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：

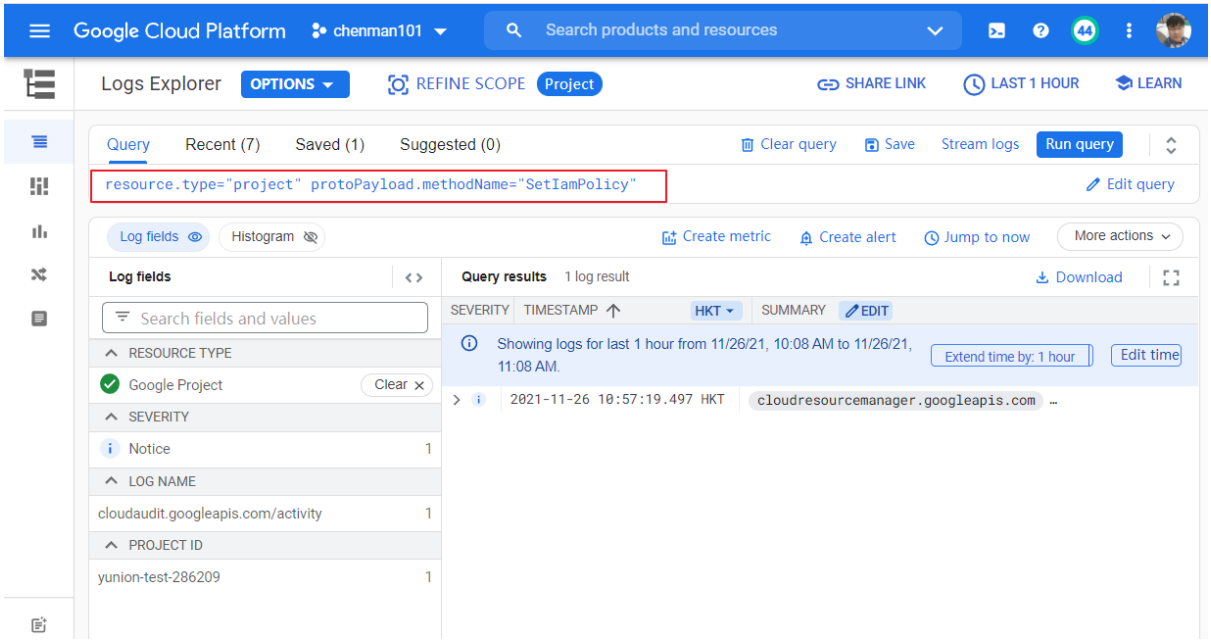
5、配置通知频率与自动关闭

6、设置通知方式：

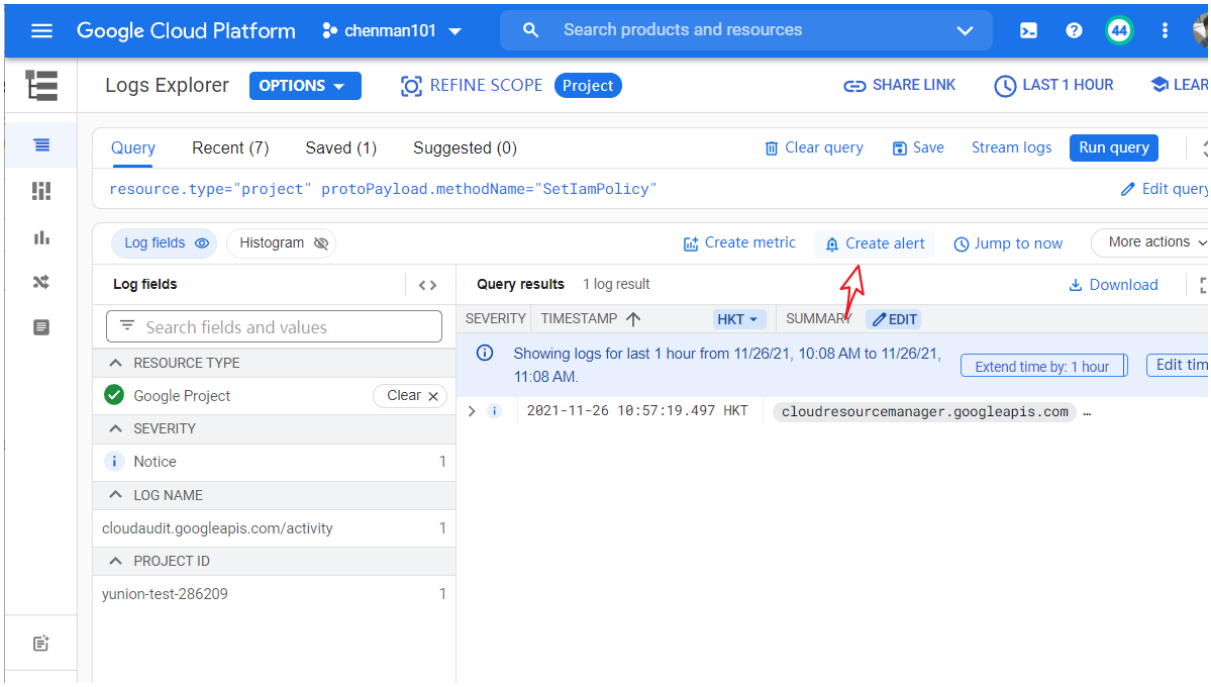
7、在Cloud monitoring 中查看日志告警策略：

