



AWS Landing Zone – Design Considerations (pt3)

Amazon Web Services

24 July 2018

Design Considerations

User Access

- Combination of automated and manual steps for user access federation

Account Vending Machine

- The Service Catalog elements that support account creation and baselining

Centralized Logging

- The optional component enabling centralized log analysis

User Access

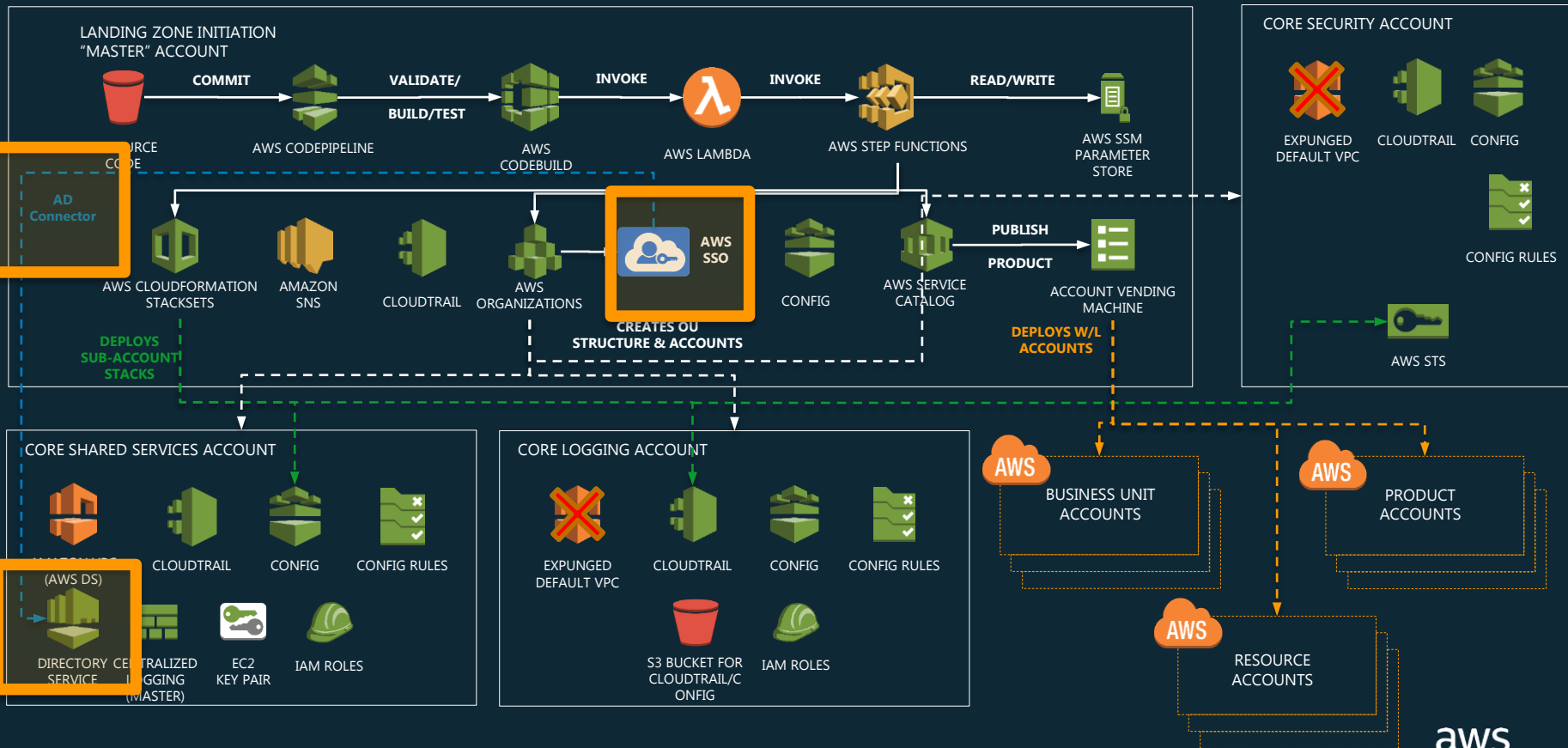
User Access with AWS Single Sign-On (SSO):

A Single Sign-On mechanism is included as part of the base Example Implementation:

Components that enable this functionality:

- AWS SSO Endpoint
- Active Directory Connector
- AWS Directory Service

AWS Landing Zone – AD and SSO



User Access with AWS Single Sign-On (SSO):

Components that enable this functionality:

- **AWS SSO Endpoint** – created to federate user access to accounts
 - Currently US East (N.Virginia) only, however it can federate into any AWS account in any region
- **Active Directory Connector** – gateway for requests from on-prem or another AWS account to Microsoft Active Directory.
 - Leverages AD Connector – to connect to SSO in the organizations account to AWS Directory Service in Shared Services account
 - Leverages VPC peering - the AD connector runs over.

User Access with AWS Single Sign-On (SSO):

