GCP Cheat Sheet ShortNotes

I. **Resource Manager :** Hierarchically manage resources by project, folder, and organization
   A. Resource Hierarchy: Organization > Folder > Project > Service Resources
   B. Project ID is a unique identifier used to link Google Cloud resources and APIs to your specific project.
   C. Project resource number is automatically assigned when you create the project, read-only.
   D. The Google Workspace super admin's main duty with respect to Google Cloud is to assign the Organization Administrator IAM role to appropriate users in their domain.
   E. The Organization Policy Service gives you Centralize control to configure restrictions on how your organization's resources can be used.
   F. To shut down (Delete) a project
      1. IAM & Admin Settings page, Click Select a project you want to delete, and click Open.
      2. Click Shut down.
      3. Enter the project ID, then click Shut down.

II. **Billing**
   A. Resource management is focused on how you should configure and grant access to the various cloud resources
   B. Labels help you categorize your Google Cloud resources
   C. If you are a reseller, you can use subaccounts to represent your customers' charges for the purpose of chargebacks.
   D. Cloud Billing budgets to monitor all of your Google Cloud charges in one place. A budget enables you to track your actual Google Cloud spend against your planned spend. Use **Programmatic Notifications** to **automate cost control responses.** Example : Capping your Google Cloud spend by automatically disabling billing or terminating resources.
   E. BigQuery to store usage data typically incurs minimal fees, When exporting and analyzing Cloud Billing data with BigQuery, we recommend using the Standard export to analyze trends in your costs, and using the Detailed export to track costs at the resource level, and identify specific resources that might be driving your costs.
   F. Billing Roles :
      1. create a budget for your Cloud Billing account, you must be a **Billing Account Administrator** (roles/billing.admin) on the Cloud Billing account.
      2. Billing Account Creator (roles/billing.creator) access to create billing accounts.
   G. To create a new budget, complete the following steps:
      1. Sign in to the Google Cloud Console and navigate to Billing to start creating a budget. Create and name the budget.
      2. Set the budget scope. A budget can be applied to the entire Cloud Billing account, or scoped to focus on a specific set of resources.
      3. Set the budget amount. The budget amount you set is your planned spend and is compared to your actual spend to calculate the thresholds that trigger sending alert emails and notifications.
      4. Set the budget threshold rules and actions. Threshold rules define the triggering events used to generate a budget notification email. Note that threshold rules are required for email notifications and are used specifically to trigger email notifications.
      5. Click Finish to save the new budget.
   H. Access your Cloud Billing data (such as usage, cost estimates, and pricing data) from BigQuery for detailed analysis, or use a tool like Google Data Studio to visualize your data.
   I. The Cloud Billing Reports page lets you view your Google Cloud usage costs at a glance and discover and analyze trends. To view the Cloud Billing reports you need to be a Billing

Account Administrator or Billing Account Viewer on your Cloud Billing account. Additionally, Project Owners, Project Editors, and Project Viewers can also view Cloud Billing reports for their specific Cloud projects.

III. IAM

A. **IAM** lets you grant granular access to specific Google Cloud resources and helps prevent access to other resources. IAM lets you adopt the security principle of least privilege, which states that nobody should have more permissions than they actually need.

B. An *allow policy*, also known as an *IAM policy*, defines and enforces what roles are granted to which principals. Use deny policies to prevent principals from using specific IAM permissions.

C. The initial IAM policy for a newly created Organization resource grants the Project Creator and Billing Account Creator roles to the entire Google Workspace domain.

D. Organization Policy roles : Access Transparency Admin, Organization Policy Administrator (roles/orgpolicy.policyAdmin) , Organization Policy Viewer

E. As an administrator, you can use Cloud Identity to manage your users, apps, and devices from a central location—the Google Admin console.

F. IAM roles and lists the predefined roles that you can grant to your principals.

G. Quotas to restrict how much of a particular shared Google Cloud resource that you can use. Each quota represents a specific countable resource, such as API calls to a particular service, the number of load balancers used concurrently by your project, or the number of projects that you can create.

H. If your project needs more of a particular resource than your quotas allow, you can request more quota for a specific service. You can find out more about how quota increase requests work in About quota increase requests. You can also add your own limits for certain quotas if you want to impose spending limits, particularly when developing or testing an application that uses expensive resources.

I. Monitoring and alerting on quota metrics

J. A service account is how applications and resources authenticate and access services in Google Cloud.

   1. Different types of IAM Roles :
      a) roles/iam.serviceAccountKeyAdmin - Create and manage (and rotate) service account keys.
      b) roles/iam.serviceAccountUser - Run operations as the service account.
      c) roles/iam.serviceAccountAdmin - Create and manage service accounts.
   2. List of roles for impersonating service accounts : allow principals and resources to *impersonate*, or act as, an IAM service account.
      a) Service Account User (`roles/iam.serviceAccountUser`)
      b) Service Account Token Creator (`roles/iam.serviceAccountTokenCreator`)
      c) Workload Identity User (`roles/iam.workloadIdentityUser`)

K. There are three types of roles in IAM:

   1. Basic roles (primitive roles), which include the Owner, Editor, and Viewer roles that existed prior to the introduction of IAM.
   2. Predefined roles, which provide granular access for a specific service and are managed by Google Cloud.
   3. Custom roles, which provide granular access according to a user-specified list of permissions.

L. **`gcloud iam list-testable-permissions <full-resource-name>`** list IAM testable permissions for a resource

M. Two types of keys are available for authentication of a service account: user managed keys and Google managed keys.

N. Short-lived credentials have a limited lifetime, with durations of just a few hours or shorter. Short-lived service account credentials are useful for scenarios where you need to grant limited access to resources for trusted service accounts.
O. Access Approval Approver (roles/accessapproval.approver) : Ability to view or act on access approval requests and view configuration
P. Project roles : Browser (roles/browser) Read access to browse the hierarchy for a project, including the folder, organization, and allow policy. This role doesn't include permission to view resources in the project.
Q. Review the IAM users and roles assigned on a specific Google Cloud project : Using the Cloud Console, navigate to the **Project**, and go to the **IAM** section. Under the **'Permissions'** tab, review the **Members and Roles** section.

IV. **Cloud APIs :** are programmatic interfaces to Google Cloud Platform services.

A. gRPC is a modern open source high performance Remote Procedure Call (RPC) framework that can run in any environment. It can efficiently connect services in and across data centers with pluggable support for load balancing, tracing, health checking and authentication. It is also applicable in last mile of distributed computing to connect devices, mobile applications and browsers to backend services.
B. Cloud Endpoints is an API management system that provides an API console, hosting, logging, monitoring, and other features to help you create, share, maintain, and secure your APIs. Endpoints works with either the Extensible Service Proxy (ESP) or the Extensible Service Proxy V2 (ESPv2) to provide API management.
C. Apigee is a platform for developing and managing APIs available to your customers and partners
D. To limit the billable usage by setting Capping API usage , explicitly cap requests by limiting the *requests per day*, *requests per minute*, or *requests per minute per user*.

V. **Google Cloud's operations suite (formerly Stackdriver)** : Integrated monitoring, logging, and trace managed services for applications and systems running on Google Cloud and beyond.

A. Cloud Monitoring : Full-stack monitoring for Google Cloud Platform and Amazon Web Services. Alerting policies and uptime checks Note : The alerting policy uses the label values to identify the resource that caused a condition to be met. Labels are key-value pairs that are associated with time series, alerting policies, and incidents.
B. Cloud Logging : Real-time log management and analysis.
    1. The Log Router checks each log entry against existing rules to determine which log entries to ingest (store) into log buckets, which log entries to route to a destination, and which log entries to exclude (discard).
    2. Sinks control how Cloud Logging routes logs. Using sinks, you can route some or all of your logs to supported destinations. Sinks type : _Required and _Default.
    3. Log entries that you routed from Cloud Logging to supported destinations: Hourly batches = Cloud Storage buckets, Near real-time = BigQuery tables, Pub/Sub topics, Cloud Logging buckets, Third-party destinations (Splunk)
    4. Logs Explorer for analyzing logs data. You can refine the scope of the logs displayed in the Logs Explorer through the **Refine scope** option.
    5. Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization:
        a) Admin Activity audit logs
        b) Data Access audit logs
        c) System Event audit logs
        d) Policy Denied audit logs

6. The Legacy Logs Viewer displays logs for a single Cloud project.The Legacy Logs viewer can filter logs based on resources, severity, including the specific time frame you want to define.
7. Cloud Logging Agent allows you to stream logs of common third-party applications and system software.
8. Cloud Console Activity Page, you can filter the activity logs based on activity type and resources.

C. Error Reporting : Identify and understand your application errors.
D. Application Performance Management
   1. Cloud Debugger : Investigate your code's behavior in production.
   2. Cloud Trace : Find performance bottlenecks in production.
   3. Cloud Profiler : Identify patterns of CPU, time, and memory consumption in production.
E. Google 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.

VI. Compute

A. Compute Engine

1. Virtual machine instances and persistent disks live in a zone.
2. Spot VMs : Affordable compute instances suitable for batch jobs and fault-tolerant workloads. Latest version of preemptible VMs. Spot VMs are available at much lower prices—60-91% discounts. Preemptible VMs are Compute Engine VM instances that last a maximum of 24 hours in general and provide no availability guarantees. Preemptible VMs are priced lower than standard Compute Engine VMs and offer the same machine types and options.Preemptible instances terminate after 30 seconds upon receiving a preemption notice.
3. Machine and series recommendations
   a) General-purpose workloads
      (1) Cost-optimized : E2
      (2) Balanced : N2, N2D, N1
      (3) Scale-out optimized : Tau T2D, Tau T2A
   b) Optimized workloads
      (1) Memory-optimized : M2, M1
      (2) Compute-optimized : C2, C2D
      (3) Accelerator-optimized : A2
4. Types of storage options for your instances.
   a) Zonal persistent disk: Efficient, reliable block storage.
   b) Regional persistent disk: Regional block storage replicated in two zones.
   c) Local SSD: High performance, transient, local block storage.
   d) Cloud Storage buckets: Affordable object storage.
   e) Filestore: High performance file storage for Google Cloud users.
   f) Local SSDs are SSDs that are designed for high IOPS and low latency disk processing. These are physically attached to the server that hosts your instance. When compared to Zonal SSD Persistent Disk, Local SSD offers higher throughput and lower latency but has availability, durability, and flexibility trade-offs.
5. Disk Type :
   a) **`pd-standard`** : standard hard disk drives (HDD)
   b) **`pd-balanced, pd-ssd, pd-extreme`** : solid-state drives (SSD)

6. **`--force-attach`** : Attach the disk to the instance even if it is currently attached to another instance.
7. **`--multi-writer`** flag enable multi-writer mode for new (share) persistent disks, so that both VMs (2) can read and write to the disk.
8. Network Tags enable you to make firewall rules and routes applicable to specific VM instances. **`gcloud compute instances add-tags`**
9. A VM's host maintenance policy determines how it behaves during following host events
    a) Maintenance events : live migrate move a VM to another host machine
    b) Host errors : must terminate or restart a VM **`automaticRestart`**
    c) By default, VMs are set to live migrate during host system events, but you can set them to terminate and optionally restart.
    d) From the **Availability policies** section, you can set the **On host maintenance** and **Automatic restart** options.
10. Managed instance groups (MIGs) let you operate apps on multiple identical VMs.MIG services, including: autoscaling, autohealing, regional (multiple zone) deployment, and automatic updating.
    a) Instance templates (VM instance's configuration) define the machine type, boot disk image or container image, labels, startup script, and other instance properties. Use deterministic instance templates to ensure identical VMs
    b) Stateful MIG : Stateful workloads where disks, IP addresses, and/or metadata are preserved on VM recreate operations.
        (1) Stateful configuration : a combination of the instance template, stateful policy, and per-instance configurations
        (2) A *stateful policy* defines items that you want to preserve for all instances in your MIG.
        (3) A *per-instance configuration* defines items to preserve for a specific VM instance.
    c) Stateless MIG : Highly available and scalable stateless workloads, where disks and IP addresses are recreated from scratch on horizontal scaling, autohealing, auto-updating, and VM recreation.
    d) Autohealing : recreates unhealthy VMs
        (1) configure an application-based health check : verifies application is responding as expected **`health-checks create http example-check --port 80`**
        (2) Create a firewall rule to allow health check probes to connect to your app. **`firewall-rules create allow-health-check`**
        (3) Apply the health check by configuring an autohealing policy
        (4) Health states
    e) Load balancing
        (1) backend service is necessary for creating most types of load balancers
        (2) A target pool is used in Network Load Balancing, where the load balancer forwards user requests to the attached target pool
        (3) Named ports are key-value pairs that represent a port's name and number.
    f) Autoscaling : autoscaling policy
        (1) Average CPU utilization.

(2) HTTP load balancing serving capacity, based on either utilization or requests per second.
(3) Cloud Monitoring metrics

g) Auto-updating `rolling-action start-update`
(1) Automatic, or **proactive**, updates
(2) Selective, or **opportunistic**, updates
(3) A canary update is applied to a subset of instances in the group.

h) Updating the instances in a managed instance group can simply be done using a rolling update.
(1) Use the maxSurge option to configure how many new instances the MIG can create above its targetSize during an automated update.
(2) Use the maxUnavailable option to configure how many instances are unavailable at any time during an automated update.

i) Recommend that you overprovision your autoscaled regional MIG to avoid overloading surviving servers during the time a zone is lost. Overprovisioning your group prevents your system from failing entirely if a zone or group of instances becomes unresponsive.

j) If your MIG cannot create or recreate instances, the problem might be related to the following situations.
(1) The boot disk already exists.
(2) The instance template is not valid.

11. Add SSH keys to instance metadata : the **Networking, disks, security, management, sole tenancy** section, and do the following:
a) Expand the **Security** section.
b) Select **Add manually generated SSH keys**.
12. Install Monitoring agent and Install Logging agent : Ops Agent & **Legacy agent**
13. Firewall rules that allow RDP access on TCP port 3389.
14. If deleted Snapshots files are not discarded make sure to enable the `discard` option or run `fstrim` on your disk.
15. Note that snapshots are different from custom images and machine images, which are useful for creating instance boot disks.
16. By setting the deletionProtection flag or Deletion Protection feature that prevents users from accidentally deleting an instance.
17. Identity-Aware Proxy simply secures your application and VMs by checking web requests and authenticating the requestor via the Google Identity service.
18. With custom images, you can save a copy of your configured and customized persistent disks and images. You can use these custom images to launch new instances. To create a custom image, you can either source disks, images, snapshots, or images stored in Cloud Storage.
19. When creating multiple copies of an instance, Google recommends creating a custom image from the snapshot of the persistent disk used by the instance; then use the custom image to launch a new instance. Creating an instance boot disk from a custom image is more efficient and quick when compared to creating from a disk snapshot.
20. **Compute OS Admin Login (**roles/compute.osAdminLogin), Access to log in to a Compute Engine instance as an administrator user. To manage instance access using IAM roles, you must enable the OS Login feature by setting a metadata key-value pair in your project or in your instance's metadata: enable-oslogin=TRUE.

