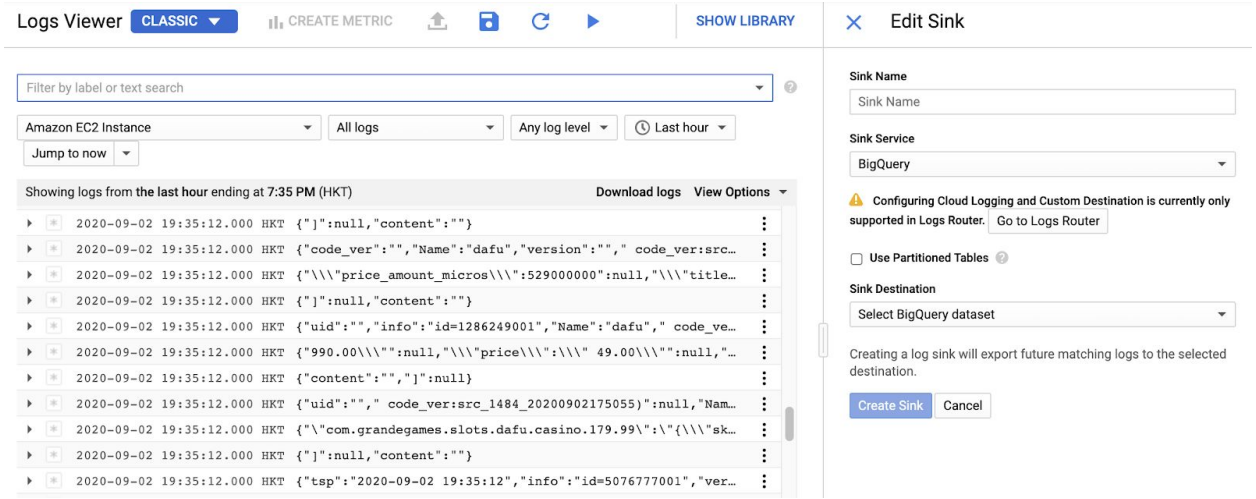
Cloud Logging Sink和Logging存储的模式:

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

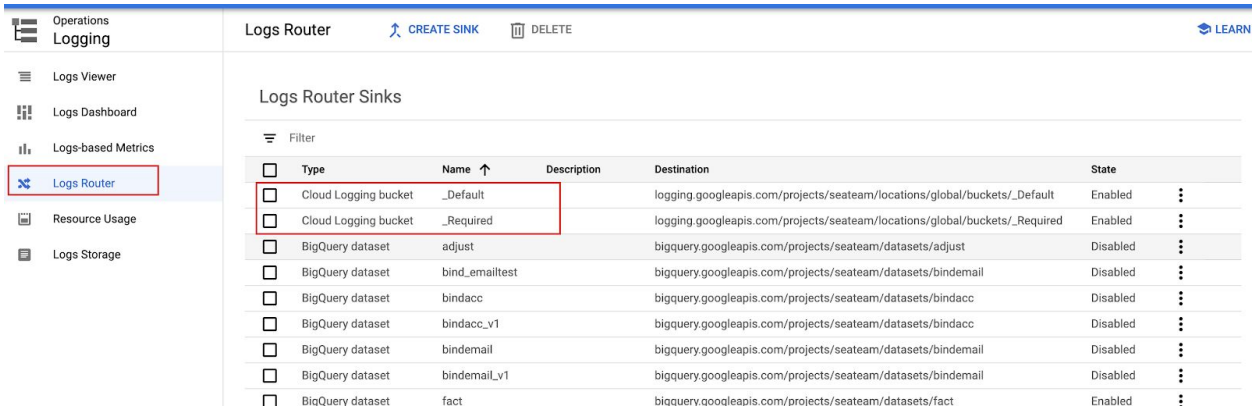
_required: 所有的audit log
_default: 所有打开了logging的云服务或者使用fluend/api的方式上传到cloud logging的自定义的日志

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



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



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 buckts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

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:

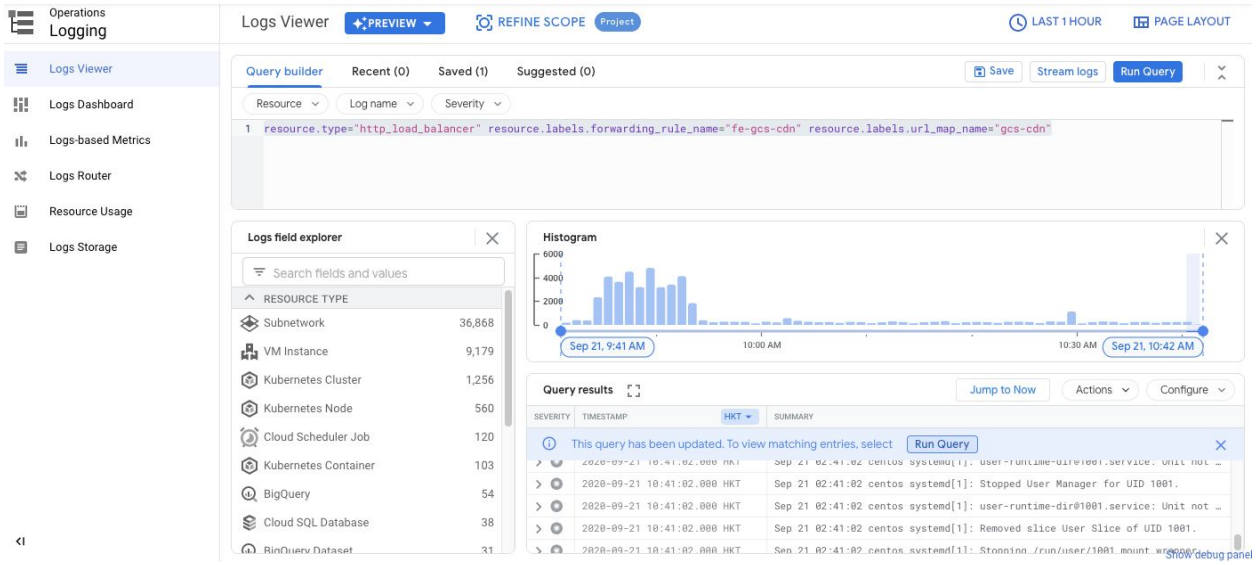
https://g3doc.corp.google.com/company/gfw/support/cloud/products/logging/index.md?cl=head

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

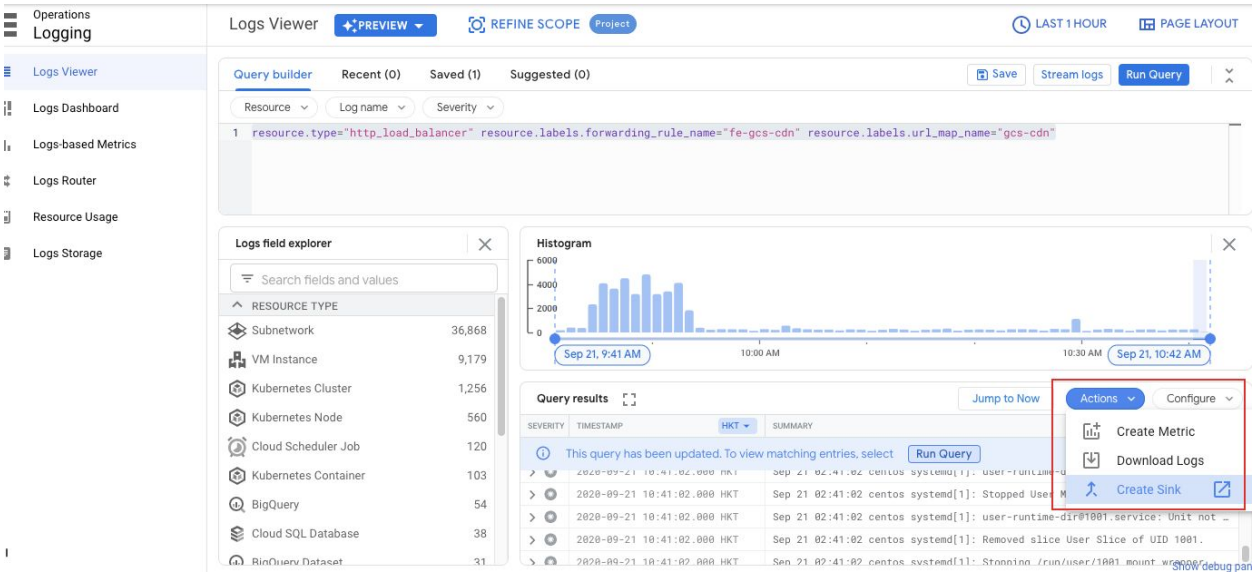
1.在logs viewer里面按照资源类型查看日志

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$)