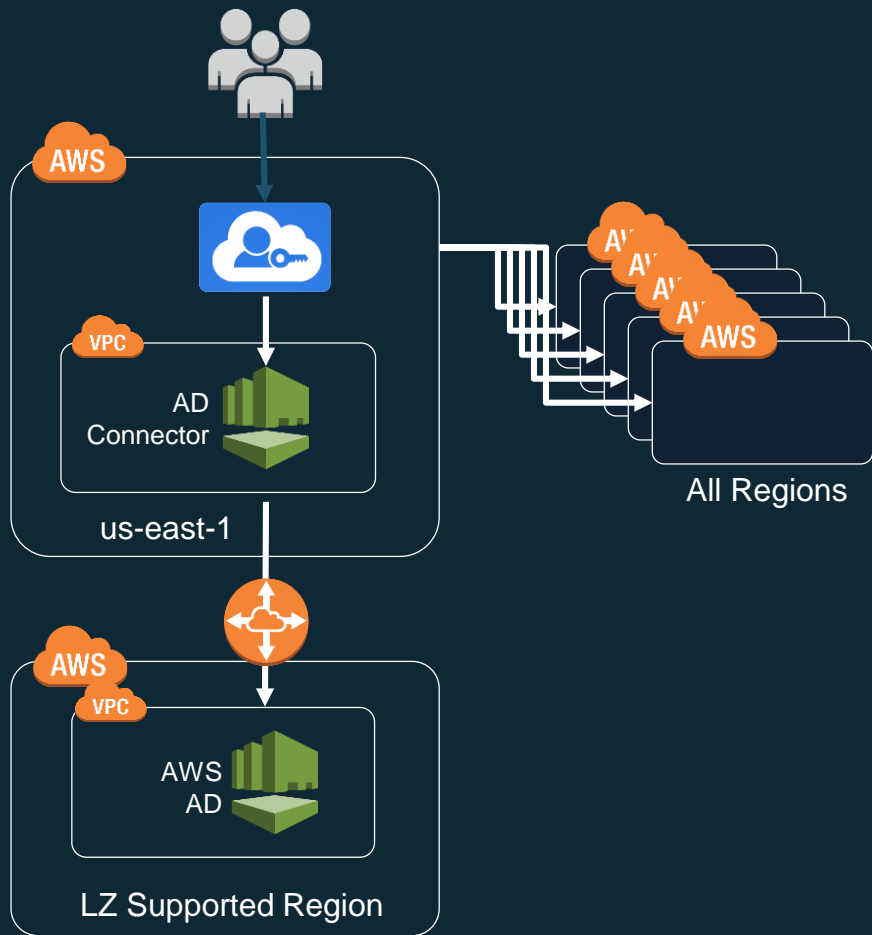
Components that enable this functionality:

- **AWS Directory Service** – Provides access SSO access to the customer's user directory.
 - AD DCs – deployed into the Shared Services account
 - This separates AD user management from LZ management functions
 - Makes it easier to Leverage AD for Apps and OS management if required.

User Access with AWS Single Sign-On (SSO):

Map **AD groups** to defined **permissions**.

Grant access to one AWS account, an OU, or the entire Organization.

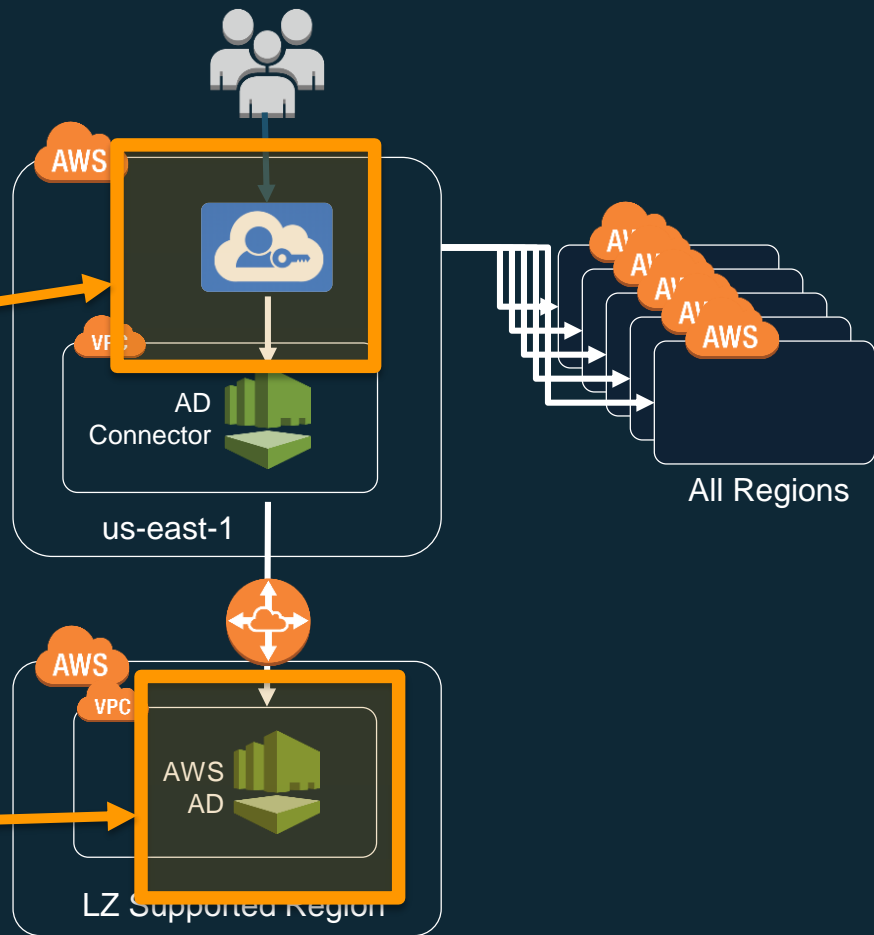


Lab 3 – Create AD User and Configure AWS SSO

User Access with AWS Single Sign-On (SSO):

**Configure
AWS SSO**

**Configure a User
in AD**



Account Vending Machine (AVM)

