AWS Landing Zone – Design Considerations (pt2)

Amazon Web Services

24 July 2018

Design Considerations

Security Baseline

- The account, logging, data security and security notifications configurations deployed to core and future accounts

Networking Baseline

  - The networking construct when accounts are deployed that require a VPC

Security Baseline

Security Baseline

The Security Baseline is made up the following elements:

- Account Security
- Audit Logging
- Data Security
- Security Notification

Security Baseline

The Security Baseline is made up the following elements:

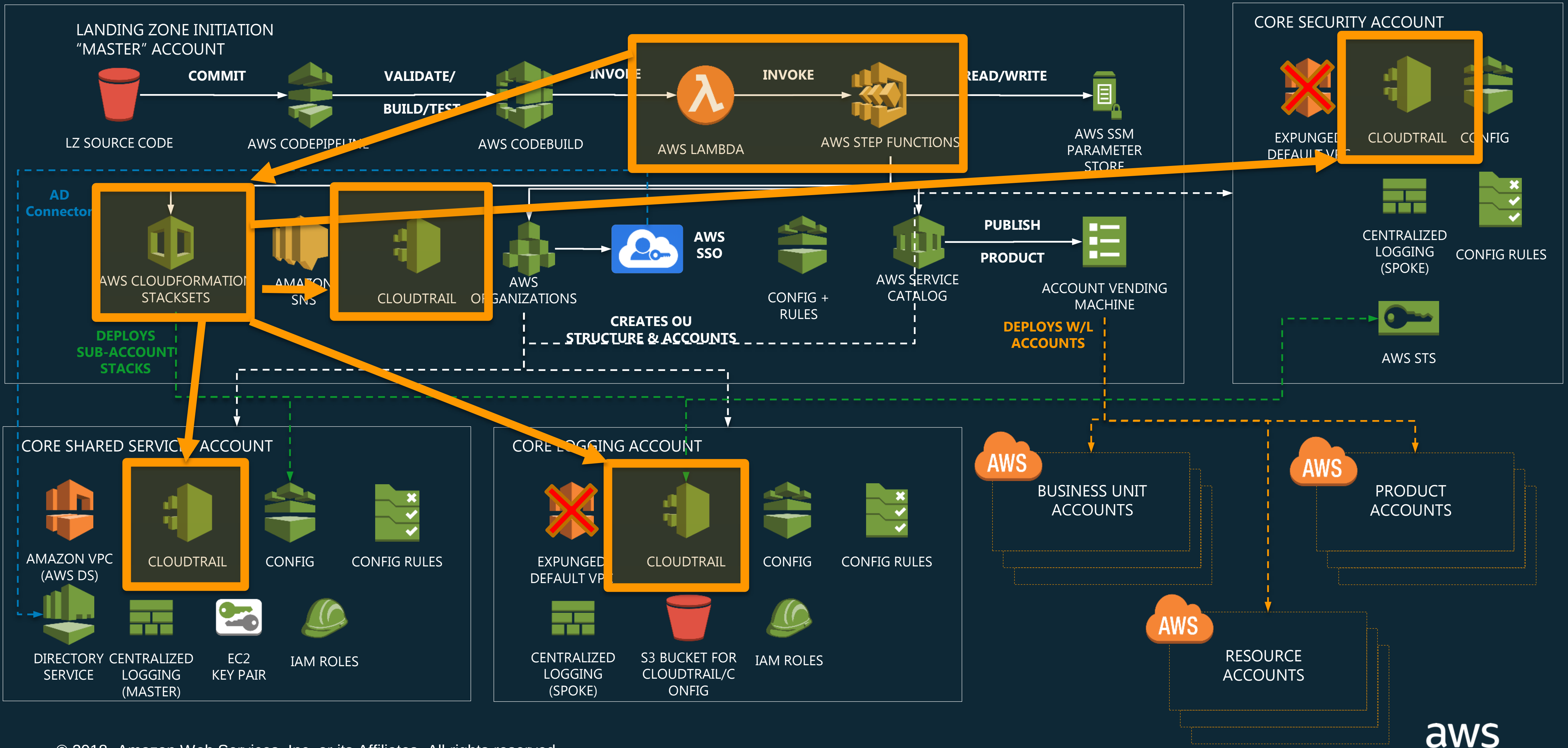
- Account Security
- Audit Logging
- Data Security
- Security Notification

