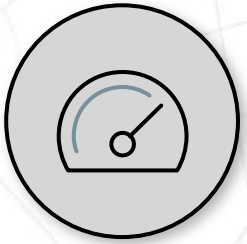
AWS Control Tower to Govern Multi-Account AWS Environments at Scale

Bill Thompson, Director, Digital Infrastructure, Lafayette College
Fernando Ibanez, AWS Solutions Architect EDU

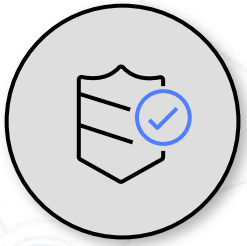
Balancing the needs of builders and central cloud IT

Builders: Stay agile



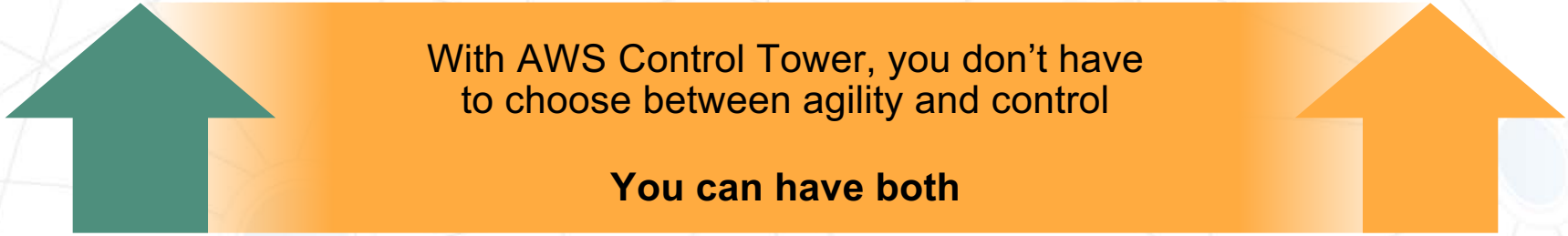
Innovate with the speed and agility of AWS

Cloud IT: Establish governance



Govern at scale with central controls

Business agility *and* governance control



Governance

Security

Compliance

Operations

Spend Management

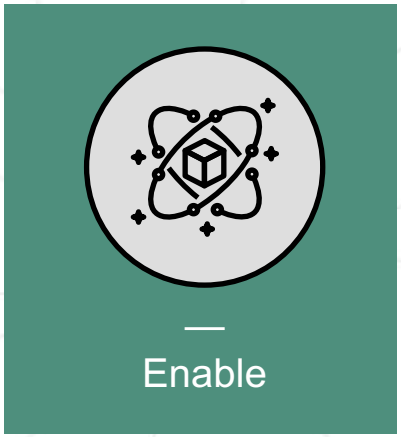
Agility

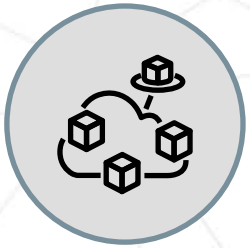
Self-service access

Experiment fast

Respond quickly
to change

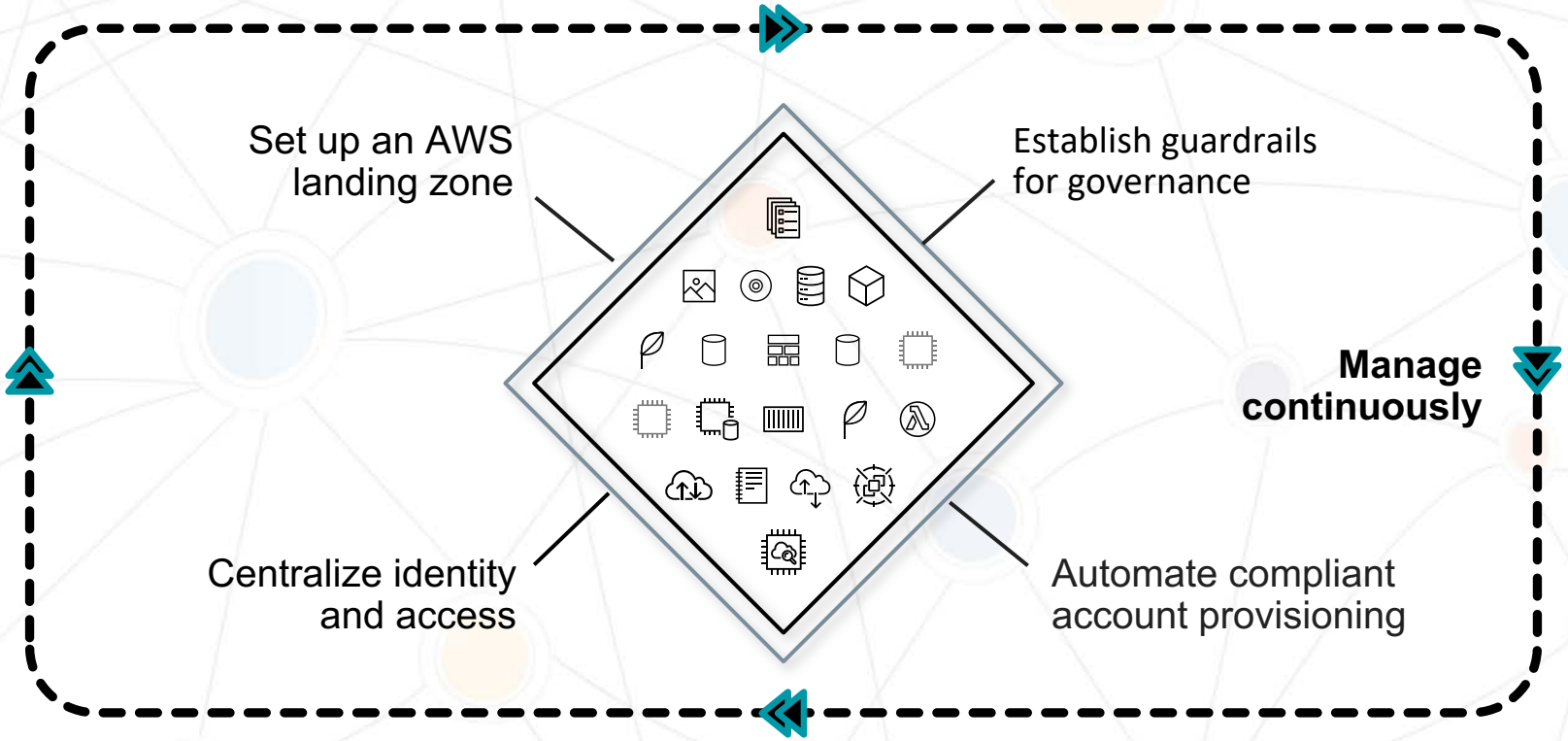
AWS Control Tower: Easiest way to set up and govern AWS at scale



