Extending the Landing Zone

Amazon Web Services

24 July 2018

Solution Extensibility

The AWS Landing Zone allows customers to modify after the fact by editing the files in LZ Configuration ZIP, Customers can:

- Add or Remove Organizational Unit
- Add or Remove Core Accounts
- Add, Update, or Remove Core Account Resources
- Add, Update, or Remove Account Baseline Resources
- Add, Update, or Remove AWS Service Catalog Products
- Add, Update, or Remove AWS Organizations Policies

aws-landing-zone-configuration ZIP File Structure

- manifest.yaml
- parameters/

  …. JSON Parameter Files
- templates/

  …. JSON/YAML CloudFormation template Files
- policies/

  …. JSON Service Control Polcies
- validation/

  …. Manifest YAML Schema

Manifest YAML File Structure

- region: us-east-1
- version: 2018-06-14
- lock_down_stack_sets_role: Yes/No
- organizational_units:

    #List of Organization Units

    core_accounts:

        #List of Core Accounts

        core_resources:

            #List of Core Resources

- organization_policies:

    #List of Service Control Policies

- portfolios:

    #List of Service Catalog portfolios

    products:

        #List of Service Catalog products

- baseline_resources:

    #List of Baseline Resources

Manifest : Organizational_units

- organizational_units:

  - name: String

    include_in_baseline_products: #List of Service Catalog products

    core_accounts:

      - List of Core Accounts

Manifest : Organizational_units -> core_accounts

- core_accounts: #List of core accounts

  - name: String

    email: String

    ssm_parameters: #List of SSM parameters

      - name: String e.g. /org/member/logging/account_id

        value: String e.g. $[AccountId], $[AccountEmail]

        core_resources: #List of core resources

aws

Manifest : Organizational_units -> core_accounts -> core_resources

- core_resources: #List of core resources

  - name: String

    template_file: String

    parameter_file: String

    deploy_method: String e.g. stack_set

    ssm_parameters: #List of SSM parameters

      - name: String e.g. /org/security/sns_topic_arn

        value: String e.g. $[output_CfnOutputVariable]

Manifest : organization_policies

- organization_policies: #List of service control policies

  - name: String

    description: String

    policy_file: String

    apply_to_accounts_in_ou: #List of String

      - String

Manifest : portfolios

- portfolios: #List of portfolios

  - name: String

    description: String

    owner: String

    principal_role: #Service Catalog Principal Role ARN

    products: #List of Service Catalog products to add to Portfolio

      - List of products

Manifest : portfolios -> products [Baseline]

- products: #List of products to add to portfolio
  - name: String
    description: String
    product_type: **baseline**
    skeleton_file: #Jinja2 template
    parameter_file: String
    hide_old_verions: Boolean
    launch_constraint_role: #Launch Constraint Role ARN
    apply_to_accounts_in_ou: #LaunchAVM
    #List of Organizations Units

Manifest : portfolios -> products [Optional]

- products: #List of products to add to portfolio
  - name: String
    description: String
    product_type: **optional**
    template_file: String
    skeleton_file: #Jinja2 template
    hide_old_verions: Boolean
    launch_constraint_role: #Launch Constraint Role ARN
    ssm_parameters: #List of SSM parameters
      - name: String
        value: String

