Cloud Security

An IAM GAME

Nathaniel Beckstead

whoami

I am here because I love to give presentations.

@scriptingislife
https://scriptingis.life
https://glimpseid.com

What is the cloud?

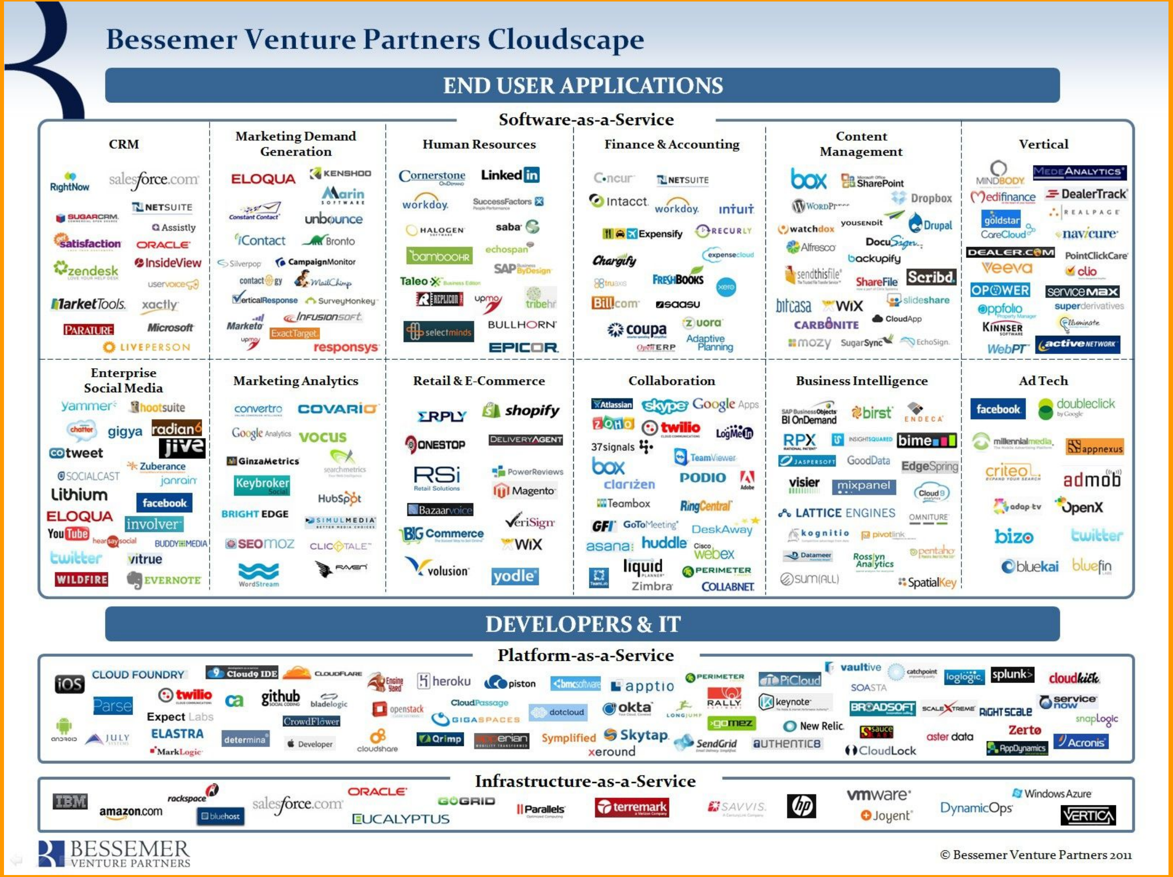
Google Cloud

Microsoft Azure

aws

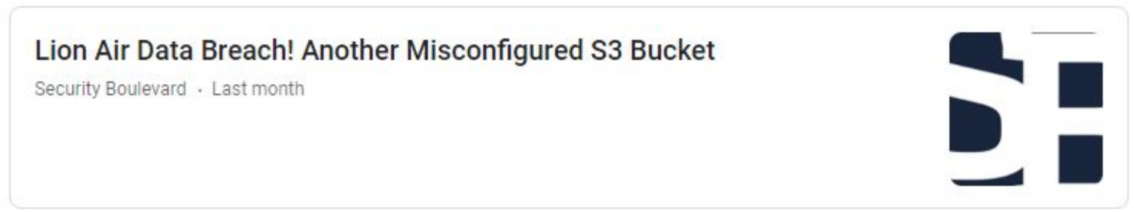
What is the cloud?

What is the cloud?



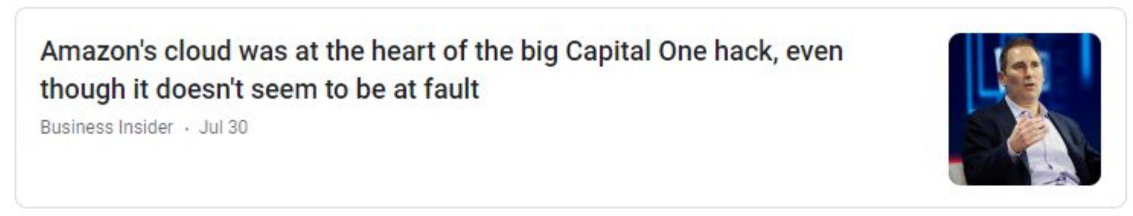
“Definitions”

- EC2 - Virtual Machine but in the cloud
- S3 - Key-value storage (mostly for files)
- DynamoDB - NoSQL database



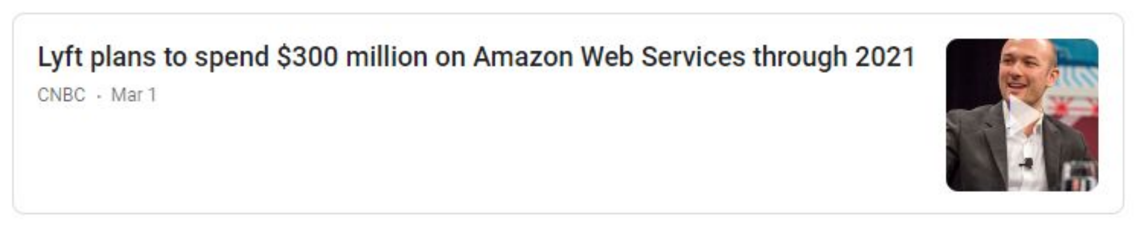
Lion Air Data Breach! Another Misconfigured S3 Bucket

