Engineer

Google Cloud

plataforma de computación en la nube de Google

Qué es

Google Cloud es la parte de Google que ofrece en alquiler recursos de computación desde sus propios centros de datos: máquinas virtuales en Compute Engine, almacenamiento de objetos en Cloud Storage, bases de datos gestionadas en Cloud SQL, clústeres Kubernetes en GKE, el almacén de datos BigQuery y muchos más servicios, todos pagados según su uso. Su nombre anterior, Google Cloud Platform o GCP, sigue muy extendido, incluso en partes de la propia documentación de Google.

Todo lo que Google Cloud ejecuta para un cliente reside dentro de un proyecto. El proyecto contiene los recursos, las API habilitadas para ellos, las cuotas que consumen y el vínculo a la cuenta de facturación que paga. Tiene un nombre visible modificable y un ID de proyecto único en todo Google Cloud y permanente una vez creado el proyecto. Los proyectos pueden agruparse en carpetas, estas pueden contener otras y todo el árbol depende de un recurso de organización perteneciente a la cuenta Google Workspace o Cloud Identity de una empresa. Cada proyecto hereda los roles y las políticas establecidos en la organización o en una carpeta superior. Un árbol bien trazado facilita el gobierno; uno mal trazado resulta difícil de desenredar.

La red se organiza de forma distinta a la de las otras grandes nubes. Una red VPC de Google Cloud, junto con sus rutas y reglas de cortafuegos, es un recurso global que no pertenece a ninguna región; solo sus subredes son regionales. Una máquina virtual en Bélgica y otra en Iowa pueden compartir una red privada y comunicarse por direcciones internas, sin VPN ni peering entre las dos regiones. En AWS, en cambio, cada VPC reside en una sola región.

Hay dos clases de identidad. Las personas inician sesión con cuentas de Google y reciben roles IAM sobre un proyecto, una carpeta o toda la organización. Los programas utilizan cuentas de servicio: identidades que pertenecen a un proyecto y bajo las que puede actuar una máquina virtual, un contenedor o un trabajo de compilación. Vincule una cuenta de servicio a una instancia de Compute Engine y el código que se ejecuta allí podrá llamar a las API de Google con sus roles sin contraseña ni archivo de claves en disco.

Utilice el concepto en una decisión

Aplique «¿Qué es Google Cloud?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Servidores dimensionados para el uso real, trasladados a la nube o fuera de ella, con la factura mensual calculada de antemano.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 20 aplicaciones Docker en Google Cloud y AWS — 20 aplicaciones en contenedores desplegadas y monitorizadas

20 aplicaciones Docker en Google Cloud y AWS Póngase en contacto →

Por qué importa

Para muchos equipos, el motivo para elegir Google Cloud son los datos. BigQuery es un almacén sin servidores que dimensionar: las tablas residen en conjuntos de datos dentro de un proyecto y las consultas se escriben en SQL estándar. En el modelo bajo demanda, cada consulta se factura por los bytes leídos; con la tarificación por capacidad se paga, en cambio, una capacidad de procesamiento reservada, medida en slots. El almacenamiento es columnar: la consulta paga por las columnas que toca, no por filas enteras. Cloud Storage sirve a su lado como zona de recepción y cargar archivos desde un bucket es una entrada habitual. Un equipo que en otra plataforma tendría que aprovisionar y ajustar un clúster de almacén de datos puede empezar con un bucket, un conjunto de datos y una consulta.

El límite del proyecto es el segundo motivo, porque reúne muchas cosas. Facturación, cuotas, API habilitadas e IAM confluyen en él: un proyecto por aplicación y entorno traza una separación clara, con permisos y líneas de factura distintos para producción y pruebas. Cerrar un proyecto detiene a la vez su facturación y todos sus recursos. Los propietarios pueden restaurarlo durante 30 días, aunque algunos servicios, entre ellos Cloud Storage, pueden eliminar sus datos antes. Por encima de los proyectos, una política de organización establecida una vez en una carpeta puede prohibir clases enteras de ajustes

arriesgados, como redes predeterminadas o claves descargables de cuentas de servicio, en todos los proyectos inferiores. Así puede un equipo pequeño mantener coherentes una docena de proyectos sin revisarlos a mano uno a uno.

Cómo se aplica en la práctica

Tres entradas del portfolio muestran Google Cloud como zona de recepción de un almacén de datos, almacenamiento externo de copias de seguridad y extremo de una red privada.

En el trabajo de datos, seis flujos ETL/ELT alimentaban BigQuery desde un almacén situado detrás de una VPN IPsec. Se exportaban conjuntos de datos y tablas seleccionados y preparados, se comprimían con gzip y se transferían a un bucket de Google Cloud Storage. La carga y el mapeo de estructuras de datos en BigQuery se automatizaron con la CLI bq y scripts de ingesta en Python. Una vez automatizados el paso por Cloud Storage y la carga en BigQuery, el trabajo completo pasó de 3+ horas manuales a menos de 20 minutos; BigQuery se actualizaba a diario en vez de semanalmente y las API de Python que lo consultaban ganaron un 30 % de rendimiento.

