opentext™

ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Google Cloud Platform SmartConnector

Document Release Date: October 2023
Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Configuration Guide for Google Cloud Platform SmartConnector

This guide provides information about Google Cloud Connector that collects events from Google Cloud Platform.

This guide provides a high level overview of ArcSight SmartConnectors for the Cloud.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors 8.4.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

Product Overview

Google Cloud Platform is a suite of public cloud computing services offered by Google. The platform includes a range of hosted services for compute, storage and application development that run on Google hardware. Google Cloud Platform services can be accessed by software developers, cloud administrators, and other enterprises IT professionals over the public internet or through a dedicated network connection.

The following services are currently supported by the SmartConnector for Google Cloud:

- **Pub/Sub** is an asynchronous messaging service that decouples services that produce events from services that process events.

  You can use Pub/Sub as messaging-oriented middleware or event ingestion and delivery for streaming analytics pipelines.

  Pub/Sub offers durable message storage and real-time message delivery with high availability and consistent performance at scale. Pub/Sub servers run in all Google Cloud regions around the world.
- **IAM** lets you grant granular access to specific Google Cloud resources and helps prevent access to other resources. IAM enables you to adopt the least privileged security principle, stating that nobody should have more permissions than needed.
- **Security Command Center Premium** offers comprehensive threat detection for Google Cloud that includes Event Threat Detection, Container Threat Detection, and Virtual Machine Threat Detection as built-in services.

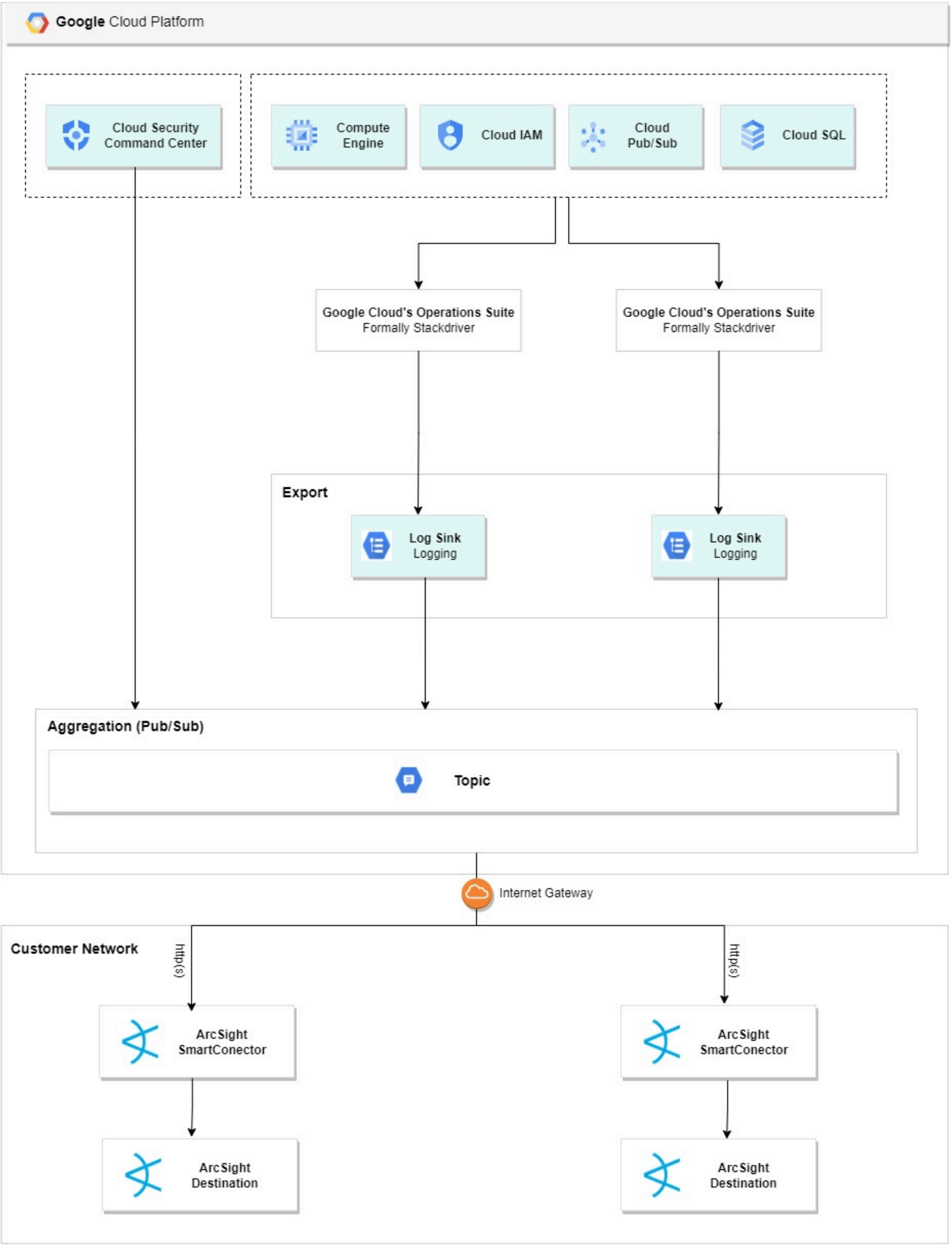
  The following log findings are supported by GSCC:
  - API key vulnerability findings
  - Compute image vulnerability findings
  - Compute instance vulnerability findings
  - Container vulnerability findings
  - Dataset vulnerability findings
  - DNS vulnerability findings
  - Firewall vulnerability findings
  - IAM vulnerability findings
  - KMS vulnerability findings
  - Monitoring vulnerability findings
  - Multi-factor authentication findings
  - Network vulnerability findings
  - Pub/Sub vulnerability findings
  - SQL vulnerability findings
  - Storage vulnerability findings
  - Subnetwork vulnerability findings
  - VM Manager findings