B. **Kubernetes Engine**

1. GKE clusters have two modes of operation :
    a) **Autopilot**: Manages the entire cluster and node infrastructure for you.
    b) **Standard**: Provides you with node configuration flexibility and full control over managing your clusters and node infrastructure.
2. A *node pool* is a group of nodes within a cluster that all have the same configuration.
3. With Autopilot clusters, you don't need to worry about provisioning nodes or managing node pools because node pools are *automatically* provisioned through Node auto-provisioning, and are automatically scaled to meet the requirements of your workloads. With *Node auto-provisioning* new node pools are created and deleted automatically.
4. Automatic upgrades for your cluster's node software
5. Node auto-repair to maintain node health and availability.
6. Node auto-upgrades help you keep the nodes in your cluster up-to-date with the cluster control plane version when your control plane is updated on your behalf. When you create a new cluster or node pool with Google Cloud console or the gcloud command, node auto-upgrade is enabled by default.
7. Pods provide networking and storage to containers, and contain dependencies the container needs to run and communicate. A Deployment manages a set of multiple identical pods. A Service is a group of pod endpoints that you can configure access for.
8. **Kubernetes Service**, which is a Kubernetes resource that lets you expose your application to external traffic. Kubernetes uses labels to group multiple related Pods into a logical unit called a Service. A Service has a stable IP address and ports, and provides load balancing among the set of Pods whose labels match all the labels you define in the label selector when you create the Service.
9. Five types of Services:
    a) ClusterIP (default): Internal clients send requests to a stable internal IP address.
    b) NodePort: Clients send requests to the IP address of a node on one or more nodePort values that are specified by the Service. Service is accessible by using the IP address of any node along with the `nodePort` value.
    c) LoadBalancer: Clients send requests to the IP address of a network load balancer.
    d) ExternalName: Internal clients use the DNS name of a Service as an alias for an external DNS name.
    e) Headless: You can use a headless service when you want a Pod grouping, but don't need a stable IP address.
10. **Secrets** are secure objects which store sensitive data, such as passwords, OAuth tokens, and SSH keys in your clusters. Storing sensitive data in Secrets is more secure than in plaintext ConfigMaps or in Pod specifications.
11. *ConfigMaps* bind non-sensitive configuration artifacts such as configuration files, command-line arguments, and environment variables to your Pod containers and system components at runtime.
12. By default, Autopilot clusters are public & node auto-upgrades are enabled by default. must configure Cloud NAT.
13. To use preemptible VMs as node pool, select the Enable preemptible nodes checkbox on the node pool creation. You can create a cluster or node pool with preemptible VMs by specifying the --preemptible flag.

14. DaemonSets are useful for deploying ongoing background tasks that you need to run on all or certain nodes, and which do not require user intervention. Examples of such tasks include storage daemons like ceph, log collection daemons like fluent-bit, and node monitoring daemons like collectd.
15. IP addresses in Kubernetes
    a) ClusterIP: The IP address assigned to a Service. Address is stable for the lifetime of the Service
    b) Pod IP: The ephemeral IP address assigned to a given Pod.
    c) Node IP: The IP address assigned to a given node.
16. A cluster that uses Alias IPs (ranges of internal IP addresses) is called a *VPC-native cluster*, default for Autopilot mode. A cluster that uses Google Cloud routes is called a *routes-based cluster*.
17. A cluster label is a key-value pair that helps you organize your Google Cloud clusters.
18. Kube-proxy is an egress-based load-balancing controller, watches the Kubernetes API server and continually maps the ClusterIP to healthy Pods by adding and removing destination NAT (DNAT) rules to the node's iptables subsystem.
19. Artifact Registry provides a single location for storing and managing your packages and Docker container images. Artifact Registry extends the capabilities of Container Registry.
    a) Container Registry uses Cloud Storage buckets as the underlying storage for container images. You control access to your images by granting appropriate Cloud Storage permissions to a user, group, service account, or other identity.
20. Release channels provide GKE best practices for versioning and upgrading your GKE clusters.
21. Stateful applications are different from stateless applications, in which client data is not saved to the server between sessions. **`volumeClaimTemplates`** array generates the PersistentVolumeClaim objects
22. Autoscale Deployments : **`kubectl autoscale deployment my-app --max 6 --min 4 --cpu-percent 50`**
23. After running **`kubectl autoscale`**, the **`HorizontalPodAutoscaler`** object is created and targets the application. When there is a change in load, the object increases or decreases the application's replicas.
24. Vertical Pod autoscaling provides recommendations for resource usage over time.
25. Gateway :
    a) Service capacity, you can define a Requests per Second (RPS) value per Pod in a Service.
26. Manually upgrade a node pool : **`gcloud container clusters upgrade CLUSTER_NAME \ --node-pool=NODE_POOL_NAME`**
27. Manually upgrading the control plane : **`gcloud container clusters upgrade CLUSTER_NAME --master`**
28. Migrate for GKE is a tool to containerize existing VM-based applications to run on GKE.
29. To deploy an application on Kubernetes once you have a dockerfile, you need to do the following:
    a) Build an image using the Dockerfile you created.
    b) Push the image to the Container Registry.

c) Create a deployment YAML file referencing the image you pushed on the container registry.
d) Deploy the application using kubectl command. (Assuming the Kubernetes cluster was created ahead).

C. **App Engine**

1. App Engine is a fully managed, serverless platform for developing and hosting web applications at scale.
2. App Engine services behave like microservices. Therefore, you can run your whole app in a single service or you can design and deploy multiple services to run as a set of microservices.
3. Having multiple versions of your app within each service allows you to quickly switch between different versions of that app for rollbacks, testing, or other temporary events. You can route traffic to one or more specific versions of your app by migrating or splitting traffic.
4. The versions within your services run on one or more *instances*.
5. App Engine flexible environment
6. App Engine standard environment
    a) Splitting traffic : use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service.
        (1) Use `gcloud app services set-traffic --splits` flag to set traffic splitting.
    b) Migrating traffic : moving traffic from one or more versions to a single new version.
7. App Engine calculates the number of instances necessary to serve your current application traffic based on scaling settings such as target_cpu_utilization and target_throughput_utilization. Setting the min_idle_instances element specifies the number of instances to run in addition to this calculated number.

D. **Cloud Run :** Serverless for containerized application, deploy stateless containers

1. **Cloud Run services.** Used to run code that responds to web requests, or events.
2. **Cloud Run jobs.** Used to run code that performs work (a job) and quits when the work is done.
3. The service is the main resource of Cloud Run.For redundancy and failover, services are automatically replicated across multiple zones in the region they are in.
4. Each deployment to a service creates a revision. A revision consists of a specific container image, along with environment settings such as environment variables, memory limits, or concurrency value.
5. Container instance autoscaling : each revision is automatically scaled to the number of container instances needed to handle all incoming requests.
    a) maximum concurrency setting : configure the maximum concurrent requests per instance. Ex. code cannot process parallel requests, set concurrency to 1.
    b) maximum number of container instances setting
    c) minimum number of container instances setting
6. Rollbacks, gradual rollouts, and traffic migration : allows you to rollback to a previous revision, gradually roll out a revision, and split traffic between multiple revisions.
7. Minimum instances services specifying a minimum number of container instances to be kept warm and ready to serve requests.
8. Cloud Run integrates : with Data storage, Logging and error reporting, Service identity, Continuous delivery, Private networking, Google Cloud APIs,

E. **Cloud Function** : pay-as-you-go functions as a service (FaaS) for Event based Serverless function execution
    1. Cloud Functions is Google's serverless compute solution for creating event-driven applications also for building and connecting cloud services.. Use cases include IoT processing and lightweight ETL.
    2. Cloud Functions for Firebase if you're a developer building a mobile app or mobile web app.
    3. *Triggers* create a response to an event.
        a) **HTTP triggers**, which react to HTTP(S) requests, and correspond to HTTP functions.
        b) **Event triggers**, which react to events within your Google Cloud project, and correspond to event-driven functions.
    4. Each instance of a function handles only one concurrent request at a time.
    5. Pub/Sub trigger enables a function to be called whenever a message is published to the specified topic.
    6. Cloud Storage trigger enables a function to be called whenever a change occurs on an object (file) within the specified bucket or called in response to changes in Cloud Storage.
    7. Create Eventarc trigger so Cloud Run service receives notifications of a specified event or set of events. By specifying filters for the trigger, you can configure the routing of the event, including the event source and the target Cloud Run service.

VII. Networking

A. Google Cloud Hybrid Connectivity : Connect your infrastructure to Google Cloud on your terms, from anywhere.
    1. Cloud VPN & Cloud Interconnect : Provide network connectivity with Google Cloud between your on-premises network and Google Cloud, or from Google Cloud to another cloud provider.
    2. If you need to encrypt traffic to Google Cloud, or you need a lower throughput solution, or you are experimenting with migrating your workloads to Google Cloud, you can choose Cloud VPN gateways: HA VPN and Classic VPN.
    3. If you need an enterprise-grade connection to Google Cloud that has higher throughput, you can choose Dedicated Interconnect or Partner Interconnect.
        a) Dedicated Interconnect provides direct physical connections between your on-premises network and Google's network.
        b) Partner Interconnect provides connectivity between your on-premises network and your Virtual Private Cloud (VPC) network through a supported service provider.
    4. Cloud Router : Provides dynamic routing by using the Border Gateway Protocol (BGP) over Interconnect connections and Cloud VPN gateways.
    5. Need access to only Google Workspace or supported Google APIs :
        a) Direct Peering to directly connect (peer) with Google Cloud at a Google edge location.
        b) Carrier Peering to peer with Google by connecting through a support provider, which in turn peers with Google.

B. Virtual Private Cloud VPC provides networking for your cloud-based resources and services that are global, scalable, and flexible.
    1. VPC Network Peering is used to connect other VPC networks in different projects or organizations.

2. Shared VPC allows an organization to connect resources from multiple projects to a common VPC network, so that they can communicate with each other securely and efficiently using internal IPs from that network.
3. Serverless VPC Access makes it possible to connect directly to your VPC network from serverless environments such as Cloud Run, App Engine, or Cloud Functions.
4. VPC networks have an internal DNS service that allows you to address instances by their DNS names rather than their internal IP addresses.
5. Direct Peering provides a direct connection whilst Carrier Peering provides connectivity through a supported partner.
6. A network tag is simply a character string added to a *tags* field in a resource
7. VPC firewall rules let you allow or deny connections to or from
8. Work with subnets : The primary IPv4 range for the subnet can be expanded, but not replaced or shrunk, after the subnet has been created.
9. *Hierarchical firewall policies* let you create and enforce a consistent firewall policy across your organization.
10. Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules.
11. With VPC Peering, a relationship between two VPCs can be established to exchange traffic. Alternatively, to use the full power of Identity Access Management (IAM) to control who and what in one project can interact with a VPC in another, you can configure a Shared VPC.
12. A project can't access another project's resources unless you use Shared VPC or VPC Network Peering.
13. 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.

C. VPC Service Controls secures your Google Cloud services
   1. Using dry run mode, you can create new service perimeters or change multiple existing perimeters with no impact to an existing environment.
   2. Configuring ingress and egress policies.

D. Cloud DNS is global Domain Name System (DNS) service

E. Network Connectivity Center offers the unique ability to easily connect your on-premises, Google Cloud, and other cloud enterprise networks.

F. Private Service Connect : Set up private connectivity to your own, third-party and Google services from your VPC.

G. Service Directory is a platform for discovering, publishing, and connecting services, regardless of the environment.

H. Cloud CDN (Content Delivery Network) uses Google's global edge network to serve content closer to users, which accelerates your websites and applications.

I. Cloud NAT (network address translation) lets certain resources create outbound connections to the internet without external IP addresses.

J. Network Service Tiers : Premium Tier delivers traffic on Google's premium backbone, while Standard Tier uses regular ISP networks. Use Premium Tier to optimize for performance, and use Standard Tier to optimize for cost.

K. Cloud Load Balancing : fully distributed, software-defined managed service. Distributes user traffic across multiple instances of your applications.
   1. Cloud Load Balancing types :
      a) Internal (Regional)
         (1) Internal TCP/UDP load balancer Layer 4 load balancer

(2) Internal HTTP(S) load balancer
(3) Internal regional TCP proxy load balancer (Preview)

b) External (Global=G / Regional=R)
(1) Global external HTTP(S) load balancer G for three-tier web services
(2) Global external HTTP(S) load balancer (classic)
(3) External SSL proxy load balancer
(4) External TCP proxy load balancer
(5) External TCP/UDP Network load balancer R
(6) Regional external HTTP(S) load balancer R

2. Architecture
a) A **backend service** distributes requests to healthy backends.
b) A **health check** periodically monitors the readiness of your backends.
c) **Firewall rules** for your backends to accept health check probes.
d) The HTTP(S) proxy uses a **URL map** to make a routing determination based on HTTP attributes (such as the request path, cookies, or headers).

L. Google Cloud Armor to protect your infrastructure from distributed denial-of-service (DDoS) attacks and other targeted application attacks.
M. Private Google Access also allows access to the external IP addresses used by App Engine, including third-party App Engine-based services.
N. On-premises hosts can reach Google APIs and services by using Cloud VPN or Cloud Interconnect from your on-premises network to Google Cloud.
O. On-premises hosts must connect to Google APIs and services by using the virtual IP addresses (VIPs) for either the restricted.googleapis.com (199.36.153.4/30) or private.googleapis.com (199.36.153.8/30) domains.

VIII. Cloud Load Balancer

A. Google Cloud HTTP(S) load balancers and Traffic Director use a Google Cloud configuration resource called a *URL map* to route HTTP(S) requests to backend services or backend buckets.
B. A forwarding rule and its corresponding IP address represent the frontend configuration of a Google Cloud load balancer.
C. With Service Directory, you can register all of your services in a single place and resolve them by using HTTP, gRPC, and DNS. Service Directory solves the following problems: Interoperability, Service management, Access Control, Limitations of pure DNS
D. A backend service defines how Cloud Load Balancing distributes traffic.
E. health checking mechanisms that determine whether backend instances respond properly to traffic. `compute health-checks list`
1. `TCP or HTTP --port=80.`
2. `SSL, HTTPS, or HTTP2, --port=443`
F. An ingress allow firewall rule that allows traffic to reach your instances.
G. A network endpoint group (NEG) is a configuration object that specifies a group of backend endpoints or services.

