



Managing Identities & Access Across AWS Accounts

Chris Mercer, Samuel Folkes
Solutions Architects, AWS

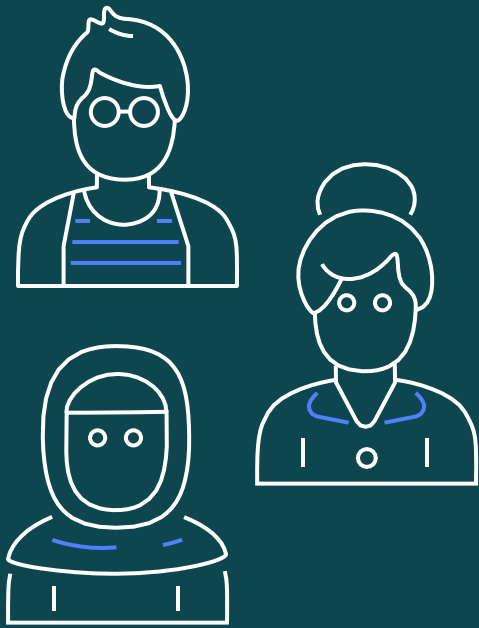
Agenda

- Introductions
- A Brief History of User Access in AWS
- AWS Single Sign-On
- Customer Reference – Sophos
- Common Patterns for Migration
 - Migrating Users
 - Migrating Roles & Policies
 - Migrating Assignments
- Additional Resources

