

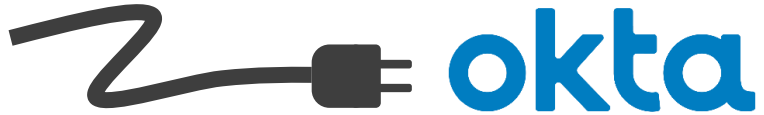


Using AWS Single Sign-On with Okta Active Directory, and AWS SSO identities

Ron Cully,
Principal Product Manager, AWS

Yuri Duchovny,
Solutions Architect, AWS

Thursday, May 28, 2020



Use Okta authentication and identities with AWS Single Sign-On!

<https://www.youtube.com/watch?v=XW5amgAuRlo>

How to Use Azure Active Directory with AWS SSO



Lior Pollack
Solutions Architect, AWS

Yuri Duchovny
Solutions Architect, AWS

February 25, 2020



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 ...



Deep Dive Working with Different Identity Sources in AWS Single Sign-On



Today...



User and group provisioning into AWS SSO

AWS SSO source of truth model

Purpose

Enable customers to...



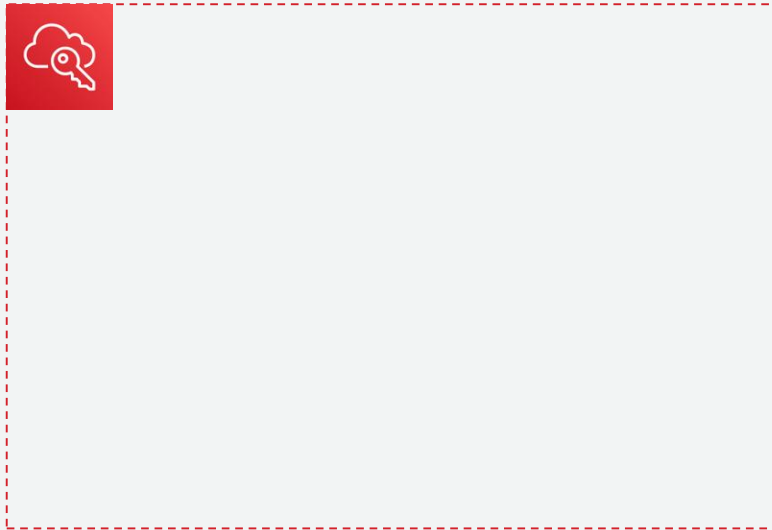
AWS SSO

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

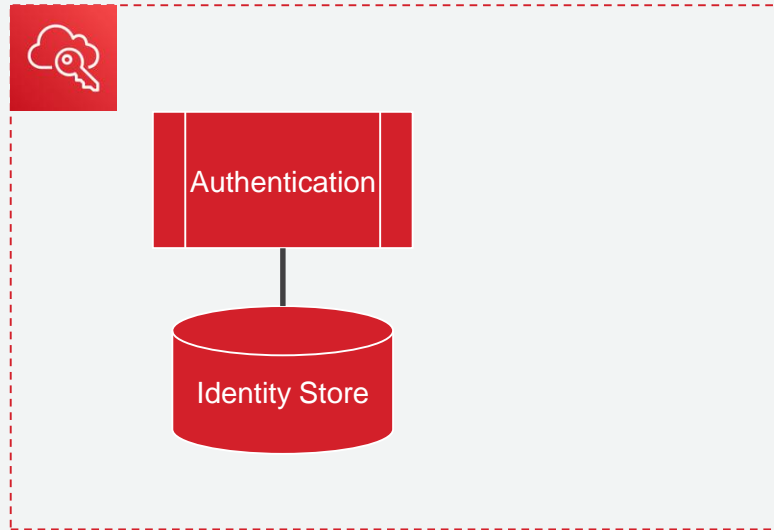
AWS SSO logical architecture



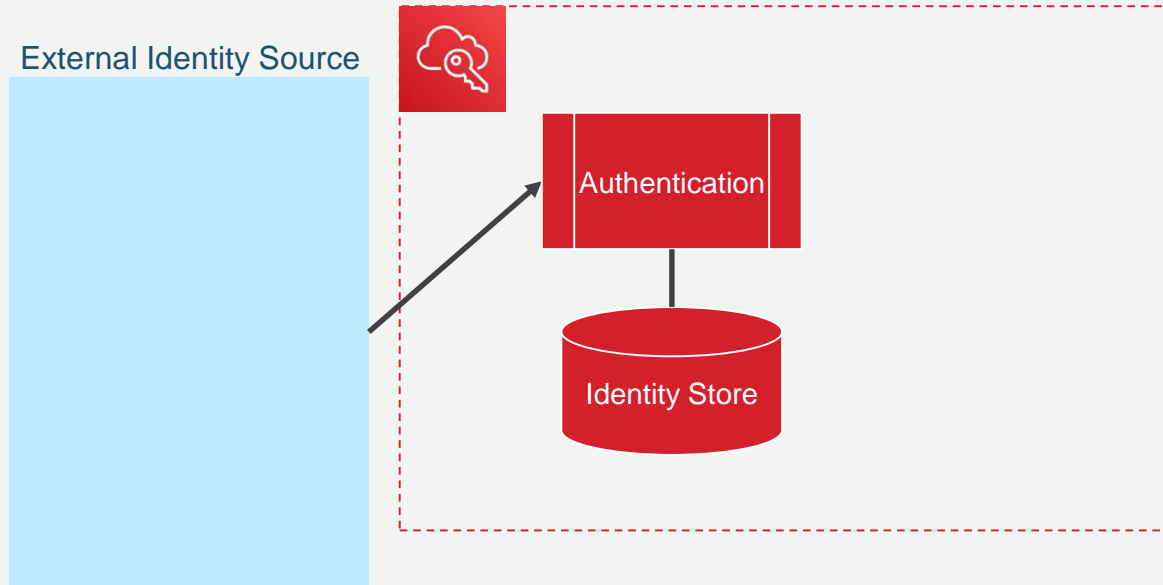
AWS SSO logical architecture



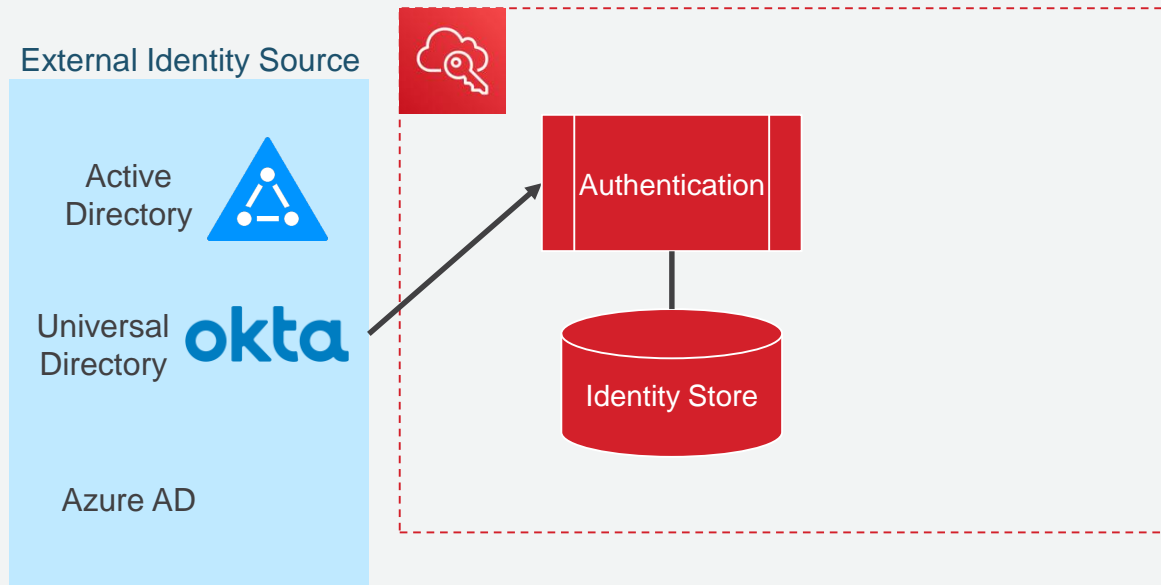
AWS SSO logical architecture



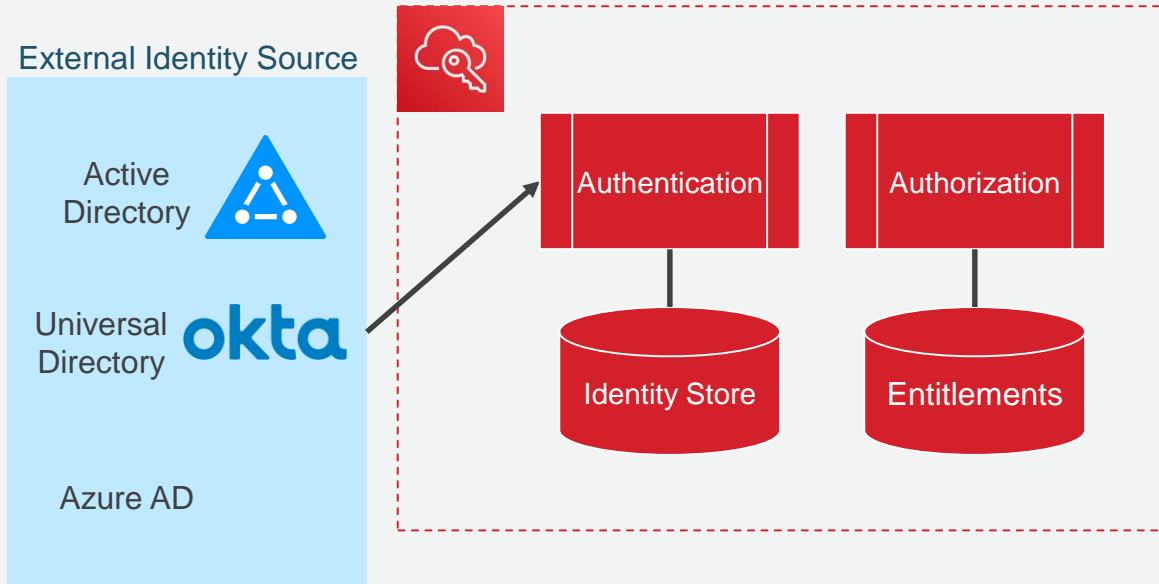
AWS SSO logical architecture



