AWS re:Invent

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

ARC312-R2

Architecting security and governance in multi-account environments

Alex Torres
Solutions Developer
AWS

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

Agenda

Characteristics of multi-account environments

AWS Organizations AWS account structure

AWS security services

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

AWS multi-account environment

CHARACTERISTICS

- Multiple accounts



- Access control

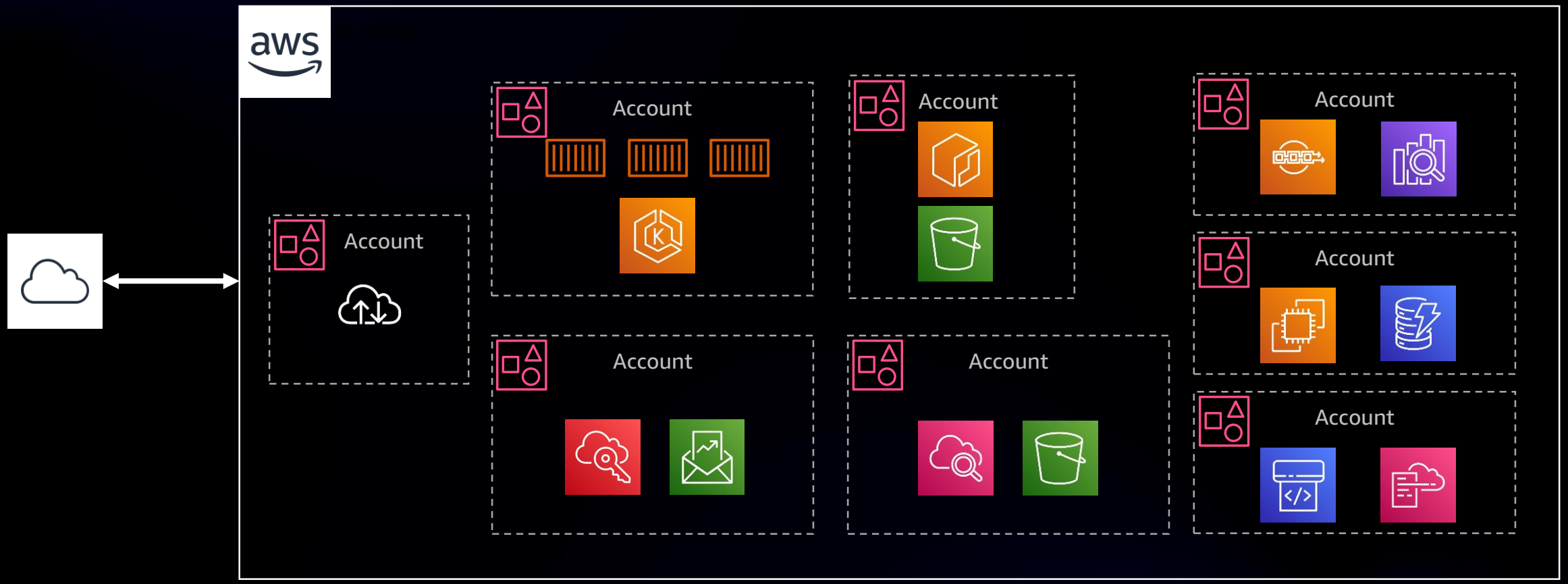


- Environment structure
- Management and operations centralized



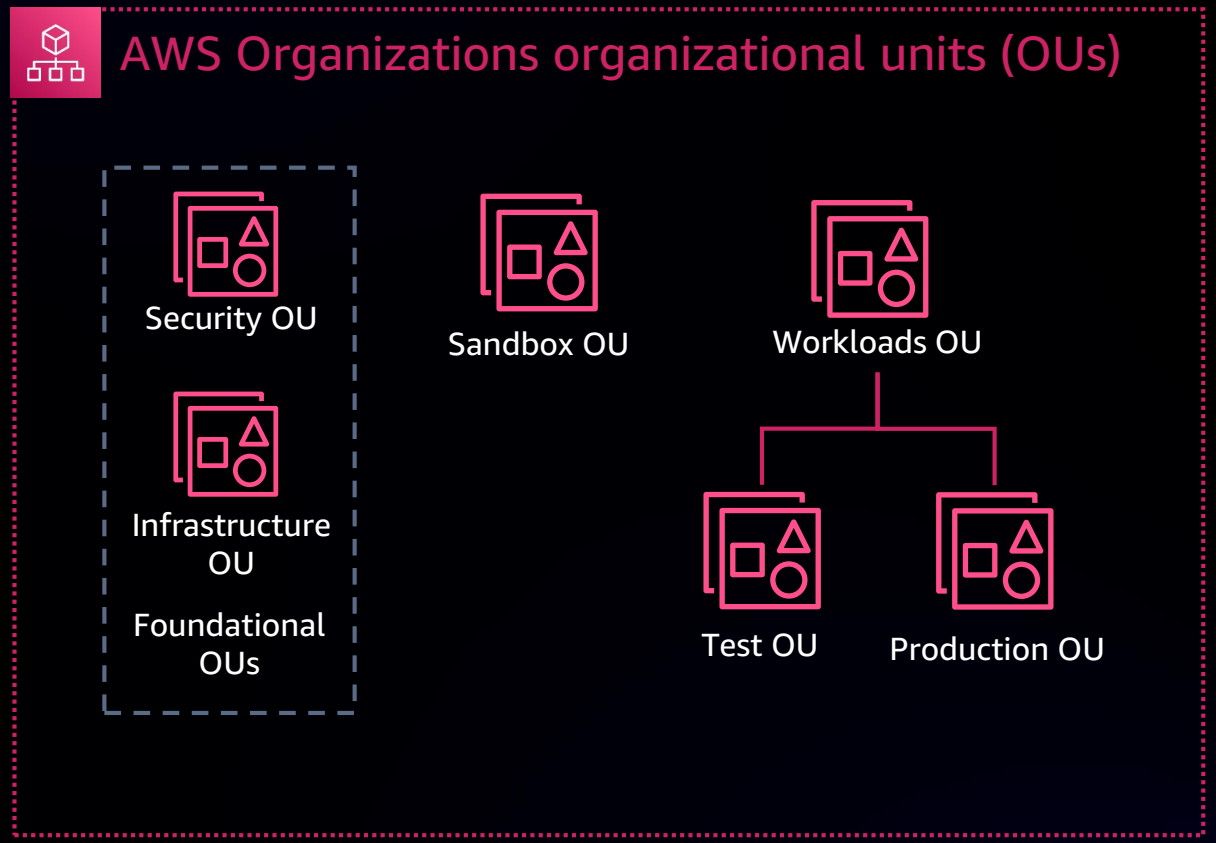
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do we leverage accounts?



