AWS re:Invent

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

COP312

Governance and security for organizations of any size

Raymond Ma (he/him)

Principal Product Manager, AWS Organizations
Amazon Web Services

Andrew Blackham (he/him)

Sr. Product Manager, AWS Organizations
Amazon Web Services

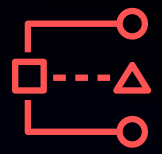
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Intro to multi-account: why we use multiple accounts

Core concepts with multi-account management

Four best practices for access and security

Securely manage your identity	Manage access at scale	Consistently monitor access patterns	Set up proactive security findings
			
AWS SSO	Service control policies	IAM Access Analyzer	AWS Security Hub

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

“Using AWS Organizations is the #1 place your security team should focus.”

Stephen Schmidt

VP and CISO, Amazon Web Services
re:Invent 2020 security keynote

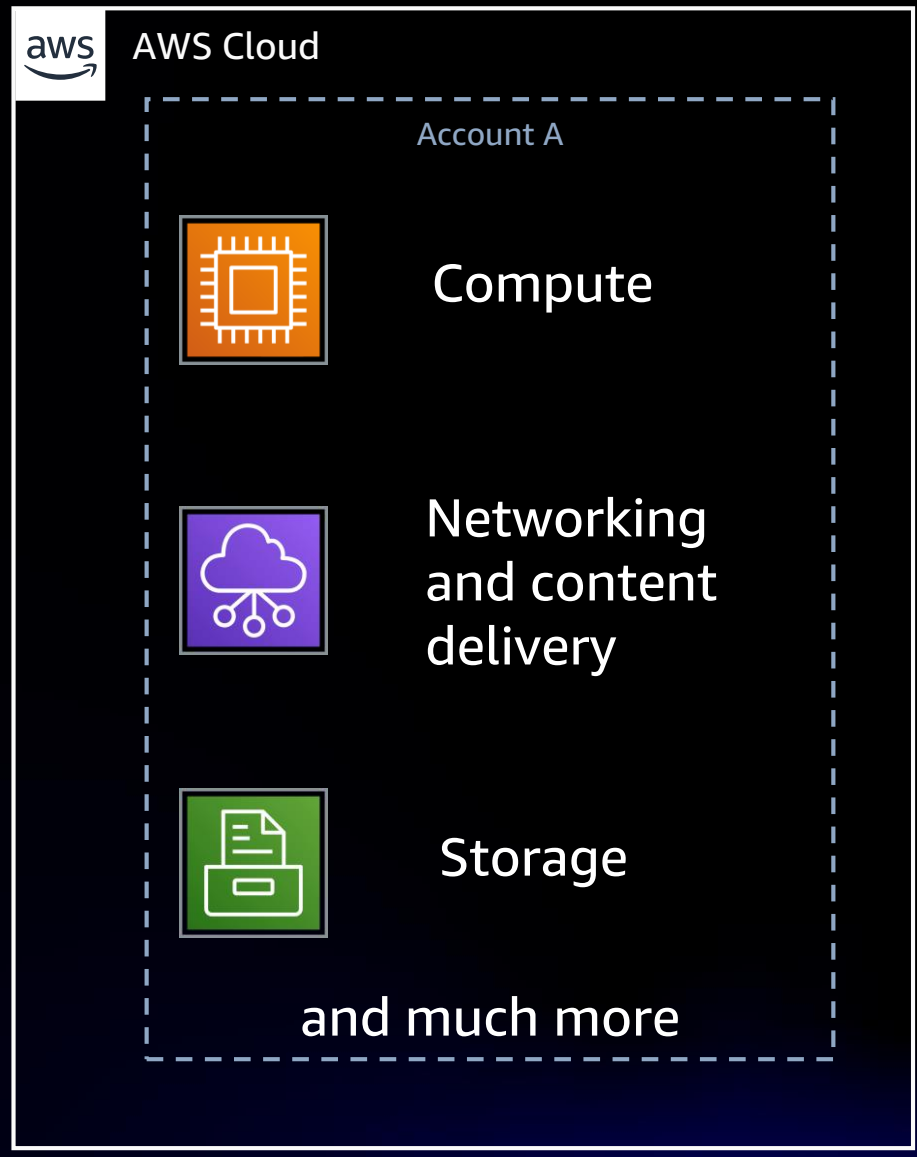
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is an AWS account?

