What's New in AWS Landing Zone

Sam Elmalak, Principal Solutions Architect

Steve Morad, Sr. Manager, AWS Solutions

May 28, 2019

aws

What do customers want to do on AWS?

Build

focus on what differentiates

Move Fast

ideation to instantiation

Stay Secure

secure and compliant environment

aws

What do customers want to do on AWS?

Secure & Compliant

meets the organization's security and auditing requirements

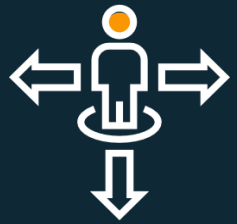
Scalable & Resilient

ready to support highly available and scalable workloads

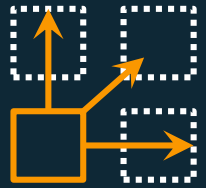
Adaptable & Flexible

configurable to support evolving business requirements

Customers are faced with



Many
design decisions



Need to configure
multiple accounts & services

establish
security baseline & governance

aws

You need a “Landing Zone”

- A configured, secure, scalable, multi-account AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time

Account security considerations

Baseline Requirements

Lock

AWS Account Credential Management (“Root Account”)

Enable

AWS CloudTrail
Amazon GuardDuty

Define

Map enterprise roles and permissions

Federate

Use identity solutions

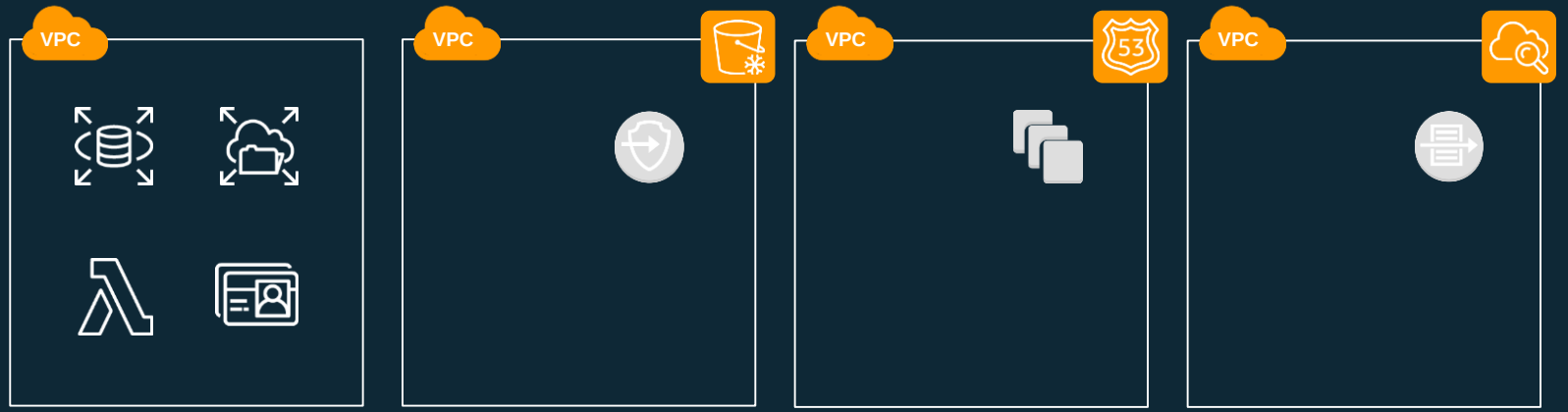
Establish

InfoSec cross-account roles

Identify

Actions and conditions to enforce governance

Network architecture considerations



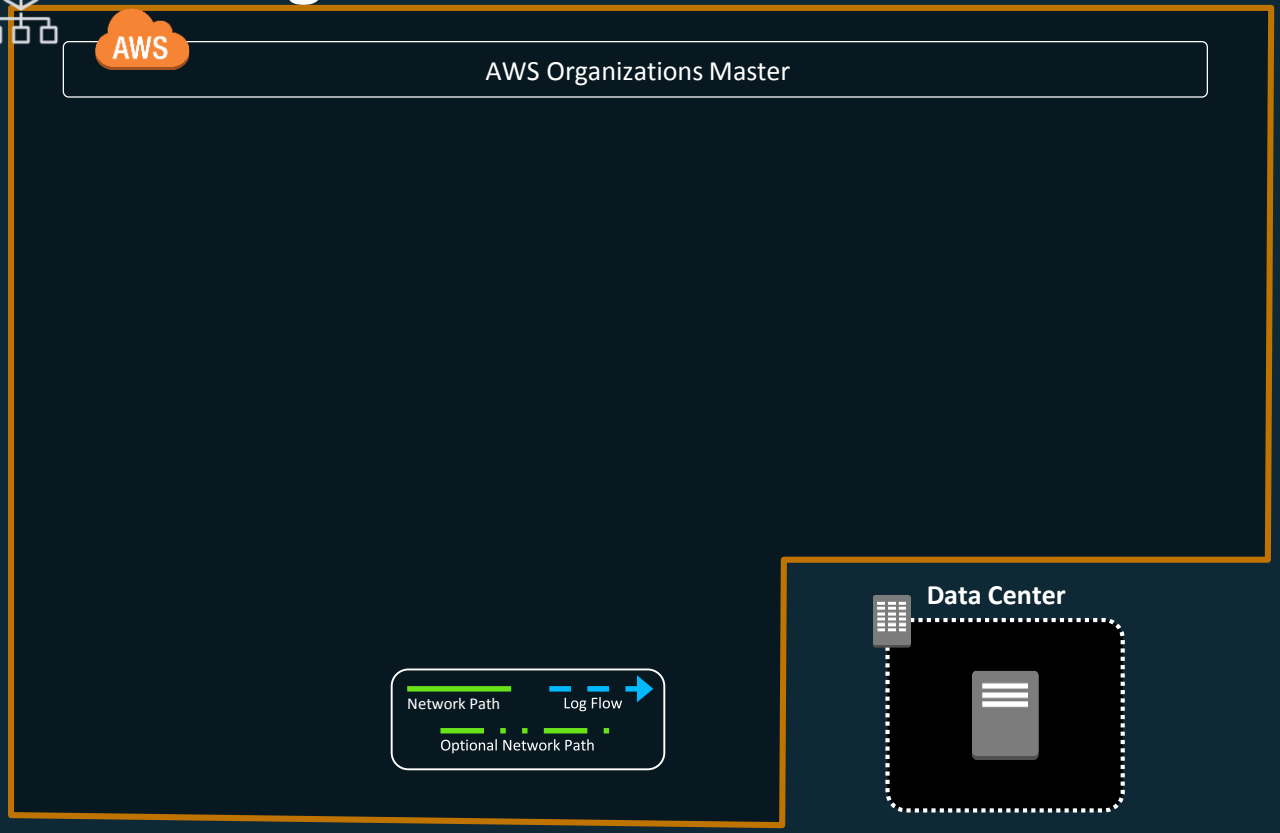
AWS Services in Your VPC

VPC Endpoints for Amazon S3

DNS in-VPC with Amazon Route 53

Logging VPC Traffic with VPC Flow Logs

AWS Organizations Master



No connection to DC

Service control policies

Consolidated billing

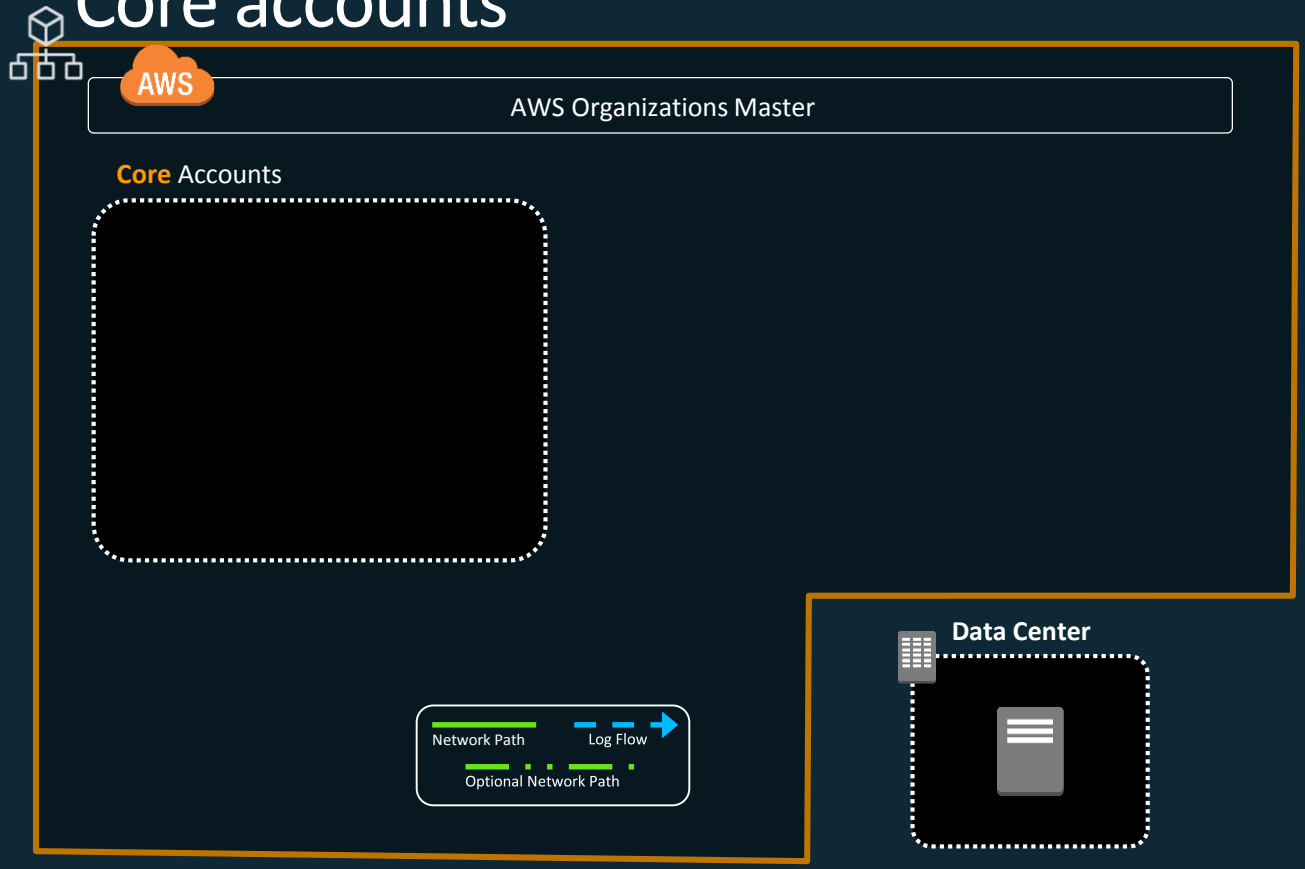
Volume discount

Minimal resources

Limited access

Restrict Orgs role!

