About me

Solution Architect
AWS User Group Organizer
5 years using AWS

@zamirajaupaj

mobiquity

Agenda

- Control Tower
- AWS Landing Zone

How I build and implement Landing Zone?

- **Additional product and services, there there's plenty of design decisions:**
- **How many accounts should I create?**
- **which would my network topology look like?**
- **How many services don't launch?**
- **what are my security, governance and baselines?**
- **And how do I deploy that in a way?**

Speed and easy way

Scalability

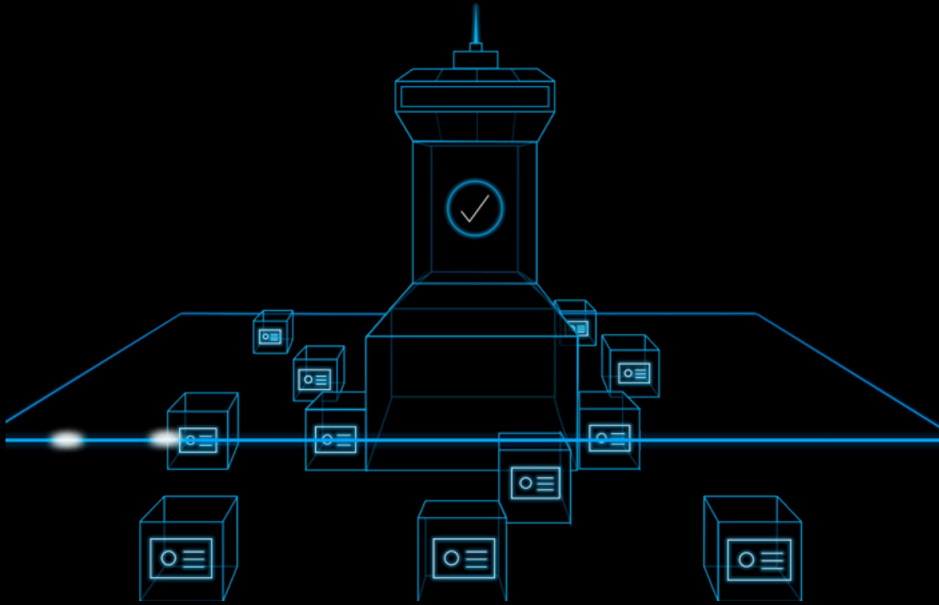
HOW WE WORK

Hight Availability

Security

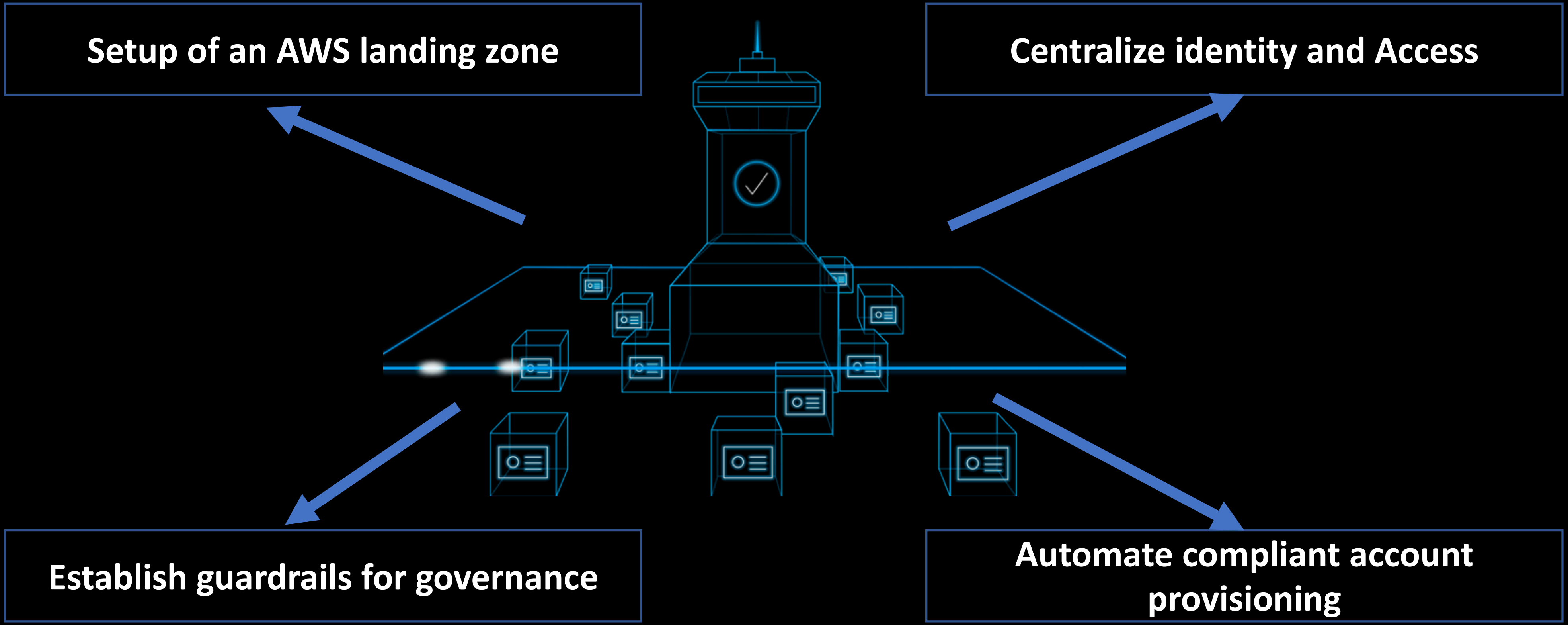
What Control Tower do?

