

Associate Cloud Engineer

Certification exam guide

An Associate Cloud Engineer deploys and secures applications, services, and infrastructure, monitors operations of multiple projects, and maintains enterprise solutions to ensure that they meet target performance metrics. This individual has experience working with public clouds and on-premises solutions. They are able to perform common platform-based tasks to maintain and scale one or more deployed solutions that leverage Google-managed or self-managed services on Google Cloud.

Section 1: Setting up a cloud solution environment (~20% of the exam)

1.1 Setting up cloud projects and accounts. Considerations include:

- Creating a resource hierarchy
- Applying organizational policies to the resource hierarchy
- Granting members IAM roles within a project
- Managing users and groups in Cloud Identity (manually and automated)
- Enabling APIs within projects
- Provisioning and setting up products in Google Cloud Observability
- Assessing quotas and requesting increases

1.2 Managing billing configuration. Considerations include:

- Creating one or more billing accounts
- Linking projects to a billing account
- Establishing billing budgets and alerts
- Setting up billing exports

Section 2: Planning and configuring a cloud solution (~17.5% of the exam)

2.1 Planning and configuring compute resources. Considerations include:

- Selecting appropriate compute choices for a given workload (e.g., Compute Engine, Google Kubernetes Engine, Cloud Run, Cloud Functions)
- Using Spot VM instances and custom machine types as appropriate

2.2 Planning and configuring data storage options. Considerations include:

- Product choice (e.g., Cloud SQL, BigQuery, Firestore, Spanner, Bigtable)
- Choosing storage options (e.g., zonal Persistent Disk, regional Persistent Disk, Standard, Nearline, Coldline, Archive)

2.3 Planning and configuring network resources. Considerations include:

- Load balancing
- Availability of resource locations in a network
- Network Service Tiers

Section 3: Deploying and implementing a cloud solution (~25% of the exam)

3.1 Deploying and implementing Compute Engine resources. Considerations include:

- Launching a compute instance (e.g., assign disks, availability policy, SSH keys)
- Creating an autoscaled managed instance group by using an instance template
- Configuring OS Login
- Configuring VM Manager

3.2 Deploying and implementing Google Kubernetes Engine resources. Considerations include:

- Installing and configuring the command line interface (CLI) for Kubernetes (kubectl)
- Deploying a Google Kubernetes Engine cluster with different configurations (e.g., Autopilot, regional clusters, private clusters, GKE Enterprise)
- Deploying a containerized application to Google Kubernetes Engine

3.3 Deploying and implementing Cloud Run and Cloud Functions resources. Considerations include:

- Deploying an application
- Deploying an application for receiving Google Cloud events (e.g., Pub/Sub events, Cloud Storage object change notification events, Eventarc)
- Determining where to deploy an application by using Cloud Run (fully managed), Cloud Run for Anthos, or Cloud Functions

Google Cloud

3.4 Deploying and implementing data solutions. Considerations include:

- Deploying data products (e.g., Cloud SQL, Firestore, BigQuery, Spanner, Pub/Sub, Dataflow, Cloud Storage, AlloyDB)
- Loading data (e.g., command line upload, load data from Cloud Storage, Storage Transfer Service)

3.5 Deploying and implementing networking resources. Considerations include:

- Creating a VPC with subnets (e.g., custom mode VPC, Shared VPC)
- Creating ingress and egress firewall rules and policies (e.g., IP subnets, network tags, service accounts)
- Peering external networks (e.g., Cloud VPN, VPC Network Peering)

3.6 Implementing resources through infrastructure as code. Considerations include:

- Infrastructure as code tooling (e.g., Cloud Foundation Toolkit, Config Connector, Terraform, Helm)

Section 4: Ensuring successful operation of a cloud solution (~20% of the exam)

4.1 Managing Compute Engine resources. Considerations include:

- Remotely connecting to the instance
- Viewing current running VM inventory (e.g., instance IDs, details)
- Working with snapshots (e.g., create a snapshot from a VM, view snapshots, delete a snapshot, schedule a snapshot)
- Working with images (e.g., create an image from a VM or a snapshot, view images, delete an image)

4.2 Managing Google Kubernetes Engine resources. Considerations include:

- Viewing current running cluster inventory (e.g., nodes, Pods, Services)
- Configuring Google Kubernetes Engine to access Artifact Registry
- Working with node pools (e.g., add, edit, or remove a node pool)
- Working with Kubernetes resources (e.g., Pods, Services, Statefulsets)
- Managing Horizontal and Vertical autoscaling configurations

4.3 Managing Cloud Run resources. Considerations include:

- Deploying new versions of an application
- Adjusting application traffic splitting parameters
- Setting scaling parameters for autoscaling instances

4.4 Managing storage and database solutions. Considerations include:

- Managing and securing objects in Cloud Storage buckets
- Setting object lifecycle management policies for Cloud Storage buckets
- Executing queries to retrieve data from data instances (e.g., Cloud SQL, BigQuery, Spanner, Firestore, AlloyDB)
- Estimating costs of data storage resources
- Backing up and restoring database instances (e.g., Cloud SQL, Firestore)
- Reviewing job status (e.g., Dataflow, BigQuery)

4.5 Managing networking resources. Considerations include:

- Adding a subnet to an existing VPC
- Expanding a subnet to have more IP addresses
- Reserving static external or internal IP addresses
- Working with Cloud DNS and Cloud NAT

4.6 Monitoring and logging. Considerations include:

- Creating Cloud Monitoring alerts based on resource metrics
- Creating and ingesting Cloud Monitoring custom metrics (e.g., from applications or logs)
- Exporting logs to external systems (e.g., on-premises, BigQuery)
- Configuring log buckets, log analytics, and log routers
- Viewing and filtering logs in Cloud Logging
- Viewing specific log message details in Cloud Logging
- Using cloud diagnostics to research an application issue
- Viewing Google Cloud status
- Configuring and deploying Ops Agent
- Deploying Managed Service for Prometheus
- Configuring audit logs

Section 5: Configuring access and security (~17.5% of the exam)

5.1 Managing Identity and Access Management (IAM). Considerations include:

- Viewing and creating IAM policies
- Managing the various role types and defining custom IAM roles (e.g., basic, predefined, custom)

5.2 Managing service accounts. Considerations include:

- Creating service accounts
- Using service accounts in IAM policies with minimum permissions
- Assigning service accounts to resources
- Managing IAM of a service account
- Managing service account impersonation
- Creating and managing short-lived service account credentials