CertyIQ


# CertyIQ

## Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

https://www.CertyIQ.com

# About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

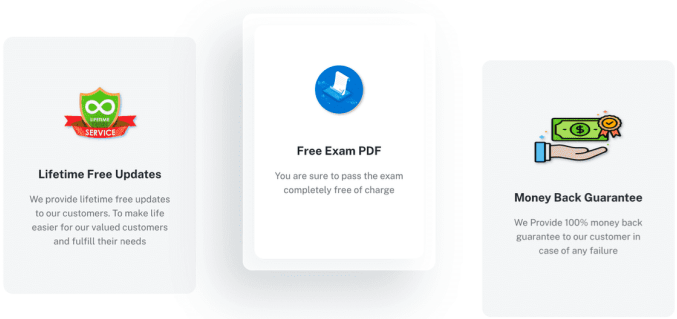
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

# Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

https://www.certyiq.com

Mail us on - certyiqofficial@gmail.com




**John**

October 19, 2022

★★★★★

Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

**Dana**

September 04, 2022

★★★★★

Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

**Ahamed Shibly**

2 months ago

★★★★★

Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022

★★★★★

Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study.
Thank You certyiq team!

**Henry Rome**

2 months ago

★★★★★

These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

**Esmaria**

2 months ago

★★★★★

Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's.Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

# Google

(Professional Cloud Architect)

Professional Cloud Architect on Google Cloud Platform

Total: **332 Questions**

Link: https://certyiq.com/papers/google/professional-cloud-architect

**Question: 1** CertyIQ

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**

**Explanation:**

D is the answer because HTTP(S) load balancer can direct traffic reaching a single IP to different backends based on the incoming URL. A is not correct because configuring a new load balancer would require a new or different SSL and DNS records which conflicts with the requirements to keep the same SSL and DNS records. B is not correct because it goes against the requirements. The company wants to keep the old API available while new customers and testers try the new API. C is not correct because it is not a requirement to decommission the implementation behind the old API. Moreover, it introduces unnecessary risk in case bugs or incompatibilities are discovered in the new API.

**Question: 2** CertyIQ

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 a 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**

**Explanation:**
BigQuery is Google's serverless, highly scalable, low cost enterprise data warehouse designed to make all your data analysts productive. Because there is no infrastructure to manage, you can focus on analyzing data to find meaningful insights using familiar SQL and you don't need a database administrator.
BigQuery enables you to analyze all your data by creating a logical data warehouse over managed, columnar storage as well as data from object storage, and spreadsheets.

Reference:
https://cloud.google.com/bigquery/

**Question: 3** CertyIQ

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 recommend? (Choose three.)

A. Port the application code to run on Google App Engine
B. Integrate Cloud Dataflow into the application to capture real-time metrics
C. Instrument the application with a monitoring tool like Stackdriver Debugger
D. Select an automation framework to reliably provision the cloud infrastructure
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: CDE**

**Explanation:**

CDE looks like correct .

Porting a J2EE application to App Engine will not work as its is - there are three arpproach for migration -

There are three major types of migrations:

Lift and shift

Improve and move

Rip and replace

So Option A can be discarded .

So the answer is CDE .

**Question: 4** CertyIQ

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?

```
import news
from flask import Flask, redirect, request
from flask.ext.api import status
from google.appengine.api import users

app = Flask(_name_)
sessions = {}

@app.route("/")
def homepage():
      user = users.get_current_user()
      if not user:
            return "Invalid login",
status.HTTP_401_UNAUTHORIZED

      if user not in sessions:
            sessions[user] = {"viewed": []}

      news_articles = news.get_new_news (user, sessions [user]
["viewed"])
      sessions [user] ["viewed"] +- [n["id"] for n
in news_articles]

      return news.render(news_articles)

if _name_ == "_main_":
      app.run()
```

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

**Answer: A**

**Explanation:**

It's A. 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.

**Question: 5** CertyIQ

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 resources 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: C**

**Explanation:**

Never impose tools for customers, It is not Good Professional Practice. Indeed, there deploying to GCP, but You need to understand the Monitoring and Logging Requirements to be effective in your proposal.

Remember, Monitoring and Logging have a Cost associate.

**Question: 6** CertyIQ

You need to reduce the number of unplanned rollbacks of erroneous production deployments in your company's web hosting platform. Improvement to the QA/
Test processes accomplished an 80% reduction.
Which additional two approaches can you take to further reduce the rollbacks? (Choose two.)

A. Introduce a green-blue deployment model
B. Replace the QA environment 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**

**Explanation:**

But, ATENTION...the model is called BLUE GREEN DEPLOYMENT no GREEN BLUE in the A option.

**Question: 7** CertyIQ

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

A. Use the - -no-auto-delete flag on all persistent disks 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**

**Explanation:**

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

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

**Question: 8** CertyIQ

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**

**Explanation:**
Relational databases were not designed to cope with the scale and agility challenges that face modern applications, nor were they built to take advantage of the commodity storage and processing power available today.
NoSQL fits well for:
✑ Developers are working with applications that create massive volumes of new, rapidly changing data types " structured, semi-structured, unstructured and polymorphic data.
Incorrect Answers:
D: The Blobstore API allows your application to serve data objects, called blobs, that are much larger than the size allowed for objects in the Datastore service.
Blobs are useful for serving large files, such as video or image files, and for allowing users to upload large data files.

Reference:
https://www.mongodb.com/nosql-explained

**Question: 9** CertyIQ

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

What should you do?

A. Ensure that a firewall 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**

**Explanation:**
The best practice when configuration a health check is to check health and serve traffic on the same port. However, it is possible to perform health checks on one port, but serve traffic on another. If you do use two different ports, ensure that firewall rules and services running on instances are configured appropriately. If you run health checks and serve traffic on the same port, but decide to switch ports at some point, be sure to update both the backend service and the health check.
Backend services that do not have a valid global forwarding rule referencing it will not be health checked and will have no health status.

Reference:
https://cloud.google.com/compute/docs/load-balancing/http/backend-service

**Question: 10** CertyIQ

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 virtual machine 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:**

1. C - Service accounts with limited access are a best practice.The use of Access scopes (Option B) is only recommended when using default service accounts, which is not a good practice recommendation either.

2. C. Create a new service account with BigQuery access and execute your script with that userService account is always a preferred option.

**Question: 11** CertyIQ

Your customer is moving an existing corporate application to Google Cloud Platform 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**

**Explanation:**

B is the correct answer

B no brainer, this method makes the AD or Azure ADFS whatever your identity provide is the single source of truth and doesn't not sync passwords.

**Question: 12** CertyIQ

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**

**Explanation:**
Cloud Dataflow is a fully-managed service for transforming and enriching data in stream (real time) and batch (historical) modes with equal reliability and expressiveness -- no more complex workarounds or compromises needed.

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

**Question: 13** CertyIQ

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

A. Work with your ISP to diagnose the problem

B. Open a support ticket to ask for network capture and flow data to diagnose the problem, then roll back your application

C. Roll back to an earlier known good release initially, then use Stackdriver Trace and Logging to diagnose the problem in a development/test/staging environment

D. Roll back to an earlier known good release, then push the release again at a quieter period to investigate. Then use Stackdriver Trace and Logging to diagnose the problem

**Answer: C**

**Explanation:**
Stackdriver Logging allows you to store, search, analyze, monitor, and alert on log data and events from Google Cloud Platform and Amazon Web Services
(AWS). Our API also allows ingestion of any custom log data from any source. Stackdriver Logging is a fully managed service that performs at scale and can ingest application and system log data from thousands of VMs. Even better, you can analyze all that log data in real time.

Reference:
https://cloud.google.com/logging/

**Question: 14** CertyIQ

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 size of the persistent disk and verify the new space is ready to use with the fdisk command in Linux

D. In the Cloud Platform Console, create a new persistent disk attached to the virtual machine, format and mount it, and configure the database service to move the files to the new disk

E. 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**

**Explanation:**
On Linux instances, connect to your instance and manually resize your partitions and file systems to use the additional disk space that you added.
Extend the file system on the disk or the partition to use the added space. If you grew a partition on your disk, specify the partition. If your disk does not have a partition table, specify only the disk ID. sudo resize2fs /dev/[DISK_ID][PARTITION_NUMBER] where [DISK_ID] is the device name and [PARTITION_NUMBER] is the partition number for the device where you are resizing the file system.

Reference:
https://cloud.google.com/compute/docs/disks/add-persistent-disk

**Question: 15** CertyIQ

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 discovery phase by labeling all of the virtual machines (VMs) that process PCI data

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

**Answer: A**

**Explanation:**

A. Create a tokenizer service and store only tokenized data

Reference:

https://www.sans.org/reading-room/whitepapers/compliance/ways-reduce-pci-dss-audit-scope-tokenizing-cardholder-data-33194

**Question: 16** CertyIQ

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

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

**Answer: B**

**Explanation:**
Google Cloud Bigtable is a scalable, fully-managed NoSQL wide-column database that is suitable for both real-time access and analytics workloads.
Good for:
- Low-latency read/write access
- High-throughput analytics
- Native time series support

Common workloads:
- IoT, finance, adtech
- Personalization, recommendations
- Monitoring
- Geospatial datasets
- Graphs

Incorrect Answers:
C: Google Cloud Storage is a scalable, fully-managed, highly reliable, and cost-efficient object / blob store.
Is good for:
- Images, pictures, and videos
- Objects and blobs
- Unstructured data

D: Google Cloud Datastore is a scalable, fully-managed NoSQL document database for your web and mobile applications.
Is good for:
- Semi-structured application data
- Hierarchical data
- Durable key-value data

✑ Common workloads:
✑ User profiles
✑ Product catalogs
✑ Game state

Reference:
https://cloud.google.com/storage-options/

**Question: 17** CertyIQ

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**

**Explanation:**

All four are correct answers. Google has built in cron job schduling with Cloud Schedule, so that would place "D" behind "C" in Google's perspective. Google also has it's own lifecycle management command line prompt gcloud lifecycle so "A" or "B" could be used. JSON is slightly faster than XML because of the " " verse "<c>" distinguisher, with a Trie tree used for alphanumeric parsing. So between "A" and "B", choose "B". Between "B" and "A", "B" is slightly more efficient from the GCP operator perspective. So choose "B".

**Question: 18** CertyIQ

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 Kubernetes Engine

**Answer: B**

**Explanation:**
Google Cloud Dataproc is a fast, easy-to-use, low-cost and fully managed service that lets you run the Apache Spark and Apache Hadoop ecosystem on Google
Cloud Platform. Cloud Dataproc provisions big or small clusters rapidly, supports many popular job types, and is integrated with other Google Cloud Platform services, such as Google Cloud Storage and Stackdriver Logging, thus helping you reduce TCO.

Reference:

https://cloud.google.com/dataproc/docs/resources/faq

**Question: 19** CertyIQ

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**

**Explanation:**

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

**Question: 20** CertyIQ

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**

**Explanation:**
Google Cloud Bigtable is a scalable, fully-managed NoSQL wide-column database that is suitable for both real-time access and analytics workloads.
Good for:
- Low-latency read/write access
- High-throughput analytics
- Native time series support

Common workloads:
- IoT, finance, adtech
- Personalization, recommendations
- Monitoring
- Geospatial datasets
- Graphs

Reference:

https://cloud.google.com/storage-options/

**Question: 21** CertyIQ

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 a 99,99% availability SLA under these conditions. However next quarter, your company will be making the portal available to all users, including unauthenticated 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 autoscale 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. Expose 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**

**Explanation:**

B caters for terminating the service in both zones randomly. You want to be able to test resiliency when either zone has an outage.

**Question: 22** CertyIQ

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 two.)

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 he package dependencies (Python and pip) are installed

**Answer: CE**

**Explanation:**

The speed of deployment can be changed by limiting the size of the uploaded app, limiting the complexity of the build necessary in the Dockerfile, if present, and by ensuring a fast and reliable internet connection.
Note: Alpine Linux is built around musl libc and busybox. This makes it smaller and more resource efficient than traditional GNU/Linux distributions. A container requires no more than 8 MB and a minimal installation to disk requires around 130 MB of storage. Not only do you get a fully-fledged Linux environment but a large selection of packages from the repository.

Reference:
https://groups.google.com/forum/#!topic/google-appengine/hZMEkmmObDU https://www.alpinelinux.org/about/

**Question: 23** CertyIQ

Your solution is producing performance bugs in production that you did not see in staging and test environments. You want 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**

**Explanation:**

C - question states it is a performance problem Therefore load testing will expose such issues in the test and staging env

C. Increase the load on your test and staging environments - The whole purpose is to test a production-like load....

**Question: 24** CertyIQ

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 requests 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**

**Explanation:**

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

Reference:

https://cloud.google.com/trace/docs/quickstart#find_a_trace

**Question: 25** CertyIQ

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**

**Explanation:**

A -> It makes no sense, you don't change your DBA software because it's misconfigured

B-> It will eventually gives you more time to fix the problem, but you don't fix "the replica is never promoted to master"

C-> Creating snapshots makes no sense about our problem here

D-> By implementing a regular failover you will have to fix the problem + doing a regular failover is a good practice

Answer is D

**Question: 26** CertyIQ

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 the default retention policies
D. Configure Stackdriver Monitoring for all Projects, and export to Google Cloud Storage

**Answer: D**

**Explanation:**

D makes more sense, BQ is very expensive as a storage

The answer is D because it is not required to the analysis straightaway or even if it actually needs to be done. The main requirement is that it needs to be stored for compliance purposes and IF NEED BE for analytics as well.

**Question: 27** CertyIQ

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**

**Explanation:**
Google Cloud Dedicated Interconnect provides direct physical connections and RFC 1918 communication between your on-premises network and Google's network. Dedicated Interconnect enables you to transfer large amounts of data between networks, which can be more cost effective than purchasing additional bandwidth over the public Internet or using VPN tunnels.
Benefits:
✑ Traffic between your on-premises network and your VPC network doesn't traverse the public Internet. Traffic traverses a dedicated connection with fewer hops, meaning there are less points of failure where traffic might get dropped or disrupted.
✑ Your VPC network's internal (RFC 1918) IP addresses are directly accessible from your on-premises network. You don't need to use a NAT device or VPN tunnel to reach internal IP addresses. Currently, you can only reach internal IP addresses over a dedicated connection. To reach Google external IP addresses, you must use a separate connection.
✑ You can scale your connection to Google based on your needs. Connection capacity is delivered over one or more 10 Gbps Ethernet connections, with a maximum of eight connections (80 Gbps total per interconnect).
✑ The cost of egress traffic from your VPC network to your on-premises network is reduced. A dedicated connection is generally the least expensive method if you have a high-volume of traffic to and from Google's network.

Reference:
https://cloud.google.com/interconnect/docs/details/dedicated

**Question: 28** CertyIQ

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 delegate access to the bucket

**Answer: B**

**Explanation:**

B. Enable Logging export to Google BigQuery and use ACLs and views to scope the data shared with the auditor. B is a neater solution as they are looking to streamline and expedite the audit process compared to D thats is a cheaper solution and not as neat.

B: https://cloud.google.com/iam/docs/job-functions/auditing#scenario_external_auditors

**Question: 29** CertyIQ

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

A. In 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**

**Explanation:**

C is the answer, since key management systems generate, use, rotate, encrypt, and destroy cryptographic keys and manage permissions to those keys.

A is incorrect because storing credentials in source code and source control is discoverable, in plain text, by anyone with access to the source code. This also introduces the requirement to update code and do a deployment each time the credentials are rotated. B is not correct because consistently populating environment variables would require the credentials to be available, in plain text, when the session is started. D is incorrect because instead of managing access to the config file and updating manually as keys are rotated, it would be better to leverage a key management system. Additionally, there is increased risk if the config file contains the credentials in plain text.

Reference:

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

**Question: 30** CertyIQ

A lead engineer wrote a custom tool that deploys virtual machines 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 two.)

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: EF**

**Explanation:**

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

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

**Question: 31** CertyIQ

A development manager is building a new application. He asks you to review his requirements and identify what cloud technologies he can use to meet them. The application must:
1. Be based on open-source technology for cloud portability
2. Dynamically scale compute capacity based on demand
3. Support continuous software delivery
4. Run multiple segregated copies of the same application stack
5. Deploy application bundles using dynamic templates
6. Route network traffic to specific services based on URL
Which combination of technologies will meet all of 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**

**Explanation:**

A seems to be the answer

A. Google Kubernetes Engine, Jenkins, and Helm. This is a better answer than D because - Load Balancing is already available for Kubernetes (The Kubernetes load balancer works by sending connections to the first server in the pool until its capacity is reached)- Helm is required for managing Kubernetes packages - install/deploy/manage/etc.

**Question: 32** CertyIQ

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**

**Explanation:**

A startup script, or a shutdown script, is specified through the metadata server, using startup script metadata

keys.

Reference:

https://cloud.google.com/compute/docs/startupscript

**Question: 33** CertyIQ

Your organization has a 3-tier web application deployed in the same network on Google Cloud Platform. 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**

**Explanation:**
Google Cloud Platform(GCP) enforces firewall rules through rules and tags. GCP rules and tags can be defined once and used across all regions.

Reference:
https://cloud.google.com/docs/compare/openstack/
https://aws.amazon.com/it/blogs/aws/building-three-tier-architectures-with-security-groups/

**Question: 34** CertyIQ

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**

**Explanation:**

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

C. Use gcloud or Cloud Console to connect to the serial console and observe the logs = Check grub messages, remember new kernel module was installed.

E. Adjust the Google Stackdriver timeline to match the failure time, and observe the batch server metrics = Zoom into the time window when problem happened.

**Question: 35** CertyIQ

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**

**Explanation:**

Answer is A as they want to load logs for analytics and E for storing data in buckets for long term

**Question: 36** CertyIQ

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 on the fox locally
B. Revert the source code change, and rerun the deployment pipeline
C. Log into the servers with the bad code change, and swap in the previous code
D. Change the instance group template to the previous one, and delete all instances

**Answer: B**

**Explanation:**

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

>> Long step, hence eliminate

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

>> This revert will be logged in the source repo. Will go with this way although D also is correct.

C. login to the servers with the bad code change, and swap in the previous code

>> C is manually doing what can be automatically done by B and C, hence eliminate.

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

>> This is similar to B but why manually do something which is automated. Hence eliminate. But is also correct. But B is better from code lifecycle perspective.

Hence B

**Question: 37** CertyIQ

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

**Answer: C**

**Explanation:**
Folders are nodes in the Cloud Platform Resource Hierarchy. A folder can contain projects, other folders, or a combination of both. You can use folders to group projects under an organization in a hierarchy. For example, your organization might contain multiple departments, each with its own set of GCP resources. Folders allow you to group these resources on a per-department basis. Folders are used to group resources that share common IAM policies. While a folder can contain multiple folders or resources, a given folder or resource can have exactly one parent.

Reference:
https://cloud.google.com/resource-manager/docs/creating-managing-folders

**Question: 38** CertyIQ

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

```
java.lang.SecurityException: SHA1 digest error for
com/Altostrat/CloakedServlet.class
     at com.google.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.JarVerifier.update
(JarVerifier.java:205)
     at
java.util.jar.JarVerifiersVerifierStream.read
(JarVerifier.java:428)
     at sun.misc.Resource.getBytes
(Resource.java:124)
     at java.net.URL.ClassLoader.defineClass
(URLClassLoader.java:273)
     at sun.reflect.GeneratedMethodAccessor5.invoke
(Unknown Source)
     at
sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
     at java.lang.reflect.Method.invoke
(Method.java:616)
     at java.lang.ClassLoader.loadClass
(ClassLoader.java:266)
```

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

**Answer: B**

**Explanation:**

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

**Question: 39** CertyIQ

You are designing a mobile chat application. You want to ensure people cannot spoof chat messages, by providing a message 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**

**Explanation:**

Option C - Use public key infrastructure (PKI) to encrypt the message client-side using the originating user's private key: Using PKI to encrypt messages using the originating user's private key provides end-to-end encryption, which means only the intended recipient can decrypt the message. This option also ensures that the message's authenticity is protected. If a malicious user changes the sender's name, the recipient will not be able to decrypt the message since it was not encrypted using the correct private key. This option is a strong method for securing chat messages.

**Question: 40** CertyIQ

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
GCP 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**

**Explanation:**

It's latency issues. That won't be solved by adding another VPN tunnel. If it was just a throughput issue then VPN would do, however to improve latency you need to go layer 2. Answer is B

**Question: 41** CertyIQ

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 personally 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 expressions to find and redact phone numbers, email addresses, and credit card numbers

**Answer: C**

**Explanation:**

Reference:
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp#using_data_loss_prevention_api_to_sanitize_data

**Question: 42** CertyIQ

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**

**Explanation:**

https://cloud.google.com/shell/docs/how-cloud-shell-works

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. Unlike the instance itself, this storage does not time out on inactivity. All files you store in your home directory, including installed software, scripts and user configuration files like .bashrc and .vimrc, persist between sessions. Your $HOME directory is private to you and cannot be accessed by other users.

**Question: 43** CertyIQ

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**

**Explanation:**

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

**Question: 44** CertyIQ

You are analyzing and defining business processes to support your startup's trial usage of GCP, and you don't yet know what consumer demand for your product will be. Your manager requires you to minimize GCP 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. Provide 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. Provide training to the team about service cost management.

**Answer: B**

**Explanation:**

Answer B

Sustained use discounts are applied on incremental use after you reach certain usage thresholds. This means that you pay only for the number of minutes that you use an instance, and Compute Engine automatically gives you the best price. There's no reason to run an instance for longer than you need it.

- https://cloud.google.com/compute/docs/sustained-use-discounts

Committed use discounts are ideal for workloads with predictable resource needs. When you purchase a committed use contract, you purchase compute resource (vCPUs, memory, GPUs, and local SSDs) at a discounted price in return for committing to paying for those resources for 1 year or 3 years. The discount is up to 57% for most resources like machine types or GPUs. The discount is up to 70% for memory-optimized machine types. For committed use prices for different machine types, see VM instances pricing.

- https://cloud.google.com/compute/docs/instances/signing-up-committed-use-discounts

**Question: 45** CertyIQ

You are building a continuous deployment pipeline for a project stored in a 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**

**Explanation:**

the best answer is D, because the 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.

Reference:

https://github.com/GoogleCloudPlatform/continuous-deployment-on-kubernetes/blob/master/README.md

**Question: 46** CertyIQ

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 into 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**

**Explanation:**

C, is the correct answer. As per the requirement linux expert would need access to VM to troubleshoot the issue. With health check enabled, old VM will be terminated as soon as health-check fails for the VM and new VM will be auto-created. So, this situation will prevent linux expert to troubleshoot the issue. Had it been the case that stack-drover logging is enabled and the expert just want to view the logs from the Cloud-logs than role to project-viewer could help. But it is specifically mentioned that expert will login into VM to troubleshoot the issue and not looking at the cloud Logs. So, Option-C is the correct answer.

**Question: 47** CertyIQ

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 GCP that is certified for PCI DSS hosting.
B. GKE cannot be used under PCI DSS because it is considered shared hosting.
C. GKE and GCP provide the tools you need to build a PCI DSS-compliant environment.
D. All Google Cloud services are usable because Google Cloud Platform is certified PCI-compliant.

**Answer: C**

**Explanation:**

C: GKE & Compute Engine is PCI DSS compliant while Cloud Function, App Engine are not PC compliant

**Question: 48** CertyIQ

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**

**Explanation:**

Answer is B:

Keynotes from question:

1- On-premise data sources

2- Unfit data; not well maintained and degraded

3- Google-recommended best practice to "detect anomalies" <<-Very important.

A & C - incorrect; Datalab does not provide anomaly detection OOTB. It is used more for data science scenarios like interactive data analysis and build ML models.

B - CORRECT; DataPrep OOTB provides for fast exploration and anomaly detection and lists cloud storage as an ingestion medium. Refer to ELT pipeline architecture here = https://cloud.google.com/dataprep

D - incorrect; At this time DataPrep cannot connect to SaaS or on-premise source. Not to be confused for DataFlow which can!

**Question: 49** CertyIQ

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 hierarchy?

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**

**Explanation:**

C Google Cloud resources are organized hierarchically, where the organization node is the root node in the hierarchy, the projects are the children of the organization, and the other resources are descendants of projects. You can set Identity and Access Management (IAM) policies at different levels of the resource hierarchy. Resources inherit the policies of the parent resource. The effective policy for a resource is the union of the policy set at that resource and the policy inherited from its parent.

Reference:

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

**Question: 50** CertyIQ

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-premise 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**

**Explanation:**

Ans is C,

https://cloud.google.com/vpc/docs/using-vpc

"Primary and secondary ranges can't conflict with on-premises IP ranges if you have connected your VPC network to another network with Cloud VPN, Dedicated Interconnect, or Partner Interconnect."

