AWS Landing Zone Solution

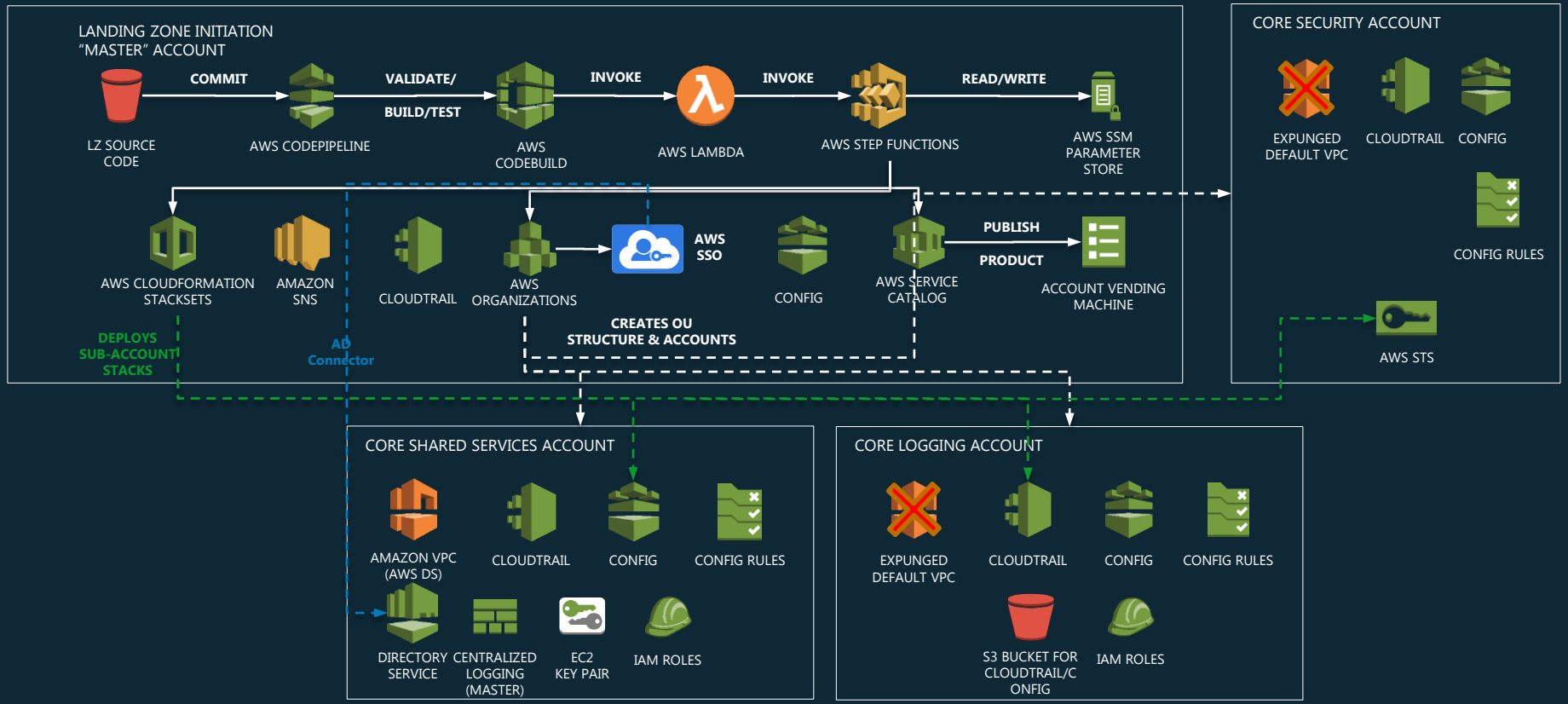
Amazon Web Services

24 July 2018

http://gltaylor-lzdocs.s3.amazonaws.com/index.html

Lab 1 – Landing Zone Example Implementation

Lab 1 - AWS Landing Zone Example Implementation



Why the AWS Landing Zone

What do customers want to do on AWS?

