Using AWS Single Sign-On with Okta Active Directory, and AWS SSO identities

Ron Cully,
Principal Product Manager, AWS

Yuri Duchovny,
Solutions Architect, AWS

Thursday, May 28, 2020

https://www.youtube.com/watch?v=XW5amgAuRIo

AWS Online Tech Talks

91.6K subscribers • 1,336 videos

AWS Online Tech Talks are live, online presentations that cover a broad range of topics at varying technical levels. These tech ...

SUBSCRIBE

Deep Dive

Working with Different Identity Sources in AWS Single Sign-On

aws

Today…

User and group provisioning into AWS SSO

AWS SSO source of truth model

Purpose
Enable customers to…

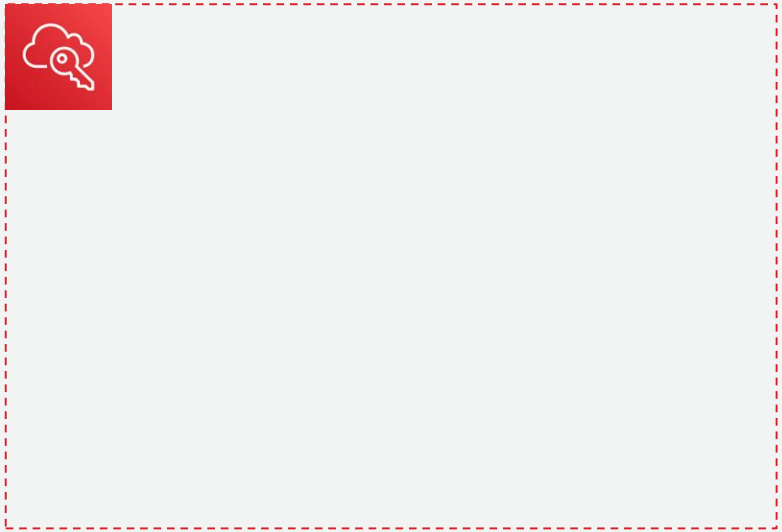
AWS SSO

Manage users and groups where you want, connect them to AWS once

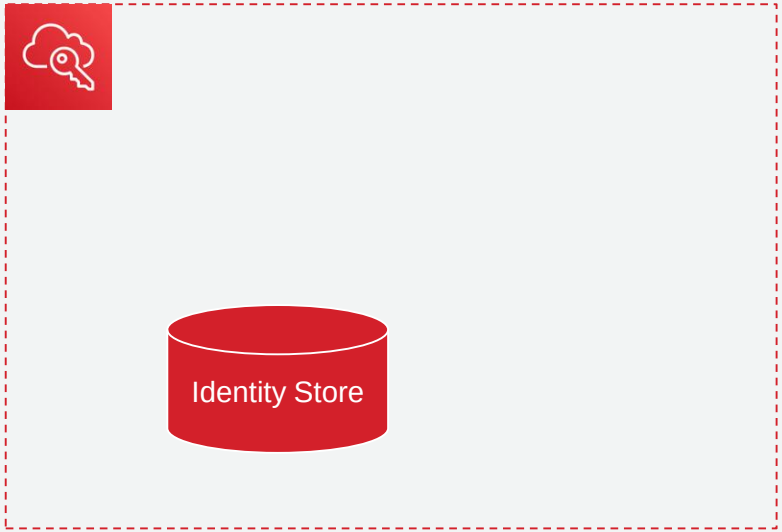
Assign access centrally to AWS accounts and AWS SSO integrated applications