IX. Storage

A. Filestore : Fully managed NFS file servers on Google Cloud
B. Cloud Storage : Object storage. Store objects and serve static content.
1. Default storage class for bucket. You can override this per object.
a) Standard is for immediate access and has no minimum storage duration
b) Nearline has a 30 day minimum duration and data retrieval charges
c) Coldline has a 90 day min duration and data retrieval charges
d) Archive has a 365 day min duration and data retrieval charges

2. A retention policy that specifies a retention period can be placed on a bucket. An object in the bucket cannot be deleted or replaced until it reaches the specified age.
3. An object hold can be placed on individual objects to prevent anyone from deleting or replacing the object until the hold is removed.
4. Object Versioning can be enabled on a bucket in order to retain older versions of objects. Object Versioning cannot be enabled on a bucket that currently has a retention policy.
5. Object Lifecycle Management can be configured for a bucket, which gives you more automated control over deleting objects. When you define a lifecycle configuration, Cloud Storage performs a specified action on an object only if the object meets your criteria. A lifecycle rule specifies exactly one of the following actions:
    a) Delete
    b) SetStorageClass
    c) AbortIncompleteMultipartUpload
6. Cloud Storage pricing :
    a) Data storage: the amount of data stored in your buckets. Storage rates vary depending on the storage class of your data and location of your buckets.
    b) Data processing: the processing done by Cloud Storage,
    c) Network usage: amount of data read from or moved between your buckets.
7. Signed URLs, give time-limited access to a specific Cloud Storage resource. Anyone in possession of the signed URL can use it while it's active, regardless of whether they have a Google account. Signed URLs is a URL that provides limited permission and time to make a request. Signed URLs contain authentication information in their query string, allowing users without credentials to perform specific actions on a resource
8. Objects stored in Cloud Storage have *metadata* associated with them. Metadata identifies properties of the object, as well as specifies how the object should be handled when it's accessed. The most commonly set metadata is Content-Type (also known as media type), which lets browsers render the object properly.
9. Cloud Storage Roles :
    a) Storage Admin - Grants full control of buckets and objects. When applied to an individual bucket, control applies only to the specified bucket and objects within the bucket.
    b) Storage Object Admin - Grants full control over objects, including listing, creating, viewing, and deleting objects.
    c) Storage Object Creator - Allows users to create objects. Does not give permission to view, delete, or replace objects.
    d) Storage Object Viewer - Grants access to view objects and their metadata, excluding ACLs. Can also list the objects in a bucket.
    e) Storage HMAC Key Admin - Full control over HMAC keys in a project. This role can only be applied to a project.

C. Cloud SQL : Fully managed relational database for MySQL, PostgreSQL, and SQL Server.
1. A Cloud SQL instance corresponds to one virtual machine (VM). The VM includes the database instance and accompanying software containers to keep the database instance up and running. When you create a new instance in the Google Cloud console, both **Automated backups** and **Enable point-in-time recovery** are automatically enabled.
2. A database instance is the set of software and files that operate the databases: MySQL, PostgreSQL or SQL Server.

3. The read replica is an exact copy of the primary instance. Data and other changes on the primary instance are updated in almost real time on the read replica.
4. Query insights helps you detect, diagnose, and prevent query performance problems for Cloud SQL databases.
5. If you need a relational database with full SQL support for an online transaction processing (OLTP) system, consider Cloud SQL.
6. In Cloud SQL, point-in-time recovery (PITR) uses binary logs. enable automated backups and binary logging for your Cloud SQL instances. This allows you to perform a point-in-time recovery, which restores your database from a backup and recovers it to a fresh Cloud SQL instance.

D. Cloud Spanner : Fully managed, Horizontally scalable, relational database. 99.999% availability
   1. Cloud Spanner Roles : **Cloud Spanner Database User** (roles/spanner.databaseUser) Read from and write to the Cloud Spanner database. Execute SQL queries on the database, including DML and Partitioned DML. View and update schema for the database
   2. When you create a Cloud Spanner instance, you choose the number of compute capacity nodes or processing units to serve your data. However, if the workload of an instance changes, Cloud Spanner doesn't automatically adjust the size of the instance.
   3. Autoscaler tool for Cloud Spanner (Autoscaler), an open source tool that you can use as a companion tool to Cloud Spanner.
      a) Deploy a per-project or centralized Autoscaler tool for Cloud Spanner
      b) Deploy a distributed Autoscaler tool for Cloud Spanner

E. Firestore : Fully managed NoSQL Document database.
   1. Realtime Database is a regional solution. Store and sync data in real time.
   2. Cloud Firestore is a regional and multi-region solution that scales automatically.
   3. The Datastore emulator provides local emulation of the production Datastore environment. You can use the emulator to develop and test your application locally. to install = gcloud components install cloud-datastore-emulator

F. Cloud Bigtable is fully managed NoSQL (Wide Column) Big Data database service for large analytical and operational workloads.

G. BigQuery : Fully managed cloud data warehouse for analytics.
   1. built-in features like machine learning, geospatial analysis, and business intelligence.
   2. BigQuery storage is automatically replicated across multiple locations to provide high availability.
   3. BigQuery Data Transfer Service automates data ingestion.
   4. To estimate costs before running a query, you can use one of the following methods:
      a) Query validator in the console
      b) --dry_run flag in the bq command-line tool
      c) dryRun parameter when submitting a query job using the API
   5. If you need interactive querying in an online analytical processing (OLAP) system, consider BigQuery.
   6. BigQuery Omni offers a cross-cloud analytics solution with the ability to analyze data where it is and the flexibility to replicate data when necessary.
   7. BigQuery supports querying Cloud Storage data in the following formats: Comma-separated values (CSV), JSON (newline-delimited), Avro, ORC, Parquet, Datastore exports, Firestore exports

8. Query an external data source in BigQuery by using a permanent table or a temporary table. Querying an external data source using a temporary table is useful for one-time, ad-hoc queries over external data, or for extract, transform, and load (ETL) processes.
9. A federated query is a way to send a query statement to an external database and get the result back as a temporary table.
10. After you submit a BigQuery job, you can view job details, list jobs, cancel a job, repeat a job, or delete job metadata.
11. On-demand queries are charged based on the number of bytes read. You can use the estimate returned by the dry run to calculate query costs in the pricing calculator. If your query processes less than 1 TB, the estimate is $0 because BigQuery provides 1 TB of on-demand query processing free per month.

H. Memorystore : Fully managed in-memory data store service. Fully managed Redis and Memcached for sub-millisecond data access.
I. Secret Manager : Create and access secrets.

X. Pub/Sub is a fully-managed real-time messaging service that allows you to send and receive messages between independent applications.
A. Pub/Sub two services: both horizontally scalable and managed messaging services.
1. **Pub/Sub service.** highest reliability
2. **Pub/Sub Lite service.** built for lower cost. lower reliability
B. A publisher creates and sends messages to a topic and a subscriber creates a subscription to a topic to receive messages from it.

XI. Eventarc allows you to build event-driven architectures without having to implement, customize, or maintain the underlying infrastructure.
A. Use a **Cloud Storage event (via Cloud Audit Logs)** to trigger a data processing pipeline
B. Use a **BigQuery event (via Cloud Audit Logs)** to initiate downstream processing in Cloud Run each time a job is completed

XII. Google Cloud Marketplace lets you quickly deploy functional software packages that run on Google Cloud.

XIII. Database Migration Service makes it easier for you to migrate your data to Google Cloud.

XIV. Datastream : Serverless and easy-to-use change data capture (CDC) and replication service.

XV. Storage Transfer Service provides options that make data transfers and synchronization easier.

XVI. Transfer Appliance is a high-capacity storage device that enables you to transfer and securely ship your data to a Google upload facility, where we upload your data to Cloud Storage.

XVII. **Cloud Source Repositories**
A. Fully featured Git repositories hosted on Google Cloud Platform
B. Supports collaborative development of cloud apps
C. Includes integration with Cloud Debugger

XVIII. **Deployment Manager :** create a set of Google Cloud resources and manage them as a unit, called a *deployment*. A configuration describes all the resources you want for a single deployment.
A. Infrastructure management service, Achieve consistent results, Easy to update
B. Create a .yaml template describing your environment and use Deployment Manager to create resources
C. Provides repeatable deployments

XIX. Cloud Foundation Toolkit : Infrastructure as code templates

XX. Anthos is a modern application management platform that provides a consistent development and operations experience for cloud and on-premises environments.
A. A hybrid and multi-cloud solution
B. Framework rests on Kubernetes and GKE On-Prem

C. Provides a rich set of tools for monitoring and maintenance
D. Anthos Config Management is a service for configuration and policy management that combines three components; Policy Controller, Config Sync, and Config Controller.
E. Config Controller is a hosted service to provision and orchestrate Anthos and Google Cloud resources.
F. Config Connector is an open source Kubernetes addon that allows you to manage Google Cloud resources through Kubernetes. `--addons ConfigConnector`

XXI. **Active Assist** refers to the portfolio of tools used in Google Cloud to generate insights and recommendations to help you optimize your cloud projects.

XXII. **Recommender** is a service provides usage recommendations and insights for Cloud products and services.

XXIII. Cloud Build : Build container images, continuous integration and delivery.

XXIV. Firebase Hosting : Fully managed hosting service for static and dynamic content with configurable CDN caching.

XXV. Google Cloud Armor : Helps protect your applications and websites against denial of service and web attacks.

XXVI. API Gateway : Fully managed API management including routing, authentication, API keys, rate limiting, and quota. The APIs Explorer uses its own API key whenever it makes a request.

XXVII. DATA Analysis

A. Dataflow is a managed service for executing a wide variety of data processing patterns. Cloud Dataflow allows you to perform extract, transform, and load operations.
    1. Throughput is the volume of data that is processed at any point in time.
    2. Dataflow SQL can query the following sources : Pub/Sub topics, Cloud Storage filesets, BigQuery tables.
B. Cloud Dataproc is a cloud-based managed Spark and Hadoop service for batch processing, querying, streaming, and machine learning.
C. Dataprep by Trifacta : An intelligent cloud data service to visually explore, clean, and prepare data for analysis and machine learning.

XXVIII. Cloud Scheduler only allows you to run cron jobs based on a schedule. Cloud Scheduler Schedule and run a cron job Ex. Trigger Cloud Run services on a schedule

XXIX. Cloud Tasks : Execute asynchronous tasks on Cloud Run.

XXX. Data Catalog is a fully managed and highly scalable data discovery and metadata management service in GCP. Data Catalog can leverage the results of a Cloud Data Loss Prevention (DLP) scan to identify sensitive data directly within Data Catalog in the form of tag templates. Provides three main functions:

A. Searching for data entries for which you have access
B. Tagging data entries with metadata
C. Providing column-level security for BigQuery tables

XXXI. Data Studio : Data Studio is a free, self-service business intelligence platform that lets users build and consume data visualizations, dashboards, and reports. With Data Studio, you can connect to your data, create visualizations, and share your insights with others.

XXXII. Identity-Aware Proxy (IAP) TCP forwarding to enable administrative access to VM instances that do not have external IP addresses or do not permit direct access over the internet. Cloud Identity-Aware Proxy (IAP) just lets you establish a central authorization layer for applications accessed by HTTPS.

XXXIII. During a major incident, the status of the issue is communicated through the

A. Google Workspace Status Dashboard : provides status information on the services that are part of Google Workspace
B. Google Cloud Service Health Dashboard : provides status information on the services that are part of Google Cloud.

1. Cymbal Superstore asks you to implement Cloud SQL as a database backend to their supply chain application. You want to configure automatic failover in case of a zone outage. You decide to use the gcloud sql instances create command set to accomplish this. Which gcloud command line argument is required to configure the stated failover capability as you create the required instances?

    a. --availability-type

        i. Correct! This option allows you to specify zonal or regional availability, with regional providing automatic failover to a standby node in another region.

2. Which Virtual Private Cloud (VPC) network type allows you to fully control IP ranges and the definition of regional subnets?

    a. Custom mode network

        i. Correct! A custom mode network gives you control over regions that you place your subnets in and lets you specify IP ranges for them as well.

3. You need to quickly deploy a containerized web application on Google Cloud. You know the services you want to be exposed. You do not want to manage infrastructure. You only want to pay when requests are being handled and need support for custom packages. What technology meets these needs?

    a. Cloud Run

        i. Correct! Cloud Run is serverless, exposes your services as an endpoint, and abstracts all infrastructure.

4. Cymbal Superstore's marketing department needs to load some slowly changing data into BigQuery. The data arrives hourly in a Cloud Storage bucket. You want to minimize cost and implement this in the fewest steps. What should you do?

    a. Use the BigQuery data transfer service to schedule a transfer between your bucket and BigQuery.

        i. Correct! BigQuery transfer service is the simplest process to set up transfers between Cloud Storage and BigQuery. It is encompassed by one command. It is also free.

5. You need to analyze and act on files being added to a Cloud Storage bucket. Your programming team is proficient in Python. The analysis you need to do takes at most 5 minutes. You implement a Cloud Function to accomplish your processing and specify a trigger resource pointing to your bucket. How should you configure the --trigger-event parameter using gcloud?

    a. --trigger-event google.storage.object.finalize

        i. Correct! Finalize event trigger when a write to Cloud Storage is complete.

6. The development team for the supply chain project is ready to start building their new cloud app using a small Kubernetes cluster for the pilot. The cluster should only be available to team members and does not need to be highly available. The developers also need the ability to change the cluster architecture as they deploy new capabilities. How would you implement this?

    a. Implement a private standard zonal cluster in us-central1-a with a default pool and an Ubuntu image.

        i. Correct! Standard clusters can be zonal. The default pool provides nodes used by the cluster.

7. You require a Cloud Storage bucket serving users in New York City. There is a need for geo-redundancy. You do not plan on using ACLs. What CLI command do you use?

    a. Run a gsutil mb command specifying a dual-region bucket and an option to turn ACL evaluation off.

        i. Feedback: Correct! NAM4 implements a dual-region bucket with us-east1 and us-central1 as the configured regions.

8. The backend of Cymbal Superstore's e-commerce system consists of managed instance groups. You need to update the operating system of the instances in an automated way using minimal resources. What do you do?

    a. Create a new instance template, then click Update VMs. Set the update type to PROACTIVE. Click Start.

        i. Correct! This institutes a rolling update where the surge is set to 1 automatically, which minimizes resources as requested.

9. What action does the terraform apply command perform?

    a. Sets up resources requested in the terraform config file

        i. Correct! Terraform Apply sets up resources specified in the terraform config file.

10. Cymbal Superstore's sales department has a medium-sized MySQL database. This database includes user-defined functions and is used internally by the marketing department at Cymbal Superstore HQ. The sales department asks you to migrate the database to Google Cloud in the most timely and economical way. What should you do?

    a. Configure a Compute Engine VM with an N2 machine type, install MySQL, and restore your data to the new instance.

        i. Correct! N2 is a balanced machine type, which is recommended for medium-large databases.

Correct Answer Details:

1. https(s) is an application protocol, so it lives at layer 7 of the TCP stack.
2. Google Kubernetes Engine gives you full control of container orchestration and availability.
3. BigQuery is a data warehouse offering optimized to query historical time-based data. BigQuery can run queries against data in its own column-based store or run federated queries against data from other data services and file stores.

