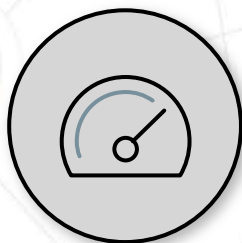


# **AWS Control Tower to Govern Multi-Account AWS Environments at Scale**

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



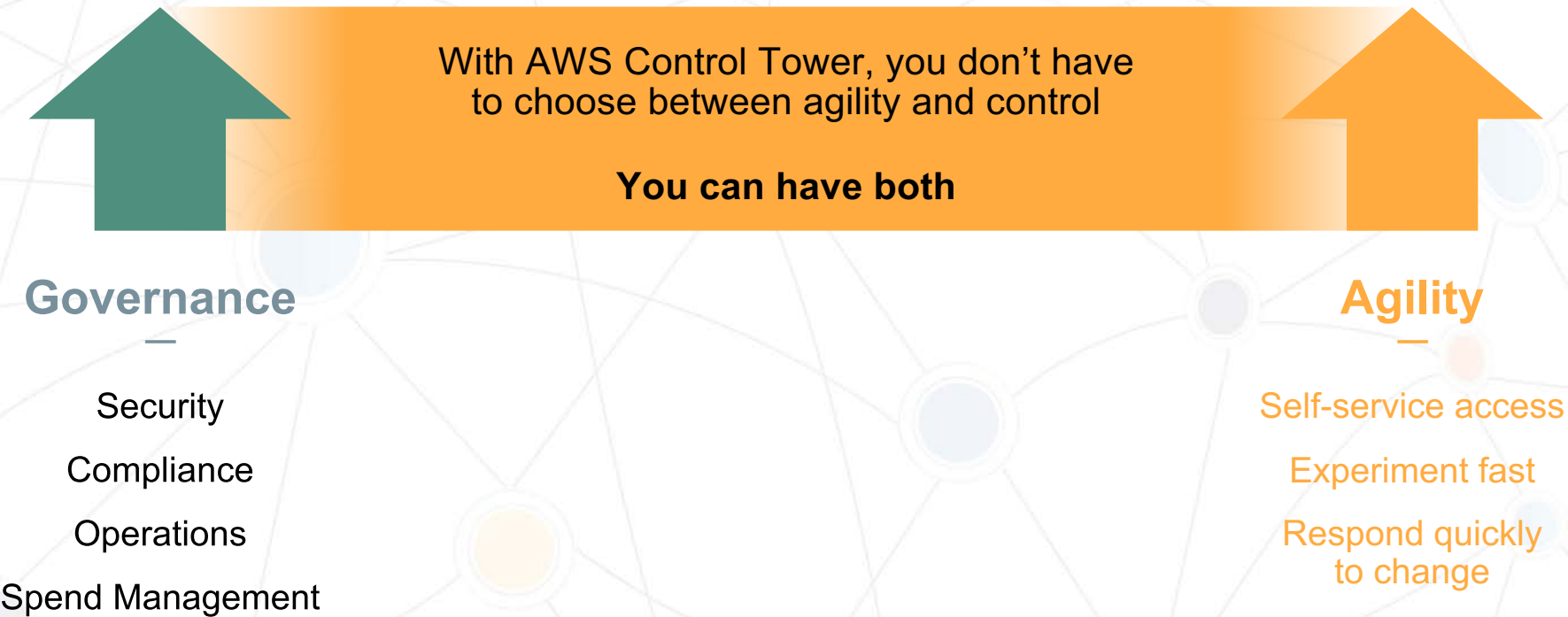
Innovate with the speed and  
agility of AWS