Provide user portal to assigned accounts and applications

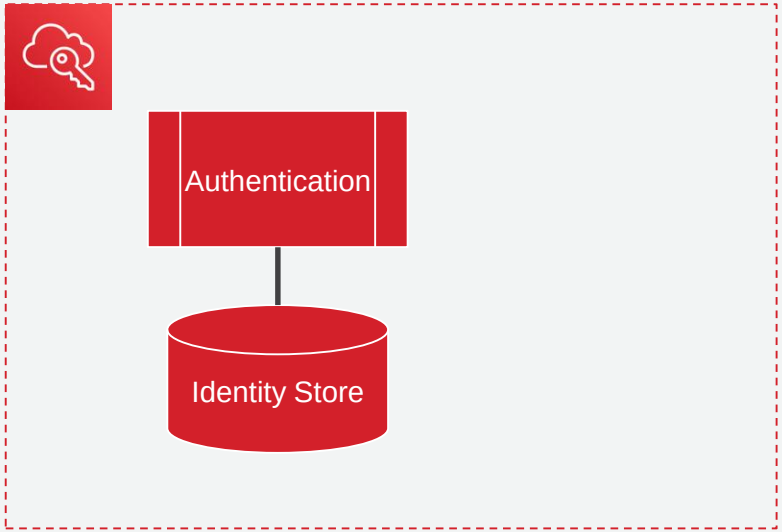
AWS SSO logical architecture



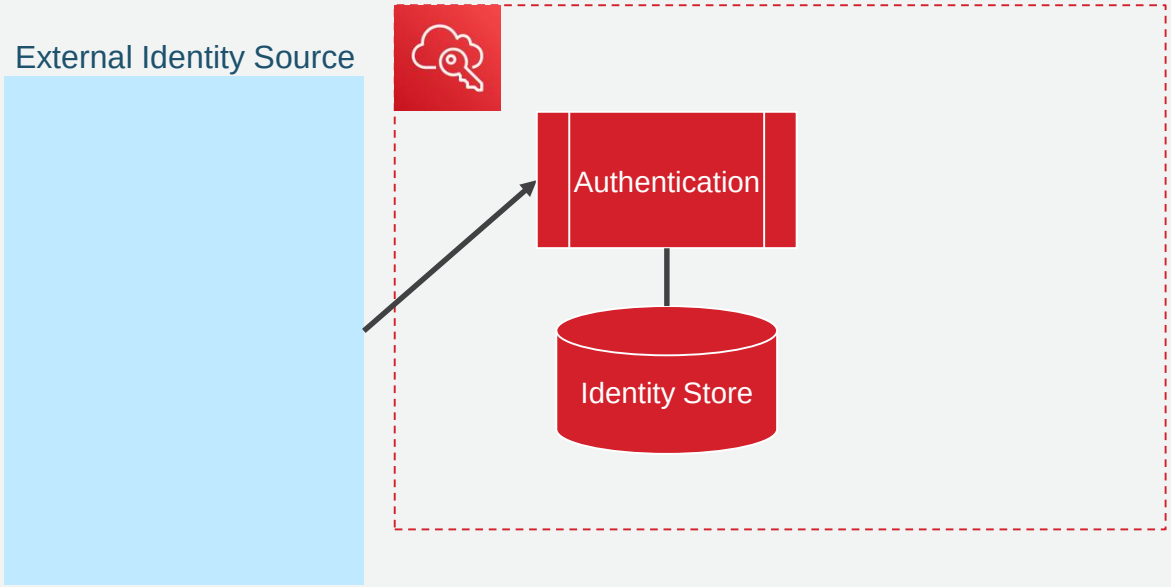
AWS SSO logical architecture



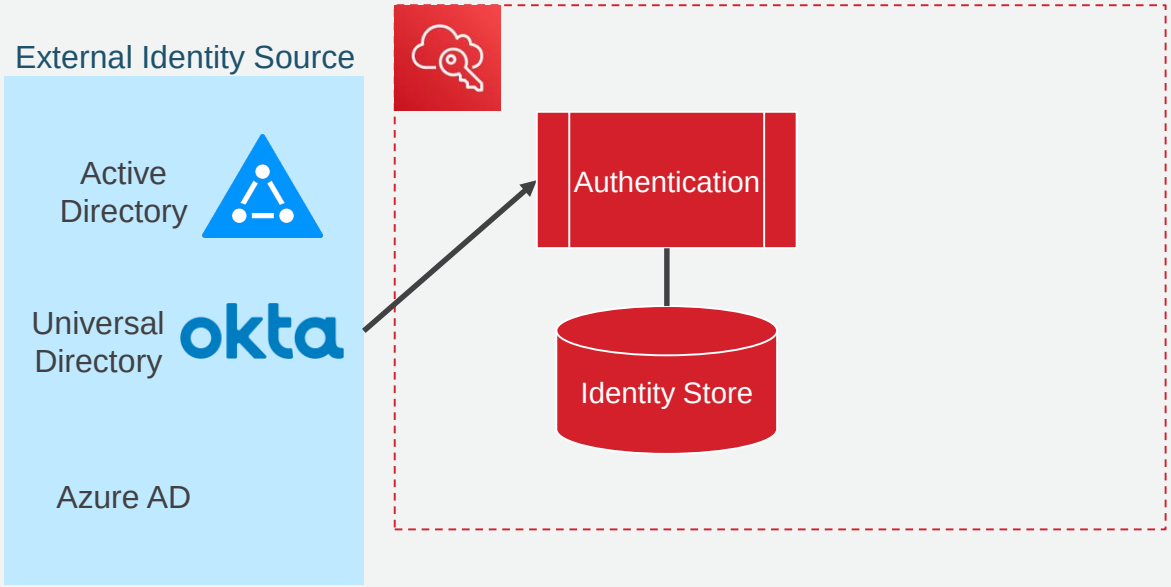
AWS SSO logical architecture



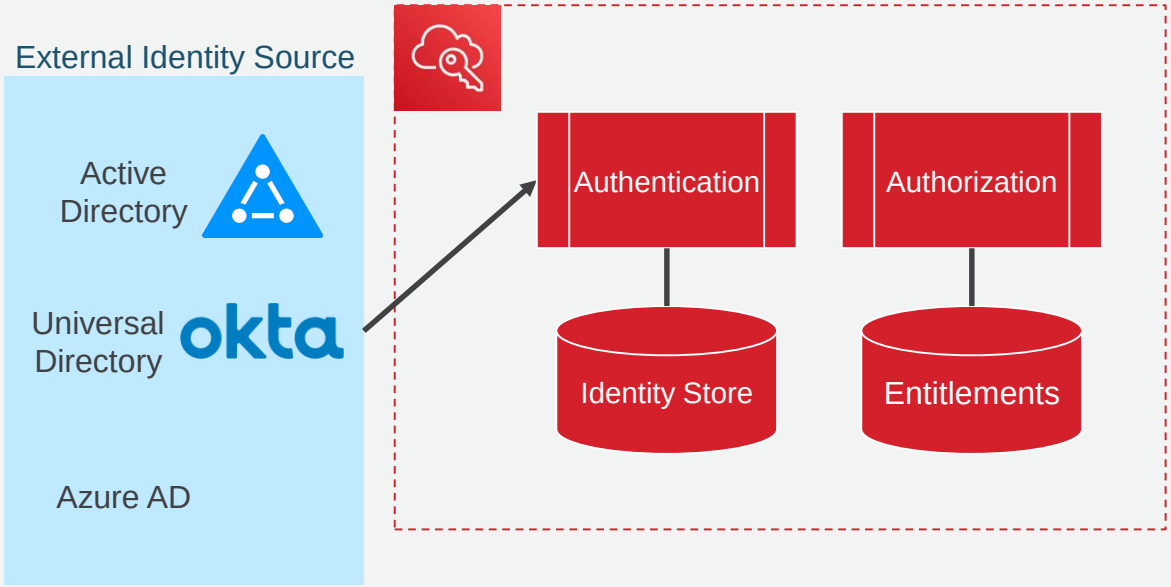
AWS SSO logical architecture



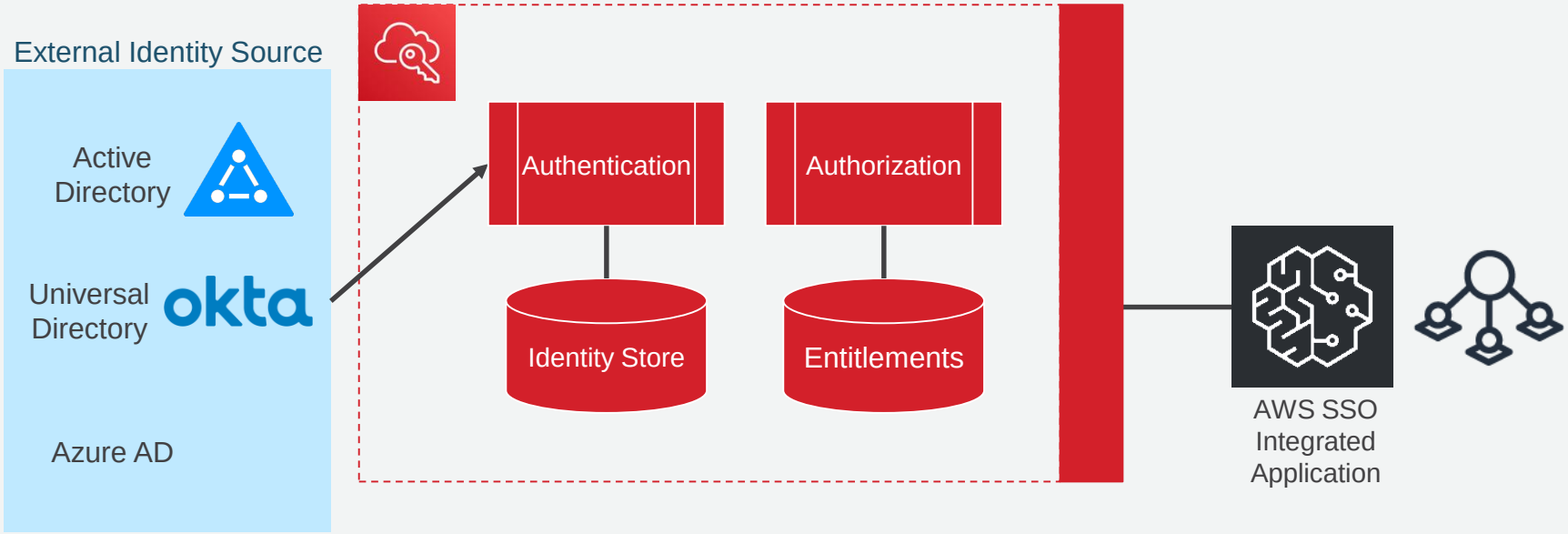
AWS SSO logical architecture



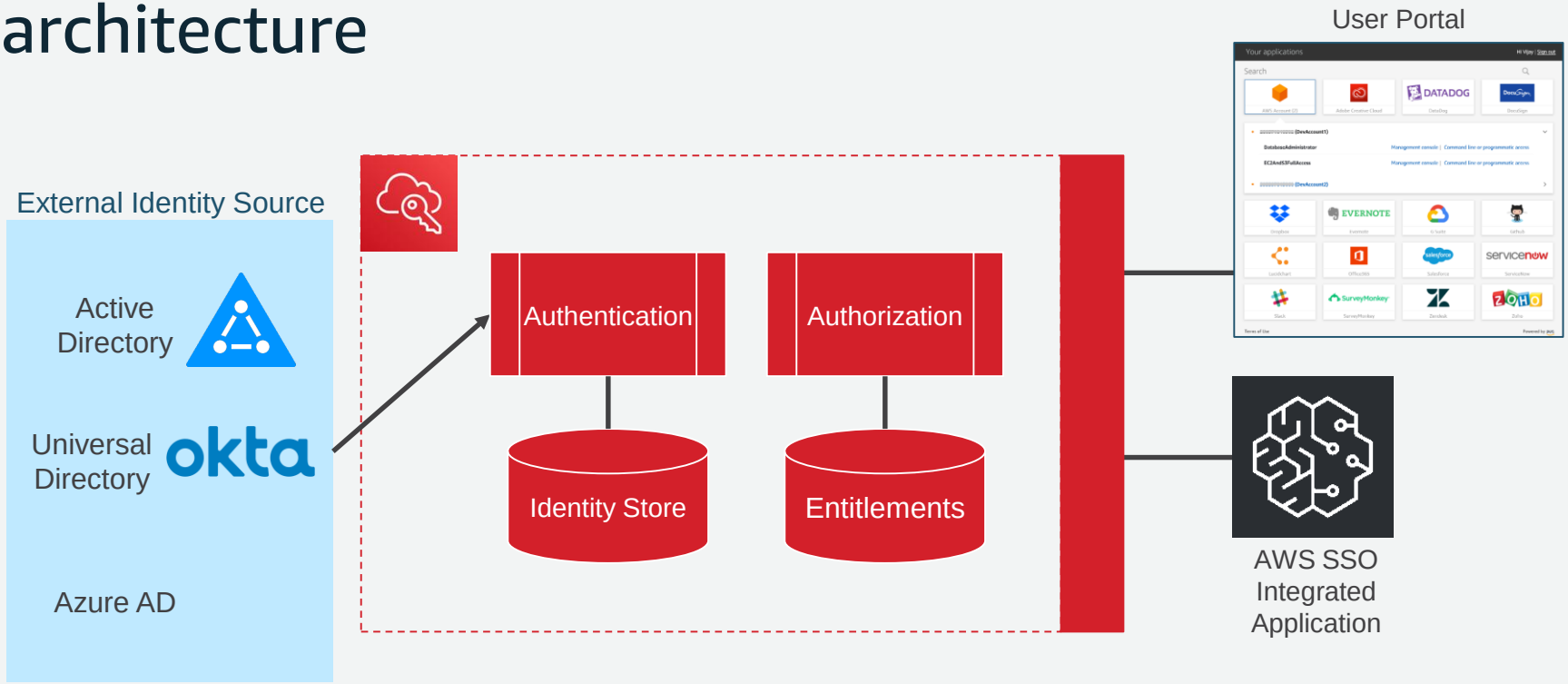
AWS SSO logical architecture



