**1.配置 IAP 隧道以与实例进行交互**

**创建虚拟机实例**

1. 在 Cloud Console 中，转到“虚拟机实例”页面：  
   [转到“虚拟机实例”页面](https://console.cloud.google.com/compute/instances?_ga=2.156050872.224621225.1609728609-1662347980.1605488090)
2. 点击**创建实例**。
3. 将**名称**设置为 www-1。
4. 将**地区**设置为 **us-central1-b**。
5. 点击**管理、安全、磁盘、网络、单独租用**。
6. 点击**网络**并进行以下设置：
   * 在**外部 IP** 下，选择**无**。
   * Network tags 输入 iap-tag
7. 点击**创建**。

**创建防火墙规则以允许开通隧道**

1. 在 Cloud Console 中，转到**防火墙**页面：  
   [转到“防火墙”页面](https://console.cloud.google.com/networking/firewalls/list)
2. 点击**创建防火墙规则**。
3. 将**名称**设置为 allow-ssh-from-iap。
4. 将 **VPC 网络**保留为 default。
5. 在**目标**下，选择**指定的目标标记**。
6. 将**目标标记**设置为 iap-tag。
7. 将**来源过滤条件**设置为 **IP 范围**。
8. 将**来源 IP 地址范围**设置为 35.235.240.0/20。
9. 将**允许的协议和端口**设置为 tcp:22。
10. 点击**创建**。

**测试隧道**

在 Cloud Shell 中，使用 IAP 连接到实例 www-1：

gcloud compute ssh www-1 \

    --zone us-central1-b \

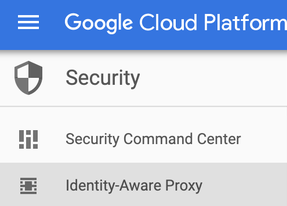
External IP address was not found; defaulting to using IAP tunneling.

    -

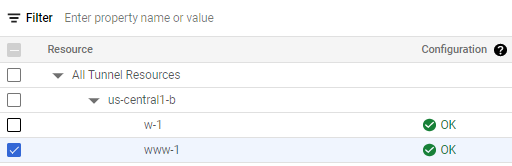
如果连接成功，将具有一个通过 IAP 隧道直接传送到专用虚拟机的 SSH 会话。

**向其他用户授予访问权限**

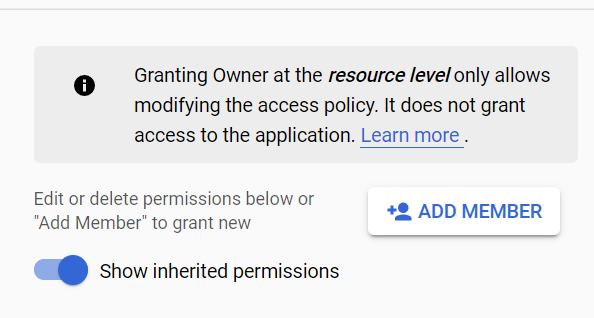
1. 在 Cloud Console 中，转到**安全性** > **Identity-Aware Proxy**：