**Question: 51** CertyIQ

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 GCP 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**

**Explanation:**

Correct A, you have to recreate the indexes

**Question: 52** CertyIQ

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

B. Deploy the application on a Compute Engine instance. Use the instance to serve traffic, and use the 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. 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.

**Answer: C**

**Explanation:**

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.

**Question: 53** CertyIQ

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 open 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**

**Explanation:**

Agree with D - "When to choose the flexible environment" "Accesses the resources or services of your Google Cloud project that reside in the Compute Engine network."

https://cloud.google.com/appengine/docs/the-appengine-environments

**Question: 54** CertyIQ

You are 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 firewall rules to block all traffic except the IP address range for Cloud Source Repositories. Download the files to the VM using gsutil.

**Answer: A**

**Explanation:**

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.

**Question: 55** CertyIQ

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**

**Explanation:**

A' Transfer Appliance lets you quickly and securely transfer large amounts of data to Google Cloud Platform via a high capacity storage server that you lease from Google and ship to our datacenter. Transfer Appliance is recommended for data that exceeds 20 TB or would take more than a week to upload.

**Question: 56** CertyIQ

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 which the new container image. Use kubectl delete service/echo-service and kubectl create "f <yaml-file>

**Answer: A**

**Explanation:**

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

**Question: 57** CertyIQ

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**

**Explanation:**

C is the correct Answer

A is wrong because bq User Permission will allow you to edit the dataset, which is something that we don't want in this scenario.

B and D is wrong because "You want to make sure that no query costs are incurred on the projects that contain the data" so you don't want users to fire quires on the Project that contains the dataset , hence the "dataViewer" permission

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

**Question: 58** CertyIQ

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**

**Explanation:**

Ans B "When should you use a signed URL? In some scenarios, you might not want to require your users to have a Google account in order to access Cloud Storage" "Signed URLs contain authentication information in their query string, allowing users without credentials to perform specific actions on a resource"

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

**Question: 59** CertyIQ

Your web application must comply with the requirements of the European Union'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 Platform, because Google already has various certifications and provides pass-on compliance when you use native features.

B. Enable the relevant GDPR compliance setting within the GCPConsole 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**

**Explanation:**

The GDPR lays out specific requirements for businesses and organizations who are established in Europe or who serve users in Europe. It:

Regulates how businesses can collect, use, and store personal data

Builds upon current documentation and reporting requirements to increase accountability

Authorizes fines on businesses who fail to meet its requirements

Reference:

https://www.mobiloud.com/blog/gdpr-compliant-mobile-app/

**Question: 60** CertyIQ

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
GCP 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**

**Explanation:**

A seems correct.

"... high availability (HA) configuration for Cloud SQL instances... A Cloud SQL instance configured for HA is also called a regional instance and is located in a primary and secondary zone within the configured region.

In the event of an instance or zone failure, this configuration reduces downtime, and your data continues to be available to client applications."

**Question: 61** CertyIQ

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:**

Deployment Manager is used to automate the process of provisioning infrastructure. Therefore, gcloud and Deployment Manager do the same thing. Meanwhile, kubectl is used to run commands against an already created cluster.

**Question: 62** CertyIQ

You need to evaluate your team readiness for a new GCP 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 GCP projects successfully to date. What should you do?

A. Allocate budget for team training. Set a deadline for the new GCP project.
B. Allocate budget for team training. Create a roadmap for your team to achieve Google Cloud certification based on job role.
C. Allocate budget to hire skilled external consultants. Set a deadline for the new GCP project.
D. Allocate budget to hire skilled external consultants. Create a roadmap for your team to achieve Google Cloud certification based on job role.

**Answer: B**

**Explanation:**

B...- Allocate budget for team training. - Create a roadmap for your team - Achieve Google Cloud certification based on "job role".

**Question: 63** CertyIQ

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**

**Explanation:**

A. Cloud Functions - managed service scales down to 0

B. Compute Engine - not a managed service

C. Google Kubernetes Engine - not a managed service and wont scale down to 0

D. AppEngine flexible environment - managed service but wont scale down to 0

**Question: 64** CertyIQ

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**

**Explanation:**

Correct Answer: A

Create the Key object for each Entity and run a batch get operation

https://cloud.google.com/datastore/docs/best-practices

Use batch operations for your reads, writes, and deletes instead of single operations. Batch operations are more efficient because they perform multiple operations with the same overhead as a single operation.

Firestore in Datastore mode supports batch versions of the operations which allow it to operate on multiple objects in a single Datastore mode call.

Such batch calls are faster than making separate calls for each individual entity because they incur the overhead for only one service call. If multiple entity groups are involved, the work for all the groups is performed in parallel on the server side.

**Question: 65** CertyIQ

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 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**

**Explanation:**

A is correct. use gsutil to upload file in Cloud Storage. And Cloud Storage configuration is defined in .boto on client side.

**Question: 66** CertyIQ

Your customer wants to capture multiple GBs of aggregate real-time key performance indicators (KPIs) from their game servers running on Google Cloud Platform 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 visualizations of them in Cloud Datalab.

**Answer: B**

**Explanation:**

Data studio cannot be used with BigTable

Reference:

https://cloud.google.com/solutions/data-lifecycle-cloud-platform

**Question: 67** CertyIQ

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 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: C**

**Explanation:**

C is the answer, B is a big of a machine for just .1cpu, if we need t run many versions of this it will be a waste of resources. now A is a fit however o much of work to get the image and deploy the machine and scaling time as well. I see that C is a better fit.

Two key aspects: maximize machine utilization and reliably deploy new versions of the application.Thinking about the option A from the perspective of the above requirement: For even a single line of code change you will have to:1. Restart the machine(s)2. Spend machine cycles for boot3. Run the startup script to clone the repository and check out the production branch4. Install the dependencies (even if the dependencies are already installed even then the code would atleast execute and check if they are there or not)5. Start the Python app.Where as in K8 environment either some of the above activities are either not required or performed efficiently. Due to layer caching in docker image building process, only the changed code is built, pulled and deployed without the need to touch other services/dependencies (note the key word imagePullPolicy set to 'IfNotPresent')

**Question: 68** CertyIQ

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 Active Directory domain controller.

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

C. Use Cloud Identity-Aware Proxy configured to use the on-premises Active Directory domain controller as an identity provider.

D. Use Compute Engine to create an Active Directory (AD) domain controller that is a replica of the on-premises AD domain controller using Google Cloud Directory Sync.

**Answer: B**

**Explanation:**

It's simple. Domain controllers are not meant authenticate saas or web applications. This includes iam. Domain controllers speak ntlm and Kerberos.

This why we use federation. Because web apps do not speak Kerberos or ntlm. They speak languages such oauth. Hence the need for ad federation proxy B is correct

**Question: 69** CertyIQ

You are running a cluster on 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 output. 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**

**Explanation:**

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

**Question: 70** CertyIQ

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**

**Explanation:**

D is the correct answer.

Cloud SQL is a regional resource.

Read Replica helps to reduce latency & improve performance.

Failover Replica is used for High Availability.

**Question: 71** CertyIQ

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**

**Explanation:**

The easiest way would be to create template from --source-instance, and then create MIG, but it is not listed here, also you cannot create a MIG from image directly, you need a template, so answer is C (image -> template -> mig).

**Question: 72** CertyIQ

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 app can autoscale. How should you restrict communications?

A. Use separate VPCs to restrict traffic

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

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**

**Explanation:**

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

**Question: 73** CertyIQ

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 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**

**Explanation:**

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.

**Question: 74** CertyIQ

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 Firestore, because it offers real-time synchronization across devices

D. BigQuery, because it is designed for large-scale processing of tabular data

**Answer: D**

**Explanation:**

The keyword in this context is OLAP. CloudSQL is Relational SQL for OLTP. Capacity wise, BQ supports for PB+ while CloudSQL only have max capacity of up to ~10TB. Again the questions specifically mention "hundreds of TB of data". So D is the answer.

Reference:

https://cloud.google.com/files/BigQueryTechnicalWP.pdf

**Question: 75** CertyIQ

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 GCP Console, navigate to Stackdriver Logging. Consult logs for (GKE) and Cloud SQL.

D. In the GCP Console, navigate to Cloud SQL. Restore the latest backup. Use kubectl to restart all pods.

**Answer: C**

**Explanation:**

post mortem always includes log analysis, answer is C

**Question: 76** CertyIQ

Your company pushes batches of sensitive transaction data from its application server VMs to Cloud Pub/Sub for processing and storage. What is the 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**

**Explanation:**

A. Ensure that VM service accounts are granted the appropriate Cloud Pub/Sub IAM roles.

**Question: 77** CertyIQ

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. Expose 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: D**

**Explanation:**

It can't be -A - VPC Network Peering only allows private RFC 1918 connectivity across two Virtual Private Cloud (VPC) networks. In this example is one VPC with on-premise network

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

It is not definitely - B - Can't be

It is not C - Because Cloud VPN gateways and tunnels are regional objects, not global

So, it the answer is D -

https://cloud.google.com/vpn/docs/how-to/creating-static-vpns

**Question: 78** CertyIQ

Your applications 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 tables 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**

**Explanation:**

B. Make the tables time-partitioned, and configure the partition expiration at 45 days

**Question: 79** CertyIQ

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**

**Explanation:**

A. Configure a HorizontalPodAutoscaler with a target CPU usage. Enable the Cluster Autoscaler from the GCP Console.

**Question: 80** CertyIQ

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**

**Explanation:**

B. Cloud VPN provides secure IPSec connection, though Direct Peering doesn't. Also, check selection diagram "What GCP connection is right for you?" on Hybrid Connectivity page. https://cloud.google.com/hybrid-connectivity/

It explicitly points that Cloud VPN and Dedicated Interconnect are for extension of you Data Center to Cloud (== of private compute resources). And Direct Peering for accessing GSuite (full set of GCP resources).

Direct Peering: https://cloud.google.com/network-connectivity/docs/direct-peering

Cloud VPN: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview

Choose Inteconnect Type: https://cloud.google.com/network-connectivity/docs/how-to/choose-product#cloud-interconnect only suggests Dedicted/Partner and Cloud VPN.

This Disaster Recovery scenario is described here, in section "Transferring data to and from GCP":

https://cloud.google.com/architecture/dr-scenarios-building-blocks#transferring_data_to_and_from

**Question: 81** CertyIQ

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**

**Explanation:**

Disabling and then discontinuing allows you to see the effects of not using the APIs, so you can gauge (check) alternatives. So that leaves B and D as viable answers. The question says only some are not time-critical which implies others are... this means preemptible VMs are good because they will secure a spot for scaling when needed. So I'm also going to choose B.

**Question: 82** CertyIQ

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 om 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**

**Explanation:**

As per google documentation(https://cloud.google.com/solutions/scalable-and-resilient-apps) answer is C.

C: A well-designed application should scale seamlessly as demand increases and decreases, and be resilient enough to withstand the loss of one or more compute resources.

Resilience: designed to withstand the unexpected

A highly-available, or resilient, application is one that continues to function despite expected or unexpected failures of components in the system. If a single instance fails or an entire zone experiences a problem, a resilient application remains fault tolerant — continuing to function and repairing itself automatically if necessary. Because stateful information isn't stored on any single instance, the loss of an instance — or even an entire zone — should not impact the application's performance.

**Question: 83** CertyIQ

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**

**Explanation:**

D. Use Cloud Audit Logging to view Cloud Audit Logs, and create a filter on the query operation to get the required information. https://cloud.google.com/bigquery/docs/reference/auditlogs#ids

**Question: 84** CertyIQ

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**

**Explanation:**

B- minimal start time means a pre-baked golden image

**Question: 85** CertyIQ

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**

**Explanation:**

Answer is A, https://cloud.google.com/bigquery/docs/dataset-access-controls

For a user to be able to query the tables in a dataset, it is not sufficient for the user to have access to the dataset. A user must also have permission to run a query job in a project. If you want to give a user permission to run a query from your project, give the user the bigquery.jobs.create permission for the project. You can do this by assigning the user the roles/bigquery.jobUser role for your project. For more information, see Access control example

**Question: 86** CertyIQ

You have been engaged by your client to lead the migration of their application infrastructure to GCP. One of their current problems is that the on-premises high performance SAN is requiring frequent and expensive upgrades to keep up with the variety of workloads that are identified as follows: 20 TB of log archives retained for legal reasons; 500 GB of VM boot/data volumes and templates; 500 GB of image thumbnails; 200 GB of customer session state data that allows customers to restart sessions even if off-line for several days.
Which of the following best reflects your recommendations for a cost-effective storage allocation?

A. Local SSD for customer session state data. Lifecycle-managed Cloud Storage for log archives, thumbnails, and VM boot/data volumes.

B. Memcache backed by Cloud Datastore for the customer session state data. Lifecycle-managed Cloud Storage for log archives, thumbnails, and VM boot/data volumes.

C. Memcache backed by Cloud SQL for customer session state data. Assorted local SSD-backed instances for VM boot/data volumes. Cloud Storage for log archives and thumbnails.

D. Memcache backed by Persistent Disk SSD storage for customer session state data. Assorted local SSD-backed instances for VM boot/data volumes. Cloud Storage for log archives and thumbnails.

**Answer: B**

**Explanation:**
1. There are two issues with this question: 1. Assuming that you only consider migration and not configuration then the answer is B. This is because the vm images will first be migrated to cloud storage only. VM images can be migrated to cloud storage first and then imported on to the compute engine and saved on persistent disks (https://cloud.google.com/compute/docs/import/import-existing-image). 2. D can only be correct if by "local SSD's for VM images" they mean persistent local SSD disks (https://cloud.google.com/compute/docs/disks/local-ssd) which may not be the case as the terminology is clear (?).In my opinion B is the better answer.
2. i think should be as local SSD not recommended for GCS VM boot volume

**Question: 87** CertyIQ

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: A**

**Explanation:**

StatefulSets is a feature of Kubernetes, which the question asks about. Yes, Persistent volumes are required by StatefulSets (https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/). See the Google documentations for mentioning of hostnames (https://cloud.google.com/kubernetes-engine/docs/concepts/statefulset)... Answer A

**Question: 88** CertyIQ

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 Cache-Region 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**

**Explanation:**

"A logo needs to be cached whether displayed through HTTP or HTTPS. When you customize the cache keys for the backend service that holds the logo, clear the Protocol checkbox so that requests through HTTP and HTTPS count as matches for the logo's cache entry."

Reference:

https://cloud.google.com/cdn/docs/best-practices#using_custom_cache_keys_to_improve_cache_hit_ratio

**Question: 89** CertyIQ

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**

**Explanation:**

B is correct answer The Logging agent streams logs from your VM instances and from selected third-party

software packages to Cloud Logging. It is a best practice to run the Logging agent on all your VM instances.

Reference:

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

**Question: 90** CertyIQ

You have an App Engine application that needs to be updated. You want to test the update with production traffic before replacing the current application version.
What should you do?

A. Deploy the update using the Instance Group Updater to create a partial rollout, which allows for canary testing.

B. Deploy the update as a new version in the App Engine application, and split traffic between the new and current versions.

C. Deploy the update in a new VPC, and use Google's global HTTP load balancing to split traffic between the update and current applications.

D. Deploy the update as a new App Engine application, and use Google's global HTTP load balancing to split traffic between the new and current applications.

**Answer: B**

**Explanation:**

B – Deploy the update as a new version in AppEngine app, and split traffic between the new and current versions.

Traffic Splitting is feature of AppEngine for A/B testing.

https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

**Question: 91** CertyIQ

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**

**Explanation:**

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.

**Question: 92** CertyIQ

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**

**Explanation:**

Model performance is generally based on the volume of its training data input. The more the data, the better the model.

**Question: 93** CertyIQ

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**

**Explanation:**

Ingress is preferred to LB

Ingress is a Kubernetes resource that encapsulates a collection of rules and configurations for routing external HTTP(S) traffic to internal services.On GKE, Ingress is implemented using Cloud Load Balancing. When you create an Ingress in your cluster, GKE creates an HTTP(S) load balancer and configures it to route traffic to your application."

**Question: 94** CertyIQ

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**

**Explanation:**

B. Create an HTTPS load balancer with URL maps.

Reference:

https://cloud.google.com/load-balancing/docs/https/url-map

**Question: 95** CertyIQ

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**

**Explanation:**

Answer is B

You should use exponential backoff to retry your requests when receiving errors with 5xx or 429 response codes from Cloud Storage.

Reference:

https://cloud.google.com/storage/docs/json_api/v1/status-codes

**Question: 96** CertyIQ

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**

**Explanation:**

Deployment Manager + Cloud Monitoring and Logging solution.

**Question: 97** CertyIQ

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**

**Explanation:**

https://cloud.google.com/storage/docs/locations A multi-region is a large geographic area, such as the United States, that contains two or more geographic places so correct answer is D

**Question: 98** CertyIQ

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**

**Explanation:**

Answer is C. Noteworthy if you are moving PHI from an on-prem source into cloud storage bucket, the object creation date recorded is the current date and not the original creation date as seen in on-prem source. To port original creation date you could script a function to write to the object metadata field called "Custom time" which is referenced in object lifecycle rules.

So to delete objects up to 4 years, you add an object lifecycle rule specifying the following form parameters:

Action = "Delete object"

Object conditions = select ""Days since custom time" checkbox and specify 1460 days.

**Question: 99** CertyIQ

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 cached_queries.

D. Set the memcache service level to shared. Create a key called cached_queries, and return database values from the key before using a query to Cloud SQL.

**Answer: A**

**Explanation:**

Dedicated and shared will resolve the problem, the key is: store all queries in only one key "cached_queries" is not good, we have limits: https://cloud.google.com/appengine/docs/standard/python/memcache

Create a key of each query is better.

**Question: 100** CertyIQ

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**

**Explanation:**

B Cloud Scheduler provides a fully managed, enterprise-grade service that lets you schedule events. After you have scheduled a job, Cloud Scheduler will call the configured event handlers, which can be App Engine services, HTTP endpoints, or Pub/Sub subscriptions.

**Question: 101** CertyIQ

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**

**Explanation:**

Agree B. 100Mbps connections for 10TB data transfer is takes too long

https://cloud.google.com/solutions/transferring-big-data-sets-to-gcp#close

**Question: 102** CertyIQ

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**

**Explanation:**

Dataflow deduplicates messages with respect to the Pub/Sub message ID

B is the answer.https://cloud.google.com/blog/products/data-analytics/handling-duplicate-data-in-streaming-pipeline-using-pubsub-dataflow

**Question: 103** CertyIQ

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**

**Explanation:**

The framework illustrated in the preceding diagram has four phases:

¢ Assess. In this phase, you assess your source environment, assess the workloads that you want to migrate to Google Cloud, and assess which VMs support each workload.

¢ Plan. In this phase, you create the basic infrastructure for Migrate for Compute Engine, such as provisioning the resource hierarchy and setting up network access.

¢ Deploy. In this phase, you migrate the VMs from the source environment to Compute Engine.

¢ Optimize. In this phase, you begin to take advantage of the cloud technologies and capabilities.

Reference:
https://cloud.google.com/architecture/migrating-vms-migrate-for-compute-engine-getting-started

**Question: 104** CertyIQ

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**

**Explanation:**

Since the Traffic is TCP, Ans A & C gets eliminated as HTTPS load balance is not supported.

B - File storage system is Cloud Firestore which do not give full control, hence eliminated.

D - Unmanaged instance group with network load balance with regional persistent disk for storage gives full control which is required for the migration.

Reference:

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

**Question: 105** CertyIQ

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**

**Explanation:**

D. Configure a Cloud Dedicated Interconnect connection between the on-premises environment and Google Cloud.Interconnect gives very high speed connection and low latency. It gives 10Gbps and 100 Gbps connection, which makes it very fast. In addition, Interconnect is an enterprise-grade connection to Google Cloud as per documentation. On the other hand, Cloud VPN is recommended for lower throughput solution, or if you are experimenting with migrating workloads to Google Cloud.

HIGH THROUGHPUT connection is needed--> Dedicated interconnect

**Question: 106** CertyIQ

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**

**Explanation:**

A. Deploy a new revision to Cloud Run with the new version. Configure traffic percentage between revisions.

Traffic managementCloud Run for Anthos can now route each request or RPC randomly between multiple revisions of a service with the traffic percentages you configure. You can use this feature to perform canary deployments of a newer version of your application, sending a small percentage of the traffic and validating if it is performing correctly, before gradually increasing the traffic.Similarly, these new traffic management capabilities make it possible to roll back to an older version of your application quickly. You can manage traffic to your service on the Cloud Console, as well as the gcloud command-line tool.

**Question: 107** CertyIQ

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**

**Explanation:**

Navigate the predefined dashboards in the Cloud Monitoring workspace, and then add metrics and create alert policies.

**Question: 108** CertyIQ

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**

**Explanation:**

Backups help you restore lost data to your Cloud SQL instance. Additionally, if an instance is having a problem, you can restore it to a previous state by using the backup to overwrite it. Enable automated backups for any instance that contains necessary data. Backups protect your data from loss or damage.
Enabling automated backups, along with binary logging, is also required for some operations, such as clone and replica creation.

Reference:
https://cloud.google.com/sql/docs/mysql/backup-recovery/backups

**Question: 109** CertyIQ

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**

**Explanation:**

Answer is (A), (B) is only masking the data without any deletion, and no need for that. Think it in KISS principle, don't overwhelm simple things.

A is the answer.B and C does not delete data which is wrong.

**Question: 110** CertyIQ

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**

**Explanation:**

A. App Engine

I chose A due to the following statement - You want to minimize the operational overhead of the solution

**Question: 111** CertyIQ

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**

**Explanation:**

B is the answer.

https://cloud.google.com/blog/products/it-ops/best-practices-for-optimizing-your-cloud-costs

Schedule VMs to auto start and stop: The benefit of a platform like Compute Engine is that you only pay for the compute resources that you use. Production systems tend to run 24/7; however, VMs in development, test or personal environments tend to only be used during business hours, and turning them off can save you a lot of money!

https://cloud.google.com/blog/products/storage-data-transfer/save-money-by-stopping-and-starting-compute-engine-instances-on-schedule

Cloud Scheduler, GCP's fully managed cron job scheduler, provides a straightforward solution for automatically stopping and starting VMs. By employing Cloud Scheduler with Cloud Pub/Sub to trigger Cloud Functions on schedule, you can stop and start groups of VMs identified with labels of your choice (created in Compute Engine). Here you can see an example schedule that stops all VMs labeled "dev" at 5pm and restarts them at 9am, while leaving VMs labeled "prod" untouched

Reference:

https://cloud.google.com/blog/products/it-ops/best-practices-for-optimizing-your-cloud-costs

**Question: 112** CertyIQ

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**

**Explanation:**

1. C because it has minimal modification to the application or database. Also it's easier to fail back to the original solution if the cloud implementation has issues (assuming that there will be a "post-go-live" monitoring period).

2. Answer is C - Very low downtime. And correct sequence of steps.

**Question: 113** CertyIQ

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**

**Explanation:**

D. Set an Organization Policy with a constraint on constraints/compute.vmExternalIpAccess. List the approved instances in the allowedValues list.

Reference:

https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

**Question: 114** CertyIQ

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**

**Explanation:**

when you create a firewall rule there is an option for firewall rule logging on/off. It is set to off by default.

To get firewall insights or view the logs for a specific firewall rule you need to enable logging while creating the rule or you can enable it by editing that rule.

Reference:

https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/using-firewall-insights

**Question: 115** CertyIQ

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**

**Explanation:**

A. Best optionB. Not all instances need this restrictionC. You are not restricting remote access. The users can still access remotely using their credentials during the business day. The ask is to restrict data retrieval from outside the office network (what if they are working from home...?)D. VPN - too much overhead

**Question: 116** CertyIQ

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**

**Explanation:**

D - By definition the MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created.

**Question: 117** CertyIQ

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**

**Explanation:**

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.

