Permission Mining in GCP

Colin Estep
Netskope Threat Labs

Agenda

- IAM Exposure
- IAM in GCP
- Privilege Escalation Example
- Tools for Auditing
- Remediation

IAM Exposure

IAM Exposure vs. Data Exposure

IAM Exposure

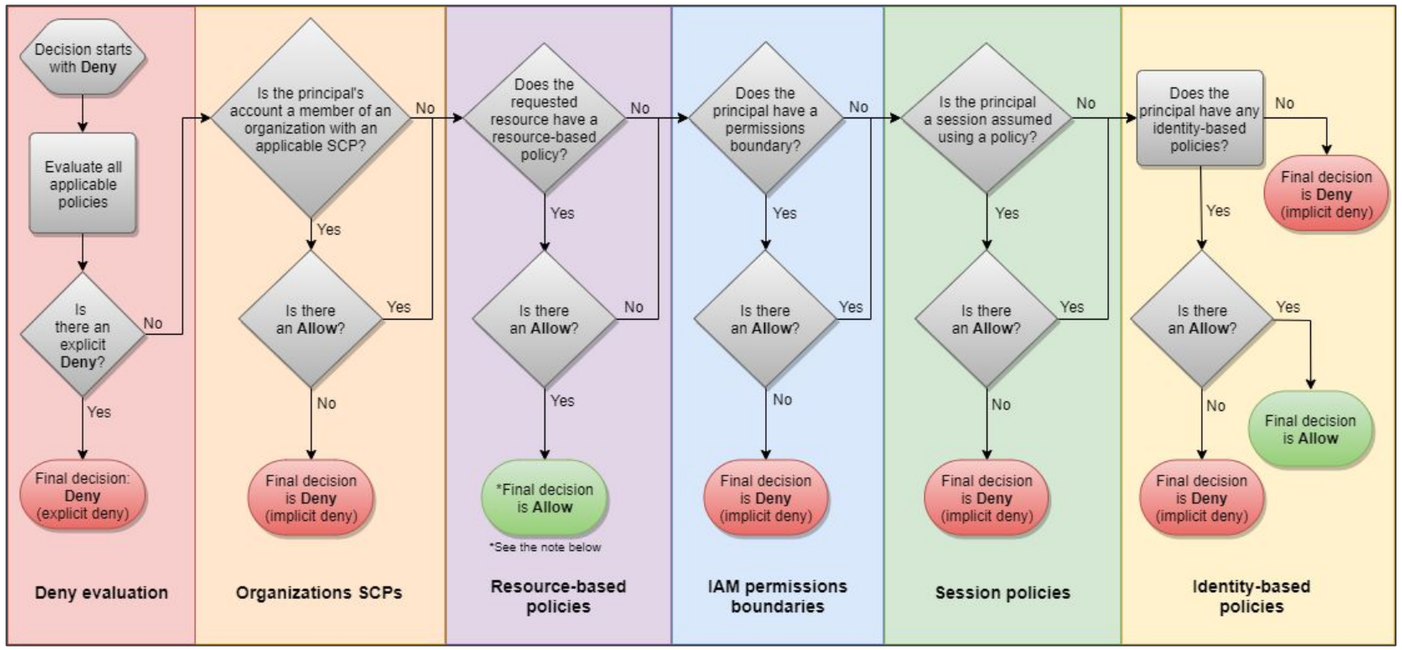
- What can your users do?
- Could a compromised credential result in administrator access?

Data Exposure

- What objects are public?
- What sensitive data could be exposed?

Why is IAM challenging?

- Rushed provisioning
- Auditing at scale
- Misunderstanding entitlements



IAM in GCP

Member Types in GCP

User

- Not created in GCP
- IdP or GSuite

Service Account

- Identity for programmatic use
- Also considered a resource

Group

- Contains Users
- IdP or GSuite

Domain

- Just like domains in GSuite
- Example: netskope.com

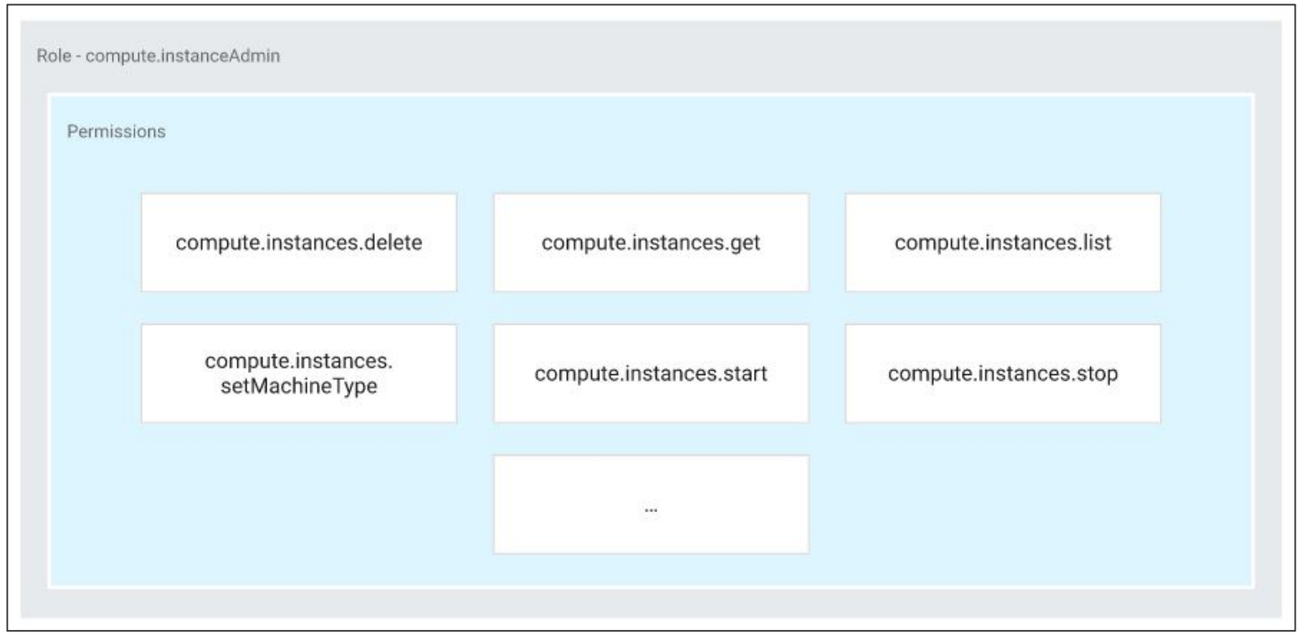
GCP Terminology

- **Permission**

  Allows a specific API call

- **Role**

  A collection of permissions



GCP Terminology

The different types of Roles:

- Basic
- Predefined
- Custom

Basic

- Maintained by Google
- Pre-dates IAM
- Overly permissive and not recommended

Examples:

- **Owner**
- **Editor**
- **Viewer**

Predefined

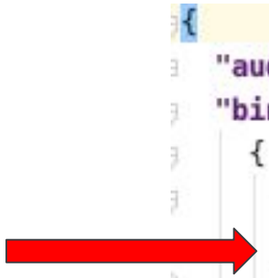
- Maintained by Google
- Focused on job roles
- Good starting point for least privilege

Examples:

- **compute.instanceAdmin**
- **compute.loadBalancerAdmin**

GCP Terminology

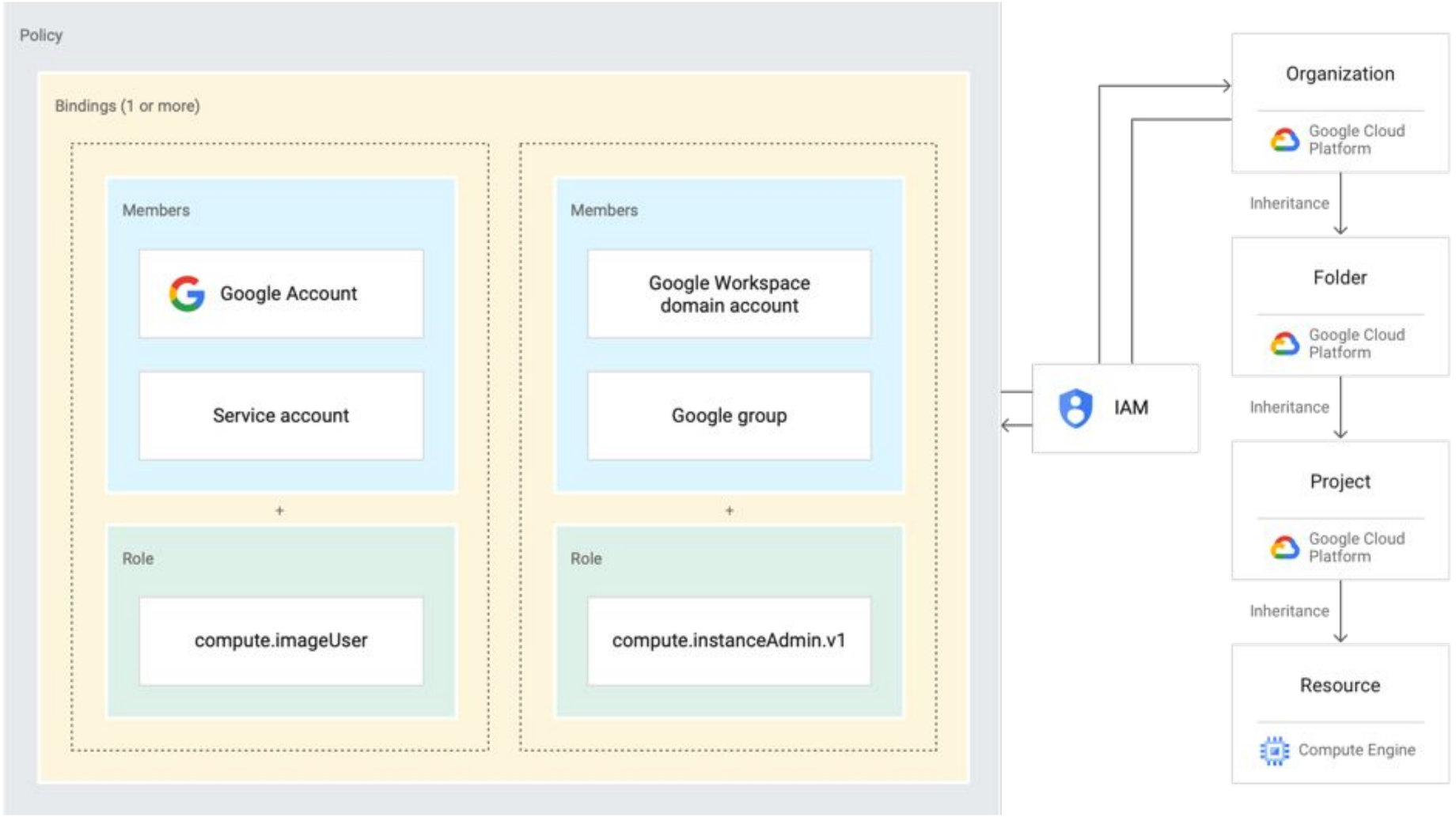
- **Binding**: When a role is assigned to a member
- **Policies**: A collection of bindings




```
{
  "auditConfigs": [...],
  "bindings": [
    {
      "members": [
        "serviceAccount:acct@siftsec-gcp-dev.iam.gserviceaccount.com"
      ],
      "role": "roles/bigtable.admin"
    },
    {
      "members": [
        "user:x@siftsec.com"
      ],
      "role": "roles/cloudkms.admin"
    },
    {
      "members": [
        "domain:siftsec.com",
        "serviceAccount:colin-testing@appspot.gserviceaccount.com"
      ],
      "role": "roles/browser"
    }
  ],
  "etag": "BwW91vxBpiM=",
  "version": 3
}
```

