AWS re:Invent

SEC308

Managing user permissions at scale with AWS SSO

Ron Cully
Principal Product Manager
AWS Identity
Amazon Web Services

AWS re:Invent

aws


Trust

“Identity is the new control plane”

Not exactly…

"If you want to go multi-cloud, what you have to do is to standardize on the lowest common denominator, and these platforms are nowhere close to the same."

Andy Jassy

CEO, Amazon Web Services

Zero Trust Architecture

Zero Trust Architecture Logical Components

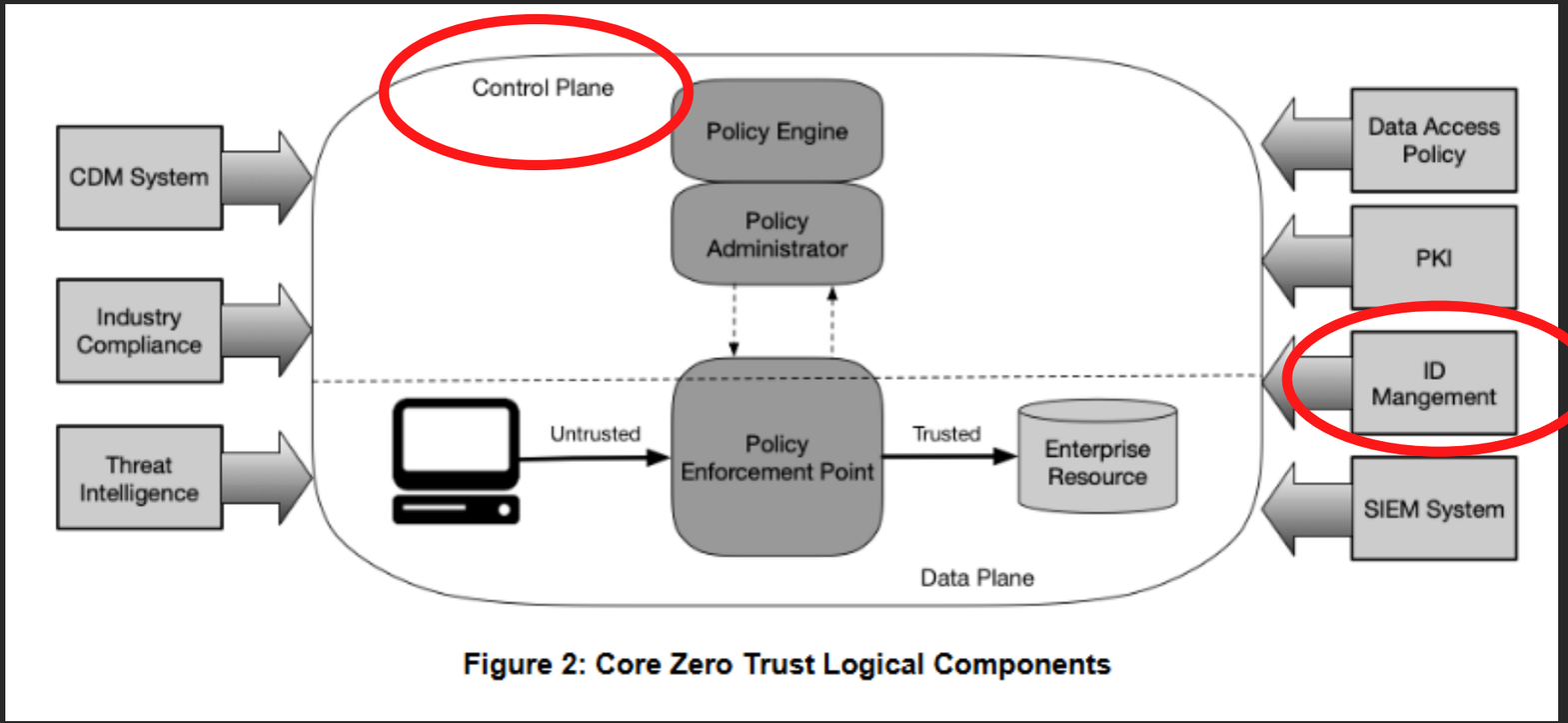


Figure 2: Core Zero Trust Logical Components

Draft NIST Special Publication 800-207

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf

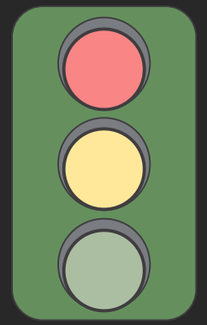
Who has access to what

Who

Identity

Name
Credentials
Meta data

has access



Access

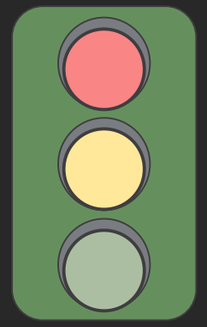
Policies
Governance