Answer is B

**Question: 118** CertyIQ

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**

**Explanation:**

- IP Should not overlap so applying new IP address is the solution

**Question: 119** CertyIQ

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**

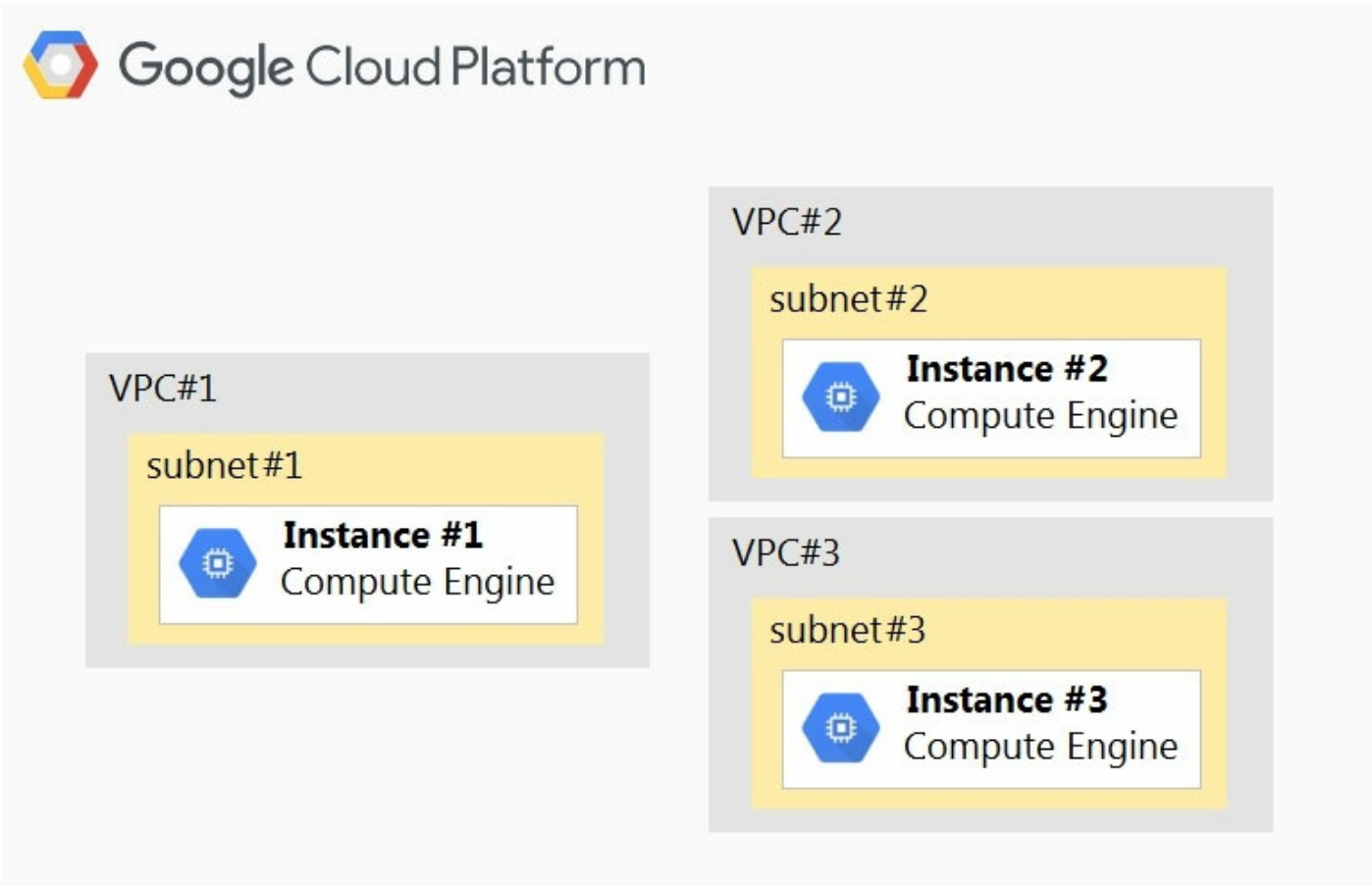
**Explanation:**

B, you want to minimize costs.

https://cloud.google.com/dataproc/docs/concepts/compute/secondary-vms#preemptible_and_non-preemptible_secondary_workers

**Question: 120** CertyIQ

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.




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 ג€‹ VPC: VPC #2 ג€‹ SUBNETWORK: subnet #2 ¢ NIC2 ג€‹ VPC: VPC #3 ג€‹ SUBNETWORK: subnet #3 Update firewall rules to enable traffic between instances.

C. Create two VPN tunnels via CloudVPN: ¢ 1 between VPC #1 and VPC #2. ¢ 1 between VPC #2 and VPC #3. Update firewall rules to enable traffic between the instances.

D. Peer all three VPCs: ¢ Peer VPC #1 with VPC #2. ¢ Peer VPC #2 with VPC #3. Update firewall rules to enable traffic between the instances.

**Answer: B**

**Explanation:**

Add two additional NICs to Instance #1 with the following configuration: ¢ NIC1 ג€‹ VPC: VPC #2 ג€‹ SUBNETWORK: subnet #2 ¢ NIC2 ג€‹ VPC: VPC #3 ג€‹ SUBNETWORK: subnet #3 Update firewall rules to enable traffic between instances.

**Question: 121** CertyIQ

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**

**Explanation:**

B. Create a Debian-based Compute Engine instance, install and configure the application, and use OS patch management to install available updates.

Reference:

https://cloud.google.com/compute/docs/os-patch-management

**Question: 122** CertyIQ

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**

**Explanation:**

A - this is a simple question, no need for Prometheus and no need to build another cluster....!

Use Promethues only in case of multi cloud solution hence AGoogle Cloud Managed Service for Prometheus is Google Cloud's fully managed multi-cloud solution for Prometheus metrics. It lets you globally monitor and alert on your workloads, using Prometheus, without having to manually manage and operate Prometheus at scale.

**Question: 123** CertyIQ

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**

**Explanation:**

C. Create a Cloud Filestore instance and mount it in each instance.

FUSE can be used, but it comes with latency. Question states, huge workload like 100 MB/sec writes, then FUSE is not a god choice. Filestore is much better solution.

**Question: 124** CertyIQ

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**

**Explanation:**

Anthos Service Mesh's robust tracing, monitoring, and logging features give you deep insights into how your services are performing, how that performance affects other processes, and any issues that might exist.

**Question: 125** CertyIQ

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**

**Explanation:**

o If a bucket has a retention policy, objects in the bucket can only be deleted or replaced once their age is greater than the retention period.

o Once you lock a retention policy, you cannot remove it or reduce the retention period it has.

Reference:

https://cloud.google.com/storage/docs/using-bucket-lock

**Question: 126** CertyIQ

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**

**Explanation:**

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

**Question: 127** CertyIQ

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**

**Explanation:**

It all depends on how you want to troubleshoot the issue. Do you want to check the application before or after increasing the max number of instances in the scaling group. I guess in real life people will ask for an increase in the max number of instances and if the application process continues to consume all the CPU then they will probably stop/restart the app. D is the only sensible option.A is not an optionB you could restart but you dont know if that will fix the issueC SSH assumes unix vm's (?)....!

I feel increasing the autoscale limit seems to be the logical answer

**Question: 128** CertyIQ

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**

**Explanation:**

EVen though there is a max concurrency of 1000, there is no upper limit to the number of containers (unless we specify). So, CloudRun will spawn as many containers as needed to run the number of requests and take care of all the requests.

Let me know if you have different interpretation of this link> https://cloud.google.com/run/docs/about-instance-autoscaling

**Question: 129** CertyIQ

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**

**Explanation:**

1. Based on the description "You want to be able to configure each microservice with a specific number of replicas.", It's a hint to use either Deployment or StatefulSet based on the service type is stateless or stateful, since the option only has Deployment, thus Option C and D is out.

2. Based on the description "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." the later part is the key point, which means the traffic direct to each service is based on some certain rules, in K8S this means URL, which is Ingress with external HTTP LB.

**Question: 130** CertyIQ

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: B**

**Explanation:**

The key words in the statement are actually "Create a second project without a VPC, configure it as a Shared VPC service project." Since the VPC being used doesn't exist in their project, they're unable to manage network changes.

1) With Shared VPC, network operations and resources are isolated in the host project and network team can be given admin access over the resources in host project

2) The dev team will have admin rights over the compute resources in the Services Project

One of the ask in the question is that - "The development team does not want the networking team to have access to the sensitive data on the instances". This can be possible only if both the network and compute resources are isolated.

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

https://cloud.google.com/vpc/docs/shared-vpc

**Question: 131** CertyIQ

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**

**Explanation:**

D for the simple reason that there is low traffic with occasional spikes. Also, Cloud CDN usually caches static content not store (wording). In addition, you can use LB's with Storage buckets. No need for multizones and expensive spanner. Therefore the only remaining option is D.

**Question: 132** CertyIQ

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**

**Explanation:**

https://cloud.google.com/blog/products/management-tools/automate-your-response-to-a-cloud-logging-event

**Question: 133** CertyIQ

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**

**Explanation:**

C --> https://cloud.google.com/solutions/connecting-securely#cloud_iap

It says "No instances can have public IP" not just the the instance we are trying to SSH. So D cannot be the answer as Bastion Host, has a public IP.C is the only available option as we need to connect specifically to an instance.

**Question: 134** CertyIQ

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**

**Explanation:**

Reference:
https://cloud.google.com/resource-manager/docs/creating-managing-folders

**Question: 135** CertyIQ

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**

**Explanation:**

B is the answer

https://istio.io/latest/docs/tasks/traffic-management/fault-injection/

**Question: 136** CertyIQ

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**

**Explanation:**

A, App Engine, you just want you people dedicated to the App

Reference:

https://cloud.google.com/terms/services

**Question: 137** CertyIQ

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 DEPRECATED to the current API version number on every backward-incompatible change. Use the current version number for the new API.

**Answer: C**

**Explanation:**

All Google API interfaces must provide a major version number, which is encoded at the end of the protobuf package, and included as the first part of the URI path for REST APIs. If an API introduces a breaking change, such as removing or renaming a field, it must increment its API version number to ensure that existing user code does not suddenly break.

**Question: 138** CertyIQ

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**

**Explanation:**

C to decouple infrastructure from application, the development team want a fully managed service approach

**Question: 139** CertyIQ

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**

**Explanation:**

1. A is the correct, no load ==> no latency checking

2. The question focuses more on the current infra and ensuring if the current setup will ensure a latency target. An only a load test can do that. Autoscaling is no need of the hour and may require in the future and that totally depends on the test results. It might be an overkill to have everything in advance even App is fine with current configs. Hence A.

**Question: 140** CertyIQ

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**

**Explanation:**

Direct answer - Dhttps://cloud.google.com/kubernetes-engine/docs/samples/container-pubsub-horizontal-pod-autoscalerapiVersion: autoscaling/v2beta2kind: HorizontalPodAutoscalermetadata: name: pubsubspec: minReplicas: 1 maxReplicas: 5 metrics: - external: metric: name: pubsub.googleapis.com|subscription|num_undelivered_messages selector: matchLabels: resource.labels.subscription_id: echo-read target: type: AverageValue averageValue: 2 type: External scaleTargetRef: apiVersion: apps/v1 kind: Deployment name: pubsubThis seems relevant https://cloud.google.com/kubernetes-engine/docs/tutorials/autoscaling-metrics#pubsubeven if it uses Deployment + HorizontalPodAutoscaler which is not mentioned in the context of the question/answer

**Question: 141** CertyIQ

Your company is developing a web-based application. You need to make sure that production deployments are linked to source code commits and are fully auditable. What should you do?

A. Make sure a developer is tagging the code commit with the date and time of commit.

B. Make sure a developer is adding a comment to the commit that links to the deployment.

C. Make the container tag match the source code commit hash.

D. Make sure the developer is tagging the commits with latest.

**Answer: C**

**Explanation:**

C is correct "By design, the Git commit hash is immutable and references a specific version of your software." as per https://cloud.google.com/architecture/best-practices-for-building-containers#tagging_using_the_git_commit_hash

C is the answer.https://cloud.google.com/architecture/best-practices-for-building-containers#tagging_using_the_git_commit_hashYou can use this commit hash as a version number for your software, but also as a tag for the Docker image built from this specific version of your software. Doing so makes Docker images traceable: because in this case the image tag is immutable, you instantly know which specific version of your software is running inside a given container.

**Question: 142** CertyIQ

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**

**Explanation:**

AppEngine Standard supports Go language now. Fully-managed service - So no operational overhead and pay-only-for-what-you-use model.

**Question: 143** CertyIQ

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**

**Explanation:**

The data needs to be stored as it is retrieved. This would mean that any processing should be done after it is stored.

**Question: 144** CertyIQ

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**

**Explanation:**

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.

**Question: 145** CertyIQ

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**

**Explanation:**

C. Configure binary authorization policies for the development, staging, and production clusters. Create attestations as part of the continuous integration pipeline.

**Question: 146** CertyIQ

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**

**Explanation:**

Use the Data Transfer appliance to perform an offline migration.

**Question: 147** CertyIQ

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**

**Explanation:**

C is the right answer

You want to maximize performance while minimizing downtime and data loss

**Question: 148** CertyIQ

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**

**Explanation:**

For those that saying BigQuery does not support CSEK, read the below. You will need to import you CSEK and it will become CMEK. From there you can use it for BigQuery

https://cloud.google.com/bigquery/docs/customer-managed-encryption

**Question: 149** CertyIQ

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**

**Explanation:**

As per question: " your company must be able to rotate the encryption key"It is easily possible with KMS: https://cloud.google.com/kms/docs/rotating-keys#kms-create-key-rotation-schedule-gcloud

For security reasons you want to create the key in GCP [KMS] then set the encryption at the bucket as the data is inside the bucket.

**Question: 150** CertyIQ

Your team needs to create a Google Kubernetes Engine (GKE) cluster to host a newly built application that requires access to third-party services on the internet.
Your company does not allow any Compute Engine instance to have a public IP address on Google Cloud. You need to create a deployment strategy that adheres to these guidelines. What should you do?

A. Configure the GKE cluster as a private cluster, and configure Cloud NAT Gateway for the cluster subnet.

B. Configure the GKE cluster as a private cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

C. Configure the GKE cluster as a route-based cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

D. Create a Compute Engine instance, and install a NAT Proxy on the instance. Configure all workloads on GKE to pass through this proxy to access third-party services on the Internet.

**Answer: A**

**Explanation:**

A is the correct answer as per this https://cloud.google.com/nat/docs/overview

Cloud NAT is the correct

**Question: 151** CertyIQ

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**

**Explanation:**

D is the correct answer https://cloud.google.com/vpc/docs/serverless-vpc-access#use_cases

D is the answer.https://cloud.google.com/vpc/docs/serverless-vpc-accessServerless VPC Access makes it possible for you to connect directly to your Virtual Private Cloud network from serverless environments such as Cloud Run, App Engine, or Cloud Functions.

**Question: 152** CertyIQ

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**

**Explanation:**

Calculate hashes on local files, which can be used to compare with gsutil ls -L output. If a specific hash option is not provided, this command calculates all gsutil-supported hashes for the files.Note that gsutil automatically performs hash validation when uploading or downloading files, so this command is only needed if you want to write a script that separately checks the hash.If you calculate a CRC32c hash for files without a precompiled crcmod installation, hashing will be very slow. See gsutil help crcmod for details.https://cloud.google.com/storage/docs/gsutil/commands/hash

D is the right answer per this doc https://cloud.google.com/storage/docs/gsutil/commands/hash

**Question: 153** CertyIQ

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**

**Explanation:**

Reference:
https://cloud.google.com/anthos/docs/tutorials/manage-slos

**Question: 154** CertyIQ

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**

**Explanation:**

C is correct, however, this question is an old question and need to be updated to use the ingress for global HTTPS LB

C is the correct answer based on https://cloud.google.com/blog/products/gcp/how-to-deploy-geographically-distributed-services-on-kubernetes-engine-with-kubemci

**Question: 155** CertyIQ

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**

**Explanation:**

I agree with D is the most accurate

A, application may not support horizontal scaling and may not run in instances whith small cpuB, dockerize third-party applications is not a requirement....Complex and costlyC, too expensiveD, simple and works

**Question: 156** CertyIQ

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**

**Explanation:**

C is the right answer

Going by definition- VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google Cloud services such as Cloud Storage and BigQuery. hence C is correct

**Question: 157** CertyIQ

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**

**Explanation:**

Y'all not reading the fine details. The question is about aligning EACH client to their dedicated nodes (D), not to a node group (C).

https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes#default_affinity_labels

The above reference clearly articulates the default affinity label for node group and node name. Unless we're thinking about growing each client to their own dedicated node groups (not in the current requirement), then the answer is not C, rather D.

Compute Engine assigns two default affinity labels to each node:

A label for the node group name:

Key: compute.googleapis.com/node-group-name

Value: Name of the node group.

A label for the node name:

Key: compute.googleapis.com/node-name

Value: Name of the individual node.

https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes#default_affinity_labels

**Question: 158** CertyIQ

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**

**Explanation:**
Google Compute Engine enables users to launch virtual machines (VMs) on demand. VMs can be launched from the standard images or custom images created by users.
Managed instance groups offer autoscaling capabilities that allow you to automatically add or remove instances from a managed instance group based on increases or decreases in load. Autoscaling helps your applications gracefully handle increases in traffic and reduces cost when the need for resources is lower.
Incorrect Answers:
B: There is no mention of incoming IP data traffic for the custom C++ applications.
C: Apache Hadoop is not fit for testing C++ applications. Apache Hadoop is an open-source software framework used for distributed storage and processing of datasets of big data using the MapReduce programming model.
D: Google App Engine is intended to be used for web applications.
Google App Engine (often referred to as GAE or simply App Engine) is a web framework and cloud computing platform for developing and hosting web applications in Google-managed data centers.

Reference:
https://cloud.google.com/compute/docs/autoscaler/

**Question: 159** CertyIQ

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

A. Help the engineer to convert his websocket code to use HTTP streaming

B. Review the encryption requirements for websocket connections with the security team

C. Meet with the cloud operations team and the engineer to discuss load balancer options

D. Help the engineer redesign the application to use a distributed user session service that does not rely on websockets and HTTP sessions.

**Answer: C**

**Explanation:**
Google Cloud Platform (GCP) HTTP(S) load balancing provides global load balancing for HTTP(S) requests destined for your instances.
The HTTP(S) load balancer has native support for the WebSocket protocol.
Incorrect Answers:
A: HTTP server push, also known as HTTP streaming, is a client-server communication pattern that sends information from an HTTP server to a client asynchronously, without a client request. A server push architecture is especially effective for highly interactive web or mobile applications, where one or more clients need to receive continuous information from the server.

Reference:
https://cloud.google.com/compute/docs/load-balancing/http/

**Question: 160** CertyIQ

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. ¢ Append metadata to file body ¢ Compress individual files ¢ Name files with serverName " Timestamp ¢ 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. ¢ Batch every 10,000 events with a single manifest file for metadata ¢ Compress event files and manifest file into a single archive file ¢ Name files using serverName " EventSequence ¢ 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. ¢ Compress individual files ¢ Name files with serverName " EventSequence ¢ Save files to one bucket ¢ Set custom metadata headers for each object after saving

D. ¢ Append metadata to file body ¢ Compress individual files ¢ Name files with a random prefix pattern ¢ Save files to one bucket

**Answer: D**

**Explanation:**

answer is D

https://cloud.google.com/storage/docs/request-rate#naming-convention

"A longer randomized prefix provides more effective auto-scaling when ramping to very high read and write

rates. For example, a 1-character prefix using a random hex value provides effective auto-scaling from the initial 5000/1000 reads/writes per second up to roughly 80000/16000 reads/writes per second, because the prefix has 16 potential values. If your use case does not need higher rates than this, a 1-character randomized prefix is just as effective at ramping up request rates as a 2-character or longer randomized prefix."

Example:

my-bucket/2fa764-2016-05-10-12-00-00/file1

my-bucket/5ca42c-2016-05-10-12-00-00/file2

my-bucket/6e9b84-2016-05-10-12-00-01/file3

**Question: 161** CertyIQ

A recent audit revealed that a new network was created in your GCP 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**

**Explanation:**
Incorrect Answers:
A: To use the Stackdriver alerting console we must first set up alerting policies.
B: Data access logs only contain read-only operations.
Audit logs help you determine who did what, where, and when.
Cloud Audit Logging returns two types of logs:
✑ Admin activity logs
✑ Data access logs: Contains log entries for operations that perform read-only operations do not modify any data, such as get, list, and aggregated list methods.

**Question: 162** CertyIQ

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

A. Use the Linux dd and netcat commands to copy and stream the root disk contents to a new virtual machine instance in the US-East region.

B. Create a snapshot of the root disk and select the snapshot as the root disk when you create a new virtual machine instance in the US-East region.

C. Create an image file from the root disk with Linux dd command, create a new virtual machine instance in the US-East region

D. Create a snapshot of the root disk, create an image file in Google Cloud Storage from the snapshot, and create a new virtual machine instance in the US-East region using the image file the root disk.

**Answer: D**

**Explanation:**

D is correct. A and B are talking about appending the file system to a new VM, not setting it at the root in a new VM set. Option C is not offered within the GCP because the image must be on the GCP platform to run the gcloud of Google Console instructions to create a VM with the image.

**Question: 163** CertyIQ

Your company runs several databases on a single MySQL instance. They need to take backups of a 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 volume as the backup location. After the backup is complete, use gsutil to move the backup to Google Cloud Storage.

C. Use gcsfise 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 virtual machine (VM) instance in a RAID10 array and use LVM to create snapshots to send to Cloud Storage

**Answer: B**

**Explanation:**

Ans: B

Persistent Disk snapshot not required: "They need to take backups of a specific database at regular intervals."

"The backup activity needs to complete as quickly as possible and cannot be allowed to impact disk performance."

This can be achieved by using both Local SSD & GCS Fuse (mounting GCS as directory), but as the question stats needs to complete as quickly as possible.

General Rule: Any addition of components introduce a latency. I could not get write throughput of GCS & Local SSD, even if we consider both provides same throughput, streaming data through network to GCS Bucket introduce latency. Attached Local SSD has advantage in this case, since there is no network involved.

From Local SSD to GCS bucket - copy job does not impact the mysql data disk.

**Question: 164** CertyIQ

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 three.)

A. Ensure that the load tests 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**

**Explanation:**

A:Run your typical workloads against Bigtable :Always run your own typical workloads against a Bigtable cluster when doing capacity planning, so you can figure out the best resource allocation for your applications.

B. Create a separate Google Cloud project to use for the load-testing environment

F : The most important/standard factor of testing, you gather logs and metrics in TEST environment for further scaling.

**Question: 165** CertyIQ

Your customer is moving their corporate applications to Google Cloud Platform. 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**

**Explanation:**

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

B is correct because:-Org viewer grants the security team permissions to view the organization's display name.

-Project viewer grants the security team permissions to see the resources within projects.

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

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

**Question: 166** CertyIQ

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 two.)

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**

**Explanation:**

B&E

Code signing only verifies the author. In other words it only check who you are, but not what have you done

**Question: 167** CertyIQ

You want to enable your running Google Kubernetes Engine cluster to scale as demand for your application changes.
What should you do?

A. Add additional nodes to your Kubernetes 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 Kubernetes Engine cluster with the following command: gcloud alpha container clusters update mycluster - -enable- autoscaling - -min-nodes=1 - -max-nodes=10

D. Create a new Kubernetes 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**

**Explanation:**

C - cluster is already running so use update instead of create new cluster.

**Question: 168** CertyIQ

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 500,000 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? (Choose two.)

A. Use Google App Engine to serve the website and Google Cloud Datastore to store user data.

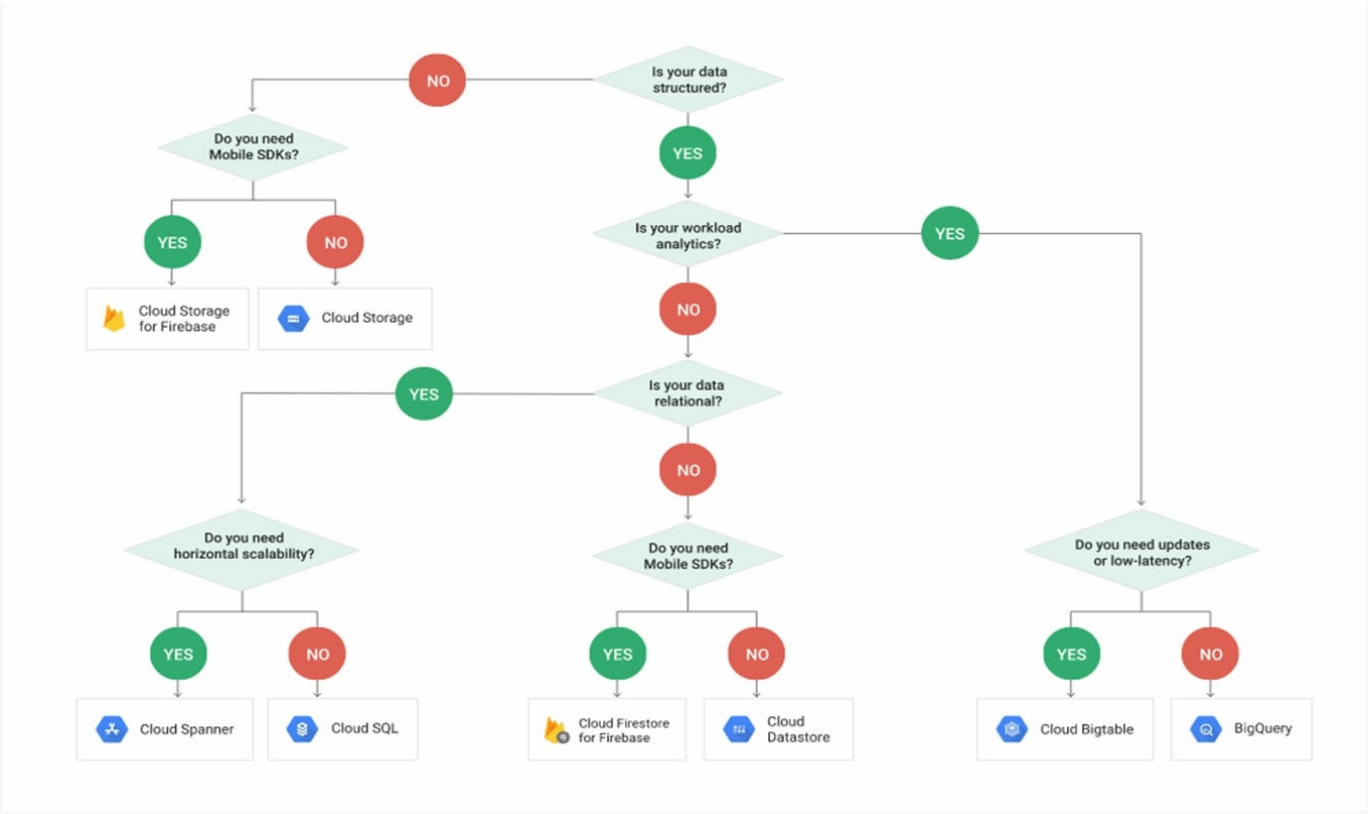
B. Use a Google Container Engine cluster to serve the website and store data to persistent disk.