- Quickly setup and configure a new AWS environment
- Automate ongoing policy management



@zamirajaupaj

Control Tower



Setup of an AWS landing zone

Centralize identity and Access

Establish guardrails for governance

Automate compliant account provisioning

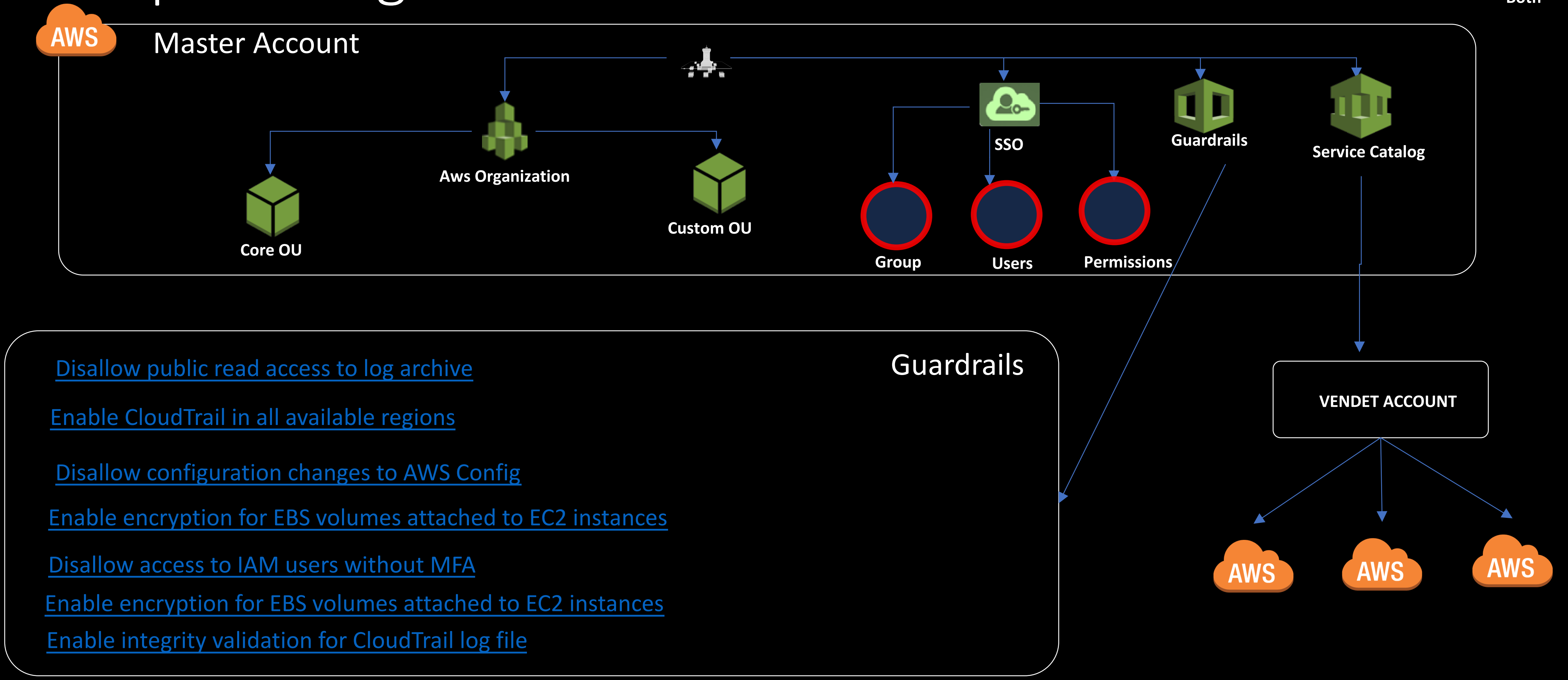
@zamirajaupaj

What AWS Landing Zone do?