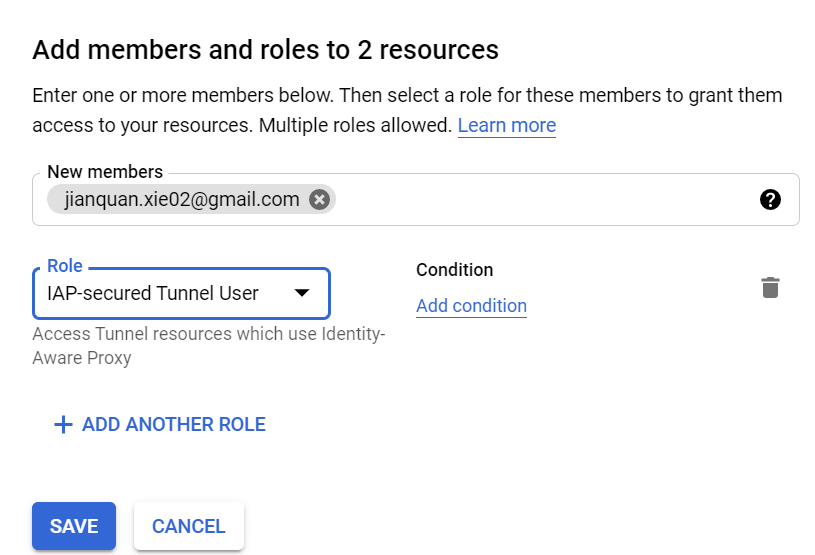
1. 选择 SSH 和 TCP 资源标签页。
2. 选择已创建的虚拟机：



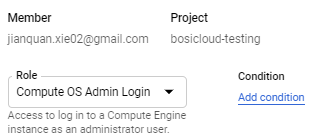
1. 在右侧，点击**添加成员**。



1. 添加要向其授予权限的用户，选择 **IAP-secured Tunnel User** 角色，然后点击**保存**：



6 在 Cloud Console 中，转到IAM,选择用户，增加以下角色：



使用在 Cloud Shell 中，使用 IAP 连接到实例 www-1：

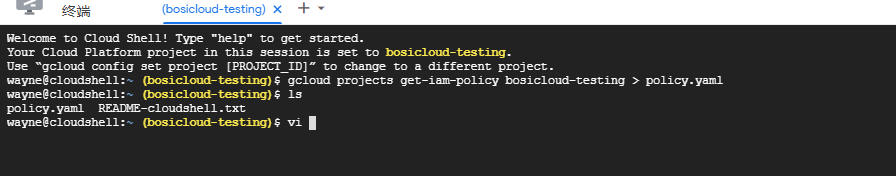
gcloud compute ssh www-1 \

    --zone us-central1-b \

