Flying Under Cloud Cover

Built-in Blind Spots in Cloud Security

Noam Dahan, Ermetic, @NoamDahan

ermetic

A trip to the cloud evasion & blindspot candy store

With some candy that most of you know & love...

ermetic

And some new ones to discover

ermetic

Why do they keep cropping up?

- Pressure to make it work
- Complexity
- Dirty CSP fixes, sewage, duct taping

Agenda

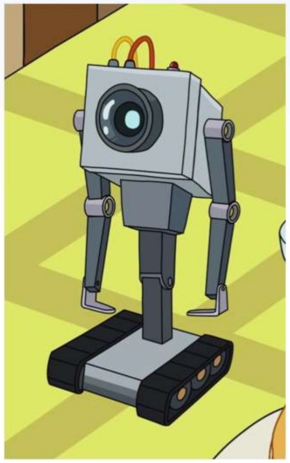
- **Trust no one!** Cloud provider design flaws
- **Hard knock life:** user misconfigurations
- **Getting too old for this…** Blind spots due to legacy support

Trust No One!

Cloud provider design choices

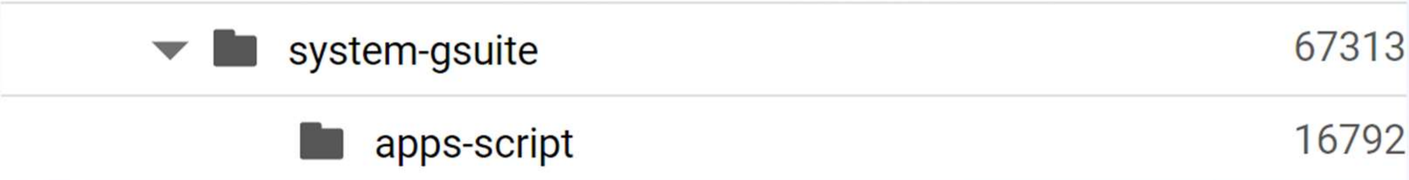
Evasion: GCP Hidden projects

- Google Apps Script
- It deploys to GCP (cool!)



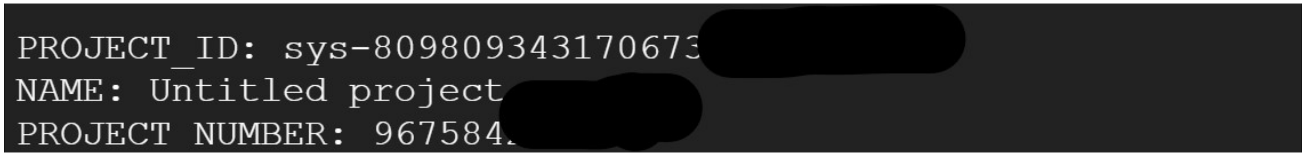
GCP Hidden projects

- It creates a hidden project (in the console):
  - system-gsuite/apps-script/sys-12345678901234567890123456



system-gsuite	67313
apps-script	16792

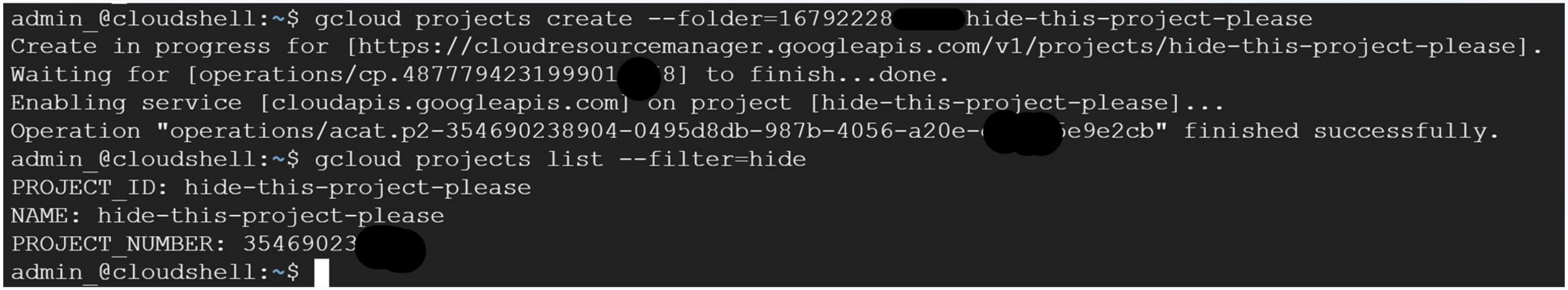
  - You can see it from the cli and even access it from the console (url)
    - gcloud projects list --filter=16792…



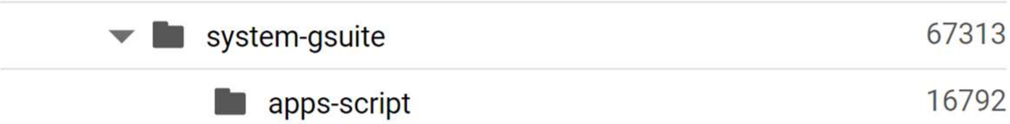
```
PROJECT_ID: sys-80980934317067[redacted]
NAME: Untitled project [redacted]
PROJECT NUMBER: 967584[redacted]
```

