PRACTICAL: 8

AIM:

Security Best Practices in Google Cloud:

1. Using Customer-Supplied Encryption Keys with Cloud Storage.
2. Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS.
3. Using Cloud Security Scanner to find vulnerabilities in an App Engine application.
4. Configuring Identity Aware Proxy to Protect a Project.
5. Configuring and Using Credentials with Secret Manager.

THEORY:

8.1 Using Customer-Supplied Encryption Keys with Cloud Storage

Cloud Storage always encrypts your data on the server side with a Google-managed encryption key, before it is written to disk, at no additional charge. As an alternative to a Google-managed server-side encryption key, you can choose to provide your own AES-256 key, encoded in standard Base64. This key is known as a customer-supplied encryption key.

Here we will configure customer-supplied encryption keys (CSEK) for Google Cloud storage. Files will then be uploaded into a storage bucket. Here we will generate a new encryption key and rotate CSEK keys.

Cloud storage does not permanently store your key on Google’s servers or otherwise manage your key. Instead, you provide your key for each Cloud Storage operation and your key is purged from Google’s servers after the operation is complete. Cloud Storage stores only a cryptographic hash of the key so that future requests can be validated against the hash. Your key cannot be recovered from this hash and the hash cannot be used to decrypt your data. If you lose your CSEK, you will permanently lose access to all of your data encrypted with the key.

8.2 Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS

Cloud KMS is cloud-hosted key management service. Encryption keys are created by Cloud KMS and managed by you in the same manner you would manage them on-premises. Using Cloud KMS you can generate, use, rotate and destroy AES256 symmetric encryption keys for direct use by all of your cloud services.

Here we will use Cloud KMS to create KeyRings and CryptoKeys and then use those keys with Cloud Storage to set default keys on buckets, and encrypt individual objects with a Cloud KMS key. Additionally, you will manually perform server-side encryption with your KMS keys, and upload encrypted data to Google Cloud storage.

KMS permissions will be managed with IAM, and Cloud Audit Logging will be used to view all activity for CryptoKeys and KeyRings.

8.3 Using Cloud Security Scanner to find vulnerabilities in an App Engine Application

Cloud Security Scanner is used to scan an App Engine application for vulnerabilities. Cloud Security Scanner is a web security scanner for common vulnerabilities in Google App Engine applications. It can automatically scan and detect four common vulnerabilities, including cross-site-scripting (XSS), Flash Injection, mixed content (HTTP in HTTPS) and outdated/insecure libraries. It enables early identification and delivers very low false positive rates. Here by setting up the environment we can easily run, schedule, and mange security scans and it is free for Google Cloud Platform users.

8.4 Configuring Identity Aware Proxy to Protect a Project

Here you can configure and enable Cloud Identity Aware Proxy (Cloud IAP) to project an application running in App Engine. Cloud IAP controls access to your cloud applications running on Google Cloud IAP works by verifying a user’s identity and determining if that user should be allowed to access the application. Cloud IAP is building block toward BeyondCorp an enterprise security model that enables every employee to work from untrusted networks without the use of VPN.

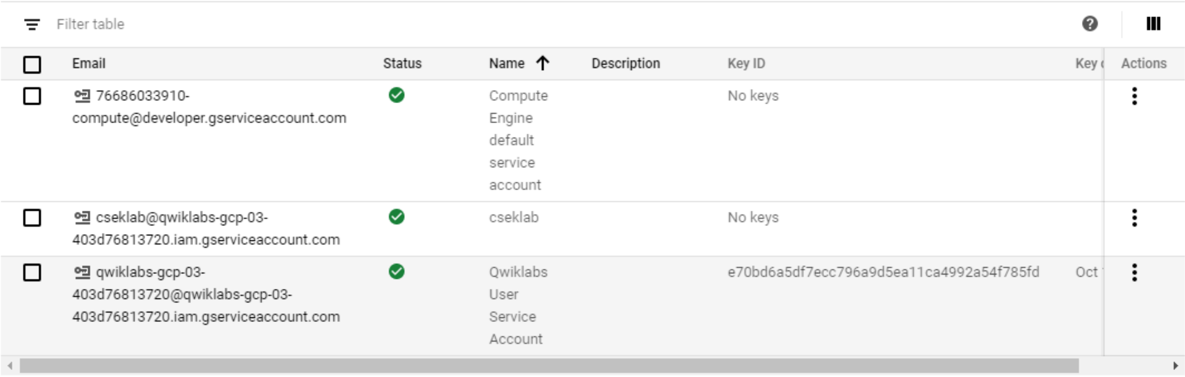
8.5 Configuring and Using Credentials with Secret Manager

Here you will use Secret Manager from Google Cloud Console and the Command Line Interface (CLI) to create and use a secret, replace a secret and finally reinstate an older version of a secret.

Secret Manager is available in Google Cloud Console. It is also available from the command line using the CLI or from a program, using the REST API or one of the supported Software Development Kits (SDKs) Supported SDKs include a complete list of programs.

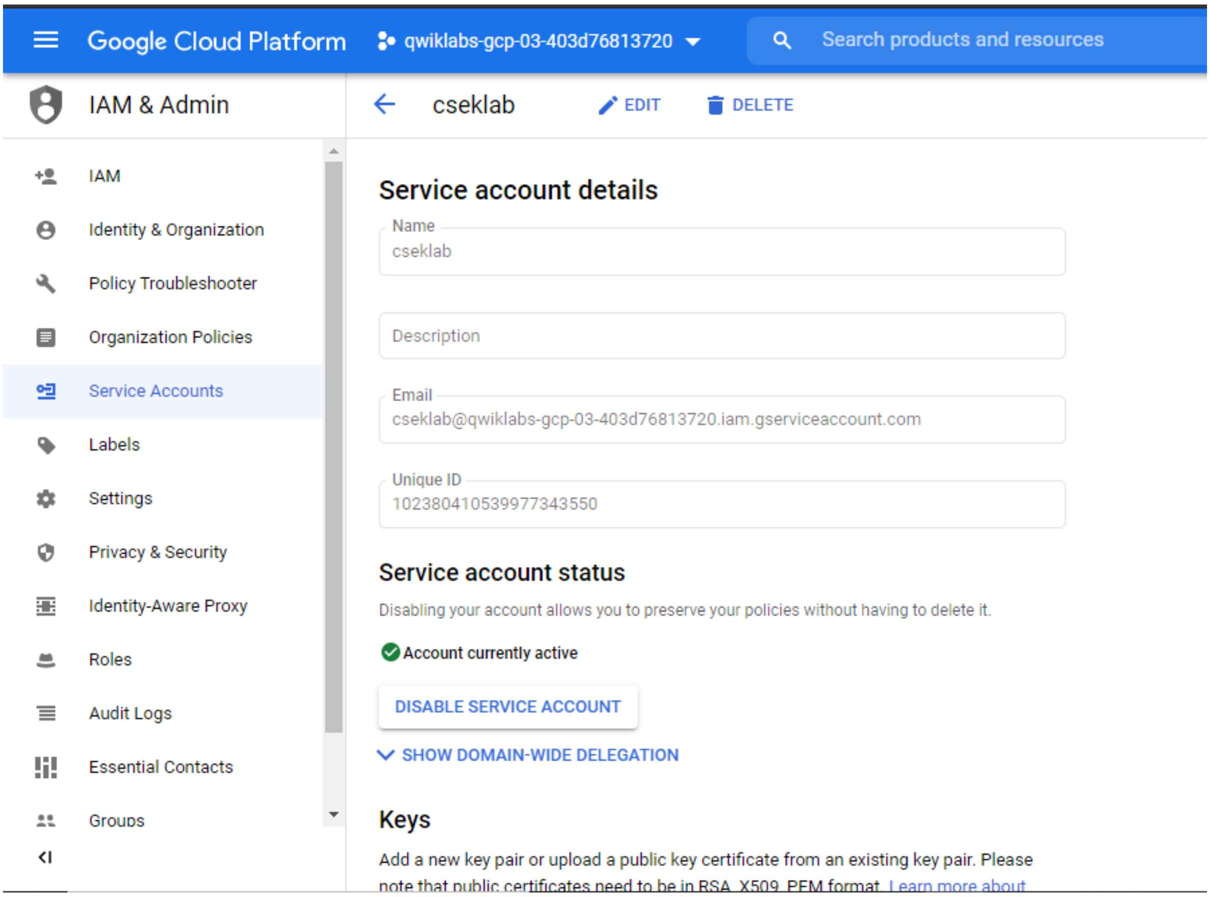
OUTPUT:

8.1 Using Customer-Supplied Encryption Keys with Cloud Storage



□	Email	Status	Name ↑	Description	Key ID	Key (	Actions
□	76686033910-compute@developer.gserviceaccount.com	✓	Compute Engine default service account		No keys		⋮
□	cseklab@qwiklabs-gcp-03-403d76813720.iam.gserviceaccount.com	✓	cseklab		No keys		⋮
□	qwiklabs-gcp-03-403d76813720@qwiklabs-gcp-03-403d76813720.iam.gserviceaccount.com	✓	Qwiklabs User Service Account		e70bd6a5df7ecc796a9d5ea11ca4992a54f785fd	Oct	⋮

Service account dashboard



Service account details

Name: cseklab

Description

Email: cseklab@qwiklabs-gcp-03-403d76813720.iam.gserviceaccount.com

Unique ID: 102380410539977343550

Service account status

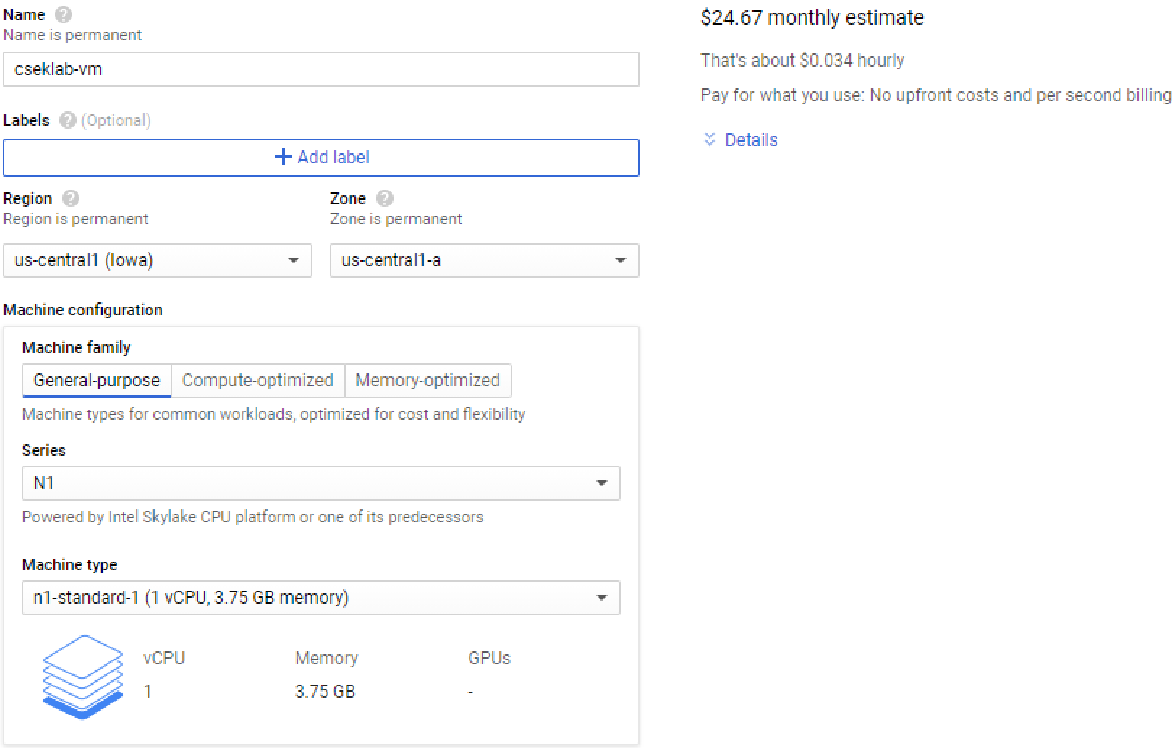
Disabling your account allows you to preserve your policies without having to delete it.

Account currently active

Keys

Add a new key pair or upload a public key certificate from an existing key pair. Please note that public certificates need to be in RSA_X509_PEM format. Learn more about

Creating IAM service account



Name
Name is permanent
cseklab-vm

Labels (Optional)

Region
Region is permanent
us-central1 (Iowa)

Zone
Zone is permanent
us-central1-a

Machine configuration

Machine family: General-purpose

Machine types for common workloads, optimized for cost and flexibility

Series: N1

Powered by Intel Skylake CPU platform or one of its predecessors

Machine type: n1-standard-1 (1 vCPU, 3.75 GB memory)

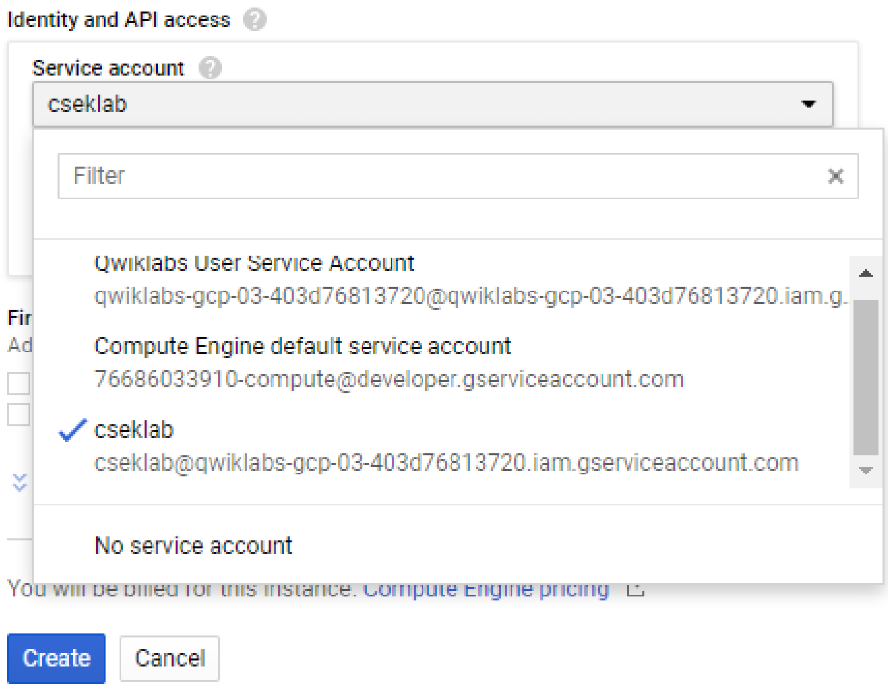
vCPU	Memory	GPUs
1	3.75 GB	-

$24.67 monthly estimate

That's about $0.034 hourly

Pay for what you use: No upfront costs and per second billing

Creating VM instance



Identity and API access

Service account

cseklab

Qwiklabs User Service Account
qwiklabs-gcp-03-403d76813720@qwiklabs-gcp-03-403d76813720.iam.g...

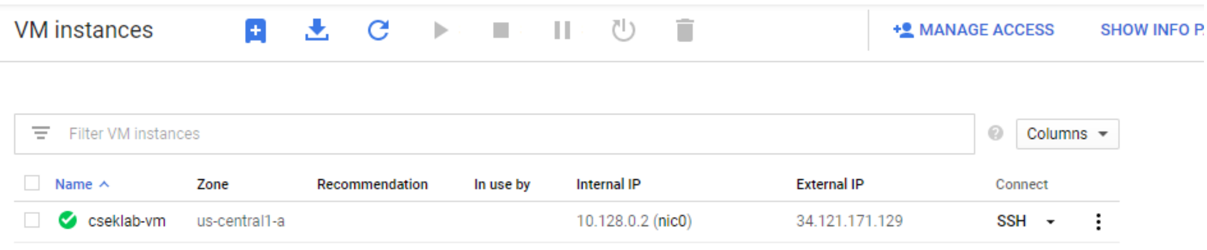
Compute Engine default service account
76686033910-compute@developer.gserviceaccount.com

✓ cseklab
cseklab@qwiklabs-gcp-03-403d76813720.iam.gserviceaccount.com

No service account

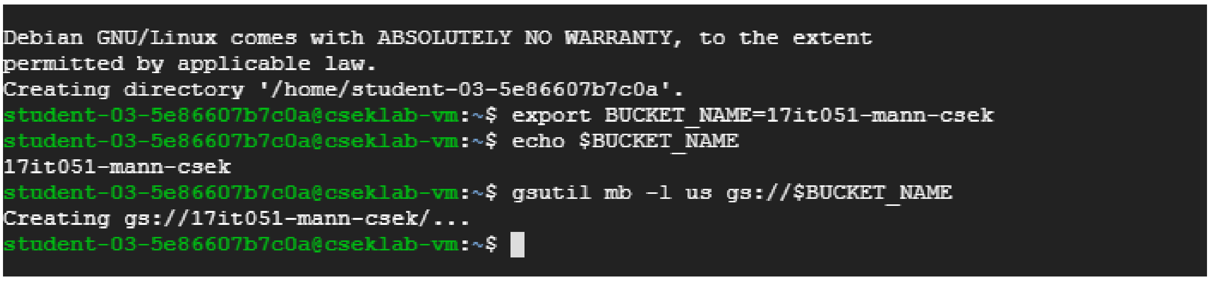
You will be billed for this instance. Compute Engine pricing

Linking service account created in previous step



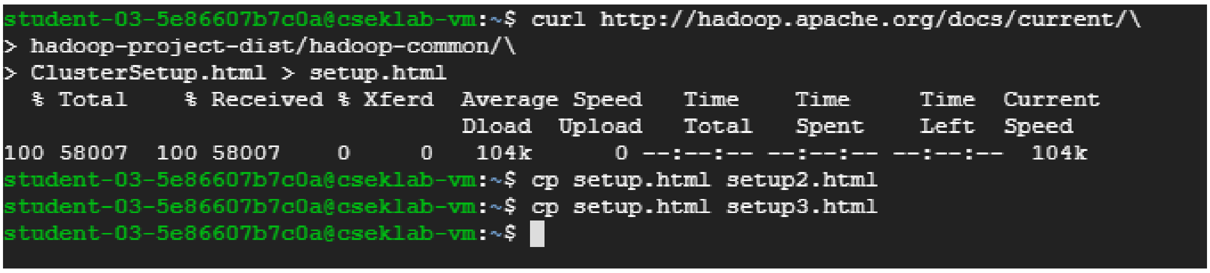
□	Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
□	✓ cseklab-vm	us-central1-a			10.128.0.2 (nic0)	34.121.171.129	SSH

VM instance created



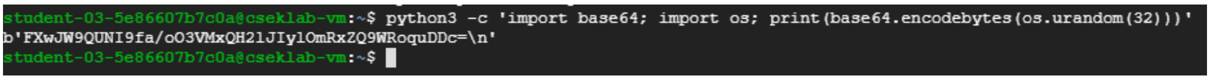
```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/student-03-5e86607b7c0a'.
student-03-5e86607b7c0a@cseklab-vm:~$ export BUCKET_NAME=17it051-mann-csek
student-03-5e86607b7c0a@cseklab-vm:~$ echo $BUCKET_NAME
17it051-mann-csek
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil mb -l us gs://$BUCKET_NAME
Creating gs://17it051-mann-csek/...
student-03-5e86607b7c0a@cseklab-vm:~$
```

Creating a Cloud Storage bucket

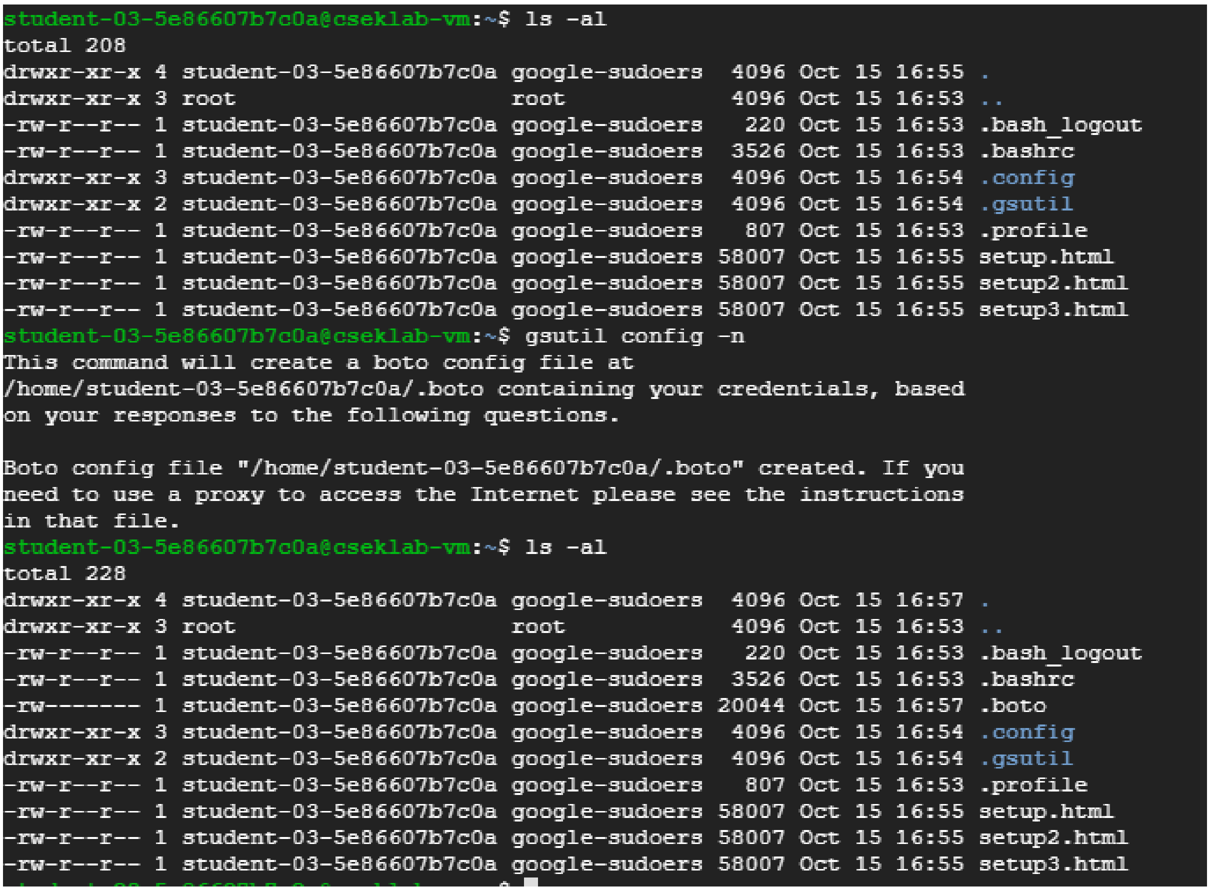


```
student-03-5e86607b7c0a@cseklab-vm:~$ curl http://hadoop.apache.org/docs/current/\
> hadoop-project-dist/hadoop-common/\
> ClusterSetup.html > setup.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 58007  100 58007    0     0   104k      0 --:--:-- --:--:-- --:--:--  104k
student-03-5e86607b7c0a@cseklab-vm:~$ cp setup.html setup2.html
student-03-5e86607b7c0a@cseklab-vm:~$ cp setup.html setup3.html
student-03-5e86607b7c0a@cseklab-vm:~$
```

