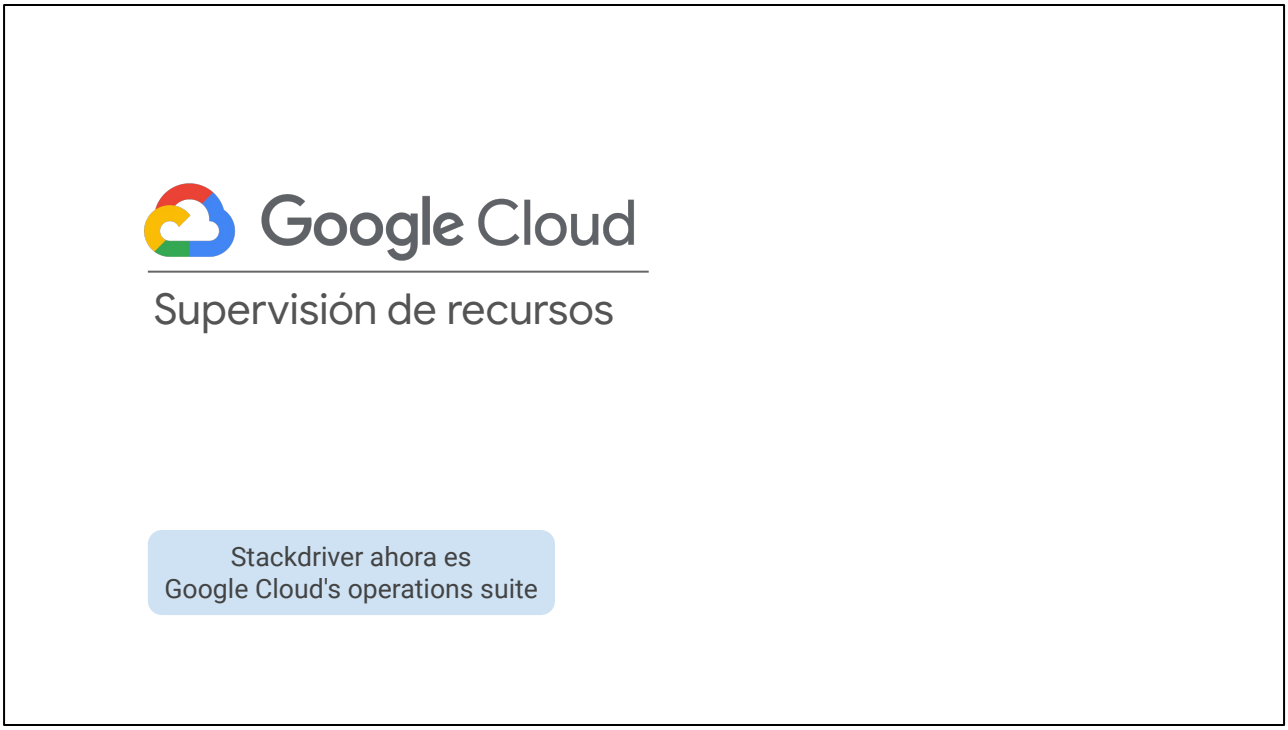
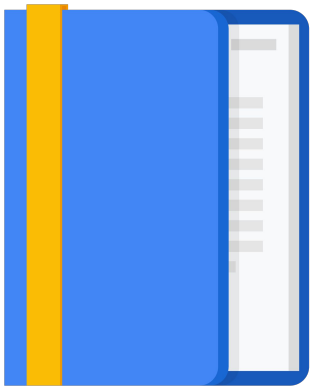


En este módulo, presentaré una descripción general de las opciones para supervisar recursos en Google Cloud.

Las funciones que analizaremos en este módulo se basan en Google Cloud's operations suite, un servicio que ofrece supervisión, registro y diagnóstico para sus aplicaciones.

Temario

- Google Cloud's operations suite
- Monitoring
- Lab
- Logging
- Creación de informes de errores
- Trace
- Debugger
- Lab



En este módulo, exploraremos los siguientes servicios: Cloud Monitoring, Cloud Logging, Error Reporting, Cloud Trace y Cloud Debugger. Tendrá la oportunidad de utilizarlos en los dos labs de este módulo.

Comenzaremos con una descripción general de Google Cloud's operations suite y sus funciones.

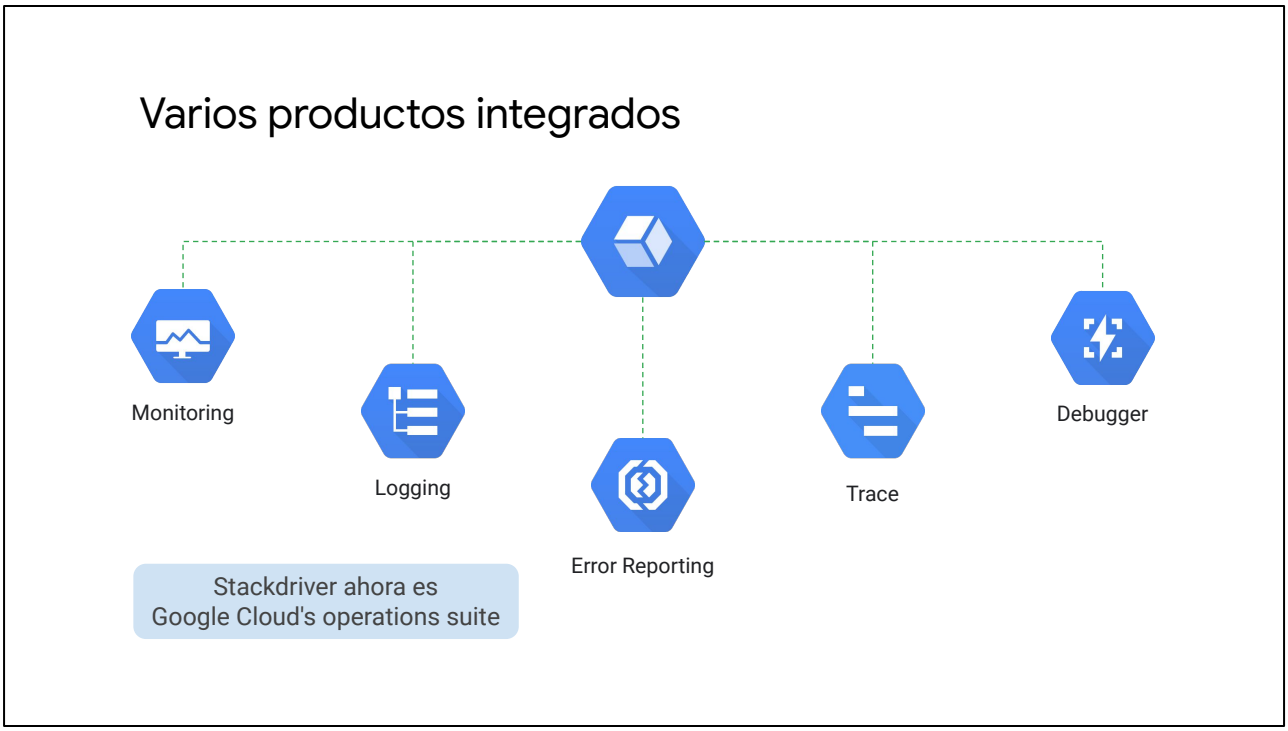
Descripción general de Google Cloud's operations suite

