

Cloud Logging Sink和Logging存储的模式:

1. Google cloud logging升级后, 生成了两个新的bucket: _default 和 _required

_required: 所有的audit log

_default: 所有打开了logging的云服务或者使用fluentd/api的方式上传到cloud logging的自定义的日志

2. 新的界面里面已经没有exclusion和inclusion界面的disable logging按钮了
3. 官方文档上说需要在sink的界面做exclusion,然而并没有exclusion的界面

<https://cloud.google.com/logging/docs/exclusions#create-filter>

The screenshot displays the Google Cloud Logging interface. On the left, the 'Logs Viewer' shows a list of logs from an 'Amazon EC2 Instance'. The logs are filtered by 'All logs' and 'Any log level' for the 'Last hour'. The logs show various JSON entries with fields like 'code_ver', 'Name', 'version', 'price_amount_micros', 'uid', 'info', 'content', and 'tsp'. On the right, the 'Edit Sink' configuration page is visible. It includes a 'Sink Name' field, a 'Sink Service' dropdown set to 'BigQuery', and a 'Sink Destination' dropdown set to 'Select BigQuery dataset'. A warning message indicates that configuring Cloud Logging and Custom Destination is currently only supported in Logs Router. There is a checkbox for 'Use Partitioned Tables' and 'Create Sink' and 'Cancel' buttons at the bottom.

4. 唯一的做法有两种, 新的设计模式是,所有的exclusion在sink中实现, 所有对应 _default和 _required有两个默认的logs router

Operations Logging

Logs Viewer

Logs Dashboard

Logs-based Metrics

Logs Router

Resource Usage

Logs Storage

Logs Router

CREATE LINK

DELETE

LEARN

Logs Router Sinks

Filter

Type	Name ↑	Description	Destination	State
<input type="checkbox"/>	Cloud Logging bucket	_Default	logging.googleapis.com/projects/seateam/locations/global/buckets/_Default	Enabled
<input type="checkbox"/>	Cloud Logging bucket	_Required	logging.googleapis.com/projects/seateam/locations/global/buckets/_Required	Enabled
<input type="checkbox"/>	BigQuery dataset	adjust	bigquery.googleapis.com/projects/seateam/datasets/adjust	Disabled
<input type="checkbox"/>	BigQuery dataset	bind_emailtest	bigquery.googleapis.com/projects/seateam/datasets/bindemail	Disabled
<input type="checkbox"/>	BigQuery dataset	bindacc	bigquery.googleapis.com/projects/seateam/datasets/bindacc	Disabled
<input type="checkbox"/>	BigQuery dataset	bindacc_v1	bigquery.googleapis.com/projects/seateam/datasets/bindacc_v1	Disabled
<input type="checkbox"/>	BigQuery dataset	bindemail	bigquery.googleapis.com/projects/seateam/datasets/bindemail	Disabled
<input type="checkbox"/>	BigQuery dataset	bindemail_v1	bigquery.googleapis.com/projects/seateam/datasets/bindemail_v1	Disabled
<input type="checkbox"/>	BigQuery dataset	fact	bigquery.googleapis.com/projects/seateam/datasets/fact	Enabled

可以直接disable `_default`的sink,这样就关闭了所有的logging了

5. 如果客户需要保留部分logging在cloud logging上,exclusion大部分日志节省成本,需要在_default的exclusion里面操作

Edit sink, 注意logs buckets选择_default; exclusion filter rate默认是0, 选择100是表示100%exclusion(文档里面没写,自己测试出来的)



Edit logs routing sink

Cloud Logging bucket

Select Logs Bucket *

_Default

DONE



Choose logs to include in sink

Create an inclusion filter to determine which logs are included in logs routing sink

Build inclusion filter

PREVIEW LOGS

```
1 NOT LOG_ID("cloudaudit.googleapis.com/activity") AND NOT
  LOG_ID("externalaudit.googleapis.com/activity") AND NOT
  LOG_ID("cloudaudit.googleapis.com/system_event") AND NOT
  LOG_ID("externalaudit.googleapis.com/system_event") AND
  NOT LOG_ID("cloudaudit.googleapis.com/
    access_transparency") AND NOT LOG_ID("externalaudit.
    googleapis.com/access_transparency")
```

DONE



Choose logs to filter out of sink (optional)

Create exclusion filters to determine which logs are excluded from logs routing sink

Exclusion filter name *

fact

Exclusion filter rate

100

Build an exclusion filter

DISABLE

DELETE

```
1 resource.type="aws_ec2_instance" AND logName!="projects/
  seateam/logs/sys_splunkinfo"
```

关于新的exclusion model,有一遍内部文档请参考:

<https://g3doc.corp.google.com/company/gfw/support/cloud/products/logging/index.md?cl=head>

常见日志管理操作(把cdn日志导出到bq并关闭本地 logging 存储):

1.在logs viewer里面按照资源类型查看日志

注意,这个时候使用的是_default的sink,把日志存在的cloud logging的默认log bucket中, 按照cloud logging的方式收费(50GB每月每project, 超过50GB,每GB收费0.5\$)

...

```
resource.type="http_load_balancer" resource.labels.forwarding_rule_name="fe-gcs-cdn"
resource.labels.url_map_name="gcs-cdn"
```

...