Core accounts



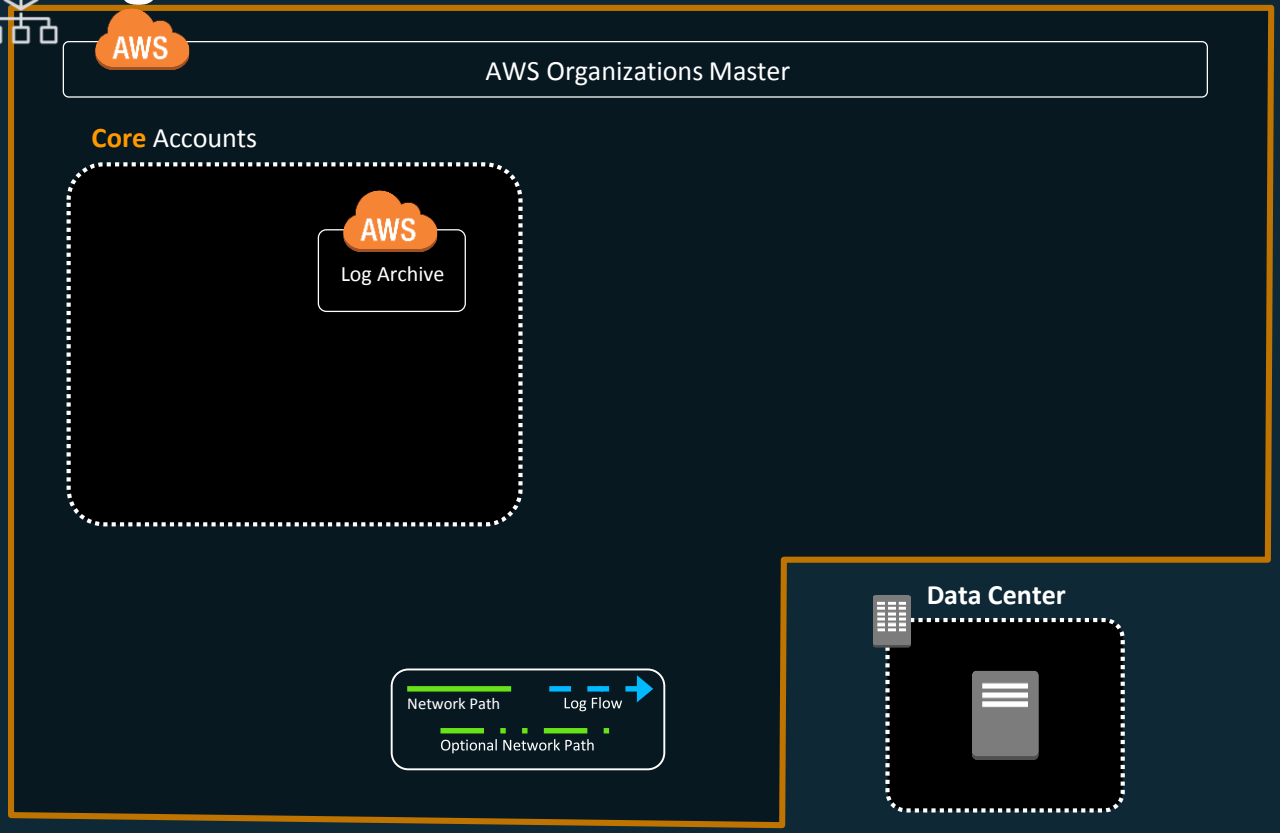
Foundational

Building Blocks

Once per organization

Have their own development life cycle (dev/qa/prod)