AWS SSO logical architecture

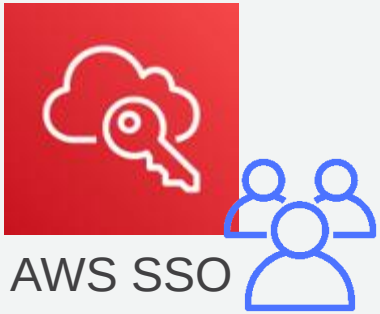


AWS SSO logical architecture



Where to manage and authenticate users

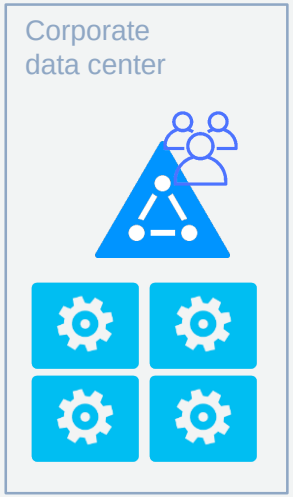
Manage users/groups in AWS SSO when…



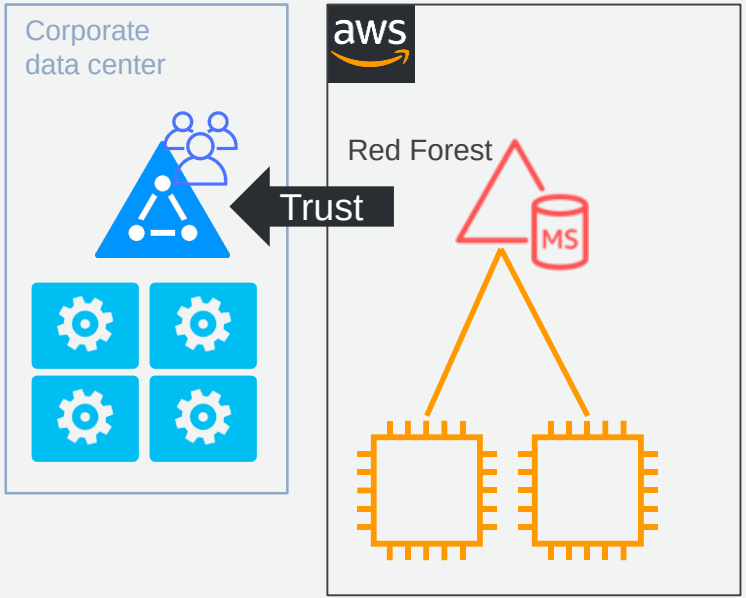
No existing identity system

Smaller scale user deployment

When migrating Active Directory workloads…

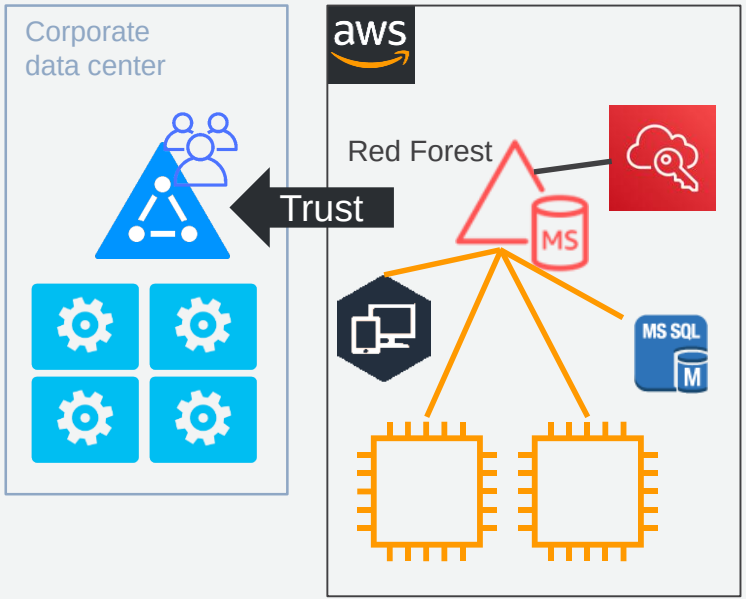


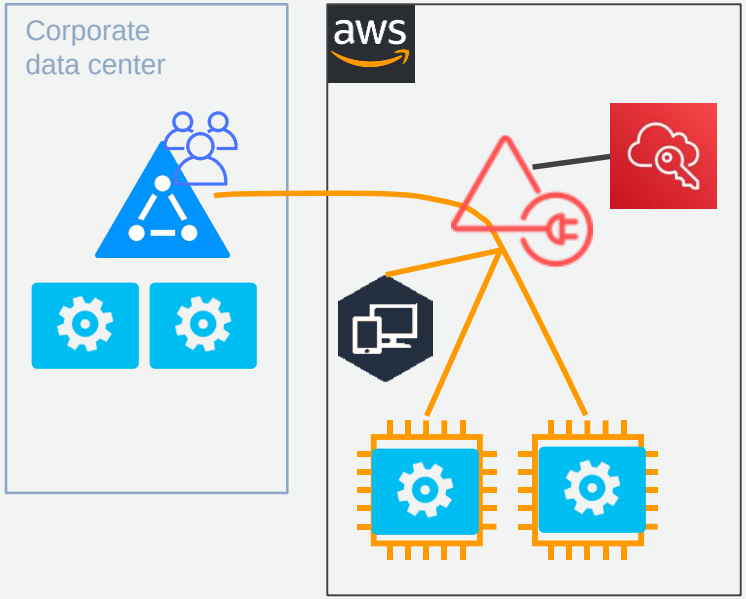
When migrating Active Directory workloads…