Downloading sample file using CURL and making two copies of it

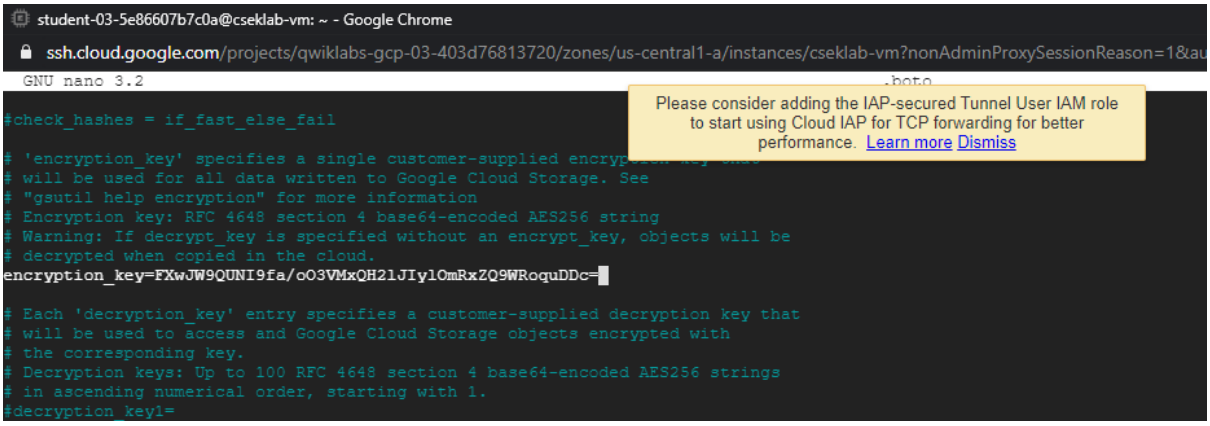


```
student-03-5e86607b7c0a@cseklab-vm:~$ python3 -c 'import base64; import os; print(base64.encodebytes(os.urandom(32)))'
b'FXwJW9QUNI9fa/oO3VMxQH2lJIylOmRxZQ9WRoquDDc=\n'
student-03-5e86607b7c0a@cseklab-vm:~$
```



```
student-03-5e86607b7c0a@cseklab-vm:~$ ls -al
total 208
drwxr-xr-x 4 student-03-5e86607b7c0a google-sudoers  4096 Oct 15 16:55 .
drwxr-xr-x 3 root                    root            4096 Oct 15 16:53 ..
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers   220 Oct 15 16:53 .bash_logout
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers  3526 Oct 15 16:53 .bashrc
drwxr-xr-x 3 student-03-5e86607b7c0a google-sudoers  4096 Oct 15 16:54 .config
drwxr-xr-x 2 student-03-5e86607b7c0a google-sudoers  4096 Oct 15 16:54 .gsutil
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers   807 Oct 15 16:53 .profile
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers 58007 Oct 15 16:55 setup.html
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers 58007 Oct 15 16:55 setup2.html
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers 58007 Oct 15 16:55 setup3.html
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil config -n
This command will create a boto config file at
/home/student-03-5e86607b7c0a/.boto containing your credentials, based
on your responses to the following questions.

Boto config file "/home/student-03-5e86607b7c0a/.boto" created. If you
need to use a proxy to access the Internet please see the instructions
in that file.
student-03-5e86607b7c0a@cseklab-vm:~$ ls -al
total 228
drwxr-xr-x 4 student-03-5e86607b7c0a google-sudoers  4096 Oct 15 16:57 .
drwxr-xr-x 3 root                    root            4096 Oct 15 16:53 ..
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers   220 Oct 15 16:53 .bash_logout
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers  3526 Oct 15 16:53 .bashrc
-rw------- 1 student-03-5e86607b7c0a google-sudoers 20044 Oct 15 16:57 .boto
drwxr-xr-x 3 student-03-5e86607b7c0a google-sudoers  4096 Oct 15 16:54 .config
drwxr-xr-x 2 student-03-5e86607b7c0a google-sudoers  4096 Oct 15 16:54 .gsutil
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers   807 Oct 15 16:53 .profile
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers 58007 Oct 15 16:55 setup.html
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers 58007 Oct 15 16:55 setup2.html
-rw-r--r-- 1 student-03-5e86607b7c0a google-sudoers 58007 Oct 15 16:55 setup3.html
```

Configuring Customer-Supplied Encryption Keys



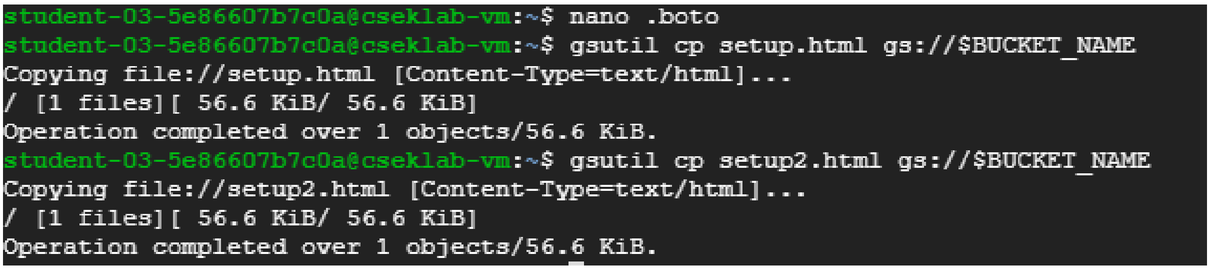
student-03-5e86607b7c0a@cseklab-vm: ~ - Google Chrome

ssh.cloud.google.com/projects/qwiklabs-gcp-03-403d76813720/zones/us-central1-a/instances/cseklab-vm?nonAdminProxySessionReason=1&au

Please consider adding the IAP-secured Tunnel User IAM role to start using Cloud IAP for TCP forwarding for better performance. Learn more Dismiss

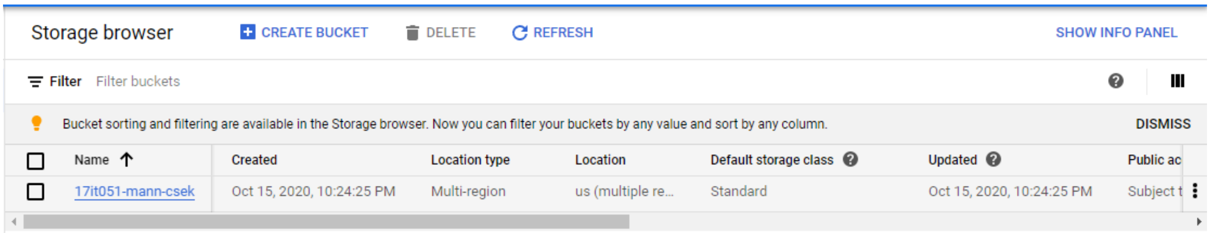
```
  GNU nano 3.2                                                          .boto

#check_hashes = if_fast_else_fail

# 'encryption_key' specifies a single customer-supplied encryp
# will be used for all data written to Google Cloud Storage. See
# "gsutil help encryption" for more information
# Encryption key: RFC 4648 section 4 base64-encoded AES256 string
# Warning: If decrypt_key is specified without an encrypt_key, objects will be
# decrypted when copied in the cloud.
encryption_key=FXwJW9QUNI9fa/oO3VMxQH21JIyl0mRxZQ9WRoquDDc=

# Each 'decryption_key' entry specifies a customer-supplied decryption key that
# will be used to access and Google Cloud Storage objects encrypted with
# the corresponding key.
# Decryption keys: Up to 100 RFC 4648 section 4 base64-encoded AES256 strings
# in ascending numerical order, starting with 1.
#decryption_key1=
```

Adding encryption_key field in .boto file



```
student-03-5e86607b7c0a@cseklab-vm:~$ nano .boto
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp setup.html gs://$BUCKET_NAME
Copying file://setup.html [Content-Type=text/html]...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp setup2.html gs://$BUCKET_NAME
Copying file://setup2.html [Content-Type=text/html]...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
```

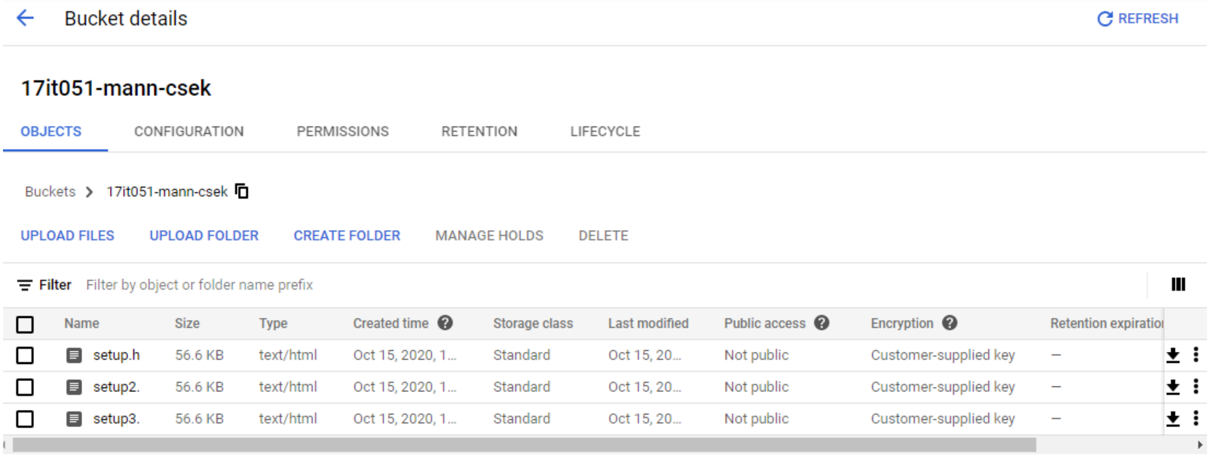
Creating two setups files



Bucket sorting and filtering are available in the Storage browser. Now you can filter your buckets by any value and sort by any column.

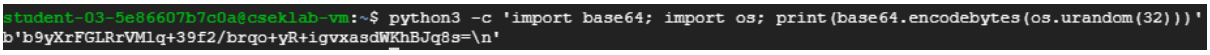
□	Name ↑	Created	Location type	Location	Default storage class	Updated	Public ac
□	17it051-mann-csek	Oct 15, 2020, 10:24:25 PM	Multi-region	us (multiple re...	Standard	Oct 15, 2020, 10:24:25 PM	Subject t

Bucket successfully created



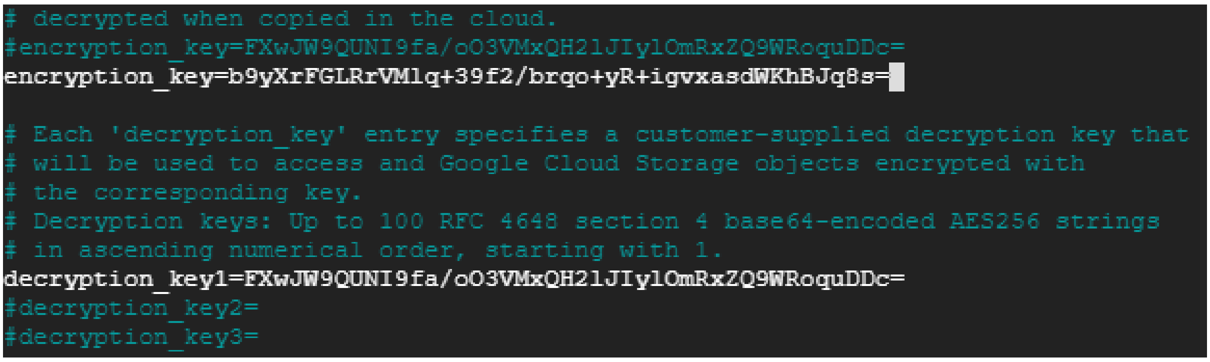
□	Name	Size	Type	Created time	Storage class	Last modified	Public access	Encryption	Retention expiratio
□	setup.h	56.6 KB	text/html	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Customer-supplied key	–
□	setup2.	56.6 KB	text/html	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Customer-supplied key	–
□	setup3.	56.6 KB	text/html	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Customer-supplied key	–

Observing bucket details which contain two setups files which uploaded via cloud shell



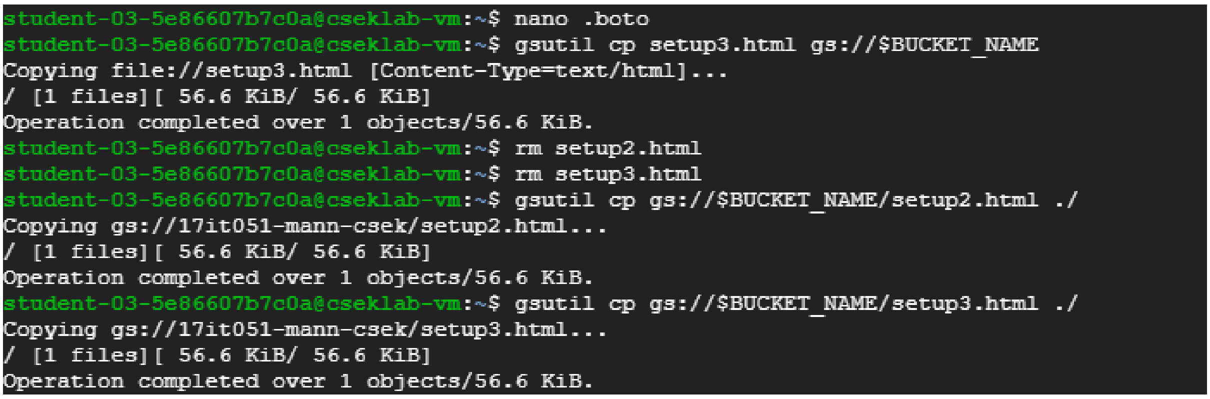
```
student-03-5e86607b7c0a@cseklab-vm:~$ python3 -c 'import base64; import os; print(base64.encodebytes(os.urandom(32)))'
b'b9yXrFGLRrVMlq+39f2/brqo+yR+igvxasdWKhBJq8s=\n'
```

Generating another key.

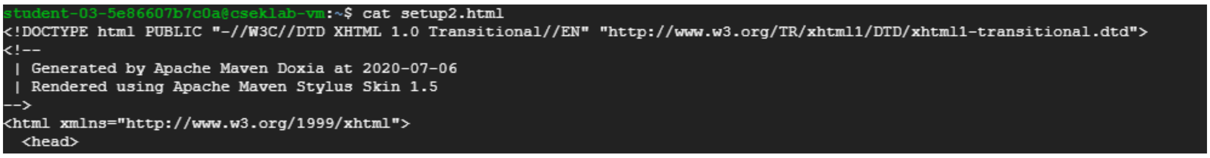


```
# decrypted when copied in the cloud.
#encryption_key=FXwJW9QUNI9fa/oO3VMxQH21JIylOmRxZQ9WRoquDDc=
encryption_key=b9yXrFGLRrVMlq+39f2/brqo+yR+igvxasdWKhBJq8s=

# Each 'decryption_key' entry specifies a customer-supplied decryption key that
# will be used to access and Google Cloud Storage objects encrypted with
# the corresponding key.
# Decryption keys: Up to 100 RFC 4648 section 4 base64-encoded AES256 strings
# in ascending numerical order, starting with 1.
decryption_key1=FXwJW9QUNI9fa/oO3VMxQH21JIylOmRxZQ9WRoquDDc=
#decryption_key2=
#decryption_key3=
```

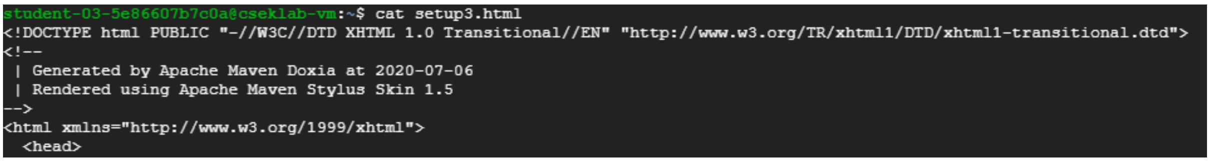
Rotating keys by adding new key to encryption_key and replacing decryption_key with old encryption_key



```
student-03-5e86607b7c0a@cseklab-vm:~$ nano .boto
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp setup3.html gs://$BUCKET_NAME
Copying file://setup3.html [Content-Type=text/html]...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
student-03-5e86607b7c0a@cseklab-vm:~$ rm setup2.html
student-03-5e86607b7c0a@cseklab-vm:~$ rm setup3.html
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp gs://$BUCKET_NAME/setup2.html ./
Copying gs://17it051-mann-csek/setup2.html...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp gs://$BUCKET_NAME/setup3.html ./
Copying gs://17it051-mann-csek/setup3.html...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
```

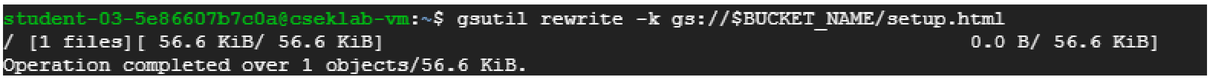


```
student-03-5e86607b7c0a@cseklab-vm:~$ cat setup2.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<!--
 | Generated by Apache Maven Doxia at 2020-07-06
 | Rendered using Apache Maven Stylus Skin 1.5
-->
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
```

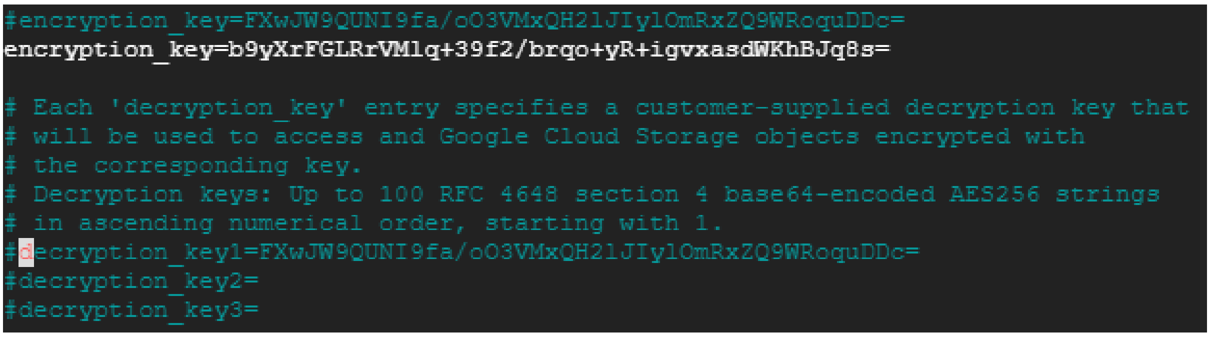


```
student-03-5e86607b7c0a@cseklab-vm:~$ cat setup3.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<!--
 | Generated by Apache Maven Doxia at 2020-07-06
 | Rendered using Apache Maven Stylus Skin 1.5
-->
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
```

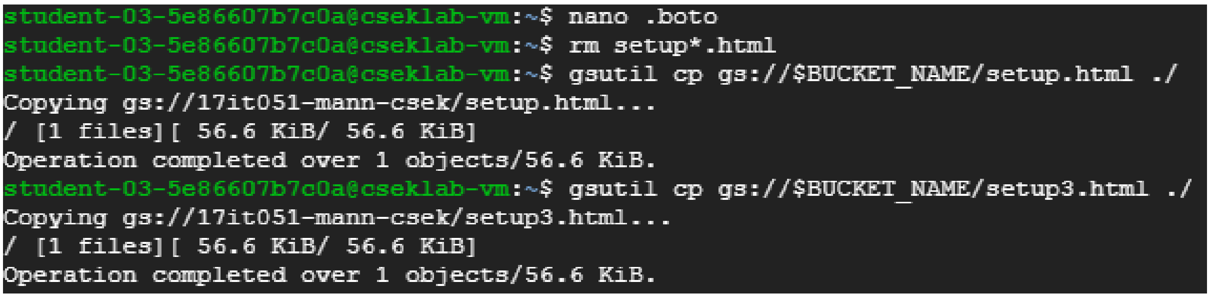
Creating and observing setup files



```
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil rewrite -k gs://$BUCKET_NAME/setup.html
/ [1 files][ 56.6 KiB/ 56.6 KiB]                                    0.0 B/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
```



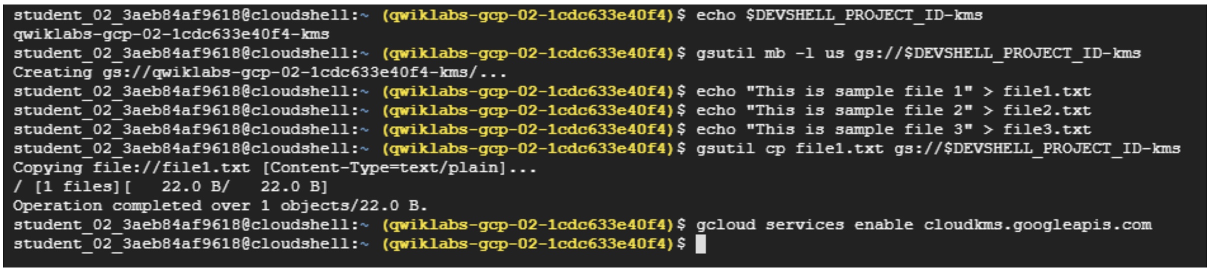
```
#encryption_key=FXwJW9QUNI9fa/oO3VMxQH21JIyl0mRxZQ9WRoquDDc=
encryption_key=b9yXrFGLRrVMlq+39f2/brqo+yR+igvxasdWKhBJq8s=

# Each 'decryption_key' entry specifies a customer-supplied decryption key that
# will be used to access and Google Cloud Storage objects encrypted with
# the corresponding key.
# Decryption keys: Up to 100 RFC 4648 section 4 base64-encoded AES256 strings
# in ascending numerical order, starting with 1.
#decryption_key1=FXwJW9QUNI9fa/oO3VMxQH21JIyl0mRxZQ9WRoquDDc=
#decryption_key2=
#decryption_key3=
```



```
student-03-5e86607b7c0a@cseklab-vm:~$ nano .boto
student-03-5e86607b7c0a@cseklab-vm:~$ rm setup*.html
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp gs://$BUCKET_NAME/setup.html ./
Copying gs://17it051-mann-csek/setup.html...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
student-03-5e86607b7c0a@cseklab-vm:~$ gsutil cp gs://$BUCKET_NAME/setup3.html ./
Copying gs://17it051-mann-csek/setup3.html...
/ [1 files][ 56.6 KiB/ 56.6 KiB]
Operation completed over 1 objects/56.6 KiB.
```

