AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

COP319

Best practices for multi-account environments

Alex Torres
Solutions Developer
AWS

Joseph Shih
Sr. Partner SA
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

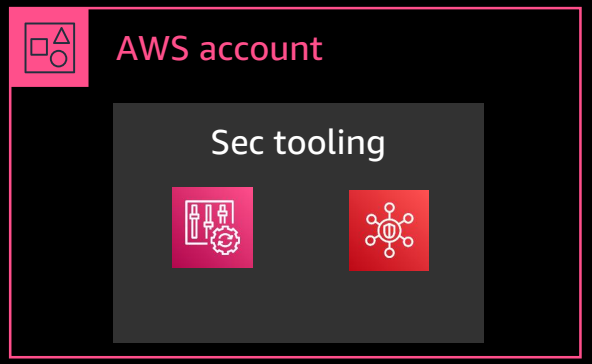
- Multi-account environments – benefits & characteristics
- Separating workloads using multiple accounts
- Architecting your environment
- Discussion
- Call to action

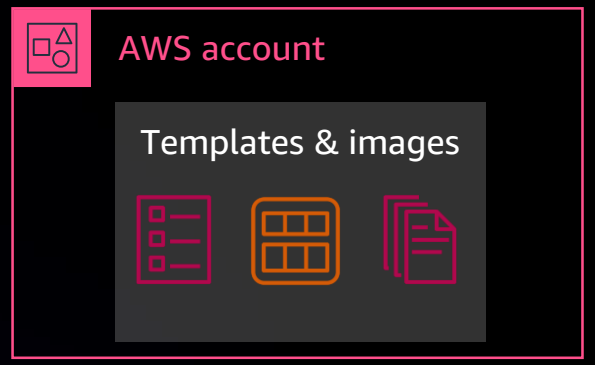
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

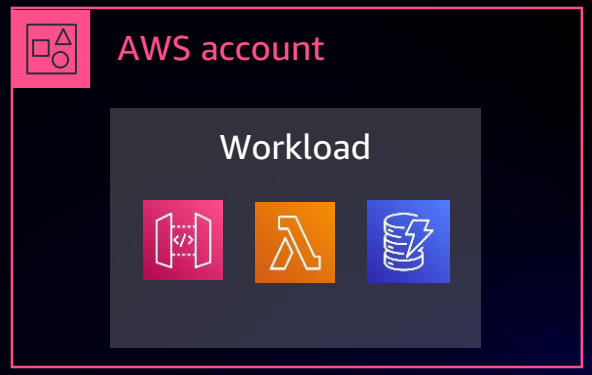
What is an AWS account?

Each AWS account:

- Is a resource container/isolation boundary for AWS services
- Is an explicit security boundary
- Is a container for cost tracking and billing

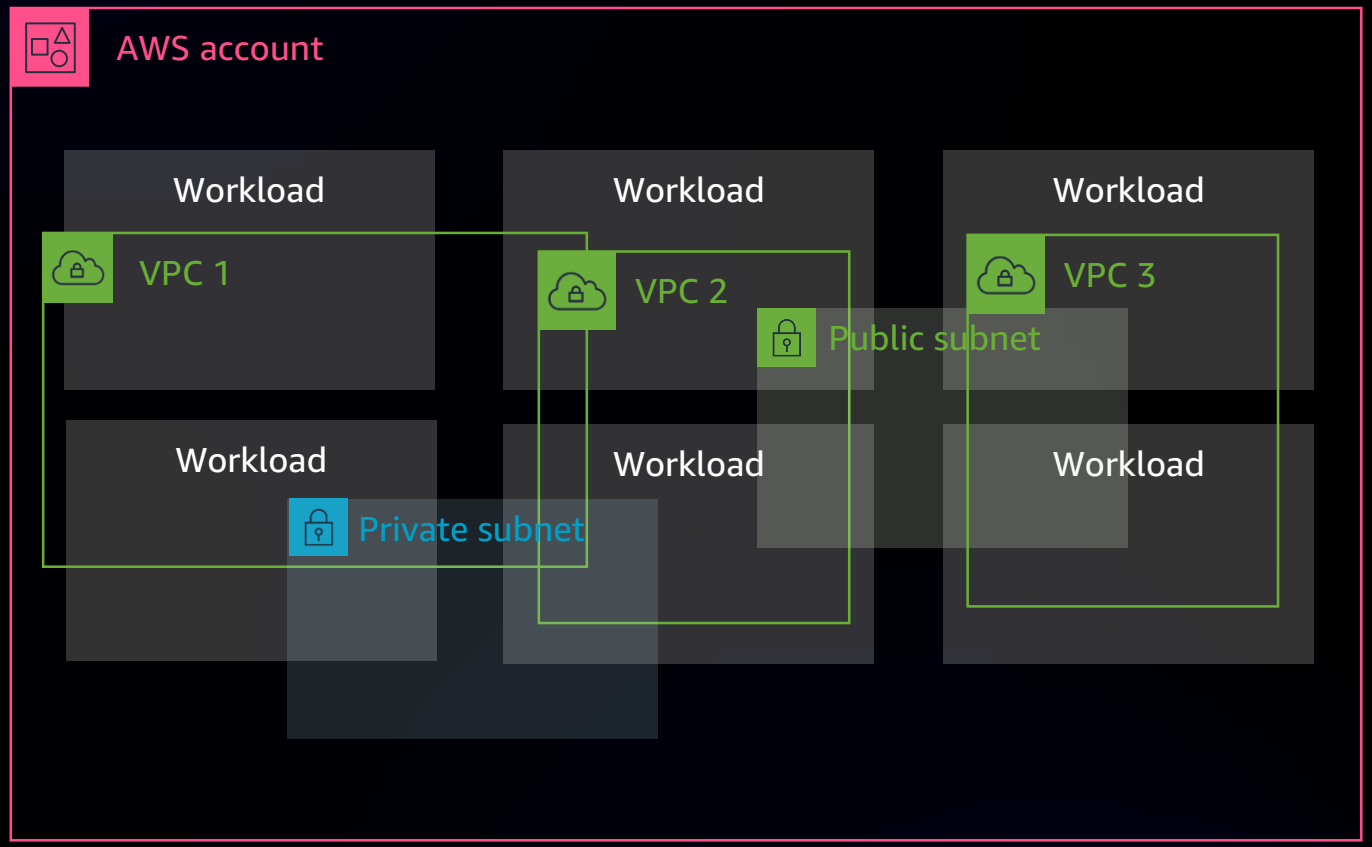






© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

With one account...



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits of a multi-account environment