C. Use a managed instance group to serve the website and Google Cloud Bigtable to store user data.

D. Use a single Compute Engine virtual machine (VM) to host a web server, backend by Google Cloud SQL.

**Answer: AC**

**Explanation:**




Reference:
https://cloud.google.com/storage-options/

**Question: 169** CertyIQ

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 two.)

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**

**Explanation:**
B: With Container Engine, Google will automatically deploy your cluster for you, update, patch, secure the nodes.
Kubernetes Engine's cluster autoscaler automatically resizes clusters based on the demands of the workloads you want to run.
C: Solutions like Datastore, BigQuery, AppEngine, etc are truly NoOps.
App Engine by default scales the number of instances running up and down to match the load, thus providing consistent performance for your app at all times while minimizing idle instances and thus reducing cost.
Note: At a high level, NoOps means that there is no infrastructure to build out and manage during usage of the platform. Typically, the compromise you make with
NoOps is that you lose control of the underlying infrastructure.

Reference:

https://www.quora.com/How-well-does-Google-Container-Engine-support-Google-Cloud-Platform%E2%80%99s-NoOps-claim

**Question: 170** CertyIQ

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**

**Explanation:**

Correct answer is C (verified from Question Bank in Whizlabs.com)

C (Correct answer) - Digitally sign each timestamp and log entry and store the signature.

Answer A, B, and D don't have any added value to verify the authenticity of your logs. Besides, Logs are mostly suitable for exporting to Cloud storage, BigQuery, and PubSub. SQL database is not the best way to be exported to nor store log data.

Simplified Explanation

To verify the authenticity of your logs if they are tampered with or forged, you can use a certain algorithm to generate digest by hashing each timestamp or log entry and then digitally sign the digest with a private key to generate a signature. Anybody with your public key can verify that signature to confirm that it was made with your private key and they can tell if the timestamp or log entry was modified. You can put the signature files into a folder separate from the log files. This separation enables you to enforce granular security policies.

**Question: 171** CertyIQ

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**

**Explanation:**

C, because managing multiple organizations is not a Google best practice

**Question: 172** CertyIQ

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**

**Explanation:**

Do not trust the official answers here, D is correct. In special for this question, never use gcsfuse in production. Performance is bad and reliability is trashy - Google states it themselves.

A is wrong because you can't be serving files directly from Compute Engine instance.GCS + CDN is best option

**Question: 173** CertyIQ

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.

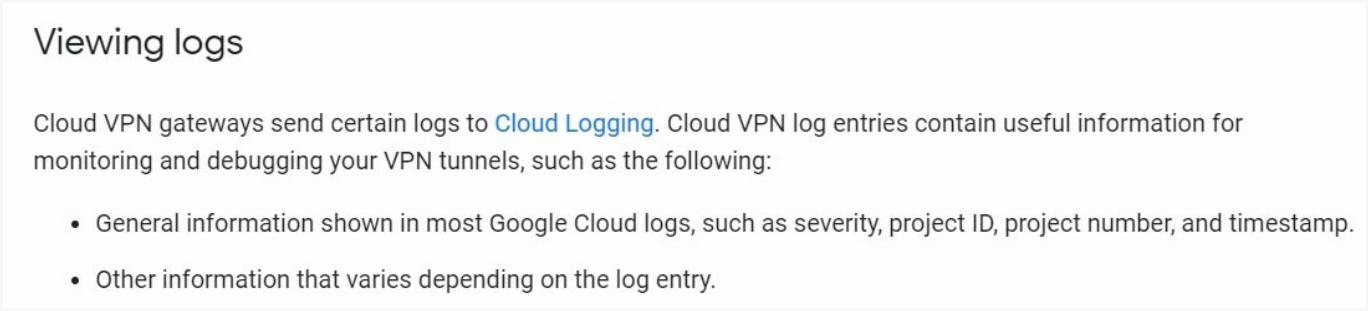
C. Set up a Cloud Logging Dashboard titled Cloud VPN Logs, and then add a chart that queries for the VPN metrics over a one-year time period.

D. Set up a filter in Cloud Logging and a topic in Pub/Sub to publish the logs.

**Answer: A**

**Explanation:**

Reference:
https://cloud.google.com/network-connectivity/docs/vpn/how-to/viewing-logs-metrics
" target="_blank" style="word-break: break-all;">



Viewing logs

Cloud VPN gateways send certain logs to Cloud Logging. Cloud VPN log entries contain useful information for monitoring and debugging your VPN tunnels, such as the following:

- General information shown in most Google Cloud logs, such as severity, project ID, project number, and timestamp.
- Other information that varies depending on the log entry.

**Question: 174** CertyIQ

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**

**Explanation:**

The correct answer is A.

Option C seems to be an option, but there are two non-conformities there. In addition to storing personal data in the GCS, it is being improperly retained.

**Question: 175** CertyIQ

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**

**Explanation:**

A is more likely, because clearly it's stated in the question that they are interested in "Production" folder/projects logging, not the entire organization.

**Question: 176** CertyIQ

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**

**Explanation:**

The answer is A.

The practice for managing logs generated on Compute Engine on Google Cloud is to install the Cloud Logging agent and send them to Cloud Logging.

The sent logs will be aggregated into a Cloud Logging sink and exported to Cloud Storage.

The reason for using Cloud Storage as the destination for the logs is that the requirement in question requires setting up a lifecycle based on the storage period.

In this case, the log will be used for active queries for 30 days after it is saved, but after that, it needs to be stored for a longer period of time for auditing purposes.

If the data is to be used for active queries, we can use BigQuery's Cloud Storage data query feature and move the data past 30 days to Coldline to build a cost-optimal solution.

Therefore, the correct answer is as follows

1. Install the Cloud Logging agent on all instances.

Create a sync that exports the logs to the region's Cloud Storage bucket.

3. Create an Object Lifecycle rule to move the files to the Coldline Cloud Storage bucket after one month. 4.

4. set up a bucket-level retention policy using bucket locking."

**Question: 177** CertyIQ

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., [email protected]), and give it the project owner role at root organization level. Write a bash script that: ¢ Lists all the IAM rules of all projects within the organization. ¢ 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**

**Explanation:**

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

A is the correct answerhttps://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

**Question: 178** CertyIQ

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**

**Explanation:**

https://cloud.google.com/bigtable/docs/schema-design#row-keys

**Question: 179** CertyIQ

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**

**Explanation:**

Reference:
https://cloud.google.com/blog/topics/developers-practitioners/bigquery-admin-reference-guide-data-governance?skip_cache=true
" target="_blank" style="word-break: break-all;">

With metadata for the production table in place, we need to focus on how to push data into this new table. As you probably know, there are lots of different ways to pre-process and ingest data into BigQuery. Often customers choose to stage data in Google Cloud Services to kick off transformation, classification or de-identification workflows. There are two pretty common paths for staging data for batch loading:

1. **Stage data in a Google Cloud storage bucket**: Pushing data into a Google Cloud storage bucket before directly ingesting it into BigQuery offers **flexibility in terms of data structure and may be less expensive** for storing large amounts of information. Additionally, you can easily kick off workflows when new data lands in a bucket by using PubSub to trigger transformation jobs. However, since transformations will happen outside of the BigQuery service, data engineers will need familiarity with other tools or languages. Blob storage also makes it difficult to track column-level metadata.

**Question: 180** CertyIQ

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.

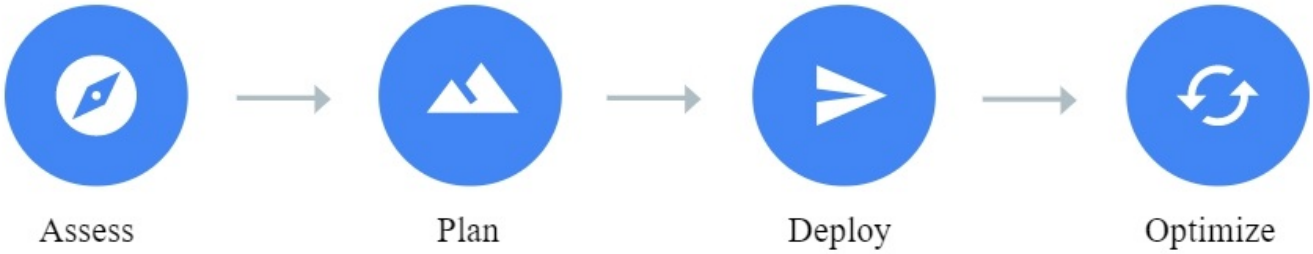
D. Download the data to the on-premises data center, and upload it to the Cloud Storage bucket.

**Answer: B**

**Explanation:**

Reference:
https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets
" target="_blank" style="word-break: break-all;">

The following diagram illustrates the path of your migration journey.




**Question: 181** CertyIQ

You have a Compute Engine managed instance group that adds and removes Compute Engine instances from the group in response to the load on your application. The instances have a shutdown script that removes REDIS database entries associated with the instance. You see that many database entries have not been removed, and you suspect that the shutdown script is the problem. You need to ensure that the commands in the shutdown script are run reliably every time an instance is shut down. You create a Cloud Function to remove the database entries. What should you do next?

A. Modify the shutdown script to wait for 30 seconds before triggering the Cloud Function.

B. Do not use the Cloud Function. Modify the shutdown script to restart if it has not completed in 30 seconds.

C. Set up a Cloud Monitoring sink that triggers the Cloud Function after an instance removal log message arrives in Cloud Logging.

D. Modify the shutdown script to wait for 30 seconds and then publish a message to a Pub/Sub queue.

**Answer: C**

**Explanation:**

C is the answer as shutdown script is run based on best effort and not a reliable method.

https://cloud.google.com/compute/docs/shutdownscript#limitations

Compute Engine executes shutdown scripts only on a best-effort basis. In rare cases, Compute Engine cannot guarantee that the shutdown script will complete.

**Question: 182** CertyIQ

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**

**Explanation:**

Reference:
https://cloud.google.com/sdk/gcloud

**Question: 183** CertyIQ

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**

**Explanation:**

VPC peering cannot be established between VPCs if there is IP range overlap. C is ok since you can establish VPN across these VPCs and only include the applications required IP ranges as its mentioned that they do not overlap

**Question: 184** CertyIQ

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**

**Explanation:**

First thing to do is to inspect logs and monitoring to see what is happening

Agree with A.First remove any non possible answers: B / C.Then we have A or D left. But D does a good action / recommended action but it says "what do we do first" which is always troubleshoot.

**Question: 185** CertyIQ

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**

**Explanation:**

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.

A is the answer.Kubernetes Health Checks with Readiness and Liveness Probeshttps://www.youtube.com/watch?v=mxEvAPQRwhw

**Question: 186** CertyIQ

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**

**Explanation:**

A: Is not necessary because you can have multiple node pools with different configurations.B: Optimizes resource usage of CPU/memory in your existing node pool but does not necessarily improve cost - still an option that should be considered.C: This looks really good. Autoscaling workloads and the node pools makes your whole infrastructure more elastic and gives you the option to rely on the same node pool.D: This might not be a good option for every type of workload. Batch and stateless workloads can often handle this quite well, but stateful workloads are not well-suited for operation on preemptible VMs.Since only one answer is accepted, I'll choose C.

C is the correct answer as it doesn't involve major changes to the current Kubernetes configuration

**Question: 187** CertyIQ

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**

**Explanation:**

B is the correct answer https://cloud.google.com/blog/products/data-analytics/taking-a-practical-approach-to-bigquery-cost-monitoringA is incorrect as there is not billing page for a project, its billing account that handles all org billing.

B is my answer.https://cloud.google.com/blog/products/data-analytics/taking-a-practical-approach-to-bigquery-cost-monitoring

**Question: 188** CertyIQ

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**

**Explanation:**

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

Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.

**Question: 189** CertyIQ

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**

**Explanation:**

Reference:
https://cloud.google.com/storage/docs/object-versioning

**Question: 190** CertyIQ

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: A**

**Explanation:**

TARGET_TYPE: the value type for the metric.

gauge: the autoscaler computes the average value of the data collected in the last couple of minutes and compares that to the utilization target.

delta-per-minute: the autoscaler calculates the average rate of growth per minute and compares that to the utilization target.

delta-per-second: the autoscaler calculates the average rate of growth per second and compares that to the utilization target. For accurate comparisons, if you set the utilization target in seconds, use delta-per-second as the target type. Likewise, use delta-per-minute for a utilization target in minutes.

**Question: 191** CertyIQ

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**

**Explanation:**

A is true only if the on-prem (peer) gateway has two separate external P addresses. The HA VPN gateway uses two tunnels, one tunnel to each external IP address on the peer device as described in https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies#configurations_that_support_9999_availability

C is a complete solution that provides full redundancy of the on-prem gateway. This is probably more expensive and having two HA VPN Gateways is an unusual configuration as the online documentation only describes using one HA VPN Gateway

A appears to be correct with assumptions...!

**Question: 192** CertyIQ

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**

**Explanation:**

"Cloud Storage supports this specification by allowing you to configure your buckets to support CORS. Continuing the above example, you can configure the example.storage.googleapis.com bucket so that a browser can share its resources with scripts from example.appspot.com."

Reference:

https://cloud.google.com/storage/docs/cross-origin#server-side-support

**Question: 193** CertyIQ

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**

**Explanation:**

Cloud NAT allows the resources in a private subnet to access the internet — for updates, patching, config management, and more — in a controlled and efficient manner.

**Question: 194** CertyIQ

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**

**Explanation:**

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.

Reference:

https://cloud.google.com/compute/docs/import/importing-virtual-disks

**Question: 195** CertyIQ

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:

•99.99% system availability
•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.A Classic Cloud VPN gateway connected with two tunnels to an on-premises VPN gateway.

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 Classic Cloud VPN gateway connected with one tunnel to an on-premises VPN gateway.

**Answer: A**

**Explanation:**

An HA Cloud VPN gateway connected with two tunnels to an on-premises VPN gateway.

**Question: 196** CertyIQ

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: D**

**Explanation:**

Upload the data with gcloud storage cp.

**Question: 197** CertyIQ

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**

**Explanation:**

Create a retention policy on the bucket for the duration of 5 years. Create a lock on the retention policy.

**Question: 198** CertyIQ

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**

**Explanation:**

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

**Question: 199** CertyIQ

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' AND`<br>`metric.label.state = 'buffered' AND`<br>`metric.label.state = 'cached' AND`<br>`metric.label.state = 'slab'` |
| 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’.

D.Change the filter to metric.label.state = ‘free’ and the Target utilization to 20.

**Answer: C**

**Explanation:**

C. Change the filter to metric.label.state = ‘used’. 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. Therefore, the filter will never match any metrics, and the autoscaling policy won't trigger.

**Question: 200** CertyIQ

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**

**Explanation:**

C is best practice as recommended by googlehttps://cloud.google.com/resource-manager/docs/creating-managing-folders

For segregation of applications and environments, C is the best reference architecture model

**Question: 201** CertyIQ

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**

**Explanation:**
D: Handling "Unable to connect on port 22" error message
Possible causes include:
➪ There is no firewall rule allowing SSH access on the port. SSH access on port 22 is enabled on all Compute Engine instances by default. If you have disabled access, SSH from the Browser will not work. If you run sshd on a port other than 22, you need to enable the access to that port with a custom firewall rule.
➪ The firewall rule allowing SSH access is enabled, but is not configured to allow connections from GCP

Console services. Source IP addresses for browser- based SSH sessions are dynamically allocated by GCP Console and can vary from session to session.
F: Handling "Could not connect, retrying..." error
You can verify that the daemon is running by navigating to the serial console output page and looking for output lines prefixed with the accounts-from-metadata: string. If you are using a standard image but you do not see these output prefixes in the serial console output, the daemon might be stopped. Reboot the instance to restart the daemon.

Reference:
https://cloud.google.com/compute/docs/ssh-in-browser
https://cloud.google.com/compute/docs/ssh-in-browser

**Question: 202** CertyIQ

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**

**Explanation:**
Migrating data to Google Cloud Platform
Let's say that you have some data processing that happens on another cloud provider and you want to transfer the processed data to Google Cloud Platform. You can use a service account from the virtual machines on the external cloud to push the data to Google Cloud Platform. To do this, you must create and download a service account key when you create the service account and then use that key from the external process to call the Cloud Platform APIs.

Reference:
https://cloud.google.com/iam/docs/understanding-service-accounts#migrating_data_to_google_cloud_platform

**Question: 203** CertyIQ

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

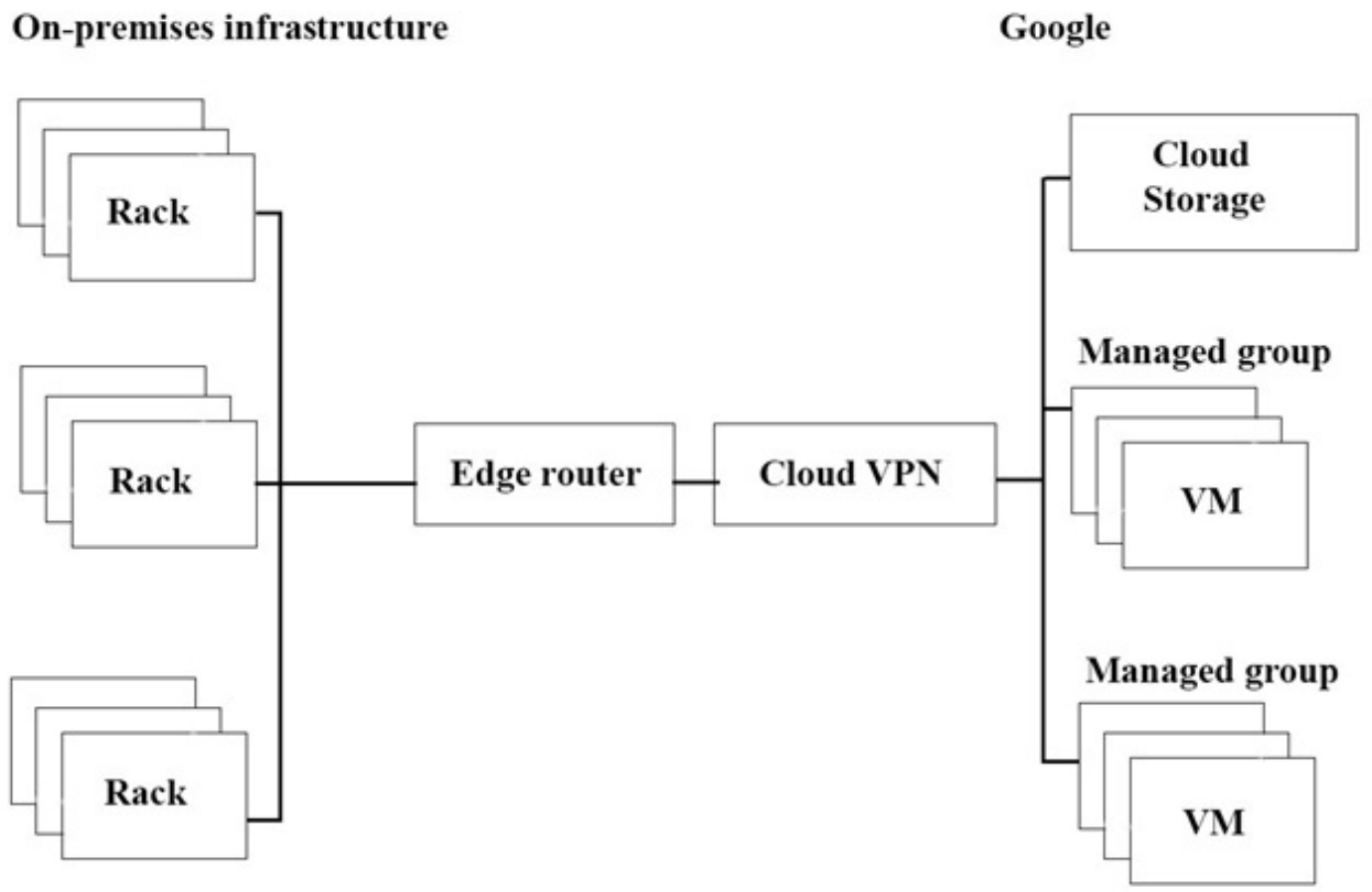
**Answer: C**

**Explanation:**

C.It says Guarantee service availability, we need to check for error rates to make sure our application is working perfectly fine.

error and latency will cover technical and visits buissness hence C

**Question: 204** CertyIQ




The migration of JencoMart's application to Google Cloud Platform (GCP) is progressing too slowly. The infrastructure is shown in the diagram. You want to maximize throughput.
What are three potential bottlenecks? (Choose three.)

A. A single VPN tunnel, which limits throughput
B. A tier of Google Cloud Storage that is not suited for this task
C. A copy command that is not suited to operate over long distances
D. Fewer virtual machines (VMs) in GCP than on-premises machines
E. A separate storage layer outside the VMs, which is not suited for this task
F. Complicated internet connectivity between the on-premises infrastructure and GCP

**Answer: ACF**

**Explanation:**

Single VPN tunnel limits throughput. Copying 20TB across long distances is a big bottleneck. VPN across internet cannot be relied upon for high performance

**Question: 205** CertyIQ

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**

**Explanation:**
Common workloads for Google Cloud Datastore:
- User profiles
- Product catalogs
- Game state

Reference:
https://cloud.google.com/storage-options/
https://cloud.google.com/datastore/docs/concepts/overview

**Question: 206** CertyIQ

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**

**Explanation:**

B as its clear in the example by google https://cloud.google.com/architecture/tokenizing-sensitive-cardholder-data-for-pci-dss

B, but should be reworded as follows for clarify."B. Encrypt the card data with a deterministic algorithm and store in Firestore using Datastore mode."https://cloud.google.com/architecture/tokenizing-sensitive-cardholder-data-for-pci-dss#a_service_for_handling_sensitive_information

**Question: 207** CertyIQ

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**

**Explanation:**

Is D:

In the GCP doc can see the same example

https://cloud.google.com/armor/docs/configure-security-policies#gcloud_11

"gcloud compute security-policies rules create 1000 \

--security-policy my-policy \

--expression "evaluatePreconfiguredExpr('sourceiplist-fastly')" \

--action "allow"

"

**Question: 208** CertyIQ

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**

**Explanation:**

C is okNeeds to be triggered by the deployment and not on a schedule. Cloud storage doesn't seem relevant in the context of the question

2. IMHO, the question is not clear. Is it a git or object repository. If its git repository than there need to be a logging or webhook that triggers the cloud function.. benefit of doubt goes to C.

**Question: 209** CertyIQ

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**

**Explanation:**

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. You can then use this information to verify that the model is behaving as expected, recognize bias in your models, and get ideas for ways to improve your model and your training data.

Reference:

https://cloud.google.com/ai-platform/prediction/docs/ai-explanations/preparing-metadata

**Question: 210** CertyIQ

For this question, refer to the Helicopter Racing League (HRL) case study. HRL is looking for a cost-effective approach for storing their race data such as telemetry. They want to keep all historical records, train models using only the previous season's data, and plan for data growth in terms of volume and information collected. You need to propose a data solution. Considering HRL business requirements and the goals expressed by CEO S. Hawke, what should you do?