GCP Hidden projects

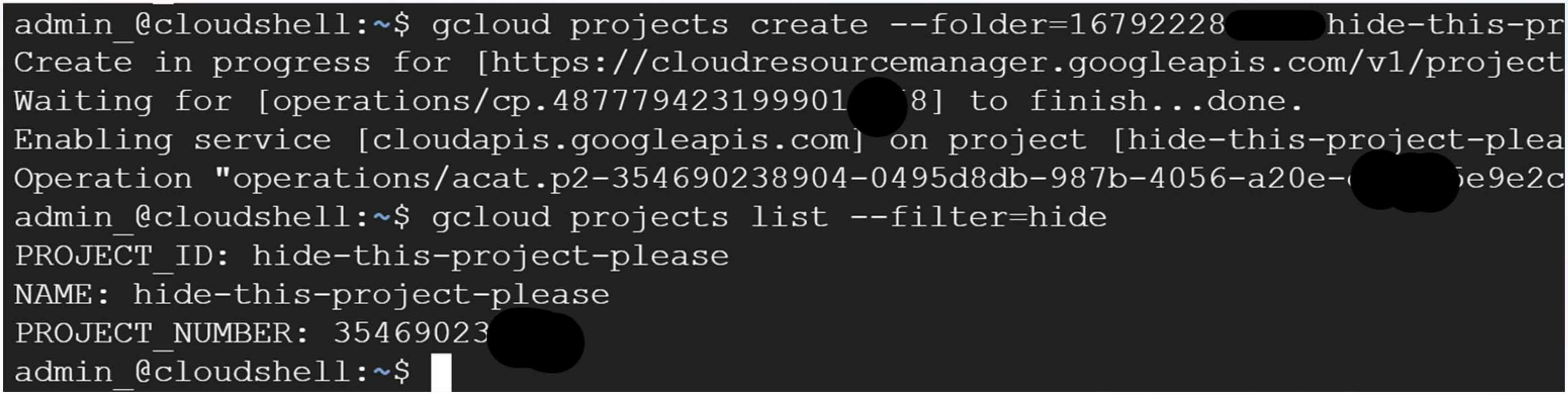
- So far, so good…
- However… 😈



```
admin_@cloudshell:~$ gcloud projects create --folder=16792228[redacted]hide-this-project-please
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/projects/hide-this-project-please].
Waiting for [operations/cp.487779423199901[redacted]8] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [hide-this-project-please]...
Operation "operations/acat.p2-354690238904-0495d8db-987b-4056-a20e-[redacted]e9e2cb" finished successfully.
admin_@cloudshell:~$ gcloud projects list --filter=hide
PROJECT_ID: hide-this-project-please
NAME: hide-this-project-please
PROJECT_NUMBER: 35469023[redacted]
admin_@cloudshell:~$
```

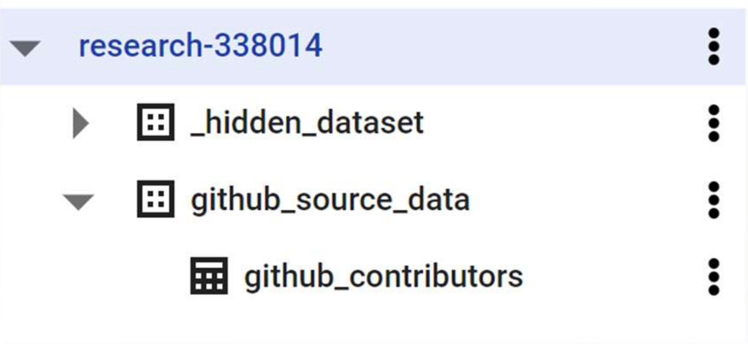


▾ system-gsuite	67313
apps-script	16792



```
admin_@cloudshell:~$ gcloud projects create --folder=16792228[redacted]hide-this-pr
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/project
Waiting for [operations/cp.487779423199901[redacted]8] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [hide-this-project-plea
Operation "operations/acat.p2-354690238904-0495d8db-987b-4056-a20e-[redacted]e9e2c
admin_@cloudshell:~$ gcloud projects list --filter=hide
PROJECT_ID: hide-this-project-please
NAME: hide-this-project-please
PROJECT_NUMBER: 35469023[redacted]
admin_@cloudshell:~$ 
```

