

Self Driving Cloud

Policy Analyzer





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.

Policy Analyzer is the **fourth and last product** within the self-driving cloud initiative that I have lead from inception to launch.

The Problem:

Reviewing access for internal governance & compliance is time consuming and painful because it's a manual process.

The Mission:

Analyzer helps customers understand who has access to what. It's backed by a power API that audits, analyzes, and investigates incidents related to access.

Let's walk through Policy Analyzer.

Policy reporting

[QUERY TEMPLATES](#)[POLICY CHANGE HISTORY](#)

Policy Reporting on org "Foo-bar"

The Policy Reporting tool allows you to figure out "who has access to what" across the resource hierarchy within your org. It also supports Group membership. [Learn more](#)

Create query from template

Select canned templates below to run a quick query. Top query questions are listed below each category template to help guide.

Query on principal

Show principals (service accounts, users, groups) with certain access to a resource.

Example

Who are the billing admins on Project A?

[CREATE PRINCIPAL QUERY](#)

Query on access

Show roles or permissions a principal has on a resource.

Example

What role does John have on a VM?

[CREATE ACCESS QUERY](#)

Query on resource

Show resources that a principal has access to, where you can define the access as well.

Example queries:

What buckets can Lily delete in project/foobar?

[CREATE RESOURCE QUERY](#)

Templated query on principal

Who can act as a service account?

[CREATE PRINCIPAL QUERY](#)

Templated query on access

What access does this terminated employee have on my production project?

[CREATE ACCESS QUERY](#)

Templated query on resource

What projects do this service account have assigned with owner or editor roles?

[CREATE RESOURCE QUERY](#)


Templated query on principal

Who can read data from this GCS bucket?


[CREATE PRINCIPAL QUERY](#)

← Query on principal


Select another template

 Query on principal

Show access grants for principals (service accounts, users, groups).

 Query on access

Show access grants on roles, permissions or both.

 Query on resource

Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Group option

List individual users inside groups in the result page

RUN QUERY

CANCEL

[← Query on principal](#)

Select another template

Query on principal

Show access grants for principals (service accounts, users, groups).

Query on access

Show access grants on roles, permissions or both.

Query on resource

Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Role

Example: Storage Admin (storage.buckets.delete)





Group option


 List individual users inside groups in the result page

← Query on principal

Select another template

 **Query on principal**
Show access grants for principals (service accounts, users, groups).

 **Query on access**
Show access grants on roles, permissions or both.

 **Query on resource**
Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Role

Example: Storage Admin (storage.buckets.delete)

-
- Browser
 - Editor
 - Owner**
 - Viewer
 - Access Approval Approver
 - Access Approval Config Editor
 - Access Approval Viewer
 - Android Management User
 - App Engine Admin
 - App Engine Viewer
 - App Engine Code Viewer
 - App Engine Deployer
 - App Engine Service Admin

RUN QUERY

CANCEL

[← Query on principal](#)

Select another template

Query on principal

Show access grants for principals (service accounts, users, groups).

Query on access

Show access grants on roles, permissions or both.

Query on resource

Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Role

Example: Storage Admin (storage.buckets.delete)



Group option

 List individual users inside groups in the result page

← Query on principal

Select another template

Query on principal

Show access grants for principals (service accounts, users, groups).

Query on access

Show access grants on roles, permissions or both.

Query on resource

Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Search input field containing "project/foobar/12345"

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Role

Example: Storage Admin (storage.buckets.delete)

Text input field containing "Owner" with a trash icon to its right

ADD ROLE button with a dropdown arrow

- ADD ROLE
- ADD PERMISSION

Group option


List individual users inside groups in the result page


RUN QUERY


CANCEL

← Query on principal

Select another template

 **Query on principal**
Show access grants for principals (service accounts, users, groups).

 **Query on access**
Show access grants on roles, permissions or both.

 **Query on resource**
Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Role

Example: Storage Admin (storage.buckets.delete)



Permission

Example: storage.buckets.delete

Search

- accessapproval.requests.approve
- accessapproval.requests.dismiss
- accessapproval.requests.get
- accessapproval.requests.list
- accessapproval.settings.get**
- accessapproval.settings.update
- accesscontextmanager.accessLevels.create
- accesscontextmanager.accessLevels.delete
- accesscontextmanager.accessLevels.get
- accesscontextmanager.accessLevels.list
- accesscontextmanager.accessLevels.update
- accesscontextmanager.accessPolicies.create
- accesscontextmanager.accessPolicies.delete

[← Query on principal](#)

Select another template

Query on principal

Show access grants for principals (service accounts, users, groups).

Query on access

Show access grants on roles, permissions or both.

Query on resource

Show resources that a certain principal has access to within a project.

Query on principal

Ex: "Who are the billing admins on Project A?"

Select resource

Example: projects/my-project

Select roles or permissions, or both

Select IAM role to query on the selected resource above. Multiple roles and permissions allowed.

Role

Example: Storage Admin (storage.buckets.delete)


Permission

Example: storage.buckets.delete

Group option

 List individual users inside groups in the result page

← Report on principal

 API time constrained. Some results might be incomplete.

Query parameters
























































Resource	project/foo/bar/12345
Role	Owner
Permission	accessapproval.settings.get

Results

A full result of individual bindings and access grants mapped to the resource, based off the queried parameters above.