Security Boulevard · Last month



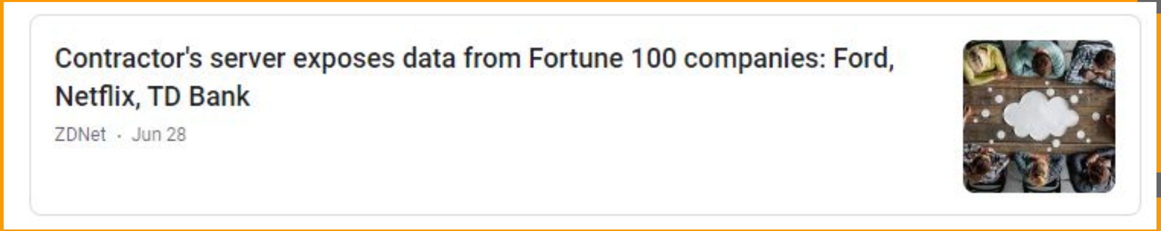
Amazon's cloud was at the heart of the big Capital One hack, even though it doesn't seem to be at fault

Business Insider · Jul 30



Lyft plans to spend $300 million on Amazon Web Services through 2021

CNBC · Mar 1

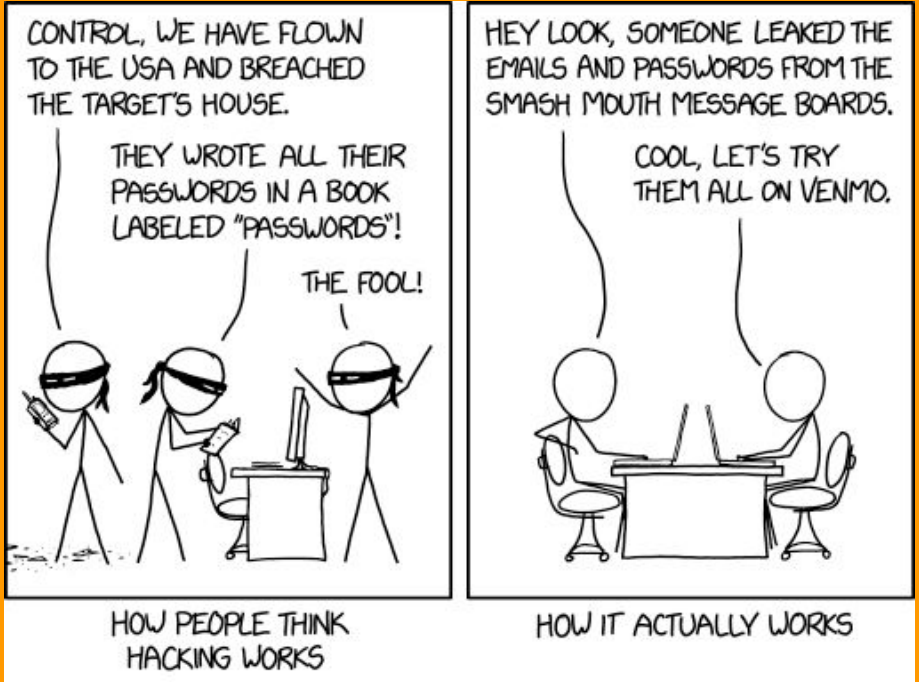


Contractor's server exposes data from Fortune 100 companies: Ford, Netflix, TD Bank

ZDNet · Jun 28

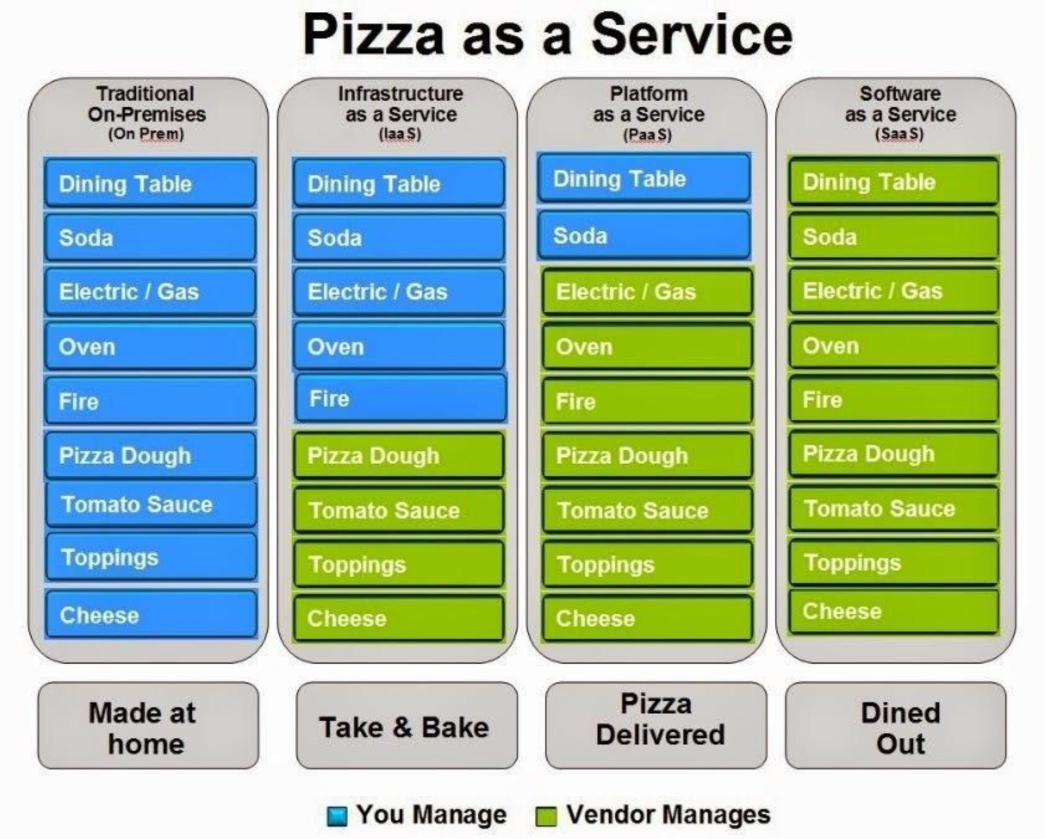
Why is it so hard to secure?

