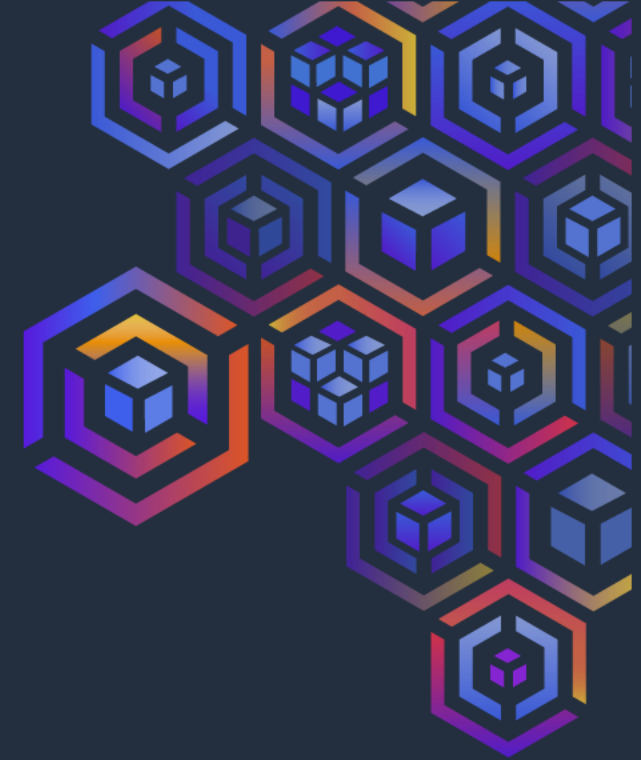




**COMMUNITY DAY**

# AWS Control Tower How to adopt it?

Peter Sankauskas | @pas256 | 2024

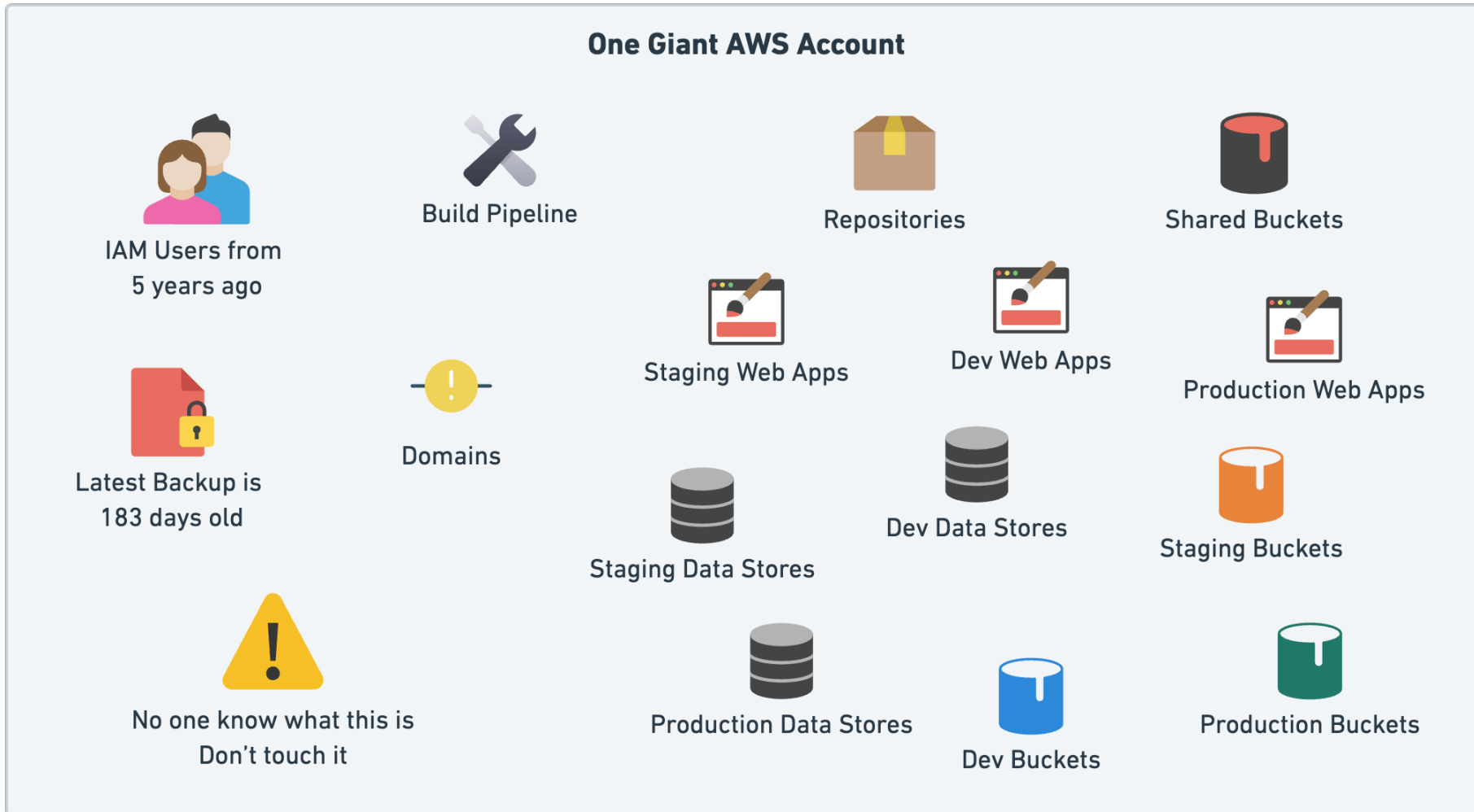


# A startup is born

- Founders create an AWS account
- Create PoC
- Hire team
- Add staging VPC
- Add development VPC
- Export data for customers



# Today



# Vision



SSO

## Shared Internal Resources



Build Pipeline



Repositories



Shared Buckets



Domains



Audit



Archives & Backups

## Production



Web Apps



Data Stores



Production Buckets

## Staging



Web Apps



Data Stores



Staging Buckets

## Development



Web Apps



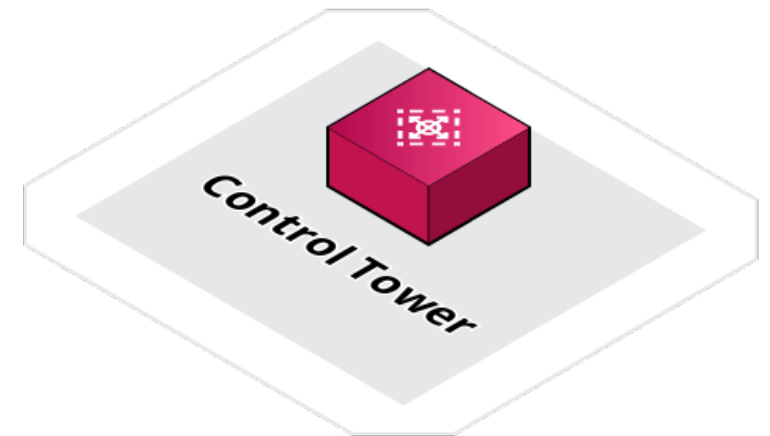
Data Stores



Dev Buckets

# AWS Control Tower

- Create and orchestrate multiple accounts
- Set up governance with pre-packaged guardrails
- Manage identities & federated access
- Centralize logging
- Enable cross-account security auditing
- Deployment of new rules



Your situation is unique



This is what we did... find what works for **you!**

# Brand new AWS Account



- This is our Management Account
- Use AWS SSO with an External Identity Provider (OneLogin or Okta)
  - Can use AWS Identity Center, Active Directory, etc
- Google Group mailing list for all AWS accounts
  - `aws@example.com`
    - ➔ `aws+management@example.com`
    - ➔ `aws+audit@example.com`

# Org Structure

- Plan this well
- Manage rollout by OU

AWS Control Tower > Controls library: All controls >  
Require an Amazon API Gateway REST and WebSocket API to have logging activated > Enable control on OU

### Enable control on OU

Choose an organizational unit (OU) to enable the following control: Require an Amazon API Gateway REST and WebSocket API to have logging activated.

