

GENESYS

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.



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 | SYSTEM | Collects logs from: Pods running in namespaces kube-system, istio-system, knative-serving, gke-system, and config-management-system. Key services that are not containerized including docker/containerd runtime, kubelet, kubelet-monitor, node-problem-detector, |

| Source | Value | Logs collected |
|----------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | and kube-container- runtime-monitor. The node's serial ports output, if the VM instance metadata serial-port-logging- enable is set to true. |
| Workload | WORKLOAD | 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.

| | Clusters | Security | | |
|----|-----------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 54 | Workloads | Binary authorization | Disabled 🧨 | |
| | | Shielded GKE nodes | Enabled 🖍 | |
| A | Services & Ingress | Confidential GKE Nodes Beta | Disabled 🔒 | |
| | Applications | Application-layer secrets encryption | Disabled 🇨 | |
| ⊞ | Configuration | Workload Identity | Disabled 🖍 | |
| | | Google Groups for RBAC | Disabler | |
| 2 | Storage | Legacy authorization | Disable Edit Cloud Logging | |
| 1 | Object Browser | Basic authentication | Disable | |
| à | Migrate to containers | Client certificate | Disable Cloud Logging is a Google Kubernetes Engine (GKE) addon that collects logs emitted by your applications and by GKE infrastructure. Learn more | |
| | Config Management | Metadata | Enable Cloud Logging | |
| | | Description | None | |
| | | Labels | None System and Workloads | |
| | | Features | | |
| | | Cloud Run for Anthos | Disabler CANCEL SAVE CHANG | ES |
| | | Cloud Logging | System | |
| | | | View Logs | |

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 gkel --zone us-westl-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 gkel \
    --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.



| ≡ | Google Cloud Platform | \$• gcpe0001 → | q Sear | arch products and resources 🗸 🗴 🖉 | 5 : 🙆 |
|----|-----------------------|--------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Ē | Operations Logging | Logs Explorer ортномз 🗸 | 🚫 REFI | INE SCOPE Project C> SHARE LINK () LAST 1 HOUR I PAGE LAYO | DUT 🗢 LEARN |
| Ξ | Logs Explorer | Query Recent (59) Saved (| 0) Sugge | jested (1) Stream logs | tun query 🗘 🗘 |
