workloads onto Google Cloud. Company policies require all workloads to run on physically separated hardware, and workloads from different clients must also be separated. You created a sole-tenant node group and added a node for each client. You need to deploy the workloads on these dedicated hosts. What should you do?

A. Add the node group name as a network tag when creating Compute Engine instances in order to host each workload on the correct node group.

B. Add the node name as a network tag when creating Compute Engine instances in order to host each workload on the correct node.

C. Use node affinity labels based on the node group name when creating Compute Engine instances in order to host each workload on the correct node group.

D. Use node affinity labels based on the node name when creating Compute Engine instances in order to host each workload on the correct node.

Answer: D

Keywords “require workloads from different client must be separated” ==>sole tenancy with node affinity labels ([link](https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes#node_affinity_and_anti-affinity))

1. topic 1 question 158

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 Compute Engine unmanaged instance groups and Network Load Balancer

B. Google Compute Engine managed instance groups with auto-scaling

C. Google Cloud Dataproc to run Apache Hadoop jobs to process each test

D. Google App Engine with Google StackDriver for logging

Answer: B

100% GCE with auto-scaling

1. topic 1 question 159

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. 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.

Answer: C

Keywords “distributed across” ==>load balancer

1. topic 1 question 160

The application reliability team at your company this added a debug feature to their backend service to send all server events to Google Cloud Storage for eventual analysis. The event records are at least 50 KB and at most 15 MB and are expected to peak at 3,000 events per second. You want to minimize data loss.

Which process should you implement?

A. ג€¢ Append metadata to file body ג€¢ Compress individual files ג€¢ Name files with serverName ג€" Timestamp ג€¢ Create a new bucket if bucket is older than 1 hour and save individual files to the new bucket. Otherwise, save files to existing bucket.

B. ג€¢ Batch every 10,000 events with a single manifest file for metadata ג€¢ Compress event files and manifest file into a single archive file ג€¢ Name files using serverName ג€" EventSequence ג€¢ Create a new bucket if bucket is older than 1 day and save the single archive file to the new bucket. Otherwise, save the single archive file to existing bucket.

C. ג€¢ Compress individual files ג€¢ Name files with serverName ג€" EventSequence ג€¢ Save files to one bucket ג€¢ Set custom metadata headers for each object after saving

D. ג€¢ Append metadata to file body ג€¢ Compress individual files ג€¢ Name files with a random prefix pattern ג€¢ Save files to one bucket

Answer: D

Append metadata and save into one bucket will do

Using completely random object names gives you the best load distribution ([link](https://cloud.google.com/storage/docs/request-rate#naming-convention))

1. topic 1 question 161

You are building a mobile application that will store hierarchical data structures in a database. The application will enable users working offline to sync changes when they are back online. A backend service will enrich the data in the database using a service account. The application is expected to be very popular and needs to scale seamlessly and securely. Which database and IAM role should you use?

A. Use Cloud SQL, and assign the roles/cloudsql.editor role to the service account.

B. Use Bigtable, and assign the roles/bigtable.viewer role to the service account.

C. Use Firestore in Native mode and assign the roles/datastore.user role to the service account.

D. Use Firestore in Datastore mode and assign the roles/datastore.viewer role to the service account.

Answer: C

100% Keywords “Mobile app” -->Firestore. “sync changes” --> datastore.user (instead of viewer role)

1. topic 1 question 162

You want to make a copy of a production Linux vm in the US-Central region. You want to manage and replace the copy easily if there are changes on the production vm. You will deploy the copy as new instance in a different project in the US-East region.

What steps must you take?

A. Use the Linux dd and netcat commands to copy and stream the root disk contents to a new vm 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 vm instance in the US-East region

C. Create an image file from the root disk with Linux dd command, create a new vm 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 the root disk.

Answer: D

1. topic 1 question 163

Your company runs several databases on a single MySQL instance. They need to take backups of specific database at regular intervals. The backup activity needs to complete as quickly as possible and cannot be allowed to impact disk performance.

How should you configure the storage?

A. Configure a cron job to use the gcloud tool to take regular backups using persistent disk snapshots.

B. Mount a local SSD volumes as the backup location. After the backup is complete, use gsutil to move the backup to Google Cloud Storage.

C. Use gcsfuse to mount a Google Cloud Storage bucket as a volume directly on the instance and write backups to the mounted location using mysqldump.

D. Mount additional persistent disk volumes onto each VM instance in a RAID10 array and use LVM to create snapshots to send to Cloud Storage.

Answer: B

GCFUSE will write to GCS which is much slower than writing directly to an added SSD.

1. topic 1 question 164

You are helping the QA team to roll out a new load-testing tool to test the scalability of your primary cloud services that run on Google Compute Engine with Cloud Bigtable.

Which three requirements should they include? Choose 3 answers.

A. Ensure that the load test validate the performance of Cloud Bigtable

B. Create a separate Google Cloud project to use for the load-testing environment

C. Schedule the load-testing tool to regularly run against the production environment

D. Ensure all third-party systems your services use is capable of handling high load

E. Instrument the production services to record every transaction for replay by the load-testing tool

F. Instrument the load-testing tool and the target services with detailed logging and metrics collection

Answer: ABF

Based on <https://cloud.google.com/bigtable/docs/performance>

1. topic 1 question 165

Your customer is moving their corporate applications to Google Cloud. The security team wants detailed visibility of all projects in the organization. You provision the Google Cloud Resource Manager and set up yourself as the org admin.

What Google Cloud Identity and Access Management (Cloud IAM) roles should you give to the security team?