- Web Security Scanner findings
- Event Threat Detection rules

> Note: Some Google Cloud event logs with common event fields might be supported by the connector.

Understanding Data Collection

The following diagram provides a high-level overview of how the ArcSight SmartConnector for Google Cloud collects the Google Cloud Platform events.


Google Cloud Platform
Cloud Security Command Center
Compute Engine
Cloud IAM
Cloud Pub/Sub
Cloud SQL
Google Cloud's Operations Suite Formally Stackdriver
Google Cloud's Operations Suite Formally Stackdriver
Export
Log Sink Logging
Log Sink Logging
Aggregation (Pub/Sub)
Topic
Internet Gateway
Customer Network
http(s)
http(s)
ArcSight SmartConector
ArcSight SmartConector
ArcSight Destination
ArcSight Destination

Preparing to Collect Data

Before you can configure services to stream logs, make sure that you have the following prerequisite requirements:

- Google Cloud Platform Permissions
- Service Account Key

Google Cloud Platform Permissions

Role	Permissions	Description
Create Custom Role For example: ArcSight_ CustomRole	• pubsub.subscriptions.consume • pubsub.subscriptions.get • pubsub.topics.get	These are the minimum roles required to retrieve the events.

Note: While creating the Service Account under **Grant this service account access to project** section, click **Select Role** drop down menu, select the **Custom Role** created above and continue with the installation.

Creating a Service Account Key

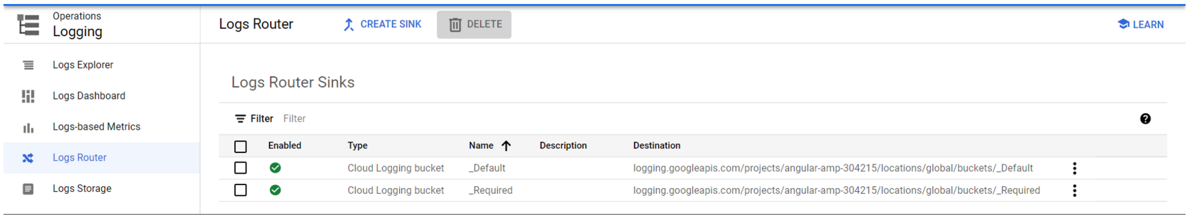
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google.

To create a new service account:

1. Go to **IAM & Admin** > **Service Accounts**.
2. Click **Create Service Account**.
3. Enter the **Service Account Details** and click **Done**.

   The account is successfully created.
4. **Click Actions** > **Create Key**.
5. Choose **JSON** as the export option and click **Create**.

The service key file is downloaded, and you will use it to access cloud resources.



Logs Router Sinks

□	Enabled	Type	Name ↑	Description	Destination
□	✓	Cloud Logging bucket	_Default		logging.googleapis.com/projects/angular-amp-304215/locations/global/buckets/_Default
□	✓	Cloud Logging bucket	_Required		logging.googleapis.com/projects/angular-amp-304215/locations/global/buckets/_Required

Configuring Log Retrieval

Creating a Topic

1. Go to the **Pub/Sub** resource.
2. Click **Topics**.
3. Click **Create Topic**.
4. Specify a unique topic ID, then click **Create Topic**.

   The topic and its subscription is successfully created.

Creating a Log Router

1. Go to **Operations** > **Logging** > **Log Router**.
2. Click **Create Sink**.
3. Enter the sink name and a description.
4. Choose the sink destination.
   a. Select the **Cloud Pub/Sub** topic as your sink service.
   b. Select the topic previously created.
5. Write a valid log query to filter out the events that are redirected to the topic.
6. If you want to create an exclusion filter, click **Create Sink** and the newly generated log is routed to the topic.

Creating a Log Router for SCC

1. Go to **Security Command Center**.
2. Click **Findings**.
3. Click **Export** > **Cloud Pub/Sub**.

4. Select your **Organization**.
5. Create a continuous export.
   a. Enter a unique name.
   b. Select Project name.
   c. Select the **Pub/Sub** topic that was created previously.
6. Save and exit.
7. Click the **Security Command Center Home** tab.
8. Click **Settings** > **Integrated Services**, then ensure that **Security Command Center** is Enabled.