Account Security

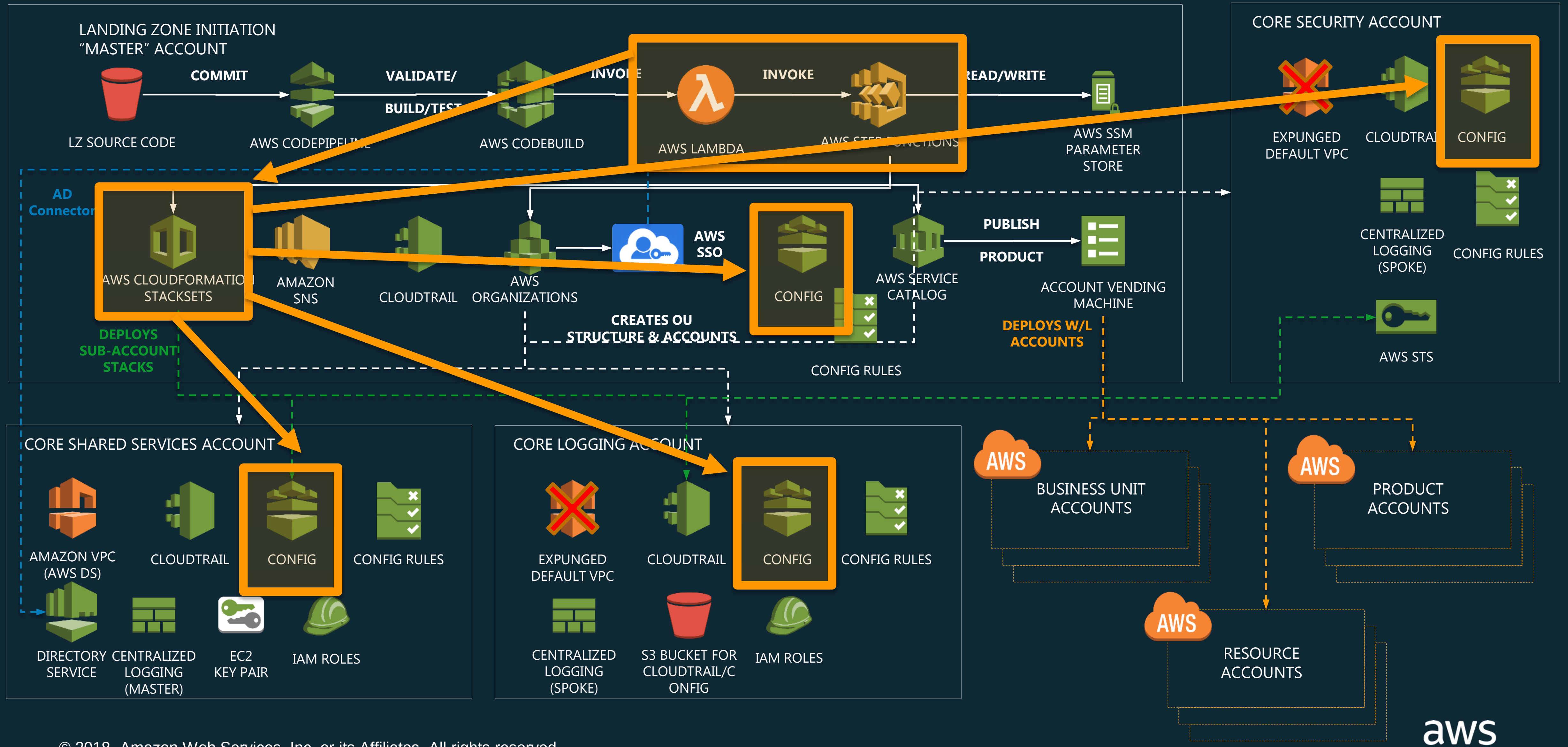
Editable default account configuration options when creating new accounts. Implements the following AWS Recommended Settings:

- AWS CloudTrail global trail configured with the following destinations
  - Remote trail logging to the Logging Account
  - CloudWatch Logs within the account for local support
- Enabling AWS Config and configuration logging to the Logging Account
- Configure IAM with complex password requirements
- Provision security account audit and administrative access
- Enable 9 Config rules (EBS/RDS/S3 encryption, IAM password policy, root MFA, S3 public read/write permissions, Insecure Security Group configurations)
- Configure account security SNS notifications