Build

focus on what differentiates

Move Fast

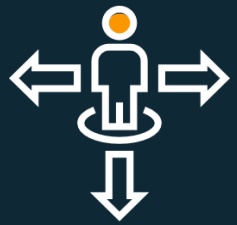
ideation to instantiation

Stay Secure

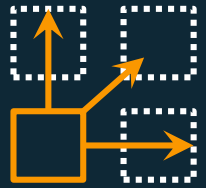
secure and compliant environment

aws

Customers are faced with



Many
design decisions



Need to configure
multiple accounts & services

Establish
security baseline & governance

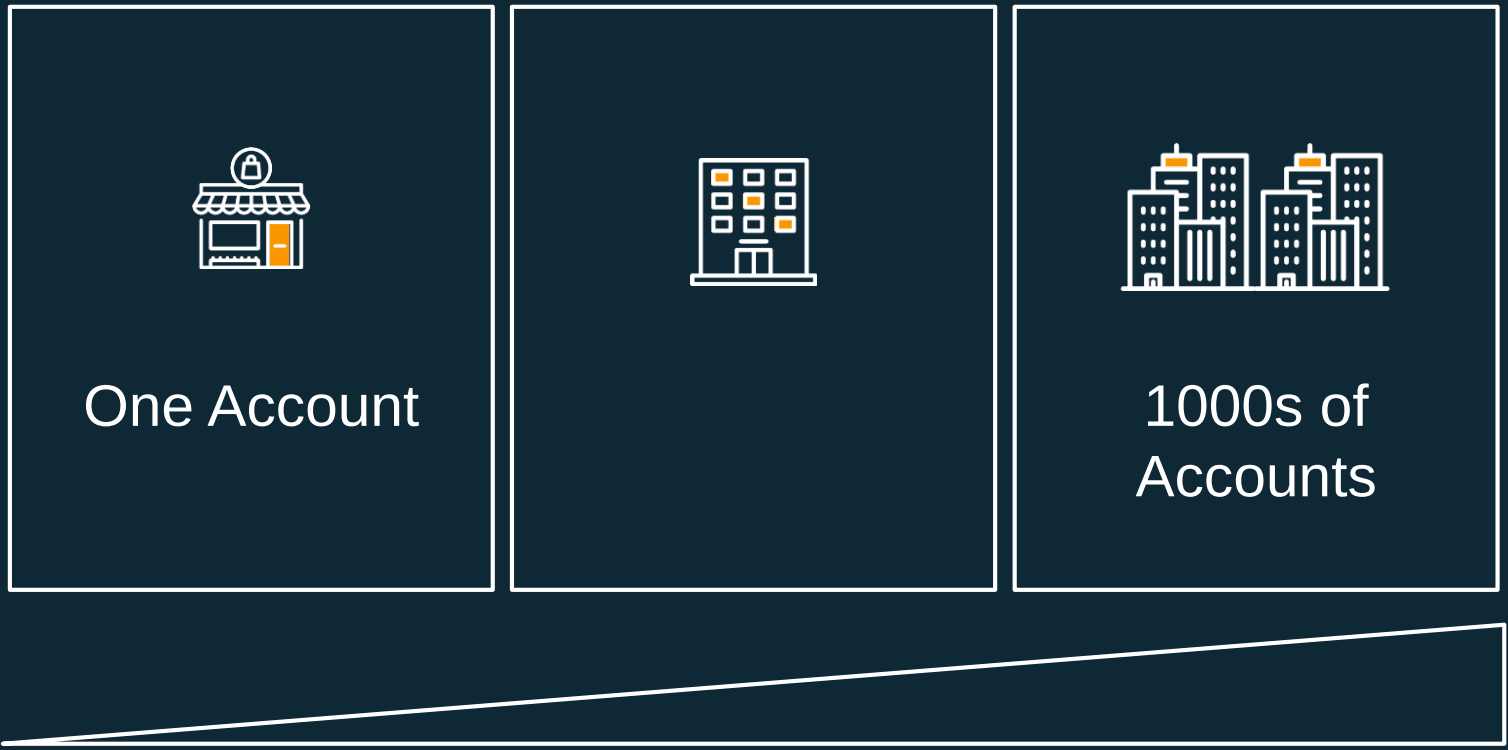
AWS Account Bourdaries

Security/Resource Boundary

API Limits/Throttling

Billing Separation

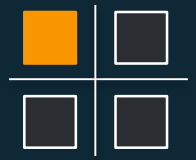
Account Models



Why One Isn’t Enough

Many Teams

Billing



Isolation

Security / Compliance Controls

Business Process

What Accounts Should I Create?

Organizations Account

Logging

Security

Network

Shared Services

Billing

Sandbox

Dev

Pre-Prod

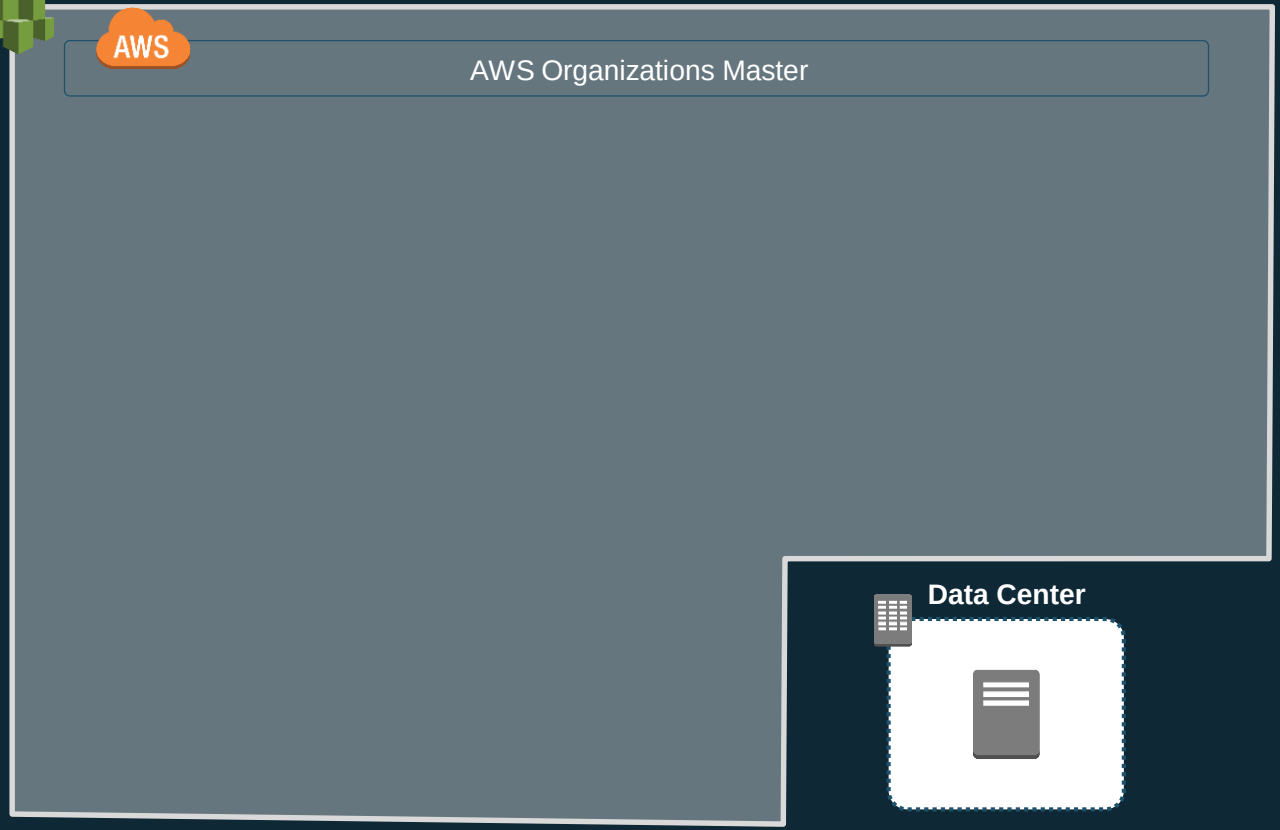
Prod

Other

aws

AWS Multi-Account Strategy

AWS Organizations (Master)



