VANDERBILT UNIVERSITY

Migrating to Control Tower and Terraform

Heather Mitchell and Allen Karns
Vanderbilt University

Existing Environment

- Organic growth since 2016
- Consolidated into one Org with 120+ accounts
- CloudFormation well established
- Services already used: Config, GuardDuty, SSO, centralized logging

Network Redesign – Optional but Fun!

- Best practices recommend a clean management account
  - Logging already separate
  - Networking still in management account
- How clean can we get without an outage?
  - Student apps rely on Direct Connects = ☹
  - Redundant VPCs to Transit Gateways = ☺
- Future benefits
  - Delegation
  - Better security boundaries

Replacing existing CloudTrail and Config

- Existing logging account but new buckets
- Dual Config Recorders until all accounts are migrated
- Read ALL the documentation -- CloudTrail x 2 isn’t free!
- Don’t forget about dependent services
  - Impact on log flow to SIEM

Switching to Terraform

- Never a good time, but no time like the present
  - Rebuilt team = less to unlearn
  - Existing IaC entropy
  - Existing centralization of logging and security lessens pressure
  - Provider-agnostic IaC = doing more with less
- Lessons learned so far
  - Terraform removes what isn’t in state
  - Enforcing repo-driven deployment is key
  - Resources come to CloudFormation first

Next Steps

- Standard Terraform templates
  - Built as part of account migrations
- GitHub-based pipelines for deployment
- Account Factory for Terraform
  - Customization to support Direct Connect VPC option