Lab 6 – Extend your Landing Zone

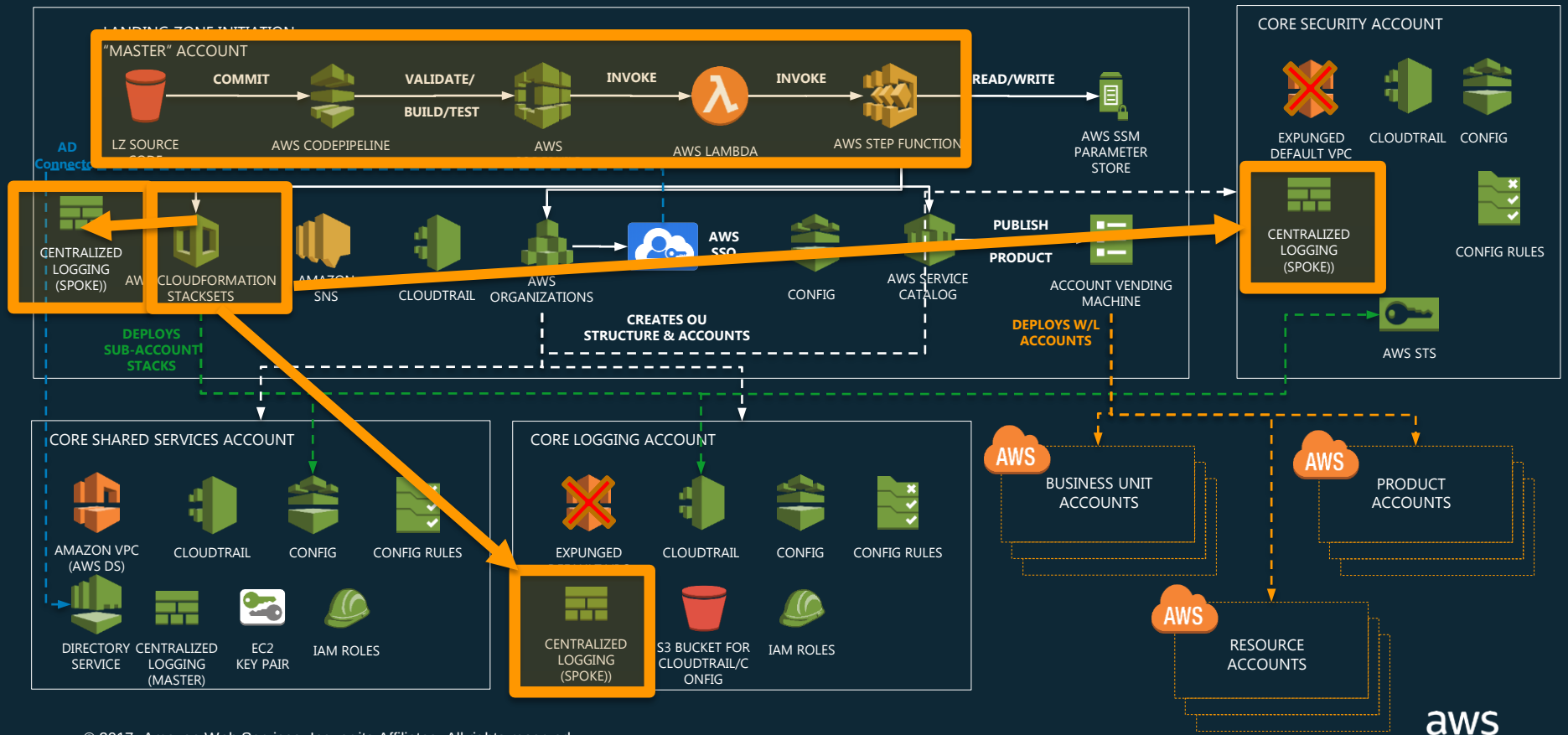
Lab 6 – Update the Manifest and Redeploy

