



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

## Operations

Logging overview and approaches

---

## Contents

- 1 Overview and approaches
- 2 Solution-level logging approaches
  - 2.1 AKS logging approach
- 3 GKE logging
  - 3.1 Enable cloud logging
  - 3.2 Accessing logs
  - 3.3 Cloud Monitoring Console
  - 3.4 GKE Console
  - 3.5 Command-Line

---

Learn about the structured, unstructured, and Sidecar logging methods that Genesys Multicloud CX private edition services use.

### Related documentation:

- 
- 

### RSS:

- [For private edition](#)

## Overview and approaches

Application log files contain the important diagnostic information for various issues that may arise. Support of Genesys services rely on access to these application logs. In Genesys Multicloud CX private edition, the Genesys Multicloud CX services write these log files using different methods and formats. Some services write to a standard out/standard error (stdout/stderr) console while others write directly into an RWX shared storage. This data must be accessible outside of the cluster environment for shipping diagnostic logs for further review.

By default, GKE clusters are natively integrated with Cloud Logging. When you create a GKE cluster, Cloud Logging is enabled by default.

## Solution-level logging approaches

Private edition services use one of the following approaches:

- **Kubernetes-supported structured logging** — The services write structured logs. These logs are written in the standard stdout/stderr console and supported by Kubernetes. Fluentd collects these logs from multiple nodes and formats them by appending Kubernetes pod and project metadata. For more information, see [Kubernetes-supported structured logging](#).
- **Sidecar processed logging** — The services write their logs in a log file. A sidecar container processes these log files and then writes them to the stdout/stderr console. A log aggregator such as Fluentd collects these logs from stdout/stderr and formats them by appending Kubernetes pod and project metadata. For more information, see [Sidecar processed logging](#).
- **RWX logging (unstructured)** — The services write unstructured logs. These unstructured logs can neither be directly processed by a sidecar container nor be collected by Fluentd. These services write their logs in a mounted Persistent Volume Claim (PVC) bound to Persistent Volume (PV) which is backed by an RWX shared storage such as NFS or NAS for ease of access. For more information, see [RWX \(unstructured\) logging](#).

---

## Important

A Cluster Administrator must create appropriate PVCs and RWX shared storage path for the services that use the RWX logging method. For more information about creating the log-specific storage, refer to the related Genesys Multicloud CX private edition services.

RWX logging is deprecated. It will be phased out with the use of sidecars to facilitate legacy logging behavior.

## AKS logging approach

In Azure, the Log Analytics workspace feature in the Azure Monitor service collects log data from multiple services and system. You can create a single or multiple workspaces and feed the application logs into them.

For more detailed instructions, refer [Genesys logging github](#).