- Supervisión, registro y diagnóstico integrados
- Administra varias plataformas
  - Google Cloud y AWS
  - Descubrimiento dinámico de Google Cloud con valores predeterminados inteligentes
  - Integraciones y agentes de código abierto
- Acceso a herramientas potentes de datos y analítica
- Colaboración con software de terceros

Google Cloud's operations suite
(anteriormente Stackdriver)

Google Cloud's operations suite descubre de forma dinámica los recursos de la nube y los servicios de aplicación según una integración profunda a Google Cloud y Amazon Web Services. Debido a que cuenta con valores predeterminados inteligentes, puede tener visibilidad central hacia la plataforma de la nube en cuestión de minutos.

Esta ventaja le brinda acceso a las potentes herramientas de datos y analítica, así como le permite colaborar con diversos proveedores de software de terceros.



Como mencionamos antes, Google Cloud's operations suite dispone de servicios de supervisión, registro, generación de informes de errores, seguimiento de fallas y depuración. Usted solo paga por lo que usa, y hay asignaciones de uso gratuito para que pueda comenzar sin necesidad de pagar tarifas o compromisos por adelantado. Para obtener más información sobre los precios, consulte la sección de vínculos del siguiente video: [https://cloud.google.com/stackdriver/pricing]

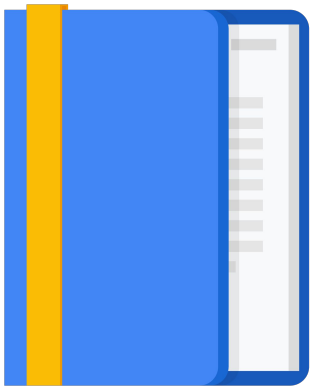
Ahora, en la mayoría de los entornos, paquetes completamente diferentes, o bien una colección de software con baja integración, administran estos servicios. Cuando vea estas funciones trabajar en conjunto en un único servicio integrado y completo, se dará cuenta de lo importante que es crear aplicaciones confiables, estables y que se puedan mantener.

Google Cloud's operations suite también admite un ecosistema enriquecido y creciente de socios de tecnología, como se muestra en esta diapositiva. Esto ayuda a expandir las capacidades de operaciones de TI, seguridad y cumplimiento disponibles para los clientes de Google Cloud. Para obtener más información sobre las integraciones, consulte la sección de vínculos del siguiente video: [https://cloud.google.com/stackdriver/partners]

Temario

- Google Cloud's operations suite
- **Monitoring**
- Lab
- Logging
- Creación de informes de errores
- Trace
- Debugger
- Lab

Stackdriver Monitoring ahora es Cloud Monitoring



Ahora que entiende Google Cloud's operations suite desde una perspectiva general, veamos en qué consiste Cloud Monitoring.

Ingeniería de confiabilidad de sitios

La supervisión es importante para Google, ya que se encuentra en la base de la ingeniería de confiabilidad de sitios (SRE).

La SRE es una disciplina que aplica diferentes aspectos de la ingeniería de software a operaciones cuyo objetivo es crear sistemas de software ultraescalables y altamente confiables. Esta disciplina le ha permitido a Google crear, implementar, supervisar y mantener algunos de los sistemas de software más grandes del mundo.

Si desea obtener más información sobre la SRE, le recomendamos explorar el libro gratuito que escribieron los miembros del equipo de SRE de Google. Se encuentra en la sección de vínculos del siguiente video:
[https://landing.google.com/sre/book.html]

Monitoring

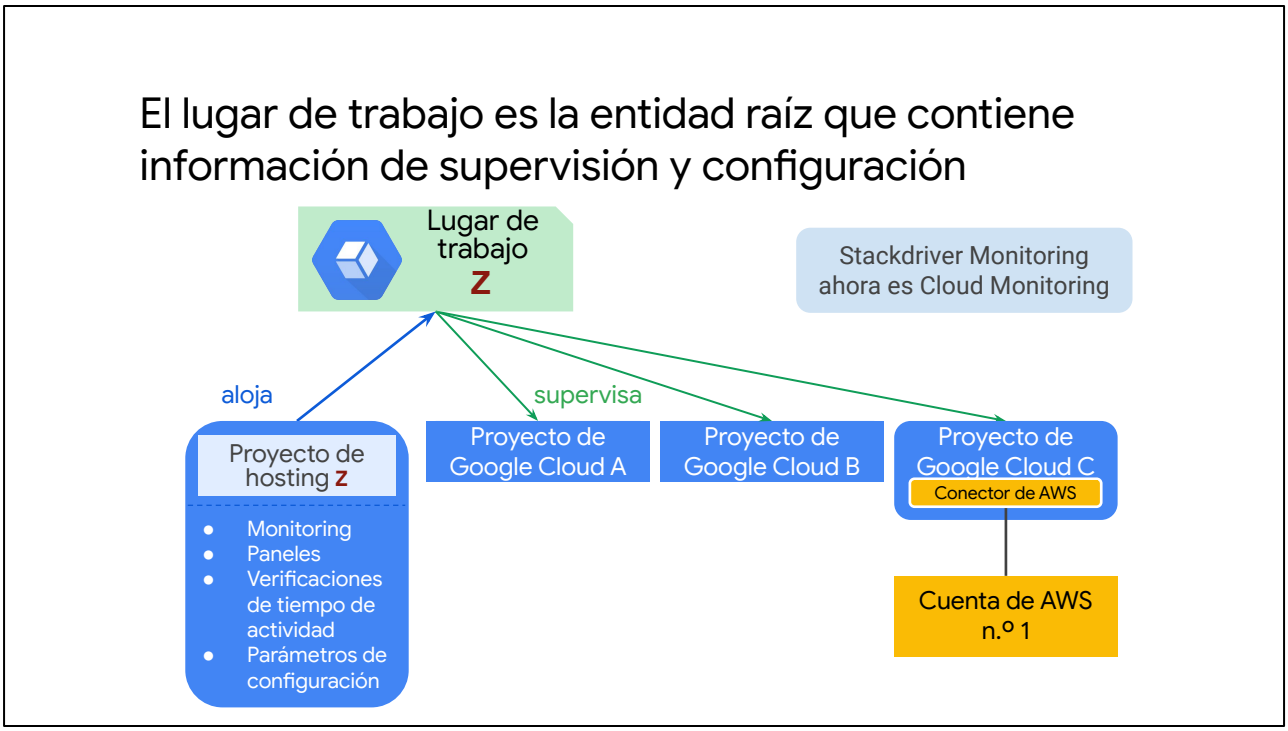
- Configuración dinámica y valores predeterminados inteligentes
- Métricas de plataformas, sistemas y aplicaciones
  - Transfiere datos: Métricas, eventos y metadatos
  - Genera estadísticas a través de paneles, gráficos y alertas
- Verificaciones de estado y tiempo de actividad
- Paneles
- Alertas

