https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/

Keep up with AWS

In a security context

We’re going to talk about how AWS IAM sucks
How we can make dealing with it less stressful

About me

Co-conspirators

Alana Kirby

Aidan Steele

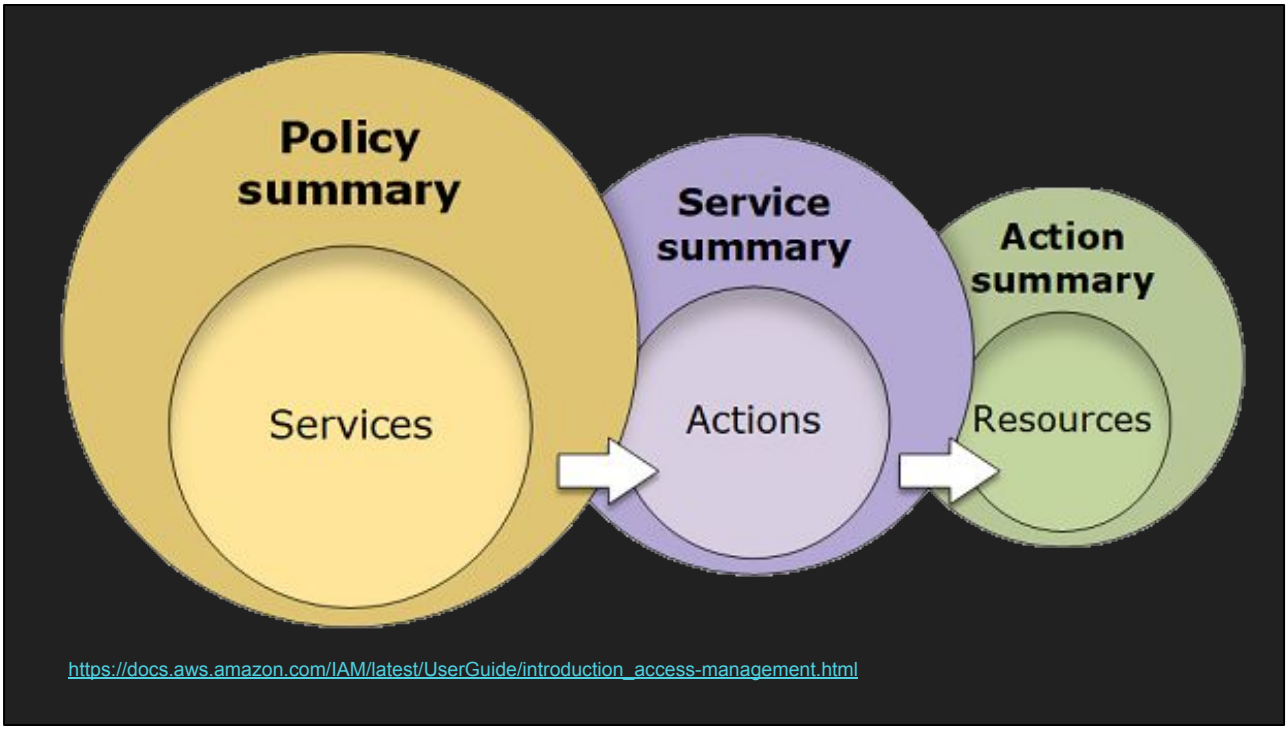
Rupert Bryant-Greene

https://github.com/alanakirby/aktion

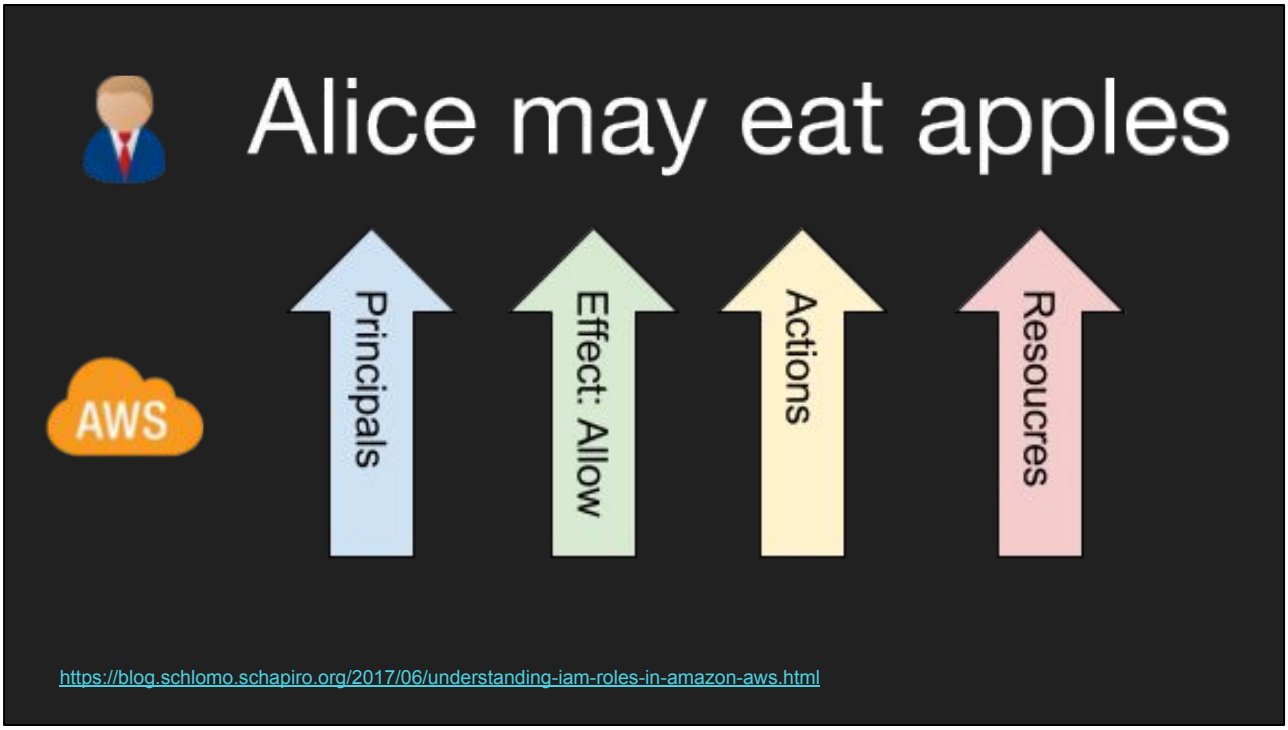
Original art by Alana, now there’s four of us.

https://commons.wikimedia.org/wiki/File:Amazon_Basics_battery,_Papenburg_(2019).jpg

Let’s start with some AWS basics
IAM is ***the*** core AWS service
It controls everything



AWS access controls are broken down into:
Principal, Resource, Action
Every time you do something it involves one of each of these



Permissions are calculated by checking if the principal can perform an action on a resource.
When you S3:ListBuckets, **you** are **listing** the **buckets**.

There are two places where policies are applied

Both Principals and Resources can have policies applied to them do control access. Sometimes there are Roles, service control policies etc. but these essentially extend either the Principal or Resource's policies.

