Managing Access to AWS

Ryan Lewis
CLOUD ENGINEER
@ryanmurakami ryanlewis.dev

Identity and Access Management

Overview

Return of the AAA concept

Users love to role play in groups

Cleaning up someone's user mess

Assuming a hamster role

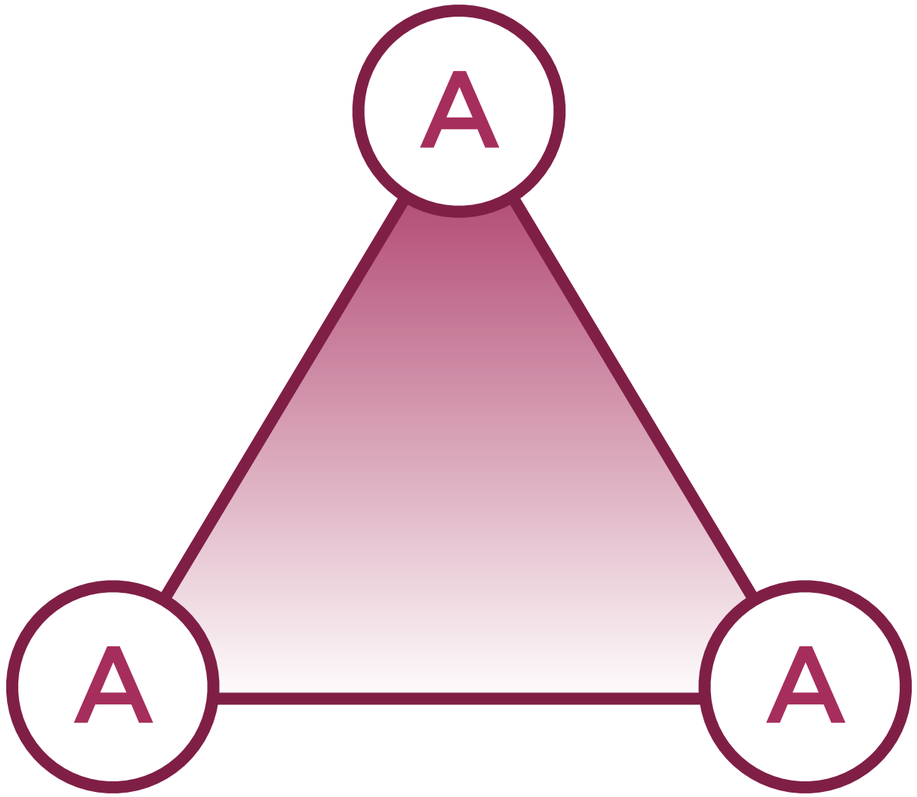
Protecting S3 content from yourself

The IAM Security Model

IAM Responsibilities

Authentication

Authorization


A
A
A

IAM Authentication

Determines if a user is who they say they are.

IAM Authentication Methods

Password

Passwords are only needed if a user will log into the AWS console

Password Policy Options

Password complexity

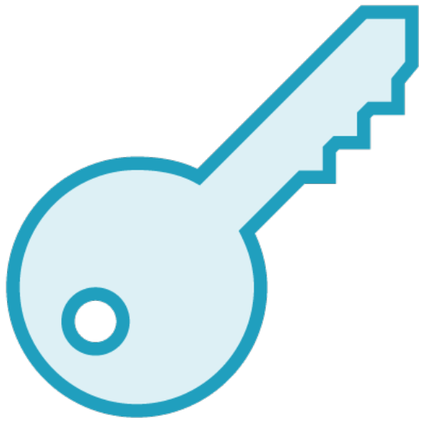
Password length

Password expiration

Requiring users to use MFA
is a simple and effective way
to drastically increase
security for your account