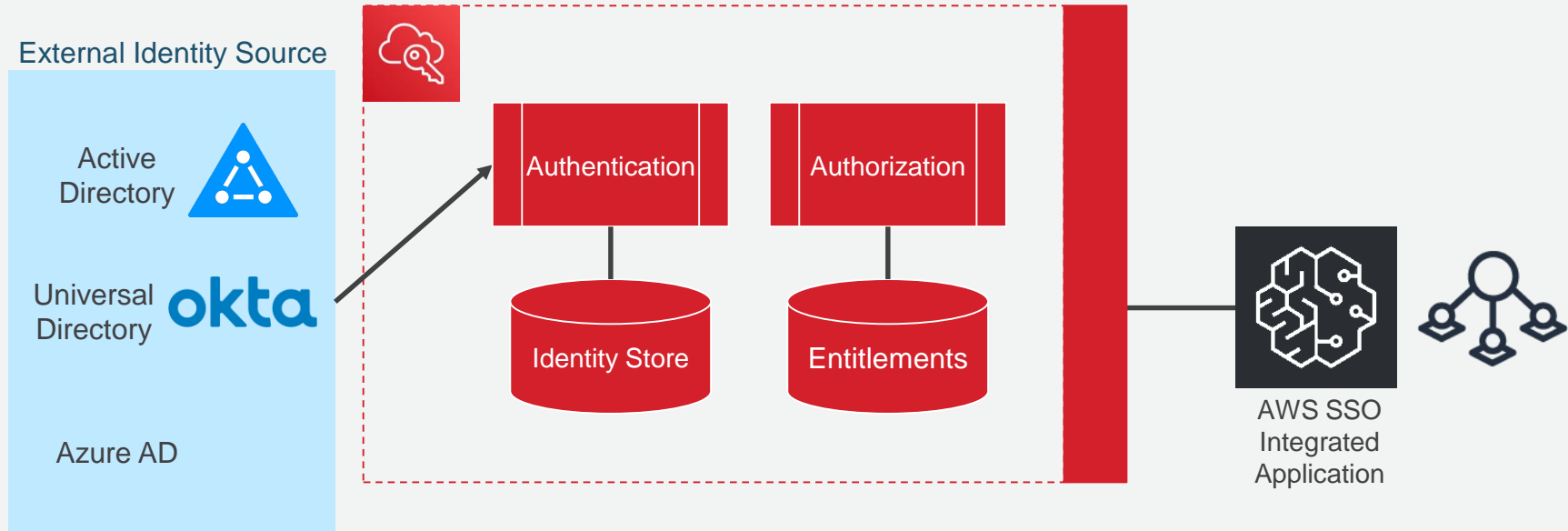
AWS SSO logical architecture



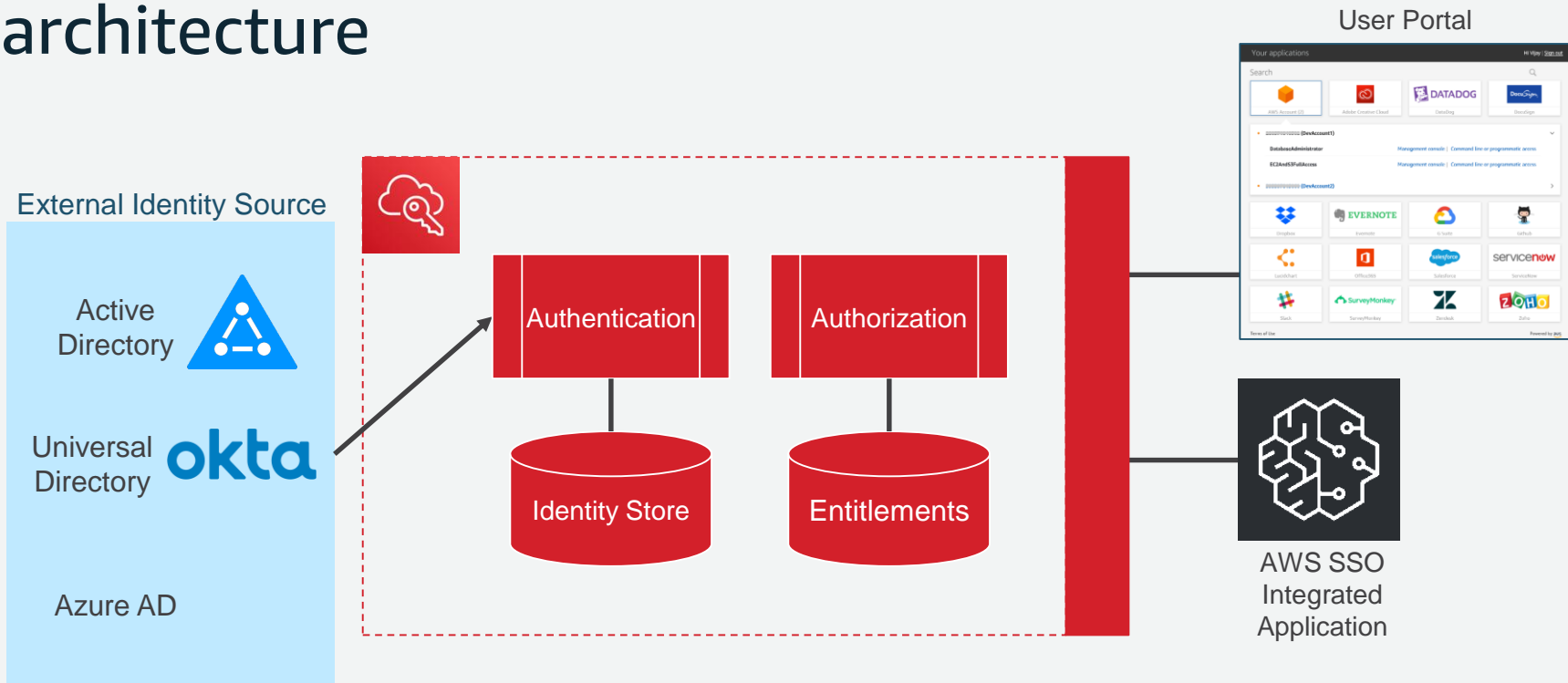
AWS SSO logical architecture



AWS SSO logical architecture

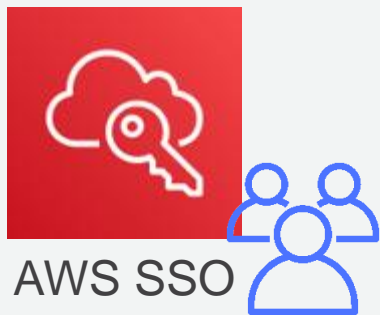


AWS SSO logical architecture



Where to manage and authenticate users

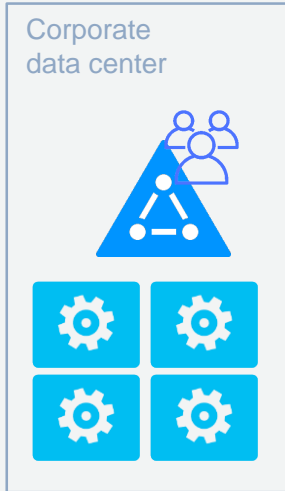
Manage users/groups in AWS SSO when...