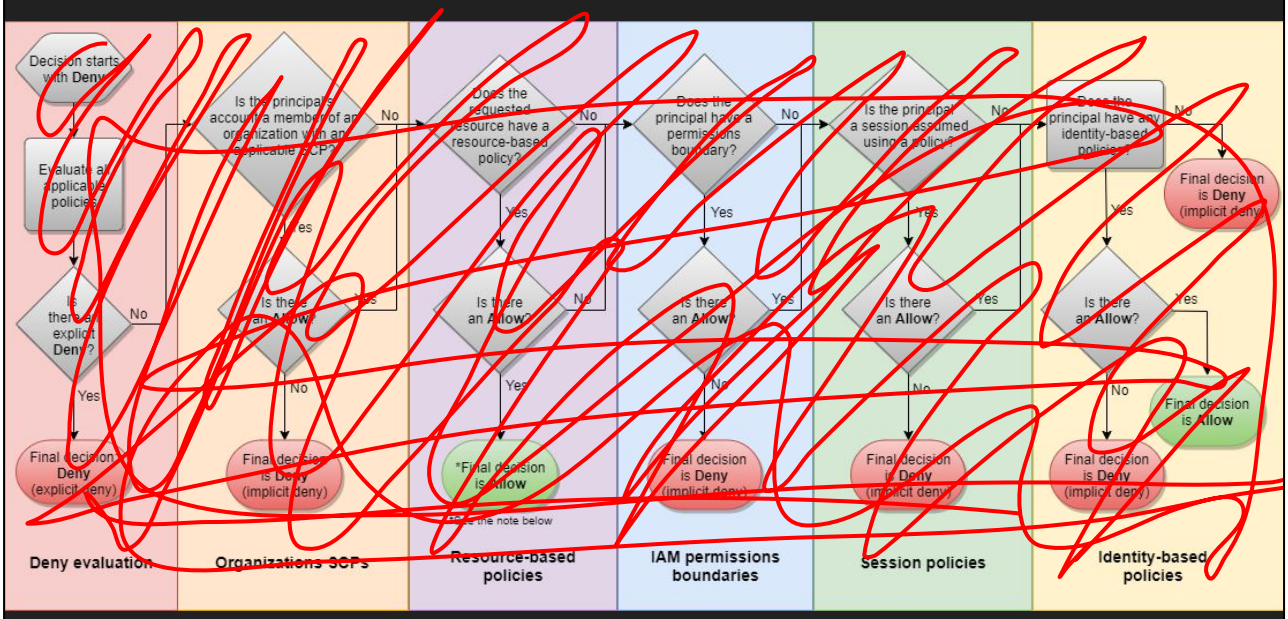
"Olly, you're over simplifying things" - IAM nerds in the room

As Dave says...

“[the] mental gymnastics of post-modern IAM policy theory”