A. Use Firestore for its scalable and flexible document-based database. Use collections to aggregate race data by season and event.
B. Use Cloud Spanner for its scalability and ability to version schemas with zero downtime. Split race data using

season as a primary key.

C. Use BigQuery for its scalability and ability to add columns to a schema. Partition race data based on season.

D. Use Cloud SQL for its ability to automatically manage storage increases and compatibility with MySQL. Use separate database instances for each season.

**Answer: C**

**Explanation:**

C. Use BigQuery for its scalability and ability to add columns to a schema. Partition race data based on season.

Reference:

https://cloud.google.com/bigquery/public-data

**Question: 211** CertyIQ

For this question, refer to the Helicopter Racing League (HRL) case study. A recent finance audit of cloud infrastructure noted an exceptionally high number of
Compute Engine instances are allocated to do video encoding and transcoding. You suspect that these Virtual Machines are zombie machines that were not deleted after their workloads completed. You need to quickly get a list of which VM instances are idle. What should you do?

A. Log into each Compute Engine instance and collect disk, CPU, memory, and network usage statistics for analysis.

B. Use the gcloud compute instances list to list the virtual machine instances that have the idle: true label set.

C. Use the gcloud recommender command to list the idle virtual machine instances.

D. From the Google Console, identify which Compute Engine instances in the managed instance groups are no longer responding to health check probes.

**Answer: C**

**Explanation:**

C. Use the gcloud recommender command to list the idle virtual machine instances.

Reference:

https://cloud.google.com/compute/docs/instances/viewing-and-applying-idle-vm-recommendations

**Question: 212** CertyIQ

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**

**Explanation:**

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.

**Question: 213** CertyIQ

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**

**Explanation:**

A & D

Binary Authorization to ensure only verified containers are deployed

To ensure deployment are secure and and consistent, automatically scan images for vulnerabilities with container analysis (https://cloud.google.com/docs/ci-cd/overview?hl=en&skip_cache=true)

**Question: 214** CertyIQ

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**

**Explanation:**

I will go A cause note in https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/modifying-interconnects says" It is not possible to change the link type on an Interconnect connection circuit from 10 Gbps to 100 Gbps. If you want to migrate to 100 Gbps, you must first provision a new 100-Gbps Interconnect connection alongside your existing 10-Gbps connection, and then migrate the traffic onto the 100-Gbps connection."

**Question: 215** CertyIQ

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**

**Explanation:**

Business requirements for this case:

* Provide a minimum 99.9% availability for all customer-facing systems.

* Provide a secure and high-performance connection between on-premises systems and Google Cloud.

A. - builds us a 99.9% SLA partner interconnect, covering all business requirements.

B. - VPN is not suitable for the business requirements.

C. - Direct peering is used for workspace, instead of DMZ, again - not suitable.

D. - builds us a 99.99% SLA dedicated interconnect, covering all business requirements.

The answer to choosing A or D lies in the question, stating: "You want to follow Google's recommended practices for production-level applications."

Google recommends using the 99.99% SLA interconnect (dedicated or partner) for production-level applications as stated here:

https://cloud.google.com/network-connectivity/docs/interconnect/tutorials/production-level-overview

The answer is D.

**Question: 216** CertyIQ

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**

**Explanation:**

C is better option, even though increasing total timeout would help reduce timeout errors but remember that that in this case we are getting too many messages from the server since load increased and we need to reduce latency

**Question: 217** CertyIQ

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**

**Explanation:**

A is the clear answer as per google recommendation

**Question: 218** CertyIQ

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**

**Explanation:**

A is the best answer https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept#overview

I'll go with A as it is the most secure option. C would be more cost-effective for when EHR has no plans for Cloud Interconnect / VPN (which they do!).

**Question: 219** CertyIQ

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**

**Explanation:**

From Scenario:

A few of their games were more popular than expected, and they had problems scaling their application servers, MySQL databases, and analytics tools.

Requirements for Game Analytics Platform include: Dynamically scale up or down based on game activity

**Question: 220** CertyIQ

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

A. Create a scalable environment in GCP for simulating production load

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

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

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

**Answer: A**

**Explanation:**

From scenario: Requirements for Game Backend Platform

1. Dynamically scale up or down based on game activity
2. Connect to a managed NoSQL database service
3. Run customize Linux distro

**Question: 221** CertyIQ

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, Google Network Load Balancer

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

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

**Answer: C**

**Explanation:**

If the Question is erroneously formulated, and they mean Google Container Registry and Google Kubernetes Engine, then C is the right answer

**Question: 222** CertyIQ

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 is service unavailable error. If the database was online everyone would get the 503 error.

**Question: 223** CertyIQ

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

**Answer: D**

**Explanation:**

In the requirement, the staging environment needs access to production, not the other way around. Answer A could allow staging and production to access each other. In answer D, staging and production are in different project, you can limit the access from either side. So D is correct.

**Question: 224** CertyIQ

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**

**Explanation:**

Ingest millions of streaming events per second from anywhere in the world with Cloud Pub/Sub, powered by Google's unique, high-speed private network. Process the streams with Cloud Dataflow to ensure reliable, exactly-once, low-latency data transformation. Stream the transformed data into BigQuery, the cloud-native data warehousing service, for immediate analysis via SQL or popular visualization tools.

From scenario: They plan to deploy the game's backend on Google Compute Engine so they can capture streaming metrics, run intensive analytics.

Requirements for Game Analytics Platform

1. Dynamically scale up or down based on game activity
2. Process incoming data on the fly directly from the game servers
3. Process data that arrives late because of slow mobile networks
4. Allow SQL queries to access at least 10 TB of historical data
5. Process files that are regularly uploaded by users' mobile devices
6. Use only fully managed services

Reference:

https://cloud.google.com/solutions/big-data/stream-analytics/

**Question: 225** CertyIQ

For this question, refer to the 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? (Choose two.)

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 shows 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**

**Explanation:**

Correct Answer A, B

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

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

Stream processing (ETL) Dataflow and

Reference

https://cloud.google.com/bigquery/docs/loading-data#loading_denormalized_nested_and_repeated_data

**Question: 226** CertyIQ

For this question, refer to the Mountkirk Games case study. You need to analyze and define the technical architecture for the compute workloads for your company, Mountkirk Games. Considering the Mountkirk 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 balancer with managed instance groups and autoscaling policies. Use preemptible Compute Engine instances.

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

**Answer: D**

**Explanation:**

D) => KPI game stability = Use non-preemptible

**Question: 227** CertyIQ

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 two.)

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 machines so they can apply critical kernel patches and package updates and reduce the risk of 0-day vulnerabilities.

**Answer: AB**

**Explanation:**

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.

**Question: 228** CertyIQ

For this question, refer to the 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 game that runs on players' mobile devices and collects response times from analytics endpoints running in Google Cloud Platform regions all over the world.

**Answer: A**

**Explanation:**

1. A seems right
2. A is ok to some extent.

**Question: 229** CertyIQ

For this question, refer to the 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 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**

**Explanation:**

Correct Answer D

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

Storing time-series data in Cloud Bigtable is a natural fit, Cloud Spanner scales horizontally and serves data with low latency while maintaining transactional consistency and industry-leading 99.999% (five 9s) availability - 10x less downtime than four nines (<5 minutes per year). Cloud Spanner helps future-proof your database backend. After you load your data into BigQuery, you can query the data in your tables. BigQuery supports two types of queries: Interactive queries, Batch queries

**Question: 230** CertyIQ

For this question, refer to the Mountkirk Games 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 Datastore

**Answer: A**

**Explanation:**

Cloud Bigtable

Storing time series data in Cloud Bigtable https://cloud.google.com/bigtable/docs/schema-design-time-series

**Question: 231** CertyIQ

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**

**Explanation:**

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

Requirements ask to minimize downtime – so needs redundancy across regions and zones inside regions. In addition, GCP Best Practicies of recommends HTTPs (L7) Load Balancer for internet facing app, to design for High-Availability. Quote from this page:

“GCP offers several variations of load balancing. The HTTP(S) load balancer is often used to expose internet-facing apps. This load balancer provides global balancing, allowing distribution of load across regions in different geographies. If a zone or region becomes unavailable, the load balancer directs traffic to a zone with available capacity. For more details, see application capacity optimizations with global load balancing”.

Check this page about LB options: Choosing a Load Balancer

Check difference between L4 and L7 LBs here.

**Question: 232** CertyIQ

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**

**Explanation:**

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

Reference:

https://cloud.google.com/storage/docs/gsutil/commands/cp

**Question: 233** CertyIQ

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**

**Explanation:**

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

**Question: 234** CertyIQ

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**

**Explanation:**

Correct answer is: A. Configure an organizational policy which constrains where resources can be deployed.

Google Cloud offers the ability to use organizational policies to constrain the deployment of resources to specific regions or zones. This allows you to control where resources can be deployed within your organization, and ensure that they are only deployed in the regions that are appropriate for your business needs. To configure an organizational policy to constrain the location of resources, you can use the Cloud Resource Manager to create and apply a policy that specifies the allowed regions or zones for resource deployment.

**Question: 235** CertyIQ

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**

**Explanation:**

The confusing thing here is that GCP has renamed the same solution multiple times. The concept is "Multi Cluster Ingress (MCI)", and kubemci was the original solution for setting this up. Then GCP released "Ingress for Anthos", which replaced kubemci. Now, they have again renamed "Ingress for Anthos" to "Multi Cluster Ingress" (because it applies to more than just Anthos). If you see this question in the exam, it should no longer provide "Ingress for Anthos" as an option, but instead will say something like "Multi Cluster Ingress". The answers can be found at these links:https://cloud.google.com/kubernetes-engine/docs/concepts/multi-cluster-ingresshttps://cloud.google.com/kubernetes-engine/docs/how-to/multi-cluster-ingress

**Question: 236** CertyIQ

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**

**Explanation:**

Answer is C. End users don't care or need to know about server uptime, CPU or memory. End- users care about their user experience.

Service Level Indicators (SLI) is the metrics for the level of service provided to end users. Real numbers of the performance.

Example: request latency to be less than 500ms in the last 15 minutes with a 95% percentile.

Service Level objective: Target level for the reliability of your service.

Example: SLI to be met 99% of the time.

SLA - the agreement that you make with the end users.

**Question: 237** CertyIQ

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**

**Explanation:**

A is correct .

https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity

Workload Identity is the recommended way to access Google Cloud services from applications running within GKE due to its improved security properties and manageability. For information about alternative ways to access Google Cloud APIs from GKE, refer to the alternatives section below.

**Question: 238** CertyIQ

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**

**Explanation:**

Correct Answer: A

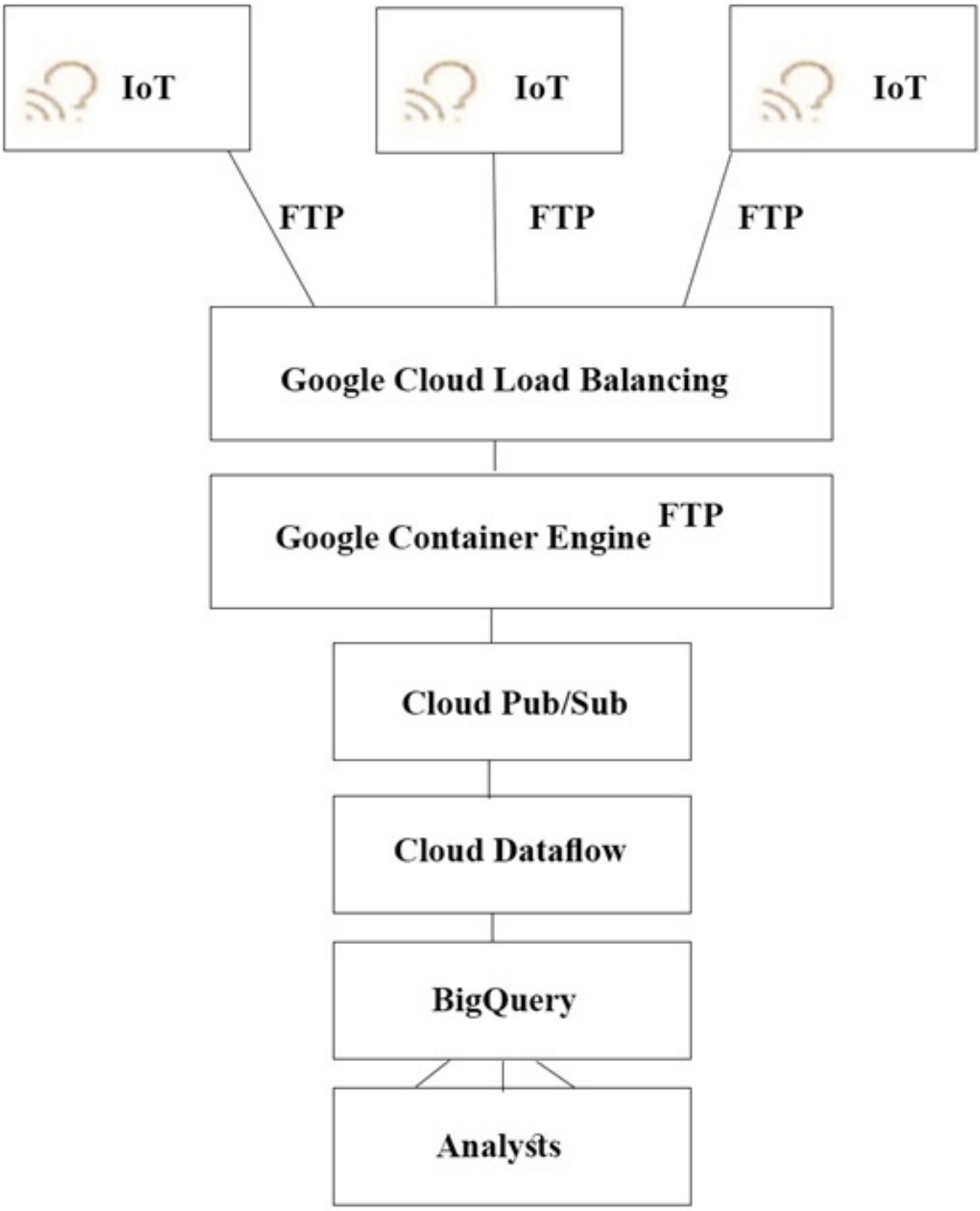
- Firebase Test Lab is a cloud-based app testing infrastructure that lets you test your app on a range of devices and configurations, so you can get a better idea of how it'll perform in the hands of live users.

- Firebase Test Lab Run tests on a wide range of Android and iOS devices hosted by Test Lab.

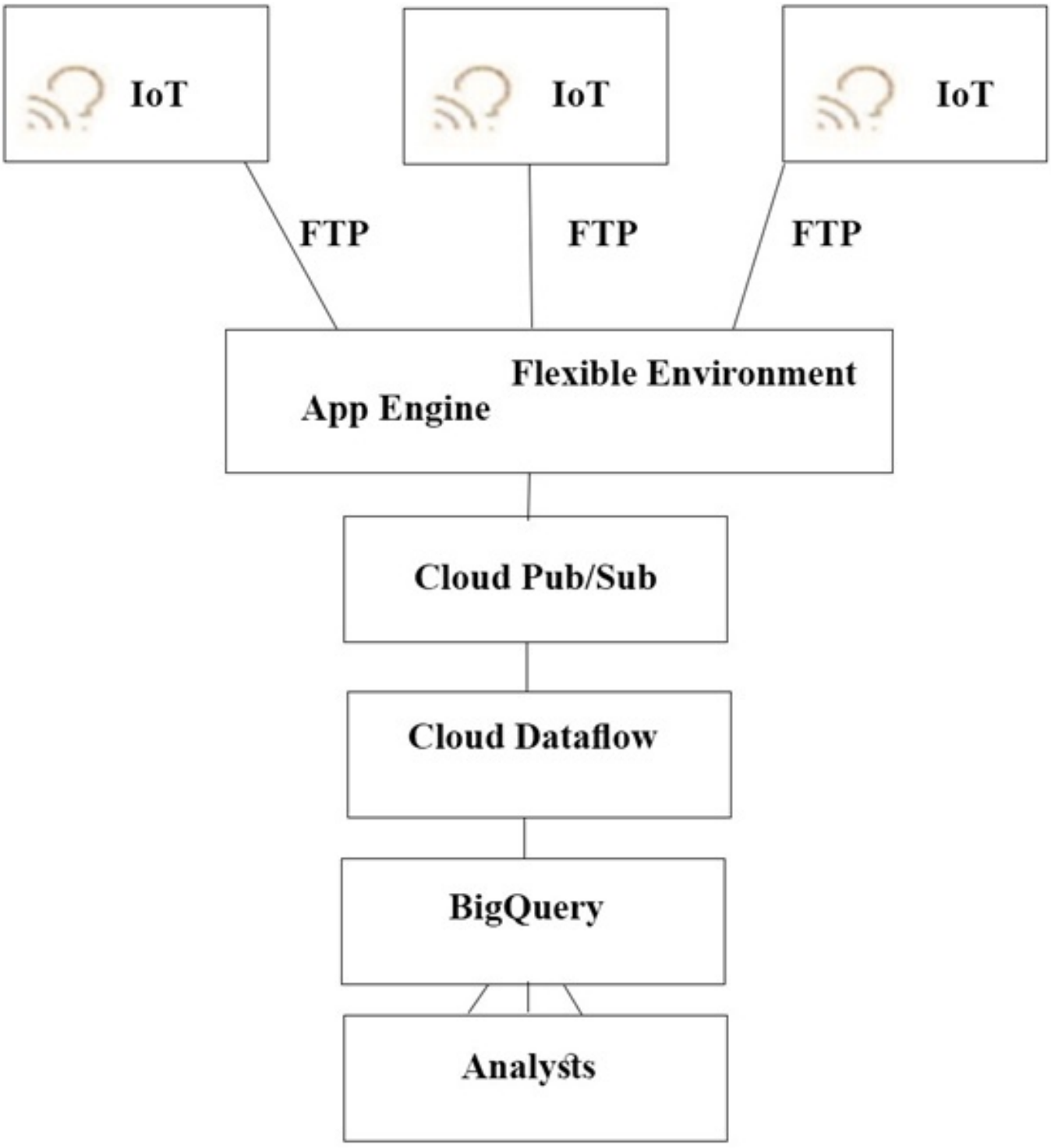
**Question: 239** CertyIQ

TerramEarth's CTO wants to use the raw data from connected vehicles to help identify approximately when a

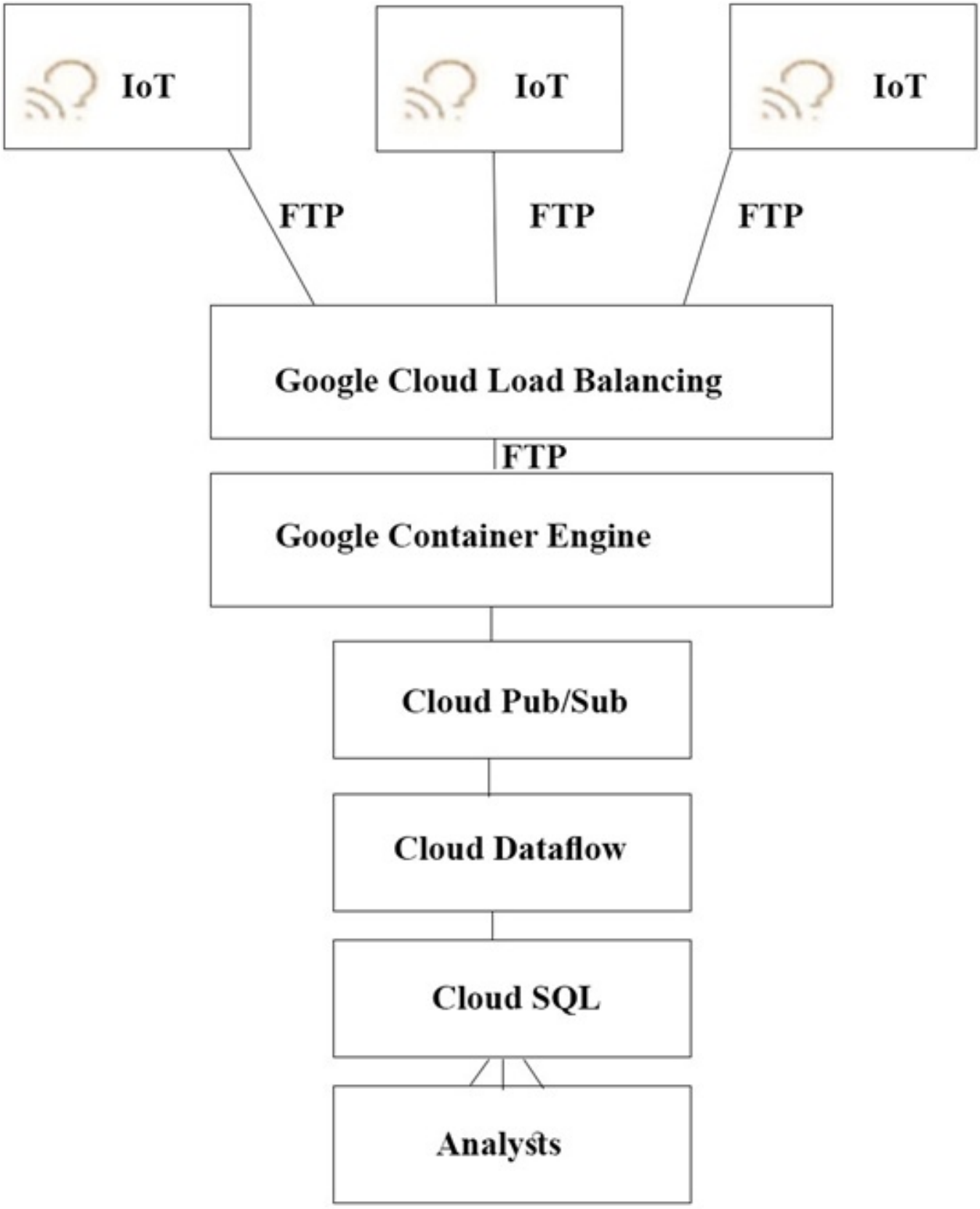
vehicle in the field will have a catastrophic failure.
You want to allow analysts to centrally query the vehicle data.
Which architecture should you recommend?
A.



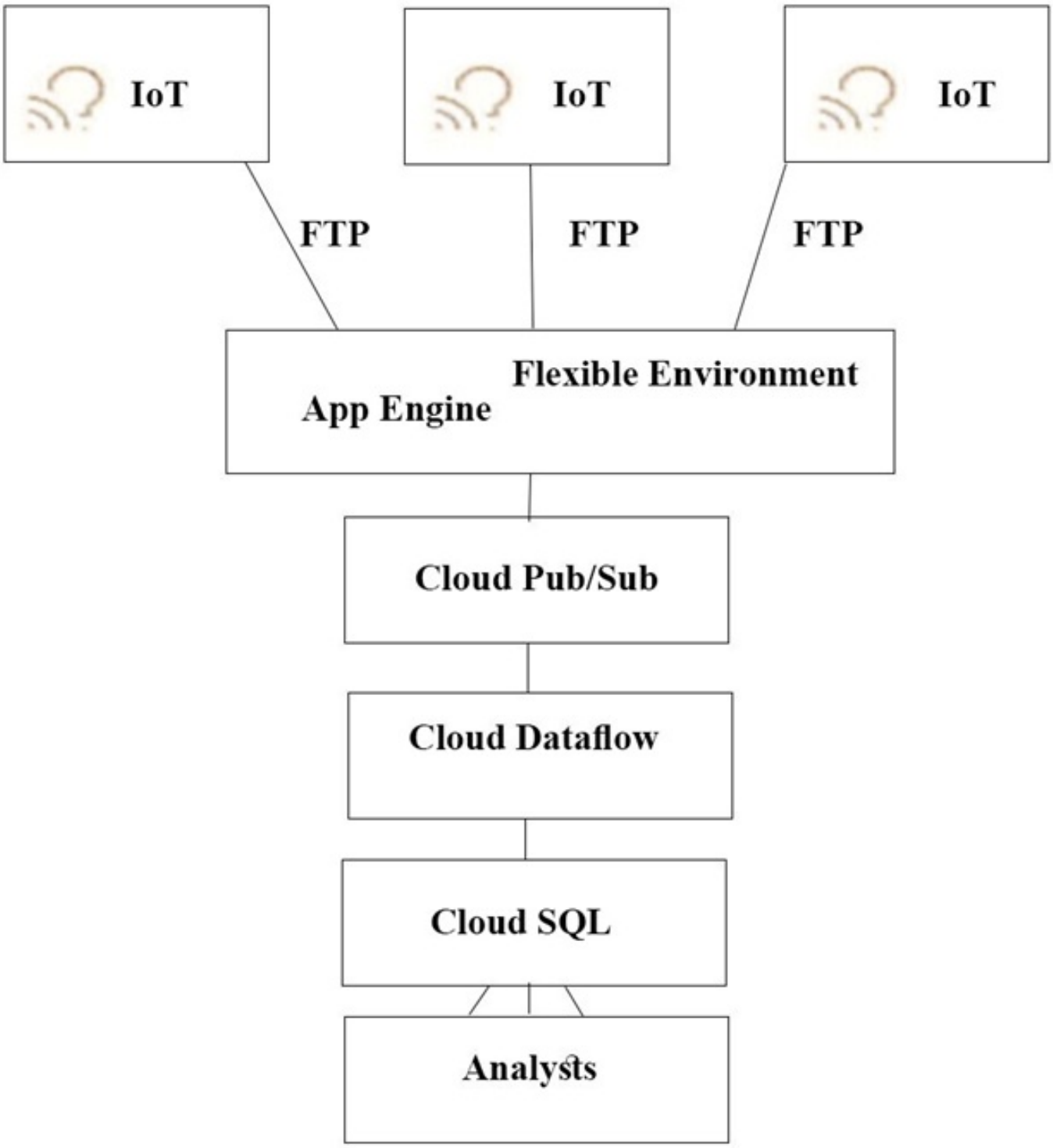

B.