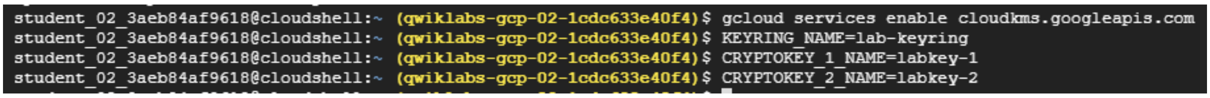
Rewriting an encrypted file causes the file to be decrypted it using the decryption_key1 that we previously set and encrypts the file with new encryption_key

8.2 Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS

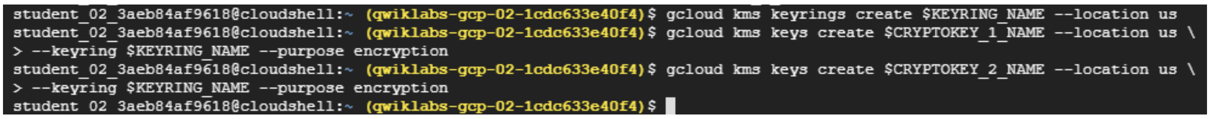


```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ echo $DEVSHELL_PROJECT_ID-kms
qwiklabs-gcp-02-1cdc633e40f4-kms
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil mb -l us gs://$DEVSHELL_PROJECT_ID-kms
Creating gs://qwiklabs-gcp-02-1cdc633e40f4-kms/...
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ echo "This is sample file 1" > file1.txt
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ echo "This is sample file 2" > file2.txt
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ echo "This is sample file 3" > file3.txt
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil cp file1.txt gs://$DEVSHELL_PROJECT_ID-kms
Copying file://file1.txt [Content-Type=text/plain]...
/ [1 files][   22.0 B/   22.0 B]
Operation completed over 1 objects/22.0 B.
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gcloud services enable cloudkms.googleapis.com
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```

Creating Cloud Storage bucket and Enabling Cloud KMS

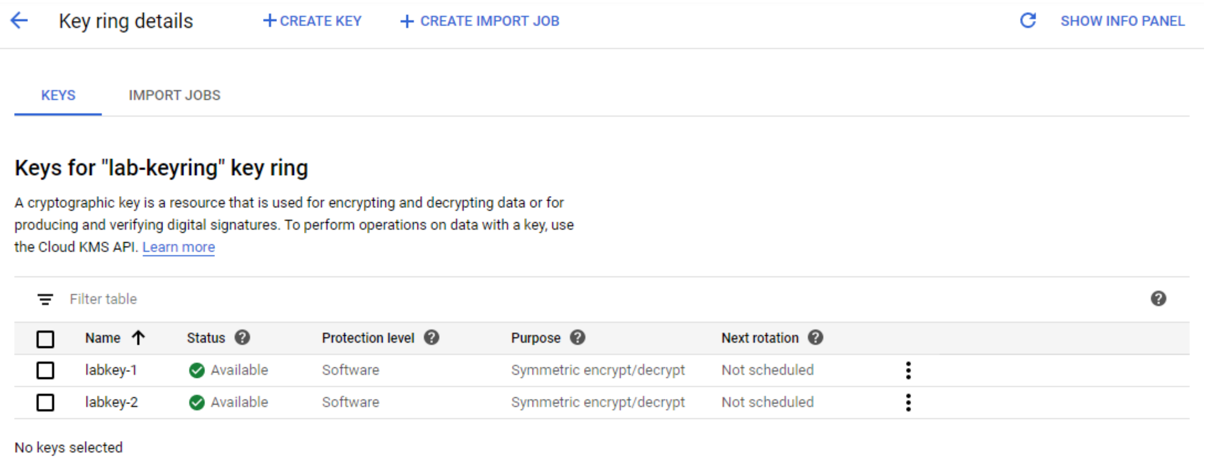


```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gcloud services enable cloudkms.googleapis.com
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ KEYRING_NAME=lab-keyring
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ CRYPTOKEY_1_NAME=labkey-1
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ CRYPTOKEY_2_NAME=labkey-2
```



```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gcloud kms keyrings create $KEYRING_NAME --location us
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gcloud kms keys create $CRYPTOKEY_1_NAME --location us \
> --keyring $KEYRING_NAME --purpose encryption
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gcloud kms keys create $CRYPTOKEY_2_NAME --location us \
> --keyring $KEYRING_NAME --purpose encryption
student 02 3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```

Creating Keyring and Cryptokey



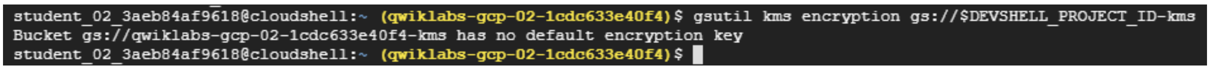
Keys for "lab-keyring" key ring

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more

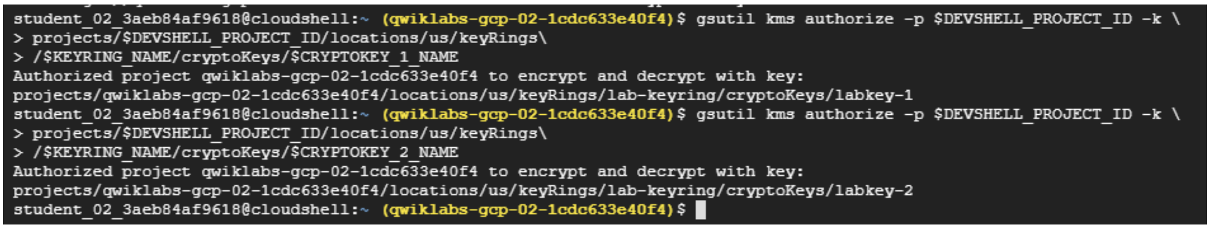
□	Name ↑	Status	Protection level	Purpose	Next rotation
□	labkey-1	✓ Available	Software	Symmetric encrypt/decrypt	Not scheduled
□	labkey-2	✓ Available	Software	Symmetric encrypt/decrypt	Not scheduled

No keys selected

Created encryption keys

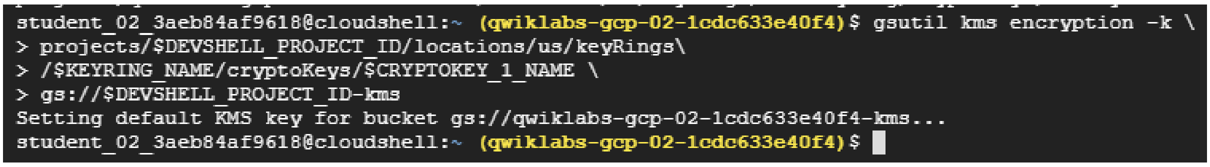


```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil kms encryption gs://$DEVSHELL_PROJECT_ID-kms
Bucket gs://qwiklabs-gcp-02-1cdc633e40f4-kms has no default encryption key
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```

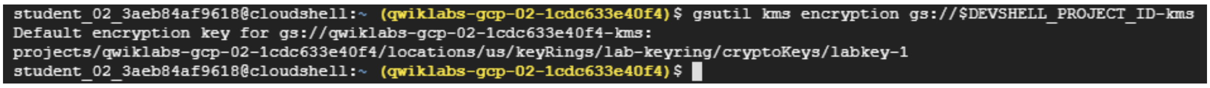


```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil kms authorize -p $DEVSHELL_PROJECT_ID -k \
> projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings\
> /$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_1_NAME
Authorized project qwiklabs-gcp-02-1cdc633e40f4 to encrypt and decrypt with key:
projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-1
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil kms authorize -p $DEVSHELL_PROJECT_ID -k \
> projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings\
> /$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_2_NAME
Authorized project qwiklabs-gcp-02-1cdc633e40f4 to encrypt and decrypt with key:
projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-2
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```

Adding default key for bucket

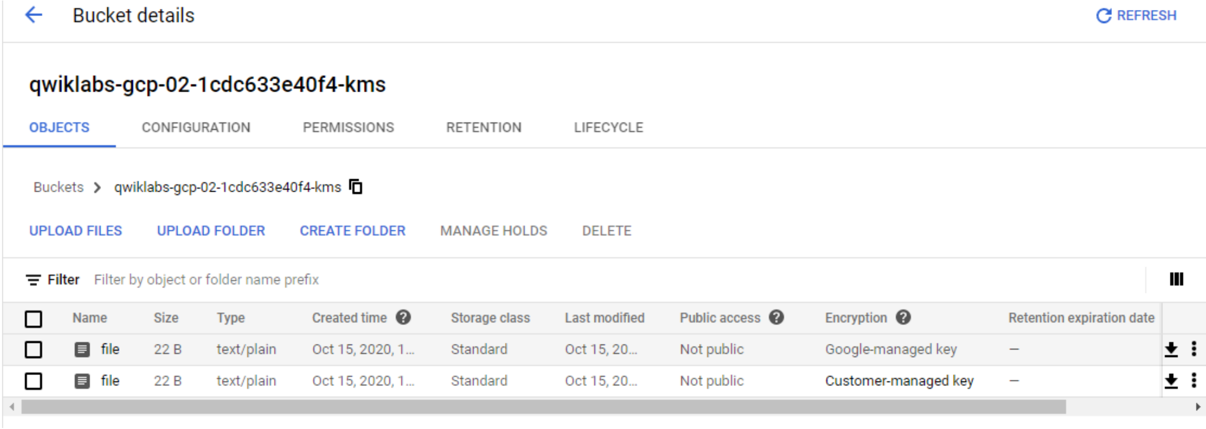


```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil kms encryption -k \
> projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings\
> /$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_1_NAME \
> gs://$DEVSHELL_PROJECT_ID-kms
Setting default KMS key for bucket gs://qwiklabs-gcp-02-1cdc633e40f4-kms...
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```



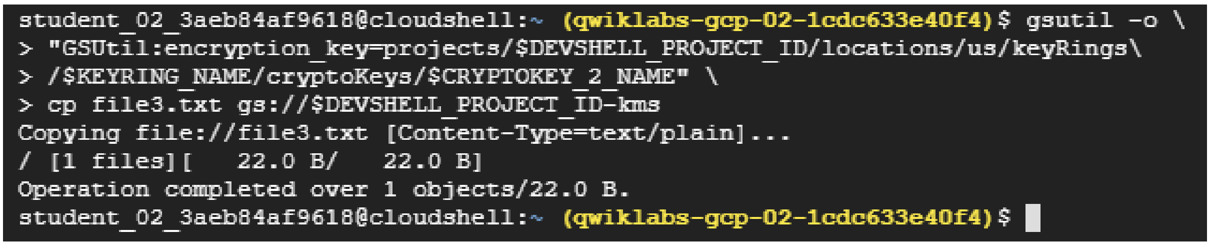
```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil kms encryption gs://$DEVSHELL_PROJECT_ID-kms
Default encryption key for gs://qwiklabs-gcp-02-1cdc633e40f4-kms:
projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-1
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```

Setting default key for a bucket



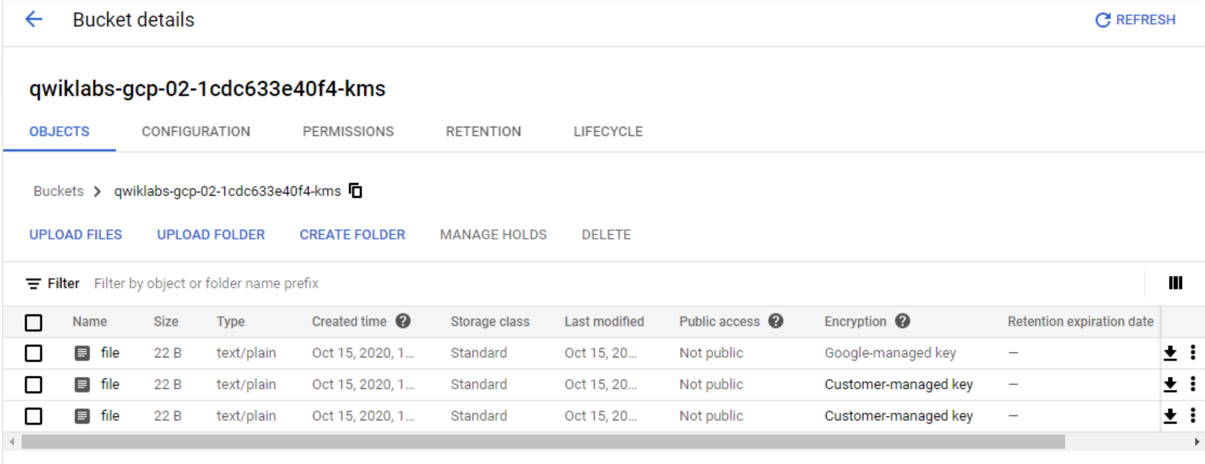
□	Name	Size	Type	Created time	Storage class	Last modified	Public access	Encryption	Retention expiration date
□	file	22 B	text/plain	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Google-managed key	–
□	file	22 B	text/plain	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Customer-managed key	–

Files



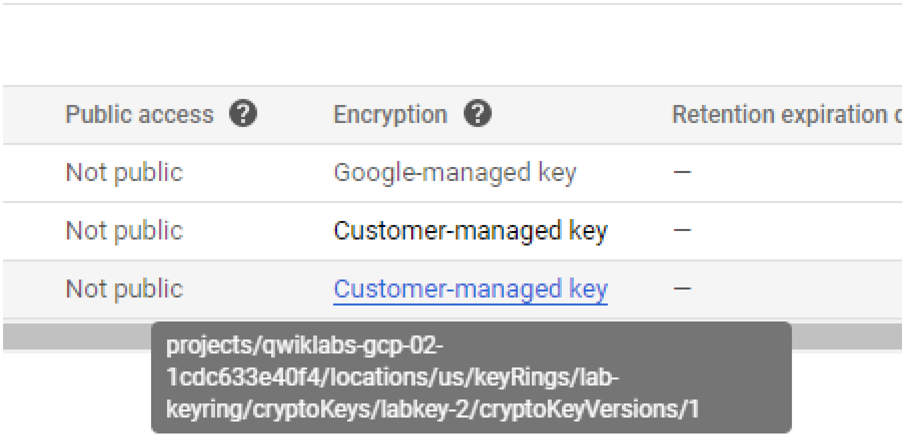
```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil -o \
> "GSUtil:encryption_key=projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings\
> /$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_2_NAME" \
> cp file3.txt gs://$DEVSHELL_PROJECT_ID-kms
Copying file://file3.txt [Content-Type=text/plain]...
/ [1 files][   22.0 B/   22.0 B]
Operation completed over 1 objects/22.0 B.
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$
```

Encrypting an object with a specific key



□	Name	Size	Type	Created time	Storage class	Last modified	Public access	Encryption	Retention expiration date
□	file	22 B	text/plain	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Google-managed key	–
□	file	22 B	text/plain	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Customer-managed key	–
□	file	22 B	text/plain	Oct 15, 2020, 1...	Standard	Oct 15, 20...	Not public	Customer-managed key	–

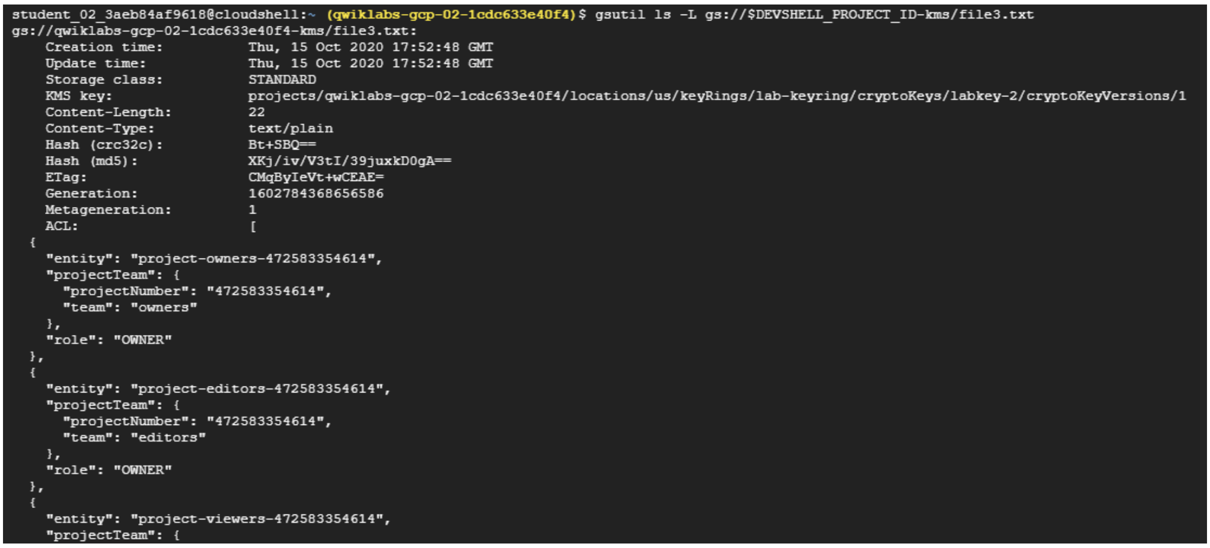
3 files are added.



Public access	Encryption	Retention expiration d
Not public	Google-managed key	—
Not public	Customer-managed key	—
Not public	Customer-managed key	—

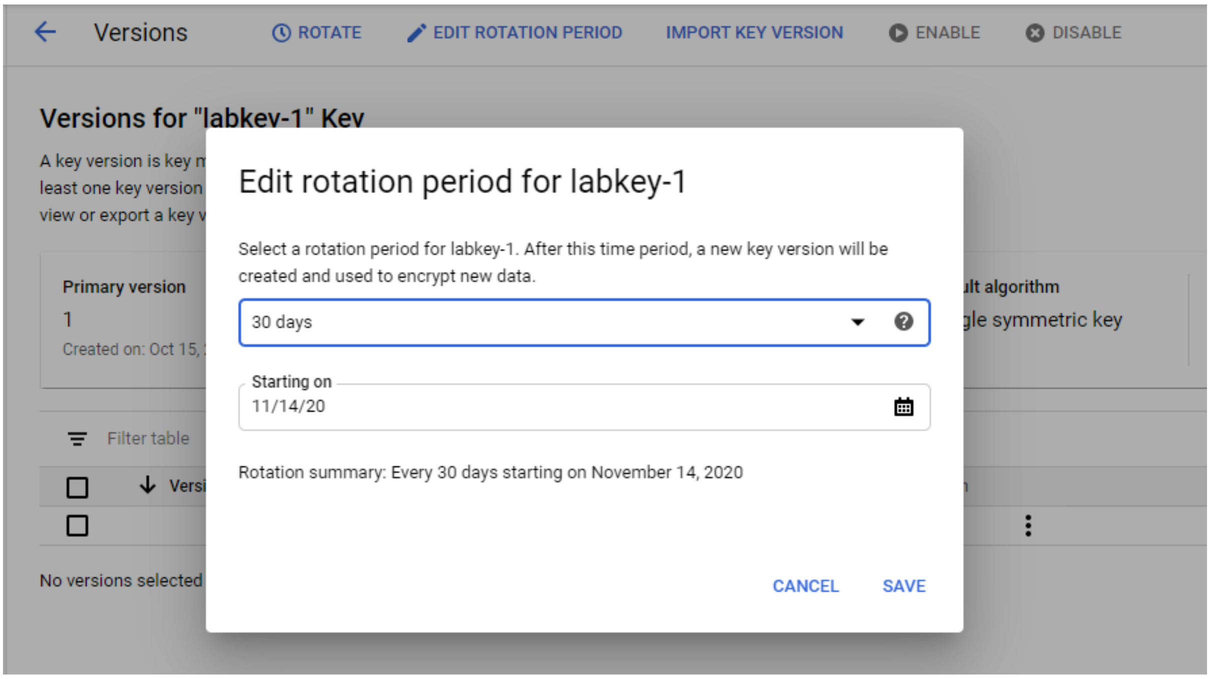
projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-2/cryptoKeyVersions/1

Observing 2 types of encryption key methods



```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil ls -L gs://$DEVSHELL_PROJECT_ID-kms/file3.txt
gs://qwiklabs-gcp-02-1cdc633e40f4-kms/file3.txt:
    Creation time:          Thu, 15 Oct 2020 17:52:48 GMT
    Update time:            Thu, 15 Oct 2020 17:52:48 GMT
    Storage class:          STANDARD
    KMS key:                projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-2/cryptoKeyVersions/1
    Content-Length:         22
    Content-Type:           text/plain
    Hash (crc32c):          Bt+SBQ==
    Hash (md5):             XKj/iv/V3tI/39juxkD0gA==
    ETag:                   CMqByIeVt+wCEAE=
    Generation:             1602784368656586
    Metageneration:         1
    ACL:                    [
  {
    "entity": "project-owners-472583354614",
    "projectTeam": {
      "projectNumber": "472583354614",
      "team": "owners"
    },
    "role": "OWNER"
  },
  {
    "entity": "project-editors-472583354614",
    "projectTeam": {
      "projectNumber": "472583354614",
      "team": "editors"
    },
    "role": "OWNER"
  },
  {
    "entity": "project-viewers-472583354614",
    "projectTeam": {
```

Identifying the key used to encrypt an object and similarly did for all files



Edit rotation period for labkey-1

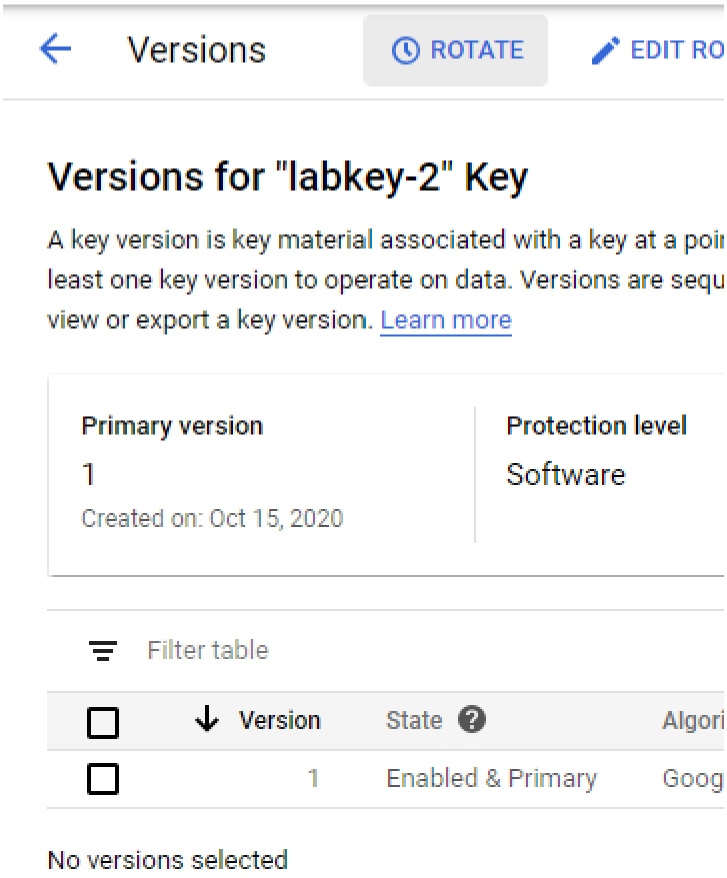
Select a rotation period for labkey-1. After this time period, a new key version will be created and used to encrypt new data.