4. Cloud Bigtable is a petabyte scale, NoSQL, column family database with row keys optimized for specific queries. It is used to store historic, time-based data and answers the need for this requirement.
5. A standard tier proxied external load balancer is effectively a regional resource. A regional internal load balancer doesn't require external IPs and is more secure.
6. Data storage pricing is based on the amount of data and storage type. Standard storage is immediately available. Nearline storage is for data accessed roughly every 30 days. Egress is the amount of data read from the bucket and is also chargeable.
7. Compute Engine is a great option for quick migration of traditional apps. You can implement a solution in the cloud without changing your existing code.
8. Compute Engine gives you full control over operating system choice and configuration.
9. Regional>> for performance reasons, you want the storage assets to be close to where the processing is taking place, so a regional storage class makes sense.
10. BigQuery is Google Cloud's implementation of a modern data warehouse. BigQuery analyzes historical data and uses a SQL query engine.
11. Cloud Run provides serverless container management. It lets you focus on code and you can deploy your solution quickly.

Details :

1. Cloud SQL is optimized for transactional reads and writes. It is not a good candidate for querying historical data as described in the scenario.
2. Cloud Spanner is an SQL-compatible relational database, but it is not built for analyzing historical data.
3. Cloud Storage is a large object store and is not queryable. It is not transactional or analytical.
4. Google Kubernetes Engine requires you to build and manage resources of a cluster to host your container in GKE.
5. App Engine is a platform as a service for deployment of your code on infrastructure managed by Google. You don't manage operating system dependencies with App Engine.
6. For performance reasons, storage is required close to where analysis and reporting is happening. Multi-regional is not a good storage type for this use case.
7. Cloud Functions manages your code as short, executable functions and does not manage your code in containers, which are more portable.

---

1. Name 3 robust networking services available to your applications on Google Cloud Platform.
    a. Cloud Virtual Network, Cloud Interconnect, Cloud DNS, Cloud Load Balancing, and Cloud CDN.
2. Name 3 Compute Engine pricing features.
    a. Per-second billing, custom machine types, preemptible instances.
3. Google Cloud Load Balancing lets you balance HTTP traffic across multiple Compute Engine regions.

    a. True

4. Your application transcodes large video files. Which storage service should you consider first?
    a. Google Cloud Storage
5. You stream huge amounts of data from devices with sensors. Which storage service should you consider first?
    a. Google Cloud Bigtable

---

1. Name two reasons for deploying applications using containers.
    a. 1. Portability across development, testing,and production environments
    b. 2. Simpler to migrate workloads
    c. 3. Loose coupling
    d. 4. Agility
2. True or False? Kubernetes lets you manage container clusters in multiple cloud providers.
    a. True But Kubernetes Engine only runs in GCP.
3. True or False? GCP provides a private, high-speed container image storage service for use with Kubernetes Engine.
    a. True It's called Google Container Registry
4. Name 3 advantages of using the App Engine flexible environment over App Engine standard.
    a. The flexible environment allows SSH access, allows disk writes, and supports third-party binaries (also allows stack customization and background processes)
5. What is the difference between Cloud Endpoints and Apigee Edge?
    a. Cloud Endpoints helps you create and maintain APIs; Apigee Edge helps you secure and monetize APIs

---

1. Which data storage service is a unique globally available, horizontally scalable database with relational semantics?
    a. Correct! Cloud Spanner is Google Çloud's globally available, horizontally scalable relational database.
2. Which services are based on logic implemented in containers?
    a. Correct! Cloud Run is a serverless offering that runs your containerized code when monitored events take place.
    b. Correct! Google Kubernetes Engine is Google Cloud's managed Kubernetes environment that lets you deploy containerized apps via pods, deployments, and services you specify.

1. What is the declarative way to initialize and update Kubernetes objects?
    a. **kubectl apply**
        i. Correct! kubectl apply creates and updates Kubernetes objects in a declarative way from manifest files.
2. You want to implement a lifecycle rule that changes your storage type from standard to nearline after a specific date. What conditions should you use? (Pick two).
    a. CreatedBefore
        i. Correct! CreatedBefore lets you specify a date.
    b. MatchesStorageClass
        i. Correct! MatchesStorageClass is required to look for objects with a standard storage type.
3. You have a Cloud Run service with a database backend. You want to limit the number of connections to your database. What should you do?
    a. Set Max instances.
        i. Correct! Max instances control costs, keeping you from starting too many instances by limiting your number of connections to a backing service.
4. Cymbal Superstore's GKE cluster requires an internal http(s) load balancer. You are creating the configuration files required for this resource. What is the proper setting for this scenario?
    a. Annotate your service object with a neg reference.
        i. Correct! because an internal http(s) load balancer can only use NEGs (network endpoint group).
5. Which of the following tasks are part of the process when configuring a managed instance group? (Pick two.)
    a. Defining Health checks
        i. Correct! Health checks are part of your managed instance group configuration.
    b. Providing Number of instances
        i. Correct! Number of instances is part of your managed instance group configuration.
6. You want to view a description of your available snapshots using the command line interface (CLI). What gcloud command should you use?
    a. **gcloud compute snapshots list**
        i. Correct! gcloud commands are built with groups and subgroups, followed by a command, which is a verb. In this example, Compute is the Group, snapshots is the subgroup, and list is the command.

7. Cymbal Superstore has a subnetwork called mysubnet with an IP range of 10.1.2.0/24. You need to expand this subnet to include enough IP addresses for at most 2000 new users or devices. What should you do?

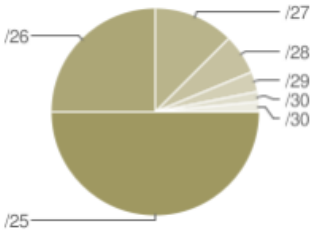
    a. **gcloud compute networks subnets expand-ip-range mysubnet --region us-central1 --prefix-length 21**

        i. Correct! This command gives a total of 2046 addresses available and meets the requirement.

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255

Subnet Mask	Wildcard
255 1111 1111	0 0000 0000
254 1111 1110	1 0000 0001
252 1111 1100	3 0000 0011
248 1111 1000	7 0000 0111
240 1111 0000	15 0000 1111
224 1110 0000	31 0001 1111
192 1100 0000	63 0011 1111
128 1000 0000	127 0111 1111
0 0000 0000	255 1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

8. Cymbal Superstore's supply chain management system has been deployed and is working well. You are tasked with monitoring the system's resources so you can react quickly to any problems. You want to ensure the CPU usage of each of your Compute Engine instances in us-central1 remains below 60%. You want an incident created if it exceeds this value for 5 minutes. You need to configure the proper alerting policy for this scenario. What should you do?

    a. Choose resource type of VM instance and metric of CPU utilization, condition trigger if any time series violates, condition is above, threshold is .60 for 5 minutes.

        i. Correct! All the values of this statement match the scenario.

9. What Kubernetes object provides access to logic running in your cluster via endpoints that you define?

    a. Services

        i. Correct! Service endpoints are defined by pods with labels that match those specified in the service configuration file. Services then specify how those pods are exposed.

10. You have a scheduled snapshot you are trying to delete, but the operation returns an error. What should you do to resolve this problem?
    a. Detach the snapshot schedule before deleting it.
        i. Correct! You can't delete a snapshot schedule that is still attached to a persistent disk.

---

1. What GKE object implements an http(s) load balancer?
    a. Correct! Ingress objects implement an http(s) load balancer based on upstream services you specify in your configuration file.
2. Which Cloud Run autoscaling setting should you set if you want to limit cost?
    a. Correct! Max instances directly affects cost by limiting the maximum amount of container instances deployed.

---

1. **Outline where Cloud Audit logs can be accessed: in the logging tab of the operations interface**
   Link: https://cloud.google.com/storage/docs/audit-logging

   You are configuring audit logging for Cloud Storage. You want to know when objects are added to a bucket. Which type of audit log entry should you monitor?
    a. DATA_WRITE log entries
        i. Correct! DATA_WRITE log entries include information about when objects are created or deleted.
2. Which Cloud Audit log is disabled by default with a few exceptions?
    a. Data Access audit logs
        i. Correct! Data Access audit logs are disabled by default except for BigQuery.
3. You need to configure access to Cloud Spanner from the GKE cluster that is supporting Cymbal Superstore's ecommerce microservices application. You want to specify an account type to set the proper permissions. What should you do?
    a. Assign permissions through service account referenced by the application
        i. Correct! A service account uses an account identity and an access key. It is used by applications to connect to services.
4. You are trying to assign roles to the dev and prod projects of Cymbal Superstore's e-commerce app but are receiving an error when you try to run **set-iam policy**. The projects are organized into an ecommerce folder in the Cymbal Superstore organizational hierarchy. You want to follow best practices for the permissions you need while respecting the practice of least privilege. What should you do?
    a. Ask your administrator for the **roles/resourcemanager.folderIamAdmin** for the ecommerce folder

i. Correct! This choice gives you the required permissions while minimizing the number of individual resources you have to set permissions for.

5. Which of the scenarios below is an example of a situation where you should use a service account?
    a. For individual GKE pods
        i. Correct! When configuring access for GKE, you set up dedicated service accounts for each pod. You then use workload identity to map them to dedicated Kubernetes service accounts.
6. You have a custom role implemented for administration of the dev/test environment for Cymbal Superstore's transportation management application. You are developing a pilot to use Cloud Run instead of Cloud Functions. You want to ensure your administrators have the correct access to the new resources. What should you do?
    a. Make the change to the custom role locally and run an update on the custom role
        i. Correct! There is a recommended process to update an existing custom role. You get the current policy, update it locally, and write the updated policy back into Google Cloud. The gcloud commands used in this process include the get and update policy subcommands.
7. Cymbal Superstore is implementing a mobile app for end users to track deliveries that are en route to them. The app needs to access data about truck location from Pub/Sub using Google recommended practices. What kind of credentials should you use?
    a. Service account key
        i. Correct! Service account keys are used for accessing private data such as your Pub/Sub truck information from an external environment such as a mobile app running on a phone.

---

1. You are authenticating an application to service APIs. Both resources are internal to the Google Cloud environment. What type of credentials should you use?
    a. Temporary credentials
        i. Correct! You should use temporary credentials of the service account provided by the environment.
2. What kind of account is meant for machine-to-machine communication in Google Cloud?
    a. Service account
        i. Correct! Service accounts are designed to provide permissions for machine-to machine or service-to-service communications in Google Cloud.

I. Instance templates are used to create a group of identical VMs. The instance templates include:
    A. Machine type, boot disk image or container image, zone, and labels

B. Cloud Storage bucket definitions
C. A load balancer description
D. App Engine configuration file
    1. Machine type, boot disk image or container image, zone, and labels are all configuration parameters or attributes of a VM and therefore would be included in an instance group configuration that creates those VMs.

II. The command-line command to create a Cloud Storage bucket is:
A. gcloud mb
B. gsutil mb
C. gcloud mkbucket
D. gsutil mkbucket
    1. gsutil is the command line for accessing and manipulating Cloud Storage from the CLI. mb is the specific command for creating, or making, a bucket.

III. Your company has an object management policy that requires that objects stored in Cloud Storage be migrated from regional storage to nearline storage 90 days after the object is created. The most efficient way to do this is to:
A. Create a cloud function to copy objects from regional storage to nearline storage.
B. Set the MigrateObjectAfter property on the stored object to 90 days.
C. Copy the object to persistent storage attached to a VM and then copy the object to a bucket created on nearline storage.
D. Create a lifecycle management configuration policy specifying an age of 90 days and SetStorageClass as nearline.
    1. The lifecycle configuration policy allows administrators to specify criteria for migrating data to other storage systems without having to concern themselves with running jobs to actually execute the necessary steps.

IV. An education client maintains a site where users can upload videos, and your client needs to assure redundancy for the files; therefore, you have created two buckets for Cloud Storage. Which command do you use to synchronize the contents of the two buckets?
A. gsutil rsync
B. gcloud cp sync
C. gcloud rsync
D. gsutil cp sync
    1. gsutil is the command-line tool for working with Cloud Storage. rsync is the specific command in gsutil for synchronizing buckets

V. VPCs are resources.

A. Regional
B. Zonal
C. Global
D. Subnet
    1. Google operates a global network, and VPCs are resources that can span that global network

VI. A remote component in your network has failed, which results in a transient network error. When you submit a gsutil command, it fails because of a transient error. By default, the command will:
    A. Terminate and log a message to Stackdriver
    B. Retry using a truncated binary exponential back-off strategy
    C. Prompt the user to decide to retry or quit
    D. Terminate and log a message to Cloud Shell
        1. gcloud by default will retry a failed network operation and will wait a long time before each retry. The time to wait is calculated using a truncated binary exponential back-off strategy

VII. All of the following are components of firewall rules except which one?
    A. Direction of traffic
    B. Action on match
    C. Time to live (TTL)
    D. Protocol
        1. Firewall rules do not have TTL parameters. Direction of traffic, action on match, and protocol are all components of firewall rules

VIII. Adding virtual machines to an instance group can be triggered in an autoscaling policy by all of the following, except which one?
    A. CPU utilization
    B. Stackdriver metrics
    C. IAM policy violation
    D. Load balancing serving capacity
        1. IAM policy violations do not trigger changes in the size of clusters. All other options can be used to trigger a change in cluster size

IX. Your company's finance department is developing a new account management application that requires transactions and the ability to perform relational database operations using fully compliant SQL. Data store options in GCP include:
    A. Spanner and Cloud SQL

B. Datastore and Bigtable
C. Spanner and Cloud Storage
D. Datastore and Cloud SQL
    1. Only Spanner and Cloud SQL databases support transactions and have a SQL interface. Datastore has transactions but does not support fully compliant SQL; it has a SQL-like query language. Cloud Storage does not support transactions or SQL

X. The marketing department in your company wants to deploy a web application but does not want to have to manage servers or clusters. A good option for them is:
A. Compute Engine
B. Kubernetes Engine
C. App Engine
D. Cloud Functions
    1. App Engine is a PaaS that allows developers to deploy full applications without having to manage servers or clusters. Compute Engine and Kubernetes Engine require management of servers. Cloud Functions is suitable for short-running Node.js or Python functions but not full applications

XI. Your company is building an enterprise data warehouse and wants SQL query capabilities over petabytes of data, but does not want to manage servers or clusters. A good option for them is:
A. Cloud Storage
B. BigQuery
C. Bigtable
D. Datastore
    1. BigQuery is designed for petabyte-scale analytics and provides a SQL interface

XII. You have been hired as a consultant to a startup in the Internet of Things (IoT) space. The startup will stream large volumes of data into GCP. The data needs to be filtered, transformed, and analyzed before being stored in GCP Datastore. A good option for the stream processing component is:
A. Dataproc
B. Cloud Dataflow
C. Cloud Endpoints
D. Cloud Interconnect

1. Cloud Dataflow allows for stream and batch processing of data and is well suited for this kind of ETL work. Dataproc is a managed Hadoop and Spark service that is used for big data analytics. Cloud Endpoints is an API service, and Cloud Interconnect is a network service

XIII. Preemptible virtual machines may be shut down at any time but will always be shut down after running:

A. 6 hours
B. 12 hours
C. 24 hours
D. 48 hours

1. If a preemptible machine has not been shut down within 24 hours, Google will stop the instance

XIV. You have been tasked with designing an organizational hierarchy for managing departments and their cloud resources. What organizing components are available in GCP?

