Workshop – AWS Control Tower

Agenda

- Introduction to AWS Control Tower
- Quick Demo

Introduction to Control Tower

- What is Control Tower?
  - It is an AWS service that facilitates creation and management of secure multi-account AWS environment based on many security best practices standards
  - If there are multiple accounts and distributed teams working on several applications, it is very difficult to setup and manage accounts and security compliances. Control Tower solves this problem

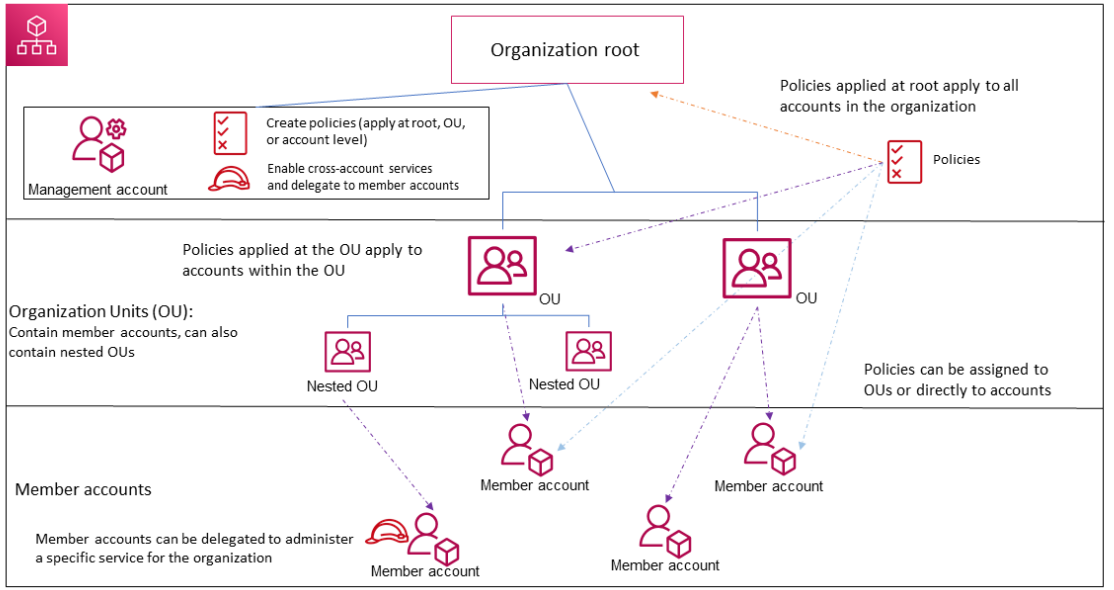
- Benefits of Control Tower
  - Can automate the setup of AWS environment with best practices blueprints for multi-account structure, IAM and account provisioning workflow
  - Easily setup and manage rules for security and compliance
  - Identity management using AWS SSO directory and access management using AWS SSO
  - Enables central logging and security audits across multiple accounts
  - Enables guardrails for governance and prevention of non-compliant resource deployment
  - Uses AWS CloudFormation for baseline, AWS Organizations Service Control Policy to prevent config changes and AWS Config rules to detect non-compliance
  - Provides visibility through the dashboard. Gives status of the resources that don’t comply with the rules enabled through preventive and detective guardrails

Pre-requisites

- AWS Organizations
- AWS Landing Zone
- Guardrails and Service control policies
- Basic Understanding of IAM, User, Group and Role
- Basic understanding of AWS Single Sign-On