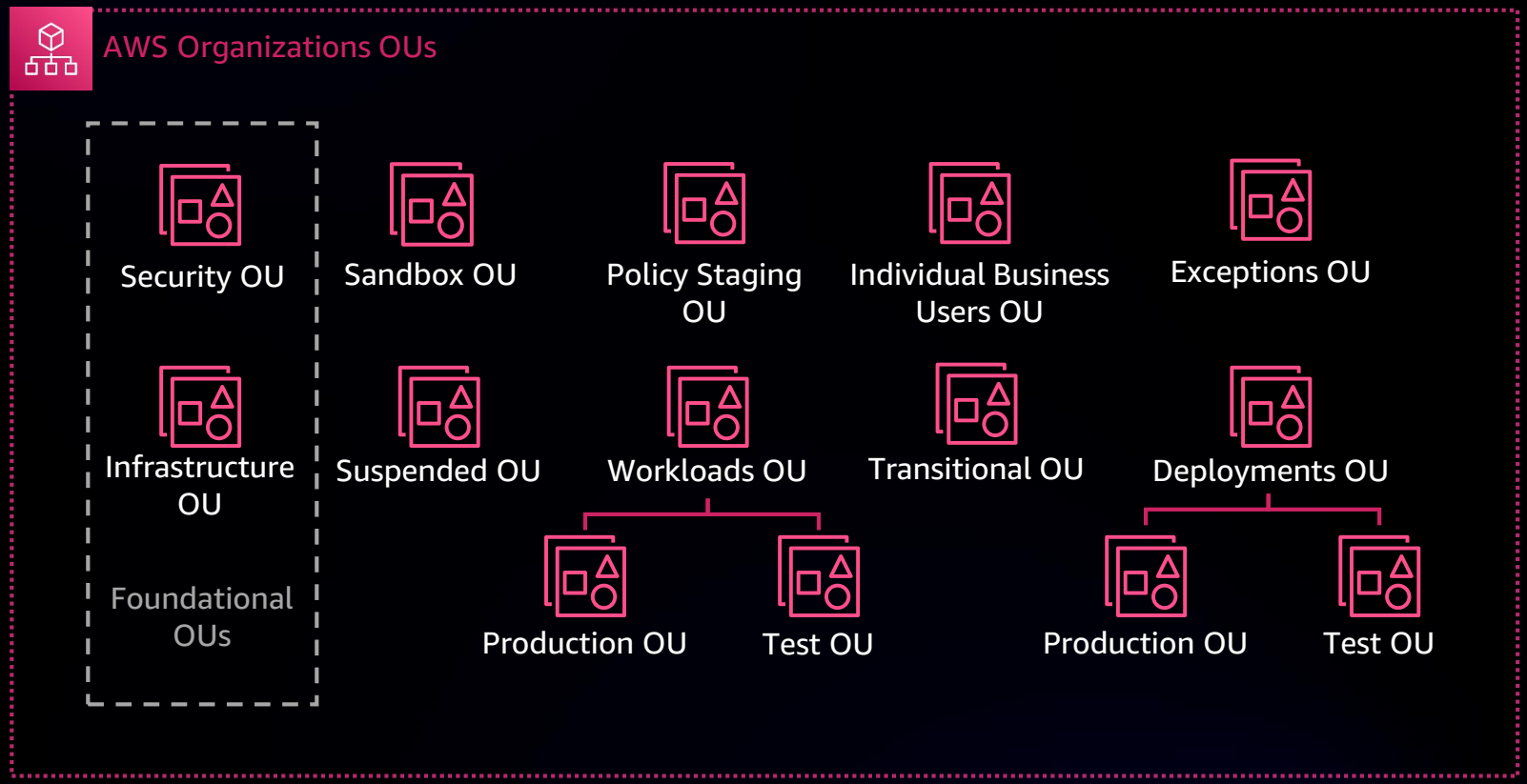
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Organizing accounts with organizational units



