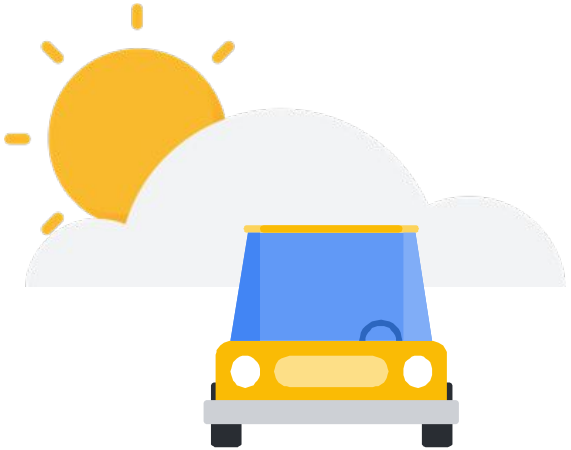
Carolyn Huynh | Google Cloud Security

Self Driving Cloud

Simulator



care0hlyn.github.com

Carolyn Huynh | Google Cloud Security

Lead UX Designer

Role

I was the first designer to join the Self Driving Cloud team and ever since, I've been the Lead UX Designer and thought leader behind the suite of SDC products three years now.

Simulator is the third product within the self-driving cloud initiative that I have lead from inception to launch.

The Problem:

Editing & releasing bad policy can result in the lost of productivity, outages, security breaches, and their trust in Google.

The Mission:

Increase customer confidence & reliance on Google by allowing them to *simulate* and *preview* IAM policy changes before applying them.

...think of this product as a playground.

Or in dev metaphors, a sandbox environment for policy, where there are no consequences if you make a mistake and you can learn and grow from it.

Hank: Platform Admin

Charlie wants to delegate control to team admins, while maintaining central control. He wants to ensure compliance with governance requirements while enabling developer teams to be very productive.

