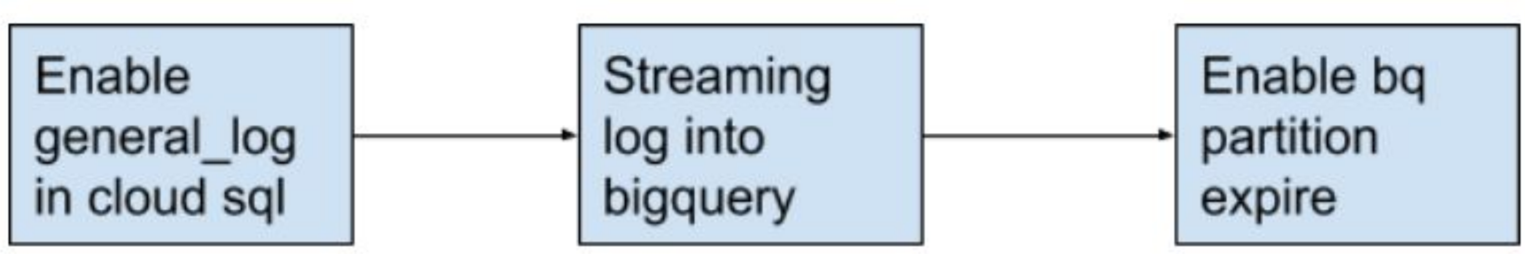
create audit log in cloud sql and monitor it efficiently

liuchenggang@google.com

基本配置流程



Enable general_log in cloud sql

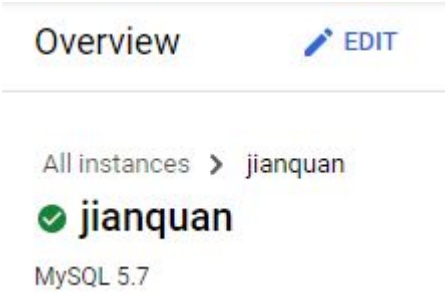
Streaming log into bigquery

Enable bq partition expire

本文档描述的是通过general_log, 查询一个登录数据库的例子

启用general_log

1.选择要配置的SQL，点击**Edit**;



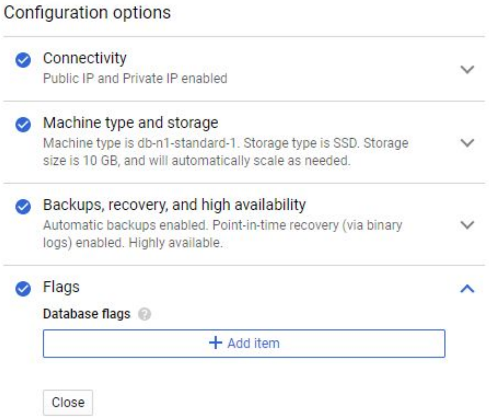
Overview

All instances > jianquan

jianquan

MySQL 5.7

2.选择**Configure Options**下的**Flags**;



Configuration options

Connectivity
Public IP and Private IP enabled

Machine type and storage
Machine type is db-n1-standard-1. Storage type is SSD. Storage size is 10 GB, and will automatically scale as needed.

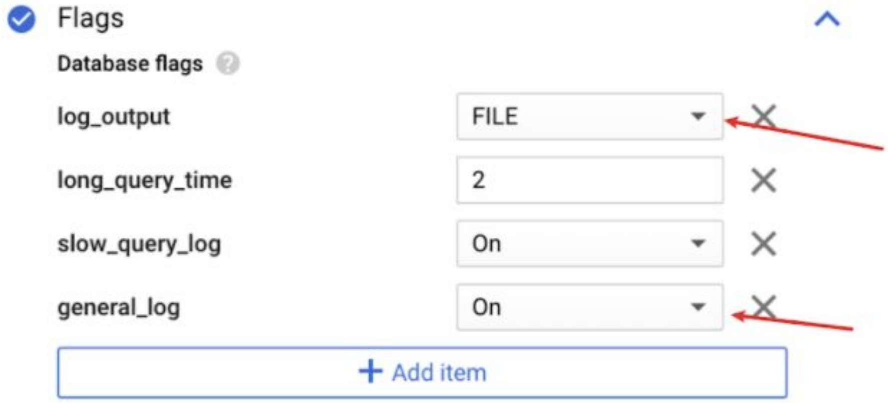
Backups, recovery, and high availability
Automatic backups enabled. Point-in-time recovery (via binary logs) enabled. Highly available.

Flags

Database flags

启用general_log

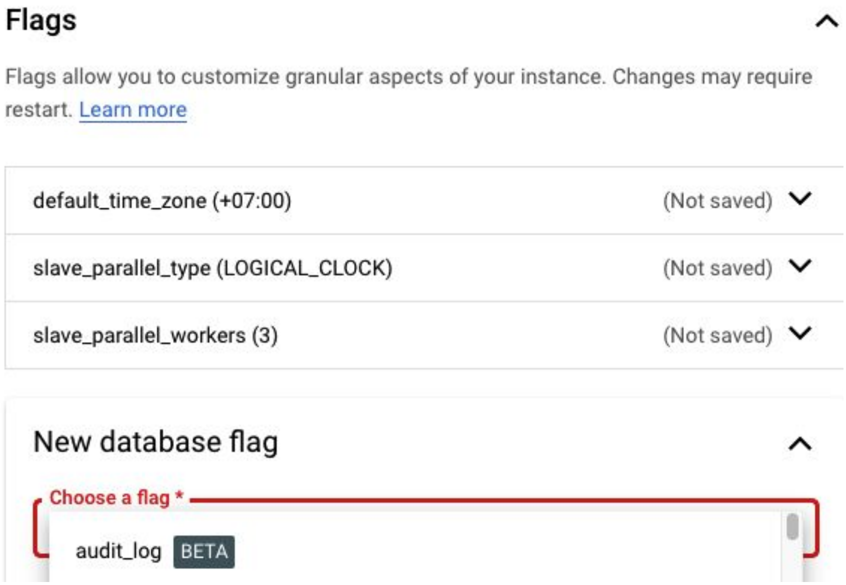
3.点击Add item,依次添加以下item;