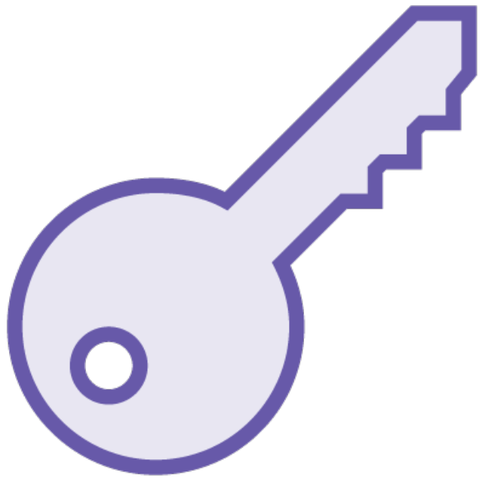
IAM Authentication Methods

Password



Access Key

Components of an Access Key

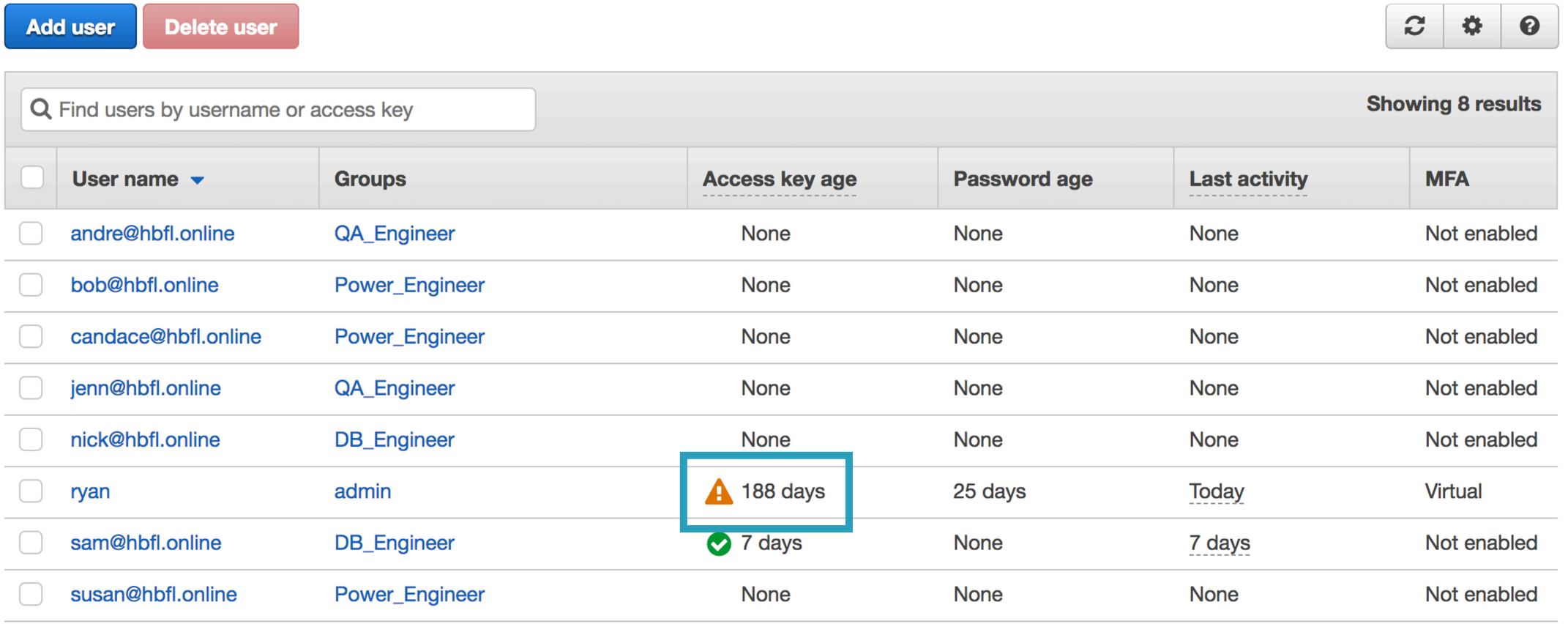


Used to identify key

+

Only visible on creation

Rotate access keys regularly



User name	Groups	Access key age	Password age	Last activity	MFA
andre@hbfl.online	QA_Engineer	None	None	None	Not enabled
bob@hbfl.online	Power_Engineer	None	None	None	Not enabled
candace@hbfl.online	Power_Engineer	None	None	None	Not enabled
jenn@hbfl.online	QA_Engineer	None	None	None	Not enabled
nick@hbfl.online	DB_Engineer	None	None	None	Not enabled
ryan	admin	188 days	25 days	Today	Virtual
sam@hbfl.online	DB_Engineer	7 days	None	7 days	Not enabled
susan@hbfl.online	Power_Engineer	None	None	None	Not enabled

Don't be like me

IAM Authorization

Determines what a user can do and can’t do.

IAM Policy

IAM Policy Properties

Allow/Deny

Action (what the user can do)

Resource (what resource the policy applies to)

Do Anything to Anything Policy

```
{
  "Effect": "Allow",
  "Action": [
    “*:*"
  ],
  "Resource": "*"
}
```

List DynamoDB Tables Policy

```
{
  "Effect": "Allow",
  "Action": [
    “dynamo:ListTables"
  ],
  "Resource": “*”
}
```

Users, Groups, and Roles

IAM User

Represents a person or service that needs access to AWS.