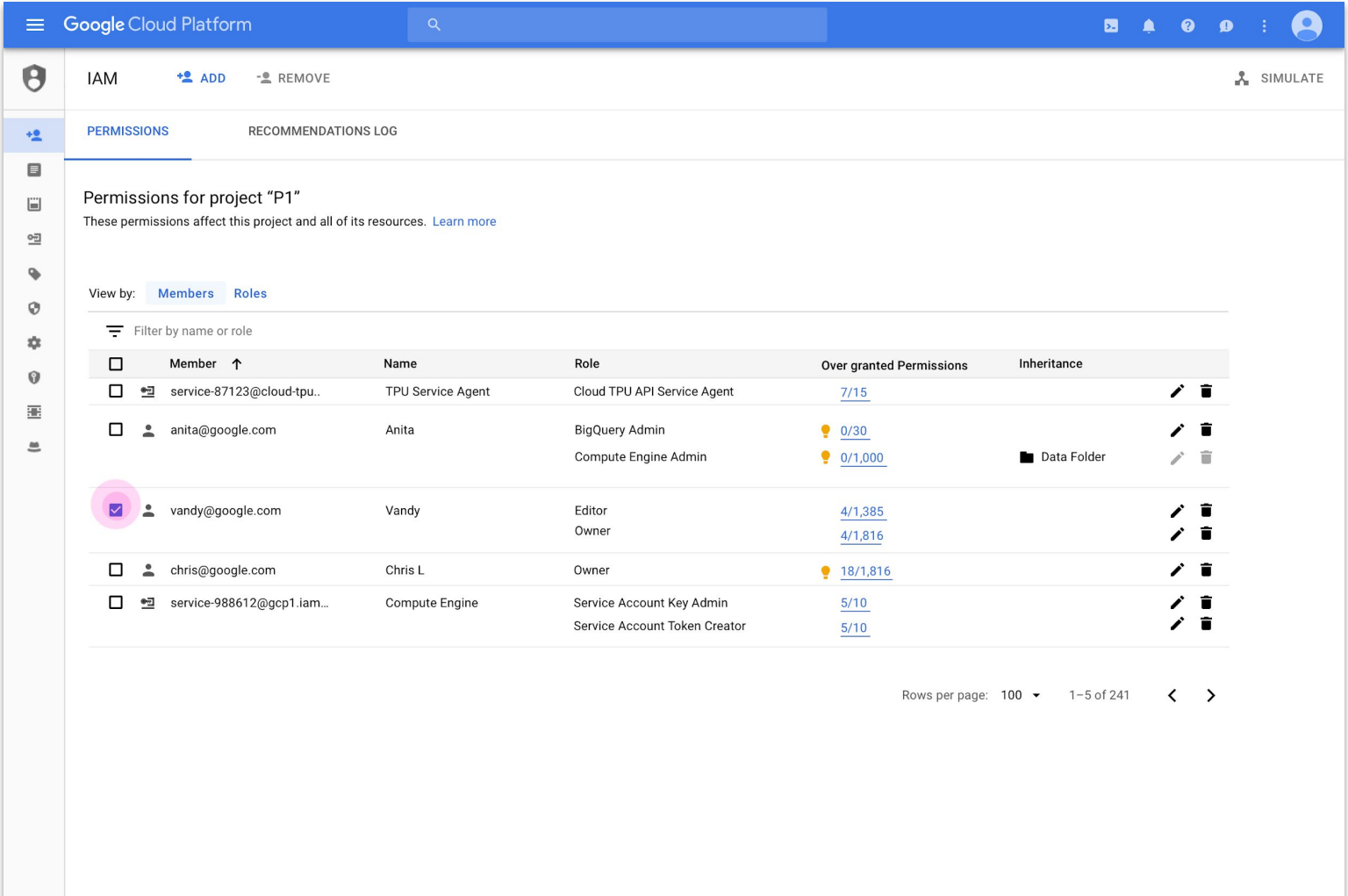
Veronica: Platform Admin

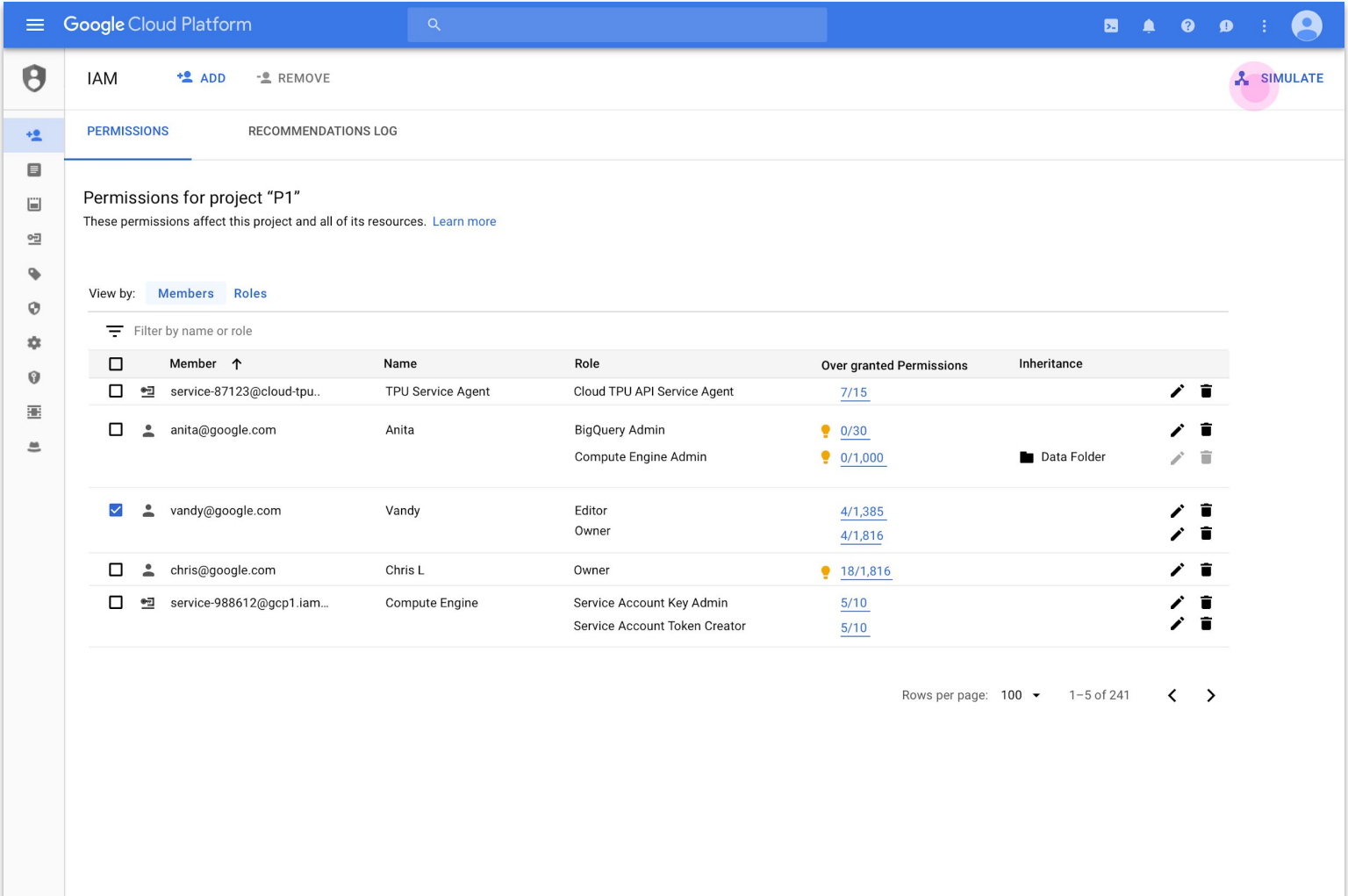
A software engineer that designs, builds, or sets up centralized infrastructure. Unlike Charlie, she is not involved in the day-to-day maintenance of the deployment.