Evasion: GCP Hidden dataset

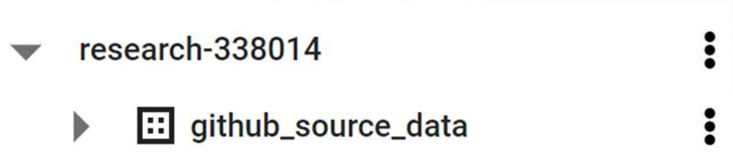


research-338014

_hidden_dataset

github_source_data

github_contributors



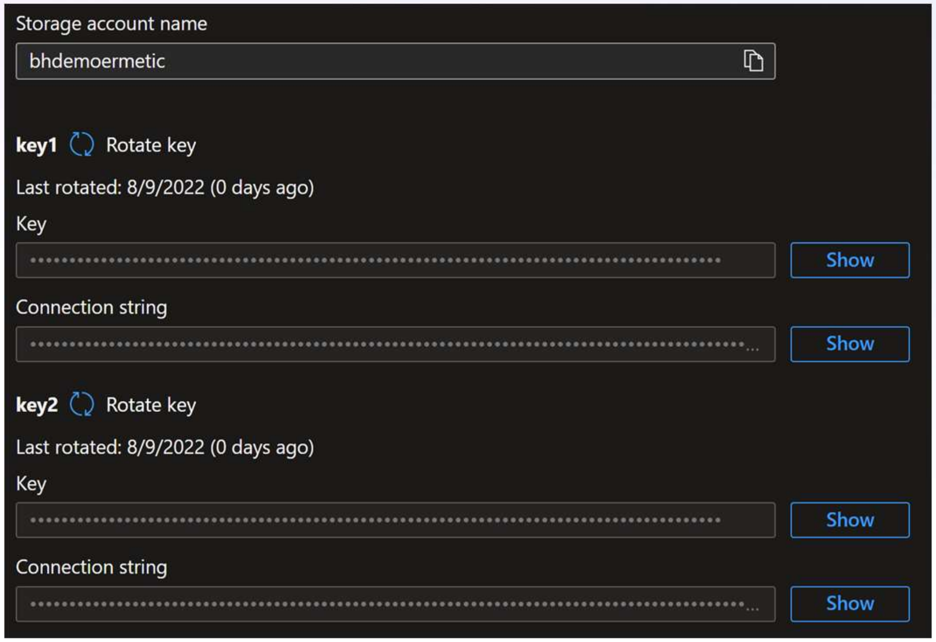
research-338014

github_source_data

Evasion/Persistency: Azure access keys

- IAM Bypass
- Created by default

Azure access keys



Storage account name

bhdemoermetic

key1 Rotate key

Last rotated: 8/9/2022 (0 days ago)

Key

••

Connection string

••...

key2 Rotate key

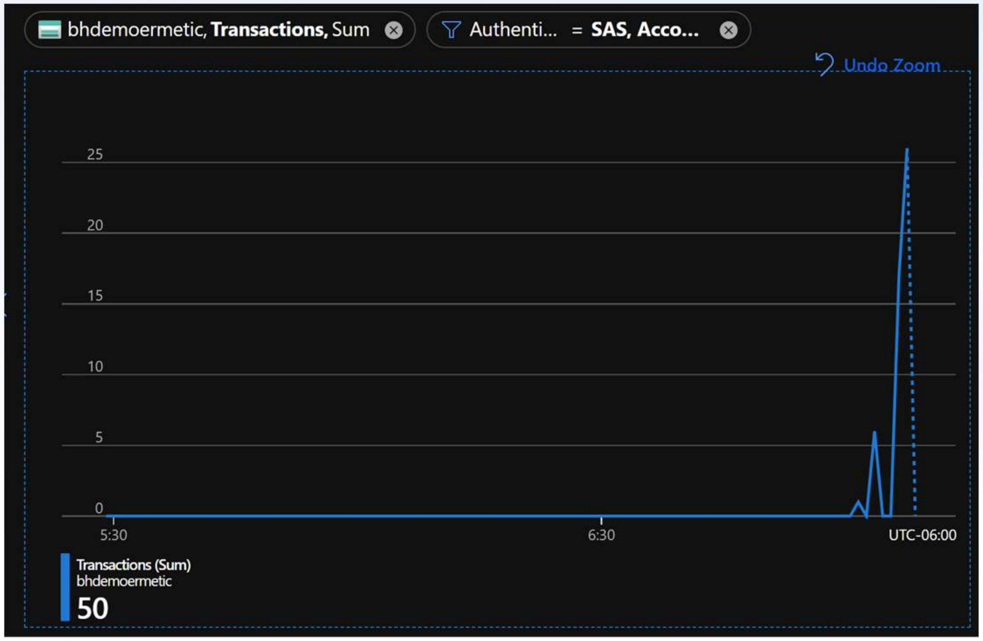
Last rotated: 8/9/2022 (0 days ago)

Key

••

Connection string

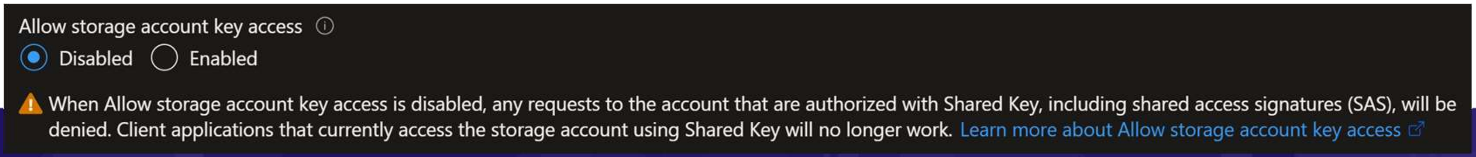
••...



bhdemoermetic, **Transactions,** Sum

Authenti... = **SAS, Acco...**

Transactions (Sum)
bhdemoermetic
50



Allow storage account key access ⓘ

● Disabled ○ Enabled

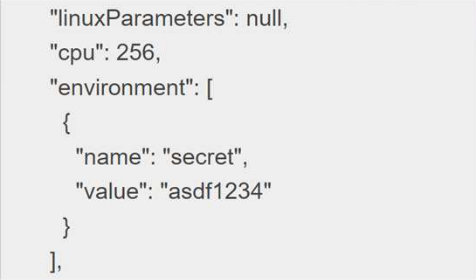
⚠ When Allow storage account key access is disabled, any requests to the account that are authorized with Shared Key, including shared access signatures (SAS), will be denied. Client applications that currently access the storage account using Shared Key will no longer work. Learn more about Allow storage account key access

Azure access keys

- Access keys can sign **SAS tokens** (shared access signature)
- Ad-hoc signature can only be revoked by deleting/regenerating the underlying key.