Benefits



Centrally provision accounts and resources



Share resources and control access



Optimize costs



Secure and audit your environment for compliance

Use cases



Many teams

Innovate with exclusive resources for each team



Business process

Organize AWS accounts



Billing

Simplify billing



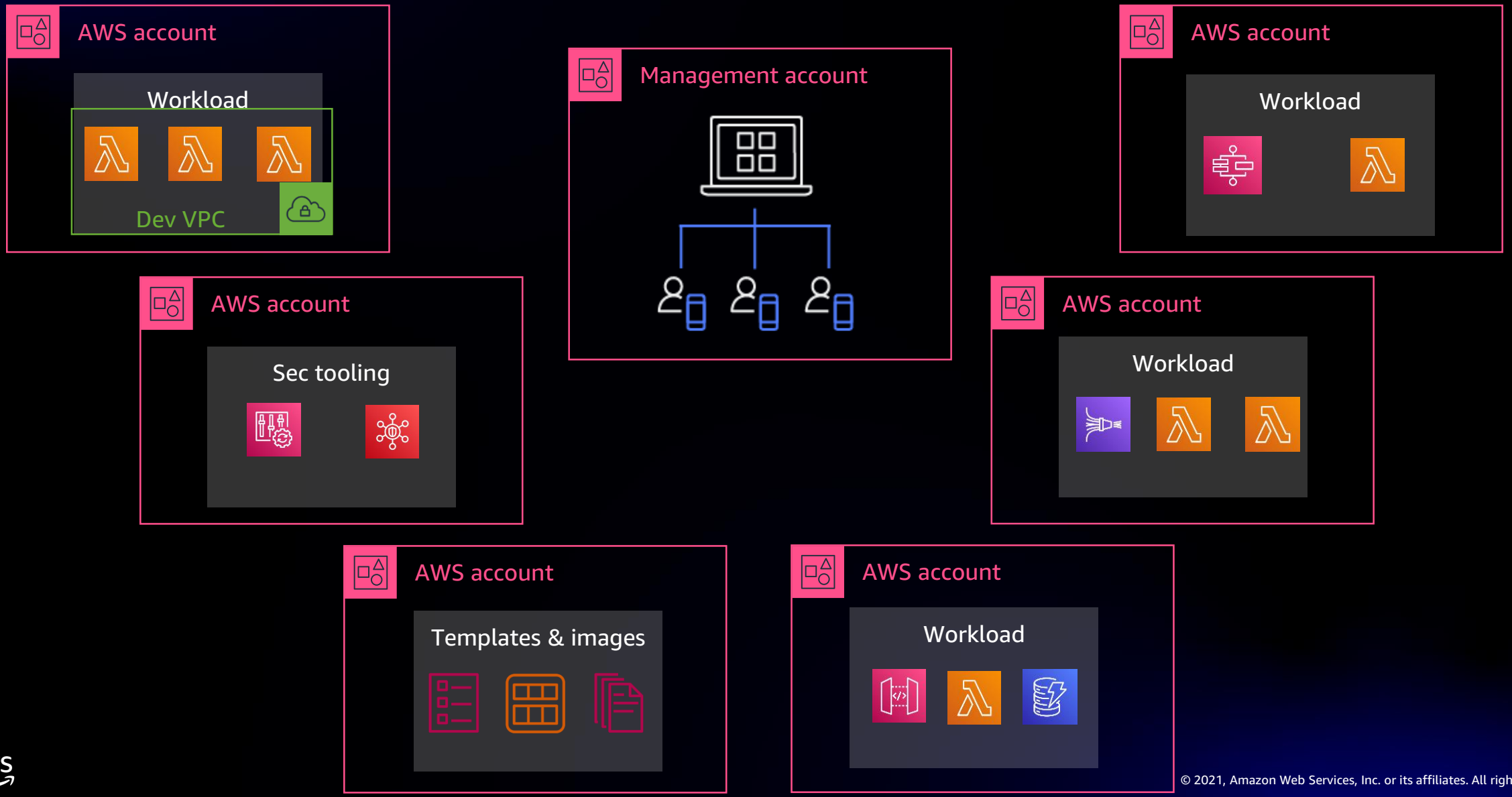
Isolation & security

Tight security boundaries

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

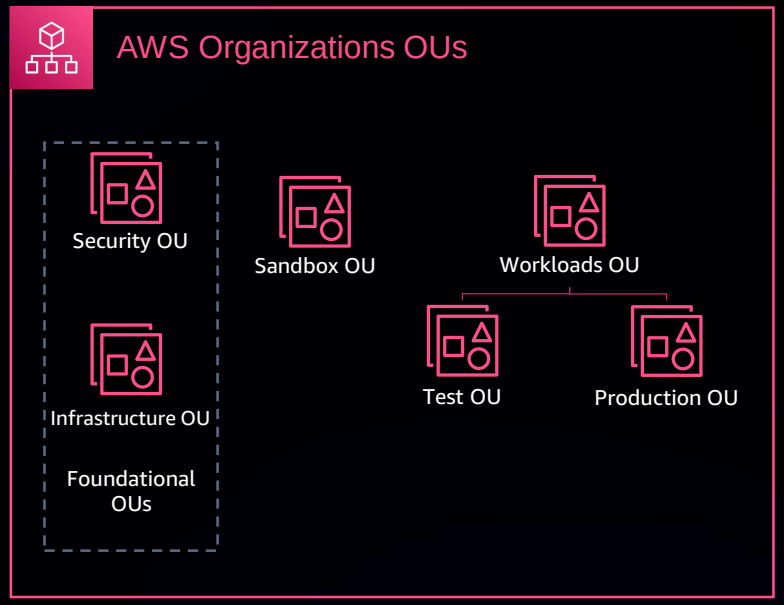
With multiple accounts...