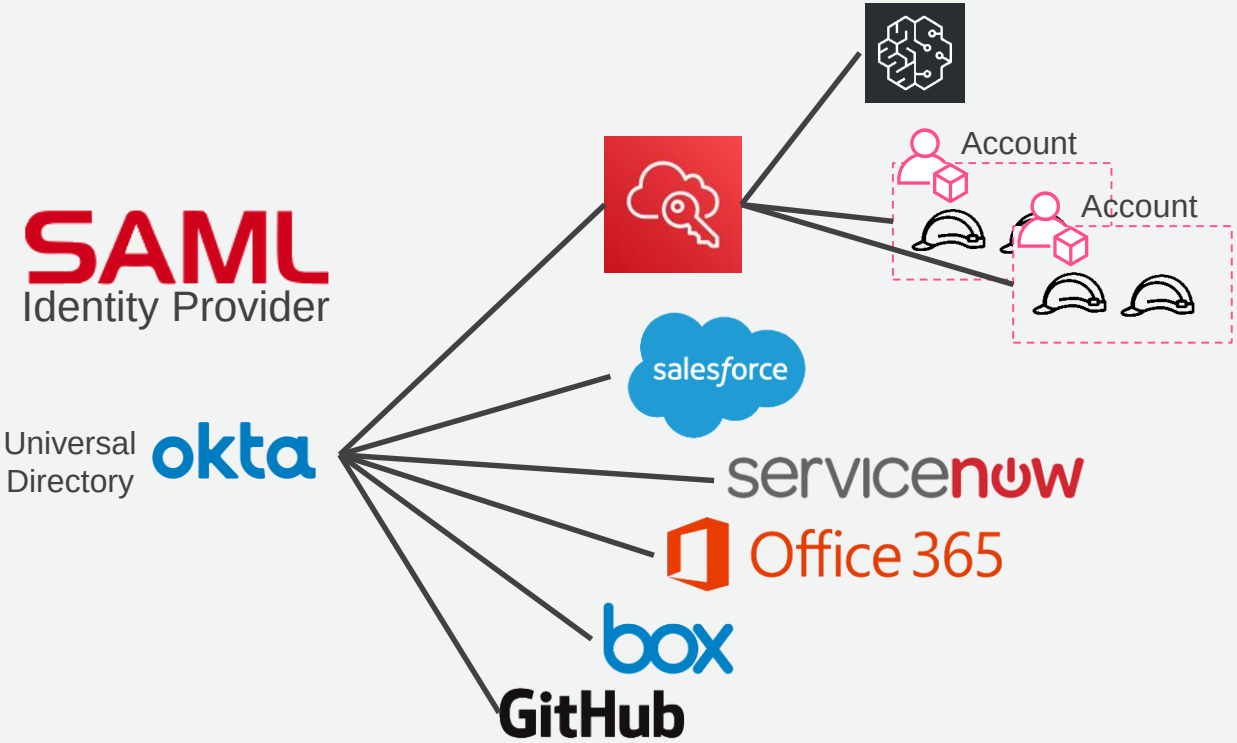
When migrating Active Directory workloads…