IoT
IoT
IoT
FTP
FTP
FTP
Flexible Environment
App Engine
Cloud Pub/Sub
Cloud Dataflow
BigQuery
Analysts

C.

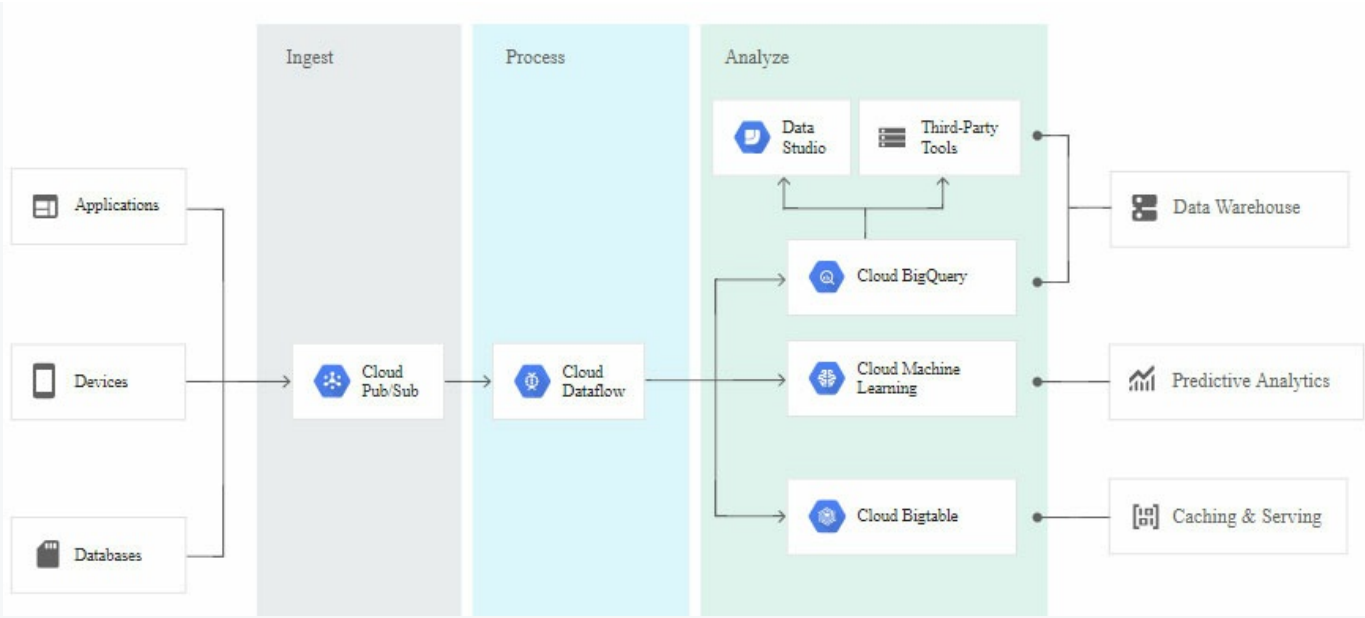

IoT
IoT
IoT
FTP
FTP
FTP
Google Cloud Load Balancing
FTP
Google Container Engine
Cloud Pub/Sub
Cloud Dataflow
Cloud SQL
Analysts

D.




**Answer: A**

**Explanation:**
The push endpoint can be a load balancer.
A container cluster can be used.
Cloud Pub/Sub for Stream Analytics




Reference:
https://cloud.google.com/pubsub/
https://cloud.google.com/solutions/iot/
https://cloud.google.com/solutions/designing-connected-vehicle-platform https://cloud.google.com/solutions/designing-connected-vehicle-platform#data_ingestion http://www.eweek.com/big-data-and-analytics/google-touts-value-of-cloud-iot-core-for-analyzing-connected-car-data https://cloud.google.com/solutions/iot/

**Question: 240** CertyIQ

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**

**Explanation:**
Develop, deploy, protect and monitor your APIs with Google Cloud Endpoints. Using an Open API Specification or one of our API frameworks, Cloud Endpoints gives you the tools you need for every phase of API development.
From scenario:

Business Requirements -
Decrease unplanned vehicle downtime to less than 1 week, without increasing the cost of carrying surplus inventory
Support the dealer network with more data on how their customers use their equipment to better position new products and services
Have the ability to partner with different companies " especially with seed and fertilizer suppliers in the fast-growing agricultural business " to create compelling joint offerings for their customers.

Reference:
https://cloud.google.com/certification/guides/cloud-architect/casestudy-terramearth

**Question: 241** CertyIQ

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**

**Explanation:**
Delegate application authorization with OAuth2
Cloud Platform APIs support OAuth 2.0, and scopes provide granular authorization over the methods that are supported. Cloud Platform supports both service- account and user-account OAuth, also called three-legged OAuth.

Reference:
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#delegate_application_authorization_with_oauth2 https://cloud.google.com/appengine/docs/flexible/go/authorizing-apps

**Question: 242** CertyIQ

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. Vehicles write data directly to GCS
B. Vehicles write data directly to Google Cloud Pub/Sub
C. Vehicles stream data directly to Google BigQuery
D. Vehicles continue to write data using the existing system (FTP)

**Answer: B**

**Explanation:**

B is the correct answer, this similar question was in google simple questions

We need to buffer, the default limit of BigQuery is 100 API calls per second, till now this cannot be changed. Hence we should ease using Pub/Sub so B.

**Question: 243** CertyIQ

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**

**Explanation:**
The Avro binary format is the preferred format for loading compressed data. Avro data is faster to load because the data can be read in parallel, even when the data blocks are compressed.
Cloud Storage supports streaming transfers with the gsutil tool or boto library, based on HTTP chunked transfer encoding. Streaming data lets you stream data to and from your Cloud Storage account as soon as it becomes available without requiring that the data be first saved to a separate file. Streaming transfers are useful if you have a process that generates data and you do not want to buffer it locally before uploading it, or if you want to send the result from a computational pipeline directly into Cloud Storage.

Reference:
https://cloud.google.com/storage/docs/streaming
https://cloud.google.com/bigquery/docs/loading-data

**Question: 244** CertyIQ

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**

**Explanation:**

Correct Answer B

Capacity planning, TCO calculations, opex/capex allocation

From the case study, it can conclude that Management (CXO) all concern rapid provision of resources (infrastructure) for growing as well as cost management, such as Cost optimization in Infrastructure, trade up front capital expenditures (Capex) for ongoing operating expenditures (Opex), and Total cost of ownership (TCO)

**Question: 245** CertyIQ

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**

**Explanation:**

c)

Multi-Region Name Multi-Region Description

asia Data centers in Asia

eu Data centers in the European Union1

us Data centers in the United States

multi-region is a large geographic area, such as the United States, that contains two or more geographic places.

**Question: 246** CertyIQ

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**

**Explanation:**

D is the correct answer. Regional bucket is required, since multi regional bucket will incur additional cost to transfer the data to a centralized location.

**Question: 247** CertyIQ

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**

**Explanation:**
Storage is the best choice for data that you plan to access at most once a year, due to its slightly lower availability, 90-day minimum storage duration, costs for data access, and higher per-operation costs. For example:
Cold Data Storage - Infrequently accessed data, such as data stored for legal or regulatory reasons, can be stored at low cost as Coldline Storage, and be available when you need it.
Disaster recovery - In the event of a disaster recovery event, recovery time is key. Cloud Storage provides low latency access to data stored as Coldline Storage.

Reference:
https://cloud.google.com/storage/docs/storage-classes

**Question: 248** CertyIQ

Your agricultural division is experimenting with fully autonomous vehicles. You want your architecture to promote strong security during vehicle operation.
Which two architectures should you consider? (Choose two.)

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

B. Require 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 electronics in a Faraday cage to isolate chips.

**Answer: AC**

**Explanation:**

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

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

**Question: 249** CertyIQ

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**

**Explanation:**

B is correct. only 200k vehicle's are connected so need to run updates locally

**Question: 250** CertyIQ

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 a SetStorageClass to NONE action when 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 a SetStorageClass to NONE action with an Age condition of 36 months.

**Answer: C**

**Explanation:**

C

Enable a bucket lifecycle management rule to delete objects older than 36 months. Use partitioned tables in BigQuery and set the partition expiration period to 36 months. is the right answer.

When you create a table partitioned by ingestion time, BigQuery automatically loads data into daily, date-based partitions that reflect the data's ingestion or arrival time.

And Google recommends you configure the default table expiration for your datasets, configure the expiration time for your tables, and configure the partition expiration for partitioned tables.

storage#use_the_expiration_settings_to_remove_unneeded_tables_and_partitions

If the partitioned table has a table expiration configured, all the partitions in it are deleted according to the table expiration settings. For our specific requirement, we could set the partition expiration to 36 months so

that partitions older than 36 months (and the data within) are automatically deleted.

Reference:

https://cloud.google.com/bigquery/docs/partitioned-tables#ingestion_time

https://cloud.google.com/bigquery/docs/managing-partitioned-tables#partition-expiration

https://cloud.google.com/bigquery/docs/best-practices-

**Question: 251** CertyIQ

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 rule 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 GCS 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 GCS life-cycle rule with Age: 91, Storage Class: Coldline, and Action: Set to Nearline.

C. Create a Cloud Storage lifecycle rule with Age: 90, Storage Class: Standard, and Action: Set to Nearline, and create a second GCS 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 GCS life-cycle rule with Age: 365, Storage Class: Nearline, and Action: Delete.

**Answer: A**

**Explanation:**

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

**Question: 252** CertyIQ

For this question, refer to the TerramEarth case study. You need to implement a reliable, scalable GCP 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**

**Explanation:**

A is the correct answer because the question was asking for a reliable way of improving the data warehouse. The reliable way is to have a table partitioned and that can be well managed.

https://cloud.google.com/solutions/bigquery-data-warehouse

BigQuery supports partitioning tables by date. You enable partitioning during the table-creation process. BigQuery creates new date-based partitions automatically, with no need for additional maintenance. In addition, you can specify an expiration time for data in the partitions.

https://cloud.google.com/solutions/bigquery-data-warehouse#partitioning_tables

Federated is an option but not a reliable option.

You can run queries on data that exists outside of BigQuery by using federated data sources, but this approach has performance implications. Use federated data sources only if the data must be maintained externally. You can also use query federation to perform ETL from an external source to BigQuery. This approach allows you to define ETL using familiar SQL syntax.

https://cloud.google.com/solutions/bigquery-data-warehouse#external_sources

**Question: 253** CertyIQ

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**

**Explanation:**

Option D, as data needs to be cleaned ..

Dataprep has the capabilities to clean dirty data

**Question: 254** CertyIQ

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**

**Explanation:**

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.

**Question: 255** CertyIQ

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**

**Explanation:**

B. Cloud IoT Core with public/private key pairs

**Question: 256** CertyIQ

Regarding Cloud Storage, which option allows any user to access to a Cloud Storage resource for a limited time, using a specific URL?

A. Open Buckets
B. Temporary Resources
C. Signed URLs
D. Temporary URLs

**Answer: C**

**Explanation:**
Signed URLs provide a way to give time-limited read or write access to anyone in possession of the URL, regardless of whether they have a Google account
In some scenarios, you might not want to require your users to have a Google account in order to access Cloud Storage, but you still want to control access using your application-specific logic. The typical way to address this use case is to provide a signed URL to a user, which gives the user read, write, or delete access to that resource for a limited time. Anyone who knows the URL can access the resource until the URL expires. You specify the expiration time in the query string to be signed.
Reference: https://cloud.google.com/storage/docs/access-control/signed-urls

**Question: 257** CertyIQ

Of the options given, which is a NoSQL database?

A. Cloud Datastore

B. Cloud SQL
C. All of the given options
D. Cloud Storage

**Answer: A**

**Explanation:**
Google Cloud Datastore is a NoSQL document database built for automatic scaling, high performance, and ease of application development. Cloud Datastore features include:
Reference: https://cloud.google.com/appengine/docs/python/datastore/

**Question: 258** CertyIQ

Container Engine allows orchastration of what type of containers?

A. Blue Whale
B. LXC
C. BSD Jails
D. Docker

**Answer: D**

**Explanation:**
Google Container Engine is a powerful cluster manager and orchestration system for running your Docker containers.
Reference: https://cloud.google.com/container-engine/

**Question: 259** CertyIQ

Regarding Cloud IAM, what type of role(s) are available?

A. Basic roles and Compiled roles
B. Primitive roles and Predefined roles
C. Simple roles
D. Basic roles and Curated roles

**Answer: B**

**Explanation:**
Prior to Cloud IAM, you could only grant Owner, Editor, or Viewer roles to users. A wide range of services and resources now surface additional IAM roles out of the box. For example, the Cloud
Pub/Sub service exposes Publisher and Subscriber roles in addition to the Owner, Editor, and Viewer roles.
There are two kinds of roles in Cloud IAM:
Primitive roles: The roles historically available in the Google Cloud Platform Console will continue to work. These are the Owner, Editor, and Viewer roles.
Predefined roles: Predefined roles are the new IAM roles that give finer-grained access control than the primitive roles. For example, the curated role Publisher provides access to only publish messages to a Pub/Sub topic.
Reference: https://cloud.google.com/iam/docs/overview

**Question: 260** CertyIQ

Which of the follow products will allow you to host a static website?

A. Cloud SDK
B. Cloud Endpoints
C. Cloud Storage
D. Cloud Datastore

**Answer: C**

**Explanation:**
Cloud Storage will allow you to host a static website. It provides the means to set an index page, and 404 page. The site can be served up a very fast speeds, and at a low cost.
Reference: https://cloud.google.com/storage/docs/static-website

**Question: 261** CertyIQ

Container Engine is built on which open source system?

A. Swarm
B. Kubernetes
C. Docker Orchastrate
D. Mesos

**Answer: B**

**Explanation:**
Google Container Engine is a powerful cluster manager and orchestration system for running your Docker containers. Container Engine schedules your containers into the cluster and manages them automatically based on requirements you define (such as CPU and memory). It's built on the open source Kubernetes system, giving you the flexibility to take advantage of on-premises, hybrid, or public cloud infrastructure.
Reference: https://cloud.google.com/container-engine/

**Question: 262** CertyIQ

Cloud Source Repositories provide a hosted version of which version control system?

A. Git
B. RCS
C. SVN
D. Mercurial

**Answer: A**

**Explanation:**
Google Cloud Source Repositories are fully-featured, private Git repositories hosted on Google Cloud Platform.
Reference: https://cloud.google.com/source-repositories/docs/

**Question: 263** CertyIQ

Which of the following is an analytics data warehouse?

A. Cloud SQL
B. Big Query
C. Datastore
D. Cloud Storage

**Answer: B**

**Explanation:**
BigQuery is Google's fully managed, petabyte scale, low cost analytics data warehouse.
BigQuery is serverless, there is no infrastructure to manage and you don't need a database administrator, so you can focus on analyzing data to find meaningful insights, use familiar SQL, and take advantage of our pay-as-you-go model. BigQuery is a powerful Big Data analytics platform used by all types of organizations, from startups to Fortune 500 companies.
Reference: https://cloud.google.com/bigquery/

**Question: 264** CertyIQ

Which service offers the ability to create and run virtual machines?

A. Google Virtualization Engine
B. Compute Containers
C. VM Engine
D. Compute Engine

**Answer: D**

**Explanation:**
Google Compute Engine delivers virtual machines running in Google's innovative data centers and worldwide fiber network. Compute Engine's tooling and workflow support enable scaling from single instances to global, load-balanced cloud computing.
Compute Engine's VMs boot quickly, come with persistent disk storage, and deliver consistent performance. Our virtual servers are available in many configurations including predefined sizes or the option to create Custom Machine Types optimized for your specific needs. Flexible pricing and automatic sustained use discounts make Compute Engine the leader in price/performance.
Reference: https://cloud.google.com/compute/

**Question: 265** CertyIQ

Which of the following is not helpful for mitigating the impact of an unexpected failure or reboot?

A. Use persistent disks
B. Configure tags and labels
C. Use startup scripts to re-configure the system as needed
D. Back up your data

**Answer: B**

**Explanation:**
At some point in time, you will experience an unexpected single instance failure and reboot. Unlike unexpected single instance failures, your instance fails and is automatically rebooted by the Google Compute Engine service. To help mitigate these events, back up your data, use persistent disks, and use startup scripts to quickly re-configure software.
Reference: https://cloud.google.com/compute/docs/tutorials/robustsystems

**Question: 266** CertyIQ

Single sign-on (SSO) with G Suite is based on _____?

A. SAML2
B. JWT
C. Service accounts
D. JSON

**Answer: A**

**Explanation:**
SSO is available for G Suite Basic, G Suite Business, and G Suite for Education. It enables users to access all of their enterprise cloud applicationsincluding administrators signing in to the Admin consoleby signing in one time for all services. If a user tries to sign in to the Admin console or another Google service when SSO is set up, they are redirected to the SSO sign-in page.
Google provides a Security Assertion Markup Language (SAML)-based SSO API that you can use to integrate into your Lightweight Directory Access Protocol
(LDAP), or other SSO system. LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.
Reference: https://support.google.com/a/answer/60224?hl=en

**Question: 267** CertyIQ

Which tool allows you to sync data in your Google domain with Active Directory?

A. Google Cloud Directory Sync (GCDS)
B. Google Active Directory (GAD)
C. Google Domain Sync Service
D. Google LDAP Sync

**Answer: A**

**Explanation:**
With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google domain with your MicrosoftActive Directory or LDAP server. Your
Google users, groups, and shared contacts are synchronized to match the information in your LDAP server. The data in your LDAP directory server is never modified or compromised. GCDS is a secure tool that help you easily keep track of users and groups.
Reference: https://support.google.com/a/answer/106368?hl=en

**Question: 268** CertyIQ

Regarding Cloud Storage: which of the following allows for time-limited access to buckets and objects without a Google account?

A. Signed URLs
B. gsutil
C. Single sign-on
D. Temporary Storage Accounts

**Answer: A**

**Explanation:**
Signed URLs are a mechanism for query string authentication for buckets and objects. Signed URLs provide a way to give time-limited read or write access to anyone in possession of the URL, regardless of whether they have a Google account.
Reference: https://cloud.google.com/storage/docs/access-control/signed-urls

**Question: 269** CertyIQ

Which of the following is a virtual machine instance that can be terminated by Compute Engine without warning?

A. A preemptible VM
B. A shared-core VM
C. A high-cpu VM
D. A standard VM

**Answer: A**

**Explanation:**
A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity so their availability varies with usage.
If your applications are fault-tolerant and can withstand possible instance preemptions, then preemptible instances can reduce your Compute Engine costs significantly. For example, batch processing jobs can run on preemptible instances. If some of those instances terminate during processing, the job slows but does not completely stop. Preemptible instances complete your batch processing tasks without placing additional workload on your existing instances, and without requiring you to pay full price for additional normal instances.
Reference: https://cloud.google.com/compute/docs/instances/preemptible

**Question: 270** CertyIQ

Regarding Compute Engine: What is a managed instance group?

A. A managed instance group combines existing instances of different configurations into one manageable group
B. A managed instance group uses an instance template to create identical instances
C. A managed instance group creates a firewall around instances
D. A managed instance group is a set of servers used exclusively for batch processing

**Answer: B**

**Explanation:**
A managed instance group uses an instance template to create identical instances. You control a managed instance group as a single entity. If you wanted to make changes to instances that are part of a managed instance group, you would apply the change to the whole instance group.
Reference: https://cloud.google.com/compute/docs/instance-groups/

**Question: 271** CertyIQ

What type of firewall rule(s) does Google Cloud's networking support?

A. deny
B. allow, deny & filtered
C. allow
D. allow & deny

**Answer: D**

**Explanation:**
You can create firewall rules to allow or deny specific connections based on a combination of IP addresses, ports, and protocol.
Reference: https://cloud.google.com/compute/docs/networking

**Question: 272** CertyIQ

How are subnetworks different than the legacy networks?

A. They're the same, only the branding is different
B. Each subnetwork controls the IP address range used for instances that are allocated to that subnetwork
C. With subnetworks IP address allocation occurs at the global network level
D. Legacy networks are the preferred way to create networks

**Answer: B**

**Explanation:**
. Legacy (non-subnetwork) mode is the original approach for networks, where IP address allocation occurs at the global network level. This means the network address space spans across all regions. You can still create a legacy network, but subnetworks are the preferred approach and default behavior going forward.
. Subnet mode is the new form of networks in which your network is subdivided into regional subnetworks. Each subnetwork controls the IP address range used for instances that are allocated to that subnetwork. The IP ranges of the different subnetworks in a network might be non-contiguous. There are two options for using subnetworks:
.Auto subnet network automatically assigns a subnetwork IP prefix range to each region in your network. The instances created in a zone in a specific region in your network get assigned an IP allocated from the regional subnetwork range. The default network for a new project is an auto subnet network.
.Custom subnet network allows you to manually define subnetwork prefixes for each region in your network. There can be zero, one, or several subnetwork prefixes created per region for a network. In order to create an instance in a zone, you must have previously created at least one subnetwork in that region. At instance creation time, you will need to specify the subnetwork in the region that the instance IP should be allocated from.
Reference: https://cloud.google.com/compute/docs/subnetworks

**Question: 273** CertyIQ

Which of the following is not a valid metric for triggering autoscaling?

A. Google Cloud Pub/Sub queuing
B. Average CPU utilization
C. Stackdriver Monitoring metrics
D. App Engine Task Queues

**Answer: D**

**Explanation:**
To create an autoscaler, you must specify the autoscaling policy and a target utilization level that the autoscaler uses to determine when to scale the group. You can choose to scale using the following policies:
. Average CPU utilization
. Stackdriver Monitoring metrics
. HTTP load balancing serving capacity, which can be based on either utilization or requests per second.
. Google Cloud Pub/Sub queuing workload (Alpha)
Reference: https://cloud.google.com/compute/docs/autoscaler/

**Question: 274** CertyIQ

Which of the following features makes applying firewall settings easier?

A. Service accounts
B. Tags
C. Metadata
D. Labels

**Answer: B**

**Explanation:**
Assign tags to help you easily apply networking or firewall settings. Tags are used by networks and firewalls to identify which instances that certain firewall rules apply to. For example, if there are several instances that perform the same task, such as serving a large website, you can tag these instances with a shared word or term and then use that tag to give HTTP access to those instances. Tags are also reflected in the metadata server, so you can use them for applications running on your instances.
Reference: https://cloud.google.com/compute/docs/label-or-tag-resources

**Question: 275** CertyIQ

What option does Cloud SQL offer to help with high availability?

A. Point-in-time recovery
B. The AlwaysOn setting
C. Snapshots
D. Failover replicas

**Answer: D**

**Explanation:**

When you create a Second Generation instance, you can configure it for high availability; Cloud SQL creates the failover replica at the same time that it creates the master.
Reference: https://cloud.google.com/sql/docs/configure-ha#test

**Question: 276** CertyIQ

Regarding Compute Engine: when executing a startup script on a Linux server which user does the instance execute the script as?

A. ubuntu
B. The Google provided "gceinstance" user
C. Whatever user you specify in the console
D. root

**Answer: D**

**Explanation:**
The instance always executes startup scripts as root, and only executes those scripts after it creates any new users whose SSH keys are included in the instance metadata.
Reference: https://cloud.google.com/compute/docs/startupscript

**Question: 277** CertyIQ

Which of the follow methods will not cause a shutdown script to be executed?