Log archive account



Versioned Amazon S3 bucket
- Restricted
- MFA delete

CloudTrail logs

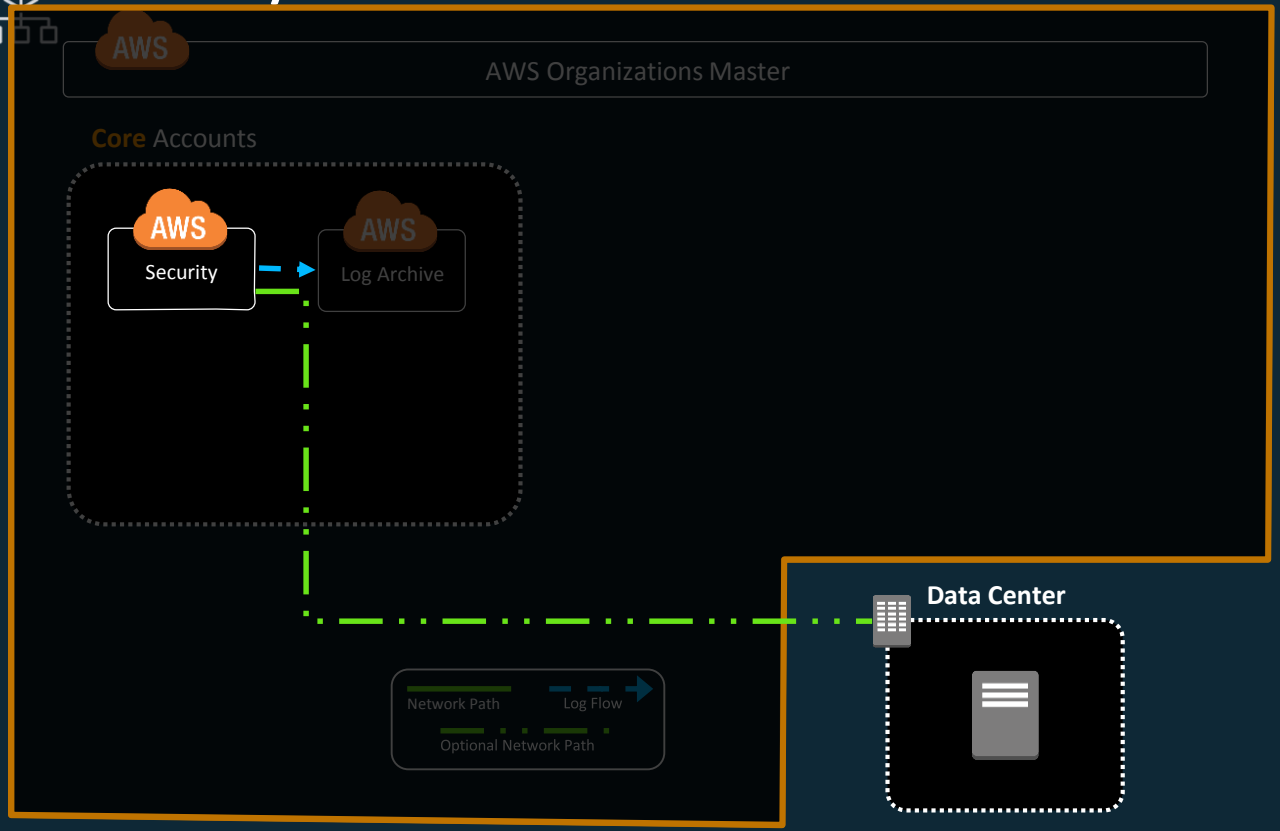
Security logs

Single source of truth

Alarm on user login

Limited access

Security account



Optional data center connectivity

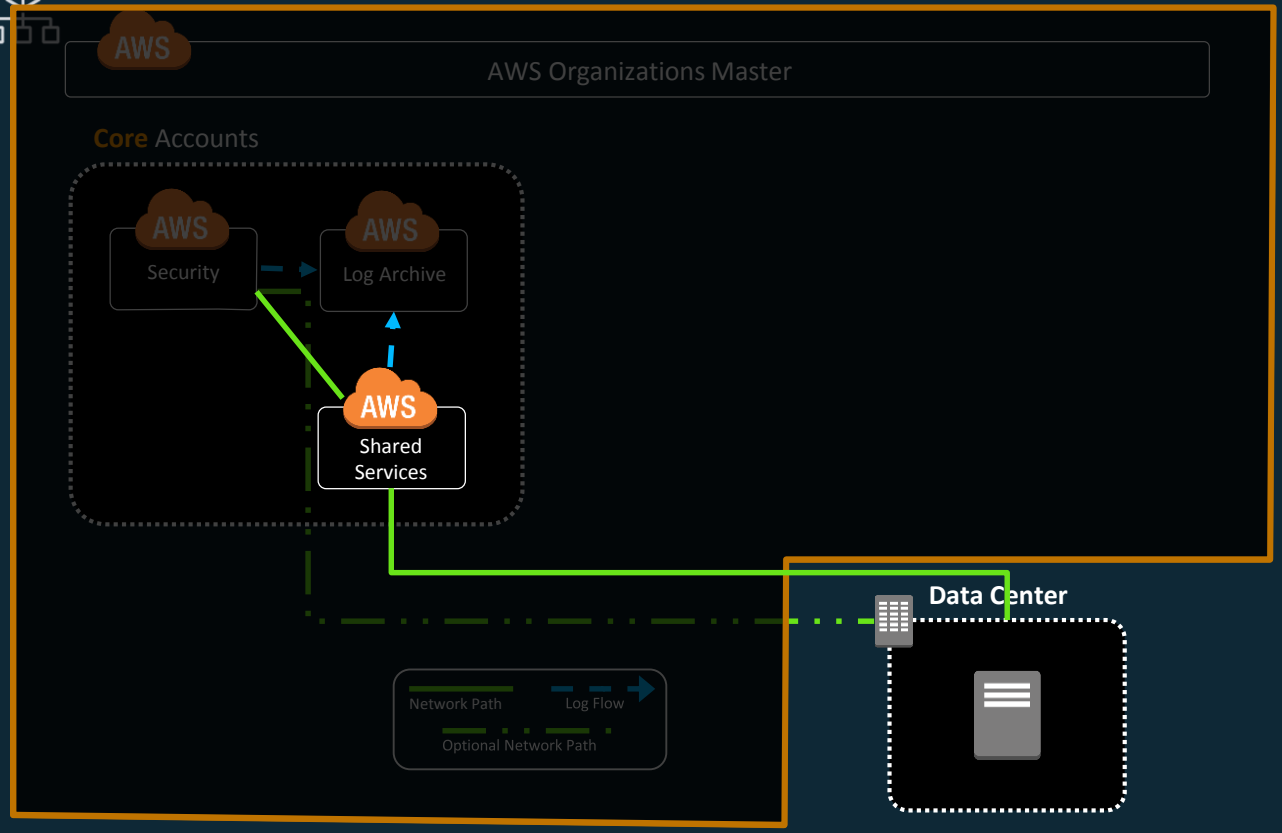
Security tools and audit

GuardDuty Master

Cross-account read/write
Automated Tooling

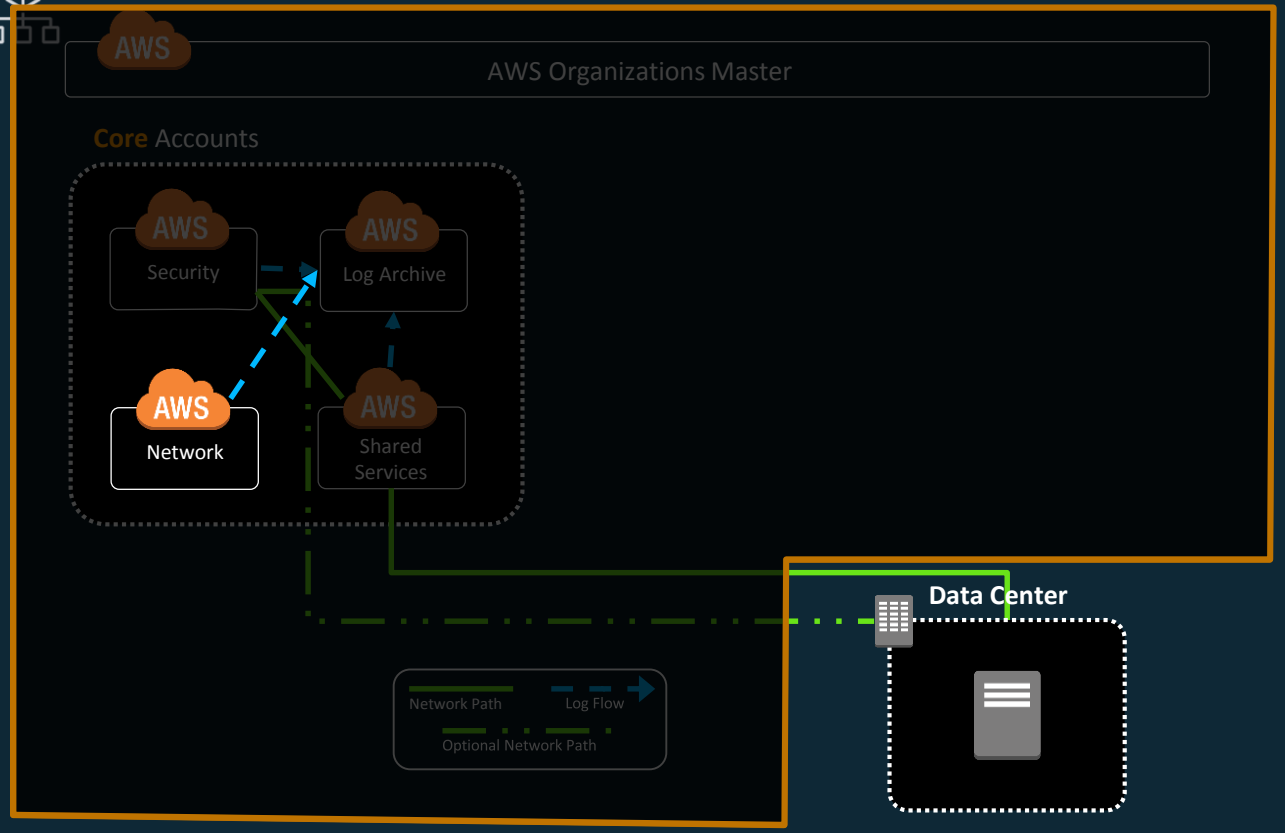
Limited access

Shared services account



- Connected to DC
- LDAP/Active Directory
- Shared Services VPC
- Deployment tools
  - Golden AMI
  - Pipeline
- Scanning infrastructure
  - Inactive instances
  - Improper tags
  - Snapshot lifecycle
- Monitoring
- Limited access