Quick win: AWS ECS Task definitions

- ECS Task definitions: run containers in ECS
- Often: secrets stored as environment variables → ***plaintext***
  - *(docker run --env)*
- This is metadata! (ViewOnlyAccess, SecurityAudit)
- **The correct practice:** AWS Secrets Manager secrets or AWS Systems Manager Parameter Store parameters[1]



```
"linuxParameters": null,
"cpu": 256,
"environment": [
  {
    "name": "secret",
    "value": "asdf1234"
  }
],
```

[1] https://docs.aws.amazon.com/AmazonECS/latest/developerguide/specifying-sensitive-data-secrets.html

AWS ECS Task definitions

- Unfortunately, ECS Task definitions **cannot be deleted**
  - Look up old revisions for secrets!
- Rotate everything

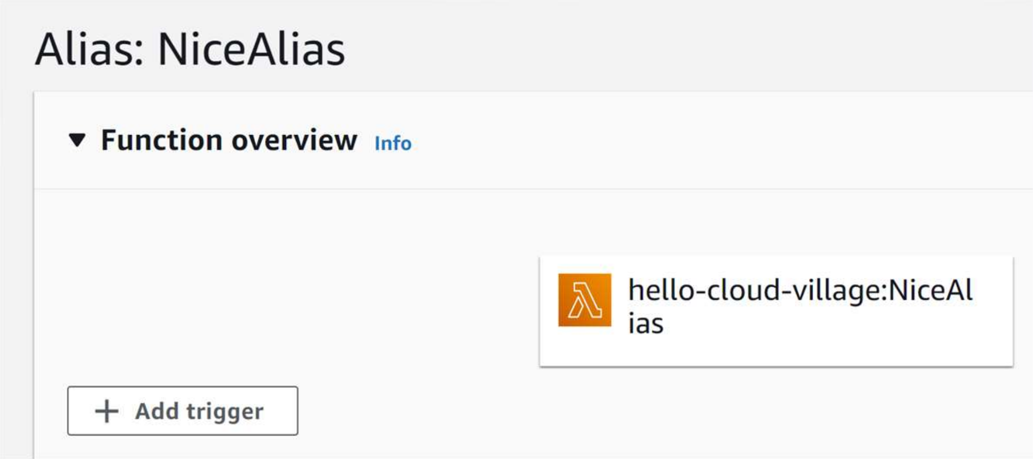
There are plaintext secrets in ECS task defs
we can just delete them, right?
imgflip.com
we can just delete them, right?

Hard knock life

Complicated things are complicated

Evasion/Persistency: AWS Lambda alias backdoor

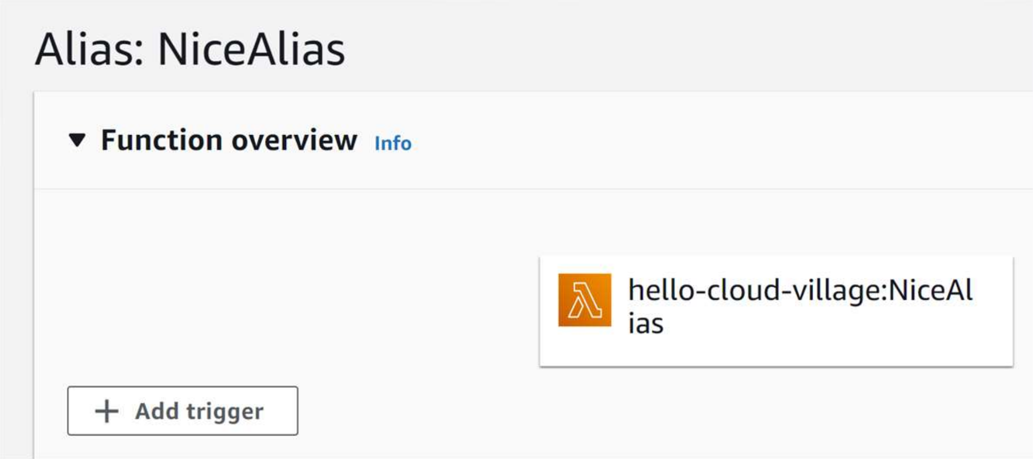
- Pointers to lambda function versions
- But not only that:
  - Different permissions
  - Different triggers
  - Different function URLs