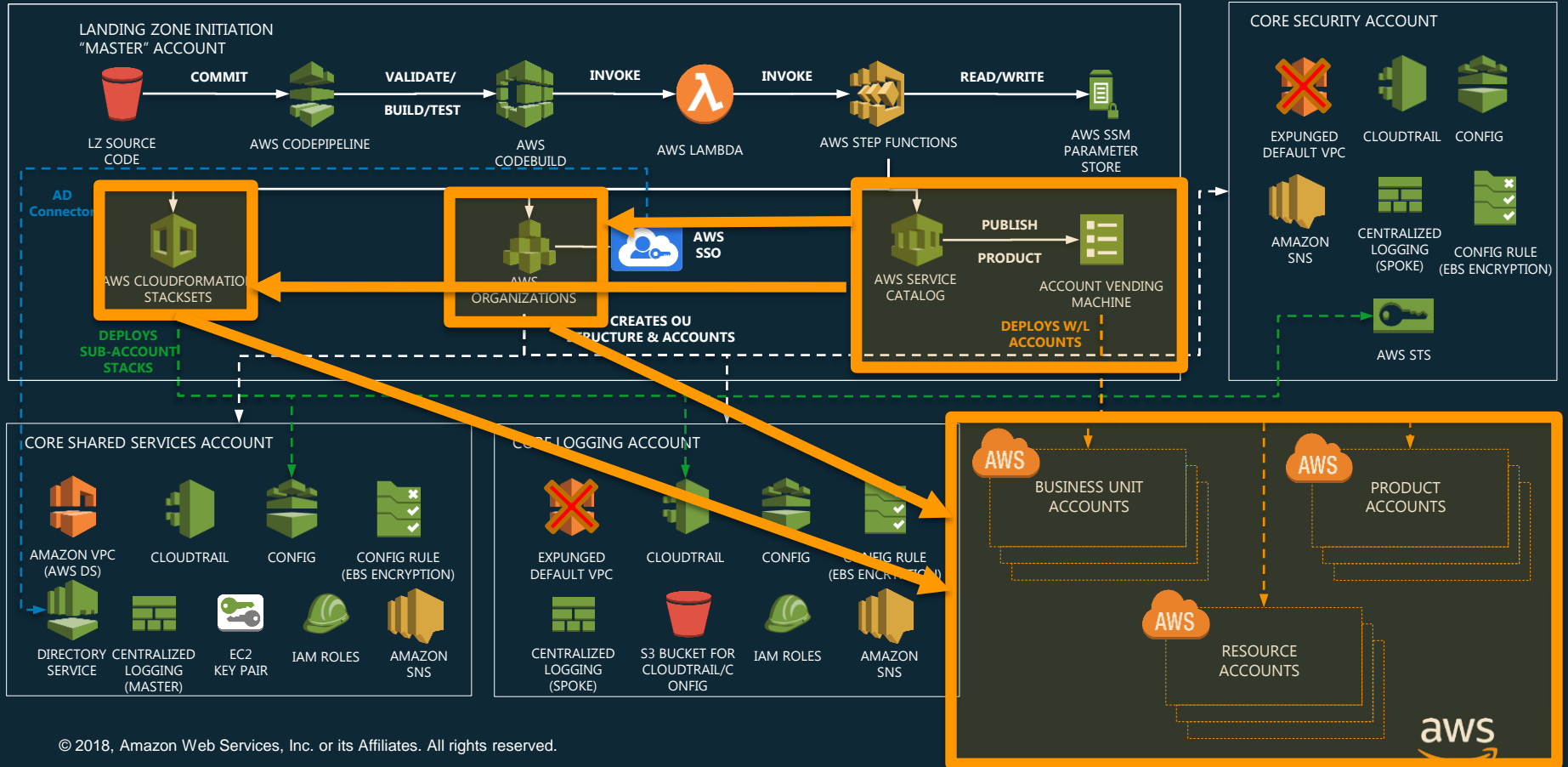
The Account Vending Machine (AVM)

End User creation of new Account:

This a Service Catalog product enabling end user self-service options:

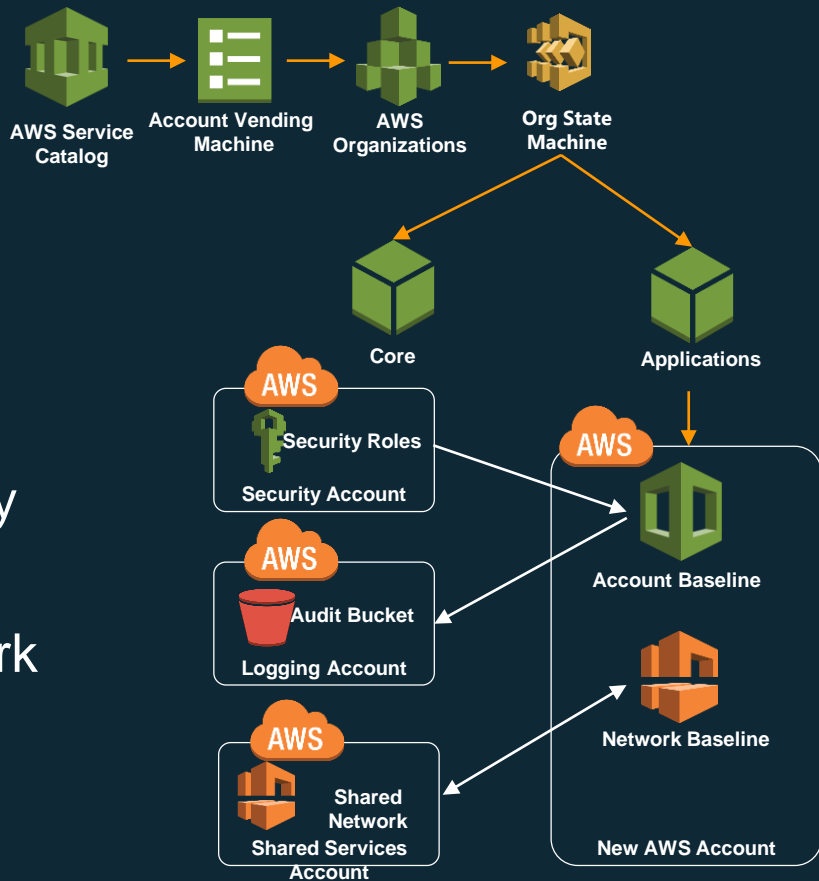
- Provides options for the requester to specify an existing or new
- Offers the choice of type of network to create
- Makes AWS Organizations API calls to create the account
- Applies the Security Baseline

AVM - Member Account Creation



Account Vending Machine (AVM) Architecture

- Service Catalog Product
- Creates New accounts
- New or Existing OUs
- Auto-Baselined with the Security Baseline
- Deploy with a predefined network



Member Account Creation – a walkthrough

The screenshot displays the AWS Service Catalog interface. The top section, 'Products list', features a search bar with the placeholder 'Ex. Name' and a 'Sort by' dropdown set to 'Product name'. Below this is a table with columns: Product name, Vendor, Owner, Description, and Support description. A red 'LAUNCH PRODUCT' button is positioned over the table. The bottom section, 'Provisioning', shows a 'Versions (1)' dropdown and a table with columns: Versions, Created time, and Description. The table contains one entry for 'AWS-Landing-Zone-Account-...'.