Network account



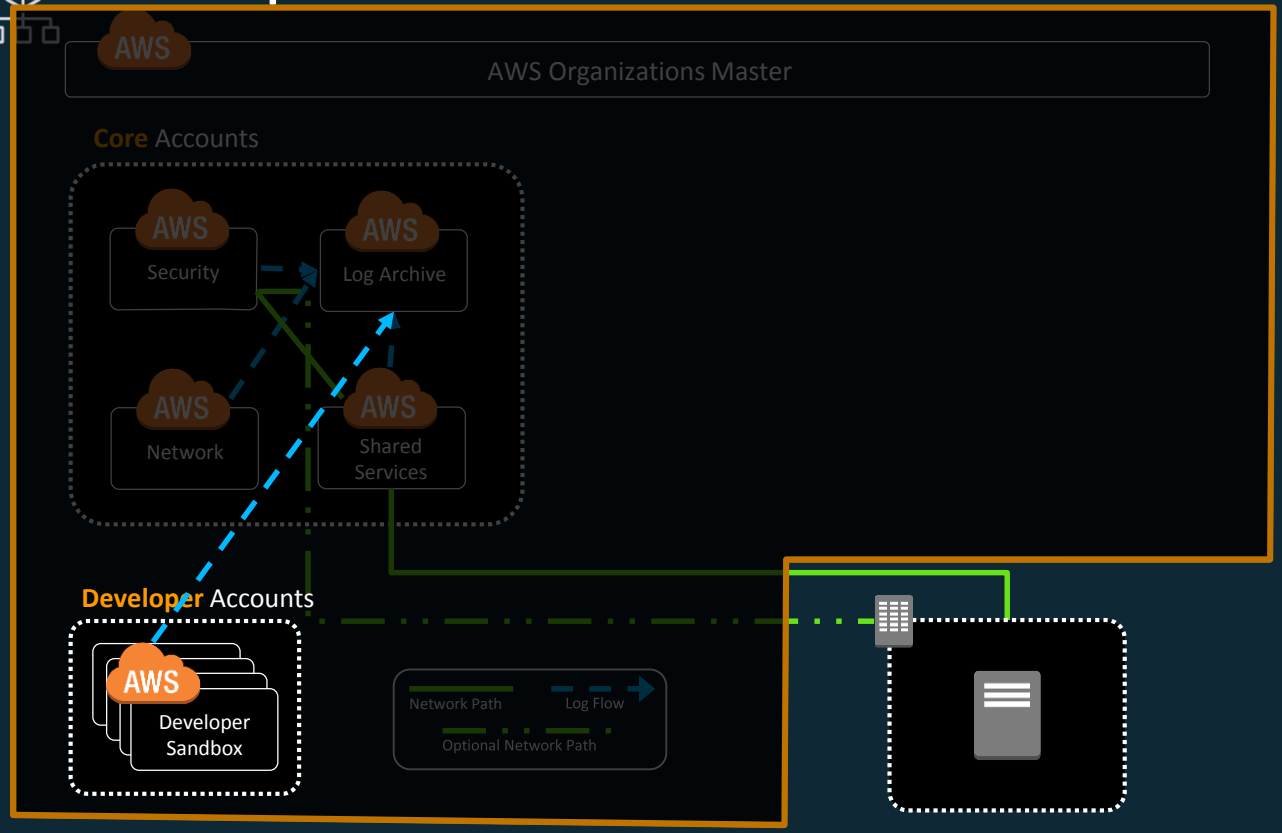
Managed by network team

Networking services

AWS Direct Connect

Limited access

Developer sandbox



No connection to DC

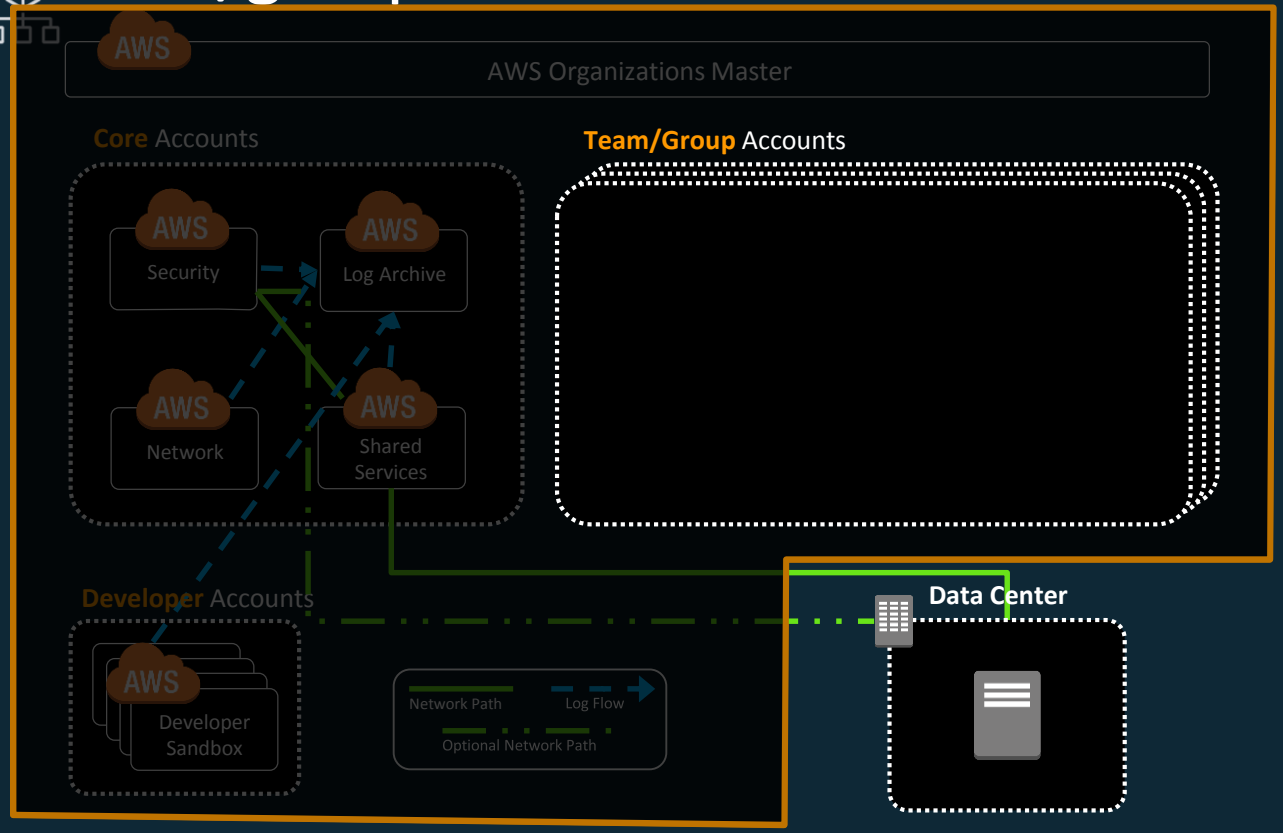
Innovation space

Fixed spending limit

Autonomous

Experimentation

Team/group accounts

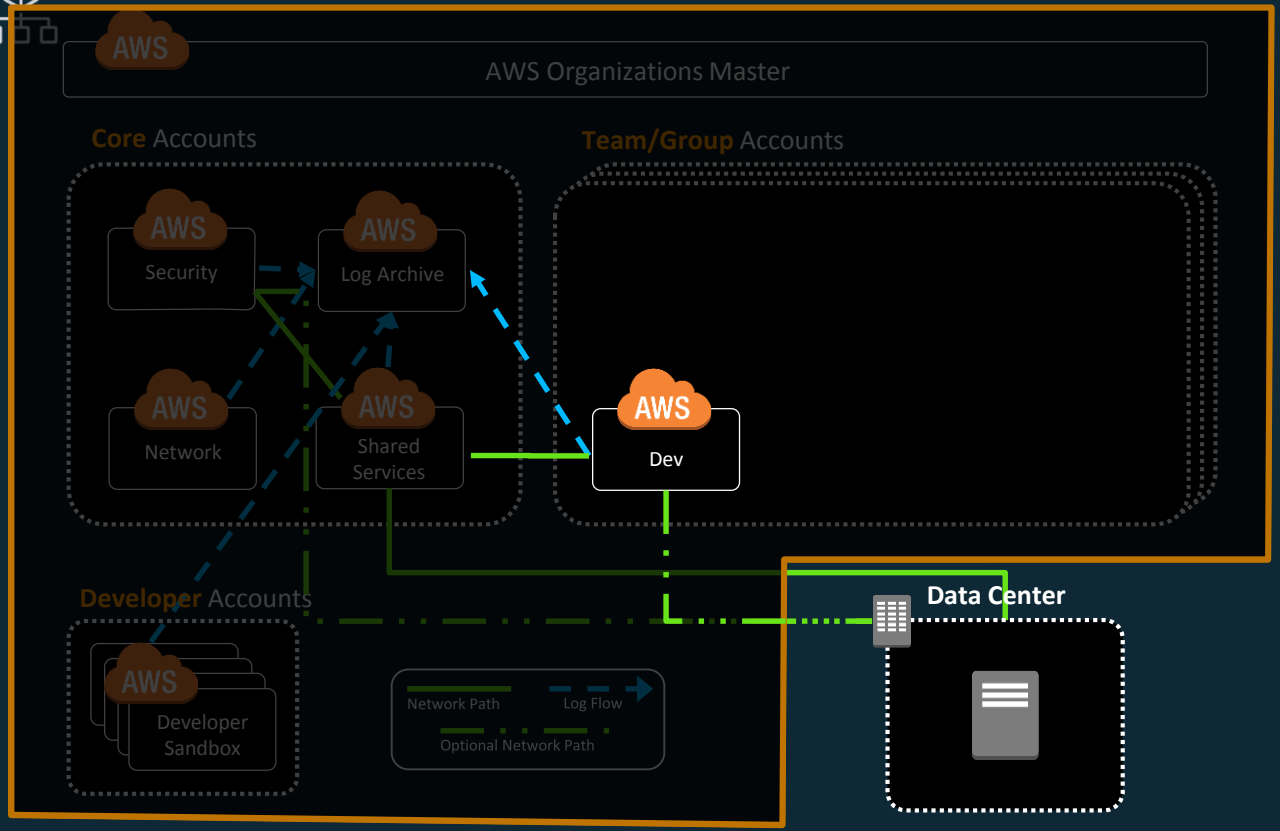


Based on level of needed isolation

Match your development lifecycle

