

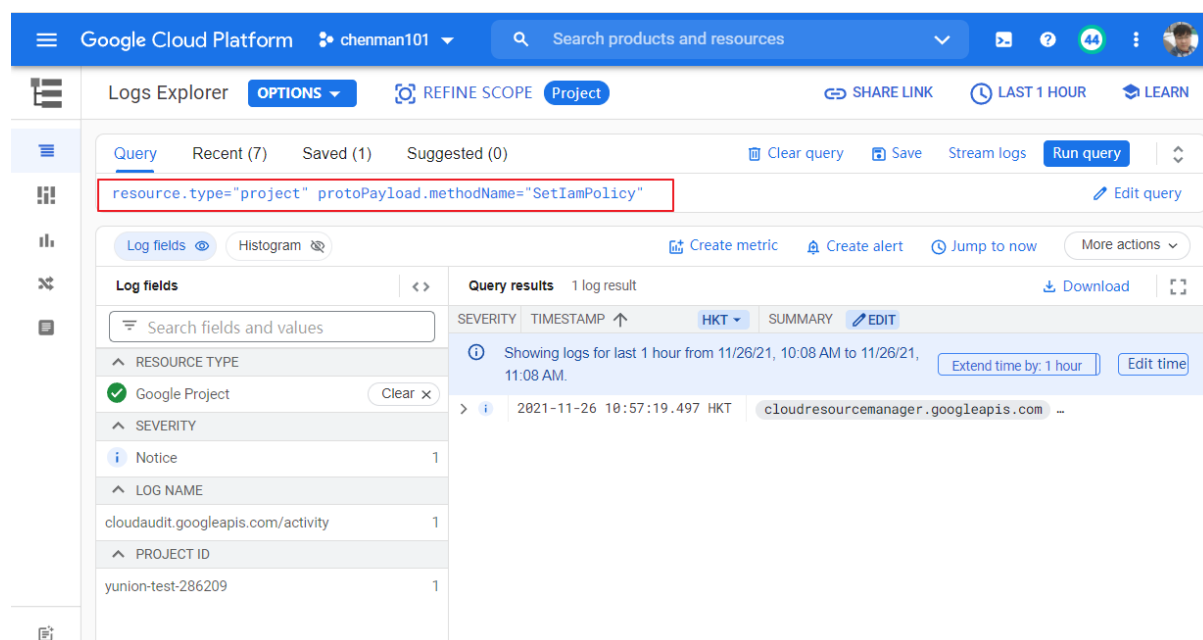
Cloud Logging 自定义日志告警通知

🕒 Created @November 26, 2021 11:06 AM

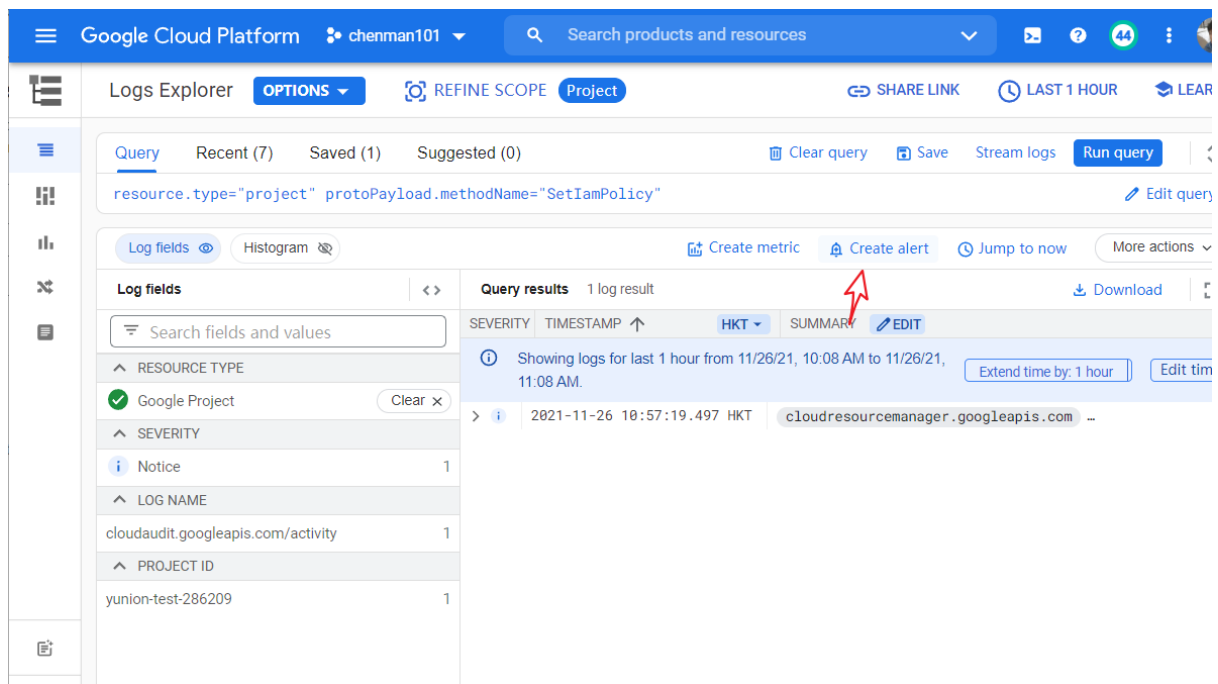
- 1、通过log query 在Logging explorer 中过滤所需的日志，以过滤项目权限更改为过滤条件，查询权限修改审计日志。
- 2、通过上面的Query 查询，然后基于log query创建项目层级的权限变更 log alert：
- 3、设置 log alert policy name:
- 4、配置log filter：
- 5、配置通知频率与自动关闭
- 6、设置通知方式：
- 7、在Cloud monitoring 中查看日志告警策略：

通过创建项目级别的修改IAM 策略的日志告警通知，实现观测项目权限变化。

1、通过log query 在Logging explorer 中过滤所需的日志，以过滤项目权限更改为过滤条件，查询权限修改审计日志。



2、通过上面的Query 查询，然后基于log query创建项目层级的权限变更 log alert：



3、设置 log alert policy name:

1 Alert details

Provide a name and description for this log alert.

Alert Name

IAM Change

11/512 characters

Alert Description

Include instructions or suggestions for solving the problem.

Your alert policies may trigger messages that include personal data. Please use appropriate communication channels for these alerts and confirm that the alert recipients are authorized to receive such data.

Optional

[Documentation](#)

Set iam Policy

Markdown preview

Set iam Policy

4、配置log filter：

```
resource.type="project"
protoPayload.methodName="SetIamPolicy"
```

✓ Alert details

Provide a name and description for this log alert.

Name	IAM Change
Description	Set iam Policy

2 Choose logs to include in the alert

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

i Alert will be scoped to logs generated by the following project:
projects/yunion-test-286209

Define log entries to alert on **?**

[PREVIEW LOGS](#)

```
resource.type="project"
protoPayload.methodName="SetIamPolicy"
```

[NEXT](#)

5、配置通知频率与自动关闭

3 Set notification frequency and auto-close

Configure the minimum amount of time between receiving notifications for logs that match this filter, and the delay to auto-close corresponding incidents.

Time between notifications *

5 min

通知间隔



Auto-close delay *

15 min



[NEXT](#)

6、设置通知方式：

4 Who should be notified? (optional)

When alerting policy violations occur, you will be notified via these channels.

