aws

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


One Giant AWS Account
IAM Users from
5 years ago
Build Pipeline
Repositories
Shared Buckets
Staging Web Apps
Dev Web Apps
Production Web Apps
Latest Backup is
183 days old
Domains
Staging Data Stores
Dev Data Stores
Staging Buckets
No one know what this is
Don't touch it
Production Data Stores
Dev Buckets
Production Buckets

Vision

SSO

Audit

Archives & Backups

Shared Internal Resources

Build Pipeline

Repositories

Shared Buckets

Domains

Production

Web Apps

Data Stores

Production Buckets

Staging

Web Apps

Data Stores

Staging Buckets

Development

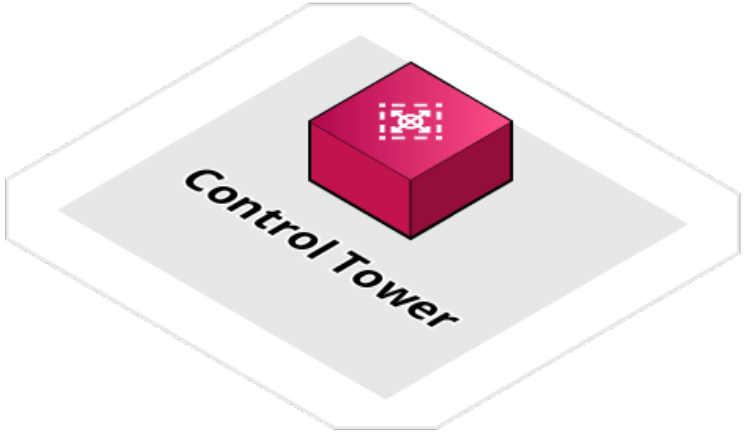
Web Apps

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

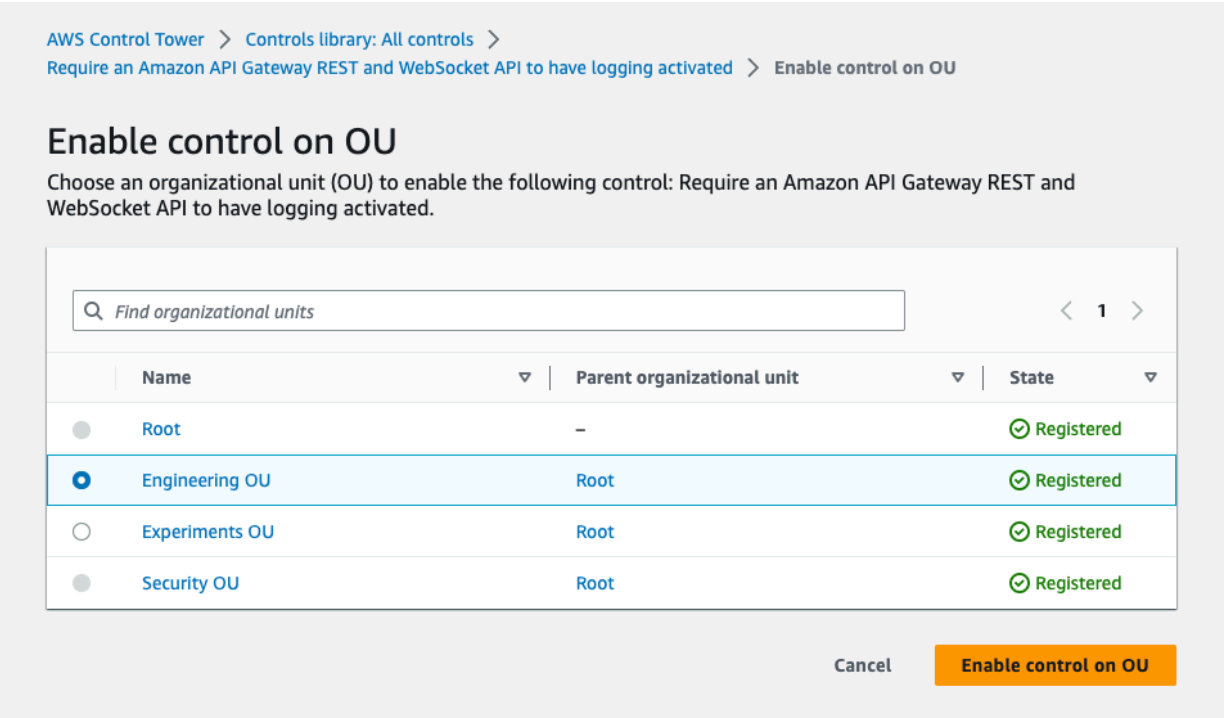
This is what we did... find what works for **you**!