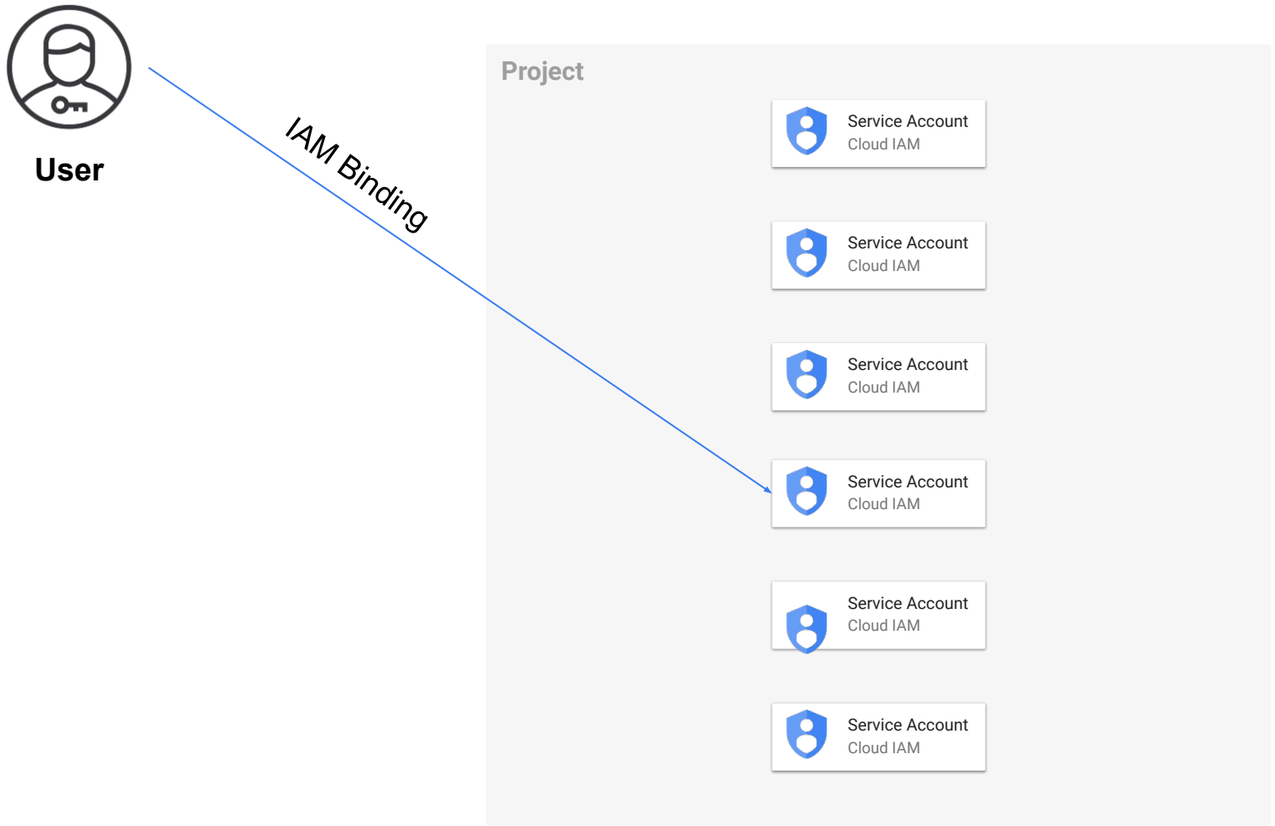

*Sample shows an IAM policy from a GCP Project

IAM Policies and GCP's hierarchy

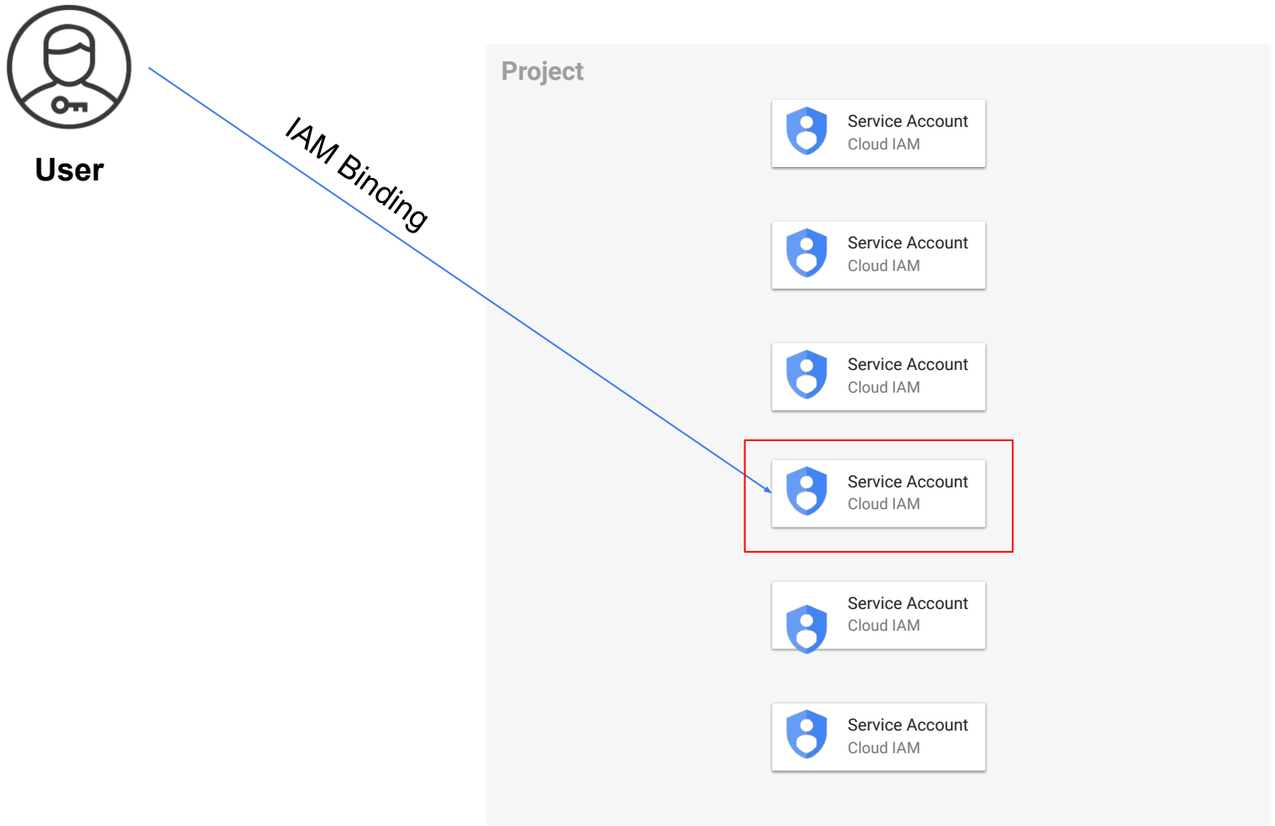


Service Accounts: Identities and Resources

