NetWitness® Platform

Google Cloud Platform (GCP) Event Source Log Configuration Guide

NETWITNESS
Platform

Google Cloud Platform

Event Source Product Information:

Vendor: Google Cloud

Event Source: Google Cloud Platform

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform 11.7 and higher

Note: Google Cloud Platform is supported from NetWitness Platform 11.5. However, NetWitness recommends you to update NetWitness Platform to the latest version.

Event Source Log Parser: cef, gcp (v11.5 & higher)

Note: The CEF parser parses this event source as **device.type=googlecloud**. The gcp parser parses this event source as **device.type=gcp**.

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Note: For 11.5.x and beyond, NetWitness can now parse JSON event data directly on the Log Decoder and there is no need to transform logs into CEF. Previously, plugins had to be tailored to each JSON schema individually. Now, all of the raw JSON event data can be sent straight to the Log Decoder. In v11.5, the plugin can collect logs in JSON event data and will pass them through to Log decoder directly in RFC 5424 format by adding a header, and it will be parsed by the JSON parser instead of the CEF parser(based on Raw JSON Event Parameter setting).

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

October, 2023

Contents

About Google Cloud Platform

Google Cloud Platform (GCP), offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning.

NetWitness Platform captures/pulls logs from Pub/Sub topic by subscribing to the same topic through the authorized service account. For more information on Cloud Logging process, see Routing and storage overview.

To configure Google Cloud Platform, you must complete these tasks:

1. Configure Google Cloud Platform Event Source.
2. Set Up the Google Cloud Platform Event Source in NetWitness Platform.

Configure Google Cloud Platform Event Source

To configure the Google Cloud Platform Event Source, follow the instructions provided in the below tasks.

I. Create a Service Account, see Create service accounts.

II. Create Service Account Key, see Create and delete service account keys.

III. Configure **Pub/Sub**, see Third-party integration with Pub/Sub.

Note: Please provide access to the domains **googleapis.com** and **pubsub.googleapis.com** in your Log collector/Virtual Log Collector (VLC) network to allow the GCP API pull the events. For more information, refer Google Cloud APIs.

NetWitness Supported Event Sources:

Event Type	Configuration Steps
VPC Flow Logs	Enable VPC Flow Logs and Route logs to BigQuery, Pub/Sub, and custom targets **IMPORTANT:** NetWitness Platform captures/pulls logs from Pub/Sub topic only.
Google Kubernetes Engine (GKE) Logs	Managing GKE logs and Collecting your logs
Cloud Storage Logs	Cloud Audit Logs with Cloud Storage and Route audit logs
Audit Logs	All the supported audit logs (Google Cloud services with audit logs) shall be routed to destination pub/sub, see Storing and routing audit logs

Windows VM Logs	Install Ops Agent: Installing the Ops Agent.
	Authorise Ops Agent: Authorize the Ops Agent.
	Configure Ops Agent: Configure the Ops Agent.
	Example config.yaml:
	`logging:`
	`  receivers:`
	`  windows_event_log:`
	`  type: windows_event_log`
	`  channels: [System, Application, Security]`
	`  receiver_version: 2`
	`  **render_as_xml: true**`

Event Type	Configuration Steps
	service: pipelines: default_pipeline: receivers: [windows_event_log]

Set Up the Google Cloud Platform Event Source in NetWitness Platform

In NetWitness Platform, perform the following tasks:

I. Deploy the **googlecloud** package and **CEF/gcp** parser from Live.

II. Configure the event source.

Deploy Google Cloud Files from Live

Google Cloud Platform uses the cef/JSON parser.

Note: For 11.5.x and beyond, While Configuring the Google Cloud Platform Event Source in the NetWitness Platform, by default **Enable Raw JSON Event** parameter will be set to False.
Based on the value for the parameter **Enable Raw JSON Event**, choose the appropriate parser.
1. If Enable Raw JSON Event set to false, then use cef parser.(Default setting).
2. If Enable Raw JSON Event set to true, then use gcp parser.

To deploy the Live content:

1. In the NetWitness Platform menu, select **CONFIGURE**.

   The **Live Content** tab is displayed.

2. Browse Live for the **cef/gcp** parser, using NetWitness Log Device as the Resource Type.
3. Select the cef/gcp parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.
4. You also need to deploy the Google Cloud package. Browse Live for Google Cloud EventLogs content, typing "Google Cloud" into the Keywords text box, then click **Search**.
5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

   Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC.

6. Restart the **nwlogcollector** service.

Note: The gcp parser can be used only for versions 11.5.x and beyond. Wherein cef parser can be used in versions 11.4.x and beyond.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the Live Services Management Guide.

