
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

ARC317-R

Architecting security and governance across your multi-account environment

Alex Torres

Senior Solutions Architect
Cloud Foundations
AWS

Todd Gruet

Senior Solutions Architect
Cloud Foundations
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Characteristics of multi-account environments
- AWS Organizations & AWS account structure
- AWS security services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

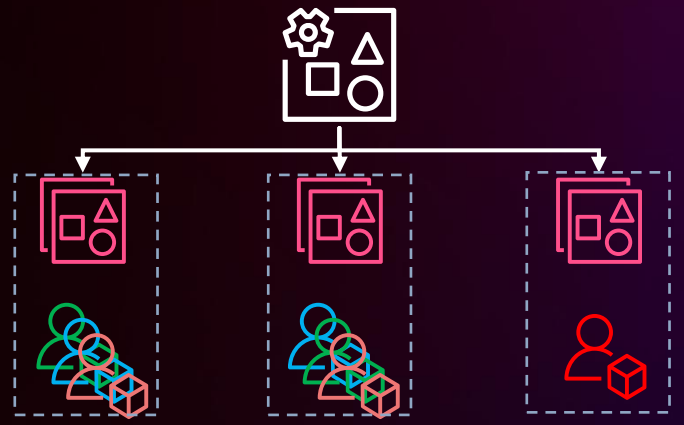
AWS multi-account environment

CHARACTERISTICS

- Multiple accounts
- Access control
- Environment structure
- Management & operations centralized