A. When an instance shuts down through a request to the guest operating system
B. A preemptible instance being terminated
C. An instances.reset API call
D. Shutting down via the cloud console

**Answer: C**

**Explanation:**
Shutdown scripts execute when an instance is scheduled to restart or terminate. There are many ways to restart or terminate an instance, but only some actions trigger the shutdown script to run. A shutdown script runs as part of the following actions:
When an instance shuts down due to an instances.delete request or an instances.stoprequest to the API.
When Compute Engine stops a preemptible instance as part of the preemption process.
When an instance shuts down through a request to the guest operating system, such as sudo shutdown or sudo reboot.
When you shut down an instance manually through the Cloud Platform Console or the gcloud compute tool.
The shutdown script will not run if the instance is reset using instances().reset.
Reference: https://cloud.google.com/compute/docs/shutdownscript

**Question: 278** CertyIQ

Which type of account would you use in code when you want to interact with Google Cloud services?

A. Google group
B. Service account

C. Code account

D. Google account

**Answer: B**

**Explanation:**
A service account is an account that belongs to your application instead of to an individual end user. When you run code that is hosted on Cloud Platform, you specify the account that the code should run as. You can create as many service accounts as needed to represent the different logical components of your application.
Reference: https://cloud.google.com/iam/docs/overview

**Question: 279** CertyIQ

Which of the following is not an IAM best practice?

A. Use primitive roles by default

B. Treat each component of your application as a separate trust boundary

C. Grant roles at the smallest scope needed

D. Restrict who has access to create and manage service accounts in your project

**Answer: A**

**Explanation:**
. Treat each component of your application as a separate trust boundary. If you have multiple services that requires different permissions, create a separate service account for each of the services so that they can be permissioned differently.
. Grant primitive roles in the following cases:
.when the Cloud Platform service does not provide a predefined role. See the predefined roles table for a list of all available predefined roles.
.when you want to grant broader permissions for a project. This often happens when youre granting permissions in development or test environments.
.when you need to allow a member to modify permissions for a project, youll want to grant them the owner role because only owners have the permission to grant access to other users for projects.
.when you work in a small team where the team members dont need granular permissions.
. Remember that a policy set on a child resource cannot restrict access granted on its parent.
Check the policy granted on every resource and make sure you understand the hierarchical inheritance.
. Grant roles at the smallest scope needed. For example, if a user only needs access to publish Pub/Sub topic, grant the Publisher role to the user for that topic.
. Restrict who can act as service accounts. Users who are granted the Service Account Actor role for a service account can access all the resources for which the service account has access. Therefore be cautious when granting the Service Account Actor role to a user.
Restrict who has access to create and manage service accounts in your project.
. Granting owner role to a member will allow them to modify the IAM policy. Therefore grant the owner role only if the member has a legitimate purpose to manage the IAM policy. This is because as your policy contains sensitive access control data and having a minimal set of users manage it will simplify any auditing that you may have to do.
Reference: https://cloud.google.com/iam/docs/using-iam-securely

**Question: 280** CertyIQ

Which of the following would not reduce your recovery time in the event of a disaster?

A. Make it as easy as possible to adjust the DNS record to cut over to your warm standby server.

B. Replace your warm standby server with a hot standby server.

C. Use a highly preconfigured machine image for deploying new instances.

D. Replace your active/active hybrid production environment (on-premises and GCP) with a warm standby server.

**Answer: D**

**Explanation:**
An active/active hybrid production environment (on-premises and GCP) can continue running in the event that either the on-premises environment or the GCP deployment fails, so its recovery time would be zero. A warm standby server requires a manual DNS adjustment, so it will always take some time to recover.
Making it easier to do the DNS adjustment will reduce the recovery time for the warm standby model, though.
A hot standby server automatically fails over in the event that the main instance becomes unhealthy, so it has a lower recovery time than a warm standby server, which requires a manual failover.
Typically, the smaller your RTO (Recovery Time Objective) is, the more preconfigured you will want your image to be.
Reference: https://cloud.google.com/solutions/disaster-recovery-cookbook

**Question: 281** CertyIQ

Which of the following is not a best practice for mitigating Denial of Service attacks on your Google Cloud infrastructure?

A. Block SYN floods using Cloud Router

B. Isolate your internal traffic from the external world

C. Scale to absorb the attack

D. Reduce the attack surface for your GCE deployment

**Answer: A**

**Explanation:**
These are all best practices for mitigating Denial of Service attacks:
Reduce the attack surface for your GCE deployment

Scale to absorb the attack -
Isolate your internal traffic from the external world
Cloud Router is used to dynamically update VPN routes. It cannot block SYN floods. On the other hand, Google's Frontend infrastructure, which terminates user traffic, automatically scales to absorb certain types of attacks (e.g., SYN floods) before they reach your compute instances.
Reference: https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf

**Question: 282** CertyIQ

Which is the fastest instance storage option that will still be available when an instance is stopped?

A. Local SSD

B. Standard Persistent Disk

C. SSD Persistent Disk

D. RAM disk

**Answer: C**

**Explanation:**
Local SSDs and RAM disks disappear when you stop an instance. Standard Persistent Disks and SSD Persistent Disks both survive when you stop an instance, but SSD Persistent Disks have up to 4 times the throughput and up to 40 times the I/O operations per second of a Standard Persistent Disk.
Reference: https://cloud.google.com/compute/docs/disks/

**Question: 283** CertyIQ

Which of these statements about Microsoft licenses is true?

A. You can migrate your existing Microsoft application licenses to Compute Engine instances, but not your Microsoft Windows licenses.

B. You can migrate your existing Microsoft Windows and Microsoft application licenses to Compute Engine instances.

C. You cannot migrate your existing Microsoft Windows or Microsoft application licenses to Compute Engine instances.

D. You can migrate your existing Microsoft Windows licenses to Compute Engine instances, but not your Microsoft application licenses.

**Answer: B**

**Explanation:**

Answer is B.

You can bring your existing Windows Server licenses to Compute Engine using Bring your own license with sole-tenant nodes or bring your existing Microsoft application licenses to your Windows Server instances to run specific applications. However, you must continue to manage those licenses yourself.

Reference:

https://cloud.google.com/compute/docs/instances/windows/

**Question: 284** CertyIQ

Which database services support standard SQL queries?

A. Cloud Bigtable and Cloud SQL

B. Cloud Spanner and Cloud SQL

C. Cloud SQL and Cloud Datastore

D. Cloud SQL

**Answer: B**

**Explanation:**
Cloud SQL is a managed service for MySQL and PostgreSQL, which both support SQL queries. Cloud Spanner supports SQL queries. Cloud Bigtable and Cloud
Datastore are NoSQL databases.
Reference: https://cloud.google.com/products/storage/

**Question: 285** CertyIQ

Which statement about IP addresses is false?

A. You are charged for a static external IP address for every hour it is in use.
B. You are not charged for ephemeral IP addresses.
C. Google Cloud Engine supports only IPv4 addresses, not IPv6.
D. You are charged for a static external IP address when it is assigned but unused.

**Answer: B**

**Explanation:**

Answer is B

https://cloud.google.com/compute/all-pricing#ipaddress

Type Price/Hours(USD)

Static IP address (assigned but unused) $0.010

Static and ephemeral IP addresses in use on standard VM instances $0.004*

*Promotion: Charges between January 1st, 2020 and March 31st, 2020 are waived.

Static and ephemeral IP addresses in use on preemptible VM instances $0.002*

*Promotion: Charges between January 1st, 2020 and March 31st, 2020 are waived.

Static and ephemeral IP addresses attached to forwarding rules No charge

**Question: 286** CertyIQ

Which Google Cloud Platform service requires the least management because it takes care of the underlying infrastructure for you?

A. Container Engine
B. Cloud Engine
C. App Engine
D. Docker containers running on Cloud Engine

**Answer: C**

**Explanation:**
App Engine is great for running web-based apps, line of business apps, and mobile backends. Compute Engine is great for when you need more control of the underlying infrastructure.
Container Engine is in between because it gives you control of the containers running on top of Compute Engine.

Reference:
https://cloud.google.com/compute/docs/faq#how_do_google_app_engine_and_product_name_relate_to_each_other

**Question: 287** CertyIQ

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

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

**Answer: D**

**Explanation:**
To account for the extreme case where one zone fails or an entire group of instances stops responding, Compute Engine strongly recommends overprovisioning your managed instance group by at least 50%. Spreading instances across three zones already helps you preserve at least 2/3 of your serving capacity and the other two zones in the region can continue to serve traffic without interruption. By overprovisioning to 150%, you can ensure that if 1/3 of the capacity is lost, 100% of traffic is supported by the remaining zones. You need to select the "Multizone" option (or the --region flag if you're using the gcloud command) when creating a managed instance group.
It is only possible to create regional managed instance groups. You cannot create regional unmanaged instance groups.

Reference:
https://cloud.google.com/compute/docs/instance-groups/distributing-instances-with-regional-instance- groups#provisioning_the_correct_managed_instance_group_size

**Question: 288** CertyIQ

If you do not grant a user named Bob permission to access a Cloud Storage bucket, but then use an ACL to grant access to an object inside that bucket to Bob, what will happen?

A. Bob will be able to access all of the objects inside the bucket because he was granted access to at least one object in the bucket.
B. Bob will be able to access the object because bucket and object ACLs are independent of each other.
C. Bob will not be able to access the object because he does not have access to the bucket.
D. It is not possible to grant access to an object when it is inside a bucket for which a user does not have access.

**Answer: B**

**Explanation:**
Bucket and object ACLs are independent of each other, which means that the ACLs on a bucket do not affect the ACLs on objects inside that bucket. It is possible for a user without permissions for a bucket to have permissions for an object inside the bucket. For example, you can create a bucket such that only GroupA is granted permission to list the objects in the bucket, but then upload an object into that bucket that allows GroupB READ access to the object. GroupB will be able to read the object, but will not be able to view the contents of the bucket or perform bucket-related tasks.
Reference: https://cloud.google.com/storage/docs/best-practices#security

**Question: 289** CertyIQ

To set up a virtual private network between your office network and Google Cloud Platform and have the routes automatically updated when the network topology changes, what is the minimal number of each type of

component you need to implement?

A. 2 Cloud VPN Gateways and 1 Peer Gateway
B. 1 Cloud VPN Gateway, 1 Peer Gateway, and 1 Cloud Router
C. 2 Peer Gateways and 1 Cloud Router
D. 2 Cloud VPN Gateways and 1 Cloud Router

**Answer: B**

**Explanation:**
VPC networks allow you to regionally segment the network IP space into prefixes (subnets) and control which prefix a VM instance's internal IP address is allocated from. If you want to avoid statically managing these subnets including the burden of adding and removing related static routes for your VPN, you can do so by enabling dynamic routing for your VPNs using Cloud Router.
The diagram at https://cloud.google.com/compute/images/cloudrouter/cr-w-subnets.svg shows a VPN Gateway, a Peer Gateway, and a Cloud Router.

Reference:
https://cloud.google.com/compute/docs/cloudrouter#cloud_router_for_vpns_with_vpc_networks

**Question: 290** CertyIQ

Which of the following statements about encryption on GCP is not true?

A. Google Cloud Platform encrypts customer data stored at rest by default.
B. Each encryption key is itself encrypted with a set of master keys.
C. If you want to manage your own encryption keys for data on Google Cloud Storage, the only option is Customer-Managed Encryption Keys (CMEK) using Cloud KMS.
D. Data in Google Cloud Platform is broken into subfile chunks for storage, and each chunk is encrypted at the storage level with an individual encryption key.

**Answer: C**

**Explanation:**
There are 3 ways to manage your own encryption keys when using Google :
. Customer-managed encryption keys (CMEK) using Cloud KMS allow you to manage your own keys that are hosted on GCP.
. Customer-supplied encryption keys (CSEK) allow you to manage your own keys on premise, but still use them on GCP.
. With client-side encryption, you encrypt the data before you send it to GCP.
Google Cloud Platform encrypts customer data stored at rest by default, with no additional action required from you.
Data in Google Cloud Platform is broken into subfile chunks for storage, and each chunk is encrypted at the storage level with an individual encryption key. The key used to encrypt the data in a chunk is called a data encryption key (DEK). Because of the high volume of keys at Google, and the need for low latency and high availability, these keys are stored near the data that they encrypt. The DEKs are encrypted with (or "wrapped" by) a key encryption key (KEK).
Customers can choose which key management solution they prefer for managing the KEKs that protect the DEKs that protect their data.
Reference: https://cloud.google.com/security/encryption-at-rest/

**Question: 291** CertyIQ

Which database service requires that you configure a failover replica to make it highly available?

A. Cloud Spanner
B. Cloud SQL
C. BigQuery
D. Cloud Datastore

**Answer: B**

**Explanation:**
Cloud Datastore, Cloud Spanner, and BigQuery are all horizontally scalable and are automatically replicated to multiple zones. Since Cloud SQL is not horizontally scalable, you must configure a failover replica to make it highly available.
Reference: https://cloud.google.com/sql/docs/mysql/configure-ha

**Question: 292** CertyIQ

Which of these is not a principle you should apply when setting roles and permissions?

A. Whenever possible, assign roles to groups instead of to individuals.
B. Grant users the appropriate permissions to facilitate least privilege
C. Whenever possible, assign primitive roles rather than predefined roles.
D. Audit all policy changes by checking the Cloud Audit Logs.

**Answer: C**

**Explanation:**
Predefined roles provide more granular access than the primitive roles. Grant predefined roles to identities when possible, so you only give the least amount of access necessary to access your resources.
Reference: https://cloud.google.com/iam/docs/using-iam-securely

**Question: 293** CertyIQ

Which of these is not a recommended method of authenticating an application with a Google Cloud service?

A. Use the gcloud and/or gsutil commands.
B. Request an OAuth2 access token and use it directly.
C. Embed the service account's credentials in the application's source code.
D. Use one of the Google Cloud Client Libraries.

**Answer: C**

**Explanation:**
Do not embed secrets related to authentication in source code, such as API keys, OAuth tokens, and service account credentials.
Authenticating applications using service account credentials
Client libraries can use Application Default Credentials to authenticate with Google APIs and send requests to those APIs.
For some applications, you might need to request an OAuth2 access token and use it directly without going

through a client library or using the gcloud or gsutil tools.
Some applications might use commands from the gcloud and gsutil tools, which are included by default in most Compute Engine images. These tools automatically recognize an instance's service account and relevant permissions granted to the service account.
Reference: https://cloud.google.com/docs/authentication#token_lifecycle_management

**Question: 294** CertyIQ

What are two different features that fully isolate groups of VM instances?

A. Firewall rules and subnetworks
B. Networks and subnetworks
C. Subnetworks and projects
D. Projects and networks

**Answer: D**

**Explanation:**
Google uses software-defined networking that enables you to subject every packet to security checks, thereby enabling complete isolation of Cloud Platform projects.
Networks within projects are used to isolate groups of VM instances.
Subnetworks on Compute Engine enable you to control the address space in which VM instances are created, while maintaining the ability to route between them.
Firewall rules only restrict incoming network traffic. They cannot restrict outgoing network traffic.

Reference:
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#use_projects_to_fully_isolate_resources

**Question: 295** CertyIQ

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

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

**Answer: ABC**

**Explanation:**
If you modify your firewall rules, it could prevent traffic from flowing to your VM.
You can't attach the VM instance's disk to a new instance without detaching it from the existing instance first, which would require shutting down the instance.
If you create a startup script to collect information, you will have to restart your VM instance to run the script.
You can view the serial console output without disrupting traffic. Running commands in the interactive serial console, on the other hand, could disrupt operations.
Connecting to port 22 using netcat will only affect the SSH server on the VM, since that is the only service that listens on port 22.
You can create a snapshot of a VM instance's disk without disrupting the VM's operation.

Reference:
https://cloud.google.com/compute/docs/troubleshooting#ssherrors

**Question: 296** CertyIQ

To configure Stackdriver to monitor a web server and let you know if it goes down, what steps do you need to take? (Select 2 answers.)

A. Install the Stackdriver Logging Agent on the web server
B. Create an alerting policy
C. Install the Stackdriver Monitoring Agent on the web server
D. Create an uptime check

**Answer: BD**

**Explanation:**
Uptime checks verify that your web server is always accessible. The alerting policy controls who is notified if the uptime checks should fail.
You don't need to install the Stackdriver Monitoring Agent to get downtime alerts. The agent provides additional information, but it's not required. The Stackdriver
Logging Agent is for additional logging, not for alerts.
Using the Monitoring agent is optional. Stackdriver Monitoring can access some metrics without the Monitoring agent, including CPU utilization, some disk traffic metrics, network traffic, and uptime information.
[https://cloud.google.com/monitoring/agent/#purpose]
Reference: https://cloud.google.com/monitoring/quickstart-lamp#gs-checks

**Question: 297** CertyIQ

Which of these tools can you use to copy data from AWS S3 to Cloud Storage? (Select 2 answers.)

A. Cloud Storage Transfer Service
B. S3 Storage Transfer Service
C. Cloud Storage Console
D. gsutil

**Answer: AD**

**Explanation:**
Cloud Storage Transfer Service transfers data from an online data source to a data sink. Your data source can be an Amazon Simple Storage Service (Amazon
S3) bucket, an HTTP/HTTPS location, or a Google Cloud Storage bucket. Your data sink (the destination) is always a Google
Cloud Storage bucket.
You can use Cloud Storage Transfer Service to:
Back up data to a Google Cloud Storage bucket from other storage providers.
Move data from a Multi-Regional Storage bucket to a Nearline Storage bucket to lower your storage costs.
Reference: https://cloud.google.com/storage/transfer/

**Question: 298** CertyIQ

What are two of the actions you can take to troubleshoot a virtual machine instance that won't start up at all? (Select 2 answers.)

A. Increase the CPU and memory on the instance by changing the machine type.
B. Validate that your disk has a valid file system.
C. Examine your virtual machine instance's serial port output.
D. Connect to your virtual machine instance using SSH.

**Answer: BC**

**Explanation:**
Here are some tips to help troubleshoot your persistent boot disk if it doesn't boot.
Examine your virtual machine instance's serial port output.
An instance's BIOS, bootloader, and kernel will print their debug messages into the instance's serial port output, providing valuable information about any errors or issues that the instance experienced.
Enable interactive access to the serial console.
You can enable interactive access to an instance's serial console so you can log in and debug boot issues from within the instance, without requiring your instance to be fully booted.
Validate that your disk has a valid file system.
If your file system is corrupted or otherwise invalid, you won't be able to launch your instance.
Validate that the disk has a valid master boot record (MBR).
If your virtual machine won't boot at all, then you can't use SSH to connect to it because the SSH server on the VM won't be running.
Increasing the CPU and memory on the instance might help if the VM boots partway, but not if it can't boot at all.
Reference: https://cloud.google.com/compute/docs/troubleshooting#pdboot

**Question: 299** CertyIQ

Which statements about application load testing are true? (Select 2 answers.)

A. You should test at the maximum load that you expect to encounter.
B. You should test at 50% more than the maximum load that you expect to encounter.
C. It is not necessary to test sudden increases in traffic since GCP scales seamlessly.
D. Your load tests should include testing sudden increases in traffic.

**Answer: AD**

**Explanation:**
Your tests should be designed to simulate real world traffic as closely as possible. You should test at the maximum load that you expect to encounter.
In addition, some applications will get a sudden increase in load, and you will need to predict the rate of increase. If you are expecting spikey load, you should also test how your application performs when traffic suddenly increases.
Although GCP services scale quickly, they do not scale instantaneously, which is why you should test sudden increases in traffic.
Reference: https://cloud.google.com/appengine/articles/scalability#loadtesting

**Question: 300** CertyIQ

Which of these statements about resilience testing are true? (Select 2 answers.)

A. In a resilience test, your application should keep running with little or no downtime.

B. To test the resilience of an autoscaling instance group, you can terminate a random instance within that group.

C. In order for an application to survive instance failures, it should not be stateless.

D. Resilience testing is the same as disaster recovery testing.

**Answer: AB**

**Explanation:**
Resilience testing is similar to disaster recovery testing because youre testing what happens when infrastructure fails, but the difference is that in resilience testing, youre expecting your application to keep running, with little or no downtime. With disaster recovery testing, some downtime is expected.
One common testing scenario is to terminate a random instance within an autoscaling instance group. Netflix created software called Chaos Monkey that automates this sort of testing. If your application in the autoscaling instance group is stateless, then it should be able to survive this sort of failure without any noticeable impact on users.
Reference: https://cloudacademy.com/google/managing-your-google-cloud-infrastructure-course/testing.html

**Question: 301** CertyIQ

Which combination of Stackdriver services will alert you about errors generated by your applications and help you locate the root cause in the code?

A. Monitoring, Trace, and Debugger

B. Monitoring and Error Reporting

C. Debugger and Error Reporting

D. Alerts and Debugger

**Answer: C**

**Explanation:**
Stackdriver Error Reporting keeps track of errors in your applications and can be configured to alert you when an error occurs.
Stackdriver Debugger lets you inspect the state of an application at any code location. If you click on an error displayed in Error Reporting, it will put you into the associated application's source code in the Debugger so you can diagnose the problem.
Stackdriver Monitoring gives real-time updates on performance metrics and uptime, not application errors. There is no service called Stackdriver Alerts, although alerting is a capability of Stackdriver Monitoring.
Stackdriver Trace collects latency data from your applications. It is useful for locating performance bottlenecks, not application errors.
Reference: https://cloud.google.com/products/

**Question: 302** CertyIQ

If you have configured Stackdriver Logging to export logs to BigQuery, but logs entries are not getting exported to BigQuery, what is the most likely cause?

A. The Cloud Data Transfer Service has not been enabled.

B. There isn't a firewall rule allowing traffic between Stackdriver and BigQuery.

C. Stackdriver Logging does not have permission to write to the BigQuery dataset.

D. The size of the Stackdriver log entries being exported exceeds the maximum capacity of the BigQuery dataset.

**Answer: C**

**Explanation:**
When you create a sink, Stackdriver Logging creates a new service account for the sink, called a unique writer identity.
In order to write logs to a BigQuery dataset, you must grant the sink's writer identity either Can edit permission or the Writer role.
It is not necessary to create a firewall rule to allow traffic between Stackdriver and BigQuery.
The Cloud Data Transfer Service is for importing data to Google Cloud Platform from an external source.
BigQuery can easily handle any volume of Stackdriver logs.
Reference:
https://cloud.google.com/logging/docs/export/configure_export_v2#errors_exporting_to_bigquery

**Question: 303** CertyIQ

You can use Stackdriver to monitor virtual machines on which cloud platforms?

A. Google Cloud Platform, Microsoft Azure

B. Google Cloud Platform

C. Google Cloud Platform, Microsoft Azure, Amazon Web Services

D. Google Cloud Platform, Amazon Web Services

**Answer: C**

**Explanation:**

C is correct We're pleased to announce that you can now join our new offering for Blue Medora. If you're using Stackdriver to monitor your Google Cloud Platform (GCP) or Amazon Web Services (AWS) resources, you can now extend your observability to on-prem infrastructure, Microsoft Azure, databases, hardware devices and more. The recently released BindPlane integration from Blue Medora lets you consolidate all your signals into Stackdriver, GCP's monitoring tool.

https://cloud.google.com/blog/products/management-tools/extending-stackdriver-to-on-prem-with-the-newbindplane-integration

**Question: 304** CertyIQ

To minimize the risk of someone changing your log files to hide their activities, which of the following principles would help? (Select 3 answers.)

A. Restrict usage of the owner role for projects and log buckets.

B. Require two people to inspect the logs.

C. Implement object versioning on the log-buckets.

D. Encrypt the logs using Cloud KMS.

**Answer: ACD**

**Explanation:**

ACD for me. Seems B is only monitoring the logs but not restricting it. D can be correct because we can encrypt it with KMS and provide access to the KMS key with certain Predefined roles like roles/cloudkms.cryptoKeyDecrypter and roles/cloudkms.cryptoKeyEncrypter only to authorized members or service account

**Question: 305** CertyIQ

If network traffic between one Google Compute Engine instance and another instance is being dropped, what is the most likely cause?

A. The instances are on a network with low bandwidth.
B. The TCP keep-alive setting is too short.
C. The instances are on a default network with no additional firewall rules.
D. A firewall rule was deleted.