Each AWS account

- Is a resource container for AWS Cloud services
- Is an explicit security boundary
- Is a container for cost tracking and billing
- Is a mechanism to enforce service quotas and API thresholds

Over time, customers will add more accounts to support more applications and services



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

Scaling to a multi-account model



Many teams

Rapid innovation with resources provisioned quickly and exclusively for each team



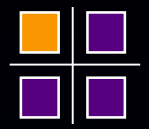
Scalability

Manage or deploy workloads across multiple accounts, allowing you to scale beyond account-level limits



Business process

Organize AWS accounts to reflect business processes with different operational, regulatory, and budgetary requirements

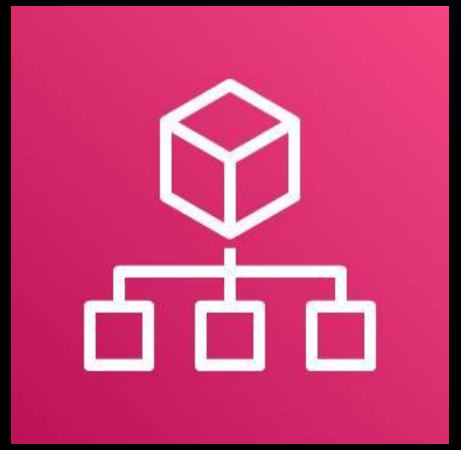


Isolation and security

Tight security boundaries enforced by built-in isolation between accounts, and consolidation for workloads with similar risk profiles

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

AWS Organizations



Provides you tools to centrally govern and manage your cloud environment

- Quickly scale by creating accounts and allocating resources
- Customize your environment by applying governance policies
- Secure and audit your environment
- Manage costs and identify cost-saving measures

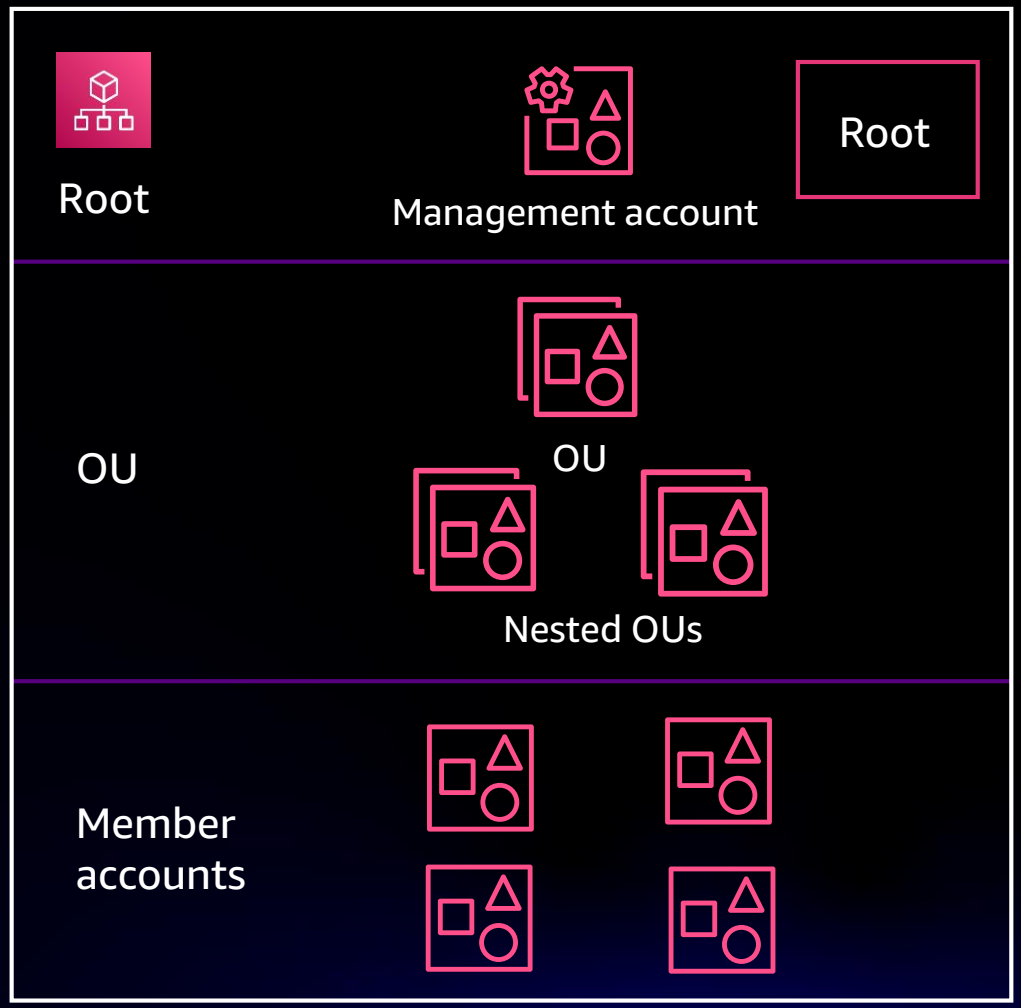
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Organization structure