Cloud IT: Establish  
governance



Govern at scale with central  
controls

# Business agility *and* governance control



With AWS Control Tower, you don't have  
to choose between agility and control

**You can have both**

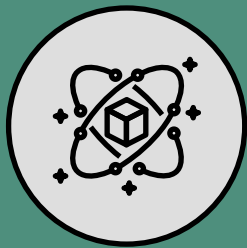
## Governance

- Security
- Compliance
- Operations
- Spend Management

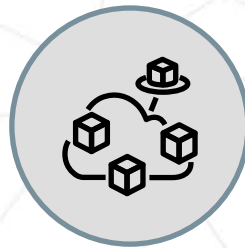
## Agility

- Self-service access
- Experiment fast
- Respond quickly  
to change

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



—  
Enable



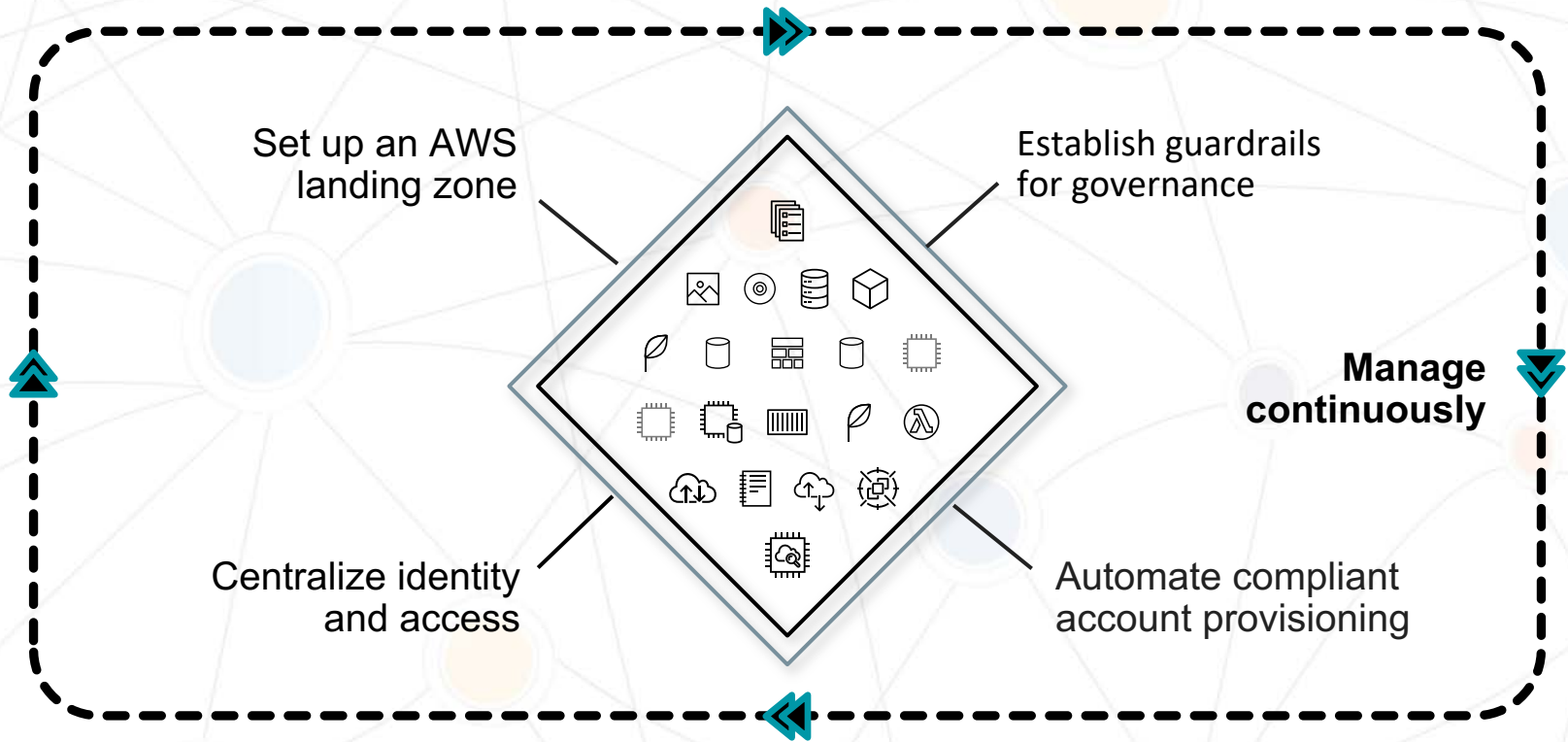
—  
Provision



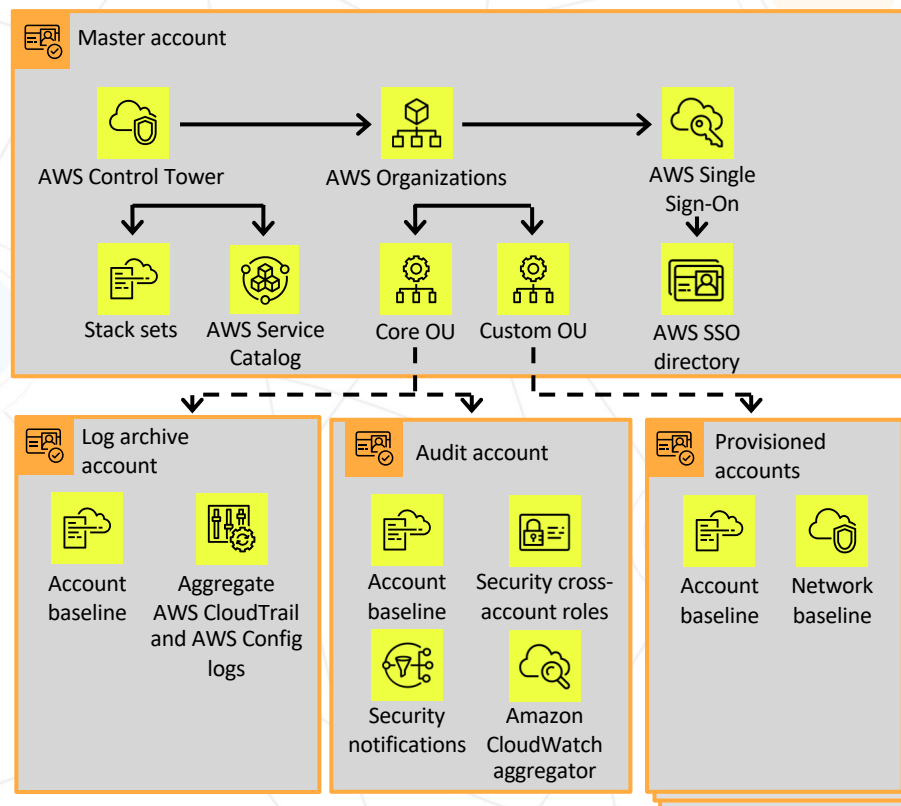
—  
Operate

**Business agility + governance control**

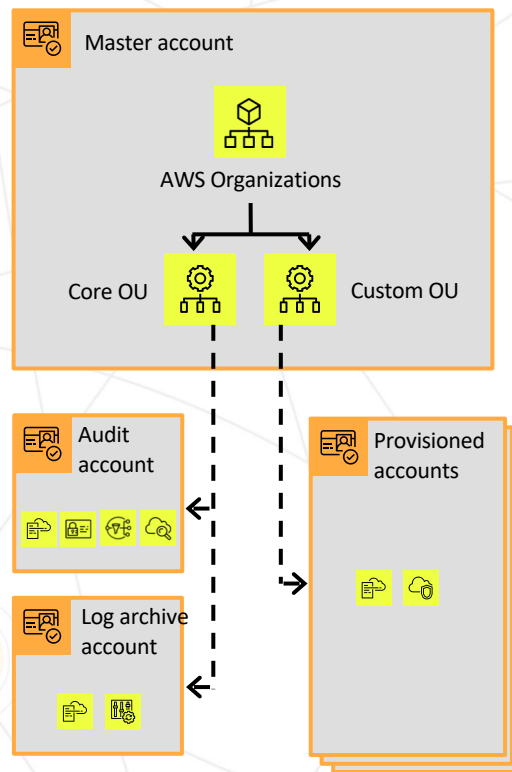
# Enable governance



# Set up an AWS landing zone



# Multi-account architecture

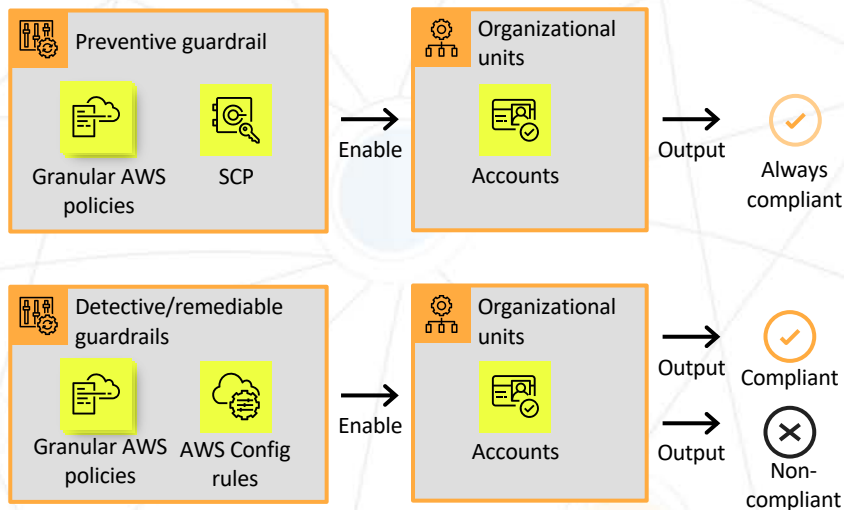


# Centralize identity and access



- 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

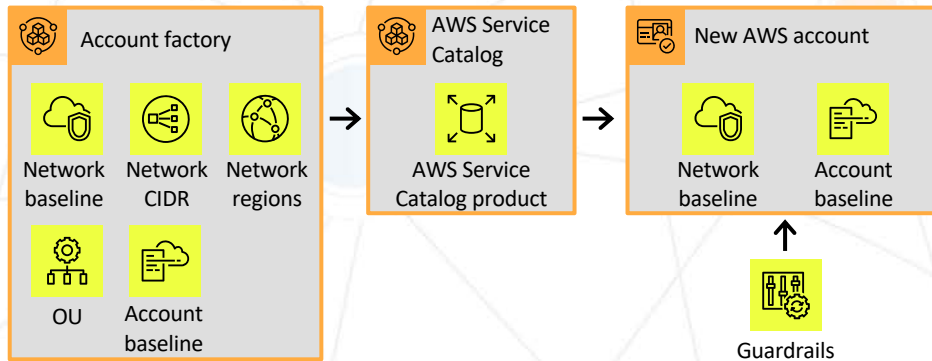


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: 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