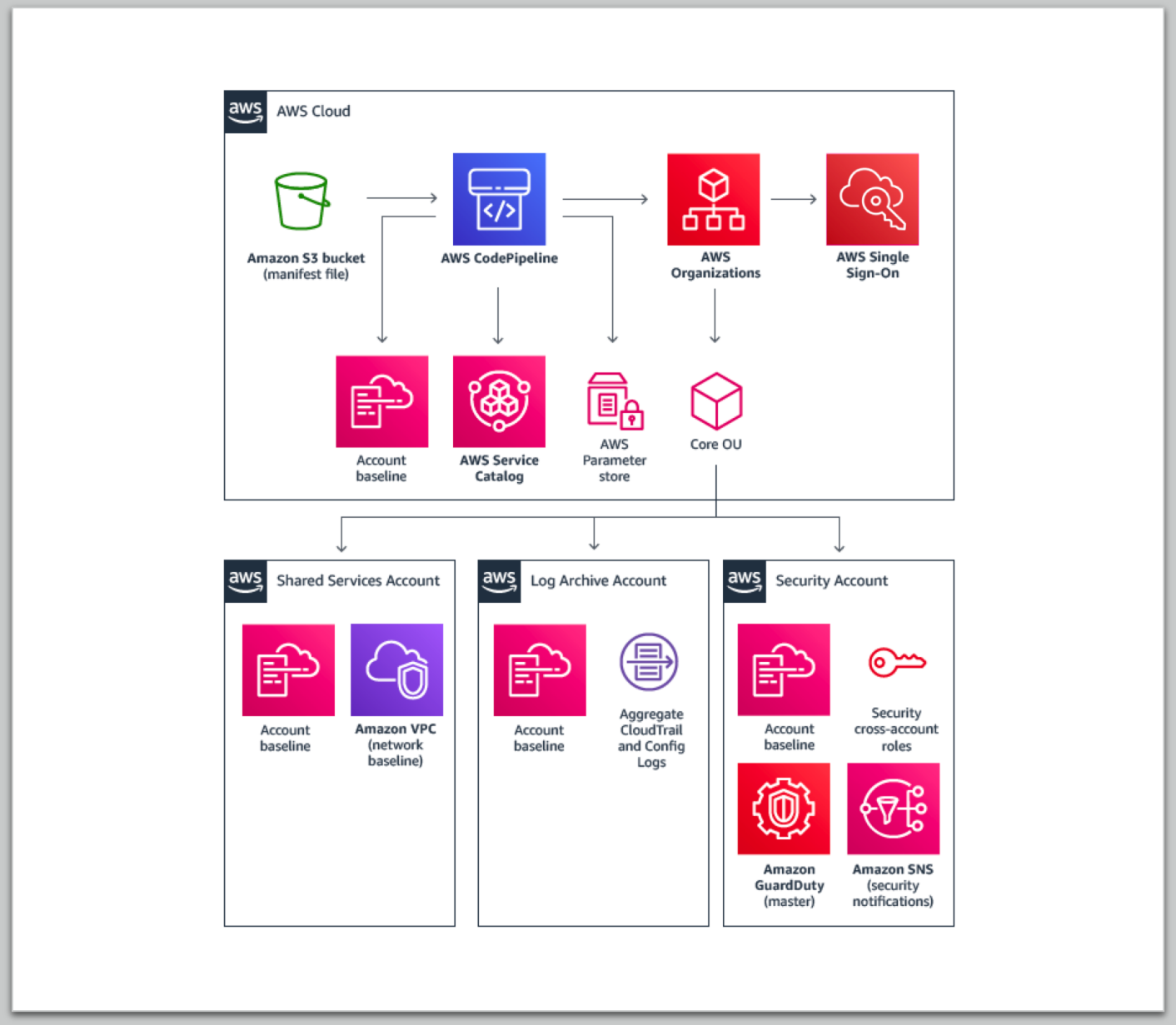
AWS Organizations

- AWS Organizations
- Centrally manage multiple accounts
- OU (Organizational Unit) : Group accounts for easy management
- Apply organizational control policies (OCP)
- Simplified Billing



AWS Landing Zone

- A pre-configured, secure, scalable, multi-account environment based on best practices blueprints
- Uses Organizations for multi account management
- Identity and federated access management using AWS SSO
- Account provisioning through AWS Service Catalog
- Centralized Cloud Trail and Config log archive using S3
- Centralized monitoring and notifications using CloudWatch and SNS