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

What is an organization?

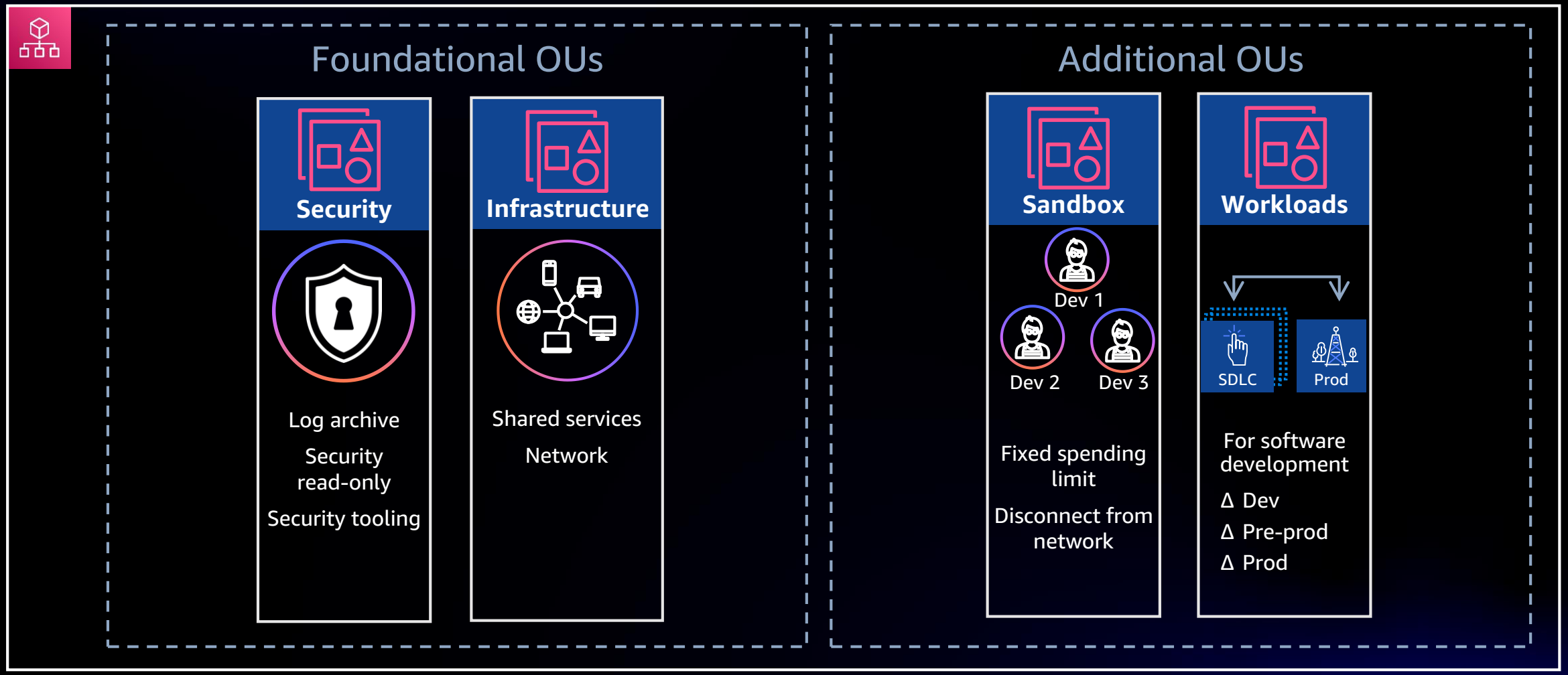
- Organizations contain a root, a management account, organizational units (OUs), and member accounts
- The organization root is the top-most node of the organization and defines the boundaries of the organization
- The management account is used to manage the organization
  - Activate cross-account services and delegate administration to member accounts
  - Limited access to management account
- OUs are groups of accounts
  - Can be used to enable policies on groups of accounts
  - Nested OUs can be used for separation – for example, dev and prod accounts