How to Let a User Do Things

Attach a managed policy

Create and attach an inline policy

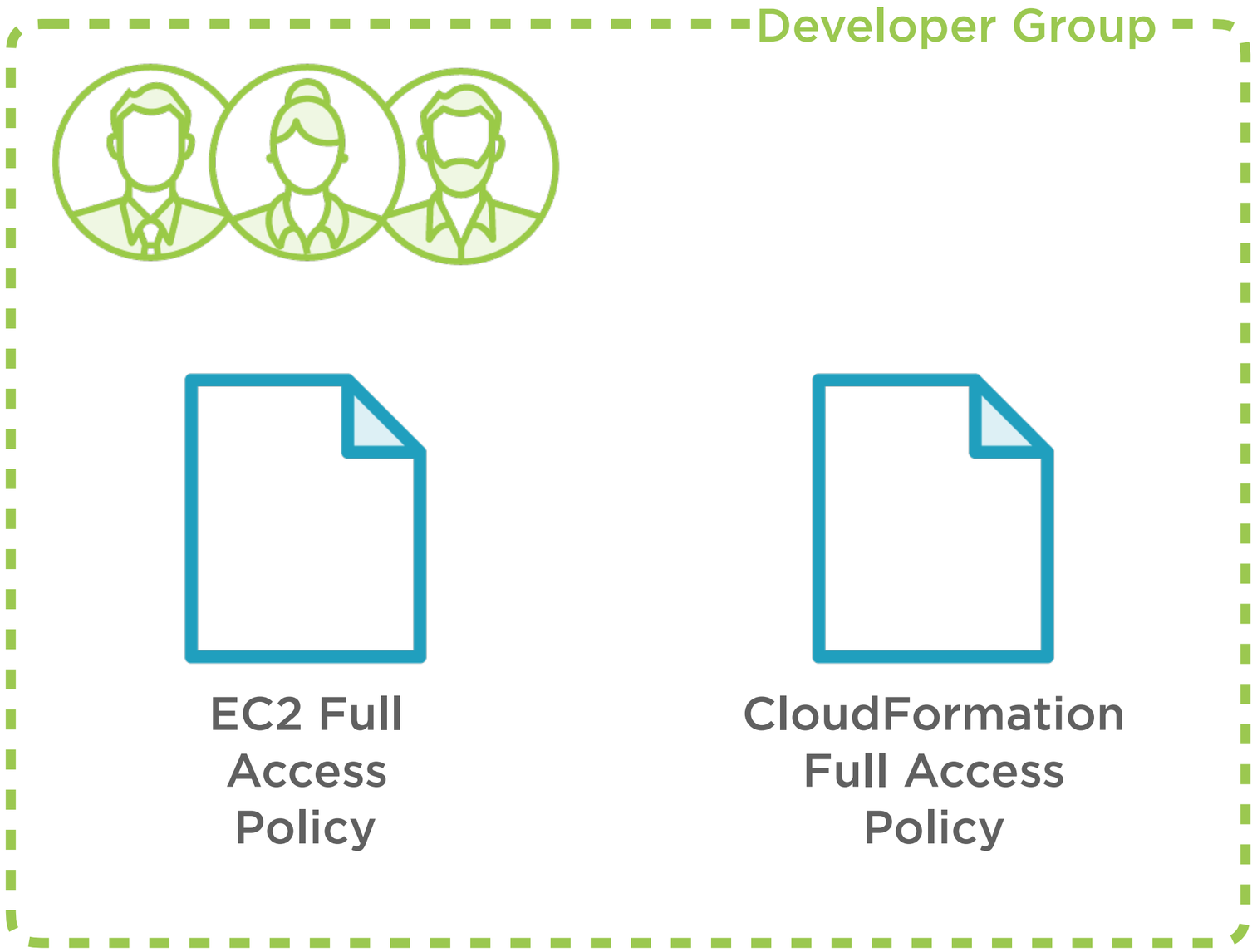
AWS recommends attaching policies to groups and then assigning users to them.