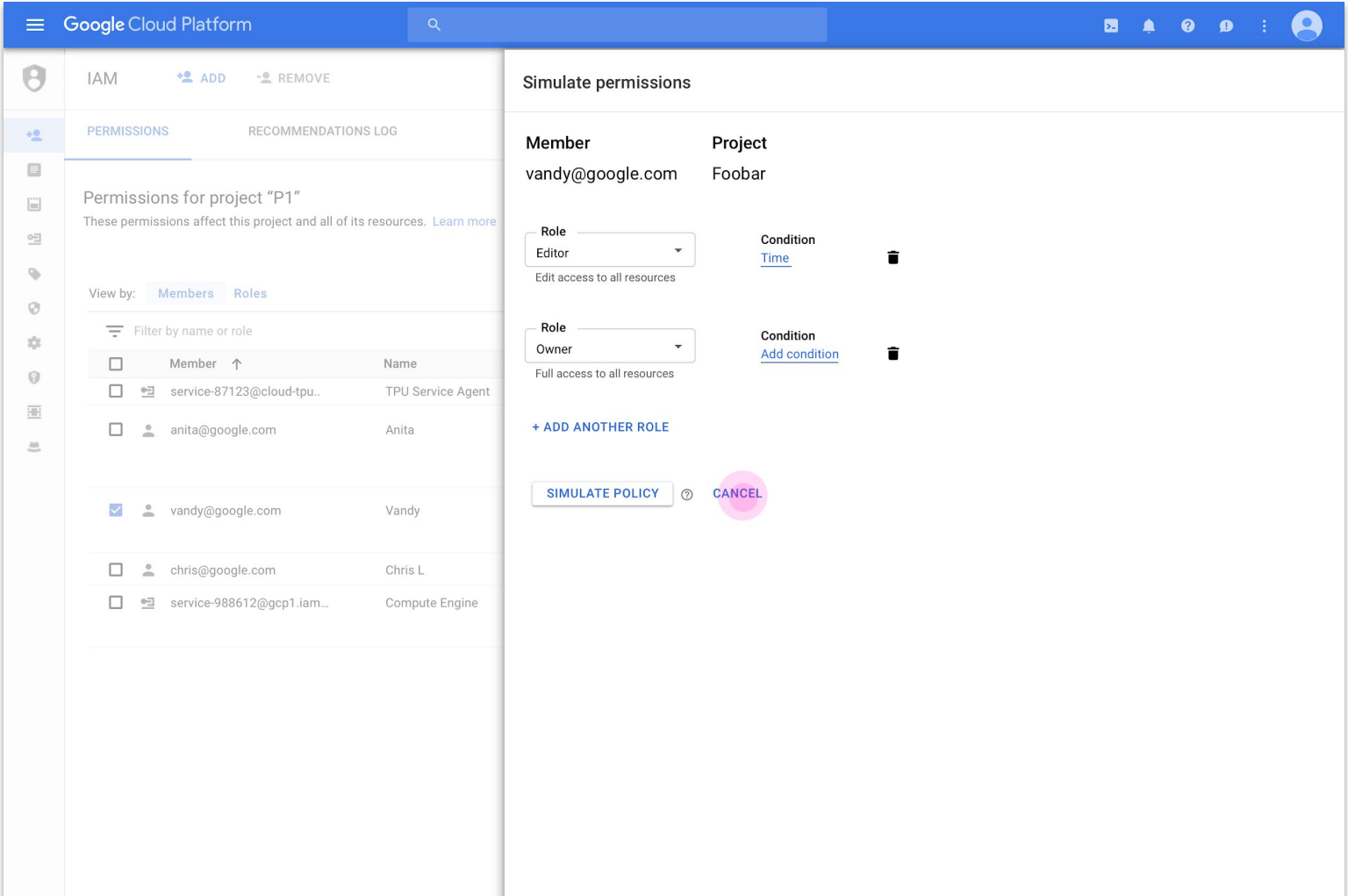
I want to simulate what access changes occur when I change a member's role from "Editor" to "Viewer" before applying this policy change.

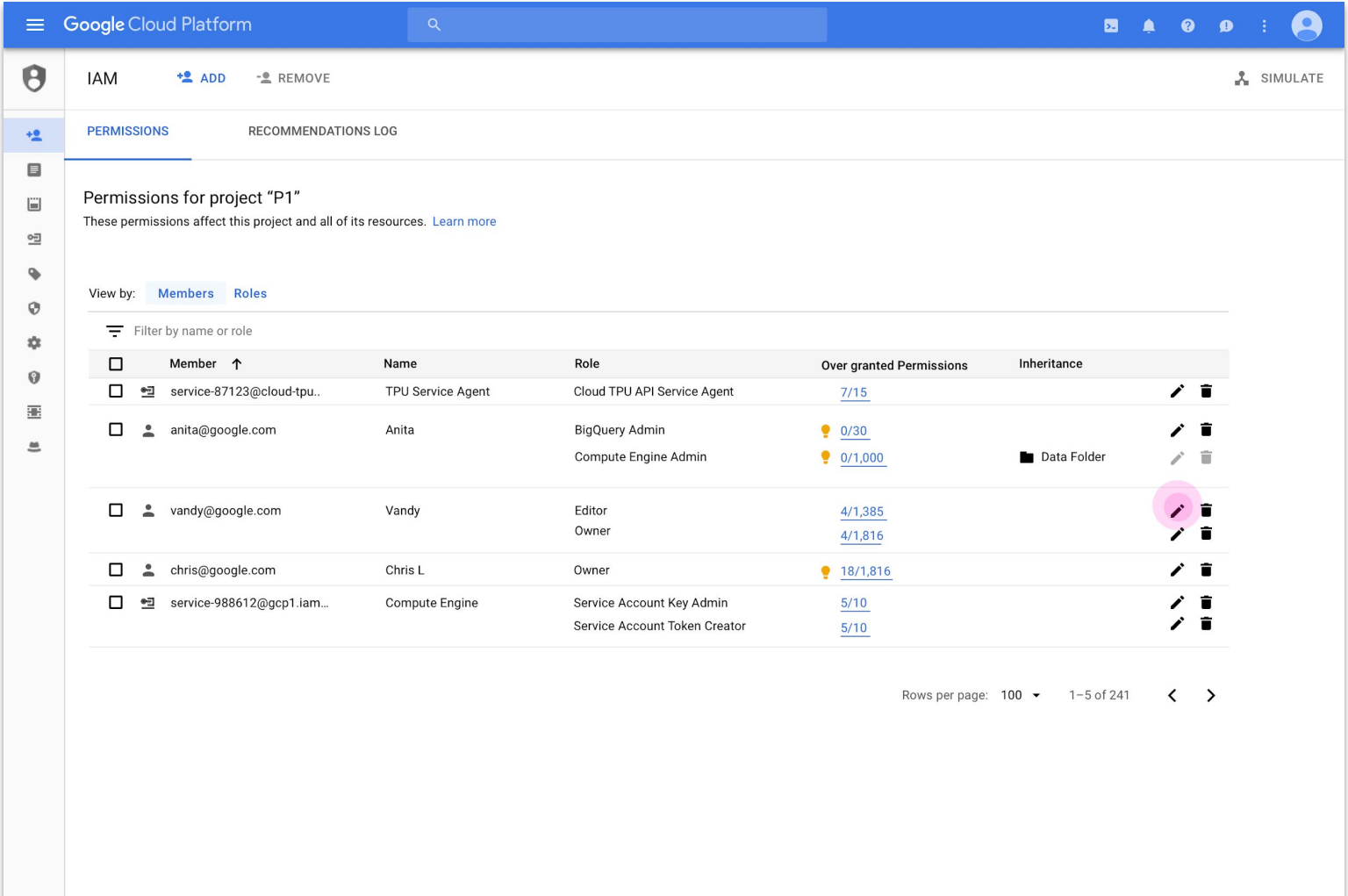
Mike
Game Infrastructure Lead at {Gaming Company X}