Flags

Database flags

log_output	FILE
long_query_time	2
slow_query_log	On
general_log	On



Flags

Flags allow you to customize granular aspects of your instance. Changes may require restart. Learn more

default_time_zone (+07:00) (Not saved)

slave_parallel_type (LOGICAL_CLOCK) (Not saved)

slave_parallel_workers (3) (Not saved)

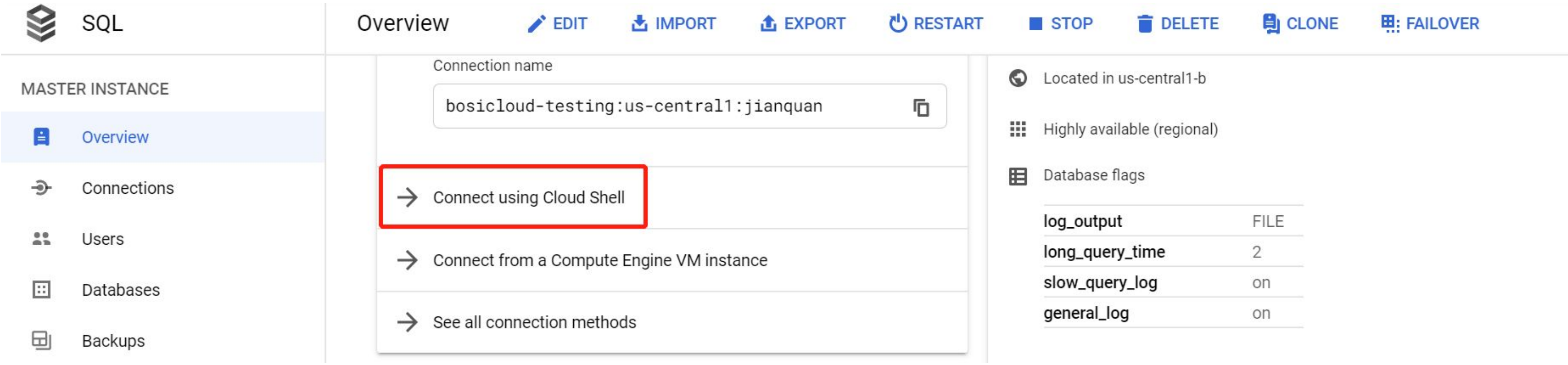
New database flag

Choose a flag *

audit_log BETA

登录数据库

1.切换到SQL的界面，选择Conect using Cloud shell,做一个登录数据库的操作动作；



Connection name

```
bosicloud-testing:us-central1:jianquan
```

Located in us-central1-b

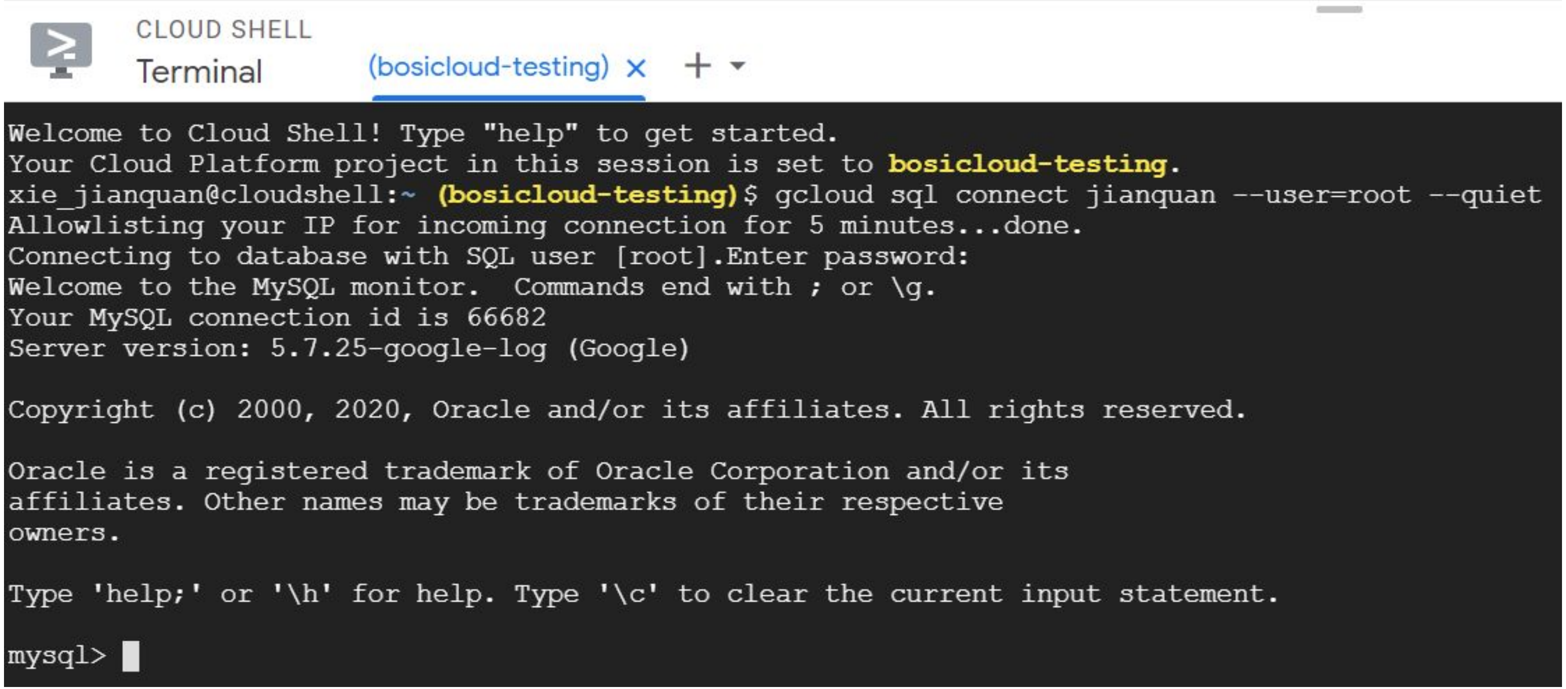
Highly available (regional)