Compliance

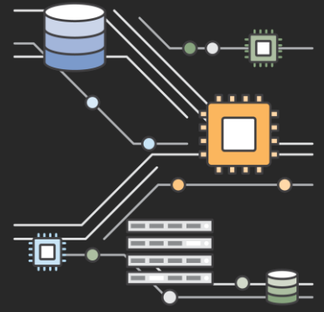
to what

Resource

Isolation
Grouping
Tagging
Sharing

Who has access to what





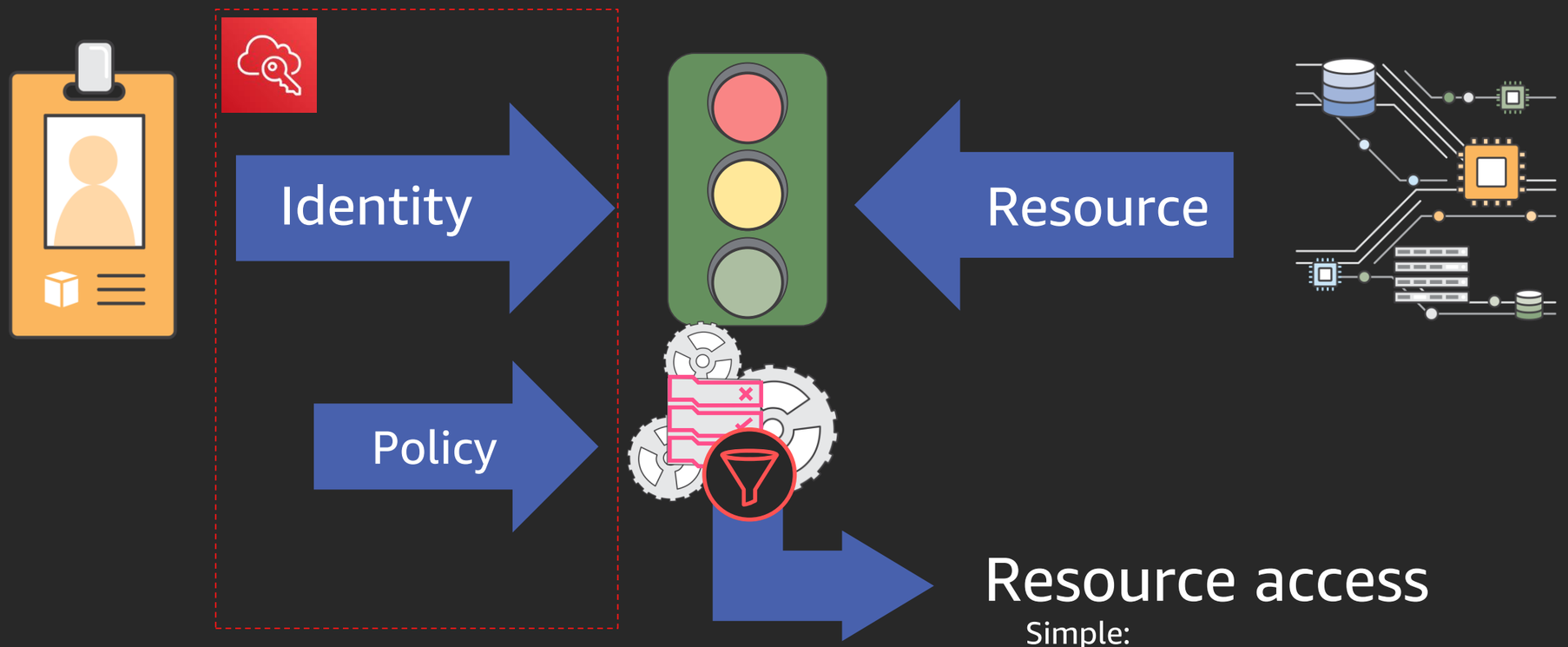
Identity

Access

Resource

Standard models

Environment-specific models



Resource access

Simple:
Access to an application

Complex:
Resource specific fine grained access

Agenda

AWS identity, access, and resource management evolution

AWS Single Sign-On (AWS SSO) access management model

Demo

AWS SSO use cases

Options for AWS SSO with your existing identities

Best practices

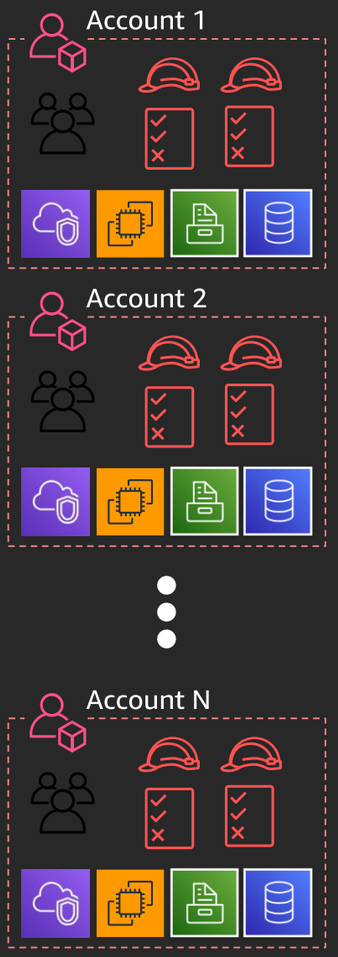
AWS identity evolution

AWS identity, access, and resource management evolution

Identities, groups, roles, and assignments per account

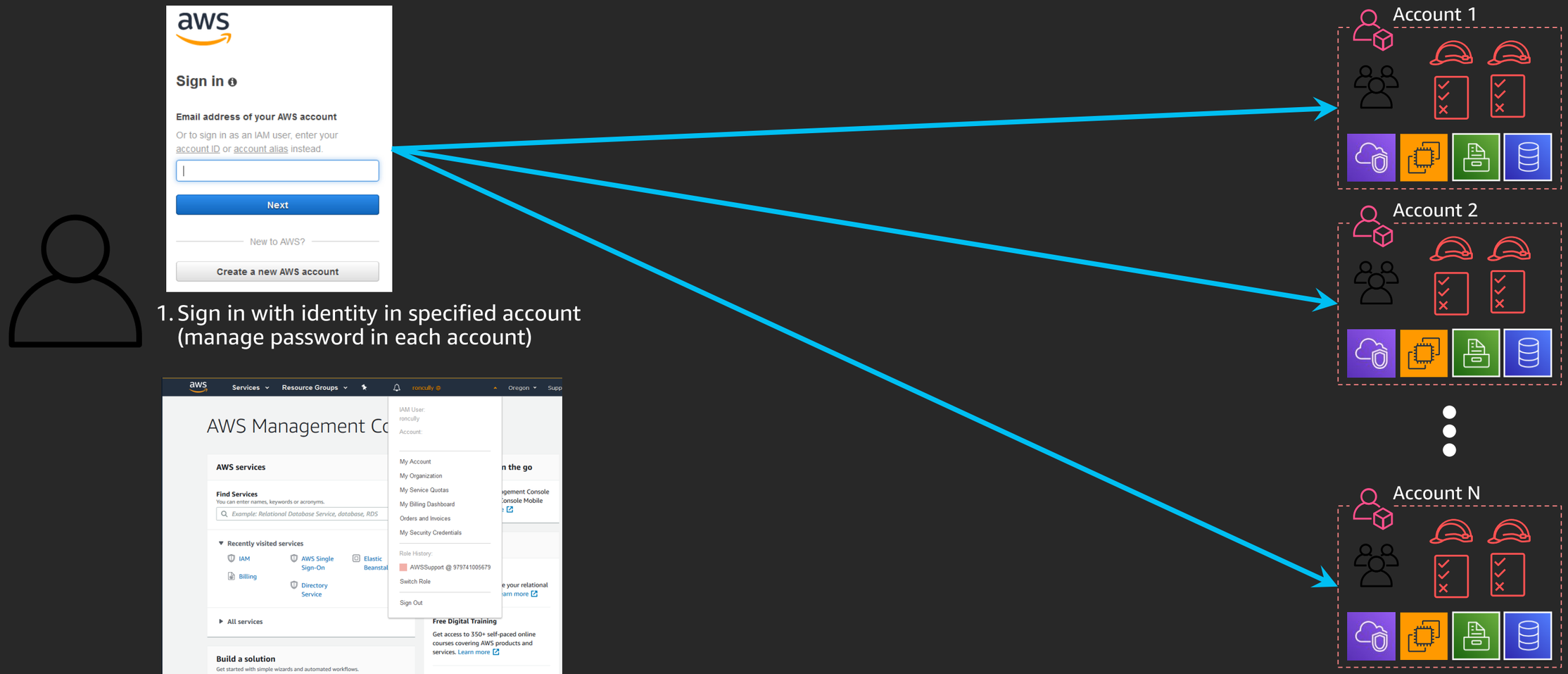
Admin tasks in every account

- Create users' identity
- Create groups and add users