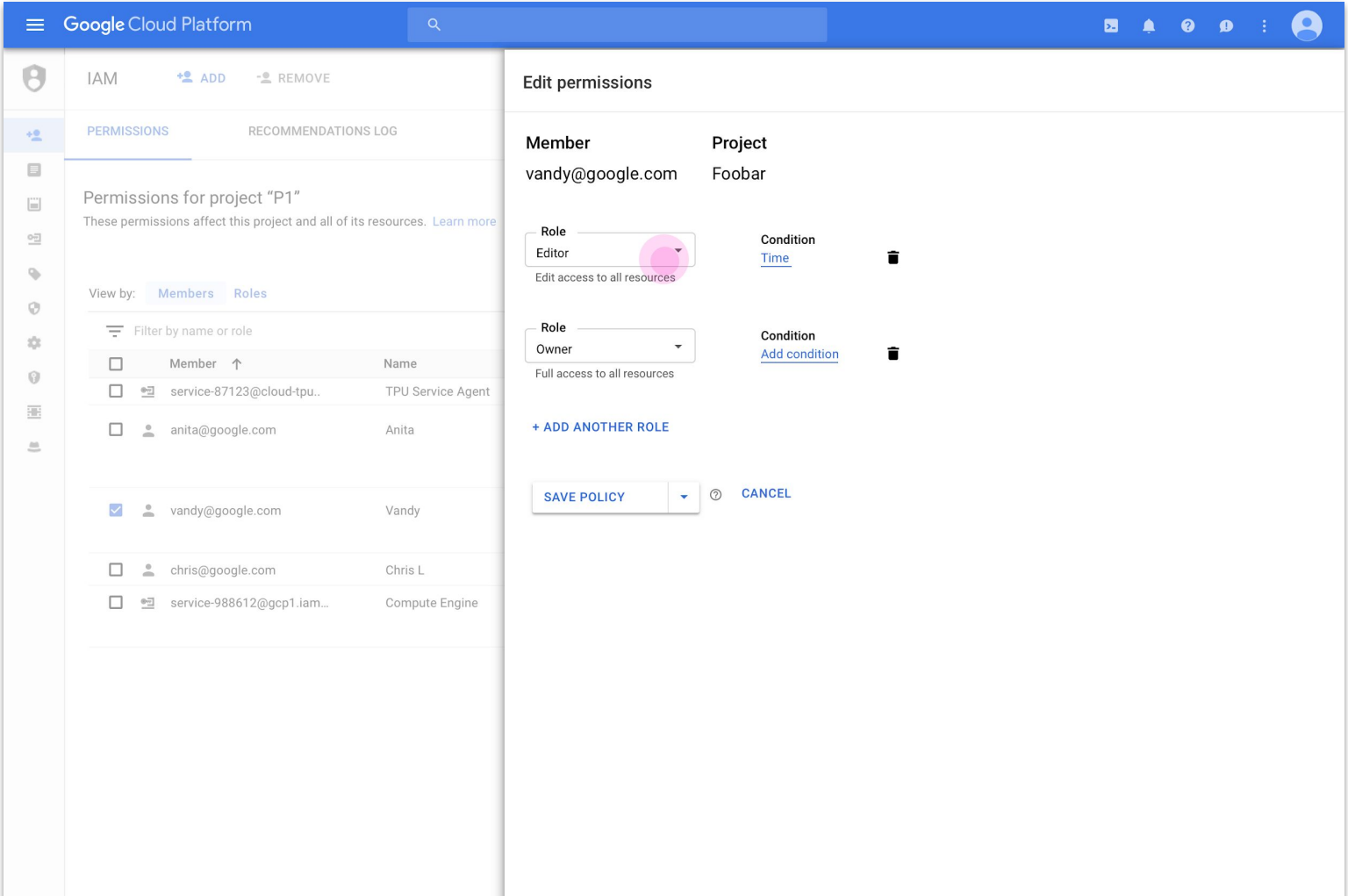
Let’s walk through Simulator.