Database flags

log_output	FILE
long_query_time	2
slow_query_log	on
general_log	on

登录数据库

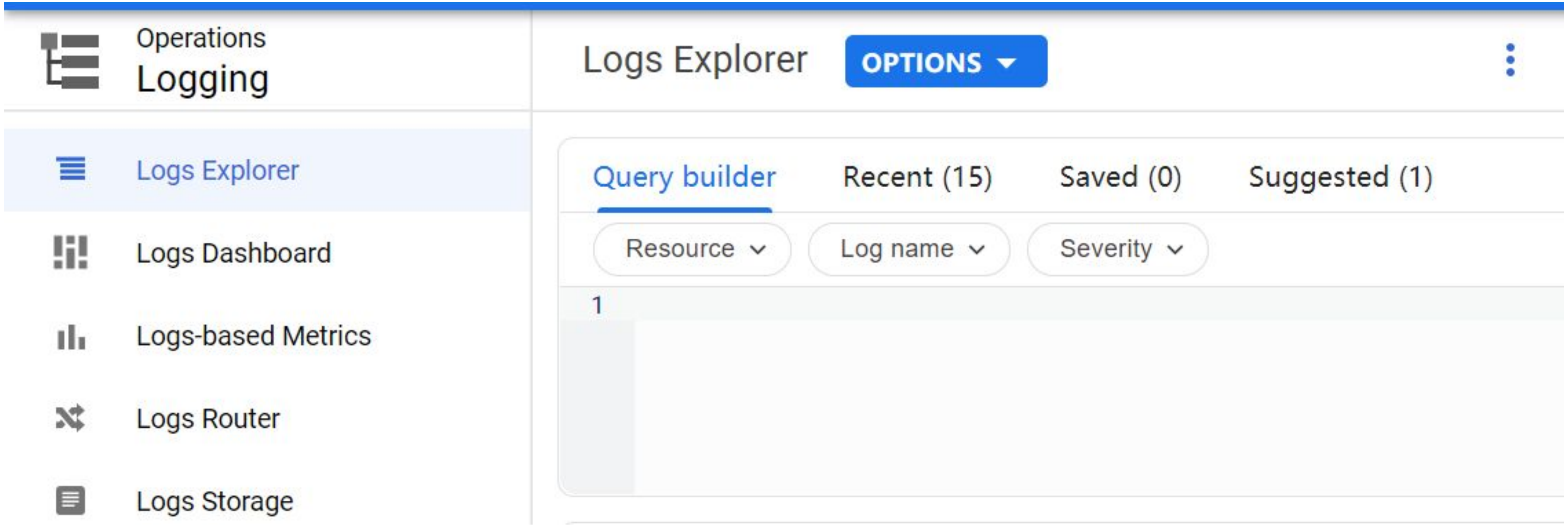
5.成功登录数据库;



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to bosicloud-testing.
xie_jianquan@cloudshell:~ (bosicloud-testing)$ gcloud sql connect jianquan --user=root --quiet
Allowlisting your IP for incoming connection for 5 minutes...done.
Connecting to database with SQL user [root].Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 66682
Server version: 5.7.25-google-log (Google)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

