NO.1 For this question, refer to the Dress4Win case study.
Dress4Win has end-to-end tests covering 100% of their endpoints. They want to ensure that the move to the cloud does not introduce any new bugs. Which additional testing methods should the developers employ to prevent an outage?
A. They should add canary tests so developers can measure how much of an impact the new release causes to latency.
B. They should run the end-to-end tests in the cloud staging environment to determine if the code is working as intended.
C. They should enable Google Stackdriver Debugger on the application code to show errors in the code.
D. They should add additional unit tests and production scale load tests on their cloud staging environment.
Answer: D

NO.2 You have created several preemptible Linux virtual machine instances using Google Compute Engine. You want to properly shut down your application before the virtual machines are preempted. What should you do?
A. Create a shutdown script 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 Stackdnver 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

NO.3 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 committed use discounts. Provide training to the team about service cost management.
B. Utilize free tier and sustained use discounts. Provision a staff position for service cost management.
C. Utilize free tier and sustained use discounts. Provide training to the team about service cost management.
D. Utilize free tier and committed use discounts. Provision a staff position for service cost management.
Answer: A
Explanation:
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#billing_and_management

NO.4 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. /usr/local/bin

B. ~/bin

C. /google/scripts

D. Cloud Storage

Answer: A

Explanation:
https://medium.com/google-cloud/no-localhost-no-problem-using-google-cloud-shell-as-my-full-time-development-environment-22d5a1942439

NO.5 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. Instrument your application with Stackdnver Trace in order to break down the request latencies at each microservice.

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

C. Send custom metrics for each of your requests to Stackdriver Monitoring.

D. Set timeouts on your application so that you can fail requests faster.

Answer: A

Explanation:
https://cloud.google.com/trace/docs/overview

NO.6 Your company captures all web traffic data in Google Analytics 260 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-analysis' group the IAM role of BigQuery dataViewer. Share the appropriate dataset with view access with each respective analyst country-group.

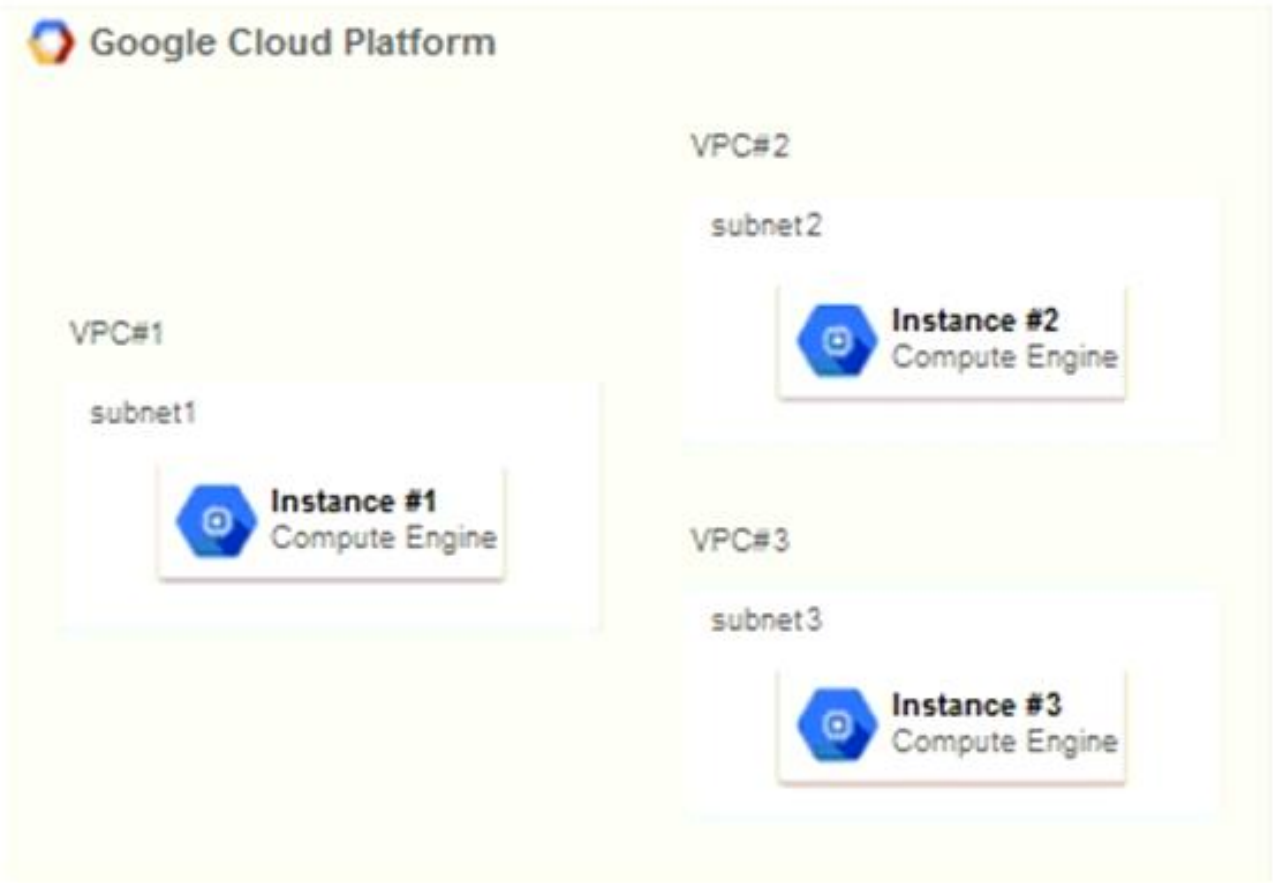
B. Create a group per country. Add analysts to their respective country-groups. Create a single group 'all_analysts', and add all country-groups as members. Grant the 'all-analysis' group the IAM role of BigQuery jobUser. Share the appropriate dataset with view access with each respective analyst country-group.

