<https://cyberdefenders.org/blueteam-ctf-challenges/googlecloudhunt/>

We need to determine if a user has fallen victim to the credential breach, which user account was compromised?

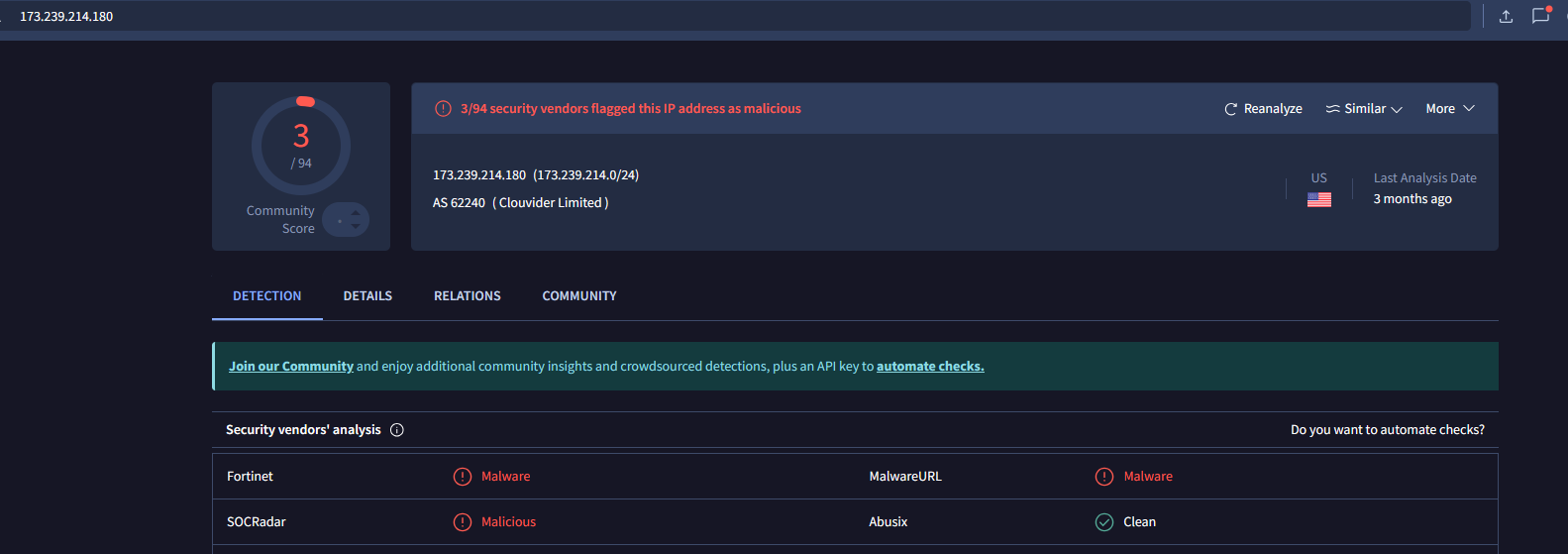
Firstly, we need to have a look at the data so we can define our query

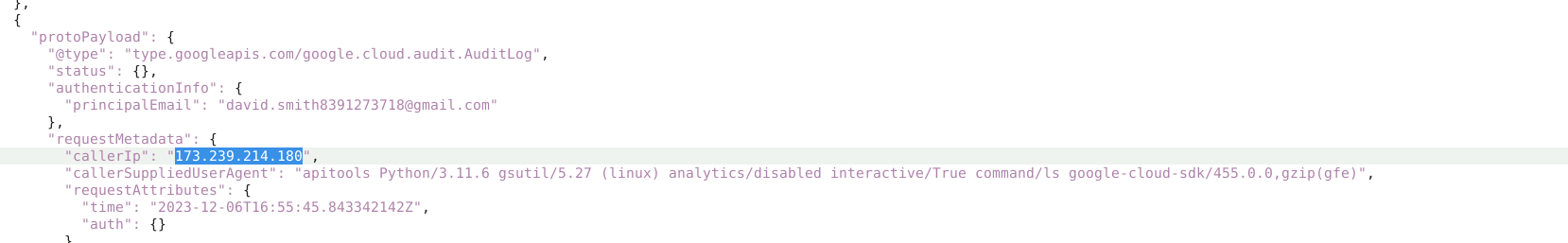


We need to get connections from malicious IPs, so we will use the following query