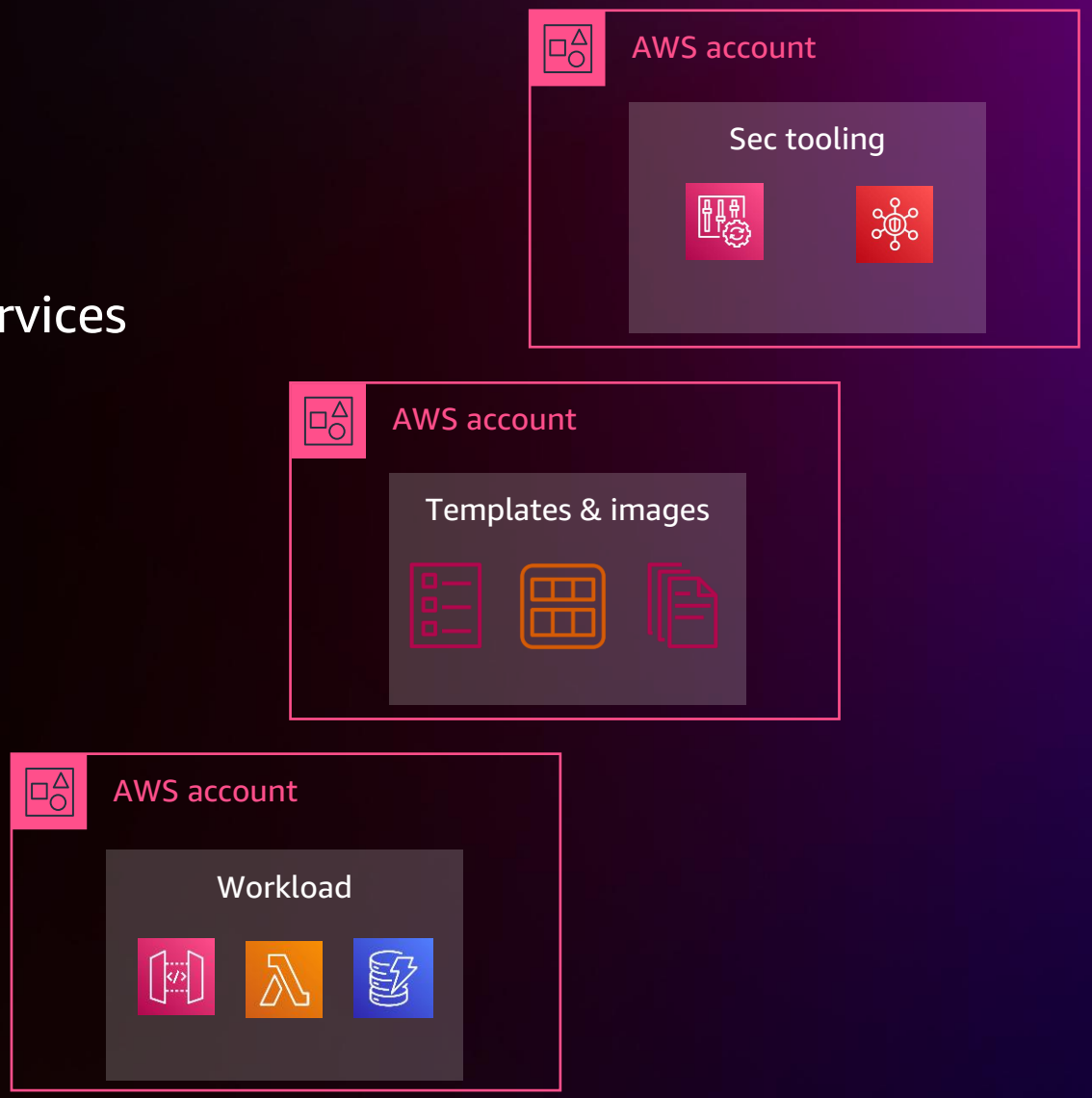


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is an AWS account?