- It's not


CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.
THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!
THE FOOL!
HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.
COOL, LET'S TRY THEM ALL ON VENMO.
HOW PEOPLE THINK HACKING WORKS
HOW IT ACTUALLY WORKS

What's different about the cloud?

- Speed
- IaaS, PaaS, SaaS
- No rules!



Pizza as a Service

Traditional On-Premises (On Prem)	Infrastructure as a Service (Iaa S)	Platform as a Service (Paa S)	Software as a Service (Saa S)
🟦 Dining Table	🟦 Dining Table	🟦 Dining Table	🟩 Dining Table
🟦 Soda	🟦 Soda	🟦 Soda	🟩 Soda
🟦 Electric / Gas	🟦 Electric / Gas	🟩 Electric / Gas	🟩 Electric / Gas
🟦 Oven	🟦 Oven	🟩 Oven	🟩 Oven
🟦 Fire	🟦 Fire	🟩 Fire	🟩 Fire
🟦 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough
🟦 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce
🟦 Toppings	🟩 Toppings	🟩 Toppings	🟩 Toppings
🟦 Cheese	🟩 Cheese	🟩 Cheese	🟩 Cheese
Made at home	Take & Bake	Pizza Delivered	Dined Out

🟦 You Manage 🟩 Vendor Manages

https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/

What is IAM?

- Identity and Access Management
- Users, API Keys, Roles, Policies
- Omnipresent in the cloud

Roles

- Like a user, but can be assumed by anyone who needs it.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

Roles

YOU GET A ROLE,
AND YOU GET A ROLE
aws
EVERYONE GETS A ROLE
imgflip.com

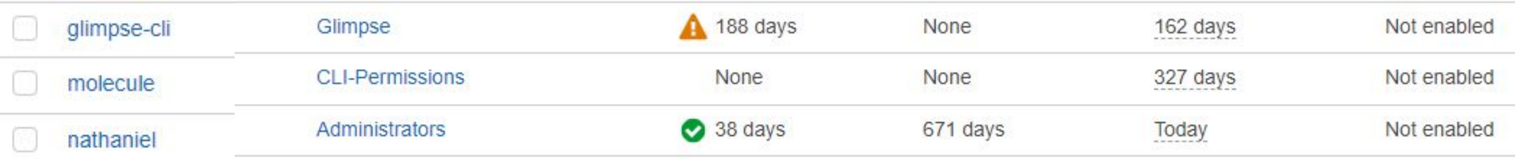
Policies

- Defines permissions for an action.

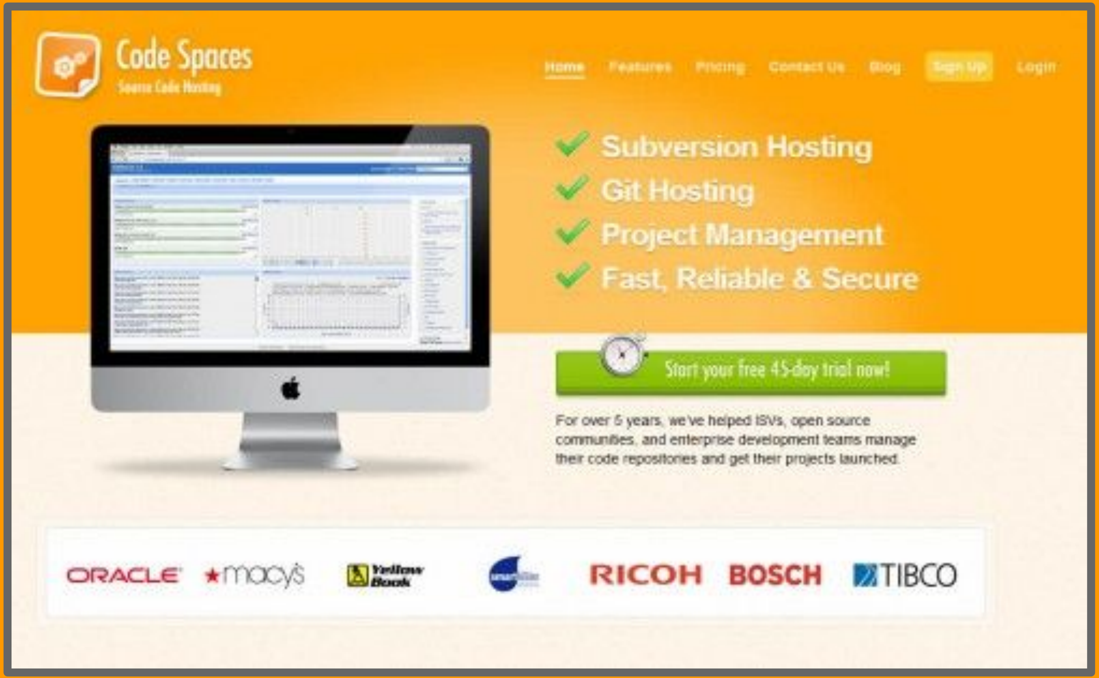
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#targetText=Policies%20and%20Permissions,or%20resource%2C%20defines%20their%20permissions.

Access Keys

- Used for programmatic access



□	glimpse-cli	Glimpse	⚠ 188 days	None	162 days	Not enabled
□	molecule	CLI-Permissions	None	None	327 days	Not enabled
□	nathaniel	Administrators	✓ 38 days	671 days	Today	Not enabled



- ✓ Subversion Hosting
- ✓ Git Hosting
- ✓ Project Management
- ✓ Fast, Reliable & Secure