Think Small

Dev

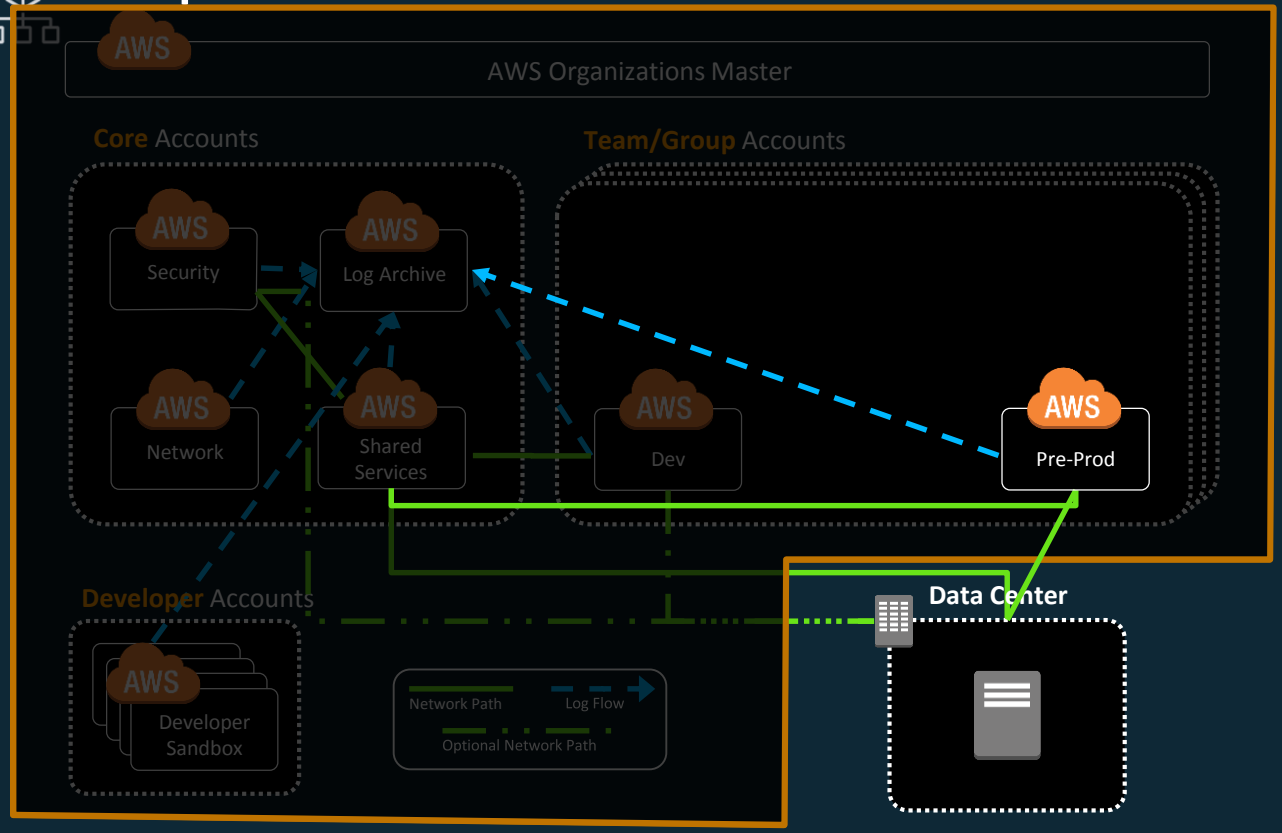


Develop and iterate quickly

Collaboration space

Stage of SDLC

Pre-production



Connected to DC

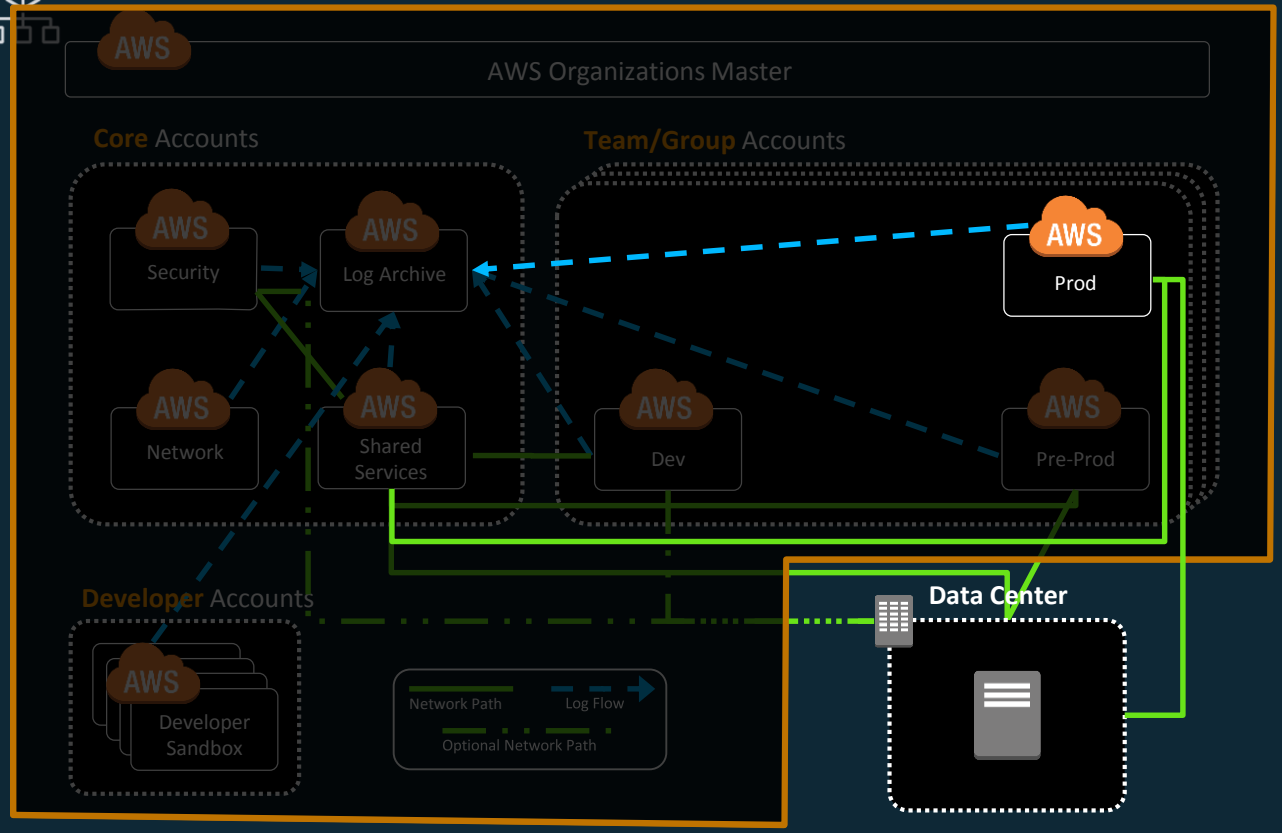
Production-like

Staging

Testing

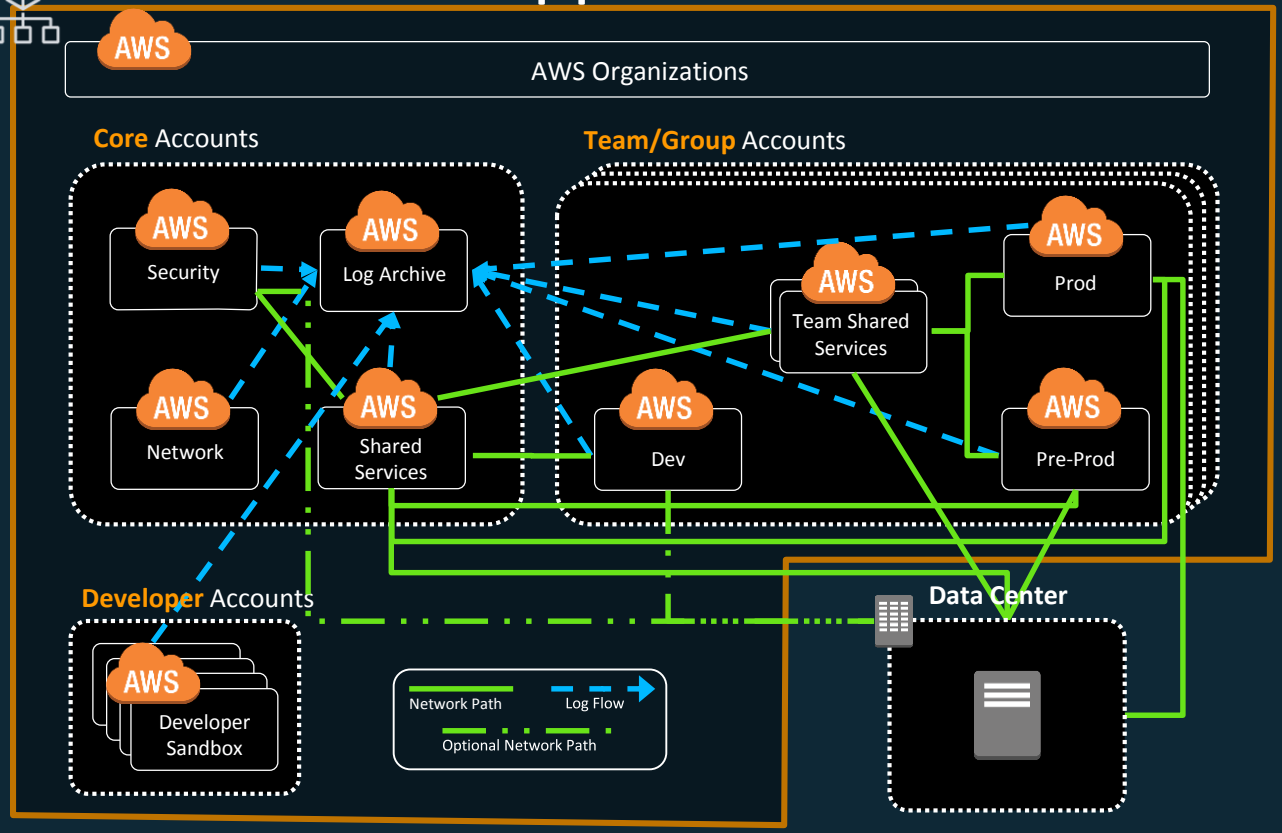
Automated Deployment

Production



- Connected to DC
- Production applications
- Promoted from Pre-Prod
- Limited access
- Automated Deployments