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



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

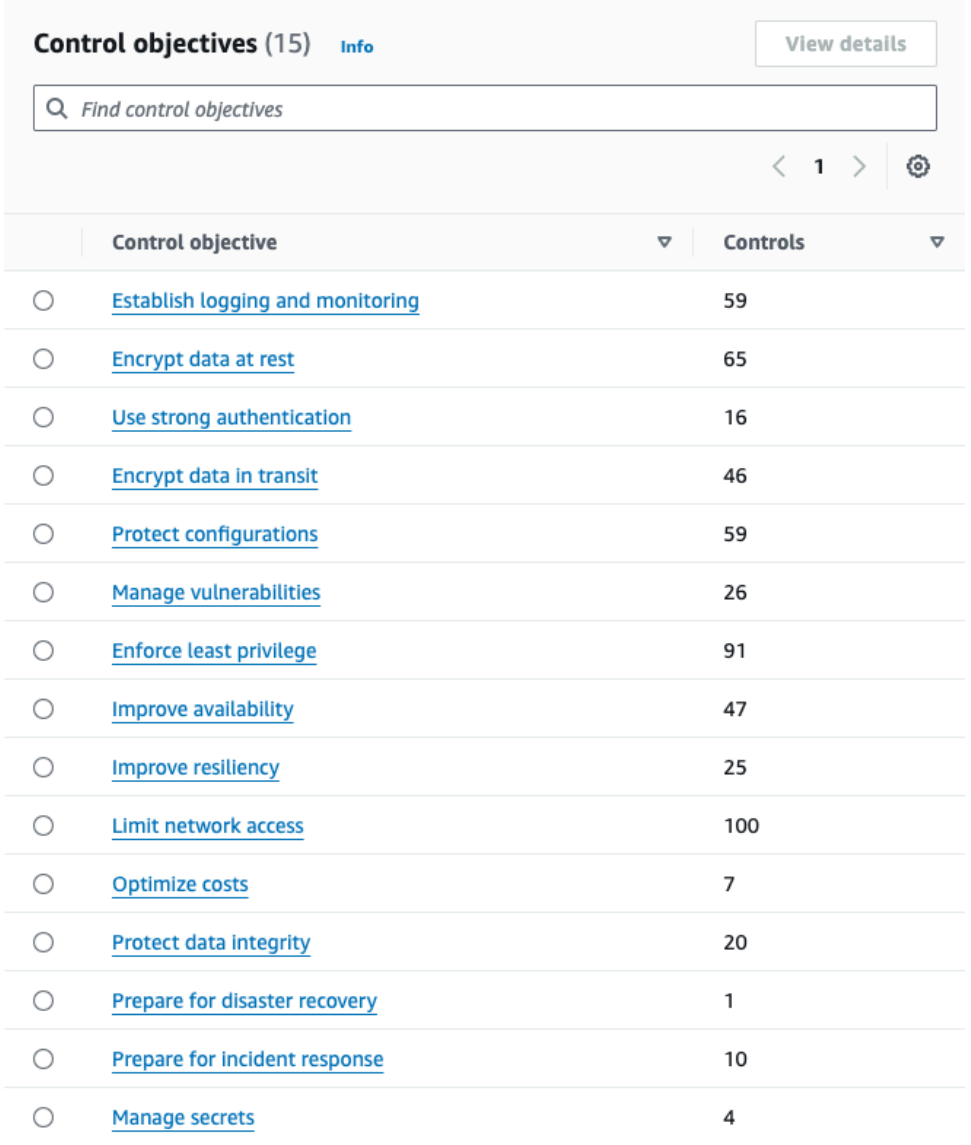
- Get team comfortable with SSO and role selection
  - Increase the ***maximum session duration*** in Identity Center to prevent frustration
- Use SSO for CLI

```
aws sso login --profile prod
```