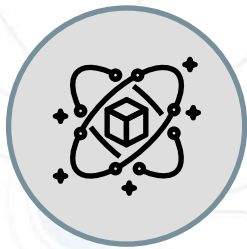
| Goal/category    | Example                                                                  |
|------------------|--------------------------------------------------------------------------|
| IAM security     | Require MFA for root user                                                |
| Data security    | 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



Enable



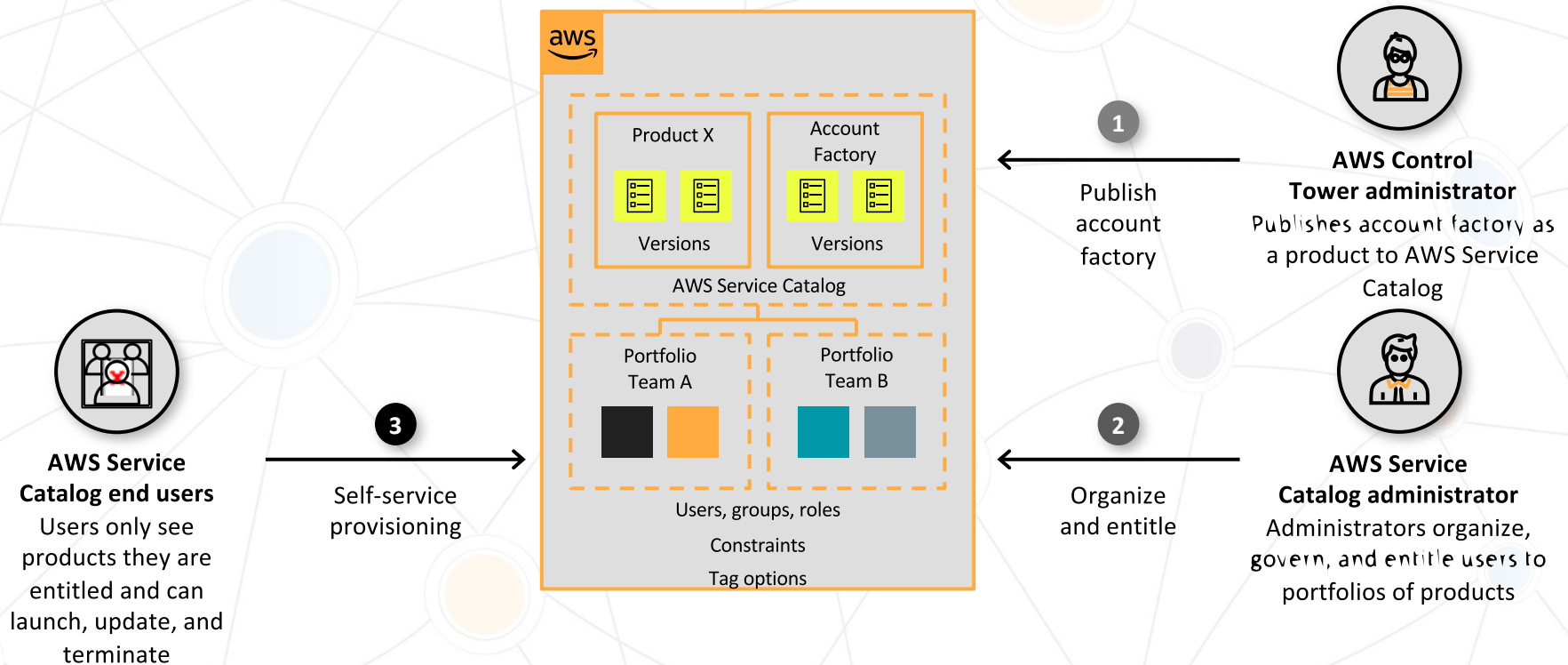
Provision



Operate

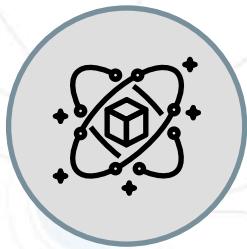
**Business agility + governance control**

# Self-service account provisioning in AWS Service Catalog

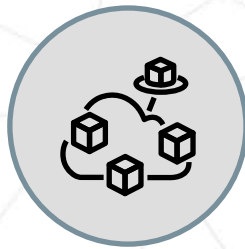


Users can configure and provision AWS accounts and resources without needing full privileges to AWS services (e.g., Amazon EC2, Amazon RDS)