A. Org viewer, project owner

B. Org viewer, project viewer

C. Org admin, project browser

D. Project owner, network admin

Answer: B

Security team needs read-only access, viewer is the answer

1. topic 1 question 166

Your company places a high value on being responsive and meeting customer needs quickly. Their primary business objectives are release speed and agility. You want to reduce the chance of security errors being accidentally introduced.

Which two actions can you take? Choose 2 answers.

A. Ensure every code check-in is peer reviewed by a security SME

B. Use source code security analyzers as part of the CI/CD pipeline

C. Ensure you have stubs to unit test all interfaces between components

D. Enable code signing and a trusted binary repository integrated with your CI/CD pipeline

E. Run a vulnerability security scanner as part of your continuous-integration / continuous-delivery (CI/CD) pipeline

Answer: BE

Code signing only verifies the author. In other words it only check who you are, but not what have you done

1. topic 1 question 167

You want to enable your running Google Container Engine cluster to scale as demand for your application changes.

What should you do?

A. Add additional nodes to your Container Engine cluster using the following command

- gcloud container clusters resize CLUSTER\_NAME - -size 10

B. Add a tag to the instances in the cluster with the following command:

- gcloud compute instances add-tags INSTANCE - -tags enable-autoscaling max-nodes=10

C. Update the existing Container Engine cluster with the following command:

- gcloud alpha container clusters update mycluster - -enable-autoscaling - -min-nodes=1 - -max-nodes=10

D. Create a new Container Engine cluster with the following command:

- gcloud alpha container clusters create mycluster - -enable-autoscaling - -min-nodes=1 - -max-nodes=10 and redeploy your application

Answer: C

100%

1. topic 1 question 168

Your marketing department wants to send out a promotional email campaign. The development team wants to minimize direct operation management. They project a wide range of possible customer responses, from 100 to 500,0000 click-through per day. The link leads to a simple website that explains the promotion and collects user information and preferences.

Which infrastructure should you recommend?

A. Use Google App Engine to serve the website and Google Cloud Datastore to store user data

B. Use Google Container Engine cluster to serve the website and store data to persistent data

C. Use a managed instance group to serve the website and Google Cloud Bigtable to store user data

D. Use a single Compute Engine vm to host a web server, backend by Google Cloud SQL

Answer: AC

100%

1. topic 1 question 169

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. Specifically, you want a system that is no-ops and auto-scaling

Which two compute products should you choose? Choose 2 answers

A. Compute Engine with containers

B. Google Kubernetes Engine with containers

C. Google App Engine standard environment

D. Compute Engine with custom instance types

E. Compute Engine with managed instance groups

Answer: BC

GAE - truly NoOps, scales instances running up or down match load.

NoOps means no infra to build out or manage during usage , but compromise the control of underlying infra.

1. topic 1 question 170

One of your primary business objectives is being able to trust the data stored in your application. You want to log all changes to the application data.

How can you design your logging system to verify authenticity of your logs?

A. Write the log concurrently in the cloud and on premises

B. Use a SQL database and limit who can modify the log table

C. Digitally sign each timestamp and log entry and store the signature

D. Create a JSON dump of each log entry and store it in Google Cloud Storage

Answer: C

100% as all other options doesn’t store any additional value for logs’ authenticity

1. topic 1 question 171

Your company has a Google Workspace account and Google Cloud Organization. Some developers in the company have created Google Cloud projects outside of the Google Cloud Organization.

You want to create an Organization structure that allows developers to create projects, but prevents them from modifying production projects. You want to manage policies for all projects centrally and be able to set more restrictive policies for production projects.

You want to minimize disruption to users and developers when business needs change in the future. You want to follow Google-recommended practices. Now should you design the Organization structure?

A. 1. Create a second Google Workspace account and Organization.

2. Grant all developers the Project Creator IAM role on the new Organization.

3. Move the developer projects into the new Organization.

4. Set the policies for all projects on both Organizations. 5. Additionally, set the production policies on the original Organization.

B. 1. Create a folder under the Organization resource named Production.

2. Grant all developers the Project Creator IAM role on the new Organization.

3. Move the developer projects into the new Organization.

4. Set the policies for all projects on the Organization.

5. Additionally, set the production policies on the Production folder.

C. 1. Create folders under the Organization resource named Development and Production.

2. Grant all developers the Project Creator IAM role on the Development folder.

3. Move the developer projects into the Development folder.

4. Set the policies for all projects on the Organization.

5. Additionally, set the production policies on the Production folder.

D. 1. Designate the Organization for production projects only.

2. Ensure that developers do not have the Project Creator IAM role on the Organization.

3. Create development projects outside of the Organization using the developer Google Workspace accounts.

4. Set the policies for all projects on the Organization.

5. Additionally, set the production policies on the individual production projects.

Answer: C

Best practice – single organization with multiple folders

1. topic 1 question 172

Your company has an application running on Compute Engine that allows users to play their favorite music. There are a fixed number of instances. Files are stored in Cloud Storage, and data is streamed directly to users. Users are reporting that they sometimes need to attempt to play popular songs multiple times before they are successful. You need to improve the performance of the application. What should you do?

A. 1. Mount the Cloud Storage bucket using gcsfuse on all backend Compute Engine instances. 2. Serve music files directly from the backend Compute Engine instance.

B. 1. Create a Cloud Filestore NFS volume and attach it to the backend Compute Engine instances. 2. Download popular songs in Cloud Filestore. 3. Serve music files directly from the backend Compute Engine instance.