Cloud Monitoring
(anteriormente
Stackdriver Monitoring)

Cloud Monitoring configura la supervisión de forma dinámica después de que se implementan los recursos, y tiene valores predeterminados inteligentes que le permiten crear gráficos fácilmente para realizar actividades de supervisión básicas.

Este servicio permite supervisar las métricas de la plataforma, los sistemas y las aplicaciones mediante la transferencia de datos, como métricas, eventos y metadatos. Puede generar estadísticas a partir de estos datos a través de paneles, gráficos y alertas.

Por ejemplo, puede configurar y medir las verificaciones de estado y tiempo de actividad que envían alertas por correo electrónico.



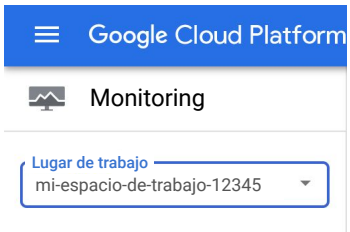
Un lugar de trabajo es la entidad raíz que contiene la información de supervisión y configuración en Cloud Monitoring. Cada lugar de trabajo puede tener entre 1 y 100 proyectos supervisados, incluidos uno o más proyectos de Google Cloud y cualquier cantidad de cuentas de AWS. Puede tener todos los lugares de trabajo que desee, pero los proyectos de Google Cloud y las cuentas de AWS no se pueden supervisar en más de un lugar de trabajo.

Un lugar de trabajo contiene los paneles personalizados, las políticas de alertas, las verificaciones de tiempo de actividad, los canales de notificaciones y las definiciones de grupo que usa con sus proyectos supervisados. Un lugar de trabajo puede acceder a los datos de métricas de los proyectos supervisados, pero las entradas de registros y los datos de métricas permanecen en los proyectos individuales.

El primer proyecto supervisado de Google Cloud en un lugar de trabajo se llama proyecto de hosting y debe especificarse cuando se crea el lugar de trabajo. El nombre de ese proyecto se convierte en el nombre del lugar de trabajo. Si desea acceder a una cuenta de AWS, debe configurar un proyecto en Google Cloud para que contenga el conector de AWS.

Un lugar de trabajo es una única “vista”

- Determine sus necesidades de supervisión de manera anticipada.
- Considere usar lugares de trabajo independientes para el aislamiento de datos y del control.



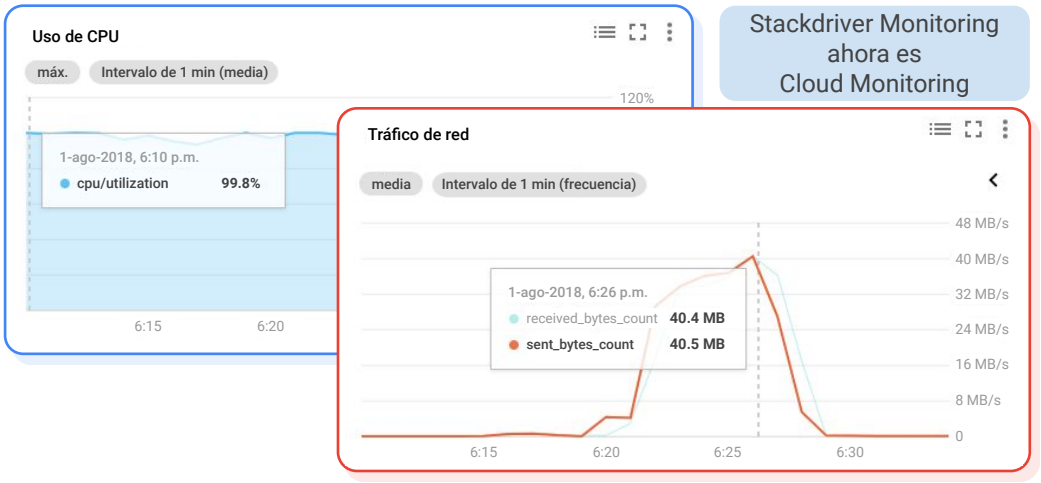
Stackdriver ahora es Google Cloud's operations suite

Gracias a que los lugares de trabajo pueden supervisar todos los proyectos de Google Cloud en un solo lugar, estos son una única “vista” a través de la cual puede ver recursos de varios proyectos de Google Cloud y cuentas de AWS. Todos los usuarios de Google Cloud's operations suite con acceso a ese lugar de trabajo también pueden acceder a todos los datos de forma predeterminada.

Esto significa que un rol asignado a una persona en un proyecto se aplica igualmente a todos los proyectos que supervisa ese lugar de trabajo.

Con el fin de darles a las personas diferentes roles por proyecto y controlar la visibilidad de los datos, considere colocar la supervisión de esos proyectos en lugares de trabajo independientes.