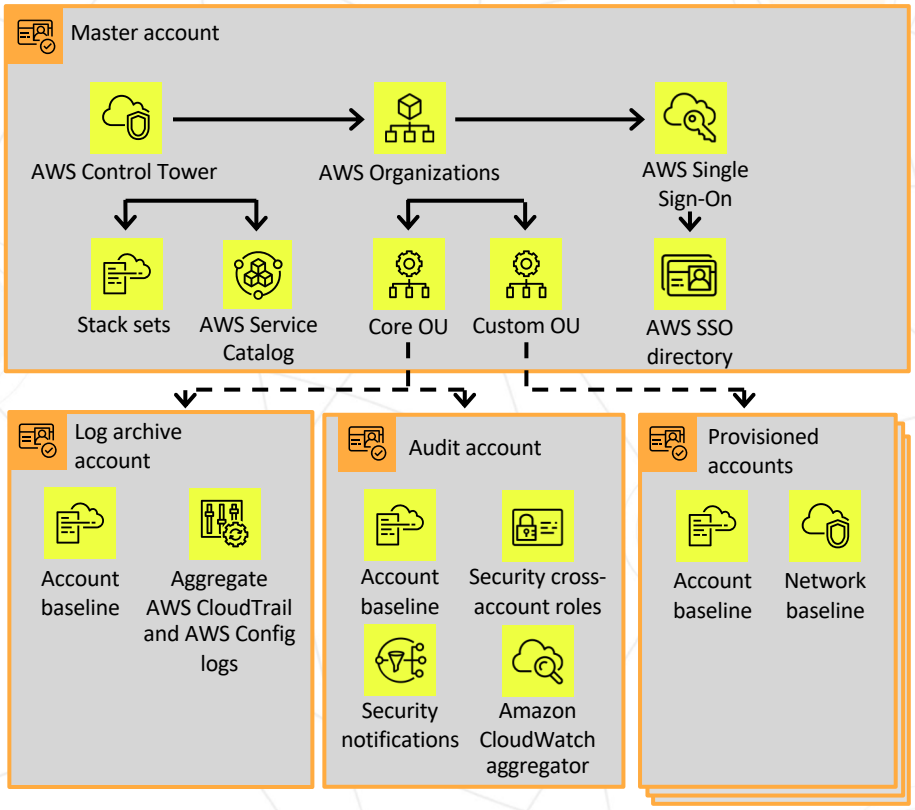


Business agility + governance control

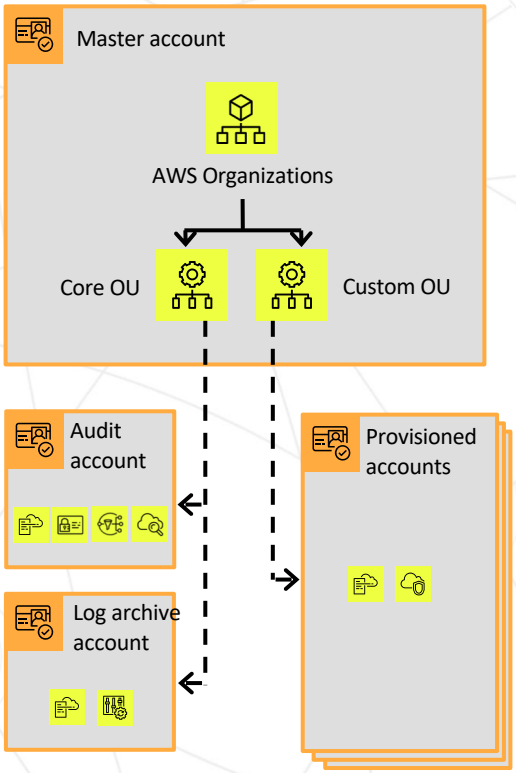
Enable governance



Set up an AWS landing zone



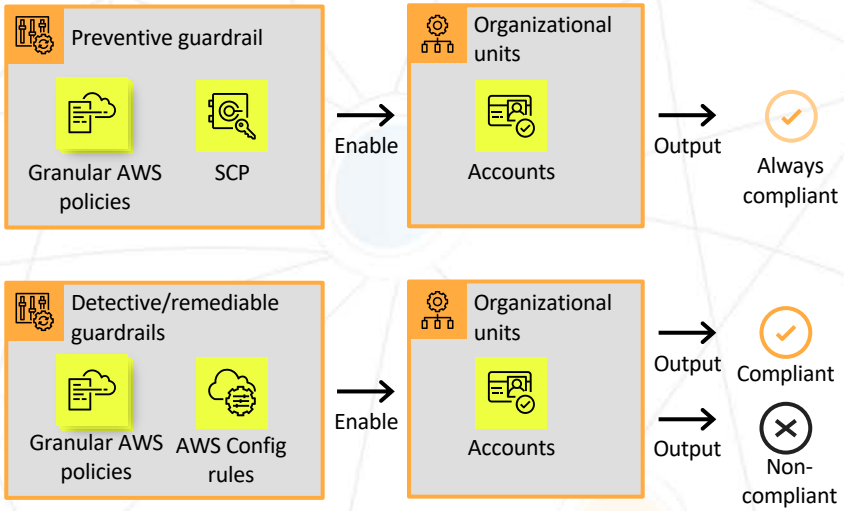
Multi-account architecture



Centralize identity and access

- AWS SSO provides default directory for identity
- AWS SSO also enables federated access management across all accounts in your organization
- Preconfigured groups (e.g., AWS Control Tower administrators, auditors, AWS Service Catalog end users)
- Preconfigured permission sets (e.g., admin, read-only, write)
- Option to integrate with your managed or on-premises Active Directory (AD) and SAML

Establish guardrails

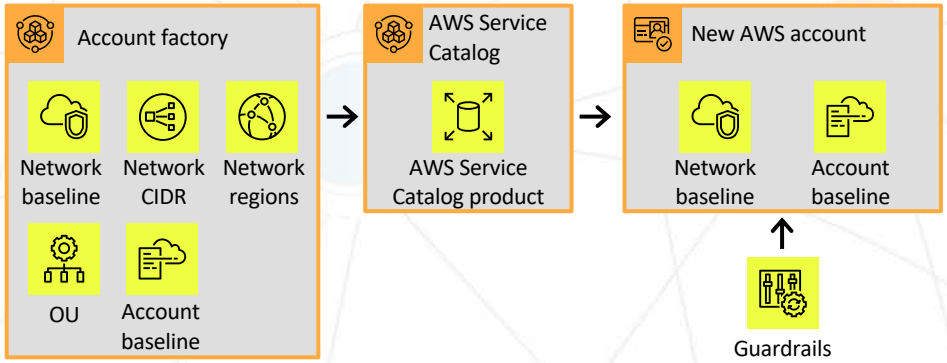


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: detect policy violations and alert in the dashboard; implemented using AWS Config rules
- Mandatory and strongly recommended guardrails for prescriptive guidance
- Easy selection and enablement on organizational units

Guardrail examples

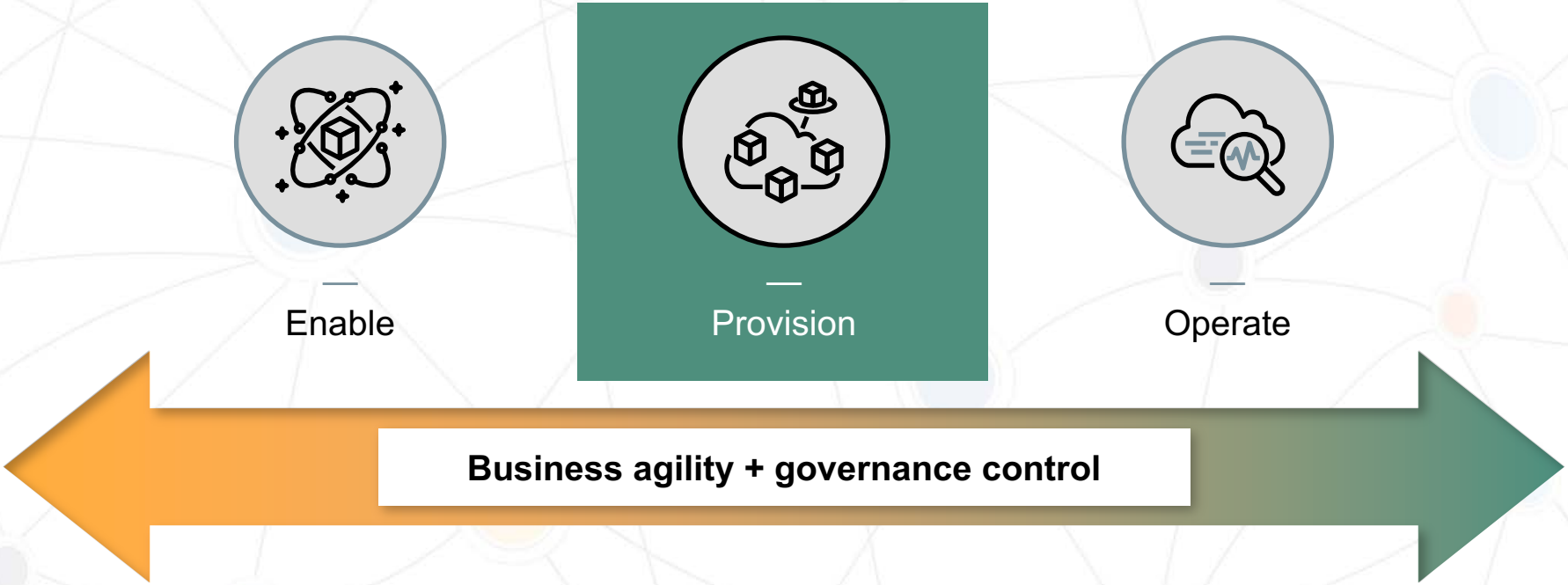
Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with Amazon CloudWatch
Encryption	Ensure encryption of Amazon EBS volumes attached to Amazon EC2 instances
Drift	Disallow changes to AWS Config rules set up by AWS Control Tower