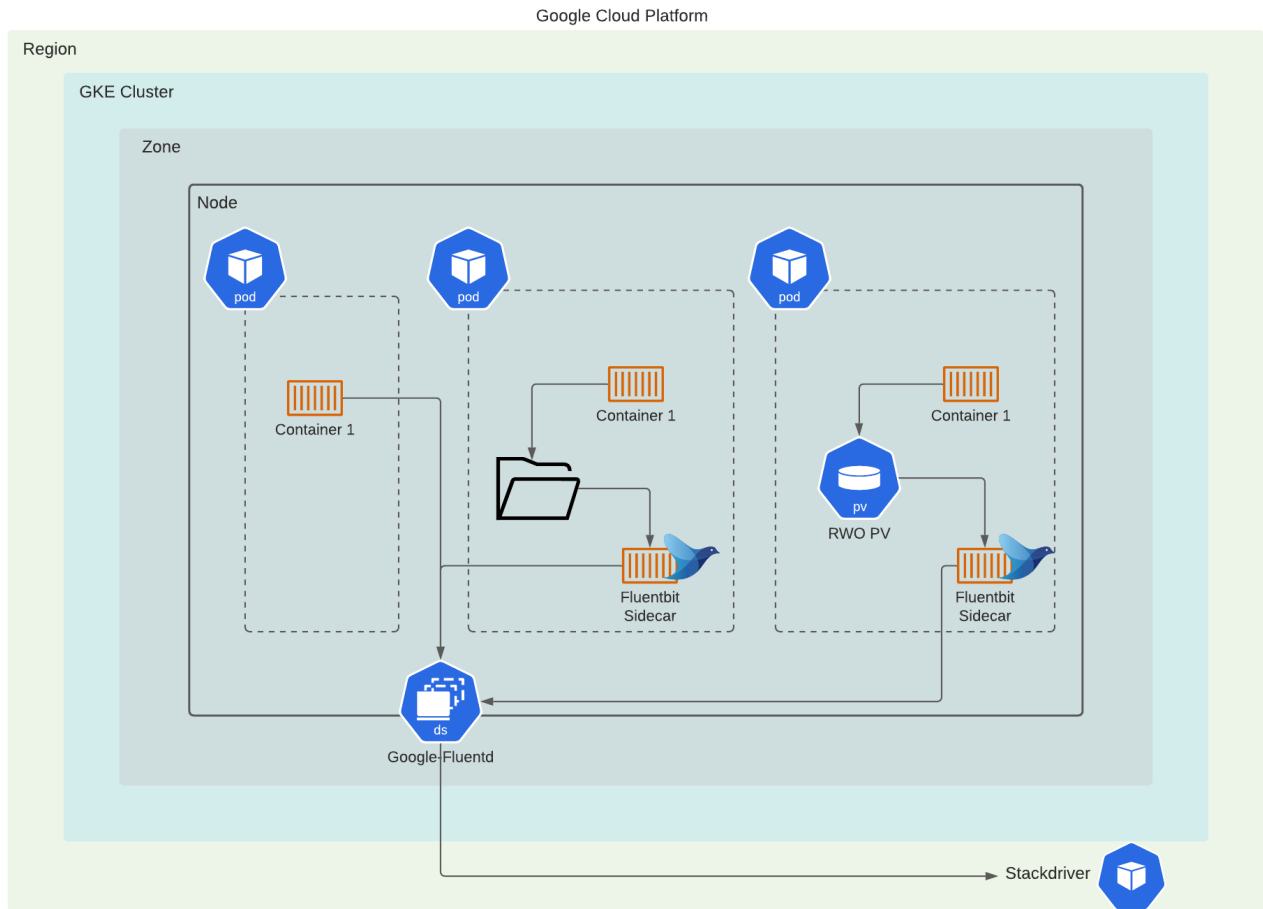
## GKE logging

Google Cloud's operations suite is backed by Google Stackdriver which controls logging, monitoring, and alerting within Google Cloud Platform. System and user workload logs are captured using Google's own Fluentd DaemonSet called Google-Fluentd that runs on each node in your cluster. The Daemon set parses container logs and pipes them to the stackdriver for processing.

Stackdriver provides built-in log metric capabilities that allows you to monitor specific log events for building dashboards and alert policies.

By default, GKE clusters are natively integrated with cloud logging. When you create a GKE cluster, cloud logging is enabled by default.

You can create a cluster with Logging enabled, or enable Logging in an existing cluster.



## Enable cloud logging

The following table provides the supported values for the `--logging` flag for the create and update commands.