Para las copias de seguridad, se automatizaron cien copias de datos críticos, con Barman para PostgreSQL y Google Cloud para las copias externas. Bash y Python orquestaban y validaban todo el proceso de copias de seguridad, con políticas de retención para mantener las copias al día y comprobaciones de integridad para confirmar que cada una era válida, no solo que existía. Después, las copias se ejecutaban automáticamente y se podían verificar en todas las bases de datos.

En la red, ocho túneles WireGuard e IPsec entre Google Cloud y sistemas Linux en las instalaciones de la organización se gestionaron y diagnosticaron como un conjunto. Se estandarizó su configuración, se supervisó su estado y los problemas recurrentes de enrutamiento e intercambio de claves se resolvieron de raíz, en vez de reiniciar. Después, los ocho túneles funcionaban de forma segura y fiable.

Dónde surgen los problemas

Los mayores riesgos de Google Cloud son sus comodidades: ajustes que facilitan la primera tarde y siguen presentes un año después, cuando nadie recuerda haberlos elegido.

La red predeterminada permanece abierta. Salvo que una política de organización lo impida, cada proyecto nuevo empieza con una red predeterminada con una subred en cada región y cuatro reglas de cortafuegos predefinidas. Tres aceptan tráfico de 0.0.0.0/0, es decir, de todo Internet: SSH en tcp:22, escritorio remoto en tcp:3389 e ICMP. La cuarta permite todo el tráfico TCP, UDP e ICMP de 10.128.0.0/9 dentro de la red. Por tanto, cualquier máquina virtual con dirección externa en esa red queda abierta a intentos SSH desde cualquier lugar. La restricción `compute.skipDefaultNetworkCreation` evita que los proyectos nuevos reciban esa red; se sustituye por una red personalizada con reglas que identifiquen sus orígenes.

Una clave de cuenta de servicio acaba en un repositorio. Una clave gestionada por el usuario es un archivo JSON que permite a quien lo tenga actuar como la cuenta de servicio; de forma predeterminada, la clave sigue siendo válida hasta que alguien la elimina. Estos archivos se propagan con facilidad a secretos de CI, imágenes de contenedor y, por error, repositorios. Google recomienda elegir una alternativa más segura siempre que exista. Las cargas de trabajo en Google Cloud usan la cuenta de servicio vinculada al recurso donde se ejecutan; las que se ejecutan en otros lugares, como un sistema CI u otra nube, usan Workload Identity Federation, que intercambia las credenciales propias del sistema externo por tokens de Google de corta duración. En las organizaciones creadas a partir del 3 de mayo de 2024, las restricciones de políticas de organización deshabilitan de forma predeterminada la creación y carga de claves; las anteriores pueden establecer las mismas restricciones.

Una consulta pequeña lee una tabla grande. En el modelo bajo demanda, BigQuery factura los bytes leídos por la consulta. En una tabla sin clustering, una cláusula `LIMIT` no cambia esa cantidad: `SELECT * ... LIMIT 10` devuelve diez filas y factura todos los bytes de todas las columnas. Seleccione solo las columnas necesarias, particione las tablas grandes por fecha para que las consultas que apliquen un filtro por fecha omitan particiones antiguas, compruebe la estimación de una simulación antes de ejecutar algo nuevo y establezca un máximo de bytes facturados. Una consulta cuya estimación lo supere falla antes de ejecutarse, sin cargo alguno.

El almacenamiento frío contiene datos de uso frecuente. Cloud Storage ofrece las clases Nearline, Coldline y Archive, más baratas por gigabyte almacenado que Standard a cambio de tarifas de recuperación y duraciones mínimas de 30, 90 y 365 días. Un objeto eliminado, sustituido o trasladado antes del mínimo se cobra como si hubiera estado almacenado todo el periodo. Las copias que rotan a diario o los archivos temporales que un flujo escribe y elimina antes de que transcurra

una hora pueden salir más caros en Archive que en Standard. Las clases más frías convienen para datos escritos una vez y leídos rara vez; una regla de ciclo de vida puede trasladarlos a ellas a medida que envejecen.

Lecturas adicionales

- Documentación de Google Cloud — El índice de Google de guías, referencias y tutoriales de todos los productos Google Cloud.
- Acerca de la jerarquía de recursos — Cómo se anidan organizaciones, carpetas y proyectos, y cómo descienden sus roles y políticas.
- Reglas de cortafuegos VPC — Cómo se evalúan las reglas, incluidas las que trae la red predeterminada.
- Buenas prácticas de gestión de claves de cuentas de servicio — Cómo se filtran, cómo restringirlas y qué usar en su lugar.
- Estimar y controlar costes — Las indicaciones de BigQuery sobre simulaciones, máximos de bytes facturados y por qué `LIMIT` ahorra poco.
- Clases de almacenamiento — Las clases comparadas, con sus duraciones mínimas, tarifas de recuperación y disponibilidad.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es Google Cloud?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/google-cloud/