

Google Cloud Certified Associate Cloud Engineer

Dominios, pesos oficiales y habilidades clave del temario de Associate Cloud Engineer, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 120 min Fuente: guía de estudio oficial de Microsoft Learn

1. Setting up a cloud solution environment

20–20%

Setting up cloud projects and accounts

- La jerarquía de recursos de Google Cloud va de la organización (raíz, que exige Cloud Identity o Google Workspace) a carpetas opcionales y proyectos; cada recurso tiene un único padre. Los roles de IAM y las políticas de organización concedidos en un nivel se heredan hacia abajo, por lo que las carpetas sirven para agrupar departamentos o entornos y delegar su administración. Las carpetas se crean con `gcloud resource-manager folders create`.
- Las políticas de organización limitan qué configuraciones se permiten (ubicaciones, claves de cuentas de servicio, acceso público a Cloud Storage), mientras que IAM decide quién actúa. Se establecen en la organización, carpetas o proyectos y se heredan; en reglas de lista prevalecen los valores denegados y las reglas booleanas del hijo sustituyen a las del padre. La mayoría no son retroactivas.
- Para dar acceso en un proyecto se concede un rol a un principal (usuario, grupo o cuenta de servicio) con `gcloud projects add-iam-policy-binding`, que añade una vinculación sin sobrescribir la política. Se recomiendan roles predefinidos o personalizados en vez de básicos y conceder a grupos. Las condiciones de IAM permiten accesos que caducan, pero no con roles básicos heredados.
- Cloud Identity gestiona de forma centralizada usuarios y grupos gestionados por la empresa. Se pueden crear a mano en la consola o automatizar con Google Cloud Directory Sync desde Active Directory (sincronización unidireccional, sin contraseñas) y SSO SAML, o con `gcloud identity groups`. Las unidades organizativas aplican ajustes como la verificación en dos pasos; el acceso se gestiona con grupos.
- Cada servicio de Google Cloud debe activarse en el proyecto antes de usarlo, desde la biblioteca de API de la consola o con `gcloud services enable`, que admite varios servicios a la vez; `gcloud services list` muestra los activados o disponibles. Hace falta el rol Service Usage Admin. Desactivar una API no borra los datos de Cloud Storage o BigQuery, y `--force` desactiva también los servicios dependientes.

Managing billing configuration

- Una cuenta de facturación de Cloud define quién paga los proyectos vinculados, funciona en una sola moneda y se asocia a un perfil de pagos de Google. En una organización hace falta el rol Billing Account Creator para crearla. El país y la moneda no se pueden cambiar, así que otro país exige otra cuenta. Un perfil de pagos de tipo Organización admite varios usuarios; el Individual, no.
- Un proyecto solo puede usar servicios de Google Cloud si está vinculado a una cuenta de facturación de Cloud activa; cada proyecto se vincula a una sola cuenta, que puede pagar muchos proyectos. Se vincula o se cambia con `gcloud billing projects link`, con Billing Account User en la cuenta y Project Billing Manager o Project Owner en el proyecto. Deshabilitar la facturación detiene los servicios y puede eliminar recursos.
- Los presupuestos de Cloud Billing comparan el gasto real o previsto con un importe y envían alertas al cruzar umbrales; pueden abarcar la cuenta, proyectos, carpetas, servicios o una etiqueta. Por defecto avisan a Billing Account Administrator y User; con canales de Cloud Monitoring se añaden otros destinatarios. Un presupuesto solo de alertas no limita el gasto: para automatizar respuestas se usan notificaciones a Pub/Sub.
- Facturación de Cloud exporta a BigQuery costes de uso estándar, costes detallados por recurso, precios y metadatos de CUD; cada tipo se habilita por separado. Se recomienda un proyecto de FinOps vinculado a la misma cuenta, un conjunto de datos multirregional (añade el mes anterior) sin caducidad de tablas, y el rol Billing Account Costs Manager o Administrator; los precios exigen la API BigQuery Data Transfer Service.