Automate compliant account provisioning

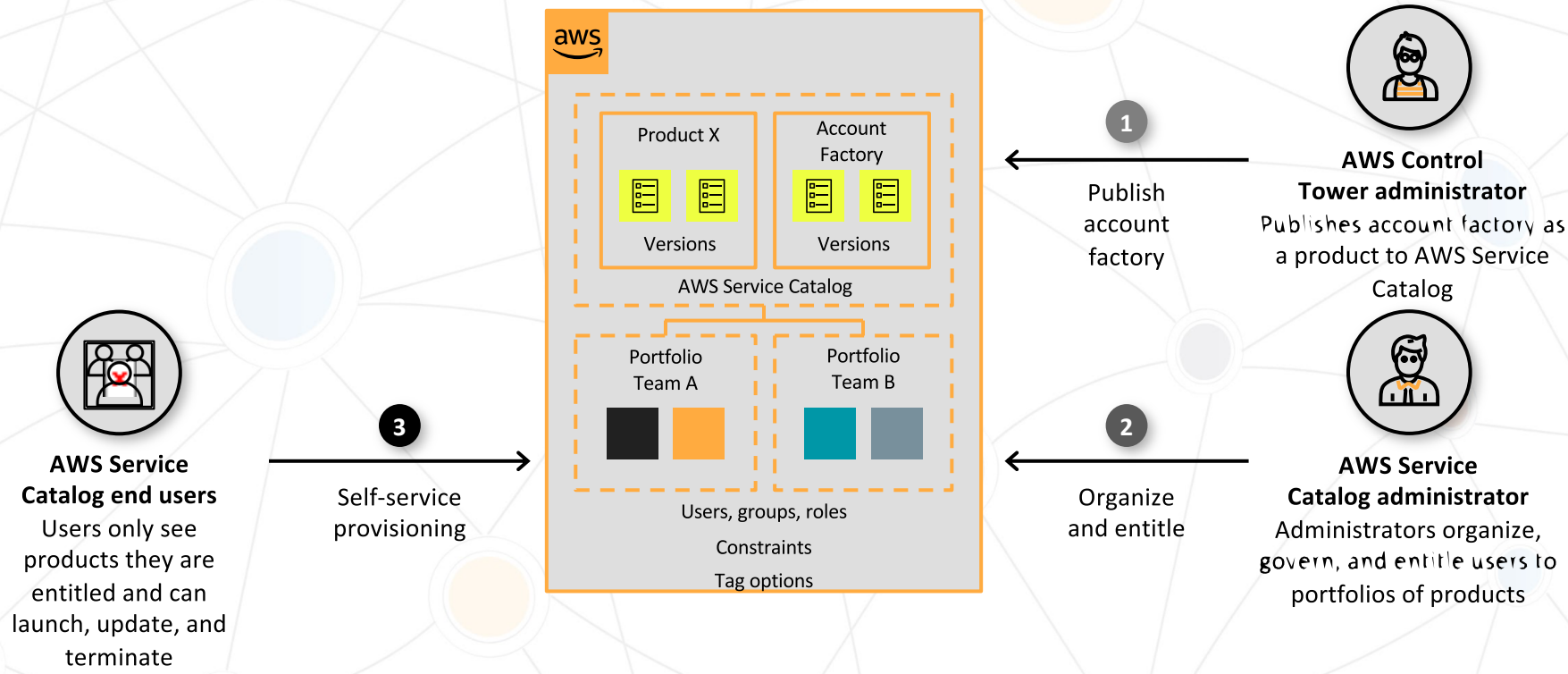


- Built-in account factory provides a template to standardize account provisioning
- Configurable network settings (e.g., subnets, IP addresses)
- Automatic enforcement of account baselines and guardrails
- Published to AWS Service Catalog

AWS Control Tower: Easiest way to set up and govern at scale

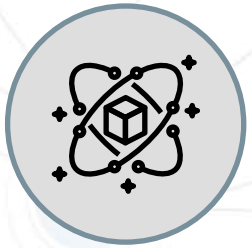


Self-service account provisioning in AWS Service Catalog

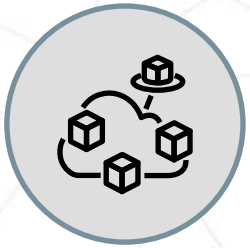


Users can configure and provision AWS accounts and resources without needing full privileges to AWS services (e.g., Amazon EC2, Amazon RDS)