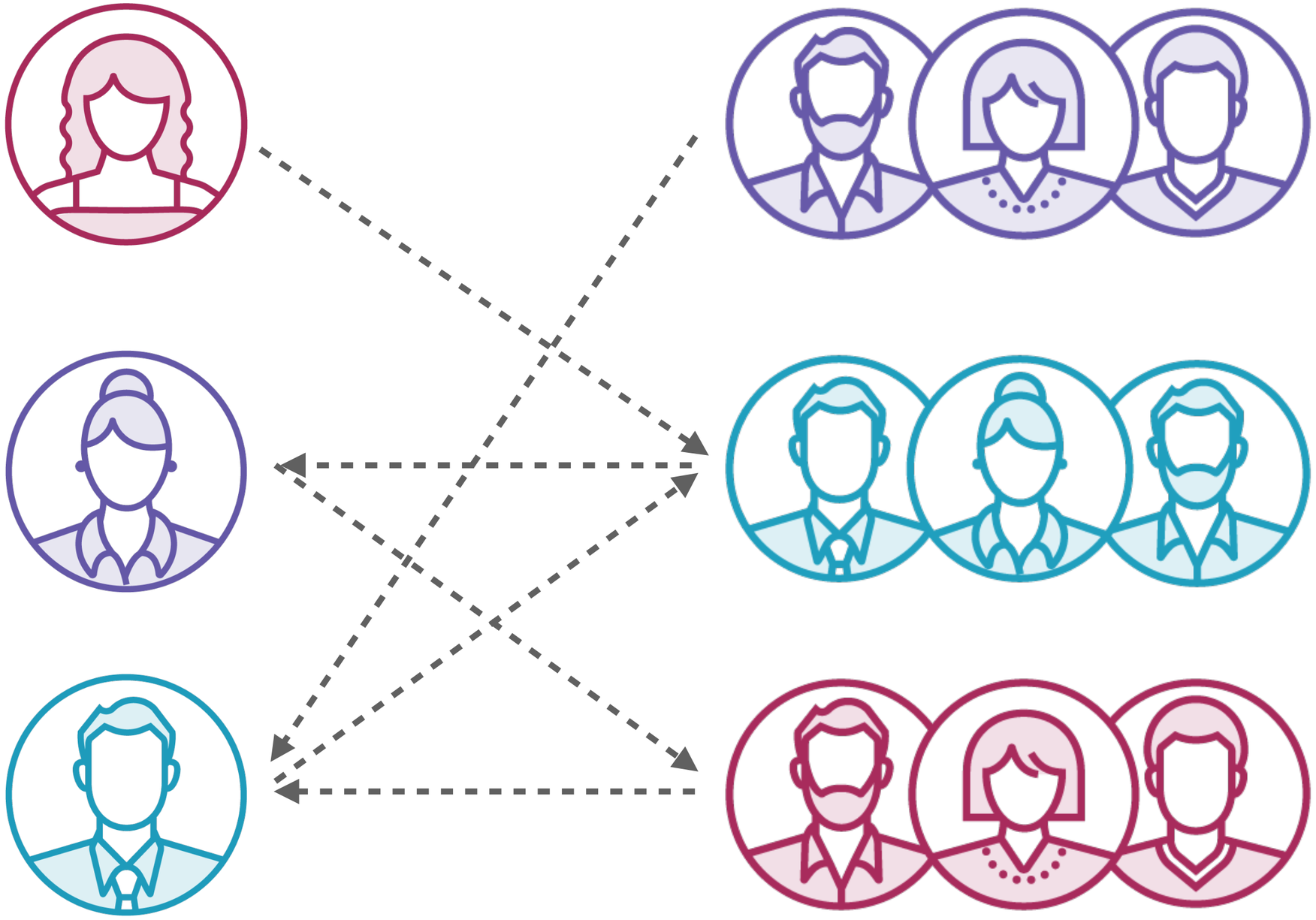
Ryan's Rule of Thumb for IAM Design

1 - 5 Users	Attach policies to users
6 - 20 Users	Assign users to groups
20+ Users	Use SAML or OpenID

IAM Group

Contains users and policies to cleanly assign permissions to users.