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

Common OU structure

RECOMMENDED STRUCTURE FOR ANY ORGANIZATION



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

Identity, access, and security

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

Basic multi-account needs

INITIAL STEPS FOR SECURING YOUR ENVIRONMENT AT SCALE

1. Identity and access
   - AWS SSO
2. Permissions and control
   - Service control policies
3. Central visibility and security
   - Security services
     - AWS Identity and Access Management (IAM) Access Analyzer
     - Security Hub
   - Delegated administration

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

AWS Control Tower automations

AWS Control Tower sets up your environment and automates many of these steps



Best-practice guardrails for policy management



Built-in identity and access management (using AWS SSO)



Preconfigured log archive and audit access to accounts



Built-in monitoring and notifications (using AWS CloudTrail and AWS Config)

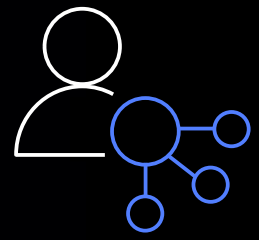
You can implement additional security measures to assist you with managing your organization created using AWS Control Tower

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

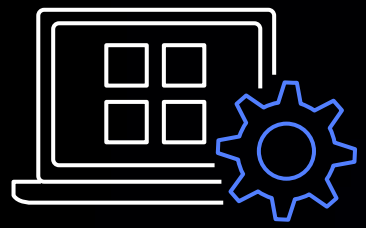
Step 1: Identity and AWS SSO



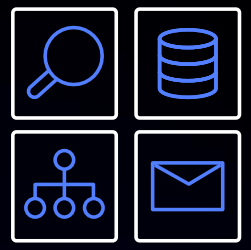
Simply and securely manage identity at scale



