

Self Driving Cloud

Troubleshooter





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.

Troubleshooter is the **second product** within the self-driving cloud initiative that I have lead from inception to launch.

The Problem:

**Troubleshooting 403 error
messages is hard.**

It's done through lots of trial & error.

Admins troubleshoot by giving *more* permissions, which makes it hard to maintain least privilege.

What are we building?

Troubleshooter is the **second product launch** within the Self Driving Cloud suite of products. This product is meant to help over granting permissions by helping admins debug denial error messages.

Built on the IAM Recommender API, it was a sophisticated backend that needed to be unpacked simply in the UI.



Example User Scenario

Anita is a developer in your organization and gets an error message informing her that she *does not* have the relevant permissions when she tries to delete images in a bucket.

Anita goes to Mike, her security admin for help, who has to manually check the policy himself, and will end up expediting the process by just granting Anita a bunch of unnecessary roles.



Translating the API to GUI

The **engineers had approached me** with a predetermined sketch in mind.

After going through many rounds of the engineers' design solution, I was convinced that **their way was not the way to go**. Through lots of research, I changed product direction by designing a different way to display IAM bindings by showing raw json policy so that advanced users would be able to click through bindings via a tree hierarchy.

I was able to change product direction with multiple stakeholders with design thinking and creating a more visual tool for developers.

...FYI, here was the engineer's idea

The screenshot shows the Google Cloud Platform interface. The left sidebar contains navigation options: IAM & admin, IAM, Troubleshooting (highlighted), Organization policies, Service accounts, Labels, GCP Privacy & Security, Settings, and Roles. The main content area is titled 'Troubleshooting' and displays a heading: 'Check on anita@google.com's bucket.update permission on bucket/goo1'. Below this is a warning message: 'You don't have permission to check the role and one of the groups here.' A table titled 'Filter table' is shown with columns: Resource, Role check, Principal check, and Conditions. The table lists several resources, with the last two rows highlighted by a pink circle.

Resource	Role check	Principal check	Conditions
▶ Foogle			⋮
▶ folder/foo2			⋮
▶ folder/foo2			⋮
▶ project/bar2	⚠		⋮
▶ bucket/goo1	✔ Check	❌ No check	⋮
▶ bucket/goo1	❌ No check	✔ Check	⋮

...another example.

Google Cloud Platform Project

IAM & admin

- IAM
- Helpdesk
- Organization policies
- Service accounts
- Labels
- GCP Privacy & Security
- Settings
- Roles

Helpdesk [VIEW TICKET](#)

Week of February 5, 2018 - February 11, 2018

Total events this week 5	Resolved 3	Pending 2	Recommendations 4
-----------------------------	---------------	--------------	----------------------

Log of all deny events for the past 7 days

Filter log

<input type="checkbox"/> Status	Date ↑	User ↑	Email address	Time	Permission	Request Attributes
<input type="checkbox"/> !	Feb 3, 2018	Anita Roy	anita@company.com	9:50 PM	Bucket.write	IP Address Time of day
<input type="checkbox"/> !	Feb 3, 2018	Carolyn Huynh	carolyn@company.com	8:00 PM	Bucket.stuff	Time of day
<input type="checkbox"/> ✓	Feb 2, 2018	Sarah W.	sarah@company.com	11:00 PM	Foo.bar	Another reason
<input type="checkbox"/> ✓	Feb 1, 2018	Vandy Ramadurai	vandy@company.com	4:00 AM	Other.stuff	Foo bar reason
<input type="checkbox"/> ✓	Jan 31, 2018	Felix M.	felix@company.com	3:00 AM	Bucket.edit	IP Address

...annnd one more.

Google Cloud Platform Project

IAM & admin

- IAM
- Helpdesk
- Organization policies
- Service accounts
- Labels
- GCP Privacy & Security
- Settings
- Roles

Helpdesk [VIEW TICKET](#)

Week of February 5, 2018 - February 11, 2018

Total events this week: 5 Resolved: 3

Log of all deny events for the past 7 days

pending

<input type="checkbox"/>	Status	Date ↑	User ↑
<input checked="" type="checkbox"/>	!	Feb 3, 2018	Anita Roy
<input type="checkbox"/>	!	Feb 3, 2018	Carolyn Hu

Ticket #000

View policy heirarchy ! [Export all policies](#)

Org name (Google)

Member/Group	Storage Admin Group
Permissions	Bucket Manager - custom role
Conditions	none
Outcome of check	Denied

Folder-A Name

Member/Group	Anita Roy
Permissions	Folder Admin Role
Conditions	SFO Office IP
Outcome of check	Denied

Project Name

Bucket (S2)

Deny incident !