Developer Group
EC2 Full Access Policy
CloudFormation Full Access Policy



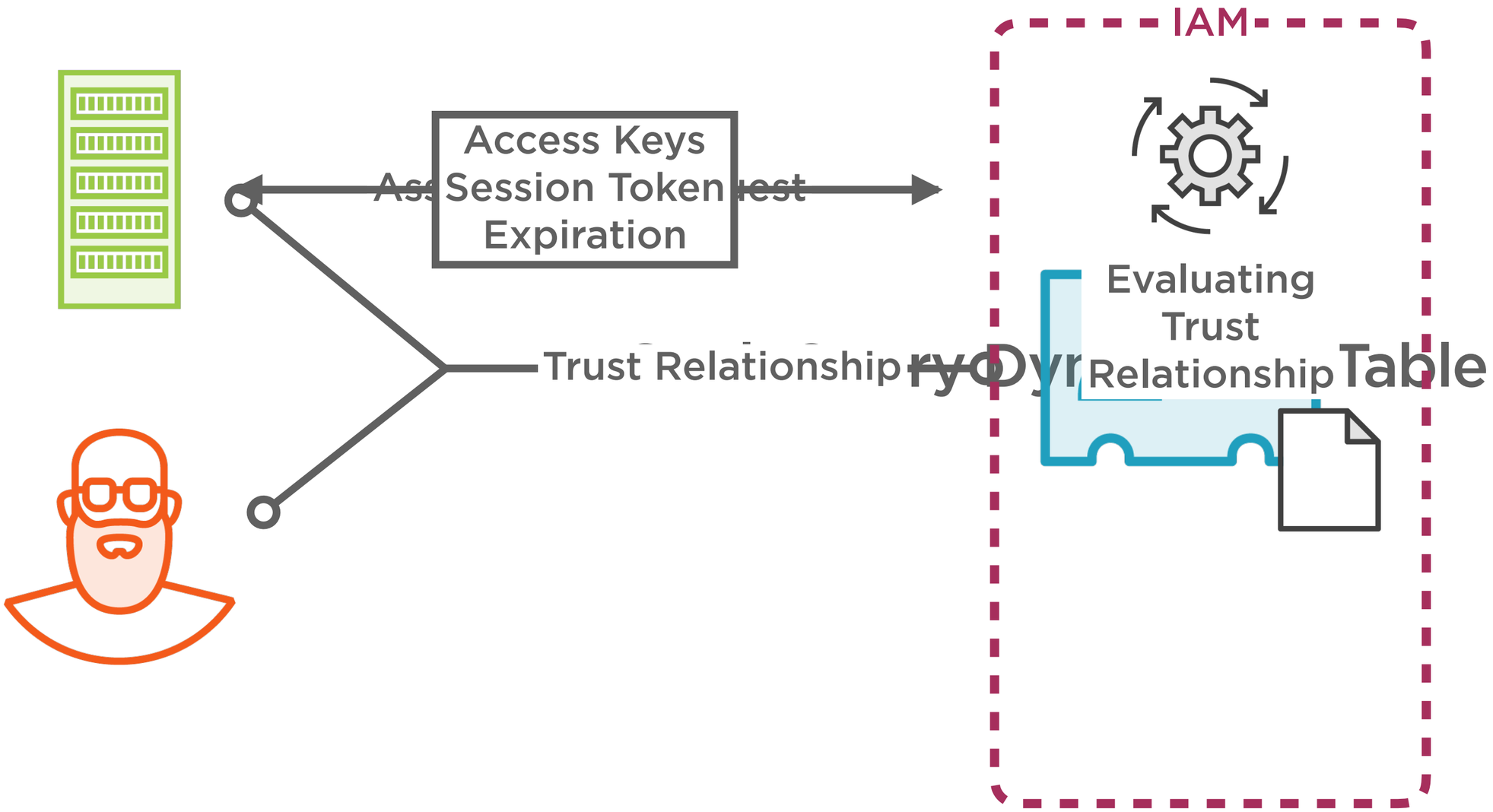
IAM Role

Entities that have attached policies. Resources can assume a role to obtain the permissions from the policies.

Roles don’t use traditional authentication methods

Roles have trust relationships with AWS resources

Assume Role Example



When credentials expire,
assume the role again

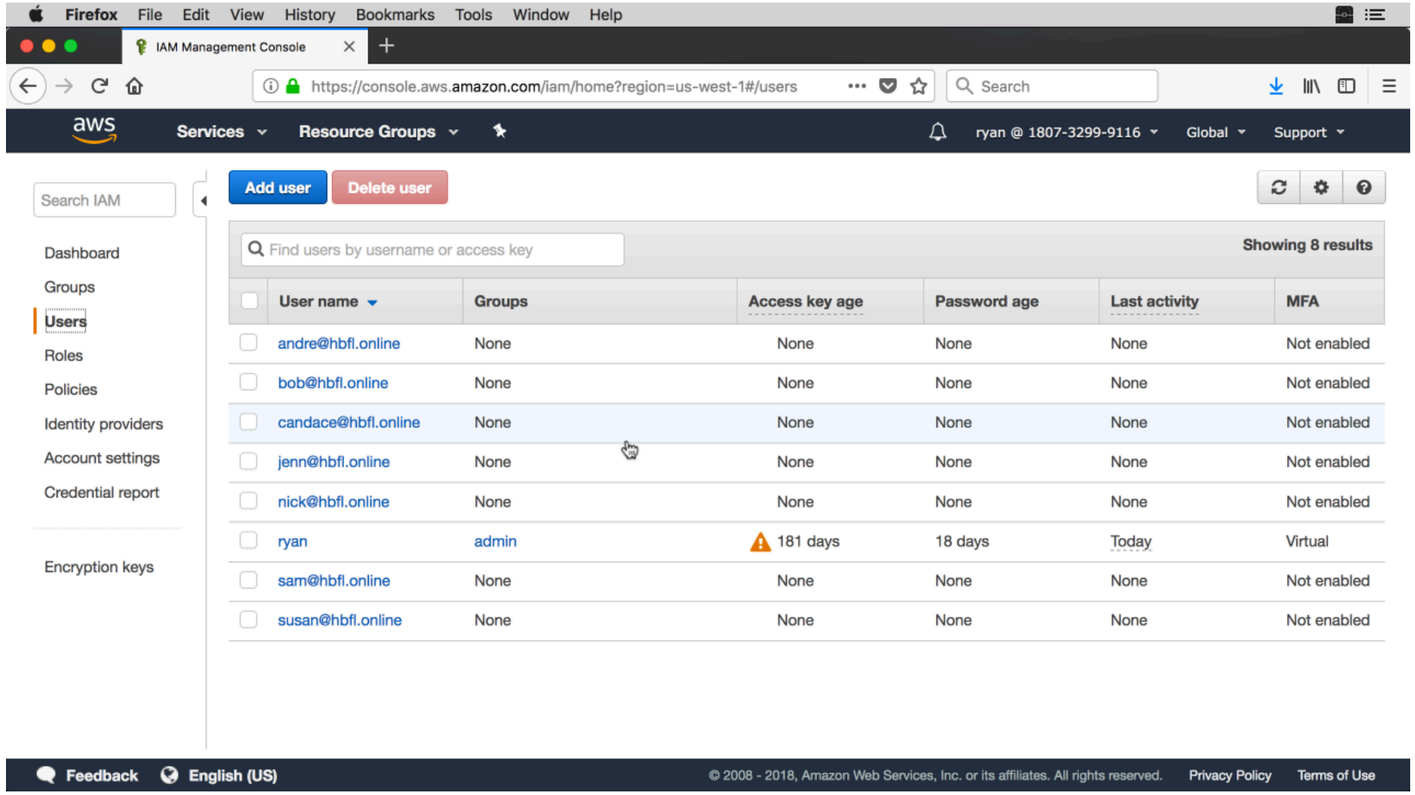
Remember This?

```
"HamsterEC2InstanceRole": {
  "Type": "AWS::IAM::Role",
  "Properties": {
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "ec2.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    },
    "ManagedPolicyArns": [ "arn:aws:iam::aws:policy/AdministratorAccess" ]
  }
},
```