查询日志

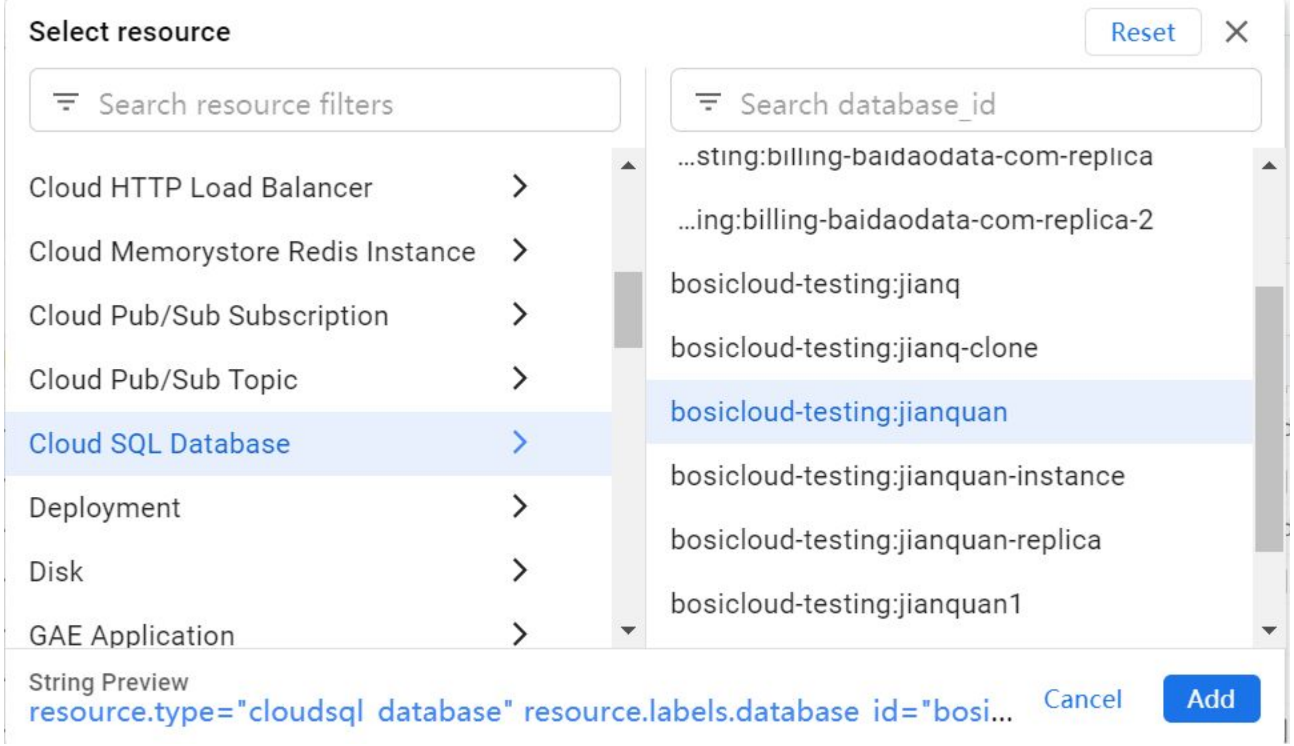
1.在导航切换到Operations,选择Logging.



查询日志

2.在Resource下选择Cloud SQL Database>项目名称:jianquan

3.点击Add.



Select resource

Search resource filters

Search database_id

Cloud HTTP Load Balancer

Cloud Memorystore Redis Instance

Cloud Pub/Sub Subscription

Cloud Pub/Sub Topic

Cloud SQL Database

Deployment

Disk

GAE Application

...sting:billing-baidaodata-com-replica

...ing:billing-baidaodata-com-replica-2

bosicloud-testing:jianq

bosicloud-testing:jianq-clone

bosicloud-testing:jianquan

bosicloud-testing:jianquan-instance

bosicloud-testing:jianquan-replica

bosicloud-testing:jianquan1

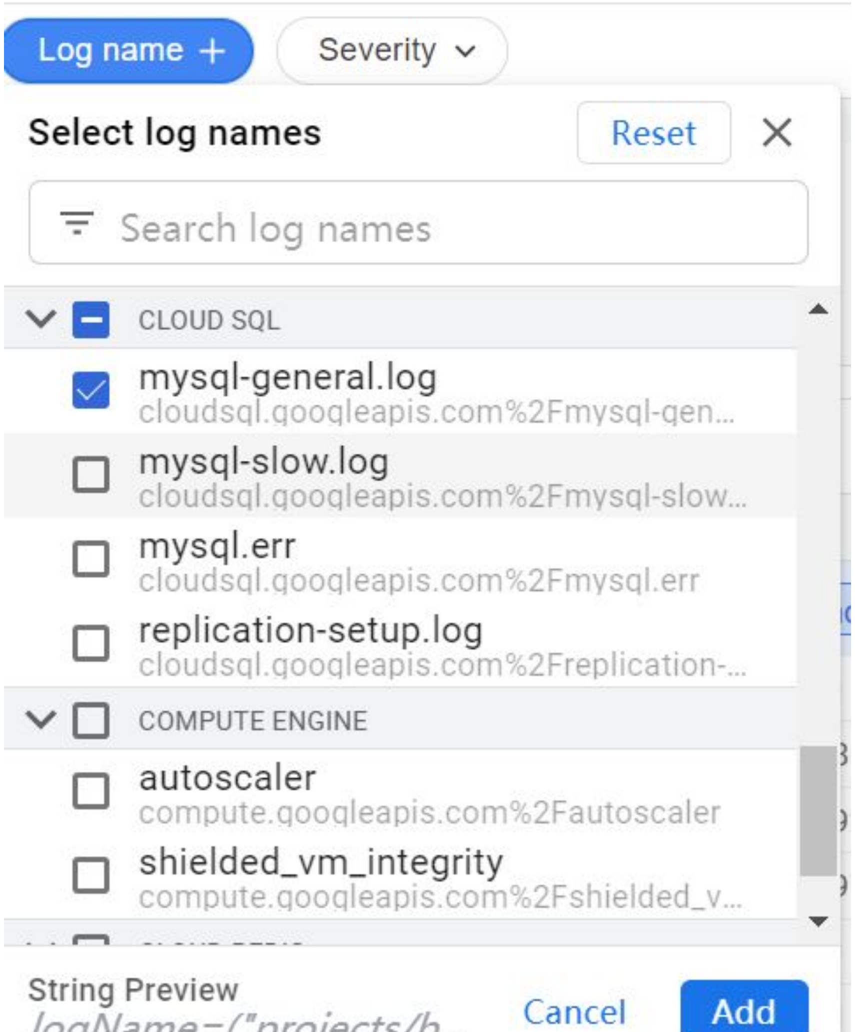
String Preview

resource.type="cloudsql_database" resource.labels.database_id="bosi...

