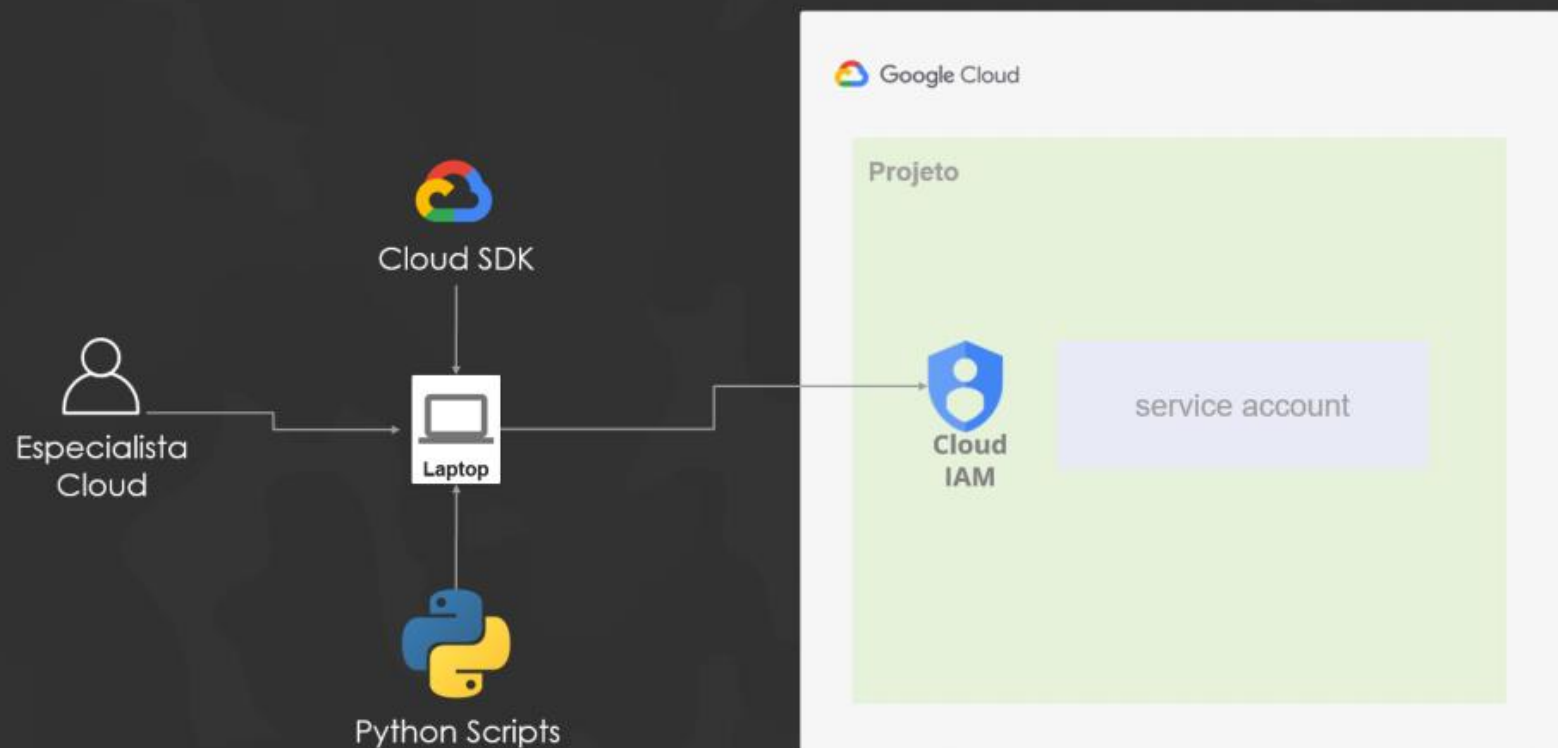




ARQUITETURA DA SOLUÇÃO

BOOTCAMP GOOGLE CLOUD

AUTOMAÇÃO NA GOOGLE CLOUD UTILIZANDO PYTHON – IAM SERVICE ACCOUNTS – PARTE 1





Requirements

- Install SDK

<https://cloud.google.com/sdk/docs/install>

Installation instructions

★ **Note:** If you are behind a proxy/firewall, see the [proxy settings](#) page for more information on installation.