Product name	Vendor	Owner	Description	Support description
Account Ve...				led

LAUNCH PRODUCT

▼ Versions (1)

By name	Created time	Description
AWS-Landing-Zone-Account-...	Mar 20th 2018 17:12:43 UT...	This product will launch a new baseline account in a new or existing org unit.

Member Account Creation – a walkthrough (cont.)

Product Version

Specify a provisioned product name and then select the version that describes the provisioned product that you want to create.

Provisioned product

A provisioned product is a collection of related resources that you provision and update as a single unit.

Name* Workload1Account

Product Version

Version*

By name <input type="text"/>				
	Versions ▾	Provided by ▾	Created time ▾	Description ▾
<input checked="" type="radio"/>	AWS-Landing-Zone-Ac...	AWS Solutions	Mar 20th 2018 17:12:4...	This product will launch a new baseline acco...

***Required**

CANCEL **NEXT**

Member Account Creation – a walkthrough (cont.)

Parameters

Specify values or use the default values for the parameters.

OU Setup

Organization Unit	
State	Existing
Destination OU ID	New

Organization Unit	New
State	'New': OU will be created. 'Existing'
Destination OU ID	ID for the existing Org Unit (Option
New OU Name	<New OU Name Here> Name for the new Org Unit

New
OU
or
Existing
OU

Account Setup

New Account Name	MyApplication1 Name for the new account
New Account Email	billing@org.com Email for the new account
New Account ID	/org/member/new_acco
Parameter Name	Parameter key to store new member account ID. (update 'new-account-name')

Destination OU ID	Development
New OU Name	Development Workload1 Workload 1 wdtest

Member Account Creation – a walkthrough (cont.)

Notifications

☒ Enable provisioned product event notifications to be streamed to an Amazon SNS topic.

- ☒ Create a new topic
- ☐ Choose a topic from your account
- ☐ Choose a topic from another account

Topic Name*

Enter topic name

NEXT

>

LAUNCH

The Account Vending Machine Architecture

AVM Permissions:

- Grants AWS Service Catalog administrators permissions to create and manage AWS Landing Zone products
- Grants end user permissions to launch and manage AVM products.
- Uses launch constraints to allow end users to be able to create new accounts without requiring account administrator permissions.
- New account provisioning access can new accounts can be granted either:
 - directly to end-users using AWS Service Catalog
 - by creation API invoked by another request management system.

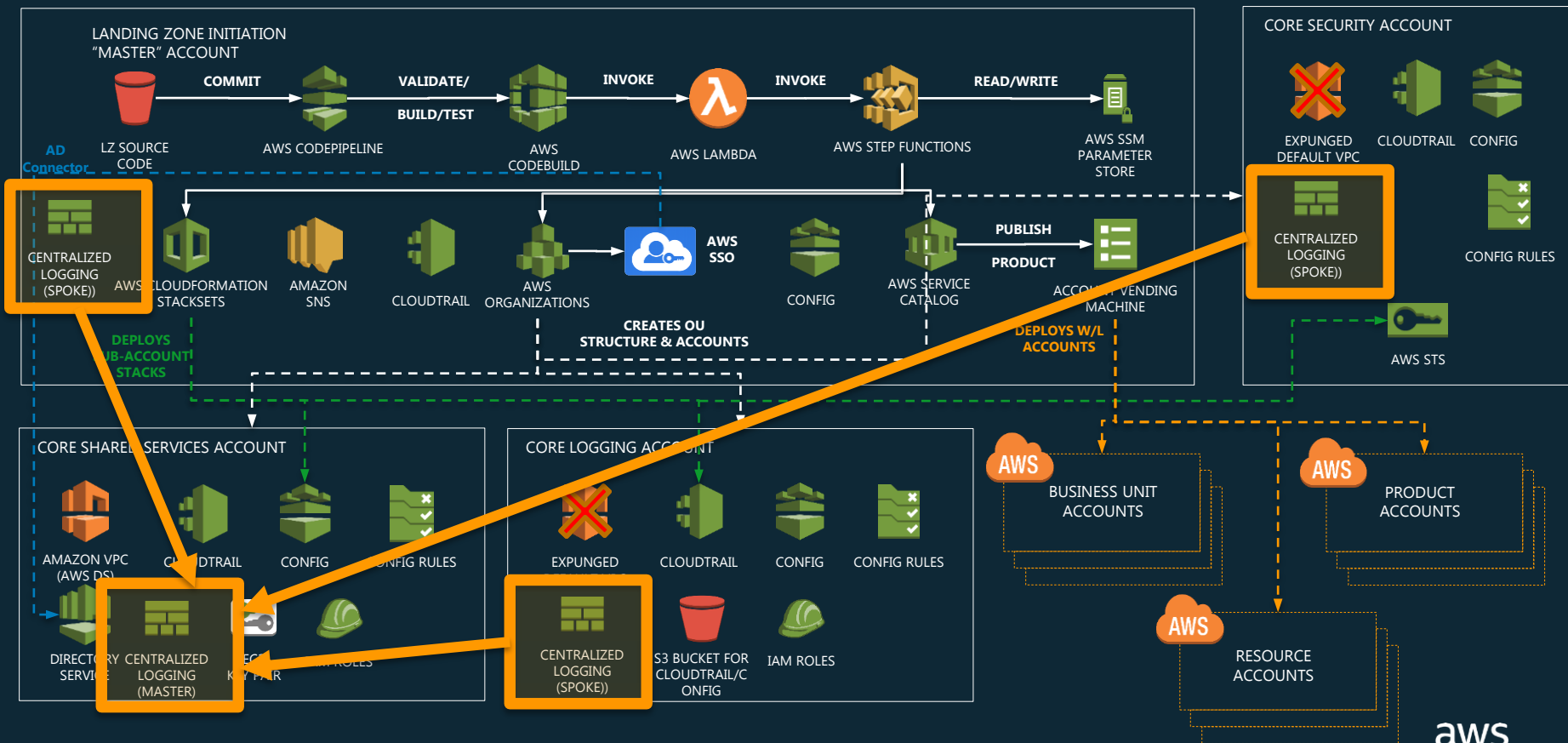
Centralized Logging (Optional Core Product)

Why Centralized Logging Solution?