Automatically update users and groups tied to your existing directory



Helps you achieve least privilege

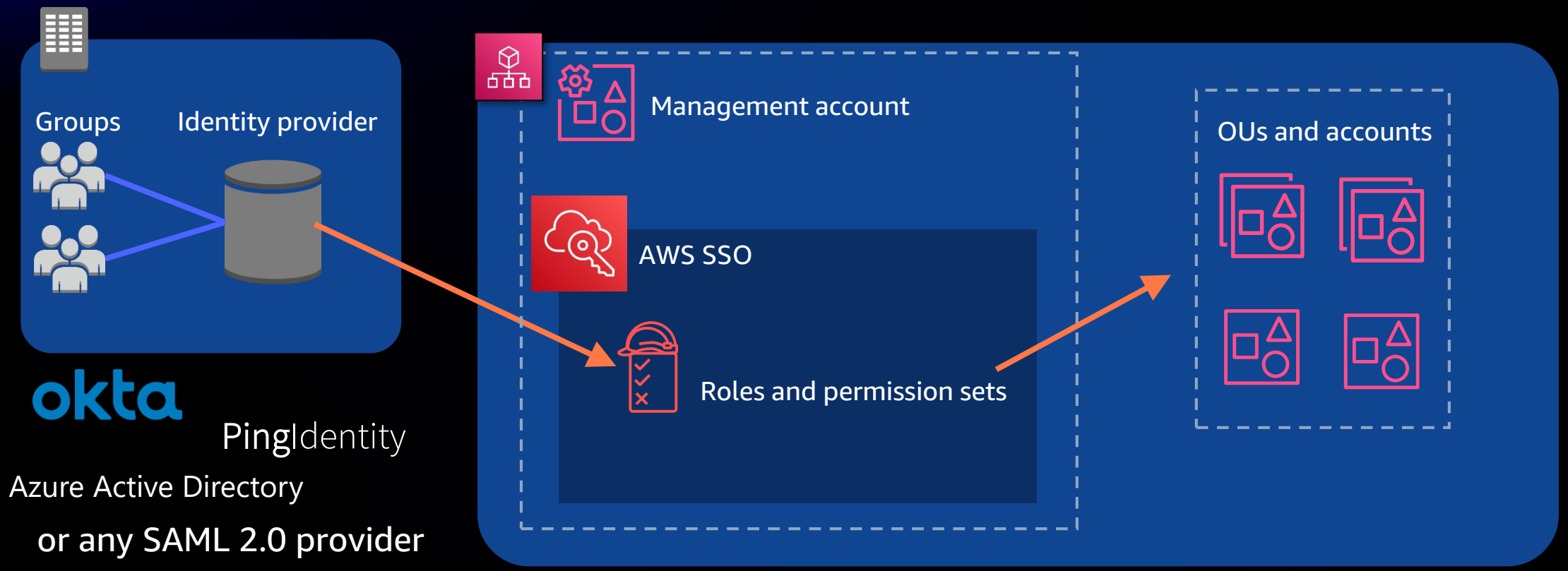


Provides dynamic permissions based on groups, security requirements, or other attributes

aws

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

AWS SSO: How it works



okta

PingIdentity

Azure Active Directory

or any SAML 2.0 provider

Configure identity provider to identify users and groups

Map groups to defined permissions

Grant access to accounts within the organization

aws

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

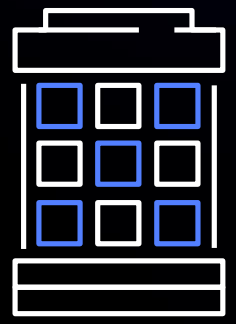
Step 2: Managing access at scale

AWS SSO enables access across accounts, but how can we centrally manage permissions within accounts?

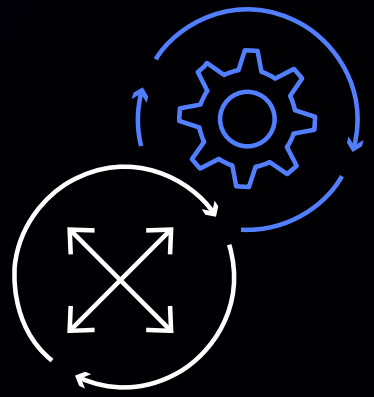
Service control policies (SCPs)

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

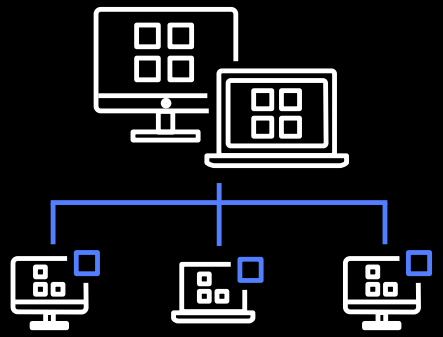
SCPs



Centrally create and apply custom guardrails for your organization



Promote increased agility from teams using simplified governance



Use granular or broad guardrails and apply them across accounts

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

“Service control policies will make your life better.”