Guardrails

- High level rule that applies to the overall AWS environment
- Applies to entire Organizational Unit (OU) and all the accounts in it
- Guardrails govern all the user actions performed on the accounts
- Account provisioning through AWS Service Catalog
- Preventive and Detective guardrails are possible
- Root user and management account are exempted from the guardrail rules

- **Preventive Guardrail**
- Ensures the accounts maintain compliance
- Preventive guardrails can be enforced or not enabled
- Supported in all AWS regions
- Implemented through SCP (Service Control Policies)

- **Detective Guardrail**
- Detects policy violations
- Provides alerts through dashboards
- Status is either clear, in violation or not enabled
- Applies to AWS regions where control tower is supported
- Implemented through AWS Config rules

Service Control Policies

- Type of organizational policy that can be used to manage permissions
- Central control across all accounts in the organization
- SCP defines the guardrail or sets limits on the actions that can be delegated to the sub accounts
- IAM policies are still required at the user and role level permissions
- Combination of SCP and IAM based polices to be used for effective management

- **SCP Example**
- Restrict creation of EC2 instance types other than t2.micro

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

Config Rules

- Used to ensure if the AWS resources comply with the best practices
- Define scope to constrain which resource will trigger a rule evaluation
- Attribute level compliance can be ensured with config rules
- Rule evaluation can be triggered if resource configuration changes or scheduled periodically
- Resource config rule compliance status can be viewed from the dashboard

- **Example**
- Managed Rule -ACCOUNT_PART_OF_ORGANIZATIONS (Periodic)
- Managed Rule - S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS (Change)

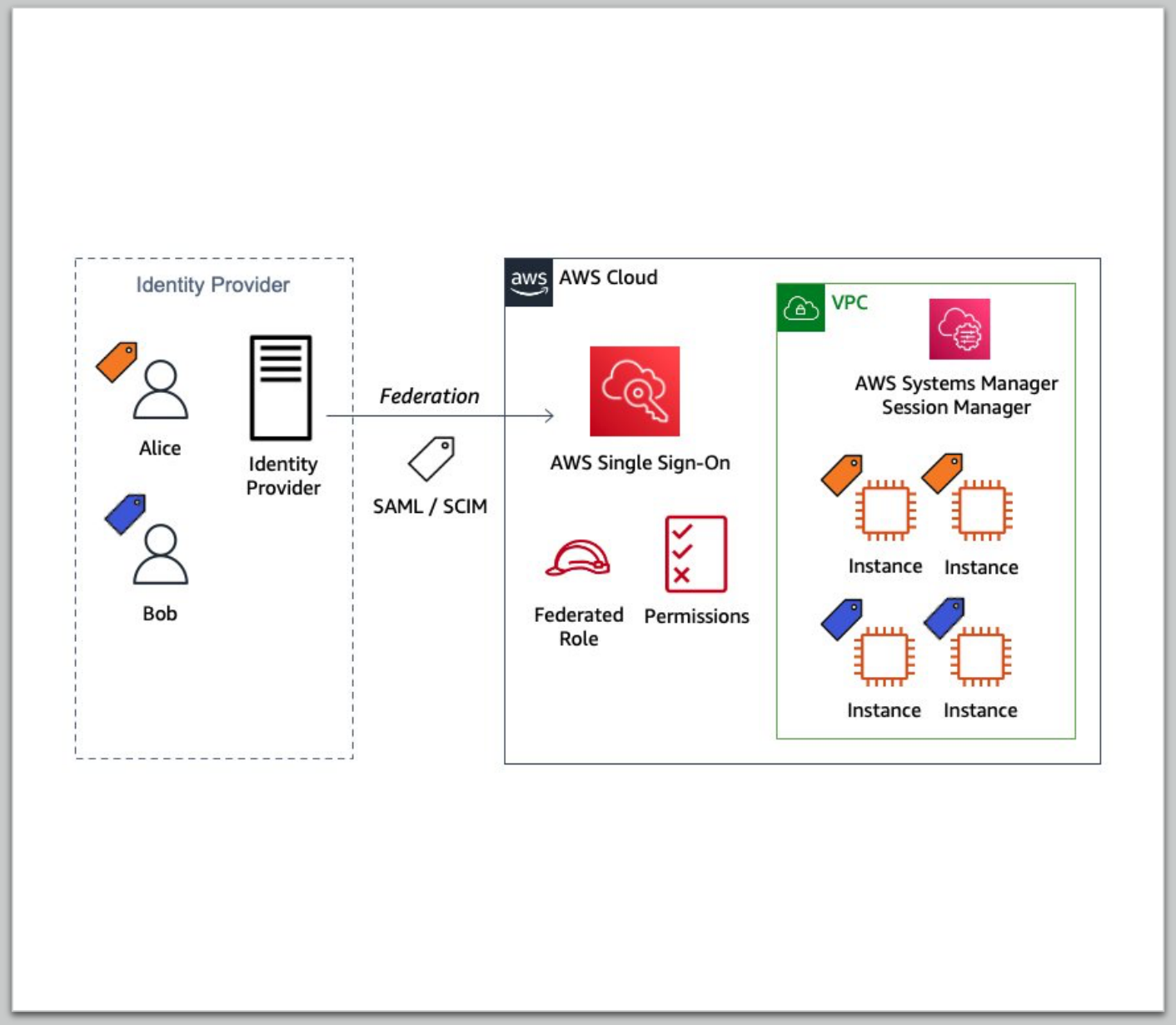
```
# This rule checks if point in time recovery (PITR) is enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
        let pitr = supplementaryConfiguration.ContinuousBackup
        %pitr == "ENABLED"
}
```