Linux

Debian/Ubuntu

Red Hat/Fedora/CentOS

macOS

Windows

1. Cloud SDK requires Python; supported versions are Python 3 (preferred, 3.5 to 3.8) and Python 2 (2.7.9 or higher).



Requirements

- Install google-cloud-compute

<https://github.com/googleapis/python-compute>

<https://googleapis.dev/python/compute/latest/index.html>

Mac/Linux

```
pip install virtualenv
virtualenv <your-env>
source <your-env>/bin/activate
<your-env>/bin/pip install google-cloud-compute
```

Windows

```
pip install virtualenv
virtualenv <your-env>
<your-env>\Scripts\activate
<your-env>\Scripts\pip.exe install google-cloud-compute
```



Requirements

- Installing Google Cloud SDK

<https://cloud.google.com/sdk/docs/install>

```
pip install --upgrade google-cloud-storage
```

```
pip install --upgrade google-cloud-compute
```

```
pip install --upgrade google-api-python-client
```

```
pip install --upgrade oauth2client
```



Creating a Project in GCP

```
gcloud projects create project-bootcamp-666999 \  
  --name="Project-Bootcamp" \  
  --labels=type=handson1
```

Google Cloud Platform Project-Bootcamp Search products and resources

DASHBOARD

Quick Access

- Google Cloud
- Getting Started

Project info

Project name Project-Bootcamp

Select a project NEW PROJECT

Search projects and folders

RECENT STARRED ALL

	Name	ID
✓ ☆	Project-Bootcamp ?	project-bootcamp-666999
☆	My First Project ?	high-science-322201
☆	My First Project ?	fiery-palace-322201



Adding an IAM Service Account

```
gcloud iam service-accounts create automation \  
  --description="TCB Bootcamper automation account" \  
  --display-name="Automation1" \  
  --project=project-bootcamp-666999
```

The screenshot shows the Google Cloud Platform console interface. At the top, there's a blue header with the Google Cloud Platform logo, the project name 'Project-Bootcamp', and a search bar. Below the header, the left sidebar contains navigation icons. The main content area shows the details of a service account named 'Automation1'. The 'DETAILS' tab is selected, showing the service account details. The 'Name' field is 'Automation1' and the 'Description' field is 'TCB Bootcamper automation account'. The 'Email' field shows the email address 'automation@project-bootcamp-666999.iam.gserviceaccount.com'. There are 'SAVE' buttons next to the Name and Description fields.

Google Cloud Platform	Project-Bootcamp	Search products and resources			
Automation1	DETAILS	PERMISSIONS	KEYS	METRICS	LOGS
Service account details					
Name	Automation1				SAVE
Description	TCB Bootcamper automation account				SAVE
Email	automation@project-bootcamp-666999.iam.gserviceaccount.com				



IAM policies -> service account

```
gcloud projects add-iam-policy-binding project-bootcamp-666999 \  
  --member="serviceAccount:automation@project-bootcamp-666999.iam.gserviceaccount.com" \  
  --role="roles/storage.admin"
```

Google Cloud Platform Project-Bootcamp

Search products and resources

IAM + ADD - REMOVE

PERMISSIONS RECOMMENDATIONS HISTORY

Permissions for project "Project-Bootcamp"

These permissions affect this project and all of its resources. [Learn more](#)

View By: MEMBERS ROLES ☐ Include Google-...