C. 1. Copy popular songs into CloudSQL as a blob. 2. Update application code to retrieve data from CloudSQL when Cloud Storage is overloaded.

D. 1. Create a managed instance group with Compute Engine instances. 2. Create a global load balancer and configure it with two backends: ג—‹ Managed instance group ג—‹ Cloud Storage bucket 3. Enable Cloud CDN on the bucket backend.

Answer: D

Since application already running in GCE, just enable auto-scaling with managed instance group.

Option A&B – save cost but not performance

1. topic 1 question 173

The operations team in your company wants to save Cloud VPN log events for one year. You need to configure the cloud infrastructure to save the logs. What should you do?

A. Set up a filter in Cloud Logging and a Cloud Storage bucket as an export target for the logs you want to save.

B. Enable the Compute Engine API, and then enable logging on the firewall rules that match the traffic you want to save.

C. Set up a Cloud Logging Dashboard titled Cloud VPN Logs, and then add a chart that queries for the VPN metrics over a one-year time period.

D. Set up a filter in Cloud Logging and a topic in Pub/Sub to publish the logs.

Answer: A

100% one year retention; and best to keep long period of data is with Cloud storage

1. topic 1 question 174

You are working with a data warehousing team that performs data analysis. The team needs to process data from external partners, but the data contains personally identifiable information (PII). You need to process and store the data without storing any of the PIIE data. What should you do?

A. Create a Dataflow pipeline to retrieve the data from the external sources. As part of the pipeline, use the Cloud Data Loss Prevention (Cloud DLP) API to remove any PII data. Store the result in BigQuery.

B. Create a Dataflow pipeline to retrieve the data from the external sources. As part of the pipeline, store all non-PII data in BigQuery and store all PII data in a Cloud Storage bucket that has a retention policy set.

C. Ask the external partners to upload all data on Cloud Storage. Configure Bucket Lock for the bucket. Create a Dataflow pipeline to read the data from the bucket. As part of the pipeline, use the Cloud Data Loss Prevention (Cloud DLP) API to remove any PII data. Store the result in BigQuery.

D. Ask the external partners to import all data in your BigQuery dataset. Create a dataflow pipeline to copy the data into a new table. As part of the Dataflow bucket, skip all data in columns that have PII data

Answer: A

Option B is wrong. bcos it still stores non-PII

Option C & D – why ask external partner to do it. extra steps and security risks.

1. topic 1 question 175

You want to allow your operations team to store logs from all the production projects in your Organization, without including logs from other projects. All of the production projects are contained in a folder. You want to ensure that all logs for existing and new production projects are captured automatically. What should you do?

A. Create an aggregated export on the Production folder. Set the log sink to be a Cloud Storage bucket in an operations project.

B. Create an aggregated export on the Organization resource. Set the log sink to be a Cloud Storage bucket in an operations project.

C. Create log exports in the production projects. Set the log sinks to be a Cloud Storage bucket in an operations project.

D. Create log exports in the production projects. Set the log sinks to be BigQuery datasets in the production projects, and grant IAM access to the operations team to run queries on the datasets.

Answer: A

Keywords “contained in a folder”

1. topic 1 question 176

Your company has an application that is running on multiple instances of Compute Engine. It generates 1 TB per day of logs. For compliance reasons, the logs need to be kept for at least two years. The logs need to be available for active query for 30 days. After that, they just need to be retained for audit purposes. You want to implement a storage solution that is compliant, minimizes costs, and follows Google-recommended practices. What should you do?

A. 1. Install a Cloud Logging agent on all instances.

2. Create a sink to export logs into a regional Cloud Storage bucket.

3. Create an Object Lifecycle rule to move files into a Coldline Cloud Storage bucket after one month.

4. Configure a retention policy at the bucket level using bucket lock.

B. 1. Write a daily cron job, running on all instances, that uploads logs into a Cloud Storage bucket.

2. Create a sink to export logs into a regional Cloud Storage bucket.

3. Create an Object Lifecycle rule to move files into a Coldline Cloud Storage bucket after one month.

C. 1. Install a Cloud Logging agent on all instances.

2. Create a sink to export logs into a partitioned BigQuery table.

3. Set a time\_partitioning\_expiration of 30 days.

D. 1. Create a daily cron job, running on all instances, that uploads logs into a partitioned BigQuery table.

2. Set a time\_partitioning\_expiration of 30 days.

Answer: A

Keywords

- “retained for audit purposes and minimize costs” – object lifecycle

- “logs to be kept for 2 years purpose” – bucket lock

1. topic 1 question 177

Your company has just recently activated Cloud Identity to manage users. The Google Cloud Organization has been configured as well. The security team needs to secure projects that will be part of the Organization. They want to prohibit IAM users outside the domain from gaining permissions from now on. What should they do?

A. Configure an organization policy to restrict identities by domain.

B. Configure an organization policy to block creation of service accounts.

C. Configure Cloud Scheduler to trigger a Cloud Function every hour that removes all users that don't belong to the Cloud Identity domain from all projects.

D. Create a technical user (e.g., crawler@yourdomain.com), and give it the project owner role at root organization level. Write a bash script that: ג€¢ Lists all the IAM rules of all projects within the organization. ג€¢ Deletes all users that do not belong to the company domain. Create a Compute Engine instance in a project within the Organization and configure gcloud to be executed with technical user credentials. Configure a cron job that executes the bash script every hour.