Instance Profile

Maps an EC2 Instance to an IAM Role that it will assume for authorization.

Organizing Users into Groups


Firefox File Edit View History Bookmarks Tools Window Help
IAM Management Console
https://console.aws.amazon.com/iam/home?region=us-west-1#/users
Search
aws
Services
Resource Groups
ryan @ 1807-3299-9116
Global
Support
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Add user
Delete user
Find users by username or access key
Showing 8 results
User name
Groups
Access key age
Password age
Last activity
MFA
andre@hbfl.online None None None None Not enabled
bob@hbfl.online None None None None Not enabled
candace@hbfl.online None None None None Not enabled
jenn@hbfl.online None None None None Not enabled
nick@hbfl.online None None None None Not enabled
ryan admin 181 days 18 days Today Virtual
sam@hbfl.online None None None None Not enabled
susan@hbfl.online None None None None Not enabled
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

In real world situations, don't create users with CloudFormation

sam@hbfl.online

AmazonEC2ReadOnlyAccess

AmazonDynamoDBFullAccess

ServiceReadPolicy

susan@hbfl.online

AmazonDynamoDBFullAccess

CloudFormationFullAccessPolicy

andre@hbfl.online

AmazonEC2ReadOnlyAccess

ServiceReadPolicy

candace@hbfl.online

AmazonEC2FullAccess

AmazonDynamoDBFullAccess

ServiceReadPolicy

jenn@hbfl.online

AmazonEC2ReadOnlyAccess

AmazonDynamoDBReadOnlyAccess

ServiceReadPolicy

bob@hbfl.online

AmazonEC2FullAccess

AmazonDynamoDBFullAccess

CloudFormationFullAccessPolicy

nick@hbfl.online

AmazonDynamoDBFullAccess


EC2ReadOnlyGroup
EC2FullAccessGroup
DynamoDBReadOnlyGroup
DynamoDBFullAccessGroup
ServiceReadOnlyGroup
CloudFormationFullAccessGroup