A. Organization, folders, projects
B. Buckets, directories, subdirectories
C. Organizations, buckets, projects
D. Folders, buckets, projects

1. Organizations, folders, and projects are the components used to manage an organizational hierarchy. Buckets, directories, and subdirectories are used to organize storage

XV. During an incident that has caused an application to fail, you suspect some resource may not have appropriate roles granted. The command to list roles granted to a resource is:

A. gutil iam list-grantable-roles
B. gcloud iam list-grantable-roles
C. gcloud list-grantable-roles
D. gcloud resources grantable-roles

1. gcloud is the command-line tool for working with IAM, and list-grantable-roles is the correct command

XVI. The availability of CPU platforms can vary between zones. To get a list of all CPU types available in a particular zone, you should use:

A. gcloud compute zones describe
B. gcloud iam zones describe
C. gutil zones describe
D. gcloud compute regions list

1. gcloud is the command-line tool for manipulating compute resources, and zones describe is the correct command

XVII. To create a custom role, a user must possess which role?

A. iam.create
B. compute.roles.create
C. iam.roles.create
D. Compute.roles.add

1. iam.roles.create is correct; the other roles do not exist

XVIII. You have been asked to create a network with 1,000 IP addresses. In the interest of minimizing unused IP addresses, which CIDR suffix would you use to create a network with at least 1,000 addresses but no more than necessary?

A. /20
B. /22
C. /28
D. /32

1. The /22 suffix produces 1,022 usable IP addresses

XIX. A team of data scientists have asked for your help setting up an Apache Spark cluster. You suggest they use a managed GCP service instead of managing a cluster themselves on Compute Engine. The service they would use is:

A. Cloud Dataproc
B. Cloud Dataflow
C. Cloud Hadoop
D. BigQuery

1. A. Cloud Dataproc is the managed Spark service. Cloud Dataflow is for stream and batch processing of data, BigQuery is for analytics, and Cloud Hadoop is not a GCP service

XX. You have created a web application that allows users to upload files to Cloud Storage. When files are uploaded, you want to check the file size and update the user's total storage used in their account. A serverless option for performing this action on load is:

A. Cloud Dataflow
B. Cloud Dataproc
C. Cloud Storage
D. Cloud Functions

1. Cloud Functions responds to events in Cloud Storage, making them a good choice for taking an action after a file is loaded

XXI. Your company has just started using GCP, and executives want to have a dedicated connection from your data center to the GCP to allow for large data transfers. Which networking service would you recommend?

A. Google Cloud Carrier Internet Peering
B. Google Cloud Interconnect – Dedicated
C. Google Cloud Internet Peering
D. Google Cloud DNS

1. Google Cloud Interconnect – Dedicated is the only option for a dedicated connection between a customer's data center and a Google data center

XXII. You want to have GCP manage cryptographic keys, so you've decided to use Cloud Key Management Services. Before you can start creating cryptographic keys, you must:

A. Enable Google Cloud Key Management Service (KMS) API and set up billing
B. Enable Google Cloud KMS API and create folders
C. Create folders and set up billing
D. Give all users grantable roles to create keys

1. Enabling the Google Cloud KMS API and setting up billing are steps common to using GCP services

XXIII. In Kubernetes Engine, a node pool is:

A. A subset of nodes across clusters
B. A set of VMs managed outside of Kubernetes Engine
C. A set of preemptible VMs
D. A subset of node instances within a cluster that all have the same configuration

1. A node pool is a subset of node instances within a cluster that all have the same configuration

XXIV. The GCP service for storing and managing Docker containers is:

A. Cloud Source Repositories
B. Cloud Build
C. Container Registry
D. Docker Repository

1. The GCP service for storing and managing Docker containers is Container Registry. Cloud Build is for creating images. The others are not GCP services

XXV. Code for Cloud Functions can be written in

A. Node.js and Python
B. Node.js, Python, and Go
C. Python and Go

D. Python and C
    1. Node.js 6, Node.js 8, and Python are the languages supported by Cloud Functions

---

1. How do you scale a Cloud Bigtable database if more queries per second are needed?
    a. Add more nodes
        i. To add more queries per second to a Cloud Bigtable cluster, simply add more nodes.
2. You are looking for an unstructured storage solution for archiving files that might never be accessed again. Which of the following is the best option?
    a. Cloud Storage Coldline class
        i. Cloud Storage Coldline storage is designed for long term storage of data that is typically not accessed more than once a year.
3. Which of the following is a multi-regional, globally available, managed relational database service?
    a. Cloud Spanner
        i. Cloud Spanner is a multi-regional, globally available managed relational database service.
4. What protocol is used by REST APIs?
    a. HTTP
        i. HTTP is the protocol used with REST APIs.
5. Which of the following API Management Systems can be used on legacy systems?
    a. Apigee Edge
        i. Apigee Edge is designed to be used with both cloud and legacy systems.
6. Select the option that is not a feature of Cloud Pub/Sub.
    a. Can process messages as they enter the queue
        i. Cloud Pub/Sub is not a messaging processing service. You write your applications to process the messages stored in Cloud Pub/Sub.
7. If a Cloud IAM policy gives you Owner permissions at the project level, your access to a resource in the project may be restricted by a more restrictive policy on that resource.
    a. False
        i. Policies are a union of the parent and the resource. If a parent policy is less restrictive, it overrides a more restrictive resource policy.
8. How are user identities created in Cloud IAM?

    a. User identities are created outside of Google Cloud using a Google-administered domain
        i. Creating users and groups within Google Cloud is not possible.
9. Which of the following is not an encryption option for Google Cloud?
    a. Scripted encryption keys is not an option with Google Cloud.
10. Select the global load balancer from the list.
    a. TCP Proxy
        i. The global load balancer is a TCP proxy.
11. What is a key distinguishing feature of networking in Google Cloud?
    a. Network topology is not dependent on the IP address layout. : Correct
12. Which one of the following is true?
    a. VPCs are global and subnets are regional.
13. Which of the following is true concerning Cloud Deployment Manager?
    a. Cloud Deployment Manager is a declarative tool
        i. Cloud Deployment Manager is a declarative tool. You're creating a configuration file in YAML format that is the configuration of the infrastructure.
14. Which of the following best describes infrastructure as code?
    a. Tool that automates the construction of an entire infrastructure
        i. Infrastructure as code tools are used to automate the construction of an entire infrastructure.
15. What service allows you to inspect detailed latency information for a single request or view aggregate latency for your entire application?
    a. Cloud Trace
        i. Cloud Trace is used to sample the latency of an application.
16. Which of the following is true concerning BigQuery?
    a. BigQuery is a fully managed service
        i. BigQuery is a fully managed service. You aren't required to build servers or manage storage.
17. Which managed service should you use if you want to do a lift and shift of an existing Hadoop cluster without having to rewrite your Spark code?
    a. Dataproc
        i. Dataproc is the best option if you want to take your existing Hadoop cluster and build something similar in the cloud.

18. Which of the following services leverages the Apache Beam SDK to perform ETL operations on both batch and streaming data?
    a. Dataflow
        i. Dataflow is a serverless managed service that can perform ETL operations on batch and streaming data using the Apache Beam SDK.

19. Consider a single hierarchy of Google Cloud resources. Which of these situations is possible? (Choose 3 responses.)
    a. There is no organization node, and there are no folders.
    b. There is an organization node, and there is at least one folder.
    c. There is an organization node, and there are no folders.
20. When would you choose to have an organization node? (Select two)
    a. When you want to create folders
    b. When you want to centrally apply organization-wide policies
21. How does the resource hierarchy control how IAM policies are inherited?
    a. IAM policies that are implemented by lower-level policies can override the policies defined at a higher level.
22. What is the difference between Identity and Access Management (IAM) basic roles and IAM predefined roles?
    a. Basic roles affect all resources in a Google Cloud project. Predefined roles apply to a specific service in a project.
23. Which way of accessing Google Cloud lets you control services through the code you write?
    a. APIs
24. Your company has two Google Cloud projects and you want them to share policies. What is the least error-prone way to set this up?
    a. Place both projects into a folder, and define the policies on that folder.
25. Which statement best describes how Google Cloud resources are associated within the resource hierarchy?
    a. All Google Cloud resources are associated with a project.
26. Select the option that displays IAM roles from general to specific.
    a. Basic roles, predefined roles, custom roles
27. Select the true statement about Google's VPC networks and subnets.
    a. Networks are global, and subnets are regional.
28. Which statement best describes how VPC routers and firewalls work?
    a. They are managed by Google as a built-in feature.

29. A Google Cloud customer wants to load-balance traffic among the backend VMs that form part of a multi-tier application. Which load-balancing option should this customer choose?
    a. The regional internal load balancer
30. Which interconnect option is a service level agreement (SLA) available for?
    a. Dedicated Interconnect
31. Preemptible VMs can offer advantages over a standard Compute Engine VM. What is a reason customers choose preemptible VMs?
    a. To reduce cost
        i. That's correct! The per-hour price of preemptible VMs incorporates a substantial discount.
32. An application running in a Compute Engine virtual machine needs high-performance scratch space. Which type of storage meets this need?
    a. Local SSD
33. Which term describes a secure, individual, private cloud-computing model hosted within a public cloud?
    a. Virtual private cloud (VPC)
34. Which database service can scale to higher database sizes?
    a. Cloud Spanner
35. Your application needs to store data with strong transactional consistency, and you want seamless scaling up. Which storage option is the best choice for your application?
    a. Cloud Spanner
36. Which statement describes the correct Cloud Storage use case?
    a. Cloud Storage provides durable and highly available object storage.
37. You manufacture devices with sensors and need to stream huge amounts of data from these devices to a storage option in the cloud. Which storage option is the best choice for your application?
    a. Bigtable
38. How are Firestore and Bigtable alike? (Select two answers.)
    a. They are both NoSQL databases.
    b. They are both highly scalable.
39. Why would a customer consider the Coldline Storage class?
    a. To save money on storing infrequently accessed data
40. Where do the resources used to build Google Kubernetes Engine clusters come from?
    a. Compute Engine
41. Select two reasons for using containers to deploy applications. (Choose 2 responses.)

    a. It creates consistency across development, testing, and production environments.
    b. Migrating workloads is simpler.

42. Anthos provides a rich set of tools for monitoring and maintaining the consistency of your applications across which of the following locations?
    a. Applications hosted on-premises, in the cloud, or in multiple clouds.
43. How do containers access an operating system?
    a. Containers use a shared base operating system stored in a shared kernel layer.
44. What is a Kubernetes pod?
    a. A group of containers
45. What is a Kubernetes cluster?
    a. A group of machines where Kubernetes can schedule workloads.
46. How do you keep your Kubernetes version updated in Google Kubernetes Engine?
    a. The Google Kubernetes Engine team periodically performs automatic upgrades of your cluster to newer stable versions.
47. Cloud Run can only pull images from:
    a. Artifact Registry
48. Which Google Cloud service should you choose to perform business analytics and billing on a customer-facing API?
    a. Apigee Edge
49. Select the managed compute platform that lets you run stateless containers through web requests or Pub/Sub events.
    a. Cloud Run
50. Which statements are true about App Engine? (Select 2).
    a. App Engine manages the hardware and networking infrastructure required to run your code.
    b. The daily billing for an App Engine application can drop to zero.
51. App Engine is best suited to the development and hosting of which type of application?
    a. A web application
52. What are the advantages of using App Engine's flexible environment instead of its standard environment? (Select 3).
    a. You can install third-party binaries.
    b. You can use SSH to connect to the virtual machines on which your application runs.
    c. Your application can write to the local disk.
53. Why might a Google Cloud customer choose to use Cloud Functions?

    a. Their application contains event-driven code that they don't want to provision compute resources for.

54. Why would a developer choose to store source code in Cloud Source Repositories? (Select 2)
    a. To keep code private to a Google Cloud project
    b. To reduce work

55. Why might a Google Cloud customer choose to use Terraform?
    a. Terraform can be used as an infrastructure management system for Google Cloud resources.

56. Select the advantage of putting the event-driven components of your application into Cloud Functions.
    a. Cloud Functions handles scaling these components seamlessly.

57. Select the two correct statements about Cloud Logging.
    a. Cloud Logging lets you define metrics based on your logs.
    b. Cloud Logging lets you view logs from your applications and filter and search on them.

58. There are "Four Golden Signals" that measure a system's performance and reliability. What are they?
    a. Latency, traffic, saturation, errors

59. Which option describes a commitment made to your customers that your systems and applications will have only a certain amount of "downtime"?
    a. Service level agreement

60. Which definition best describes a service level indicator (SLI)?
    a. A time-bound measurable attribute of a service

61. You want to create alerts on your Google Cloud resources, such as when health checks fail. Which is the best Google Cloud product to use?
    a. Cloud Monitoring

62. Which of the following is not a type of IAM role?
    a. Advanced
        i. correct! There are three types of roles in IAM: basic roles, predefined roles, and custom roles. There are no "advanced" roles in IAM.

63. What abstraction is primarily used to administer user access in IAM ?
    a. Roles, an abstraction of job roles.

i. IAM administration uses pre-defined roles for administration of user access. The roles are defined by more granular permissions. But permissions are not applied to users directly, only through the roles that are assigned to them.

64. Which of the following is not a type of IAM member?
    a. Organization Account
        i. correct! There are five different types of members: Google Accounts, Service Accounts, Google Groups, Google Workspace domain, and Cloud Identity domains. There are no "Organization Accounts" in IAM.