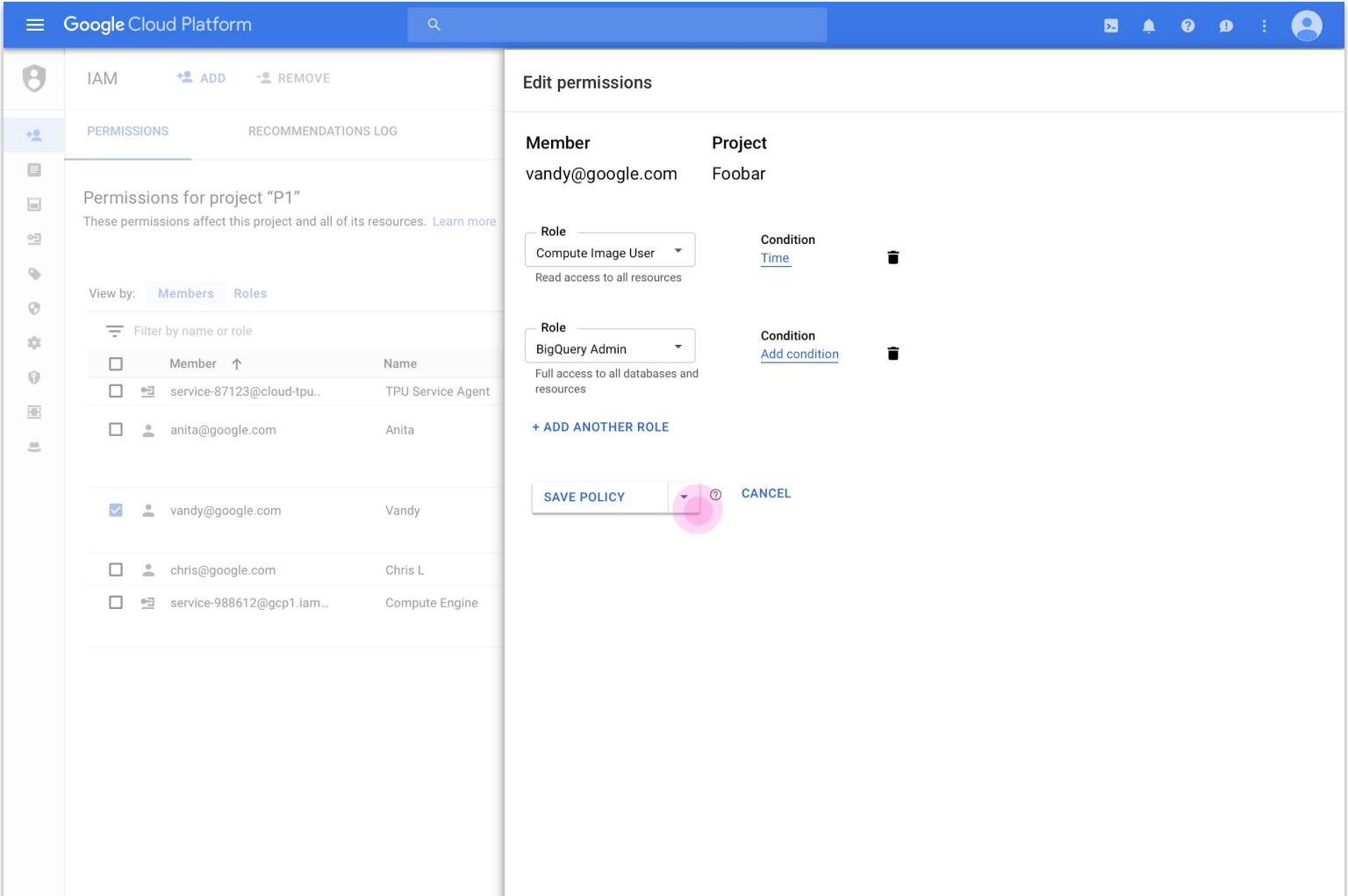

Google Cloud Platform
IAM
ADD
REMOVE
SIMULATE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
Role
Over granted Permissions
Inheritance
service-87123@cloud-tpu..
TPU Service Agent
Cloud TPU API Service Agent
7/15
anita@google.com
Anita
BigQuery Admin
0/30
Compute Engine Admin
0/1,000
Data Folder
vandy@google.com
Vandy
Editor
4/1,385
Owner
4/1,816
chris@google.com
Chris L
Owner
18/1,816
service-988612@gcp1.iam...
Compute Engine
Service Account Key Admin
5/10
Service Account Token Creator
5/10
Rows per page: 100
1–5 of 241