No connection to DC

Service control policies

Consolidated billing

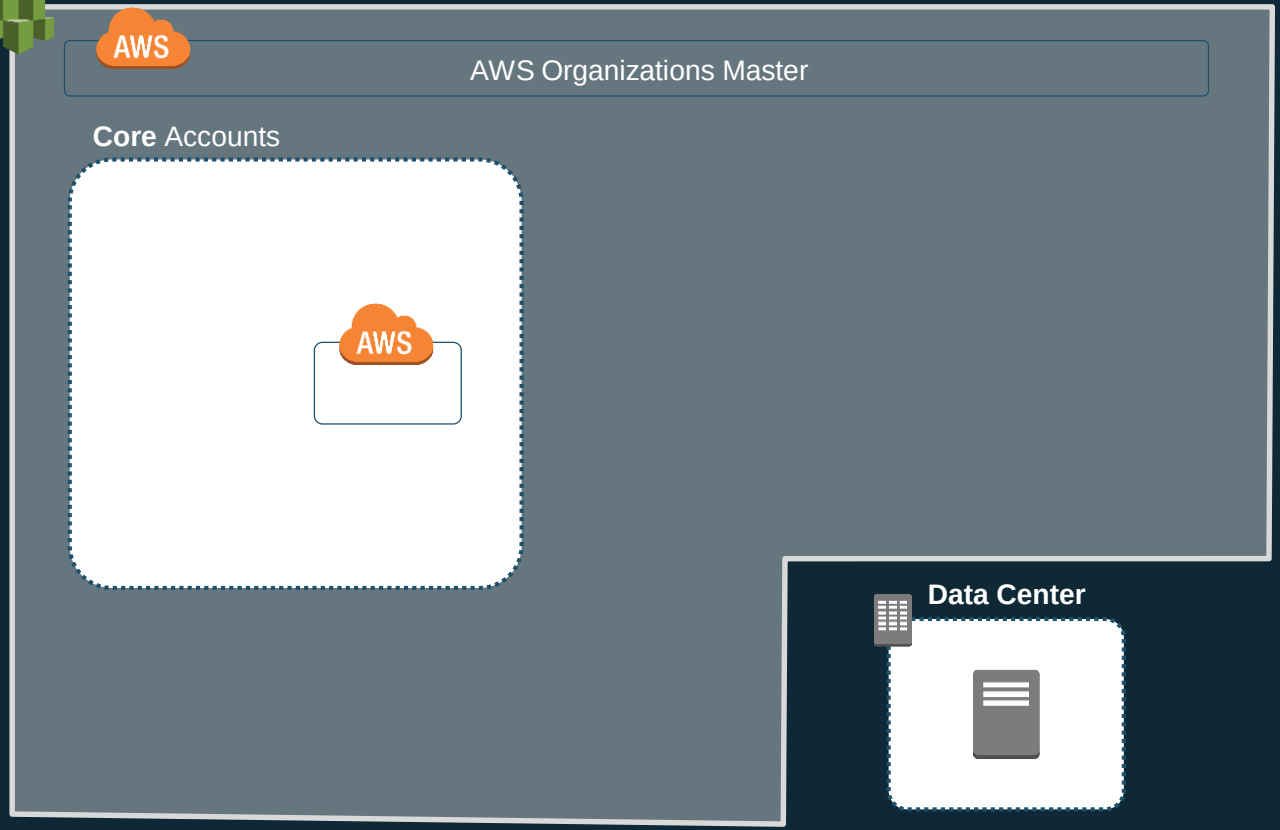
Volume discount

Minimal resources

Limited access

Retrict Orgs role!