Grouping Method #1

Group by Service Need

Control access to services
in one place

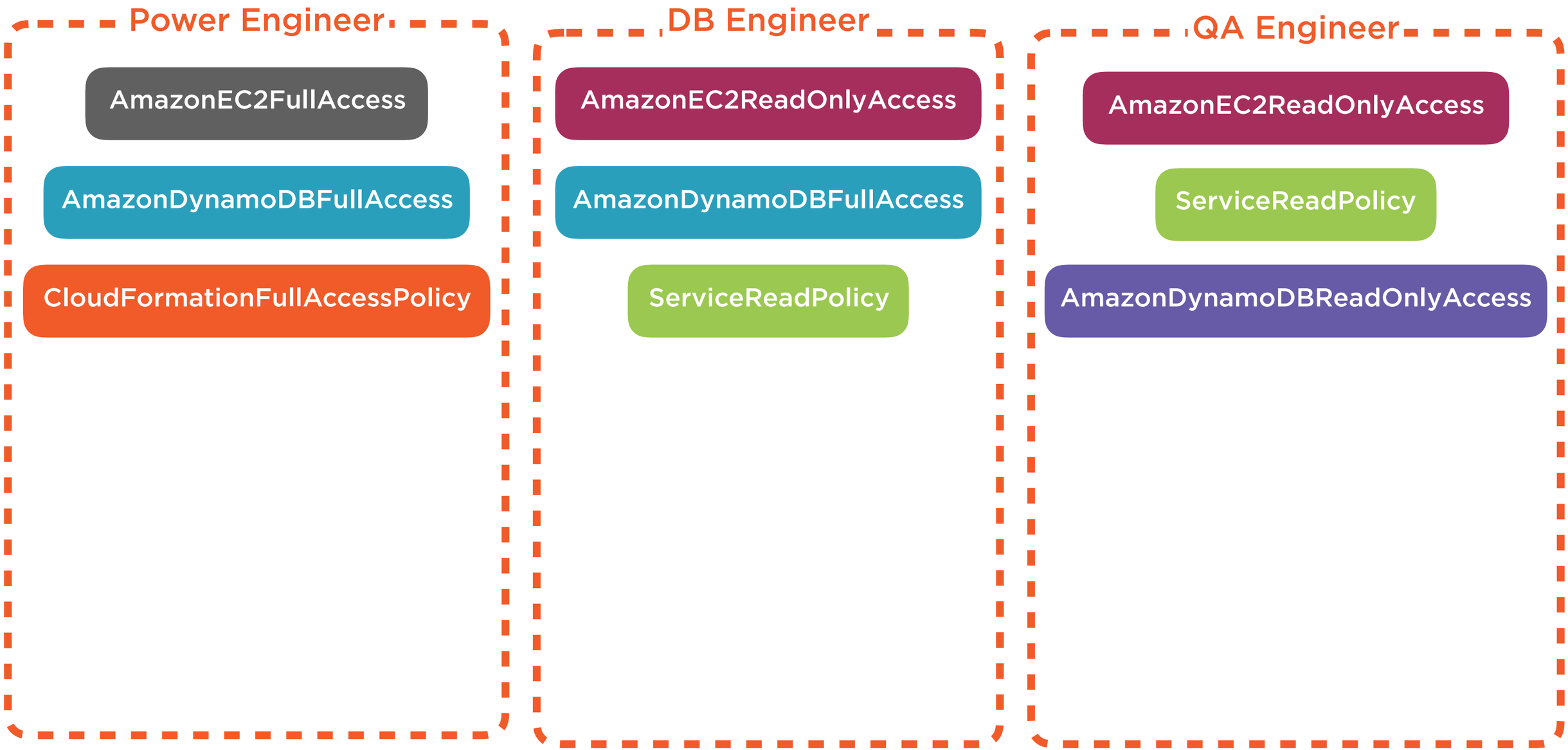
Many groups,
often mirroring policies

Grouping Method #2

Group by Responsibility

Matches closely to job title

Doesn't follow principle of least privilege


Power Engineer
AmazonEC2FullAccess
AmazonDynamoDBFullAccess
CloudFormationFullAccessPolicy
DB Engineer
AmazonEC2ReadOnlyAccess
AmazonDynamoDBFullAccess
ServiceReadPolicy
QA Engineer
AmazonEC2ReadOnlyAccess
ServiceReadPolicy
AmazonDynamoDBReadOnlyAccess

sam@hbfl.online

AmazonEC2ReadOnlyAccess

DB Engineer Group

ServiceReadPolicy

jenn@hbfl.online

AmazonEC2ReadOnlyAccess

QA Engineer Group

ServiceReadPolicy

candace@hbfl.online

AmazonEC2FullAccess

Power Engineer Group

ServiceReadPolicy

susan@hbfl.online

Power Engineer Group

CloudFormationFullAccessPolicy

bob@hbfl.online

AmazonEC2FullAccess

Power Engineer Group

CloudFormationFullAccessPolicy

andre@hbfl.online

AmazonEC2ReadOnlyAccess

QA Engineer Group

nick@hbfl.online

DB Engineer Group

Managing Users and Groups in IAM

Creating and Assuming IAM Roles

Managing Access to S3 Content

Object Access Methods in S3

IAM Policy

S3 Bucket Policy

S3 Bucket ACL

S3 Object ACL

When should I use each method?