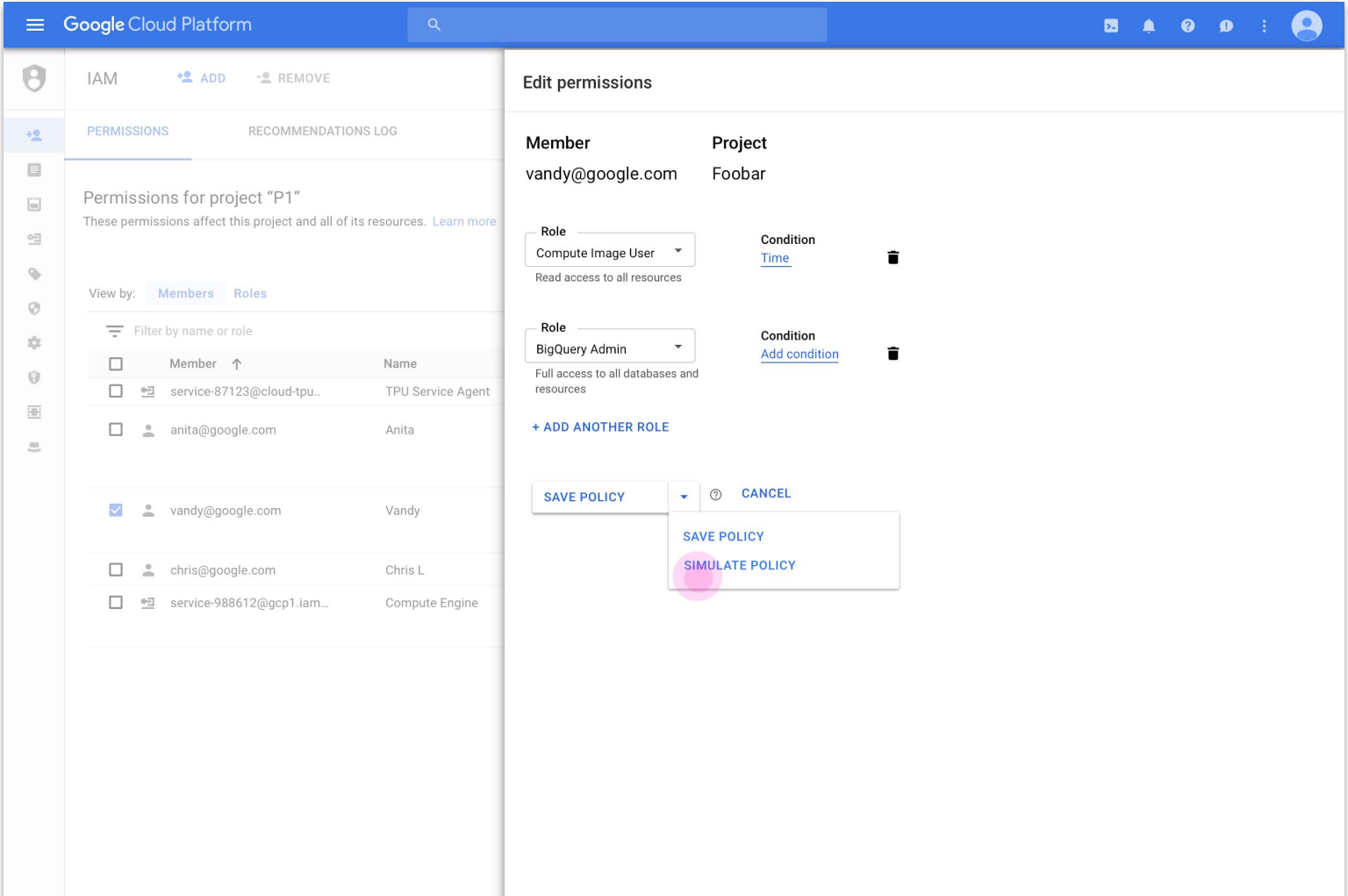

Google Cloud Platform
IAM
ADD
REMOVE
SIMULATE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
Role
Over granted Permissions
Inheritance
service-87123@cloud-tpu..
TPU Service Agent
Cloud TPU API Service Agent
7/15
anita@google.com
Anita
BigQuery Admin
0/30
Compute Engine Admin
0/1,000
Data Folder
vandy@google.com
Vandy
Editor
4/1,385
Owner
4/1,816
chris@google.com
Chris L
Owner
18/1,816
service-988612@gcp1.iam...
Compute Engine
Service Account Key Admin
5/10
Service Account Token Creator
5/10
Rows per page: 100
1–5 of 241