Answer: A

100%. <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>

1. topic 1 question 178

Your company has an application running on Google Cloud that is collecting data from thousands of physical devices that are globally distributed. Data is published to Pub/Sub and streamed in real time into an SSD Cloud Bigtable cluster via a Dataflow pipeline. The operations team informs you that your Cloud

Bigtable cluster has a hotspot, and queries are taking longer than expected. You need to resolve the problem and prevent it from happening in the future. What should you do?

A. Advise your clients to use HBase APIs instead of NodeJS APIs.

B. Delete records older than 30 days.

C. Review your RowKey strategy and ensure that keys are evenly spread across the alphabet.

D. Double the number of nodes you currently have.

Answer: C

100%. <https://cloud.google.com/bigtable/docs/schema-design#row-keys>

Good RowKey strategy helps distribute data evenly across the cluster and improve query performance

1. topic 1 question 179

Your company has a Google Cloud project that uses BigQuery for data warehousing. There are some tables that contain personally identifiable information (PII).

Only the compliance team may access the PII. The other information in the tables must be available to the data science team. You want to minimize cost and the time it takes to assign appropriate access to the tables. What should you do?

A. 1. From the dataset where you have the source data, create views of tables that you want to share, excluding PII.

2. Assign an appropriate project-level IAM role to the members of the data science team.

3. Assign access controls to the dataset that contains the view.

B. 1. From the dataset where you have the source data, create materialized views of tables that you want to share, excluding PII.

2. Assign an appropriate project-level IAM role to the members of the data science team.

3. Assign access controls to the dataset that contains the view.

C. 1. Create a dataset for the data science team.

2. Create views of tables that you want to share, excluding PII.

3. Assign an appropriate project-level IAM role to the members of the data science team.

4. Assign access controls to the dataset that contains the view.

5. Authorize the view to access the source dataset.

D. 1. Create a dataset for the data science team.

2. Create materialized views of tables that you want to share, excluding PII.

3. Assign an appropriate project-level IAM role to the members of the data science team.

4. Assign access controls to the dataset that contains the view.

5. Authorize the view to access the source dataset.

Answer: C

Option B&D is eliminated due to fact materialized view is too costly. (link)

To protect PII, creating a view on the original dataset should be sufficient ([link](https://cloud.google.com/bigquery/docs/view-access-controls))

1. topic 1 question 180

Your operations team currently stores 10 TB of data in an object storage service from a third-party provider. They want to move this data to a Cloud Storage bucket as quickly as possible, following Google-recommended practices. They want to minimize the cost of this data migration. Which approach should they use?

A. Use the gsutil mv command to move the data.

B. Use the Storage Transfer Service to move the data.

C. Download the data to a Transfer Appliance, and ship it to Google.

D. Download the data to the on-premises data center, and upload it to the Cloud Storage bucket.

Answer: B

100% Keyword “object storage service from third-party provider”

Transfer appliance is from on-prem to google cloud storage.

1. topic 1 question 181

You have an outage in your Compute Engine managed instance group: all instances keep restarting after 5 seconds. You have a health check configured, but autoscaling is disabled. Your colleague, who is a Linux expert, offered to look in the issue. You need to make sure that he can access the VMs. What should you do?

A. Grant your colleague the IAM role of project Viewer.

B. Perform a rolling restart on the instance group.

C. Disable the health check for the instance group. Add his SSH key to the project-wide SSH keys.

D. Disable autoscaling for the instance group. Add his SSH key to the project-wide SSH keys.

Answer: C

Explanations: To control access to VM, ofc we need SSH key; but ensure to stop the HC from

1. topic 1 question 182

You are managing several projects on Google Cloud and need to interact on a daily basis with BigQuery, Bigtable, and Kubernetes Engine using the gcloud CL tool. You are travelling a lot and work on different workstations during the week. You want to avoid having to manage the gcloud CLI manually. What should you do?

A. Use Google Cloud Shell in the Google Cloud Console to interact with Google Cloud.

B. Create a Compute Engine instance and install gcloud on the instance. Connect to this instance via SSH to always use the same gcloud installation when interacting with Google Cloud.

C. Install gcloud on all of your workstations. Run the command gcloud components auto-update on each workstation

D. Use a package manager to install gcloud on your workstations instead of installing it manually.

Answer: A

100%. Cloud Shell provides the CLI consistently – fitting the requirement “daily basis with gcloud CL tool.

1. topic 1 question 183

Your company recently acquired a company that has infrastructure in Google Cloud. Each company has its own Google Cloud organization. Each company is using a Shared Virtual Private Cloud (VPC) to provide network connectivity for its applications. Some of the subnets used by both companies overlap. In order for both businesses to integrate, the applications need to have private network connectivity. These applications are not on overlapping subnets. You want to provide connectivity with minimal re-engineering. What should you do?

A. Set up VPC peering and peer each Shared VPC together.

B. Migrate the projects from the acquired company into your company's Google Cloud organization. Re-launch the instances in your companies Shared VPC.

C. Set up a Cloud VPN gateway in each Shared VPC and peer Cloud VPNs.

D. Configure SSH port forwarding on each application to provide connectivity between applications in the different Shared VPCs.

Answer: C

A cant due to overlapping subnets

B and D not minimal re-engineering

1. topic 1 question 184

You are managing several internal applications that are deployed on Compute Engine. Business users inform you that an application has become very slow over the past few days. You want to find the underlying cause in order to solve the problem. What should you do first?