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecting your environment

START SMALL



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

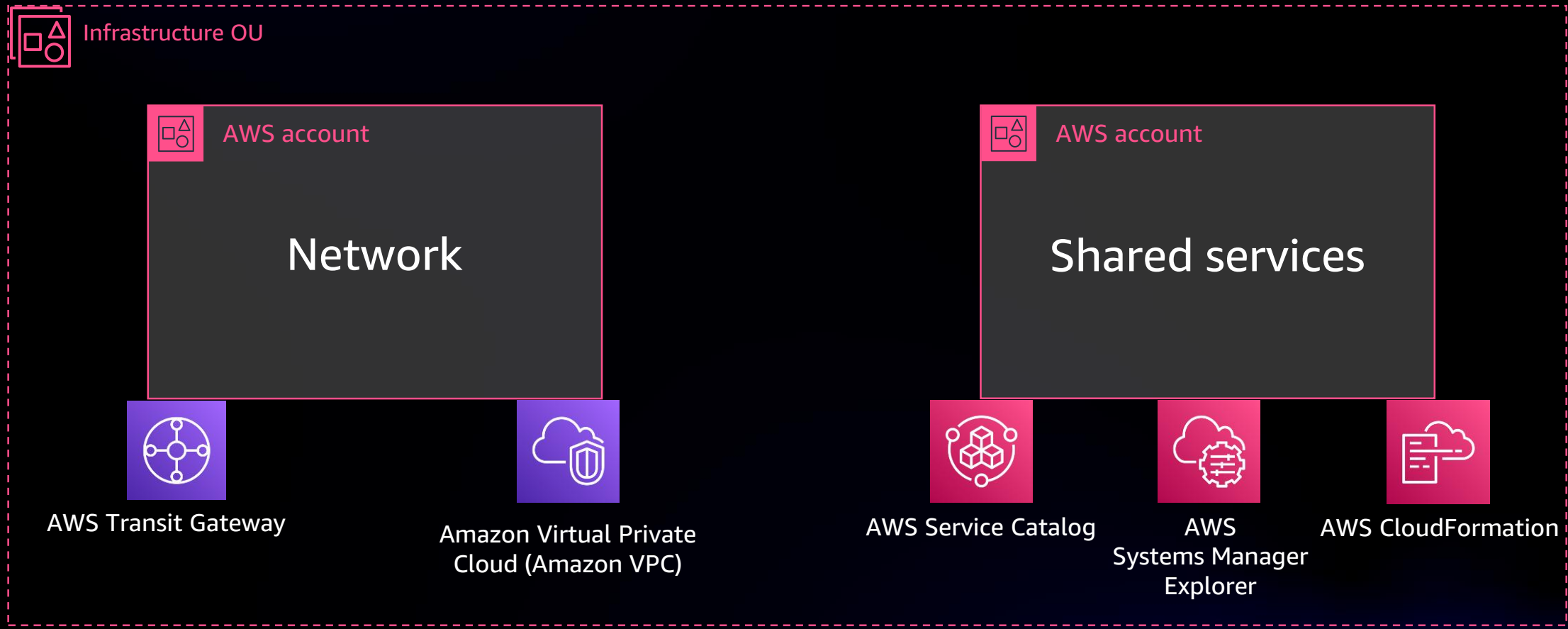
Management account

CENTRALIZE ACCESS, CONTROL, AND RESOURCE MANAGEMENT



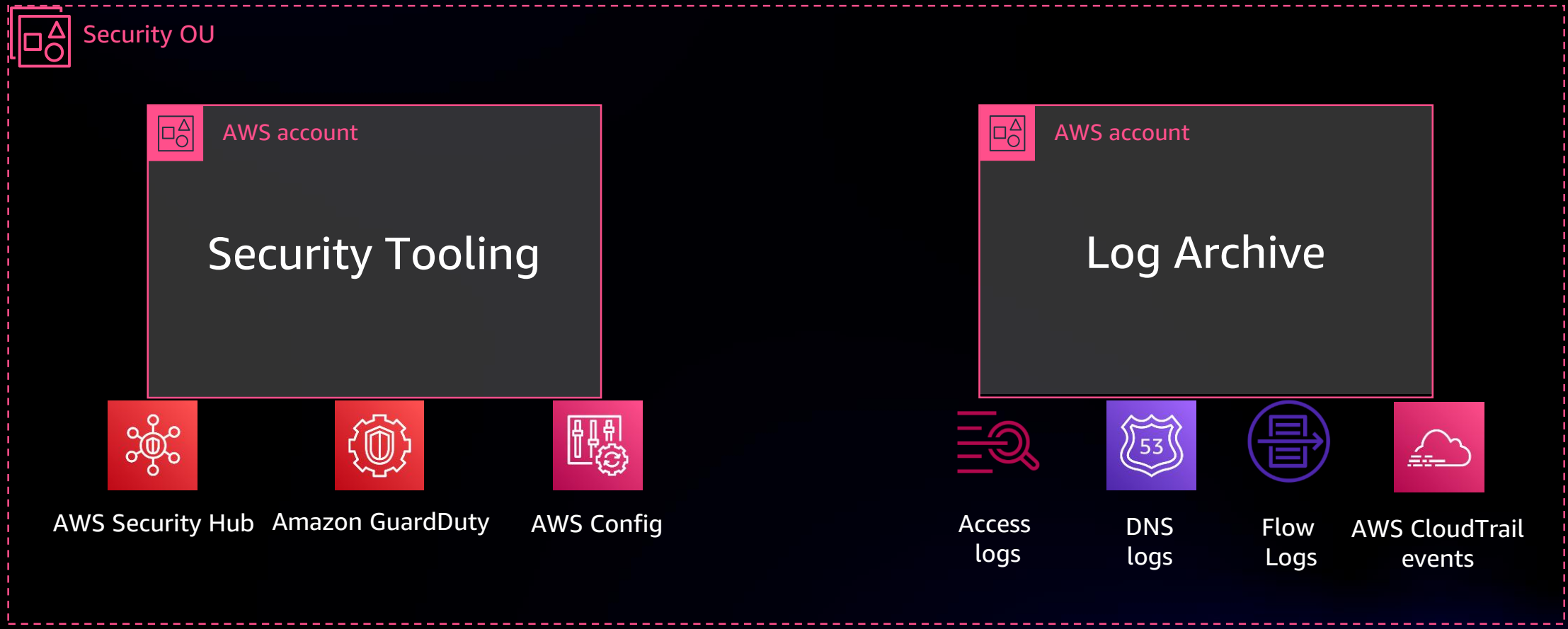
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure organizational unit



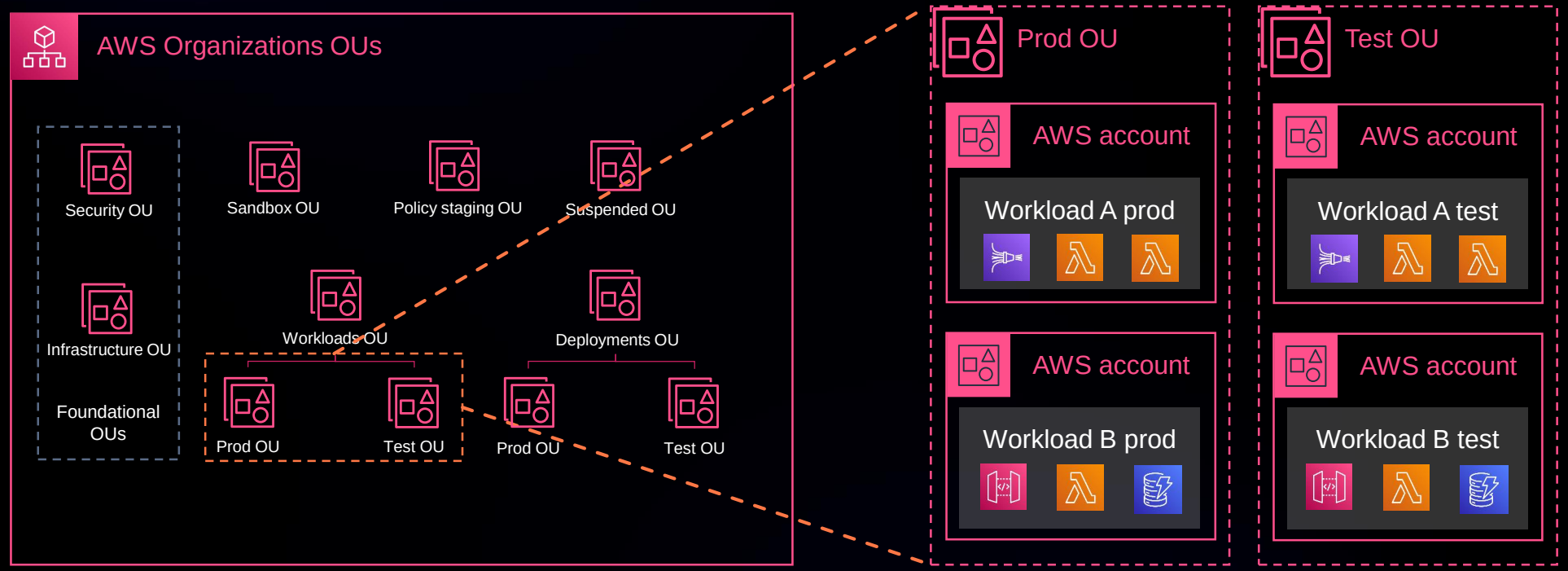
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security organizational unit



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Separating workloads in the workload OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS multi-account environment

SUMMARY

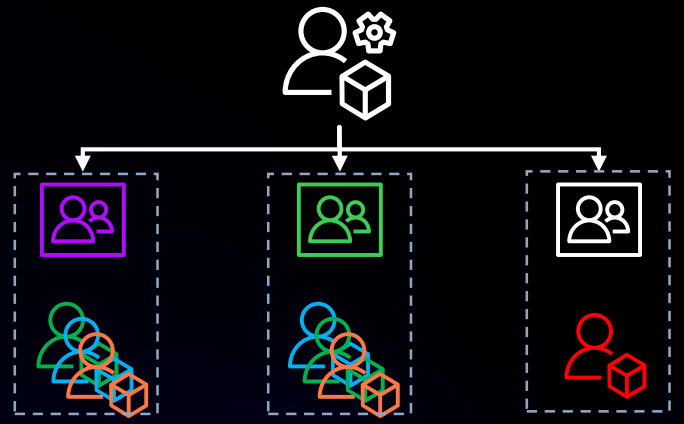
- Multiple AWS accounts



- Access control



- Environment structure
- Centralized management & operations



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Call to action

WHAT'S NEXT

- Review our multi-account strategy whitepaper for the latest guidance
- Explore AWS Organizations and AWS Control Tower
- Check out our multi-account workshops and Immersion Days
- Attend the following sessions related to multi-account if you want to learn more!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-account and foundations sessions

#CLOUD-FOUNDATIONS-TRACK

Architecture



[SEC203 – Breakout]
AWS Security Reference Architecture: Visualize your security

[ARC312 – Chalk Talk]
Architecting security & governance in multi-account environments

[ARC318 – Chalk Talk]
Designing a multi-account environment for disaster recovery

[COP319 – Chalk Talk]
Best practices for multi-account environments

Implementation



[SEC201 – Chalk Talk]
Manage and customize control policies at scale

[SEC314 – Chalk Talk]
The journey to least privilege on AWS

[DOP402 – Breakout]
Automating cross-account CI/CD pipelines

Discussion



[ARC303 – Chalk Talk]
Getting started on AWS for production workloads

[COP303– Chalk Talk]
How to prepare your cloud environment for scale and migrations