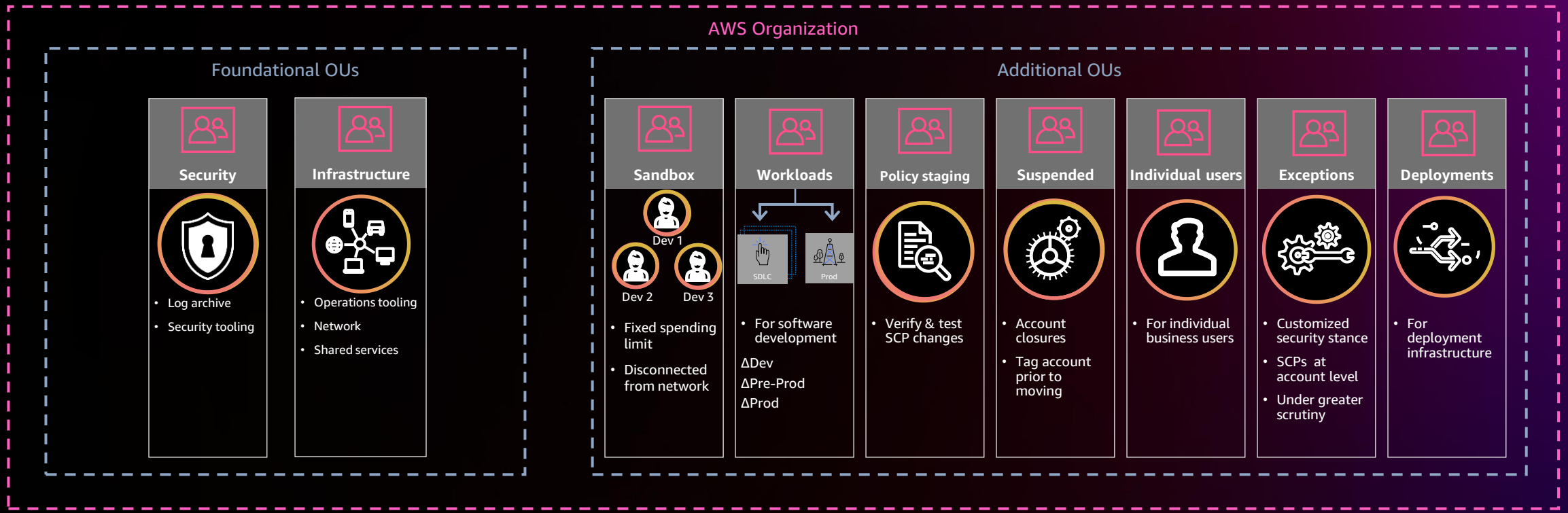
Each AWS account

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



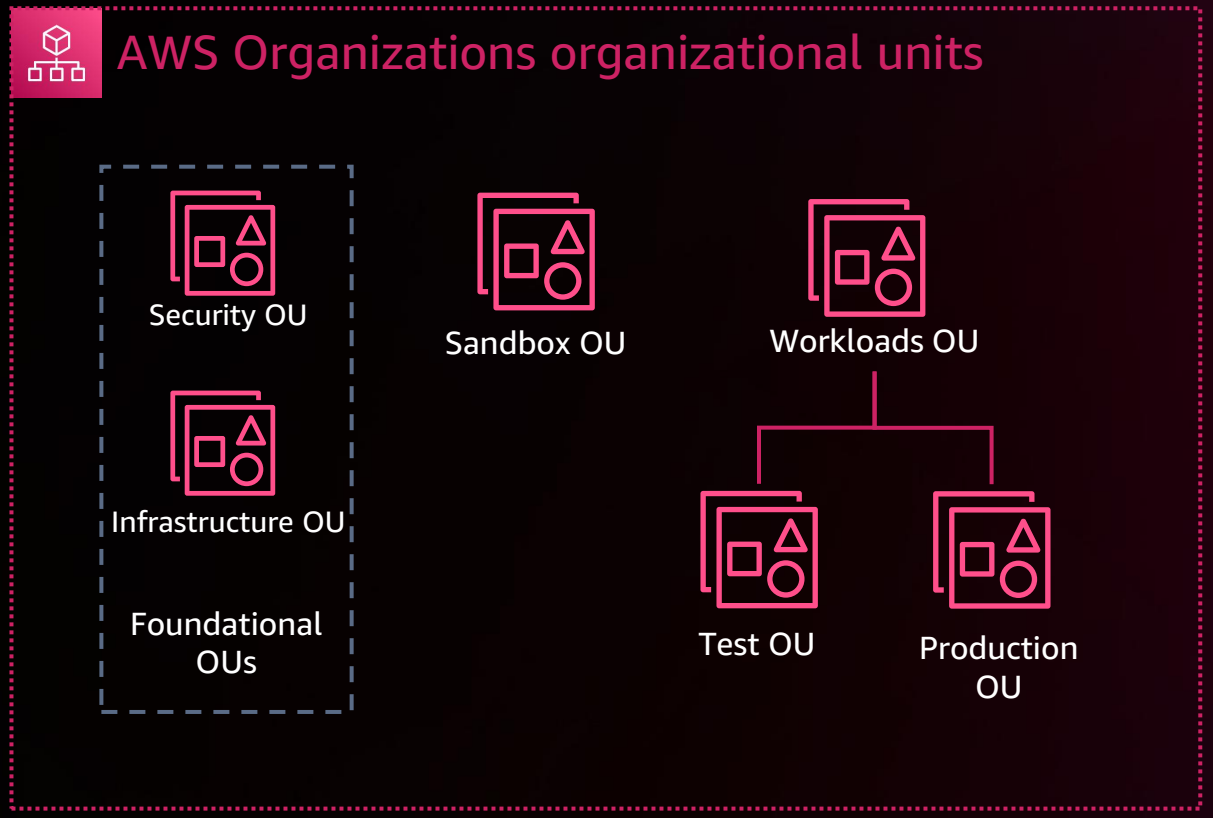
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Structure your multi-account environment



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Start small – production starter organization



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

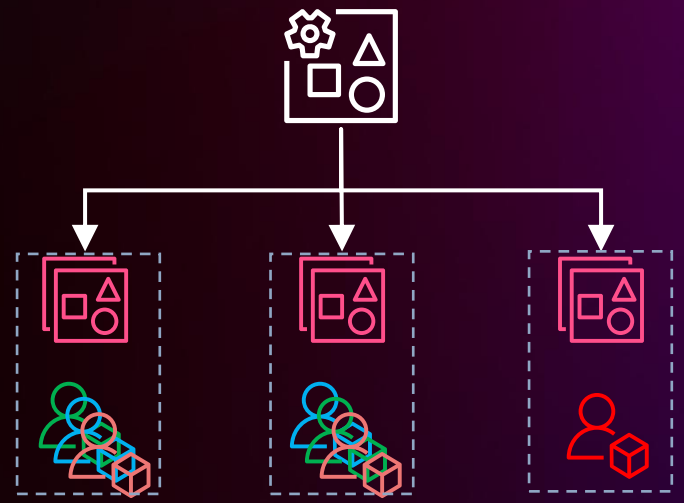
Foundational accounts



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Management account

- AWS Organizations
- Service control policies
- Tag policies
- AWS CloudTrail



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configuring security services