查询日志

4.在log name下选择mysql-general.log.

5.点击Add.



CLOUD SQL

☑ mysql-general.log
cloudsql.googleapis.com%2Fmysql-gen...

□ mysql-slow.log
cloudsql.googleapis.com%2Fmysql-slow...

□ mysql.err
cloudsql.googleapis.com%2Fmysql.err

□ replication-setup.log
cloudsql.googleapis.com%2Freplication-...

□ COMPUTE ENGINE

□ autoscaler
compute.googleapis.com%2Fautoscaler

□ shielded_vm_integrity
compute.googleapis.com%2Fshielded_v...

String Preview
logName=("projects/b

查询日志

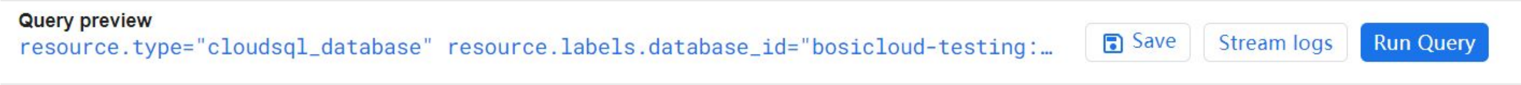
6.再在命令行上加多一行，一般根据你需要查询的事件来做过滤：textPayload =~ "root@35."

resource.type="cloudsql_database" resource.labels.database_id="bosicloud-testing:jianquan"

logName="projects/bosicloud-testing/logs/cloudsql.googleapis.com%2Fmysql-general.log"

textPayload =~ "root@35."

7.点击Run Query;

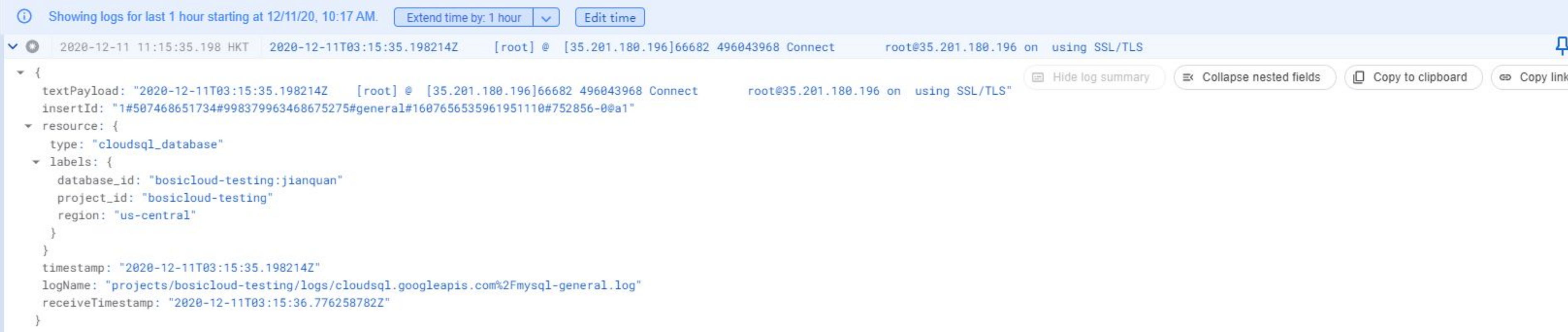


Query preview

```
resource.type="cloudsql_database" resource.labels.database_id="bosicloud-testing:…
```

查询日志

8.查看日志



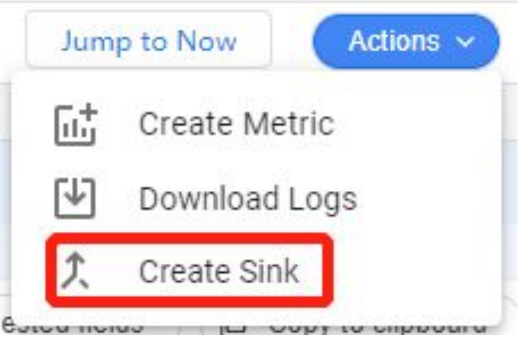
Showing logs for last 1 hour starting at 12/11/20, 10:17 AM.