**2.配置日志**

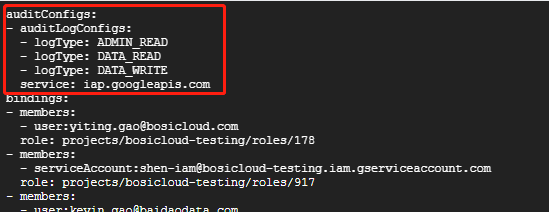
1. 下载项目的身份和访问权限管理 (IAM) 政策设置

gcloud projects get-iam-policy bosicloud-testing > policy.yaml



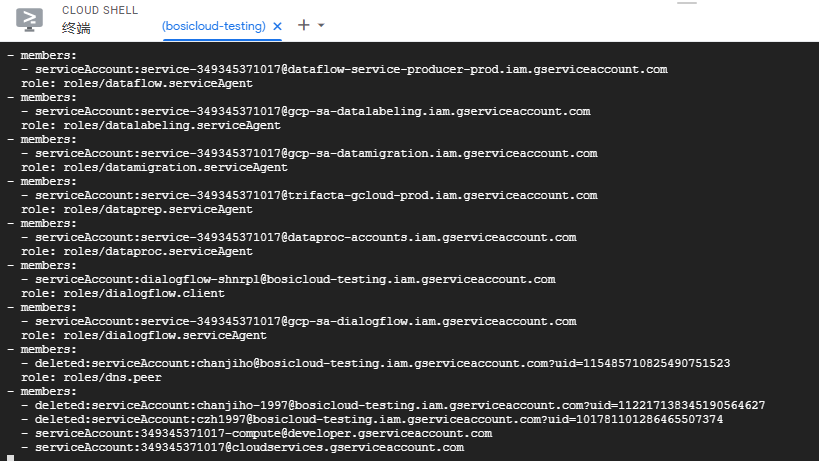
bosicloud-testing是project名称

2.修改 policy.yaml文件，如下红框部分



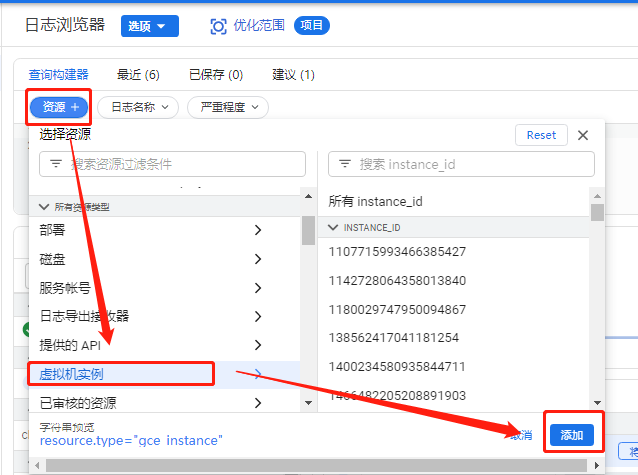
1. 更新 IAM 政策设置

gcloud projects set-iam-policy bosicloud-testing policy.yaml

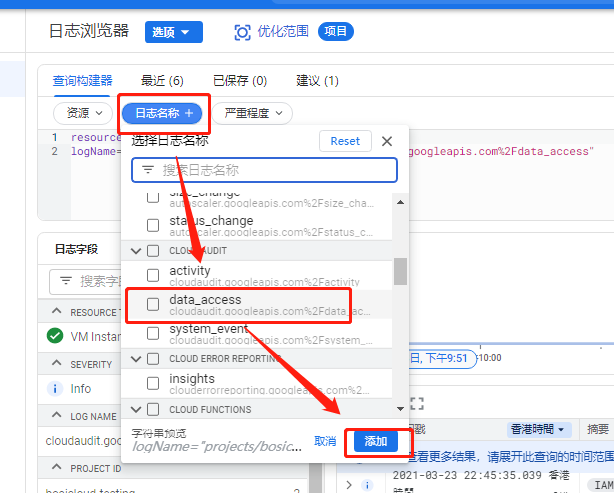


1. 查看 Cloud Audit Logs 日志