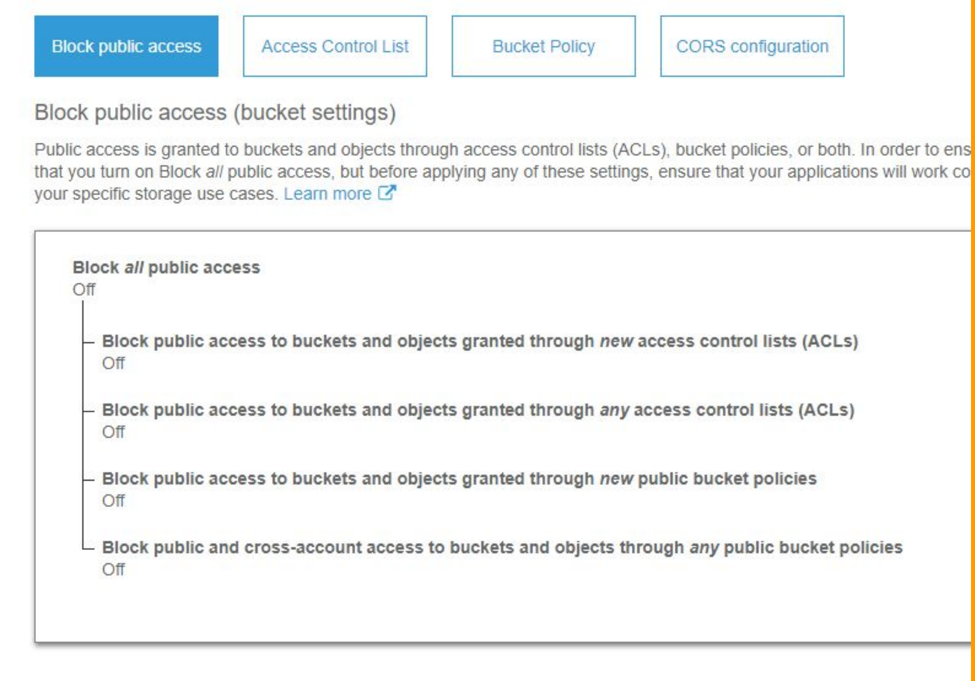
For over 5 years, we've helped ISVs, open source communities, and enterprise development teams manage their code repositories and get their projects launched.

https://blog.trendmicro.com/the-code-spaces-nightmare/

Why is IAM so hard?

- It’s complicated.

Why is IAM so hard?



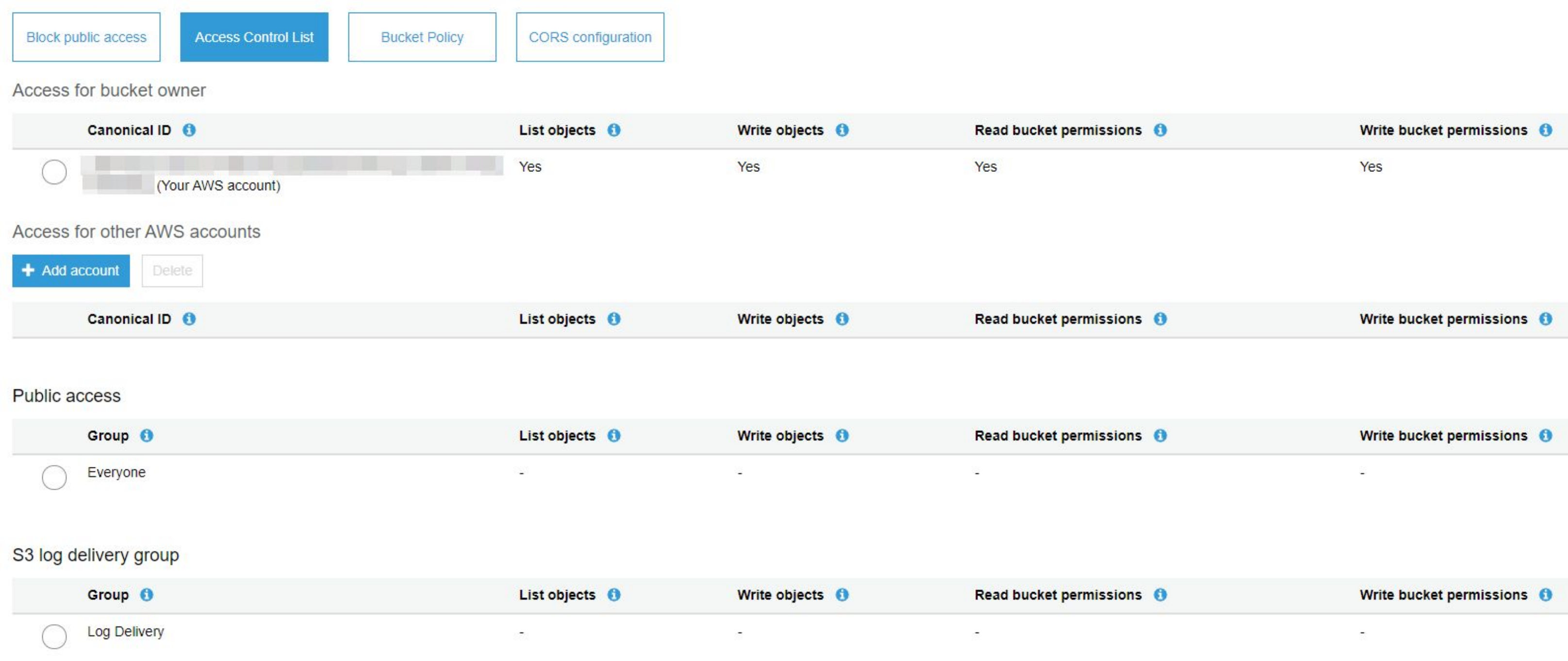
Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ens
that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work co
your specific storage use cases. Learn more

Block *all* public access
Off

- **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  Off
- **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  Off
- **Block public access to buckets and objects granted through *new* public bucket policies**
  Off
- **Block public and cross-account access to buckets and objects through *any* public bucket policies**
  Off

Why is IAM so hard?