 Filter access

	Resource	Principal ↑	Role grant	Permission grant	Inheritance	
<input type="checkbox"/>	 foobar/12345	 vandyrgoogle.com	Owner		 Google	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 830334396924@foobar...	Owner	access.approval.settings.get	 Sandbox	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 sophia@google.com	Owner	access.approval.settings.get	 Data Folder	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 chris@google.com	Owner		 Prod	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 carolyn@google.com	Owner		 Vision-2020	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 107261923744@foobar...	Owner		 Alphabet	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 dominique@google.com	Owner	access.approval.settings.get	 Verily	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 laura@google.com	Owner	access.approval.settings.get	 Ads	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 dev-ux@google.com (36) 	Owner		 Vision-2019	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 prod@google.com (12) 	Owner	access.approval.settings.get	 VM-image-store	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 dev-admin@google.com (3) 	Owner	access.approval.settings.get	 London Fog	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 matt@google.com		access.approval.settings.get	 Prod-2020	VIEW BINDING 
<input type="checkbox"/>	 foobar/12345	 lane@google.com	Access Context Manager Admin	access.approval.settings.get	 Test	VIEW BINDING 

Rows per page: 100 1-13 of 13  

[EXPAND TO VIEW ALL BINDINGS](#)

← Report on principal

⚠ API time constrained. Some results might be incomplete.

Query parameters

Resource	project/foo/bar/12345
Role	Owner
Permission	accessapproval.settings.get

Results

A full result of individual bindings and access grants mapped to the resource, based off the queried parameters above.

Filter access

Close, Refresh, Filter icons

	Resource	Principal ↑	Role grant	Permission grant	Inheritance	
<input type="checkbox"/>	foobar/12345	vandyr@google.com	Owner		Google	VIEW BINDING
<input type="checkbox"/>	foobar/12345	830334396924@foobar...	Owner	access.approval.settings.get	Sandbox	View binding
<input type="checkbox"/>	foobar/12345	sophia@google.com	Owner	access.approval.settings.get	Data Folder	View policy history
<input type="checkbox"/>	foobar/12345	chris@google.com	Owner		Prod	VIEW BINDING
<input type="checkbox"/>	foobar/12345	carolyn@google.com	Owner		Vision-2020	VIEW BINDING
<input type="checkbox"/>	foobar/12345	107261923744@foobar...	Owner		Alphabet	VIEW BINDING
<input type="checkbox"/>	foobar/12345	dominique@google.com	Owner	access.approval.settings.get	Verily	VIEW BINDING
<input type="checkbox"/>	foobar/12345	laura@google.com	Owner	access.approval.settings.get	Ads	VIEW BINDING
<input type="checkbox"/>	⚠ foobar/12345	dev-ux@google.com (36) ✓	Owner		Vision-2019	VIEW BINDING
<input type="checkbox"/>	⚠ foobar/12345	prod@google.com (12) ✓	Owner	access.approval.settings.get	VM-image-store	VIEW BINDING
<input type="checkbox"/>	⚠ foobar/12345	dev-admin@google.com (3) ✓	Owner	access.approval.settings.get	London Fog	VIEW BINDING
<input type="checkbox"/>	foobar/12345	matt@google.com		access.approval.settings.get	Prod-2020	VIEW BINDING
<input type="checkbox"/>	foobar/12345	lane@google.com	Access Context Manager Admin	access.approval.settings.get	Test	VIEW BINDING

Rows per page: 100 1-13 of 13

EXPAND TO VIEW ALL BINDINGS

← Report on principal

BINDING FOR VANDY@GOOGLE.COM

POLICY HISTORY FOR GOOGLE

⚠ API time constrained. Some results may be missing.

Query parameters

Resource	project/fo
Role	Owner
Permission	accessap

Results

A full result of individual bindings and

☰ Filter access

	Resource	P
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	⚠ foobar/12345	
<input type="checkbox"/>	⚠ foobar/12345	
<input type="checkbox"/>	⚠ foobar/12345	
<input type="checkbox"/>	foobar/12345	
<input type="checkbox"/>	foobar/12345	

```
1 {
2   "role": "roles/owner",
3   "members": [
4     "group:watchers@foogle.com",
5     "user:anita@google.com",
6     "user:vandy@google.com",
7     "user:chris@google.com",
8     "user:sophia@google.com"
9   ]
10 }
11
```

EXPAND TO VIEW ALL BINDINGS

CANCEL

API time constrained. Some results may be missing.

Query parameters

Resource	project/fo
Role	Owner
Permission	accessap

Results

A full result of individual bindings and

Filter access

Resource	P
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	
<input type="checkbox"/> foobar/12345	

EXPAND TO VIEW ALL BINDINGS

Policy history for vandy@google.com on Google

BINDING FOR VANDY@GOOGLE.COM

POLICY HISTORY FOR GOOGLE

Policy history for Google

May 1, 2020

```

1 {
2   "bindings": [
3     {
4       "role": "roles/computeAdmin",
5       "members": [
6         "group:dev-admins@foogle.com",
7       ]
8     },
9     {
10      "role": "roles/security",
11      "members": [
12        "group:dev-group@foogle.com"
13      ]
14    },
15  ]

```

```

1 {
2   "bindings": [
3     {
4       "role": "roles/Owner",
5       "members": [
6         "group:dev-admins@foogle.com",
7       ]
8     },
9     {
10      "role": "roles/security",
11      "members": [
12        "group:sre-group@foogle.com"
13      ]
14    },
15  ]

```



CANCEL



Thank You