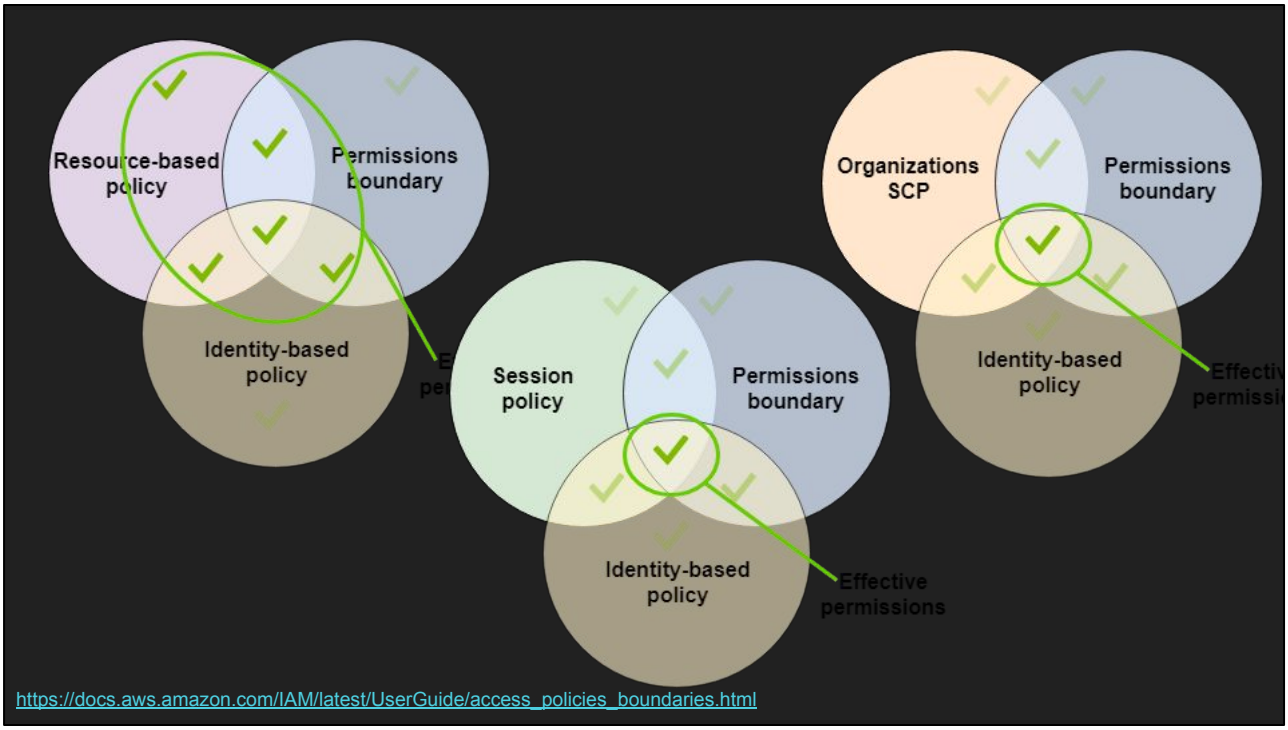
It gets more complex

I’m not going to do this with you today,
but if I don’t mention it other IAM nerds will at me



https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

If you hang out with IAM nerds, you'll have seen this referenced
We don't have time to go down that rabbit hole



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

Permissions boundaries are also just more policies
Organisation Service Control Policies and Session Policy also
Caveat that you might have permission even if not all of these are set

Whitelists vs Blacklists
Whitelists are great but often impractical
Blacklists aren’t strict enough
Everyone sits somewhere in the middle

Whitelisting is the ideal scenario for Security
people who don't care or want to get work done,
get frustrated and cut corners
Most people use it because it includes PutObject and PutObjectTag
Who knows how many PutObject* actions there are?

s3:PutObject

s3:PutObjectAcl

s3:PutObjectLegalHold

s3:PutObjectRetention

s3:PutObjectTagging

s3:PutObjectVersionAcl

s3:PutObjectVersionTagging

s3:PutObjectLockConfiguration

There are 8!
What is a LegalHold?
Prevents object from being deleted or overriden
Don’t worry s3:BypassGovernanceRetention exists

It can’t be changing that fast...

	31 Oct 2019	31 Dec 2019		20 Feb 2020	
Services	191	216	▲25	217	▲1
Actions	6858	7801	▲943	7884	▲83
Managed Policies	566	621	▲55	631	▲10

re:Invent

Granted, it was re:invent season

Do you know for sure, which of the
217 Services,
7801 actions and
631 managed policies
your org uses and how that compares to the access granted?

I want to show you something that can help, but first an example

```
"PolicyId": "ANPAIJLU43R6AGRBK76DM",
"PolicyName": "AWSMobileHub_FullAccess",
"PolicyVersion": {
  "CreateDate": "2018-02-05T23:44:29Z",
  "CreateDate": "2019-12-19T23:15:52Z",
  "Document": {
    "Statement": [
      {
        "Action": [
          "apigateway:GET",
          "apigateway:GetResources",
          "apigateway:GetRestApis",
          "apigateway:POST",
          "apigateway:TestInvokeMethod",
          "cloudfront:GetDistribution",
          "devicefarm:CreateProject",
          "devicefarm:GetProject",
```

```
26 +37,7 @@
          "lex:GetIntents",
          "lex:GetSlotType",
          "lex:GetSlotTypes",
          "mobilehub:CreateProject",
          "mobilehub:DeleteProject",
          "mobilehub:DeleteProjectSnapshot",
          "mobilehub:DescribeBundle",
          "mobilehub:ExportBundle",
          "mobilehub:ExportProject",
          "mobilehub:GenerateProjectParameters",
          "mobilehub:GetProject",
          "mobilehub:GetProjectSnapshot",
          "mobilehub:ImportProject",
          "mobilehub:ListAvailableConnectors",
          "mobilehub:ListAvailableFeatures",
          "mobilehub:ListAvailableRegions",
          "mobilehub:ListBundles",
          "mobilehub:ListProjectSnapshots",
          "mobilehub:ListProjects",
          "mobilehub:SynchronizeProject",
          "mobilehub:UpdateProject",
          "mobilehub:ValidateProject",
          "mobilehub:VerifyServiceRole",
          "mobilehub:*",
          "sns:ListTopics"
```