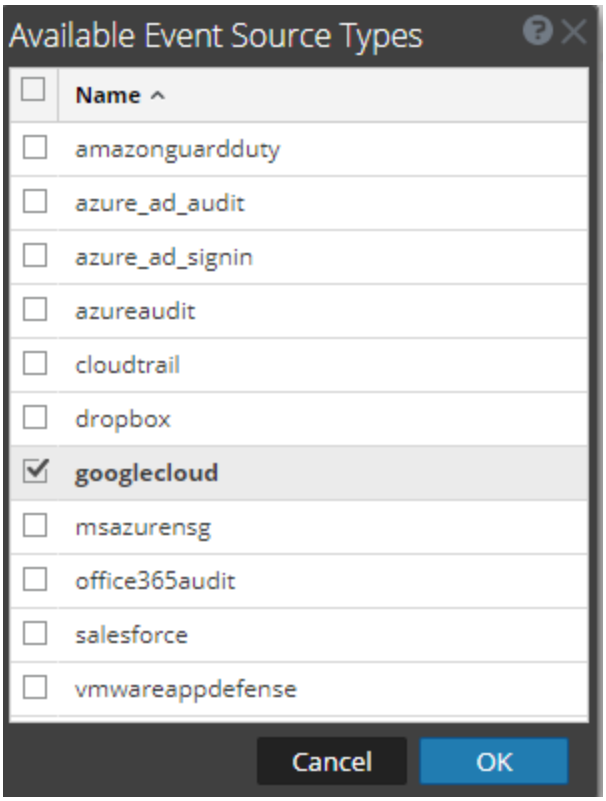
Configure the Event Source

To configure the Google Cloud Platform Event Source:

1. In the NetWitness Platform menu, select **Admin > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

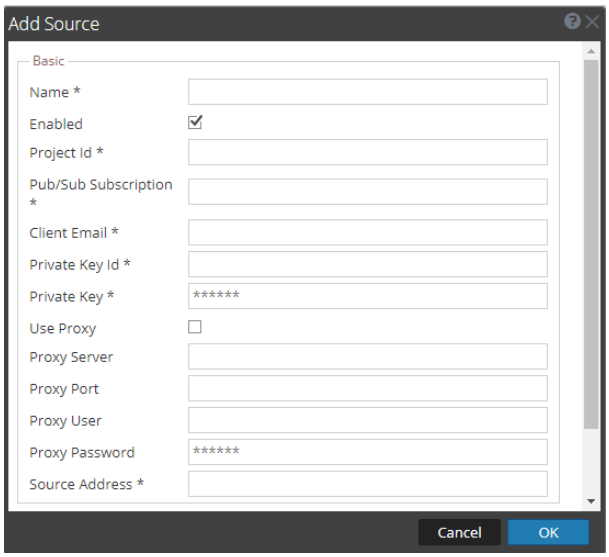


5. Select **googlecloud** from the list, and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.



7. Define parameter values, as described in Google Cloud Platform Collection Configuration Parameters.
8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.

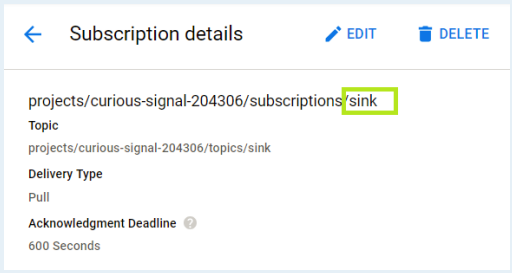
   The new event source is displayed in the Sources panel.

Google Cloud Platform Collection Configuration Parameters

The following table describes the configuration parameters for the Google Cloud Platform integration with NetWitness Platform.

Note: Fields marked with an asterisk (*) are required.

Basic Parameters

Name	Description
Name*	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
Project ID*	The Project ID is obtained from the JSON key file.
Pub/Sub Subscription*	Name of the Subscription from which the logs need to be pulled. **Note:** The subscription name is case sensitive. 
Client Email	Client_email obtained from the downloaded JSON file.
Private Key ID*	The Private Key ID is obtained from the JSON key file.
Private Key*	The Private Key is obtained from the JSON key file.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).

Name	Description
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	IP address that is to be provided to the Google cloud plugin instance. (Logs from this event source are collected with this device IP.)
Enable Raw JSON event	Enable Raw JSON event in configuration UI is applicable only on LC version 11.5 or above. Default behavior is that the raw events are transformed to cef format. Enabling this skips the transformation as the raw json events are sent to decoder in syslog 5424 format. To parse these logs collected in raw json format, need to deploy gcp parser from live.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Parameter	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.**> 300** is the default value.
Command Args	Optional arguments to be added to the script invocation.

Parameter	Description
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables and disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
SSL Enable	Uncheck this box to disable SSL certificate verification.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.