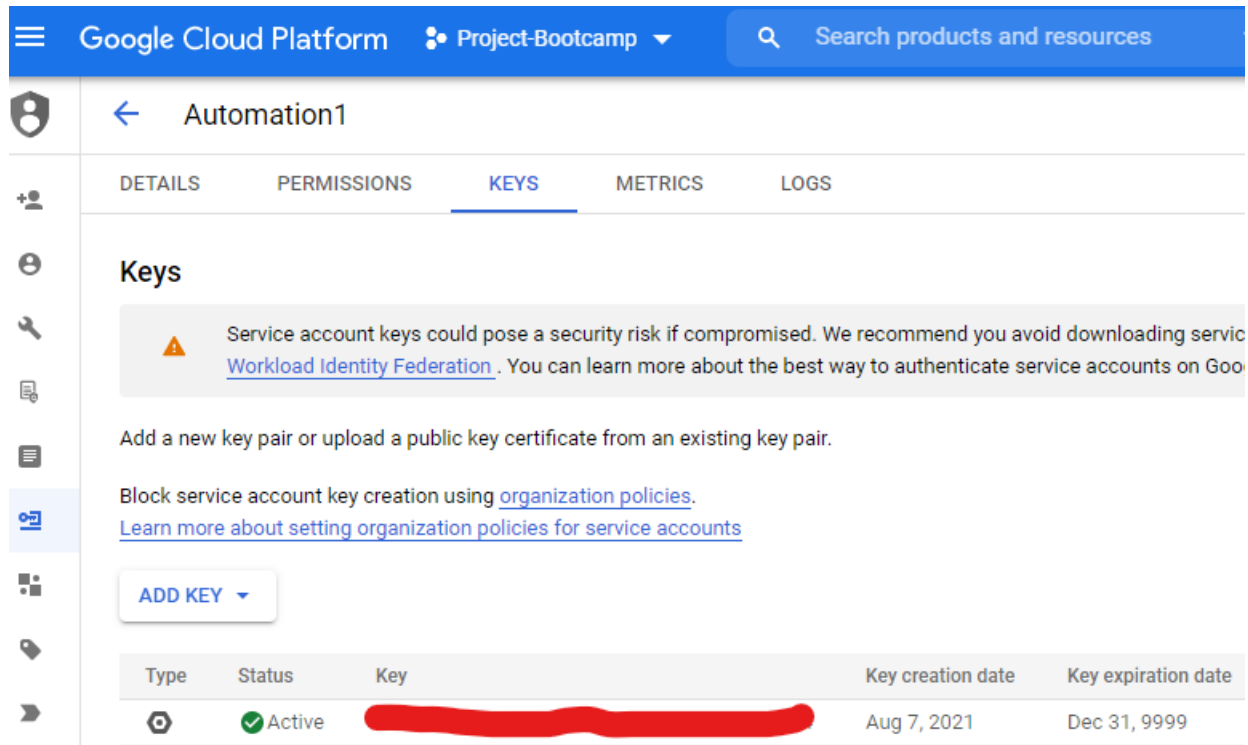
Filter automation@project-bootcamp-666999.iam.gserviceaccount.com Enter property name or value

Type	Member ↑	Name	Role	Security insights
<input type="checkbox"/>	automation@project-bootcamp-666999.iam.gserviceaccount.com	Automation1	Compute Instance Admin (v1) Storage Admin	23/24 excess permissions



Authentication Key

```
gcloud iam service-accounts keys create key-file \  
--iam-account=sa-name@project-id.iam.gserviceaccount.com
```



The screenshot shows the Google Cloud Platform console interface. At the top, there's a blue header with the Google Cloud Platform logo, the project name 'Project-Bootcamp', and a search bar. Below the header, the left sidebar contains various navigation icons. The main content area is titled 'Automation1' and has tabs for 'DETAILS', 'PERMISSIONS', 'KEYS' (which is selected), 'METRICS', and 'LOGS'. Under the 'KEYS' tab, there's a section titled 'Keys' with a warning message: 'Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys. We recommend you use [Workload Identity Federation](#). You can learn more about the best way to authenticate service accounts on Google Cloud.' Below the warning, there's a button 'ADD KEY' with a dropdown arrow. At the bottom, there's a table with columns: 'Type', 'Status', 'Key', 'Key creation date', and 'Key expiration date'. The table contains one row with a key icon, a green checkmark and the word 'Active', a redacted key name, the date 'Aug 7, 2021', and the date 'Dec 31, 9999'.

