Launch Faster using AWS Landing Zones

Sam Elmalak, Solutions Architect

Steve Morad, Manager Solutions Builders

What do customers want to do on AWS?

Build

focus on what differentiates

Move Fast

ideation to instantiation

Stay Secure

secure and compliant environment

Building a Landing Zone can be challenging

Many
design decisions

Need to configure
multiple accounts & services

Must establish
security baseline & governance

You need a Landing Zone that is ...

✓ **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

What is 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 customers’ application migration journey
- An environment that allows for iteration and extension over time

Account Security Considerations

Baseline Requirements

Lock

AWS Account Credential Management (“Root Account”)

Federate

Use Identity Solutions

Enable

AWS CloudTrail

Establish

InfoSec Cross Account Roles

Define

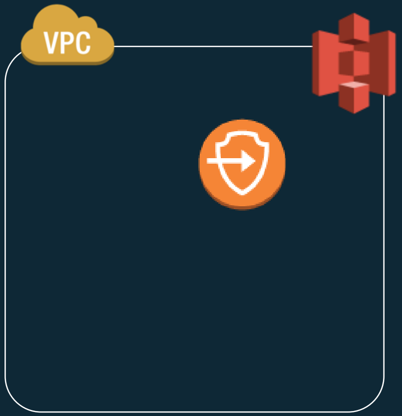
Map Enterprise Roles and Permissions

Identify

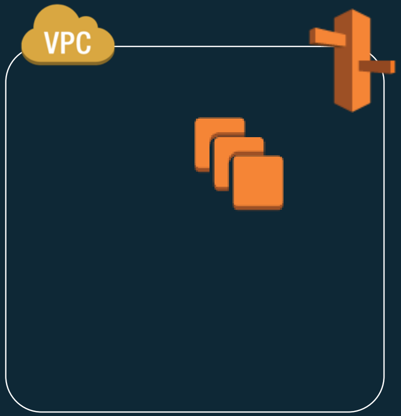
Actions and Conditions to Enforce Governance