This is an AWS Managed Policy
That they can’t even be bothered keeping up to date

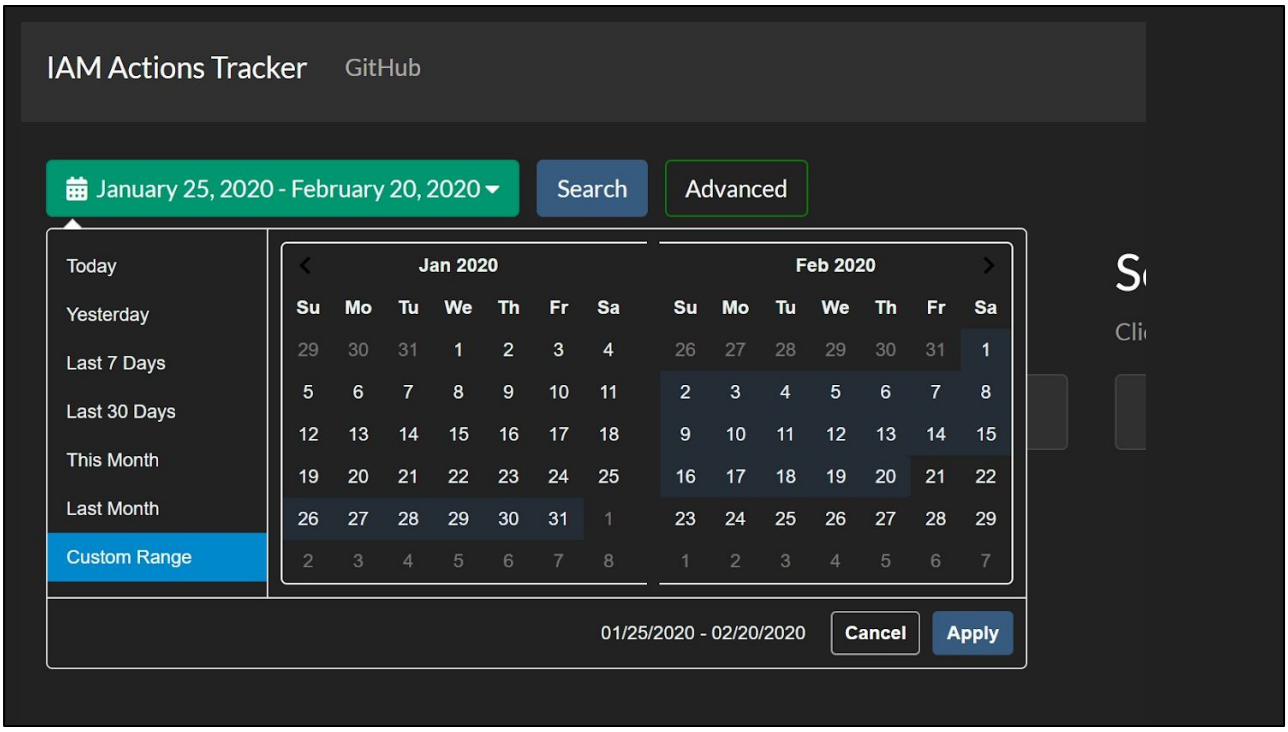
```
"mobilehub:ValidateProject",
"mobilehub:VerifyServiceRole",
"mobilehub:*",
"sns:ListTopics"
```

Policy version numbers can’t be used to control which version of an AWS managed policy is being used,
only by AWS to roll back just like you can yourself.
The only thing it allows you to do is (manually) track when AWS changes the policy.

