Stackdriver Logging allows you to store, search, analyze, monitor and alert on log data and events from Google Cloud and Amazon Web Services. This page shows how to manage Stackdriver Logging using PowerShell. It walks through a simple example of creating logs, log sinks and log metrics.

Read the Cloud Tools for PowerShell cmdlet reference (http://googlecloudplatform.github.io/google-cloud-powershell/) to learn more about Stackdriver Logging cmdlets. To learn more about Stackdriver Logging in general, read the Overview of Stackdriver Logging (/logging) guide.

A log is a named collection of log entries within the project. A log entry records status or an event. The entry might be created by Google Cloud services, AWS services, third party applications, or your own applications. The "message" the log entry carries is called the payload, and it can be a simple string or structured data. Each log entry indicates where it came from by including the name of a monitored resource.

The cmdlet `New-GcLogEntry` can be used to create a log entry. You will have to specify the log that the entry belongs to (if the log does not exist, it will be created). To associate the log with a monitored resource, you can use the `-MonitoredResource` parameter. By default, the log entry is associated with the "global" resource. To create a monitored resource, use the `New-GcLogMonitoredResource` cmdlet.

You can retrieve log entries with the cmdlet `Get-GcLogEntry.`

To export log entries, you can create log sinks with the cmdlet `New-GcLogSink`. Stackdriver Logging will match incoming log entries against your sinks and all log entries matching each sink are then copied to the associated destination. Log entries that exist before the sink is created will not be exported.

Destinations for exported logs can be Cloud Storage Buckets, BigQuery Datasets or Pub/Sub Topics.

You can create log metrics that count the number of log entries that match certain criteria with the cmdlet `New-GcLogMetric`. These metrics can be used to create charts and alerting policies in Stackdriver Monitoring.