- Setup, in a 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

Setup Landing Zone

default
Custom
Both



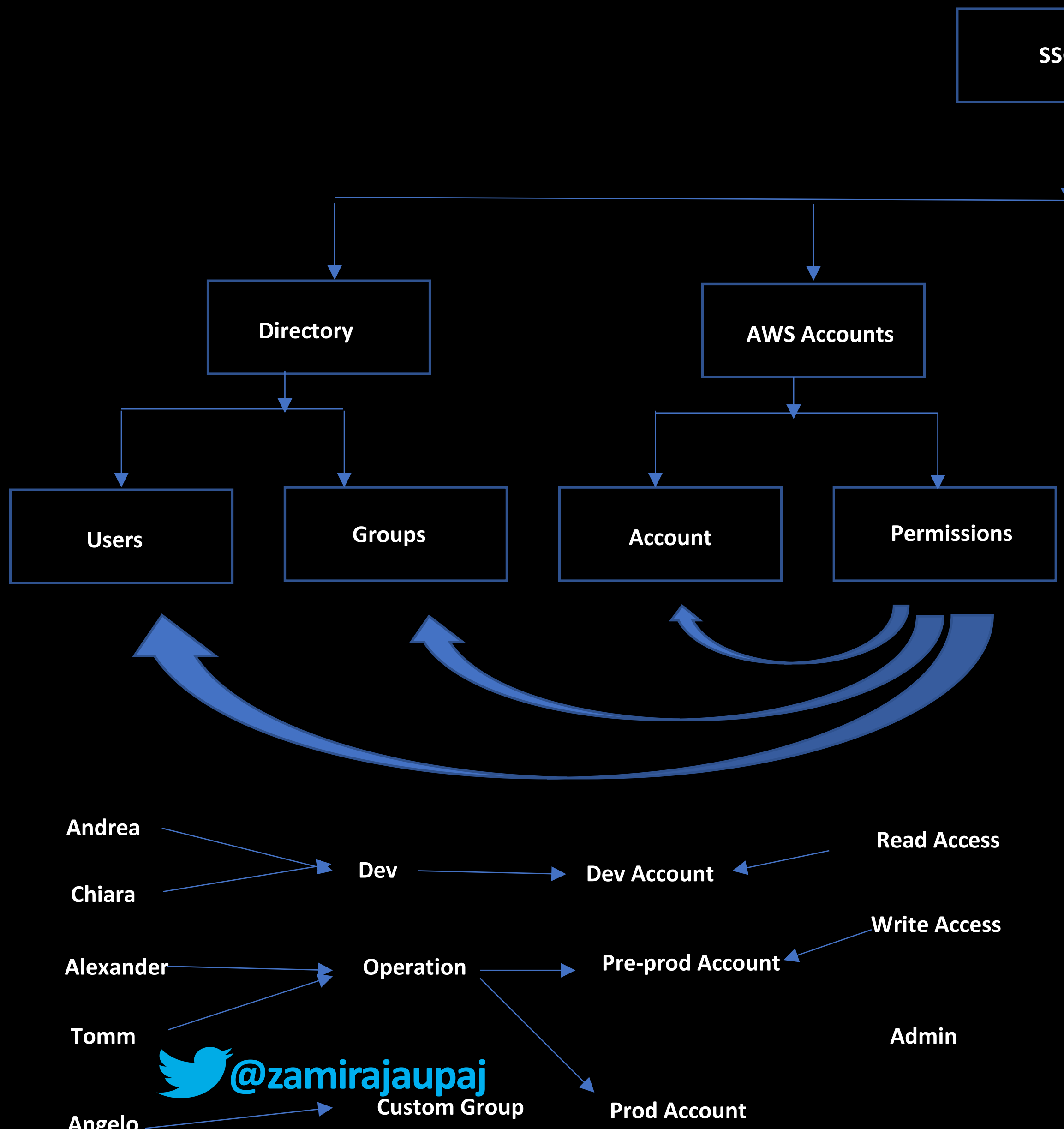
Guardrails

- Disallow public read access to log archive
- Enable CloudTrail in all available regions
- Disallow configuration changes to AWS Config
- Enable encryption for EBS volumes attached to EC2 instances
- Disallow access to IAM users without MFA
- Enable encryption for EBS volumes attached to EC2 instances
- Enable integrity validation for CloudTrail log file