Add Centralised Logging Spoke and Config Rule to manifest
Deploy to all accounts

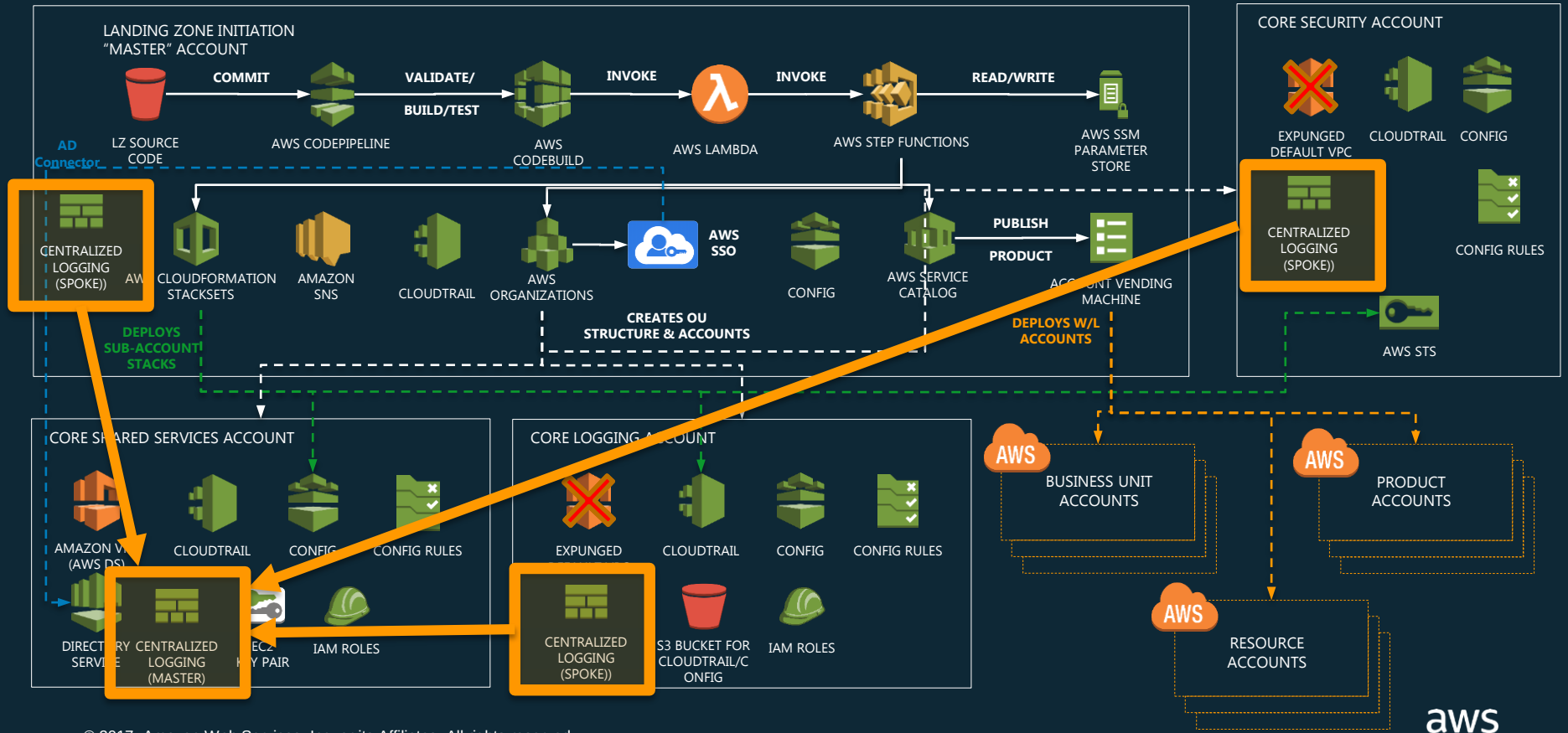
- Download the config file
- Edit the manifest
- Uncomment the Logging Spoke
- Add the Config Rule
- Zip and upload the config
- Release Change