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



Enable



Provision



Operate

**Business agility + governance control**

# Operate with agility + control



# Dashboard for oversight

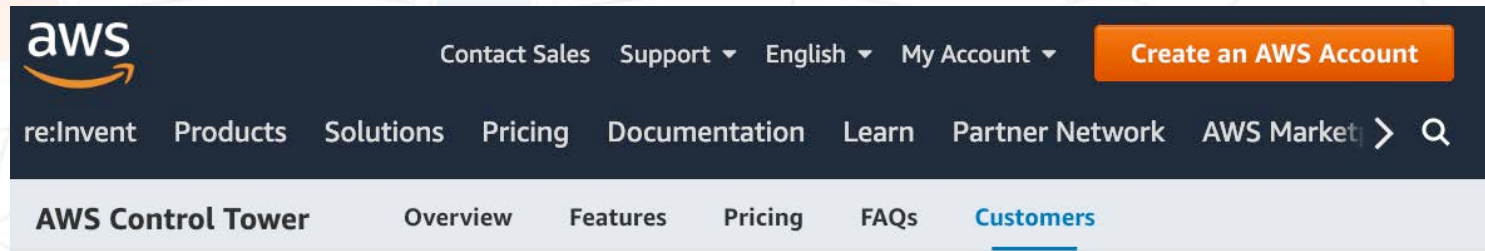
The screenshot displays the AWS Control Tower Dashboard. The left sidebar contains navigation links: Dashboard, Accounts, Organizational units, Guardrails, Users and access, Account factory, and Shared accounts. The main content area is titled 'AWS Control Tower > Dashboard' and includes a 'Recommended actions' section. Below this are two summary cards: 'Environment summary' showing 3 Organizational units and 34 Accounts, and 'Guardrail summary' showing 28 Preventive guardrails and 12 Detective guardrails. The 'Noncompliant resources' section lists three items: a Volume (vol-842jhdksj83821234) with Guardrail 'Enable encryption for EBS volumes at', another Volume (vol-05flia830kd209897) with the same Guardrail, and a Security Group (sg-031234b83bac98765) with Guardrail 'Disallow internet connection through'. The 'Organizational units' section shows three OUs: Core (Compliant), Project 1 (Noncompliant), and Custom (Noncompliant). The 'Accounts' section is partially visible at the bottom.

| Resource ID           | Resource type  | Service | Region    | Account name      | OU        | Guardrail                            |
|-----------------------|----------------|---------|-----------|-------------------|-----------|--------------------------------------|
| vol-842jhdksj83821234 | Volume         | EC2     | us-west-2 | db-uswest-1-gamma | Custom    | Enable encryption for EBS volumes at |
| vol-05flia830kd209897 | Volume         | EC2     | us-east-1 | testing-beta-1    | Project 1 | Enable encryption for EBS volumes at |
| sg-031234b83bac98765  | Security Group | EC2     | eu-west-1 | ops-test-4        | Project 1 | Disallow internet connection through |

| Name      | Parent OU | Compliance   |
|-----------|-----------|--------------|
| Core      | Root      | Compliant    |
| Project 1 | Root      | Noncompliant |
| Custom    | Root      | Noncompliant |

| Account name | Account email | Organizational unit | Owner | Compliance status |
|--------------|---------------|---------------------|-------|-------------------|
|--------------|---------------|---------------------|-------|-------------------|

# AWS Control Tower Adoption at Lafayette



## 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

 Services ▾ Resource Groups ▾ ⭐

AWSReservedSSO\_AWSAdmini... ▾ N. Virginia ▾ Support ▾

**AWS Control Tower** ✕

**Dashboard**

Accounts

Organizational units

Guardrails

Users and access

Settings

Account factory

► Shared accounts

Activities

[AWS Control Tower](#) > Dashboard

 **Your landing zone is now available.**  
AWS Control Tower has set up the following:

- 2 organizational units, one for your shared accounts and one for accounts that will be provisioned by your users.
- 3 shared accounts, which are the master account and isolated accounts for log archive and security audit.
- A native cloud directory with preconfigured groups and single sign-on access.
- 17 preventive guardrails to enforce policies and 2 detective guardrails to detect configuration violations.

▼ Recommended actions

  
**Add organizational units**  
Add organizational units (OUs) to organize accounts and projects.

  
**Configure your account factory**  
Define settings and configuration options for AWS accounts that your users can provision from AWS Service Catalog.

  
**Enable more guardrails**  
Enable additional guardrails to meet your security, operational, and compliance requirements.

  
**Review users and access**  
Review your user identity store and single sign-on access for your users across accounts.

  
**Review shared accounts**  
Review the settings of the shared accounts that AWS Control Tower has set up for you.

**Environment summary**

**10**  
Organizational units

**42**  
Accounts

**Guardrail summary**

**20**  
Preventive guardrails

**5**  
Detective guardrails

# Automatic Guardrails

 Services ▾ Resource Groups ▾ ★

AWS Control Tower ×

Dashboard

Accounts

Organizational units

**Guardrails**

Users and access

Settings

Account factory

► Shared accounts

Activities

AWS Control Tower > Guardrails

## Guardrails Info

Guardrails are governance rules that you can enable on your organizational units (OUs) to enforce policies or detect violations.