Network Architecture considerations

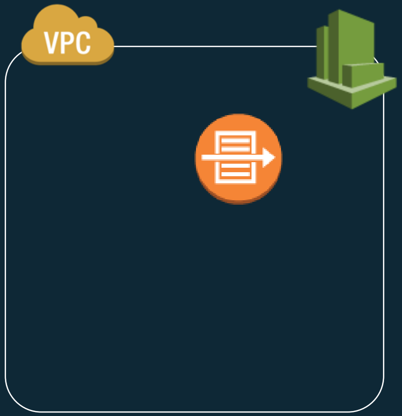
AWS Services in Your VPC



VPC Endpoints for Amazon S3

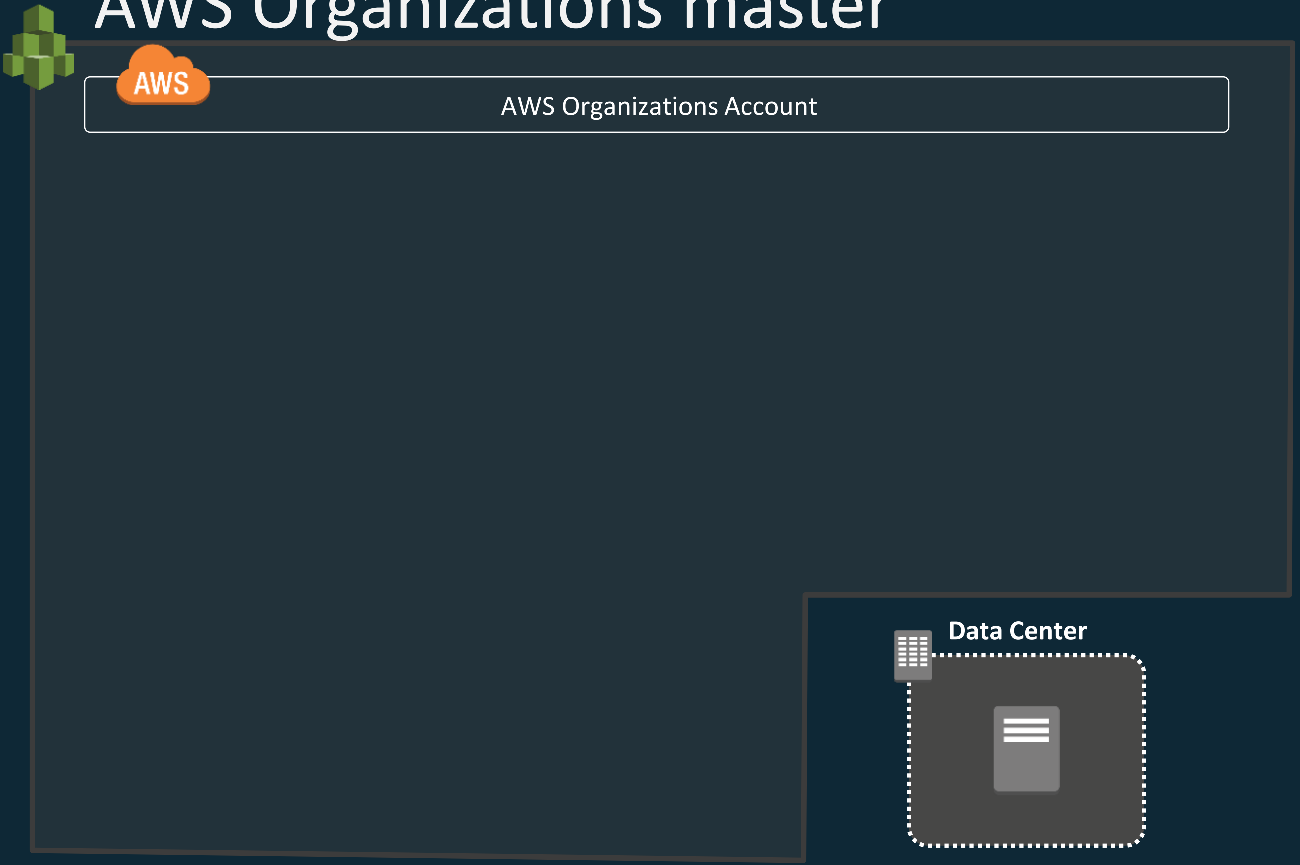


DNS in-VPC with Amazon Route 53



Logging VPC Traffic with VPC Flow Logs

AWS Organizations master



No connection to DC

Service control policies

Consolidated billing

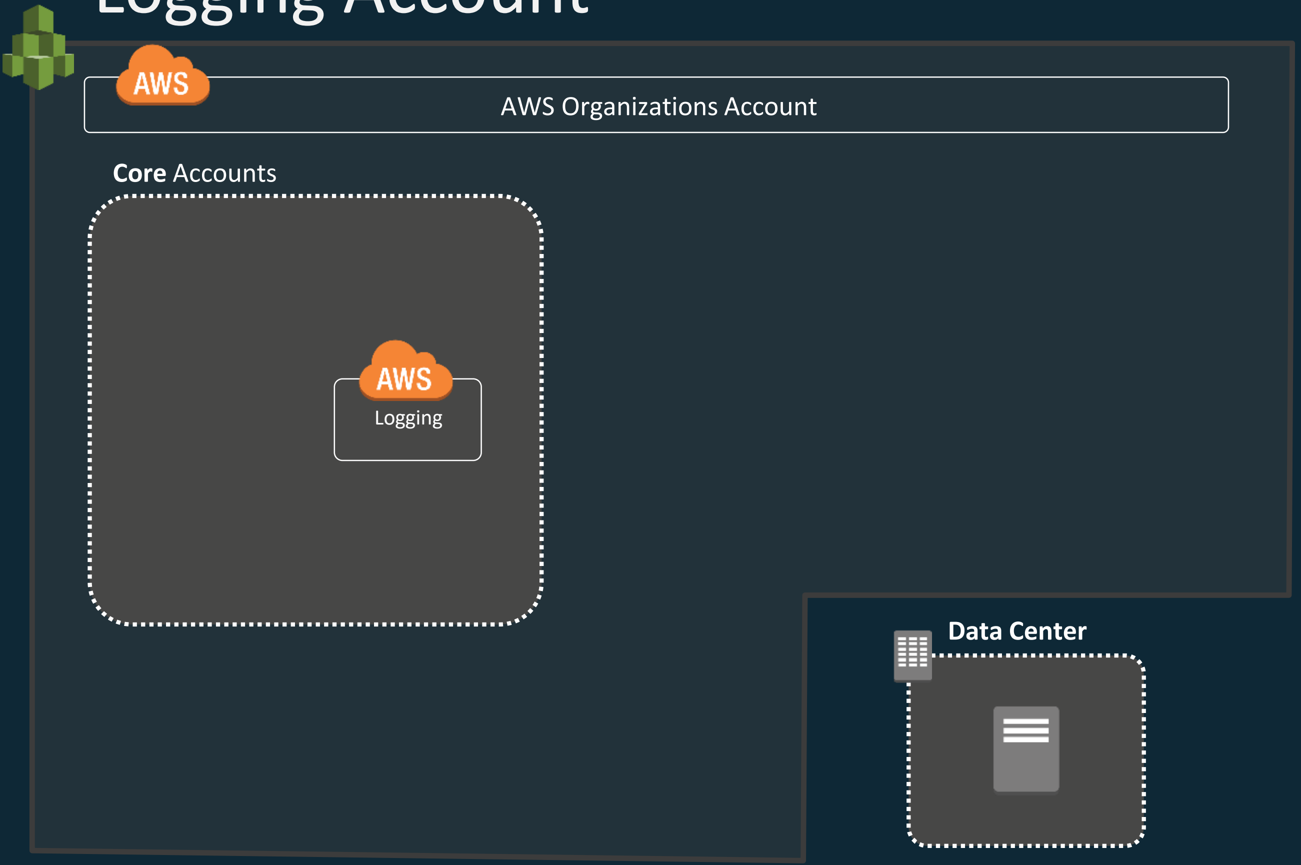
Volume discount

Minimal resources

Limited access

Limit Orgs role!