S3 Access Method #1

IAM Policy

Need access to create IAM policies

Separates bucket access from the bucket itself

S3 Access Method #2

S3 Bucket Policy

Same type of access control as IAM policy

Configuration is kept with the bucket

Can enable full public access

S3 Access Method #3

S3 Bucket ACL

Can give similar access as S3 bucket policy

AWS recommends only using for S3 logs

S3 Access Method #3

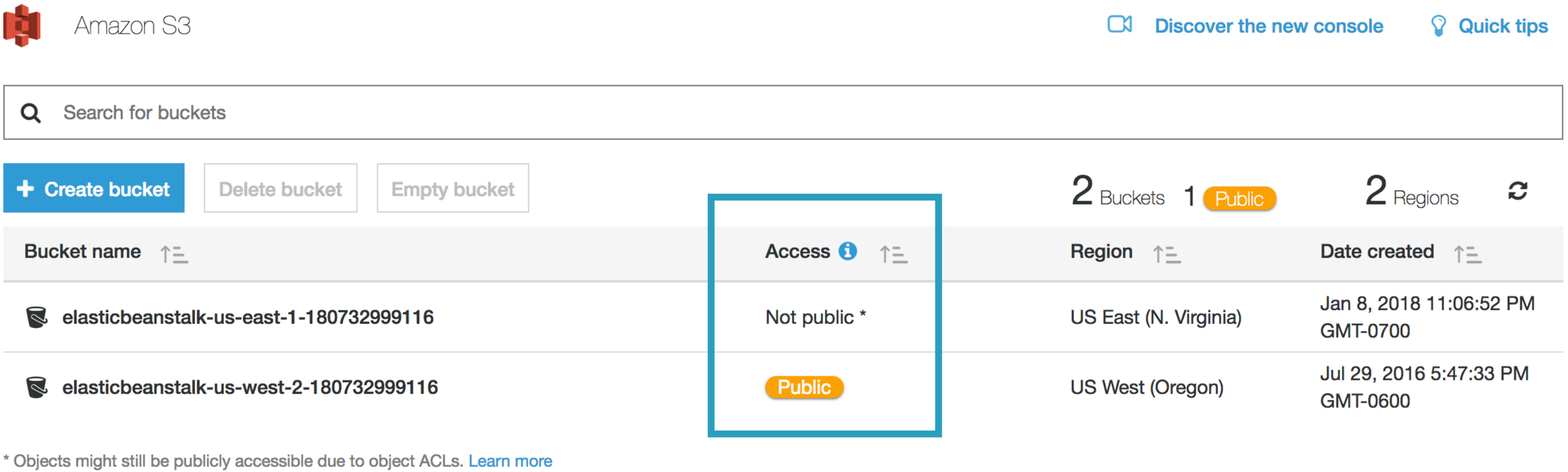
S3 Object ACL

Give access similar to S3 bucket ACL

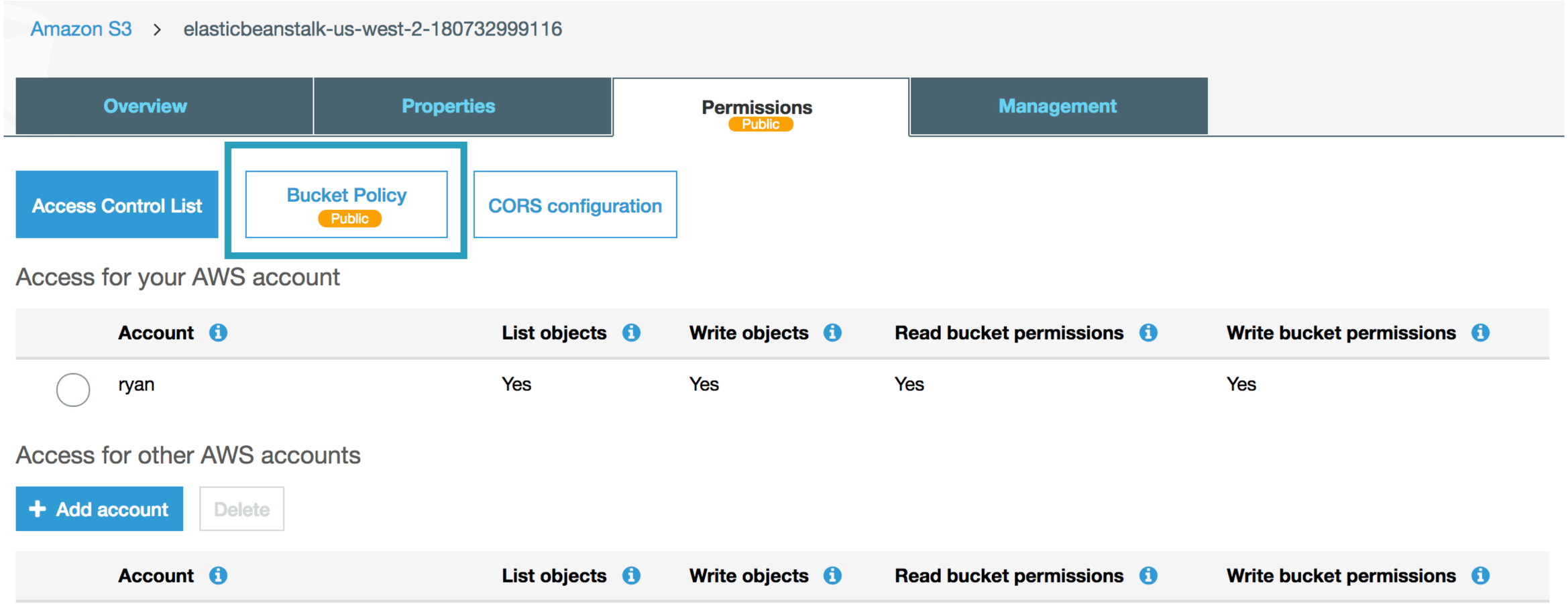
Only method that applies to individual objects

Each object ACL is unique to that object

S3 Dashboard



S3 Bucket Permissions



Don’t become a statistic

Keep your S3 objects secure

Conclusion

I've learned the most about IAM by just trying things to understand how the service affects permissions

Summary

IAM: Authorizing and authenticating since 2012

Swapping policies between users and groups

Groups and policies > Users and policies

Becoming the hamster

I thought ACLs were just for VPCs?

Thank you!

Ryan Lewis
CLOUD ENGINEER

@ryanmurakami ryanlewis.dev