Access for bucket owner

	Canonical ID	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	[redacted] (Your AWS account)	Yes	Yes	Yes	Yes

Access for other AWS accounts

	Canonical ID	List objects	Write objects	Read bucket permissions	Write bucket permissions

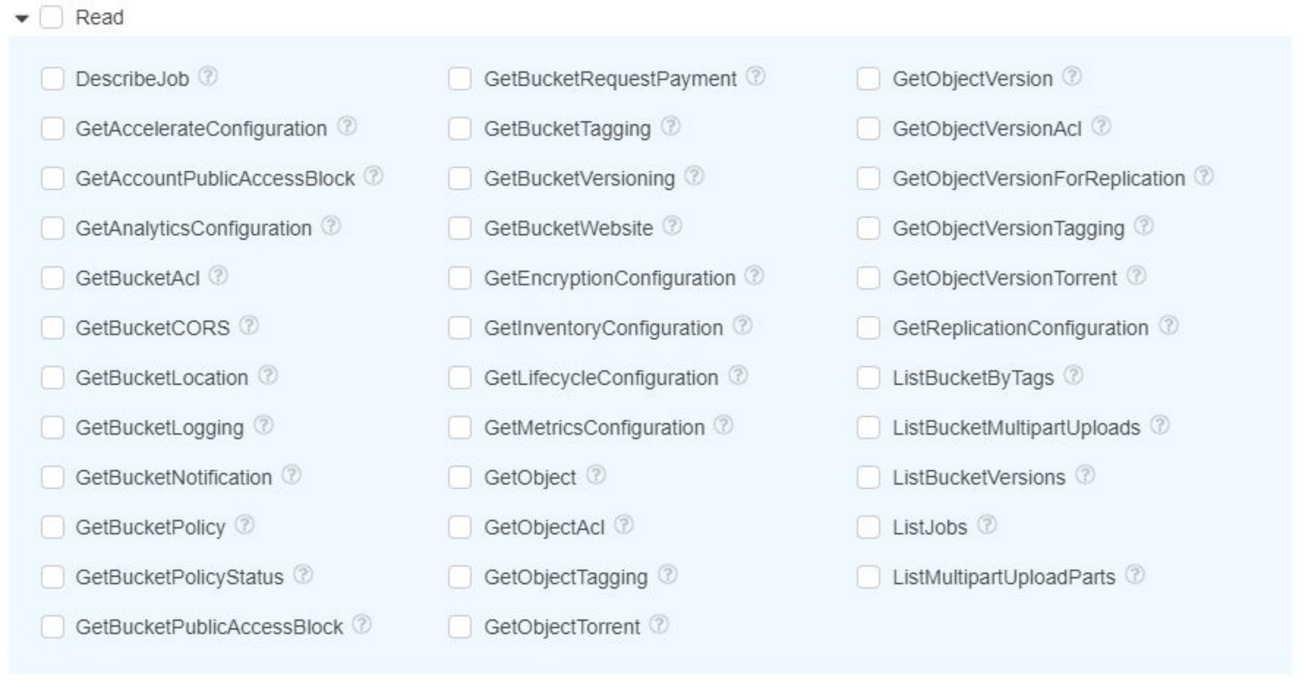
Public access

	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Everyone	-	-	-	-

S3 log delivery group

	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Log Delivery	-	-	-	-

Why is IAM so hard?