资源选择器下拉列表中，选择GCE 虚拟机实例。



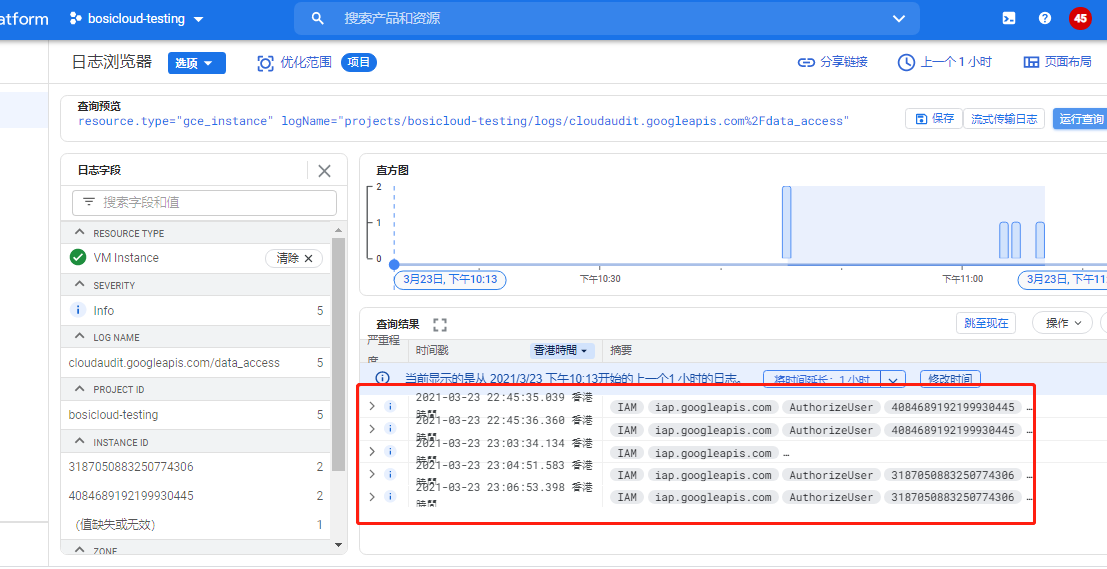
在日志类型下拉列表中，选择 data\_access



点击以展开要查看的访问所对应的日期和时间。

已获授权的访问带有一个蓝色 i 图标。

未经授权的访问带有一个橙色 !! 图标。

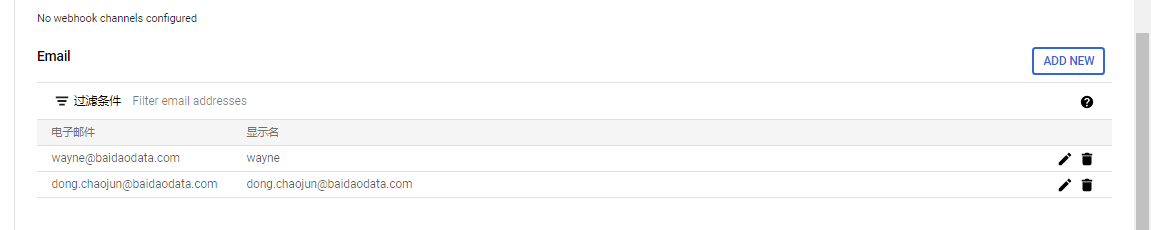


**3.创建告警**

1. 创建指标







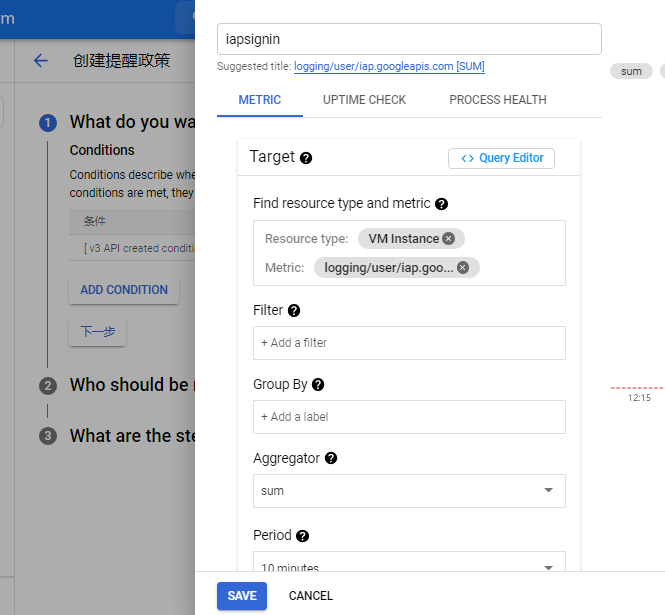
过滤条件

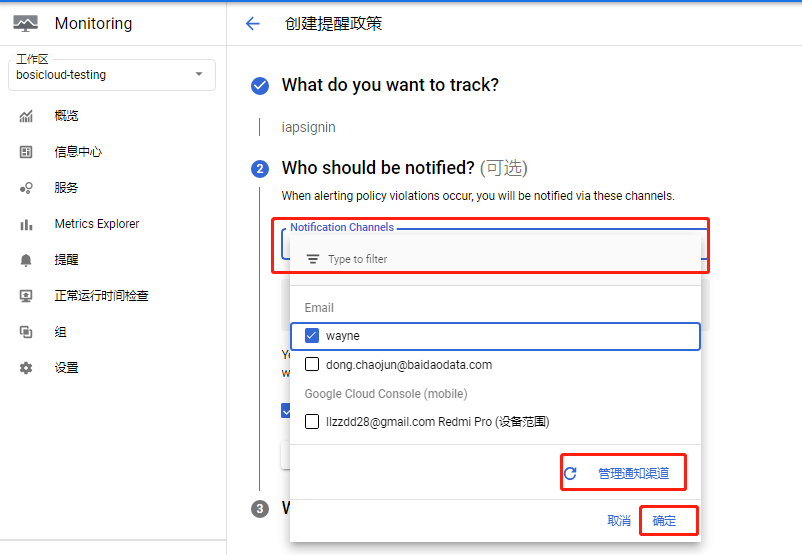
resource.type="gce\_instance" resource.labels.instance\_id="4084689192199930445"