@zamirajaupaj

mobiquity

Centralize identity and Access



SSO

Directory

AWS Accounts

Application

Dashboard

Users

Groups

Account

Permissions

Custom Applications

Andrea

Chiara

Dev

Dev Account

Read Access

Write Access

Alexander

Operation

Pre-prod Account

Tomm

Admin

Angelo

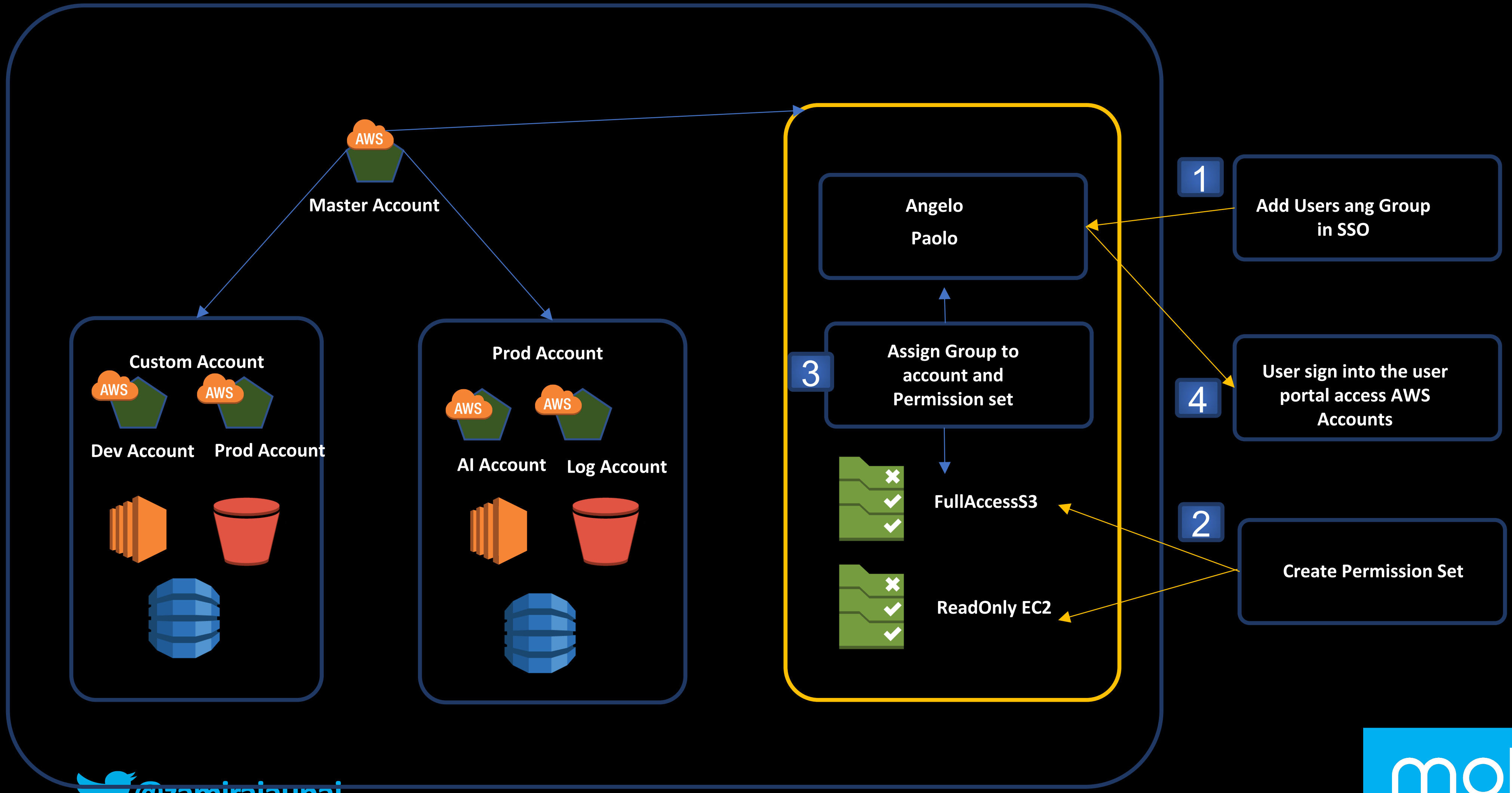
Custom Group

Prod Account

NO IAM USER

@zamirajaupaj

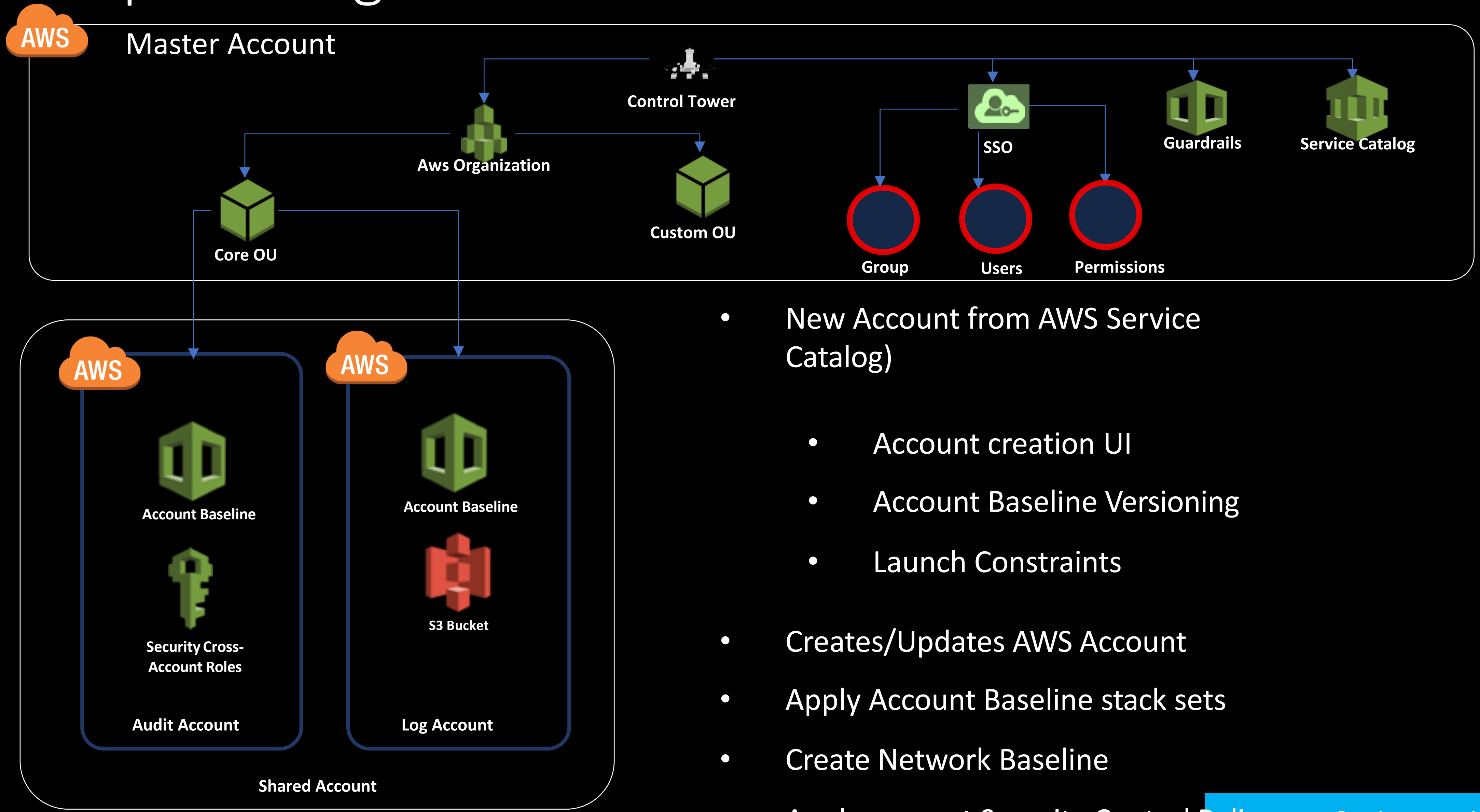
SSO



@zamirajaupaj

mobiquity

Setup Landing Zone



- New Account from 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

@zamirajaupaj

Account baseline

AWS CloudTrail

- Central Amazon S3 bucket and local AWS CloudWatch Logs

AWS Config

- 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

More …

Baseline Requirements

Lock

AWS Account Credential Management (“Root Account”)