- Create roles and attach policies
- Assign roles to groups and users



AWS identity, access, and resource management evolution

Identities, groups, roles, and assignments per account



AWS identity, access, and resource management evolution

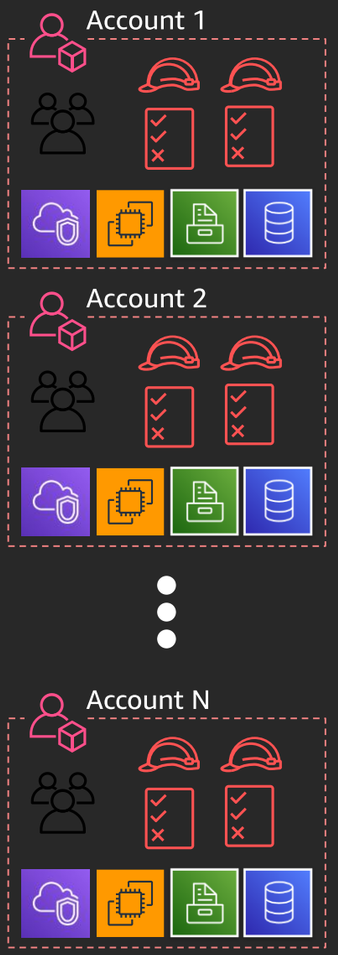
IAM federation: One identity, with per account roles and assignments

Admin tasks in every account

- Create cross-account trusts
- Create SAML trust
- Create roles and attach policies

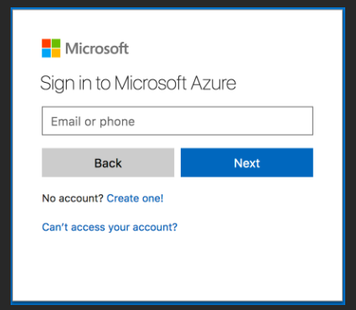
Admin tasks at identity provider

- Create SAML trust to each account
- Create assertion rules that match roles in AWS

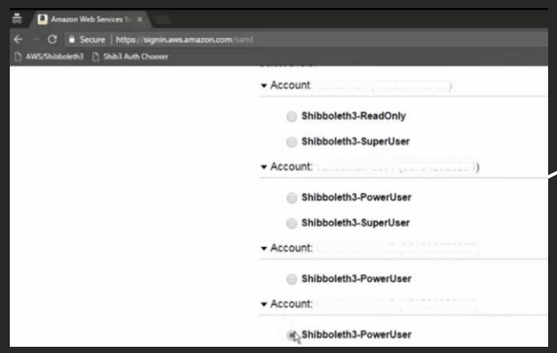


AWS identity, access, and resource management evolution

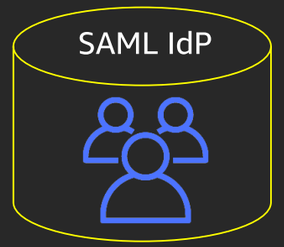
IAM federation: One identity, with per account roles and assignments