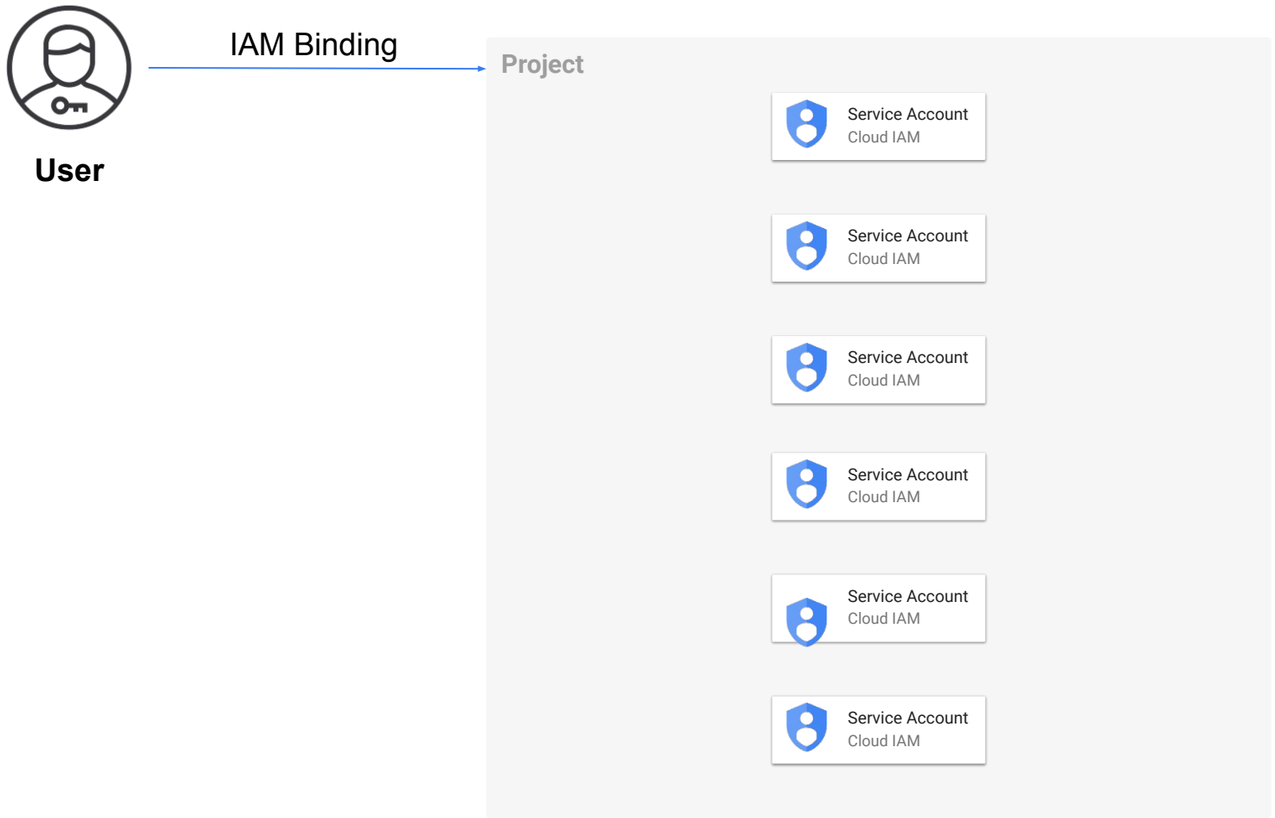
Binding at a Service Account



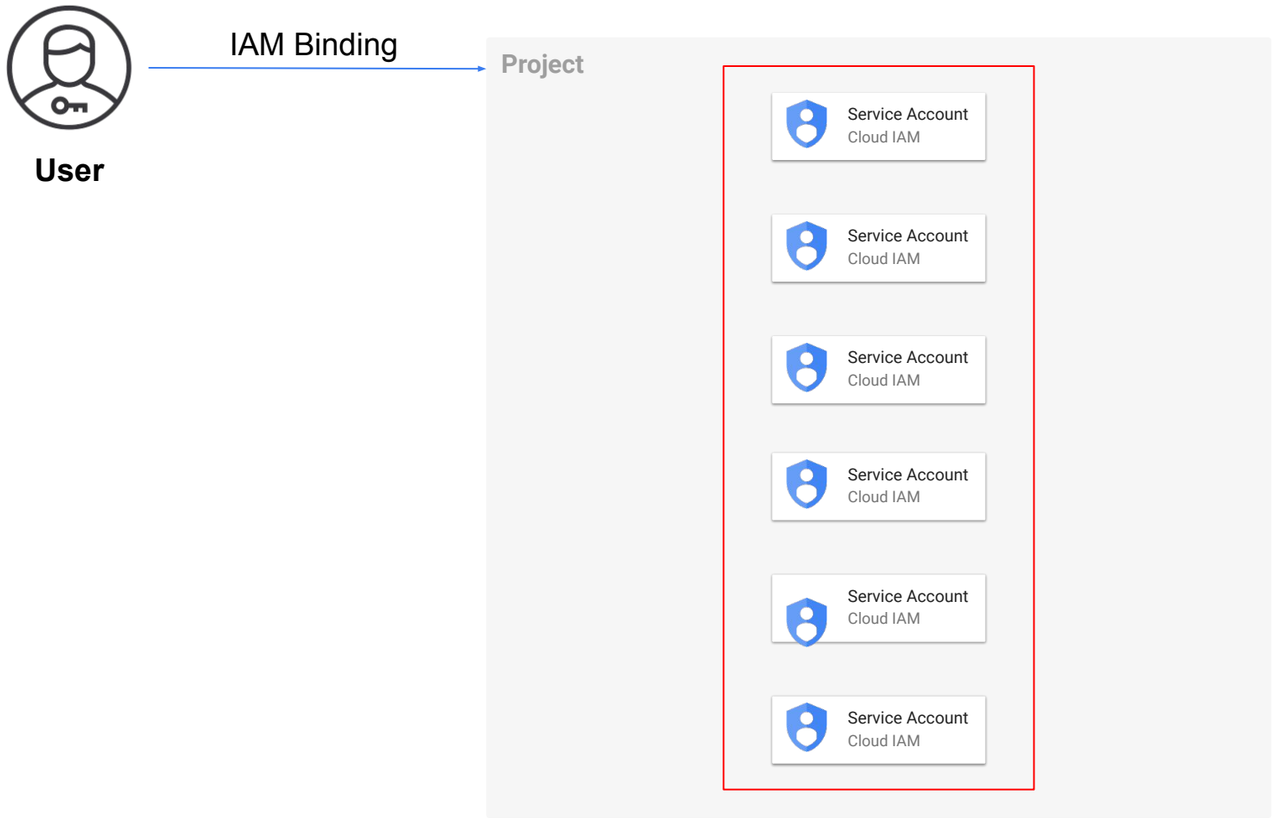
Binding at a Service Account



Binding at a Project

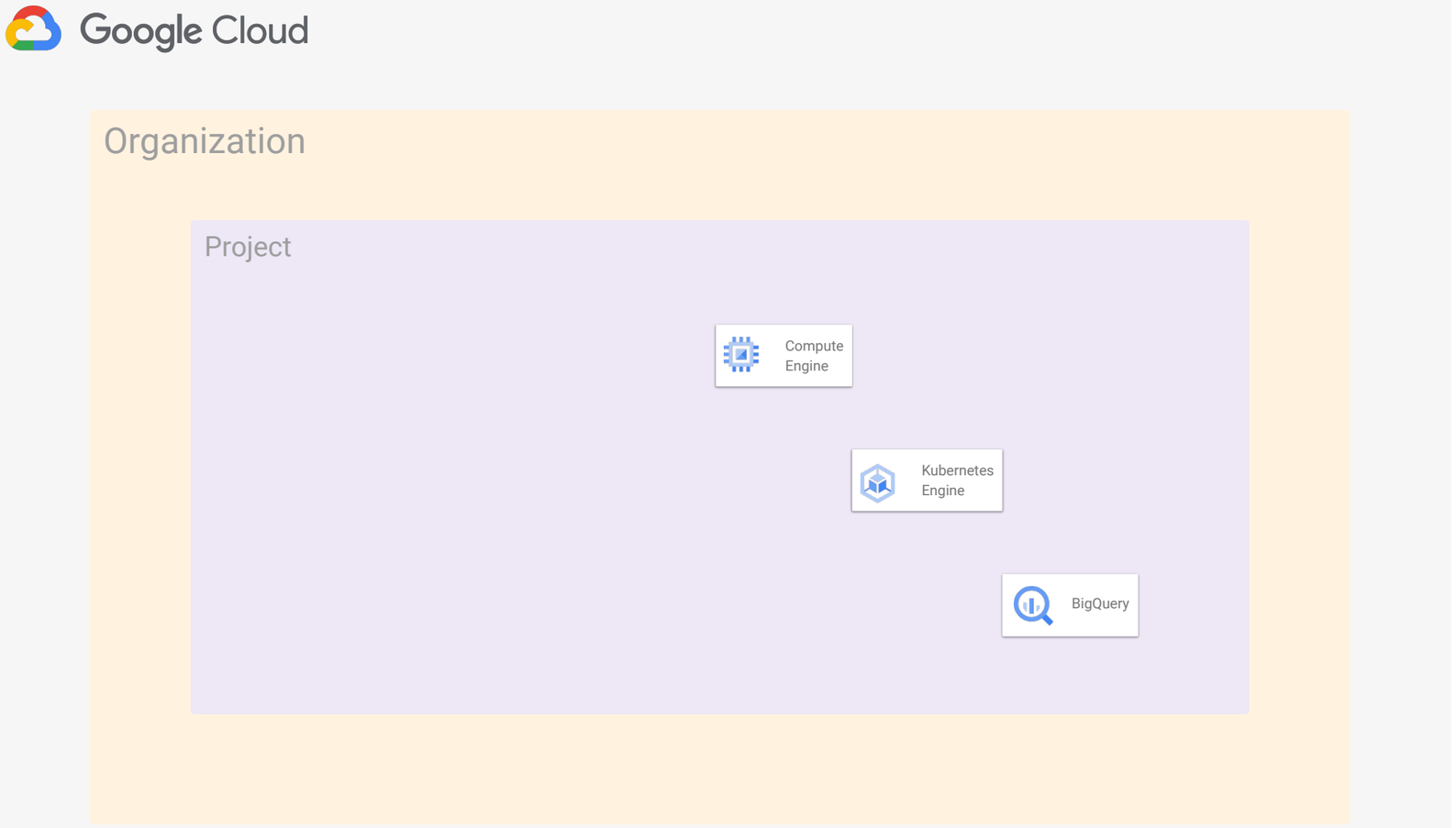