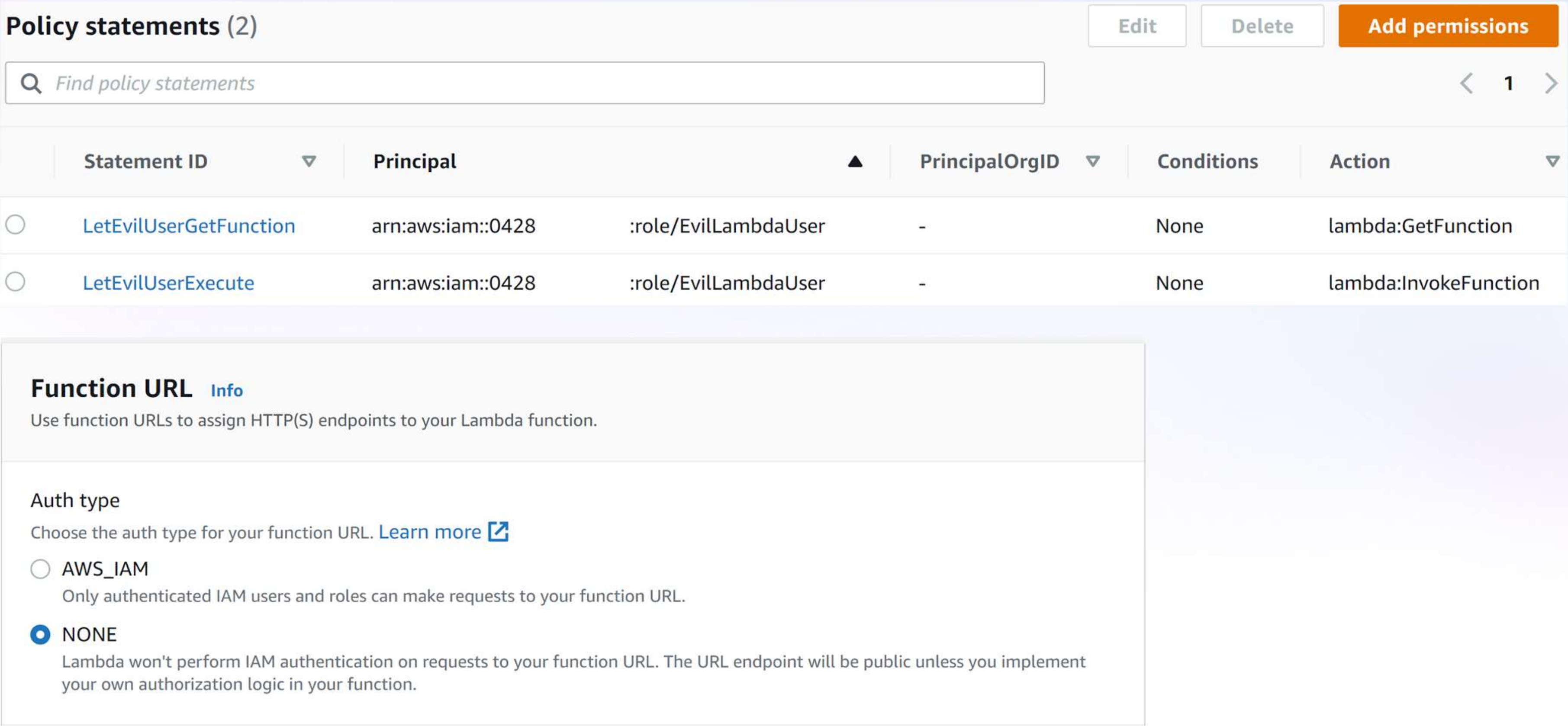
Alias: NiceAlias

AWS Lambda alias backdoor

- TTPs:
  - Add an alias to backdoor access to powerful function
  - Add an “evil” version with backdoored access, then add back the regular version
- Depends on detection model



Alias: NiceAlias



Policy statements (2)

	Statement ID	Principal	PrincipalOrgID	Conditions	Action
○	LetEvilUserGetFunction	arn:aws:iam::0428 :role/EvilLambdaUser	-	None	lambda:GetFunction
○	LetEvilUserExecute	arn:aws:iam::0428 :role/EvilLambdaUser	-	None	lambda:InvokeFunction

Function URL

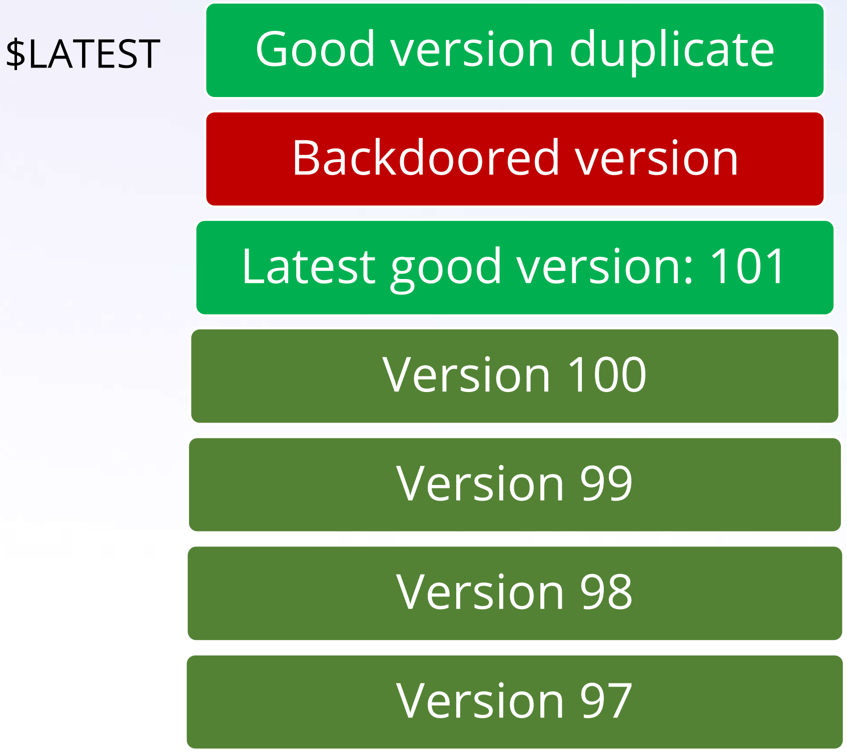
Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Auth type

Choose the auth type for your function URL. Learn more

○ AWS_IAM
Only authenticated IAM users and roles can make requests to your function URL.