The first IP is malicious

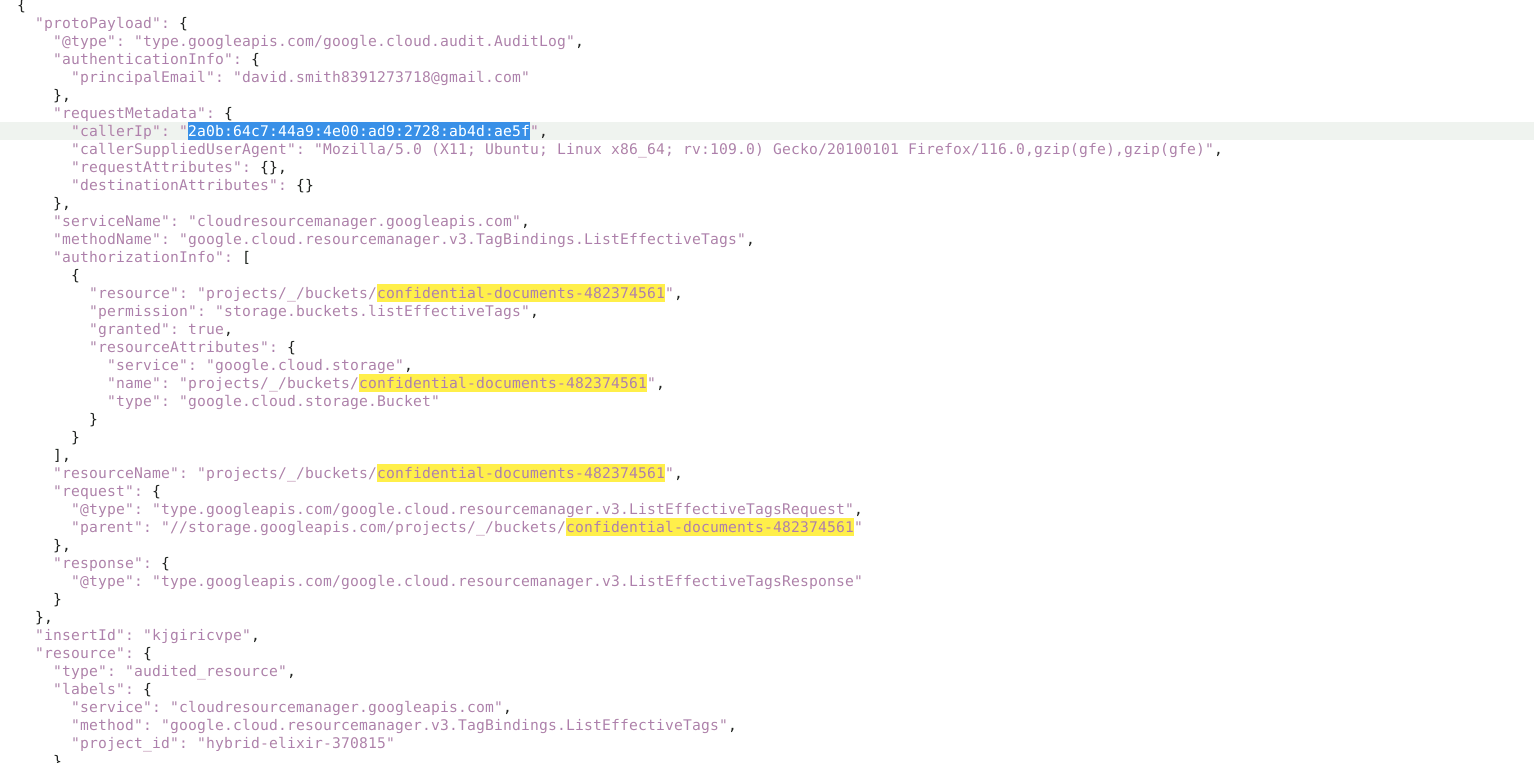


Track the user involved in this connection 

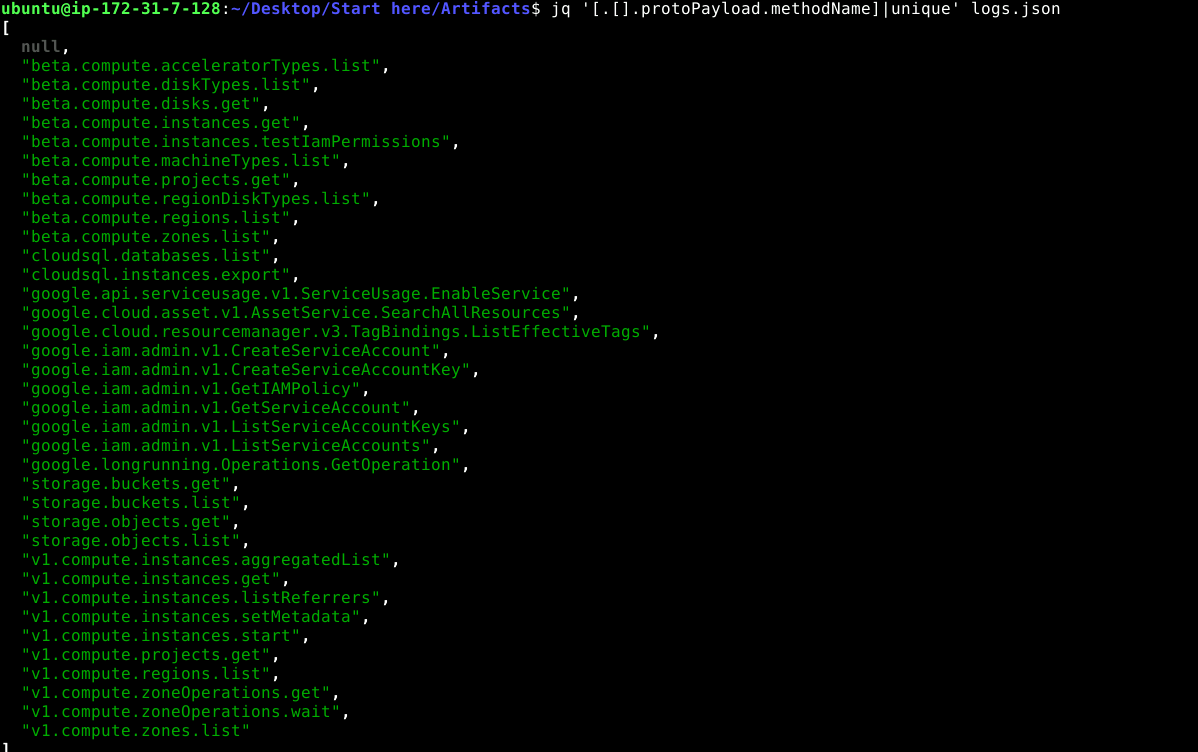
Our compromised user is [david.smith8391273718@gmail.com](mailto:david.smith8391273718@gmail.com)

First bucket the attacker accessed is confidential-documents-482374561 from IP address