Hands-on



[COP309 - Workshop]
Managing multi-account environments following best practices

[NET308 – Workshop]
Protect your web applications across multiple AWS accounts

[ENT301 – Workshop]
Discover, plan, and migrate at scale

[ENT302 – Workshop]
Incremental refactoring: Evolve existing apps with microservices

aws

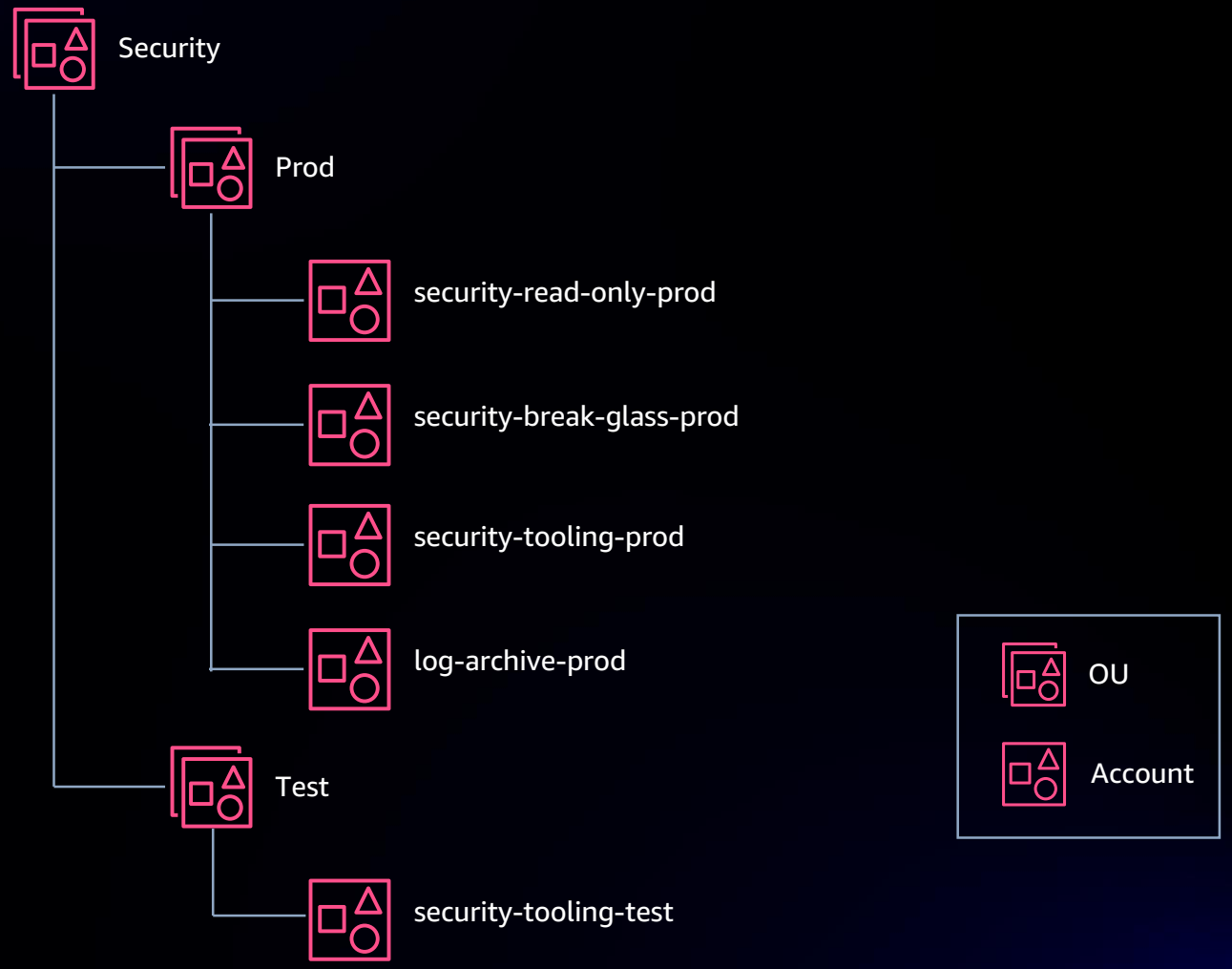
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security organizational unit

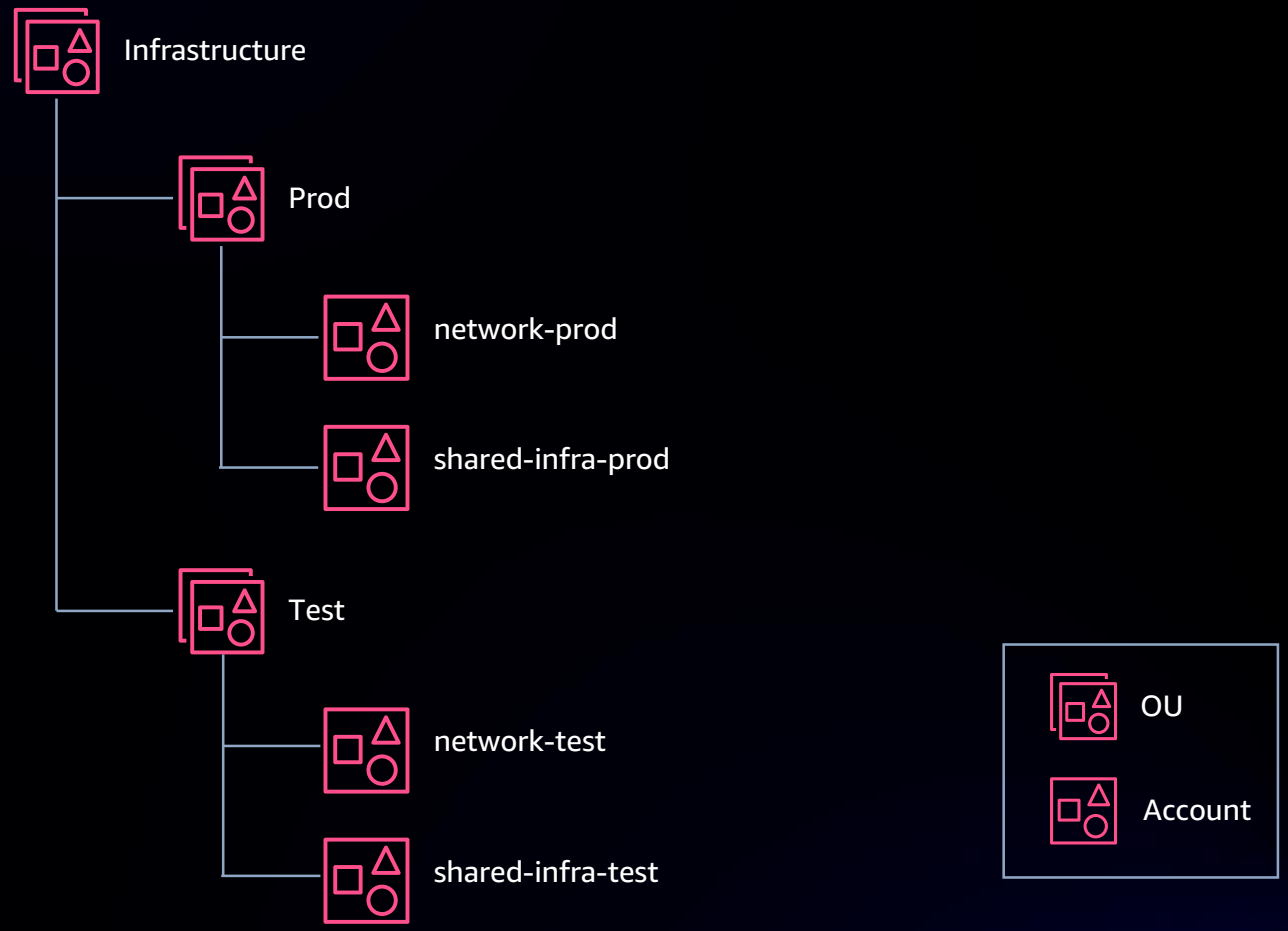
EXAMPLE STRUCTURE OF SECURITY OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure organizational unit

EXAMPLE STRUCTURE OF INFRASTRUCTURE OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sandbox organizational unit