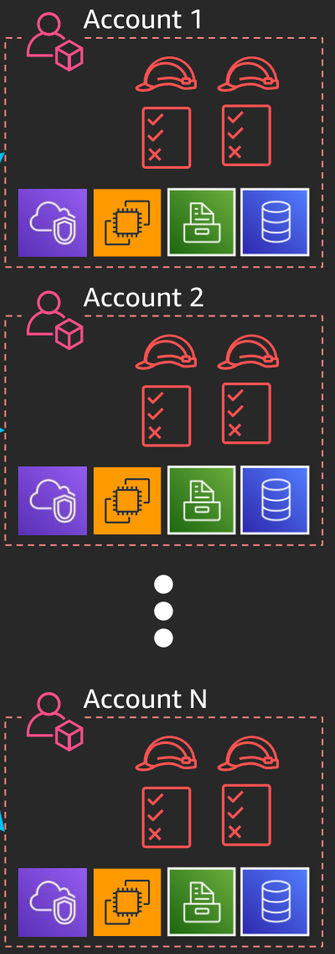


1. Sign-in to federated identity provider



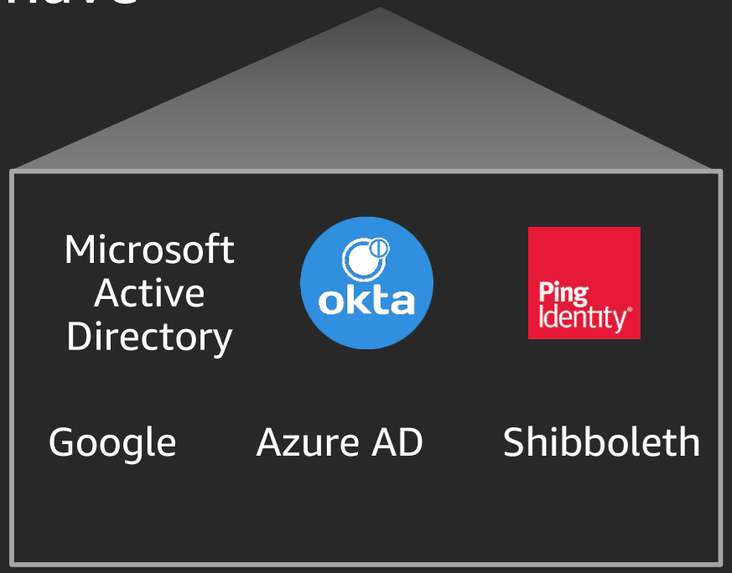
2. Use AWS role chooser to select role and account





Enterprise customer requests

"Let us use the enterprise identities we already have"



"Make it easier to manage access at scale across AWS accounts"

Startups/Smaller customer requests

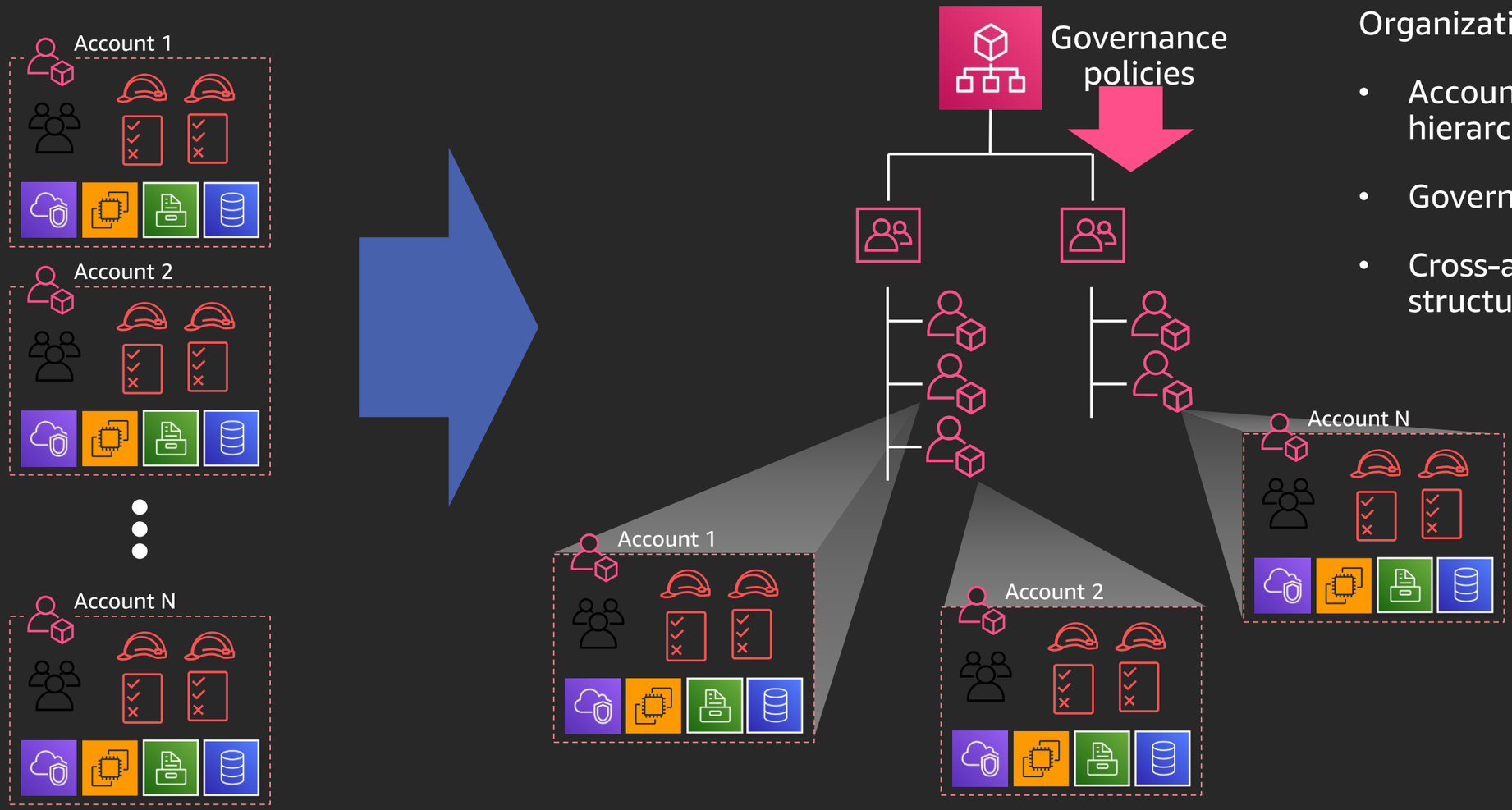
“Give us identities we can use inside and outside AWS”