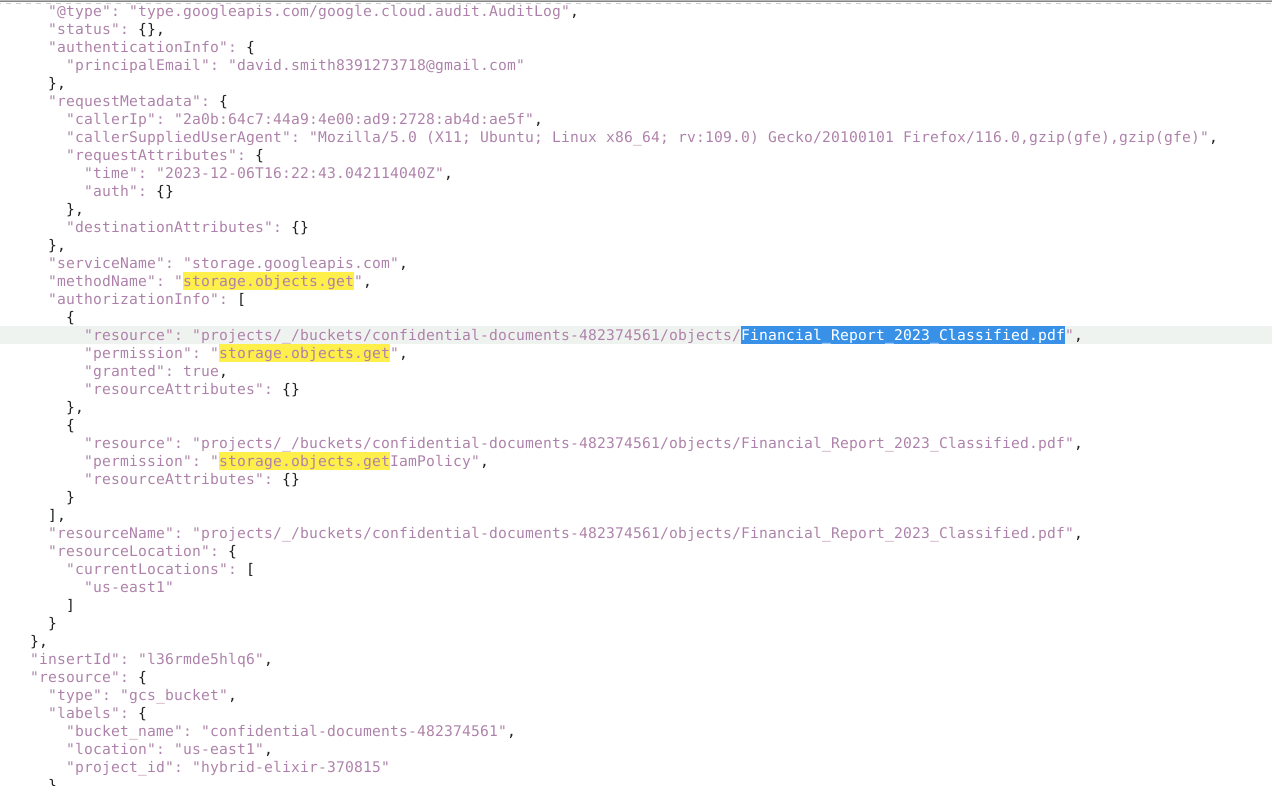
2a0b:64c7:44a9:4e00:ad9:2728:ab4d:ae5f with user-agent Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/116.0,gzip(gfe),gzip(gfe)



To get the list of methods in the log



Apparently storage.objects.get is the operation that we need to look at to define the first object exfiltrated