User	anita@company.com
Permission	Bucket.write
Status	Denied
Time	9:50PM
Permission	S2
Request Attributes	IP Address
	Time of day

[GRANT ACCESS](#)

No matter how many **versions of tables** I designed, the **problem was that developers** still couldn't understand and **debug readable text.**

...jk, last one.

Google Cloud Platform

IAM & admin

- IAM
- Troubleshooting
- Organization policies
- Service accounts
- Labels
- GCP Privacy & Security
- Settings
- Roles

← Troubleshooting

Check on anita@google.com's bucket.delete permission on bucket/goo

Checker status

- Conditional

Filter table

Checker ↑	Resource ↑	Role	Principal	Conditions
▼ Denied	Foogle.com	✓ Owner	✗ group/admin	
		✓ Owner	✗ group/boss	
		✓ Editor	✗ group/exec	
▼ Conditional	folder/dev	✓ Owner	✗ group/admin	
		✗ Security	✗ group/watchers	
		✓ Editor	✓ group/dev-eng	From 9AM - 5PM
▼ Denied	folder/dev-SFO	✓ Owner	✗ group/sfo-admin	
		✗ Security reviewer	✗ group/sfo-watchers	
▼ Denied	project/demo			

```
{
  "bindings": [
    {
      "members": [
        "user:jie@example.com"
      ],
      "role": "roles/resourcemanager.organizationAdmin"
    },
    {
      "members": [
        "user:divya@example.com",
        "user:jie@example.com"
      ],
      "role": "roles/resourcemanager.projectCreator"
    }
  ],
  "etag": "BwUjMhCsNvY=",
  "version": 1
}
```

Research

Research had shown that the original idea behind the engineer's mocks for the product had one consistent theme:

Nobody could tell that each row in the table represented a binding within an IAM policy.

So, I literally went through the API and the subsequent raw json policy and began scrubbing it, in an attempt to find UI components that would explicitly show what each section of the policy meant.

I decided to be as **explicit as possible** and **expose raw json policy**, just like how developers see it today.

I took a look at some of the most competitive products on the market and **understood a rising trend in policy-as-code**.

I decided to **mimic the policy-as-code** trend as best as I could, while understanding the **constraints of the API**.

We couldn't provide a way to version control policy, but we **could** provide a way for customers to integrate with **3rd party tools** that will allow them to.

```
{
  "bindings": [
    {
      "members": [
        "user:jie@example.com"
      ],
      "role": "roles/resourcemanager.organizationAdmin"
    },
    {
      "members": [
        "user:divya@example.com",
        "user:jie@example.com"
      ],
      "role": "roles/resourcemanager.projectCreator"
    }
  ],
  "etag": "BwUjMhCsNvY=",
  "version": 1
}
```



A preview of the end solution I designed.

The screenshot shows the Google Cloud Platform IAM & admin console. The left sidebar contains navigation options: IAM, Troubleshooter, Organization policies, Service accounts, Labels, GCP Privacy & Security, Settings, and Roles. The main content area displays a breadcrumb trail: ← 11 bindings are affecting bucket/goo throughout the resource hierarchy. Below this, there are sections for 'Bindings by resource' and a detailed view of the 'dev's policy'. The 'dev's policy' section shows a list of bindings with a red highlight on the 'dev's policy' header. The bindings list includes:

- Owner role binding (with a red minus icon)
- Security role binding (with a red minus icon)
- Editor role binding (with a grey minus icon)

The detailed view of the 'dev's policy' shows a JSON configuration with the following bindings:

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

There is a condition in this binding

Access granted if condition is true for API call for anita@foogle.com, bucket.delete, bucket/goo. For further information and assistance, contact your support team. [CONTACT SUPPORT](#)



Research 2.0

My researcher ran with my idea of exposing raw json (something that **hadn't been done before within GCP**), and we **ran lots of customer sessions**, often times changing up the **design on the spot**.