AWS SSO

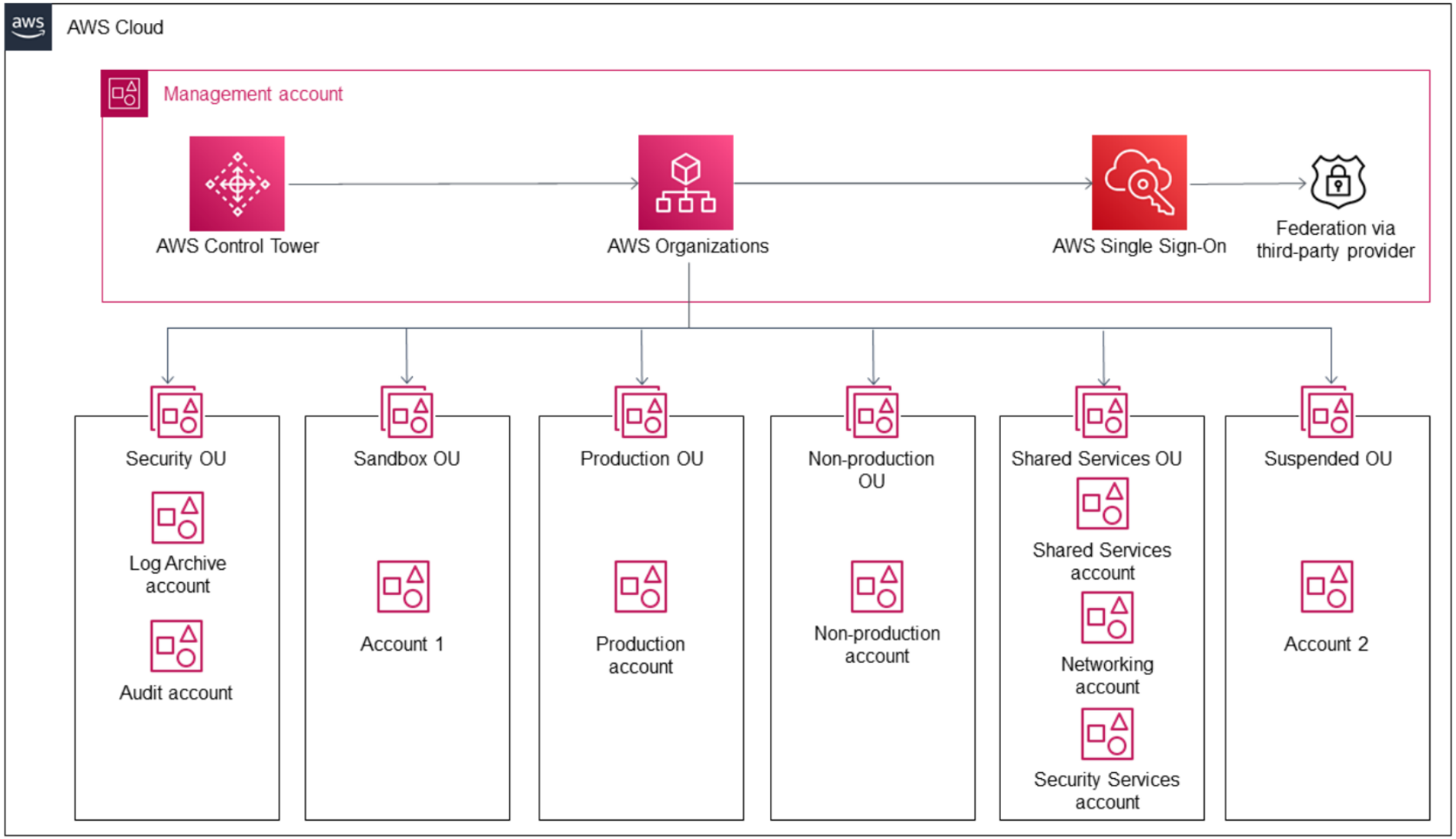
- Supports federated identity providers
- Supports SAML based applications
- Supports AD as identity store and has AWS SSO identity store
- Permissions managed centrally
- Accounts can access the services without directly using a IAM user account