Notification Channels

Filter Type to filter

Google Cloud Console (mobile)

☐ (voice scope)

SMS

☒ (selected)

Web

☐ (selected)

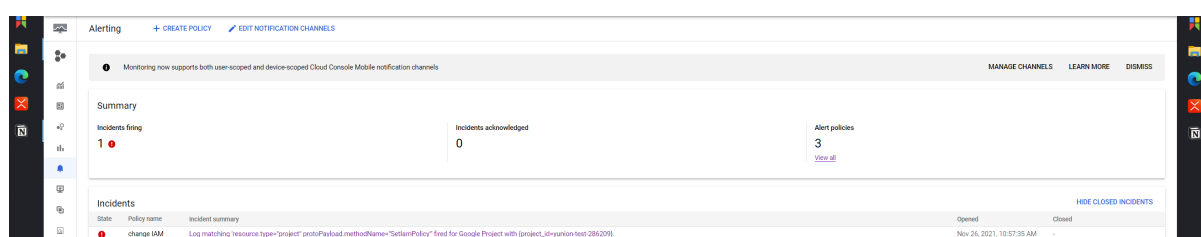
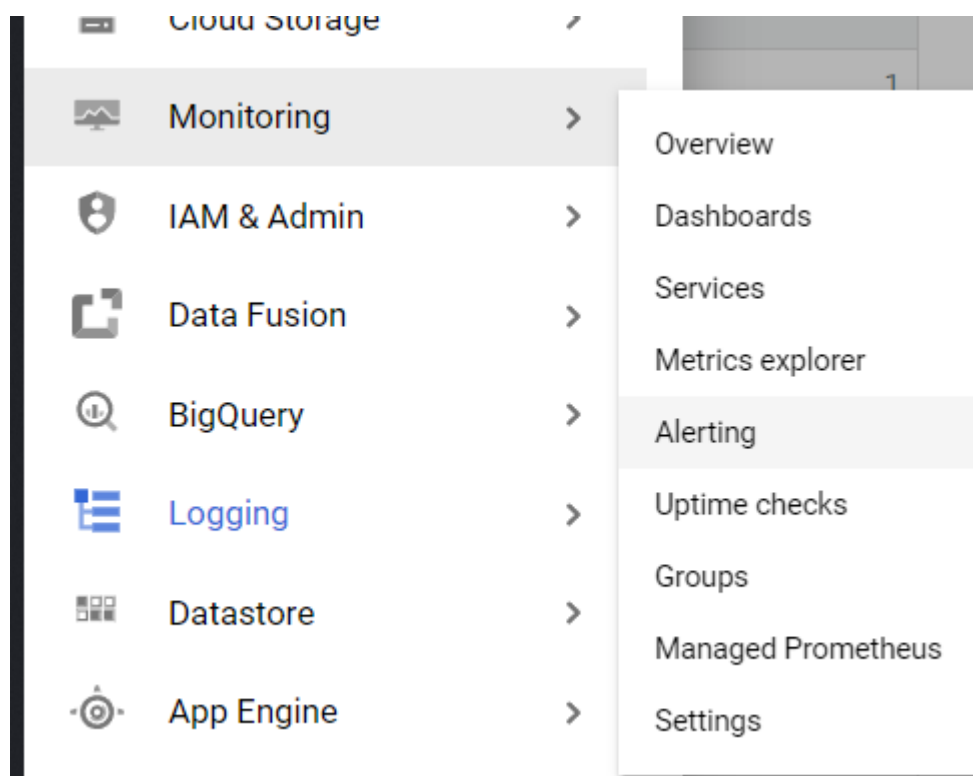
Email

☐ (selected)

MANAGE NOTIFICATION CHANNELS

CANCEL OK

7、在Cloud monitoring 中查看日志告警策略：



查看详细的告警策略：

change IAM

Conditions

Policy violates when ANY condition is met

Configurations

Log query

resource.type="project" protoPayload.methodName="SetIamPolicy"

Notification rate limit

One notification per 5 minutes

Auto close delay

15 minutes

Logs Severity Default Filter Filter logs

Loading...

Incidents

State	Policy name	Incident summary	Opened	Closed
🔴	change IAM	Log matching 'resource.type="project" protoPayload.methodName="SetIamPolicy"' fired for Google Project with (project_id=yunion-test-286209).	Nov 26, 2021, 10:57:35 AM	-