“Simplify multi-account permission management”

No company identity system

AWS identity, access, and resource management evolution

AWS Organizations

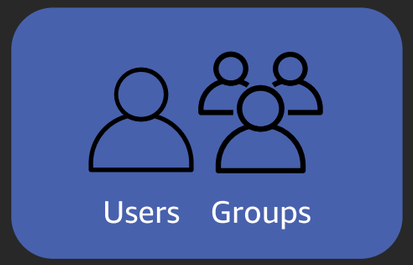


Organizations adds

- Account management hierarchy
- Governance policies
- Cross-account sharing structure

AWS SSO access management model

AWS account access

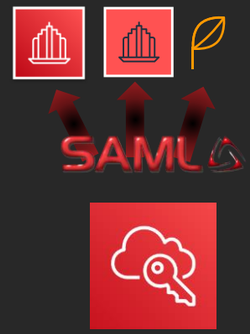


Choose identity source

Define role-oriented permission sets

Assign groups/users to permission sets in selected accounts

Application access



Connect cloud apps with SAML

Assign groups/users to apps

Demo

AWS SSO use cases

Manage access to AWS accounts and roles

Increase developer productivity with AWS Command Line Interface (AWS CLI) v2

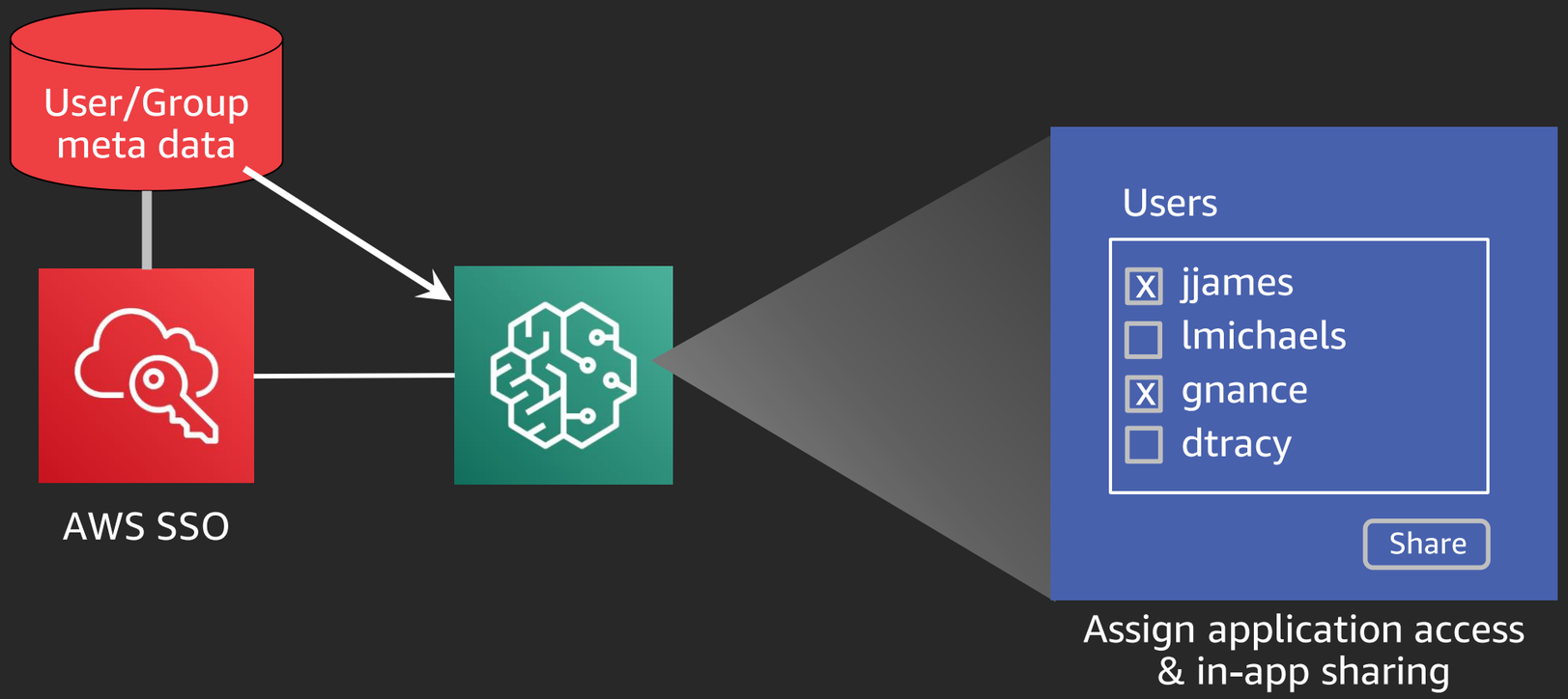
Manage access and sign-in to AWS SSO integrated applications