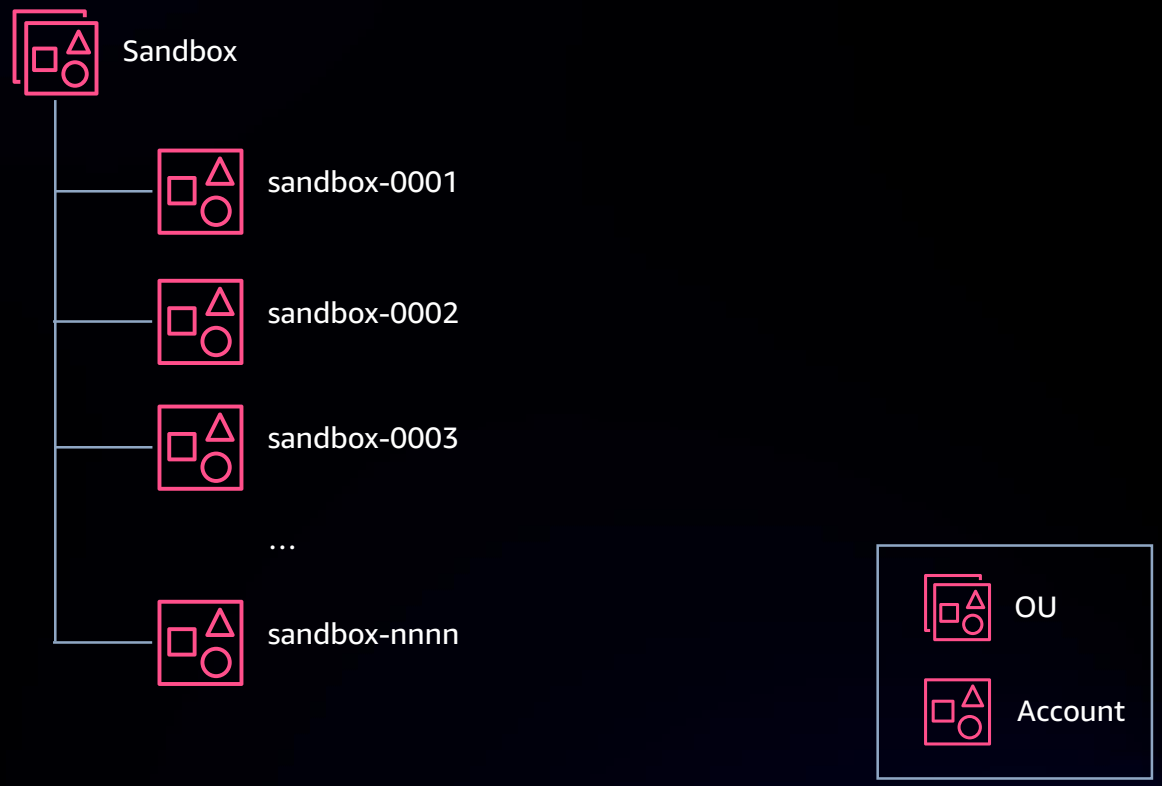
EXAMPLE STRUCTURE OF SANDBOX OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sandbox organizational unit

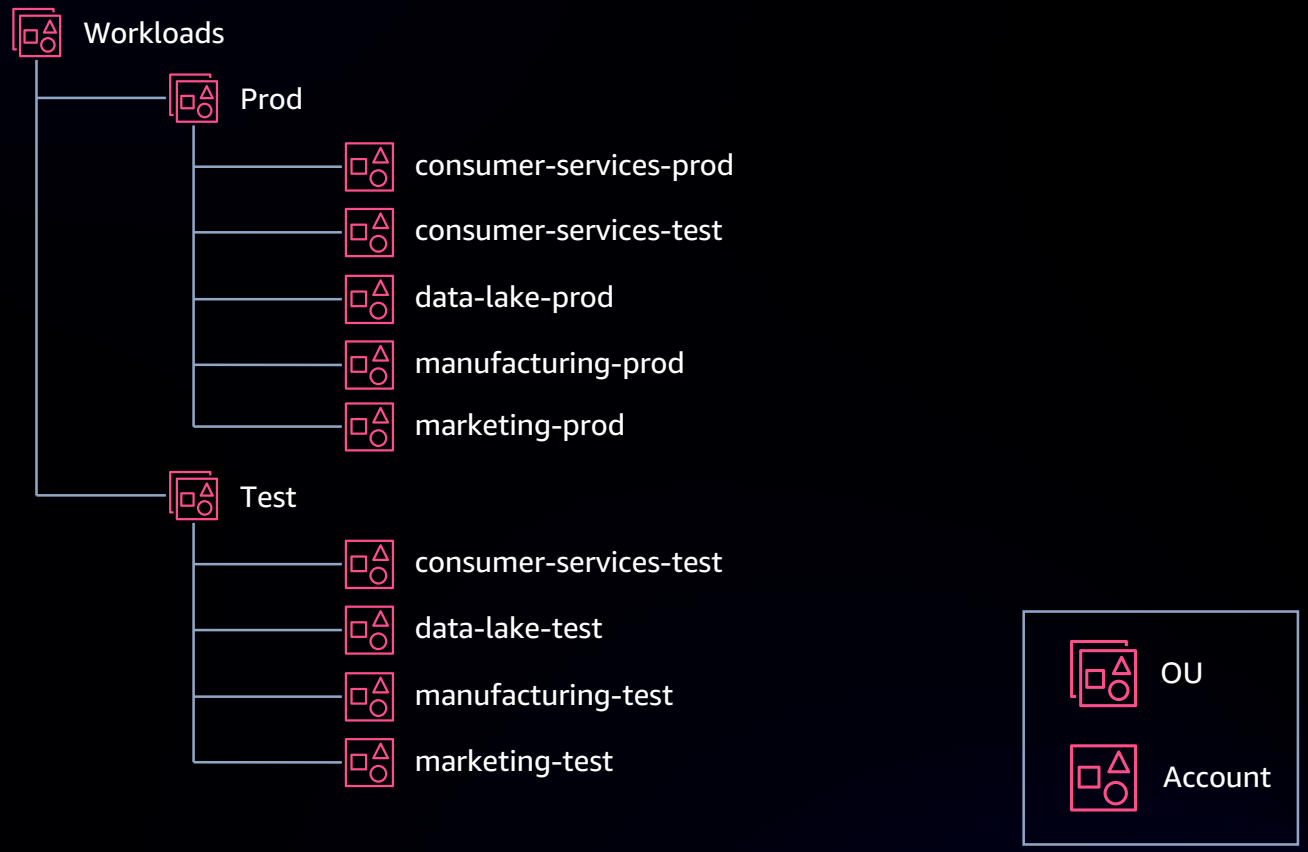
EXAMPLE STRUCTURE OF SANDBOX OU WITH RECYCLED ACCOUNTS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workloads organizational unit