Federate

Use Identity Solutions

Enable

AWS CloudTrail

Establish

InfoSec Cross Account Roles

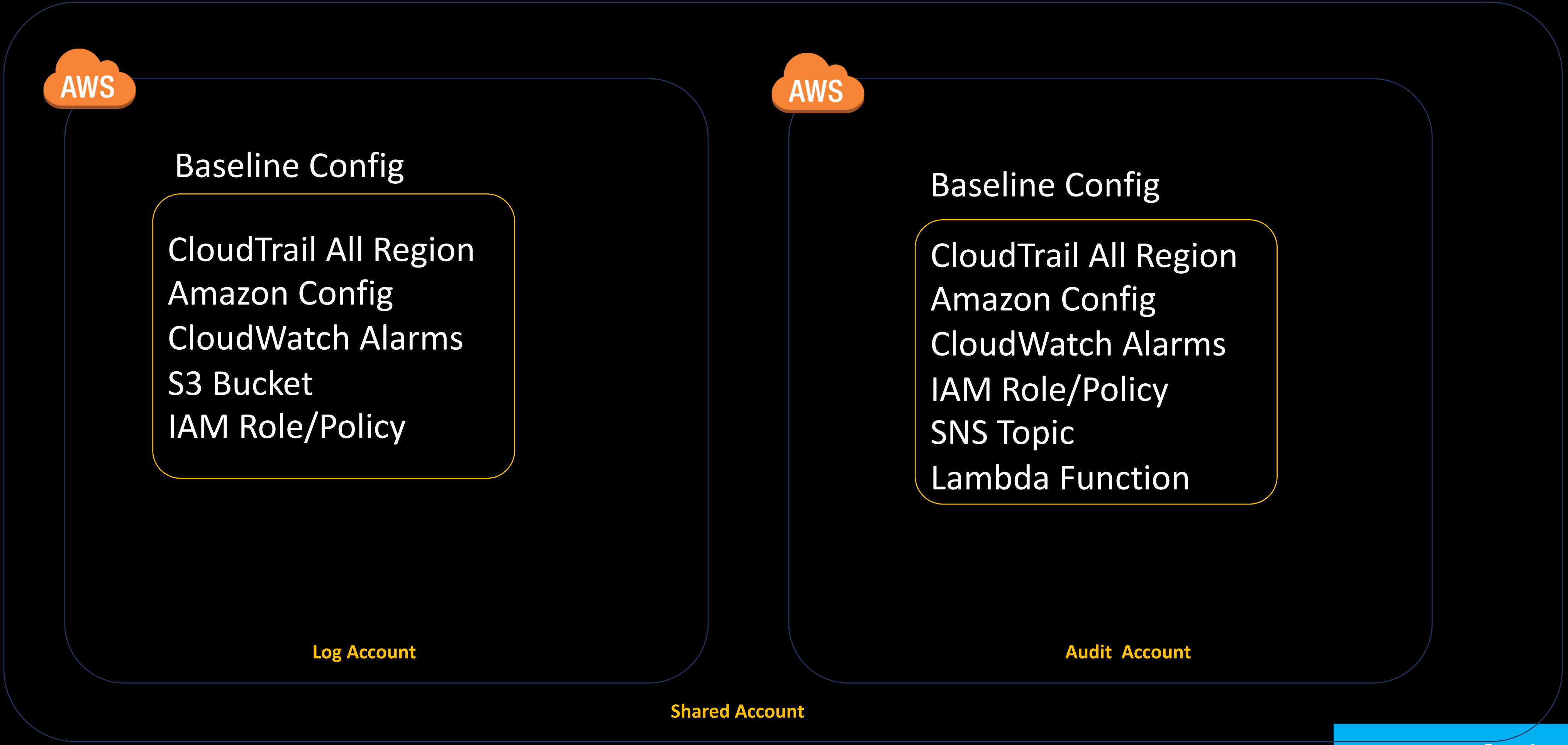
Define

Map Enterprise Roles and Permissions

Identify

Actions and Conditions to Enforce Governance

Shared Account



Baseline Config

- CloudTrail All Region
- Amazon Config
- CloudWatch Alarms
- S3 Bucket
- IAM Role/Policy

Log Account

Baseline Config

- CloudTrail All Region
- Amazon Config
- CloudWatch Alarms
- IAM Role/Policy
- SNS Topic
- Lambda Function