aws

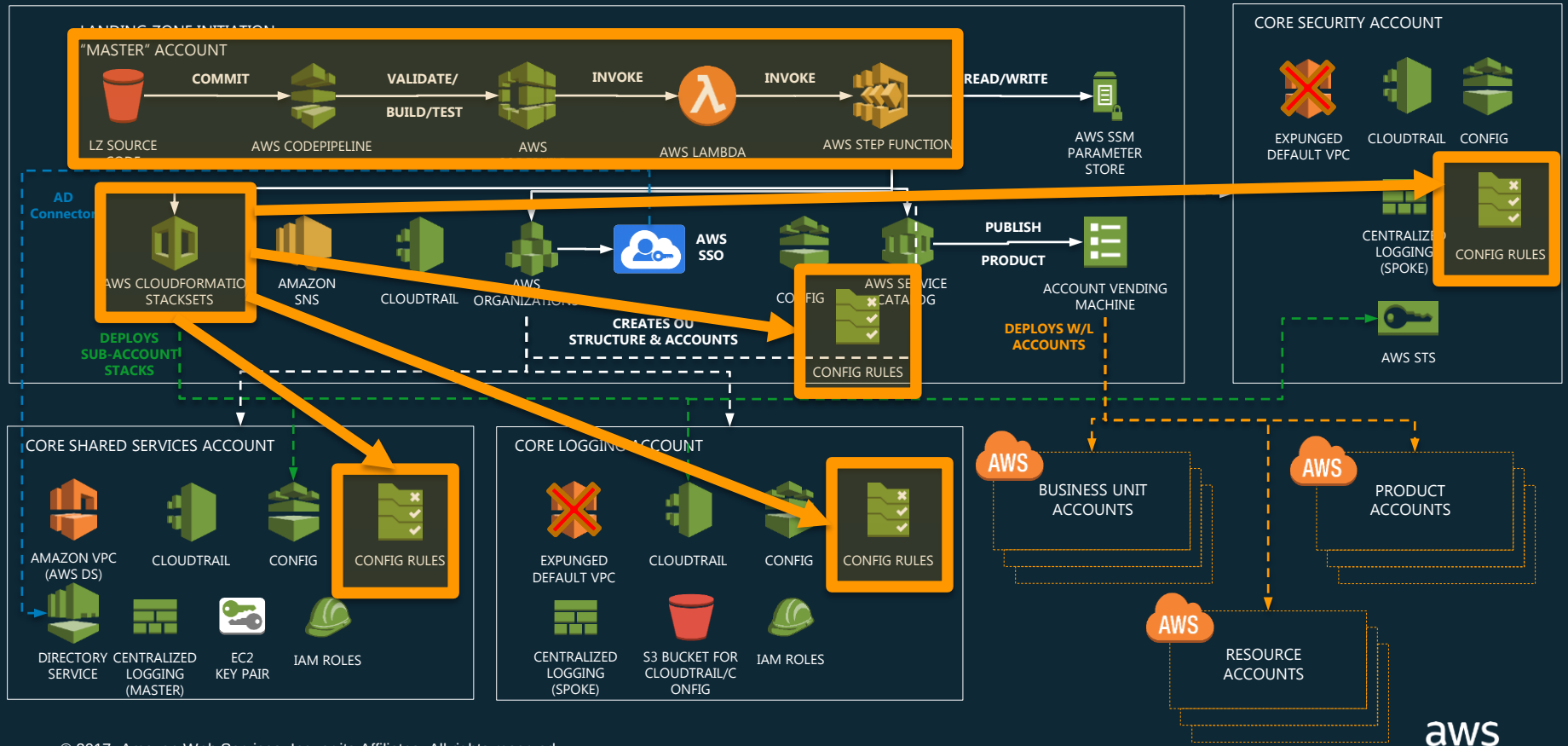
AWS Landing Zone – Centralised Logging Spoke