● NONE
Lambda won't perform IAM authentication on requests to your function URL. The URL endpoint will be public unless you implement your own authorization logic in your function.



$LATEST

Good version duplicate

Backdoored version

Latest good version: 101

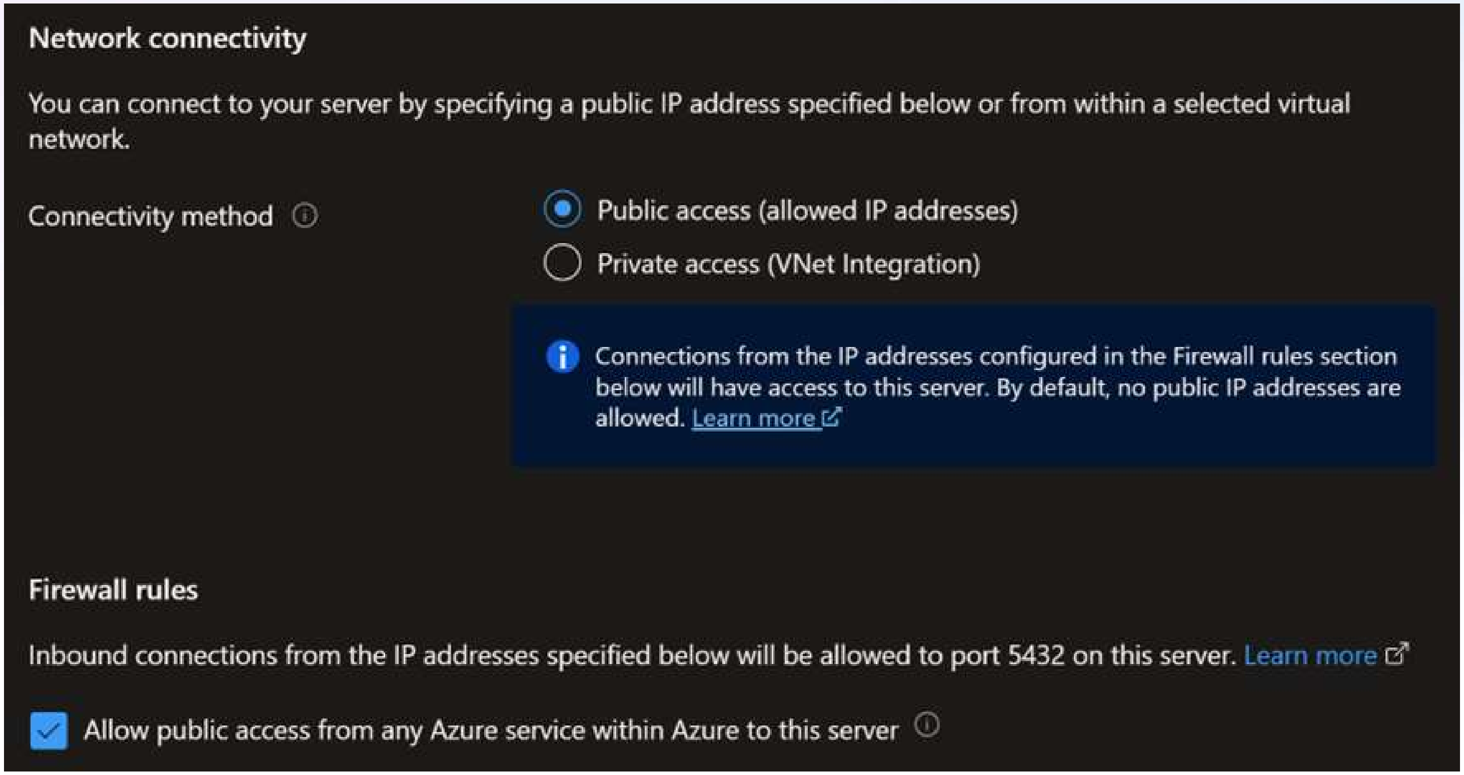
Version 100

Version 99

Version 98

Version 97

Quick win: “Allow Azure services” – the little checkbox that could



Network connectivity

You can connect to your server by specifying a public IP address specified below or from within a selected virtual network.

Connectivity method ⓘ

● Public access (allowed IP addresses)

○ Private access (VNet Integration)

ⓘ Connections from the IP addresses configured in the Firewall rules section below will have access to this server. By default, no public IP addresses are allowed. Learn more

Firewall rules

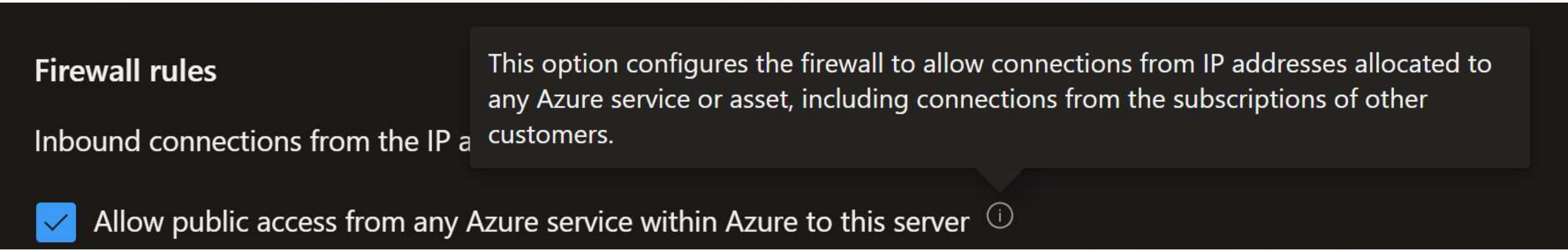
Inbound connections from the IP addresses specified below will be allowed to port 5432 on this server. Learn more