20–20%

- Sin IP externa, se accede por SSH con IAP TCP forwarding (--tunnel-through-iap), que exige permitir 35.235.240.0/20 y el rol IAP-secured Tunnel User. OS Login controla SSH con IAM mediante roles/compute.osLogin
- gcloud/compute.instances.login muestra las instancias de todas las zonas del proyecto y admite filtros y formatos globales
- gcloud/compute.instances describe una configuración completa de una VM, incluido su ID inmutable. Para toda instancia en estado y de archivo se añaden incrementales y se crean a lo largo del disco para los archivos de arranque
- Las instantáneas estándar de archivo se añaden incrementales y se crean a lo largo del disco para los archivos de arranque
- Las imágenes se crean a partir de las imágenes de arranque y se crean a lo largo del disco para los archivos de arranque
- Las imágenes se crean a partir de las imágenes de arranque y se crean a lo largo del disco para los archivos de arranque

- **Reclamando un cluster de GKE** con kubectl primero se obtienen las credenciales con `gcloud container clusters get-credentials`, que actualiza kubeconfig. Después, `kubectl get nodes`, `kubectl get pods` y `kubectl get services` listan GKE, entre otras imágenes de Artifact Registry con las que se crean los nodos, o donde añadir detalles de este tipo de artefactos para leerlos y así, por ejemplo, poder acceder a los logs de los pods de un modo más sencillo.
- En GKE, **Standard** es el tipo de nodos que se crean con `gcloud container nodes --size=standard-1 create` y `gcloud container clusters resize` (en clusters regionales --num-nodes es por zona) y se eliminan con `gcloud container clusters delete`.
- Un **StorageSet** de cada Pod, que por defecto es `storage.googleapis.com/volumes` y `ClaimTemplate` es un `PersistentVolumeClaim` de `ReadWriteOnce` con `ServiceName` de `cluster-IP:None`, que publica por DNS las IP de los Pods. Un `Service` de tipo `Headless` publica también el número de réplicas según `CPUs`, `memory` y `key` y `key` es personalizable (`kubectl autoscale`) y necesita solicitudes de recursos para objetivos en porcentaje; no añade nodos, eso lo hace el escalador de clusters. El `VerticalPodAutoscaler` ajusta solicitudes de CPU y memoria: `Off` solo recomienda y `Auto` desaloja

- Cada despliegue o cambio de configuración en Cloud Run crea una revisión inmutable; una etiqueta de imagen se resuelve a un digest al desplegar `gcloud run deploy --image` despliega una imagen y `--source` compila el código.
- Cloud Run reparte el tráfico entre revisiones con `gcloud run services update-traffic --to-revisions REV=PERCENTAGE` para revertir o dividir, `LATEST` para la revisión más reciente y `--to-latest` para enviarle siempre el 100 %. Tras
- Cloud Run, los despliegues siguientes pueden hacer `gcloud run services update-traffic --to-latest` manteniendo y escalando.

- Cloud Storage no otorga roles a los objetos con roles de IAM por bucket (Object Viewer, Object Creator, Object User, Object Admin), con acceso uniforme a nivel de bucket, que desactiva las ACL, y con la prevención del acceso público.
- Las reglas de acceso de Cloud Storage se crean en la forma de una expresión de lenguaje SQL con la cláusula `SELECT` y se aplican en un formato de `WHERE` con operadores de acceso como `age`, `matchesPrefix`, `isLive` o `numNewerVersions`. Si varias reglas coinciden, el resultado es `TRUE` si alguna de ellas coincide. Las reglas se aplican a los objetos de Cloud Storage que se aplican a los objetos de Cloud Storage que se aplican a los objetos de Cloud Storage.
- `EXTERNAL_QUERY` de BigQuery es un operador de BigQuery que permite a BigQuery consultar datos de Cloud Storage, las bases de datos de terceros y los servicios de terceros (como el procesamiento de datos de terceros). Las consultas federadas usan `EXTERNAL_QUERY` de BigQuery para consultar los datos de Cloud Storage.
- `EXTERNAL_QUERY` de BigQuery es un operador de BigQuery que permite a BigQuery consultar datos de Cloud Storage, las bases de datos de terceros y los servicios de terceros (como el procesamiento de datos de terceros). Las consultas federadas usan `EXTERNAL_QUERY` de BigQuery para consultar los datos de Cloud Storage.

- **hacer redes de VPC con subredes globales y subredes regionales:** se añaden con `gcloud compute networks subnets create` indicando `red`, `rango principal` y `región`. Los rangos no pueden solaparse con otras subredes de la red ni de redes
- El **rango IPv4 principal** de una subred se amplía con `gcloud compute networks subnets expand-internal-range`, una acción de perfil `google` sin `interactiva` al tráfico. La ampliación no se puede deshacer ni reducir, así que conviene
- una **dirección estática**. Después hay que `revisar` como `tags` de `construimos` `global` para `range endpoints`, `global` `CKE`, `regiones para VMs` `balancers` de `regionales`, y `--region` con `--subnet` para `direcciones internas`. Una `dirección`
- `Cloud DNS` `ofre` se `puede` `pública`, `visible` `en` `internet` `o` `privada`. Las `direcciones` `de` `reservadas` `no` `se` `liberan` `autorizadas` `para` `public`, y `las` `externas` `si` `hay` `que` `nombrar` `en` `el` `registro` `por` `los` `servidores` `de` `nombres` `de` `Cloud` `DNS`. `Cloud`