Comprehensive log management and analysis strategy is mission critical

- Understand relationship between operational, security and change management events.
- Maintain a comprehensive understanding of the infrastructure
- Leverage AWS service specific metrics and log files
- Effectively consolidate, manage and analyze logs
- Operational excellence through streamlined view of application, system and AWS log information
- **What is it?** - an optional Service Catalog product to easily deploy an Amazon Elasticsearch and Kibana-base centralized log analysis solution

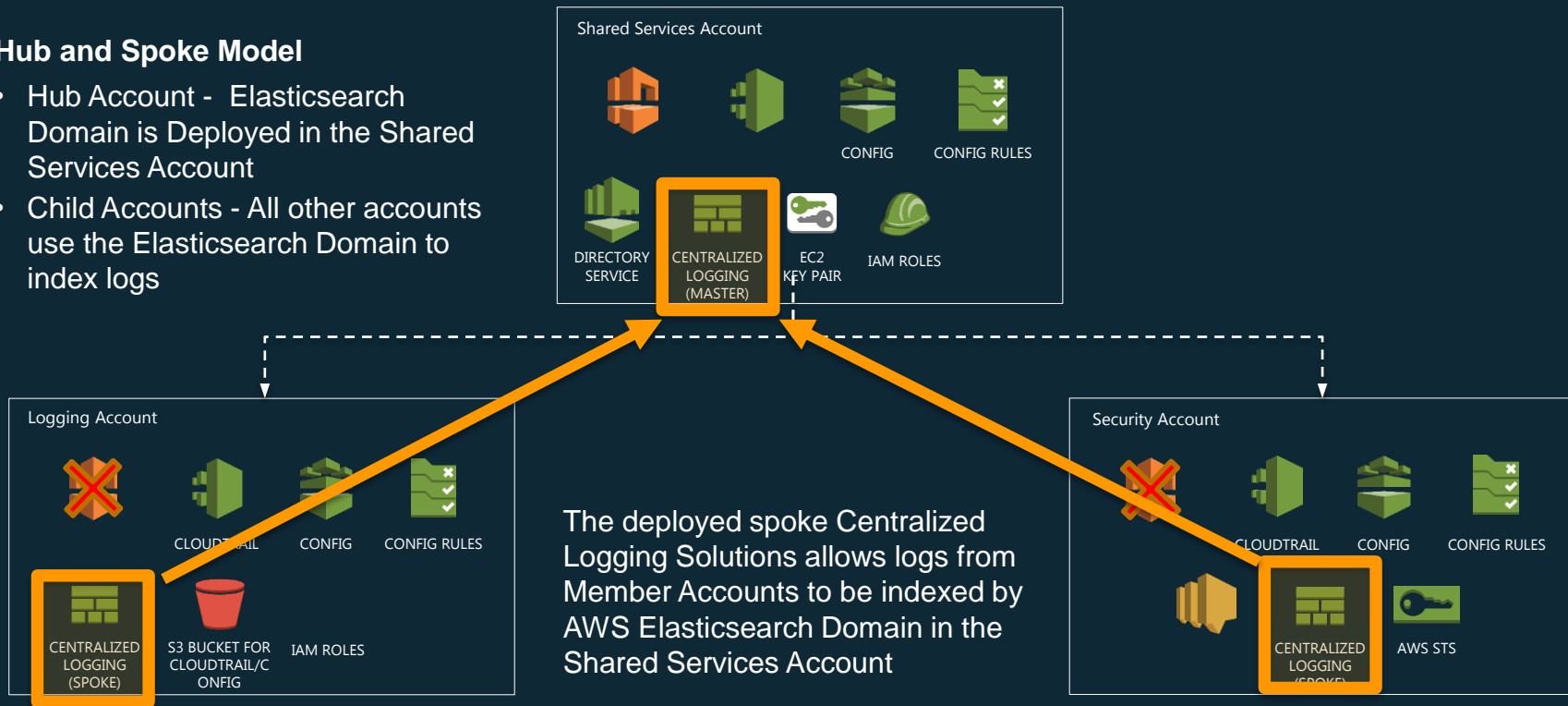
AWS Landing Zone – Centralised Logging



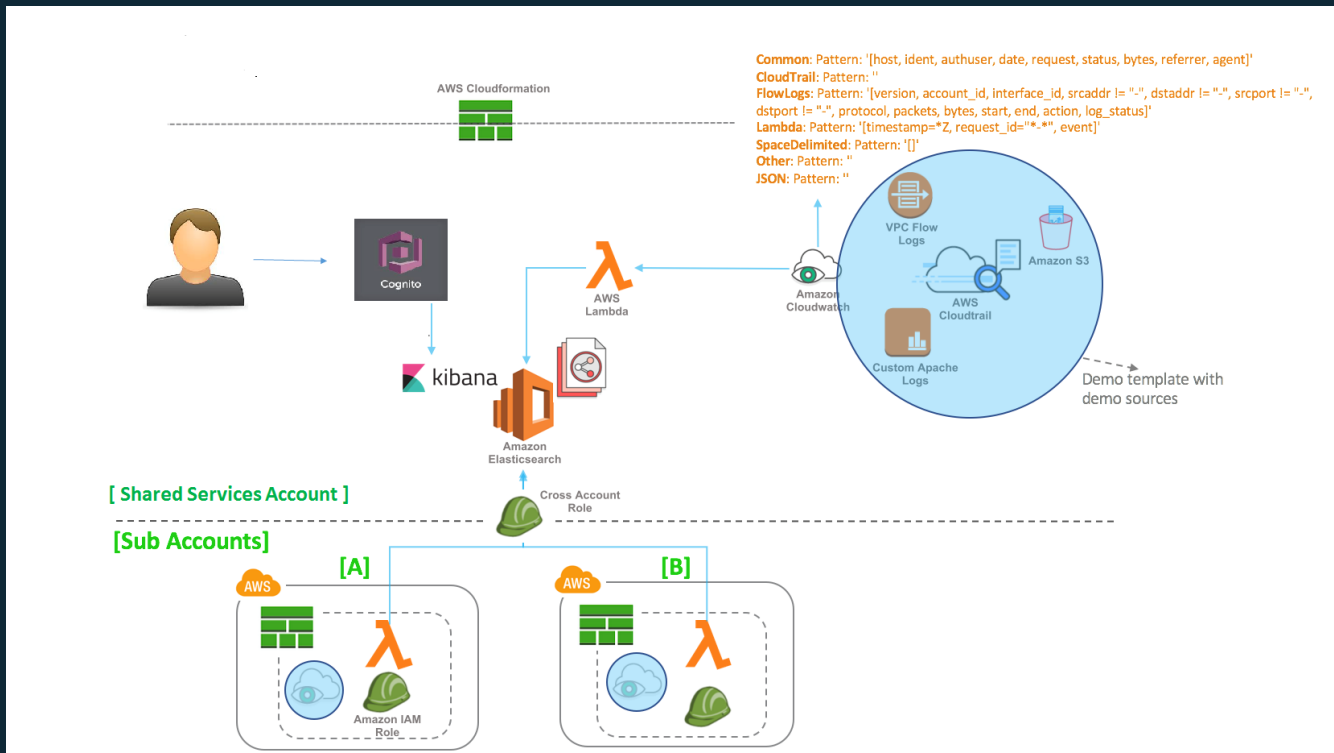
Centralized Logging Solution Hub And Spoke Model