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

# Control Tower Account Inventory

 Services ▾ Resource Groups ▾ ⚙

🔔 AWSReservedSSO\_AWSAdminl... ▾ N. Virginia ▾ Support ▾

AWS Control Tower

×

Dashboard

Accounts

Organizational units

Guardrails

Users and access

Settings

Account factory

▶ Shared accounts

Activities

AWS Control Tower > Accounts

Accounts Info

Accounts in your organization are governed by account configuration controls and guardrails that you enable. Accounts are either created by AWS Control Tower as part of the landing zone or provisioned by you and your users through AWS Service Catalog. Accounts provisioned outside of the account factory in AWS Service Catalog are not managed by AWS Control Tower and are not shown below.

Provision new account 

< 1 2 ... >

| Account name                          | Account email    | Organizational unit   | Owner             | State   |
|---------------------------------------|------------------|-----------------------|-------------------|---------|
| Web Content Management [PROD]         | v...@...<br>f... | Projects - Production | Self              | ✔ Ready |
| kalbj-test-account                    | k...@...         | Sandboxes             | Self              | ✔ Ready |
| IAM Docker Images                     | i...@...         | Shared Services       | Self              | ✔ Ready |
| CAS PROD                              | i...@...         | Projects - Production | Self              | ✔ Ready |
| bucklerm-sandbox                      | b...@...         | Sandboxes             | Self              | ✔ Ready |
| storage-gateway                       | j...@...         | Shared Services       | Self              | ✔ Ready |
| DigitalScholarshipServices-Production | j...@...         | Projects - Production | Self              | ✔ Ready |
| Master                                | i...@...         | Root                  | AWS Control Tower | ✔ Ready |
| IP Blocker                            | s...@...         | Projects - Production | Self              | ✔ Ready |
| Log archive                           | i...@...         | Core                  | AWS Control Tower | ✔ Ready |

# Lafayette DynamoDB Account Inventory

AccountInventory [Close](#)



[Overview](#) [Items](#) [Metrics](#) [Alarms](#) [Capacity](#) [Indexes](#) [Global Tables](#) [Backups](#) [Contributor Insights](#) [Triggers](#) [Access control](#) [Tags](#)

[Create item](#) [Actions](#)