En los paneles, se visualiza la utilización y el tráfico de red



Cloud Monitoring permite crear paneles personalizados que contienen gráficos de las métricas que desea supervisar. Por ejemplo, puede crear gráficos en los que se muestre el uso de CPU de sus instancias, los paquetes o bytes que envían y reciben esas instancias, y los paquetes o bytes que rechaza el firewall en ellas.

En otras palabras, los gráficos brindan visibilidad a la utilización y el tráfico de red de sus instancias de VM, como se muestra en esta diapositiva. Estos gráficos se pueden personalizar con filtros para quitar el ruido, grupos para reducir la cantidad de series temporales y conjuntos para agrupar varias series temporales.

Para obtener una lista completa de las métricas admitidas, consulte el vínculo a la documentación del siguiente video:
[https://cloud.google.com/monitoring/api/metrics_gcp]

Las políticas de alertas pueden notificar ciertas condiciones

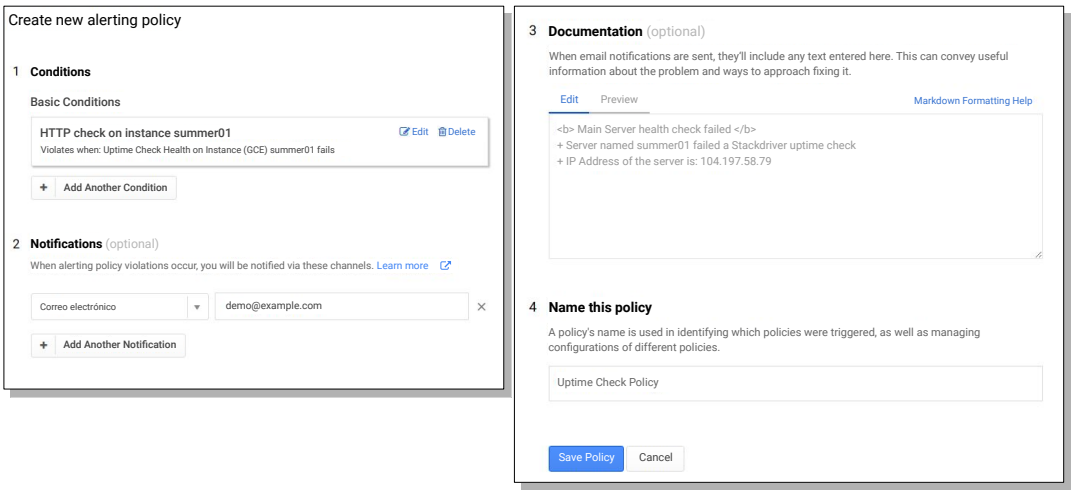
Si bien los gráficos son extremadamente útiles, solo pueden brindar estadísticas mientras alguien los revisa, pero ¿qué sucede si el servidor se apaga en medio de la noche o durante el fin de semana? ¿Espera que alguien siempre esté pendiente de los paneles para determinar si sus servidores están disponibles o si tienen suficiente capacidad o ancho de banda?

Si no es así, le recomendamos crear políticas de alertas que le notifiquen cuándo se cumplen condiciones específicas.

Por ejemplo, como se muestra en esta diapositiva, puede crear una política de alertas cuando la salida de red de su instancia de VM supera algún umbral por un período específico. Cuando se cumpla esta condición, usted o alguien más recibirá automáticamente una notificación por correo electrónico, SMS o cualquier otro canal con el fin de solucionar este problema.

También puede crear una política de alertas que supervise su uso de Google Cloud's operations suite y le envíe alertas cuando se acerque al umbral de facturación. Para obtener más información sobre esto, consulte la sección de vínculos del siguiente video:
[https://cloud.google.com/stackdriver/pricing#alert-usage]

Cree una política de alertas

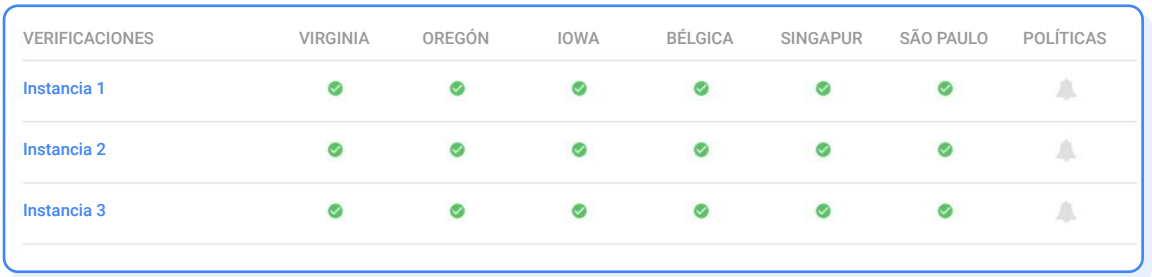


Este es un ejemplo de cómo luce el proceso para crear una política de alertas. A la izquierda, puede ver una condición de verificación de HTTP en la instancia summer01. Esta condición enviará un correo electrónico que se personaliza con el contenido de la sección de documentación a la derecha.

Analicemos algunas de las siguientes prácticas recomendadas para crear alertas:

- Recomendamos generar alertas sobre síntomas, no necesariamente sobre causas. Por ejemplo, se recomienda supervisar las consultas con errores de una base de datos y, luego, identificar si la base de datos dejó de funcionar.
- Posteriormente, asegúrese de que use varios canales de notificaciones, como correo electrónico y SMS, para evitar un punto único de fallo en su estrategia de alertas.
- Además, también recomendamos personalizar sus alertas según las necesidades del público describiendo las acciones necesarias que deben tomarse o los recursos requeridos que deben examinarse.
- Finalmente, evite el ruido, ya que este podría causar alertas que deberán descartarse con el tiempo. Específicamente, ajuste las alertas de supervisión de modo que sean prácticas. No configure alertas sobre todos los eventos posibles.