MULTI-ACCOUNT ENVIRONMENTS



AWS CloudTrail



AWS Config



Permissions



AWS IAM Identity Center
(successor to
AWS Single Sign-On)



AWS Security Hub



Amazon GuardDuty



Amazon Detective



AWS Identity and
Access Management
Access Analyzer



Amazon Macie

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security accounts



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Tooling account

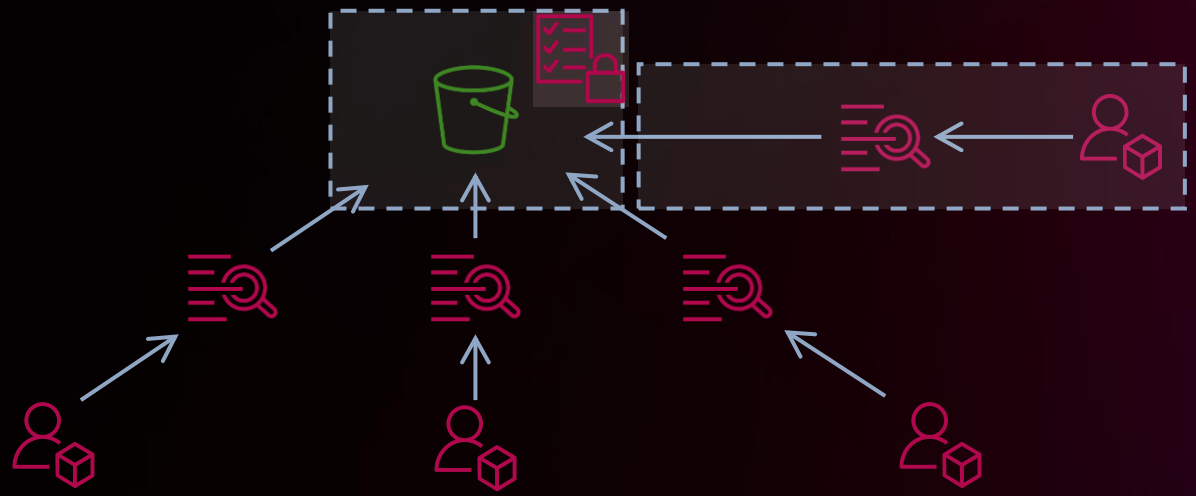
- AWS Security Hub
- Amazon GuardDuty
- Amazon Macie
- Amazon Detective
- AWS Config
- IAM Access Analyzer