---

1. **Your company has reserved a monthly budget for your project. You want to be informed automatically of your project spend so that you can take action when you approach the limit. What should you do?**
    a. Link a credit card with a monthly limit equal to your budget.
    b. Create a budget alert for 50%, 90%, and 100% of your total monthly budget.
    c. In App Engine Settings, set a daily budget at the rate of 1/30 of your monthly budget.
    d. In the GCP Console, configure billing export to BigQuery. Create a saved view that queries your total spend.
2. **You are creating a Kubernetes Engine cluster to deploy multiple pods inside the cluster. All container logs must be stored in BigQuery for later analysis. You want to follow Google-recommended practices. Which two approaches can you take?**
    a. Turn on Stackdriver Logging during the Kubernetes Engine cluster creation.
    b. Turn on Stackdriver Monitoring during the Kubernetes Engine cluster creation.
    c. Develop a custom add-on that uses Cloud Logging API and BigQuery API. Deploy the add-on to your Kubernetes Engine cluster.
    d. Use the Stackdriver Logging export feature to create a sink to Cloud Storage. Create a Cloud Dataflow job that imports log files from Cloud Storage to BigQuery.
    e. Use the Stackdriver Logging export feature to create a sink to BigQuery. Specify a filter expression to export log records related to your Kubernetes Engine cluster only.
3. **You have an application server running on Compute Engine in the europe-west1-d zone. You need to ensure high availability and replicate the server to the europe-west2-c zone using the fewest steps possible. What should you do?**
    a. Create a snapshot from the disk. Create a disk from the snapshot in the europe-west2-c zone. Create a new VM with that disk.
    b. Create a snapshot from the disk. Create a disk from the snapshot in the europe-west1-d zone and then move the disk to europe-west2-c. Create a new VM with that disk.
    c. Use "gcloud" to copy the disk to the europe-west2-c zone. Create a new VM with that disk.
    d. Use "gcloud compute instances move" with parameter "--destination-zone europe-west2-c" to move the instance to the new zone.
4. **You are a project owner and need your co-worker to deploy a new version of your application to App Engine. You want to follow Google's recommended practices. Which IAM roles should you grant your co-worker?**
    a. Project Editor
    b. App Engine Service Admin

c. App Engine Deployer
d. App Engine Code Viewer

5. **You want to find out who in your organization has Owner access to a project called "my-project". What should you do?**
   a. In the Google Cloud Platform Console, go to the IAM page for your organization and apply the filter "Role:Owner".
   b. In the Google Cloud Platform Console, go to the IAM page for your project and apply the filter "Role:Owner".
   c. Use "gcloud iam list-grantable-role --project my-project" from your Terminal.
   d. Use "gcloud iam list-grantable-role" from Cloud Shell on the project page.
6. **You created an update for your application on App Engine. You want to deploy the update without impacting your users. You want to be able to roll back as quickly as possible if it fails. What should you do?**
   a. Delete the current version of your application. Deploy the update using the same version identifier as the deleted version.
   b. Notify your users of an upcoming maintenance window. Deploy the update in that maintenance window.
   c. Deploy the update as the same version that is currently running.
   d. Deploy the update as a new version. Migrate traffic from the current version to the new version.
7. **Your application has a large international audience and runs stateless virtual machines within a managed instance group across multiple locations. One feature of the application lets users upload files and share them with other users. Files must be available for 30 days; after that, they are removed from the system entirely. Which storage solution should you choose?**
   a. A Cloud Datastore database.
   b. A multi-regional Cloud Storage bucket.
   c. Persistent SSD on virtual machine instances.
   d. A managed instance group of Filestore servers.
8. **You need to verify the assigned permissions in a custom IAM role. What should you do?**
   a. Use the GCP Console, IAM section to view the information.
   b. Use the "gcloud init" command to view the information.
   c. Use the GCP Console, Security section to view the information.
   d. Use the GCP Console, API section to view the information.
9. **Your project has all its Compute Engine resources in the europe-west1 region. You want to set europe-west1 as the default region for gcloud commands. What should you do?**
   a. Use Cloud Shell instead of the command line interface of your device. Launch Cloud Shell after you navigate to a resource in the europe-west1 region. The europe-west1 region will automatically become the default region.
   b. Use "gcloud config set compute/region europe-west1" to set the default region for future gcloud commands.
   c. Use "gcloud config set compute/zone europe-west1" to set the default region for future gcloud commands.
   d. Create a VPN from on-premises to a subnet in europe-west1, and use that connection when executing gcloud commands.
10. **Your company has a mission-critical application that serves users globally. You need to select a transactional, relational data storage system for this application. Which two products should you consider?**
    a. BigQuery

b. Cloud SQL
c. Cloud Spanner
d. Cloud Bigtable
e. Cloud Datastore

---

1. **You are designing a mobile game which you hope will be used by numerous users around the world. The game backend requires a Relational DataBase Management System (RDBMS) for persisting game state and player profiles. You want to select a database that can scale to a global audience with minimal configuration updates. Which database should you choose?**
    a. Cloud Firestore.
    b. Cloud Spanner.
    c. Cloud SQL.
    d. Cloud Datastore.
2. **You want to list all the compute instances in zones us-central1-b and europe-west1-d. Which of the commands below should you run to retrieve this information?**
    a. gcloud compute instances get --filter="zone:(us-central1-b)" and gcloud compute instances list --filter="zone:(europe-west1-d)" and combine the results.
    b. gcloud compute instances list --filter="zone:(us-central1-b)" and gcloud compute instances list --filter="zone:(europe-west1-d)" and combine the results.
    c. gcloud compute instances list --filter="zone:(us-central1-b europe-west1-d)"
    d. gcloud compute instances get --filter="zone:(us-central1-b europe-west1-d)"
3. **Which of the below mentioned claims about Cloud Storage is false?**
    Cloud Storage buckets may have retention periods.
    a. Cloud Storage does not allow access of block-level to the data within files that are stored in buckets.
    b. Lifecycle configurations are used in altering the storage class from regional to multiregional.
    c. Cloud Storage is designed for high durability.
    d. None of these
4. **While running a Second Generation MySQL database in Cloud SQL, which of the following features can be configured?**
    a. Failover replicas can be configured
    b. All of these can be configured
    c. Maintenance windows can be configured
    d. Machine type can be configured
    e. None of these
5. **You want to create a new role and grant it to the SME team. The new role should provide your SME team BigQuery Job User and Cloud Bigtable User roles on all projects in the organization. You want to minimize operational overhead. You want to follow Google recommended practices. How should you create the new role?**
    a. Execute command gcloud iam combineroles --global to combine the 2 roles into a new custom role and grant them globally to SME team group.
    b. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Use gcloud iam promote-role to promote the role to all other projects and grant the role in each project to the SME team group.
    c. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at the organization level.

    d. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Repeat this step for each project.
6. **You have a collection of audio/video files over 80GB each that you need to migrate to Google Cloud Storage. The files are in your on-premises data center. What migration method can you use to help speed up the transfer process?**
    a. Use the Cloud Transfer Service to transfer.
    b. Start a recursive upload.
    c. Use parallel uploads to break the file into smaller chunks then transfer it simultaneously.
    d. Use multithreaded uploads using the -m option.
7. **A mission-critical application running on a Managed Instance Group (MIG) in Google Cloud has been having scaling issues. Although the scaling works, it is not quick enough, and users experience slow response times. The solution architect has recommended moving to GKE to achieve faster scaling and optimize machine resource utilization. Your colleague containerized the application and provided you with a Dockerfile. You now need to deploy this in a GKE cluster. How should you do it?**
    Deploy the application using kubectl app deploy .
    a. Deploy the application using gcloud app deploy .
    b. Build a container image from the Dockerfile and push it to Google Container Registry (GCR). Create a Kubernetes Deployment YAML file and have it use the image from GCR. Use kubectl apply -f to deploy the application to the GKE cluster.
    c. Build a container image from the Dockerfile and push it to Google Cloud Storage (GCS). Create a Kubernetes Deployment YAML file and have it use the image from GCS. Use kubectl apply -f to deploy the application to the GKE cluster.
8. **As per the company policies of TPT Ltd. it is critical to back the Datastore database at least once a day. John has been asked to explain about the sufficiency of the Datastore export, to an Auditor. Which of the following should John use to explain the outputs generated by the Datastore export command?**
    a. The Datastore export commands produces a Metadata file as an output
    b. The Datastore export commands produces A single entity file as an output
    c. The Datastore export commands produces A metadata file, an entity file, and a folder with the data as an output
    d. The Datastore export commands produces a metadata file and a folder with the data as an output
    e. None of these

---

01. You are a project owner and need your co-worker to deploy a new version of your application to App Engine. You want to follow Google's recommended practices. Which IAM roles should you grant your co-worker?
    a. Project Editor
    b. App Engine Service Admin
    c. App Engine Deployer
    d. App Engine Code Viewer
        i. https://cloud.google.com/iam/docs/understanding-roles
02. Your company has reserved a monthly budget for your project. You want to be informed automatically of your project spend so that you can take action when you approach the limit. What should you do?
    a. Link a credit card with a monthly limit equal to your budget.
    b. B. Create a budget alert for 50%, 90%, and 100% of your total monthly budget.
    c. In App Engine Settings, set a daily budget at the rate of 1/30 of your monthly budget.

    d. D. In the GCP Console, configure billing export to BigQuery. Create a saved view that queries your total spend.
    e. https://cloud.google.com/appengine/pricing#spending_limit
    f. https://cloud.google.com/billing/docs/how-to/budgets
03. You have a project using BigQuery. You want to list all BigQuery jobs for that project. You want to set this project as the default for the bq command-line tool. What should you do?
    a. A. Use "gcloud config set project" to set the default project.
    b. B. Use "bq config set project" to set the default project.
    c. C. Use "gcloud generate config-url" to generate a URL to the Google Cloud Platform Console to set the default project.
    d. D. Use "bq generate config-url" to generate a URL to the Google Cloud Platform Console to set the default project.
    e. https://cloud.google.com/bigquery/docs/reference/bq-cli-reference
    f. https://cloud.google.com/sdk/gcloud/reference/config/set
04. Your project has all its Compute Engine resources in the europe-west1 region. You want to set europe-west1 as the default region for gcloud commands. What should you do?
    a. Use Cloud Shell instead of the command line interface of your device. Launch Cloud Shell after you navigate to a resource in the europe-west1 region. The europe-west1 region will automatically become the default region.
    b. Use "gcloud config set compute/region europe-west1" to set the default region for future gcloud commands.
    c. Use "gcloud config set compute/zone europe-west1" to set the default region for future gcloud commands.
    d. Create a VPN from on-premises to a subnet in europe-west1, and use that connection when executing gcloud commands.
    e. https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region
05. You developed a new application for App Engine and are ready to deploy it to production. You need to estimate the costs of running your application on Google Cloud Platform as accurately as possible. What should you do?
    a. Create a YAML file with the expected usage. Pass this file to the "gcloud app estimate" command to get an accurate estimation.
    b. Multiply the costs of your application when it was in development by the number of expected users to get an accurate estimation.
    c. Use the pricing calculator for App Engine to get an accurate estimation of the expected charges.
    d. D. Create a ticket with Google Cloud Billing Support to get an accurate estimation.
06. Your company processes high volumes of IoT data that are time-stamped. The total data volume can be several petabytes. The data needs to be written and changed at a high speed. You want to use the most performant storage option for your data. Which product should you use?
    a. Cloud Datastore
    b. Cloud Storage
    c. Cloud Bigtable
    d. D. BigQuery
        i. Cloud Bigtable is the most performant storage option to work with IoT and time series data.
    e. https://cloud.google.com/bigtable/docs/schema-design-time-series
07. Your application has a large international audience and runs stateless virtual machines within a managed instance group across multiple locations. One feature of the application lets users upload files and share them with other users. Files must be available for 30 days; after that, they are removed from the system entirely. Which storage solution should you choose?
    a. A Cloud Datastore database.
    b. A multi-regional Cloud Storage bucket.
    c. Persistent SSD on virtual machine instances.
    d. A managed instance group of Filestore servers.
        i. buckets can be multi-regional and have lifecycle management.
08. You have a definition for an instance template that contains a web application. You are asked to deploy the application so that it can scale based on the HTTP traffic it receives. What should you do?

a. Create a VM from the instance template. Create a custom image from the VM's disk. Export the image to Cloud Storage. Create an HTTP load balancer and add the Cloud Storage bucket as its backend service.
b. Create a VM from the instance template. Create an App Engine application in Automatic Scaling mode that forwards all traffic to the VM.
c. Create a managed instance group based on the instance template. Configure autoscaling based on HTTP traffic and configure the instance group as the backend service of an HTTP load balancer.
d. D. Create the necessary amount of instances required for peak user traffic based on the instance template. Create an unmanaged instance group and add the instances to that instance group. Configure the instance group as the Backend Service of an HTTP load balancer.
    i. managed instance group can use an instance template to scale based on HTTP traffic.
e. https://cloud.google.com/compute/docs/instance-groups/#managed_instance_groups_and_autoscaling
f. https://cloud.google.com/compute/docs/images/export-image
g. https://cloud.google.com/compute/docs/load-balancing/http/adding-a-backend-bucket-to-content-based-load-balancing

09. You are creating a Kubernetes Engine cluster to deploy multiple pods inside the cluster. All container logs must be stored in BigQuery for later analysis. You want to follow Google-recommended practices. Which 2 approaches can you take?
    a. Turn on Stackdriver Logging during the Kubernetes Engine cluster creation.
    b. Turn on Stackdriver Monitoring during the Kubernetes Engine cluster creation.
    c. Develop a custom add-on that uses Cloud Logging API and BigQuery API. Deploy the add-on to your Kubernetes Engine cluster.
    d. Use the Stackdriver Logging export feature to create a sink to Cloud Storage. Create a Cloud Dataflow job that imports log files from Cloud Storage to BigQuery.
    e. Use the Stackdriver Logging export feature to create a sink to BigQuery. Specify a filter expression to export log records related to your Kubernetes Engine cluster only.
        i. creating a cluster with Stackdriver Logging option will enable all the container logs to be stored in Stackdriver Logging. Stackdriver Logging support exporting logs to BigQuery by creating sinks
    f. https://cloud.google.com/kubernetes-engine/docs/how-to/logging
    g. https://cloud.google.com/logging/docs/export/configure_export_v2
    h. https://kubernetes.io/docs/reference/labels-annotations-taints/
10. You need to create a new Kubernetes Cluster on Google Cloud Platform that can autoscale the number of worker nodes. What should you do?
    a. Create a cluster on Kubernetes Engine and enable autoscaling on Kubernetes Engine.
    b. Create a cluster on Kubernetes Engine and enable autoscaling on the instance group of the cluster.
    c. Configure a Compute Engine instance as a worker and add it to an unmanaged instance group. Add a load balancer to the instance group and rely on the load balancer to create additional Compute Engine instances when needed.
    d. Create Compute Engine instances for the workers and the master, and install Kubernetes. Rely on Kubernetes to create additional Compute Engine instances when needed.
    e. https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler
11. You have an application server running on Compute Engine in the europe-west1-d zone. You need to ensure high availability and replicate the server to the europe-west2-c zone using the fewest steps possible. What should you do?
    a. Create a snapshot from the disk. Create a disk from the snapshot in the europe-west2-c zone. Create a new VM with that disk.
    b. Create a snapshot from the disk. Create a disk from the snapshot in the europe-west1-d zone and then move the disk to europe-west2-c. Create a new VM with that disk.
    c. Use "gcloud" to copy the disk to the europe-west2-c zone. Create a new VM with that disk.
    d. Use "gcloud compute instances move" with parameter "–destination-zone europe-west2-c" to move the instance to the new zone.