AWS Landing Zone – Centralised Logging

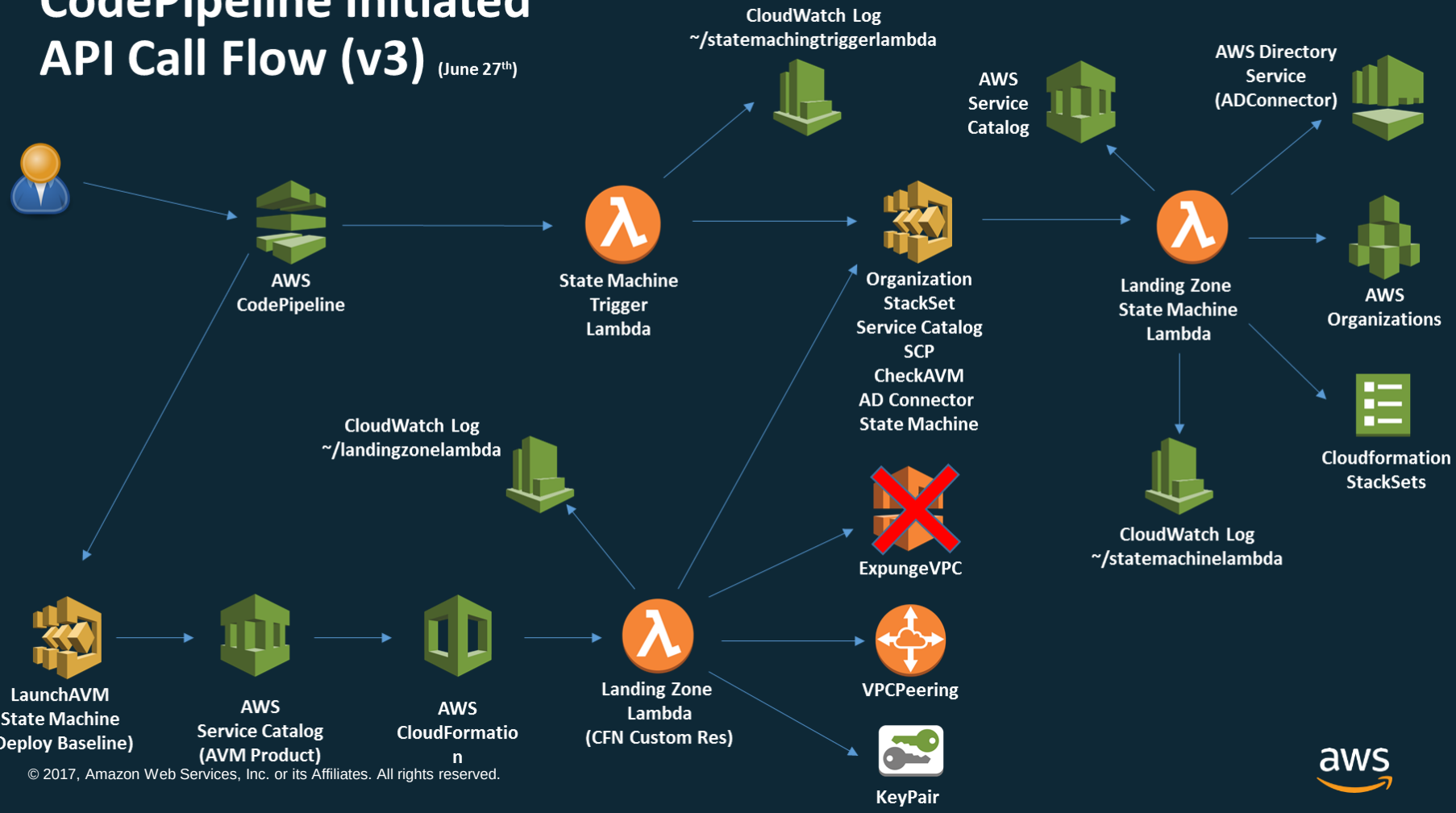


Data Security– AWS Config Rules

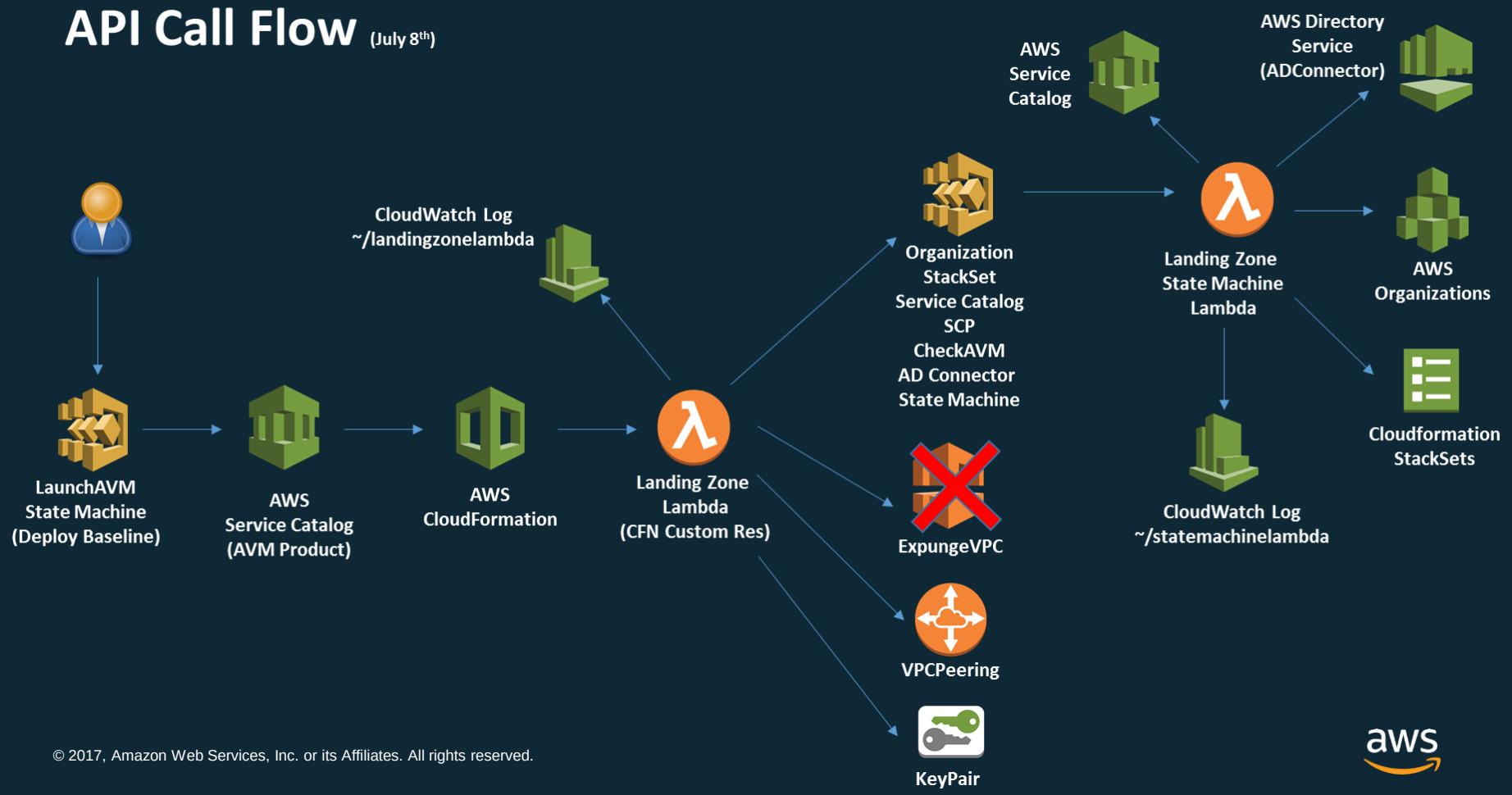


Under the Hood

CodePipeline Initiated API Call Flow (v3) (June 27th)



User / AVM Initiated API Call Flow (July 8th)