Key Features

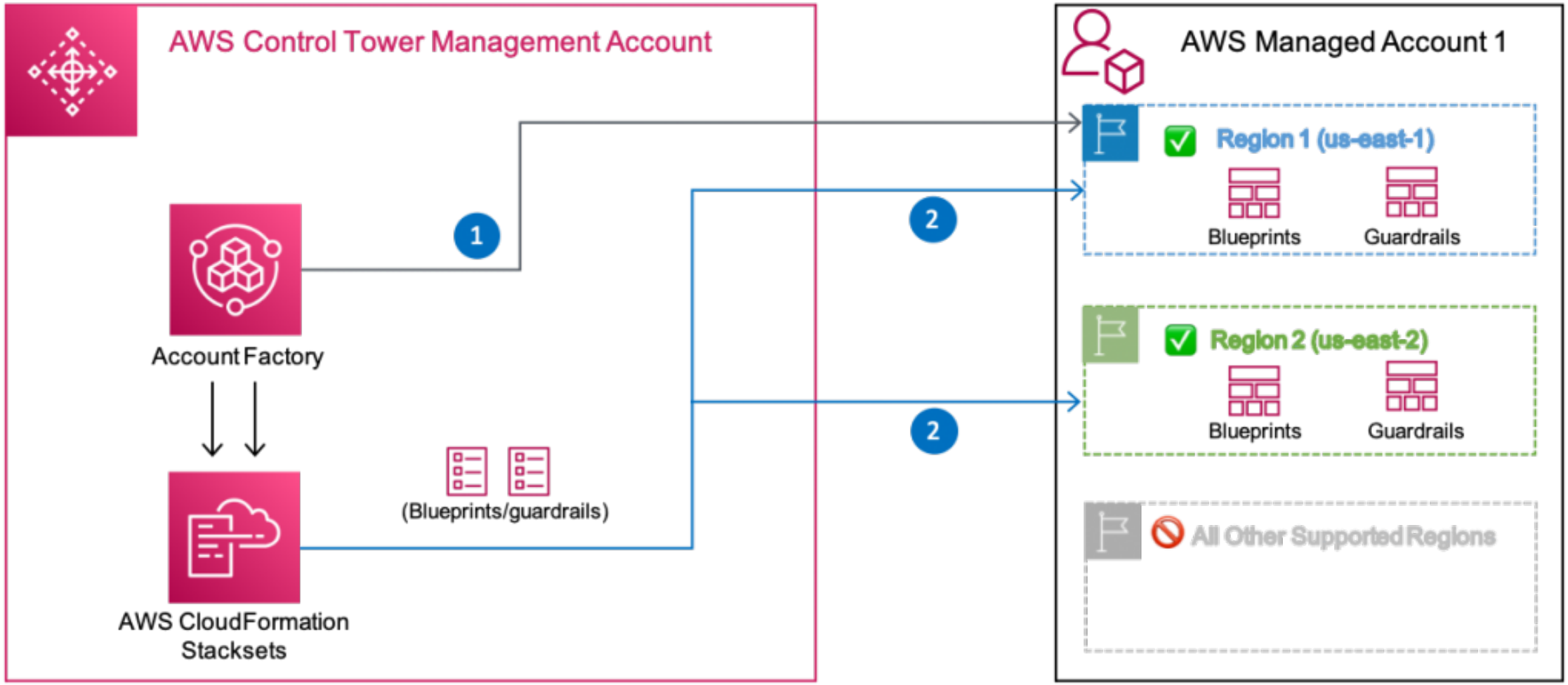
- Landing zone automation along with best practices blueprints
- Guardrails for policy management
- Account factory for user account management
- Built in identity and access management
- Pre-configured log archive and audit access to accounts
- Dashboard for visibility and actions
- Built-in monitoring and notifications
- Centralized billing for all accounts