AWS Control Tower: Easiest way to set up and govern at scale



Enable



Provision

Operate

Business agility + governance control

Operate with agility + control

Monitor

Monitor resources and workloads

Act

Take operational action on resources

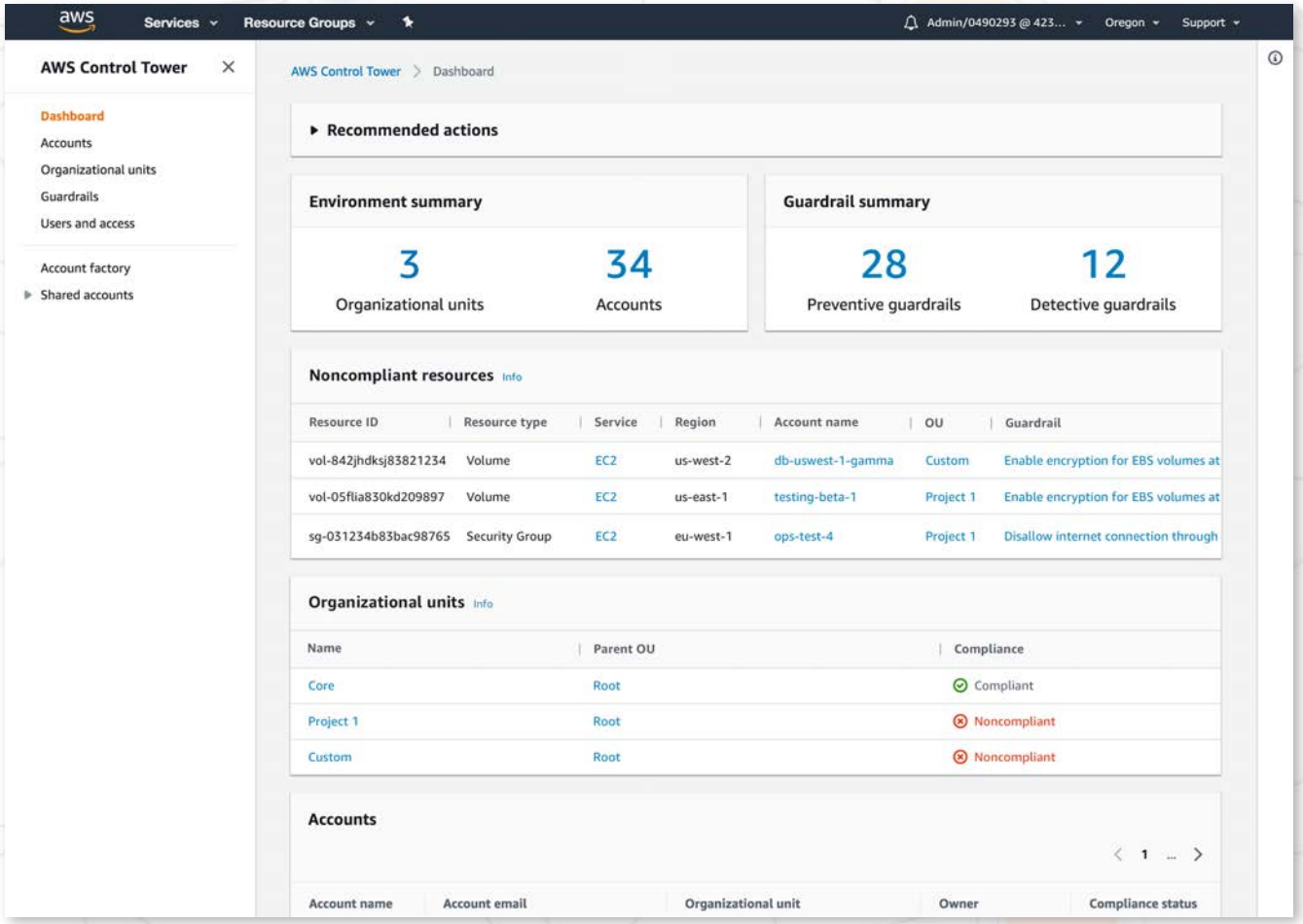
Audit

Audit resource configurations, user access, and policy enforcement

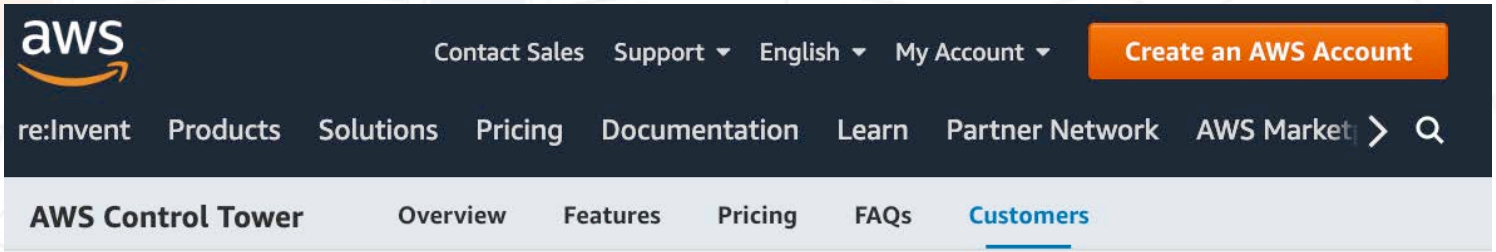
Dashboard

Continuous visibility into your multi-account environment

Dashboard for oversight



AWS Control Tower Adoption at Lafayette



LAFAYETTE COLLEGE

Lafayette College

Lafayette College is a liberal arts college based in Easton, Pennsylvania that offers bachelor of arts degrees in 37 fields and a bachelor of science in 14, including 4 in engineering. The organization uses AWS services to provide a cloud environment for over 2,600 students and 215 full-time faculty across the campus. With AWS Control Tower, the Lafayette Infrastructure team can expedite this transition to the cloud and ensure consistent provisioning of AWS accounts.

> "We selected Control Tower to accelerate our cloud adoption process while simultaneously implementing best practices for operations, management, and security. With Control Tower, we can set up guardrails that enforce governance policies for every AWS account that is created in our environment. And through the Account Factory feature in Control Tower, teams can quickly provision new accounts and start building."

Bill Thompson, Director of Digital Infrastructure - Lafayette College

Lafayette AWS Adoption Working Group

- Prudent and responsible operations and management
- Enable service teams to move quickly and securely
- Address common deployment needs
- Who is going to do and be responsible for what?
- Skills and roles transitions

- Waiting for Control Tower release…in the meantime:
  - Established initial sandbox account for exploration and training
  - A Cloud Guru classes
  - AWS Solutions Architect associates certifications

But first, we need to get some AWS friends...

EDUCAUSE

Jobs .EDU Domain

Topics Insights Conferences & Learning Community Who We Are

Home › Community Groups › Cloud Computing Community Group

Cloud Computing Community Group

The Cloud Computing Community Group provides participants with the opportunity to learn about and discuss the challenges and opportunities associated with the adoption of cloud computing in colleges and universities. Examples of discussion topics include cloud contract

UNICON

aws partner network

Advanced Consulting Partner

Public Sector Partner

Education Competency

aws partner network | immersion days

EdgeCon ANNUAL CONFERENCE 2020

Initial AWS projects

- Let’s get started…learn as we go
  - New technology
  - New roles and responsibilities
  - New organizing principles
  - Hash out strategy, issues, operations

- AWS Control Tower
- Low risk static web hosting – S3, Route53
- Data archive – Snowball and Glacier
- File services - AWS Storage Gateway
- Common Networking Services

Lafayette Cloud Custodians

- Take care of the college and take care of each other
  - Prudent and responsible management
  - Budget and billing
  - Security and baseline config
  - Change in job responsibilities - systems team
  - New hire! Sysadmin / Cloud engineer
  - Back and forth discussion between builders and custodians
  - Framework for rules of engagement

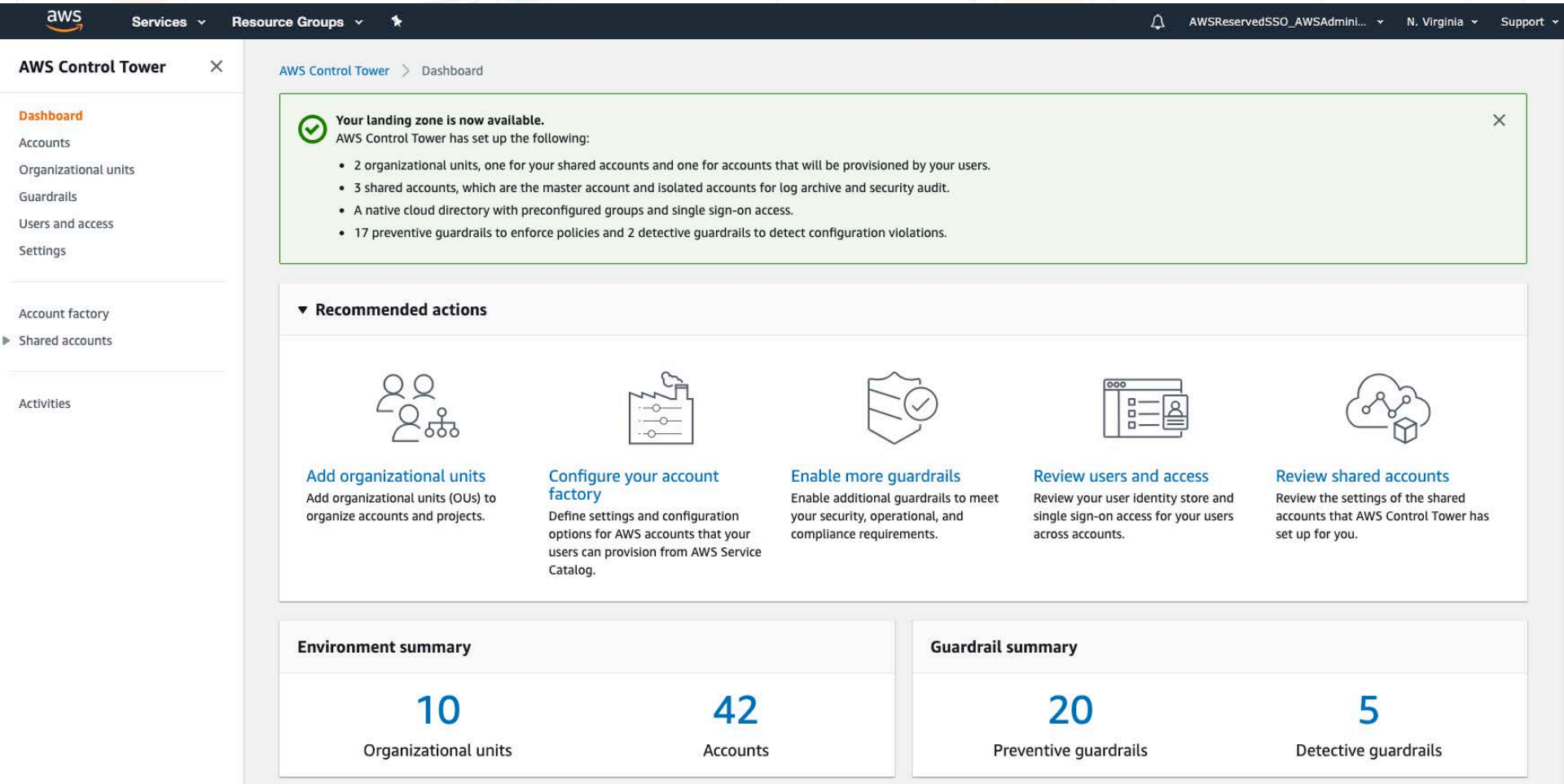
The Hitchhiker's Guide to Responsible AWS Management