Audit Account

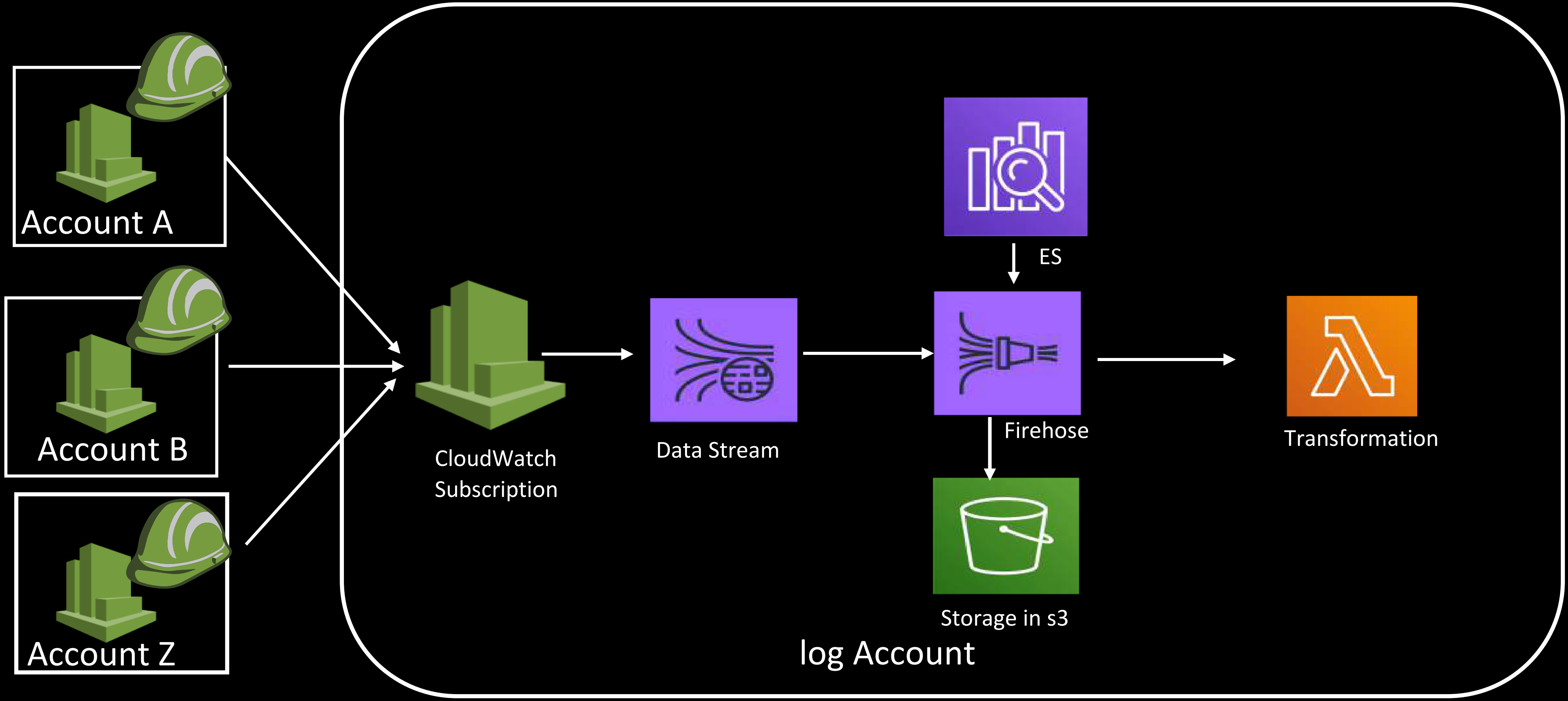
Shared Account

@zamirajaupaj

Shared Service Account!

- Services and tooling and our common to our organization
- Active Directory
- Inactive Instances
- EBS volumes
- Golden AMI
- Simple DNS
- Disaster Recovery Purpose
- Shared service network

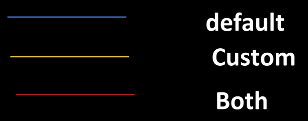
What About Logs?