30 days

Starting on
11/14/20

Rotation summary: Every 30 days starting on November 14, 2020

Setting Rotation period



Versions for "labkey-2" Key

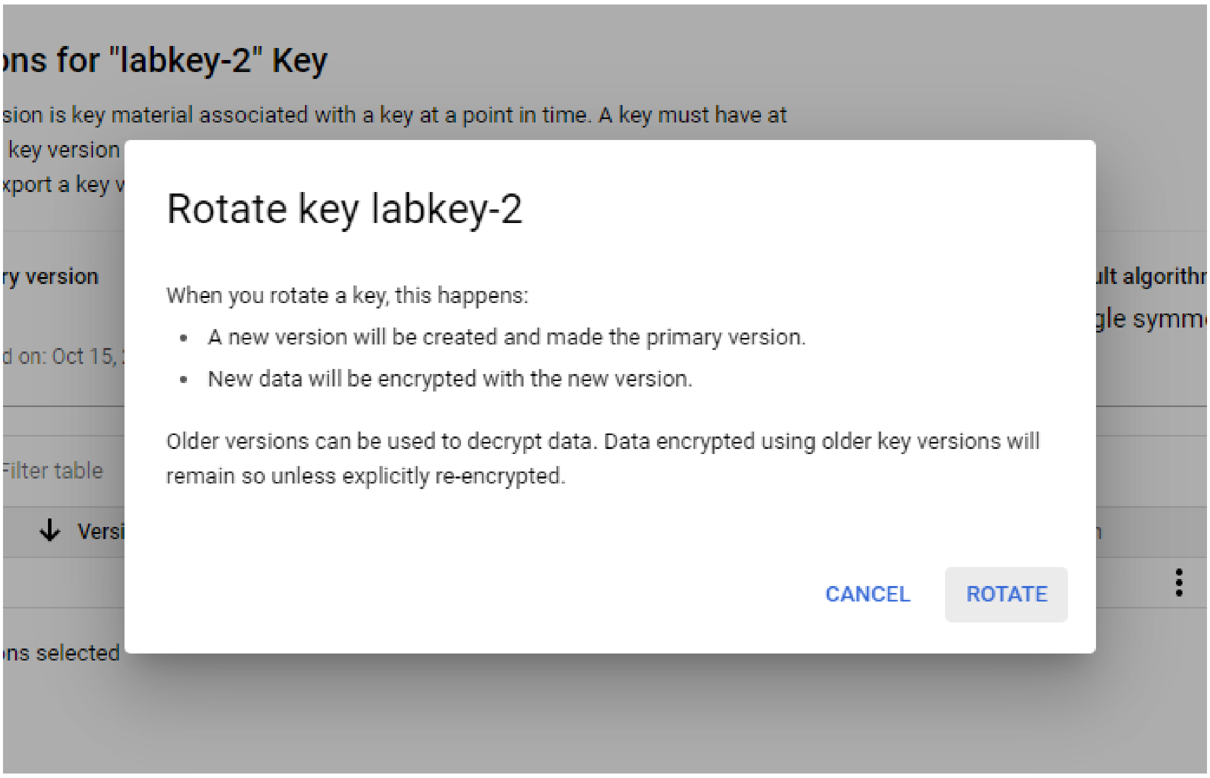
A key version is key material associated with a key at a poi
least one key version to operate on data. Versions are sequ
view or export a key version. Learn more

Primary version
1
Created on: Oct 15, 2020

Protection level
Software

□	Version	State	Algori
□	1	Enabled & Primary	Goog

No versions selected



ons for "labkey-2" Key

sion is key material associated with a key at a point in time. A key must have at key version xport a key v

ry version

d on: Oct 15, :

Filter table

ns selected

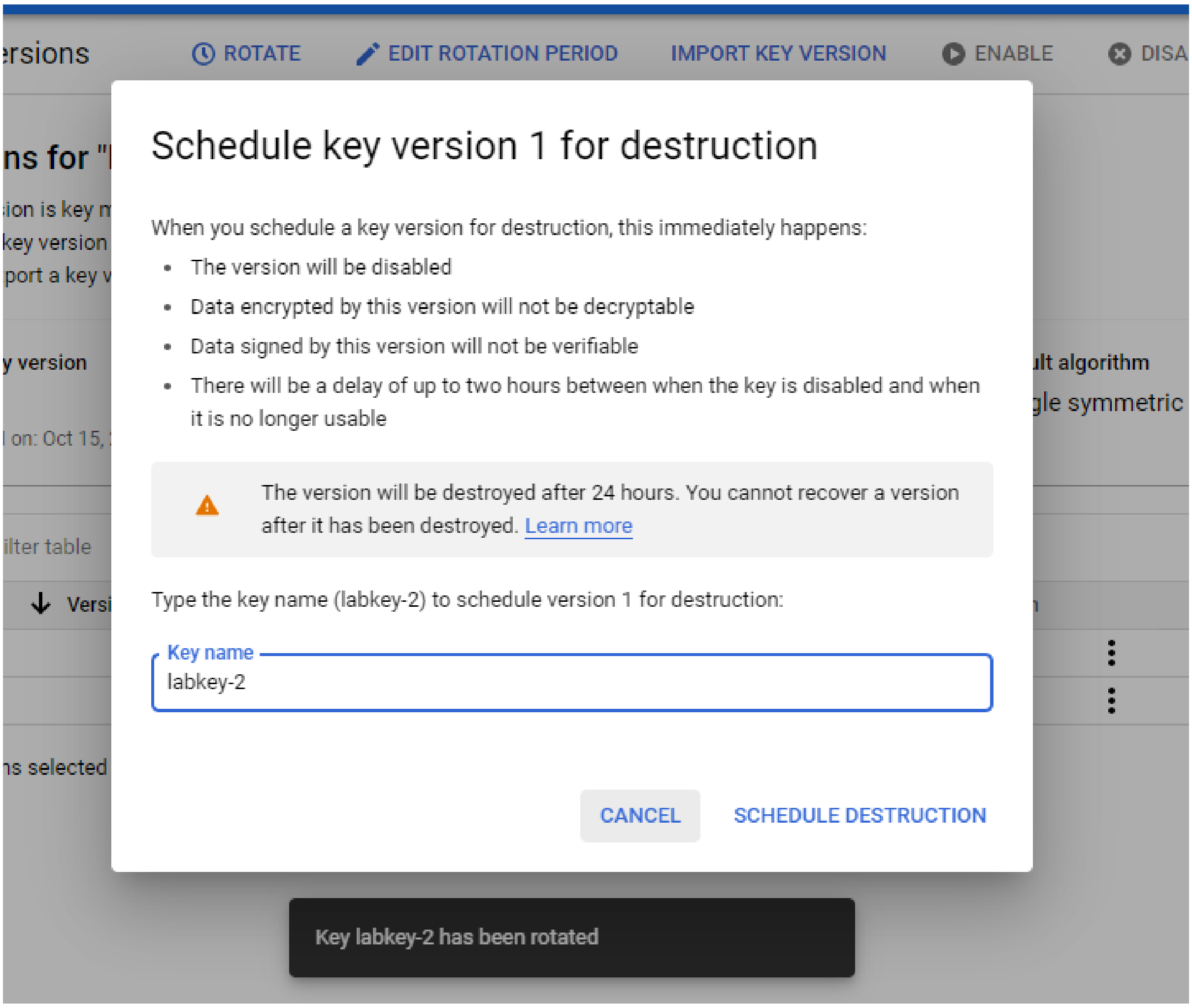
Rotate key labkey-2

When you rotate a key, this happens:

- A new version will be created and made the primary version.
- New data will be encrypted with the new version.

Older versions can be used to decrypt data. Data encrypted using older key versions will remain so unless explicitly re-encrypted.

Manually Rotating the keys



Schedule key version 1 for destruction

When you schedule a key version for destruction, this immediately happens:

- The version will be disabled
- Data encrypted by this version will not be decryptable
- Data signed by this version will not be verifiable
- There will be a delay of up to two hours between when the key is disabled and when it is no longer usable

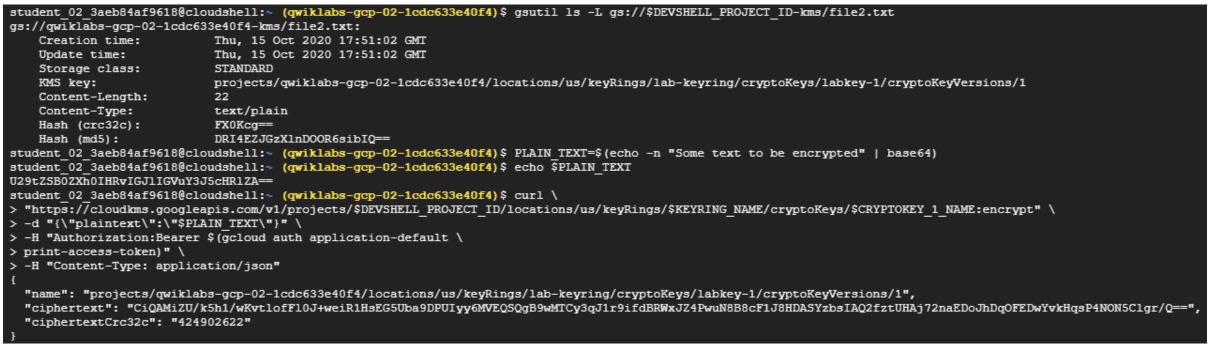
⚠ The version will be destroyed after 24 hours. You cannot recover a version after it has been destroyed. Learn more

Type the key name (labkey-2) to schedule version 1 for destruction:

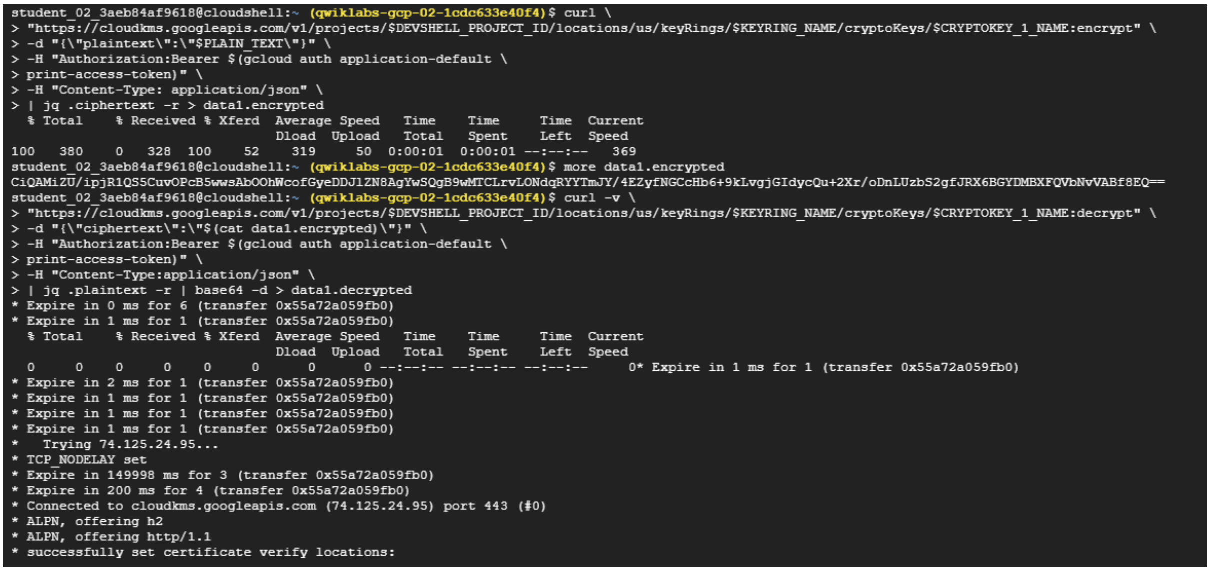
Key name: labkey-2

Key labkey-2 has been rotated

Destructing the keys

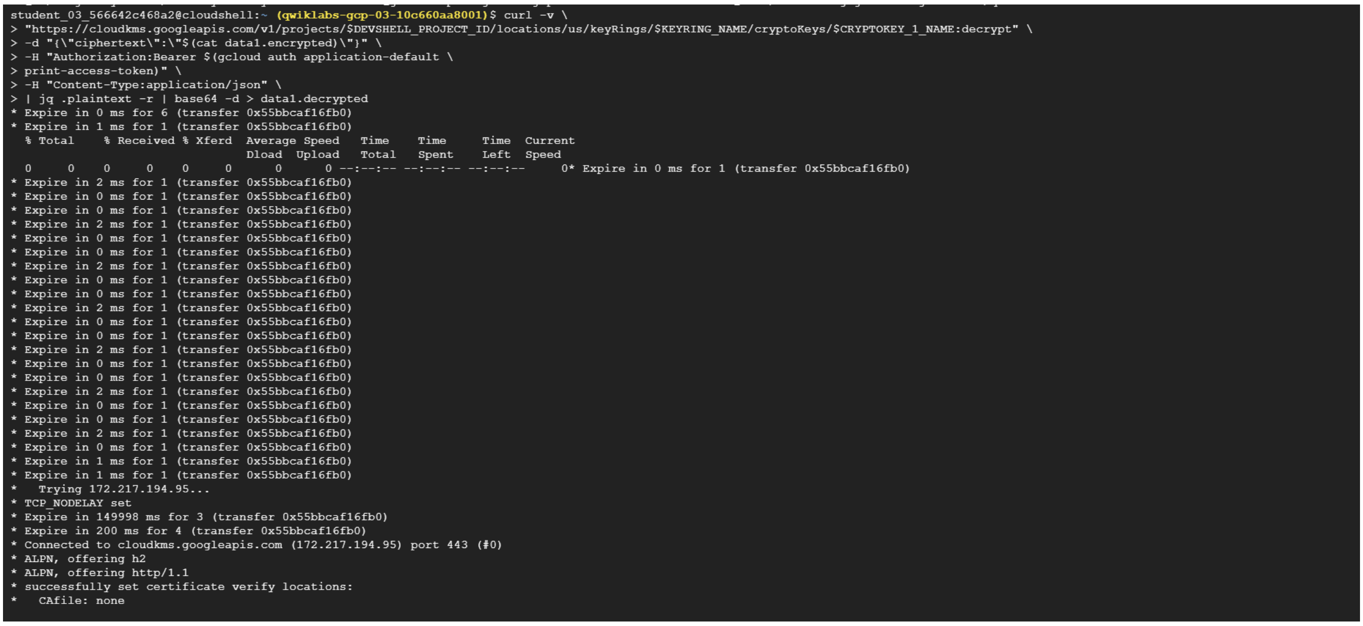


```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ gsutil ls -L gs://$DEVSHELL_PROJECT_ID-kms/file2.txt
gs://qwiklabs-gcp-02-1cdc633e40f4-kms/file2.txt:
    Creation time:          Thu, 15 Oct 2020 17:51:02 GMT
    Update time:            Thu, 15 Oct 2020 17:51:02 GMT
    Storage class:          STANDARD
    KMS key:                projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-1/cryptoKeyVersions/1
    Content-Length:         22
    Content-Type:           text/plain
    Hash (crc32c):          FX0Kcg==
    Hash (md5):             DRI4EZJGzXlnDOOR6sibIQ==
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ PLAIN_TEXT=$(echo -n "Some text to be encrypted" | base64)
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ echo $PLAIN_TEXT
U29tZSB0ZXh0IHRvIGJlIGVuY3J5cHRlZA==
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ curl \
> "https://cloudkms.googleapis.com/v1/projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings/$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_1_NAME:encrypt" \
> -d "{\"plaintext\":\"$PLAIN_TEXT\"}" \
> -H "Authorization:Bearer $(gcloud auth application-default \
> print-access-token)" \
> -H "Content-Type: application/json"
{
  "name": "projects/qwiklabs-gcp-02-1cdc633e40f4/locations/us/keyRings/lab-keyring/cryptoKeys/labkey-1/cryptoKeyVersions/1",
  "ciphertext": "CiQAMiZU/k5h1/wKvtlofFl0J+weiR1HsEG5Uba9DPUIyy6MVEQSQgB9wMTCy3qJ1r9ifdBRWxJZ4PwuN8B8cF1J8HDASYzbsIAQ2fztUHAj72naEDoJhDqOFEDwYvkHqsP4NON5Clgr/Q==",
  "ciphertextCrc32c": "424902622"
}
```



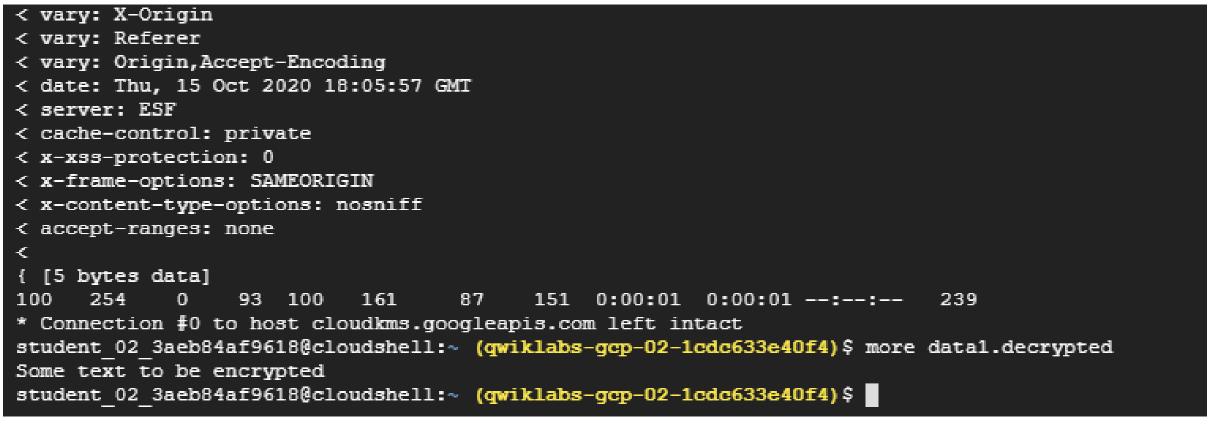
```
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ curl \
> "https://cloudkms.googleapis.com/v1/projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings/$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_1_NAME:encrypt" \
> -d "{\"plaintext\":\"$PLAIN_TEXT\"}" \
> -H "Authorization:Bearer $(gcloud auth application-default \
> print-access-token)" \
> -H "Content-Type: application/json" \
> | jq .ciphertext -r > data1.encrypted
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   380    0   328  100    52    319     50  0:00:01  0:00:01 --:--:--   369
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ more data1.encrypted
CiQAMiZU/ipjR1QS5CuvOPcB5wwsAbOOhWcofGyeDDJ1ZN8AgYwSQgB9wMTCLrvLONdqRYYTmJY/4EZyfNGCcHb6+9kLvgjGIdycQu+2Xr/oDnLUzbS2gfJRX6BGYDMBXFQVbNvVABf8EQ==
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ curl -v \
> "https://cloudkms.googleapis.com/v1/projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings/$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_1_NAME:decrypt" \
> -d "{\"ciphertext\":\"$(cat data1.encrypted)\"}" \
> -H "Authorization:Bearer $(gcloud auth application-default \
> print-access-token)" \
> -H "Content-Type:application/json" \
> | jq .plaintext -r | base64 -d > data1.decrypted
* Expire in 0 ms for 6 (transfer 0x55a72a059fb0)
* Expire in 1 ms for 1 (transfer 0x55a72a059fb0)
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0* Expire in 1 ms for 1 (transfer 0x55a72a059fb0)
* Expire in 2 ms for 1 (transfer 0x55a72a059fb0)
* Expire in 1 ms for 1 (transfer 0x55a72a059fb0)
* Expire in 1 ms for 1 (transfer 0x55a72a059fb0)
* Expire in 1 ms for 1 (transfer 0x55a72a059fb0)
*   Trying 74.125.24.95...
* TCP_NODELAY set
* Expire in 149998 ms for 3 (transfer 0x55a72a059fb0)
* Expire in 200 ms for 4 (transfer 0x55a72a059fb0)
* Connected to cloudkms.googleapis.com (74.125.24.95) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
```

Encrypting data with REST API



```
student_03_566642c468a2@cloudshell:~ (qwiklabs-gcp-03-10c660aa8001)$ curl -v \
> "https://cloudkms.googleapis.com/v1/projects/$DEVSHELL_PROJECT_ID/locations/us/keyRings/$KEYRING_NAME/cryptoKeys/$CRYPTOKEY_1_NAME:decrypt" \
> -d "{\"ciphertext\":\"$(cat data1.encrypted)\"}" \
> -H "Authorization:Bearer $(gcloud auth application-default \
> print-access-token)" \
> -H "Content-Type:application/json" \
> | jq .plaintext -r | base64 -d > data1.decrypted
* Expire in 0 ms for 6 (transfer 0x55bbcaf16fb0)
* Expire in 1 ms for 1 (transfer 0x55bbcaf16fb0)
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 2 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 0 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 1 ms for 1 (transfer 0x55bbcaf16fb0)
* Expire in 1 ms for 1 (transfer 0x55bbcaf16fb0)
*   Trying 172.217.194.95...
* TCP_NODELAY set
* Expire in 149998 ms for 3 (transfer 0x55bbcaf16fb0)
* Expire in 200 ms for 4 (transfer 0x55bbcaf16fb0)
* Connected to cloudkms.googleapis.com (172.217.194.95) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: none
```