Hub and Spoke Model

- Hub Account - Elasticsearch Domain is Deployed in the Shared Services Account
- Child Accounts - All other accounts use the Elasticsearch Domain to index logs

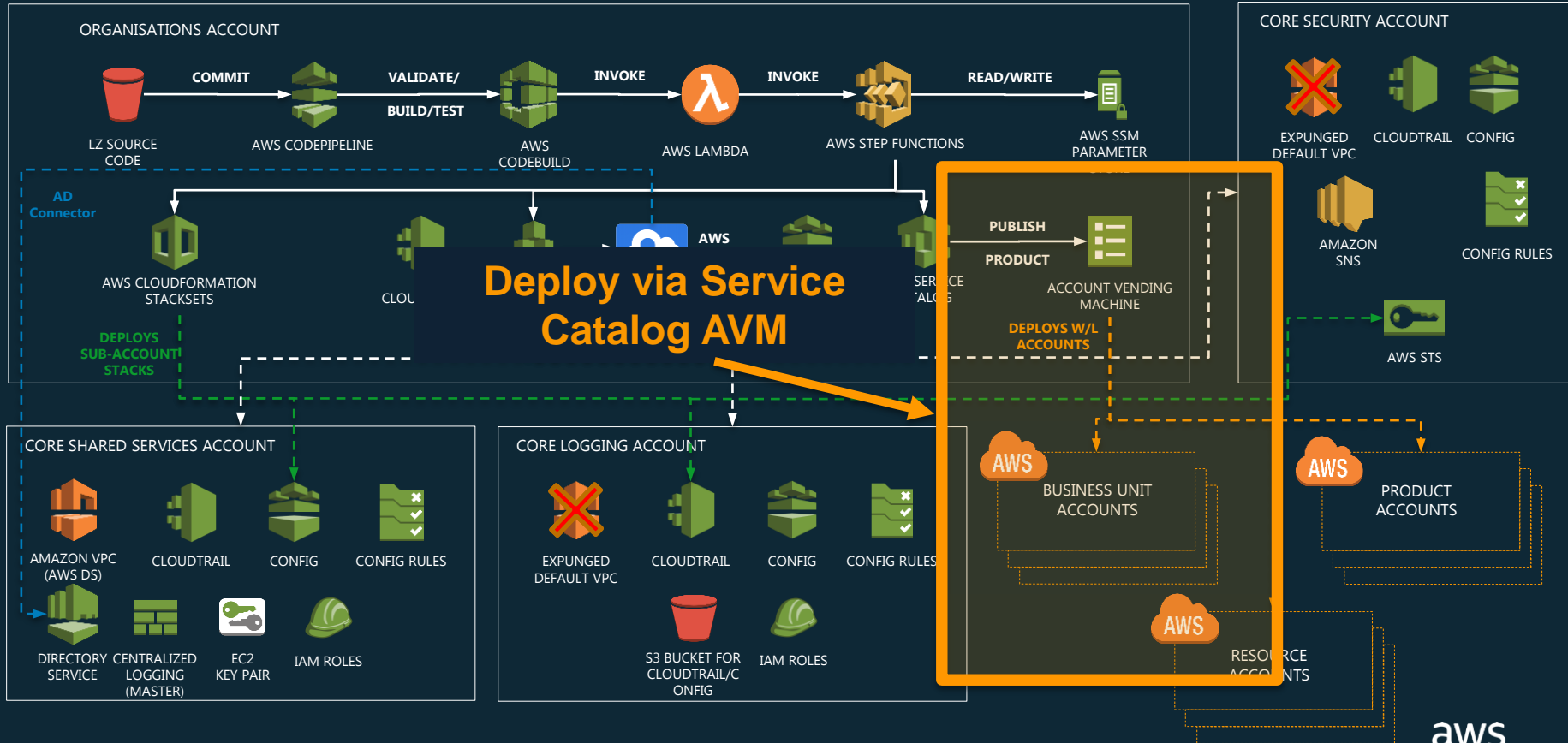


Centralized Logging Implementation



Lab 4 – Deploy a Member Account

Lab 4 – Deploy a Member Account

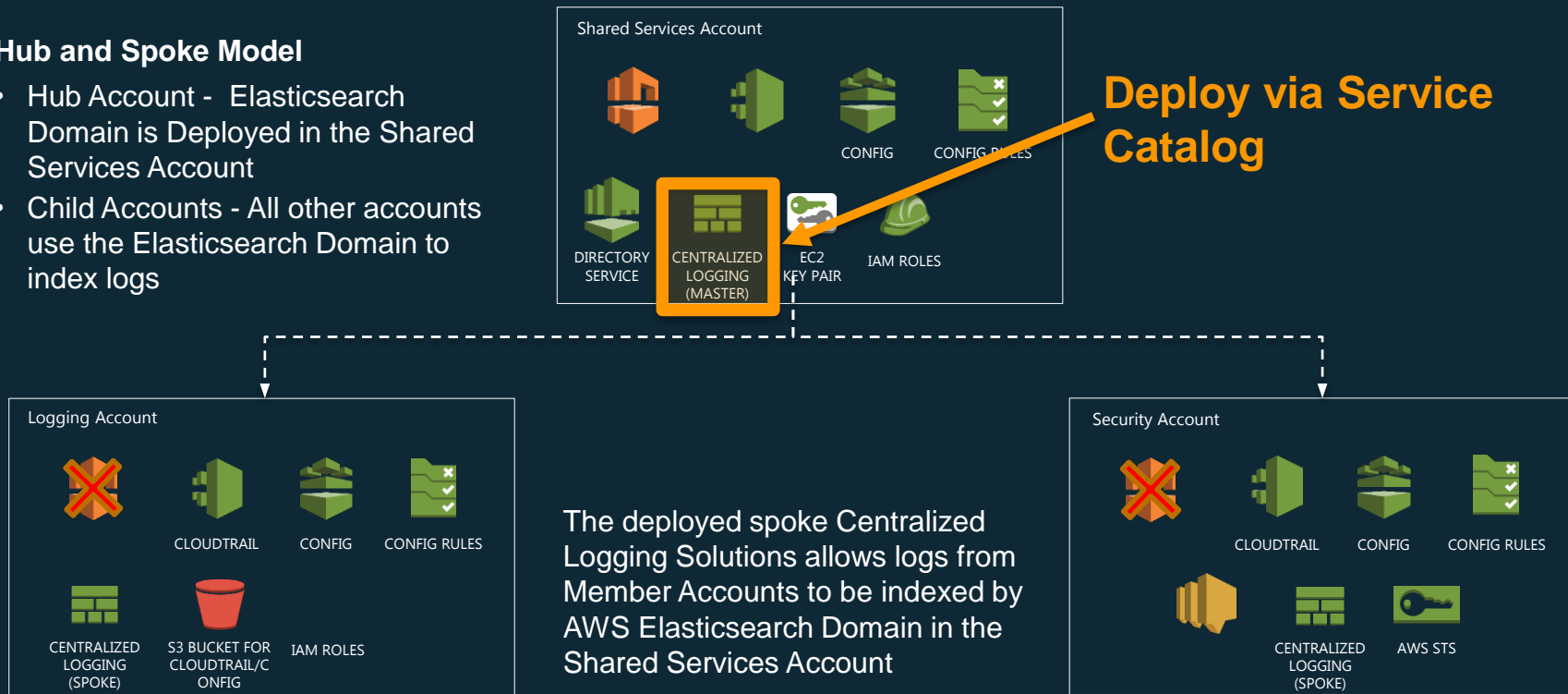


Lab 5 – Deploy Centralized Logging


Centralized Logging Solution Hub And Spoke Model


Hub and Spoke Model


- Hub Account - Elasticsearch Domain is Deployed in the Shared Services Account
- Child Accounts - All other accounts use the Elasticsearch Domain to index logs



Centralized Logging - Deployment

 **aws** service catalog

 **Products list**

 **Provisioned products list**


Admin

Products list

Search

Ex. Name

⋮



AWS Centralized Logging Solution

Install the centralized log aggregation and monitoring solution

LAUNCH PRODUCT

Centralized Logging – Deployment (cont.)

Step 1 : Product version

Step 2 : Parameters

Step 3 : Tags

Step 4 : Notifications

Step 5 : Review

Product Version

Specify a provisioned product name and then select the version that describes the provisioned product that you want to create.

Provisioned product

A provisioned product is a collection of related resources that you provision and update as a single unit.

Name* LZCentralizedLogging

Product Version

Version*

By name

	Versions ▾	Provided by ▾	Created time ▾	Description ▾
<input checked="" type="radio"/>	v1	AWS Solutions	Jun 5th 2018 07:11:59 ...	Install the centralized log aggregation and monitorin...

*Required

CANCEL NEXT

Centralized Logging – Deployment (cont.)

Launch - AWS Centralized Logging Solution

Step 1 : Product version

Step 2 : Parameters