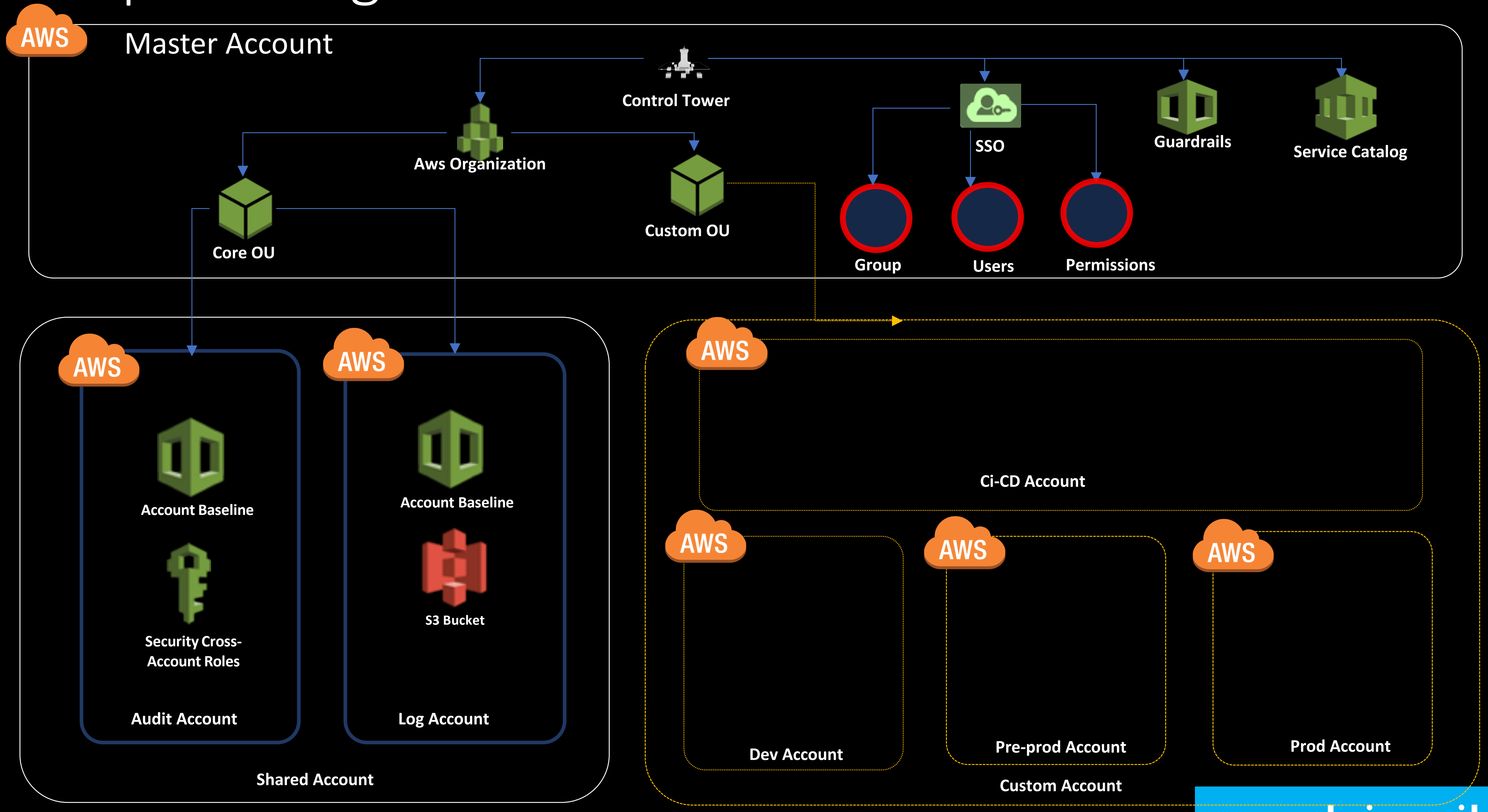


@zamirajaupaj

mobiquity

Setup Landing Zone



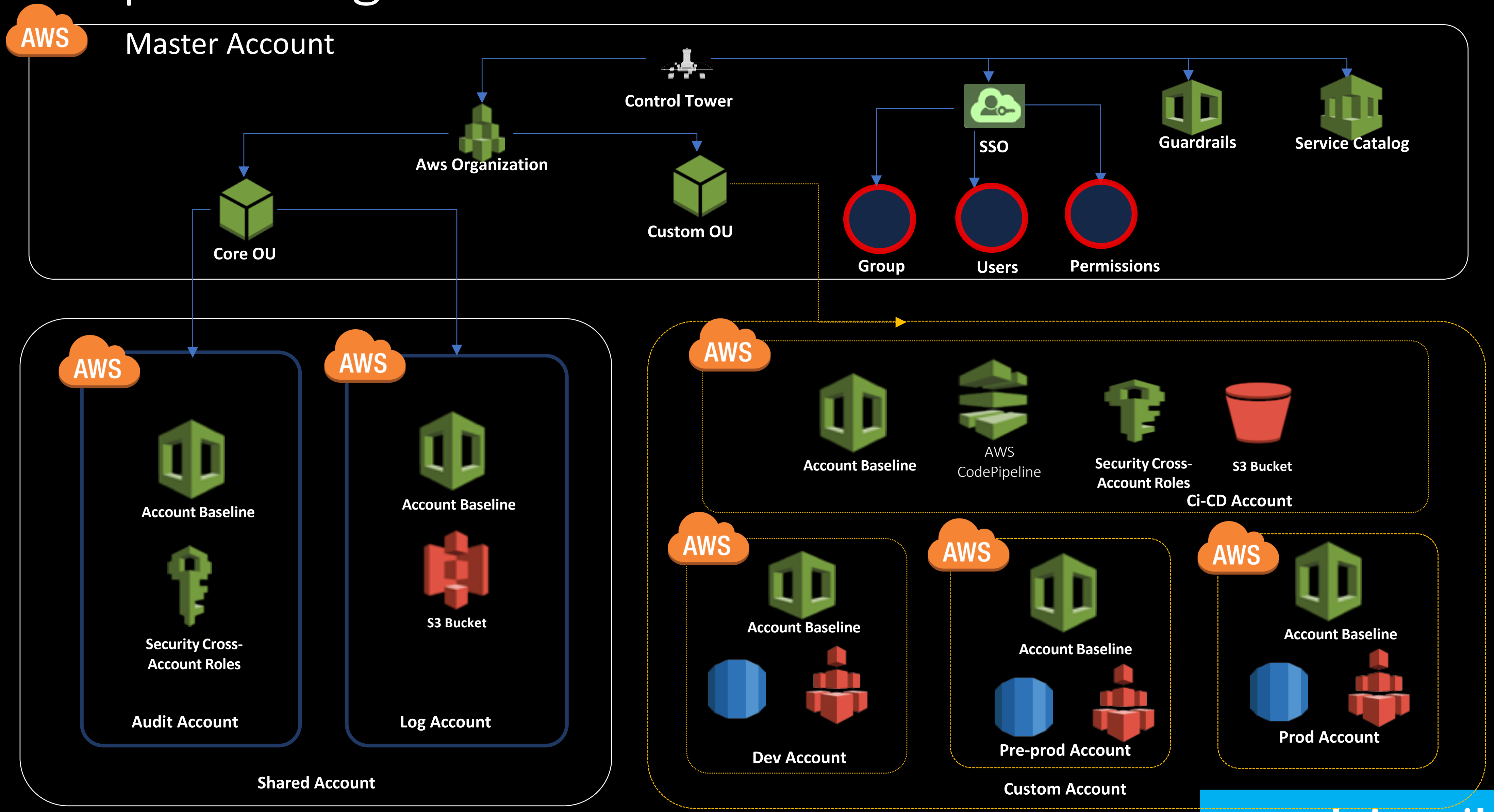


@zamirajaupaj

mobiquity

Setup Landing Zone

default
Custom
Both



AWS

Master Account

Control Tower

Aws Organization

SSO

Guardrails

Service Catalog

Core OU

Custom OU

Group

Users

Permissions

AWS

Account Baseline

Security Cross-Account Roles

Audit Account

AWS

Account Baseline

S3 Bucket

Log Account

Shared Account

AWS

Account Baseline

AWS CodePipeline

Security Cross-Account Roles

S3 Bucket

Ci-CD Account

AWS

Account Baseline

Dev Account