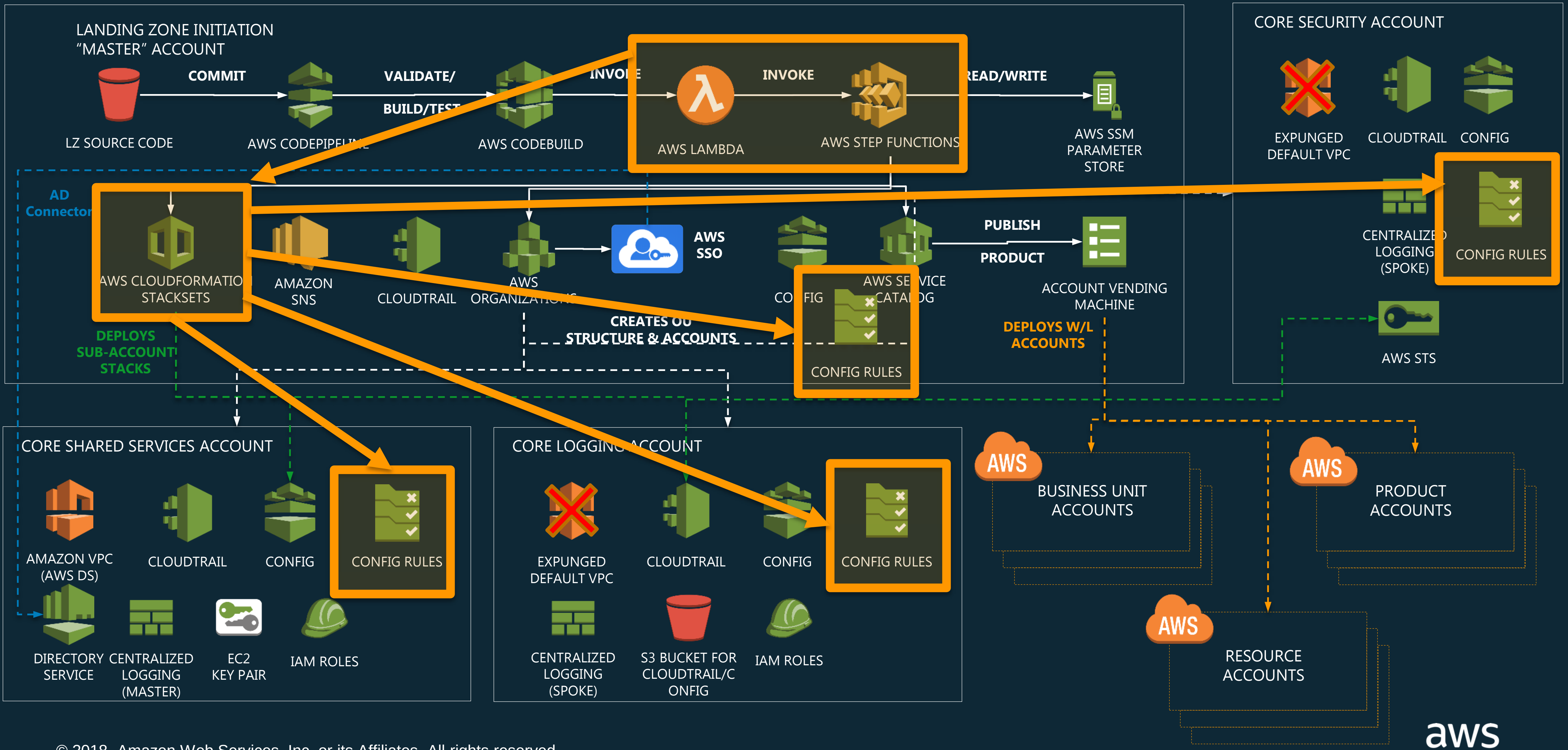
Account Security– CloudTrail



Account Security – AWS Config



Account Security – AWS Config Rules



Security Baseline

The Security Baseline is made up the following elements:

- Account Security
- Audit Logging
- Data Security
- Security Notification

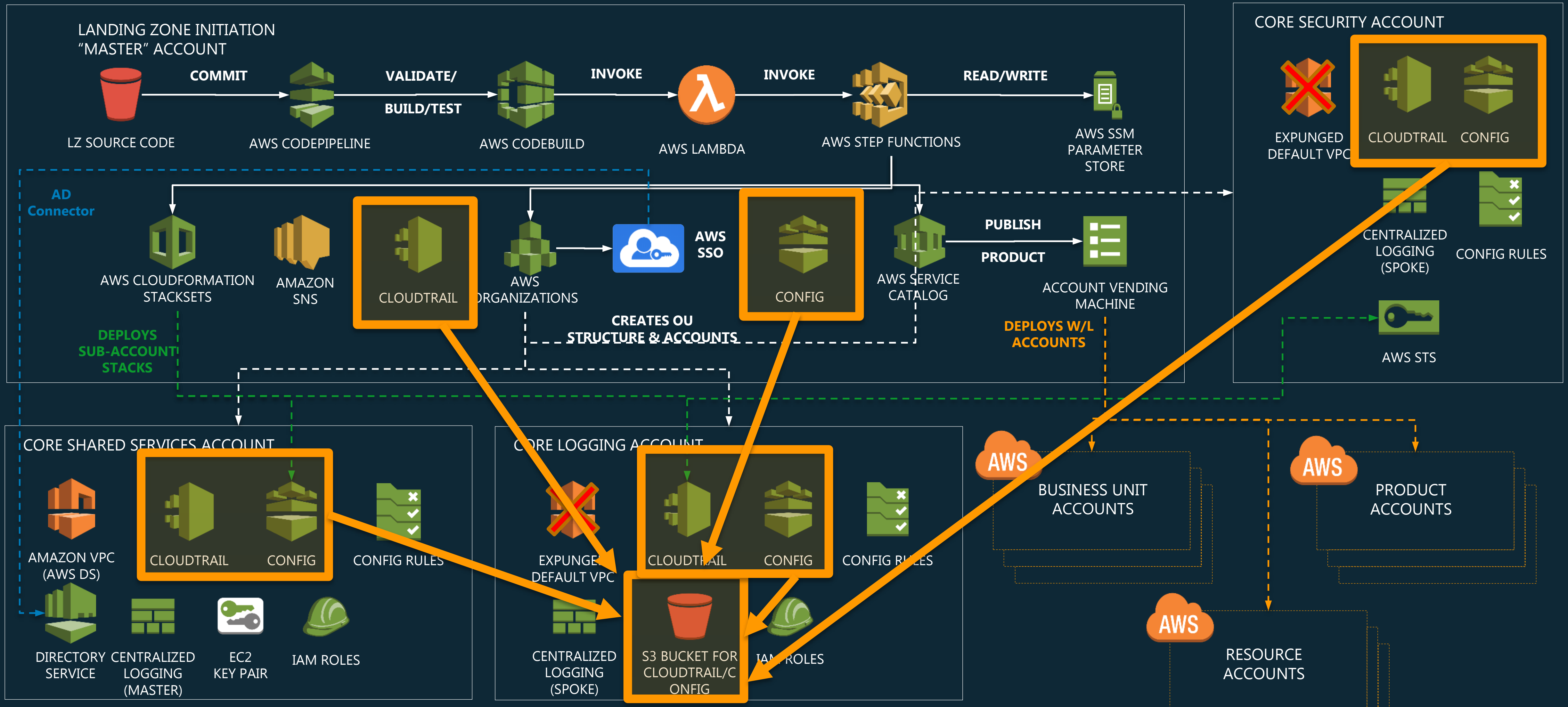
Security Logging

Provides customers with a centralized location for log storage.

- Centralised CloudTrail and Config storage into a single S3 bucket
- Enables bucket encryption and integrity checking.
- Also provides optional log analysis packages
- Initial focus on AWS-native, Cloudwatch Logs and Elasticsearch-based tooling

Integration with log partner products like Splunk, Sumo Logic, Loggly, Data Dog are also on the roadmap.

AWS Landing Zone – Security Logging



Security Baseline

The Security Baseline is made up the following elements:

- Account Security
- Audit Logging
- Data Security
- Security Notification

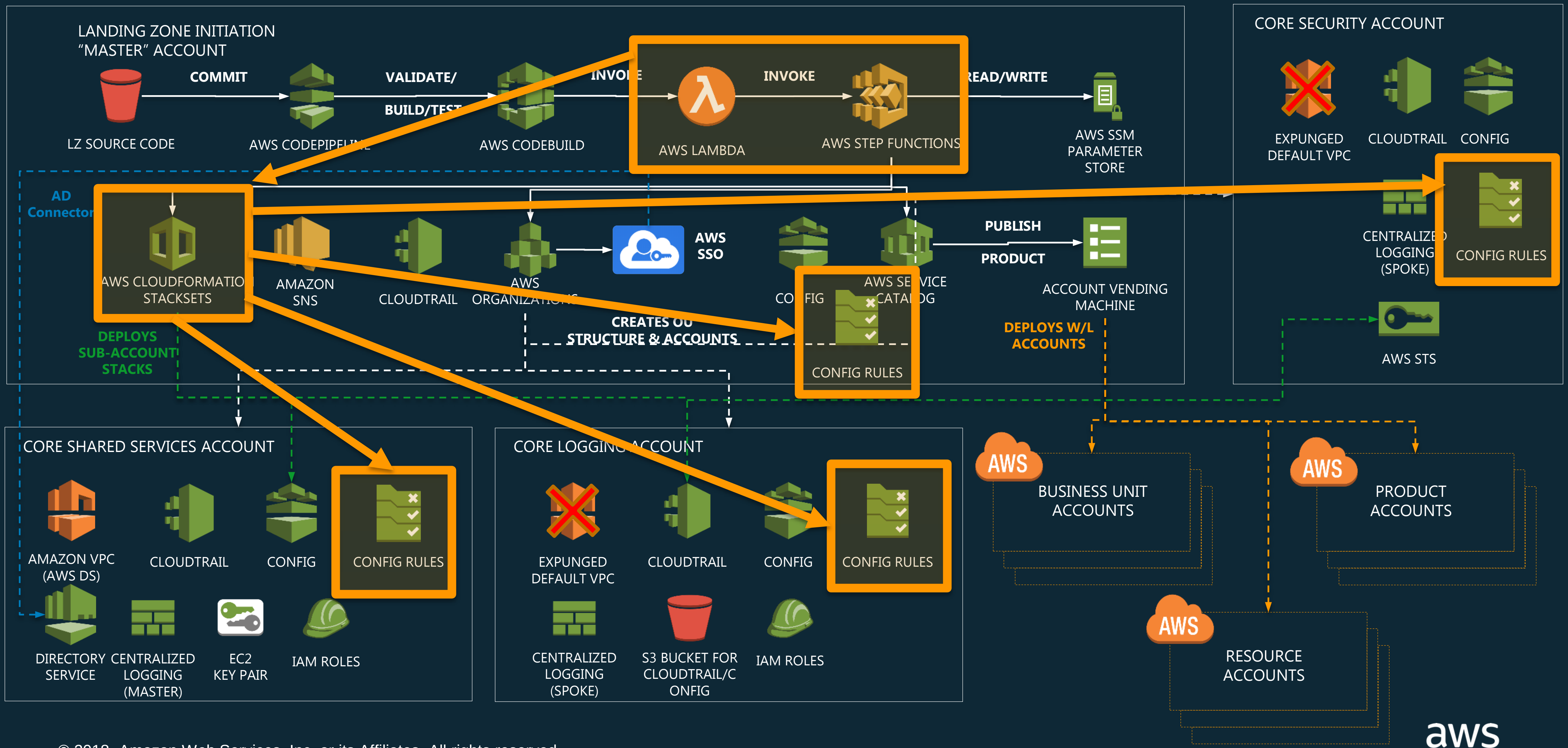
Data Security

Provide customers with the ability to configure data security services. Consists of the Following Capabilities:

- Enable and configure out-of-the-box data related Config Rules
  - EBS and S3 data encryption
  - Public S3 Buckets
- Enable additional Config Rules to suit your requirements