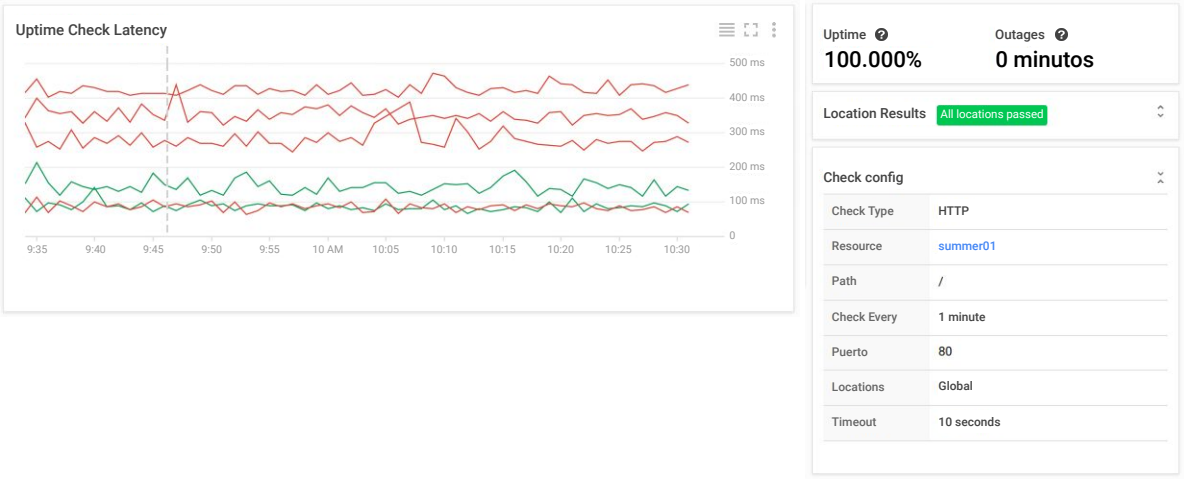
Las verificaciones de tiempo de actividad prueban la disponibilidad de sus servicios públicos



Las verificaciones de tiempo de actividad se pueden configurar para probar la disponibilidad de sus servicios públicos en diferentes ubicaciones en el mundo, como puede ver en esta diapositiva. El tipo de verificación de tiempo de actividad se puede configurar en HTTP, HTTPS o TCP. El recurso que se verificará puede ser una aplicación de App Engine, una instancia de Compute Engine, una URL de un host, o una instancia o un balanceador de cargas de AWS.

Para cada verificación de tiempo de actividad, puede crear una política de alertas y ver la latencia de cada ubicación global.

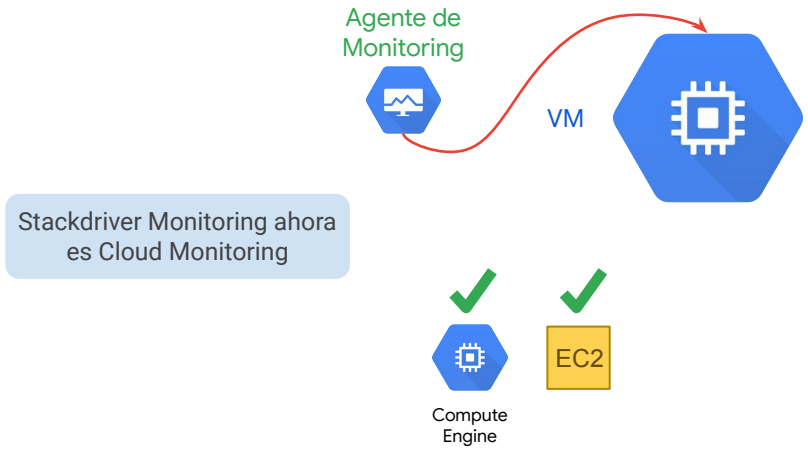
Ejemplo de verificación de tiempo de actividad



Este es un ejemplo de una verificación de tiempo de actividad de HTTP. El recurso se verifica cada minuto con un tiempo de espera de 10 segundos. Las verificaciones de tiempo de actividad que no reciban una respuesta dentro de este tiempo de espera se considerarán fallas.

Hasta ahora, hay un 100% de tiempo de actividad sin interrupciones.

Agente de Monitoring



Cloud Monitoring puede acceder a algunas métricas sin este agente, incluidos el uso de CPU, algunas métricas de tráfico de disco, información sobre el tiempo de actividad y tráfico de red.

Sin embargo, para acceder a recursos del sistema y servicios de aplicaciones adicionales, debe instalar el agente de Monitoring.

El agente de Monitoring es compatible con instancias de EC2 y Compute Engine.

Instale el agente de Monitoring

Instale el agente de Monitoring (ejemplo)

```
curl -sSO https://dl.google.com/cloudagents/add-monitoring-agent-repo.sh
sudo bash add-monitoring-agent-repo.sh
```

El agente de Monitoring se puede instalar con estos dos simples comandos, que puede incluir en su secuencia de comandos de inicio.

Se supone que tiene una instancia de VM con Linux que está supervisada por un lugar de trabajo y que su instancia tiene las credenciales adecuadas para el agente. Para conocer los comandos actualizados, consulte la documentación.

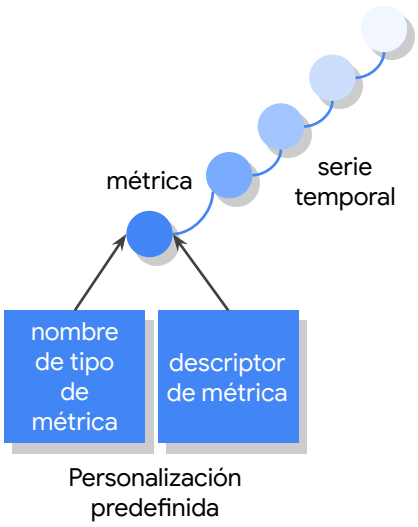
Métricas personalizadas

Ejemplo de métrica personalizada en Python:

```
client = monitoring.Client()
descriptor = client.metric_descriptor(
    'custom.googleapis.com/my_metric',

metric_kind=monitoring.MetricKind.GAUGE,
    value_type=monitoring.ValueType.DOUBLE,
    description='This is a simple example
of a custom metric.')
descriptor.create()
```

Stackdriver Monitoring ahora es Cloud Monitoring



Si las métricas estándar que proporciona Cloud Monitoring no se ajustan a sus necesidades, puede crear métricas personalizadas.

Por ejemplo, supongamos que tiene un servidor de juegos con capacidad para 50 usuarios. ¿Qué indicador de métricas podría usar para activar los eventos de escalamiento? Desde un punto de vista de la infraestructura, podría considerar usar la carga de CPU o, quizá, la carga de tráfico de red como valores que están relacionados de algún modo con la cantidad de usuarios. Con una métrica personalizada, podría pasar la cantidad actual de usuarios directamente de su aplicación a Cloud Monitoring.