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-analysis' group the IAM role of BigQuery dataViewer. Share the appropriate table with view access with each respective analyst countrygroup.

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-analysis' group the IAM role of BigQuery jobUser. Share the appropriate tables with view access with each respective analyst countrygroup.

Answer: B

NO.7 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. Add two additional NICs to Instance #1 with the following configuration:
* NIC1
* VPC: VPC #2
* SUBNETWORK: subnet #2
* NIC2
* VPC: VPC #3
* SUBNETWORK: subnet #3

Update firewall rules to enable traffic between instances.

B. 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.

C. 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.

D. Create a cloud router to advertise subnet #2 and subnet #3 to subnet #1.

Answer: A
Explanation:
As per GCP documentation: "By default, every instance in a VPC network has a single network interface. Use these instructions to create additional network interfaces. Each interface is attached to a different VPC network, giving that instance access to different VPC networks in Google Cloud. You cannot attach multiple network interfaces to the same VPC network." Refer to:
https://cloud.google.com/vpc/docs/create-use-multiple-interfaces
https://cloud.google.com/vpc/docs/create-use-multiple-interfaces#i_am_not_able_to_connect_to_secondary_interfaces_internal_ip

NO.8 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. Configure Stackdriver Monitoring for all Projects, and export to Google Cloud Storage.
B. Configure Stackdriver Monitoring for all Projects, and export to BigQuery.
C. Configure Stackdriver Monitoring for all Projects with the default retention policies.
D. Grant the security team access to the logs in each Project.
Answer: A
Explanation:
Overview of storage classes, price, and use cases https://cloud.google.com/storage/docs/storage-classes Why export logs? https://cloud.google.com/logging/docs/export/ StackDriver Quotas and Limits for Monitoring https://cloud.google.com/monitoring/quotas The BigQuery pricing. https://cloud.google.com/bigquery/pricing

NO.9 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. Implement a Cloud NAT solution to remove the need for external IP addresses entirely.
B. Remove the default route on all VPCs. Move all approved instances into a new subnet that has a default route to an internet gateway.
C. 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.
D. Set an Organization Policy with a constraint on constraints/compute.vmExternalIpAccess. List the approved instances in the allowedValues list.
Answer: D
Reference:
https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip you might want to restrict external IP address so that only specific VM instances can use them. This option can help to prevent data exfiltration or maintain network isolation. Using an Organization Policy, you can restrict external IP addresses to specific VM instances with constraints to control use of external IP addresses for your VM instances within an organization or a project.