| 58 | Logs Dashboard | resource.type="k8s_container" | resource.la | labels.project_id="gcpe0001" resource.labels.location="us-west1-a" resource.labels.cluster_name="gke1"_ | / Edit query |
| ւհ | Logs-based Metrics | Log fields | × | Histogram | Q Q X |
| × | Logs Router | | | | |
| | Logs Storage | ▲ RESOURCE TYPE | | | |
| | | V Kubernetes Container | lear × | | 29. 2:04 PM |
| | | SEVERITY | | (Sep 29, 133 PM) | 5 29, 2:04 PM |
| | | i Info | 237 | Query results [] Jump to now Actions ~ | Configure v |
| | | LOG NAME | | SEVERITY TIMESTAMP ADT - SUMMARY | |
| | | stdout | 237 | <pre>> i 2021-09-29 14:02:36.077 ADT voice-sipproxy {"date":"2021-09-29T17:02:36.0770000000Z", "level":"debug"</pre> | "module |
| | | PROJECT ID | | > i) 2021-09-29 14:02:39.519 ADT 📪 voice-sipproxy {"date":"2021-09-29T17:02:39.5180000002", "level":"debug" | "module |
| | | Sector C | lear × | > i 2021-09-29 14:02:39.519 ADT (\$voice-sipproxy) {"date":"2021-09-29T17:02:39.519000001Z", "level":"debug" | "module |
| | | LOCATION | | > i 2021-09-29 14:02:45.672 ADT 📪 voice-sipproxy {"date":"2021-09-29T17:02:45.6720000002", "level":"debug" | "module |
| | | 🖌 us-west1-a | lear × | > i) 2021-09-29 14:02:46.065 ADT 📪 voice-sipproxy {"date":"2021-09-29T17:02:46.0650000008Z", "level":"debug" | "module |
| | | CLUSTER NAME | _ | > 1 2021-09-29 14:02:46.065 ADT voice-sipproxy {"date":"2021-09-29T17:02:46.0650000022", "level":"debug", | "module |
| | | A aka1 | lear Y | > 1 2021-09-29 14:02:52.595 ADT voice-sipproxy ("date":"2021-09-29717:02:52.595000000Z", "level":"debug" | "module |
| | | | | i 2021-09-29 14:02:52.595 ADT voice-sipproxy {"date":"2021-09-29T17:02:52.595000002Z", "level":"debug" | "module |
| E) | Release Notes | | | > i 2821-89-29 14:82:55.679 ADT ■ voice-sipproxy {"date":"2821-89-29717:82:55.67888808082", "level":"debug", | "module |
| E | Noieude Noied | Voice C | lear × | > i 2821-89-29 14:82:59.154 ADI ■ voice-sipproxy {"date":"2821-89-29117:82:59.1548880882", "level":"debug", | "module |
| <1 | | POD NAME | | 2021-09-224 14:02:29, 135 AUT WOLCE-STPPTOXY { (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 1340000022; "Level::debug (alte::2221-09-29117:02:29, 134000002; "Level::debug (alte::2221-09-29117:02:29, 134000002; "Level::debug (alte::2221-09-29117:02:29, 13400002; "Level::debug (alte::2221-09-29117:02:29, 134000; "Level::2000"; "Level::debug (alte::2221-09-29117:02:29, 13400; "Level::2000"; "Level::2000"; "Level::2000"; "Level::200"; "L | 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.