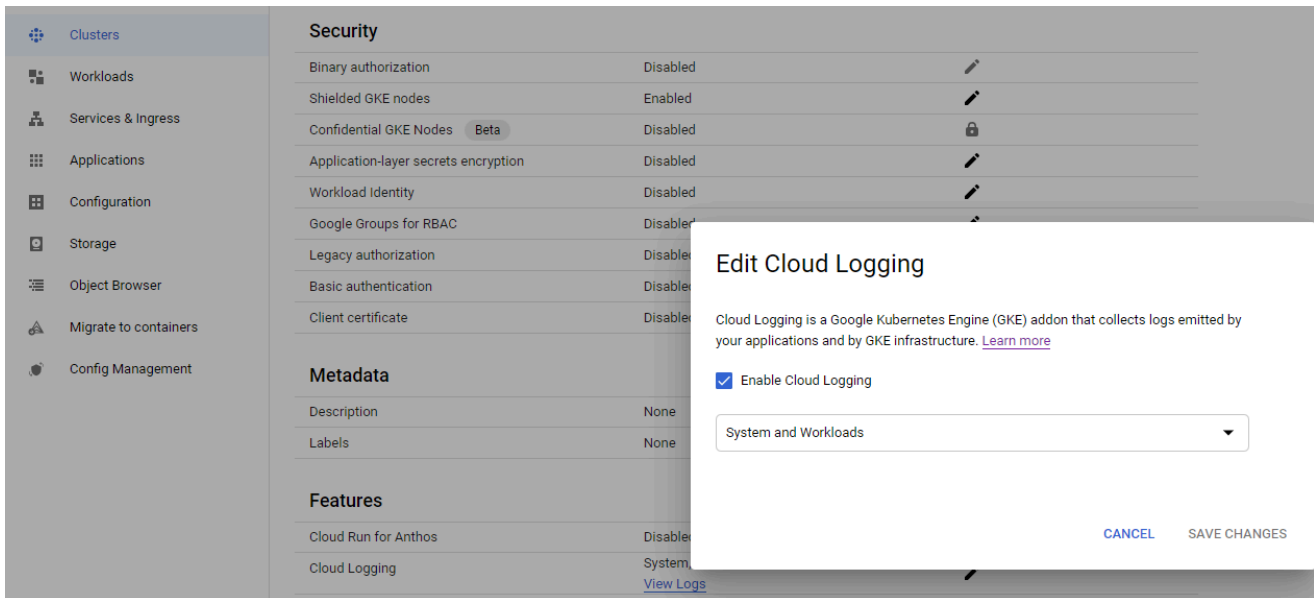
Source	Value	Logs collected
System	<b>SYSTEM</b>	Collects logs from: <ul style="list-style-type: none"> <li>Pods running in namespaces <code>kube-system</code>, <code>istio-system</code>, <code>knative-serving</code>, <code>gke-system</code>, and <code>config-management-system</code>.</li> <li>Key services that are not containerized including <code>docker/containerd runtime</code>, <code>kubelet</code>, <code>kubelet-monitor</code>, <code>node-problem-detector</code>,</li> </ul>

Source	Value	Logs collected
		and kube-container-runtime-monitor. <ul style="list-style-type: none"> <li>The node's serial ports output, if the VM instance metadata serial-port-logging-enabled is set to <b>true</b>.</li> </ul>
Workload	<b>WORKLOAD</b>	All logs generated by non-system containers running on user nodes.

## Console UI

To enable cloud logging through console UI, follow these steps:

1. Navigate to Console UI using: <https://console.cloud.google.com/kubernetes/list/overview?project=gcpe0001>
2. Select **Clusters** and then select the cluster name.
3. Under **Features**, select **Cloud Logging**, and then click **Edit**.
4. Select **Enable Cloud Logging** and then select **System and Workflow** from drop-down.
5. Save the changes.



## GCloud CLI

To enable cloud logging through GCloud CLI, follow these steps:

1. Log on to the existing GCloud cluster.

---

```
gcloud container clusters get-credentials gke1 --zone us-west1-a --project gcpe0001
```

2. Configure the logs to be sent to Cloud Logging by updating a comma-separated list of values to the `gcloud container clusters update` with `--logging` flag.