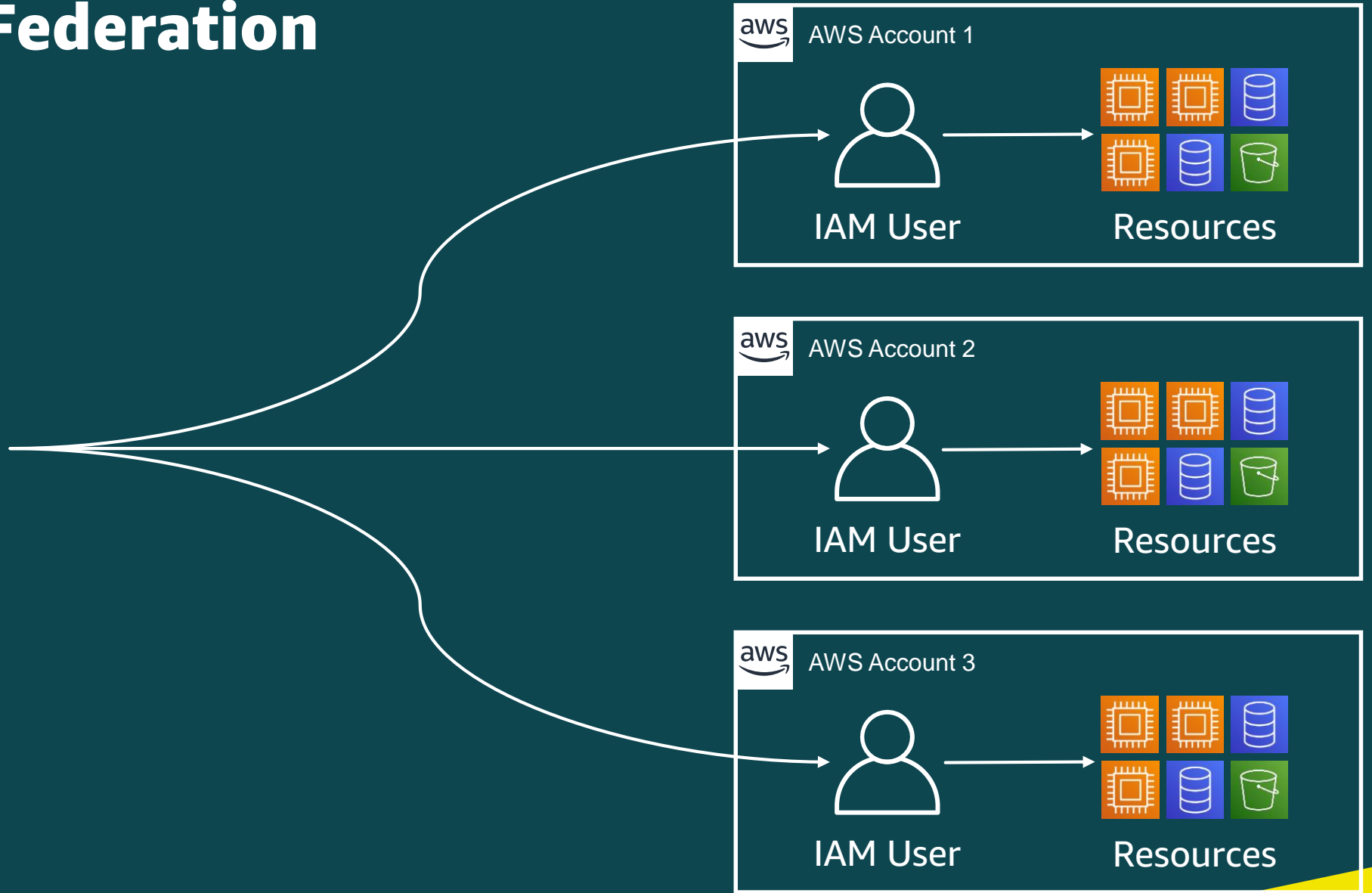
A Brief History of User Access in AWS



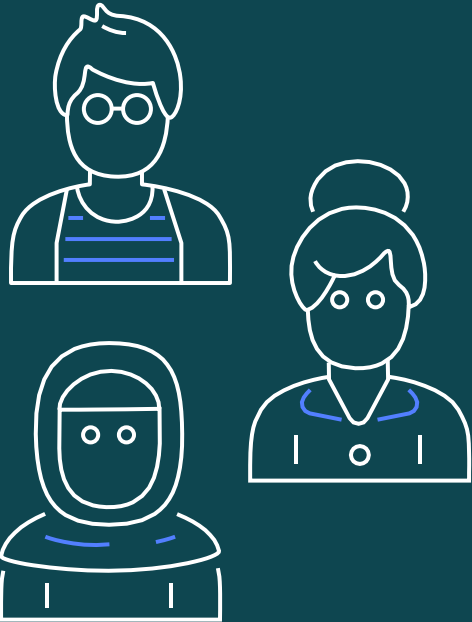
Evolution of Federation



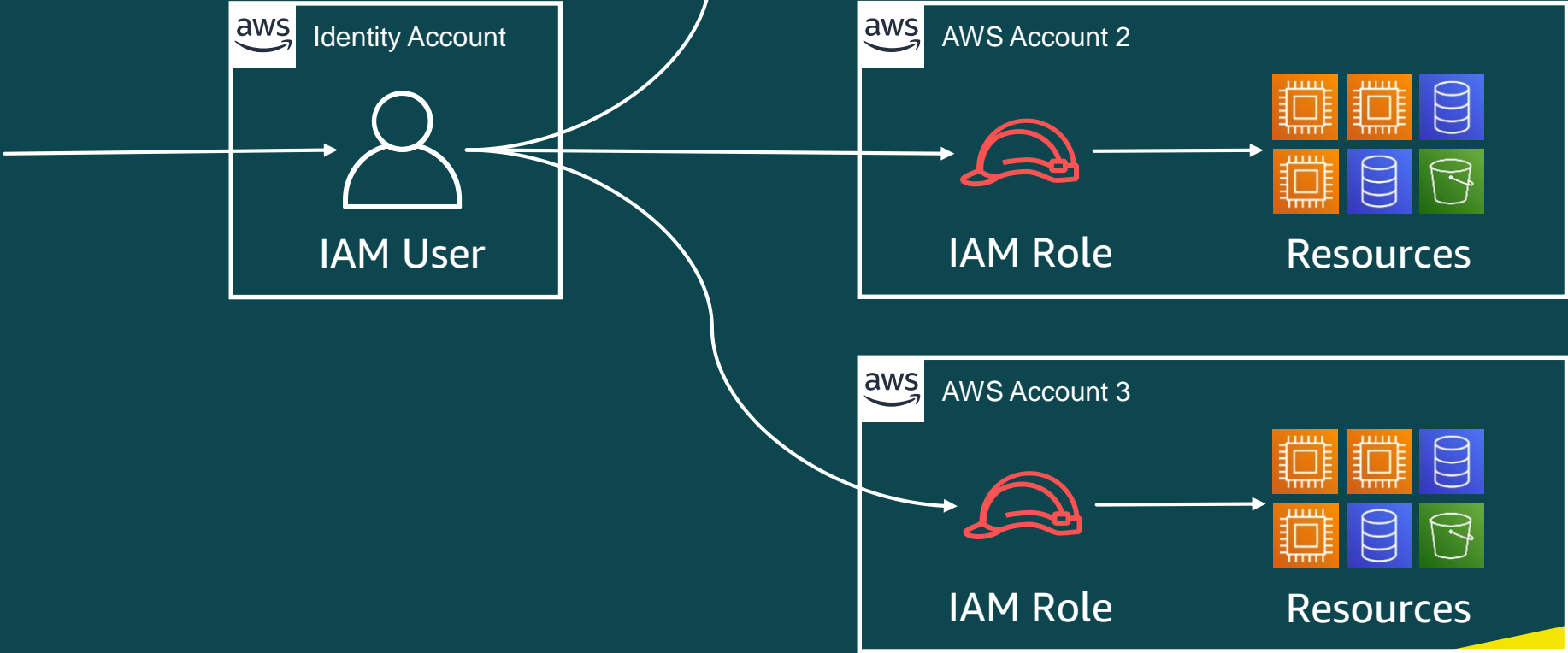