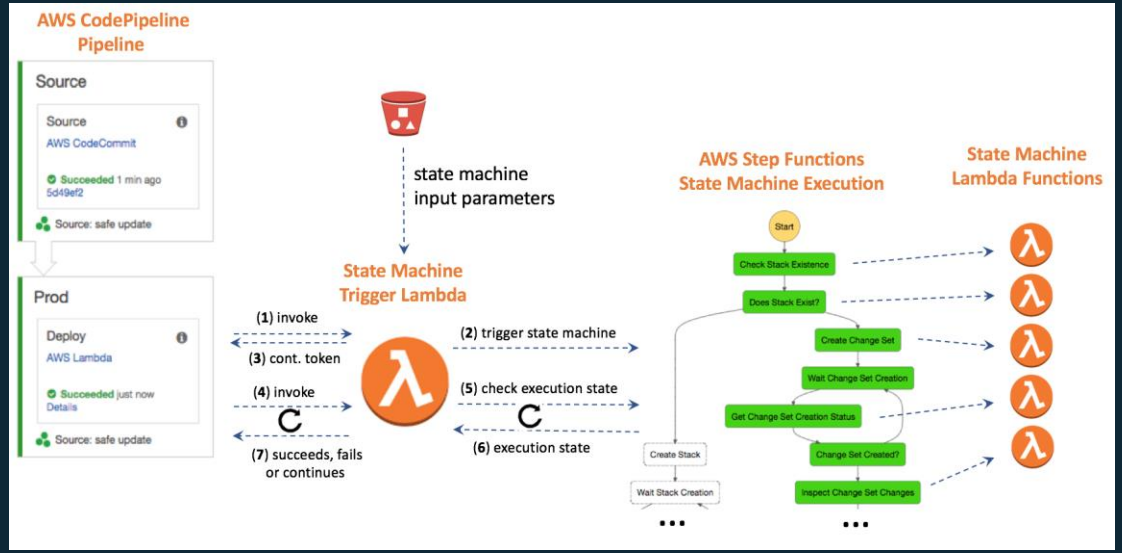


Codepipeline – TriggerLambda – State Machine

(1) Code Pipeline invokes a Lambda based Action called the State Machine Trigger Lambda

(2) The Lambda function triggers a Step Functions State Machine to process the request

(3) The Lambda function sends a continuation token back to Code Pipeline telling Code Pipeline to continue its execution later and terminates

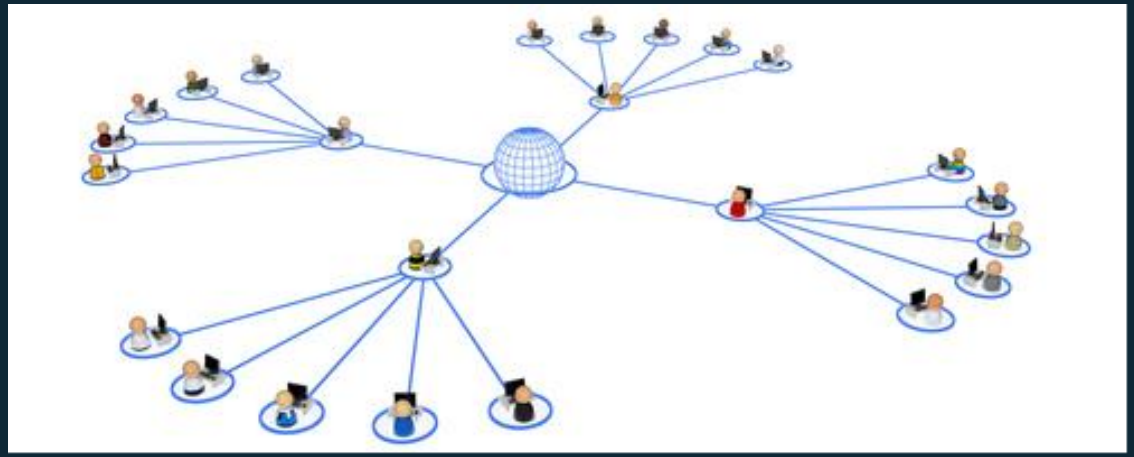


(4) Seconds later, Code Pipeline invokes the State Machine Lambda function again, passing the continuation token it received

(5,6) The Lambda function checks the execution state of the state machine and communicates the status to the pipeline

(7) Then the Lambda function notifies Code Pipeline that the corresponding Code Pipeline Action is complete. If the state machine has failed, the Lambda will fail the Code Pipeline Action and the Stage will stop with an error

Lambda Function Routing



- Step Functions team/SMEs recommend 1 lambda for each state
- Landing Zone selected the opposite model, more like Onion routing
- The “Router <-> Handler <-> Library” flow helped reduce the number of Lambda functions and provided faster response time as LZ only instantiates certain portion of the code

Existing Accounts – Work in Progress

You need to ensure existing accounts meet the following criteria

1. The account must be part of the Landing Zone Organisation
2. The account cannot be in the Core or Applications OU
3. The account email you enter must match the account you want to adopt
4. The account must not have a Config Recorder – Config only allows one
5. The account must not have a Cloudtrail Trailname the same name as the LZ Trail
6. The account must have a AWSCloudFormationStackSetExecutionRole with admin permissions and a trust policy that lets the Master account switch role to it
7. The account much not contain any resources/config associated with the Default VPCs in ANY region e.g. security groups cannot exist associated with the Default VPC

Import existing Core Accounts via the manifest

1. Edit the manifest and add in the account details

Import non-Core Accounts via the AVM

1. Open Service Catalog -> AVM and enter the existing account details

aws

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

aws