Scan: [Table] AccountInventory: AccountID ^

Viewing 1 to 45

Scan [Table] AccountInventory: AccountID ^

+ Add filter

Start search

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

# Compliance automation

 Services ▾ Resource Groups ▾ ☆

 AWSReservedSSO\_AWSAdmini... ▾ N. Virginia ▾ Support

**AWS Control Tower** ✕

**Dashboard**  
Accounts  
Organizational units  
Guardrails  
Users and access  
Settings

**Accounts**

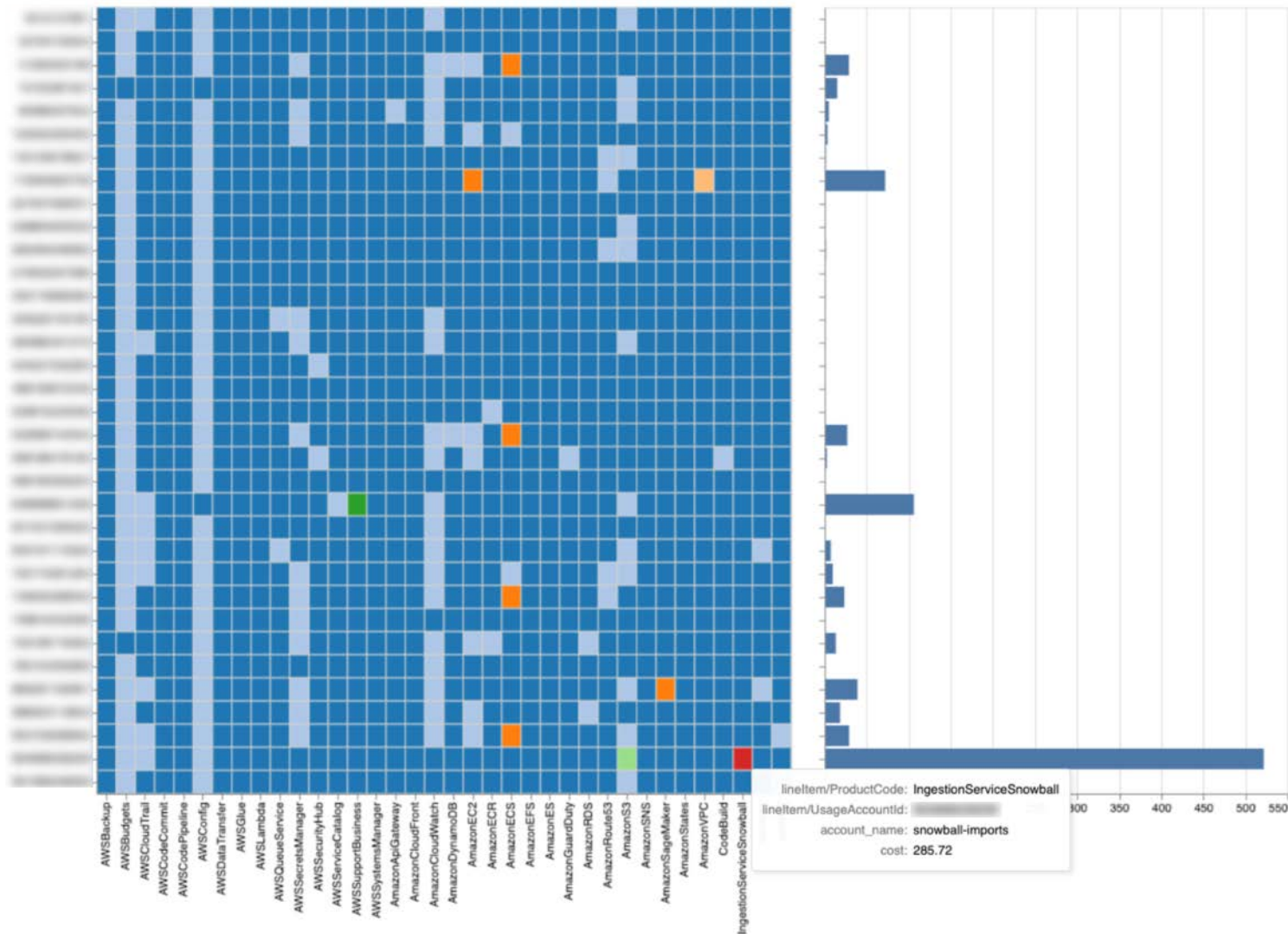
| Account name                       | Account email | Organizational unit    | Owner | Compliance status              | State       |
|------------------------------------|---------------|------------------------|-------|--------------------------------|-------------|
| Webdev Custom Apps PROD            |               | Projects - Production  | Self  | ✔ Compliant                    | ✔ Ready     |
| DigitalScholarshipServices-Sandbox |               | Sandboxes              | Self  | ✔ Compliant                    | ✔ Ready     |
| CAS STAGE                          |               | Projects - Development | Self  | ✔ Compliant                    | ✔ Ready     |
| Calendar Event Integrations STAGE  |               | Projects - Development | Self  | ⚠ Unknown <a href="#">Info</a> | ⚠ Not found |
| Legal-Holds-LC                     |               | Isolated Storage       | Self  | ✔ Compliant                    | ✔ Ready     |