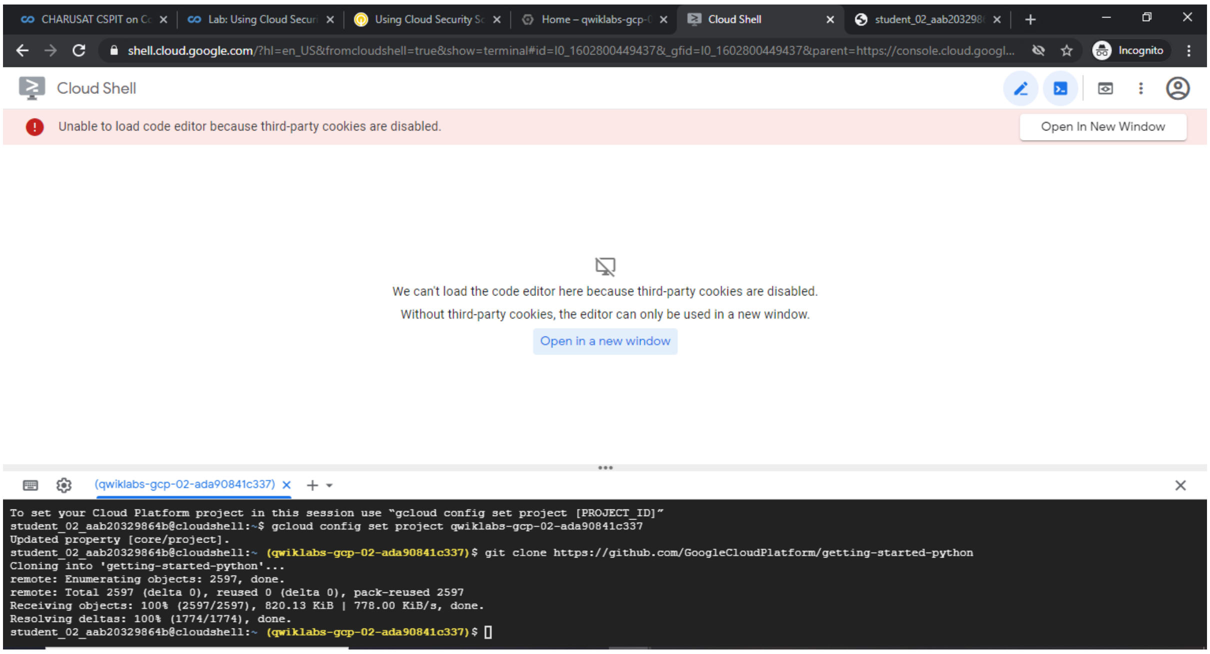
Decrypting the data



```
< vary: X-Origin
< vary: Referer
< vary: Origin,Accept-Encoding
< date: Thu, 15 Oct 2020 18:05:57 GMT
< server: ESF
< cache-control: private
< x-xss-protection: 0
< x-frame-options: SAMEORIGIN
< x-content-type-options: nosniff
< accept-ranges: none
<
{ [5 bytes data]
100   254    0    93  100   161     87    151  0:00:01  0:00:01 --:--:--   239
* Connection #0 to host cloudkms.googleapis.com left intact
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ more data1.decrypted
Some text to be encrypted
student_02_3aeb84af9618@cloudshell:~ (qwiklabs-gcp-02-1cdc633e40f4)$ █
```

Observing decrypted data

8.3 Using Cloud Security Scanner to find vulnerabilities in an App Engine application

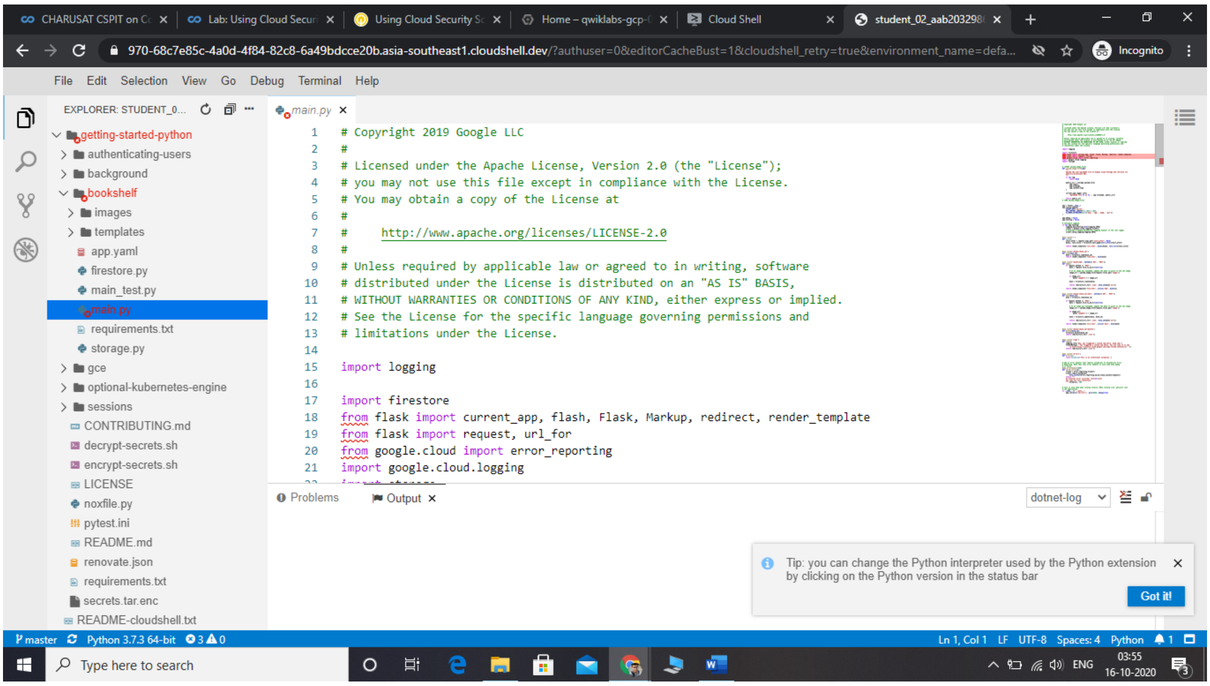


Unable to load code editor because third-party cookies are disabled.

We can't load the code editor here because third-party cookies are disabled.
Without third-party cookies, the editor can only be used in a new window.

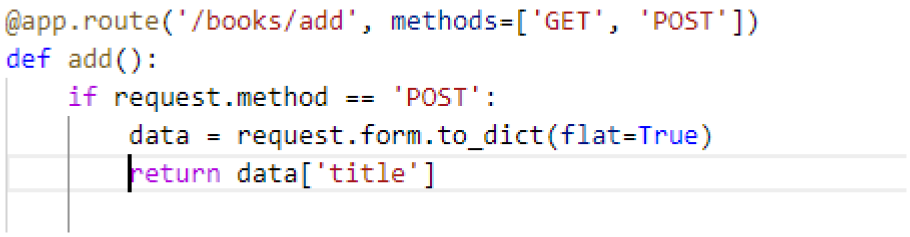
```
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
student_02_aab20329864b@cloudshell:~$ gcloud config set project qwiklabs-gcp-02-ada90841c337
Updated property [core/project].
student_02_aab20329864b@cloudshell:~ (qwiklabs-gcp-02-ada90841c337)$ git clone https://github.com/GoogleCloudPlatform/getting-started-python
Cloning into 'getting-started-python'...
remote: Enumerating objects: 2597, done.
remote: Total 2597 (delta 0), reused 0 (delta 0), pack-reused 2597
Receiving objects: 100% (2597/2597), 820.13 KiB | 778.00 KiB/s, done.
Resolving deltas: 100% (1774/1774), done.
student_02_aab20329864b@cloudshell:~ (qwiklabs-gcp-02-ada90841c337)$
```

Getting the sample app



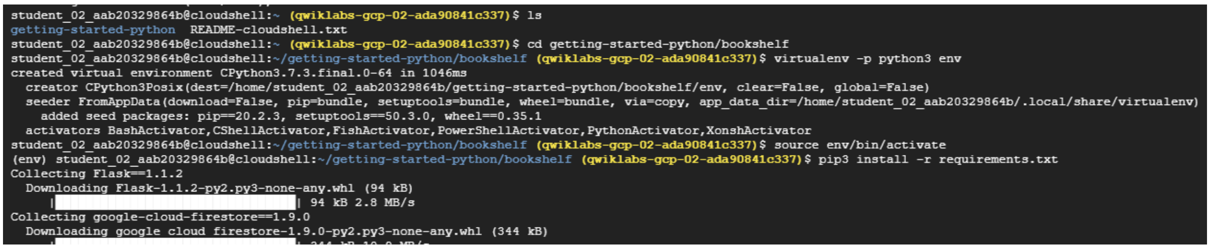
```python
# Copyright 2019 Google LLC
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.

import logging

import firestore
from flask import current_app, flash, Flask, Markup, redirect, render_template
from flask import request, url_for
from google.cloud import error_reporting
import google.cloud.logging
```

Tip: you can change the Python interpreter used by the Python extension by clicking on the Python version in the status bar



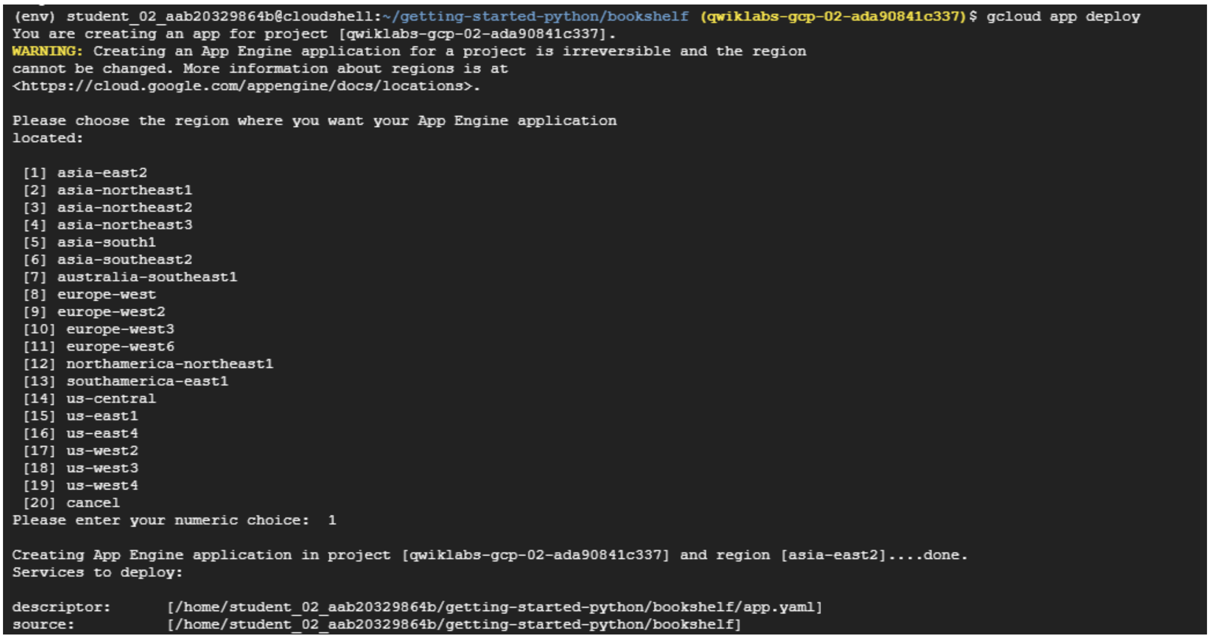
```
@app.route('/books/add', methods=['GET', 'POST'])
def add():
    if request.method == 'POST':
        data = request.form.to_dict(flat=True)
        return data['title']
```

Adding this line to make site vulnerable using code editor



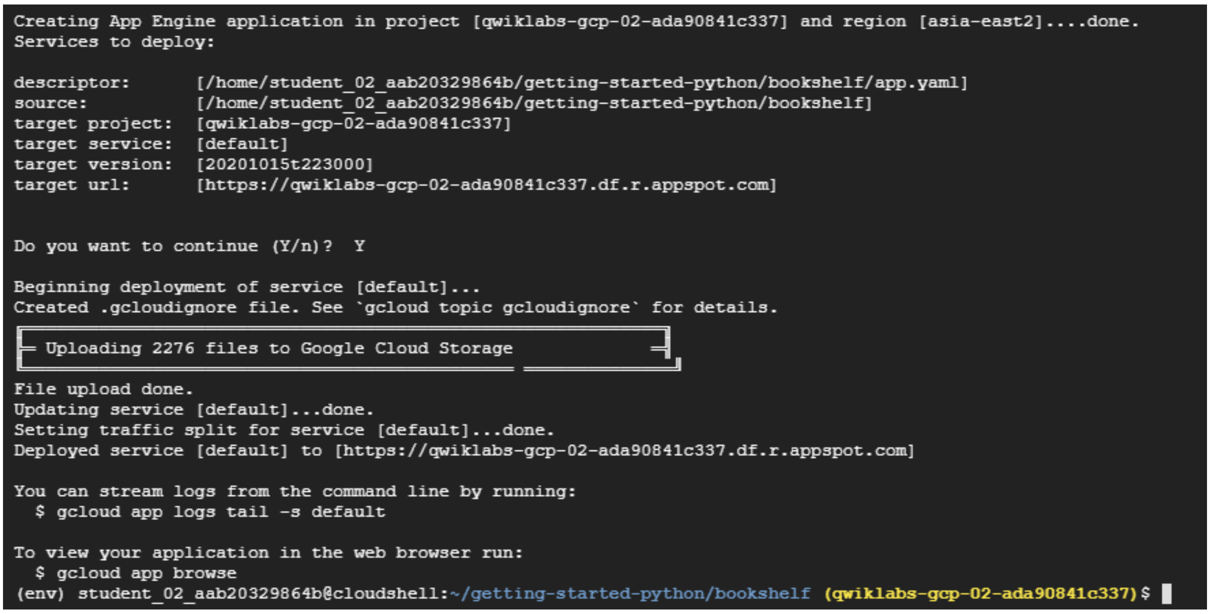
```
student_02_aab20329864b@cloudshell:~ (qwiklabs-gcp-02-ada90841c337)$ ls
getting-started-python  README-cloudshell.txt
student_02_aab20329864b@cloudshell:~ (qwiklabs-gcp-02-ada90841c337)$ cd getting-started-python/bookshelf
student_02_aab20329864b@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-ada90841c337)$ virtualenv -p python3 env
created virtual environment CPython3.7.3.final.0-64 in 1046ms
  creator CPython3Posix(dest=/home/student_02_aab20329864b/getting-started-python/bookshelf/env, clear=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/student_02_aab20329864b/.local/share/virtualenv)
    added seed packages: pip==20.2.3, setuptools==50.3.0, wheel==0.35.1
  activators BashActivator,CShellActivator,FishActivator,PowerShellActivator,PythonActivator,XonshActivator
student_02_aab20329864b@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-ada90841c337)$ source env/bin/activate
(env) student_02_aab20329864b@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-ada90841c337)$ pip3 install -r requirements.txt
Collecting Flask==1.1.2
  Downloading Flask-1.1.2-py2.py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 2.8 MB/s
Collecting google-cloud-firestore==1.9.0
  Downloading google_cloud_firestore-1.9.0-py2.py3-none-any.whl (344 kB)
```

Deploying an app engine application by installing all the necessary modules



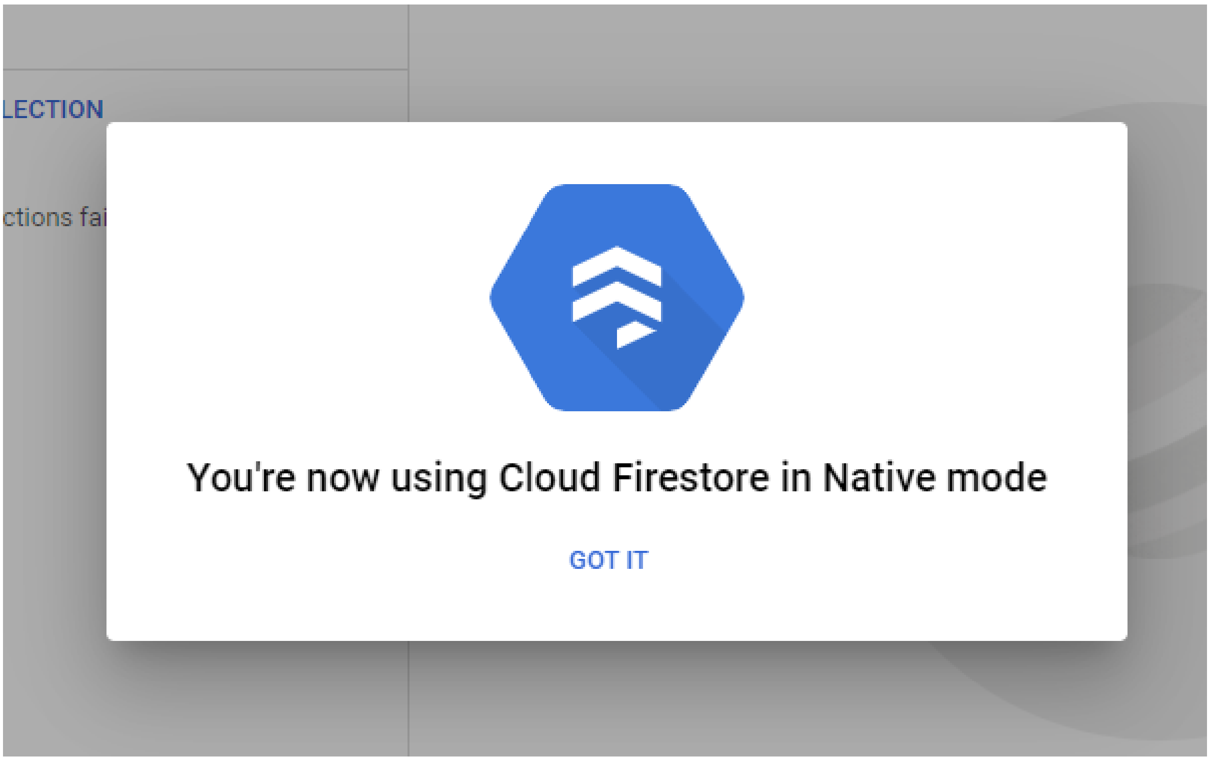
```
(env) student_02_aab20329864b@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-ada90841c337)$ gcloud app deploy
You are creating an app for project [qwiklabs-gcp-02-ada90841c337].
WARNING: Creating an App Engine application for a project is irreversible and the region
cannot be changed. More information about regions is at
<https://cloud.google.com/appengine/docs/locations>.

Please choose the region where you want your App Engine application
located:

 [1] asia-east2
 [2] asia-northeast1
 [3] asia-northeast2
 [4] asia-northeast3
 [5] asia-south1
 [6] asia-southeast2
 [7] australia-southeast1
 [8] europe-west
 [9] europe-west2
 [10] europe-west3
 [11] europe-west6
 [12] northamerica-northeast1
 [13] southamerica-east1
 [14] us-central
 [15] us-east1
 [16] us-east4
 [17] us-west2
 [18] us-west3
 [19] us-west4
 [20] cancel
Please enter your numeric choice:  1

Creating App Engine application in project [qwiklabs-gcp-02-ada90841c337] and region [asia-east2]....done.
Services to deploy:

descriptor:      [/home/student_02_aab20329864b/getting-started-python/bookshelf/app.yaml]
source:          [/home/student_02_aab20329864b/getting-started-python/bookshelf]
```

Deploying app

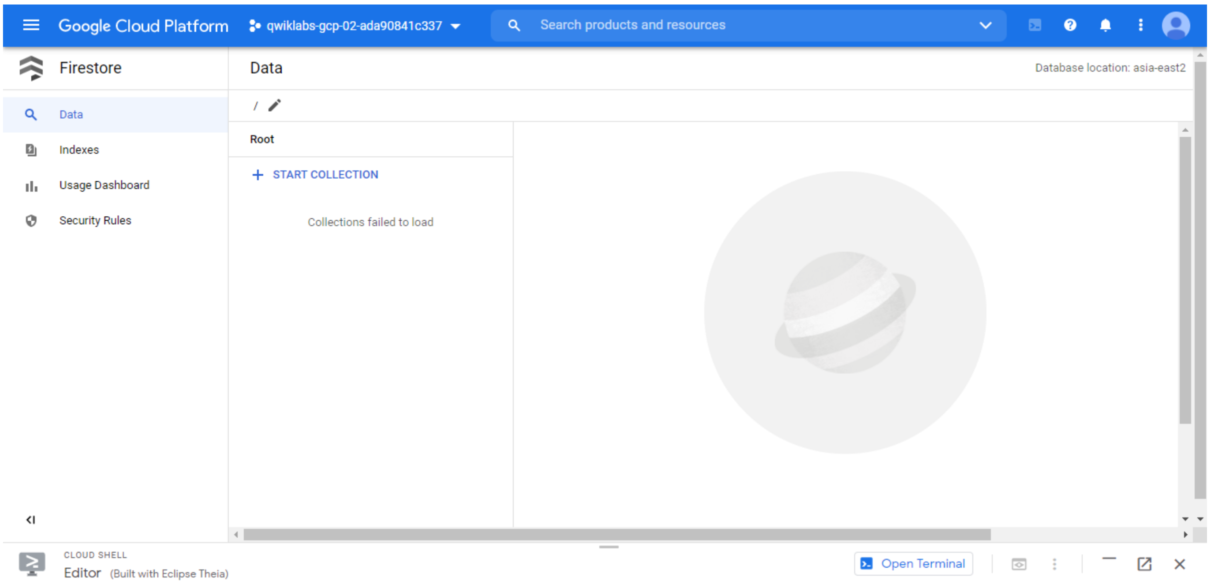


```
Creating App Engine application in project [qwiklabs-gcp-02-ada90841c337] and region [asia-east2]....done.
Services to deploy:

descriptor:      [/home/student_02_aab20329864b/getting-started-python/bookshelf/app.yaml]
source:          [/home/student_02_aab20329864b/getting-started-python/bookshelf]
target project:  [qwiklabs-gcp-02-ada90841c337]
target service:  [default]
target version:  [20201015t223000]
target url:      [https://qwiklabs-gcp-02-ada90841c337.df.r.appspot.com]


Do you want to continue (Y/n)?  Y

Beginning deployment of service [default]...
Created .gcloudignore file. See `gcloud topic gcloudignore` for details.
╔════════════════════════════════════════════════════════════╗
╠═ Uploading 2276 files to Google Cloud Storage             ═╣
╚════════════════════════════════════════════════════════════╝
File upload done.
Updating service [default]...done.
Setting traffic split for service [default]...done.
Deployed service [default] to [https://qwiklabs-gcp-02-ada90841c337.df.r.appspot.com]

You can stream logs from the command line by running:
  $ gcloud app logs tail -s default

To view your application in the web browser run:
  $ gcloud app browse
(env) student_02_aab20329864b@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-ada90841c337)$
```