Step 3 : Tags

Step 4 : Notifications

Step 5 : Review

Parameters

Specify values or use the default values for the parameters.

Account Selection

AccountName

shared-services



Name of the Account to deploy this stack


Region

us-east-1

Region to deploy the primary template

Centralized Logging – Deployment (cont.)

Centralized Logging Primary Setup

Domain Name	<input type="text" value="centralized-logging"/> <small>Name for the Amazon ES domain that this template will create. Domain names must start with a lowercase letter and must be between 3 and 28 characters. Valid characters are a-z (lowercase only), 0-9, and - (hyphen)</small>
Primary Cluster Size	<input type="text" value="Small"/>  <small>Amazon ES cluster size; small (2 data nodes), medium (4 data nodes), large (10 data nodes)</small>
User Name	<input type="text" value="XXXXXXX"/> <small>User name for kibana proxy servers</small>
Password	<input type="password"/> <small>Password for dashboard access via the proxy server. Must be six characters or longer, and must contain one uppercase letter, one lower case letter, and a special character (!@#\$%^&+)</small>
Retype Password	<input type="password" value="....."/> <small>Retype the password</small>
SSH Access CIDR	<input type="text" value="X.X.X.X/X"/> <small>IP address range that can SSH into Nginx proxy servers</small>
VPC CIDR for Proxy Servers	<input type="text" value="10.249.0.0/24"/> <small>CIDR block for VPC</small>
Subnet 1 for Proxy Server	<input type="text" value="10.249.0.0/27"/> <small>IP address range for subnet created in AZ1</small>
Subnet 2 for Proxy Server	<input type="text" value="10.249.0.32/27"/> <small>IP address range for subnet created in AZ2</small>

Centralized Logging – Deployment (cont.)