A. Inspect the logs and metrics from the instances in Cloud Logging and Cloud Monitoring.

B. Change the Compute Engine Instances behind the application to a machine type with more CPU and memory.

C. Restore a backup of the application database from a time before the application became slow.

D. Deploy the applications on a managed instance group with autoscaling enabled. Add a load balancer in front of the managed instance group, and have the users connect to the IP of the load balancer.

Answer: A

100% First thing to do is to inspect logs and monitoring to see what is happening

1. topic 1 question 185

Your company has an application running as a Deployment in a Google Kubernetes Engine (GKE) cluster. When releasing new versions of the application via a rolling deployment, the team has been causing outages. The root cause of the outages is misconfigurations with parameters that are only used in production. You want to put preventive measures for this in the platform to prevent outages. What should you do?

A. Configure liveness and readiness probes in the Pod specification.

B. Configure health checks on the managed instance group.

C. Create a Scheduled Task to check whether the application is available.

D. Configure an uptime alert in Cloud Monitoring.

Answer: A

A: Configuring the right liveness and readiness probes prevents outages when rolling out a new ReplicaSet of a Deployment, because Pods are only getting traffic when they are considered ready.

B: With GKE, you do not deal with MIGs.

C: Does not use GKE tools and is therefore not the best option.

D: Does alert you but does not prevent the outage.

1. topic 1 question 186

Your company uses Google Kubernetes Engine (GKE) as a platform for all workloads. Your company has a single large GKE cluster that contains batch, stateful, and stateless workloads. The GKE cluster is configured with a single node pool with 200 nodes. Your company needs to reduce the cost of this cluster but does not want to compromise availability. What should you do?

A. Create a second GKE cluster for the batch workloads only. Allocate the 200 original nodes across both clusters.

B. Configure CPU and memory limits on the namespaces in the cluster. Configure all Pods to have a CPU and memory limits.

C. Configure a HorizontalPodAutoscaler for all stateless workloads and for all compatible stateful workloads. Configure the cluster to use node auto scaling.

D. Change the node pool to use preemptible VMs.

Answer: C

100%. Reduce cost? ==> via Autoscaling the cluster ofc

topic 1 question 194

Your company is planning to migrate their Windows Server 2022 from their on-premises data center to Google Cloud. You need to bring the licenses that are currently in use in on-premises virtual machines into the target cloud environment. What should you do?

A. 1. Create an image of the on-premises virtual machines and upload into Cloud Storage.

2. Import the image as a virtual disk on Compute Engine.

B. 1. Create standard instances on Compute Engine.

2. Select as the OS the same Microsoft Windows version that is currently in use in the on-premises environment.

C. 1. Create an image of the on-premises virtual machine.

2. Import the image as a virtual disk on Compute Engine.

3. Create a standard instance on Compute Engine, selecting as the OS the same Microsoft Windows version that is currently in use in the on-premises environment.

4. Attach a data disk that includes data that matches the created image.

D. 1. Create an image of the on-premises virtual machines.

2. Import the image as a virtual disk on Compute Engine using --os=windows-2022-dc-v.

3. Create a sole-tenancy instance on Compute Engine that uses the imported disk as a boot disk.

Answer:

1. topic 1 question 187

Your company has a Google Cloud project that uses BigQuery for data warehousing on a pay-per-use basis. You want to monitor queries in real time to discover the most costly queries and which users spend the most. What should you do?

A. 1. In the BigQuery dataset that contains all the tables to be queried, add a label for each user that can launch a query. 2. Open the Billing page of the project. 3. Select Reports. 4. Select BigQuery as the product and filter by the user you want to check.

B. 1. Create a Cloud Logging sink to export BigQuery data access logs to BigQuery. 2. Perform a BigQuery query on the generated table to extract the information you need.

C. 1. Create a Cloud Logging sink to export BigQuery data access logs to Cloud Storage. 2. Develop a Dataflow pipeline to compute the cost of queries split by users.

D. 1. Activate billing export into BigQuery. 2. Perform a BigQuery query on the billing table to extract the information you need.

Answer: B

Keyword real time ==>Logging sink. and continue to use Bigquery to filter information

1. topic 1 question 188

Your company and one of its partners each have a Google Cloud project in separate organizations. Your company's project (prj-a) runs in Virtual Private Cloud

(vpc-a). The partner's project (prj-b) runs in vpc-b. There are two instances running on vpc-a and one instance running on vpc-b. Subnets defined in both VPCs are not overlapping. You need to ensure that all instances communicate with each other via internal IPs, minimizing latency and maximizing throughput. What should you do?

A. Set up a network peering between vpc-a and vpc-b.

B. Set up a VPN between vpc-a and vpc-b using Cloud VPN.

C. Configure IAP TCP forwarding on the instance in vpc-b, and then launch the following gcloud command from one of the instances in vpc-a gcloud: gcloud compute start-iap-tunnel INSTANCE\_NAME\_IN\_VPC\_8 22 \ --local-host-port=localhost:22

D. 1. Create an additional instance in vpc-a. 2. Create an additional instance in vpc-b. 3. Install OpenVPN in newly created instances. 4. Configure a VPN tunnel between vpc-a and vpc-b with the help of OpenVPN.

Answer: A

100%.

1. topic 1 question 189

You want to store critical business information in Cloud Storage buckets. The information is regularly changed, but previous versions need to be referenced on a regular basis. You want to ensure that there is a record of all changes to any information in these buckets. You want to ensure that accidental edits or deletions can be easily rolled back. Which feature should you enable?