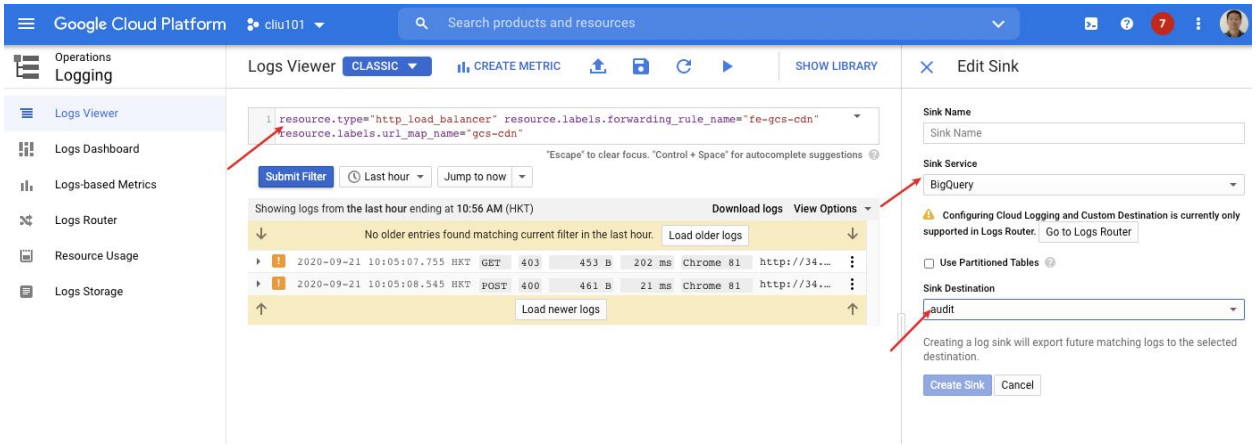
```
resource.type="http_load_balancer" resource.labels.forwarding_rule_name="fe-gcs-cdn" resource.labels.url_map_name="gcs-cdn"
```