| | 55 5 | | | |
|----------|-----------------------|---|------------------------------|-----|
| <u> </u> | Monitoring | > | Overview | 1 |
| PROD | UCTS 🔨 | | Dashboards | an |
| | Network services | > | Services | |
| ÷ | Hybrid Connectivity | > | Metrics explorer Alerting | ain |
| 0 | Network Service Tiers | | Uptime checks | |
| A | Network Security | > | Groups | |
| | Network Intelligence | > | Settings | |

| ≡ | Google Cloud Platform | ঃ gcpe0001 → ৎ | Namespace details Sep 30 8:04 AM - 9:04 AM | SEND FEEDBACK |
|----------|-----------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <u>~</u> | Monitoring | ← GKE Dashboard - SEND I | THE FILTER BY RESOURCE | |
| •• | Metrics Scope | Namespaces No active alerts () namespa | gauth | ^ |
| | Overview | Name Alerts 2 | System labels | |
| | Dashboards | cert-manager 0 | name : "gauth" cluster_name : "gke1" location : "us-west1-a" monitoring_service : "monitoring.googleapis.com/i | kubernetes" |
| •° | Services | default 0 | ALERTS SLOS EVENTS METRICS | LOGS |
| th | Metrics explorer | elastic-system 0 | Severity Filter Filter | a ra |
| | Alerting | epiphone 0 | | |
| I | Uptime checks | gauth 0 | Scanned up to 9/30/21, 9:02 AM. Scanned 1.1 NB. 201-00.20110-0.150 404/26337. 2031/00/28 13:09:50 [accord 22879: ±49273 disentery index of "/usr/www/www/" disentery index of "//usr/www/www/" disentery index of "//usr/www/www/" disentery index of "//usr/www/www/" disentery index of "//usr/www/www/" disentery index of "//usr/www/ww/" disentery index of "//usr/www/ww/" disentery index of "//wsr/www/ww/" disentery index of "//wsr/www/wsr/wsr/www//wsr/www/wsr/wsr/w | e forhidden |
| (iii) | Groups | | I 2021-09-30T12:02:59.694433630Z 2021-09-30T12:02:59+00:00 [-] 403 "GET / HTTP/1.1" 118 [-] [-] [-] [GoogleHC/1 | .0] 130.211.2 🖄 |
| \$ | Settings | V Nodes No active alerts 0 nodes with active | ew log details 21-09-30T12:03:05.343204388Z 2021/09/30 12:03:05 [error] 22#22: *42274 directory index of "/var/www/gws/" i | s forbidden, .0] 130.211.2 |
| | | Name Alerts 🕐 | 2021-09-30T12:83:14.393601259Z 2021-09-30T12:03:14+00:00 [-] 403 "GET / HTTP/1.1" 118 [-] [-] [-] [GoogleHC/1 | .0] 130.211.2 |
| | | gke-gke1-default-pool-8d 0 | ▶ 🔢 2021-09-30T12:03:14.393604762Z 2021/09/30 12:03:14 [error] 16#16: *42275 directory index of "/var/www/gws/" i | s forbidden, … |
| | | gke-gke1-default-pool-8d 0 | 2021-09-30T12:03:14.696021781Z 2021/09/30 12:03:14 [error] 22#22: *42276 directory index of "/var/www/gws/" i | s forbidden, … |
| | | gke-gke1-default-pool-8d 0 | 2021-09-30T12:03:14.696101381Z 2021-09-30T12:03:14+00:00 [-] 403 "GET / HTTP/1.1" 118 [-] [-] [-] [GoogleHC/1 | .0] 130.211.2 |
| E) | Release Notes | gke-gke1-default-pool-8d 0 | El 2021-09-30T12:83:20.345176365Z 2021-09-30T12:03:20+00:00 [-] 403 "GET / HTTP/1.1" 118 [-] [-] [-] [GoogleHC/1 | .0] 130.211.2 |
| | 1010003110103 | gke-gke1-default-pool-8d 0 | P E2 2021-07-30112.03.20.34516/0502 2021/09/30 12:03.20 [error] 22#22; *42278 directory index of "/var/www/gws/" 1 | s forbidden |
| <1 | | | 2821-09-30T12:83:29.395319582Z 2021-09-30T12:83:29+00:00 [-] 403 "GET / HTTP/1.1" 118 [-] [-] [-] [GoogleHC/1 | .0] 130.211.2 |

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.