Multi-account approach



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: Direct Connect

Dev Sandbox: Experiments, Learning

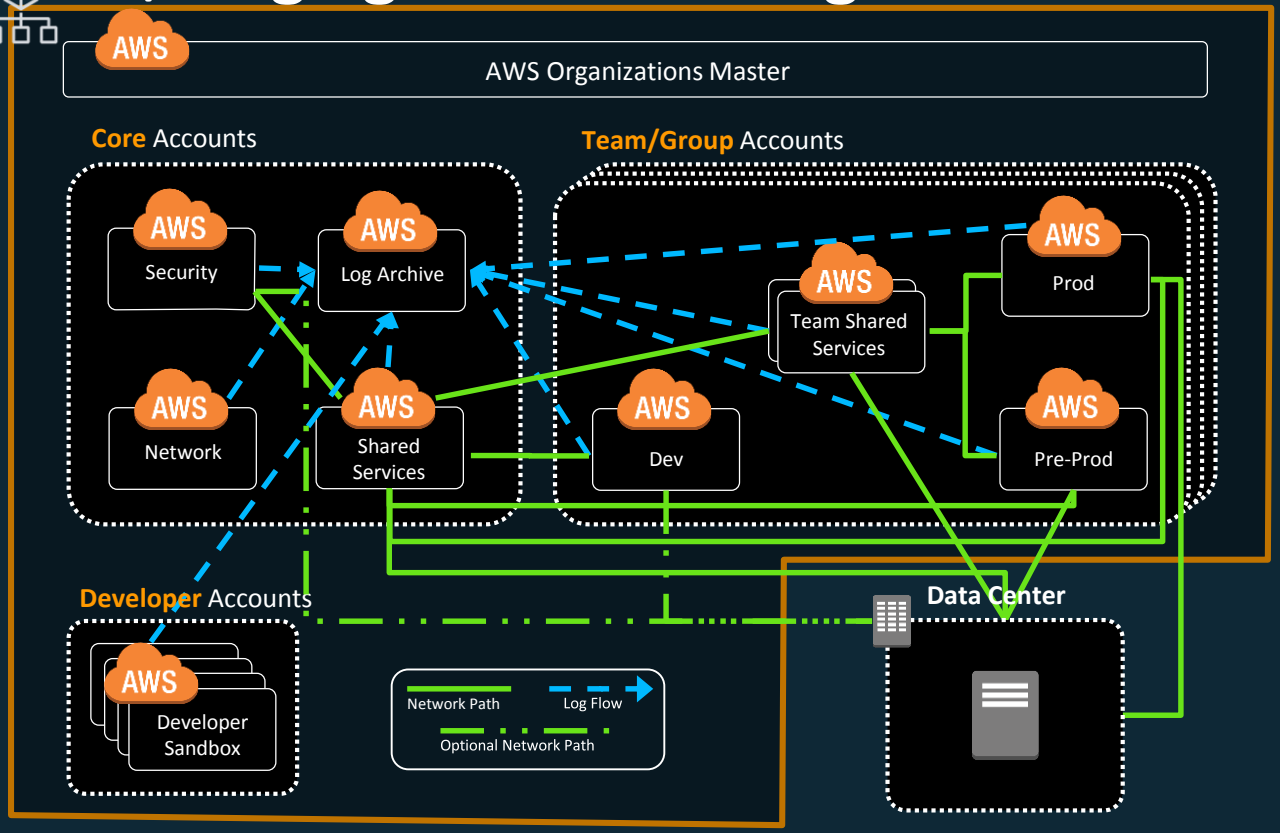
Dev: Development

Pre-Prod: Staging

Prod: Production

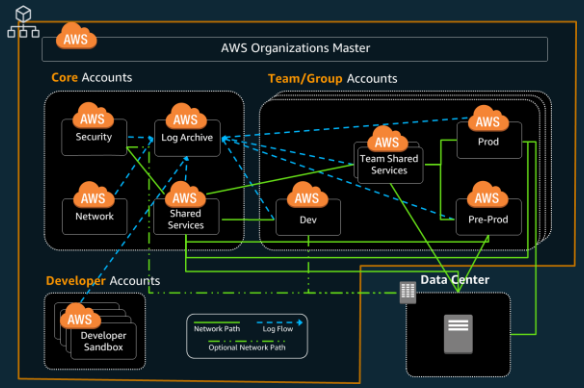
Team SS: Team Shared Services, Data Lake

QA/Staging for the landing zone



Test Landing Zone changes

Another Landing Zone



The AWS Landing Zone solution

An easy-to-deploy solution that automates the setup of **new AWS multi-account environments**

Based on AWS best practices and recommendations

Initial security and governance controls

Baseline accounts and account vending machine

Automated deployment

What you get with the AWS Landing Zone

Account Management

- Framework for creating and baselining a multi-account environment
- Initial multi-account structure including security, audit, & shared service requirements
- An account vending machine that enables automated deployment of additional accounts with a set of security baselines

---

Identity & Access Management

- User account access managed through AWS SSO federation
- Cross-account roles enable centralized management

Security & Governance

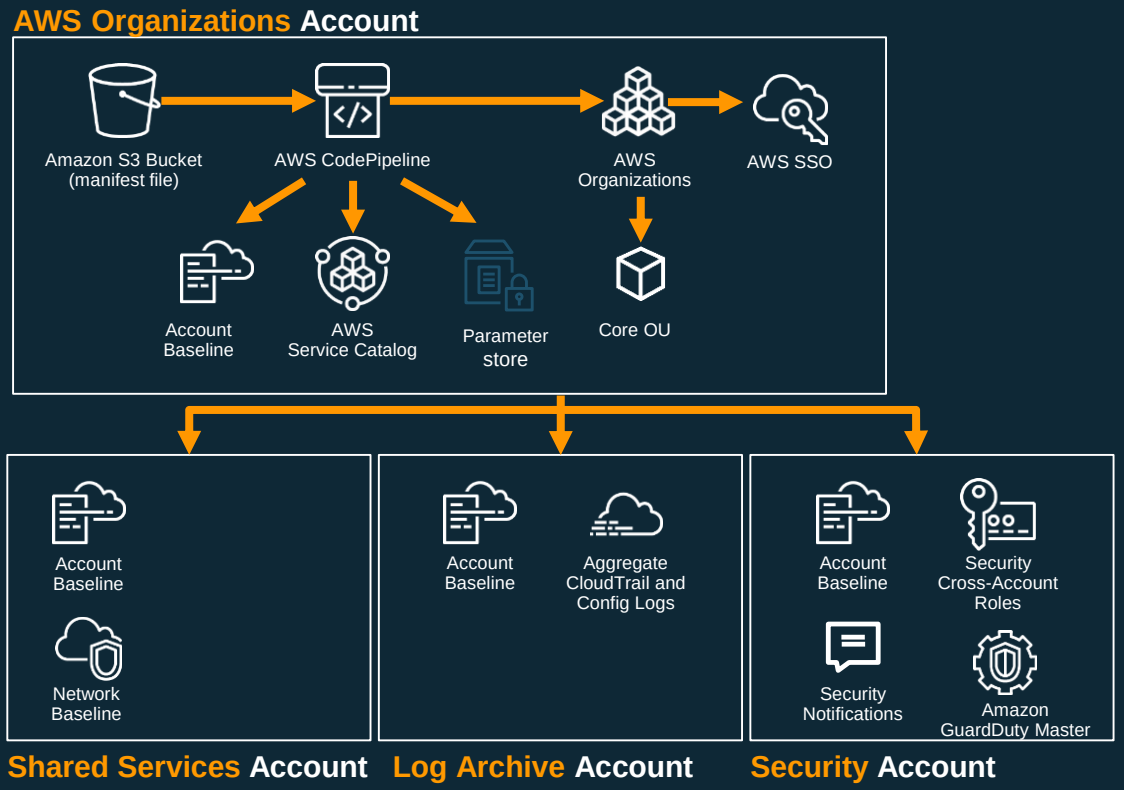
- Multiple accounts enable separation of duties
- Initial account security and AWS Config rules baseline
- Network baseline
- Sets up monitoring and intelligent threat detection (through Amazon GuardDuty)

Solution Extensibility

- Easily deploy optional Add-Ons to extend your AWS Landing Zone

aws

AWS Landing Zone structure - basic



Organizations Account

- Account Provisioning
- Account Access (SSO)

Shared Services Account

- Active Directory
- Log Analytics

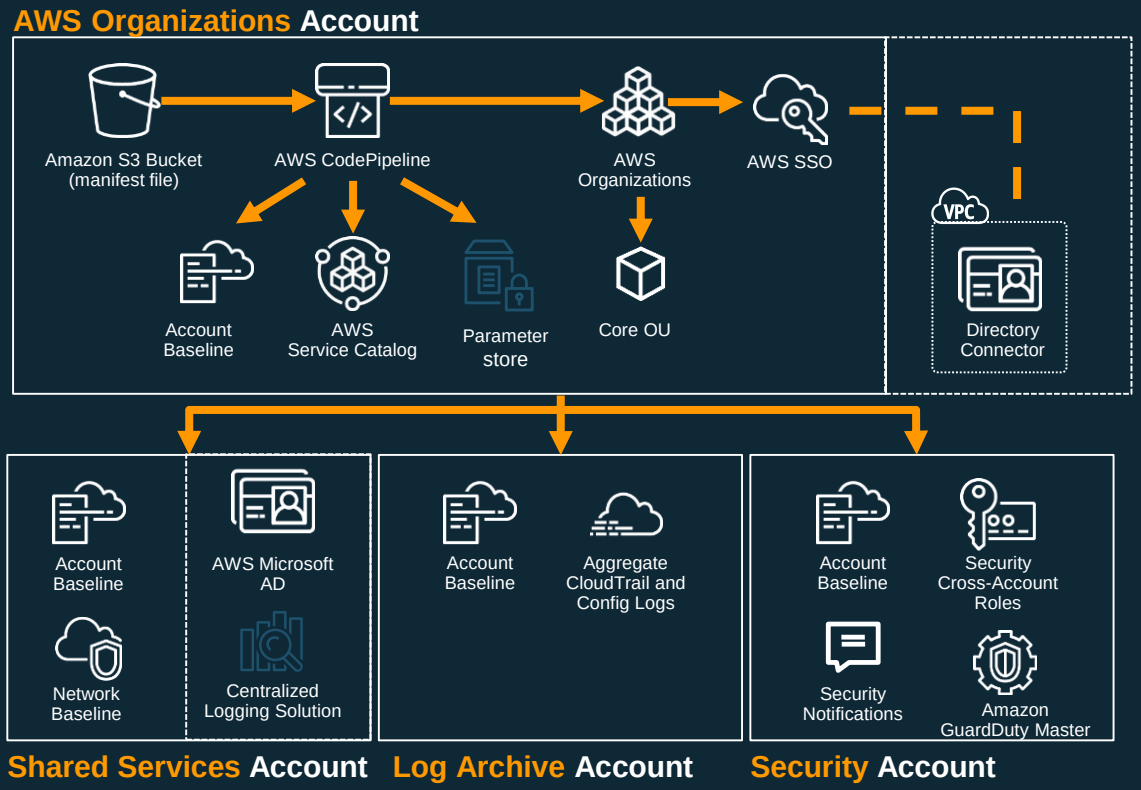
Log Archive

- Security Logs

Security Account

- Audit / Break-glass

AWS Landing Zone structure – with Add-Ons



Organizations Account

- Directory Connector

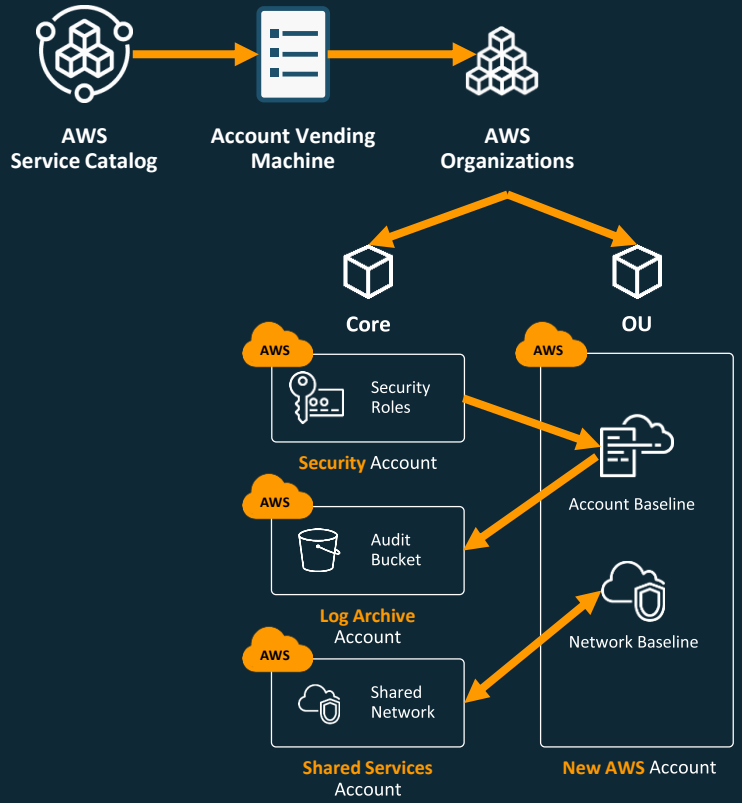
Shared Services Account

- Microsoft AD
- Centralized Logging Solution

Custom Add-ons

- Loosely Coupled
- Self-contained
- Autonomous
- Granular

Account Vending Machine



Account Vending Machine (AWS Service Catalog)