Logging Account



Versioned Amazon S3 bucket
- Restricted
- MFA delete

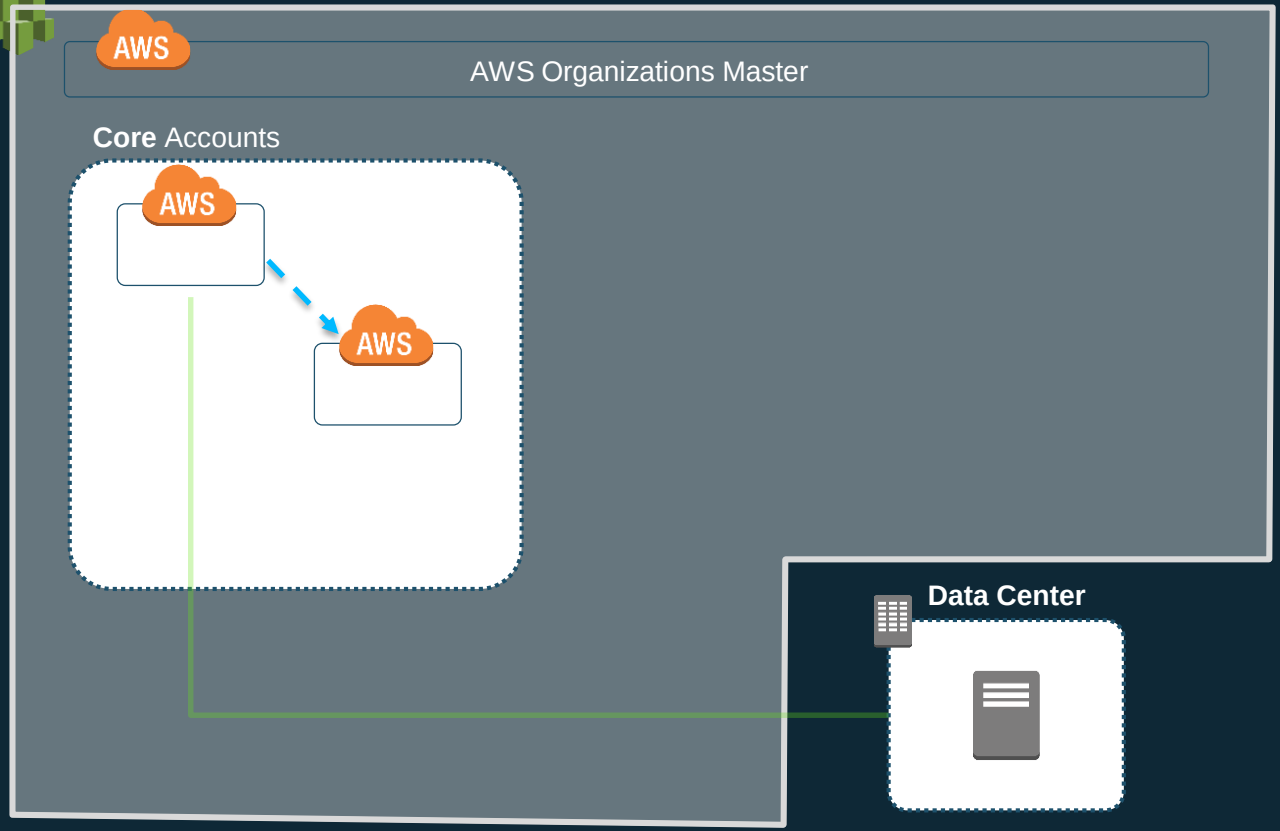
CloudTrail logs

Security logs

Single source of truth

Limited access

Security Account



Optional data center connectivity

Security tools and audit

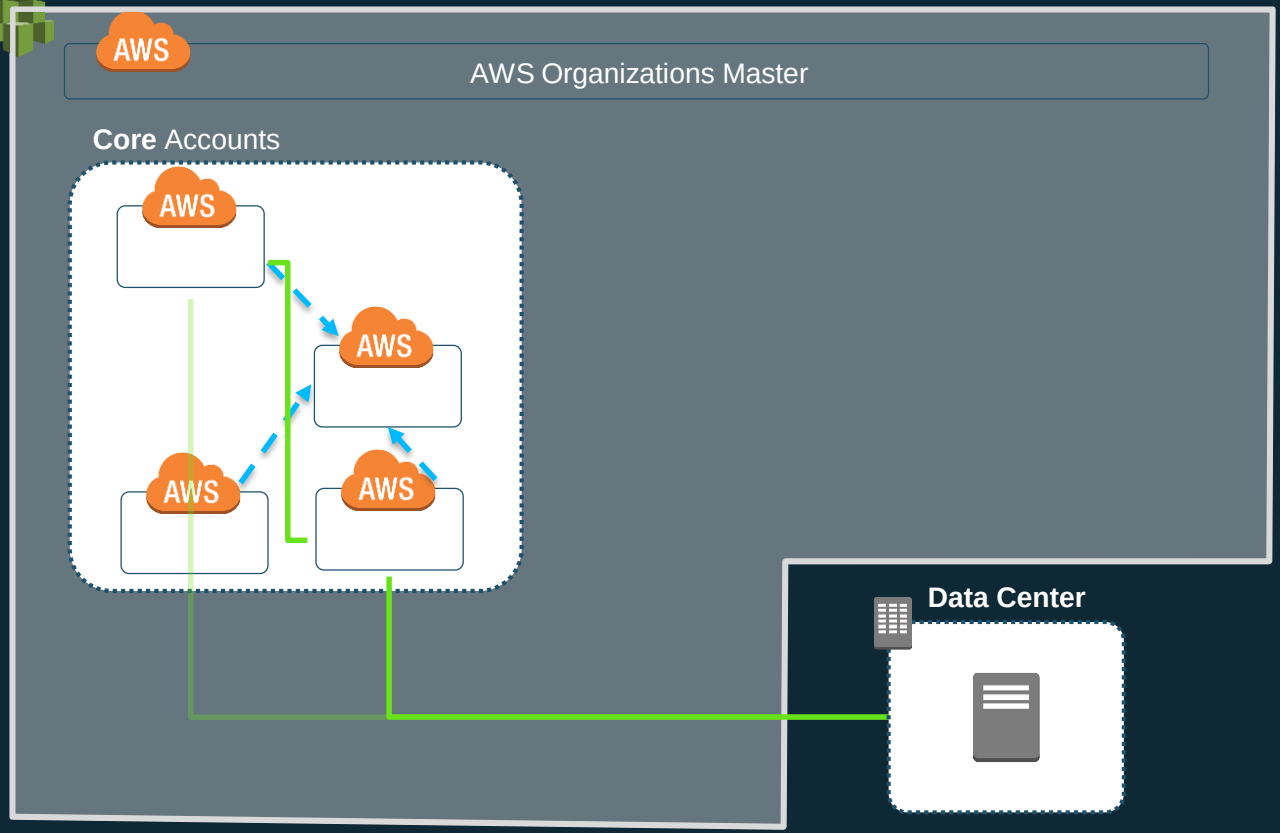
Cross-account read/write

Limited access

AWS CloudTrail

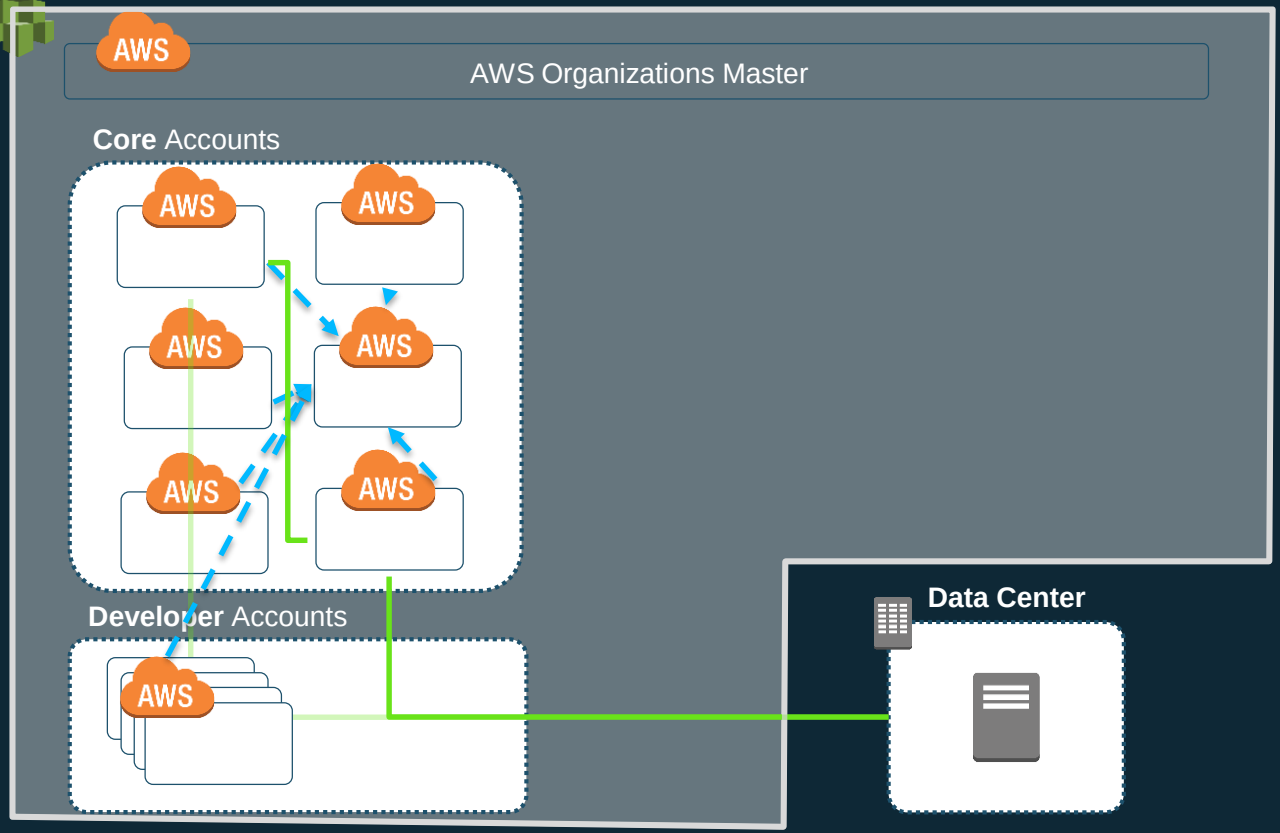
AWS Config

Shared Services Account



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

Developer Sandbox



No connection to DC