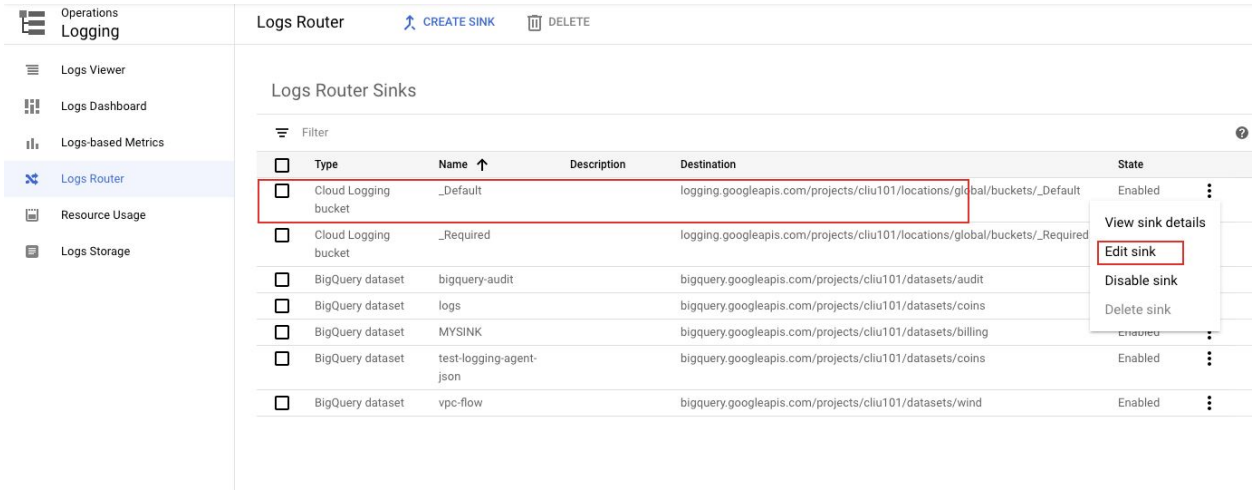
2.创建sink, 把日志流式的导入到bigquery中

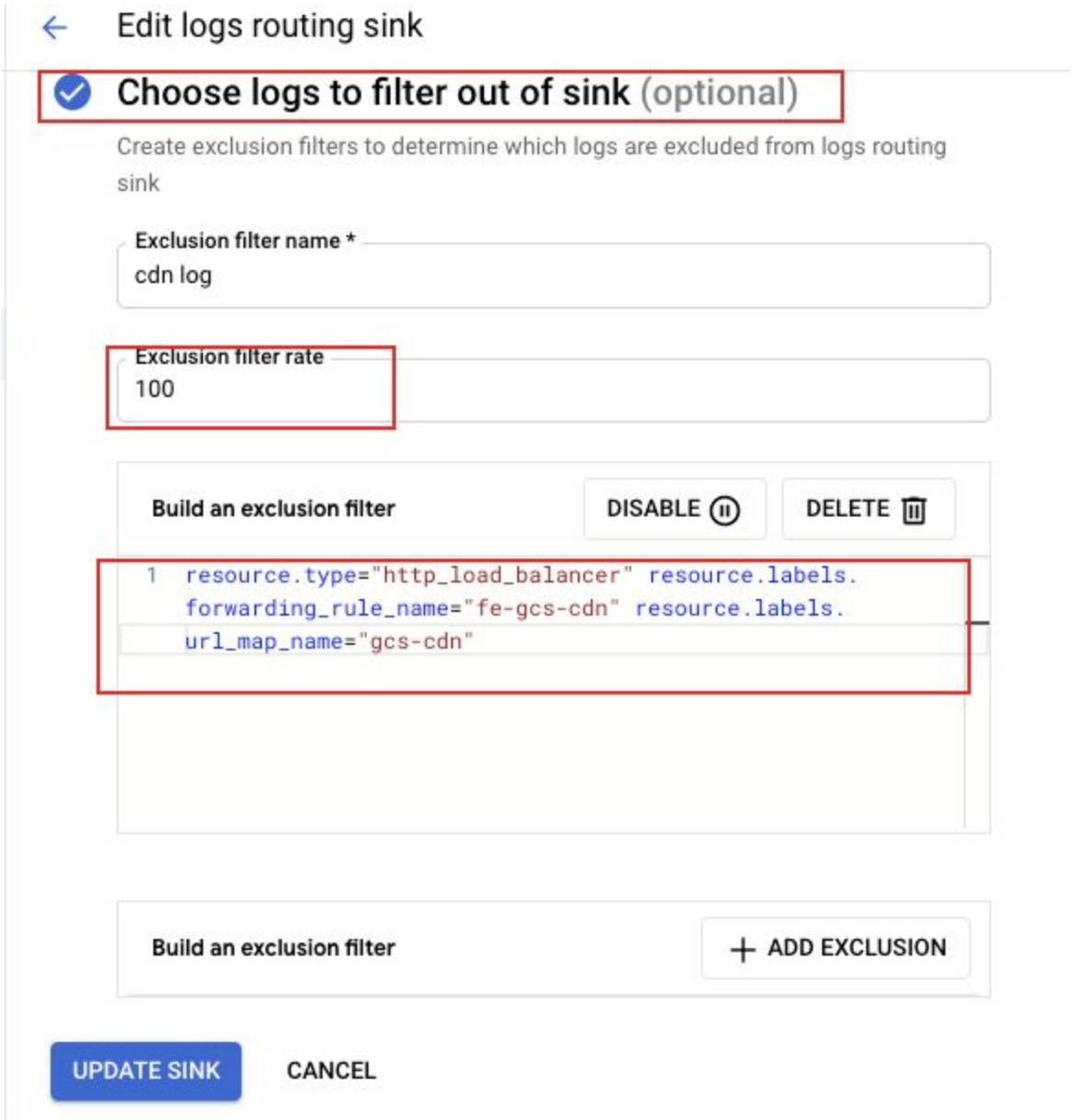


3.选择Biqquery Dataset, 注意保留这个日志的查询语言,后面需要用来创建exclusion



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
CREATE SINK
DELETE
Logs Router Sinks
Filter
Type
Name
Description
Destination
State
Cloud Logging bucket
_Default
logging.googleapis.com/projects/cliu101/locations/global/buckets/_Default
Enabled
Cloud Logging bucket
_Required
logging.googleapis.com/projects/cliu101/locations/global/buckets/_Required
BigQuery dataset
bigquery-audit
bigquery.googleapis.com/projects/cliu101/datasets/audit
BigQuery dataset
logs
bigquery.googleapis.com/projects/cliu101/datasets/coins
BigQuery dataset
MYSINK
bigquery.googleapis.com/projects/cliu101/datasets/billing
BigQuery dataset
test-logging-agent-json
bigquery.googleapis.com/projects/cliu101/datasets/coins
Enabled
BigQuery dataset
vpc-flow
bigquery.googleapis.com/projects/cliu101/datasets/wind
Enabled
View sink details
Edit sink
Disable sink
Delete sink


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