At Lafayette College

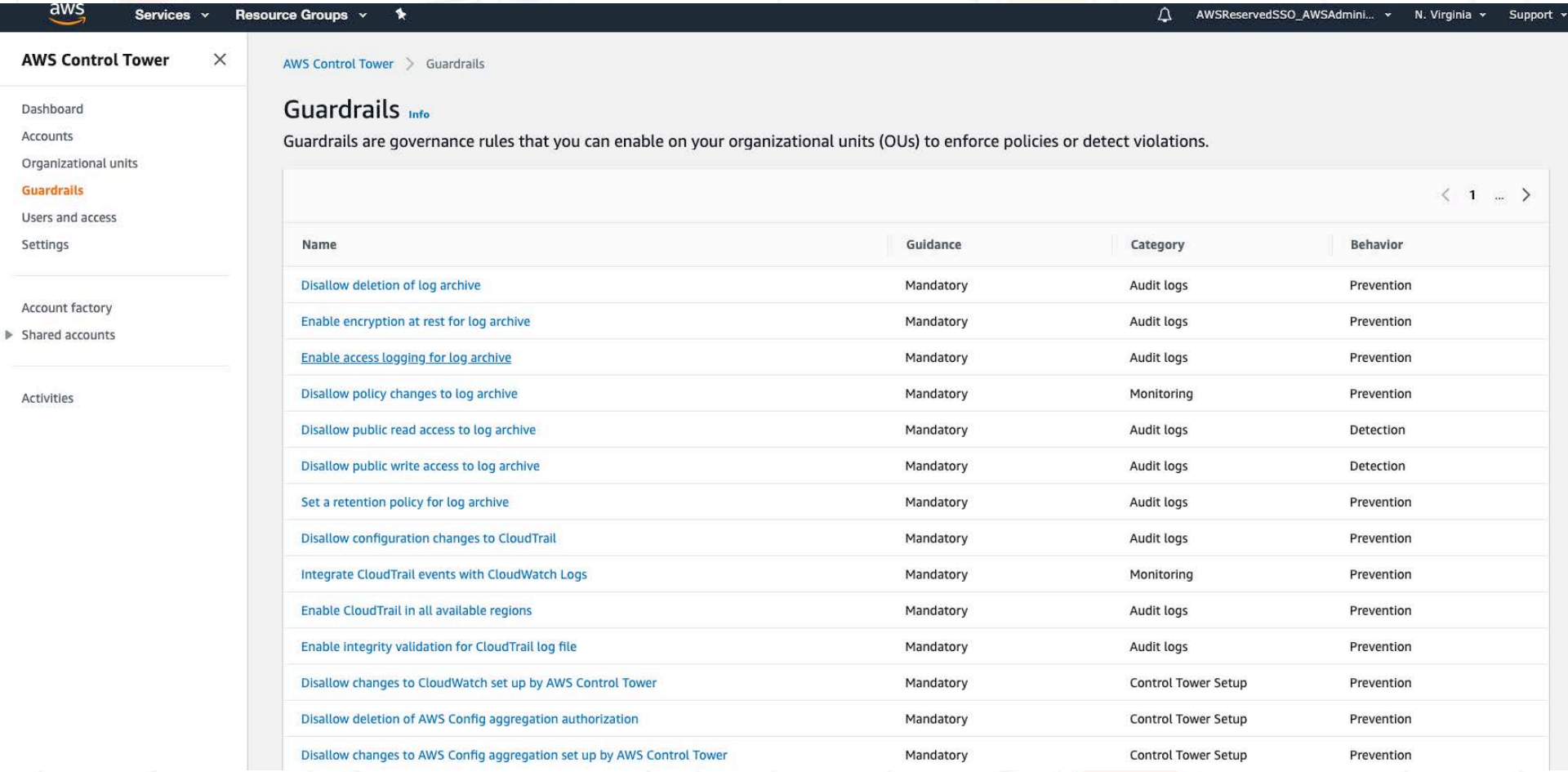
Abstract

All your workloads are moving to the cloud! But there is still stuff on premise. Now everyone is spinning up their own infrastructure and it is going to be a mess! **DON'T PANIC!!!** This guide aims to establish some minimum rules of engagement for responsible AWS management. From a reasonable but workable permission strategy to a **shared responsibility and governance model**, this guide will try to walk you through the key things you need to do to be perceived as a trustworthy, responsible custodian of IT resources, even if you are basically irreverent and lazy at heart.