Users



Evolution of Federation



Users



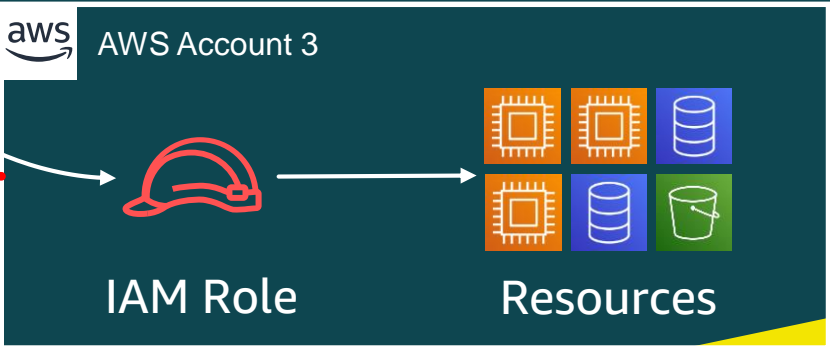
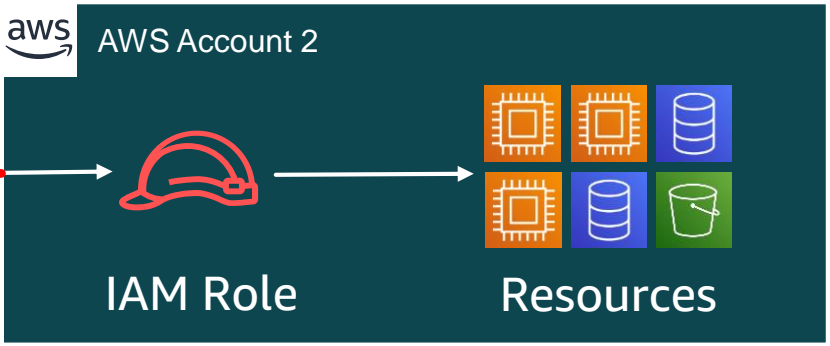
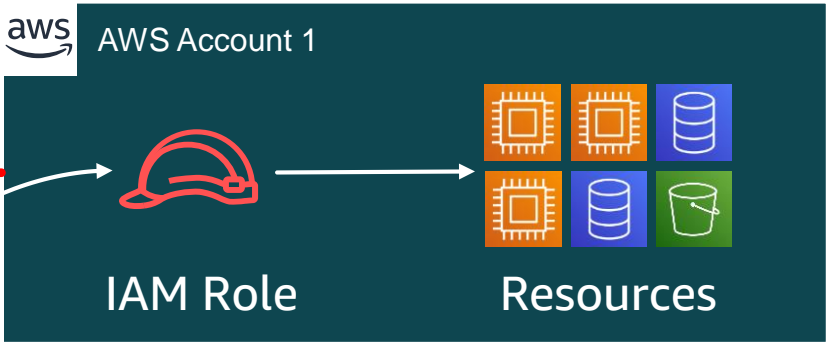
Evolution of Federation