A. Bucket Lock

B. Object Versioning

C. Object change notification

D. Object Lifecycle Management

Answer: B

100%

1. topic 1 question 190

You have a Compute Engine application that you want to autoscale when total memory usage exceeds 80%. You have installed the Cloud Monitoring agent and configured the autoscaling policy as follows:

✑ Metric identifier: agent.googleapis.com/memory/percent\_used

✑ Filter: metric.label.state = 'used'

✑ Target utilization level: 80

✑ Target type: GAUGE

You observe that the application does not scale under high load. You want to resolve this. What should you do?

A. Change the Target type to DELTA\_PER\_MINUTE.

B. Change the Metric identifier to agent.googleapis.com/memory/bytes\_used.

C. Change the filter to metric.label.state = 'used' AND metric.label.state = 'buffered' AND metric.label.state = 'cached' AND metric.label.state = 'slab'.

D. Change the filter to metric.label.state = 'free' and the Target utilization to 20.

Answer: C

Option A is wrong. utilization target measured in minutes instead of percentage %. Scenario not time based.

Option B is not applicable

Option D is wrong. because it filter free memory which is 20% instead of 80%

1. topic 1 question 191

You are deploying an application to Google Cloud. The application is part of a system. The application in Google Cloud must communicate over a private network with applications in a non-Google Cloud environment. The expected average throughput is 200 kbps. The business requires:

✑ as close to 100% system availability as possible

✑ cost optimization

You need to design the connectivity between the locations to meet the business requirements. What should you provision?

A. An HA Cloud VPN gateway connected with two tunnels to an on-premises VPN gateway

B. Two Classic Cloud VPN gateways connected to two on-premises VPN gateways Configure each Classic Cloud VPN gateway to have two tunnels, each connected to different on-premises VPN gateways

C. Two HA Cloud VPN gateways connected to two on-premises VPN gateways Configure each HA Cloud VPN gateway to have two tunnels, each connected to different on-premises VPN gateways

D. A single Cloud VPN gateway connected to an on-premises VPN gateway

Answer: A

A HA VPN do support two tunnels to achive 99.99%. Classic VPN does not.

1. topic 1 question 192

Your company has an application running on App Engine that allows users to upload music files and share them with other people. You want to allow users to upload files directly into Cloud Storage from their browser session. The payload should not be passed through the backend. What should you do?

A. 1. Set a CORS configuration in the target Cloud Storage bucket where the base URL of the App Engine application is an allowed origin.

2. Use the Cloud Storage Signed URL feature to generate a POST URL.

B. 1. Set a CORS configuration in the target Cloud Storage bucket where the base URL of the App Engine application is an allowed origin.

2. Assign the Cloud Storage WRITER role to users who upload files.

C. 1. Use the Cloud Storage Signed URL feature to generate a POST URL.

2. Use App Engine default credentials to sign requests against Cloud Storage.

D. 1. Assign the Cloud Storage WRITER role to users who upload files.

2. Use App Engine default credentials to sign requests against Cloud Storage.

Answer: A

CORS = Cross-origin resource sharing (bucket level)

WRITE role grant too much permission to users. ([link](https://cloud.google.com/storage/docs/access-control/iam-roles#legacy-roles))

Signed URL to enable time-limited access.

1. topic 1 question 193

You are configuring the cloud network architecture for a newly created project in Google Cloud that will host applications in Compute Engine. Compute Engine virtual machine instances will be created in two different subnets (sub-a and sub-b) within a single region:

• Instances in sub-a will have public IP addresses.

• Instances in sub-b will have only private IP addresses.

To download updated packages, instances must connect to a public repository outside the boundaries of Google Cloud. You need to allow sub-b to access the external repository. What should you do?

A. Enable Private Google Access on sub-b.

B. Configure Cloud NAT and select sub-b in the NAT mapping section.

C. Configure a bastion host instance in sub-a to connect to instances in sub-b.

D. Enable Identity-Aware Proxy for TCP forwarding for instances in sub-b.

Answer: B

PGA connect to google services only

Bastion host for remote ssh into VM

IAP similarly for remote ssh into VM

1. topic 1 question 194

Your company is planning to migrate their Windows Server 2022 from their on-premises data center to Google Cloud. You need to bring the licenses that are currently in use in on-premises virtual machines into the target cloud environment. What should you do?

A. 1. Create an image of the on-premises virtual machines and upload into Cloud Storage.

2. Import the image as a virtual disk on Compute Engine.

B. 1. Create standard instances on Compute Engine.

2. Select as the OS the same Microsoft Windows version that is currently in use in the on-premises environment.

C. 1. Create an image of the on-premises virtual machine.

2. Import the image as a virtual disk on Compute Engine.

3. Create a standard instance on Compute Engine, selecting as the OS the same Microsoft Windows version that is currently in use in the on-premises environment.

4. Attach a data disk that includes data that matches the created image.

D. 1. Create an image of the on-premises virtual machines.

2. Import the image as a virtual disk on Compute Engine using --os=windows-2022-dc-v.

3. Create a sole-tenancy instance on Compute Engine that uses the imported disk as a boot disk.

Answer: D

Keyword “sole-tenancy”. in order to install Windows Server with BYOL. ([link](https://cloud.google.com/compute/docs/images/creating-custom-windows-byol-images#use_the_custom_image))

1. topic 1 question 195

You are building an application that uses a distributed microservices architecture. You want to measure the performance and system resource utilization in one of the microservices written in Java. What should you do?

A. Instrument the service with Cloud Profiler to measure CPU utilization and method-level execution times in the service.