Manage access to cloud-based business applications

One AWS access control model

You choose your identity source

AWS SSO integrated application model



Identity source options

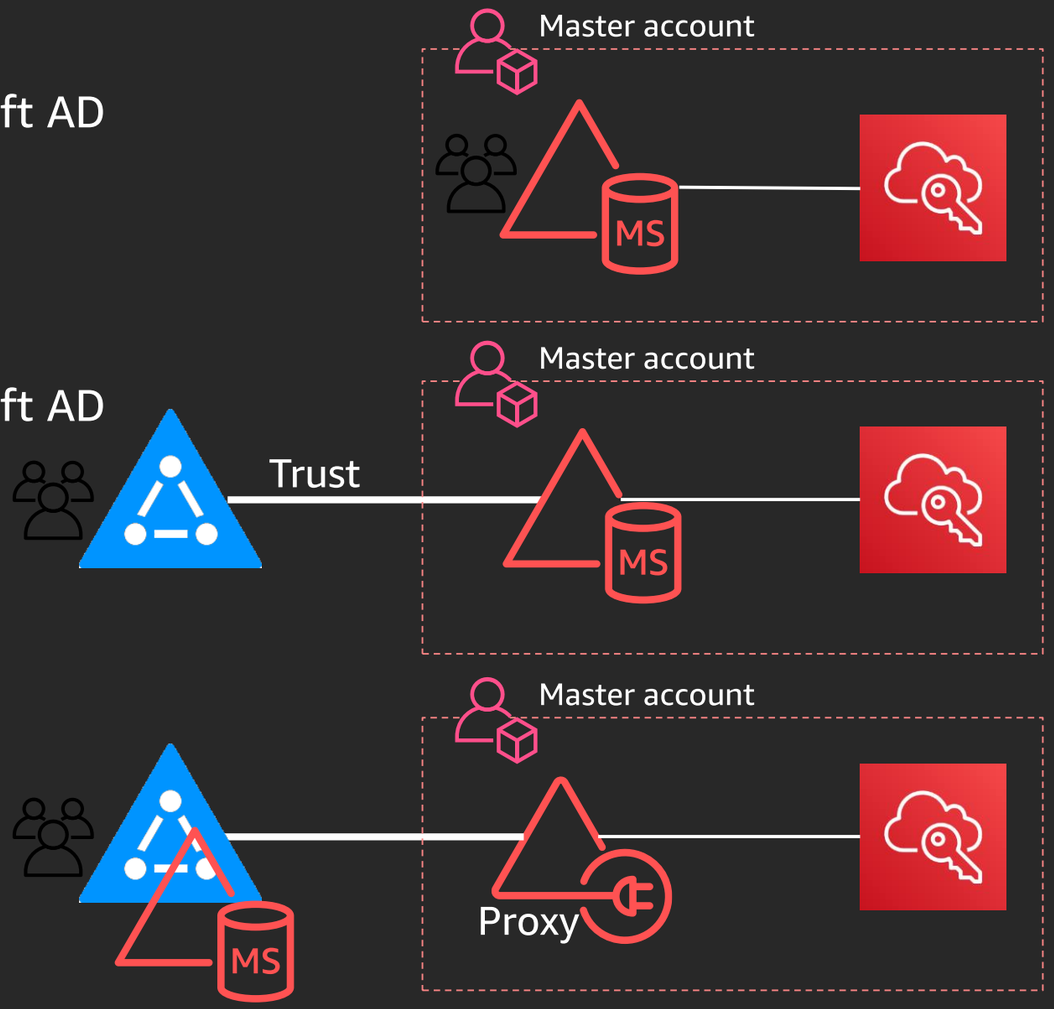
Using AWS SSO with Microsoft Active Directory Domain Services

AD DS connection options

AWS Managed Microsoft AD
(user forest)

AWS Managed Microsoft AD
(resource forest)

AD Connector



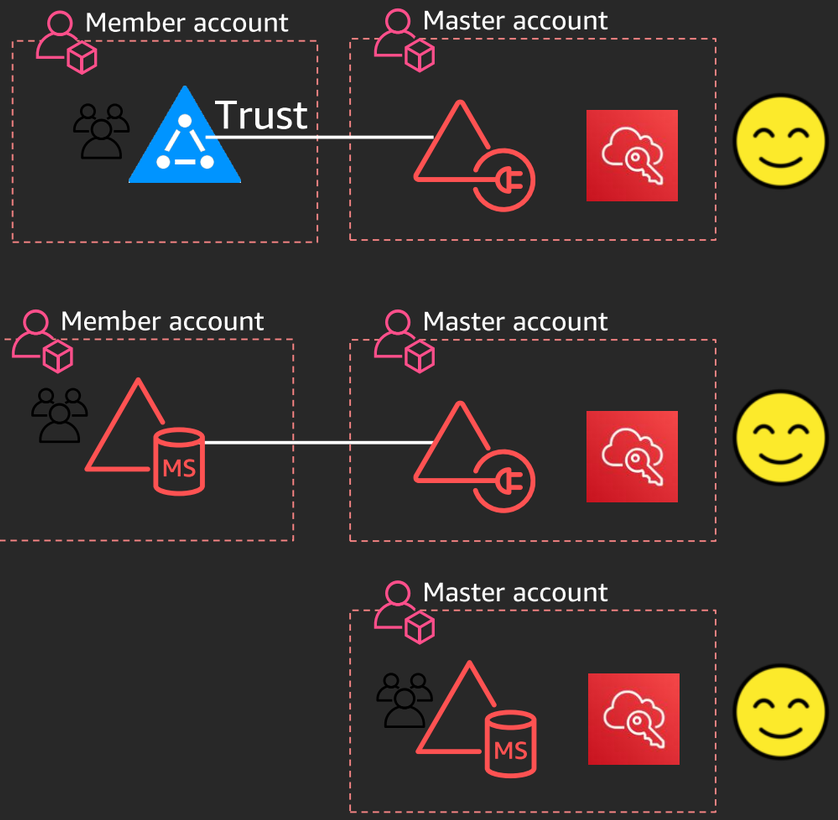
AWS SSO required
in AWS Organizations
master account