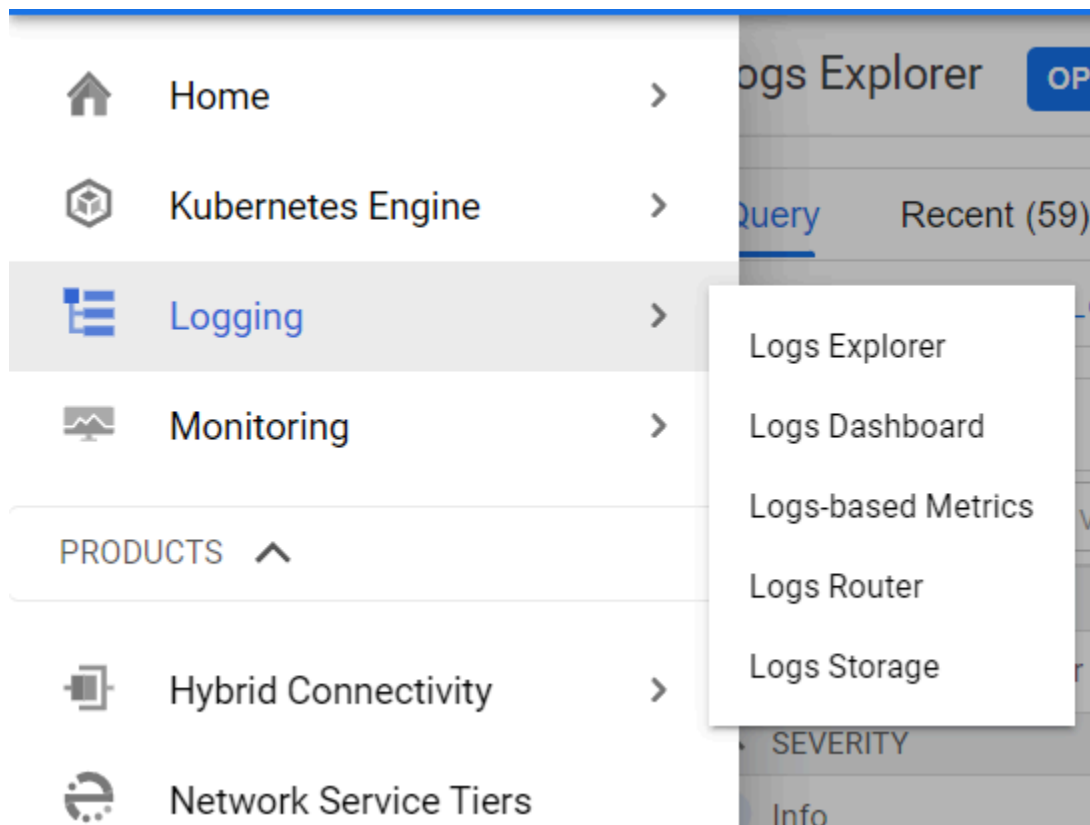
```
gcloud container clusters update gke1 \  
  --zone=us-west1-a \  
  --logging=SYSTEM,WORKLOAD
```

## Accessing logs

### Log Explorer

Log explorer is Google's central Logging UI. You can access logs for your Google cloud resources from this console, including GKE, Cloud SQL, VM instances and so on. You can then use logging filters to select the Kubernetes resources, such as cluster, node, namespace, pod, or container logs.

For more details about the console, click [here](#).



The screenshot shows the Google Cloud Platform Logs Explorer interface. At the top, there's a search bar and navigation options. The main area is divided into a left sidebar with filters, a central query editor, a histogram, and a table of query results.

**Log fields sidebar:**

- RESOURCE TYPE:  Kubernetes Container
- SEVERITY:  Info (237)
- LOG NAME:  stdout (237)
- PROJECT ID:  gcpe0001
- LOCATION:  us-west1-a
- CLUSTER NAME:  gke1
- NAMESPACE NAME:  voice
- POD NAME:

**Query:** `resource.type="k8s_container" resource.labels.project_id="gcpe0001" resource.labels.location="us-west1-a" resource.labels.cluster_name="gke1"`

**Histogram:** Shows log volume over time, with a peak around 1:30 PM on Sep 29.

**Query results table:**

SEVERITY	TIMESTAMP	ADT	SUMMARY
>	2021-09-29 14:02:36.077 ADT		voice-sipproxy {"date":"2021-09-29T17:02:36.077000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:39.519 ADT		voice-sipproxy {"date":"2021-09-29T17:02:39.518000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:39.519 ADT		voice-sipproxy {"date":"2021-09-29T17:02:39.519000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:45.672 ADT		voice-sipproxy {"date":"2021-09-29T17:02:45.672000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:46.065 ADT		voice-sipproxy {"date":"2021-09-29T17:02:46.065000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:46.065 ADT		voice-sipproxy {"date":"2021-09-29T17:02:46.065000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:52.595 ADT		voice-sipproxy {"date":"2021-09-29T17:02:52.595000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:52.595 ADT		voice-sipproxy {"date":"2021-09-29T17:02:52.595000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:55.679 ADT		voice-sipproxy {"date":"2021-09-29T17:02:55.679000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:59.154 ADT		voice-sipproxy {"date":"2021-09-29T17:02:59.154000000Z", "level":"debug", "module..."
>	2021-09-29 14:02:59.155 ADT		voice-sipproxy {"date":"2021-09-29T17:02:59.154000000Z", "level":"debug", "module..."