B. Instrument the service with Debugger to investigate service errors.

C. Instrument the service with Cloud Trace to measure request latency.

D. Instrument the service with OpenCensus to measure service latency, and write custom metrics to Cloud Monitoring.

Answer: A

100%. Keywords “measure performance and resource utilization” --> Profiler

1. topic 1 question 196

Your company wants to migrate their 10-TB on-premises database export into Cloud Storage. You want to minimize the time it takes to complete this activity and the overall cost. The bandwidth between the on-premises environment and Google Cloud is 1 Gbps. You want to follow Google-recommended practices. What should you do?

A. Develop a Dataflow job to read data directly from the database and write it into Cloud Storage.

B. Use the Data Transfer appliance to perform an offline migration.

C. Use a commercial partner ETL solution to extract the data from the on-premises database and upload it into Cloud Storage.

D. Upload the data with gcloud storage cp.

Answer: B

This question similar to topic 1 question 146. but slight different answer choice. answer remains the same, use Data Transfer appliance

1. topic 1 question 197

You are working at a financial institution that stores mortgage loan approval documents on Cloud Storage. Any change to these approval documents must be uploaded as a separate approval file. You need to ensure that these documents cannot be deleted or overwritten for the next 5 years. What should you do?

A. Create a retention policy on the bucket for the duration of 5 years. Create a lock on the retention policy.

B. Create a retention policy organizational constraint constraints/storage.retentionPolicySeconds at the organization level. Set the duration to 5 years.

C. Use a customer-managed key for the encryption of the bucket. Rotate the key after 5 years.

D. Create a retention policy organizational constraint constraints/storage.retentionPolicySeconds at the project level. Set the duration to 5 years.

Answer: A

100%

1. topic 1 question 198

You have an application deployed in Google Kubernetes Engine (GKE) that reads and processes Pub/Sub messages. Each Pod handles a fixed number of messages per minute. The rate at which messages are published to the Pub/Sub topic varies considerably throughout the day and week, including occasional large batches of messages published at a single moment.

You want to scale your GKE Deployment to be able to process messages in a timely manner. What GKE feature should you use to automatically adapt your workload?

A. Vertical Pod Autoscaler in Auto mode

B. Vertical Pod Autoscaler in Recommendation mode

C. Horizontal Pod Autoscaler based on an external metric

D. Horizontal Pod Autoscaler based on resources utilization

Answer: C

in GKE/K8s, there is no such thing as vertical pod autoscaler. Pub/Sub is an external source to GKE

1. topic 1 question 199

You have a Compute Engine application that you want to autoscale when total memory usage exceeds 80%. You have installed the Cloud Monitoring agent and configured the autoscaling policy as follows:  
  
A screenshot of a computer

AI-generated content may be incorrect.  
  
You observe that the application does not scale under high load. You want to resolve this. What should you do?

A. Change the Target type to DELTA\_PER\_MINUTE.

B. Change the Metric identifier to agent.googleapis.com/memory/bytes\_used.

C. Change the filter to metric.label.state = ‘used’.

D. Change the filter to metric.label.state = ‘free’ and the Target utilization to 20.

Answer: C

100%

The current filter is set up with multiple AND conditions, which means it's looking for a metric that simultaneously has all these states: 'used', 'buffered', 'cached', and 'slab'. This is logically impossible, as a memory location can't be in multiple states at once.

1. topic 1 question 200

Your company has a Google Cloud project that uses BigOuery for data warehousing. The VPN tunnel between the on-premises environment and Google Cloud is configured with Cloud VPN. Your security team wants to avoid data exfiltration by malicious insiders, compromised code, and accidental oversharing. What should you do?

A. Configure Private Service Connect.

B. Configure VPC Service Controls and configure Private Google Access for on-promises hosts.

C. Create a service account, grant the BigQuery JobUser role and Storage Object Viewer role to the service account, and remove all other Identity and Access Management (IAM) access from the project.

D. Configure Private Google Access.

Answer: B

This question similar to **topic 1 question 156** but with slightly different wording in answers

**VPC Service Controls** help you create a security perimeter around your Google Cloud services (like BigQuery) to reduce the risk of data exfiltration, even if credentials are compromised or insiders attempt to overshare data.

**Private Google Access** for on-premises hosts ensures that on-premises systems can securely access Google APIs and services without going over the public internet, further reducing exposure.

1. topic 1 question 201

Your company uses Cloud Logging to manage large volumes of log data. You need to build a real-time log analysis architecture that pushes logs to a third-party application for processing. What should you do?

A. Create a Cloud Logging log export to Pub/Sub.

B. Create a Cloud Logging log export to BigQuery.

C. Create a Cloud Logging log export to Cloud Storage.

D. Create a Cloud Function to read Cloud Logging log entries and send them to the third-party application.

Answer: A

A: Creating a Cloud Logging log export to Pub/Sub is the correct solution for this scenario. Pub/Sub is designed for real-time messaging and can push messages (in this case, log entries) to a third-party application for processing.

B: While BigQuery is great for analyzing large volumes of data, it's not designed for real-time data pushing to third-party applications. D: Creating a Cloud Function to read log entries and send them to a third-party application could work, but it would add unnecessary complexity. Using Pub/Sub is a simpler and more efficient solution.

1. topic 1 question 203

As part of implementing their disaster recovery plan, your company is trying to replicate their production MySQL database from their private data center to their Google Cloud project using a Google Cloud VPN connection.

They are experiencing latency issues and a small amount of packet loss that is disrupting the replication.

What should they do?