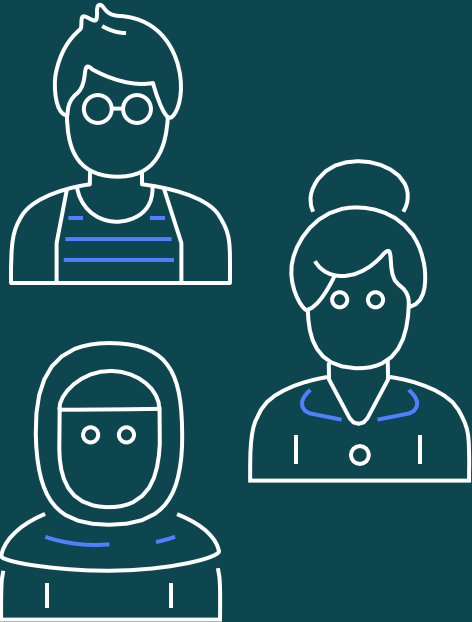
Users



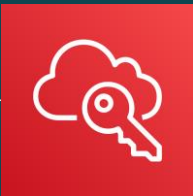
Identity Provider



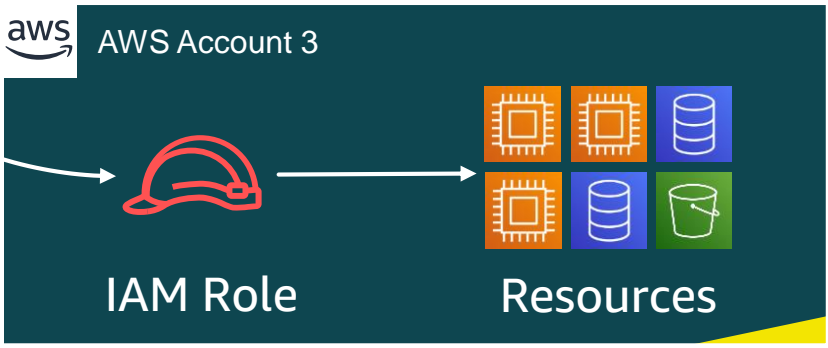
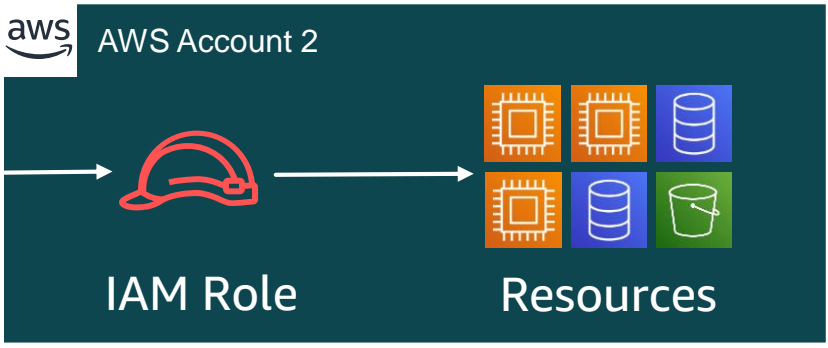
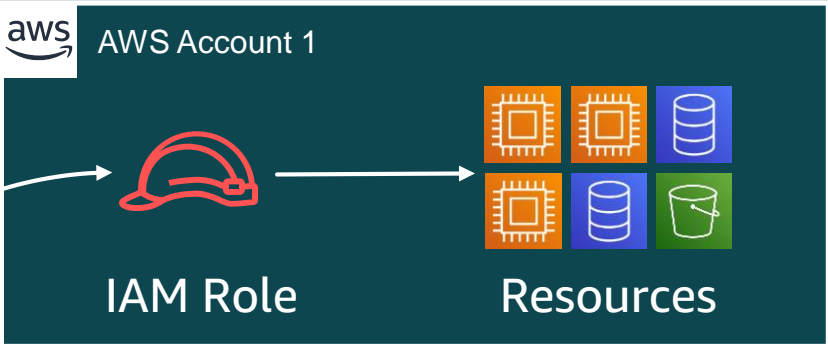
Evolution of Federation