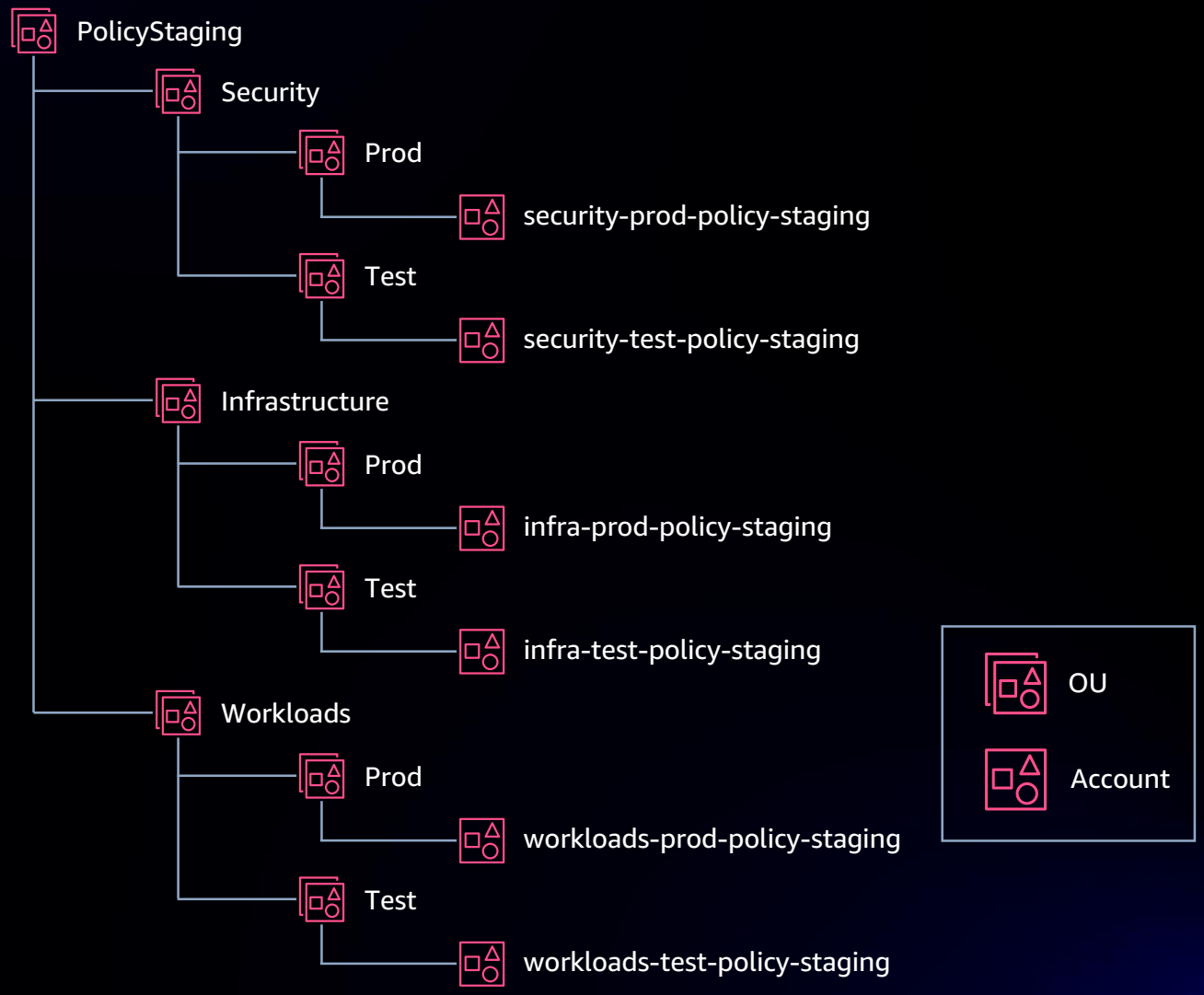
EXAMPLE STRUCTURE OF WORKLOADS OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Policy staging organizational unit

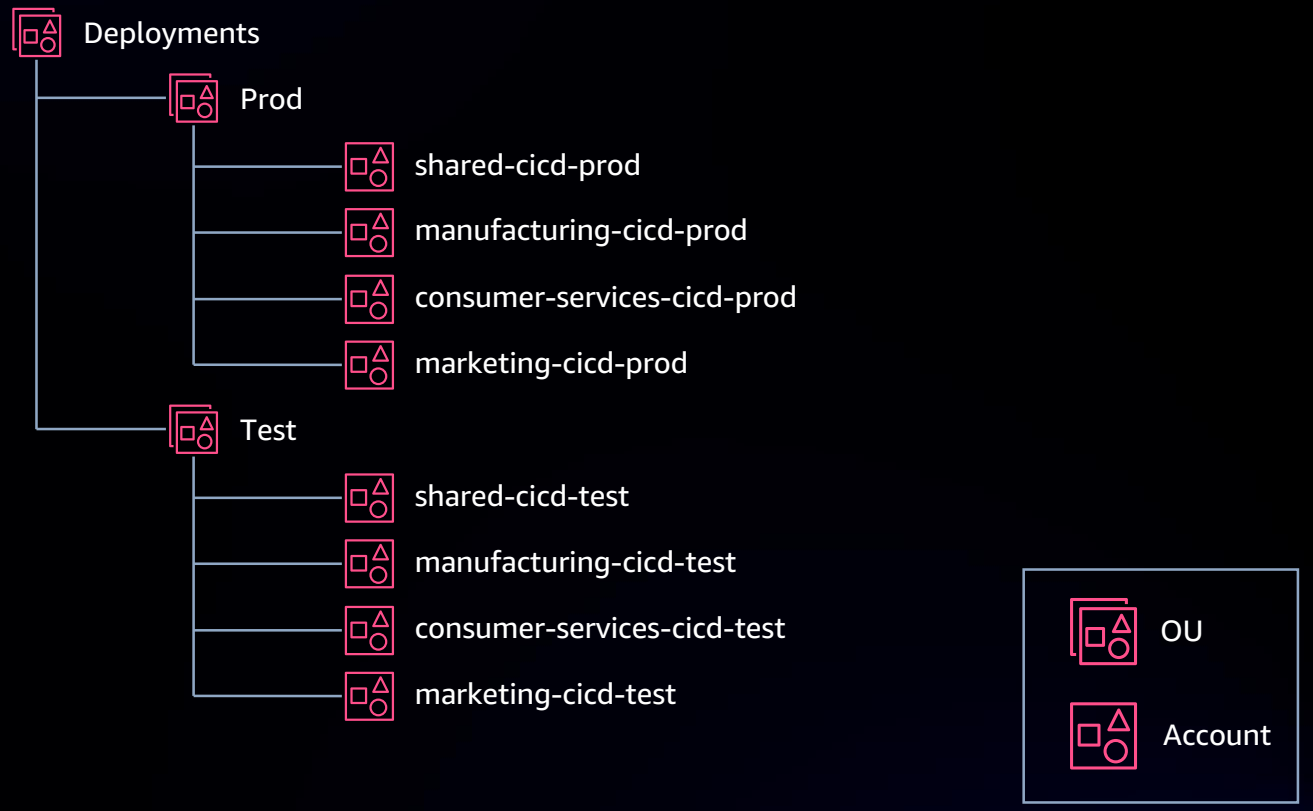
EXAMPLE STRUCTURE OF POLICY STAGING OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