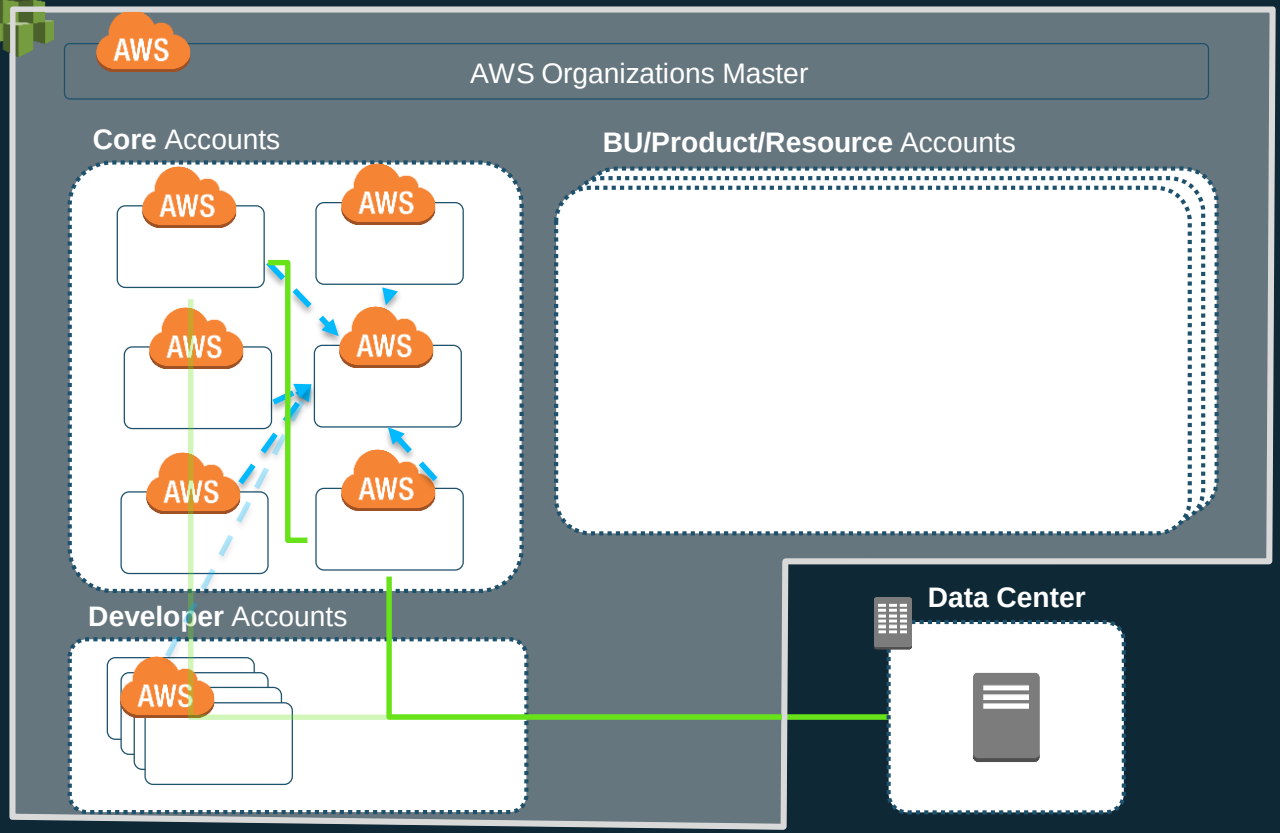
Innovation space

Monitor spending

Autonomous

Experimentation

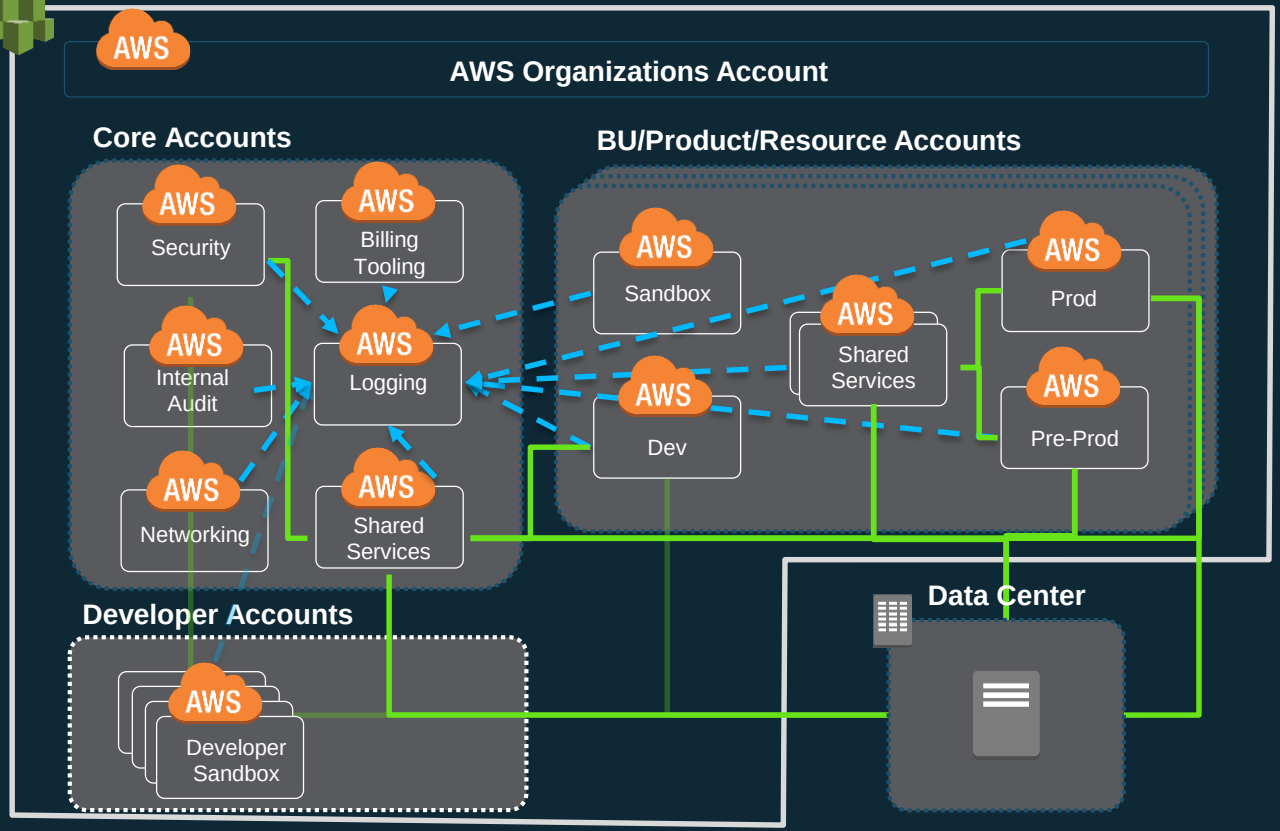
BU/Product/Resource



Based on level of needed isolation

Match your development lifecycle

Multi-Account structure



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

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

How can we make this easier?

The AWS Landing Zone solution

An **easy-to-deploy solution** that automates the setup of new AWS 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 