< 1 >

| Name           | Parent organizational unit | State      |
|----------------|----------------------------|------------|
| Root           | -                          | Registered |
| Engineering OU | Root                       | Registered |
| Experiments OU | Root                       | Registered |
| Security OU    | Root                       | Registered |

Cancel **Enable control on OU**

## Root

- ▶ Management account
- ▶ Core OU
  - ▶ Shared Internal
  - ▶ Dev
  - ▶ Staging
  - ▶ Production
- ▶ Security OU
  - ▶ Log Archive
  - ▶ Audit
- ▶ Sandboxes OU
  - ▶ Project 1
  - ▶ Project 2



# Enroll your existing AWS account



- Read the prerequisites

<https://docs.aws.amazon.com/controltower/latest/userguide/enrollment-prerequisites.html>

- Add account to the AWS Organization
- Disable AWS Config in the account to enroll
- Add the **AWSControlTowerExecution** IAM role

# Things will break

- Get team comfortable with SSO and role selection
  - Increase the *maximum session duration* in Identity Center to prevent frustration
- Use SSO for CLI

```
aws sso login --profile prod
```
- Renew **RI**s and **Savings Plans** in the *Management Account* to share across the Organization
- Modify build pipeline to also use OIDC credentials provider
  - Start to remove old IAM Users



# Guardrails

- Customize 520+ controls
  - Detective = Config
  - Preventive = SCP
  - Proactive = CloudFormation

Control objectives (15) [Info](#) [View details](#)

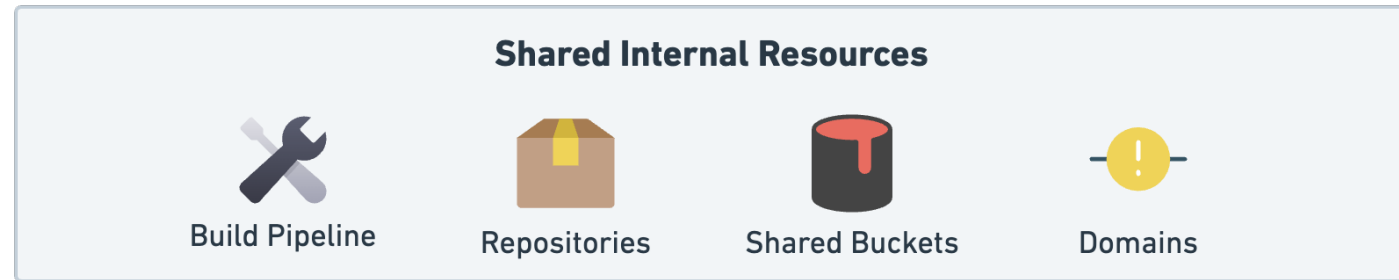
Find control objectives

< 1 > ⚙

|                       | Control objective                                | Controls |
|-----------------------|--|----------|
| <input type="radio"/> | <a href="#">Establish logging and monitoring</a> | 59       |
| <input type="radio"/> | <a href="#">Encrypt data at rest</a>             | 65       |
| <input type="radio"/> | <a href="#">Use strong authentication</a>        | 16       |
| <input type="radio"/> | <a href="#">Encrypt data in transit</a>          | 46       |
| <input type="radio"/> | <a href="#">Protect configurations</a>           | 59       |
| <input type="radio"/> | <a href="#">Manage vulnerabilities</a>           | 26       |
| <input type="radio"/> | <a href="#">Enforce least privilege</a>          | 91       |
| <input type="radio"/> | <a href="#">Improve availability</a>             | 47       |
| <input type="radio"/> | <a href="#">Improve resiliency</a>               | 25       |
| <input type="radio"/> | <a href="#">Limit network access</a>             | 100      |
| <input type="radio"/> | <a href="#">Optimize costs</a>                   | 7        |
| <input type="radio"/> | <a href="#">Protect data integrity</a>           | 20       |
| <input type="radio"/> | <a href="#">Prepare for disaster recovery</a>    | 1        |
| <input type="radio"/> | <a href="#">Prepare for incident response</a>    | 10       |
| <input type="radio"/> | <a href="#">Manage secrets</a>                   | 4        |

# Don't boil the ocean

- Use Account Factory to create new ***Shared Internal Account***



- Why this account first?
  - Modify build pipeline to push artifacts to this account
    - Accessed by Dev, Staging & Prod
  - Migrate Route53 domains and zones
  - Get comfortable with cross-account IAM Roles & Policies



# Dev account

- Likely need to modify IaC to support multiple environments/accounts
- Account Factory customization
  - AFC = CloudFormation
  - AFT = Terraform
- Create accounts *without* a Control Tower VPC

## Edit account factory network configuration

### VPC configuration options for new accounts

#### Internet-accessible subnet

- Allow your users to create a public subnet in the VPC when provisioning a new account. If you edit the account factory configuration to enable public subnets when provisioning a new account, account factory configures Amazon VPC to create a [NAT Gateway](#). You will be billed for your usage by [Amazon VPC](#).