Logging Account



Versioned Amazon S3 bucket

- Restricted
- MFA delete

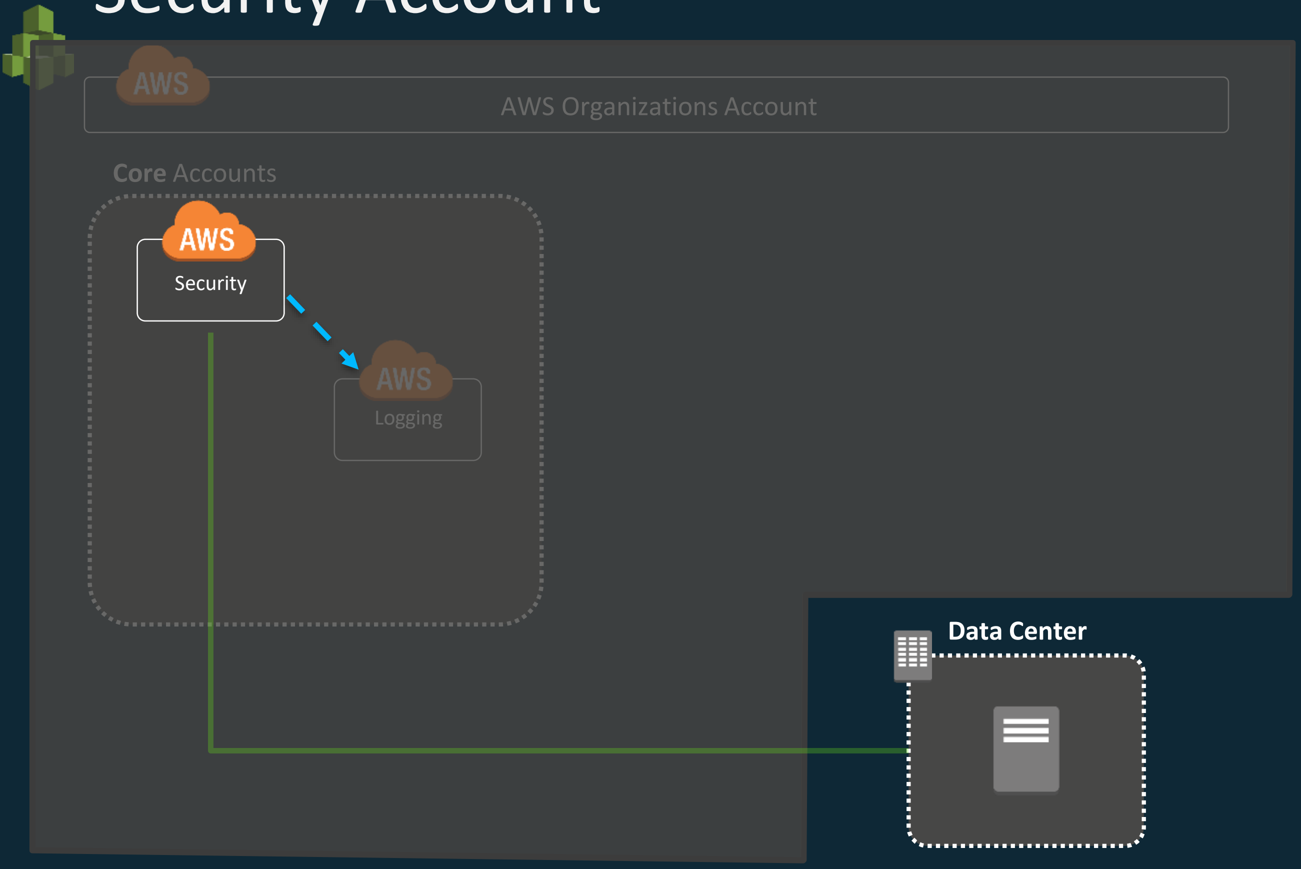
CloudTrail logs

Security logs

Single source of truth

Limited access

Security Account



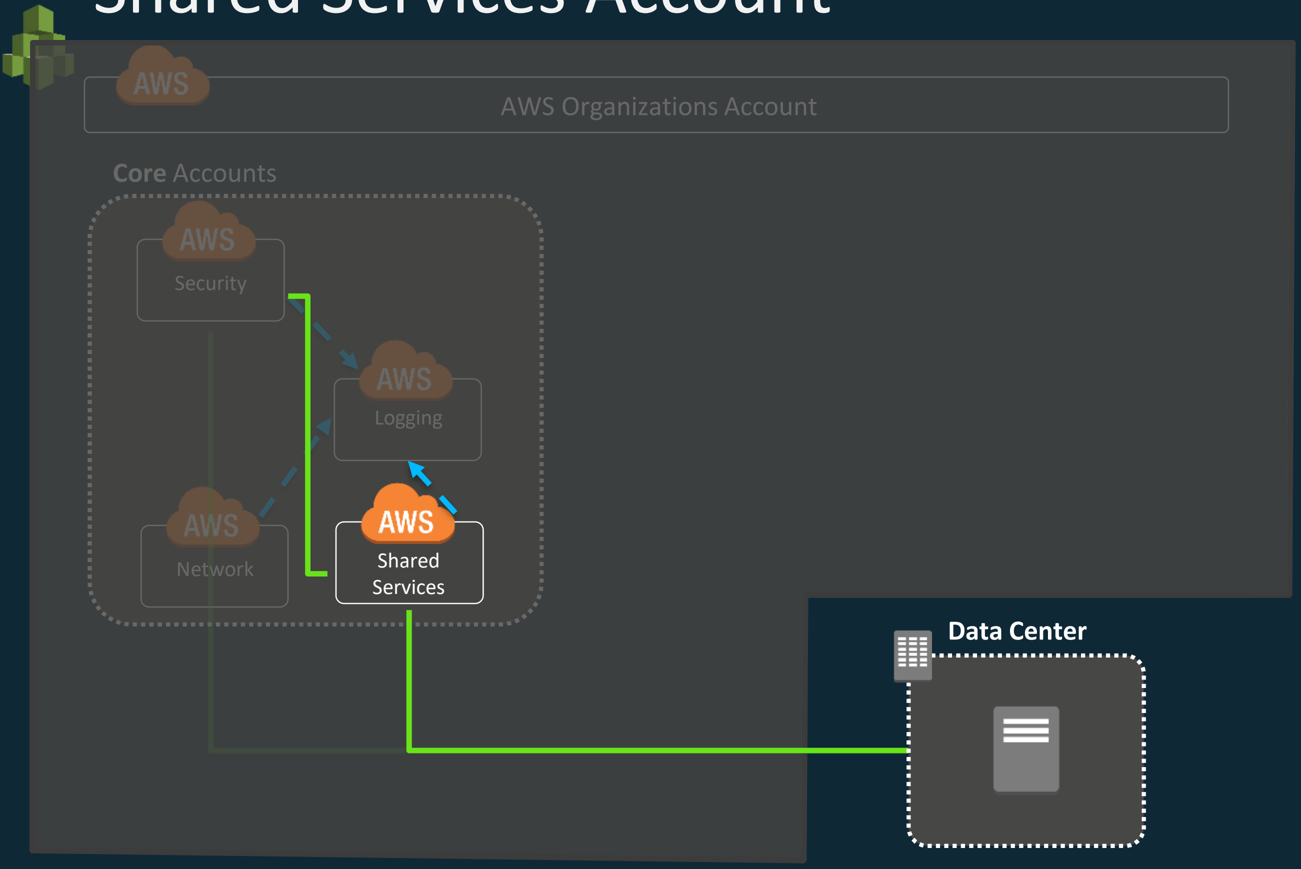
Optional data center connectivity

Security tools and audit

Cross-account read/write

Limited access

Shared Services Account



Connected to DC

LDAP/Active Directory

Shared Services VPC

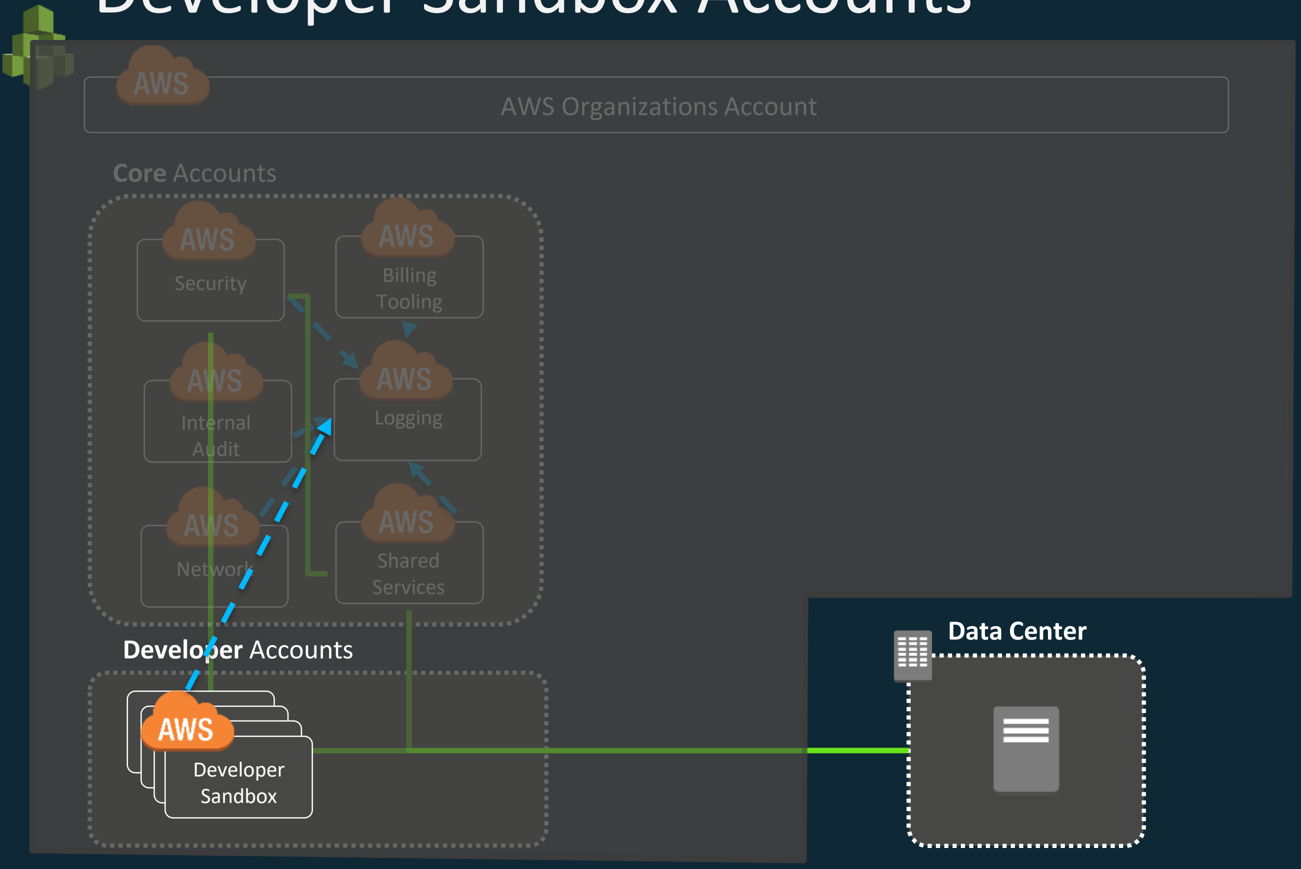
Deployment tools
Golden AMI
Pipeline

Scanning infrastructure
Inactive instances
Improper tags
Snapshot lifecycle

Monitoring

Limited access