Delegated administrator account



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Log Archive account



Access logs

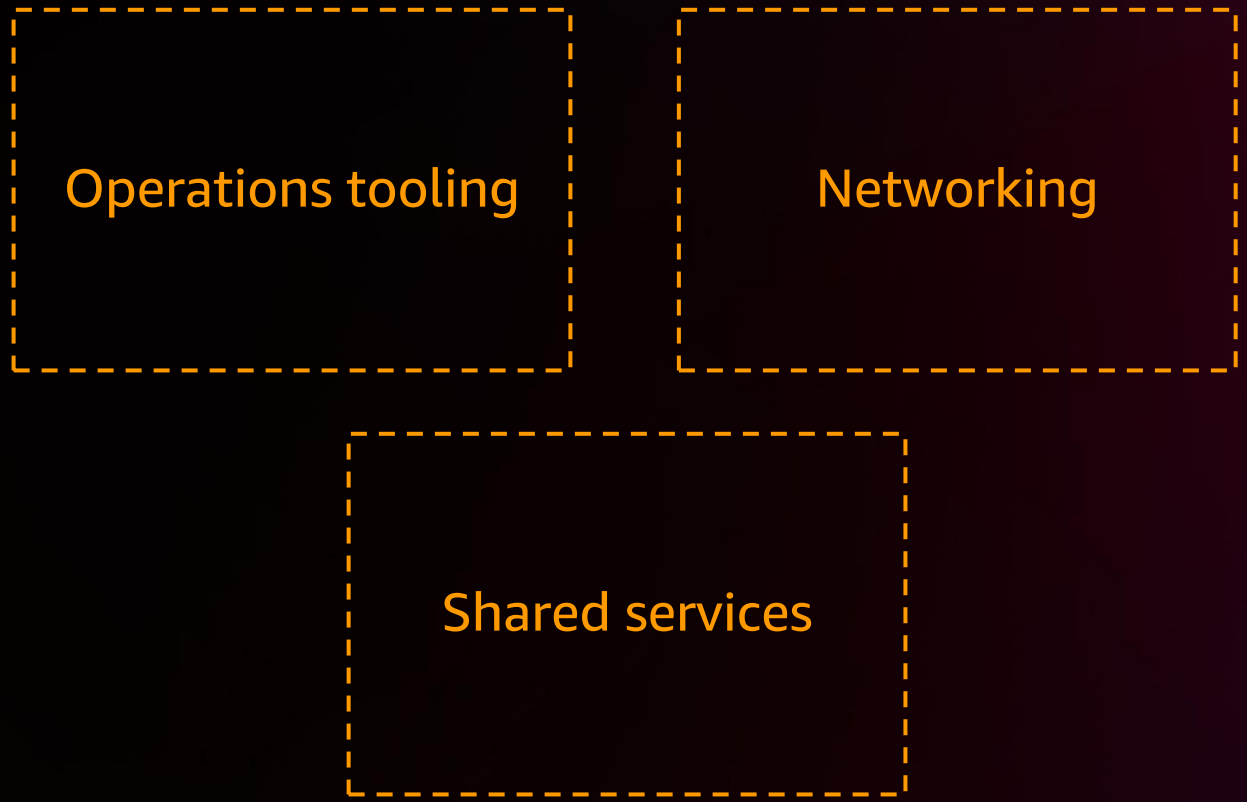
DNS logs

Flow logs

AWS CloudTrail events

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure accounts



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configuring infrastructure services

MULTI-ACCOUNT ENVIRONMENTS


AWS CloudFormation


Amazon CloudWatch


Amazon Virtual Private Cloud (Amazon VPC)


AWS Systems Manager


IAM Identity Center


AWS Network Firewall


AWS License Manager

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operations Tooling account

AWS CloudFormation

AWS Systems Manager

Delegated administrator account



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network account

Hybrid connectivity



AWS Client VPN



AWS Direct Connect

Network core



AWS Cloud WAN



AWS Transit Gateway

IP management



Amazon VPC IP Address Manager (IPAM)

Centralized egress



NAT gateway



AWS Network Firewall

Network monitoring



NAT gateway



Flow log analysis

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared Services account(s)

IAM Identity Center

AWS License Manager

Delegated administrator account



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecting a secure multi-account environment



To help meet the organization's security and governance requirements

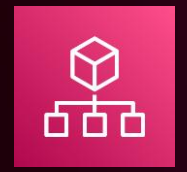
- ✓ Centralize identity and access
- ✓ Set controls (guardrails) centrally
- ✓ Manage accounts centrally
- ✓ Configure services and resources centrally
- ✓ Using accounts to separate workloads

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workload isolation boundary guidance

1. Multi-account architecture
2. Provisioning process for new accounts
3. Baseline new accounts
4. Centralize management of organization
5. Decommissioning process accounts