AWS Control Tower Dashboard

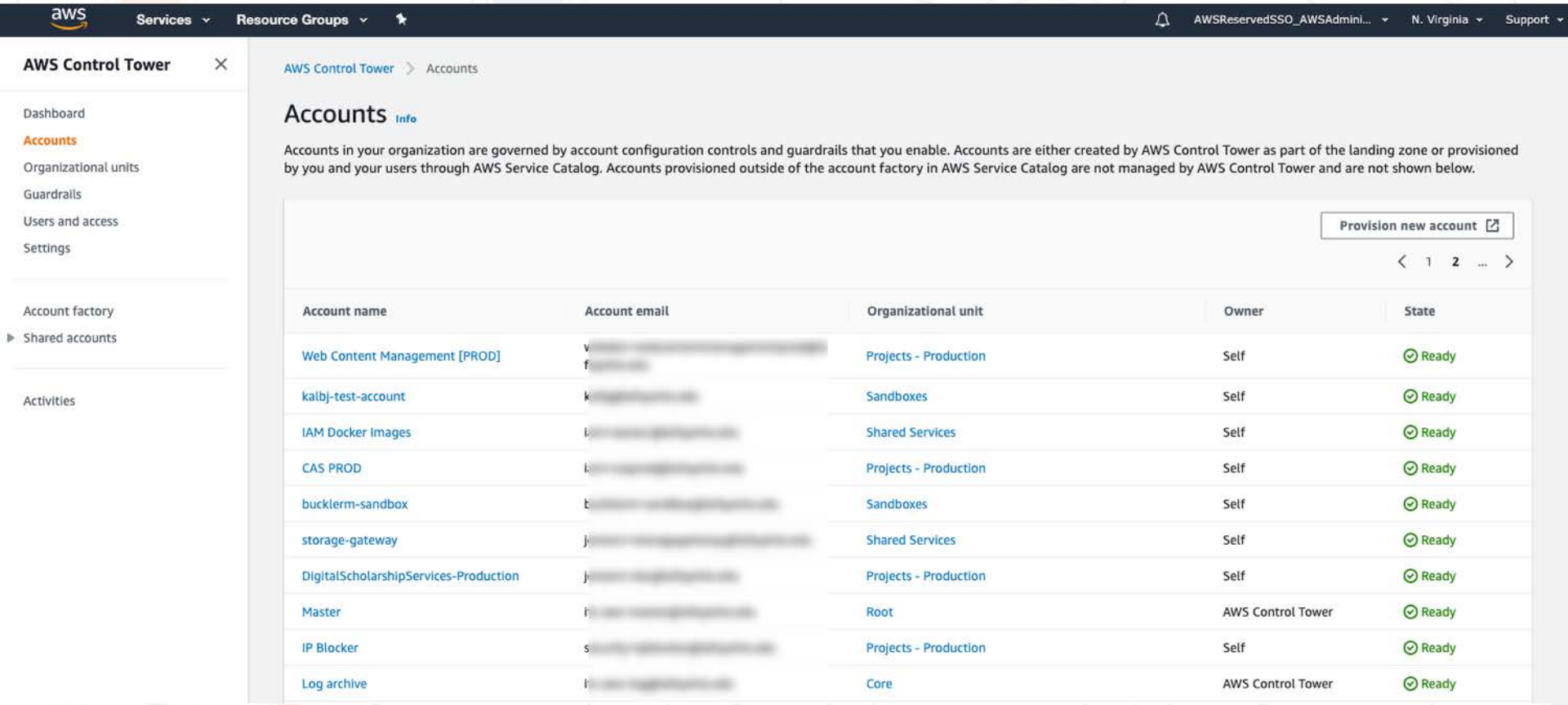


Automatic Guardrails

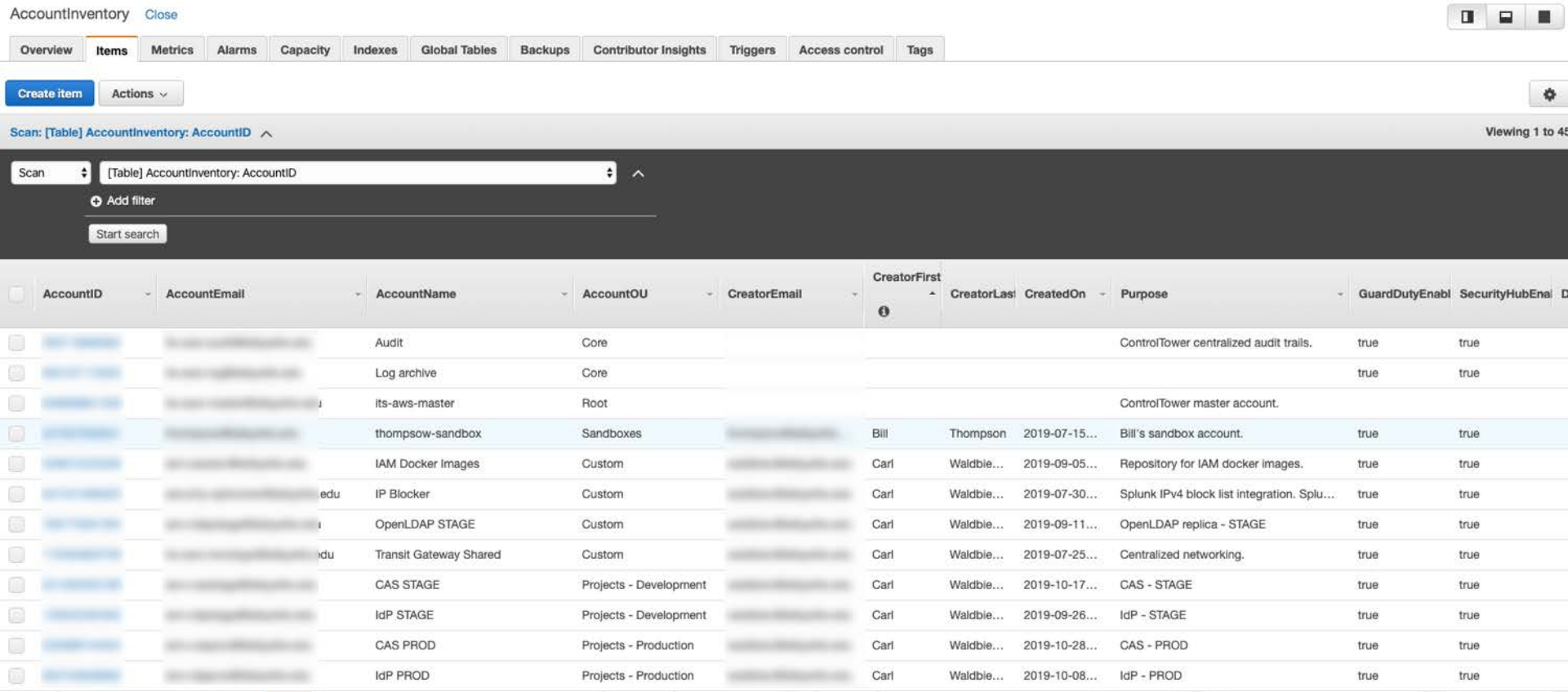


Name	Guidance	Category	Behavior
Disallow deletion of log archive	Mandatory	Audit logs	Prevention
Enable encryption at rest for log archive	Mandatory	Audit logs	Prevention
Enable access logging for log archive	Mandatory	Audit logs	Prevention
Disallow policy changes to log archive	Mandatory	Monitoring	Prevention
Disallow public read access to log archive	Mandatory	Audit logs	Detection
Disallow public write access to log archive	Mandatory	Audit logs	Detection
Set a retention policy for log archive	Mandatory	Audit logs	Prevention
Disallow configuration changes to CloudTrail	Mandatory	Audit logs	Prevention
Integrate CloudTrail events with CloudWatch Logs	Mandatory	Monitoring	Prevention
Enable CloudTrail in all available regions	Mandatory	Audit logs	Prevention
Enable integrity validation for CloudTrail log file	Mandatory	Audit logs	Prevention
Disallow changes to CloudWatch set up by AWS Control Tower	Mandatory	Control Tower Setup	Prevention
Disallow deletion of AWS Config aggregation authorization	Mandatory	Control Tower Setup	Prevention
Disallow changes to AWS Config aggregation set up by AWS Control Tower	Mandatory	Control Tower Setup	Prevention