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。

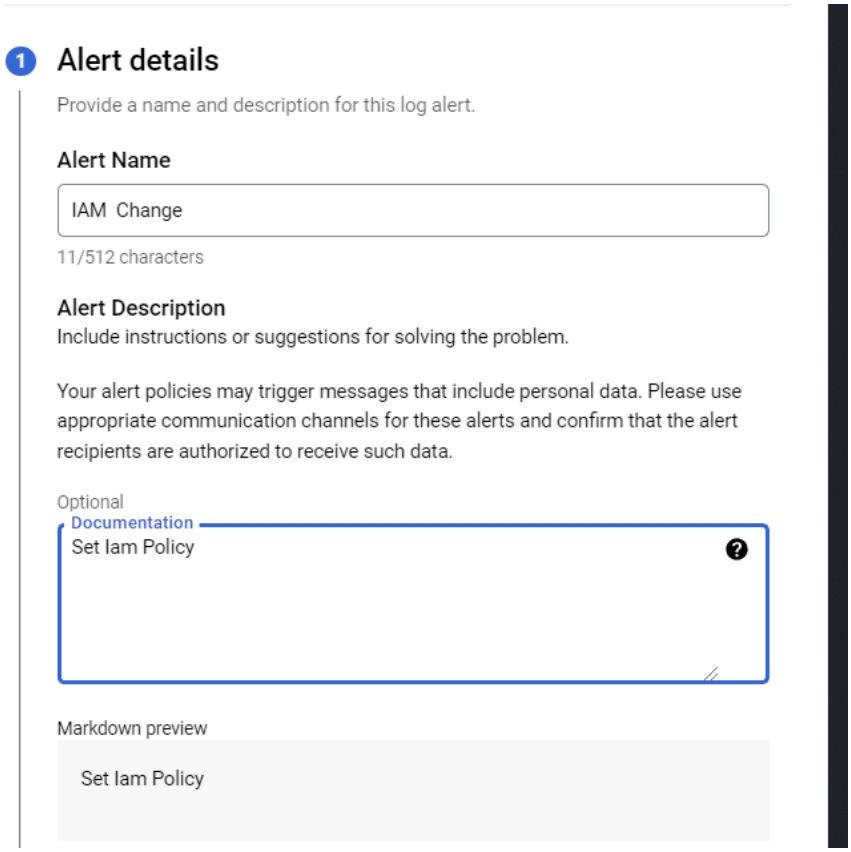
1、通过log query 在Logging explorer 中过滤所需的日志，以过滤项目权限更改为过滤条件，查询权限修改审计日志。