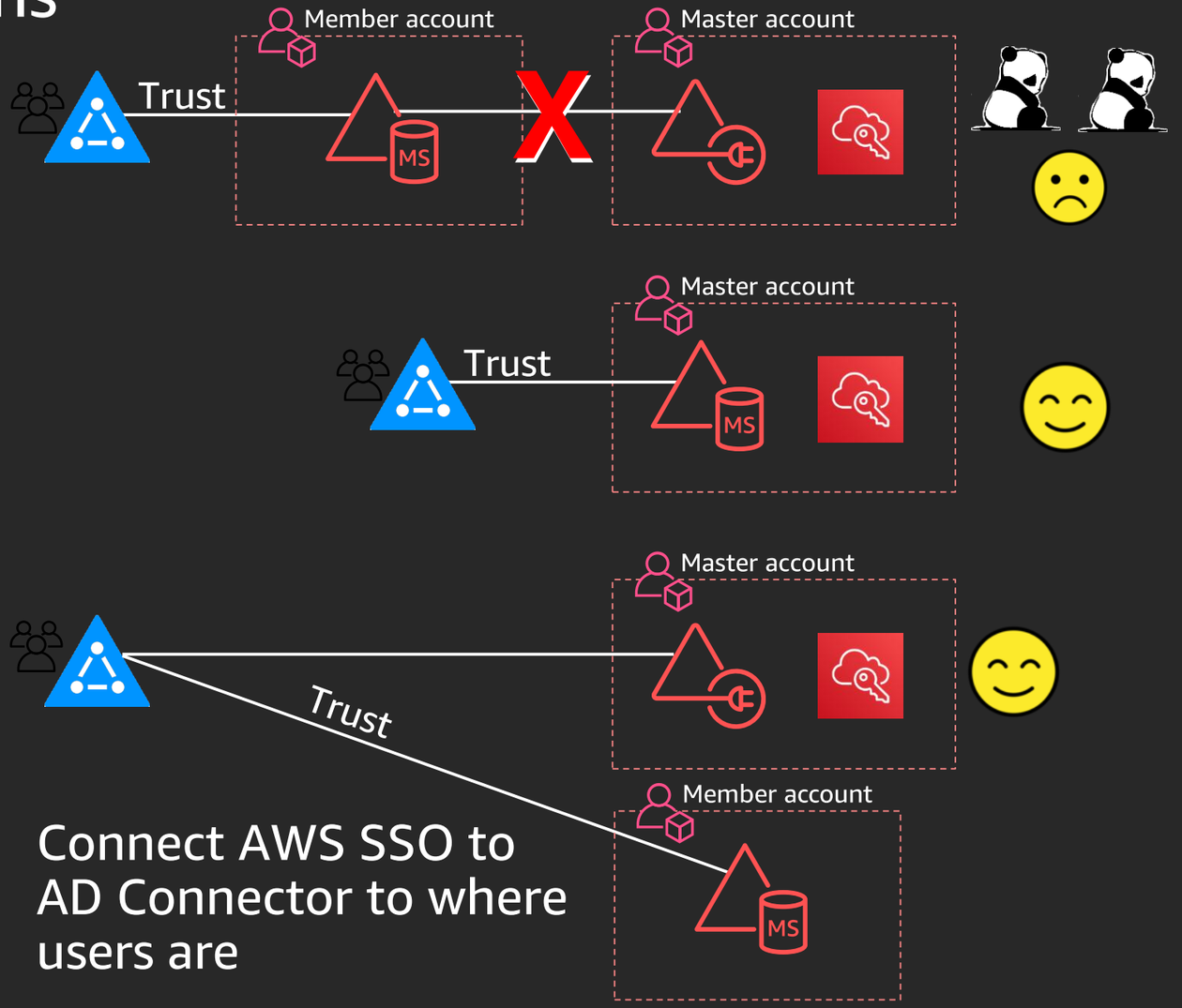
AD Connector or
AWS Managed Microsoft AD
required in master account