The **PM of Troubleshooter** was impressed by the amount of praise the new UI was getting from customers, and began to take the idea of exposing the raw policy and **reusing** the pattern in other areas of self driving cloud.



Expert interface. Looks just like an API response.

Customer on GCP
Name and Company redacted

(I swear they said this).



Now, let's walk through the whole product from **start to finish**.



IAM & admin

IAM

Troubleshooting

Organization policies

Service accounts

Labels

GCP Privacy & Security

Settings

Roles

Troubleshooter

IAM Troubleshooter assesses if a specific API call will grant the identity access to a resource.

Troubleshooter ⓘ

If you have data access logs turned on, you can retrieve them from [Stackdriver](#)

Principal

Enter email address such as user@company.com

Permission

Enter the permission such as "storage.buckets.getIamPolicy"

Resource

Enter the name of the resource on the API call

CLEAR

CHECK API CALL



IAM & admin

IAM

Troubleshooting

Organization policies

Service accounts

Labels

GCP Privacy & Security

Settings

Roles

Troubleshooter

IAM Troubleshooter assesses if a specific API call will grant the identity access to a resource.

Troubleshooter ⓘ

If you have data access logs turned on, you can retrieve them from [Stackdriver](#)

Principal

anita@foogle.com ⓘ

Enter email address such as user@company.com

Permission

bucket.delete ⓘ

Enter the permission such as "storage.buckets.getIamPolicy"

Resource

bucket/goo ⓘ

Enter the name of the resource on the API call

CLEAR

CHECK API CALL

IAM & admin

← 11 policy bindings are affecting bucket/goo throughout the resource hierarchy

IAM

Troubleshooter

Organization policies

Service accounts

Labels

GCP Privacy & Security

Settings

Roles

Bindings by resource

🗄️ Foogle's policy (3)

Owner role binding 🔴

Viewer role binding 🔴

Editor role binding 🔴

👤 dev's policy (3)

Owner role binding 🔴

Security role binding 🔴

Editor role binding 🔴

👤 dev-SFO's policy (3)

Owner role binding 🔴

Security reviewer role binding 🔴

👤 demo's policy (2)

Owner role binding 🔴

Editor role binding 🔴

🗄️ goo's policy (1)

Editor role binding 🔴

[COLLAPSE ALL BINDINGS](#)

🔴 Access denied for API call for anita@foogle.com, bucket.delete, bucket/goo.
For further information and assistance, contact your support team.

[CONTACT SUPPORT](#)


🗄️ Foogle's policy

```
1 {
2   "bindings": [
3     {
4       "role": "roles/owner",
5       "members": [
6         "group:adminfoogle.com",
7       ]
8     },
9     {
10      "role": "roles/viewer",
11      "members": [
12        "group:boss@foogle.com"
13      ]
14     },
15     {
16      "role": "roles/editor",
17      "members": [
18        "group:exec@foogle.com",
19      ]
20     }
21   ]
22   "etag": "123457"
23 }
```


👤 dev's policy

```
1 {
2   "bindings": [
3     {
4       "role": "roles/owner",
5       "members": [
6         "group:watchers@foogle.com",
7       ]
8     },
9     {
10      "role": "roles/security",
11      "members": [
12        "group:admin@foogle.com"
13      ]
14     },
15     {
16      "role": "roles/editor",
17      "members": [
18        "group:dev-eng@foogle.com",
19      ]
20     }
21   ]
22   "etag": "123457"
23 }
```


dev-SFO's policy (3)

Owner role binding Security reviewer role binding 


demo's policy (2)

Owner role binding Editor role binding 

goo's policy (1)

Editor role binding 

COLLAPSE ALL BINDINGS

dev json policy copied anita@foogle.com is not
in group

```

14 },
15   "role": "roles/editor",
16   "members": [
17     "group:exec@foogle.com",
18   ]
19 }
20 }
21 }
22 "etag": "123457"
23 }

```

dev's policy

anita@foogle.com is not
in group

```

1 {
2   "bindings": [
3     {
4       "role": "roles/owner",
5       "members": [
6         "group:watchers@foogle.com",
7       ]
8     },
9     {
10      "role": "roles/security",
11      "members": [
12        "group:admin@foogle.com"
13      ]
14    },
15    {
16      "role": "roles/editor",
17      "members": [
18        "group:dev-eng@foogle.com",
19      ]
20    }
21  ]
22  "etag": "123457"
23 }