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：

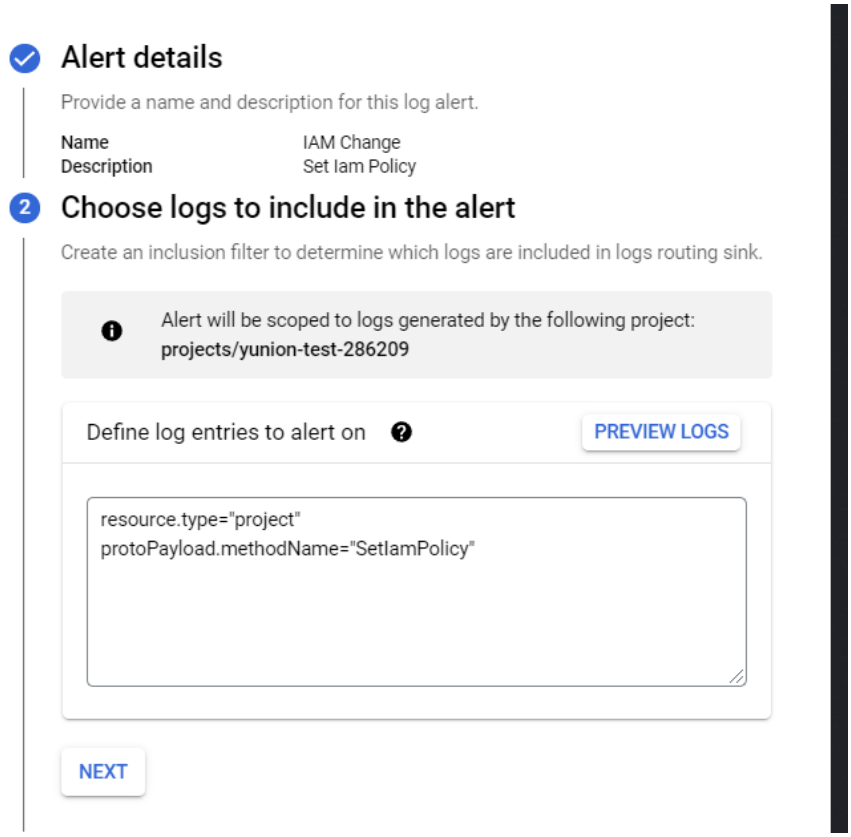


3、设置 log alert policy name:

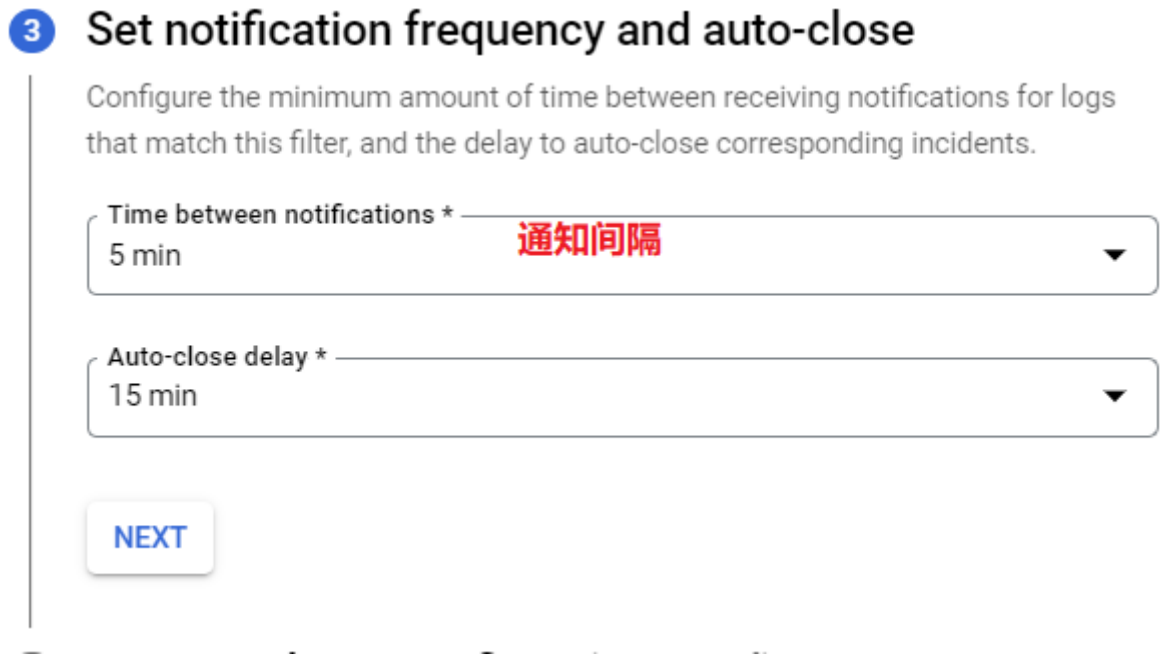


4、配置log filter：

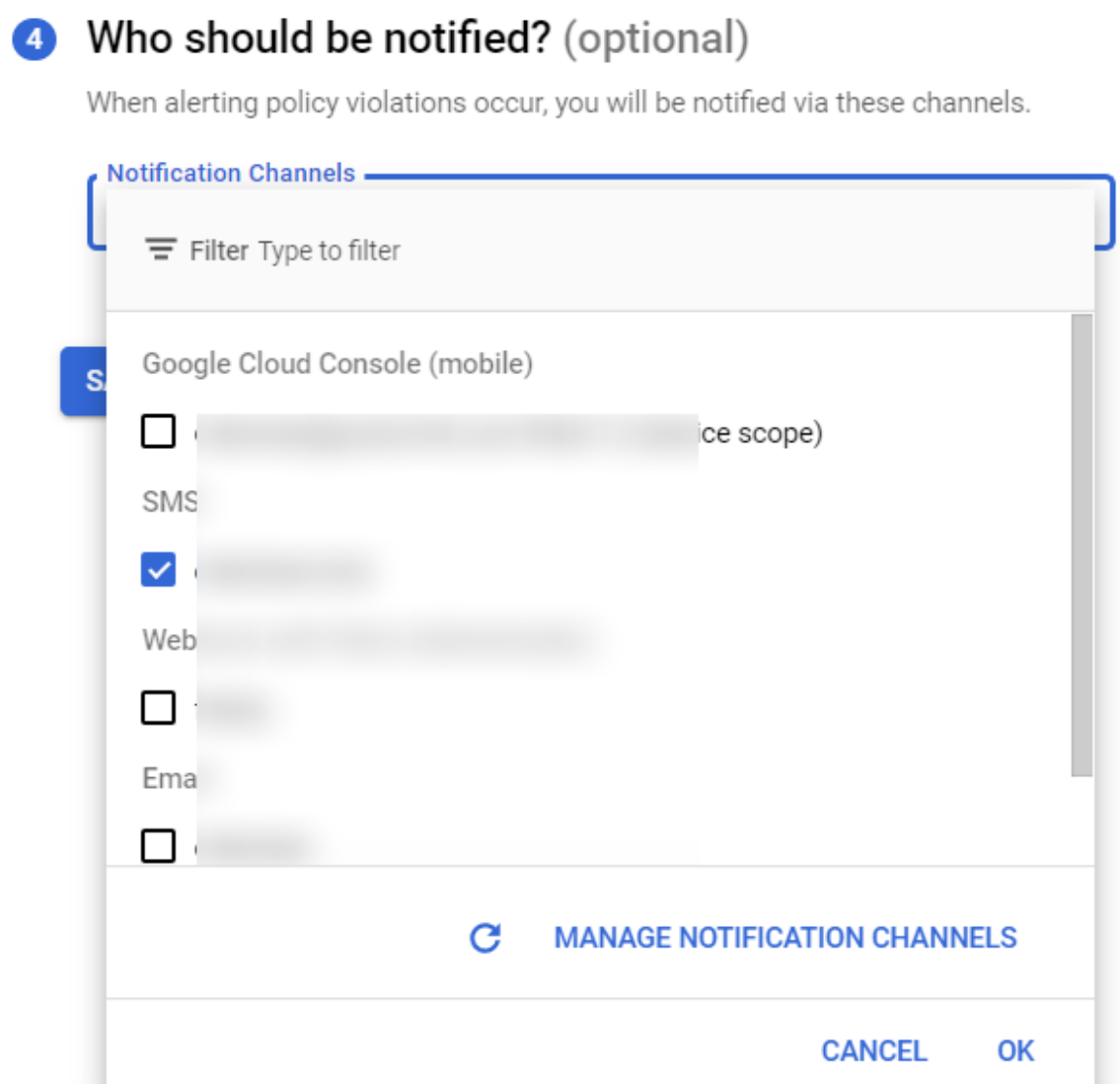
```
resource.type="project"
protoPayload.methodName="SetIamPolicy"
```