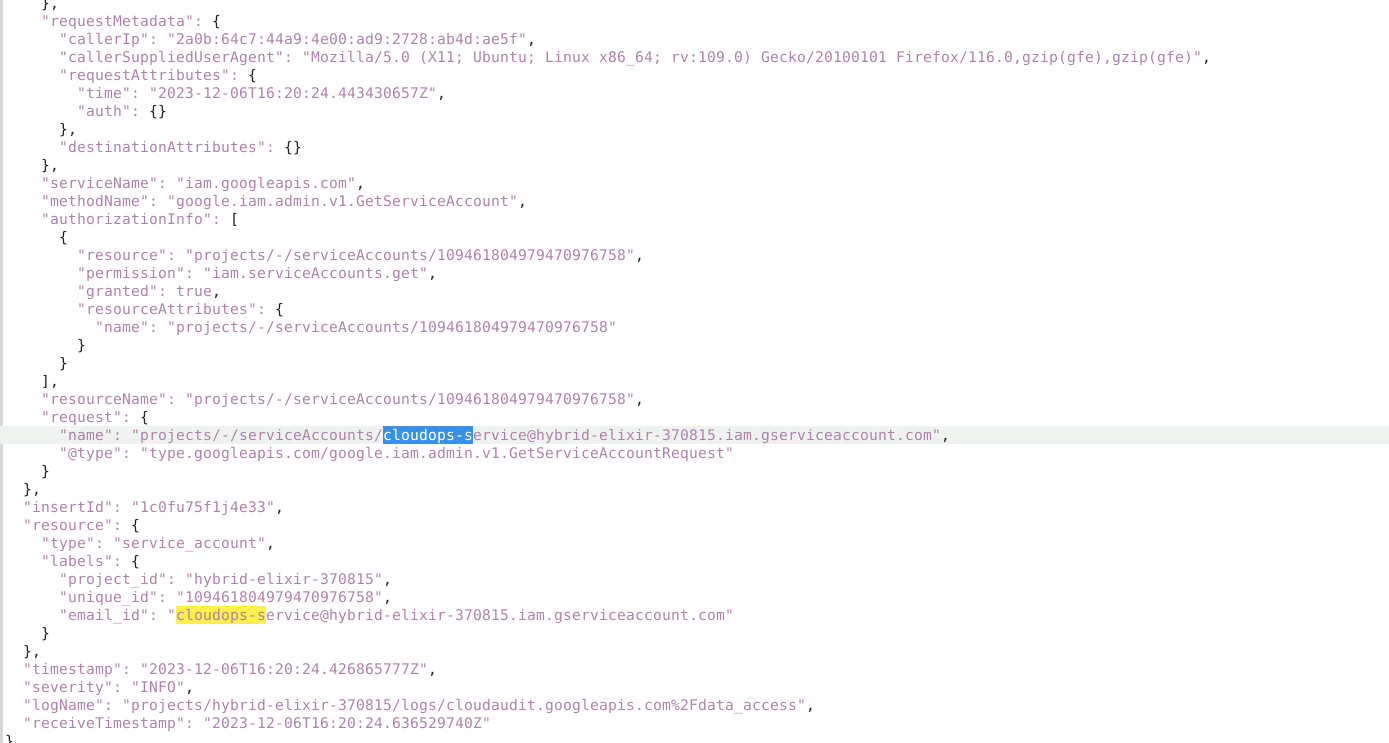
Let’s extract only the activities performed by this IP



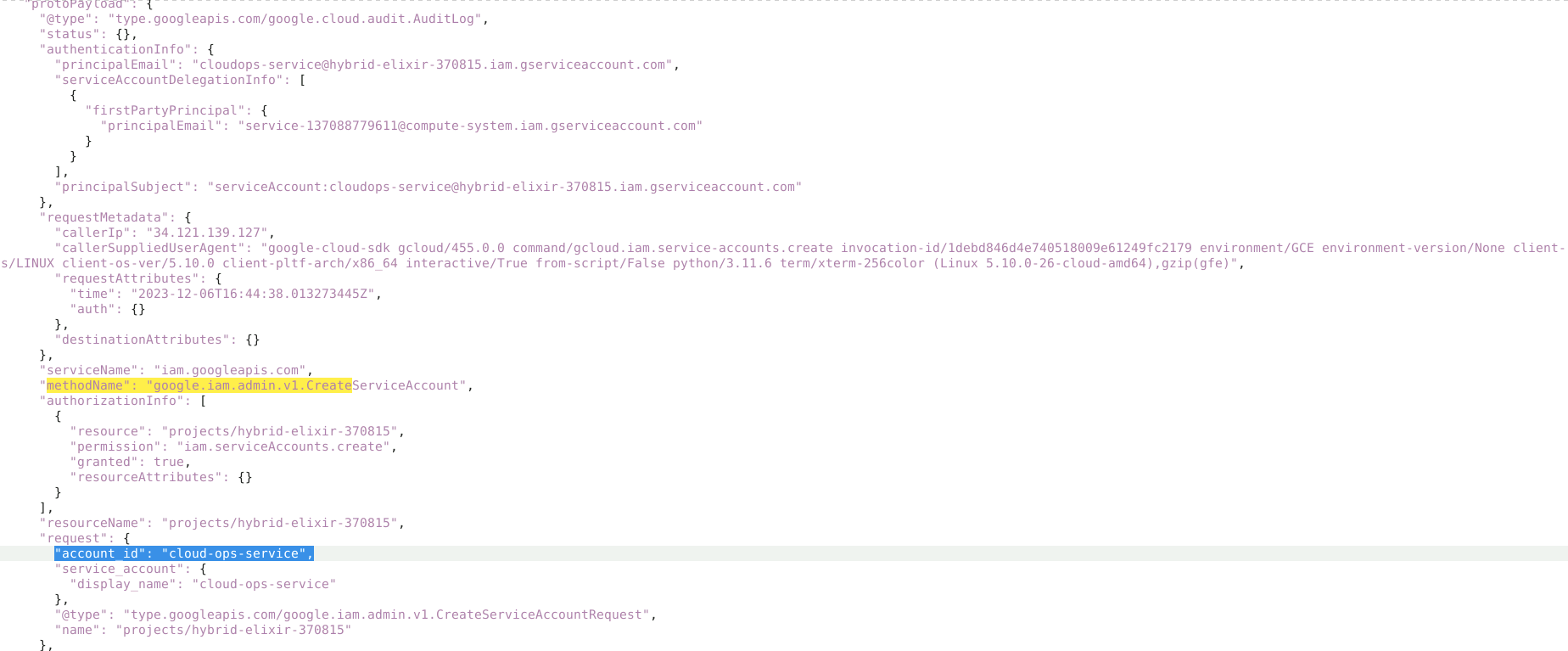
To get the instance he accessed , let’s look for method v1.instances.start