The screenshot shows the Google Cloud Logs Viewer interface. The left sidebar contains the 'Operations Logging' menu with options like 'Logs Viewer', 'Logs Dashboard', 'Logs-based Metrics', 'Logs Router', 'Resource Usage', and 'Logs Storage'. The main panel is titled 'Logs Viewer' and includes a 'Query builder' section with a search bar and filters. Below the query builder is a 'Logs field explorer' showing various resource types and their counts. To the right of the field explorer is a 'Histogram' chart showing log volume over time. At the bottom, the 'Query results' section displays a table of log entries with columns for severity, timestamp, and summary. A notification banner at the bottom indicates that the query has been updated.

2. 创建sink, 把日志流式的导入到bigquery中

The screenshot shows the Google Cloud Logging interface. On the left is a sidebar with navigation options: Operations, Logging, Logs Viewer, Logs Dashboard, Logs-based Metrics, Logs Router, Resource Usage, and Logs Storage. The main area is titled 'Logs Viewer' and includes a 'Query builder' section with filters for Resource, Log name, and Severity. A query is entered: `resource.type="http_load_balancer" resource.labels.forwarding_rule_name="fe-gcs-cdn" resource.labels.url_map_name="gcs-cdn"`. Below the query is a 'Log field explorer' showing a list of resource types and their counts. To the right of the explorer is a 'Histogram' chart. At the bottom, the 'Query results' table is visible, showing columns for Severity, Timestamp, and Summary. A red box highlights the 'Actions' menu, which includes options like 'Create Metric', 'Download Logs', and 'Create Sink'.

3. 选择Biqquery Dataset, 注意保留这个日志的查询语言,后面需要用来创建exclusion

The screenshot shows the 'Edit Sink' configuration page in Google Cloud Logging. The 'Sink Name' field is empty. The 'Sink Service' is set to 'BigQuery'. The 'Sink Destination' is set to 'audit'. A red arrow points to the 'Sink Service' dropdown. Another red arrow points to the 'Sink Destination' dropdown. The 'Create Sink' button is at the bottom right. The left sidebar is the same as in the previous screenshot. The main area shows the 'Logs Viewer' with a query filter and a table of log entries. A red arrow points to the 'Submit Filter' button.

4. 修改_default的sink, 增加exclusion

- Operations
Logging
- Logs Viewer
- Logs Dashboard
- Logs-based Metrics
- Logs Router
- Resource Usage
- Logs Storage

Logs Router Sinks

Filter

<input type="checkbox"/>	Type	Name ↑	Description	Destination	State	
<input type="checkbox"/>	Cloud Logging bucket	_Default		logging.googleapis.com/projects/cliu101/locations/global/buckets/_Default	Enabled	<div>View sink details Edit sink Disable sink Delete sink</div>
<input type="checkbox"/>	Cloud Logging bucket	_Required		logging.googleapis.com/projects/cliu101/locations/global/buckets/_Required	Enabled	
<input type="checkbox"/>	BigQuery dataset	bigquery-audit		bigquery.googleapis.com/projects/cliu101/datasets/audit	Enabled	
<input type="checkbox"/>	BigQuery dataset	logs		bigquery.googleapis.com/projects/cliu101/datasets/coins	Enabled	
<input type="checkbox"/>	BigQuery dataset	MYSINK		bigquery.googleapis.com/projects/cliu101/datasets/billing	Enabled	
<input type="checkbox"/>	BigQuery dataset	test-logging-agent-json		bigquery.googleapis.com/projects/cliu101/datasets/coins	Enabled	
<input type="checkbox"/>	BigQuery dataset	vpc-flow		bigquery.googleapis.com/projects/cliu101/datasets/wind	Enabled	

← Edit logs routing sink

✓ Choose logs to filter out of sink (optional)

Create exclusion filters to determine which logs are excluded from logs routing sink

Exclusion filter name *

cdn log

Exclusion filter rate

100

Build an exclusion filter

DISABLE ⏸

DELETE 🗑

```
1 resource.type="http_load_balancer" resource.labels.  
  forwarding_rule_name="fe-gcs-cdn" resource.labels.  
  url_map_name="gcs-cdn"
```

Build an exclusion filter

+ ADD EXCLUSION

UPDATE SINK

CANCEL