Type	Status	Key	Key creation date	Key expiration date
	✓ Active	[Redacted]	Aug 7, 2021	Dec 31, 9999



Creating and validating

Cloud Storage Bucket using gcloud CLI and Python

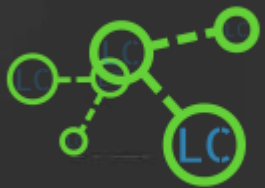
```
gsutil mb gs://BUCKET_NAME
```

```
@lucianod2$  
@lucianod2$gsutil mb gs://caetano-iam-project1  
Creating gs://caetano-iam-project1/...  
@lucianod2$
```

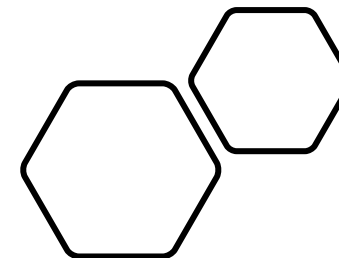
validating the installation

```
python lista_storage.py key-automation.json
```

```
@lucianod2$# GCP hands-on  
@lucianod2$  
@lucianod2$python lista_storage.py key-automation.json  
[<Bucket: caetano-iam-project1>]  
@lucianod2$#  
@lucianod2$# Listing files  
@lucianod2$gsutil ls gs://caetano-iam-project1  
gs://caetano-iam-project1/file1.txt  
gs://caetano-iam-project1/file2.txt  
gs://caetano-iam-project1/file3.txt  
@lucianod2$
```



THE SDK



"Would it be possible for this python script, making a small adjustment, to read all the virtual machines that are created there in the Google Cloud?"

YES!



Google
Cloud Platform



THE SDK Challenge

Python script gcp_list_vms.py



 <https://github.com/lucianod2/gcp-api-python>

Demo – see the similarity with gcloud cli

This python script run similar the gcloud compute instances list

gcp_list_vms.py

```
from pprint import pprint
from googleapiclient import discovery
from oauth2client.client import GoogleCredentials
from six.moves import input

import googleapiclient.discovery
import argparse
import os
#os.environ["GOOGLE_APPLICATION_CREDENTIALS"] = "/full-path/service-account-key-automation.json"

# Project ID for this request.
project = "project-name"
zone = "us-east1-b"
compute = googleapiclient.discovery.build('compute', 'v1')
space = ' '

def list_instances(compute, project, zone):
    result = compute.instances().list(project=project, zone=zone).execute()

    print ("{:<7} {:<11} {:<13} {:<12} {:<12} {:<15} {:<15}".format('NAME','ZONE','MACHINE_TYPE','PREEMP'))

    for item in result['items']:
        if item['status'] == "RUNNING":
            var_name = item['name']
            var_zone = item['zone']
            var_machine_type = item['machineType']
            var_preemptible = item['scheduling']['preemptible']
            var_internal_ip = item['networkInterfaces'][0]['networkIP']
            var_external_ip = '{:<14}'.format(item['networkInterfaces'][0]['accessConfigs'][0]['natIP'])
            var_status = item['status'].rjust(8)
```

```
@lucianod2$
@lucianod2$
@lucianod2$# THE SDK challenge
@lucianod2$# THE CLOUD BOOTCAMP - GOOGLE CLOUD PLATFORM TRAINING
@lucianod2$# BOOTCAMPER: LUCIANO CAETANO
@lucianod2$#
@lucianod2$python gcp_list_vms.py
NAME     ZONE     MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
vm-01t   us-east1-b  e2-micro      True         10.142.0.12  34.74.193.118  RUNNING
vm-02t   us-east1-b  e2-micro      True         10.142.0.14  35.237.165.207  RUNNING
vm-03t   us-east1-b  e2-micro      True         10.142.0.15  34.73.12.42     RUNNING
```

Winners never quit, and quitters never win.

Vencedores nunca desistem e desistentes nunca ganham.

#praxima

```
@lucianod2$# Runnin gcloud CLI version
@lucianod2$gcloud compute instances list
NAME     ZONE     MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
vm-01t   us-east1-b  e2-micro      true         10.142.0.12  34.74.193.118  RUNNING
vm-02t   us-east1-b  e2-micro      true         10.142.0.14  35.237.165.207  RUNNING
vm-03t   us-east1-b  e2-micro      true         10.142.0.15  34.73.12.42     RUNNING
@lucianod2$
```