```

dev-SFO's policy

anita@foogle.com is not
in groupbucket.delete
permission is not in
role
anita@foogle.com is not
in group

```

1 {
2   "bindings": [
3     {
4       "role": "roles/owner",
5       "members": [
6         "group:sfo-admin@foogle.com",
7       ]
8     },
9     {
10      "role": "roles/security-reviewer",
11      "members": [
12        "group:sfo-watchers@foogle.com"
13      ]
14    }
15  ]
16  "etag": "123457"
17 }

```

demo's policy

```

1 {
2   "bindings": [
3     {

```



IAM & admin

← 11 bindings are affecting bucket/goo throughout the resource hierarchy

IAM

Troubleshooter

Organization policies

Service accounts

Labels

GCP Privacy & Security

Settings

Roles

Bindings by resource

▶️ 📁 Foogle's policy (3)

▼ 📁 dev's policy (3)

Owner role binding



Security role binding



Editor role binding



▶️ 📁 dev-SFO's policy (3)

▶️ 📁 demo's policy (2)

▶️ 📁 goo's policy (1)

[EXPAND ALL BINDINGS](#)

⊖ Access granted if condition is true for API call for anita@foogle.com, bucket.delete, bucket/goo.
For further information and assistance, contact your support team.

[CONTACT SUPPORT](#)

📁 dev's policy

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

anita@foogle.com is not in group

bucket.delete

permission is not in role

anita@foogle.com is not in group

There is a condition in this binding

← 11 bindings are affecting bucket/goo throughout the resource hierarchy

IAM

Troubleshooter

Organization policies

Service accounts

Labels

GCP Privacy & Security

Settings

Roles

Bindings by resource

⚠ There are policy bindings that are not shown because you do not have permissions to see them.

dev's policy (3)

Owner role binding -

Security role binding -

Editor role binding -

dev-SFO's policy (3)

demo's policy (2)

goo's policy (1)

[EXPAND ALL BINDINGS](#)

- Access denied for API call for anita@foogle.com, bucket.delete, bucket/goo. You do not have permission to view all policy bindings affecting bucket/goo. You do not have permission to view specific group memberships. For further information and assistance, contact your support team.

[CONTACT SUPPORT](#)

dev's policy

```

1  {
2  "bindings": [
3  {
4    "role": "roles/owner",
5    "members": [
6      "group:watchers@foogle.com",
7    ]
8  },
9  {
10   "role": "roles/security",
11   "members": [
12     "group:admin@foogle.com"
13   ]
14 },
15 {
16   "role": "roles/editor",
17   "members": [
18     "group:dev-eng@foogle.com",
19   ]
20 }
21 ]
22 "etag": "123457"
    
```

anita@foogle.com is not in group

bucket.delete permission is not in role
anita@foogle.com is not in group

You do not know if anita@foogle.com is in this group or not because you do not have permission to view group membership.

Debuted on stage at **Google Cloud NEXT**.

One of the **top most used products** within GCP, making close to a **[redacted #]** API calls a month.

Key Takeaways & Reflections

As the **Lead Designer** (and *only* designer) to ship a second **self driving cloud** product...



1

Accessibility

Since this is highly visual tool that really (and literally) highlights areas that helps developers debug 403 messages, in a mad rush to ship, I had forgotten the most *foundational* part of shipping any visual tool: accessibility.

I hadn't taken into account those were were colorblind.



2

Accessibility

I knew my mistake immediately after we shipped.

Unlike role recommender which had the traditional +/- pattern, (which by the way, is the standard way for those who are colorblind to go through a code diff), Troubleshooter didn't have that pattern.



3

Accessibility

I knew that icons were needed, along with a hidden tag within each icon that would describe what each denial message meant.

I deeply regretted this error, and as someone who prides myself n being an inclusive designer, I knew I had excluded a large portion of users..

Though I talk a lot about inclusivity in design, I hadn't even **held myself accountable**, and had prioritized **shipping > doing right by the user**. It ended up creating tech debt to fix the problem.

I will do **much, *much* better** next time.

As we all should.



Thank You