Integration with additional service capabilities like aggregated AWS Config Rules, Macie, GuardDuty, WAF managed firewall, etc. are on the roadmap.

Data Security Baseline – Additional Rules



Security Baseline

The Security Baseline is made up the following elements:

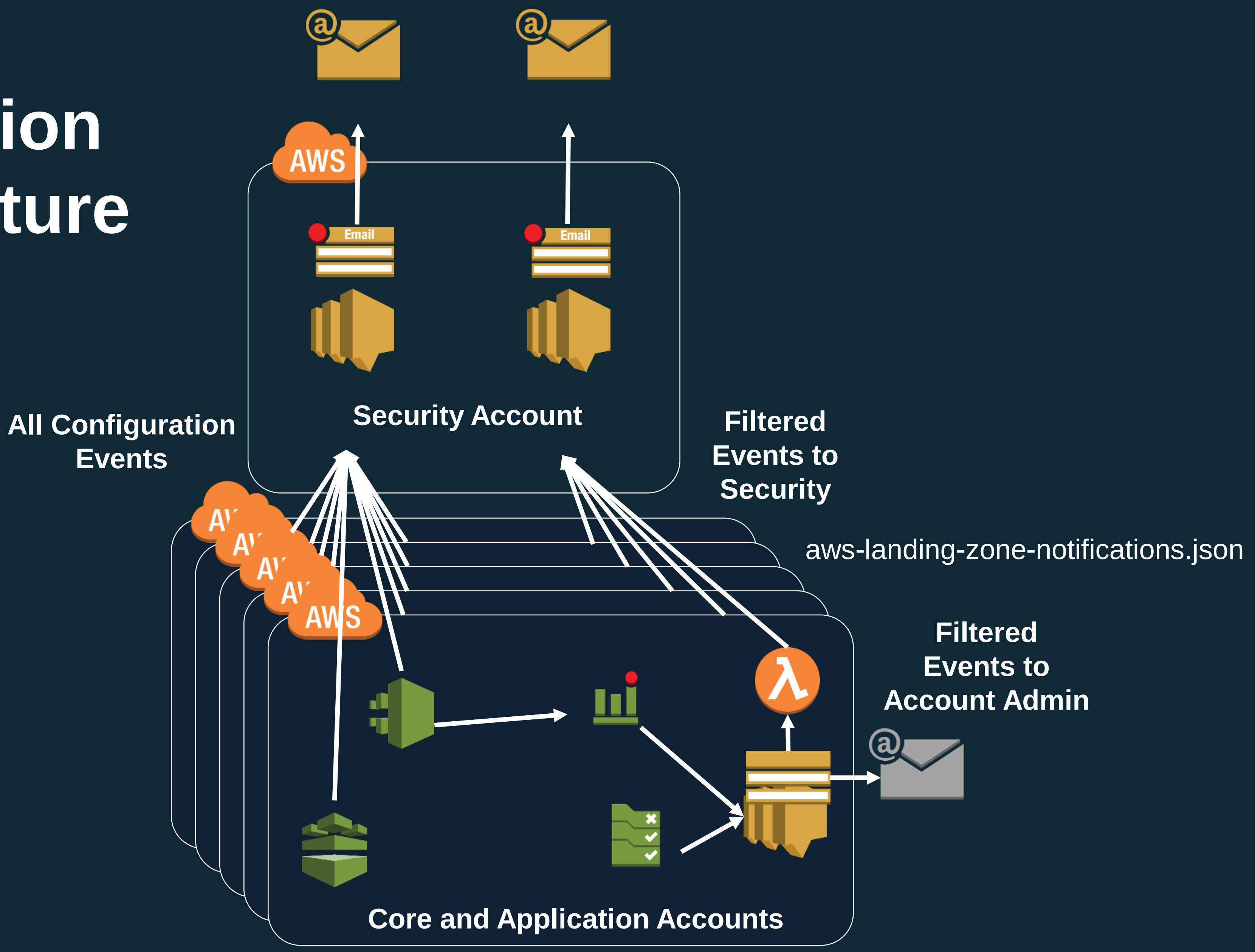
- Account Security
- Audit Logging
- Data Security
- Security Notification