## Cloud Monitoring Console

Cloud Monitoring Console allows you to track metrics of resources within your GCP/GKE environment. This console allows you to access your logs from a particular Cluster, Namespace, Node, and Pod.

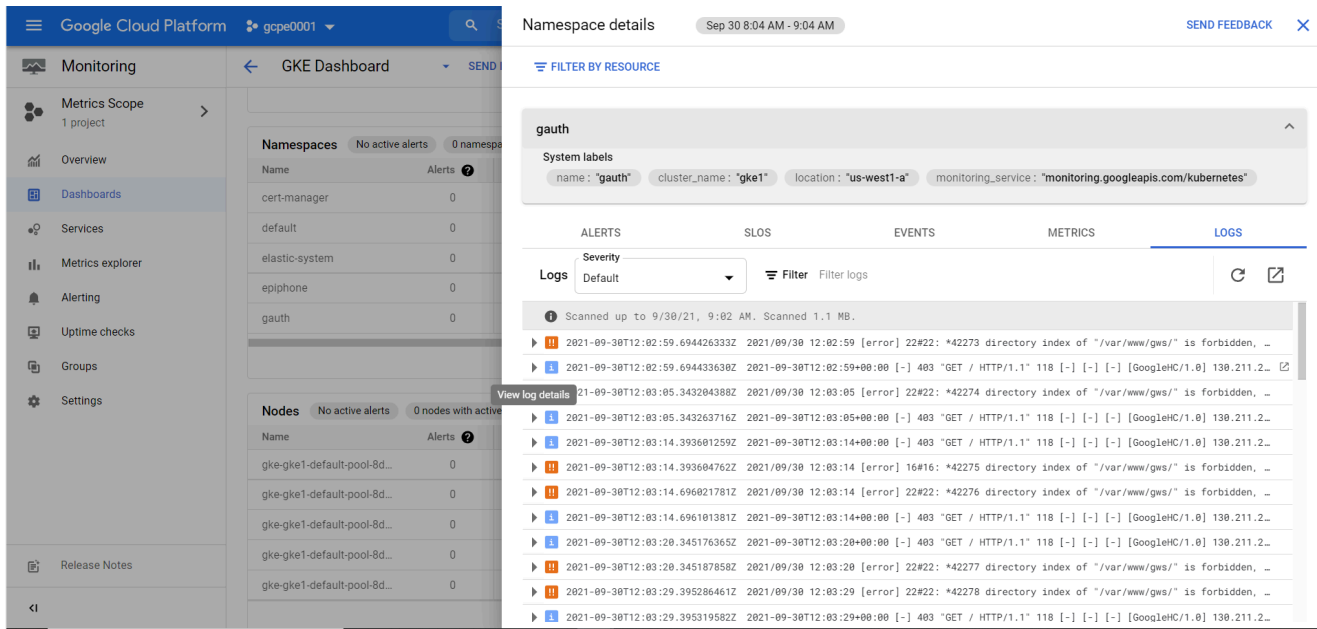
The screenshot shows the navigation menu of the Cloud Monitoring Console. The 'Monitoring' menu is open, displaying a list of options.

- Monitoring >
- PRODUCTS ^
- Network services >
- Hybrid Connectivity >
- Network Service Tiers
- Network Security >
- Network Intelligence >

The 'Monitoring' dropdown menu includes the following items:

- Overview
- Dashboards
- Services
- Metrics explorer
- Alerting
- Uptime checks
- Groups
- Settings





## GKE Console

GKE web console enables you to access to logs on individual pods actively running within a workload.