use Active Directory via AWS Directory Service for Microsoft AD or AD Connector

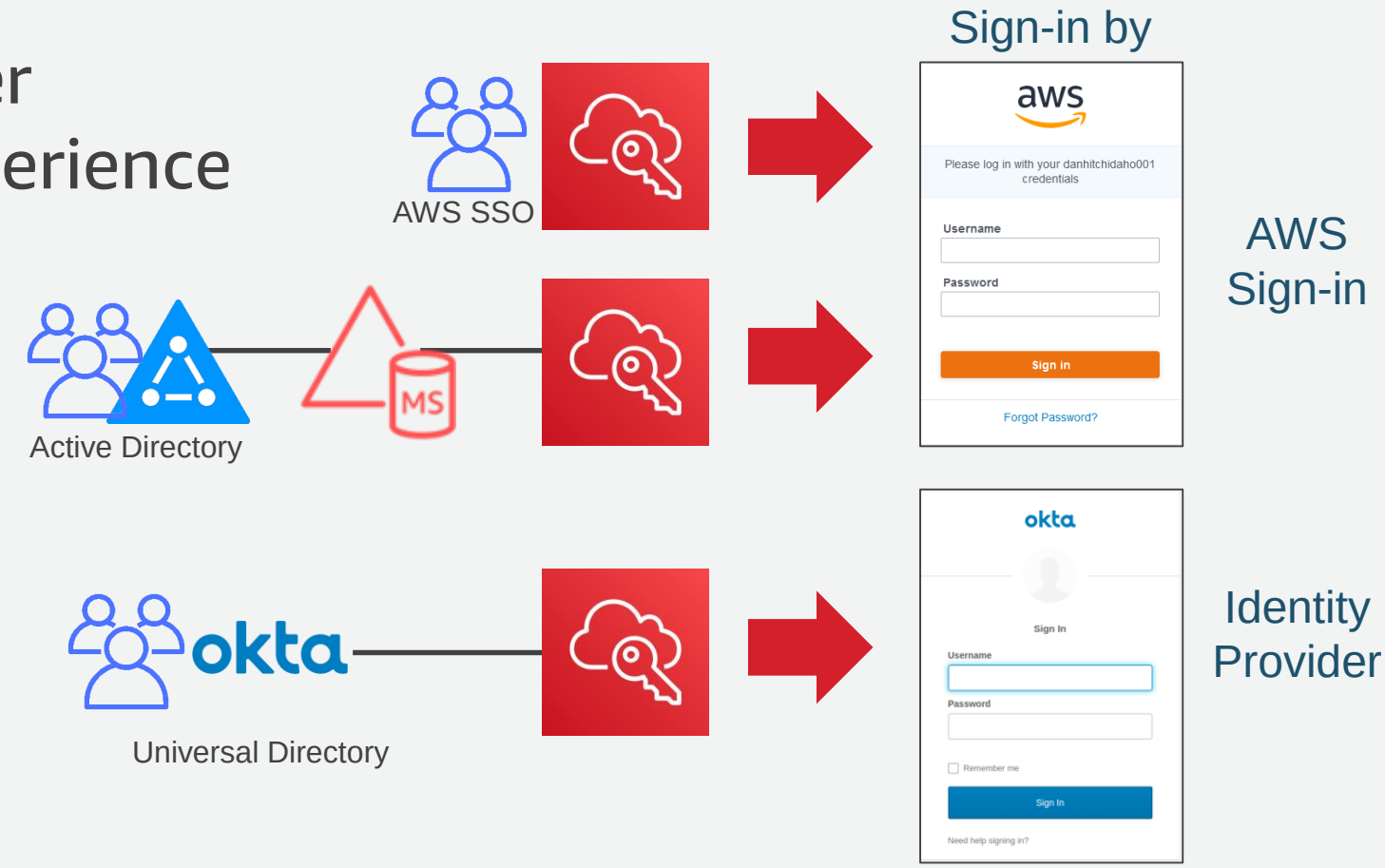




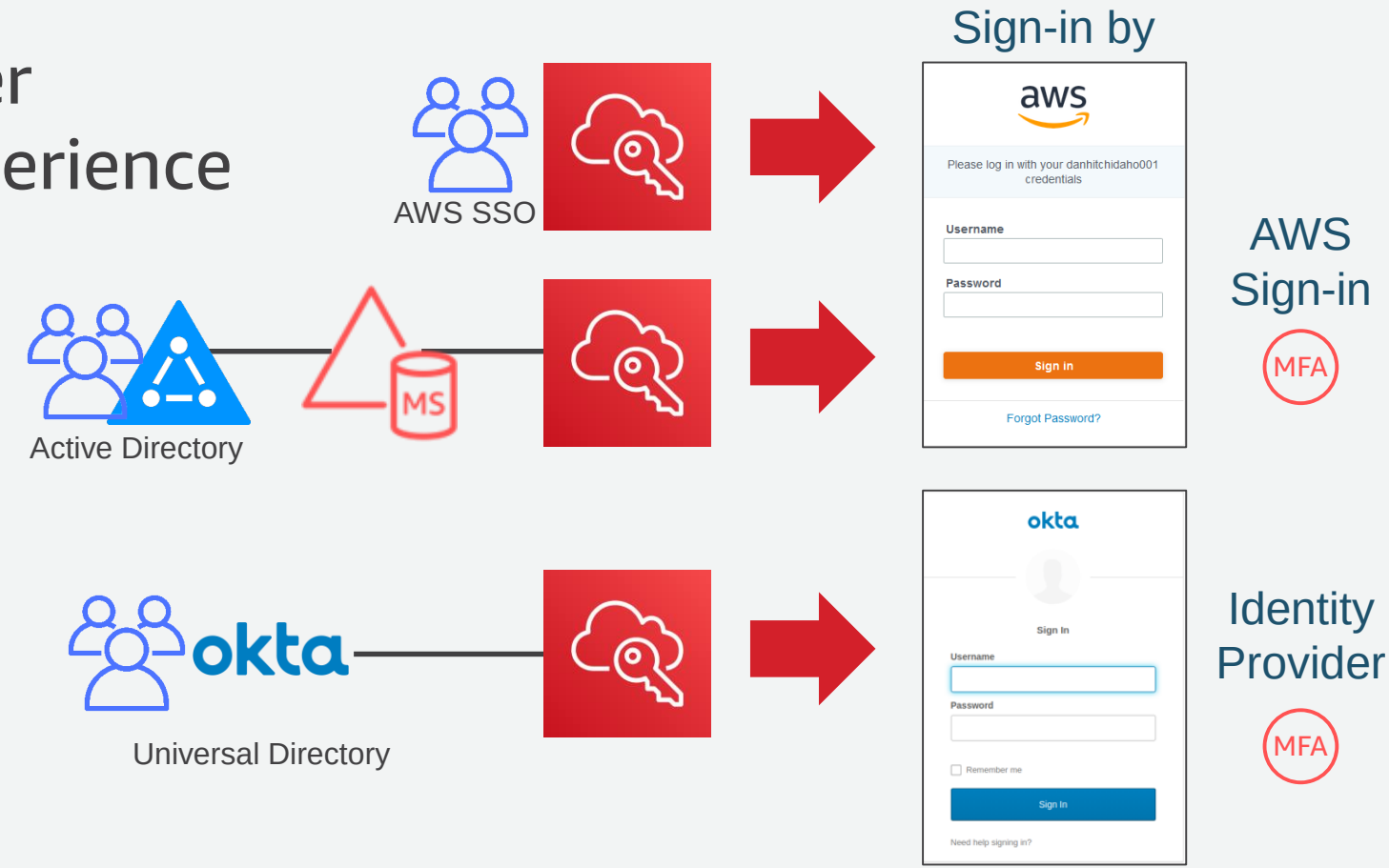
When using an existing identity provider (IdP)…