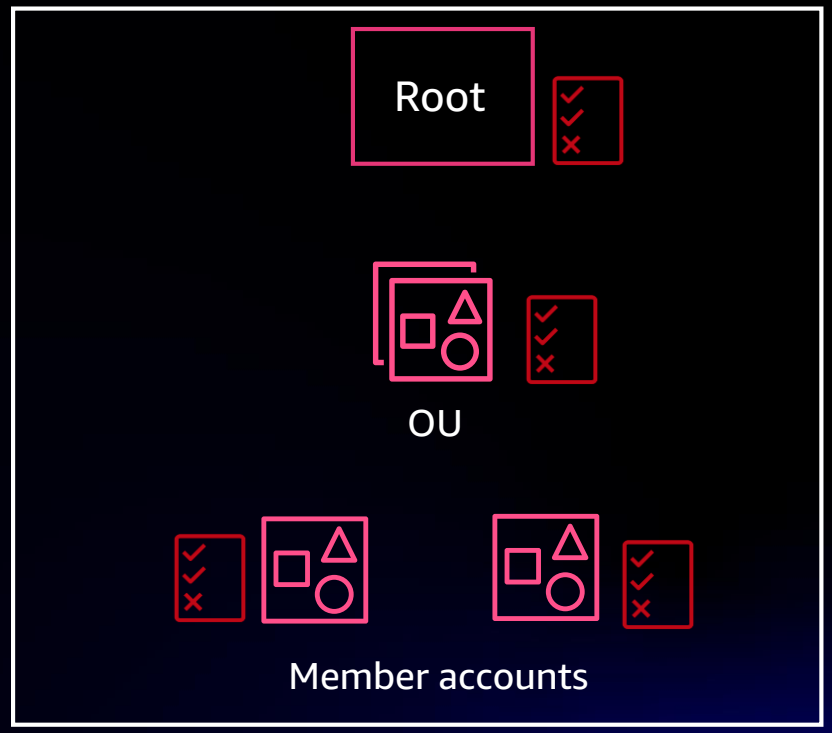
Stephen Schmidt
VP and CISO, Amazon Web Services
re:Invent 2020 security keynote

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

How SCPs work

- Granular policies can allow or limit API actions from users in member accounts
- They can be applied to member accounts, OUs, or the organization root
  - Simplifies permissions at scale; member accounts "inherit" policies or permissions applied at other levels