AWS

Account Baseline

Pre-prod Account

AWS

Account Baseline

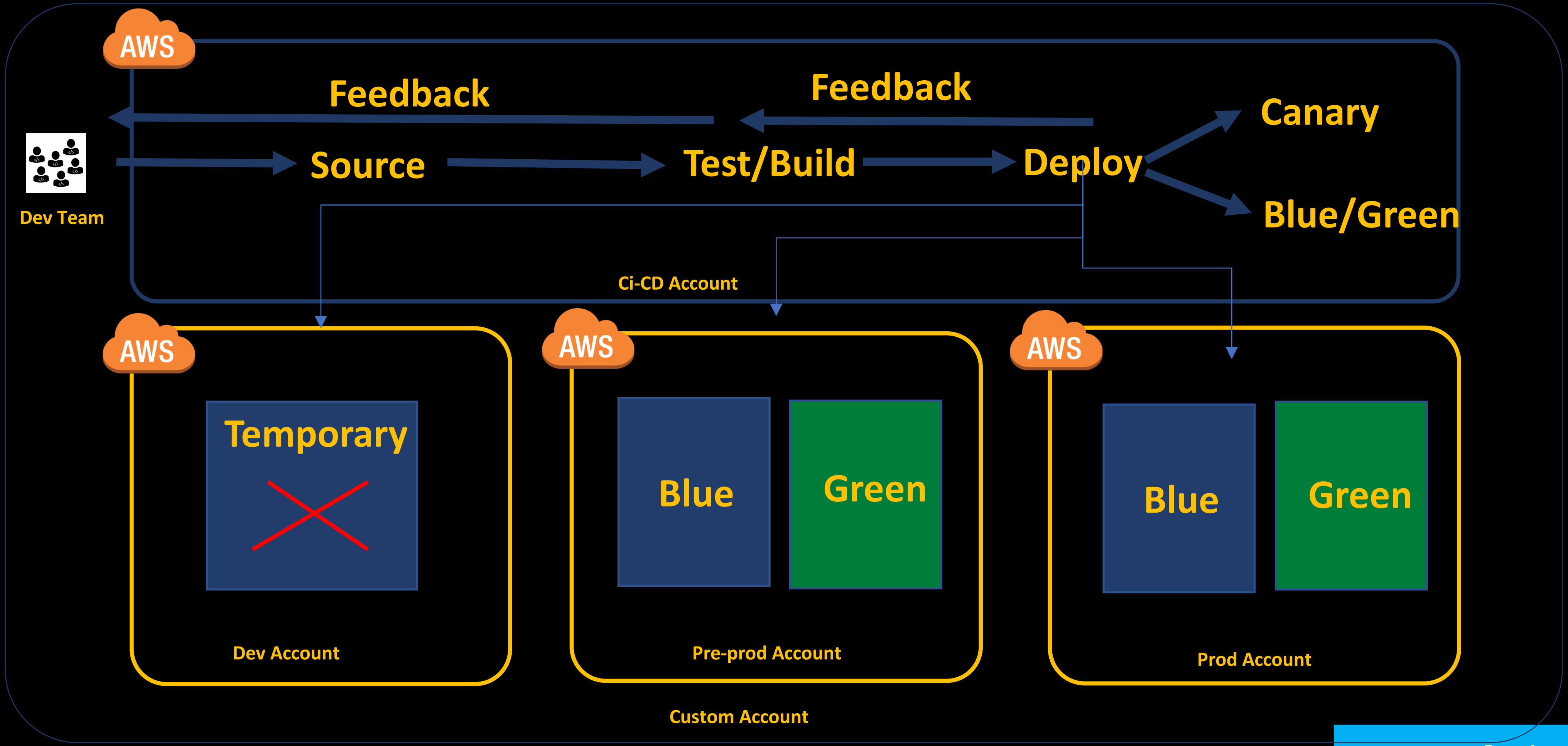
Prod Account

Custom Account

@zamirajaupaj

mobiquity

Custom Account Dev/PreProd/Prod



@zamirajaupaj

mobiquity

Benefits of the AWS Automated Landing Zone

Automated

Scalable

Self-Service

Guardrails NOT Blockers

Auditable

Flexible

@zamirajaupaj

Recommendation

EC2

SSM
NO Port 22
NO Public IP
No Key Pair

Infrastructure

Secret Manager
CloudWatch
CloudTrail
Config

HTTPS Protocol
Encryption KMS
NO IAM USER
NO Public Bucket
NO “*” per le policy

THANK YOU

@zamirajaupaj

mobiquity