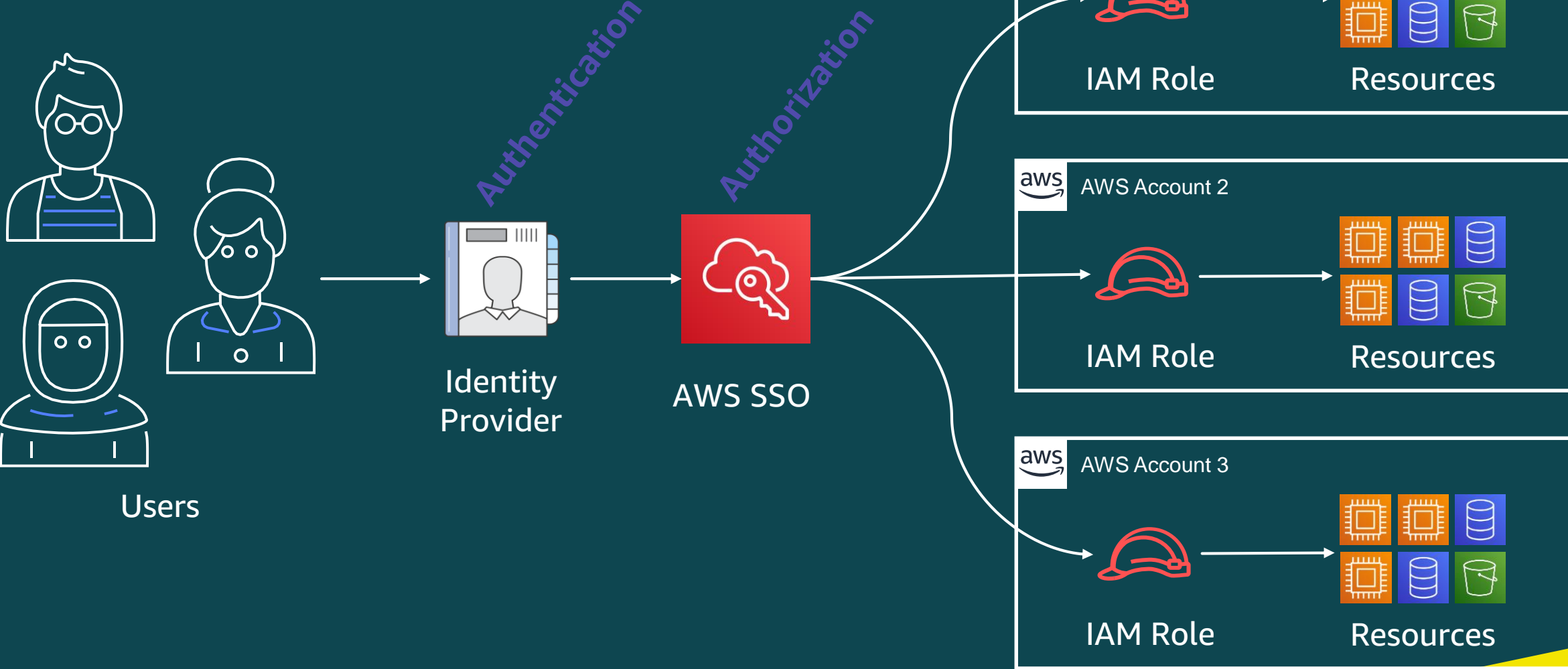
Users



AWS SSO



Evolution of Federation




AWS Single Sign-On




AWS Single Sign-On

Your applications Hi John | [Sign out](#)


Search




AWS Account (3)




Dropbox




Office365






Salesforce




Slack

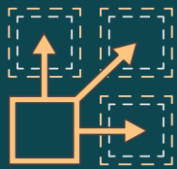


Workplace by Facebook

 111122223333 (Stage Account) >
 444455556666 (Production Account) v
Administrator Management console Command line or programmatic access
SecurityAudit Management console Command line or programmatic access
 777788889999 (Test Account) >

Terms of Use Powered by 

AWS Single Sign-On



Easy Management

Easily manage AWS account and role access at scale



One logon

One sign-in experience for cloud business applications



Existing IdP

Bring your own identities, or create them natively

AWS Single Sign-On



CLI

SSO from Command
Line Interface (CLI)



**First Party
Application Integration**

One sign-in for integrated
applications.
AWS IoT SiteWise Monitor
Amazon SageMaker
Notebooks

AWS Single Sign-On

aws Services Resource Groups

N. Virginia Support

Dashboard
AWS accounts
Applications
Users
Groups
Settings

AWS SSO > AWS Accounts

AWS Accounts

You can designate which users and groups have SSO access to AWS accounts in your AWS organization. You can also manage permission sets to control the users' level of access to these AWS accounts. [Learn more](#)