There is a filter option available to filter specific events, and a drop-down field to target specific severity of log events.

Logs provide a link to access **Logs Explorer** from a given pod to access the main logs explorer page for enhanced querying capabilities and other features.

Deployment details REFRESH EDIT DELETE ACTIONS KUBECTL SHOW INFO PANEL

**webrtc-gateway-blue**

OVERVIEW DETAILS REVISION HISTORY EVENTS LOGS YAML

Container logs Showing 23 log entries Severity: Default Filter Filter logs

Scanned up to 11/26/21, 3:59 AM. Scanned 44.6 KB.

- 2021-11-26T15:02:43.764094003Z <<< POST /sign\_in HTTP/1.1 X-Request-ID: f3c293ac833e2e2b2487cc7e5713db21 X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1 X-Forwarded-For: 10.198.64.1
- 2021-11-26T15:02:43.898335376Z HTTP session is created
- 2021-11-26T15:02:43.914271711Z >>> HTTP/1.1 200 Added Server: WEBRTCgw-100.0.016.0000 Cache-Control: no-cache Expires: 0 Connection: close Content-Type: text/plain Content-Length: 11
- 2021-11-26T15:02:43.914401356Z 200 Added
- 2021-11-26T15:02:44.025108583Z <<< GET /blue/wait HTTP/1.1 Host: webrtc.gke1-uswest1.gcp.e02.gcpce.com X-Request-ID: f9e101f52526718c9686c418fb7d674f X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1
- 2021-11-26T15:03:14.013783259Z >>> HTTP/1.1 200 OK Server: WEBRTCgw-100.0.016.0000 Cache-Control: no-cache Expires: 0 Connection: keep-alive Content-Type: text/plain Content-Length: 11
- 2021-11-26T15:03:14.131020590Z <<< GET /blue/wait HTTP/1.1 Host: webrtc.gke1-uswest1.gcp.e02.gcpce.com X-Request-ID: 43dd21f483fe5c499ea716a3b349933 X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1
- 2021-11-26T15:03:44.122467741Z >>> HTTP/1.1 200 OK Server: WEBRTCgw-100.0.016.0000 Cache-Control: no-cache Expires: 0 Connection: keep-alive Content-Type: text/plain Content-Length: 11
- 2021-11-26T15:03:44.235827814Z <<< GET /blue/wait HTTP/1.1 Host: webrtc.gke1-uswest1.gcp.e02.gcpce.com X-Request-ID: 0c24a3791840f48367405e869417192f X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1
- 2021-11-26T15:04:14.233171256Z >>> HTTP/1.1 200 OK Server: WEBRTCgw-100.0.016.0000 Cache-Control: no-cache Expires: 0 Connection: keep-alive Content-Type: text/plain Content-Length: 11
- 2021-11-26T15:04:14.359002048Z <<< GET /blue/wait HTTP/1.1 Host: webrtc.gke1-uswest1.gcp.e02.gcpce.com X-Request-ID: d2879de3bd8739fcd291f26a71fd9a9 X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1
- 2021-11-26T15:04:44.356324020Z >>> HTTP/1.1 200 OK Server: WEBRTCgw-100.0.016.0000 Cache-Control: no-cache Expires: 0 Connection: keep-alive Content-Type: text/plain Content-Length: 11
- 2021-11-26T15:04:44.469342809Z <<< GET /blue/wait HTTP/1.1 Host: webrtc.gke1-uswest1.gcp.e02.gcpce.com X-Request-ID: 3a710c48c7271ccf18d2110798d345f0 X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1
- 2021-11-26T15:05:14.458473441Z >>> HTTP/1.1 200 OK Server: WEBRTCgw-100.0.016.0000 Cache-Control: no-cache Expires: 0 Connection: keep-alive Content-Type: text/plain Content-Length: 11
- 2021-11-26T15:05:14.571867859Z <<< GET /blue/wait HTTP/1.1 Host: webrtc.gke1-uswest1.gcp.e02.gcpce.com X-Request-ID: 6afb35648e149b88f657e97c651bab07 X-Real-IP: 10.198.64.1 X-Forwarded-For: 10.198.64.1

## Command-Line

The standard **kubectl** logs commands are supported in GKE. They provide actively running stdout logs from containers.