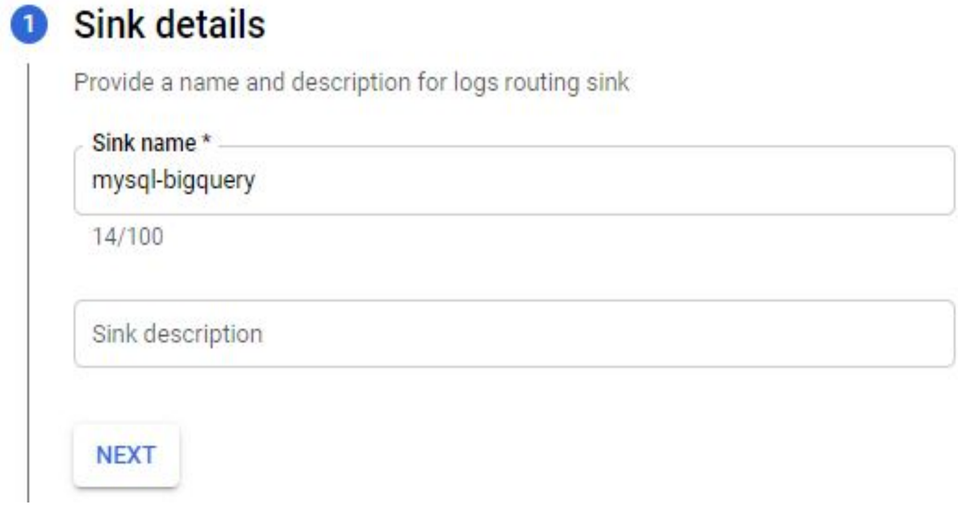
```
2020-12-11 11:15:35.198 HKT   2020-12-11T03:15:35.198214Z     [root] @  [35.201.180.196]66682 496043968 Connect       root@35.201.180.196 on  using SSL/TLS
{
  textPayload: "2020-12-11T03:15:35.198214Z     [root] @  [35.201.180.196]66682 496043968 Connect       root@35.201.180.196 on  using SSL/TLS"
  insertId: "1#507468651734#998379963468675275#general#1607656535961951110#752856-0@a1"
  resource: {
   type: "cloudsql_database"
   labels: {
    database_id: "bosicloud-testing:jianquan"
    project_id: "bosicloud-testing"
    region: "us-central"
   }
  }
  timestamp: "2020-12-11T03:15:35.198214Z"
  logName: "projects/bosicloud-testing/logs/cloudsql.googleapis.com%2Fmysql-general.log"
  receiveTimestamp: "2020-12-11T03:15:36.776258782Z"
}
```

导入到Bigquery

1.点击Actions,选择Create Sink;

2.填写名称后，点击Next;





1 Sink details

Provide a name and description for logs routing sink

Sink name *
mysql-bigquery
14/100

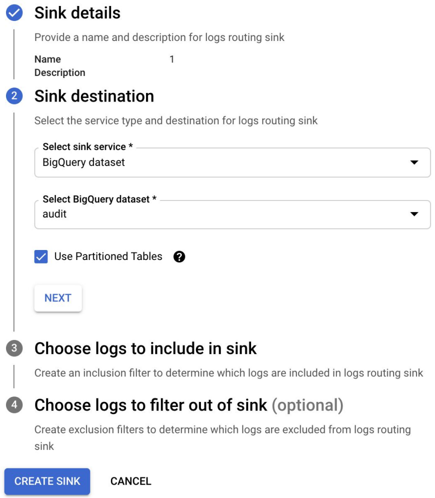
Sink description

导入到Bigquery

3.选择BigQuery dataset为Sink service;

4.选择创建新的BigQuery dataset(注意选择分区);

5.通过logs查询语句选定需要导出到bq的内容



Sink details

Provide a name and description for logs routing sink

Name 1

Description

Sink destination

Select the service type and destination for logs routing sink

Select sink service *
BigQuery dataset

Select BigQuery dataset *
audit

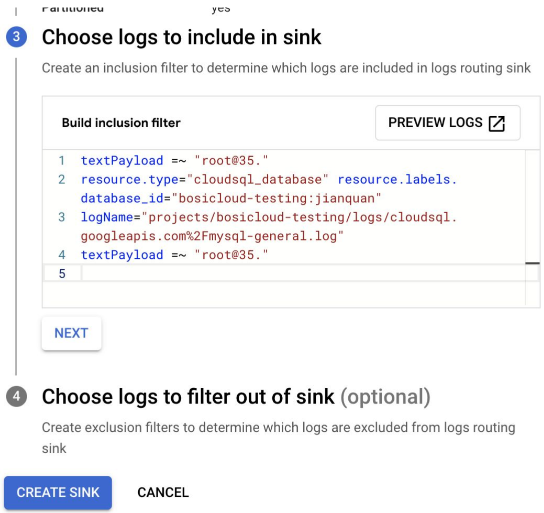
☑ Use Partitioned Tables

Choose logs to include in sink

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

Choose logs to filter out of sink (optional)

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



Partitioned yes

Choose logs to include in sink

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

Build inclusion filter

```
textPayload =~ "root@35."
resource.type="cloudsql_database" resource.labels.database_id="bosicloud-testing:jianquan"
logName="projects/bosicloud-testing/logs/cloudsql.googleapis.com%2Fmysql-general.log"
textPayload =~ "root@35."
```

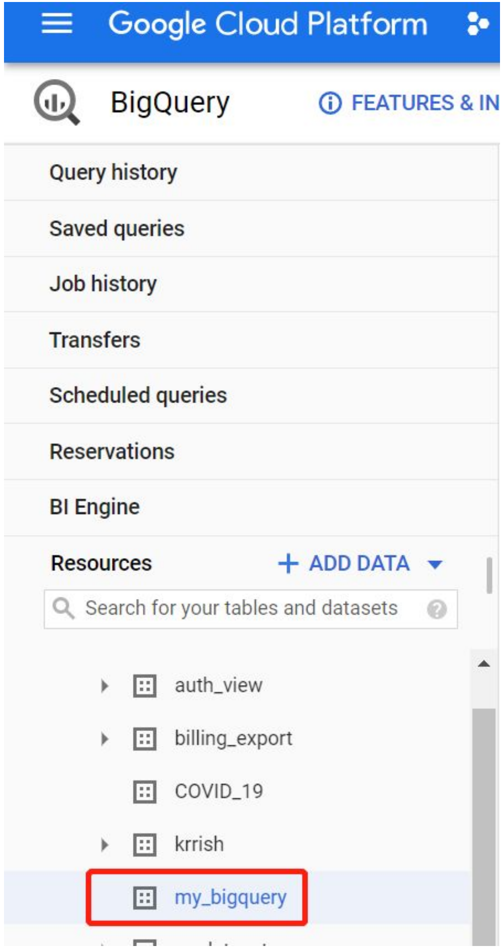
Choose logs to filter out of sink (optional)