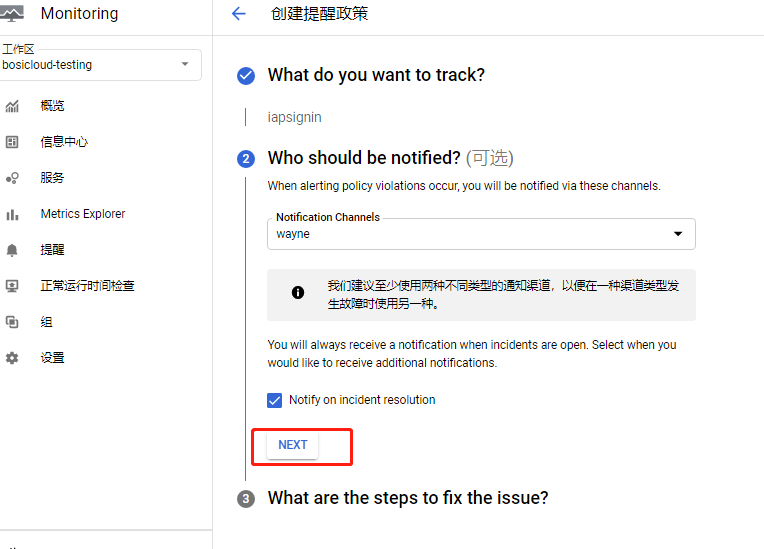
logName="projects/bosicloud-testing/logs/cloudaudit.googleapis.com%2Fdata\_access"

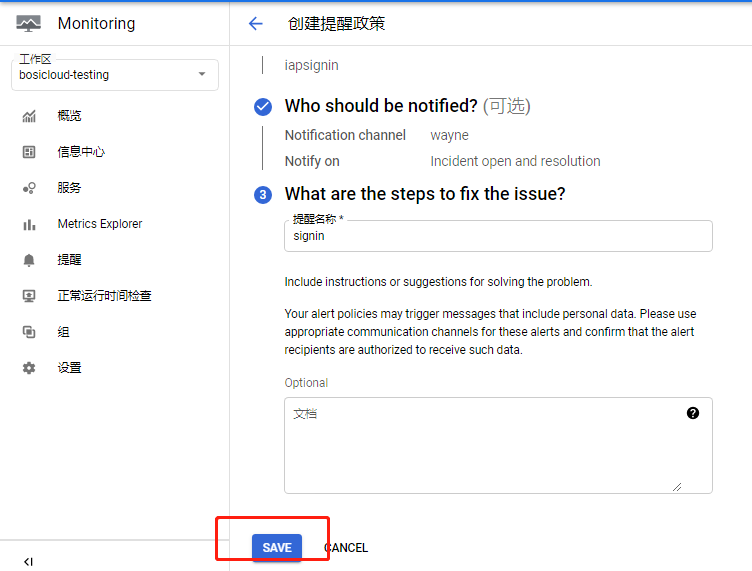
1. 创建告警



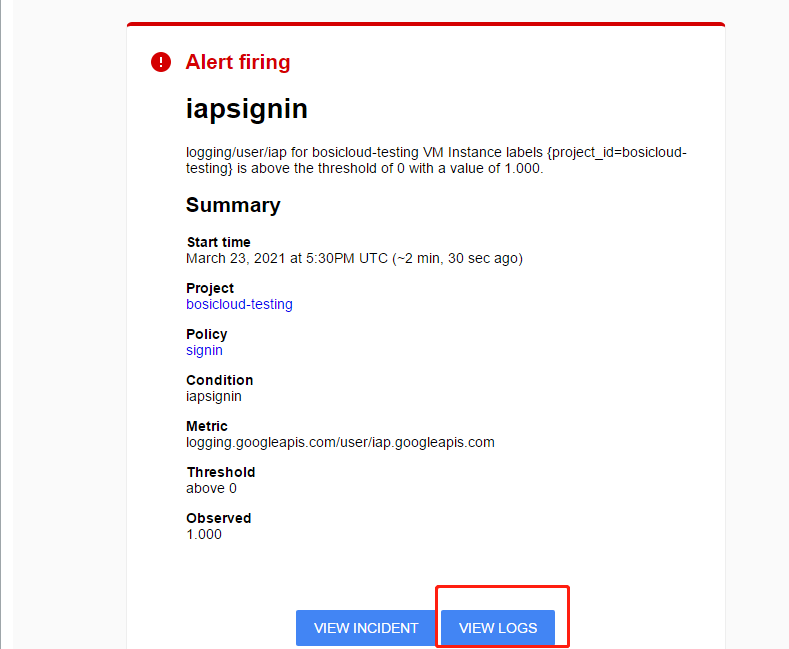








会收到邮件



点击“view logs”可查看详情