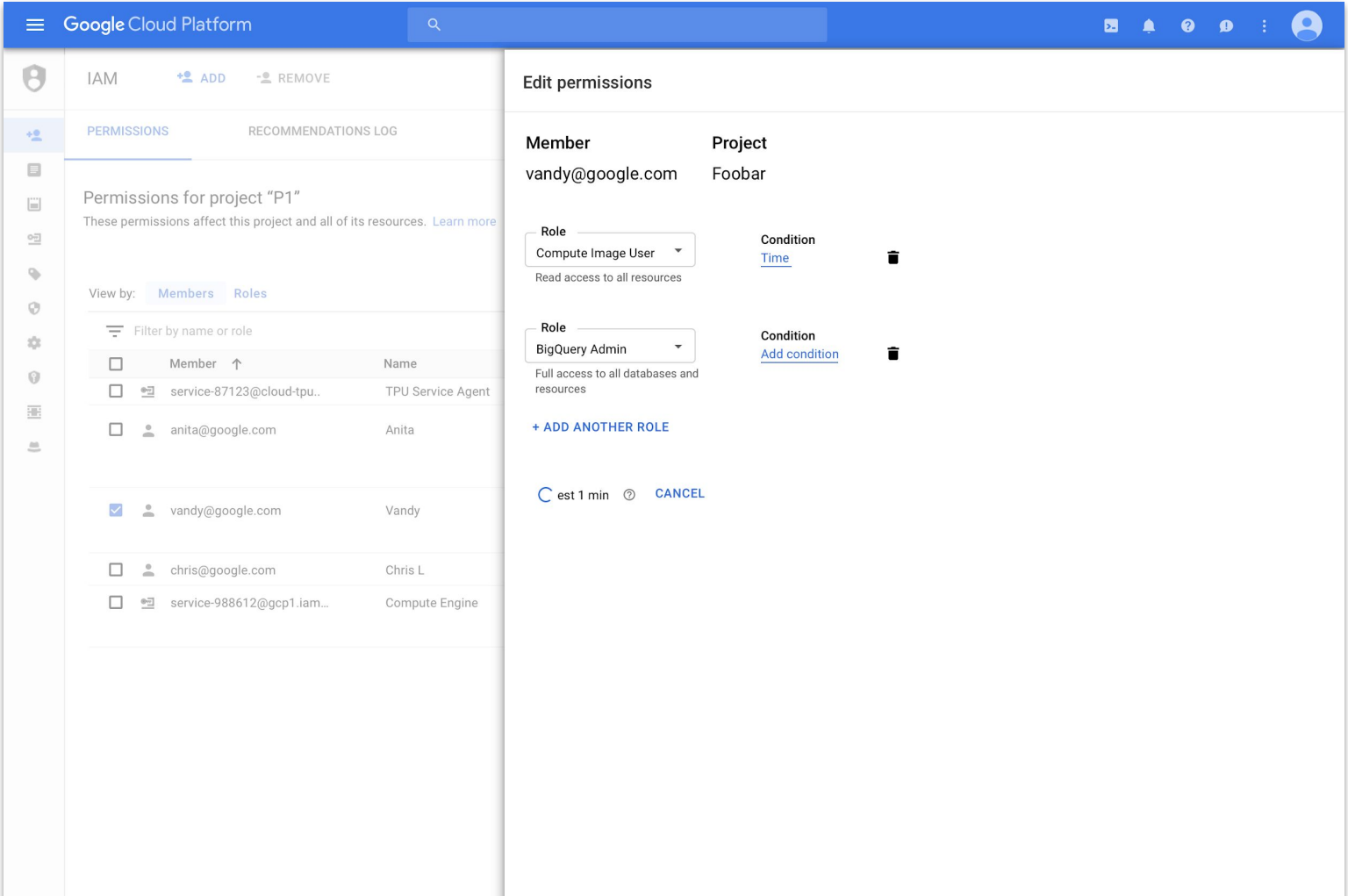

Google Cloud Platform
IAM
ADD
REMOVE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
service-87123@cloud-tpu..
TPU Service Agent
anita@google.com
Anita
vandy@google.com
Vandy
chris@google.com
Chris L
service-988612@gcp1.iam...
Compute Engine
Simulate permissions
Member
vandy@google.com
Project
Foobar
Role
Editor
Edit access to all resources
Condition
Time
Role
Owner
Full access to all resources
Condition
Add condition
+ ADD ANOTHER ROLE
SIMULATE POLICY
CANCEL

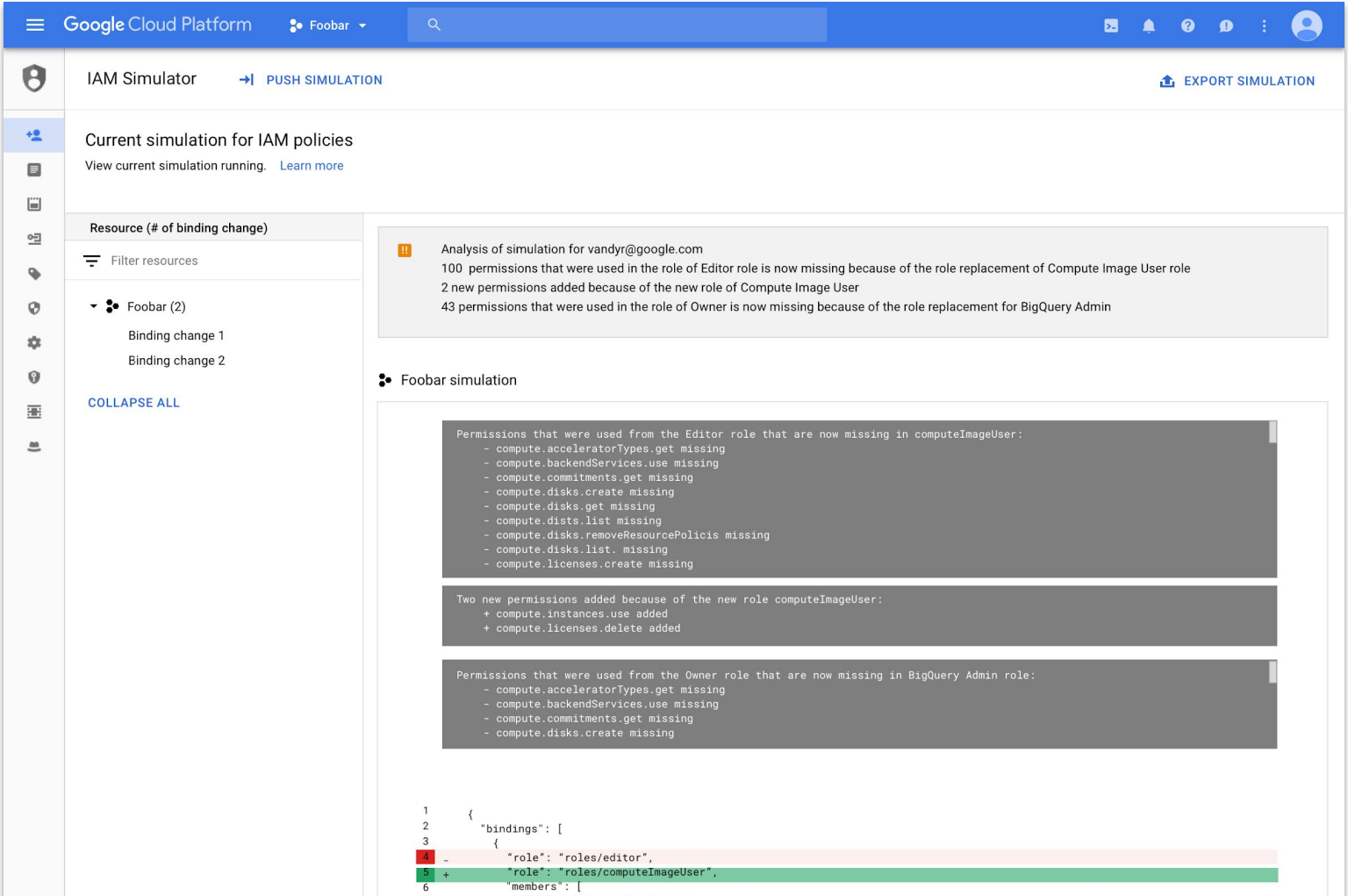

Google Cloud Platform
IAM
ADD
REMOVE
SIMULATE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
Role
Over granted Permissions
Inheritance
service-87123@cloud-tpu..
TPU Service Agent
Cloud TPU API Service Agent
7/15
anita@google.com
Anita
BigQuery Admin
0/30
Compute Engine Admin
0/1,000
Data Folder
vandy@google.com
Vandy
Editor
4/1,385
Owner
4/1,816
chris@google.com
Chris L
Owner
18/1,816
service-988612@gcp1.iam...
Compute Engine
Service Account Key Admin
5/10
Service Account Token Creator
5/10
Rows per page: 100
1–5 of 241