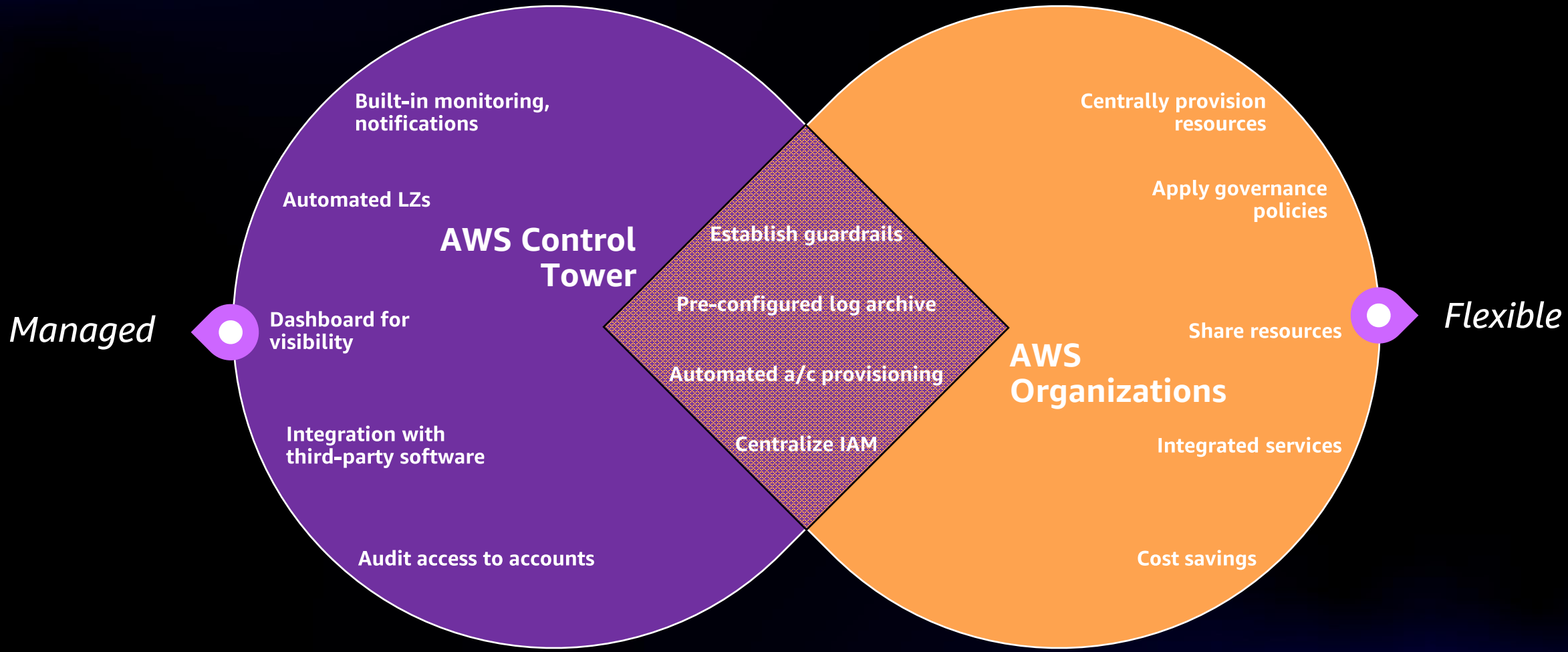
Deployments organizational unit

EXAMPLE STRUCTURE OF DEPLOYMENTS OU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

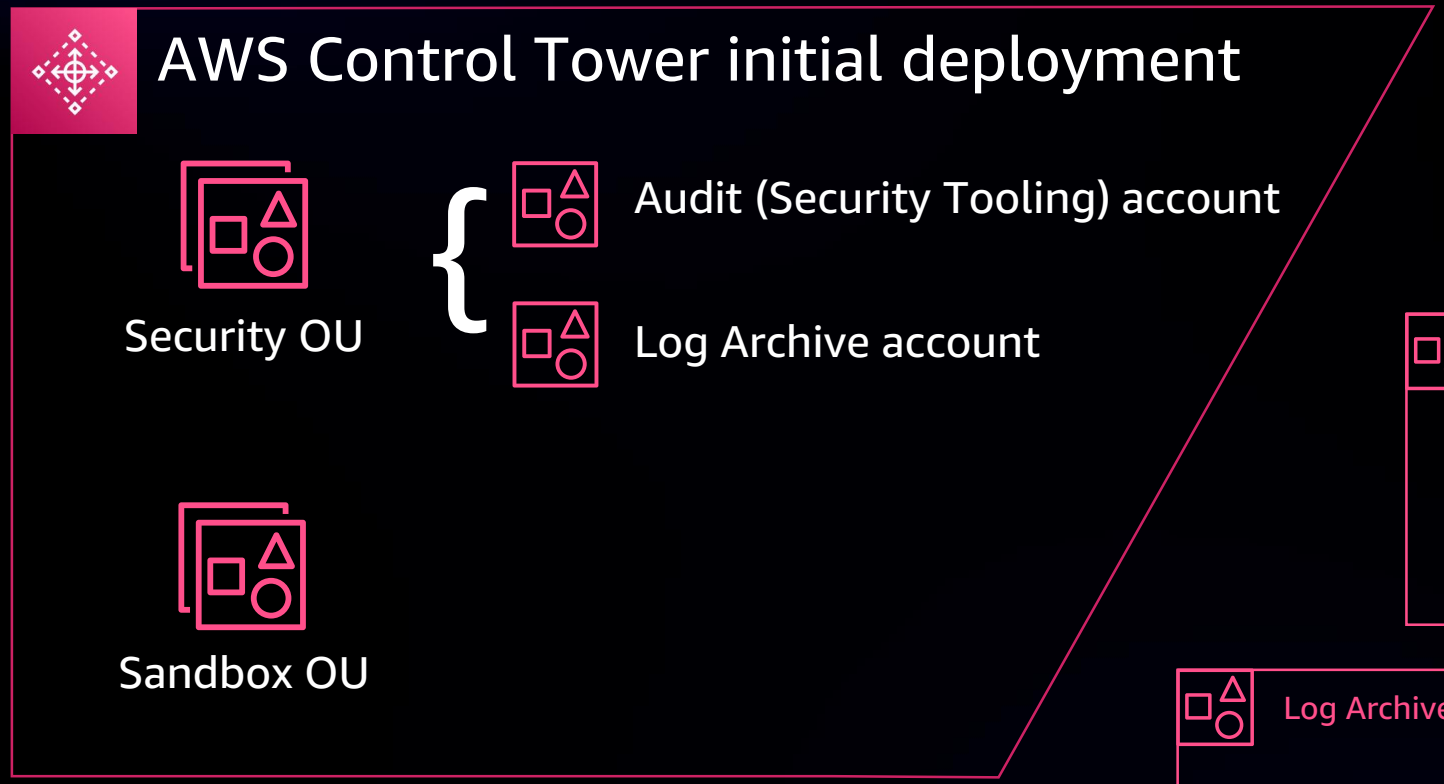
AWS Control Tower and AWS Organizations



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

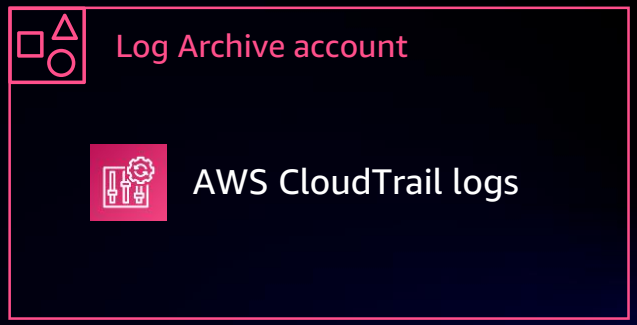
AWS Control Tower

INITIAL ENVIRONMENT









© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enhance governance with AWS Organizations

Centrally provision resources

- AWS CloudFormation
- AWS Systems Manager
- AWS Service Catalog

Share resources and control access to accounts

- AWS Personal Health Dashboard
- AWS Resource Access Manager (AWS RAM)
- AWS Backup & backup policies
- Tag Policies

Optimize costs and identify cost-saving measures

- AWS Trusted Advisor
- AWS Compute Optimizer
- AWS Cost Explorer
- AWS License Manager
- Amazon S3 Storage Lens

Secure and audit your environment for compliance

- AWS Audit Manager
- Amazon Cloud Directory
- Amazon Macie
- AWS Identity and Access Management Access Analyzer
- AI/ML policies

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deploying Control Tower on your organization

Jump-start your organization

Service Catalog SCPs with AWS Control Tower

AWS SSO AWS Config



Review and test requirements:

- AWS Single Sign-On
- AWS Security Token Service (AWS STS)
- Service control policies (SCPs)
- AWS Config
- AWS CloudTrail
- AWS CloudFormation stack sets

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Organizations

POLICY TYPES

- Service control policies (SCPs)



- Tagging policies



- AI/ML policies



- Backup policies



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Organizations features

DELEGATE THE ADMINISTRATION OF RESOURCES

Trusted access

Enables a compatible AWS service to perform operations across all of the AWS accounts in your organization