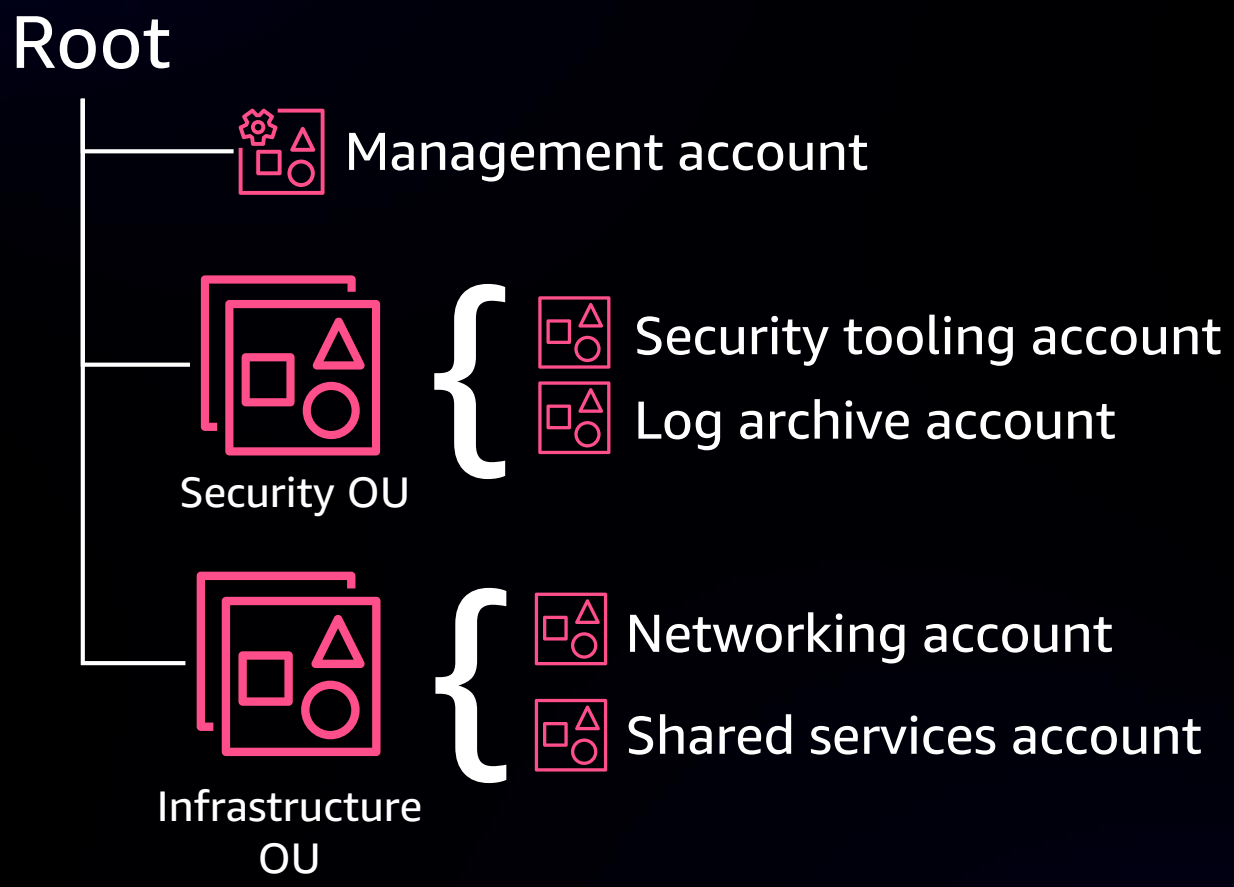
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Expanding your organization’s structure



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

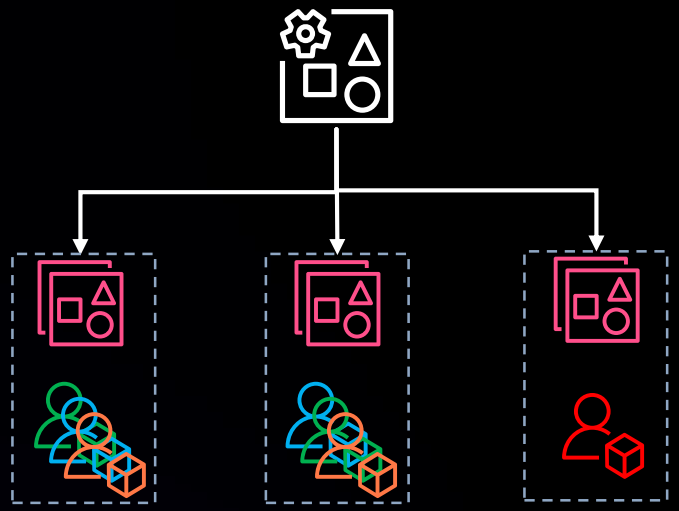
Foundational accounts



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

Management account

- AWS Organizations
- AWS Single Sign-On
- Service control policies
- Tag policies
- AWS CloudTrail



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

Configuring security services

MULTI-ACCOUNT ENVIRONMENTS



AWS CloudTrail



AWS Config



Permissions



AWS Single Sign-On



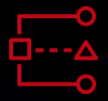
AWS Security Hub



Amazon GuardDuty



Amazon Detective



AWS IAM Access Analyzer



Amazon Macie

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

Integrating AWS services in your environment

AWS ORGANIZATIONS FEATURES

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.