- Account creation factory
- User Interface to create new accounts
- Account baseline versioning
- Launch constraints

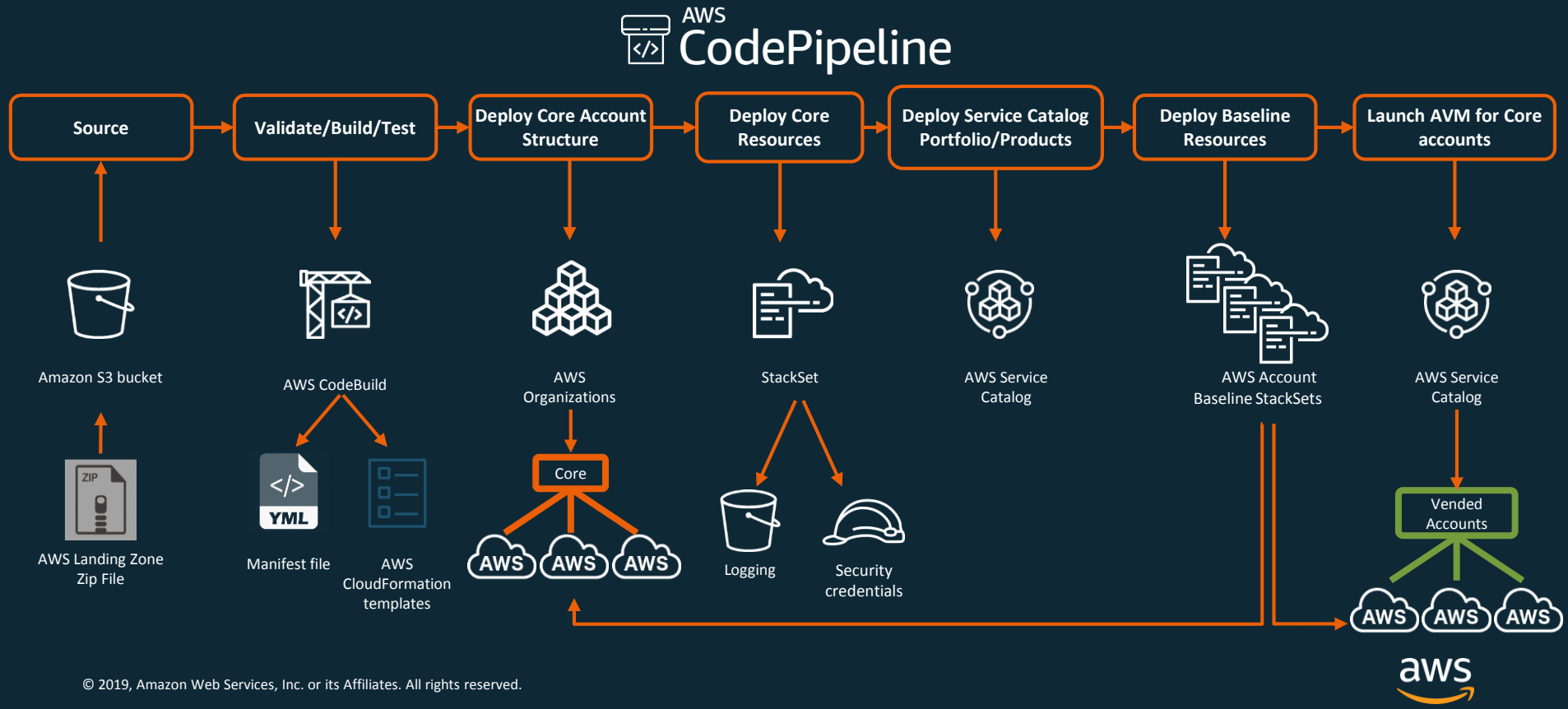
Creates/updates AWS account

Apply account baseline stack sets

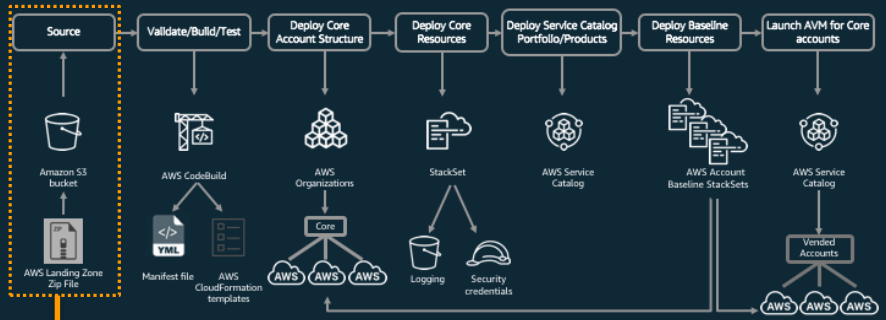
Create network baseline

Apply account security control policy

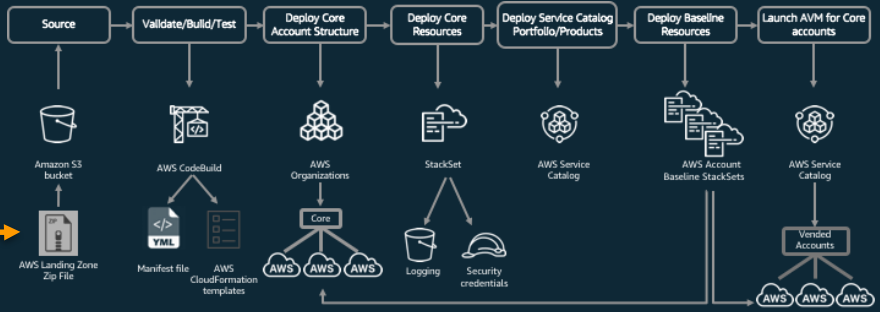
The AWS Landing Zone Pipeline



The AWS Landing Zone Development Pipeline

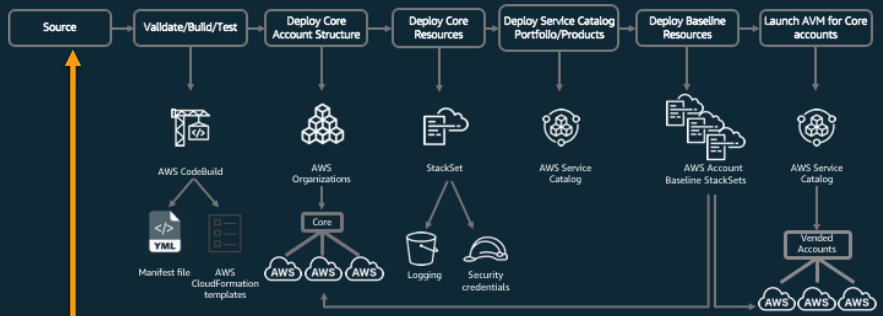


Development Landing Zone



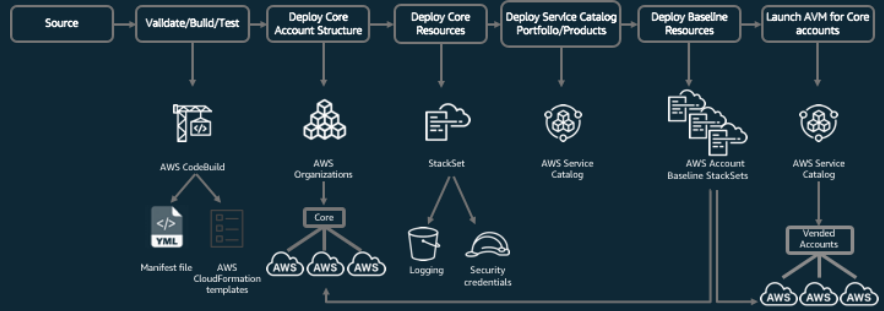
Production Landing Zone

The AWS Landing Zone Development Pipeline



Development Landing Zone

AWS CodeCommit



Production Landing Zone

Benefits

Automated

Scalable

Self-Service

Guardrails
NOT Blockers

Auditable

Flexible

aws

Pricing

No additional charge for the AWS Landing Zone solution.

Customers are responsible for the charges of the underlying services (e.g., AWS Config Service, AWS CloudTrail, etc.).

Cost for the basic solution: ~$200 / month

Monthly cost for optional add-ons:

- Centralized logging solution: <$400
- Directory Connector: <$50
- AWS Managed AD plus Remote Desktop Gateway: ~$300

Introducing AWS Control Tower (preview)

Consistent and simple multi account management.

