08-31-2026

Google

Google Cloud Platform is a suite of cloud computing services. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning. Google Cloud Platform provides infrastructure as a service, platform as a service, and serverless computing environments. In April 2008, Google announced App Engine, a platform for developing and hosting web applications in Google-managed data centers. Since the announcement of App Engine, Google added multiple cloud services to the platform. Google Cloud Platform is a part of Google Cloud, which includes the Google Cloud Platform public cloud infrastructure, as well as Google Workspace (G Suite), enterprise versions of Android and ChromeOS, and application programming interfaces (APIs) for machine learning and enterprise mapping services.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Getting data in

We recommend starting with Selecting the best method for Google data ingestion and then looking in more detail at options for the source types listed below.

Source	Add-ons and Apps	Guidance
Chrome Google Chrome is a widely used web browser developed by Google. Chrome offers a streamlined browsing experience with features such as tabbed browsing, synchronization across devices, integrated Google services, and advanced security protections. It supports a vast ecosystem of extensions and web applications, enabling users to customize their browsing experience, improve productivity, and enhance security.	**Splunk platform** • Google Chrome Add-on for Splunk	**Splunk Lantern Articles** • Getting started with the Google Chrome App for Splunk
	Splunk platform	**Configuration**

Source	Add-ons and Apps	Guidance
Cloud Platform Google Cloud Platform is a suite of public cloud computing services offered by Google. The platform includes a range of hosted services for for compute, storage, networking, big data, machine learning and IoT, as well as cloud management, security and developer tools, with a variety of different products available.	• Splunk Add-on for Google Cloud Platform	• Splunk Add-on for Google Cloud Platform • Google Cloud Platform Services in Splunk Observability Cloud **Splunk Lantern Articles** • Ingesting Google Cloud asset inventory data • Ingesting Google Cloud data into Splunk using command line programs • Monitoring Google Cloud SQL • Using ingest actions to route data to Google Cloud Storage
Kubernetes Engine Google Kubernetes Engine (GKE) provides a managed environment for deploying, managing, and scaling your containerized applications using Google infrastructure. The GKE environment consists of multiple machines (specifically, Compute Engine instances) grouped together to form a cluster.	**Splunk Observability Cloud** • The Splunk OpenTelemetry Collector for Kubernetes	**Configuration** • Collect Kubernetes data on Splunk Observability Cloud **Splunk Lantern Articles** • Integrating Google

Source	Add-ons and Apps	Guidance
		Kubernetes Engine with Splunk Observability Cloud

Pub/Sub

Google Pub/Sub is used for streaming analytics and data integration pipelines to ingest and distribute data. It enables the user to create systems of event producers and consumers, called publishers and subscribers. Publishers communicate with subscribers asynchronously by broadcasting events to the Pub/Sub service. Pub/Sub then delivers events to all services that need to react to them. In the Common Information Model, Google Pub/Sub data can be mapped to the Authentication data model.

Configuration

- Pub/Sub to Splunk

Splunk Lantern Articles

- Deploying Workload Identity Federation between AWS and GCP
- Customizing the Splunk OpenTelemetry distribution to accommodate unsupported use cases

Workspace

Google Workspace, formerly GSuite, provides custom email for businesses and include collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, Sites, and more.

The Splunk Add-on for Google Workspace allows a Splunk administrator to collect Google Workspace event data using Google Workspace APIs. You can then analyze the data in the Splunk platform.

Splunk platform

- Splunk Add-on for Google Workspace
- Google Workspace for Splunk

Splunk SOAR

- Google People
- Google Vault
- G Suite for

Configuration

- Splunk Add-on for Google Workspace
- Set up your own custom SAML application
- SAML app error messages

Splunk Lantern Articles

Source	Add-ons and Apps	Guidance
	Drive • Safe Browsing	• Configuring Google Workspace as a SAML IdP with Splunk Cloud Platform • Investigating Gsuite phishing attacks • Setting up a Google Workspace abuse mailbox asset in Enterprise Security using the IMAP v2 app

BigQuery

BigQuery is Google Cloud's fully managed and completely serverless enterprise data warehouse. BigQuery supports all data types, works across clouds, and has built-in machine learning and business intelligence, all within a unified platform.

Splunk SOAR

- Big Query

Splunk Lantern Articles

- Configuring Splunk DB Connect for use with Google BigQuery