Deploying the app after adding database



You're now using Cloud Firestore in Native mode



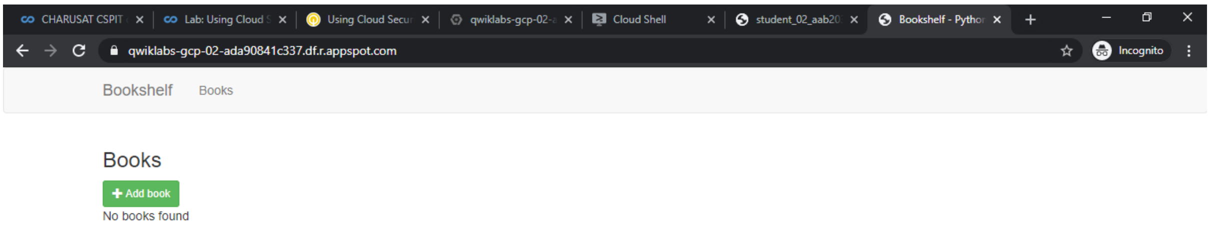
Data

Database location: asia-east2

Root

Collections failed to load

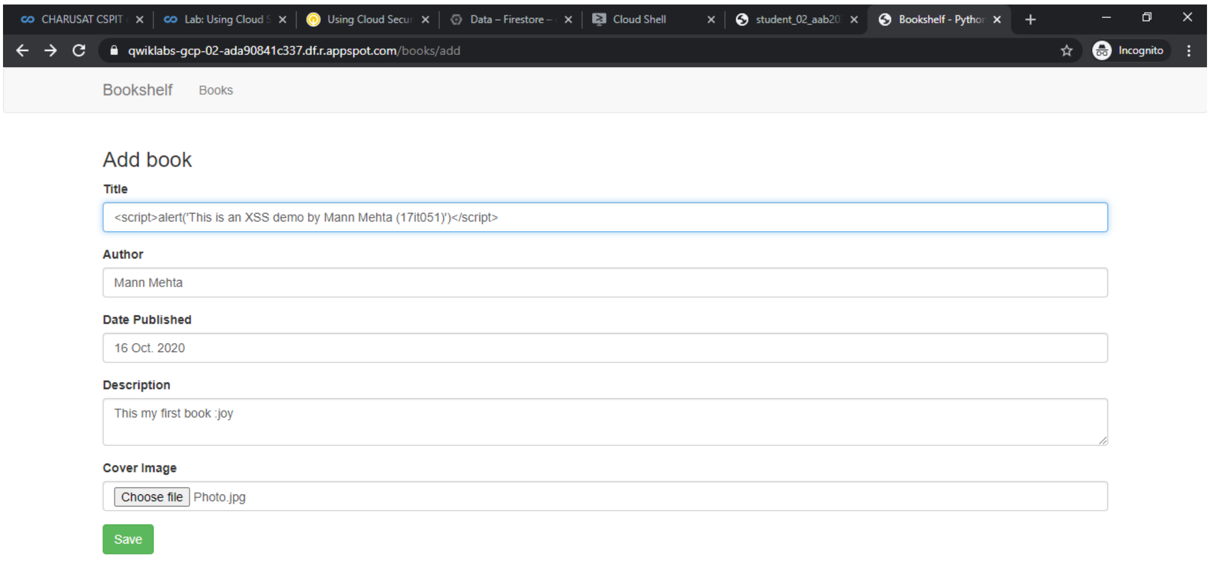
Swithcing to cloud firestore store native mode.



qwiklabs-gcp-02-ada90841c337.df.r.appspot.com

Books

No books found



qwiklabs-gcp-02-ada90841c337.df.r.appspot.com/books/add

Add book

Title: <script>alert('This is an XSS demo by Mann Mehta (17it051)')</script>

Author: Mann Mehta

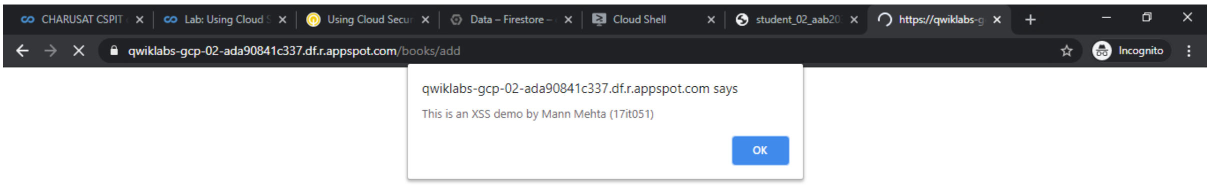
Date Published: 16 Oct. 2020

Description: This my first book :joy

Cover Image: Choose file Photo.jpg

Save

App Engine application deployed successfully and been able to view it

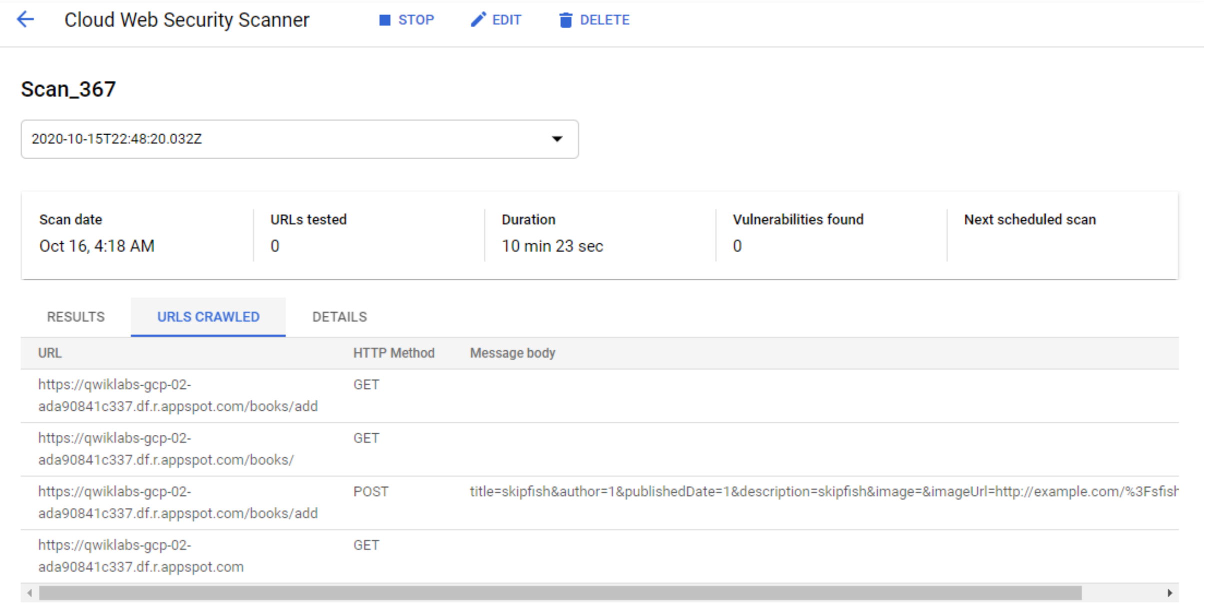


qwiklabs-gcp-02-ada90841c337.df.r.appspot.com/books/add

qwiklabs-gcp-02-ada90841c337.df.r.appspot.com says

This is an XSS demo by Mann Mehta (17it051)

Site is vulnerable to XSS



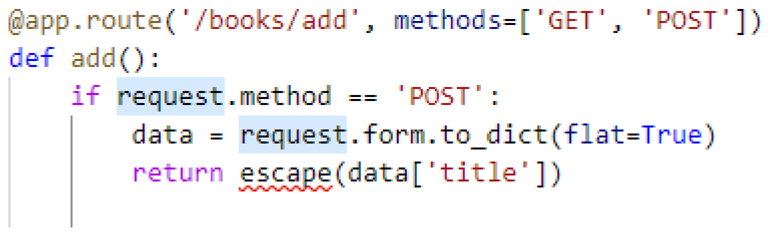
Scan_367

2020-10-15T22:48:20.032Z

Scan date	URLs tested	Duration	Vulnerabilities found	Next scheduled scan
Oct 16, 4:18 AM	0	10 min 23 sec	0	

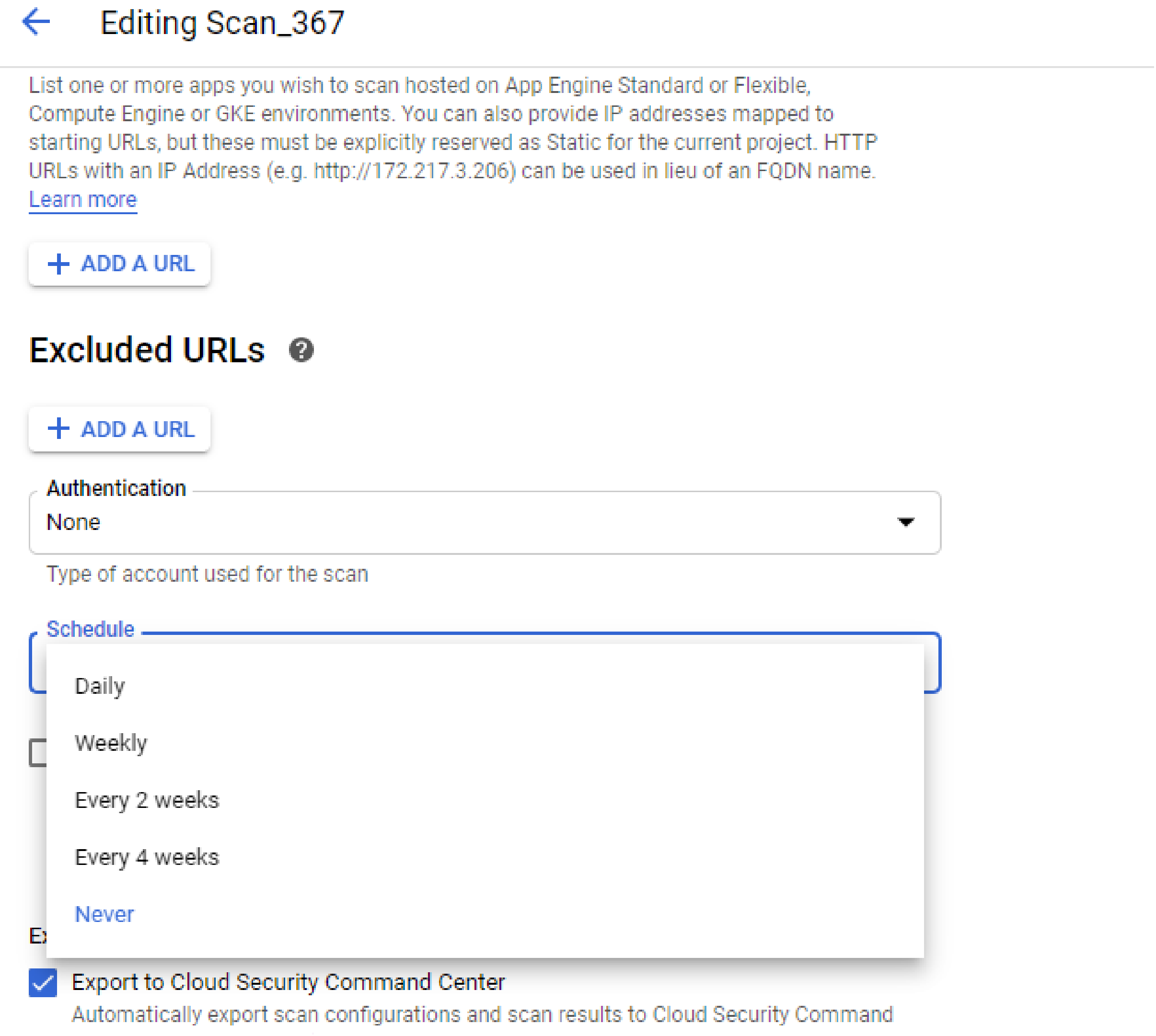
URL	HTTP Method	Message body
https://qwiklabs-gcp-02-ada90841c337.df.r.appspot.com/books/add	GET	
https://qwiklabs-gcp-02-ada90841c337.df.r.appspot.com/books/	GET	
https://qwiklabs-gcp-02-ada90841c337.df.r.appspot.com/books/add	POST	title=skipfish&author=1&publishedDate=1&description=skipfish&image=&imageUrl=http://example.com/%3Fsfish
https://qwiklabs-gcp-02-ada90841c337.df.r.appspot.com	GET	

Observing vulnerabilities and crawled urls



```
@app.route('/books/add', methods=['GET', 'POST'])
def add():
    if request.method == 'POST':
        data = request.form.to_dict(flat=True)
        return escape(data['title'])
```

Correcting the vulnerability in the application



Editing Scan_367

List one or more apps you wish to scan hosted on App Engine Standard or Flexible, Compute Engine or GKE environments. You can also provide IP addresses mapped to starting URLs, but these must be explicitly reserved as Static for the current project. HTTP URLs with an IP Address (e.g. http://172.217.3.206) can be used in lieu of an FQDN name. Learn more

Excluded URLs

Authentication: None

Type of account used for the scan

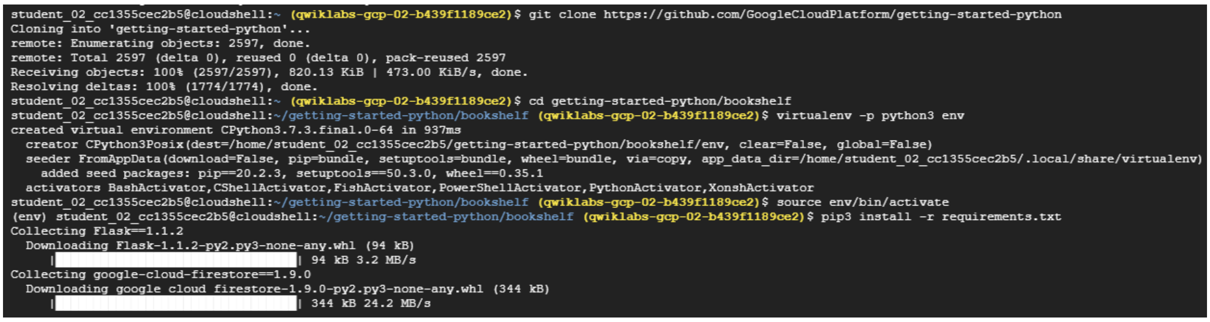
Schedule

☑ Export to Cloud Security Command Center

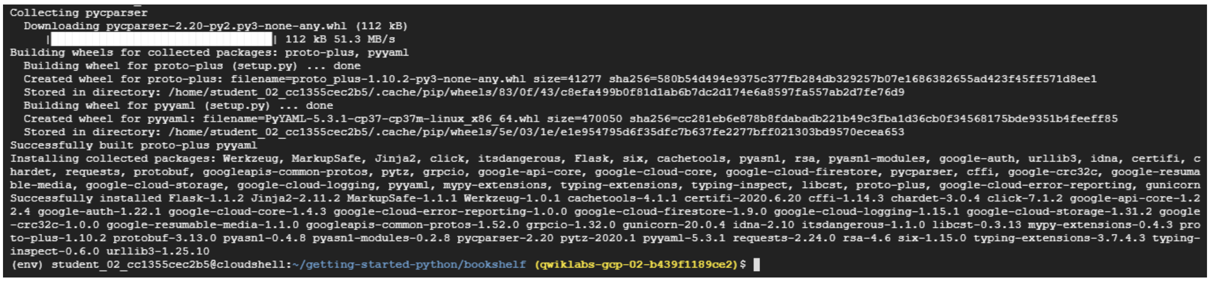
Automatically export scan configurations and scan results to Cloud Security Command

Scheduling the scans

8.4 Configuring Identity Aware Proxy to Protect a Project

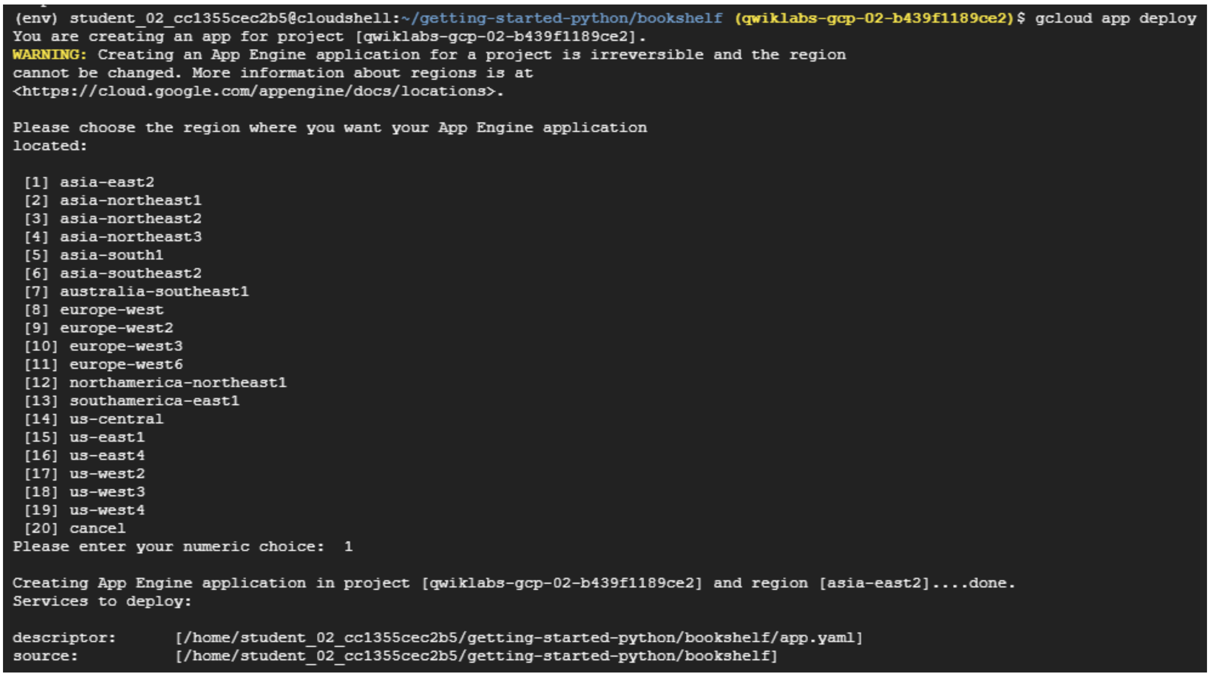


```
student_02_cc1355cec2b5@cloudshell:~ (qwiklabs-gcp-02-b439f1189ce2)$ git clone https://github.com/GoogleCloudPlatform/getting-started-python
Cloning into 'getting-started-python'...
remote: Enumerating objects: 2597, done.
remote: Total 2597 (delta 0), reused 0 (delta 0), pack-reused 2597
Receiving objects: 100% (2597/2597), 820.13 KiB | 473.00 KiB/s, done.
Resolving deltas: 100% (1774/1774), done.
student_02_cc1355cec2b5@cloudshell:~ (qwiklabs-gcp-02-b439f1189ce2)$ cd getting-started-python/bookshelf
student_02_cc1355cec2b5@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-b439f1189ce2)$ virtualenv -p python3 env
created virtual environment CPython3.7.3.final.0-64 in 937ms
  creator CPython3Posix(dest=/home/student_02_cc1355cec2b5/getting-started-python/bookshelf/env, clear=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/student_02_cc1355cec2b5/.local/share/virtualenv)
    added seed packages: pip==20.2.3, setuptools==50.3.0, wheel==0.35.1
  activators BashActivator,CShellActivator,FishActivator,PowerShellActivator,PythonActivator,XonshActivator
student_02_cc1355cec2b5@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-b439f1189ce2)$ source env/bin/activate
(env) student_02_cc1355cec2b5@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-b439f1189ce2)$ pip3 install -r requirements.txt
Collecting Flask==1.1.2
  Downloading Flask-1.1.2-py2.py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 3.2 MB/s
Collecting google-cloud-firestore==1.9.0
  Downloading google_cloud_firestore-1.9.0-py2.py3-none-any.whl (344 kB)
     |████████████████████████████████| 344 kB 24.2 MB/s
```