Developer Sandbox Accounts



No connection to DC

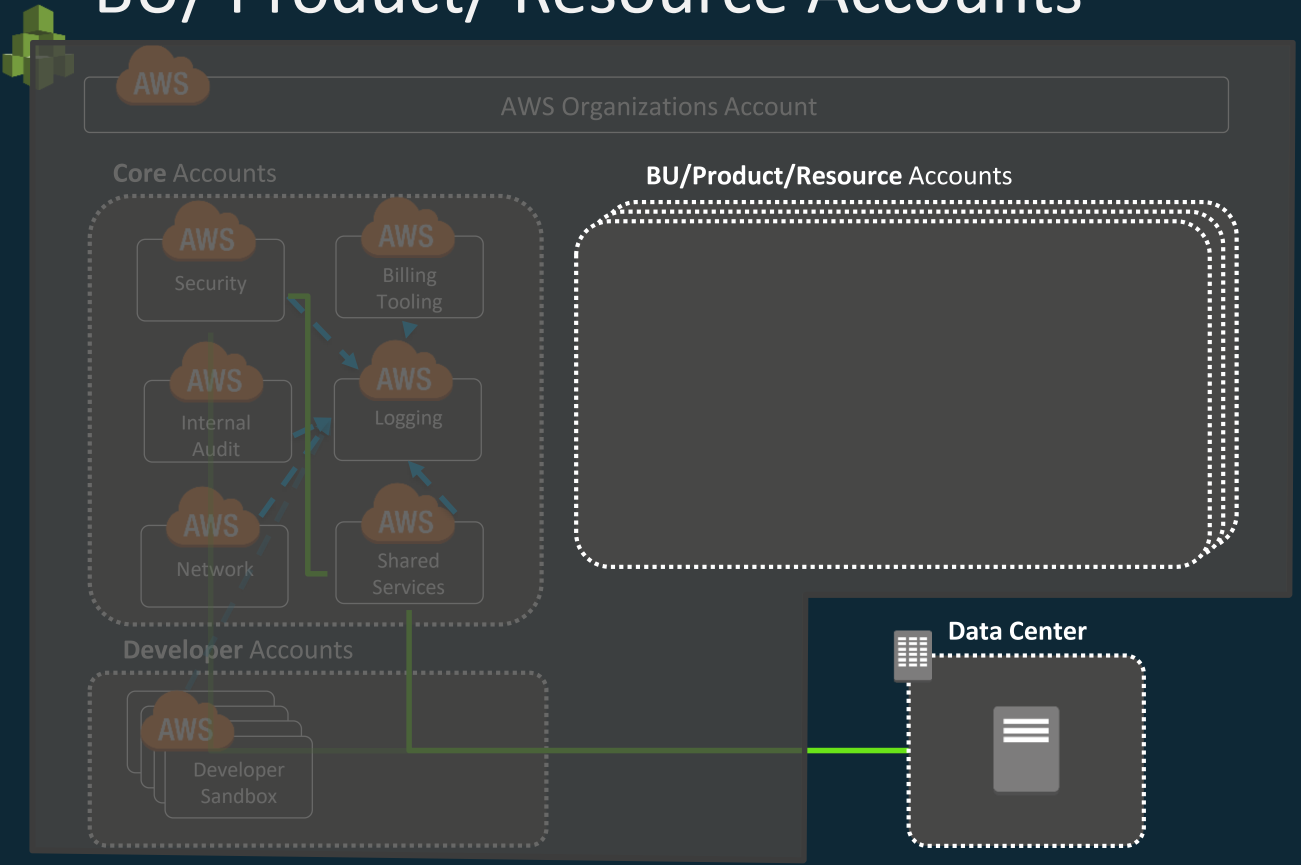
Innovation space

Fixed spending limit

Autonomous

Experimentation

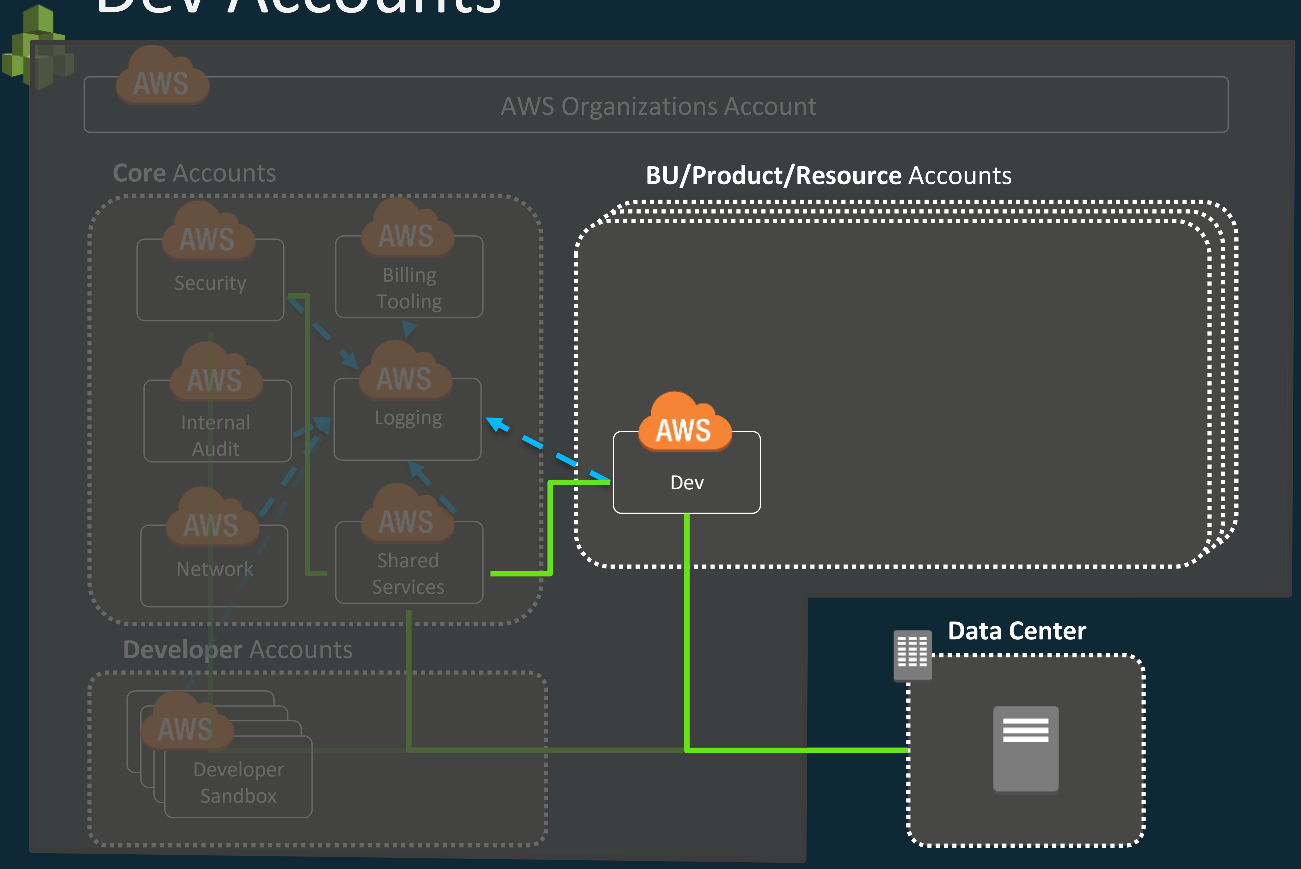
BU/ Product/ Resource Accounts



Based on level of needed isolation

Match your development lifecycle

Dev Accounts

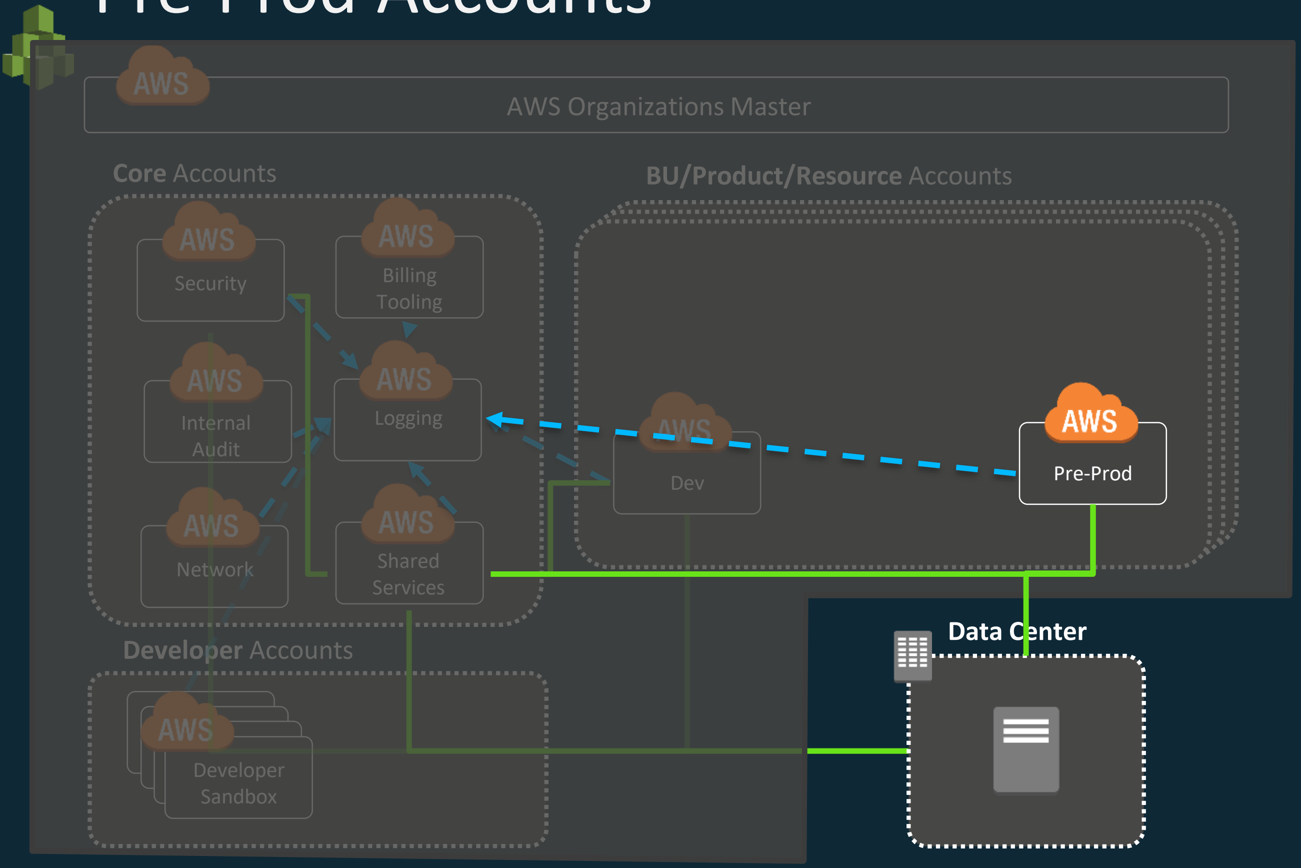


Develop and iterate quickly

Collaboration space

Stage of SDLC

Pre-Prod Accounts



Connected to DC

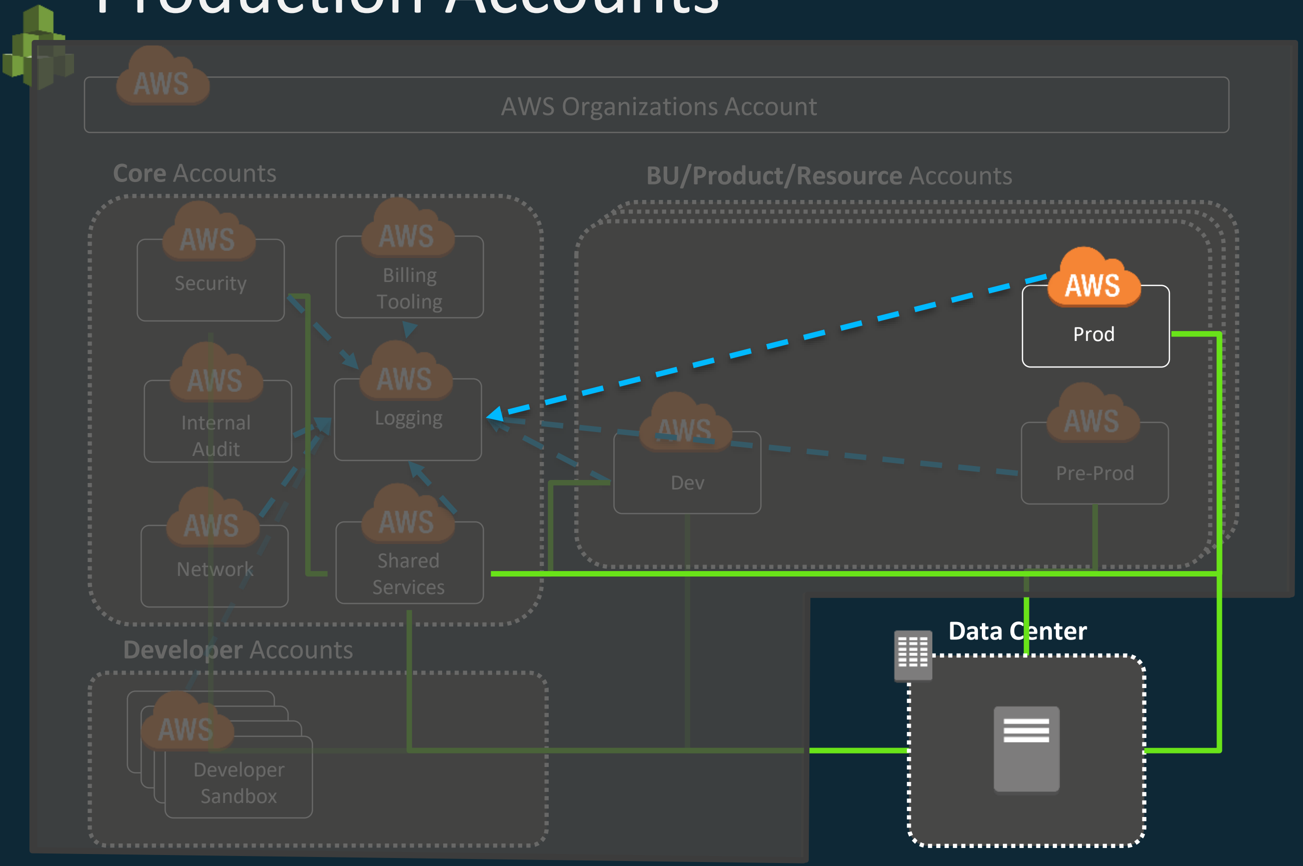
Production-like

Staging

QA

Automated deployments

Production Accounts



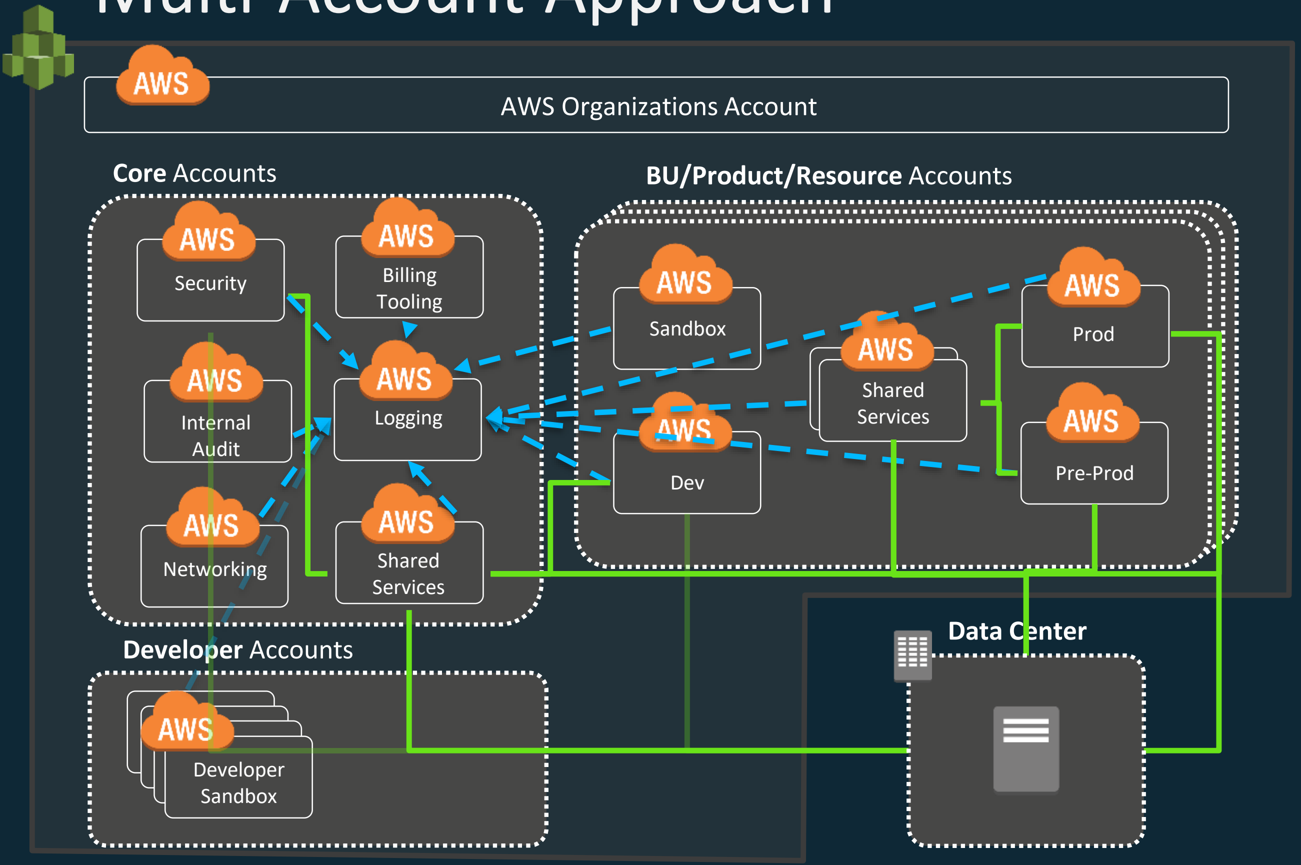
Connected to DC