#### Maximum number of private subnets

Specify the maximum number of private subnets in the VPC.

0

#### Address range (CIDR) restriction for account VPCs

Range of addresses within which your account VPCs will be created.

172.31.0.0/16

Must be a valid 0.0.0.0/x format

#### Regions for VPC creation

Regions where VPCs are automatically created when an account is provisioned.

- US East (N. Virginia)  
 US East (Ohio)  
 US West (Oregon)

# Staging, then Production

- Staging should be easier after Dev
- Production cut over
  - Easy: Planned maintenance window for downtime
  - Hard: Zero downtime
    - Data - carefully plan cut-over
    - DNS - don't rely on this for cut-over (not atomic)
      - Use LBs, API Gateways - things that are observable inside your infrastructure



# Clean up

## Legacy account

- Introduce SCPs to prevent usage
- Monitor CloudTrail for remaining activity



# Achievement Unlocked



- In the end, you get:
  - Isolation by environment, without complex IAM policies
  - Billing separation
  - No more long-live credentials on employee laptops
  - Guardrails
- Next steps
  - Enable IAM Access Analyzer
  - Enable GuardDuty
  - Enable Security Hub
  - Deploy ^^ from the Management Account
  - View results in the Audit Account



# Tips

- Plan
  - Break it down into phases - this could take a year to complete
- Persuade
  - Convince the team it is worth it
- Provision
  - Roll out incrementally - celebrate wins along the way
- Patience
  - Don't push forward if something is broken