AWS organization | Permission sets

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. [Learn more](#)

[Assign users](#)

	AWS account	Permission sets
• All accounts	<input type="checkbox"/> Test Account #895187509657 xyz-test@amazon.com	None
▶ Root	<input type="checkbox"/> Stage Account #435458152495 xyz-stage@amazon.com	None
	<input type="checkbox"/> Preprod Account #584863750692 xyz-preprod@amazon.com	None
	<input type="checkbox"/> Production Account #985974384474 xyz-prod@amazon.com	None

Feedback English (US)

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Setting Up AWS SSO



AWS Single Sign-On (SSO)

AWS Single Sign-On is a cloud service that makes it easy to manage SSO access to multiple AWS accounts and business applications.

[Enable AWS SSO](#)

AWS Single Sign-On

Change identity source



Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. [Learn more](#)

- AWS SSO**
You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.
- Active Directory**
You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.
- External identity provider**
You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

Configure external identity provider

AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source, you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision users manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. [Learn more](#)

Sophos Simplifies and Centralizes AWS Account Management

Challenge

Sophos wanted a simpler and more scalable way to manage access across a growing number of AWS accounts and gain more flexible options when assigning user roles and permissions.

Solution

Sophos transitioned to AWS SSO, a service that makes it simpler to centrally manage access to multiple AWS accounts and business applications.

Benefits

- Simplified and centralized AWS account access management
- Achieved user satisfaction with no negative feedback
- Decreased time needed to onboard new AWS accounts

“ I don't think we got any negative feedback about AWS SSO. For a change that affects the daily workflow of about 1,500 people, that's kind of unprecedented.

—Guy Davies, principal cloud architect, Sophos

SOPHOS

Company: Sophos
Industry: Software & Internet
Country: United Kingdom
Website: sophos.com

About Sophos

Sophos provides 24/7 threat protection, monitoring, and response to stop cyberthreats targeting hybrid cloud environments. The Sophos Central security solution, built using AWS, protects more than 400,000 organizations in over 150 countries.