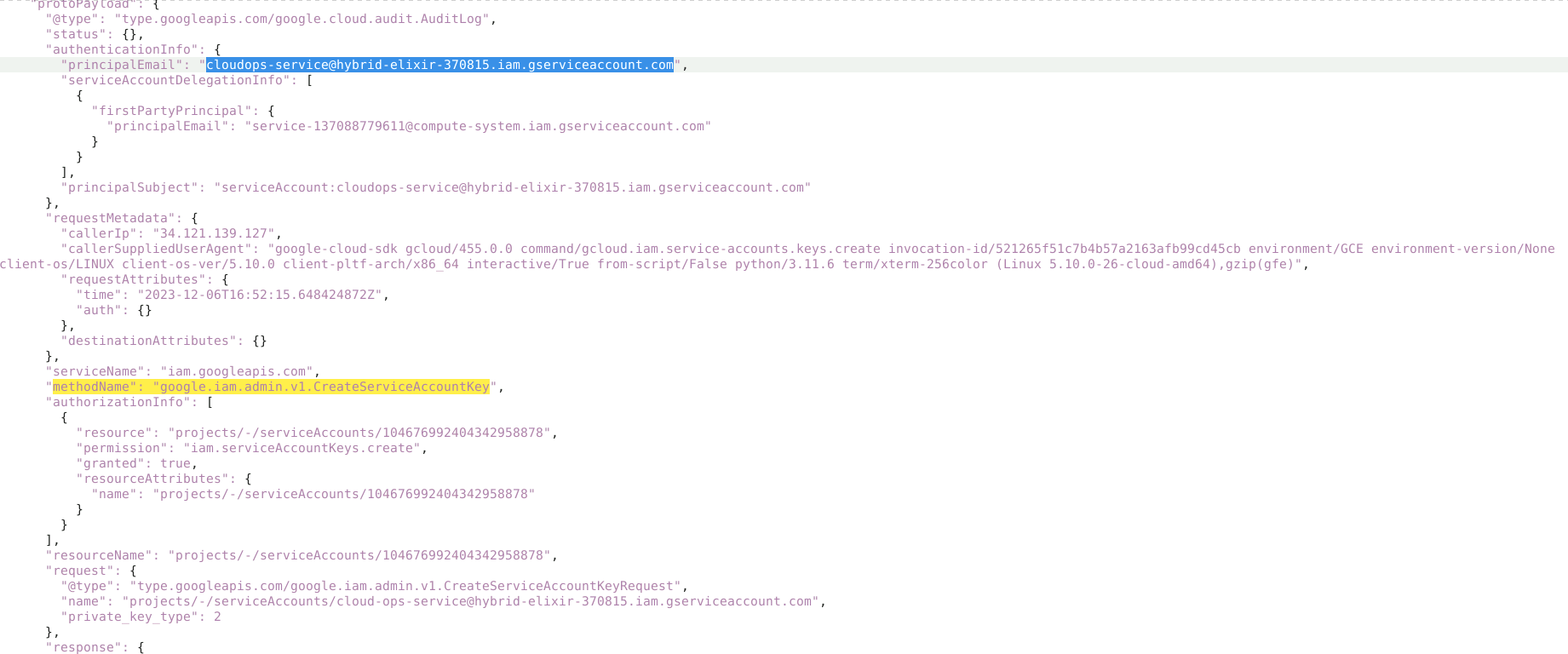
What service account is used by the Compute instance for calls to Google Cloud APIs?