Security Notifications

Two aggregate security notification Amazon SNS topics are also created in the Security Account:

- **AWS CloudTrail/Config Aggregation** - notifications from all managed accounts.
    - Integrate with configuration management / change control / security systems (automatic change notifications)
- **Specific CloudWatch Events** - aggregates security notifications from specific Amazon CloudWatch events.
- Initially send alerts to a local Amazon **SNS topic** > **Amazon Lambda subscription** > **Security account**.
- Allows local admins to subscribe to specific account notifications,
- Also aggregates ALL account notifications to a centralized security account.

Security Notification Architecture


AWS
Email
Email
All Configuration Events
Security Account
Filtered Events to Security
aws-landing-zone-notifications.json
AWS
Filtered Events to Account Admin
Core and Application Accounts

Networking Baseline

Networking Baseline

We cover two elements in this section:

- Networks (VPC Networking Options)
- Network Security

Networking Baseline

We cover two elements in this section:

- Networks (VPC Networking Options)
- Network Security

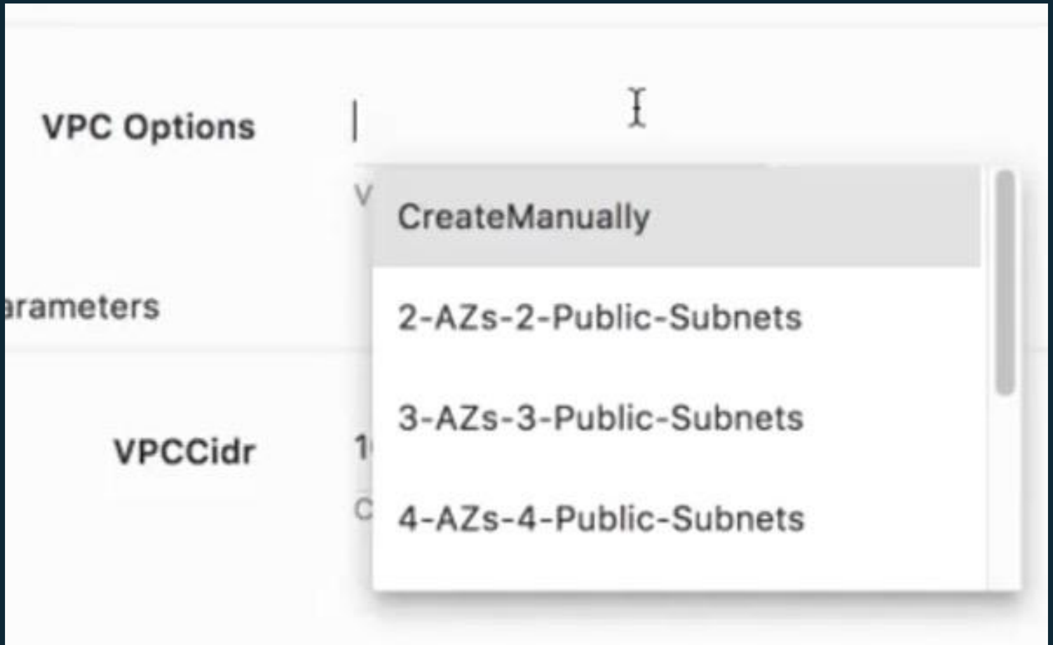
VPC Networking Options

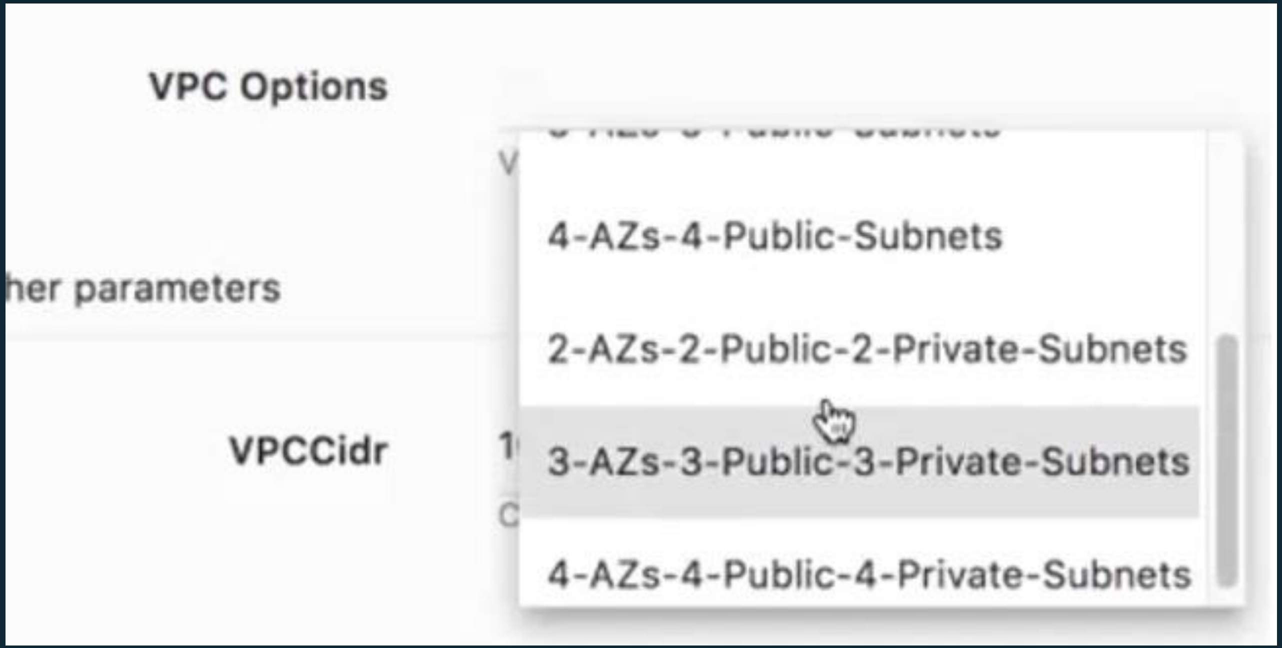
The customer can choose a network configuration based on commonly implemented, recommended network patterns.

- **Manual network creation:** Does not deploy a VPC automatically. Network creation will be delegated to users in the account.
- **Internet-facing network:** Implements a VPC consisting of public subnets and an IGW.
- **Internally-facing network:** Implements a VPC consisting of private subnets and a VGW.
- **2-tier hybrid network:** Implements a VPC consisting of public and private subnets, NAT gateways, IGW, and VGW.
- **3-tier hybrid network:** Implements a VPC consisting of public, private, and routing isolated subnets, NAT gateways, IGW, and VGW

Member Account - VPC Selection

Multiple VPC Configuration Options




VPC Options
4-AZs-4-Public-Subnets
2-AZs-2-Public-2-Private-Subnets
3-AZs-3-Public-3-Private-Subnets
4-AZs-4-Public-4-Private-Subnets
her parameters
VPCCidr

VPC Networking Options – Cont'd

Other items of note…

- Users can select whether to enable VPC Peering to the Shared Services VPC as part of the AVM deployment
- There is custom VPC Peering Resource that handles both local and Cross-Region VPC Peering
- CIDR Blocks are evenly distributed across the number of subnets required to create the selected VPC
- Subnets CIDRs are identified using a CFN Custom Resources

Networking Baseline

We cover two elements in this section:

- Networks (VPCs)
- Network Security

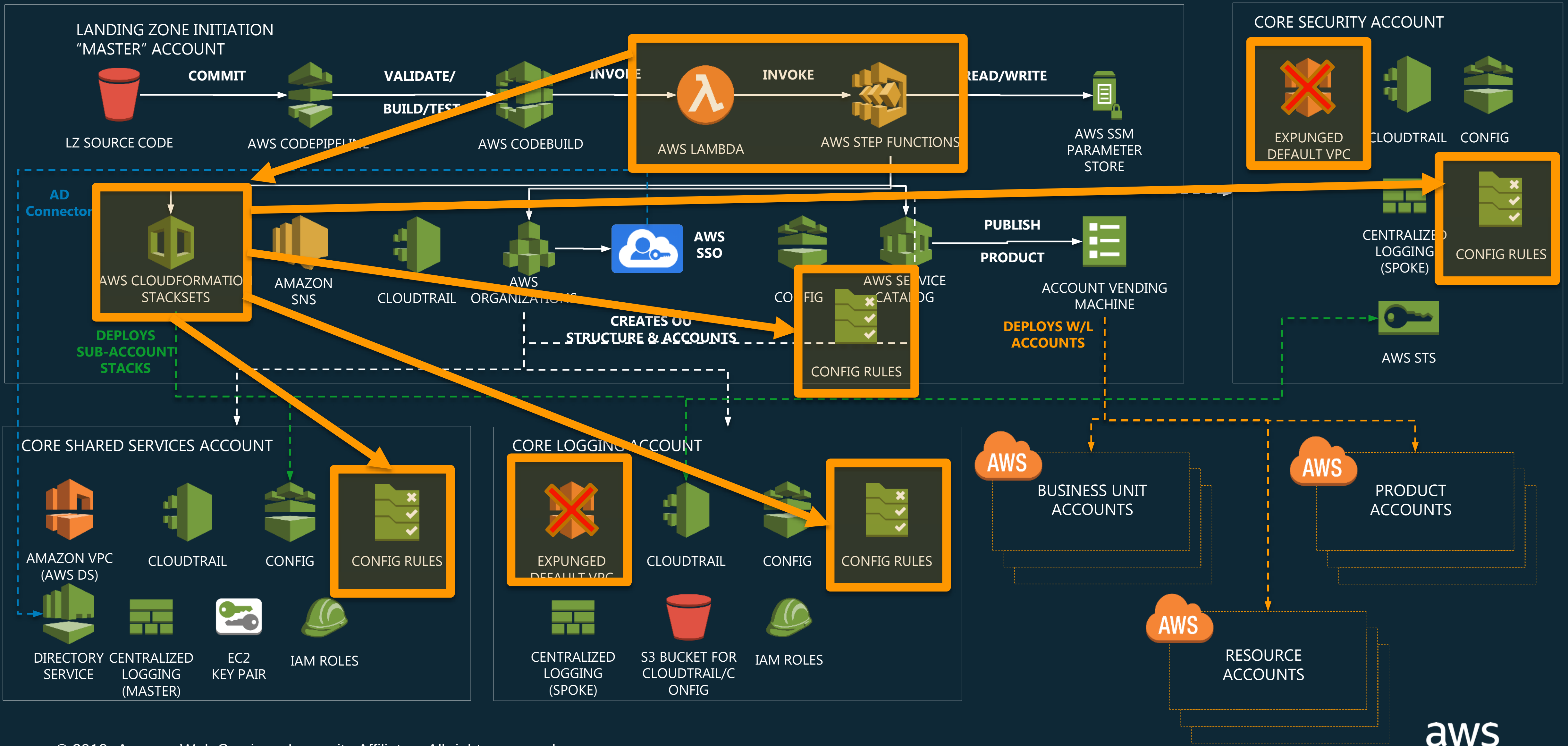
Network Security

Allow customers to specify default network security options for all new accounts. Initial configuration consists of the following:

- Delete the default VPC in all regions
- Enable Config Rules for monitoring insecure Security Group configurations
- After creating a VPC, enable VPC Flow Logs

Additional network security features, such as automated integration with network partner products like Aviatrix or Palo Alto Networks, and determining ways to incorporate additional services (e.g. AWS WAF) are on the Landing Zone roadmap

Data Security Baseline – Additional Rules



What’s next?

- ✓ Module 1 / Lab 1 – Initial Thought Process / Deploy Example Landing Zone
- ✓ Module 2 / Lab 2 – Design Considerations (pt1) / Review Deployment
- ✓ Module 3 - Design Considerations (pt2)
- ○ Module 4 - Design Considerations (pt3)
  - Lab 3 - Configure AD and SSO
  - Lab 4 - Deploy a Member Account
  - Lab 5 - Deploy Centralised Logging Hub
- ○ Module 5 – Extending the Landing Zone
- ○ Lab 6 – Configure Centralised Logging Spoke and new Config Rule