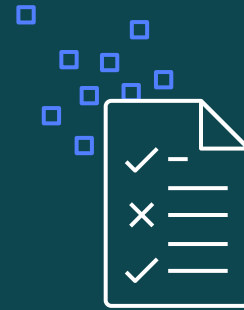
Migration Patterns



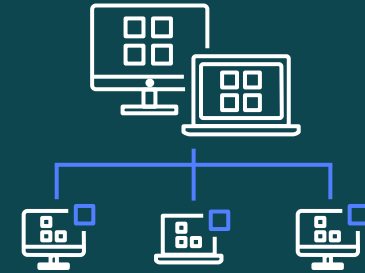
Migration is a Three Step Process



1. Migrate Your Users



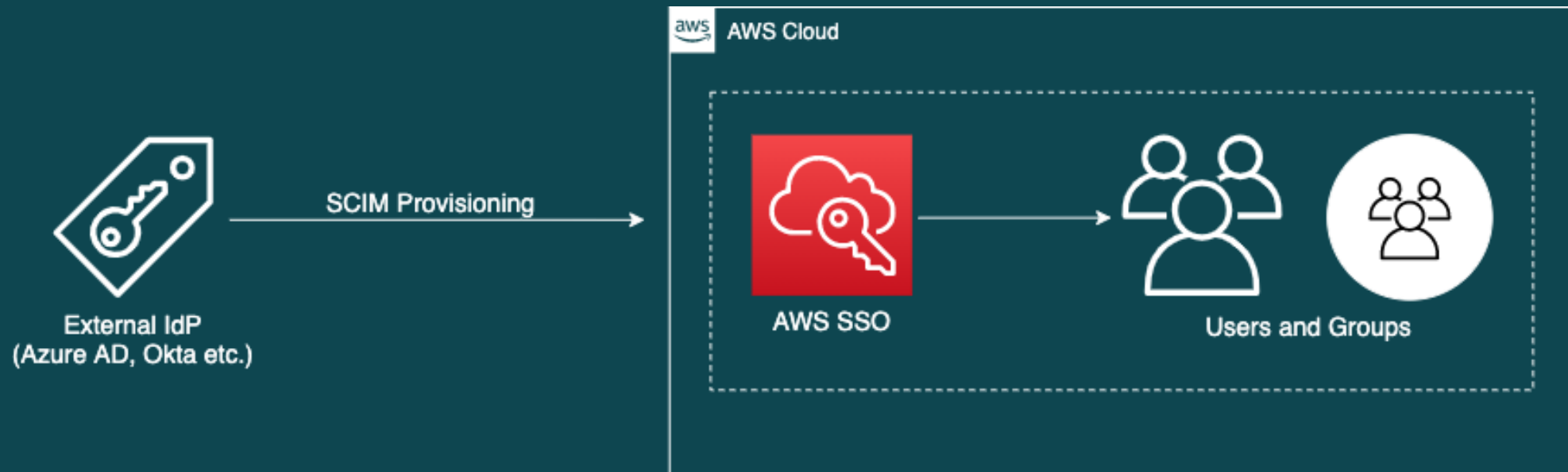
2. Migrate Your Permissions



3. Migrate Your Assignments

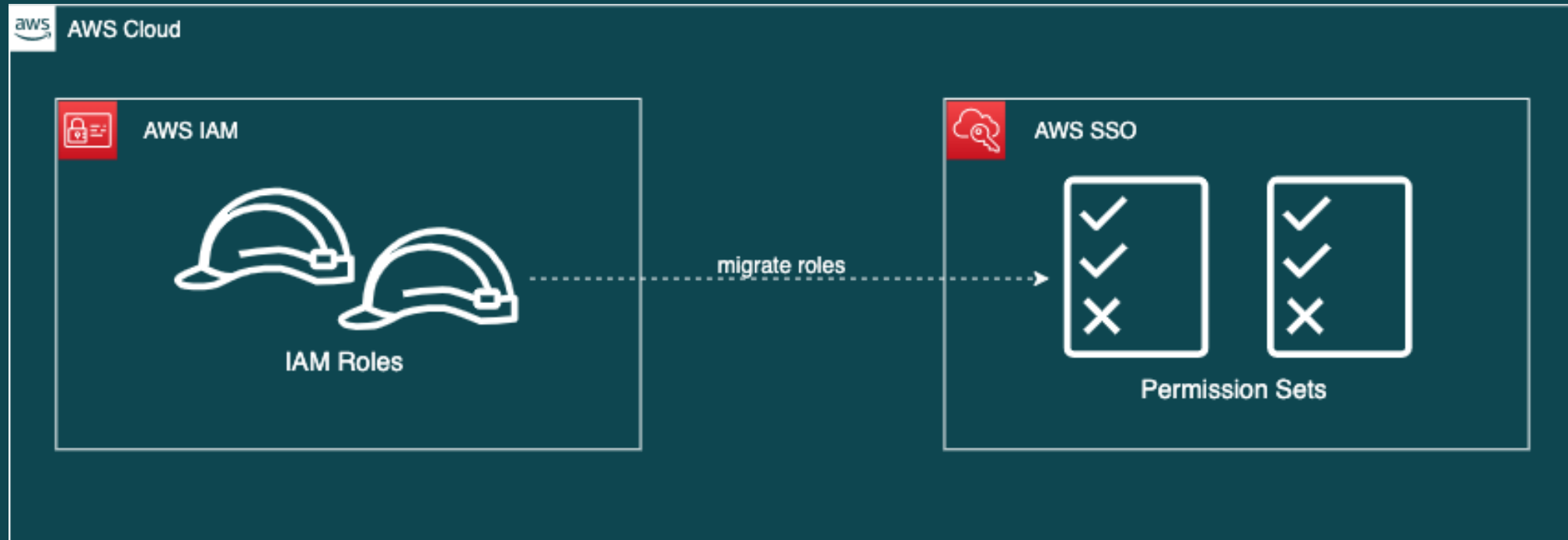
Migrate Your Users

- Setup SCIM and SAML federation for a new application in external IdP
- Sync across all users and groups via SCIM



Migrate Your Permissions

- Export existing federated IAM roles and policies from each account
- Import into AWS SSO as permission sets



Migrate Your Assignments

- Fetch existing User-Role assignments from external IdP
- Recreate assignments in AWS SSO



Additional Resources

- AWS Single Sign-On - <https://aws.amazon.com/single-sign-on>



Thank you!