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "organizations:LeaveOrganization"
         ],
         "Resource": "*"
      }
   ]
}
```

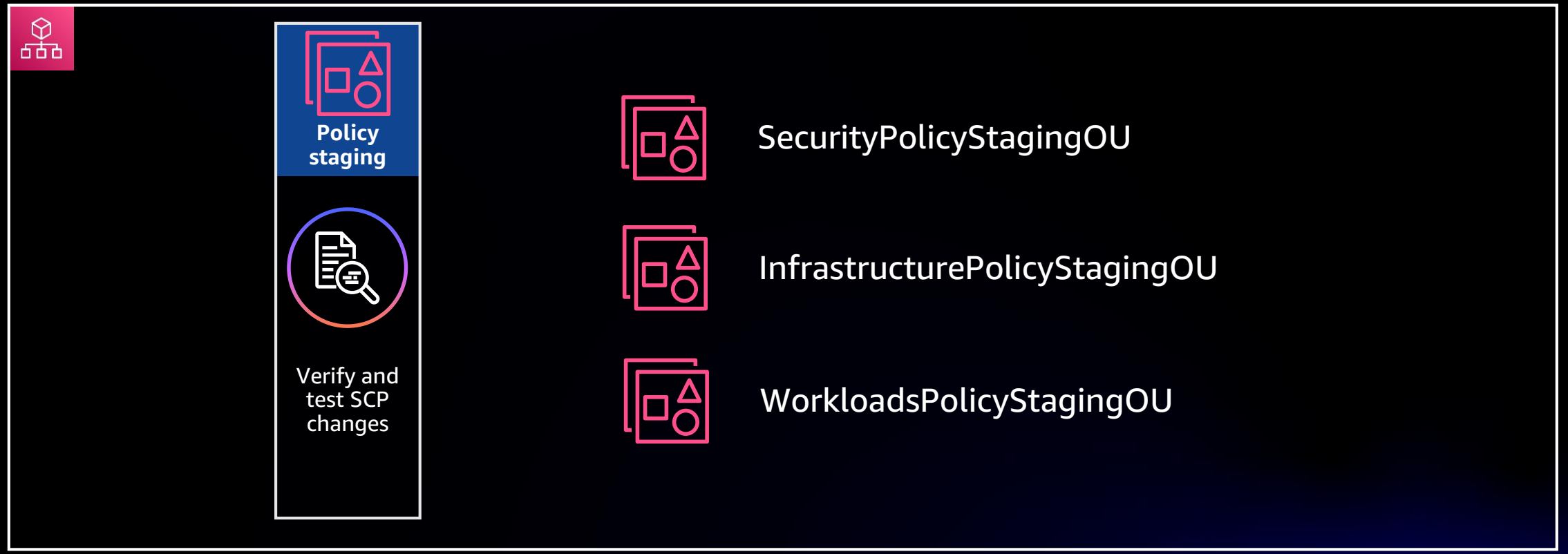


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Testing SCPs

Testing can be done in a PolicyStaging OU

Create nested OUs and member accounts to reflect your organization OU structure



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

SCP use cases

SCENARIOS FOR USING SCPs

Use of common services within each OU

Limit usage to certain AWS Regions

Require tags upon resource creation

Specify allowed instance sizes

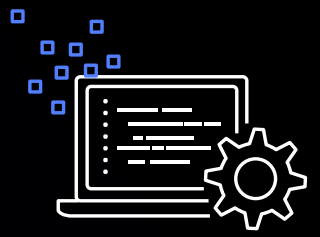
Prevent actions from root users

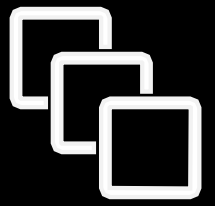
Prevent deletion or modification of IAM roles

Prevent default encryption from being turned off







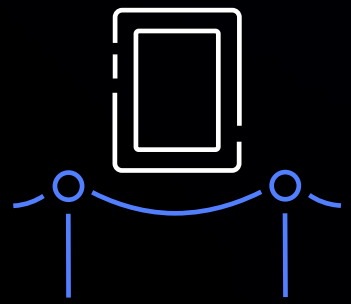






© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 3: Monitor access – IAM Access Analyzer



Simplify access analysis



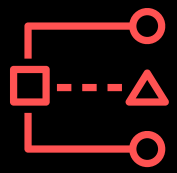
Scale permission management



Ensure least privilege using existing access patterns

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

Access Analyzer: How it works



Access Analyzer evaluates resource policies

Provides you with a list of resources or policies that permit external visibility

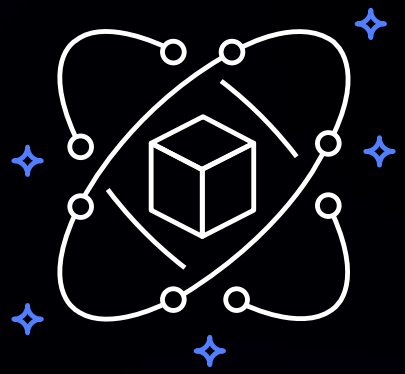
Simply identify and mitigate unintended access

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

Step 4: Consistent security – Security Hub



Security tools available in a single destination



Enable services that scale with your organization with the click of a button