that includes security, audit, and 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

4 Components of the Landing Zone

Landing Zone Implementation & Configuration Pipeline

- Easily modify and extend the Landing Zone to grow with your Organization
- This is deployed by means of the **Initialization Template**

Example Multi-Account Implementation

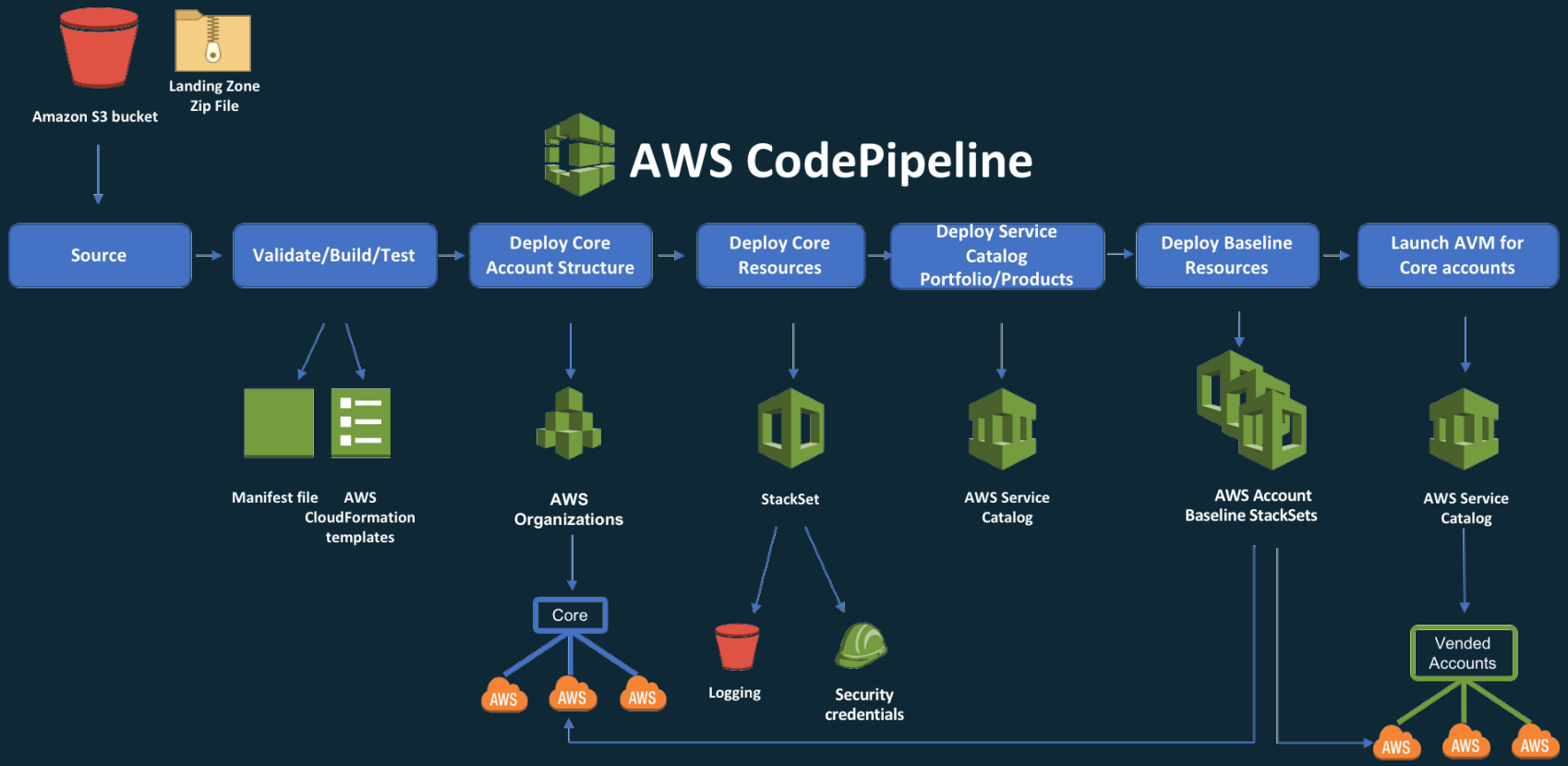
- Out-of-the-box example Landing Zone implementation to get started quickly.This can optionally be deployed during pipeline deployment or separately