Binding at a Project

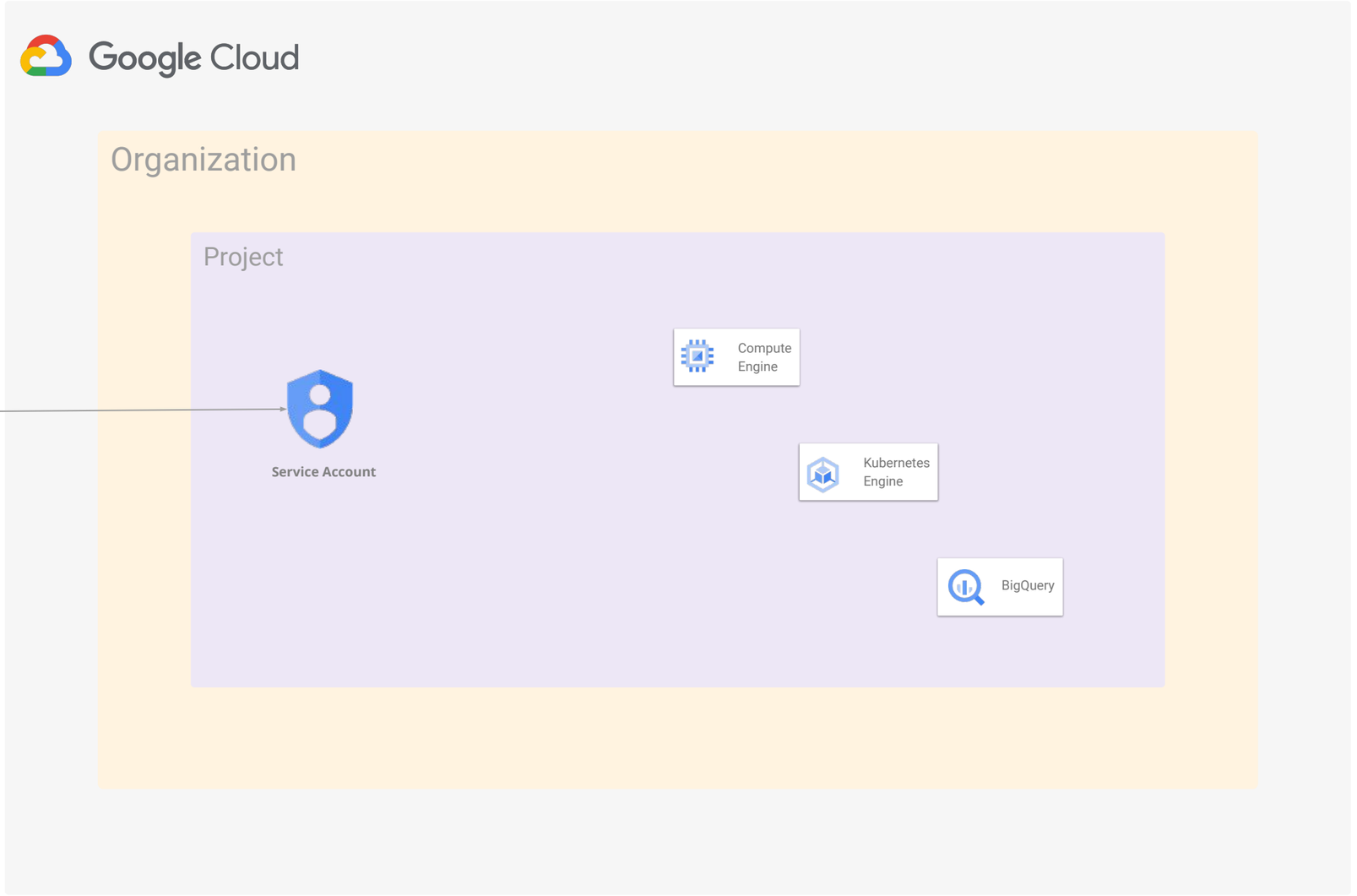


Privilege Escalation Example

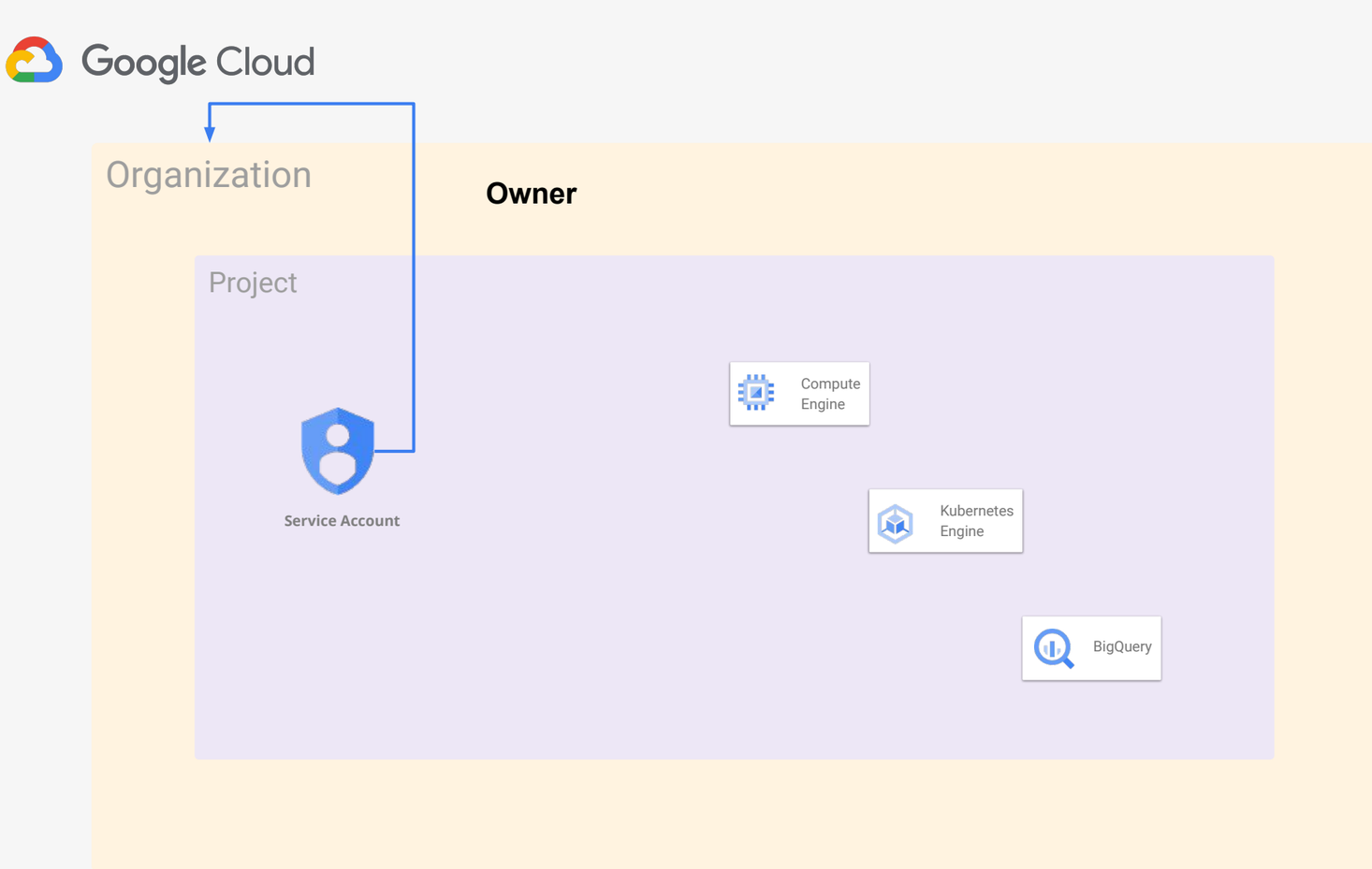
(An example from a production GCP environment)