☑ Allow public access from any Azure service within Azure to this server ⓘ

“Allow Azure services” – the little checkbox that could

- “any Azure service within Azure” ⊇ VMs in different subscriptions

“Allow Azure services” – the little tooltip that tried

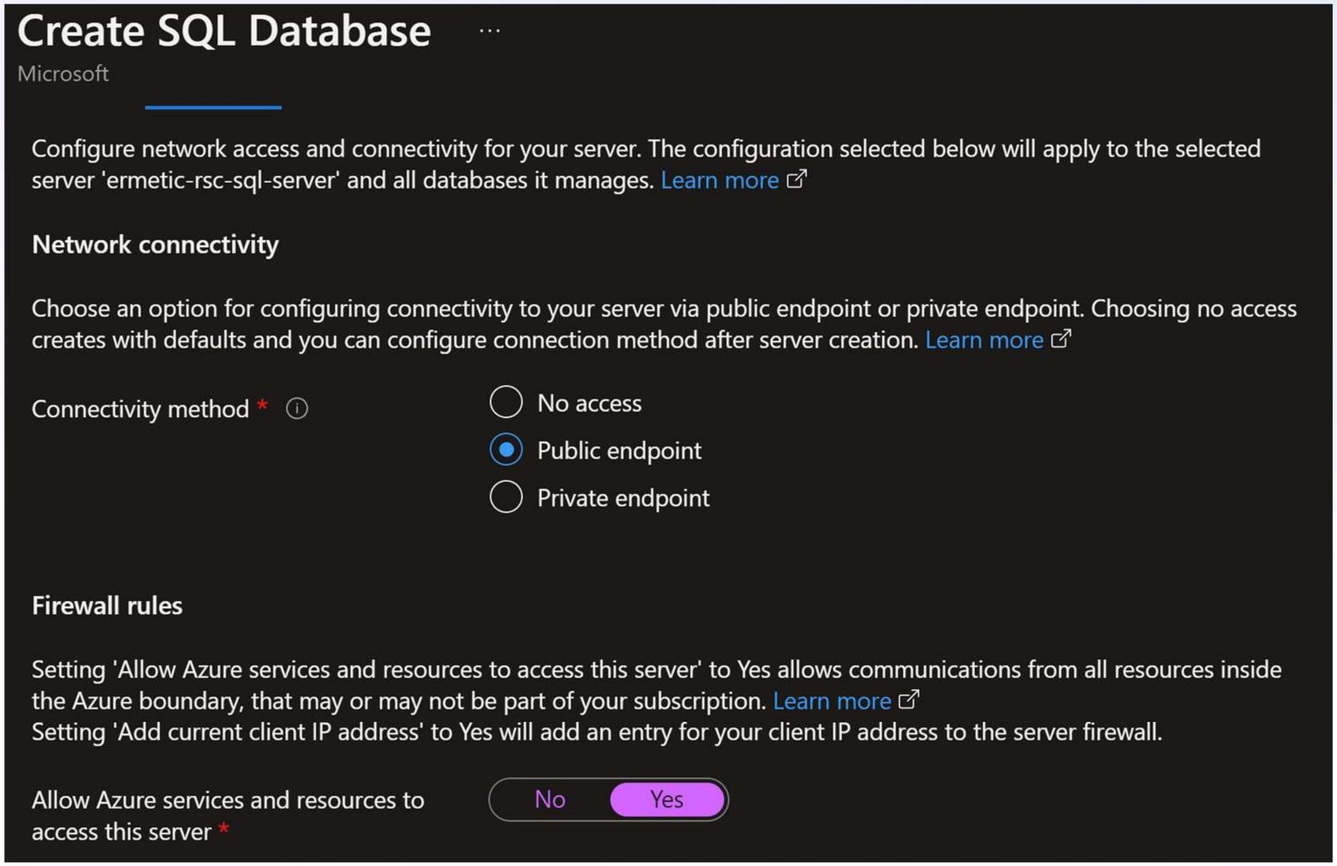


Firewall rules

Inbound connections from the IP a

This option configures the firewall to allow connections from IP addresses allocated to any Azure service or asset, including connections from the subscriptions of other customers.

☑ Allow public access from any Azure service within Azure to this server



Create SQL Database

Microsoft

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'ermetic-rsc-sql-server' and all databases it manages. Learn more

Network connectivity

Choose an option for configuring connectivity to your server via public endpoint or private endpoint. Choosing no access creates with defaults and you can configure connection method after server creation. Learn more

Connectivity method *

○ No access
● Public endpoint
○ Private endpoint

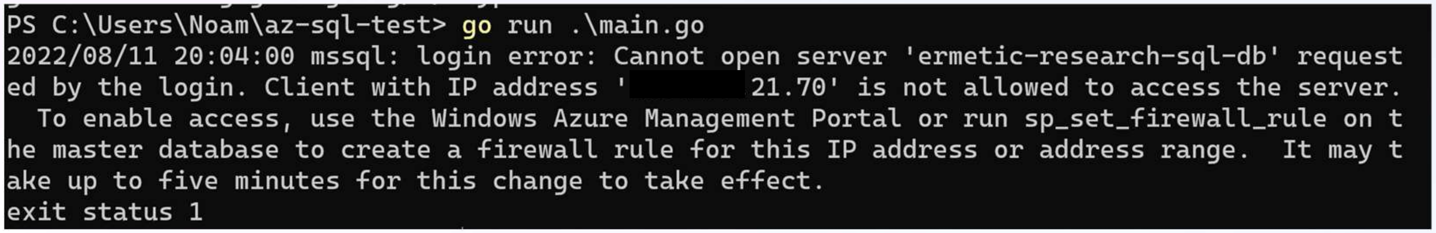
Firewall rules

Setting 'Allow Azure services and resources to access this server' to Yes allows communications from all resources inside the Azure boundary, that may or may not be part of your subscription. Learn more
Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the server firewall.