The attacker abused this service account to create another service account for persistence



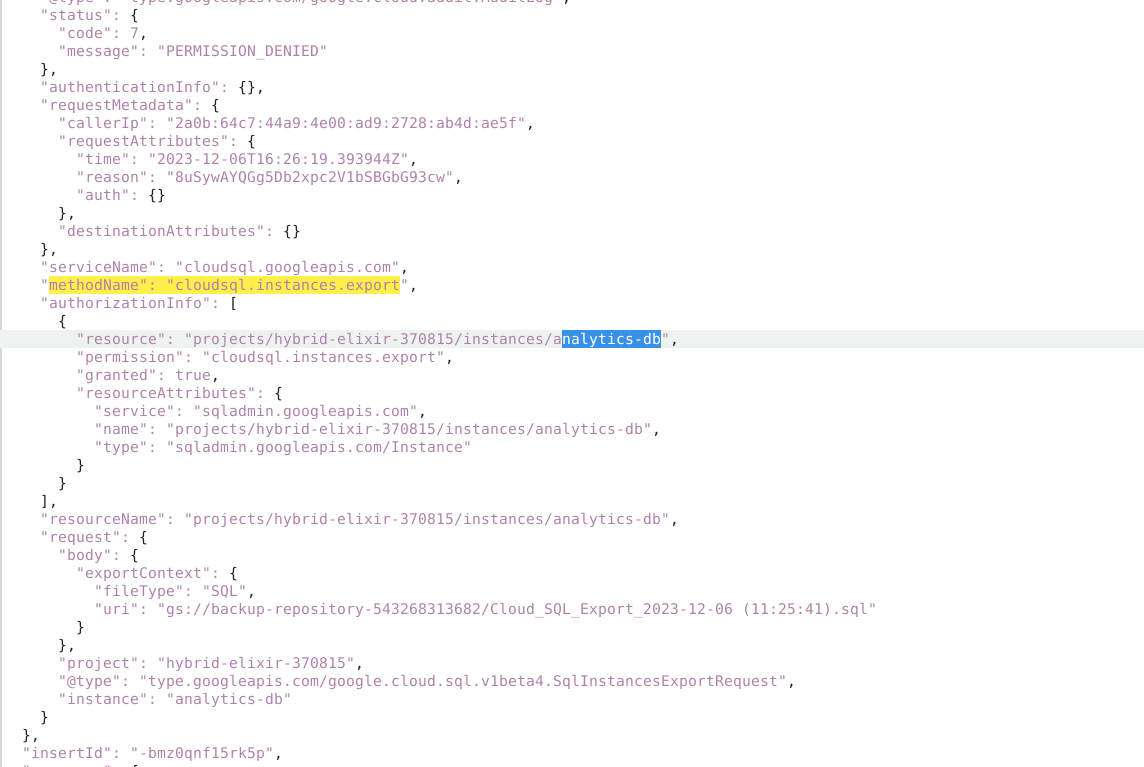
Then create a secret key for this service account





The secret Key is 16569af4fb98194fc210770d353a2513bada24b3

In the process of exfiltrating data, identify the Google Cloud SQL database the attacker attempted to export. What is the database's name?



The attacker tried to export the database to google cloud bucket backup-repository-543268313682