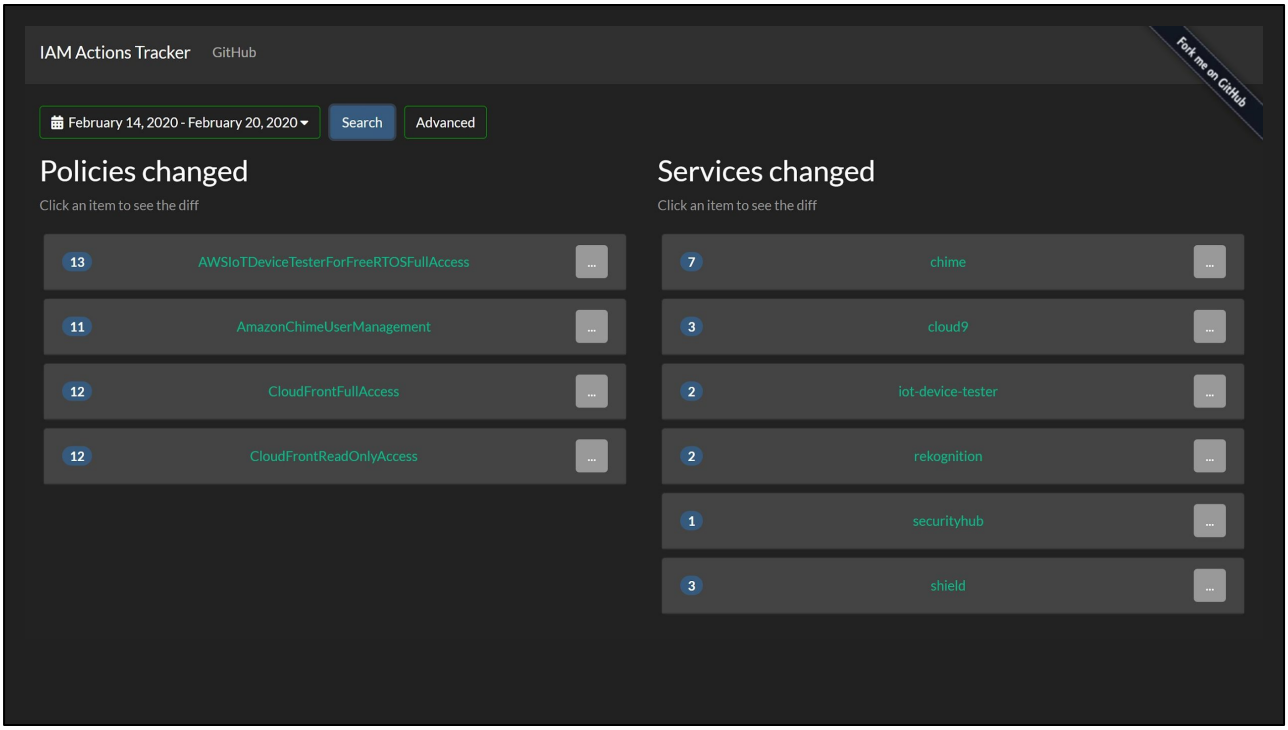
Demo Time

[see backup slides later]