Allow Azure services and resources to access this server * No [✓ Yes]

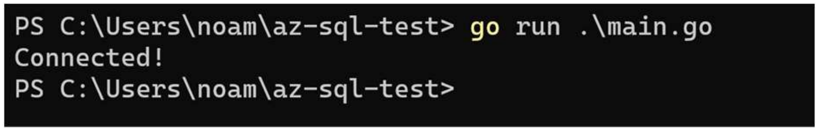
Trying to connect...

- From local machine



```
PS C:\Users\Noam\az-sql-test> go run .\main.go
2022/08/11 20:04:00 mssql: login error: Cannot open server 'ermetic-research-sql-db' request
ed by the login. Client with IP address '[redacted]21.70' is not allowed to access the server.
  To enable access, use the Windows Azure Management Portal or run sp_set_firewall_rule on t
he master database to create a firewall rule for this IP address or address range.  It may t
ake up to five minutes for this change to take effect.
exit status 1
```

- From VM in different Azure subscription



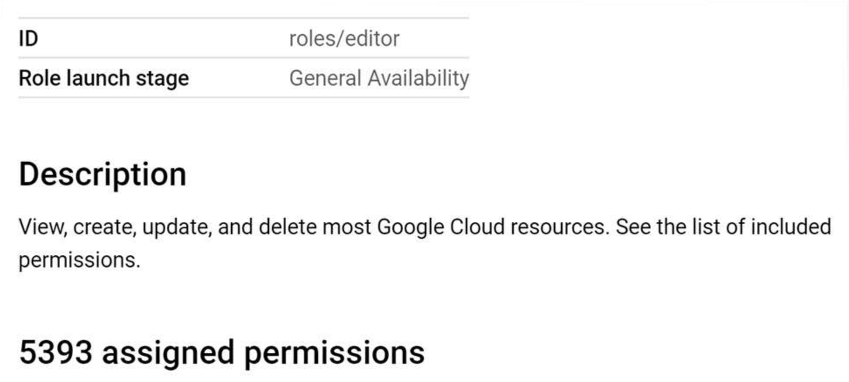
```
PS C:\Users\noam\az-sql-test> go run .\main.go
Connected!
PS C:\Users\noam\az-sql-test>
```

Getting too old for this…

Legacy support

Quick win: GCP Basic Roles

- **Basic roles** (Viewer, Editor) have strong and broad permissions
- GCE legacy mechanism: **Access scopes**
- **Default service accounts**
- Compute engine default service account



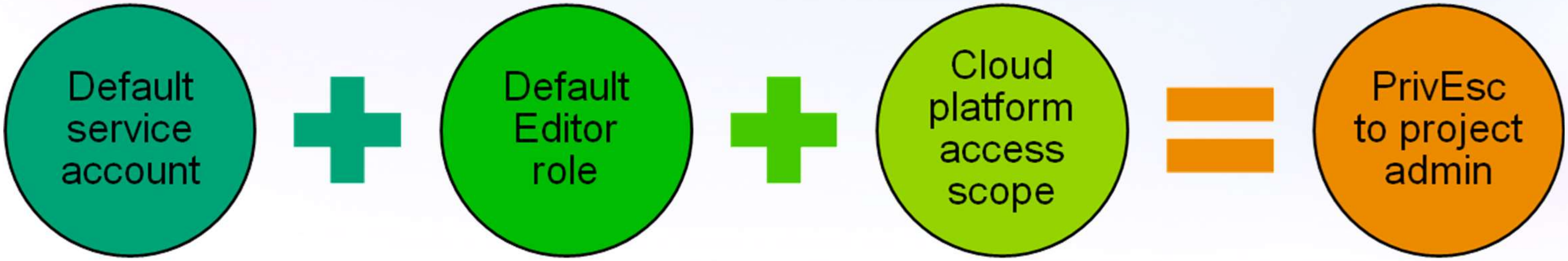
ID	roles/editor
Role launch stage	General Availability

Description

View, create, update, and delete most Google Cloud resources. See the list of included permissions.

5393 assigned permissions

GCP Basic Roles



Default service account + Default Editor role + Cloud platform access scope = PrivEsc to project admin

Evasion/Persistency: AWS KMS Grants

- Give direct permission to use keys
- Revoking is your responsibility
- Meant as temporary, but weakly enforced
- Persistence + evasion

Final thoughts

- CSPs: Should treat and manage these things even if they’re not 0-dAy vUlNerAbiliTies, they form TTPs and direct behavior
- Red team: TTPs to use
- Blue team:
  - note the stuff that’s outside the limelight
  - Build detections for these!

Questions?

- noam@ermetic.com
- Twitter: @NoamDahan
- Github: noamsdahan