AWS Organizations

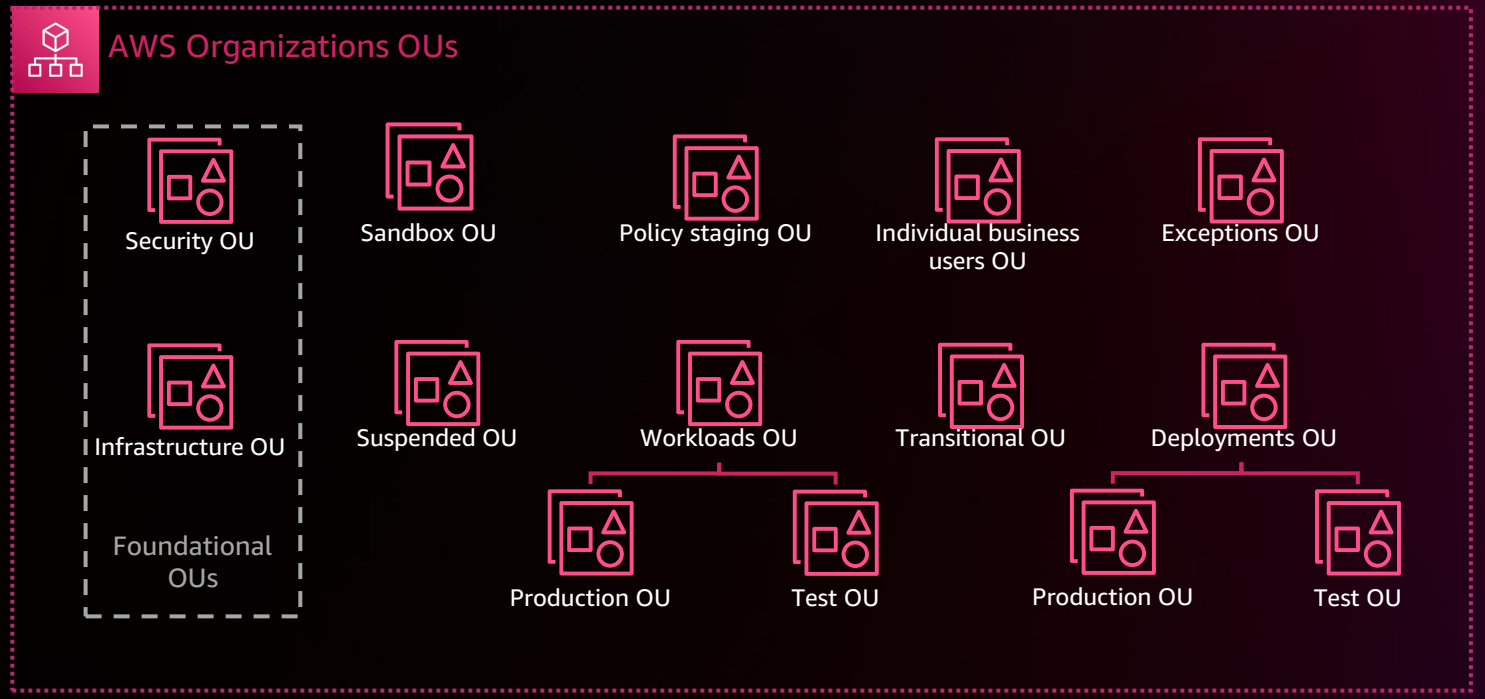


AWS Control Tower

aws

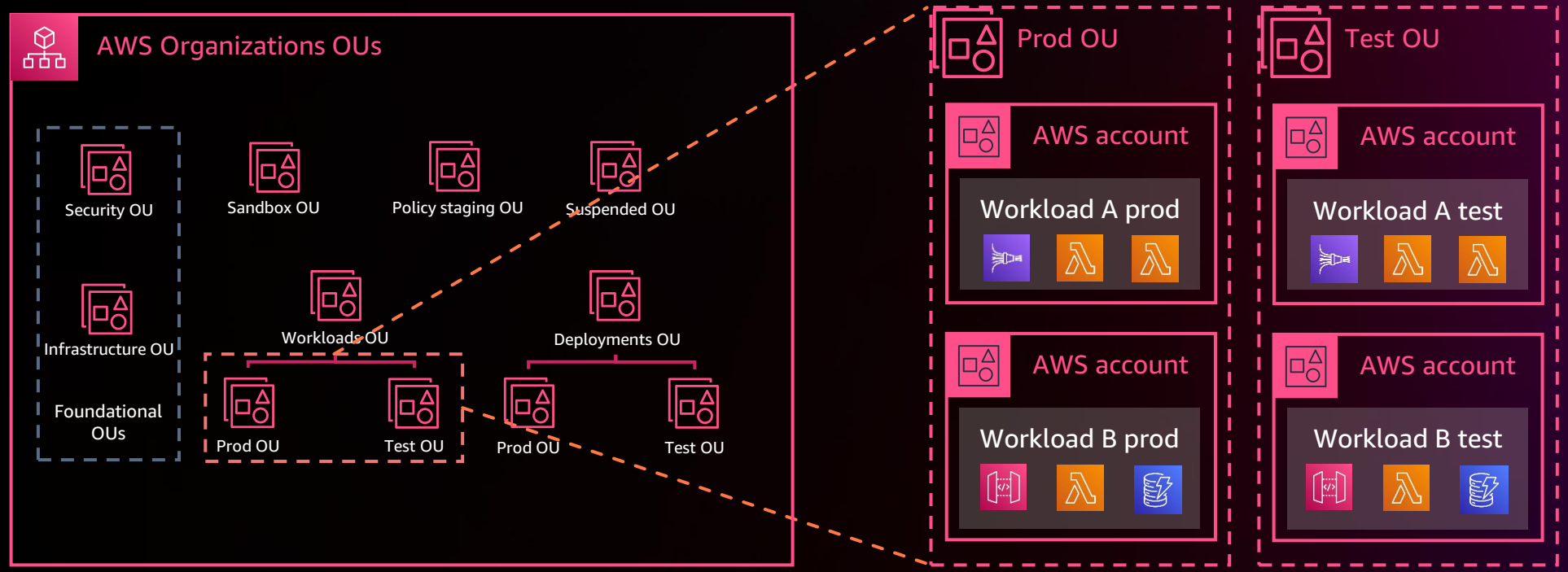
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Expanding your organizations structure



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Separating workloads in the workload OU



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Break glass access

Remediation by the team who owns the resources

Security or operations team access

Usual authentication mechanisms are down

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-factor authentication

Management account users

Federated users

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Control recommendations

Control types

Preventative

- Identity & access management
- Service control policy

Detective

- Event detection
- Infrastructure detection

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommended next steps



- See multi-account strategy whitepaper

  https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/organizing-your-aws-environment.html

- See "*Establishing Your Cloud Foundation on AWS*" whitepaper

  https://docs.aws.amazon.com/whitepapers/latest/establishing-your-cloud-foundation-on-aws

- Start building your environment with our virtual workshop

  https://pages.awscloud.com/Episode-1-Accounts-Access-and-Audit-trails_2022_VW_s48e01-MIG_OD