Para comenzar a crear métricas personalizadas, consulte la sección de vínculos del siguiente video:
[https://cloud.google.com/monitoring/custom-metrics/creating-metrics#monitoring-create-metric-python]

Lab

Supervisión de recursos

Stackdriver Monitoring
ahora es Cloud Monitoring

Tomemos algunos de los conceptos de supervisión que acabamos de analizar y apliquémoslos en el lab.

En este lab, aprenderá a usar Cloud Monitoring para obtener estadísticas sobre las aplicaciones que se ejecutan en Google Cloud. Específicamente, habilitará Cloud Monitoring, agregará gráficos a paneles y creará alertas, grupos de recursos y verificaciones de tiempo de actividad.

Repaso del lab

Supervisión de recursos

Stackdriver Monitoring
ahora es Cloud Monitoring

En este lab, obtuvo una descripción general de Cloud Monitoring. Aprendió a supervisar su proyecto, crear alertas con varias condiciones, agregar gráficos a los paneles, y crear grupos de recursos y verificaciones de tiempo de actividad para sus servicios.

La supervisión es fundamental para el buen estado de su aplicación y Cloud Monitoring proporciona un conjunto completo de funciones con el fin de supervisar su infraestructura, visualizar los datos de supervisión y activar alertas y eventos por usted.

Puede continuar con un recorrido por el lab, pero recuerde que la interfaz de usuario de Google Cloud puede cambiar, por lo que su entorno podría ser un poco diferente.

Temario

Google Cloud's operations suite

Monitoring

Lab

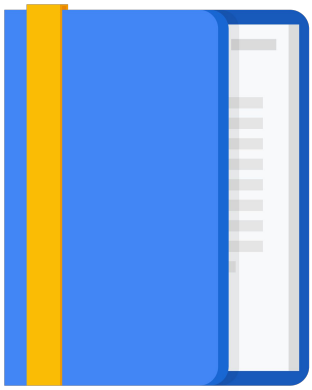
Logging

Creación de informes de errores

Trace

Debugger

Lab



La supervisión es la base de Google Cloud's operations suite, pero el servicio también ofrece registro, generación de informes de errores, seguimiento y depuración. Aprendamos sobre los registros.

Logging

- Registros de plataformas, sistemas y aplicaciones
  - API para escribir registros
  - Retención de 30 días
- Búsqueda, visualización y filtro de registros
- Métricas basadas en registros
- Posibilidad de configurar alertas de supervisión en eventos de registros
- Posibilidad de exportar datos a Cloud Storage, BigQuery y Pub/Sub

Cloud Logging
(anteriormente Stackdriver Logging)

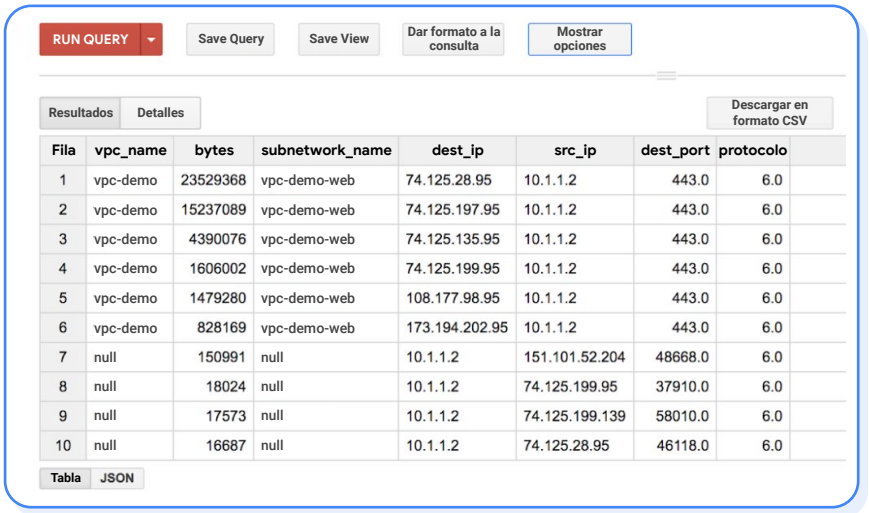
Cloud Logging le permite almacenar, buscar, analizar y supervisar los datos y eventos de registro de Google Cloud y AWS, así como emitir alertas sobre ellos. Es un servicio completamente administrado que funciona a gran escala y puede transferir datos de registro de aplicaciones y sistemas desde miles de VM.

Incluye almacenamiento para registros, una interfaz de usuario denominada el visor de registros y una API con la que se pueden administrar los registros de manera programática. El servicio permite leer y escribir entradas de registro, buscar y filtrar sus registros, y crear métricas basadas en registros.

Los registros solo se retienen por 30 días, pero puede exportarlos a buckets de Cloud Storage, conjuntos de datos de BigQuery y temas de Pub/Sub.

Exportar registros a Cloud Storage tiene sentido si se los quiere almacenar por más de 30 días, pero ¿por qué debería exportarlos a BigQuery o Pub/Sub?

Analice registros en BigQuery y visualícelos en Data Studio



Fila	vpc_name	bytes	subnetwork_name	dest_ip	src_ip	dest_port	protocolo
1	vpc-demo	23529368	vpc-demo-web	74.125.28.95	10.1.1.2	443.0	6.0
2	vpc-demo	15237089	vpc-demo-web	74.125.197.95	10.1.1.2	443.0	6.0
3	vpc-demo	4390076	vpc-demo-web	74.125.135.95	10.1.1.2	443.0	6.0
4	vpc-demo	1606002	vpc-demo-web	74.125.199.95	10.1.1.2	443.0	6.0
5	vpc-demo	1479280	vpc-demo-web	108.177.98.95	10.1.1.2	443.0	6.0
6	vpc-demo	828169	vpc-demo-web	173.194.202.95	10.1.1.2	443.0	6.0
7	null	150991	null	10.1.1.2	151.101.52.204	48668.0	6.0
8	null	18024	null	10.1.1.2	74.125.199.95	37910.0	6.0
9	null	17573	null	10.1.1.2	74.125.199.139	58010.0	6.0
10	null	16687	null	10.1.1.2	74.125.28.95	46118.0	6.0

Exportar registros a BigQuery permite analizar registros y hasta visualizarlos en Data Studio.