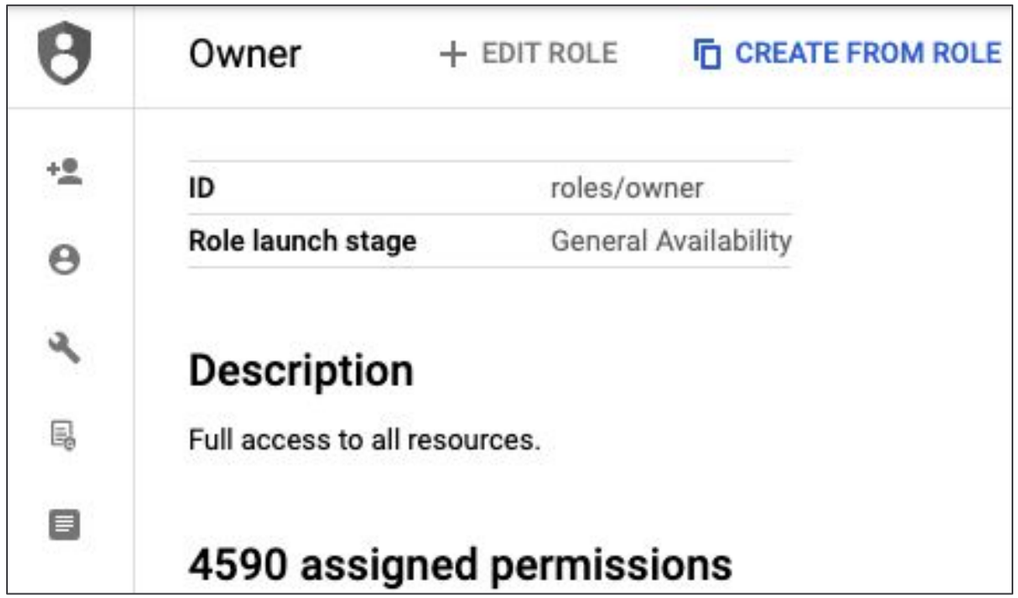
Service Account Created

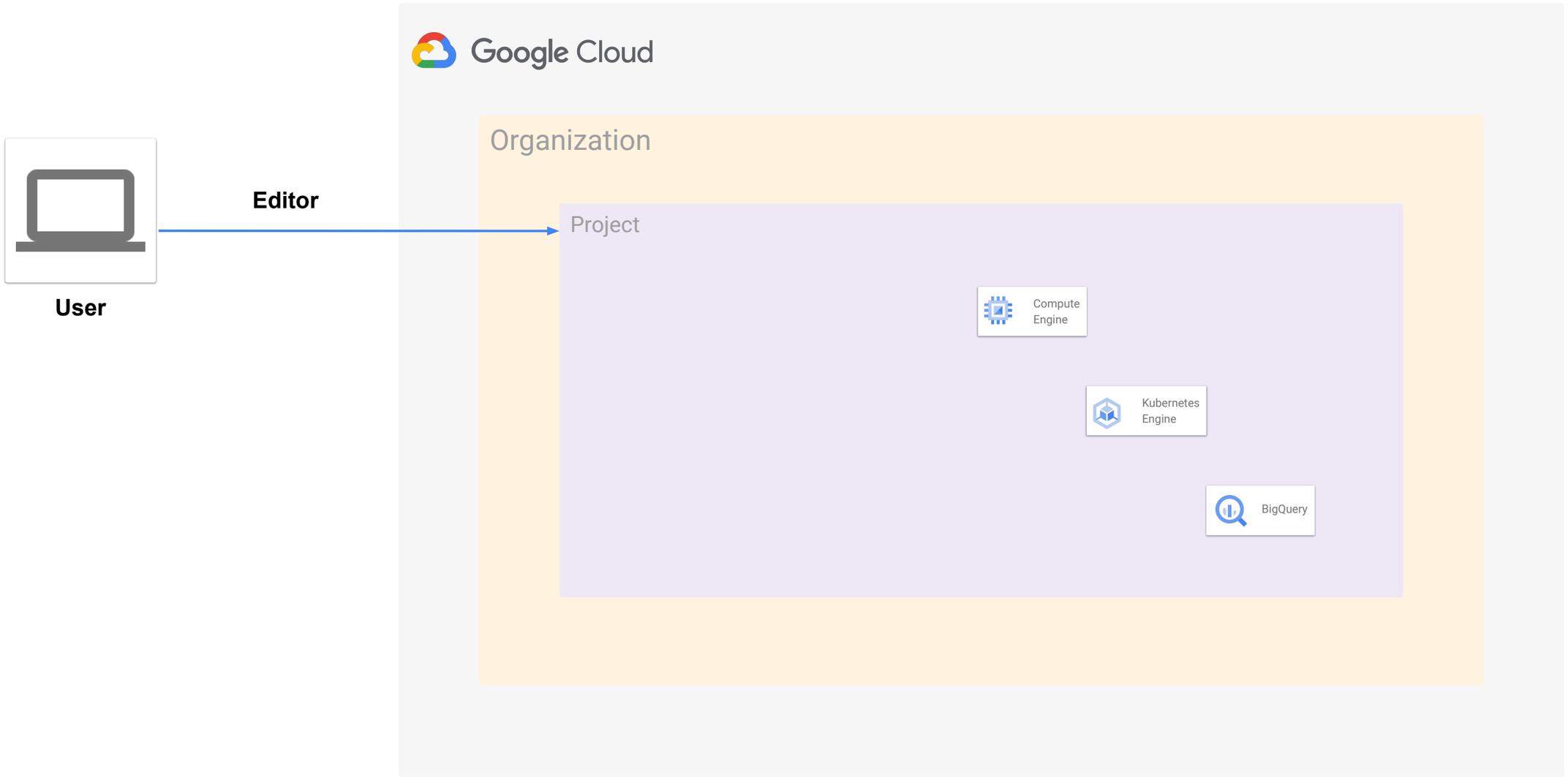


“**Owner**”
Permission Granted

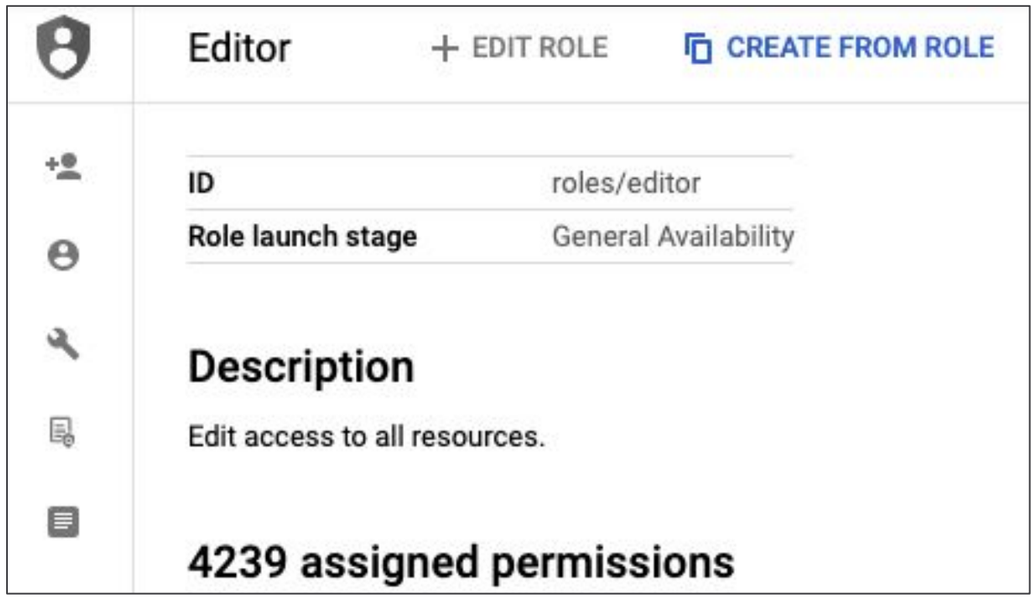


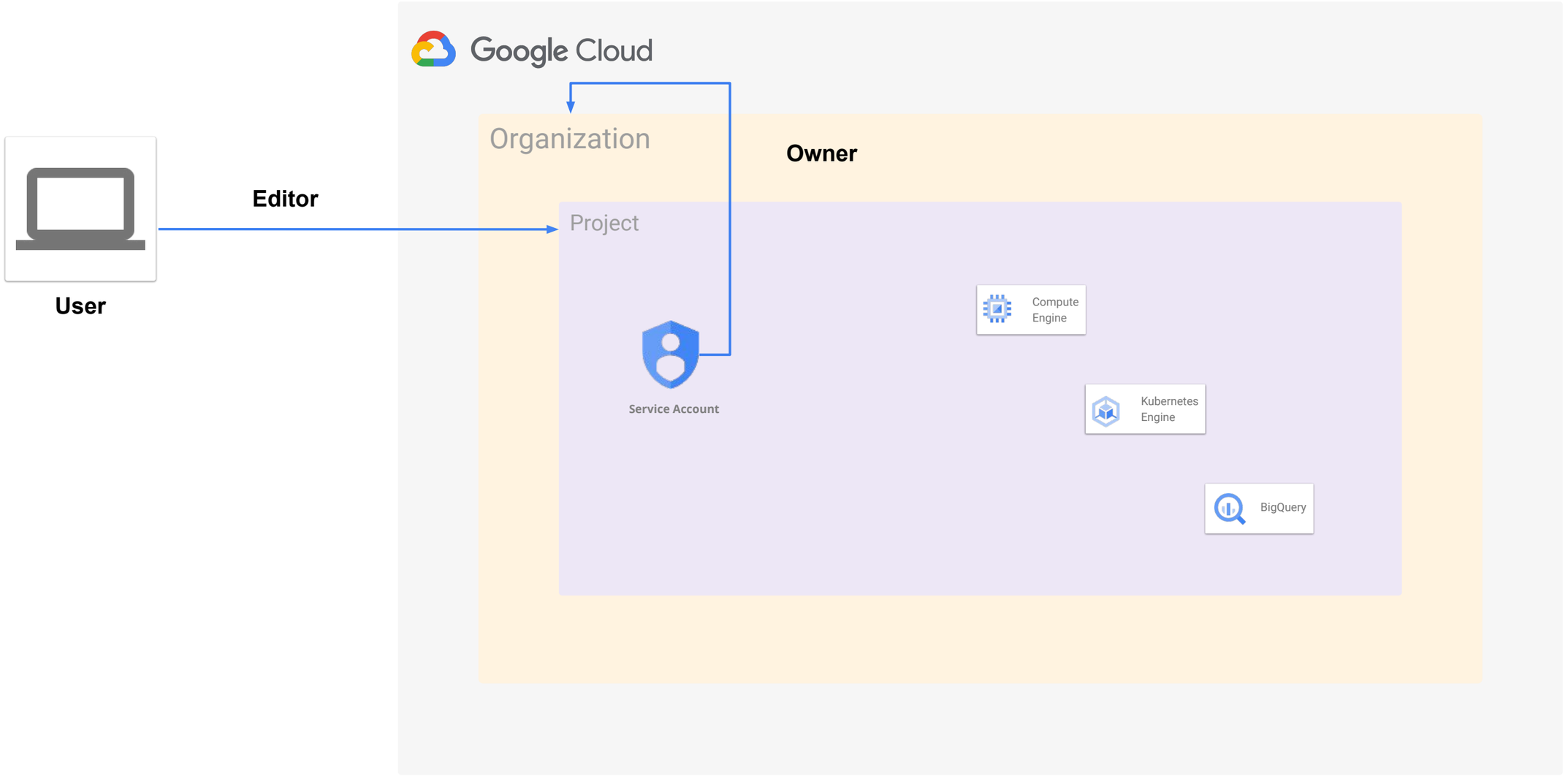
Owner

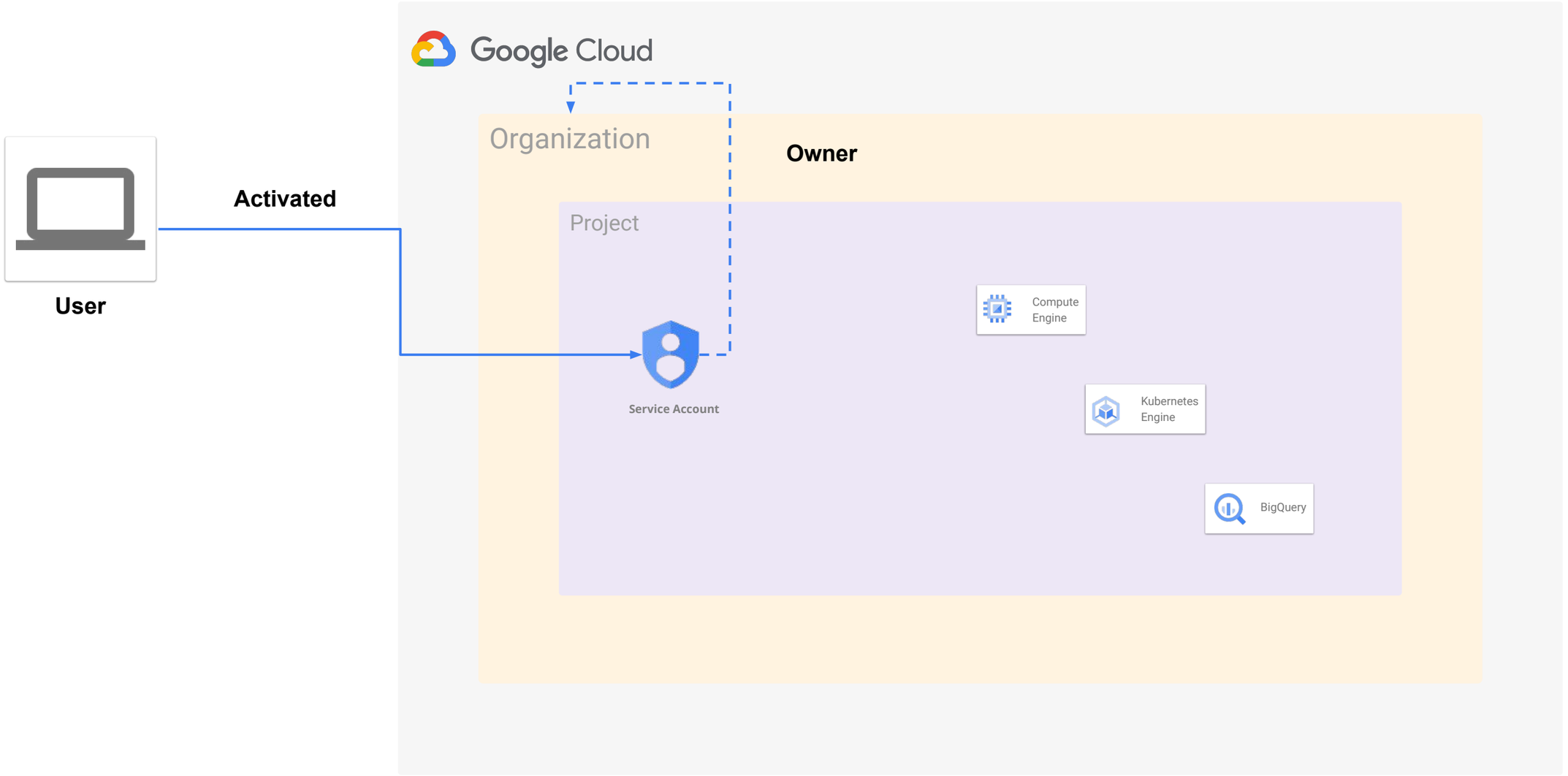




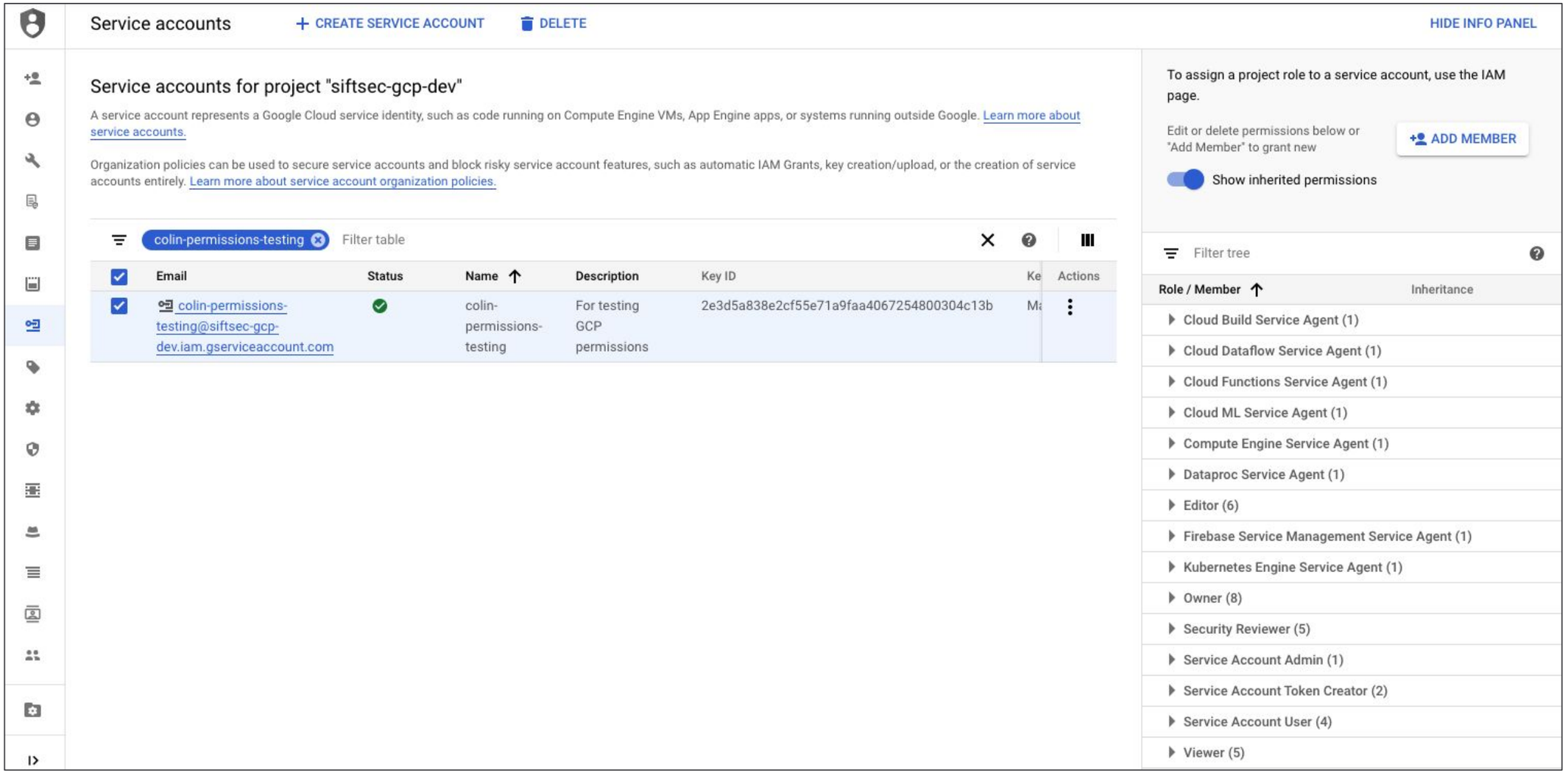
Editor







Why is this difficult to manage?



Tools for Auditing

GCP IAM Analyzer

Output all members that can impersonate a service account from the Organization level

```
gcloud asset analyze-iam-policy --organization="123456789" \
    --permissions="iam.serviceAccounts.actAs, iam.serviceAccounts.getAccessToken, iam.serviceAccounts.getOpenIdToken,
     iam.serviceAccounts.implicitDelegation, iam.serviceAccounts.signBlob, iam.serviceAccounts.signJwt"
```

GCP IAM Analyzer


```
"ACLs": [
  {
    "accesses": [
      {
        "permission": "iam.serviceAccounts.actAs"
      }
    ],
    "identities": [
      {
        "name": "user:x@siftsec.com"
      },
      {
        "name": "user:y@siftsec.com"
      },
      {
        "name": "user:z@siftsec.com"
      }
    ],
    "resources": [
      {
        "fullResourceName": "//iam.googleapis.com/projects/siftsec-gcp-dev/serviceAccounts/colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com'
      }
    ]
  }
],
"policy": {
  "attachedResource": "//iam.googleapis.com/projects/siftsec-gcp-dev/serviceAccounts/colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com",
  "binding": {
    "members": [
      "user:x@siftsec.com",
      "user:y@siftsec.com",
      "user:z@siftsec.com"
    ],
    "role": "roles/iam.serviceAccountUser"
  }
```


Individual Permission

Role Name

GCP IAM Analyzer

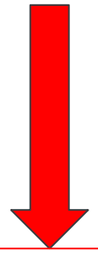

```
"ACLs": [
  {
    "accesses": [
      {
        "permission": "iam.serviceAccounts.actAs"
      }
    ],
    "identities": [
      {
        "name": "user:x@siftsec.com"
      },
      {
        "name": "user:y@siftsec.com"
      },
      {