Active Directory users may
be in any account

Using AWS SSO with Microsoft Active Directory Domain Services

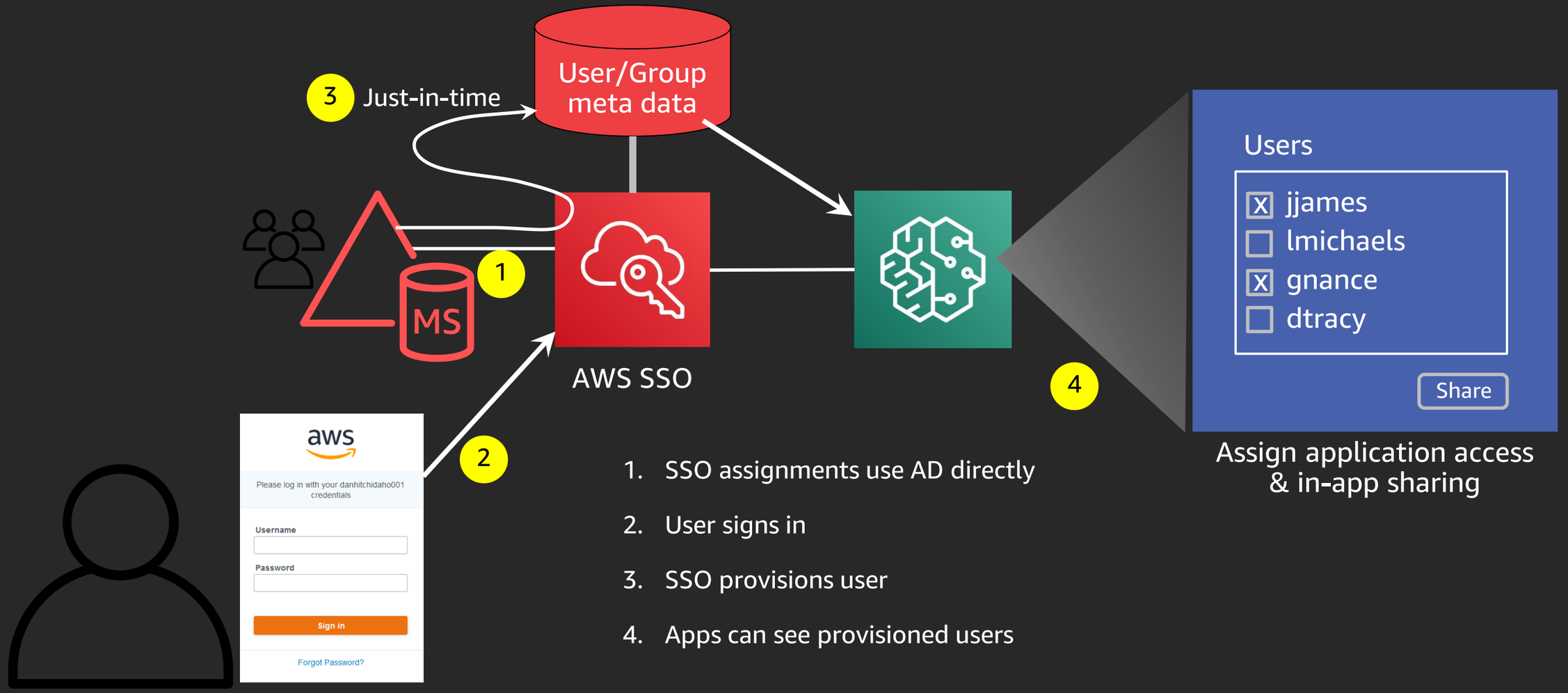
Example AD DS topology variations





Connect AWS SSO to AD Connector to where users are

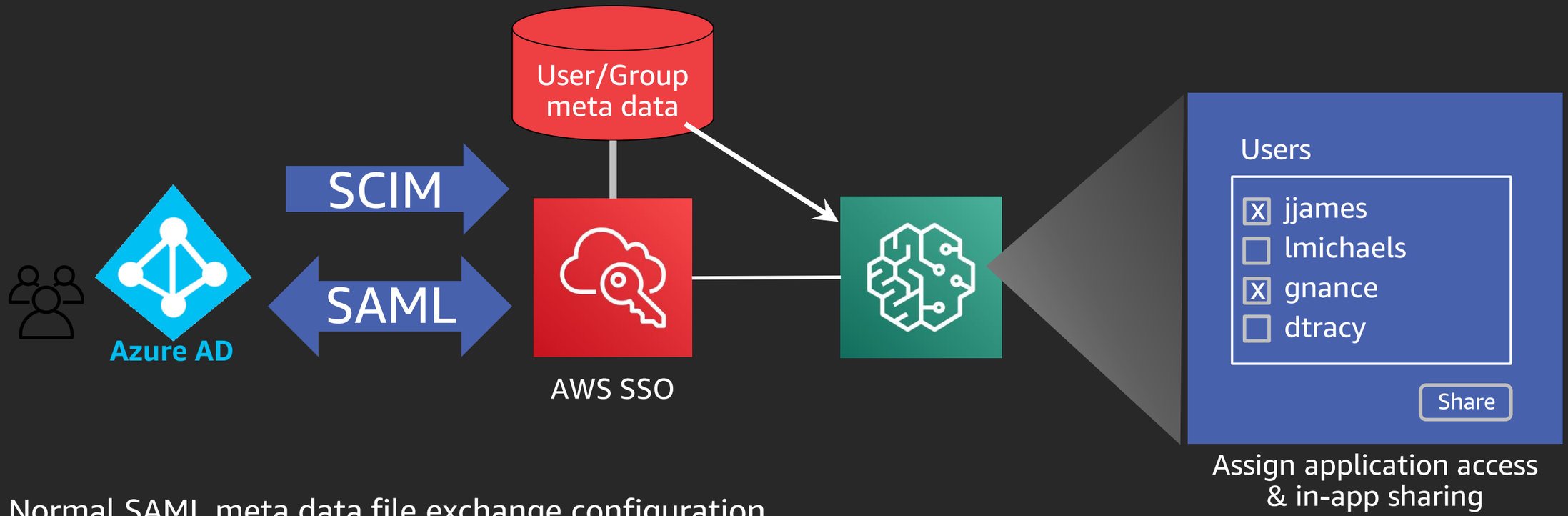
Provisioning and AWS application integration



Assign application access & in-app sharing

1. SSO assignments use AD directly
2. User signs in
3. SSO provisions user
4. Apps can see provisioned users

Using AWS SSO with Azure Active Directory with SCIM



Normal SAML meta data file exchange configuration

Configure Azure AD with AWS SSO SCIM end-point + bearer token

SCIM is optional (recommend)

IMPORTANT: Be sure to synchronize email attributes

Differences based on identity source configuration

Feature	AWS SSO	AWS Managed Microsoft AD	AD Connector	SAML 2.0 w/manual provisioning	SAML 2.0 w/SCIM provisioning
Create user/group	Yes	No	No	Provisioning only	No
Delete user/group	Yes	No	No	Provisioning only	Provisioning only
Reset user passwords	Yes	N/A	N/A	Identity Provider	Identity Provider
Where to configure MFA	AWS SSO	AWS SSO or AWS Managed AD	AWS SSO or AD Connector	Identity Provider	Identity Provider
Provisioning	AWS SSO Console	Just In Time	Just In Time	AWS SSO Console	Identity Provider
Switch to AD	Deletes users, groups, entitlements	Deletes users, groups, entitlements	Deletes users, groups, entitlements	Deletes users, groups, entitlements	Deletes users, groups, entitlements
Switch to IdP	Preserves entitlements for matching users	Deletes users, groups, entitlements	Deletes users, groups, entitlements	Preserves entitlements for matching users	Preserves entitlements for matching users
Switch to AWS SSO	N/A	Deletes users, groups, entitlements	Deletes users, groups, entitlements	Preserves entitlements, password reset?	Preserves entitlements, password reset?
Session duration	AWS SSO permission set session duration	AWS SSO permission set session duration	AWS SSO permission set session duration	Lesser of IdP session or AWS SSO permission set session duration	Lesser of IdP session or AWS SSO permission set session duration

Best practices

Use group assignments

Use SCIM for best security/consistency/convenience

Make sure users have email address attribute in AWS SSO

Specify IdP user/group names when provisioning manually or doing POCs

Configure virtual MFA when using AD DS or AWS SSO as identity source

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security

Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

Ron Cully

rcully@amazon.com

AWS re:Invent

aws

Please complete the session survey in the mobile app.