The Account Vending Machine

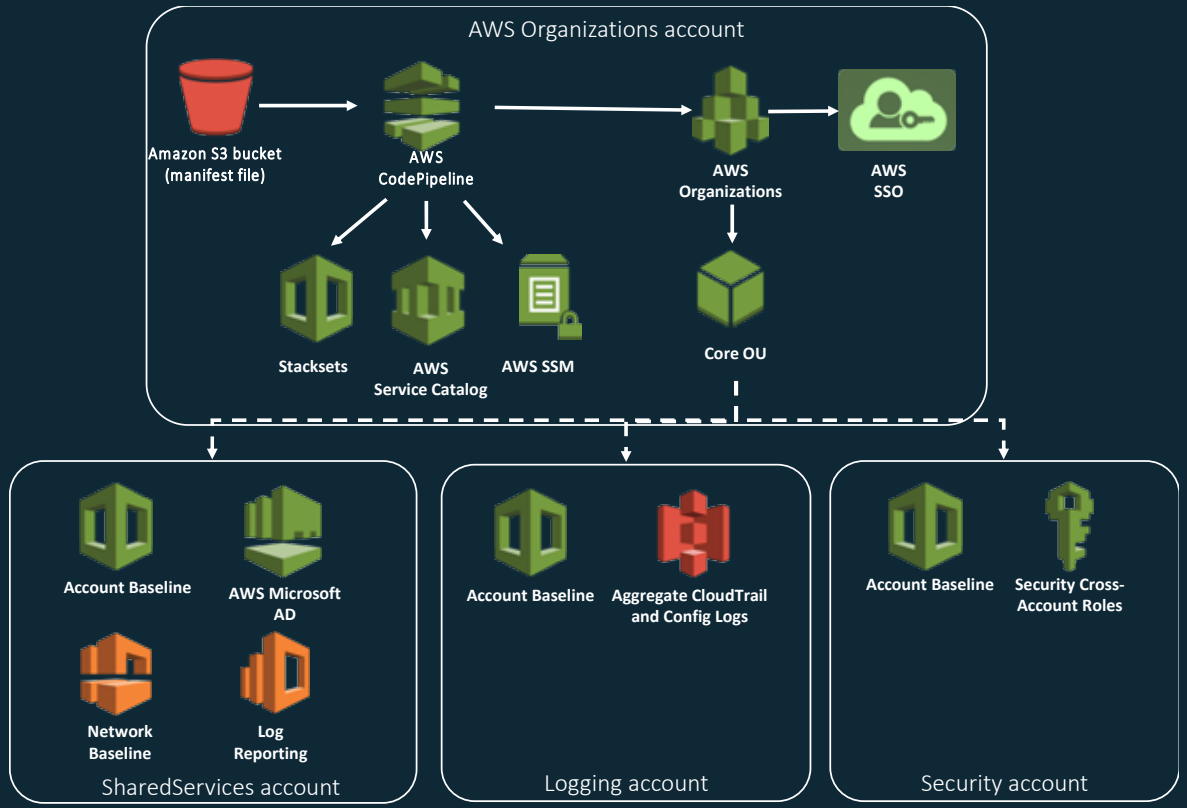
- This allows end-user customers to request new accounts through a product catalog

aws

Landing Zone Pipeline – High Level



Core Accounts and Resources- High Level



Organizations account:

- Account Provisioning
- Account Access (SSO)

Shared Services account:

- Active Directory
- Log Analytics

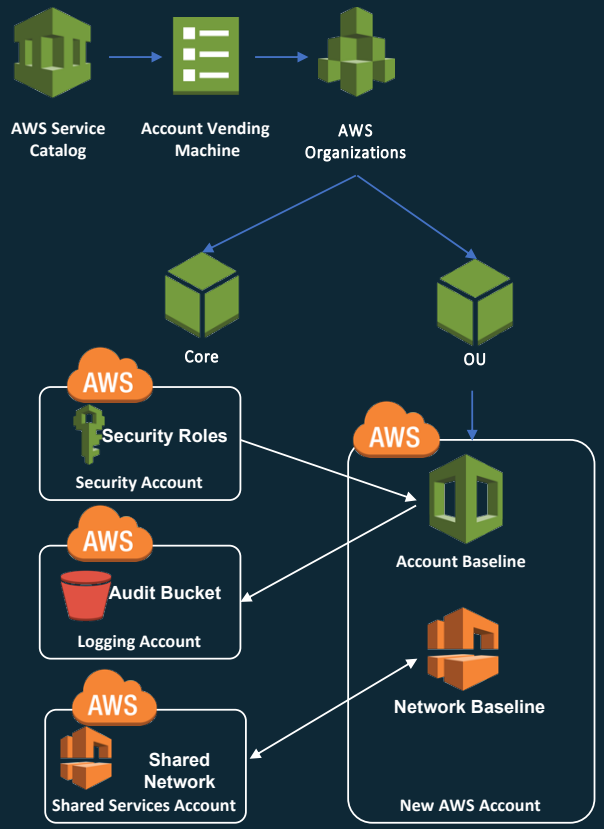
Logging account:

- CloudTrail/Config logs

Security account:

- Audit/Break-glass

Account Vending Machine – High Level



- 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

Benefits of the AWS Automated Landing Zone

Automated

Scalable

Self-Service

Guardrails
NOT Blockers

Auditable

Flexible

AWS Landing Zone Pricing

- No additional charge for the AWS Landing Zone solution.
- Customer is responsible for charges for services deployed (e.g., AWS Config Service, AWS CloudTrail, etc.). Estimated cost for underlying services is ~$500/month
- If you add the optional centralized logging product (Elasticsearch/Kibana) it would be an additional ~$400/month.

Key things you should know:

- The solution sets up new environments, it does not modify existing environments
- Both new and mature customers can use the solution
- This is a partner/proserv deployable solution, not a service
- It is available now and designed to be used for production deployments
- The solution was designed to scale. Migration ProServe practice helped in design so that it can be used for MAP engagements and large scale migrations

Customers with existing accounts

- New Master account: The solution requires a new Organizations master
- Existing accounts: The solution does not currently support the importing of existing accounts
- Use cases for mature customers:
    - Set up a new environment for a new team/ business unit
    - Learn if there are things they want to build into their existing environments
    - Create a scalable environment if they are running into limits with their current AWS environment set up
- If customers want modifications or integration of AWS Landing Zone into existing environments, engage ProServe / Partners

Availability

All services are available (White)

- US – ALL
- AP (Tokyo)
- AP (Singapore)
- AP (Sydney)
- Canada (Central)
- EU (Frankfurt)
- EU (Ireland)
- EU (London)

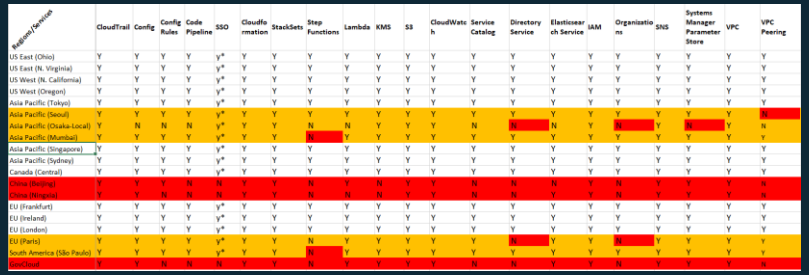
Not supported (Red):

- China (Beijing & Ningxia)
- GovCloud

Additional considerations needed (Yellow)

- AP (Seoul, Osaka, Mumbai)
- EU (Paris)
- SA (Sao Paulo)

See Field Enablement Portal for availability matrix and instructions for yellow regions



Regions / Services	CloudTrail	Config	Config Rules	Code Pipeline	SSO	Cloudformation	StackSets	Step Functions	Lambda	KMS	S3	CloudWatch	Service Catalog	Directory Service	Elasticsearch Service	IAM	Organizations	SNS	Systems Manager Parameter Store	VPC	VPC Peering
US East (Ohio)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
US East (N. Virginia)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
US West (N. California)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
US West (Oregon)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Asia Pacific (Tokyo)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Asia Pacific (Seoul)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Asia Pacific (Osaka-Local)	Y	N	N	N	y*	Y	Y	N	N	Y	Y	Y	N	N	N	Y	N	Y	Y	N	N
Asia Pacific (Mumbai)	Y	Y	Y	Y	y*	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Asia Pacific (Singapore)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Asia Pacific (Sydney)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Canada (Central)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
China (Beijing)	Y	Y	Y	N	N	Y	Y	N	Y	N	Y	Y	N	N	N	Y	N	Y	Y	Y	N
China (Ningxia)	Y	Y	Y	N	N	Y	Y	N	N	N	Y	Y	N	N	Y	Y	N	Y	Y	Y	N
EU (Frankfurt)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
EU (Ireland)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
EU (London)	Y	Y	Y	Y	y*	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
EU (Paris)	Y	Y	Y	Y	y*	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y
South America (São Paulo)	Y	Y	Y	Y	y*	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
GovCloud	Y	Y	N	N	N	Y	Y	N	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y	Y	N

Licensing and Publishing of the Code

Licensing

- Amazon Software License: https://w.amazon.com/index.php/Open_Source/LicensingForGitHubProjectsI

Publishing the Code to Github

- Yes, we will host it in GitHub once we make it publicly deployable later in 2018, now it is available through SA, ProServe or trained partners

- **What will we publish?**
  - The entire solution, including templates, lambda, step function and all other components

Access to the solution

- Current access is through account teams through SA (Immersion Day), ProServe, or Partner
- Later in 2018 we intend to make the solution self-service (downloadable from the website)

After Landing Zone is set up:

- Use and extend the Landing Zone (see User & Developer Guides)
- Create a workload account using the Account Vending Machine (AVM)
- Deploy a solution in <2 hours using AWS Solutions / QuickStarts in the new accounts
- Discuss how to operate in the new environment

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