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

导入到Bigquery

6.选择Next,选择Create SINK;

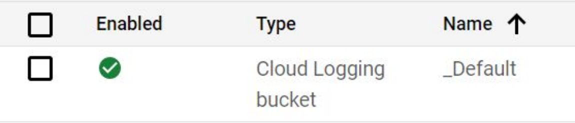
7.切换到BigQuery，查看dataset;



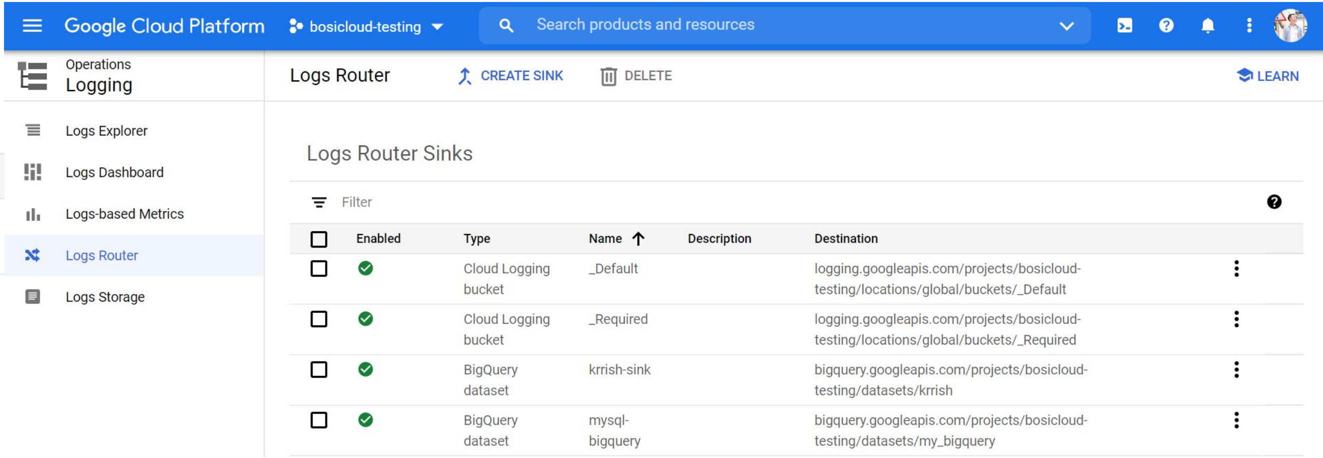
配置exclusion

1.在导航切换到Operations,选择Logging>log Router.

2.选择_Default



□	Enabled	Type	Name ↑
□	✓	Cloud Logging bucket	_Default

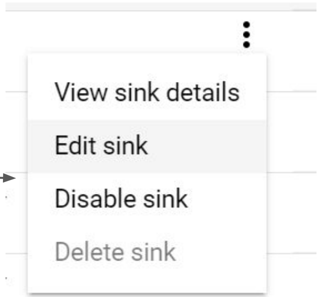


Logs Router Sinks

□	Enabled	Type	Name ↑	Description	Destination
□	✓	Cloud Logging bucket	_Default		logging.googleapis.com/projects/bosicloud-testing/locations/global/buckets/_Default
□	✓	Cloud Logging bucket	_Required		logging.googleapis.com/projects/bosicloud-testing/locations/global/buckets/_Required
□	✓	BigQuery dataset	krrish-sink		bigquery.googleapis.com/projects/bosicloud-testing/datasets/krrish
□	✓	BigQuery dataset	mysql-bigquery		bigquery.googleapis.com/projects/bosicloud-testing/datasets/my_bigquery

配置exclusion

3.选择Edit sink

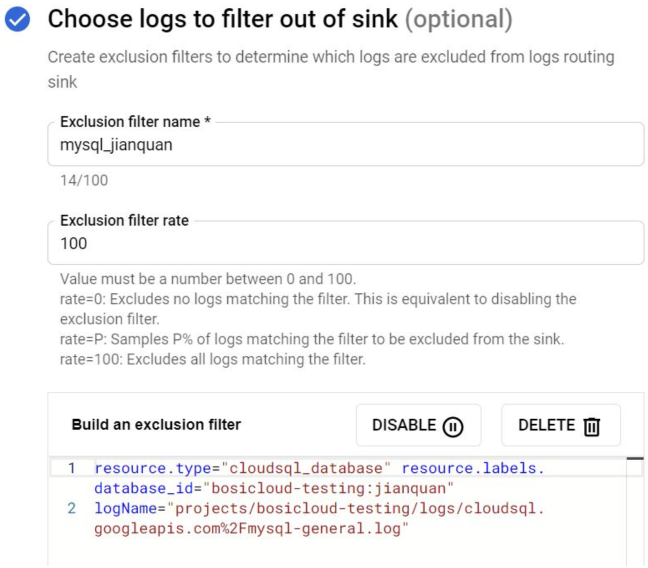


4.选择Choose logs to filter out of sink

主要填写以下三个重要信息：

- Exclusion filter rate:100　过滤100%的日志
- ENABLE，默认是DISABLE,需要点一下，启用过滤
- 输入需要过滤的SQL查询语句，可以从sink上查询到