    i. this makes sure the VM gets replicated in the new zone.
12. Your company has a mission-critical application that serves users globally. You need to select a transactional, relational data storage system for this application. Which 2 products should you consider
    a. BigQuery
    b. Cloud SQL
    c. Cloud Spanner
    d. Cloud Bigtable
    e. Cloud Datastore
        i. Cloud SQL is a relational and transactional database in the list. Spanner is a relational and transactional database in the list.
13. You have a Kubernetes cluster with 1 node-pool. The cluster receives a lot of traffic and needs to grow. You decide to add a node. What should you do?
    a. Use "gcloud container clusters resize" with the desired number of nodes.
    b. Use "kubectl container clusters resize" with the desired number of nodes.
    c. Edit the managed instance group of the cluster and increase the number of VMs by 1.
    d. Edit the managed instance group of the cluster and enable autoscaling.
        i. resizes the cluster to the desired number of nodes.
14. You created an update for your application on App Engine. You want to deploy the update without impacting your users. You want to be able to roll back as quickly as possible if it fails. What should you do?
    a. Delete the current version of your application. Deploy the update using the same version identifier as the deleted version.
    b. Notify your users of an upcoming maintenance window. Deploy the update in that maintenance window.
    c. Deploy the update as the same version that is currently running.
    d. Deploy the update as a new version. Migrate traffic from the current version to the new version.
        i. this makes sure there is no downtime and you can roll back the fastest.
    e. https://cloud.google.com/appengine/docs/admin-api/migrating-splitting-traffic
15. You have created a Kubernetes deployment, called Deployment-A, with 3 replicas on your cluster. Another deployment, called Deployment-B, needs access to Deployment-A. You cannot expose Deployment-A outside of the cluster. What should you do?
    a. Create a Service of type NodePort for Deployment A and an Ingress Resource for that Service. Have Deployment B use the Ingress IP address.
    b. Create a Service of type LoadBalancer for Deployment A. Have Deployment B use the Service IP address.
    c. Create a Service of type LoadBalancer for Deployment A and an Ingress Resource for that Service. Have Deployment B use the Ingress IP address.
    d. Create a Service of type ClusterIP for Deployment A. Have Deployment B use the Service IP address.
        i. this exposes the service on a cluster-internal IP address. Choosing this method makes the service reachable only from within the cluster.
    e. https://kubernetes.io/docs/concepts/services-networking/service/
16. You need to estimate the annual cost of running a Bigquery query that is scheduled to run nightly. What should you do?
    a. Use "gcloud query –dry_run" to determine the number of bytes read by the query. Use this number in the Pricing Calculator.
    b. Use "bq query –dry_run" to determine the number of bytes read by the query. Use this number in the Pricing Calculator.
    c. Use "gcloud estimate" to determine the amount billed for a single query. Multiply this amount by 365.
    d. Use "bq estimate" to determine the amount billed for a single query. Multiply this amount by 365.
        i. the correct way to estimate the yearly BigQuery querying costs.
17. You want to find out who in your organization has Owner access to a project called "my-project".What should you do?

a. In the Google Cloud Platform Console, go to the IAM page for your organization and apply the filter “Role:Owner”.
b. In the Google Cloud Platform Console, go to the IAM page for your project and apply the filter “Role:Owner”.
c. Use “gcloud iam list-grantable-role –project my-project” from your Terminal.
d. Use “gcloud iam list-grantable-role” from Cloud Shell on the project page.

18. You want to create a new role for your colleagues that will apply to all current and future projects created in your organization. The role should have the permissions of the BigQuery Job User and Cloud Bigtable User roles. You want to follow Google’s recommended practices. How should you create the new role?
    a. Use “gcloud iam combine-roles –global” to combine the 2 roles into a new custom role.
    b. For one of your projects, in the Google Cloud Platform Console under Roles, select both roles and combine them into a new custom role. Use “gcloud iam promote-role” to promote the role from a project role to an organization role.
    c. For all projects, in the Google Cloud Platform Console under Roles, select both roles and combine them into a new custom role.
    d. For your organization, in the Google Cloud Platform Console under Roles, select both roles and combine them into a new custom role.
        i. This creates a new role with the combined permissions on the organization level.
19. You work in a small company where everyone should be able to view all resources of a specific project. You want to grant them access following Google’s recommended practices. What should you do?
    a. Create a script that uses “gcloud projects add-iam-policy-binding” for all users’ email addresses and the Project Viewer role.
    b. Create a script that uses “gcloud iam roles create” for all users’ email addresses and the Project Viewer role.
    c. Create a new Google Group and add all users to the group. Use “gcloud projects add-iam-policy-binding” with the Project Viewer role and Group email address.
    d. Create a new Google Group and add all members to the group. Use “gcloud iam roles create” with the Project Viewer role and Group email address.
        i. Google recommends to use groups where possible.
    e. https://cloud.google.com/sdk/gcloud/reference/iam/
20. You need to verify the assigned permissions in a custom IAM role. What should you do?
    a. Use the GCP Console, IAM section to view the information.
    b. Use the “gcloud init” command to view the information.
    c. Use the GCP Console, Security section to view the information.
    d. Use the GCP Console, API section to view the information.
        i. console area to view permission assigned to a custom role in a particular project.
    e. https://cloud.google.com/iam/docs/understanding-roles
    f. https://cloud.google.com/iam/docs/creating-custom-roles
21. Which of the following services provides real-time messaging?
    a. Cloud Pub/Sub
    b. Big Query
    c. App Engine
    d. Datastore
22. Which of the following tasks would Nearline Storage be well suited for?
    a. A mounted Linux file system
    b. Image assets for a high traffic website
    c. Frequently read files
    d. D. Infrequently read data backups
    e. https://cloud.google.com/storage/docs/storage-classes#comparison_of_storage_classes
23. Which of the following products will allow you to administer your projects through a browser based command-line?
    a. Cloud Datastore
    b. Cloud Command-line
    c. Cloud Terminal
    d. Cloud Shell
    e. https://cloud.google.com/shell/

24. Cloud SQL is based on which database engine?
    a. A. Microsoft SQL Server
    b. B. MySQL
    c. C. Oracle
    d. D. Informix
    e. https://cloud.google.com/sql/docs/features#differences
25. Which of the following products will allow you to perform live debugging without stopping your application?
    a. App Engine Active Debugger (AEAD)
    b. Stackdriver Debugger
    c. Code Inspector
    d. Pause IT
    e. https://cloud.google.com/debugger/docs/
26. Which of these options is not a valid Cloud Storage class?
    a. Glacier Storage
    b. Nearline Storage
    c. Coldline Storage
    d. Regional Storage
27. 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
    e. https://cloud.google.com/storage/docs/access-control/signed-urls
28. Of the options given, which is a NoSQL database?
    a. Cloud Datastore
    b. Cloud SQL
    c. All of the given options
    d. Cloud Storage
    e. https://cloud.google.com/appengine/docs/python/datastore/
29. Container Engine allows orchastration of what type of containers?
    a. Blue Whale
    b. LXC
    c. BSD Jails
    d. Docker
30. 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
    e. https://cloud.google.com/iam/docs/overview
31. Which of the following products will allow you to host a static website?
    a. Cloud SDK
    b. Cloud Endpoints
    c. Cloud Storage
    d. Cloud Datastore
32. Container Engine is built on which open source system?
    a. Swarm
    b. Kubernetes
    c. Docker Orchastrate
    d. Mesos
    e. https://cloud.google.com/container-engine/
33. Cloud Source Repositories provide a hosted version of which version control system?
    a. Git
    b. RCS
    c. SVN

    d. Mercurial
    e. https://cloud.google.com/source-repositories/docs/
34. Which of the following is an analytics data warehouse?
    a. Cloud SQL
    b. Big Query
    c. Datastore
    d. Cloud Storage
    e. https://cloud.google.com/bigquery/
35. Which service offers the ability to create and run virtual machines?
    a. Google Virtualization Engine
    b. Compute Containers
    c. VM Engine
    d. Compute Engine
36. 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
    e. https://cloud.google.com/compute/docs/tutorials/robustsystems
37. 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
    e. https://support.google.com/a/answer/106368?hl=en
38. 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
    e. https://cloud.google.com/storage/docs/access-control/signed-urls
39. 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
    e. https://cloud.google.com/compute/docs/instances/preemptible
40. 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
    e. https://cloud.google.com/compute/docs/instance-groups/
41. What type of firewall rule(s) does Google Cloud's networking support?
    a. A deny
    b. allow, deny & filtered
    c. allow
    d. allow & deny
    e. https://cloud.google.com/compute/docs/networking
42. 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
    e. https://cloud.google.com/compute/docs/subnetworks
43. 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
    e. https://cloud.google.com/compute/docs/autoscaler/
44. Which of the following features makes applying firewall settings easier?
    a. Service accounts
    b. Tags
    c. Metadata
    d. Labels
    e. https://cloud.google.com/compute/docs/label-or-tag-resources
45. 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
    e. https://cloud.google.com/sql/docs/configure-ha#test
46. 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
    e. https://cloud.google.com/compute/docs/startupscript
47. 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
    e. https://cloud.google.com/compute/docs/shutdownscript
48. 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
    e. https://cloud.google.com/iam/docs/overview
49. 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
    e. https://cloud.google.com/iam/docs/using-iam-securely
50. 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.
    e. https://cloud.google.com/solutions/disaster-recovery-cookbook
51. 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
e. https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf

52. 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
    e. https://cloud.google.com/compute/docs/disks/
53. 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.
    e. https://cloud.google.com/compute/docs/instances/windows/bring-your-own-license/
54. 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
    e. https://cloud.google.com/products/storage/
55. 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.
    e. https://cloud.google.com/compute/all-pricing
56. Which Google Cloud Platform service requires the least management because it takes care of the underlying infrastructure for you?
    a. A. Container Engine
    b. B. Cloud Engine
    c. C. App Engine
    d. D. Docker containers running on Cloud Engine
57. 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%.
    e. https://cloud.google.com/compute/docs/instance-groups/distributing-instances-with-regional-instance-groups
58. 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.
    e. https://cloud.google.com/storage/docs/best-practices#security

59. 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
    e. https://cloud.google.com/compute/docs/cloudrouter#cloud_router_for_vpns_with_vpc_networks
60. 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.
    e. https://cloud.google.com/security/encryption-at-rest/
61. 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
    e. https://cloud.google.com/sql/docs/mysql/configure-ha
62. 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.
    e. https://cloud.google.com/iam/docs/using-iam-securely
63. 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.
    e. https://cloud.google.com/docs/authentication#token_lifecycle_management
64. 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
    e. https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#use_projects_to_fully_isolate_resources
65. 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.
        i. You can enable interactive access to an instance's serial console so you can connect and troubleshoot instances through the serial console.
66. 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

67. 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
    e. https://cloud.google.com/storage/transfer/
68. 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.
    e. https://cloud.google.com/compute/docs/troubleshooting#pdboot
69. 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.
    e. https://cloud.google.com/appengine/articles/scalability#loadtesting
70. 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.
    e. https://cloudacademy.com/google/managing-your-google-cloud-infrastructure-course/testing.html
71. 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
    e. https://cloud.google.com/products/
72. 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.
    e. https://cloud.google.com/logging/docs/export/configure_export_v2#errors_exporting_to_bigquery
73. 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
    e. https://cloud.google.com/stackdriver/
74. 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. D. Encrypt the logs using Cloud KMS.
e. https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#prevent_unwanted_changes_to_logs

75. 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.
    e. https://cloud.google.com/compute/docs/troubleshooting#networktraffic
76. 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
77. 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
    e. https://cloud.google.com/storage/docs/lifecycle#expirationtime
78. If you have object versioning enabled on a multi-regional bucket, what will the following lifecycle config file do?
    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
    e. https://cloud.google.com/storage/docs/managing-lifecycles#enable
79. 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
    e. https://cloud.google.com/trace/docs/reference
80. 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
    e. https://cloud.google.com/storage-options/
81. 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
e. https://cloud.google.com/storage-options/

Associate Cloud Engineer Sample Questions

I. Your organization plans to migrate its financial transaction monitoring application to Google Cloud. Auditors need to view the data and run reports in BigQuery, but they are not allowed to perform transactions in the application. You are leading the migration and want the simplest solution that will require the least amount of maintenance. What should you do?
   A. Assign roles/bigquery.dataViewer to the individual auditors.
   B. Create a group for auditors and assign roles/viewer to them.
   C. Create a group for auditors, and assign roles/bigquery.dataViewer to them.
   D. Assign a custom role to each auditor that allows view-only access to BigQuery.
      1. Feedback : Understanding roles
      2. A is not correct because Google recommended practice is to assign IAM roles to groups, not individuals. Groups are easier to manage than individual users and they provide high level visibility into roles and permissions.
      3. B is not correct because it uses a basic role to give auditors view access to all resources on the project.
      4. C is correct because it uses a predefined role to provide view access to BigQuery for the group of auditors. Auditors can be added or deleted from the group if job responsibilities change.
      5. D is not correct because using a predefined role can accomplish the goal and requires less maintenance.

II. You are managing your company's first Google Cloud project. Project leads, developers, and internal testers will participate in the project, which includes sensitive information. You need to ensure that only specific members of the development team have access to sensitive information. You want to assign the appropriate Identity and Access Management (IAM) roles that also require the least amount of maintenance. What should you do?
   A. Assign a basic role to each user.
   B. Create groups. Assign a basic role to each group, and then assign users to groups.
   C. Create groups. Assign a Custom role to each group, including those who should have access to sensitive data. Assign users to groups.
   D. Create groups. Assign an IAM Predefined role to each group as required, including those who should have access to sensitive data. Assign users to groups.
      1. Feedback : Understanding roles AND Understanding IAM custom roles
      2. A is not correct for two reasons: The recommended practice is to use groups and not to assign roles to each user. Beyond that, Basic Roles do not have enough granularity to account for access to sensitive data.
      3. B is not correct because Basic roles do not have enough granularity to account for access to sensitive data.
      4. C is not correct because creating and maintaining Custom roles will require more maintenance than using Predefined roles.

5. D is correct because Predefined roles are fine-grained enough to set permissions for specific roles requiring sensitive data access. This solution also uses groups, which is the recommended practice for managing permissions for individual roles.

III. You are responsible for monitoring all changes in your Cloud Storage and Firestore instances. For each change, you need to invoke an action that will verify the compliance of the change in near real time. You want to accomplish this with minimal setup. What should you do?

A. Use the trigger mechanism in each datastore to invoke the security script.
B. Use Cloud Function events, and call the security script from the Cloud Function triggers.
C. Redirect your data-changing queries to an App Engine application, and call the security script from the application.
D. Use a Python script to get logs of the datastores, analyze them, and invoke the security script.

1. Feedback : Cloud Functions triggers
2. A is not correct because setting triggers in each individual database requires additional setup.
3. B is correct because it provides fast response and requires the minimal amount of setup.
4. C is not correct because it requires custom programming.
5. D is not correct because it requires significant custom programming.

IV. Your application needs to process a significant rate of transactions. The rate of transactions exceeds the processing capabilities of a single virtual machine (VM). You want to spread transactions across multiple servers in real time and in the most cost-effective manner. What should you do?

A. Send transactions to BigQuery. On the VMs, poll for transactions that do not have the 'processed' key, and mark them 'processed' when done.
B. Set up Cloud SQL with a memory cache for speed. On your multiple servers, poll for transactions that do not have the 'processed' key, and mark them 'processed' when done.
C. Send transactions to Pub/Sub. Process them in VMs in a managed instance group.
D. Record transactions in Cloud Bigtable, and poll for new transactions from the VMs.

1. Feedback : Pub/Sub
2. A is not correct because its latency is significantly higher than the real-time response required.
3. B is not correct because it will not deliver the desired performance.
4. C is correct because Pub/Sub is a scalable solution that can effectively distribute a large number of tasks among multiple servers at a low cost.
5. D is not correct because, although fast, it will introduce an additional expense for storing the data.