BigQuery ejecuta consultas en SQL extremadamente rápidas en gigabytes o petabytes de datos, lo que le permite analizar registros, como el tráfico de red, de modo que pueda entender mejor el crecimiento del tráfico para prever la capacidad, el uso de red a fin de optimizar los gastos de tráfico de red, o las intrusiones en la red para analizar incidentes.

Por ejemplo, en esta captura de pantalla, consultamos mis registros para identificar las direcciones IP principales que intercambiaron tráfico con mi servidor web. Según la ubicación de estas direcciones IP y a quién pertenezcan, podríamos reubicar parte de mi infraestructura para ahorrar en costos de redes o rechazar algunas de estas direcciones IP si no queremos que accedan a mi servidor web.

Si desea visualizar sus registros, le recomendamos conectar sus tablas de BigQuery a Data Studio. Esta herramienta transforma sus datos sin procesar en métricas y dimensiones que puede usar para crear informes y paneles fáciles de entender.

Mencionamos que también puede exportar registros a Cloud Pub/Sub, lo que le permite transmitirlos a aplicaciones o extremos.

Instale el agente de Logging

Instale el agente de Logging

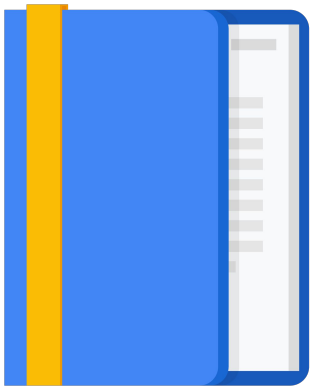
```
curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
sudo bash install-logging-agent.sh
```

Al igual que con el agente de Cloud Monitoring, es una práctica recomendada instalar el agente de Logging en todas sus instancias de VM. El agente de Logging se puede instalar con estos dos simples comandos, que puede incluir en su secuencia de comandos de inicio.

Este agente es compatible con instancias de EC2 y Compute Engine.

Temario

- Google Cloud's operations suite
- Monitoring
- Lab
- Logging
- **Creación de informes de errores**
- Trace
- Debugger
- Lab



Descubramos otra función de Google Cloud's operations suite: el informe de errores.

Error Reporting

Agrupa y muestra errores de servicios de nube en ejecución.

- Notificaciones de errores
- Panel de errores
- App Engine, Apps Script, Compute Engine, Cloud Functions, Cloud Run, GKE y Amazon EC2
- Go, Java, .NET, Node.js, PHP, Python y Ruby

Error Reporting

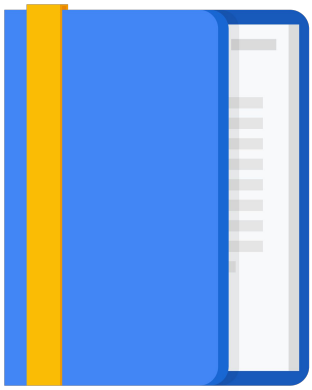
Error Reporting cuenta, analiza y recopila los errores de los servicios de nube en ejecución. En una interfaz centralizada de administración de errores, se muestran los resultados, los cuales se pueden ordenar y filtrar, y usted puede incluso configurar notificaciones en tiempo real que se envíen cuando se detecten errores nuevos.

En términos de lenguajes de programación, el analizador de seguimiento de pila de excepciones puede procesar Go, Java, .NET, Node.js, PHP, Python y Ruby.

Por cierto, menciono App Engine porque explorará Error Reporting en una app implementada en esa plataforma en el próximo lab.

Temario

- Google Cloud's operations suite
- Monitoring
- Lab
- Logging
- Creación de informes de errores
- **Trace**
- Debugger
- Lab



El seguimiento es otra función de Cloud Operations integrada en Google Cloud.

Trace

Sistema de seguimiento

- Los datos se muestran casi en tiempo real
- Informe de latencia
- Muestras de latencia por URL

Recopilación de datos de latencia

- App Engine
- Balanceadores de cargas de Google HTTP(S)
- Aplicaciones instrumentadas con los SDK de Cloud Trace

Cloud Trace
(anteriormente Stackdriver Trace)

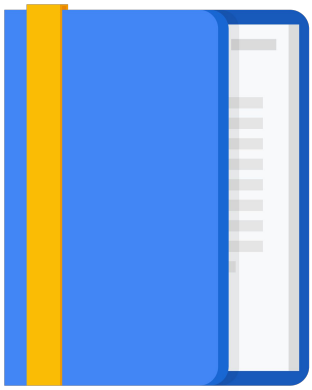
Cloud Trace es un sistema de seguimiento distribuido con el que se recopilan los datos de la latencia de sus aplicaciones, que luego se muestran en Cloud Console. Puede hacer un seguimiento de cómo se propagan las solicitudes a través de sus aplicaciones y recibir estadísticas de rendimiento detalladas casi en tiempo real.

Cloud Trace analiza automáticamente todos los seguimientos de su aplicación para generar informes detallados de latencia en los que se muestra el deterioro del rendimiento y se pueden captar seguimientos de App Engine, balanceadores de cargas HTTP(S) y aplicaciones instrumentadas con la API de Cloud Trace.

Administrar la cantidad de tiempo que tarda su aplicación en manejar las solicitudes entrantes y las operaciones de rendimiento es una parte importante de la administración del rendimiento general de la aplicación. Cloud Trace se basa, de hecho, en las herramientas que usamos en Google para mantener nuestros servicios en ejecución a una escala extrema.

Temario

- Google Cloud's operations suite
- Monitoring
- Lab
- Logging
- Creación de informes de errores
- Trace
- **Debugger**
- Lab



Finalmente, hablaremos de la última función de Google Cloud's operations suite que veremos en este módulo: el generador de perfiles.

Debugger

- Inspeccione una aplicación sin detenerla ni disminuir su velocidad significativamente
- Instantáneas de depuración:
  - Capture la pila de llamadas y las variables locales de una aplicación activa
- Puntos de registro de depuración:
  - Inserte registros en un servicio sin detenerlo
- Java, Python, Go, Node.js, Ruby, PHP y .NET Core

Cloud Debugger
(anteriormente
Stackdriver Debugger)

Cloud Debugger es una función de Google Cloud con la que puede examinar en tiempo real el estado de una aplicación en ejecución sin tener que detenerla ni disminuir su velocidad. Específicamente, el depurador agrega menos de 10 ms a la latencia de la solicitud cuando se captura el estado de la aplicación. En la mayoría de los casos, los usuarios no lo notan.