        "name": "user:z@siftsec.com"
      }
    ],
    "resources": [
      {
        "fullResourceName": "//iam.googleapis.com/projects/siftsec-gcp-dev/serviceAccounts/colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com'
      }
    ]
  }
],
"policy": {
  "attachedResource": "//iam.googleapis.com/projects/siftsec-gcp-dev/serviceAccounts/colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com",
  "binding": {
    "members": [
      "user:x@siftsec.com",
      "user:y@siftsec.com",
      "user:z@siftsec.com"
    ],
    "role": "roles/iam.serviceAccountUser"
  }
```


Identities

GCP IAM Analyzer


```
"ACLs": [
  {
    "accesses": [
      {
        "permission": "iam.serviceAccounts.actAs"
      }
    ],
    "identities": [
      {
        "name": "user:x@siftsec.com"
      },
      {
        "name": "user:y@siftsec.com"
      },
      {
        "name": "user:z@siftsec.com"
      }
    ],
    "resources": [
      {
        "fullResourceName": "//iam.googleapis.com/projects/siftsec-gcp-dev/serviceAccounts/colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com"
      }
    ]
  }
],
"policy": {
  "attachedResource": "//iam.googleapis.com/projects/siftsec-gcp-dev/serviceAccounts/colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com",
  "binding": {
    "members": [
      "user:x@siftsec.com",
      "user:y@siftsec.com",
      "user:z@siftsec.com"
    ],
    "role": "roles/iam.serviceAccountUser"
  }
```


Resource



GCP Permission Miner


```
"member": {
  "name": "x@siftsec.com",
  "type": "user",
  "external_member": false,
  "service_account_access": true,
  "admin_level_access": true,
  "direct_bindings": {
    "organization": {
      "siftsec.com": [
        "roles/billing.admin",
        "roles/owner",
        "roles/resourcemanager.folderAdmin",
        "roles/resourcemanager.organizationAdmin",
        "roles/resourcemanager.projectCreator"
      ]
    },
    "folder": {...},
    "project": {...},