User experience



User experience

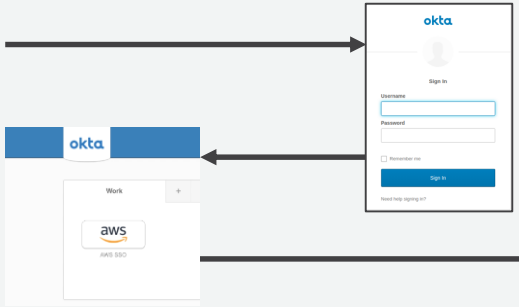


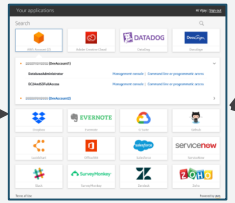
Sign-in flows: SP initiated

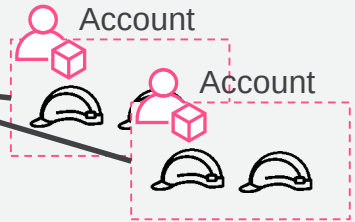
IdP

okta

SP

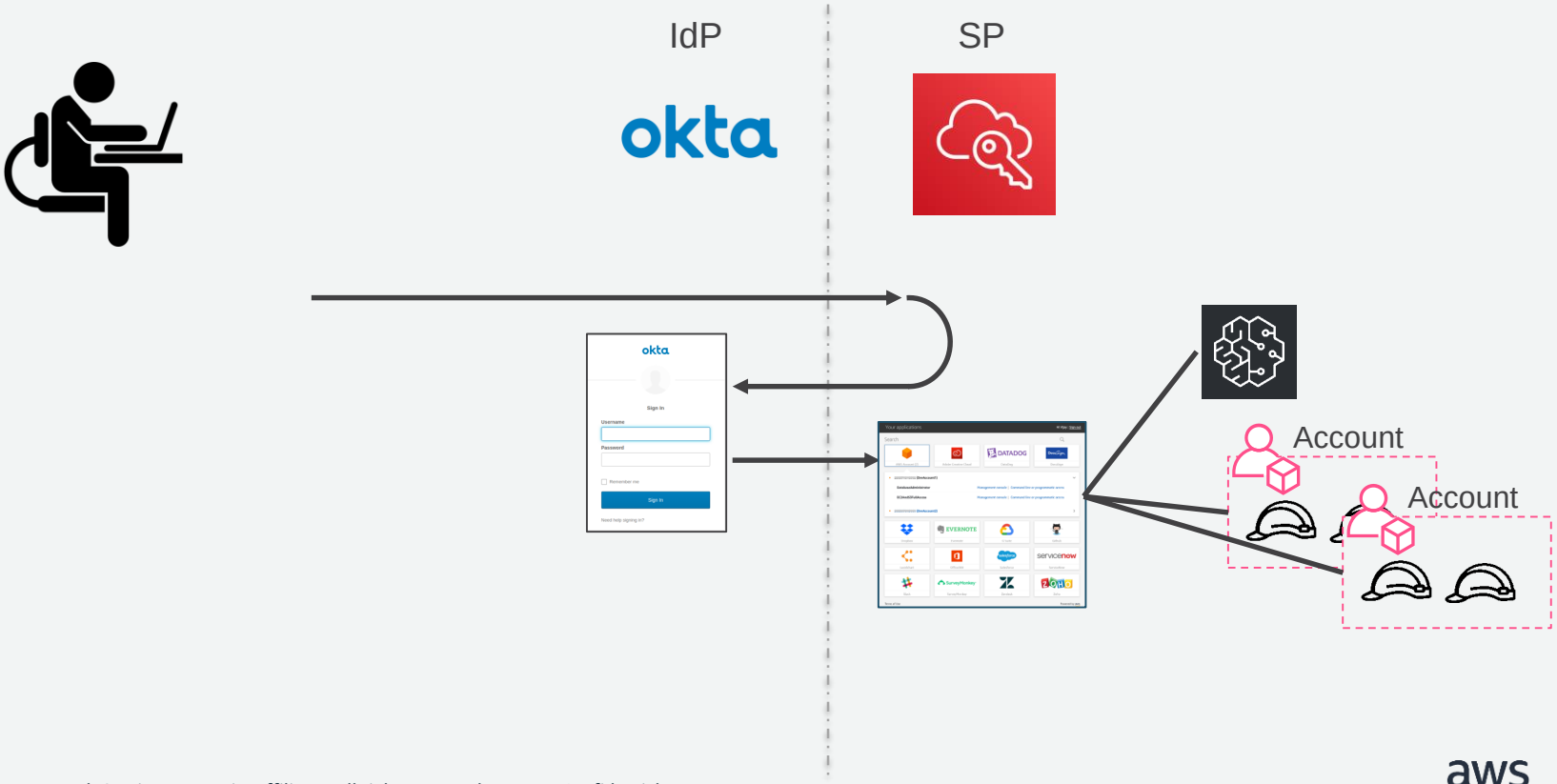




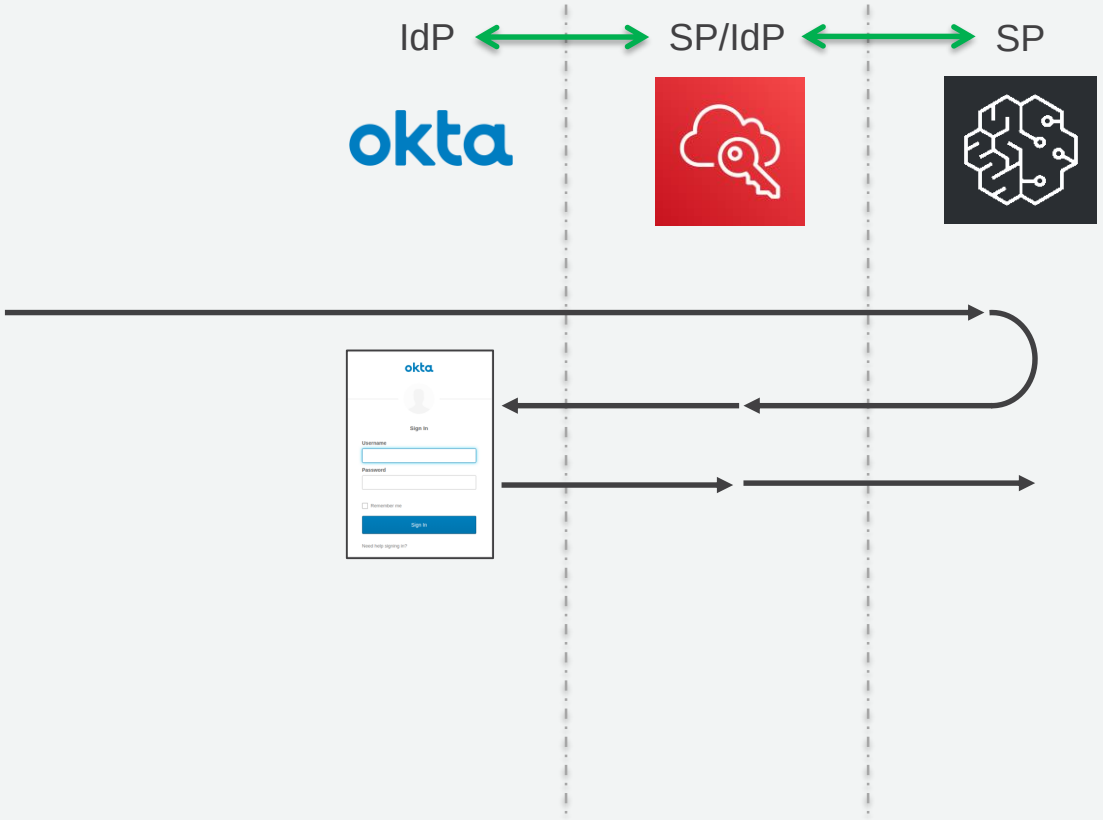


aws

Sign-in flows: SP initiated authentication



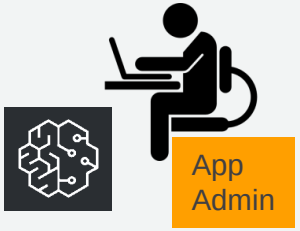
Sign-in flows: Chained SP initiated