Creating a Log Router for Topics Located in a Different Project

1. Go to **Operations** > **Logging** > **Log Router**.
2. Click **Create Sink**.
3. Enter the sink name and a description.
4. Choose the sink destination.
   a. Select a fully qualified topic name.
   b. Prepend **pubsub.googleapis.com** to it.

      The format is

      `pubsub.googleapis.com/projects/PROJECT_NAME/topics/TOPIC_NAME`

      for example

      `pubsub.googleapis.com/projects/angular-amp-304215/topics/ArcSight-Topic`
5. Write a valid log query to filter out the events that are redirected to the topic.
6. If you want to create an exclusion filter, click **Create Sink** and the newly generated log is routed to the topic.

Installing the Connector

Preparing to Install the Connector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

1. Before installing the SmartConnector, make sure that the following are available:
   - Local access to the machine where the SmartConnector is to be installed
   - Administrator passwords

Installing the Connector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Select **Google Cloud** from the **Type** drop-down list, then click **Next**
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Details
Proxy Host	Enter the proxy host IP address or name.
Proxy Port (Optional)	The proxy port used to access the Internet.
Proxy User Name (Optional)	The proxy user used to access the Internet.
Proxy Password (Optional)	The proxy password used to access the Internet.
Service Account File Path	Service account file path
Subscription Name	PubSub topic subscription name

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.

> **Note**: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.

10. Complete the installation.
11. Run the SmartConnector.

    For instructions about upgrading the connector or modifying parameters, see Installation and User Guide for SmartConnector.

Device Event Mapping to ArcSight Fields

Mappings for Pub/Sub and IAM

ArcSight ESM Field	Device-Specific Field
Device Product	protoPayload/serviceName
Device Vendor	Google Cloud
device Receipt Time	timestamp
Device Event Class Id	Last word of the (protoPayload/methodName) + "|" + (success|failure)
Name	protoPayload/methodName
Device Severity	severity
Device Custom String 1	resource/labels/project_id
Device Custom String 2	protoPayload/resourceName
Source User Name	protoPayload/authenticationInfo/principalEmail
Device Custom String 4	protoPayload/authenticationInfo/principalSubject
Device Custom String 5	protoPayload/request/messageRetentionDuration
Device Custom Date 1	protoPayload/requestMetadata/requestAttributes/time
Device Custom Date 2	receiveTimestamp
Device Custom Number 1	protoPayload/request/ackDeadlineSeconds
Source Address	protoPayload/requestMetadata/callerIp
Request Method	protoPayload/methodName
Request Client Application	protoPayload/requestMetadata/callerSuppliedUserAgent
Source Service Name	protoPayload/serviceName

ArcSight ESM Field	Device-Specific Field
Message	protoPayload/request/role/description
File Permission	protoPayload/serviceData/permissionDelta/addedPermissions
File Id	protoPayload/request/role_id

Mappings for Security Command Center

ArcSight Field	Vendor Field
Event Device Product	Security Command Center
Event Device Vendor	Google Cloud
Event Device Event Class ID	category
Event Name	category
Event Device Severity	severity_gscc
Event Device Receipt Time	eventTime
Event Device Custom Date 1	createTime
Event Device Custom String 1	ScannerName
Event Device Custom String 2	mitreAttack
Event Device Custom String 3	VulnerableNodePools
Event Device Custom String 4	OpenPorts/ExternallyAccessibleProtocolsAndPorts/remote_port_list
Event Device Custom String 5	role_member
Event Device Custom String 6	ep_string
Event Old File ID	OffendingIamRoles
Event Source Address	callerIp_gscc/Reverse_Shell_Stdin_Redirection_Src_Ip/vm_ips
Event Source User Name	principalEmail_gscc
Event Request Method	httpMethod
Event Message	Explanation/description_gscc
Event Device Dns Domain	canonicalName
Event Device Event Category	findingClass
Event File Path	name
Event File Type	type
Event Old File Path	ResourcePath

ArcSight Field	Vendor Field
Event File Name	VM_Instance_Name
Event Destination Service Name	ExposedService
Event Request URL	fuzzedUrl
Event Source Process Name	methodName_gscc
Event Destination Address	Reverse_Shell_Stdin_Redirection_Dst_Ip/abuse_target_ips
Event Source Port	Reverse_Shell_Stdin_Redirection_Src_Port
Event Destination Port	Reverse_Shell_Stdin_Redirection_Dst_Port

Troubleshooting

The Google SmartConnector cannot authenticate token with Google API.

The following error is displayed when when the connector is being used from ArcMc with the One-Click feature:

```
{ “error” : “invalid_grant”, “error_description” : "Invalid JWT: Token mustbe
a short-lived token (60 minutes) and in a reasonable timeframe. Check youriat
and exp values in the JWT claim." }
```

Workaround:

The common cause is that the clock from which you are executing your task is not in sync with the NTP (Network Time Protocol). Match the connector time with the current time.

For more information, see troubleshooting.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Google Cloud Platform SmartConnector (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!