NO.10 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 a Compute Engine instance with 96 CPUs.
B. Replace the existing data warehouse with BigQuery. Use table partitioning.
C. Replace the existing data warehouse with a Compute Engine instance with 96 CPUs. Add an additional Compute Engine pre-emptible instance with 32 CPUs.
D. Replace the existing data warehouse with BigQuery. Use federated data sources.
Answer: D
Explanation:
https://cloud.google.com/solutions/bigquery-data-warehouse#external_sources
https://cloud.google.com/solutions/bigquery-data-warehouse

NO.11 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 Compute Engine, Jenkins, and Cloud Load Balancing
B. Google Compute Engine and Cloud Deployment Manager
C. Google Container Engine, Jenkins, and Helm
D. Google Container Engine and Cloud Load Balancing
Answer: C
Explanation:
Helm for managing Kubernetes
Kubernetes can base on the URL to route traffic to different location (path)
https://cloud.google.com/kubernetes-engine/docs/tutorials/http-balancer eg.apiVersion:
networking.k8s.io/v1beta1 kind: Ingress metadata:
name: fanout-ingress
spec:
rules:
- http:
paths:
- path: /*
backend:
serviceName: web
servicePort: 8080
- path: /v2/*
backend:
serviceName: web2
servicePort: 8080

NO.12 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 failover replica instance in the same region, but in a different zone
B. Create a read 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 a different region
Answer: D
Explanation:
https://cloud.google.com/sql/docs/mysql/high-availability

NO.13 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 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.
B. 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.
C. 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.
D. 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.
Answer: C
Explanation:
https://cloud.google.com/load-balancing/docs/https/setting-up-https-serverless#gcloud:-cloud-functions
https://cloud.google.com/blog/products/networking/better-load-balancing-for-app-engine-cloud-run-and-functions

NO.14 A recent audit that a new network was created in Your GCP project. In this network, a GCE instance has an SSH port open the world. You want to discover this network's origin. What should you do?
A. Connect to the GCE instance using project SSH Keys. Identify previous logins in system logs, and match these with the project owners list.
B. Search for Create VM entry in the Stackdriver alerting console.
C. Navigate to the Activity page in the Home section. Set category to Data Access and search for Create VM entry.
D. In the logging section of the console, specify GCE Network as the logging section. Search for the Create Insert entry.
Answer: D
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

NO.15 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. In the GCP Console, use Datastore Admin to delete the current indexes and upload the new configuration file
B. Point gcloud datastore create-indexes to your configuration file
C. Create an HTTP request to the built-in python module to send the index configuration file to your application
D. Upload the configuration file the App Engine's default Cloud Storage bucket, and have App Engine detect the new indexes
Answer: B

NO.16 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 using the Cloud Storage and use lifecycle management to delete files when they expire.
B. Store the data in Cloud Storage and run a nightly batch script that deletes all expired datA.
C. Anonymize the data using the Cloud Data Loss Prevention API and store it indefinitely.
D. Store the data in Google Drive and manually delete records as they expire.
Answer: A
Explanation:
https://cloud.google.com/storage/docs/lifecycle

NO.17 You are helping the QA team to roll out a new load-testing tool to test the scalability of your primary cloud services that run on Google Compute Engine with Cloud Bigtable. Which three requirements should they include? Choose 3 answers
A. Ensure all third-party systems your services use are capable of handling high load.
B. Schedule the load-testing tool to regularly run against the production environment.
C. Instrument the load-testing tool and the target services with detailed logging and metrics collection.
D. Instrument the production services to record every transaction for replay by the load-testing tool.
E. Create a separate Google Cloud project to use for the load-testing environment.
F. Ensure that the load tests validate the performance of Cloud Bigtable.
Answer: C,E,F

NO.18 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. Deploy Cloud VPN Gateway in each region. Ensure that each region has at least one VPN tunnel to the on-premises peer gateway.
D. Create a global Cloud VPN Gateway with VPN tunnels from each region to the on-premises peer gateway.
Answer: D
Explanation:
https://cloud.google.com/vpn/docs/how-to/creating-static-vpns