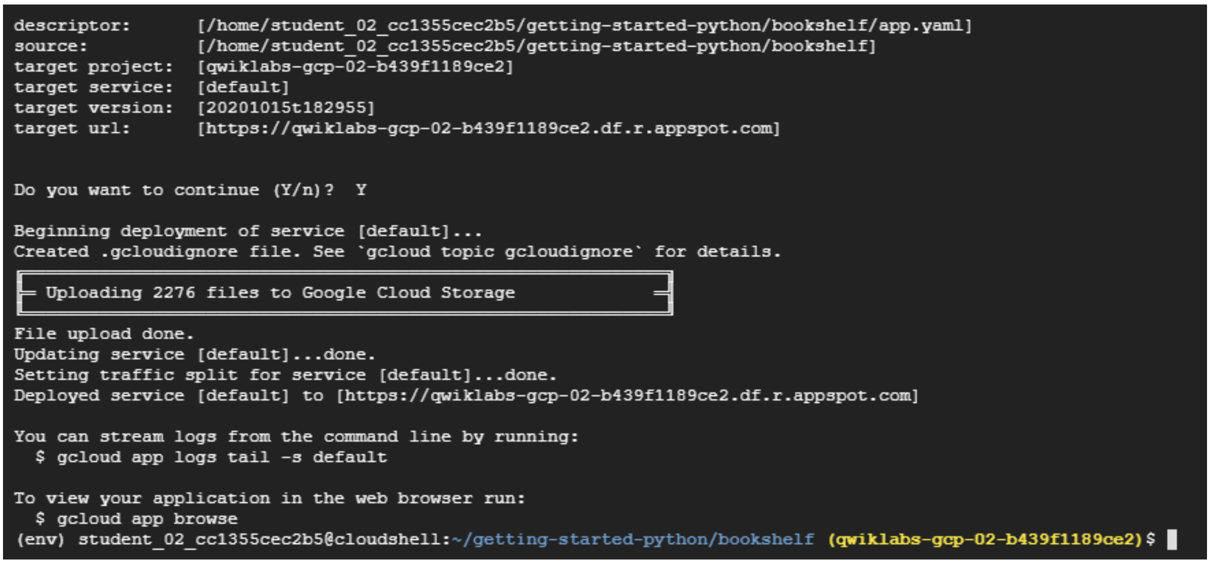


```
Collecting pycparser
  Downloading pycparser-2.20-py2.py3-none-any.whl (112 kB)
     |████████████████████████████████| 112 kB 51.3 MB/s
Building wheels for collected packages: proto-plus, pyyaml
  Building wheel for proto-plus (setup.py) ... done
  Created wheel for proto-plus: filename=proto_plus-1.10.2-py3-none-any.whl size=41277 sha256=580b54d494e9375c377fb284db329257b07e1686382655ad423f45ff571d8ee1
  Stored in directory: /home/student_02_cc1355cec2b5/.cache/pip/wheels/83/0f/43/c8efa499b0f81d1ab6b7dc2d174e6a8597fa557ab2d7fe76d9
  Building wheel for pyyaml (setup.py) ... done
  Created wheel for pyyaml: filename=PyYAML-5.3.1-cp37-cp37m-linux_x86_64.whl size=470050 sha256=cc281eb6e878b8fdabadb221b49c3fba1d36cb0f34568175bde9351b4feeff85
  Stored in directory: /home/student_02_cc1355cec2b5/.cache/pip/wheels/5e/03/1e/e1e954795d6f35dfc7b637fe2277bff021303bd9570ecea653
Successfully built proto-plus pyyaml
Installing collected packages: Werkzeug, MarkupSafe, Jinja2, click, itsdangerous, Flask, six, cachetools, pyasn1, rsa, pyasn1-modules, google-auth, urllib3, idna, certifi, c
hardet, requests, protobuf, googleapis-common-protos, pytz, grpcio, google-api-core, google-cloud-core, google-cloud-firestore, pycparser, cffi, google-crc32c, google-resuma
ble-media, google-cloud-storage, google-cloud-logging, pyyaml, mypy-extensions, typing-extensions, typing-inspect, libcst, proto-plus, google-cloud-error-reporting, gunicorn
Successfully installed Flask-1.1.2 Jinja2-2.11.2 MarkupSafe-1.1.1 Werkzeug-1.0.1 cachetools-4.1.1 certifi-2020.6.20 cffi-1.14.3 chardet-3.0.4 click-7.1.2 google-api-core-1.2
2.4 google-auth-1.22.1 google-cloud-core-1.4.3 google-cloud-error-reporting-1.0.0 google-cloud-firestore-1.9.0 google-cloud-logging-1.15.1 google-cloud-storage-1.31.2 google
-crc32c-1.0.0 google-resumable-media-1.1.0 googleapis-common-protos-1.52.0 grpcio-1.32.0 gunicorn-20.0.4 idna-2.10 itsdangerous-1.1.0 libcst-0.3.13 mypy-extensions-0.4.3 pro
to-plus-1.10.2 protobuf-3.13.0 pyasn1-0.4.8 pyasn1-modules-0.2.8 pycparser-2.20 pytz-2020.1 pyyaml-5.3.1 requests-2.24.0 rsa-4.6 six-1.15.0 typing-extensions-3.7.4.3 typing-
inspect-0.6.0 urllib3-1.25.10
(env) student_02_cc1355cec2b5@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-b439f1189ce2)$ █
```

Cloning the application and installing the requirements

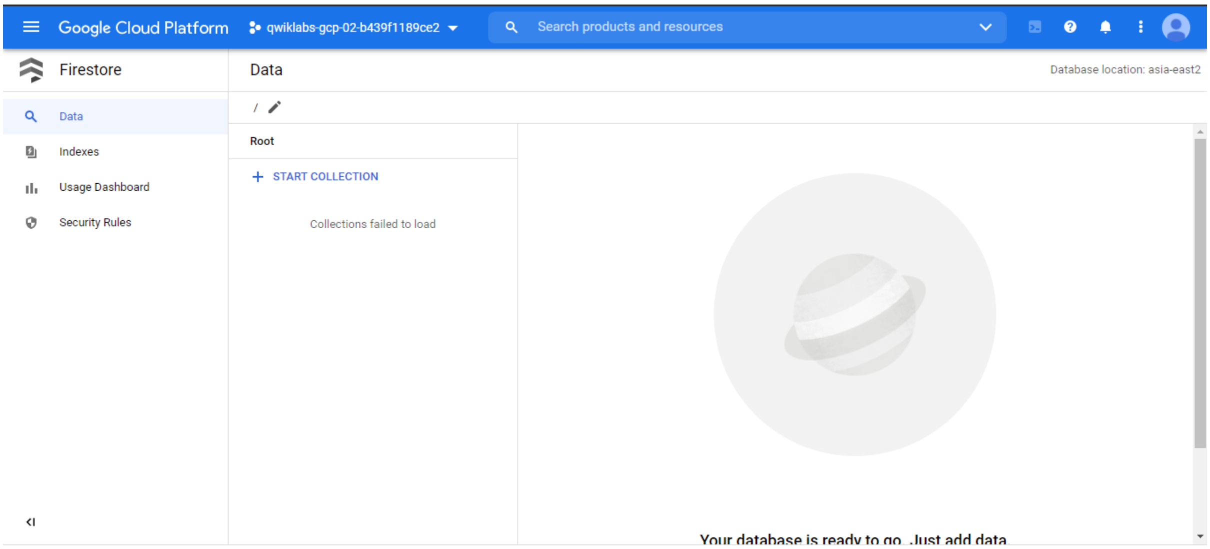


```
(env) student_02_cc1355cec2b5@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-b439f1189ce2)$ gcloud app deploy
You are creating an app for project [qwiklabs-gcp-02-b439f1189ce2].
WARNING: Creating an App Engine application for a project is irreversible and the region
cannot be changed. More information about regions is at
<https://cloud.google.com/appengine/docs/locations>.

Please choose the region where you want your App Engine application
located:

 [1] asia-east2
 [2] asia-northeast1
 [3] asia-northeast2
 [4] asia-northeast3
 [5] asia-south1
 [6] asia-southeast2
 [7] australia-southeast1
 [8] europe-west
 [9] europe-west2
 [10] europe-west3
 [11] europe-west6
 [12] northamerica-northeast1
 [13] southamerica-east1
 [14] us-central
 [15] us-east1
 [16] us-east4
 [17] us-west2
 [18] us-west3
 [19] us-west4
 [20] cancel
Please enter your numeric choice:  1

Creating App Engine application in project [qwiklabs-gcp-02-b439f1189ce2] and region [asia-east2]....done.
Services to deploy:

descriptor:      [/home/student_02_cc1355cec2b5/getting-started-python/bookshelf/app.yaml]
source:          [/home/student_02_cc1355cec2b5/getting-started-python/bookshelf]
```



```
descriptor:      [/home/student_02_cc1355cec2b5/getting-started-python/bookshelf/app.yaml]
source:          [/home/student_02_cc1355cec2b5/getting-started-python/bookshelf]
target project:  [qwiklabs-gcp-02-b439f1189ce2]
target service:  [default]
target version:  [20201015t182955]
target url:      [https://qwiklabs-gcp-02-b439f1189ce2.df.r.appspot.com]


Do you want to continue (Y/n)?  Y

Beginning deployment of service [default]...
Created .gcloudignore file. See `gcloud topic gcloudignore` for details.
╔════════════════════════════════════════════════════════════╗
╠═ Uploading 2276 files to Google Cloud Storage             ═╣
╚════════════════════════════════════════════════════════════╝
File upload done.
Updating service [default]...done.
Setting traffic split for service [default]...done.
Deployed service [default] to [https://qwiklabs-gcp-02-b439f1189ce2.df.r.appspot.com]

You can stream logs from the command line by running:
  $ gcloud app logs tail -s default

To view your application in the web browser run:
  $ gcloud app browse
(env) student_02_cc1355cec2b5@cloudshell:~/getting-started-python/bookshelf (qwiklabs-gcp-02-b439f1189ce2)$
```

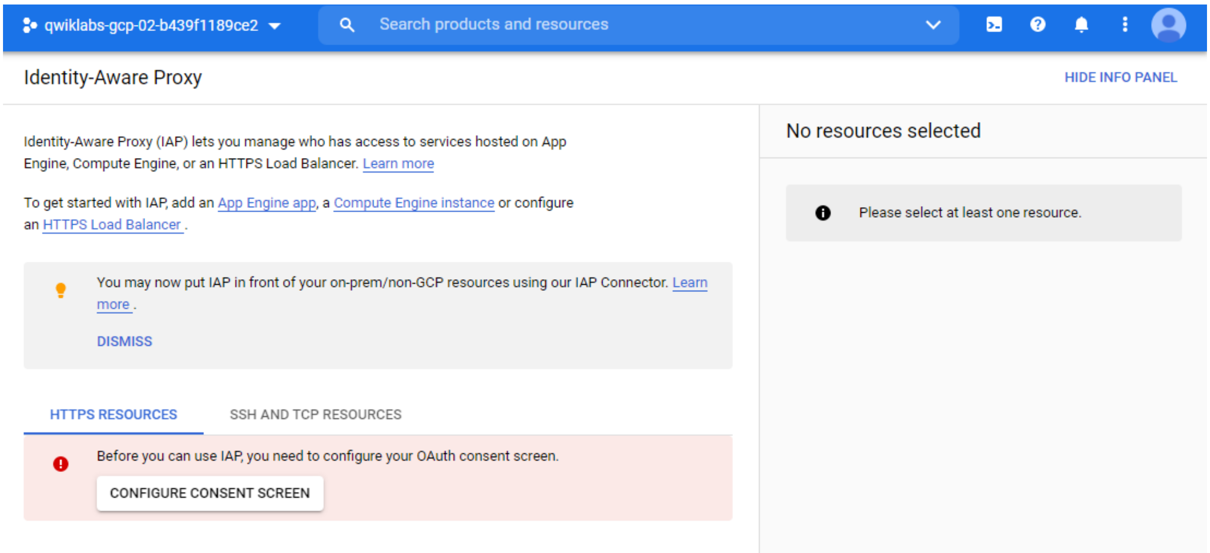
Deploying the application



Collections failed to load

Your database is ready to go. Just add data.

Firestore setting up



Identity-Aware Proxy

Identity-Aware Proxy (IAP) lets you manage who has access to services hosted on App Engine, Compute Engine, or an HTTPS Load Balancer. Learn more

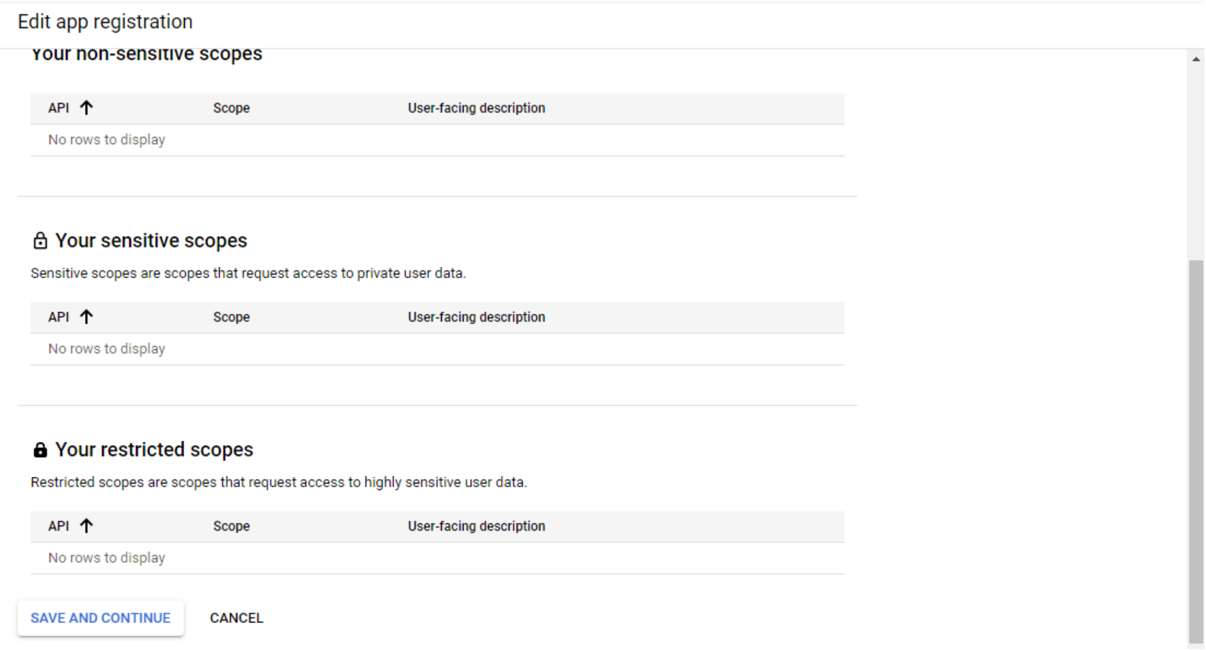
To get started with IAP, add an App Engine app, a Compute Engine instance or configure an HTTPS Load Balancer .

You may now put IAP in front of your on-prem/non-GCP resources using our IAP Connector. Learn more .

Before you can use IAP, you need to configure your OAuth consent screen.

No resources selected

Please select at least one resource.



Edit app registration

Your non-sensitive scopes

API ↑	Scope	User-facing description
No rows to display		

🔒 Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

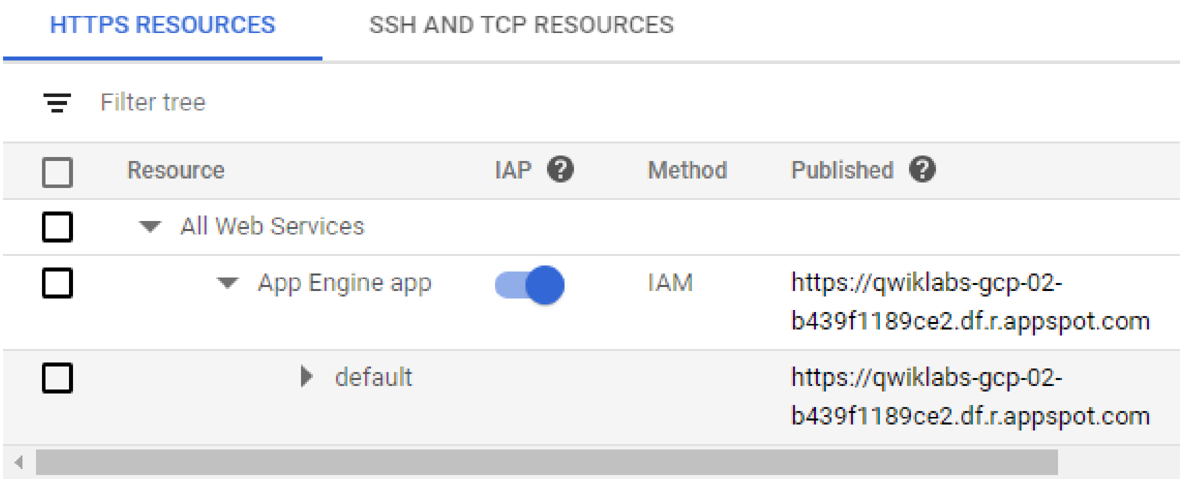
API ↑	Scope	User-facing description
No rows to display		

🔒 Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

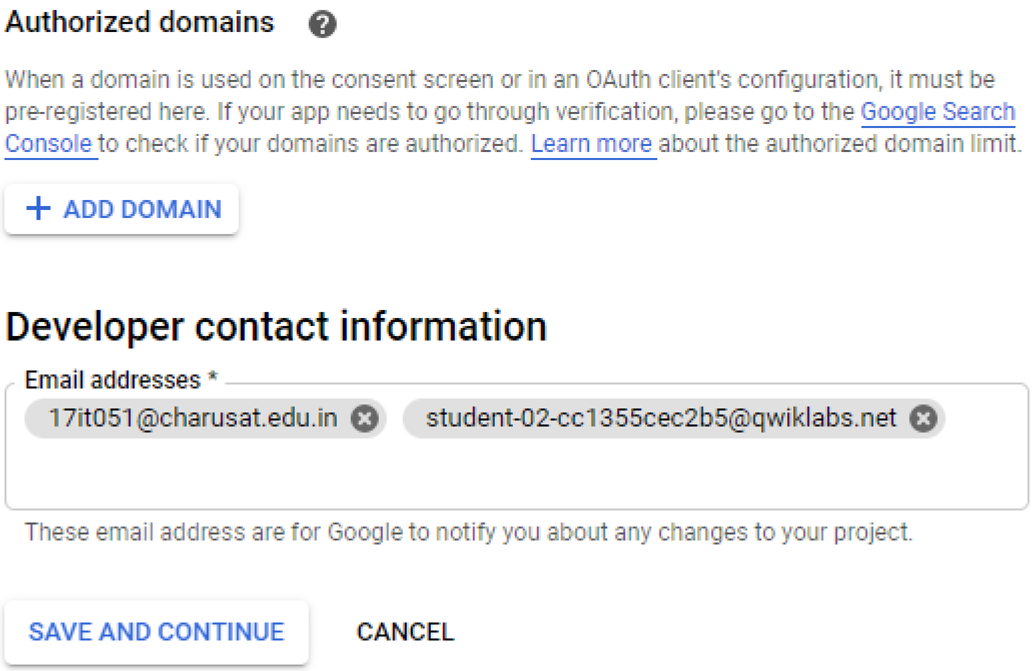
API ↑	Scope	User-facing description
No rows to display		

Setting up the OAuth Consent screen



□	Resource	IAP	Method	Published
□	All Web Services			
□	App Engine app	●	IAM	https://qwiklabs-gcp-02-b439f1189ce2.df.r.appspot.com
□	default			https://qwiklabs-gcp-02-b439f1189ce2.df.r.appspot.com

Configured the OAuth Consent Screen



Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the Google Search Console to check if your domains are authorized. Learn more about the authorized domain limit.

Developer contact information

Email addresses *

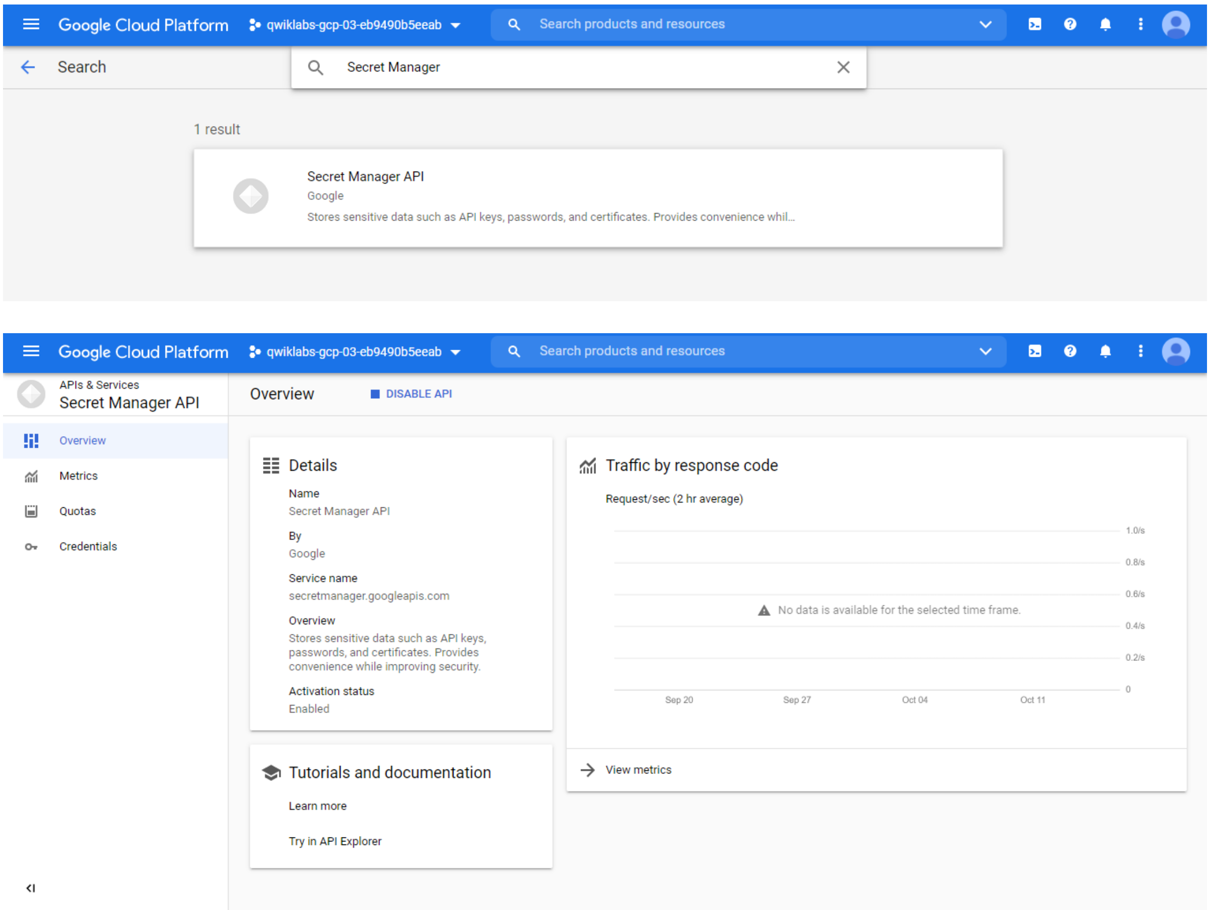
17it051@charusat.edu.in

student-02-cc1355cec2b5@qwiklabs.net

These email address are for Google to notify you about any changes to your project.

Adding only admin/specific members to access the application

8.5 Configuring and Using Credentials with Secret Manager



Secret Manager API
Google
Stores sensitive data such as API keys, passwords, and certificates. Provides convenience whil...