Automated AWS Setup

Launch an automated landing zone with best-practices blueprints

Policy Enforcement

Pre-packaged guardrails to enforce policies or detect violations

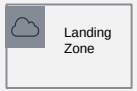
Dashboard for Oversight

Continuous visibility into workload compliance with controls

aws

Key Features / Benefits

Account Setup



Automated secure and scalable landing zone

Multi-account management using AWS Organizations

Account provisioning wizard

Central Logging and Multi-account configuration consistency

Guardrails

Built-in best practices

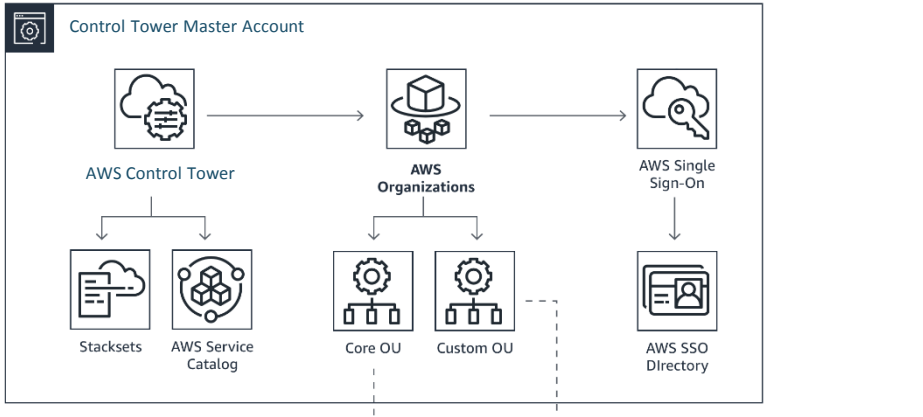
Multi-account Preventive and detective guardrails

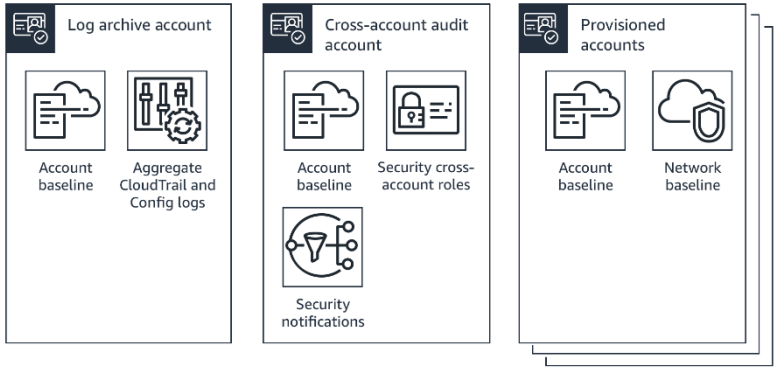
Curated rules in plain English

Easy to use Dashboard and notifications

aws

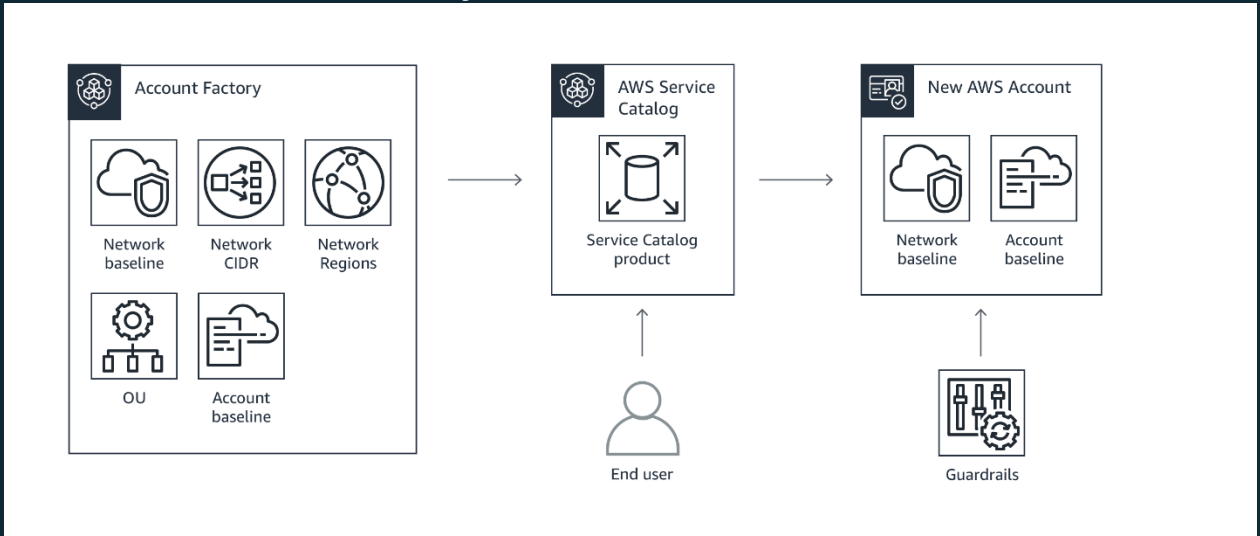
AWS Control Tower's automated landing zone





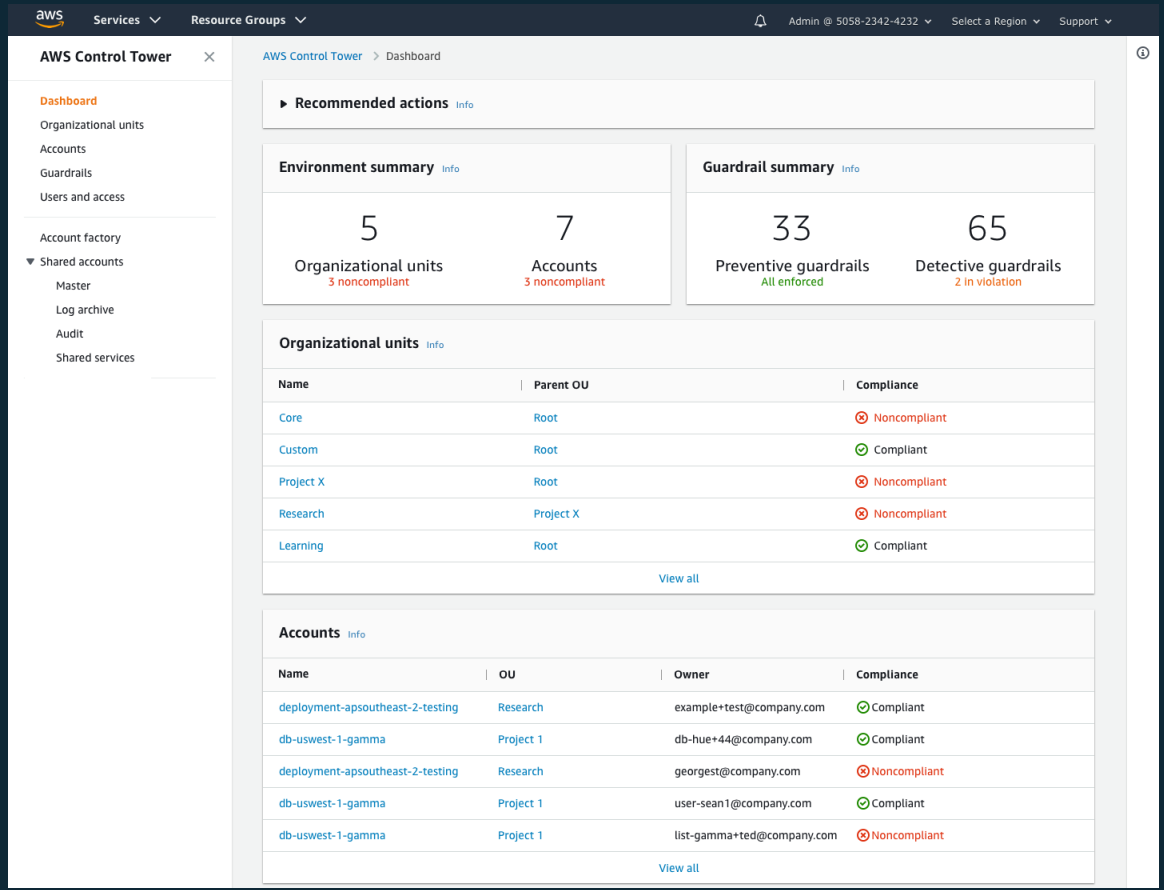
- ✓ AWS Organizations with a master and pre-created accounts for central log archive and cross-account audit
- ✓ Pre-configured directory and single sign-on using AWS SSO (with Active Directory custom option)
- ✓ Centralized monitoring and alerts using AWS Config, AWS CloudTrail, and AWS CloudWatch

Account Factory



- Account factory for controls on account provisioning
  - Pre-approved account baselines with VPC options
  - Pre-approved configuration options
- End user configuration and provisioning through AWS Service Catalog
- Creates/updates AWS accounts under organizational units

Dashboard for Oversight



Options for operating your AWS Landing Zone

Well-Operated State

- Working backwards
- Operating like code
- Designing for failure
- Embracing enterprise DevOps
- Applying guardrails not barriers
- Running lean teams
- Automating everything

Paths to a Well-Operated State

Self Managed

- Service Catalog
- Modeling and Provisioning
- Automation and Operations
- Monitoring and Logging

AWS Managed via AMS

- Month to Month
- AWS Out of the Box
- Curated Services & Management Tools
- Infrastructure Ops, Security & Compliance

Partner/MSP Managed

- 100+ Partners
- Certification Program
- Third Party Audit
- End-to-End Services

AWS Managed + Partner/MSP Managed

aws + Partner

aws

Get Started

To learn more about AWS Control Tower visit:

aws.amazon.com/controltower

To learn more about AWS Landing Zone, please talk with your account team or visit:

aws.amazon.com/solutions/aws-landing-zone

Title Only

Title + Content

Section Title

Section Title

Two Content

Comparison

Three Content

Four Content - Graphics

Six Content - Graphics