You can use Stackdriver Monitoring (/monitoring) and Stackdriver Logging (/logging) with Cloud IoT Core.

Stackdriver Monitoring automatically provides metrics at the registry level. You can use Stackdriver Monitoring to create dashboards, such as a dashboard for the total number of active devices in a registry. You can also set up alerts for when a particular metric exceeds a threshold, such as when the amount of billable bytes sent to and from the devices in a registry exceeds a limit you've set. Stackdriver Logging also provides the ability to use logs-based metrics (/logging/docs/logs-based-metrics/) from Stackdriver Monitoring. You can configure user-defined metrics to gain insights such as the number of devices that published data to a particular Pub/Sub topic.

For information on using monitoring with Cloud IoT Core, see Monitoring Resources (/iot/docs/how-tos/monitoring).

Cloud IoT Core produces two types of logs: audit logs and device logs. Both are available for viewing in Stackdriver Logging.

Audit logs can help you answer the questions, "Who did what, where, and when?" For example, you can use audit logs to see who created a device at a particular time, who recently sent a device configuration, or when the last time a registry's IAM policy was set.

Cloud IoT Core writes, and **provides by default**, audit logs for the following **Admin Activity** operations. These logs don't cost anything, nor do they count toward Stackdriver Logging quotas (/logging/quotas).

- `CreateDeviceRegistry`

- `DeleteDeviceRegistry`
- `UpdateDeviceRegistry`
- `CreateDevice`
- `DeleteDevice`
- `UpdateDevice`
- `ModifyCloudToDeviceConfig`
- `SetIamPolicy`

Cloud IoT Core writes, and **doesn't provide by default**, audit logs for **Data Access**. These logs are subject to Stackdriver Logging quotas (/logging/quotas) and pricing (/stackdriver/pricing):

- `GetDeviceRegistry`
- `ListDeviceRegistries`
- `GetDevice`
- `ListDevices`
- `GetIamPolicy`

For more information on using audit logs with Cloud IoT Core, see Viewing Cloud Audit Logs (/iot/docs/how-tos/audit-logging).

You can use device logs to find information about device connections, errors, and other lifecycle events. Whereas audit logs provide information about registry-level operations, device logs can be used to pinpoint issues with individual devices.

Device logs are not automatically collected and must be enabled manually. They are subject to their own quotas and limits (/iot/quotas#rate_limits) that are separate from and do not count toward Stackdriver Logging quotas (/logging/quotas). However, they are subject to Stackdriver Logging pricing (/stackdriver/pricing).

For information on using device logs with Cloud IoT Core, see Viewing Device Logs (/iot/docs/how-tos/device-logs).