V. Your team needs to directly connect your on-premises resources to several virtual machines inside a virtual private cloud (VPC). You want to provide your team with fast and secure access to the VMs with minimal maintenance and cost. What should you do?

A. Set up Cloud Interconnect.
B. Use Cloud VPN to create a bridge between the VPC and your network.
C. Assign a public IP address to each VM, and assign a strong password to each one.
D. Start a Compute Engine VM, install a software router, and create a direct tunnel to each VM.

1. Feedback : VPN

2. A is not correct because it is significantly more expensive than other existing solutions.
3. B is correct because it agrees with the Google recommended practices.
4. C is not correct because it will require a sizable maintenance effort.
5. D is not correct because setting up connections for each individual VM requires a significant amount of maintenance.

VI. You are implementing Cloud Storage for your organization. You need to follow your organization's regulations. They include: 1) Archive data older than one year. 2) Delete data older than 5 years. 3) Use standard storage for all other data. You want to implement these guidelines automatically and in the simplest manner available. What should you do?

A. Set up Object Lifecycle management policies.
B. Run a script daily. Copy data that is older than one year to an archival bucket, and delete five-year-old data.
C. Run a script daily. Set storage class to ARCHIVE for data that is older than one year, and delete five-year-old data.
D. Set up default storage class for three buckets named: STANDARD, ARCHIVE, DELETED. Use a script to move the data in the appropriate bucket when its condition matches your company guidelines.
    1. Feedback : Object Lifecycle Management & Storage classes
    2. A is correct because Object Lifecycle allows you to automate the implementation of your organization's data policy.
    3. B is not correct because changing an object's storage class does not require copying the object to another bucket.
    4. C is not correct because it requires custom programming.
    5. D is not correct because moving an object to a DELETED bucket does not really delete it.

VII. You are creating a Cloud IOT application requiring data storage of up to 10 petabytes (PB). The application must support high-speed reads and writes of small pieces of data, but your data schema is simple. You want to use the most economical solution for data storage. What should you do?

A. Store the data in Cloud Spanner, and add an in-memory cache for speed.
B. Store the data in Cloud Storage, and distribute the data through Cloud CDN for speed.
C. Store the data in Cloud Bigtable, and implement the business logic in the programming language of your choice.
D. Use BigQuery, and implement the business logic in SQL.
    1. Feedback : BigTable
    2. A is not correct because Cloud Spanner would not be the most economical solution.
    3. B is not correct because blob-oriented Cloud Storage is not a good fit for reading and writing small pieces of data.
    4. C is correct because Bigtable provides high-speed reads and writes, accommodates a simple schema, and is cost-effective.
    5. D is not correct because BigQuery does not provide the high-speed reads and writes required by IoT.

VIII. You have created a Kubernetes deployment on Google Kubernetes Engine (GKE) that has a backend service. You also have pods that run the frontend service. You want to ensure that there is no interruption in communication between your frontend and backend service pods if they are moved or restarted. What should you do?

A. Create a service that groups your pods in the backend service, and tell your frontend pods to communicate through that service.
B. Create a DNS entry with a fixed IP address that the frontend service can use to reach the backend service.
C. Assign static internal IP addresses that the frontend service can use to reach the backend pods.
D. Assign static external IP addresses that the frontend service can use to reach the backend pods.
    1. Feedback : Exposing applications using services
    2. A is correct because Kubernetes service serves the purpose of providing a destination that can be used when the pods are moved or restarted.
    3. B is not correct because a DNS entry is created by service creation.
    4. C is not correct because static internal IP addresses do not automatically change when pods are restarted.
    5. D is not correct because static external IP addresses do not automatically change when pods are restarted, and they take traffic outside of Google networks.

IX. You are responsible for the user-management service for your global company. The service will add, update, delete, and list addresses. Each of these operations is implemented by a Docker container microservice. The processing load can vary from low to very high. You want to deploy the service on Google Cloud for scalability and minimal administration. What should you do?
A. Deploy your Docker containers into Cloud Run.
B. Start each Docker container as a managed instance group.
C. Deploy your Docker containers into Google Kubernetes Engine.
D. Combine the four microservices into one Docker image, and deploy it to the App Engine instance.
    1. Feedback : Cloud Run
    2. A is correct because Cloud Run is a managed service that requires minimal administration.
    3. B is not correct because managed instance groups lack management capabilities to expose their services.
    4. C is not correct because, although GKE provides scalability, it requires ongoing administration of the cluster.
    5. D is not correct because it required effort to reimplement the four microservices in one Docker container. You will also lose your microservice architecture.

X. You provide a service that you need to open to everyone in your partner network. You have a server and an IP address where the application is located. You do not want to have to change the IP address on your DNS server if your server crashes or is replaced. You also want to avoid downtime and deliver a solution for minimal cost and setup. What should you do?
A. Create a script that updates the IP address for the domain when the server crashes or is replaced.
B. Reserve a static internal IP address, and assign it using Cloud DNS.
C. Reserve a static external IP address, and assign it using Cloud DNS.
D. Use the Bring Your Own IP (BYOIP) method to use your own IP address.
    1. Feedback : Virtual Private Cloud (VPC) networks Alias IP ranges Bring your own IP Reserving a static external IP address
    2. A is not correct because updating DNS records could take up to 24 hours and it will cause downtime.

3. B is not correct because internal IPs are not routable and cannot be seen on the internet.
4. C is correct because external IPs are routable and can be advertised and seen on the internet, and this is also the most cost-effective solution.
5. D is not correct because, while it is possible, bringing your own IP address is not as cost effective as Google Cloud DNS.

XI. Your team is building the development, test, and production environments for your project deployment in Google Cloud. You need to efficiently deploy and manage these environments and ensure that they are consistent. You want to follow Google-recommended practices. What should you do?

A. Create a Cloud Shell script that uses gcloud commands to deploy the environments.
B. Create one Terraform configuration for all environments. Parameterize the differences between environments.
C. For each environment, create a Terraform configuration. Use them for repeated deployment. Reconcile the templates periodically.
D. Use the Cloud Foundation Toolkit to create one deployment template that will work for all environments, and deploy with Terraform.

1. Feedback : Cloud Foundation Toolkit
2. A is not correct because creating a custom script of gcloud commands that adheres to Google Cloud recommended practices would require substantial development and maintenance effort.
3. B is not correct because parameterizing the environment differences is time consuming and error prone.
4. C is not correct because it is prone to error and involves significant reconciliation work.
5. D is correct because the Cloud Foundation Toolkit (CFT) provides ready-made templates that reflect Google Cloud recommended practices and can be used to automate creation of the environments.

XII. You receive an error message when you try to start a new VM: “You have exhausted the IP range in your subnet.” You want to resolve the error with the least amount of effort. What should you do?

A. Create a new subnet and start your VM there.
B. Expand the CIDR range in your subnet, and restart the VM that issued the error.
C. Create another subnet, and move several existing VMs into the new subnet.
D. Restart the VM using exponential backoff until the VM starts successfully.

1. Feedback : Expand a primary IPv4 range
2. A is not correct because you do not need a new subnet. Once you expand the CIDR range, the initial VM will work by redeploying it.
3. B is correct because once you expand the CIDR range, you can redeploy it, and it will work.
4. C is not correct because moving your VMs to another subnet is an additional time-consuming effort that is not required.
5. D is not correct because once the CIDR range is exhausted, redeploying the failed VM will not resolve the issue.

XIII. You are running several related applications on Compute Engine virtual machine (VM) instances. You want to follow Google-recommended practices and expose each application through a DNS name. What should you do?

A. A. Use the Compute Engine internal DNS service to assign DNS names to your VM instances, and make the names known to your users.
B. B. Assign each VM instance an alias IP address range, and then make the internal DNS names public.
C. C. Assign Google Cloud routes to your VM instances, assign DNS names to the routes, and make the DNS names public.
D. D. Use Cloud DNS to translate your domain names into your IP addresses.
    1. Feedback : Set up a domain by using Cloud DNS
    2. A is not correct because email is not the way for submitting DNS publication requests.
    3. B is not correct because you cannot make the internal DNS name public.
    4. C is not correct because you cannot make DNS names public.
    5. D is correct because Cloud DNS is the proper tool for translating domain names into IP addresses.

XIV. You are charged with optimizing Google Cloud resource consumption. Specifically, you need to investigate the resource consumption charges and present a summary of your findings. You want to do it in the most efficient way possible. What should you do?

A. Rename resources to reflect the owner and purpose. Write a Python script to analyze resource consumption.
B. Attach labels to resources to reflect the owner and purpose. Export Cloud Billing data into BigQuery, and analyze it with Data Studio.
C. Assign tags to resources to reflect the owner and purpose. Export Cloud Billing data into BigQuery, and analyze it with Data Studio.
D. Create a script to analyze resource usage based on the project to which the resources belong. In this script, use the IAM accounts and services accounts that control given resources.
    1. Feedback : Export to BigQuery Common uses of labels VM labels and network tags
    2. A is not correct because it requires custom programming and does not follow Google recommended practices and is not the most efficient solution.
    3. B is correct because it describes Google Recommended practice: labels are attached to resources and these labels are then propagated into billing items.
    4. C is not correct because tags are no longer created when a label is created for a resource and cannot be used for tracking resources.
    5. D is not correct because it requires custom programming.

XV. You are creating an environment for researchers to run ad hoc SQL queries. The researchers work with large quantities of data. Although they will use the environment for an hour a day on average, the researchers need access to the functional environment at any time during the day. You need to deliver a cost-effective solution. What should you do?

A. Store the data in Cloud Bigtable, and run SQL queries provided by Bigtable schema.
B. Store the data in BigQuery, and run SQL queries in BigQuery.
C. Create a Dataproc cluster, store the data in HDFS storage, and run SQL queries in Spark.
D. Create a Dataproc cluster, store the data in Cloud Storage, and run SQL queries in Spark.
    1. Feedback : BigQuery
    2. A is not correct because HBase does not allow ad-hoc queries.

3. B is correct because BigQuery allows for ad hoc queries and is cost effective.
4. C is not correct because HDFS is not the recommended storage to use with Dataproc on Google Cloud.
5. D is not correct because it is not the most cost-effective solution, because cluster is always running.

XVI. You are migrating your workload from on-premises deployment to Google Kubernetes Engine (GKE). You want to minimize costs and stay within budget. What should you do?

A. Configure Autopilot in GKE to monitor node utilization and eliminate idle nodes.
B. Configure the needed capacity; the sustained use discount will make you stay within budget.
C. Scale individual nodes up and down with the Horizontal Pod Autoscaler.
D. Create several nodes using Compute Engine, add them to a managed instance group, and set the group to scale up and down depending on load.
    1. Feedback : Autopilot overview
    2. A is correct because Autopilot is designed to reduce the operational cost of managing clusters and optimize your clusters for production.
    3. B is not correct because it violates the principle of provisioning on-demand rather than overprovisioning. Although sustained use discount lowers the budget, not using unnecessary resources will keep costs down more.
    4. C is not correct because Horizontal Pod Autoscaler is for adjusting the Kubernetes parameters for performance, not for taking out unnecessary resources.
    5. D is not correct because, although Google Kubernetes Engine uses Compute Engine internally, managed instance groups lack the Autopilot capabilities for scaling Kubernetes.

XVII. Your application allows users to upload pictures. You need to convert each picture to your internal optimized binary format and store it. You want to use the most efficient, cost-effective solution. What should you do?

A. Store uploaded files in Cloud Bigtable, monitor Bigtable entries, and then run a Cloud Function to convert the files and store them in Bigtable.
B. Store uploaded files in Firestore, monitor Firestore entries, and then run a Cloud Function to convert the files and store them in Firestore.
C. Store uploaded files in Filestore, monitor Filestore entries, and then run a Cloud Function to convert the files and store them in Filestore.
D. Save uploaded files in a Cloud Storage bucket, and monitor the bucket for uploads. Run a Cloud Function to convert the files and to store them in a Cloud Storage bucket.
    1. Feedback : Cloud Storage
    2. A is not correct because BigTable has limitations on storing binary files.
    3. B is not correct because Firestore is not efficient for large binary files.
    4. C is not correct because it is not the most cost-effective solution.
    5. D is correct because it follows Google recommended-practices and is the most efficient, cost-effective solution.

XVIII. You are migrating your on-premises solution to Google Cloud. As a first step, the new cloud solution will need to ingest 100 TB of data. Your daily uploads will be within your current bandwidth limit of 100 Mbps. You want to follow Google-recommended practices for the most cost-effective way to implement the migration. What should you do?

A. Set up Partner Interconnect for the duration of the first upload.
B. Obtain a Transfer Appliance, copy the data to it, and ship it to Google.

C. Set up Dedicated Interconnect for the duration of your first upload, and then drop back to regular bandwidth.
D. Divide your data between 100 computers, and upload each data portion to a bucket. Then run a script to merge the uploads together.
    1. Feedback : Transfer Appliance
    2. A is not correct because Partner Interconnect, although less expensive than Dedicated Interconnect, is still not the most cost effective solution for this migration.
    3. B is correct because it follows Google recommended practices for these data sizes and is the most cost-effective solution to implement the migration.
    4. C is not correct because Dedicated Interconnect is not the most cost-effective for this use case.
    5. D is not correct because it is not the most cost effective solution.

XIX. You are setting up billing for your project. You want to prevent excessive consumption of resources due to an error or malicious attack and prevent billing spikes or surprises. What should you do?
A. A. Set up budgets and alerts in your project.
B. B. Set up quotas for the resources that your project will be using.
C. C. Set up a spending limit on the credit card used in your billing account.
D. D. Label all resources according to best practices, regularly export the billing reports, and analyze them with BigQuery.

E. Feedback : Quotas and limits
F. A is not correct because budgets and alerts will result in notifications, but will not prevent excessive resource consumption.
G. B is correct because setting up quotas will prevent resource consumption from exceeding specified limits.
H. C is not correct because it will not prevent excessive resource consumption. Instead, your credit card will incur an unpaid balance; you will receive an email about it from Google and will still be liable to pay.
I. D is not correct because analyzing the root cause for going over the budget will not prevent overspend.

XX. Your project team needs to estimate the spending for your Google Cloud project for the next quarter. You know the project requirements. You want to produce your estimate as quickly as possible. What should you do?
A. A. Build a simple machine learning model that will predict your next month's spend.
B. B. Estimate the number of hours of compute time required, and then multiply by the VM per-hour pricing.
C. C. Use the Google Cloud Pricing Calculator to enter your predicted consumption for all groups of resources.
D. D. Use the Google Cloud Pricing Calculator to enter your consumption for all groups of resources, and then adjust for volume discounts.
    1. Feedback : Price Calculator

    2. A is not correct because, although ML produces excellent results in many areas, there are more straightforward approaches that require less time to produce an estimate.
    3. B is not correct because you need to add other charges, such as storage and data egress charges.

4. C is correct because the Google Cloud Pricing Calculator quickly gives the result, and you know the resources required for the project.
5. D is not correct because volume discounts, also called sustained use discounts, are applied automatically and are included in the calculator estimates.