▾ □ Read

□ DescribeJob

□ GetAccelerateConfiguration

□ GetAccountPublicAccessBlock

□ GetAnalyticsConfiguration

□ GetBucketAcl

□ GetBucketCORS

□ GetBucketLocation

□ GetBucketLogging

□ GetBucketNotification

□ GetBucketPolicy

□ GetBucketPolicyStatus

□ GetBucketPublicAccessBlock

□ GetBucketRequestPayment

□ GetBucketTagging

□ GetBucketVersioning

□ GetBucketWebsite

□ GetEncryptionConfiguration

□ GetInventoryConfiguration

□ GetLifecycleConfiguration

□ GetMetricsConfiguration

□ GetObject

□ GetObjectAcl

□ GetObjectTagging

□ GetObjectTorrent

□ GetObjectVersion

□ GetObjectVersionAcl

□ GetObjectVersionForReplication

□ GetObjectVersionTagging

□ GetObjectVersionTorrent

□ GetReplicationConfiguration

□ ListBucketByTags

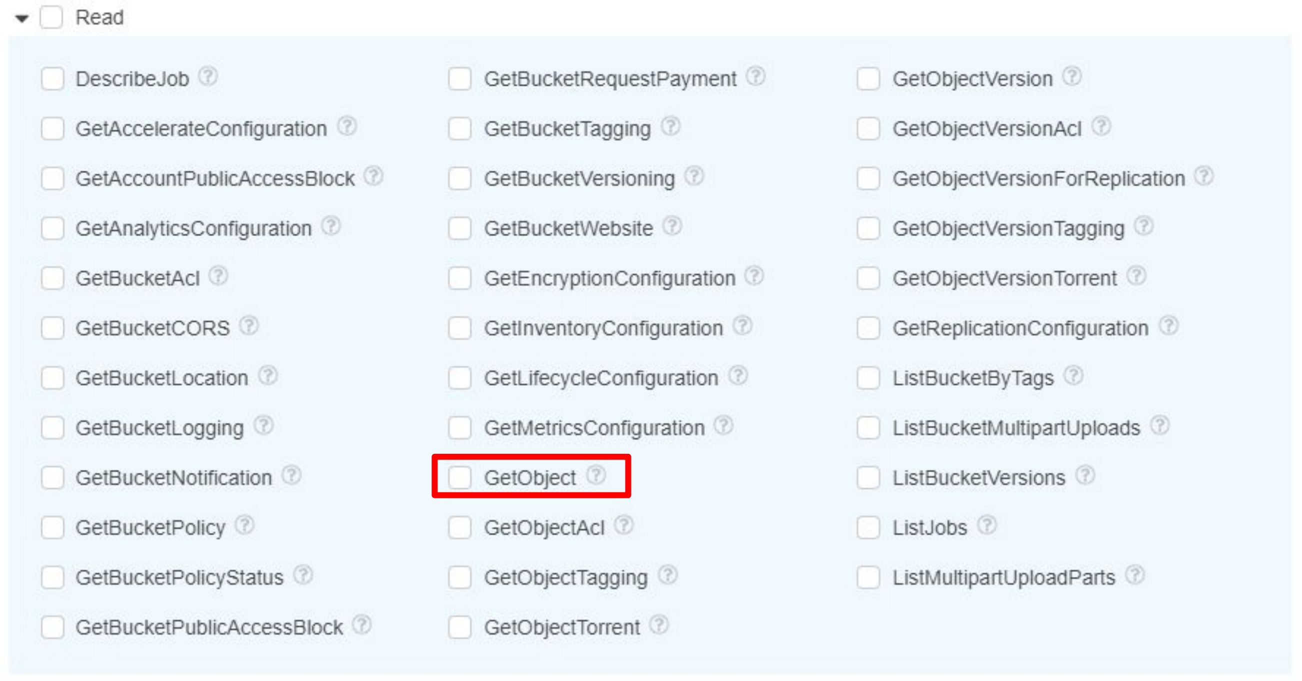
□ ListBucketMultipartUploads

□ ListBucketVersions

□ ListJobs

□ ListMultipartUploadParts

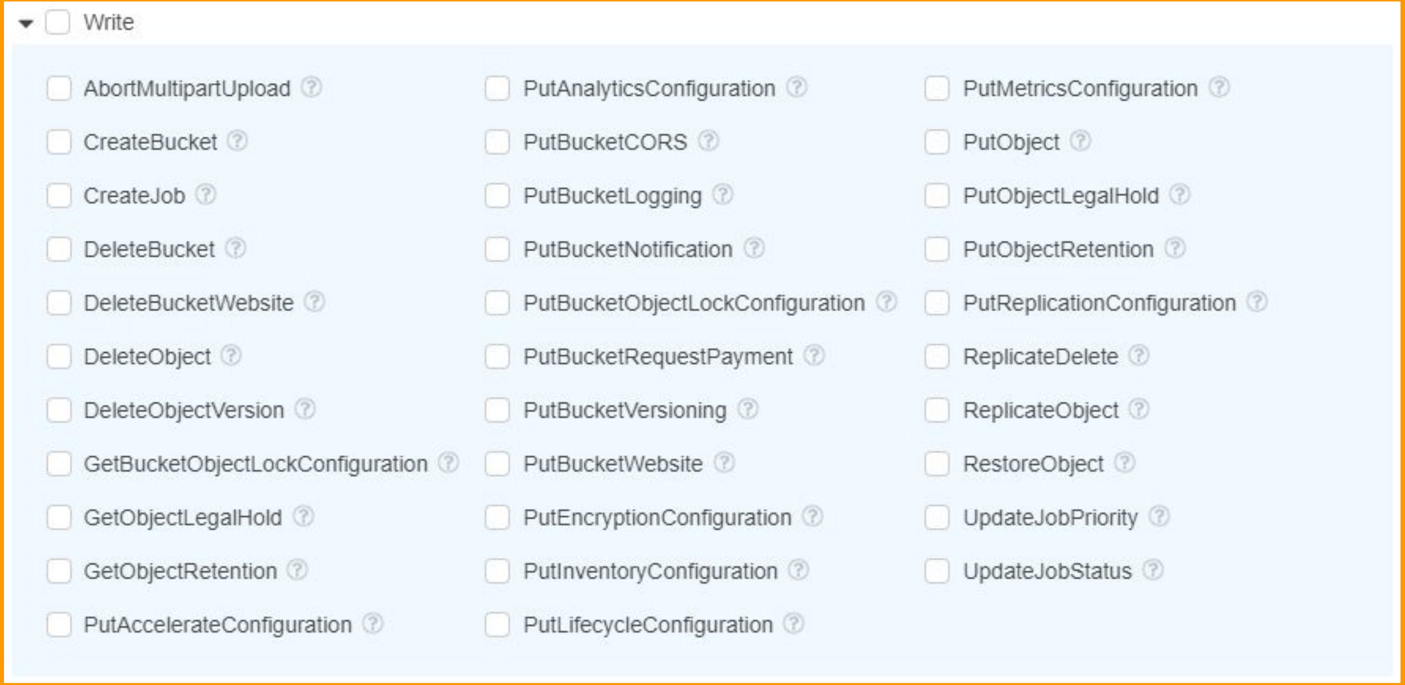
Why is IAM so hard?



□ Read

- □ DescribeJob
- □ GetAccelerateConfiguration
- □ GetAccountPublicAccessBlock
- □ GetAnalyticsConfiguration
- □ GetBucketAcl
- □ GetBucketCORS
- □ GetBucketLocation
- □ GetBucketLogging
- □ GetBucketNotification
- □ GetBucketPolicy
- □ GetBucketPolicyStatus
- □ GetBucketPublicAccessBlock
- □ GetBucketRequestPayment
- □ GetBucketTagging
- □ GetBucketVersioning
- □ GetBucketWebsite
- □ GetEncryptionConfiguration
- □ GetInventoryConfiguration
- □ GetLifecycleConfiguration
- □ GetMetricsConfiguration
- □ GetObject
- □ GetObjectAcl
- □ GetObjectTagging
- □ GetObjectTorrent
- □ GetObjectVersion
- □ GetObjectVersionAcl
- □ GetObjectVersionForReplication
- □ GetObjectVersionTagging
- □ GetObjectVersionTorrent
- □ GetReplicationConfiguration
- □ ListBucketByTags
- □ ListBucketMultipartUploads
- □ ListBucketVersions
- □ ListJobs
- □ ListMultipartUploadParts