A. Configure their replication to use UDP.

B. Configure a Google Cloud Dedicated Interconnect.

C. Restore their database daily using Google Cloud SQL.

D. Add additional VPN connections and load balance them.

E. Send the replicated transaction to Google Cloud Pub/Sub.

Answer: B

Explanations:

additional VPN not good choice here due to fact Classic is active-passive connection

cant use to load balance them.

# Google Cloud Developer Qs

1. topic 1 question 202

You are developing a new public-facing application that needs to retrieve specific properties in the metadata of users’ objects in their respective Cloud Storage buckets. Due to privacy and data residency requirements, you must retrieve only the metadata and not the object data. You want to maximize the performance of the retrieval process. How should you retrieve the metadata?

A. Use the patch method.

B. Use the compose method.

C. Use the copy method.

D. Use the fields request parameter.

Answer: D

100%

1. topic 1 question 204

You work at a rapidly growing financial technology startup. You manage the payment processing application written in Go and hosted on Cloud Run in the Singapore region (asia-southeast1). The payment processing application processes data stored in a Cloud Storage bucket that is also located in the Singapore region.

The startup plans to expand further into the Asia Pacific region. You plan to deploy the Payment Gateway in Jakarta, Hong Kong, and Taiwan over the next six months. Each location has data residency requirements that require customer data to reside in the country where the transaction was made. You want to minimize the cost of these deployments. What should you do?

A. Create a Cloud Storage bucket in each region, and create a Cloud Run service of the payment processing application in each region.

B. Create a Cloud Storage bucket in each region, and create three Cloud Run services of the payment processing application in the Singapore region.

C. Create three Cloud Storage buckets in the Asia multi-region, and create three Cloud Run services of the payment processing application in the Singapore region.

D. Create three Cloud Storage buckets in the Asia multi-region, and create three Cloud Run revisions of the payment processing application in the Singapore region.

Answer: A

Keywords "Each location has data residency requirements "

# Additional Information

## Cloud SQL

* Additional **read replicas** to increase read performance. replicas can be within region or different region. Multiple read replicas can be configured
* **HA configuration** create secondary instance in secondary zone within configured region. Only one HA instance. ([link](https://cloud.google.com/sql/docs/sqlserver/high-availability#normal))

## Computing platform:

App Engine

- just to run any developer codes. Focus on codes not infra. Cheap, has auto-scale.

- has two environments: Standard (design to scale to zero) and Flexible (has lot of features)

Compute Engine

- with Managed Instance Group can enable auto-scaling

Kubernetes Engine

- main thing to runs containerized applications

- cluster already has auto-scaling.

- application deployment can be auto-scaled with Horizontal Pod Autoscaler (HPA). can use CPU as standard metric or external customized metrics

## Database or Storage selection:

Cloud Storage – long period retention/archived data. has bucket lock retention to prevention deletion/changes

Cloud SQL – RDBMS. Can choose between MySQL, PostGreSQL or Microsoft SQL Server.

BigQuery – Read-only Data analytics, cheaper than BigTable.

BigTable – Read/Write data analytics, very expensive. Time-series, IoT, low latency updates. Massive amount of data

Datastore – meant to EOL, replaced by firestore

FileStore – NAS Storage

Firestore – Multi-regional but lightweight. Ideal database solution for mobile/web application1

Persistent Disks – Attached only to GCE instance

## Data transfer options: ([link](https://cloud.google.com/storage-transfer/docs/transfer-options?_gl=1*1theuv*_up*MQ..&gclid=Cj0KCQjwxJvBBhDuARIsAGUgNfgEIPrI3f9k50LEBBpsQ7T0cYd8x6-It-LXhT3CPKkAntgKK4c-sWcaAm3zEALw_wcB&gclsrc=aw.ds))

|  |  |
| --- | --- |
| Transfer scenario | Recommendation |
| Transferring from another cloud storage provider | Use Storage Transfer Service. |
| Transferring less than 1 TB from on-premises | [Use gcloud storage.](https://cloud.google.com/sdk/gcloud/reference/storage) |
| Transferring more than 1 TB from on-premises | Use Storage Transfer Service or Transfer Appliance. |
| Transferring less than 1 TB from another Cloud Storage region | [Use gcloud storage.](https://cloud.google.com/sdk/gcloud/reference/storage) |
| Transferring more than 1 TB from another Cloud Storage region | Use Storage Transfer Service. |

## Private connection + Security

* **Direct VPC egress** enable your Cloud Run service or job to send traffic to a VPC network by using Direct VPC egress with no Serverless VPC Access connector required. this feature has lots of limitations as compared to Serverless VPC Access
* **Google NAT** lets you restrict inbound communications to your app instances while allowing them to have outbound communications to the internet without using public IPs.
* **Private Google Access** for on-premises hosts or VM on VPC networks with only internal IP addresses can securely access Google APIs and services without going over the public internet, further reducing exposure.
* **Private Service Access** lets youreach the internal IP addresses of these Google services and third-party services that hosted in Google VPC network by using private connections.VM instances in VPC network only uses internal IP
* **VPC Service Controls** help you create a security perimeter around your Google Cloud services (like BigQuery) to reduce the risk of data exfiltration, even if credentials are compromised or insiders attempt to overshare data.
* **Serverless VPC Access** to connect directly to your VPC network from serverless environments such as Cloud Run and App Engine.

Pub/Sub

- messaging platform

https://www.examtopics.com/discussions/google/55/

## Serverless Computing

Cloud Function

- run any java/python/php codes when got triggered by event. best works with message directed to Pub/Sub

Cloud Run

- runs stateless container