    "service_account": {
      "colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com": [
        "roles/iam.serviceAccountUser"
      ]
    }
  },
  "indirect_bindings": {
    "organization": {
      "siftsec.com": [
        "roles/logging.viewer",
        "roles/logging.logWriter",
        "roles/pubsub.editor",
        "roles/owner",
        "roles/browser",
        "roles/iam.securityReviewer",
        "roles/viewer"
      ]
    },
```


Identity

Direct entitlements

Indirect entitlements

GCP Permission Miner


```
"member": {
  "name": "x@siftsec.com",
  "type": "user",
  "external_member": false,
  "service_account_access": true,
  "admin_level_access": true,
  "direct_bindings": {
    "organization": {
      "siftsec.com": [
        "roles/billing.admin",
        "roles/owner",
        "roles/resourcemanager.folderAdmin",
        "roles/resourcemanager.organizationAdmin",
        "roles/resourcemanager.projectCreator"
      ]
    },
    "folder": {...},
    "project": {...},
    "service_account": {
      "colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com": [
        "roles/iam.serviceAccountUser"
      ]
    }
  },
  "indirect_bindings": {
    "organization": {
      "siftsec.com": [
        "roles/logging.viewer",
        "roles/logging.logWriter",
        "roles/pubsub.editor",
        "roles/owner",
        "roles/browser",
        "roles/iam.securityReviewer",
        "roles/viewer"
      ]
    },
```


Identity

Direct entitlements

Possible Privilege Escalation!

Indirect entitlements

Remediation

Remediation

- Bringing service account bindings down the hierarchy
- Changing out basic roles for more granular roles
- Removing bindings that are not needed

We want to proactively reduce risk in the environment without waiting for a compromise.

Talk Feedback: https://bit.ly/fwdcs21-estep

Thank you!

Colin Estep
@colinestep
https://www.linkedin.com/in/colinestep/

Project URL:
github.com/netskopeoss/iaas_permission_mining