# Slides

Slides available at

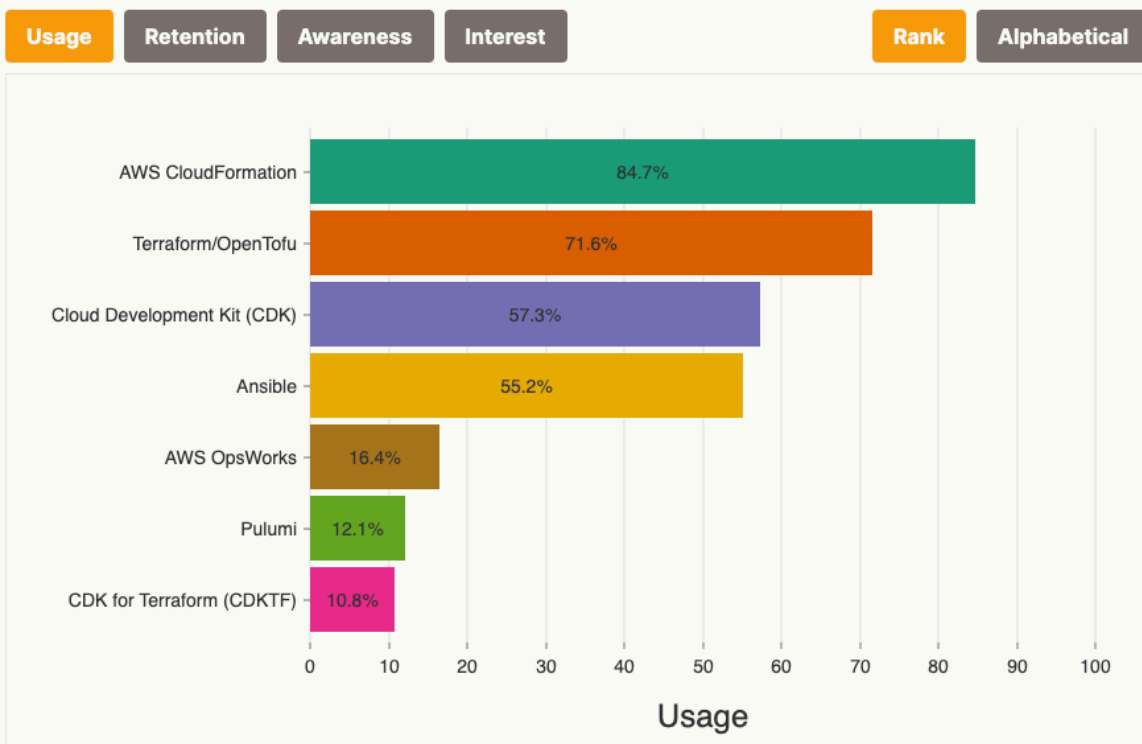
<https://answersforaws.com/slides>





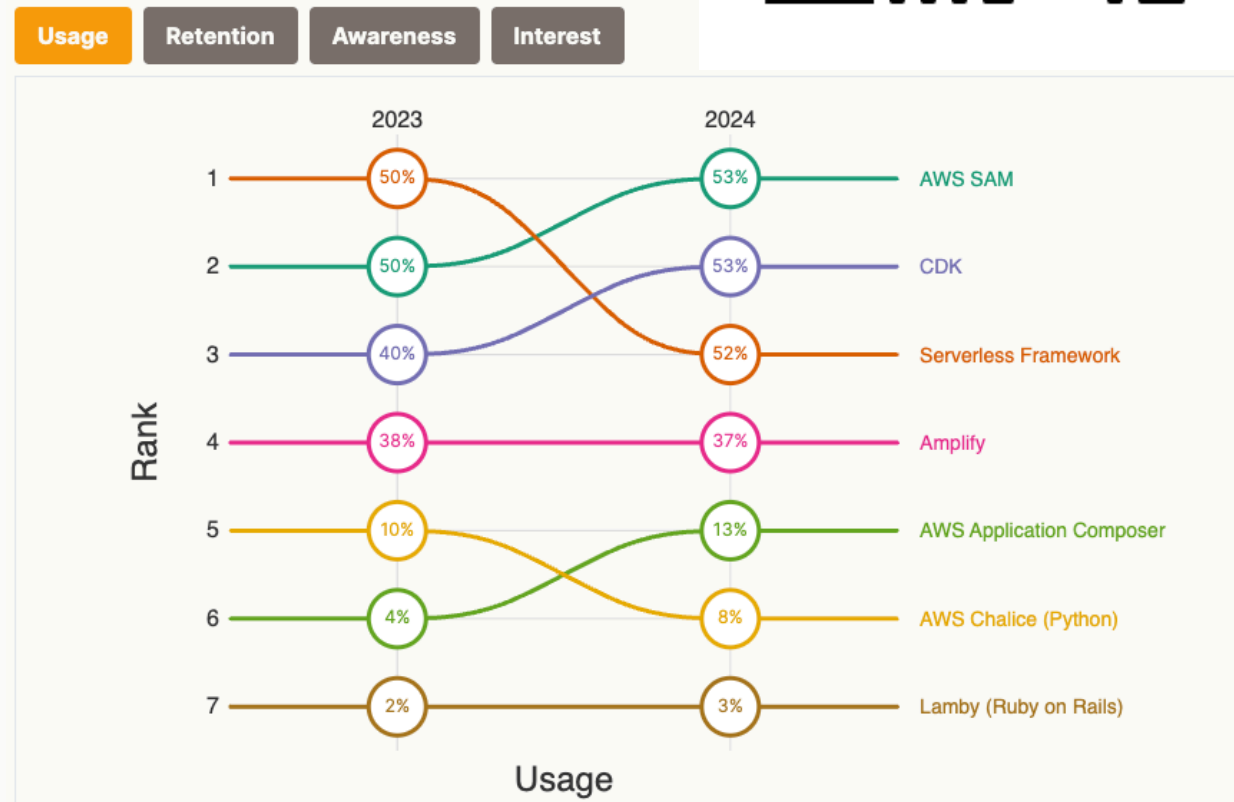
## Infrastructure as Code

Ranking of Infrastructure as Code (IaC) tools and services used to manage AWS resources.



## Serverless

Trend over the years



# Resources

Workshop: AWS Control Tower immersion/Activation Day

- <https://controltower.aws-management.tools/immersionday/>

## Videos

- AWS Control Tower
  - 19 videos
  - <https://youtube.com/playlist?list=PLhr1KZpdzukdS9skEXbY0z67F-wrcpbjm>
- AWS Management and Governance
  - 170+ videos
  - [https://www.youtube.com/playlist?list=PLhr1KZpdzukcaA06WlloeNmGlnM\\_f1LrdP](https://www.youtube.com/playlist?list=PLhr1KZpdzukcaA06WlloeNmGlnM_f1LrdP)

## Blog posts

- <https://aws.amazon.com/blogs/mt/category/management-tools/aws-control-tower/>