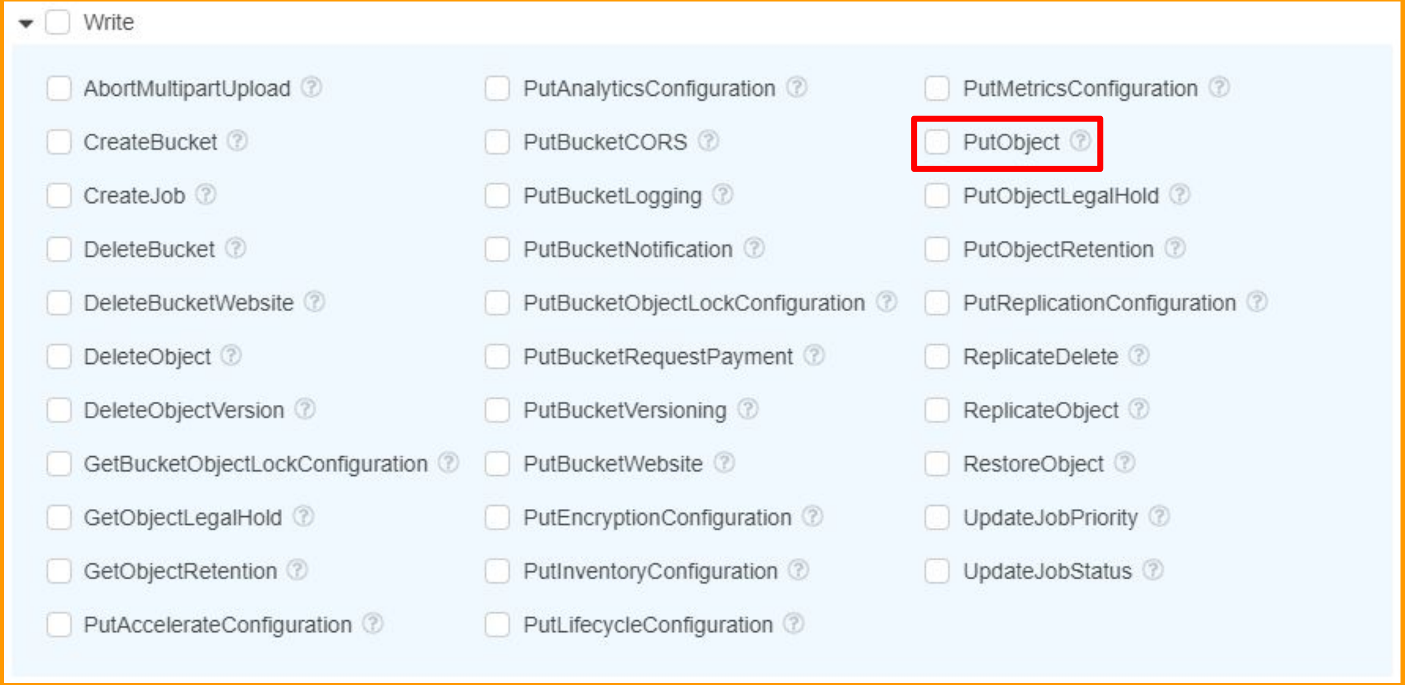
Why is IAM so hard?



▾ □ Write

- □ AbortMultipartUpload
- □ CreateBucket
- □ CreateJob
- □ DeleteBucket
- □ DeleteBucketWebsite
- □ DeleteObject
- □ DeleteObjectVersion
- □ GetBucketObjectLockConfiguration
- □ GetObjectLegalHold
- □ GetObjectRetention
- □ PutAccelerateConfiguration
- □ PutAnalyticsConfiguration
- □ PutBucketCORS
- □ PutBucketLogging
- □ PutBucketNotification
- □ PutBucketObjectLockConfiguration
- □ PutBucketRequestPayment
- □ PutBucketVersioning
- □ PutBucketWebsite
- □ PutEncryptionConfiguration
- □ PutInventoryConfiguration
- □ PutLifecycleConfiguration
- □ PutMetricsConfiguration
- □ PutObject
- □ PutObjectLegalHold
- □ PutObjectRetention
- □ PutReplicationConfiguration
- □ ReplicateDelete
- □ ReplicateObject
- □ RestoreObject
- □ UpdateJobPriority
- □ UpdateJobStatus

Why is IAM so hard?



▼ □ Write

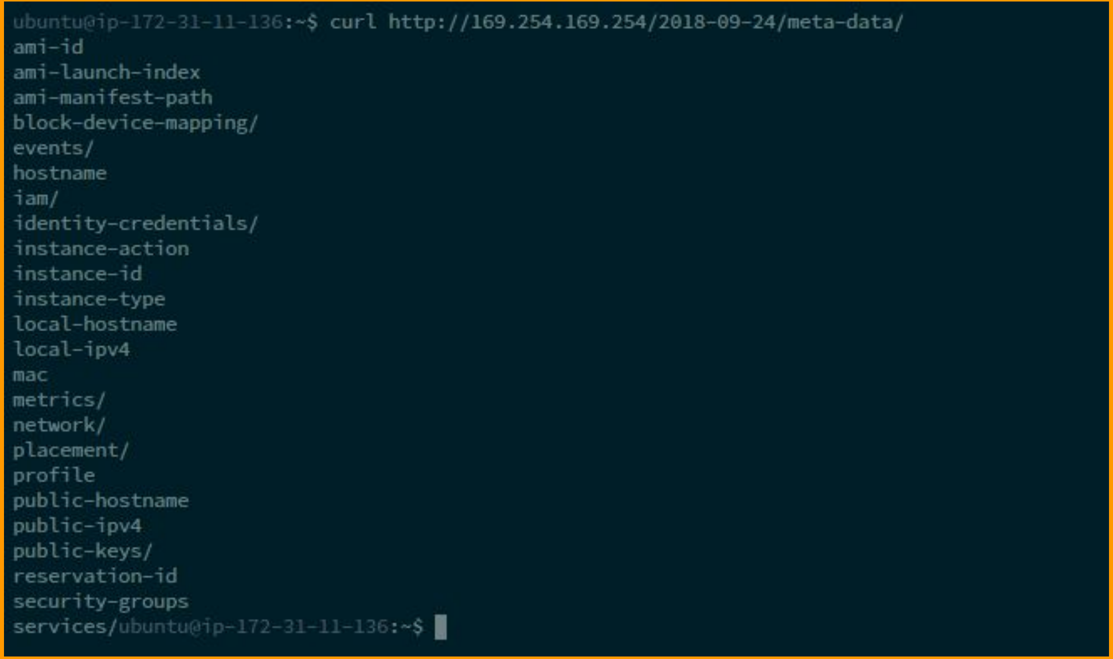
- □ AbortMultipartUpload
- □ CreateBucket
- □ CreateJob
- □ DeleteBucket
- □ DeleteBucketWebsite
- □ DeleteObject
- □ DeleteObjectVersion
- □ GetBucketObjectLockConfiguration
- □ GetObjectLegalHold
- □ GetObjectRetention
- □ PutAccelerateConfiguration
- □ PutAnalyticsConfiguration
- □ PutBucketCORS
- □ PutBucketLogging
- □ PutBucketNotification
- □ PutBucketObjectLockConfiguration
- □ PutBucketRequestPayment
- □ PutBucketVersioning
- □ PutBucketWebsite
- □ PutEncryptionConfiguration
- □ PutInventoryConfiguration
- □ PutLifecycleConfiguration
- □ PutMetricsConfiguration
- □ PutObject
- □ PutObjectLegalHold
- □ PutObjectRetention
- □ PutReplicationConfiguration
- □ ReplicateDelete
- □ ReplicateObject
- □ RestoreObject
- □ UpdateJobPriority
- □ UpdateJobStatus

Why is IAM so hard?