Control Tower Account Inventory

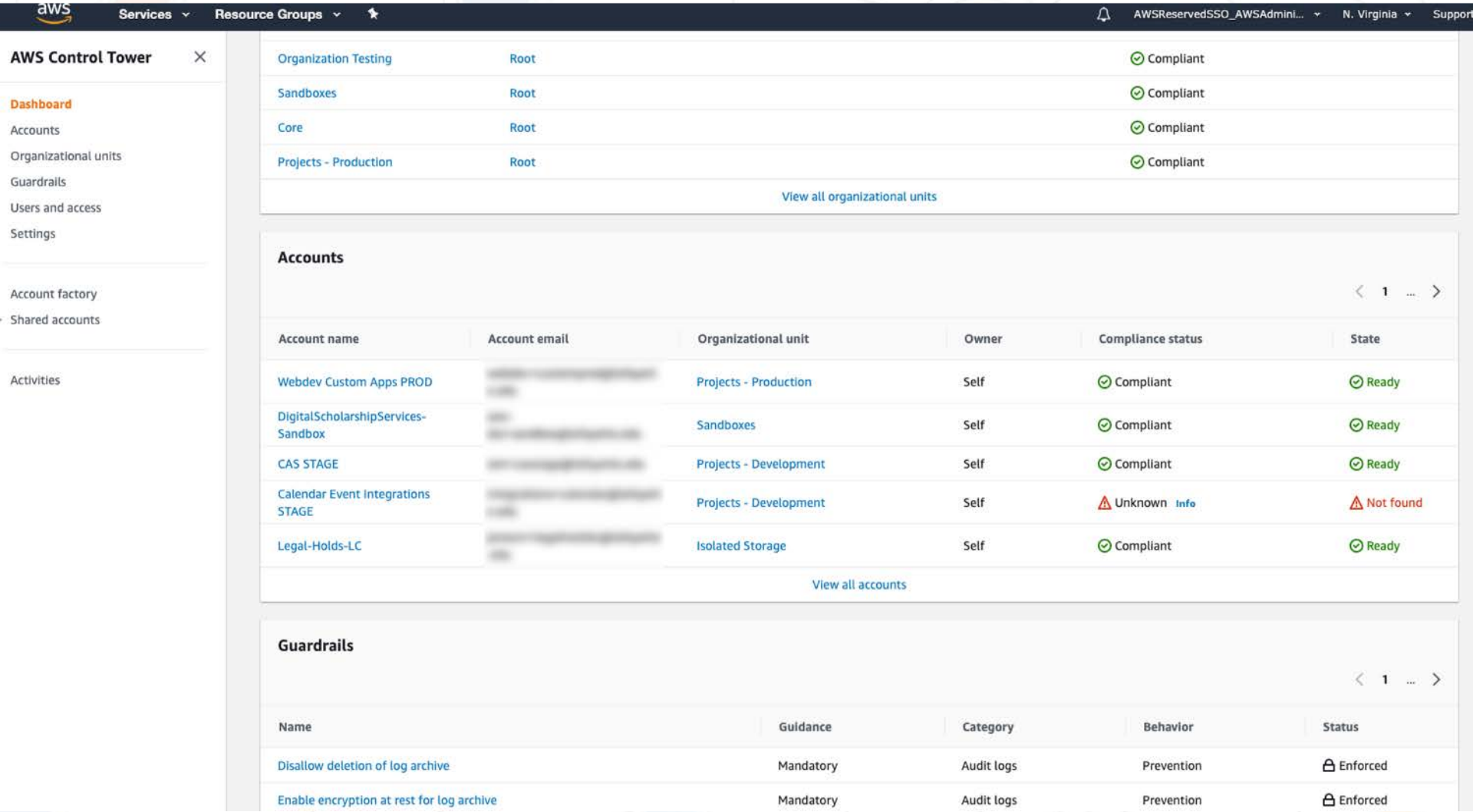


Lafayette DynamoDB Account Inventory

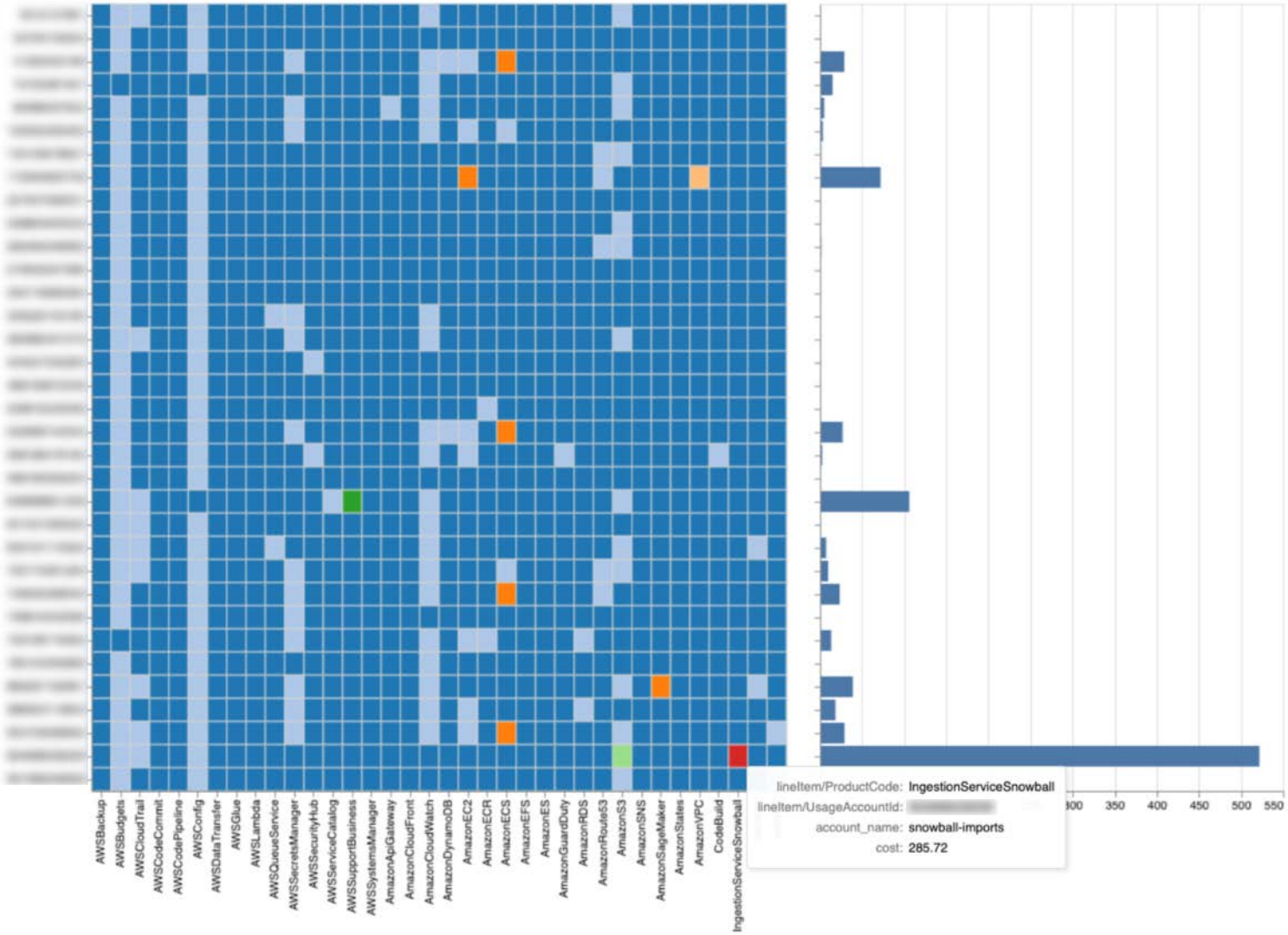


AccountID	AccountEmail	AccountName	AccountOU	CreatorEmail	CreatorFirst	CreatorLast	CreatedOn	Purpose	GuardDutyEnabl	SecurityHubEnal
[redacted]	[redacted]	Audit	Core					ControlTower centralized audit trails.	true	true
[redacted]	[redacted]	Log archive	Core						true	true
[redacted]	[redacted]	its-aws-master	Root					ControlTower master account.		
[redacted]	[redacted]	thompsow-sandbox	Sandboxes	[redacted]	Bill	Thompson	2019-07-15...	Bill's sandbox account.	true	true
[redacted]	[redacted]	IAM Docker Images	Custom	[redacted]	Carl	Waldbie...	2019-09-05...	Repository for IAM docker images.	true	true
[redacted]	[redacted]edu	IP Blocker	Custom	[redacted]	Carl	Waldbie...	2019-07-30...	Splunk IPv4 block list integration. Splu...	true	true
[redacted]	[redacted]	OpenLDAP STAGE	Custom	[redacted]	Carl	Waldbie...	2019-09-11...	OpenLDAP replica - STAGE	true	true
[redacted]	[redacted]du	Transit Gateway Shared	Custom	[redacted]	Carl	Waldbie...	2019-07-25...	Centralized networking.	true	true
[redacted]	[redacted]	CAS STAGE	Projects - Development	[redacted]	Carl	Waldbie...	2019-10-17...	CAS - STAGE	true	true
[redacted]	[redacted]	IdP STAGE	Projects - Development	[redacted]	Carl	Waldbie...	2019-09-26...	IdP - STAGE	true	true
[redacted]	[redacted]	CAS PROD	Projects - Production	[redacted]	Carl	Waldbie...	2019-10-28...	CAS - PROD	true	true
[redacted]	[redacted]	IdP PROD	Projects - Production	[redacted]	Carl	Waldbie...	2019-10-08...	IdP - PROD	true	true