Launch - AWS Centralized Logging Solution

Step 1 : Product version

Step 2 : Parameters

Step 3 : Tags

Step 4 : Notifications

Step 5 : Review

Tags

You can specify tags (key-value pairs) for resources in your provisioned product. You can add up to 10 unique key-value pairs for each provisioned product. [Learn more.](#)

Key (127 characters maximum)	Value (255 characters maximum)	
AWS Solutions	Landing Zone Solution	
AWS Solutions	Landing Zone Solution	
		+

CANCEL PREVIOUS NEXT

Centralized Logging – Deployment (cont.)

Step 1 : Product version

Step 2 : Parameters

Step 3 : Tags

Step 4 : Notifications

Step 5 : Review

Notifications

☒ Enable provisioned product event notifications to be streamed to an Amazon SNS topic.

- ☒ Create a new topic
- ☐ Choose a topic from your account
- ☐ Choose a topic from another account

Topic Name*

Enter topic name


*Required


CANCEL


PREVIOUS

LAUNCH


Centralized Logging – Deployment (cont.)


aws service catalog

Products list

Provisioned products list

Admin

Products list

Portfolios list

Provisioned products list

GO BACK TO OLD LC

Search

Ex. Name OR status:available

Filter by

User ▾

Sort by

Relevance ▾

Count

100 ▾

Refresh



Grid/List

Showing 1-1

<

1


>

	Provisioned Product name	Created	Status	Status message
	LZCentralizedLogg	2018-06-06 20:21:57 UTC+0100	 UNDER_CHANGE	

Centralized Logging – Deployment (cont.)

LZCentralizedLogg

ACTIONS ▾




Status Under change

Product AWS Centralized Logging Solution

Version v1

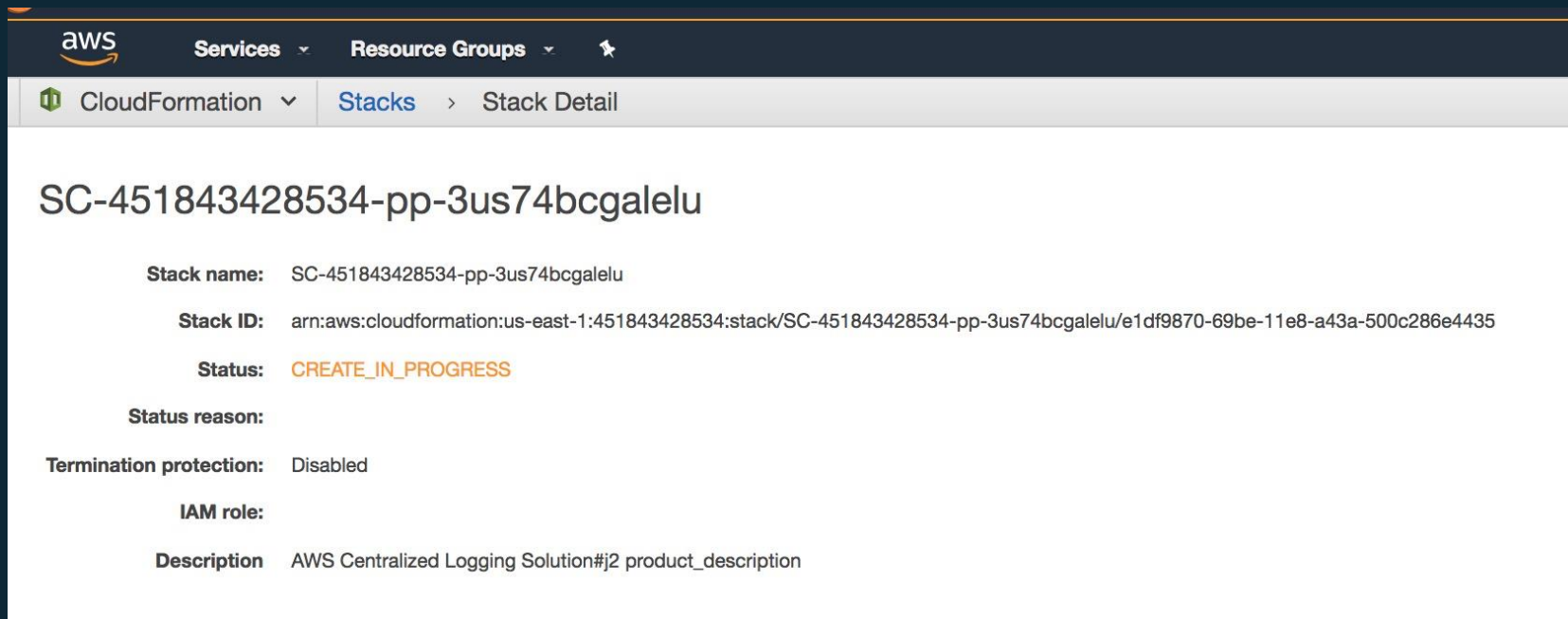
Provided by AWS Solutions

▾ Events (1)



Jun 6th 2018	Status	Type	Event message
▾ 20:21:59 UTC+0100	In progress	PROVISION_PRODUCT	
Record ID: rec-eyas3pe6bo6bu			
Provisioned product ID: pp-3us74bcgalelu			
▾ Outputs:			
Key	Value	Description	
CloudformationStackARN	arn:aws:cloudformation:us-east-1:451843428534:stack/SC-451843428534-pp-3us74bcgalelu/e1df9870-69be-1e8-a43a-500c286e4435	The ARN of the launched Cloudformation Stack	

Centralized Logging – Deployment (cont.)



The screenshot displays the AWS CloudFormation console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a search icon. Below this, the breadcrumb trail shows 'CloudFormation' > 'Stacks' > 'Stack Detail'. The main content area features the stack name 'SC-451843428534-pp-3us74bcgalelu' in a large font. Below the name, the following details are listed:

- Stack name:** SC-451843428534-pp-3us74bcgalelu
- Stack ID:** arn:aws:cloudformation:us-east-1:451843428534:stack/SC-451843428534-pp-3us74bcgalelu/e1df9870-69be-11e8-a43a-500c286e4435
- Status:** CREATE_IN_PROGRESS
- Status reason:**
- Termination protection:** Disabled
- IAM role:**
- Description:** AWS Centralized Logging Solution#j2 product_description

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