View all accounts

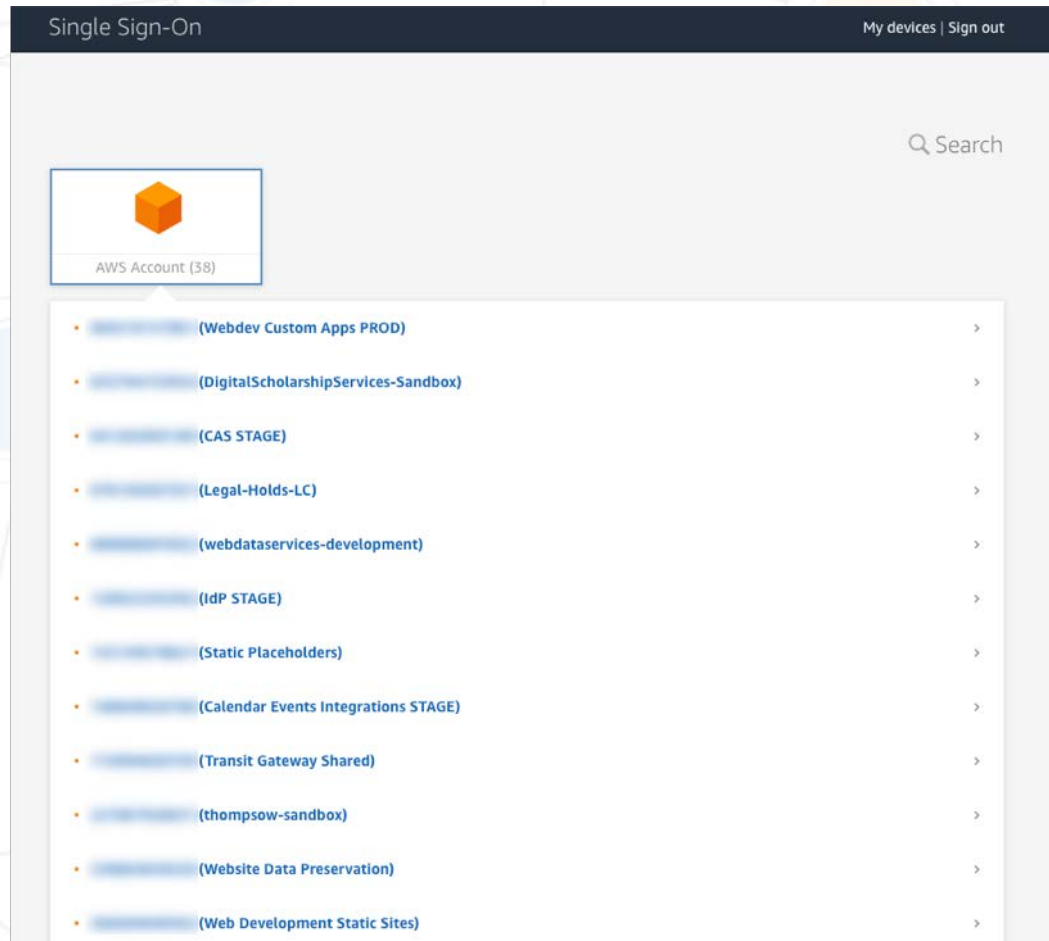
**Guardrails**

| Name                                                      | Guidance  | Category   | Behavior   | Status     |
|-----------------------------------------------------------|-----------|------------|------------|------------|
| <a href="#">Disallow deletion of log archive</a>          | Mandatory | Audit logs | Prevention | 🔒 Enforced |
| <a href="#">Enable encryption at rest for log archive</a> | Mandatory | Audit logs | Prevention | 🔒 Enforced |

# 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

**AWS Control Tower** ×

Dashboard

Accounts

Organizational units

Guardrails

Users and access

**Settings**

Account factory

Shared accounts

Activities

AWS Control Tower > Settings

## Settings Info

View your landing zone version details, update and repair.

### Details

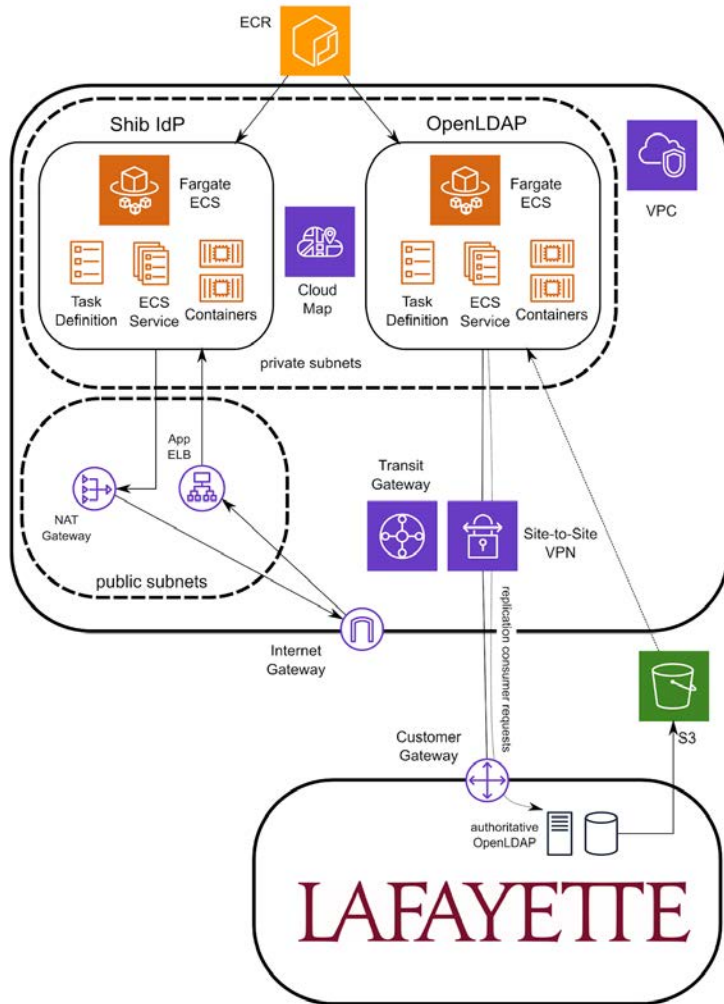
|                |                 |                           |
|----------------|-----------------|---------------------------|
| Latest Version | Current Version | Status                    |
| 2.2            | 2.2             | <span>✓ Up to date</span> |

### Versions

RepairUpdate

|                                  | Version Number | Release Date      | Release Notes                                                             |
|----------------------------------|----------------|-------------------|---------------------------------------------------------------------------|
| <input type="radio"/>            | 2.2            | November 13, 2019 | Updates to the latest blueprints and guardrails.                          |
| <input checked="" type="radio"/> | 2.1            | June 24, 2019     | Updates to the latest blueprints, guardrails, and expanded functionality. |
| <input checked="" type="radio"/> | 2.0            | April 22, 2019    | Updates to the latest blueprints and guardrails.                          |
| <input checked="" type="radio"/> | 1.0            | November 28, 2018 | Initial version.                                                          |

# 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 ~]#
```

**Setting up your landing zone**  
Estimated time remaining: 60 minutes.