aws

How AWS SSO works with identities to assign access

AWS SSO application access assignment



AWS SSO
Integrated
Applications

Office 365

salesforce

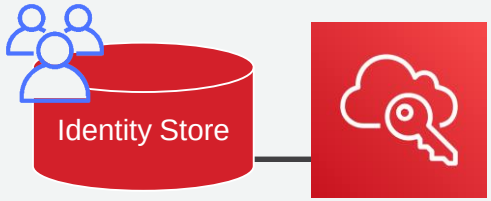
servicenow

SaaS
Applications

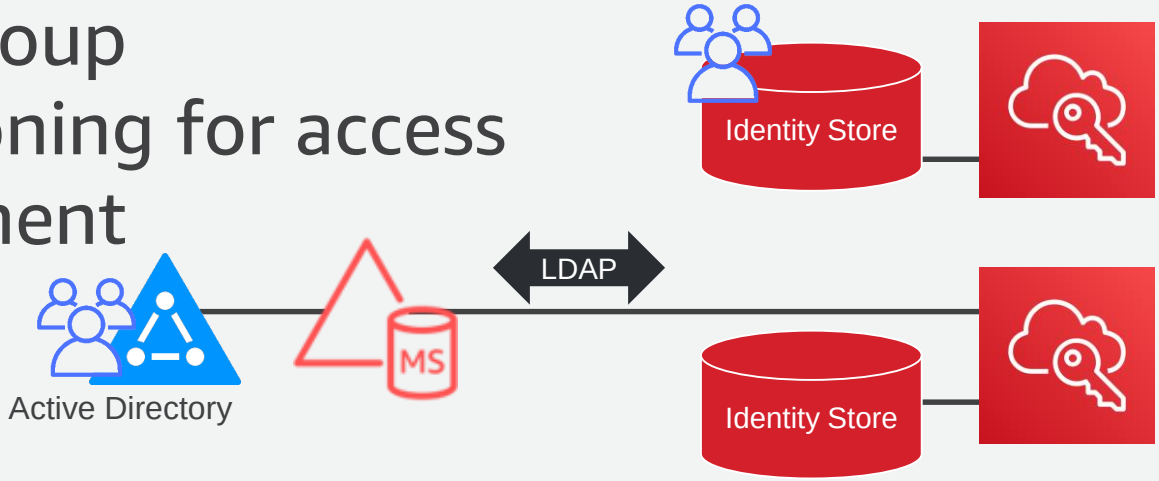
aws

AWS SSO permission set assignment

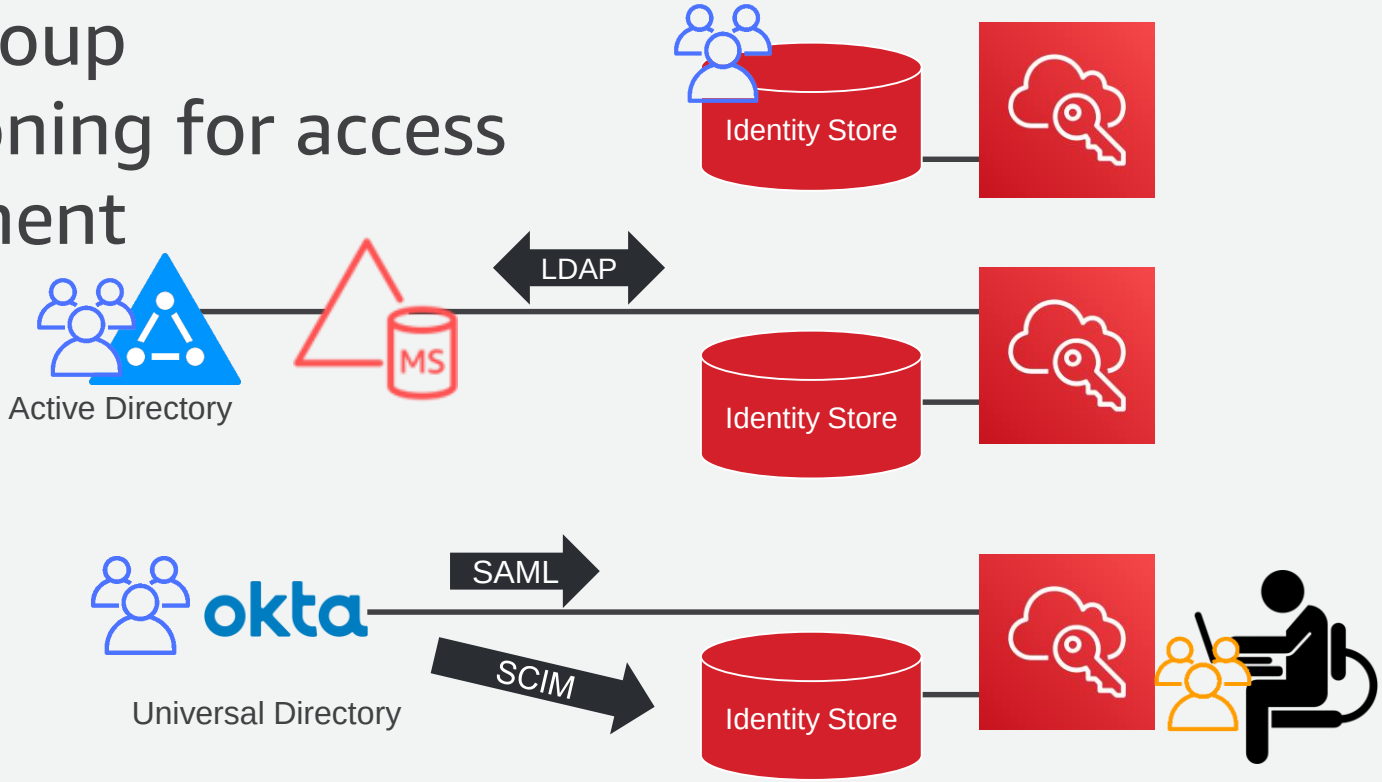
User/group provisioning for access assignment