- Una política de estándares en la métrica avisa cuando una métrica supera o queda por debajo de un umbral durante toda la ventana de nueva prueba, que evita alertas por una sola medición. Las series temporales se pueden agregar y definir en el usuario como se hace con preferencias con `OpenTelemetry (Kubernetes)`, `Prometheus` o `Elasticsearch`.
- Las métricas definidas en el usuario se hacen con `OpenTelemetry (Kubernetes)`, `Prometheus` o `Elasticsearch` en `Gemstone Engine` como `Analysis Monitoring`, eligiendo un recurso supervisado adecuado como `generic_task` en `Prometheus`.
- Para exportar registros remotos a `Pub/Sub` para enviarlos caso en tiempo real a herramientas externas, uso de `BigQuery` para guardar los registros de manera local y `S3` para archivarlos. La identidad de escritura del almacenamiento de registro se evalúa cada entrada con los sinks del recurso. Requiere no se puede modificar y `Default` es `gcp://storage.googleapis.com/gcloud-logging-read-log-sinks`.
- El Explorador de registros y `BigQuery` y `gcloud logging read` usan el lenguaje de consulta de `LogQL` para hacer consultas comunes operando en unidades de `AND/OR` sin corchetes ni mayúsculas, con `AND` implícito entre líneas. La gravedad se compara por orden numérico, `NOT` sobre un campo ausente es verdadero y `!=` es falso, y en `gcloud logging read` la marca `--freshness` amplía la antigüedad de las entradas devueltas.

5. Configuring access and security

17-18%

Managing Identity and Access Management (IAM)

- Una política de permiso reúne enlaces de rol (principales, rol y condición opcional) más etag y version; se adjunta a un recurso y la heredan sus descendientes. `gcloud projects add-iam-policy-binding` añade un enlace, mientras que `set-iam-policy` sustituye la política entera y exige leer-modificar-escribir con el etag. `get-iam-policy` no muestra roles heredados; para eso se usa `Policy Troubleshooter`.
- IAM tiene roles básicos (muy amplios; no recomendados en producción), predefinidos (mantenidos por Google) y personalizados. Los personalizados se crean en una organización o un proyecto, nunca en una carpeta, y solo se conceden allí; se gestionan con `gcloud iam roles create`, `update`, `delete` y `undelete`, y la fase `DISABLED` los deja sin efecto sin quitarlos de las políticas.

Managing service accounts

- Una cuenta de servicio se crea con `gcloud iam service-accounts create ID --display-name`; su correo es `ID@PROJECT_ID.iam.gserviceaccount.com` y el ID no se puede cambiar. El rol necesario es `roles/iam.serviceAccountCreator`. Google recomienda una cuenta por aplicación, prefijos como `vm-` y una descripción con el contacto, y reintentar con espera exponencial si la cuenta nueva aún no es visible.
- Una cuenta de servicio debe recibir solo los roles que necesita y en el recurso más concreto posible, por ejemplo un bucket en lugar del proyecto. Los ámbitos de acceso no sustituyen a IAM, la restricción `iam.automaticIamGrants-ForDefaultServiceAccounts` evita que las cuentas predeterminadas reciban `Editor`, y las recomendaciones de roles señalan los permisos que no se usan.
- Asociar una cuenta de servicio a un recurso (máquina virtual, servicio de Cloud Run) exige `iam.serviceAccounts.actAs`, incluido en `roles/iam.serviceAccountUser` sobre la cuenta. En Compute Engine hay que detener la máquina antes de cambiar la cuenta y conviene usar el ámbito `cloud-platform`; en GKE se usa `Workload Identity Federation` for GKE; entre proyectos, no se debe aplicar `iam.disableCrossProjectServiceAccountUsage`.
- Una cuenta de servicio también es un recurso con su propia política de permiso, que se consulta y modifica con `gcloud iam service-accounts get-iam-policy` y `add-iam-policy-binding`. Quien tiene `roles/iam.serviceAccountAdmin` puede concederse la suplantación, así que conviene conceder el acceso por cuenta y no por proyecto. Es mejor inhabilitar una cuenta antes de eliminarla, porque conserva sus enlaces.
- Suplantar una cuenta de servicio significa que un principal autenticado obtiene credenciales de corta duración de esa cuenta; requiere `iam.serviceAccounts.getAccessToken`, incluido en `roles/iam.serviceAccountTokenCreator`. Se usa con `--impersonate-service-account`, con la propiedad `auth/impersonate_service_account` o con `gcloud auth application-default login` para las bibliotecas de cliente, y evita las claves.