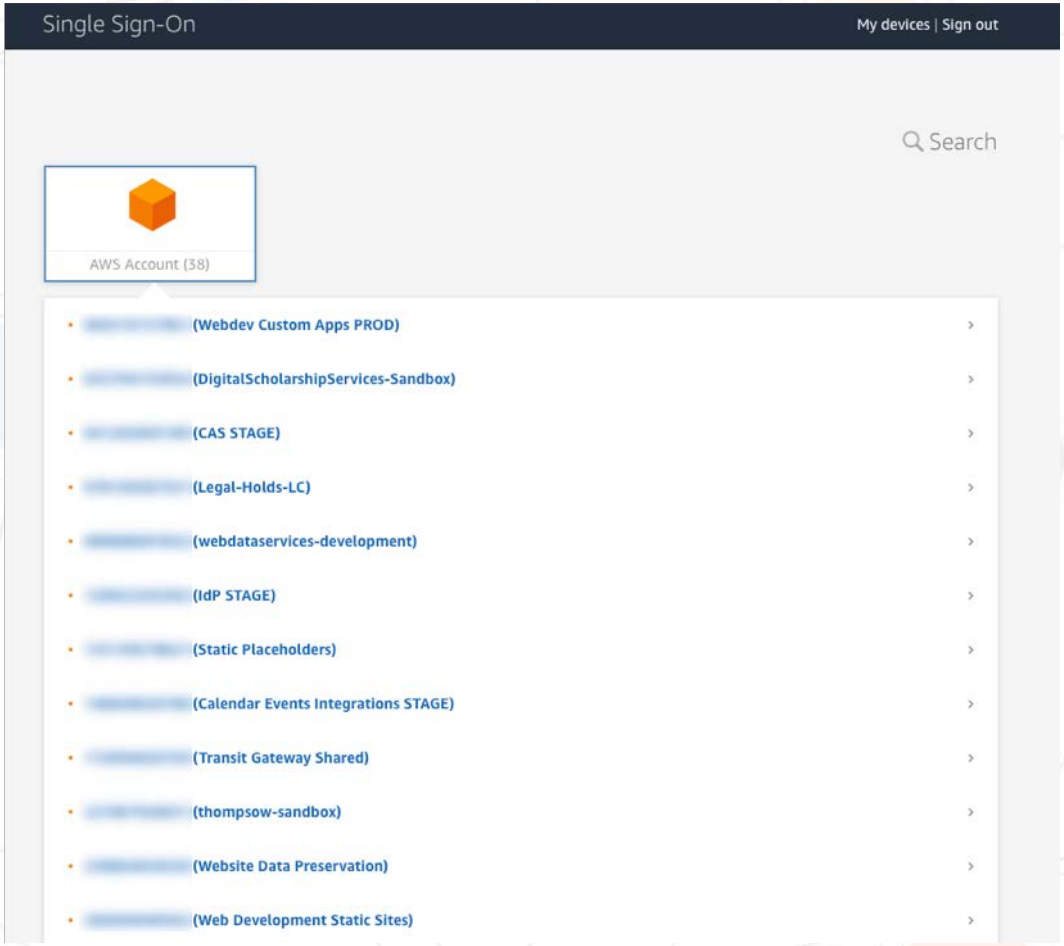
Compliance automation



Lafayette Billing Heatmap



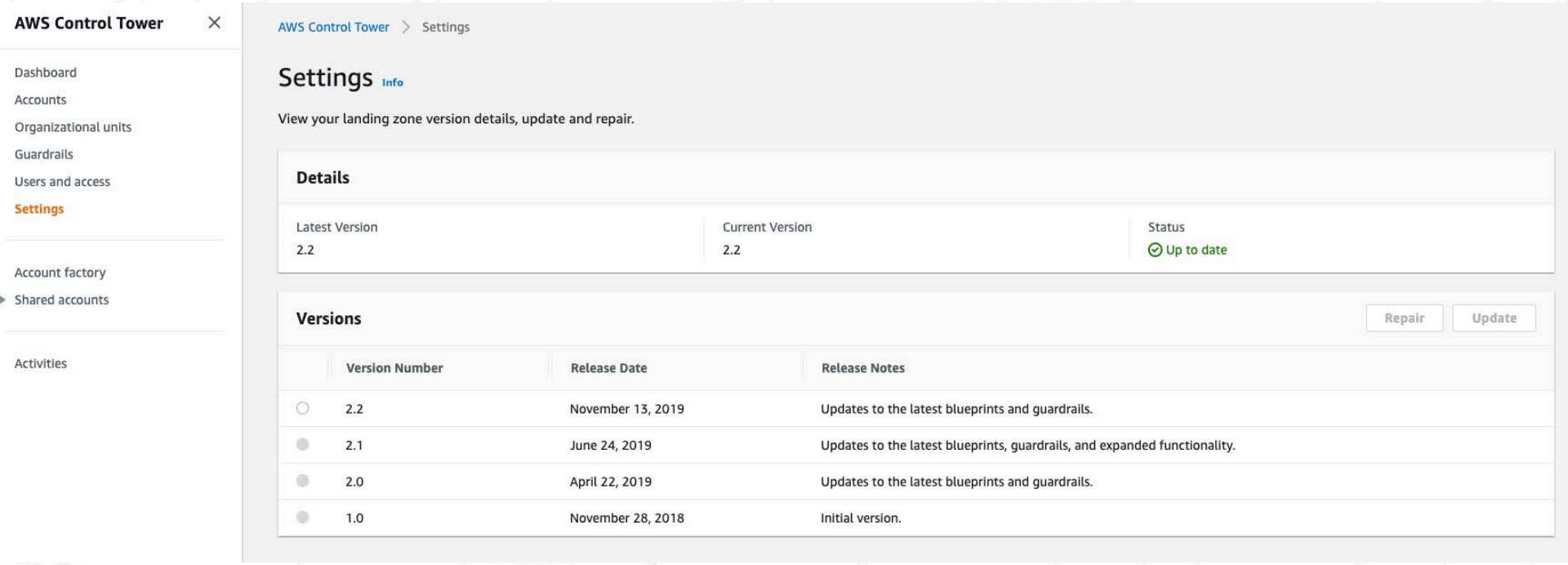
AWS SSO Portal



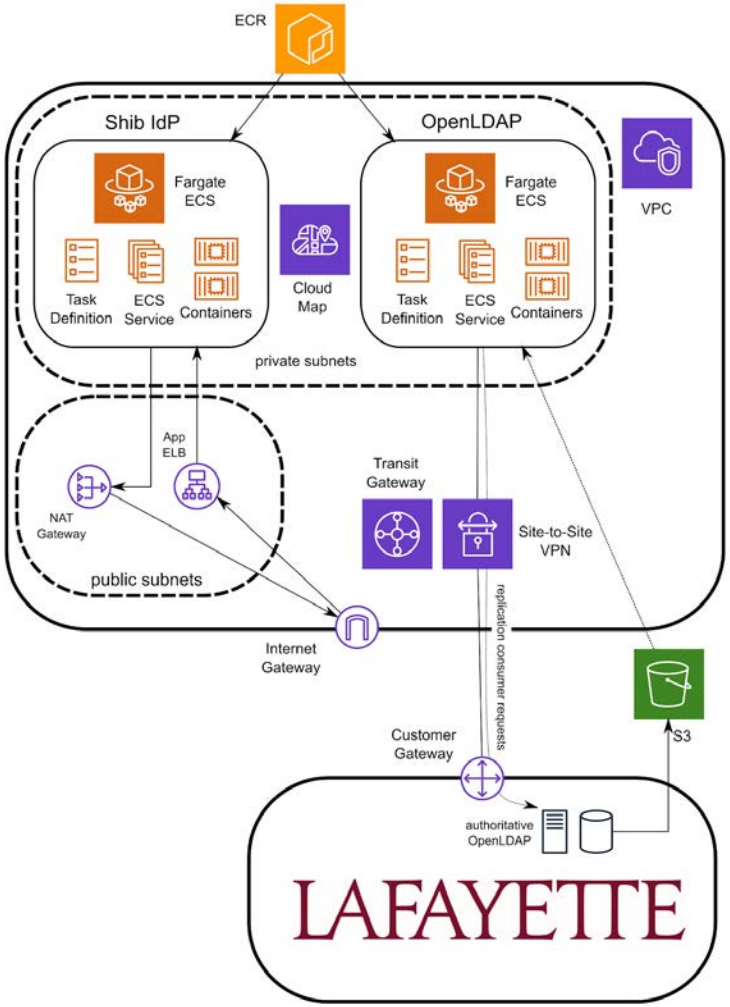
Not all smooth sailing…

- Control Tower still relatively new…although Landing Zone around for a while
- Quota Hard Limits
  - Initially only allowed 5 sub accounts, error messages not entirely clear
- Can get into trouble if you don't do it the Control Tower way
- Can't have nested Organizational Units – somewhat limiting to Service Control Policy management
- AWS SSO Portal MFA options limited

AWS Control Tower upgrades over time



Actually, things are looking up...



Pasta_Fazole 09:35

Actually, things are looking up:

```
[root@monongahela ~]# /home/jonesrn/snowball-client-linux-1.0.1-327/bin/snowball status

Snowball status: OK
Snowball appliance version: 1.0.1 build 2018-03-28.5774009395
Snowball client version: 1.0.1 Build 327
IP: 139.147.60.88
Used space      Free space      Total space
6299.03 GB      65620.94 GB     71919.97 GB

[root@monongahela ~]#
```