5.点击UPDATE 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 * mysql_jianquan

14/100

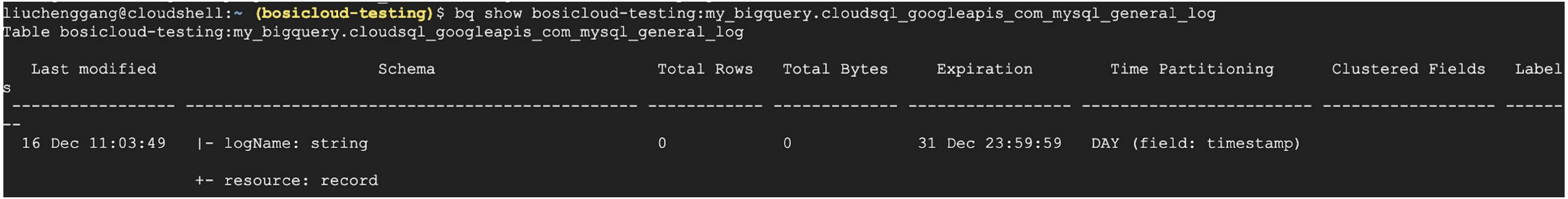
Exclusion filter rate 100

Value must be a number between 0 and 100.
rate=0: Excludes no logs matching the filter. This is equivalent to disabling the exclusion filter.
rate=P: Samples P% of logs matching the filter to be excluded from the sink.
rate=100: Excludes all logs matching the filter.

```
resource.type="cloudsql_database" resource.labels.database_id="bosicloud-testing:jianquan"
logName="projects/bosicloud-testing/logs/cloudsql.googleapis.com%2Fmysql-general.log"
```

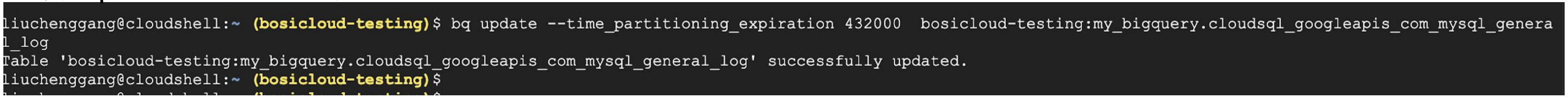
对导出的日志表做基于Partition的分区过期设置

默认的配置中没有基于 Partition的过期设置



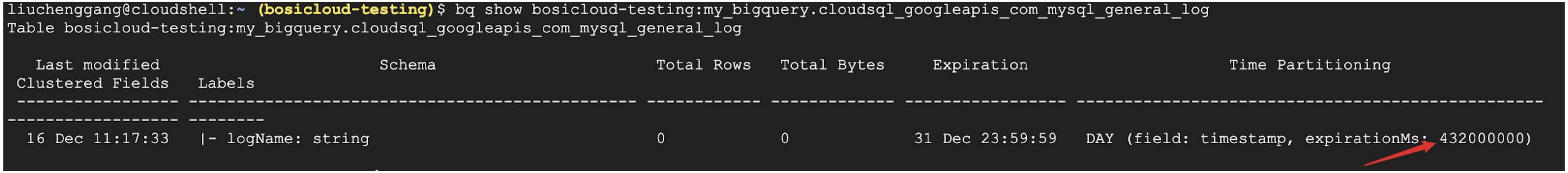
```
liuchenggang@cloudshell:~ (bosicloud-testing)$ bq show bosicloud-testing:my_bigquery.cloudsql_googleapis_com_mysql_general_log
Table bosicloud-testing:my_bigquery.cloudsql_googleapis_com_mysql_general_log

   Last modified                     Schema                      Total Rows   Total Bytes     Expiration        Time Partitioning      Clustered Fields   Label
s
 ----------------- ------------------------------------------------ ------------ ------------- ----------------- ------------------------ ------------------ ------
--
  16 Dec 11:03:49    |- logName: string                            0            0             31 Dec 23:59:59   DAY (field: timestamp)

                     +- resource: record
```

设置partition 过期时间为5天



```
liuchenggang@cloudshell:~ (bosicloud-testing)$ bq update --time_partitioning_expiration 432000  bosicloud-testing:my_bigquery.cloudsql_googleapis_com_mysql_genera
l_log
Table 'bosicloud-testing:my_bigquery.cloudsql_googleapis_com_mysql_general_log' successfully updated.
liuchenggang@cloudshell:~ (bosicloud-testing)$
```

确认设置生效



```
liuchenggang@cloudshell:~ (bosicloud-testing)$ bq show bosicloud-testing:my_bigquery.cloudsql_googleapis_com_mysql_general_log
Table bosicloud-testing:my_bigquery.cloudsql_googleapis_com_mysql_general_log

   Last modified                     Schema                      Total Rows   Total Bytes     Expiration                   Time Partitioning
 Clustered Fields   Labels
 ----------------- ------------------------------------------------ ------------ ------------- ----------------- ---------------------------------------------------
 ----------------- --------
  16 Dec 11:17:33    |- logName: string                            0            0             31 Dec 23:59:59   DAY (field: timestamp, expirationMs: 432000000)
```