Google Cloud Platform
IAM
ADD
REMOVE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
service-87123@cloud-tpu..
TPU Service Agent
anita@google.com
Anita
vandy@google.com
Vandy
chris@google.com
Chris L
service-988612@gcp1.iam...
Compute Engine
Edit permissions
Member
vandy@google.com
Project
Foobar
Role
Editor
Edit access to all resources
Condition
Time
Role
Owner
Full access to all resources
Condition
Add condition
+ ADD ANOTHER ROLE
SAVE POLICY
CANCEL


Google Cloud Platform
IAM
ADD
REMOVE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
service-87123@cloud-tpu..
TPU Service Agent
anita@google.com
Anita
vandy@google.com
Vandy
chris@google.com
Chris L
service-988612@gcp1.iam...
Compute Engine
Edit permissions
Member
vandy@google.com
Project
Foobar
Role
Compute Image User
Read access to all resources
Condition
Time
Role
BigQuery Admin
Full access to all databases and resources
Condition
Add condition
+ ADD ANOTHER ROLE
SAVE POLICY
CANCEL


Google Cloud Platform
IAM
ADD
REMOVE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by: Members Roles
Filter by name or role
Member
Name
service-87123@cloud-tpu..
TPU Service Agent
anita@google.com
Anita
vandy@google.com
Vandy
chris@google.com
Chris L
service-988612@gcp1.iam...
Compute Engine
Edit permissions
Member
vandy@google.com
Project
Foobar
Role
Compute Image User
Read access to all resources
Condition
Time
Role
BigQuery Admin
Full access to all databases and resources
Condition
Add condition
+ ADD ANOTHER ROLE
SAVE POLICY
CANCEL
SAVE POLICY
SIMULATE POLICY


Google Cloud Platform
IAM
ADD
REMOVE
PERMISSIONS
RECOMMENDATIONS LOG
Permissions for project “P1”
These permissions affect this project and all of its resources. Learn more
View by:
Members
Roles
Filter by name or role
Member
Name
service-87123@cloud-tpu..
TPU Service Agent
anita@google.com
Anita
vandy@google.com
Vandy
chris@google.com
Chris L
service-988612@gcp1.iam...
Compute Engine
Edit permissions
Member
vandy@google.com
Project
Foobar
Role
Compute Image User
Read access to all resources
Condition
Time
Role
BigQuery Admin
Full access to all databases and resources
Condition
Add condition
+ ADD ANOTHER ROLE
est 1 min
CANCEL


Google Cloud Platform
Foobar
IAM Simulator
PUSH SIMULATION
EXPORT SIMULATION
Current simulation for IAM policies
View current simulation running. Learn more
Resource (# of binding change)
Filter resources
Foobar (2)
Binding change 1
Binding change 2
COLLAPSE ALL
Analysis of simulation for vandyr@google.com
100 permissions that were used in the role of Editor role is now missing because of the role replacement of Compute Image User role
2 new permissions added because of the new role of Compute Image User
43 permissions that were used in the role of Owner is now missing because of the role replacement for BigQuery Admin
Foobar simulation
Permissions that were used from the Editor role that are now missing in computeImageUser:
- compute.acceleratorTypes.get missing
- compute.backendServices.use missing
- compute.commitments.get missing
- compute.disks.create missing
- compute.disks.get missing
- compute.dists.list missing
- compute.disks.removeResourcePolicis missing
- compute.disks.list. missing
- compute.licenses.create missing
Two new permissions added because of the new role computeImageUser:
+ compute.instances.use added
+ compute.licenses.delete added
Permissions that were used from the Owner role that are now missing in BigQuery Admin role:
- compute.acceleratorTypes.get missing
- compute.backendServices.use missing
- compute.commitments.get missing
- compute.disks.create missing
{
"bindings": [
{
- "role": "roles/editor",
+ "role": "roles/computeImageUser",
"members": [

Binding change 1

Binding change 2

COLLAPSE ALL

Foobar simulation

```
Permissions that were used from the Editor role that are now missing in computeImageUser:
    - compute.acceleratorTypes.get missing
    - compute.backendServices.use missing
    - compute.commitments.get missing
    - compute.disks.create missing
    - compute.disks.get missing
    - compute.dists.list missing
    - compute.disks.removeResourcePolicis missing
    - compute.disks.list. missing
    - compute.licenses.create missing
```

```
Two new permissions added because of the new role computeImageUser:
    + compute.instances.use added
    + compute.licenses.delete added
```

```
Permissions that were used from the Owner role that are now missing in BigQuery Admin role:
    - compute.acceleratorTypes.get missing
    - compute.backendServices.use missing
    - compute.commitments.get missing
    - compute.disks.create missing
```

```
1    {
2      "bindings": [
3        {
4  -       "role": "roles/editor",
5  +       "role": "roles/computeImageUser",
6          "members": [
7            "group:watchers@foogle.com",
8            "user:vandyr@google.com",
9          ],
10         "condition": {
11           title: "Time Condition"
12           expression: 'resource.type == "iam.roles"
13           && request.time > timestamp("%sZ")'
14           },
15       },
16       {
17         "role": "roles/security",
18         "members": [
19           "group:admin@foogle.com"
20         ]
21       },
22       {
23 -       "role": "roles/owner",
24 +       "role": "roles/computeAdmin,"
25         "members": [
26           "group:dev-eng@foogle.com",
27         ]
28       }
29     ]
30     "etag": "123457"
31   }
```

Thank You