**Answer: D**

**Explanation:**
Google Compute Engine (GCE) only allows network traffic that is explicitly permitted by your project's firewall rules to reach your instance. By default, all projects automatically come with a default network that allows certain kinds of connections. If you delete one of the default network firewall rules, then the associated traffic will no longer be allowed.
Dropped traffic can be caused by the TCP keep-alive setting being too long, not by being too short.
All GCE instances have high-bandwidth connections.
Reference: https://cloud.google.com/compute/docs/troubleshooting#networktraffic

**Question: 306** CertyIQ

Which of the following practices can help you develop more secure software? (Select 3 answers.)

A. Penetration tests
B. Integrating static code analysis tools into your CI/CD pipeline
C. Encrypting your source code
D. Peer review of code

**Answer: ABD**

**Explanation:**
There are four basic techniques for analyzing the security of a software application - automated scanning, manual penetration testing, static analysis, and manual code review.
Despite the many claims that code review is too expensive or time consuming, there is no question that it is the fastest and most accurate way to find and diagnose many security problems. There are also dozens of serious security problems that simply can't be found any other way.
Encrypting your source code might help with keeping it out of the hands of hackers, but it won't help you develop more secure software.
Reference: https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf

**Question: 307** CertyIQ

Which two places hold information you can use to monitor the effects of a Cloud Storage lifecycle policy on

specific objects? (Select 2 answers.)

A. Cloud Storage Lifecycle Monitoring
B. Expiration time metadata
C. Access logs
D. Lifecycle config file

**Answer: BC**

**Explanation:**
If a Delete action is specified for a bucket with the Age condition (and no NumberOfNewerVersions condition), then some objects may be tagged with expiration time metadata. An object's expiration time indicates the time at which the object becomes (or became) eligible for deletion by Object Lifecycle Management. The expiration time may change as the bucket's lifecycle configuration changes.
To find out what lifecycle management actions have been taken, you can enable access logs for your bucket. A value of "GCS Lifecycle Management" in the
"cs_user_agent" field in the log entry indicates the action was taken by Google Cloud Storage based on the lifecycle configuration.
A lifecycle config file is used to configure a lifecycle policy, but it does not contain information about how that policy has affected specific objects.
There is no service called "Cloud Storage Lifecycle Monitoring".
Reference: https://cloud.google.com/storage/docs/lifecycle#expirationtime

**Question: 308** CertyIQ

If you have object versioning enabled on a multi-regional bucket, what will the following lifecycle config file do?
"lifecycle":
"rule": [
"action": "type": "Delete" ,
"condition":
"age": 30,
"isLive": true ,
"action":
"type": "SetStorageClass",
"storageClass": "COLDLINE" ,
"condition":
"age": 365,
"matchesStorageClass": ["MULTI_REGIONAL"] ]

A. Archive objects older than 30 days (the second rule doesn't do anything)
B. Delete objects older than 30 days (the second rule doesn't do anything)
C. Archive objects older than 30 days and move objects to Coldline Storage after 365 days
D. Delete objects older than 30 days and move objects to Coldline Storage after 365 days

**Answer: C**

**Explanation:**
If object versioning is enabled and the Delete rule has an "isLive:true" condition, then objects will be archived rather than deleted. If object versioning is disabled, then the first rule would actually delete objects after 30 days and the second rule would never match any objects. The question says that object versioning is enabled, so that's not the case.
The second rule moves objects older than 365 days from Multi-Regional Storage to Coldline Storage. Since all live objects are archived after 30 days, only archived objects will be old enough to be moved by this rule. Also, since this is a Multi-Regional bucket, this rule will match all archived objects older than 365 days (other than those that have already been moved to Coldline Storage).

Reference: https://cloud.google.com/storage/docs/managing-lifecycles

**Question: 309** CertyIQ

Which of the following statements about Stackdriver Trace are true? (Select 2 answers.)

A. Stackdriver Trace tracks the performance of the virtual machines running the application.

B. Stackdriver Trace tracks the latency of incoming requests.

C. Applications in App Engine automatically submit traces to Stackdriver Trace. Applications outside of App Engine need to use the Trace SDK or Trace API.

D. To make an application work with Stackdriver Trace, you need to add instrumentation code using the Trace SDK or Trace API, even if the application is in App

**Answer: BC**

**Explanation:**

By default, Stackdriver Trace collects data from any Google App Engine application where the feature is enabled. For other applications, use the Stackdriver
Trace API [either directly or through the Trace SDK] to send latency data to Stackdriver Trace.
[https://cloud.google.com/trace/docs/reference]
Stackdriver Trace helps you understand how long it takes your application to handle incoming requests from users or other applications, and how long it takes to complete operations like RPC calls performed when handling the requests. [https://cloud.google.com/trace/docs/overview]
Reference: https://cloud.google.com/trace/docs/reference

**Question: 310** CertyIQ

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**

**Explanation:**

B Authentication function to function calls. Add calling function service account as a member on the receiving function and grant that member the cloud functions invoker

https://cloud.google.com/functions/docs/securing/authenticating

**Question: 311** CertyIQ

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**

**Explanation:**

B is the answer.https://cloud.google.com/load-balancing/docs/negs/serverless-neg-conceptsA serverless NEG is a backend that points to a Cloud Run, App Engine, Cloud Functions, or API Gateway service.

**Question: 312** CertyIQ

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**

**Explanation:**

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

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

**Question: 313** CertyIQ

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**

**Explanation:**

Cloud monitoring for Uptime check to validate the application URL and leverage pub/sub to trigger Cloud Function to switch URL

https://cloud.google.com/monitoring/uptime-checks?hl=en

**Question: 314** CertyIQ

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**

**Explanation:**

Google Cloud has two services for storing and managing container images such as Artifact Registry and Container Registry.

https://cloud.google.com/container-registry/docs/overview

**Question: 315** CertyIQ

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**

**Explanation:**

Answer is A.

https://cloud.google.com/transfer-appliance/docs/4.0/overview#location-availability

With a typical network bandwidth of 100 Mbps, one petabyte of data takes about 3 years to upload. However, with Transfer Appliance, you can receive the appliance and capture a petabyte of data in under 25 days. Your data can be accessed in Cloud Storage within another 25 days, all without consuming any outbound network bandwidth.

with 1GBps - online STS will take 124 days ..

**Question: 316** CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a website and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a premium app model.

Company Background -
Dress4Win's application has grown from a few servers in the founder's garage to several hundred servers and appliances in a collocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster, Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is considering moving their development and test environments. They are also considering building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location.
Databases:
- MySQL - user data, inventory, static data
- Redis - metadata, social graph, caching
Application servers:
- Tomcat - Java micro-services
- Nginx - static content
- Apache Beam - Batch processing
Storage appliances:
- iSCSI for VM hosts
- Fiber channel SAN - MySQL databases
- NAS - image storage, logs, backups
Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
MQ servers:
- Messaging
- Social notifications

- Events
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.
Migrate fully to the cloud if all other requirements are met.

Technical Requirements -
Evaluate and choose an automation framework for provisioning resources in cloud.
Support failover of the production environment to cloud during an emergency.
Identify production services that can migrate to cloud to save capacity.
Use managed services whenever possible.
Encrypt data on the wire and at rest.
Support multiple VPN connections between the production data center and cloud environment.

CEO Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a new competitor could use a public cloud platform to offset their up-front investment and freeing them to focus on developing better features.

CTO Statement -
We have invested heavily in the current infrastructure, but much of the equipment is approaching the end of its useful life. We are consistently waiting weeks for new gear to be racked before we can start new projects. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.

CFO Statement -
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost of ownership (TCO) analysis over the next 5 years puts a cloud strategy between 30 to 50% lower than our current model.QuestionThe Dress4Win security team has disabled external SSH access into production virtual machines (VMs) on Google Cloud Platform (GCP).
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 operations engineer access to use Google Cloud Shell.

B.Configure a VPN connection to GCP 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**

**Explanation:**

Grant the operations engineer access to use Google Cloud Shell.

**Question: 317** CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a website and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a premium app model.

Company Background -
Dress4Win's application has grown from a few servers in the founder's garage to several hundred servers and appliances in a collocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster, Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is considering moving their development and test environments. They are also considering building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location.
Databases:
- MySQL - user data, inventory, static data
- Redis - metadata, social graph, caching
Application servers:
- Tomcat - Java micro-services
- Nginx - static content
- Apache Beam - Batch processing
Storage appliances:
- iSCSI for VM hosts
- Fiber channel SAN - MySQL databases
- NAS - image storage, logs, backups
Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
MQ servers:
- Messaging
- Social notifications
- Events
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.
Migrate fully to the cloud if all other requirements are met.

Technical Requirements -
Evaluate and choose an automation framework for provisioning resources in cloud.
Support failover of the production environment to cloud during an emergency.
Identify production services that can migrate to cloud to save capacity.
Use managed services whenever possible.
Encrypt data on the wire and at rest.
Support multiple VPN connections between the production data center and cloud environment.

CEO Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a new competitor could use a public cloud platform to offset their up-front investment and freeing them to focus on developing better features.

CTO Statement -
We have invested heavily in the current infrastructure, but much of the equipment is approaching the end of its useful life. We are consistently waiting weeks for new gear to be racked before we can start new projects. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.

CFO Statement -
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost

of ownership (TCO) analysis over the next 5 years puts a cloud strategy between 30 to 50% lower than our current model.QuestionAt Dress4Win, an operations engineer wants to create a tow-cost solution to remotely archive copies of database backup files.
The database files are compressed tar files stored in their current data center.
How should he proceed?

A.Create a cron script using gsutil to copy the files to a Coldline Storage bucket.

B.Create a cron script using gsutil to copy the files to a Regional Storage bucket.

C.Create a Cloud Storage Transfer Service Job to copy the files to a Coldline Storage bucket.

D.Create a Cloud Storage Transfer Service job to copy the files to a Regional Storage bucket.

**Answer: C**

**Explanation:**

C https://cloud.google.com/storage-transfer/docs/on-prem-overviewEspecially, when Google docs explicitly states, that custom scripts are unreliable, slow, insecure, difficult to maintain and troubleshoot.

**Question: 318** CertyIQ

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**

**Explanation:**

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.

**Question: 319** CertyIQ

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 ebb 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: C**

**Explanation:**

Monitoring, Logging, Alerts, Error Reporting.

**Question: 320** CertyIQ

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 advise?

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: A**

**Explanation:**

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

**Question: 321** CertyIQ

Dress4Win has asked you for advice on how to migrate their on-premises MySQL deployment to the cloud. They want to minimize downtime and performance impact to their on-premises solution during the migration.
Which approach should you recommend?

A.Create a dump of the on-premises MySQL master server, and then shut it down, upload it to the cloud environment, and load into a new MySQL cluster.

B.Setup a MySQL replica server/slave in the cloud environment, and configure it for asynchronous replication from the MySQL master server on-premises until cutover.

C.Create a new MySQL cluster in the cloud, configure applications to begin writing to both on premises and cloud MySQL masters, and destroy the original cluster at cutover.

D.Create a dump of the MySQL replica server into the cloud environment, load it into: Google Cloud Datastore, and configure applications to read/write to Cloud Datastore at cutover.

**Answer: B**

**Explanation:**

Setup a MySQL replica server/slave in the cloud environment, and configure it for asynchronous replication from the MySQL master server on-premises until cutover.

**Question: 322** CertyIQ

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 rule

C.Configure their load balancer to pass through the User-Agent HTTP header when the value matches GoogleStackdriverMonitoring-UptimeChecks (https:// cloud.google.com/monitoring)

D.Configure their legacy web servers to allow requests that contain user-Agent HTTP header when the value matches GoogleStackdriverMonitoring- UptimeChecks (https://cloud.google.com/monitoring)

**Answer: D**

**Explanation:**

D. Configure their legacy web servers to allow requests that contain the User-Agent HTTP header when the value matches GoogleStackdriverMonitoring-UptimeChecks (https://cloud.google.com/monitoring). Google Cloud Monitoring uptime checks use a specific User-Agent (GoogleStackdriverMonitoring-UptimeChecks) to make health checks on services. If the legacy web servers are not configured to accept these requests or block certain User-Agent headers, they will reject the checks, causing them to be reported as unhealthy.By configuring the legacy web servers to allow traffic from uptime checks that include the proper User-Agent header, Dress4Win ensures that the uptime check traffic can reach the services, allowing Google Monitoring to report accurate health status.

**Question: 323** CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a website and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a premium app model.

Company Background -
Dress4Win's application has grown from a few servers in the founder's garage to several hundred servers and appliances in a collocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster,
Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is considering moving their development and test environments. They are also considering building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location.
Databases:
- MySQL - user data, inventory, static data
- Redis - metadata, social graph, caching
Application servers:
- Tomcat - Java micro-services
- Nginx - static content
- Apache Beam - Batch processing
Storage appliances:
- iSCSI for VM hosts
- Fiber channel SAN - MySQL databases

- NAS - image storage, logs, backups
Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
MQ servers:
- Messaging
- Social notifications
- Events
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.
Migrate fully to the cloud if all other requirements are met.

Technical Requirements -
Evaluate and choose an automation framework for provisioning resources in cloud.
Support failover of the production environment to cloud during an emergency.
Identify production services that can migrate to cloud to save capacity.
Use managed services whenever possible.
Encrypt data on the wire and at rest.
Support multiple VPN connections between the production data center and cloud environment.

CEO Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a new competitor could use a public cloud platform to offset their up-front investment and freeing them to focus on developing better features.

CTO Statement -
We have invested heavily in the current infrastructure, but much of the equipment is approaching the end of its useful life. We are consistently waiting weeks for new gear to be racked before we can start new projects. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.

CFO Statement -
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost of ownership (TCO) analysis over the next 5 years puts a cloud strategy between 30 to 50% lower than our current model.QuestionAs part of their new application experience, Dress4Wm allows customers to upload images of themselves.
The customer 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 ID, 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**

**Explanation:**

A is correct. The whole idea is simply build and maintain an external metadata service using NoSQL database to associate the GS object key with its metadata, in order to facilitate object findings based on attributes you pre defined in metatdataThis AWS blog provides a solution in the context of AWS S3, but the idea behind is applicable to Google Storage as well

https://aws.amazon.com/blogs/big-data/building-and-maintaining-an-amazon-s3-metadata-index-without-servers/

**Question: 324** CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a website and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a premium app model.

Company Background -
Dress4Win's application has grown from a few servers in the founder's garage to several hundred servers and appliances in a collocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster,
Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is considering moving their development and test environments. They are also considering building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location.
Databases:
- MySQL - user data, inventory, static data
- Redis - metadata, social graph, caching
Application servers:
- Tomcat - Java micro-services
- Nginx - static content
- Apache Beam - Batch processing
Storage appliances:
- iSCSI for VM hosts
- Fiber channel SAN - MySQL databases
- NAS - image storage, logs, backups
Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
MQ servers:
- Messaging
- Social notifications
- Events
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.
Migrate fully to the cloud if all other requirements are met.

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

Support failover of the production environment to cloud during an emergency.
Identify production services that can migrate to cloud to save capacity.
Use managed services whenever possible.
Encrypt data on the wire and at rest.
Support multiple VPN connections between the production data center and cloud environment.

CEO Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a new competitor could use a public cloud platform to offset their up-front investment and freeing them to focus on developing better features.

CTO Statement -
We have invested heavily in the current infrastructure, but much of the equipment is approaching the end of its useful life. We are consistently waiting weeks for new gear to be racked before we can start new projects. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.

CFO Statement -
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost of ownership (TCO) analysis over the next 5 years puts a cloud strategy between 30 to 50% lower than our current model.QuestionDress4Win 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: B**

**Explanation:**

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

**Question: 325** CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a website and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a premium app model.

Company Background -
Dress4Win's application has grown from a few servers in the founder's garage to several hundred servers and appliances in a collocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster,
Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is considering moving their development and test environments. They are also considering building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location.
Databases:

- MySQL - user data, inventory, static data
- Redis - metadata, social graph, caching
Application servers:
- Tomcat - Java micro-services
- Nginx - static content
- Apache Beam - Batch processing
Storage appliances:
- iSCSI for VM hosts
- Fiber channel SAN - MySQL databases
- NAS - image storage, logs, backups
Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
MQ servers:
- Messaging
- Social notifications
- Events
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.
Migrate fully to the cloud if all other requirements are met.

Technical Requirements -
Evaluate and choose an automation framework for provisioning resources in cloud.
Support failover of the production environment to cloud during an emergency.
Identify production services that can migrate to cloud to save capacity.
Use managed services whenever possible.
Encrypt data on the wire and at rest.
Support multiple VPN connections between the production data center and cloud environment.

CEO Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a new competitor could use a public cloud platform to offset their up-front investment and freeing them to focus on developing better features.

CTO Statement -
We have invested heavily in the current infrastructure, but much of the equipment is approaching the end of its useful life. We are consistently waiting weeks for new gear to be racked before we can start new projects. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.

CFO Statement -
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost of ownership (TCO) analysis over the next 5 years puts a cloud strategy between 30 to 50% lower than our current model.QuestionYou want to ensure Dress4Win's sales and tax records remain available for infrequent viewing by auditors for at least 10 years.
Cost optimization is your top priority.
Which cloud services should you choose?

A.Google Cloud Storage Coldline to store the data, and gsutil to access the data.

B.Google Cloud Storage Nearline to store the data, and gsutil to access the data.

C.Google Bigtabte with US or EU as location to store the data, and gcloud to access the data.

D.BigQuery to store the data, and a web server cluster in a managed instance group to access the data. Google Cloud SQL mirrored across two distinct regions to store the data, and a Redis cluster in a managed instance group to access the data.

**Answer: A**

**Explanation:**

A, because when you read documentation both of them (nearline and coldline) you can see the expresion infrecuent access. And in this case, your priority is the cost, and you are going to sabe 10 years

Reference:

https://cloud.google.com/storage/docs/storage-classes

**Question: 326** CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a website and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a premium app model.

Company Background -
Dress4Win's application has grown from a few servers in the founder's garage to several hundred servers and appliances in a collocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster, Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is considering moving their development and test environments. They are also considering building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location.
Databases:
- MySQL - user data, inventory, static data
- Redis - metadata, social graph, caching
Application servers:
- Tomcat - Java micro-services
- Nginx - static content
- Apache Beam - Batch processing
Storage appliances:
- iSCSI for VM hosts
- Fiber channel SAN - MySQL databases
- NAS - image storage, logs, backups
Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
MQ servers:
- Messaging
- Social notifications
- Events
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.
Migrate fully to the cloud if all other requirements are met.

Technical Requirements -
Evaluate and choose an automation framework for provisioning resources in cloud.
Support failover of the production environment to cloud during an emergency.
Identify production services that can migrate to cloud to save capacity.
Use managed services whenever possible.
Encrypt data on the wire and at rest.
Support multiple VPN connections between the production data center and cloud environment.

CEO Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a new competitor could use a public cloud platform to offset their up-front investment and freeing them to focus on developing better features.

CTO Statement -
We have invested heavily in the current infrastructure, but much of the equipment is approaching the end of its useful life. We are consistently waiting weeks for new gear to be racked before we can start new projects. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.

CFO Statement -
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost of ownership (TCO) analysis over the next 5 years puts a cloud strategy between 30 to 50% lower than our current model.QuestionThe 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 its system architecture to multiple locations when Google cloud platform.
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**

**Explanation:**

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.

**Question: 327**

CertyIQ

Introductory InfoCompany Overview -
Dress4Win is a web-based company that helps their users organize and manage their personal wardrobe using a web app and mobile application. The company also cultivates an active social network that connects their users with designers and retailers. They monetize their services through advertising, e-commerce, referrals, and a freemium app model. The application has grown from a few servers in the founder's garage to several hundred servers and appliances in a colocated data center. However, the capacity of their infrastructure is now insufficient for the application's rapid growth. Because of this growth and the company's desire to innovate faster, Dress4Win is committing to a full migration to a public cloud.

Solution Concept -
For the first phase of their migration to the cloud, Dress4Win is moving their development and test environments. They are also building a disaster recovery site, because their current infrastructure is at a single location. They are not sure which components of their architecture they can migrate as is and which components they need to change before migrating them.

Existing Technical Environment -
The Dress4Win application is served out of a single data center location. All servers run Ubuntu LTS v16.04.
Databases:
MySQL. 1 server for user data, inventory, static data:
- MySQL 5.8
- 8 core CPUs
- 128 GB of RAM
- 2x 5 TB HDD (RAID 1)
Redis 3 server cluster for metadata, social graph, caching. Each server is:
- Redis 3.2
- 4 core CPUs
- 32GB of RAM
Compute:
40 Web Application servers providing micro-services based APIs and static content.
`"
- Tomcat

Java -
- Nginx
- 4 core CPUs
- 32 GB of RAM
20 Apache Hadoop/Spark servers:
- Data analysis
- Real-time trending calculations
- 8 core CPUs
- 128 GB of RAM
- 4x 5 TB HDD (RAID 1)
3 RabbitMQ servers for messaging, social notifications, and events:
- 8 core CPUs
- 32GB of RAM
Miscellaneous servers:
- Jenkins, monitoring, bastion hosts, security scanners
- 8 core CPUs
- 32GB of RAM
Storage appliances:
iSCSI for VM hosts
Fiber channel SAN `" MySQL databases
- 1 PB total storage; 400 TB available
NAS `" image storage, logs, backups
- 100 TB total storage; 35 TB available

Business Requirements -
Build a reliable and reproducible environment with scaled parity of production.
Improve security by defining and adhering to a set of security and Identity and Access Management (IAM) best practices for cloud.
Improve business agility and speed of innovation through rapid provisioning of new resources.
Analyze and optimize architecture for performance in the cloud.

Technical Requirements -
Easily create non-production environments in the cloud.
Implement an automation framework for provisioning resources in cloud.
Implement a continuous deployment process for deploying applications to the on-premises datacenter or cloud.
Support failover of the production environment to cloud during an emergency.
Encrypt data on the wire and at rest.
Support multiple private connections between the production data center and cloud environment.

Executive Statement -
Our investors are concerned about our ability to scale and contain costs with our current infrastructure. They are also concerned that a competitor could use a public cloud platform to offset their up-front investment and free them to focus on developing better features. Our traffic patterns are highest in the mornings and weekend evenings; during other times, 80% of our capacity is sitting idle.
Our capital expenditure is now exceeding our quarterly projections. Migrating to the cloud will likely cause an initial increase in spending, but we expect to fully transition before our next hardware refresh cycle. Our total cost of ownership (TCO) analysis over the next 5 years for a public cloud strategy achieves a cost reduction between 30% and 50% over our current model.QuestionFor this question, refer to the Dress4Win case study. Dress4Win is

expected 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 the Tomcat and Nginx. Migrate MySQL to Cloud SQL, RabbitMQ to Cloud Pub/Sub, Hadoop to Cloud Dataproc, and NAS to Cloud Storage.

**Answer: D**

**Explanation:**

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

**Question: 328** CertyIQ

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**

**Explanation:**

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.

**Question: 329** CertyIQ

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 applications 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: C**

**Explanation:**

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

**Question: 330** CertyIQ

For this question, refer to the Dress4Win case study. To be legally compliant during an audit, Dress4Win must be able to give insights in all administrative actions that modify the configuration or metadata of resources on Google Cloud.
What should you do?

A.Use Stackdriver Trace to create a Trace list analysis.

B.Use Stackdriver Monitoring to create a dashboard on the project's activity.

C.Enable Cloud Identity-Aware Proxy in all projects, and add the group of Administrators as a member.

D.Use the Activity page in the GCP Console and Stackdriver Logging to provide the required insight.

**Answer: D**

**Explanation:**

Use the Activity page in the GCP Console and Stackdriver Logging to provide the required insight.

**Question: 331** CertyIQ

For this question, refer to the Dress4Win case study. You are responsible for the security of data stored in Cloud Storage for your company, Dress4Win. You have already created a set of Google Groups and assigned the appropriate users to those groups. You should use Google best practices and implement the simplest design to meet the requirements.
Considering Dress4Win's business and technical requirements, what should you do?

A.Assign custom IAM roles to the Google Groups you created in order to enforce security requirements. Encrypt data with a customer-supplied encryption key when storing files in Cloud Storage.

B.Assign custom IAM roles to the Google Groups you created in order to enforce security requirements. Enable default storage encryption before storing files in Cloud Storage.

C.Assign predefined IAM roles to the Google Groups you created in order to enforce security requirements. Utilize Google's default encryption at rest when storing files in Cloud Storage.

D.Assign predefined IAM roles to the Google Groups you created in order to enforce security requirements. Ensure that the default Cloud KMS key is set before storing files in Cloud Storage.

**Answer: C**

**Explanation:**

Assign predefined IAM roles to the Google Groups you created in order to enforce security requirements.
Utilize Google's default encryption at rest when storing files in Cloud Storage.

**Question: 332** CertyIQ

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**

**Explanation:**

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

# Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.
Your insights can help me improve our writing and better understand our readers.

## Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam
Keep your head up, stay positive, and go show that exam what you're made of!

Feedback

More Papers