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud foundations and multi-account strategy sessions

Architecture



[ARC205 – Breakout]
Establishing your cloud foundation on AWS—beyond your landing zone

[ARC321 – Chalk Talk]
Using a multi-account strategy to enable hyperscale

[ARC318 – Chalk Talk]
Best practices for disaster recovery of workloads on AWS

[COP305 – Breakout]
Best practices for organizing and operating on AWS

Implementation



[COP325 – Chalk Talk]
Best practices for automating AWS account migration

[ARC319 – Chalk Talk]
Designing a multi-account environment for disaster recovery

[DOP322 – Chalk Talk]
Optimizing runtime performance with AWS X-Ray and Amazon CodeGuru Profiler

[DOP402 – Chalk Talk]
Implementing DevSecOps pipelines with compliance in mind

Discussion

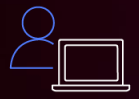


[COP324 – Chalk Talk]
Extend your multi-account governance with automation

[ARC317– Chalk Talk]
Architecting security and governance for your multi-account environment

[COP323 – Chalk Talk]
Delegating access in a multi-account environment with IAM Identity Center

Hands On



[COP206 – Workshop]
Build a complete DevSecOps pipeline on AWS

[ARC301 – Workshop]
Building a monitoring strategy

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Alex Torres

Todd Gruet



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.