Architecture



Reference from aws.amazon.com

Account Factory



Reference from aws.amazon.com

Key Steps to Enable Governance

- Set up an AWS Landing Zone
- Establish guardrails
- Automate compliant account provisioning
- Centralized Identity and Access Management

Set up an AWS Landing Zone

- Select a region and additional regions to which the guardrails to be applied
- Configure organizational units
  - Security OU
  - Sandbox OU
- Configure shared accounts for log archive and audit
- Configure service permissions
  - Provide permissions for Control Tower to access SCPs to enforce guardrails
  - IAM Roles
    - AWSControlTowerAdmin
    - AWSControlTowerStackSetRole
    - AWSControlTowerCloudTrailRole
    - AWSControlTowerConfigAggregatorRoleForOrganizations

Results of AWS Landing Zone

- When you set up a landing zone, AWS Control Tower performs the following actions in your management account on your behalf:
- Creates two AWS Organizations organizational units (OUs): Security, and Sandbox (optional), contained within the organizational root structure
- Creates two shared accounts in the Security OU: the Log Archive account and the Audit account
- Creates a cloud-native directory in AWS SSO, with preconfigured groups and single sign-on access
- Applies 20 mandatory, preventive guardrails to enforce policies
- Applies two mandatory, detective guardrails to detect configuration violations
- Preventive guardrails are not applied to the management account
- Except for the management account, guardrails are applied to the organization as a whole

References

Links

https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html
https://aws.amazon.com/blogs/architecture/field-notes-aws-control-tower-governance-on-selected-regions-and-improved-account-provisioning/
https://aws.amazon.com/solutions/implementations/aws-landing-zone/
https://docs.aws.amazon.com/prescriptive-guidance/latest/designing-control-tower-landing-zone/designing-control-tower-landing-zone.pdf
https://docs.aws.amazon.com/controltower/latest/userguide/how-control-tower-works.html#how-guardrails-work

Videos

https://www.youtube.com/watch?v=1124VPrQiWo
https://www.youtube.com/watch?v=-HsfTwdRxRI
https://www.youtube.com/watch?v=zbIrxwSy66Y
https://www.youtube.com/watch?v=_50P0o14Ul0