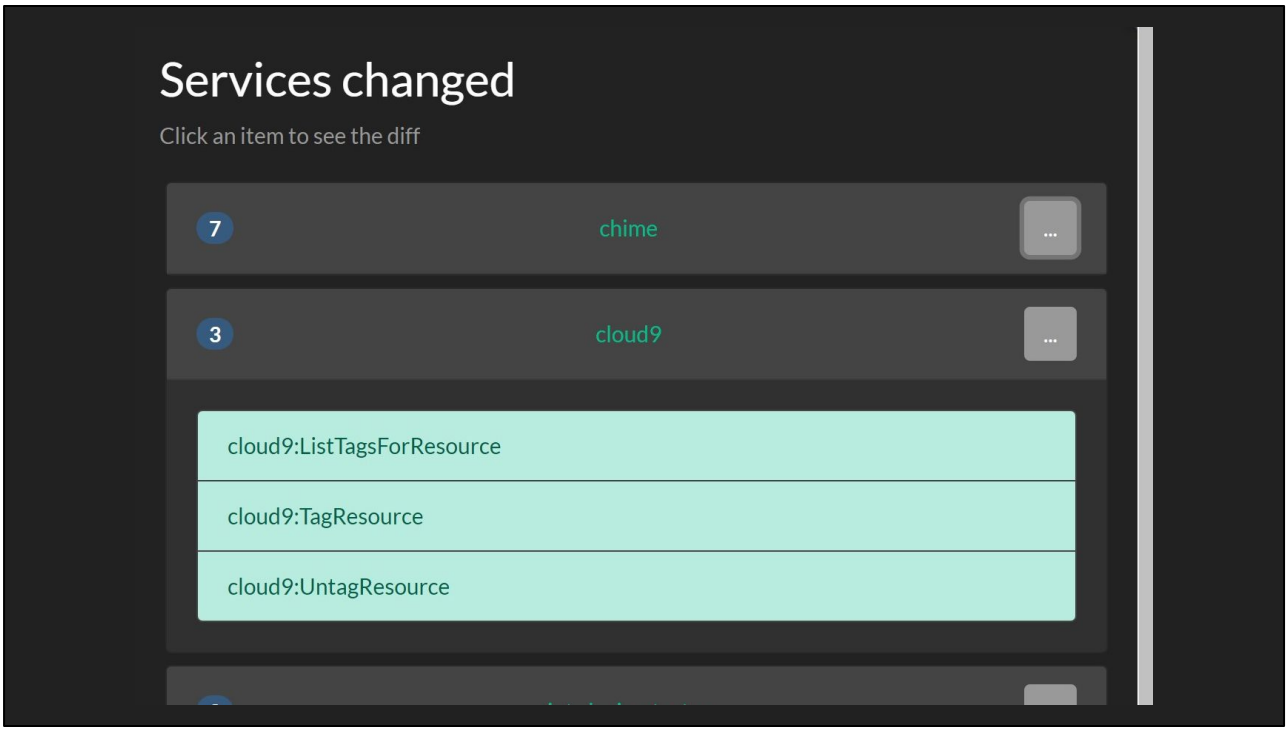
Freudian Llama



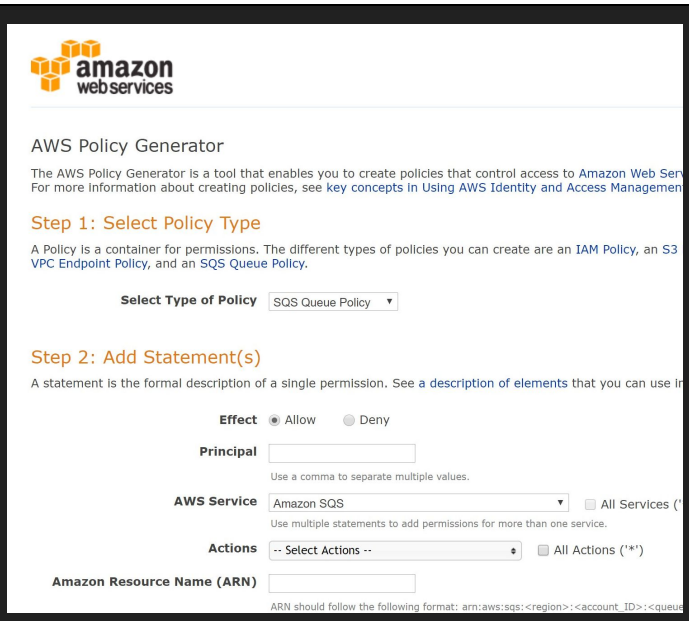
https://action.io/
Select date range



Shows you what's changed



Tada! Cloud9 added Tagging support



https://awspolicygen.s3.amazonaws.com/policygen.html

How it works

- Cron
- Scrapy Scrape Policy Generator and SDKs
- Commit
- Caching stuffs
- Static + serverless
- Netlify??