User/group provisioning for access assignment

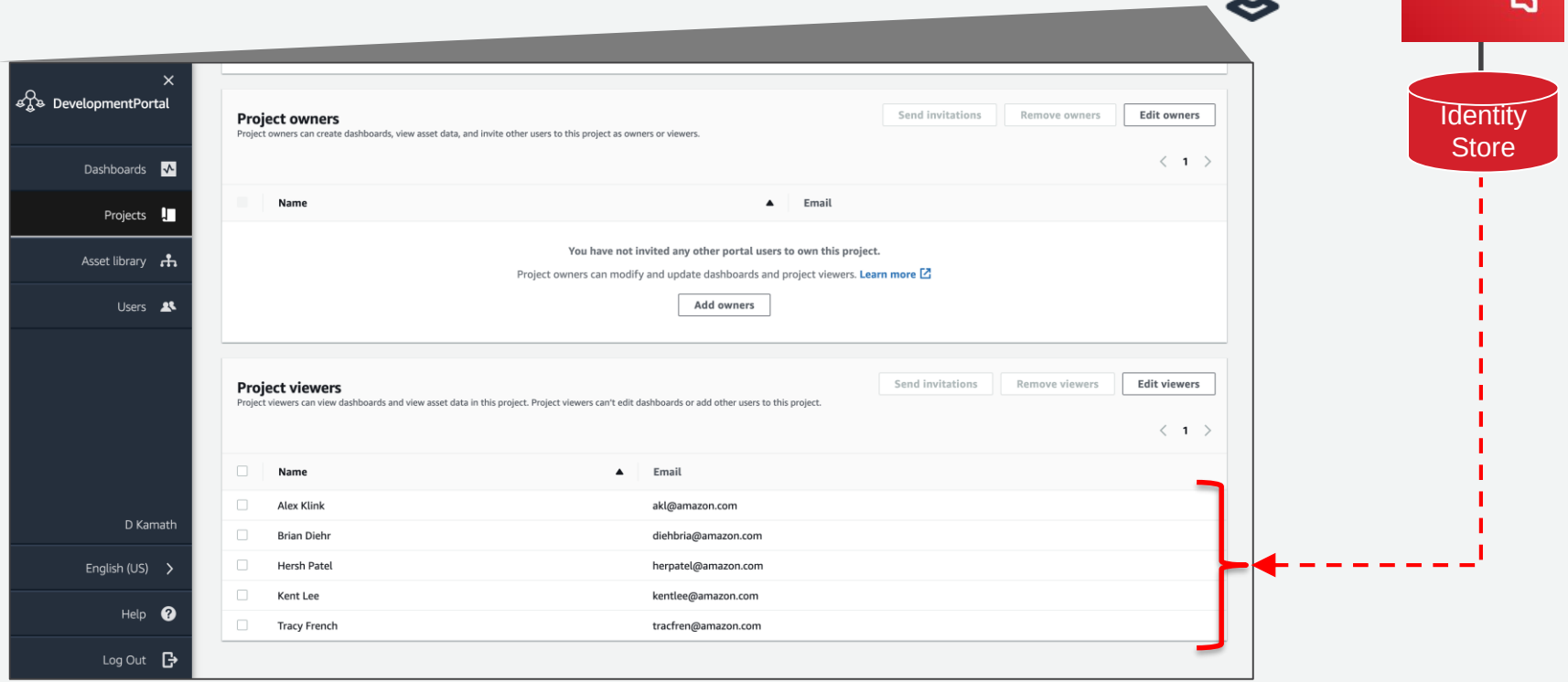


User/group provisioning for access assignment

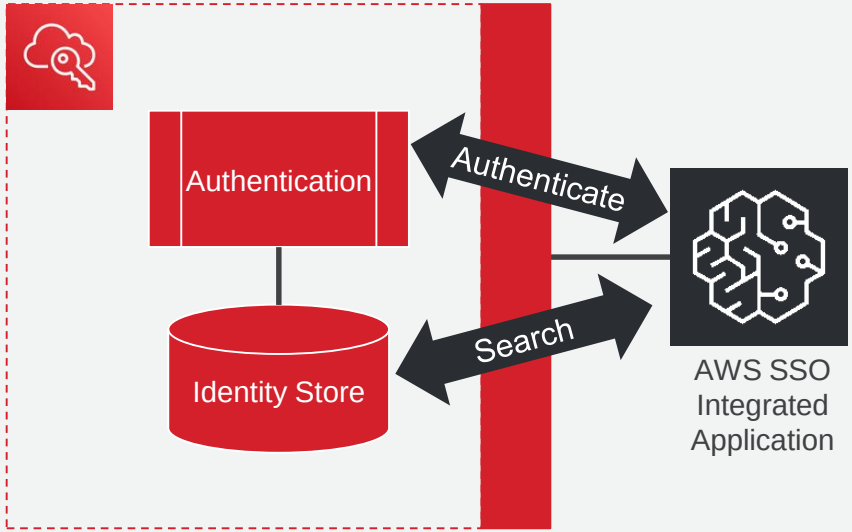


AWS SSO integrated applications

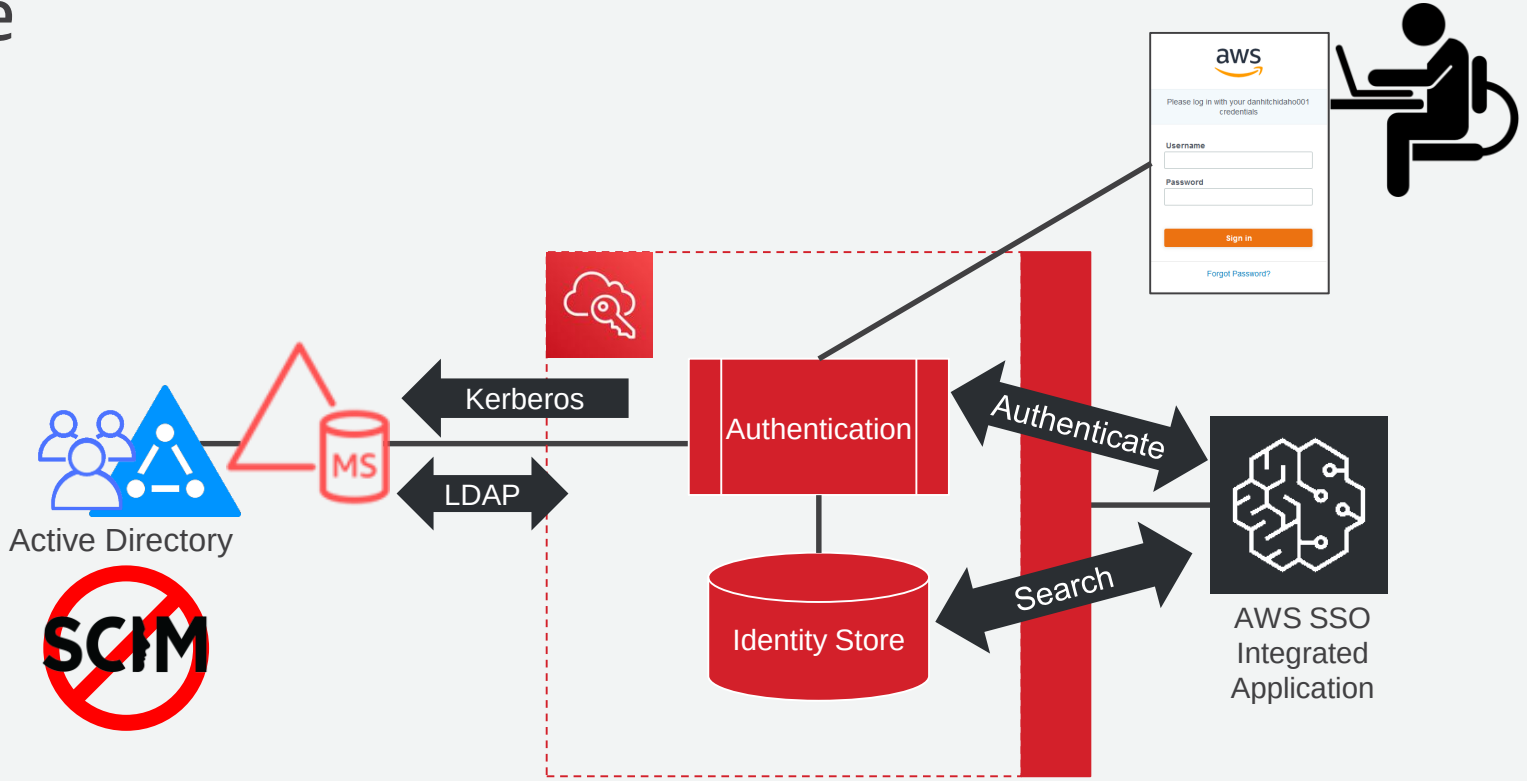
Example: AWS IoT SiteWise Monitor



User/group provisioning for application use



User/group provisioning for application use



AWS SSO Source of Truth Table

Identity source configuration	Authentication performed by	MFA control by	Users for assignment from	Users for application use from

AWS SSO Source of Truth Table

Identity source configuration	Authentication performed by	MFA control by	Users for assignment from	Users for application use from
AWS SSO	AWS SSO	AWS SSO	AWS SSO	AWS SSO

AWS SSO Source of Truth Table

Identity source configuration	Authentication performed by	MFA control by	Users for assignment from	Users for application use from
AWS SSO	AWS SSO	AWS SSO	AWS SSO	AWS SSO
Active Directory[1]	Active Directory	AWS SSO or AWS Directory Service	Active Directory (LDAP)	Active Directory (JIT)

[1] AWS SSO connects through AWS Directory Service for Microsoft AD or AD Connector

AWS SSO Source of Truth Table

Identity source configuration	Authentication performed by	MFA control by	Users for assignment from	Users for application use from
AWS SSO	AWS SSO	AWS SSO	AWS SSO	AWS SSO
Active Directory[1]	Active Directory	AWS SSO or AWS Directory Service	Active Directory (LDAP)	Active Directory (JIT)
IdP w/o SCIM	IdP	IdP	AWS SSO	AWS SSO

[1] AWS SSO connects through AWS Directory Service for Microsoft AD or AD Connector

AWS SSO Source of Truth Table

Identity source configuration	Authentication performed by	MFA control by	Users for assignment from	Users for application use from
AWS SSO	AWS SSO	AWS SSO	AWS SSO	AWS SSO
Active Directory[1]	Active Directory	AWS SSO or AWS Directory Service	Active Directory (LDAP)	Active Directory (JIT)
IdP w/o SCIM	IdP	IdP	AWS SSO	AWS SSO
IdP with SCIM	IdP	IdP	IdP	IdP

[1] AWS SSO connects through AWS Directory Service for Microsoft AD or AD Connector

aws

Demos

Recap

You can create users inside of AWS SSO or connect them from Active Directory or a SAML 2.0 IdP

When using Active Directory or a SAML IdP, AWS SSO always authenticates at the identity source

AWS SSO is source of truth for user meta data, groups, and group membership if you can edit them in AWS SSO

Active Directory uses a just-in-time sync-- AWS SSO integrated apps only see users after they have signed in at least once

Recap

When switching from AWS SSO to IdP users, AWS SSO preserves users, groups, and their assignments when user and group names match the IdP

We announced that Okta and AWS SSO now work together for SCIM synchronization and SAML authentication

Use case demos with AWS SSO users, Active Directory, and Okta users

To learn more and get started…

Learn more

- https://aws.amazon.com/single-sign-on
- https://aws.amazon.com/directoryservice
- https://www.okta.com/partners/aws

To get started

- Enable AWS SSO from the AWS Management Console
- Use the AWS Single Sign-on integration from the Okta App Catalog

Questions?