- Renew **RIs** 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

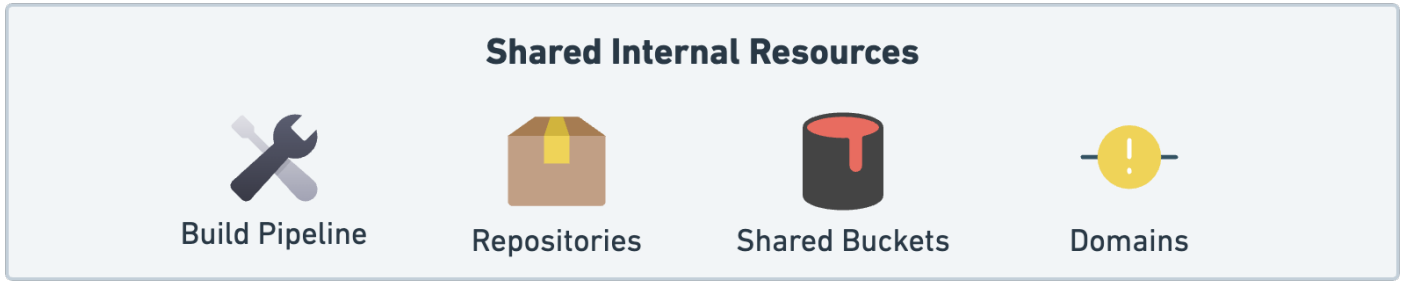
Guardrails

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



Don't boil the ocean

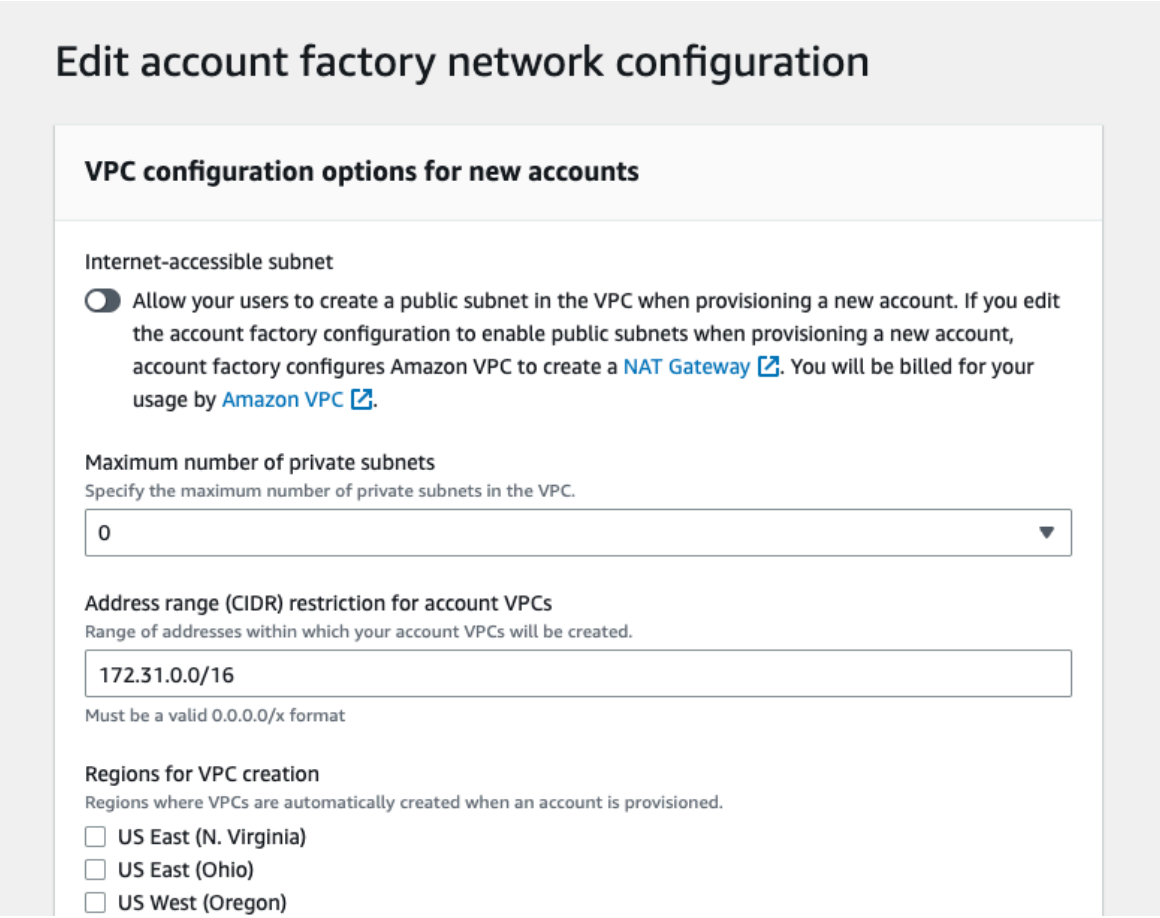
- Use Account Factory to create new ***Shared Internal Account***