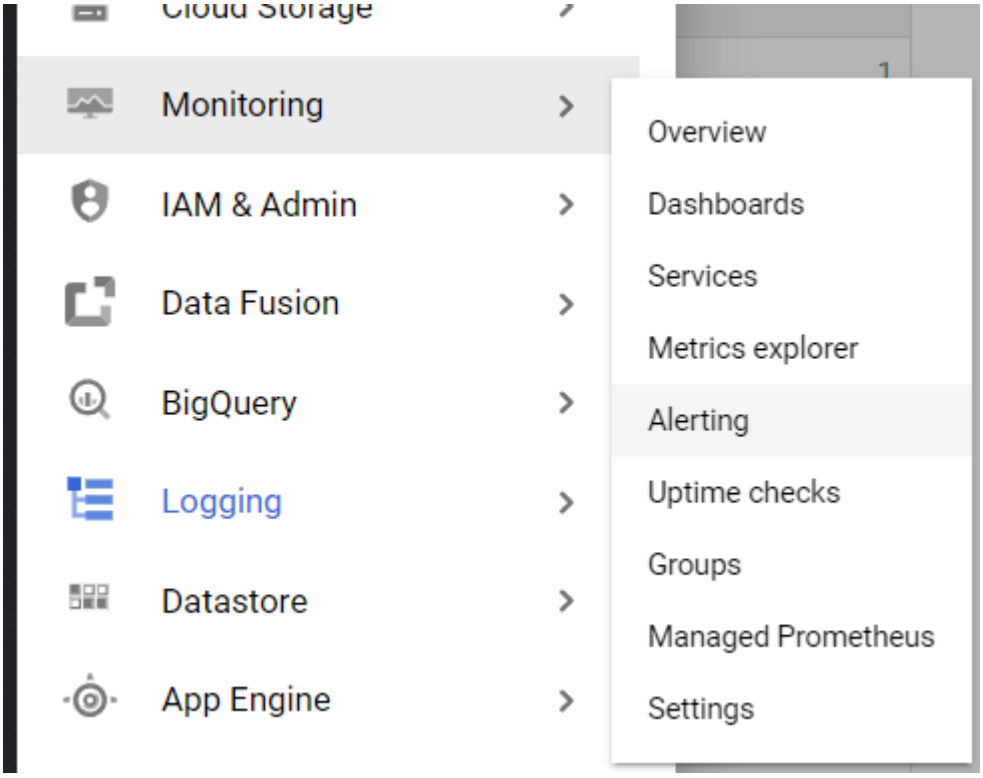
5、配置通知频率与自动关闭

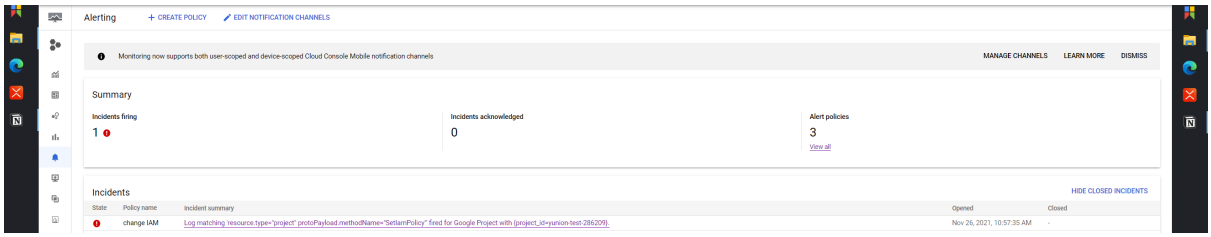


6、设置通知方式：

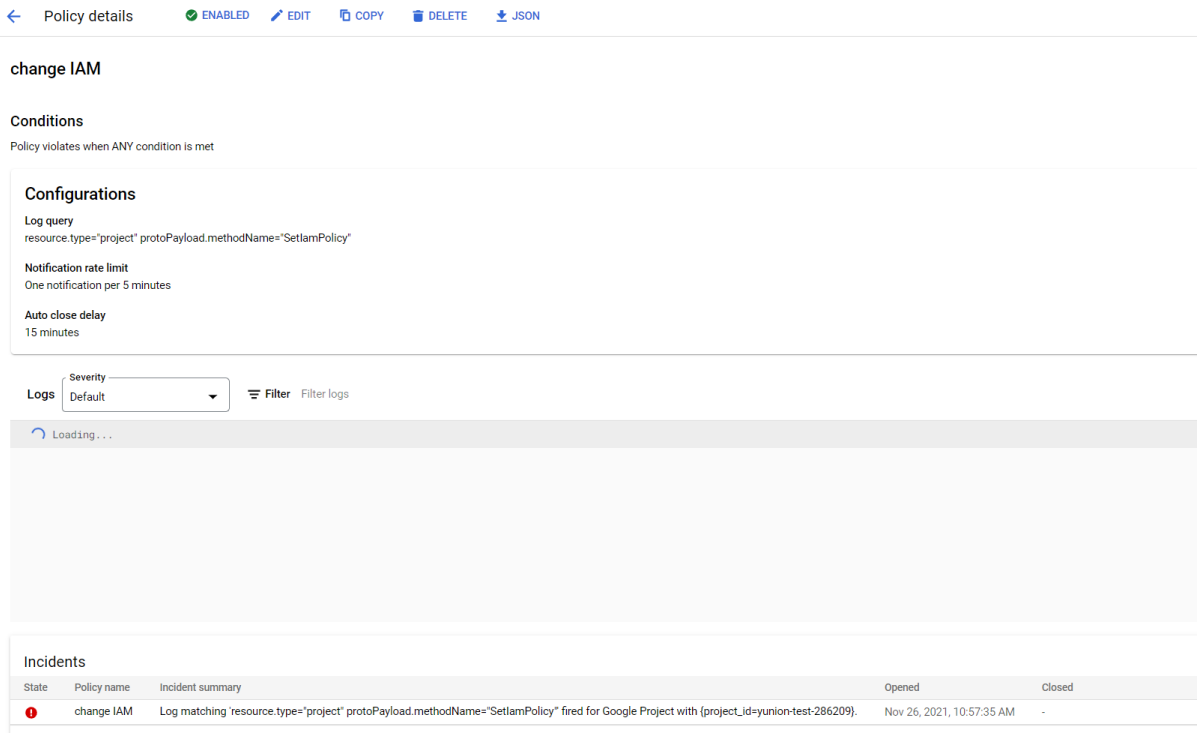


7、在Cloud monitoring 中查看日志告警策略：


Cloud Storage
Monitoring
IAM & Admin
Data Fusion
BigQuery
Logging
Datastore
App Engine
Overview
Dashboards
Services
Metrics explorer
Alerting
Uptime checks
Groups
Managed Prometheus
Settings


Alerting
+ CREATE POLICY
EDIT NOTIFICATION CHANNELS
Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels
MANAGE CHANNELS
LEARN MORE
DISMISS
Summary
Incidents firing
1
Incidents acknowledged
0
Alert policies
3
View all
Incidents
HIDE CLOSED 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=union-test-286209}.
Nov 26, 2021, 10:57:35 AM

查看详细的告警策略：


Policy details
ENABLED
EDIT
COPY
DELETE
JSON
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
-