## Example:

```
kubectl logs gvp-mcp-0 -n gvp -c fluentbit | more
```

```
mcooke@GEN-3HJ08F3:/mnt/c/Users/mcooke/PAT$ kubectl logs -n gvp gvp-mcp-0 -c fluentbit | more
[0] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.82959642, {"log=>"2021-11-18T06:27:25.051 Int 50019 00640219-1000DEA1 14058808077184 prompt_end done"}]
[1] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.829604394, {"log=>"2021-11-18T06:27:25.051 Int 50036 00640219-1000DEA1 140588090100032 appl_end ""}]
[2] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.829605409, {"log=>"2021-11-18T06:27:25.053 Int 50152 00640219-1000DEA1 1405880403950032 rtp_stats RTP 38190: Rx 0/0 lost 0 dropped 0 dec_err 0 jitter 0, tx 102/31384 enc_err 0"}]
[3] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.829606269, {"log=>"2021-11-18T06:27:25.053 Int 50001 00640219-1000DEA1 140588225337664 incall_end spled"}]
[4] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.829607118, {"log=>"2021-11-18T06:27:25.222 Int 50052 00640219-1000DEA2 140588225337664 incall_initiated 0:0"}]
[5] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.829607867, {"log=>"2021-11-18T06:27:25.231 Int 50056 00640219-1000DEA2 140588225337664 call_reference 1-38137@10.198.60.76|3F05FE9E-9123-708B-B378-944898C0D665|N/A|N/A|N/A"}]
[6] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216845.829608641, {"log=>"2021-11-18T06:27:25.231 Int 50000 00640219-1000DEA2 140588225337664 incall_begin sip:mml@127.0.0.1:5060|sip:vleg1@10.198.60.76:1236|20211118216845593|N/A|N/A|N/A"}]
[0] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216851.840976950, {"log=>"2021-11-18T06:27:30.251 Int 50152 00640219-1000DEA2 1405880402948416 rtp_stats RTP 38192: Rx 0/0 lost 0 dropped 0 dec_err 0 jitter 0, tx 249/42828 enc_err 0"}]
[1] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216851.840980893, {"log=>"2021-11-18T06:27:30.251 Int 50001 00640219-1000DEA2 140588225337664 incall_end usrend"}]
[0] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216855.845891724, {"log=>"2021-11-18T06:27:35.263 Int 50052 00640219-1000DEA3 140588225337664 incall_initiated 0:0"}]
[1] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216855.845896570, {"log=>"2021-11-18T06:27:35.263 Int 50056 00640219-1000DEA3 140588225337664 call_reference 1-21321@10.198.65.79|8298697A-E371-0623-FA67-0987F67110EE|Environment|IVRAppDefault|N/A"}]
[2] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216855.845897577, {"log=>"2021-11-18T06:27:35.263 Int 50000 00640219-1000DEA3 140588225337664 incall_begin sip:mml-dn@127.0.0.1:5060|sip:sipp@10.198.65.79:1236|20211118216855594|N/A|N/A|N/A"}]
[3] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216855.845898481, {"log=>"2021-11-18T06:27:35.263 Int 50130 00640219-1000DEA3 140588080902416 appl_begin INIT_URL=file://./samples/ulaw/helloworld.vxm|[DEFAULTS-File://usr/local/genesis/mcp/config/defaults-ng-dev.vxm|ANI=sip:sipp@10.198.65.79:1236|DNIS=sip:mml-dn@127.0.0.1:5060|PROTOCOLNAME=sip|PROTOCOLVERSION=2.0|CALLIDREF=1-21321@10.198.65.79|VXMLI_TYPE=NGI"}]
[4] MCP_genesis_log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216855.845899240, {"log=>"2021-11-18T06:27:35.263 Int 50016 00640219-1000DEA3 140588080902416 of_lookup_file://./samples/ulaw/helloid.vxm"}]

```