- 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



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

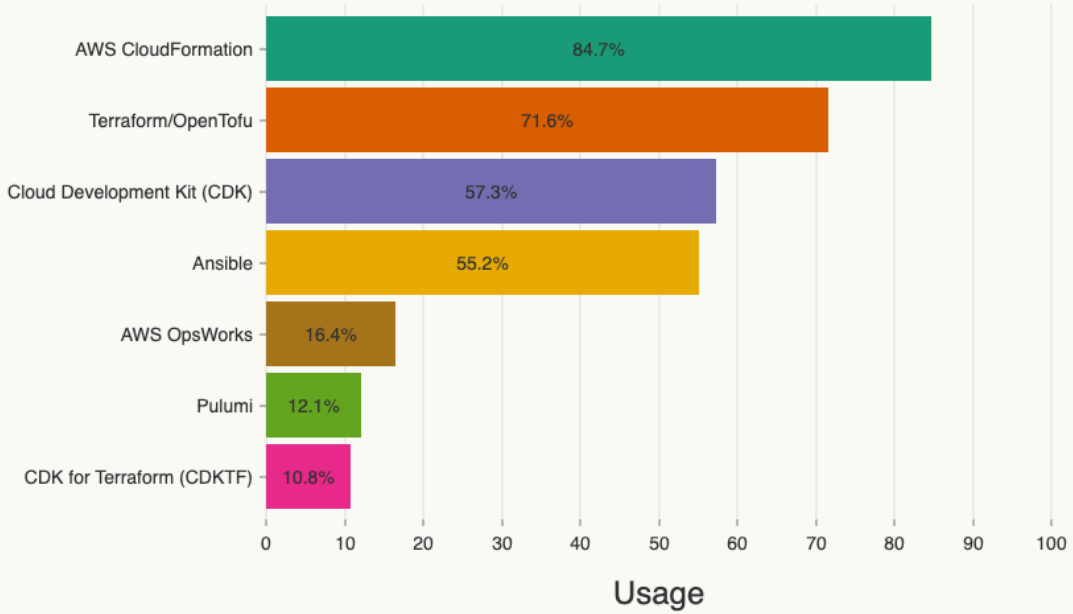
https://answersforaws.com/slides

answersforaws.com

Infrastructure as Code

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

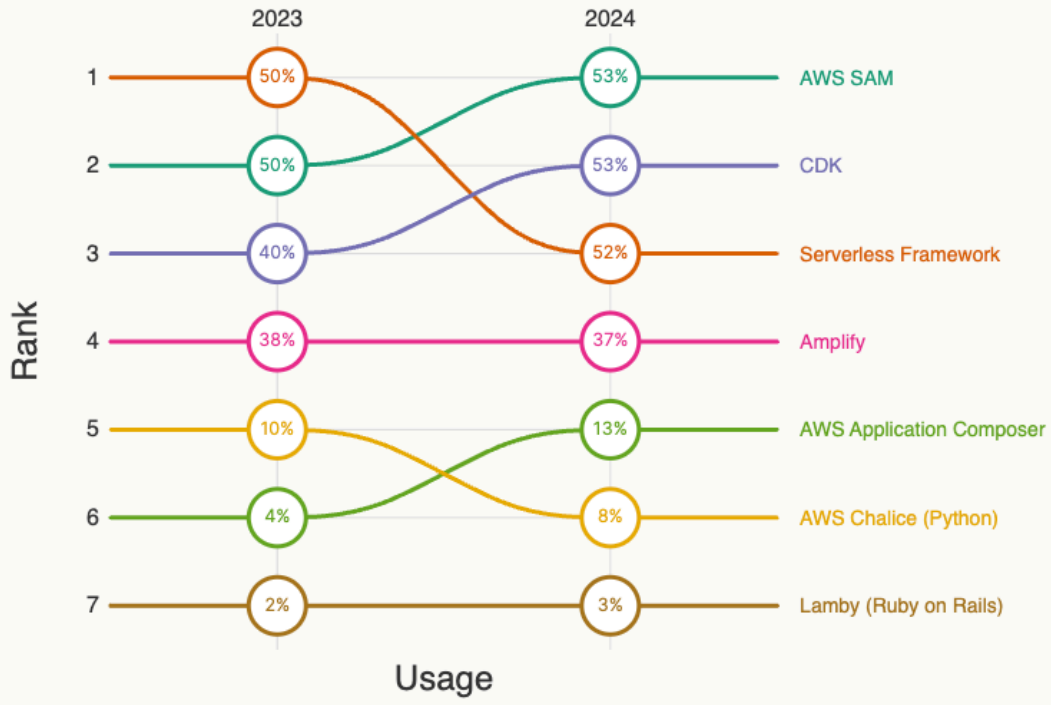
Usage | Retention | Awareness | Interest | Rank | Alphabetical



Serverless

Trend over the years

Usage | Retention | Awareness | Interest



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=PLhr1KZpdzukcaA06WloeNmGlnM_f1LrdP

Blog posts

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