- It's preventive.

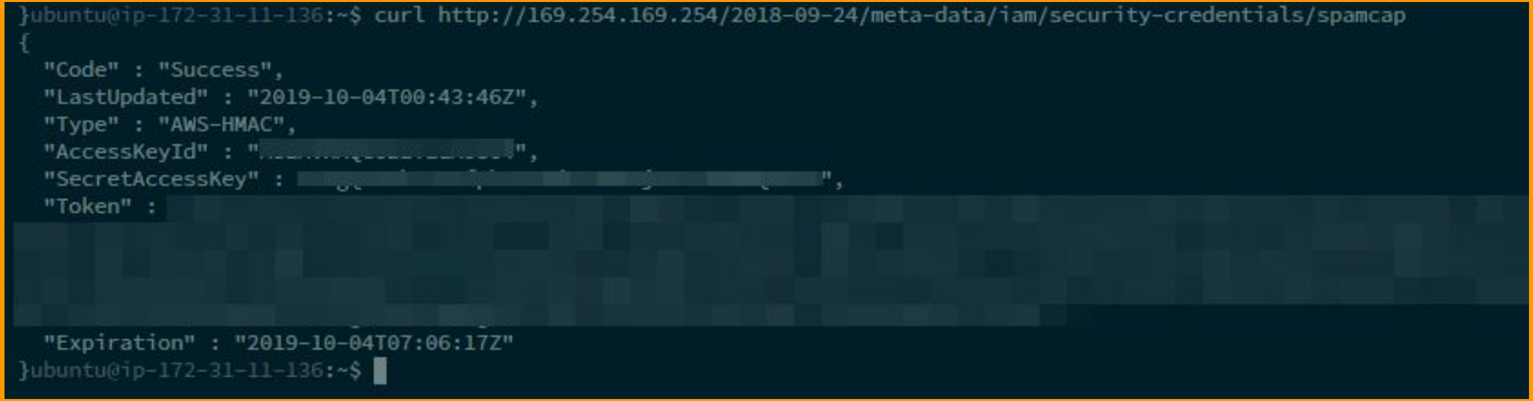
Every developer using the cloud. (Circa 2019)

AWS Metadata Service



```
ubuntu@ip-172-31-11-136:~$ curl http://169.254.169.254/2018-09-24/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/ubuntu@ip-172-31-11-136:~$ 
```

AWS Metadata Service



```
}ubuntu@ip-172-31-11-136:~$ curl http://169.254.169.254/2018-09-24/meta-data/iam/security-credentials/spamcap
{
  "Code" : "Success",
  "LastUpdated" : "2019-10-04T00:43:46Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "[redacted]",
  "SecretAccessKey" : [redacted]",
  "Token" : [redacted]
  "Expiration" : "2019-10-04T07:06:17Z"
}ubuntu@ip-172-31-11-136:~$ █
```

Capital One

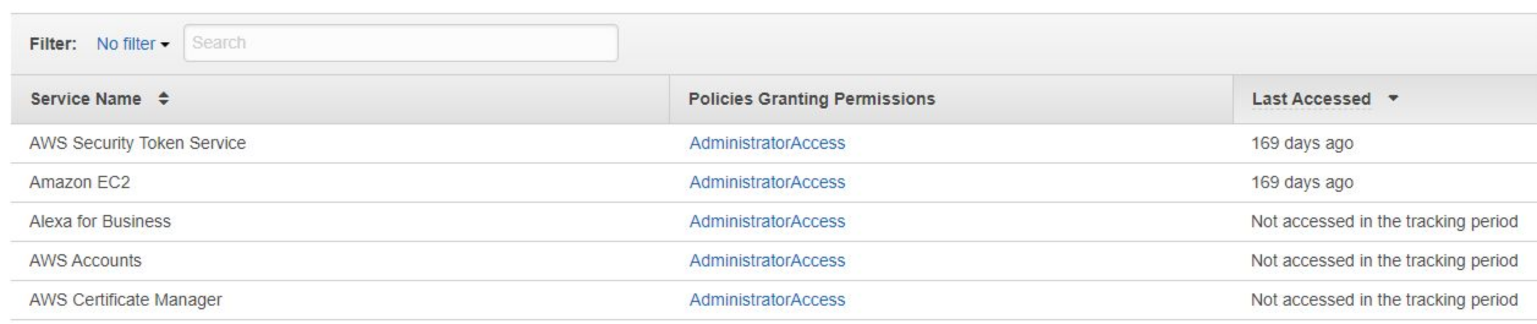
- Some application was vulnerable to SSRF
- WAF let SSRF through
- Role had read access to all S3 buckets

What is the solution?

- Cloud is special
- Least privilege is best privilege
- Monitor API key usage
- Automate, automate, automate

Least Privilege in AWS

AWS Access Advisor



Filter: No filter ▾ Search

Service Name	Policies Granting Permissions	Last Accessed
AWS Security Token Service	AdministratorAccess	169 days ago
Amazon EC2	AdministratorAccess	169 days ago
Alexa for Business	AdministratorAccess	Not accessed in the tracking period
AWS Accounts	AdministratorAccess	Not accessed in the tracking period
AWS Certificate Manager	AdministratorAccess	Not accessed in the tracking period

Netflix / **repokid**

duo-labs / **cloudtracker**

Resources

https://expel.io/blog/

Corey Quinn at Monktoberfest
@QuinnyPig

Cloud Economist at the Duckbill Group. Father to @QuinnyPiglet. Writes lastweekinaws.com. Podcast: screaminginthecloud.com he/him

San Francisco, CA duckbillgroup.com Joined December 2009

Rhino Security Labs
@RhinoSecurity

Rhino Security Labs is a top penetration testing and security assessment firm with a focus on cloud (AWS, GCP, Azure), network, and web application pentesting.

Seattle, WA RhinoSecurityLabs.com Joined February 2013

https://flaws.cloud
https://flaws2.cloud

CloudGoat (☁ 🐐)

rhino vulnerable | tool python 3.6+ license BSD PRs welcome

CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool.

Questions?