| Contraction Contractica Con | nt details C | REFRESH 📝 EDIT | DELETE | I≣ ACTIONS ▼ | ► KUBECTL 👻 | | SHOW INFO PANEL |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|--------------------------|----------------|----------------------|-----------------------------|--------------------------------------|---------------------------------|
| Swebrtc-ga | teway-blue DETAILS REVISI | ON HISTORY EVENTS | LOGS | YAML | | | |
| Container l | ogs Showing 23 log entries | Severity Default | → = | Filter Filter logs | | | |
| Scanne | d up to 11/26/21, 3:59 | AM. Scanned 44.6 KB. | | | | | |
| 2021-11 | I-26T15:02:43.764094003Z | <<< POST /sign_in HTTP/1 | .1 X-Request-1 | ID: f3c293ac833e2e2t | 2487cc7e5713db21 X-Real-IP: | 10.198.64.1 X-Forwarded-For: 10.198 | .64.1 X-Forwarded-X-Forwarded-F |
| 1 2021-11 | -26T15:02:43.898335376Z | HTTP session is created | | | | | |
| 11 2021-11 | I-26T15:02:43.914271711Z | >>> HTTP/1.1 200 Added S | erver: WEBRTCO | GW-100.0.016.0000 Ca | che-Control: no-cache Expir | es: 0 Connection: close Content-Type | : text/plain Content-Length: 11 |
| 1 2021-11 | I-26T15:02:43.914401356Z | 200 Added | | | | | |
| 11 2021-11 | I-26T15:02:44.025108583Z | <<< GET /blue/wait HTTP/ | 1.1 Host: web | rtc.gke1-uswest1.gcp | e002.gencpe.com X-Request-I | D: f9e101f52526718c9686c418fb7d674f | X-Real-IP: 10.198.64.1 X-Forwar |
| 11 2021-11 | I-26T15:03:14.013783259Z | >>> HTTP/1.1 200 OK Serv | er: WEBRTCGW-1 | 100.0.016.0000 Cache | -Control: no-cache Expires: | 0 Connection: keep-alive Content-Ty | pe: text/plain Content-Length: |
| 11 2021-11 | I-26T15:03:14.131020590Z | <<< GET /blue/wait HTTP/ | 1.1 Host: web | rtc.gke1-uswest1.gcp | e002.gencpe.com X-Request-I | D: 43dd21f483fe5c499ea716a3b3493933 | X-Real-IP: 10.198.64.1 X-Forwar |
| ▶ <u></u> 2021-11 | I-26T15:03:44.122467741Z | >>> HTTP/1.1 200 OK Serv | er: WEBRTCGW-1 | 100.0.016.0000 Cache | -Control: no-cache Expires: | 0 Connection: keep-alive Content-Ty | pe: text/plain Content-Length: |
| 2021-11 | I-26T15:03:44.235827814Z | <<< GET /blue/wait HTTP/ | 1.1 Host: web | rtc.gke1-uswest1.gcp | e002.gencpe.com X-Request-I | D: 0c24a3791840f48367405e869417192f | X-Real-IP: 10.198.64.1 X-Forwar |
| ▶ <u></u> 2021-11 | I-26T15:04:14.233171256Z | >>> HTTP/1.1 200 OK Serv | er: WEBRTCGW-1 | 100.0.016.0000 Cache | -Control: no-cache Expires: | 0 Connection: keep-alive Content-Ty | pe: text/plain Content-Length: |
| 2021-11 | 1-26T15:04:14.359002048Z | <<< GET /blue/wait HTTP/ | 1.1 Host: web | rtc.gke1-uswest1.gcp | e002.gencpe.com X-Request-I | D: d2879de3bd8739fcde291f26a71fd9a9 | X-Real-IP: 10.198.64.1 X-Forwar |
| 2021-11 | I-26T15:04:44.356324020Z | >>> HTTP/1.1 200 OK Serv | er: WEBRTCGW-1 | 100.0.016.0000 Cache | -Control: no-cache Expires: | 0 Connection: keep-alive Content-Ty | pe: text/plain Content-Length: |
| 2021-11 | 1-26T15:04:44.469342809Z | <<< GET /blue/wait HTTP/ | 1.1 Host: web | rtc.gke1-uswest1.gcp | e002.gencpe.com X-Request-I | D: 3a710c48c7271ccf18d2110798d345f0 | X-Real-IP: 10.198.64.1 X-Forwar |
| ▶ <u></u> 2021-11 | I-26T15:05:14.458473441Z | >>> HTTP/1.1 200 OK Serv | er: WEBRTCGW-1 | 100.0.016.0000 Cache | -Control: no-cache Expires: | 0 Connection: keep-alive Content-Ty | pe: text/plain Content-Length: |
| ▶ 🛄 2021-11 | 1-26T15:05:14.571867859Z | <<< GET /blue/wait HTTP/ | 1.1 Host: web | rtc.gke1-uswest1.gcp | e002.gencpe.com X-Request-I | D: 6afb35648e149b88f657e97c651bab07 | X-Real-IP: 10.198.64.1 X-Forwar |

Command-Line

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

Example:

kubebctl logs gvp-mcp-0 -n gvp -c fluentbit | more

| mcooke@GEN-3HJD0F3:/mmt/c/Users/mcooke/PAT\$ kubectl logs -n gvp gvp-mcp-0 -c fluentbit more |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [0] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_1404055_624.log: [1637216845.829599642, {"log">"2021-11-18T06:27:25.051 Int 50019 00640219-10000EA1 140580807077184 prompt_end done"}] |
| [1] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_104055_624.log: [1637216845.829604394, {"log"=>"2021-11-18T06:27:25.051 Int 50036 00640219-10000EA1 140588090100032 appl_end "}] |
| [2] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_104055_624.log: [1637216845.829605409, {"log"=>"2021-11-18T06:27:25.053 Int 50152 00640219-10000EA1 140588403956032 rtp_stats RTP 38190: Rx 0/0 lost 0 dropped 0 dec_err |
| 0 jitter 0, Tx 182/31304 enc_err 0"}] |
| [3] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_164055_624.log: [1637216845.829606269, {"log"=>"2021-11-18T06:27:25.053 Int 50001 00640219-10000EA1 140588225337664 incall_end aplend"}] |
| [4] MCP.genesys.log.gvp.mcp.gvp.mcp.04.MCP.20211109_104055_624.log: [1637216845.829607118, {"log"=>"2021-11-18T06:27:25.222 Int 50052 00640219-10000EA2 140588225337664 incall_initiated 0:0"}] |
| [5] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_1404055_624.log: [1637216845.829607867, {"log">"2021-11-18T06:27:25.231 Int 50056 00640219-10000EA2 140588225337664 call_reference 1-38137@10.198.68.76]3F05FE9E-9123-708 |
| B-837B-944898C60865 [N/A]N/A[N/A"]] |
| [6] MCP.genesys.log.gvp.mcp.gvp-mcp-0.MCP.20211109_1404055_624.log: [1637216845.829608641, {"log"=>"2021-11-18T06:27:25.231 Int 50000 00640219-10000EA2 140588225337664 incall_begin sip:msml@127.0.0.1:5070 sip:vleg1@10.198 |
| .68.76:1236[20211118216845593]N/A[N/A[N/A"}] |
| [0] MCP.genesys.log.gvp.mcp.gvp-mcp-0.MCP.20211109_184055_624.log: [1637216851.840976950, {"log"=>"2021-11-18T06:27:30.251 Int 50152 00640219-10000EA2 140588402948416 rtp_stats RTP 38192: Rx 0/0 lost 0 dropped 0 dec_err |
| 0 jitter 0, Tx 249/42828 enc_err 0"}] |
| [1] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_104055_624.log: [1637216851.840980903, {"log">>"2021-11-18T06:27:30.251 Int 50001 006640219-10000EA2 140588225337664 incall_end usrend"}] |
| [0] MCP.genesys.log.gvp.mcp.gvp-mcp-0.MCP.20211109_104055_624.log: [1637216855.845891724, {"log"=>"2021-11-18T06:27:35.263 Int 50052 00640219-10000EA3 140588225337664 incall_initiated 0:0"}] |
| [1] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_104055_624.log: [1637216855.845896570, {"log"=>"2021-11-18T06:27:35.263 Int 50056 00640219-10000EA3 140588225337664 call_reference 1-21321@10.198.65.79[B298697A-E371-062 |
| 3-FA67-0987F67110EE[Environment IVRAppDefault[N/A"}] |
| [2] MCP.genesys.log.gvp.mcp.gvp-mcp-0.MCP.20211109_1404055_624.log: [1637216855.845897577, {"log"=>"2021-11-18T06:27:35.263 Int 50000 00640219-10000EA3 140588225337664 incall_begin sip:msml-dng127.0.0.1:5060 sip:sipg010.1 |
| 98.65.79:1236[20211118216855594]N/A N/A N/A N/A"}] |
| [3] MCP.genesys.log.gvp.mcp.gvp.mcp.0.MCP.20211109_1404055_624.log: [1637216855.845898481, ("log"=>"2021-11-18T06:27:35.263 Int 50130 00640219-10000EA3 140588089092416 appl_begin INIT_URL=file:///samples/ulaw/helloworld |
| .vxml DEFAULTS=File:///usr/local/genesys/mcp/config/defaults-ng-dev.vxml ANI=sip:sipp@10.198.65.79:1236 DNIS=sip:msml-dn@127.0.0.1:5060 PROTOCOLVAME=sip PROTOCOLVAME_sip |
| |
| |