Estas funciones le permiten entender el comportamiento de su código en producción y analizar su estado para ubicar esos errores difíciles de detectar. Podrá tomar una instantánea del estado de la aplicación en ejecución o insertar una nueva instrucción de registro con solo unos clics.

Cloud Debugger admite varios lenguajes, incluidos Java, Python, Go, Node.js y Ruby.

Lab

Informes y depuración de errores

Stackdriver ahora es Google Cloud's operations suite

Apliquemos lo que acabamos de aprender sobre registros, generación de informes de errores, seguimientos y depuraciones en un lab.

En este lab, implementará una aplicación pequeña de “Hello, World” en App Engine. Luego, introducirá un error en la aplicación, que lo expondrá a las funciones de generación de informes y depuración de errores.

Repaso del lab

Informes y depuración de errores

Stackdriver ahora es Google Cloud's operations suite

En este lab, implementó una aplicación en App Engine. Luego, introdujo un error en el código, que interrumpió su funcionamiento. Usó Error Reporting para identificar y analizar el problema y encontró la causa raíz con Cloud Debugger. Por último, modificó el código para solucionar el problema.

Integrar todas estas herramientas en GCP le permite enfocarse en su código y en cualquier solución de problemas que incluya.

Puede continuar con un recorrido por el lab, pero recuerde que la interfaz de usuario de GCP puede cambiar, por lo que su entorno podría ser un poco diferente.

Repaso

Supervisión de recursos

Stackdriver ahora es
Google Cloud's operations suite

En este módulo, le presentamos una descripción general de Google Cloud's operations suite y sus funciones de supervisión, registro, generación de informes de errores, seguimiento de fallas y depuración. Tener todas estas funciones integradas en GCP le permite operar y mantener sus aplicaciones, lo que se conoce como ingeniería de confiabilidad de sitios o SRE.

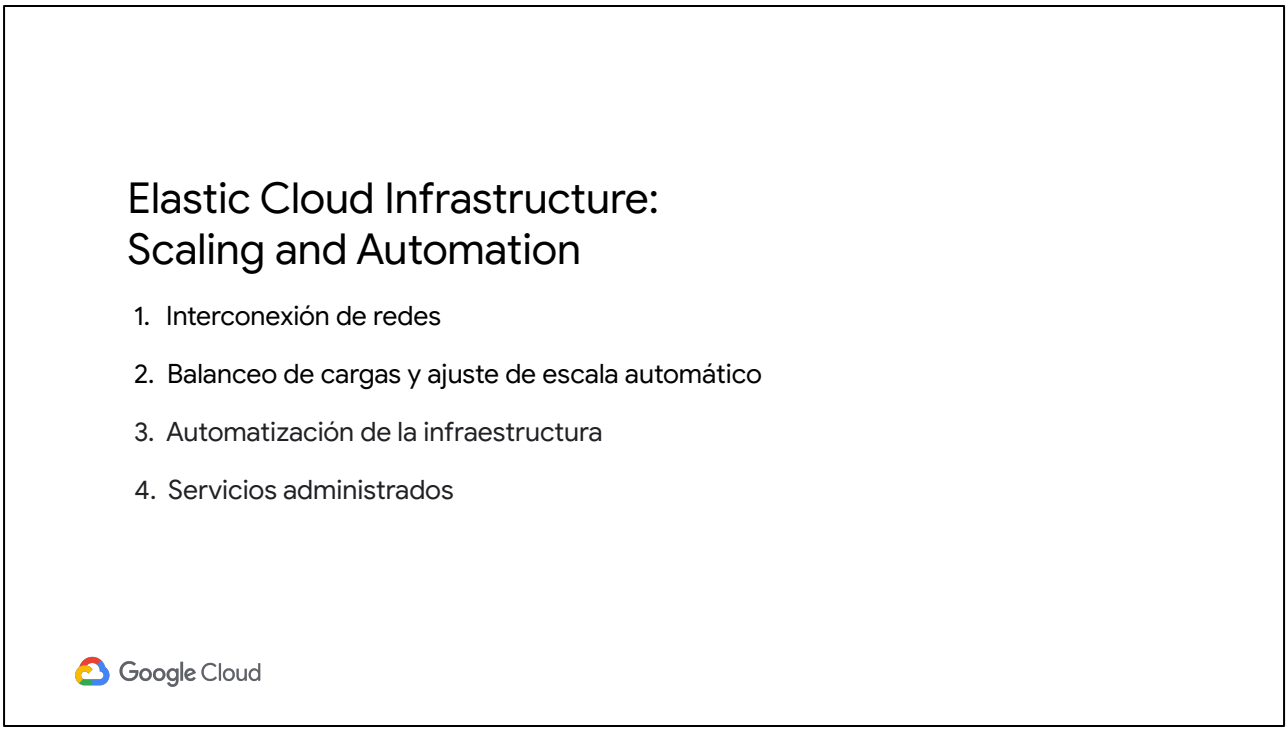
Si le interesa aprender más sobre la SRE, puede explorar el libro o algunos de nuestros cursos relacionados.

Repaso

Essential Cloud
Infrastructure: Core Services

Google Cloud

Gracias por realizar el curso “Essential Cloud Infrastructure: Core Services”. Esperamos que comprenda mejor cómo administrar la IAM, elegir entre diferentes servicios de almacenamiento de datos en GCP, examinar la facturación de recursos de GCP y supervisar esos recursos. Esperamos que las demostraciones y labs lo hayan ayudado a conocer mejor los diferentes servicios de GCP que ofrecemos.



A continuación, le recomendamos que se inscriba en el curso “Elastic Cloud Infrastructure: Scaling and Automation” de la serie “Architecting with Google Compute Engine”.

1. En primer lugar, abordaremos las distintas opciones para interconectar redes a fin de que pueda conectar su infraestructura a GCP.
2. Luego, analizaremos los servicios de balanceo de cargas y ajuste de escala automático de GCP para que pueda explorarlos de forma directa.
3. Luego, veremos los servicios de automatización de infraestructura, como Terraform, para que pueda automatizar la implementación de servicios de infraestructura de GCP.
4. Por último, hablaremos sobre otros servicios administrados que podría aprovechar en GCP.

Esperamos que disfrute el curso.