Security accounts



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

Security tooling account

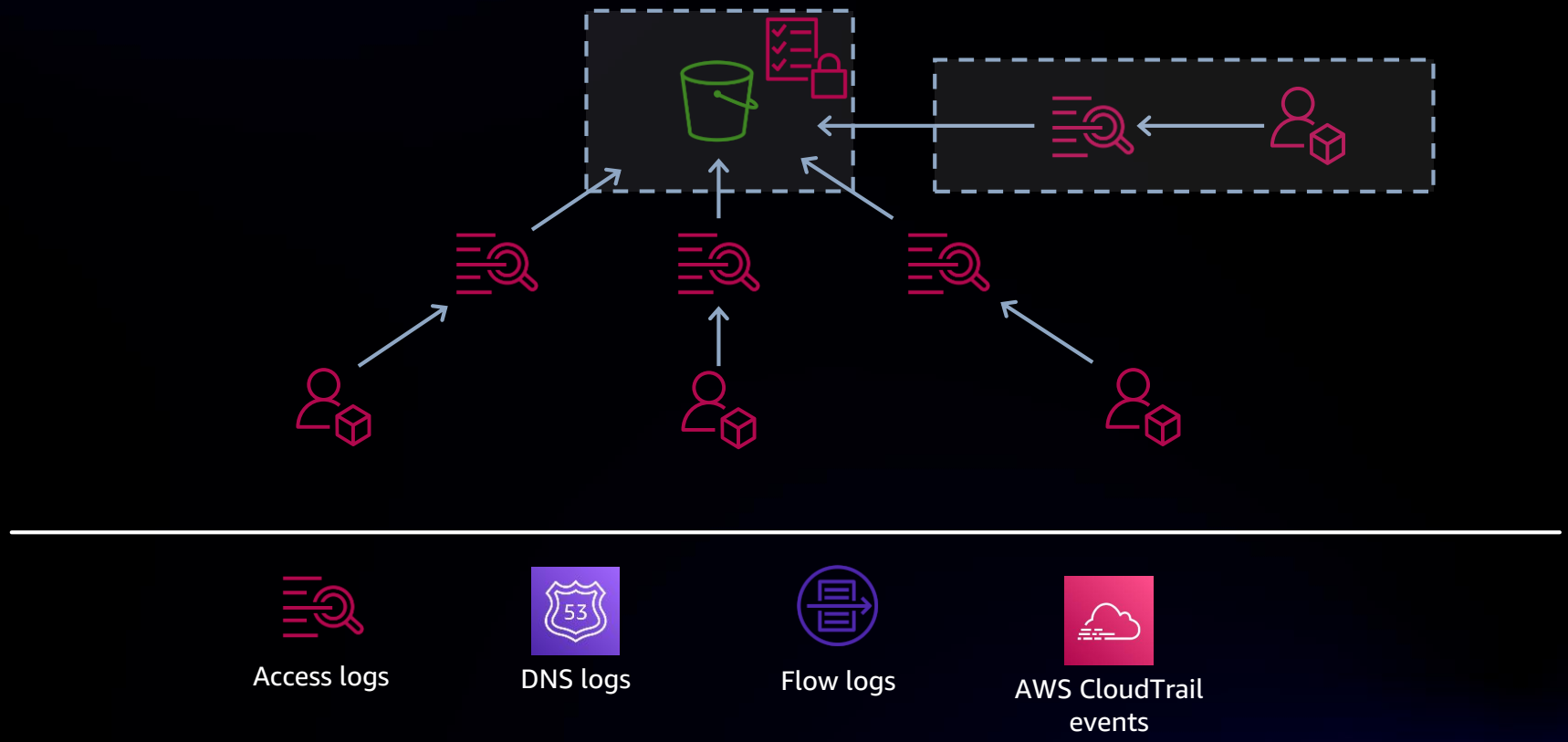
- AWS Security Hub
- Amazon GuardDuty
- Amazon Macie
- Amazon Detective
- AWS Config
- AWS IAM Access Analyzer

Delegated administrator account



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

Log archive account



Access logs

DNS logs

Flow logs

AWS CloudTrail events

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

Architecting a secure multi-account environment



To meet the organization's security and governance requirements

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

aws

© 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 and 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 service 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

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

Thank you!

Alex Torres

alejtr@amazon.com



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