Name
Secret Manager API

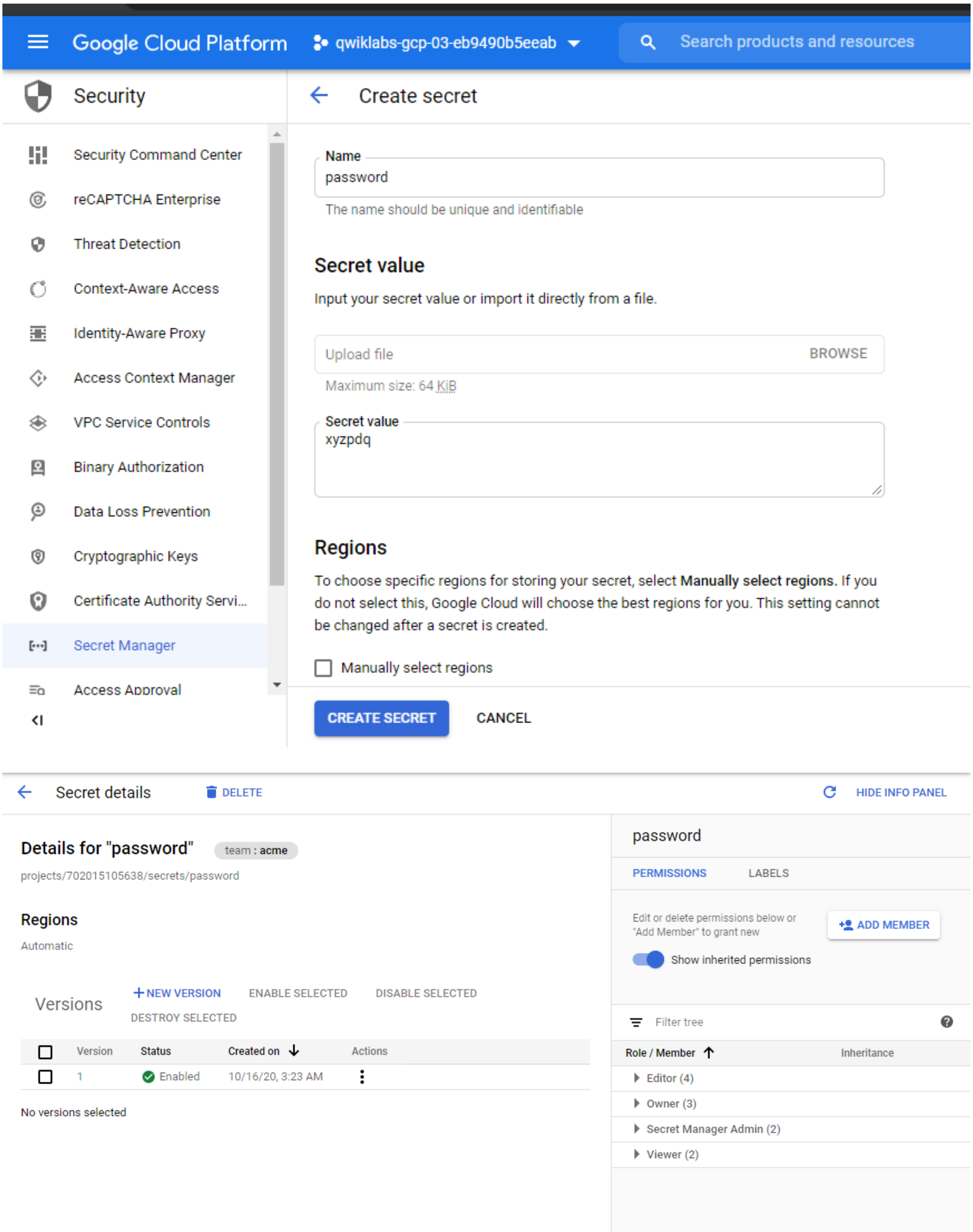
By
Google

Service name
secretmanager.googleapis.com

Overview
Stores sensitive data such as API keys, passwords, and certificates. Provides convenience while improving security.

Activation status
Enabled

Enabling Secret Manager API



Create secret

Name: password

The name should be unique and identifiable

Secret value

Input your secret value or import it directly from a file.

Upload file

Maximum size: 64 KiB

Secret value: xyzpdq

Regions

To choose specific regions for storing your secret, select **Manually select regions.** If you do not select this, Google Cloud will choose the best regions for you. This setting cannot be changed after a secret is created.

□ Manually select regions

Secret details

Details for "password" team : acme

projects/702015105638/secrets/password

Regions

Automatic

Versions

□	Version	Status	Created on	Actions
□	1	✓ Enabled	10/16/20, 3:23 AM	⋮

No versions selected

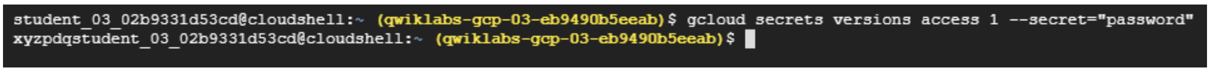
password

Edit or delete permissions below or "Add Member" to grant new

Show inherited permissions

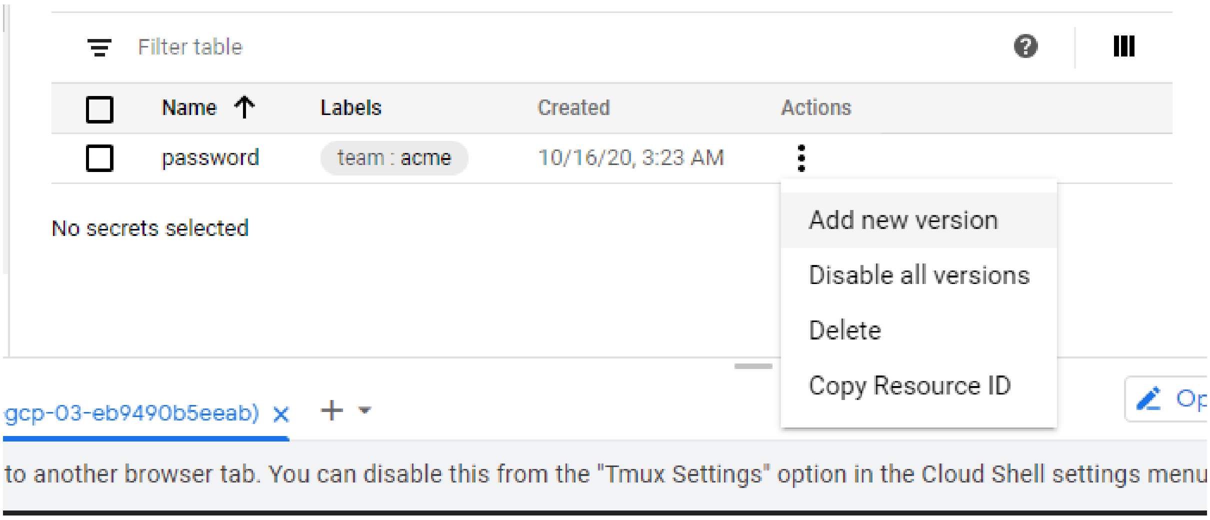
Role / Member	Inheritance
Editor (4)	
Owner (3)	
Secret Manager Admin (2)	
Viewer (2)	

Creating new secret with name "password"



```
student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$ gcloud secrets versions access 1 --secret="password"
xyzpdqstudent_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$ 
```

Accessing secret with name "password" from shell.

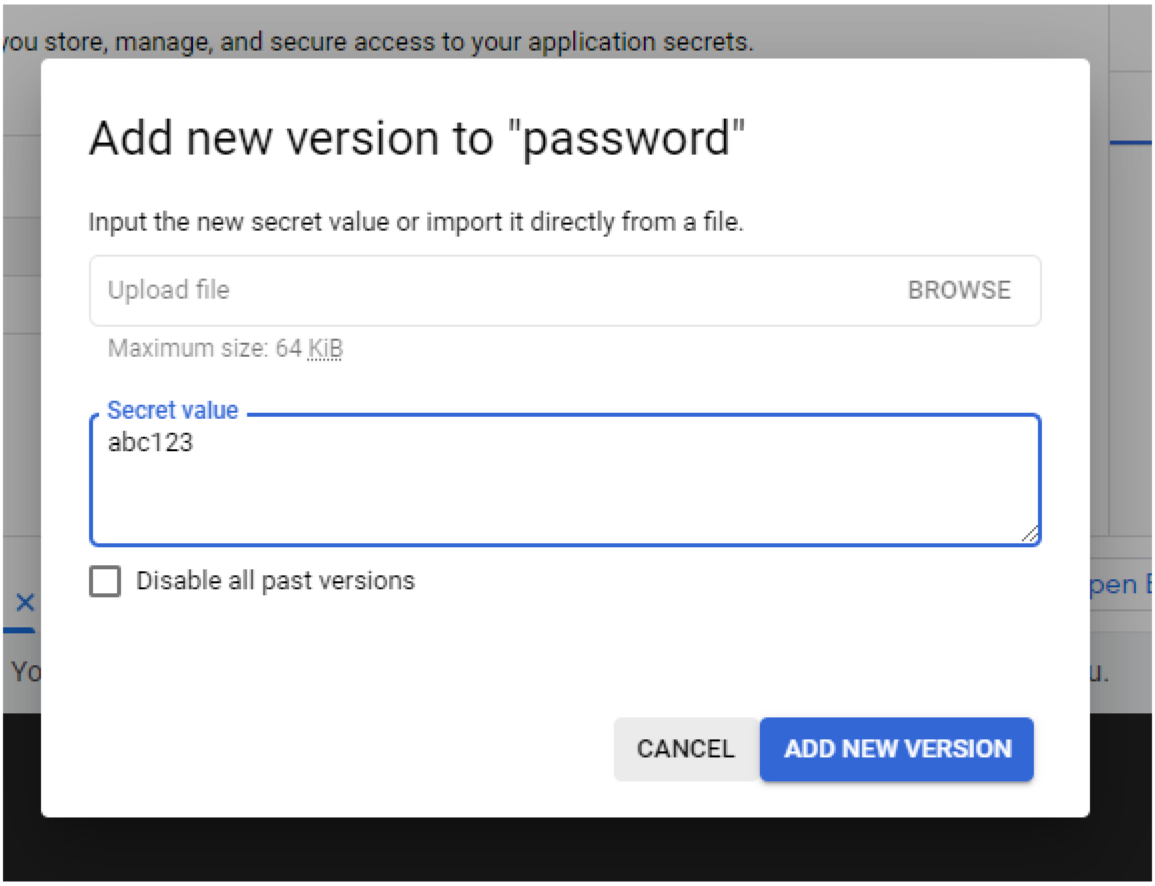


Filter table

☐	Name ↑	Labels	Created	Actions
☐	password	team : acme	10/16/20, 3:23 AM	⋮

No secrets selected

to another browser tab. You can disable this from the "Tmux Settings" option in the Cloud Shell settings menu



/ou store, manage, and secure access to your application secrets.

Add new version to "password"

Input the new secret value or import it directly from a file.

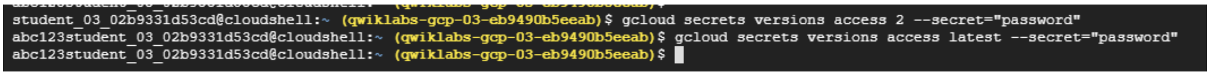
Upload file

Maximum size: 64 KiB

Secret value
abc123

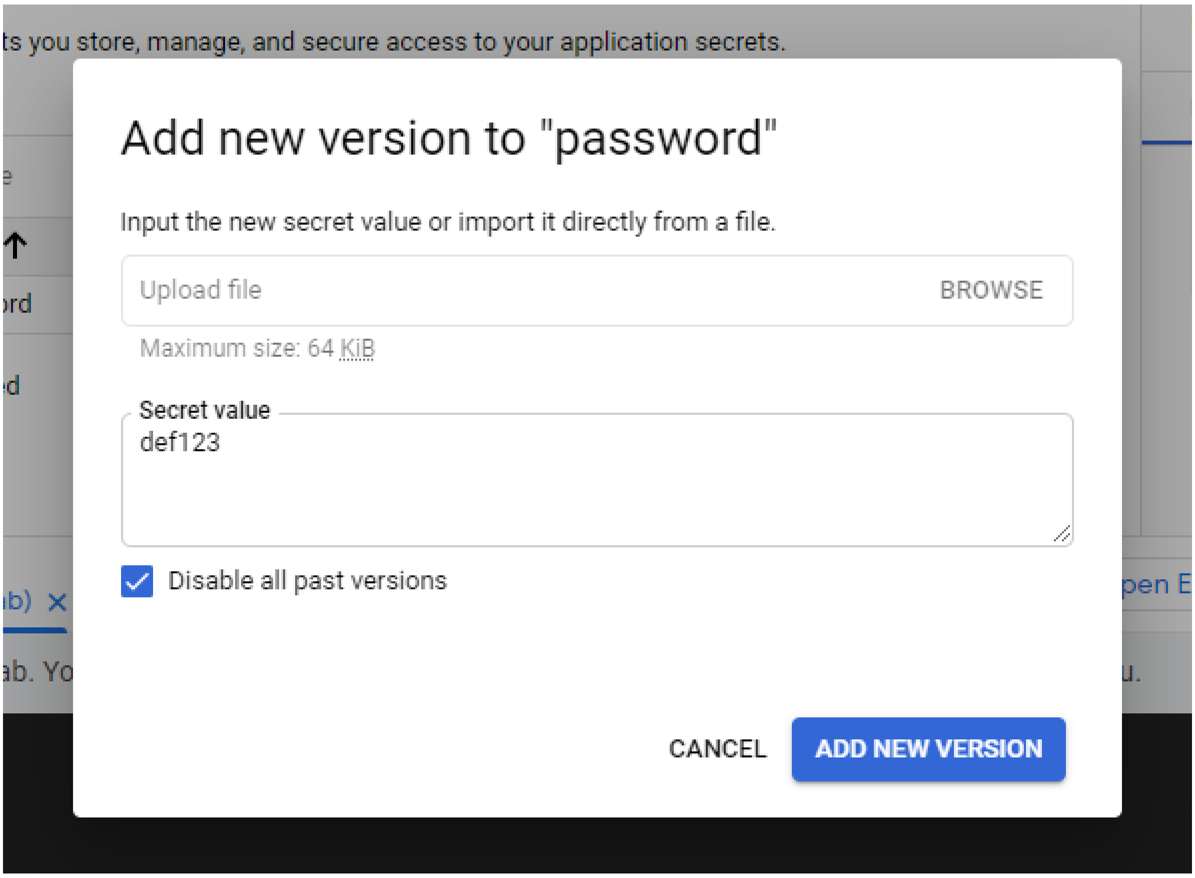
☐ Disable all past versions

Adding New Secret Version



```
student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$ gcloud secrets versions access 2 --secret="password"
abc123student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$ gcloud secrets versions access latest --secret="password"
abc123student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$
```

Checking for new version


ts you store, manage, and secure access to your application secrets.

Add new version to "password"

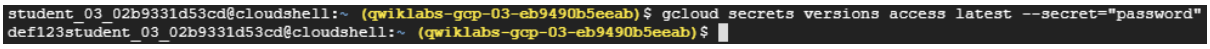
Input the new secret value or import it directly from a file.

Upload file
BROWSE
Maximum size: 64 KiB

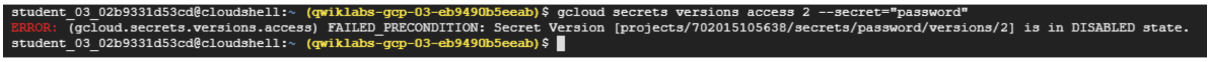
Secret value
def123

☑ Disable all past versions

Adding new version and along with checking disable past versions

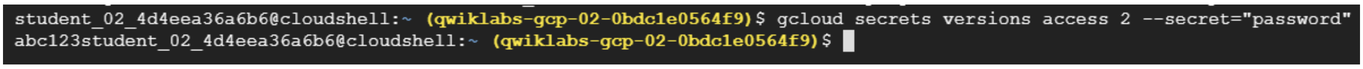


```
student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$ gcloud secrets versions access latest --secret="password"
def123student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$
```



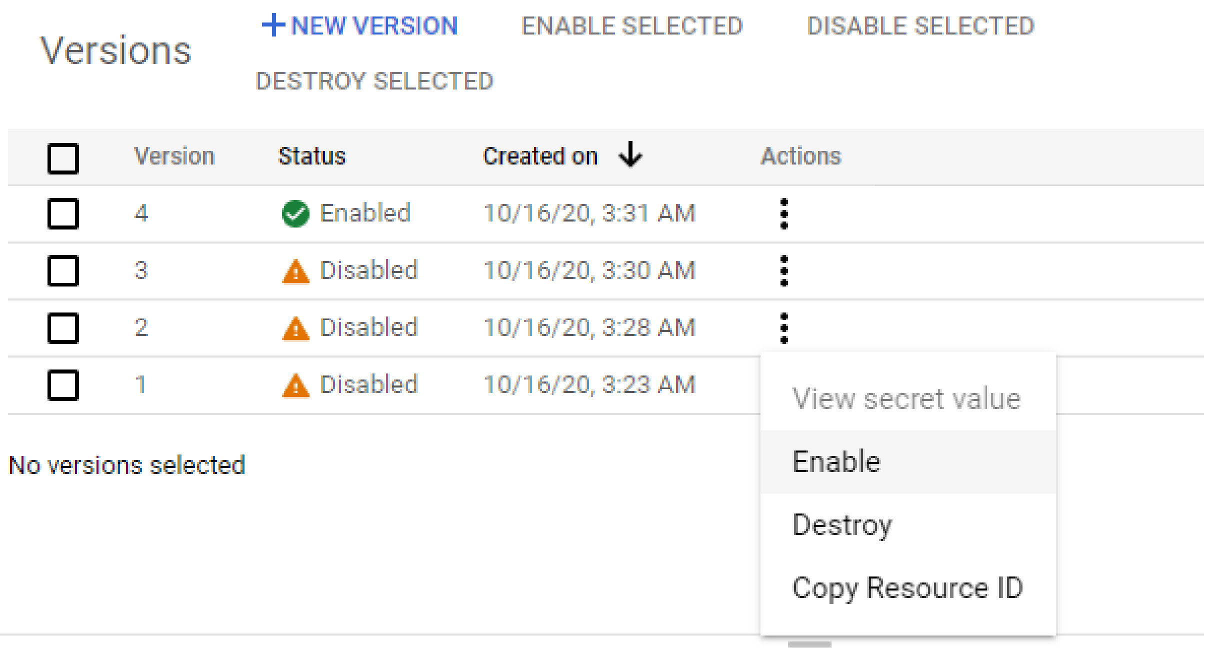
```
student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$ gcloud secrets versions access 2 --secret="password"
ERROR: (gcloud.secrets.versions.access) FAILED_PRECONDITION: Secret Version [projects/702015105638/secrets/password/versions/2] is in DISABLED state.
student_03_02b9331d53cd@cloudshell:~ (qwiklabs-gcp-03-eb9490b5eeab)$
```

Accessing the new version and also trying to access old version and getting errors



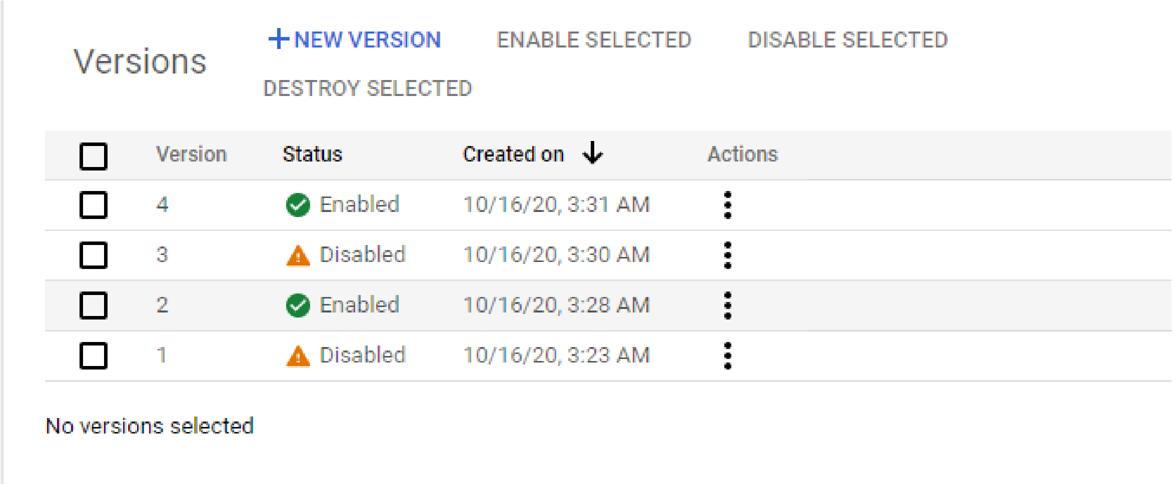
```
student_02_4d4eea36a6b6@cloudshell:~ (qwiklabs-gcp-02-0bdc1e0564f9)$ gcloud secrets versions access 2 --secret="password"
abc123student_02_4d4eea36a6b6@cloudshell:~ (qwiklabs-gcp-02-0bdc1e0564f9)$
```

Accessing version 2



☐	Version	Status	Created on ↓	Actions
☐	4	✓ Enabled	10/16/20, 3:31 AM	⋮
☐	3	⚠ Disabled	10/16/20, 3:30 AM	⋮
☐	2	⚠ Disabled	10/16/20, 3:28 AM	⋮
☐	1	⚠ Disabled	10/16/20, 3:23 AM	

No versions selected



☐	Version	Status	Created on ↓	Actions
☐	4	✓ Enabled	10/16/20, 3:31 AM	⋮
☐	3	⚠ Disabled	10/16/20, 3:30 AM	⋮
☐	2	✓ Enabled	10/16/20, 3:28 AM	⋮
☐	1	⚠ Disabled	10/16/20, 3:23 AM	⋮

No versions selected

Old version 2 enabled again

LATEST APPLICATIONS:

Providing security controls and techniques on real time applications and also managing timely updating and rotating the keys for accessing complete benefits of gcp security.

LEARNING OUTCOME:

Configure CSEK for google cloud storage, uploading files on storage bucket and generate and rotate the encryption keys then generate manage and encrypted data using cloud kms, create key rings and crypto keys then install sample app engine and sue cloud security scanner to scan application and find vulnerabilities along with scheduling the scans then configure OAuth consent screen and setup cloud IAP access and enable cloud API.

REFERENCE:

1. https://googlecoursera.qwiklabs.com/focuses/11115438?parent=lti_session
2. https://googlecoursera.qwiklabs.com/focuses/11115450?parent=lti_session
3. https://googlecoursera.qwiklabs.com/focuses/11115455?parent=lti_session
4. https://googlecoursera.qwiklabs.com/focuses/11115459?parent=lti_session
5. https://googlecoursera.qwiklabs.com/focuses/11115466?parent=lti_session