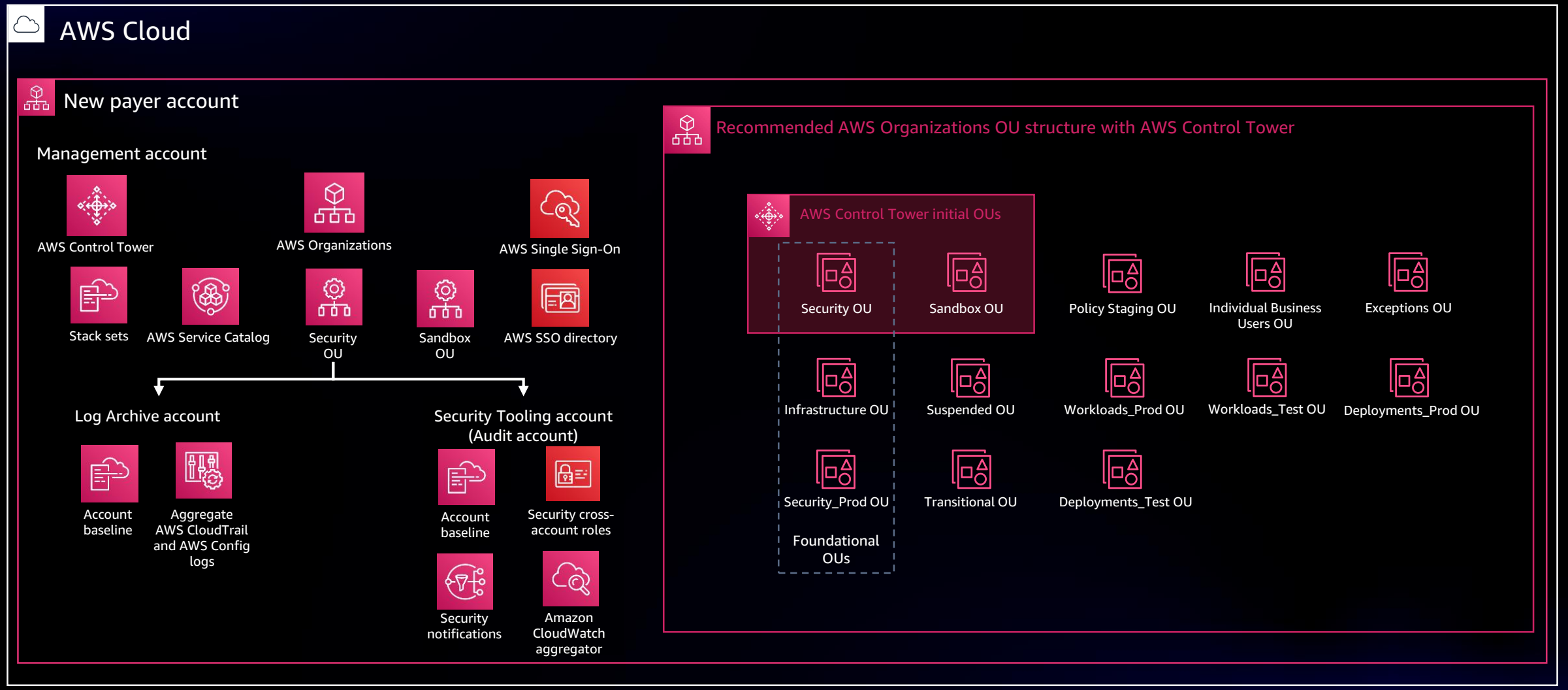
Delegated administrator

A compatible AWS service can register an AWS member account in the organization as an administrator for the organization's accounts in that service

Reference compatibility table in AWS Organizations User Guide

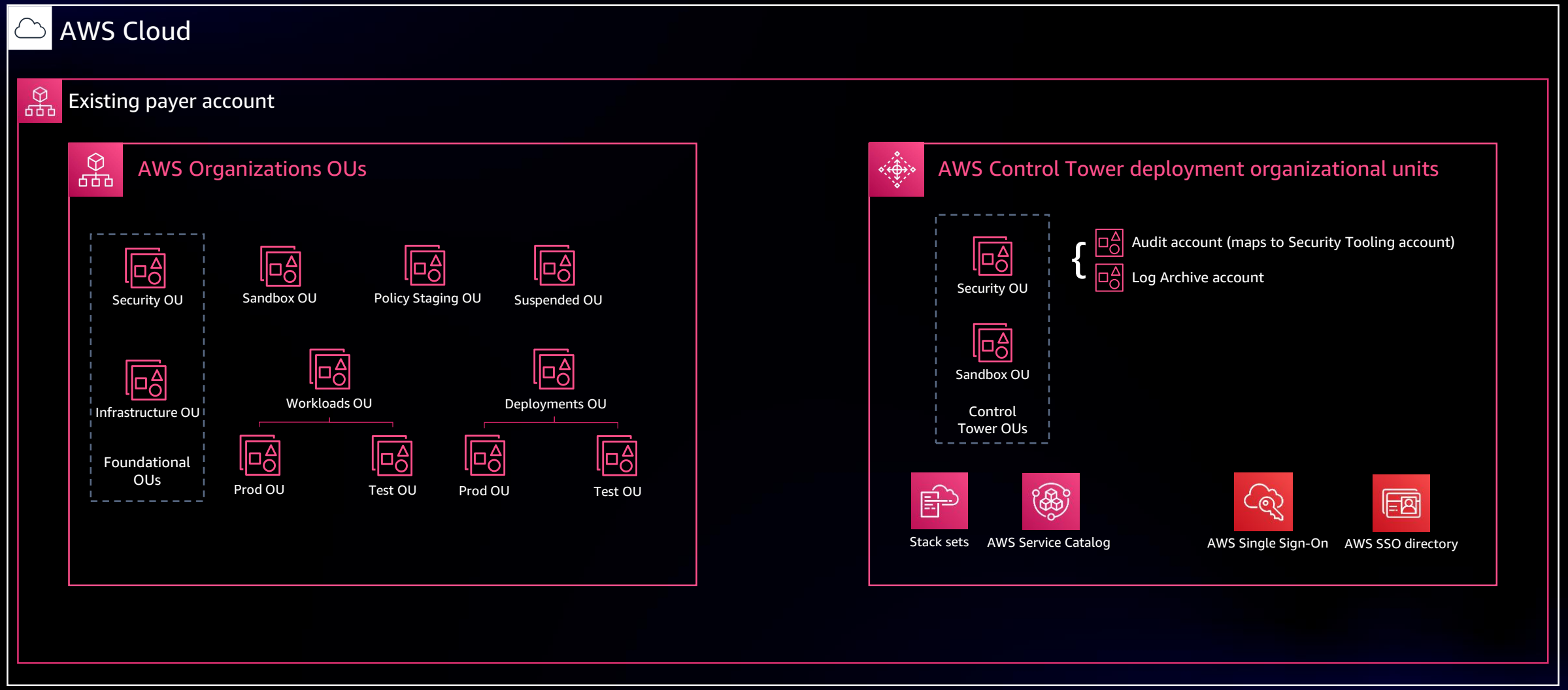
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New customer journey



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Existing customer journey



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sandbox organizational unit

- Drive innovation
- Budgets
- Isolation of resources
- Not connected to the corporate network

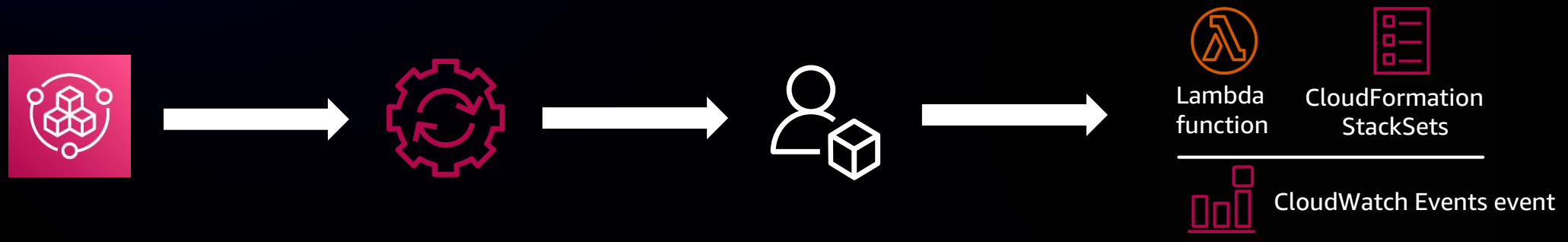
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

More governance features

- AWS budgets
- Cost anomaly detection
- AWS CloudFormation StackSets integration
- Amazon S3 Storage Lens
- Consolidated billing

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lifecycle events with AWS Control Tower



CONTROL TOWER LIFECYCLE EVENT NAMES

- CreateManagedAccount
- UpdateManagedAccount
- EnableGuardrail
- DisableGuardrail
- SetupLandingZone
- UpdateLandingZone
- RegisterOrganizationalUnit
- DeregisterOrganizationalUnit

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.