Recent Announcements APP 10:02 AM

AWS CodeBuild Adds Support for Amazon EFS

You can now use Amazon Elastic Filesystem (EFS) in AWS CodeBuild build jobs. This can be achieved by specifying the EFS file system Id in your CodeBuild Project. (edited)

GitHub APP 10:05 AM

github-actions[bot]

1 new commit **pushed to** `master`

`2ff715d7` - New actions

glassechidna/trackiam

github-pages[bot]

Successfully deployed `2ff715d` to github-pages

glassechidna/trackiam

We're pretty good at keeping up

```
{
  "Arn": "arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess",
  "CreateDate": "2016-12-01T19:04:44Z",
- "DefaultVersionId": "v8",
+ "DefaultVersionId": "v9",
  "IsAttachable": true,
  "Path": "/",
  "PolicyId": "ANPAJQJGIOIE3CD2TQXDS",
  "PolicyName": "AWSCodeBuildAdminAccess",
  "PolicyVersion": {
-   "CreateDate": "2019-11-05T22:12:30Z",
+   "CreateDate": "2020-02-06T20:26:30Z",
    "Document": {
      "Statement": [
        {

2,6 +42,7 @@
            "ec2:DescribeVpcs",
            "ecr:DescribeRepositories",
            "ecr:ListImages",
+           "elasticfilesystem:DescribeFileSystems",
            "events:DeleteRule",
            "events:DescribeRule",
            "events:DisableRule",
```

Aidan bot
authored 2/7/2020 @ 10:05 AM

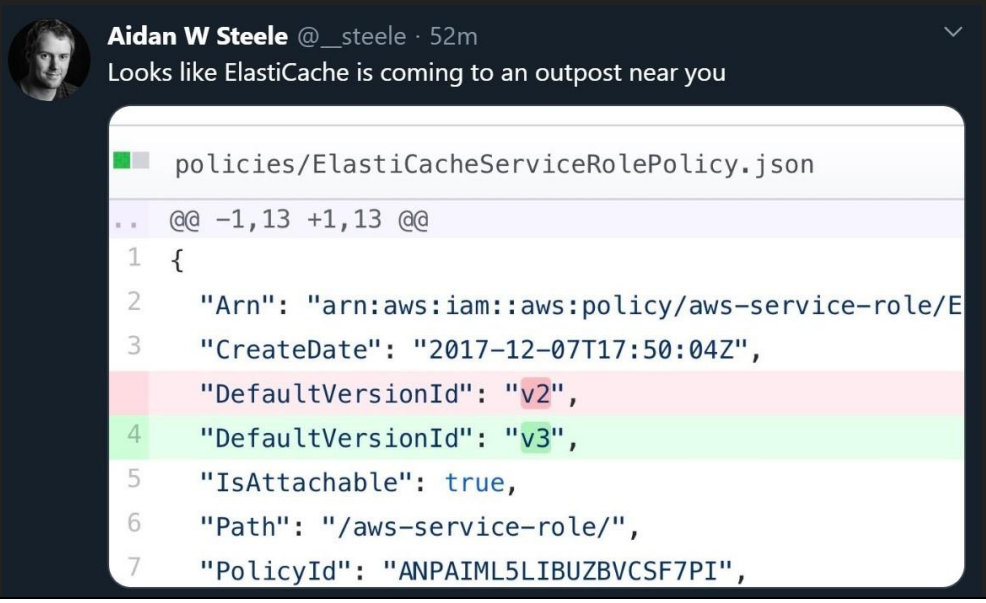
1 modified

Path

policies/AWSCodeBuildAdminAcces

Do you check all the managed policies you give your developers access to?

Check out Aktion.io or follow @__steele on Twitter



Sometimes we get the scoop on things before they're official
And by "we" I mean Aidan

Where to next?

TLS transparency logs
Track what actions go in CloudTrail
RSS / WebHooks / Twitterbot / Slackbot
Linking to relevant material
Classifying changes
See GitHub for details

Mainly making consumption easier

Please check out GitHub / Contribute

https://aktion.io/

- There is so, so much to keep up with
- Even AWS can't keep up
- You're not alone

https://ewert.co.nz/slides

@OllyTheNinja

If you are scared you should be, but know that everyone else is too
Because it's hard and even AWS has trouble staying up to date
One more tool in your belt
Enjoyed being here, great community, please don't be a stranger in person or online