Reduce strain on your security team, helping them to focus on prioritized needs

aws

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

Security Hub



Security Hub provides a centralized view of reports across security services



Amazon GuardDuty, AWS Config, Access Analyzer, and even third-party services

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

Security services

Security Hub demo

- Enable Security Hub
- Set delegated admin account



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

What we've accomplished today

INITIAL STEPS FOR SECURING YOUR ENVIRONMENT AT SCALE

- ✓ Identity and access
  - ✓ Enabled AWS SSO
- ✓ Permissions and control
  - ✓ Set service control policies
- ✓ Central visibility and security
  - ✓ Enabled security services
    - ✓ IAM Access Analyzer
    - ✓ Security Hub
  - ✓ Delegated to security team

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

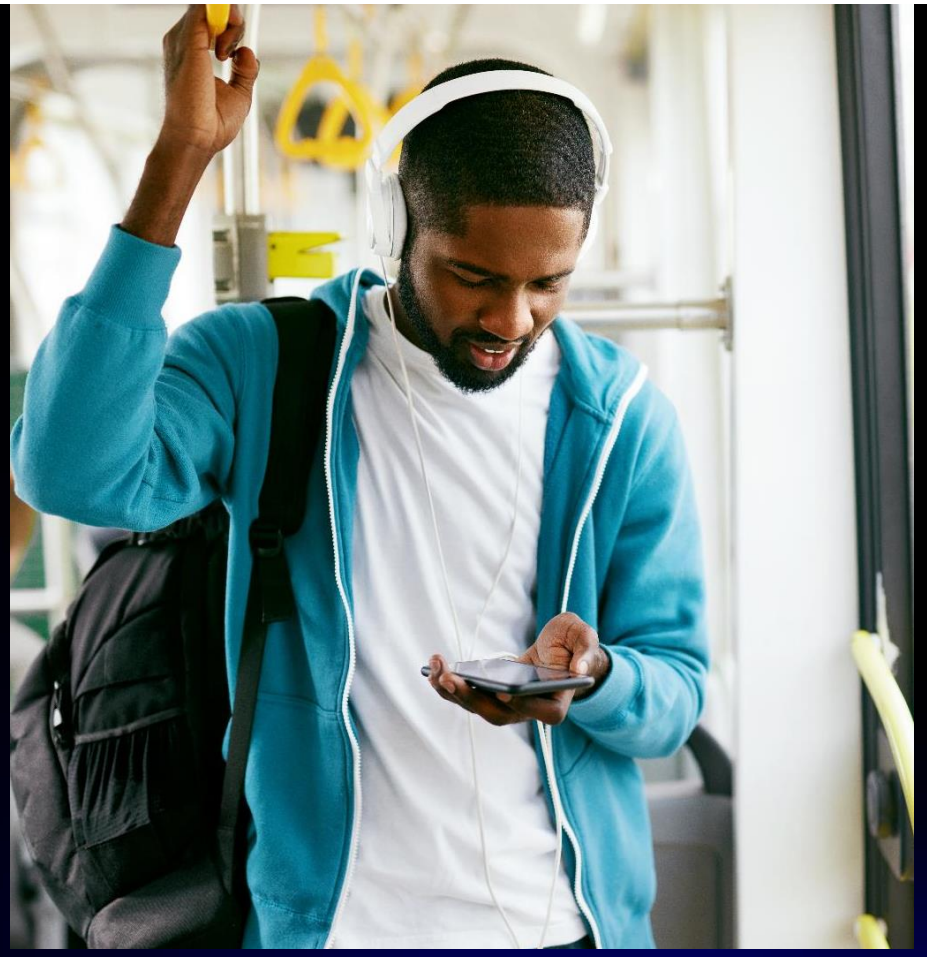
Customer testimonial

"Using AWS SSO with AWS Organizations allowed us to centralize authentication to our identity provider (IdP), which has been a massive improvement on a daily basis for our employees so they don't have different sets of credentials for accessing multiple AWS accounts.

In addition, our infrastructure security team was able to centralize access management, resulting in an increase in platform security and a decrease in operational costs."

Rocco Zanni, CTO
Spreaker

Spreaker



aws

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

Thank you!

Raymond Ma

LinkedIn: /in/raysma

Andrew Blackham

Twitter: @a_blackham
LinkedIn: /in/andrew-blackham

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