Production applications

Promoted from Pre-Prod

Limited access

Multi-Account Approach



Orgs: Account management

Logging: Centralized logs

Security: AWS Config Rules, security tools

Shared services: Directory, DNS, limit monitoring

Billing Tooling: Cost monitoring

Sandbox: Experiments

Dev: Development

Pre-Prod: Staging

Prod: Production

Introducing the AWS Landing Zone solution

An automated, **easy-to-deploy solution** to help you set up new AWS environments and get started with running secure and scalable workloads on AWS

- 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
- Example initial multi-account structure based on common security, audit, and shared service requirements.
- An account vending machine which enables automated deployment of additional accounts with a set of security baselines

Identity & Access Management

- User account access managed through AWS SSO federation

Security & Governance

- Multiple accounts and defining cross account-roles allow implementation of separation of duties across all accounts
- Initial account security and AWS Config rules baseline
- Network baseline

AWS Landing Zone components

Initialization Template

- Easily deploy the AWS Landing Zone

Multi-Account implementation starting point

- Out-of-the-box Landing Zone implementation to get started quickly

Landing Zone update and configuration pipeline

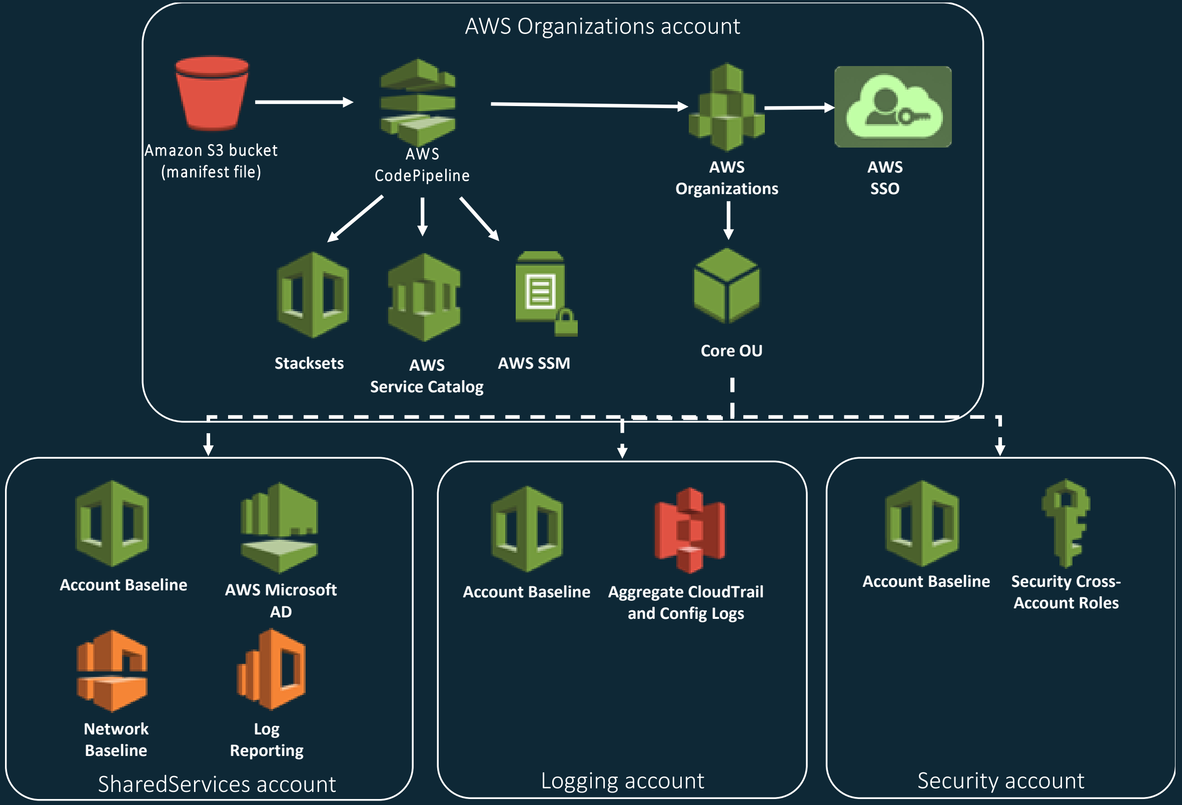
- Easily modify and extend the Landing Zone to grow with your Organization

Initialization Template

CloudFormation Template

- Creates Landing Zone deployment and configuration update pipeline
- Creates a customized AWS Landing Zone implementation package in your account
- Optionally deploys your customized AWS Landing Zone automatically

Multi-Account implementation



Organizations account:

Account Provisioning

Account Access (SSO)

Shared Services account:

Active Directory

Log Analytics

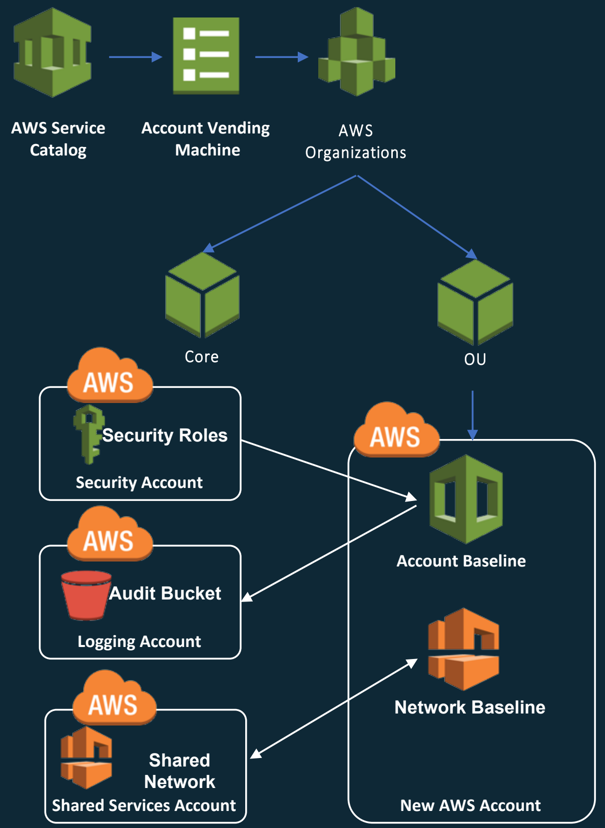
Logging account:

CloudTrail/Config logs

Security account:

Audit/Break-glass

Account Vending Machine implementation



- Account Vending Machine (AWS Service Catalog)
  - Account creation UI
  - Account Baseline Versioning
  - Launch Constraints
- Creates/Updates AWS Account
- Apply Account Baseline stack sets
- Create Network Baseline
- Apply account Security Control Policy

Account baseline

AWS CloudTrail

- Central Amazon S3 bucket and local AWS CloudWatch Logs

AWS Config

- 7 Config Rules (EBS/RDS/S3 encryption, IAM password policy, root MFA, S3 public read/write permissions)

IAM Password Policy

- User password change, password complexity/reuse/age/minimum length

Amazon VPC

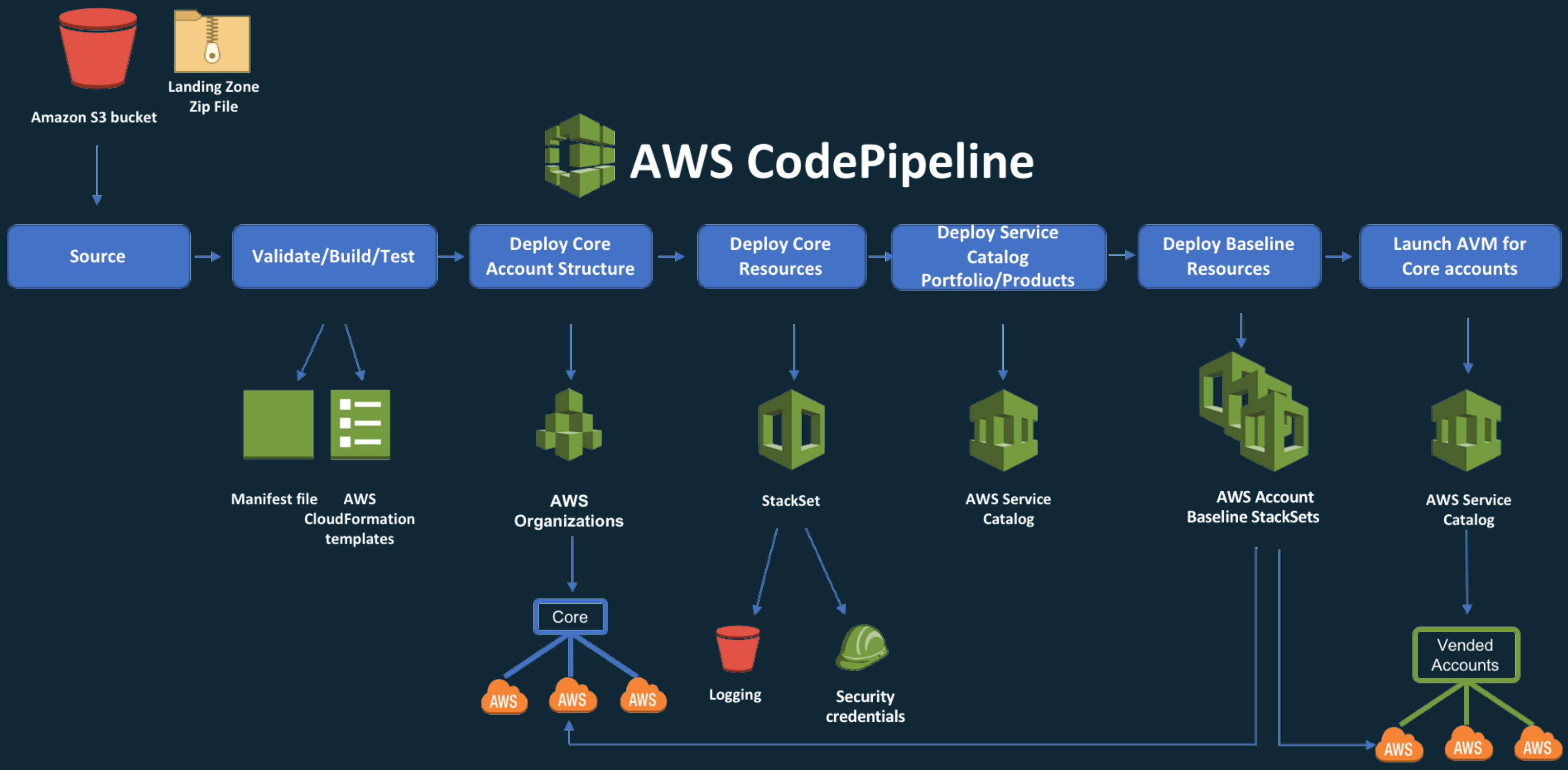
- Delete default VPC, (optional) create VPC

Optional product(s)

Centralized Logging

- Amazon Elasticsearch Service integration
- Kibana-based log reporting and analysis
  - AWS CloudTrail
  - Amazon VPC Flow Logs
  - Amazon CloudWatch Logs (Apache web server, Common Log Format, Space Delimited, JSON)

Deployment and configuration update pipeline



Benefits of the AWS Automated Landing Zone

Automated

Scalable

Self-Service

Guardrails
NOT Blockers

Auditable

Flexible

AWS Landing Zone pricing and availability

- No additional charge for the AWS Landing Zone solution
- Customer responsible for charges for services deployed (e.g., Amazon S3, AWS Config Service, AWS CloudTrail, etc.)
- Can be deployed in any region that has the underlying services available

Options for operating your 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**

Learn More

To learn more, please talk with your account team or visit:

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

Thank you