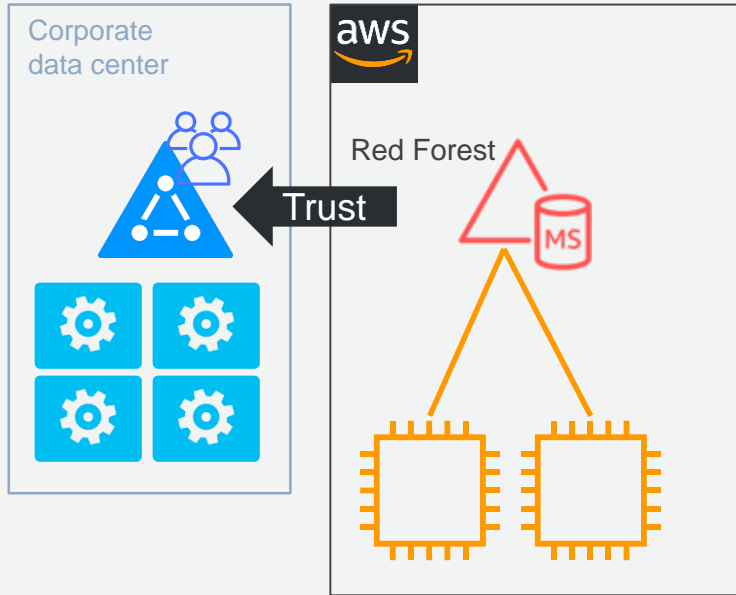
No existing identity system

Smaller scale user deployment

When migrating Active Directory workloads...

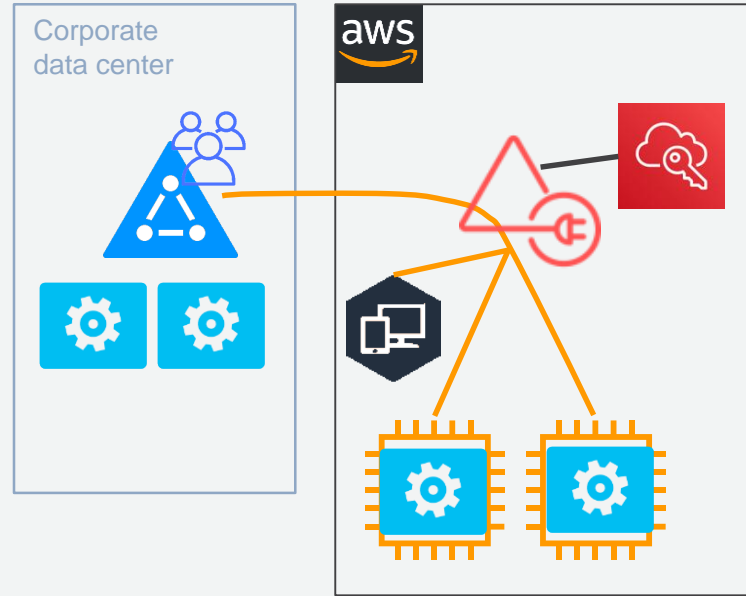
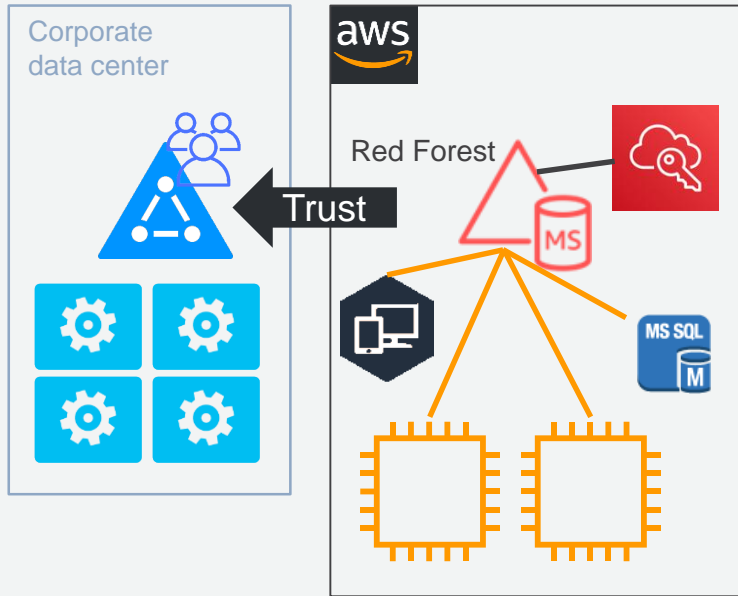


When migrating Active Directory workloads...

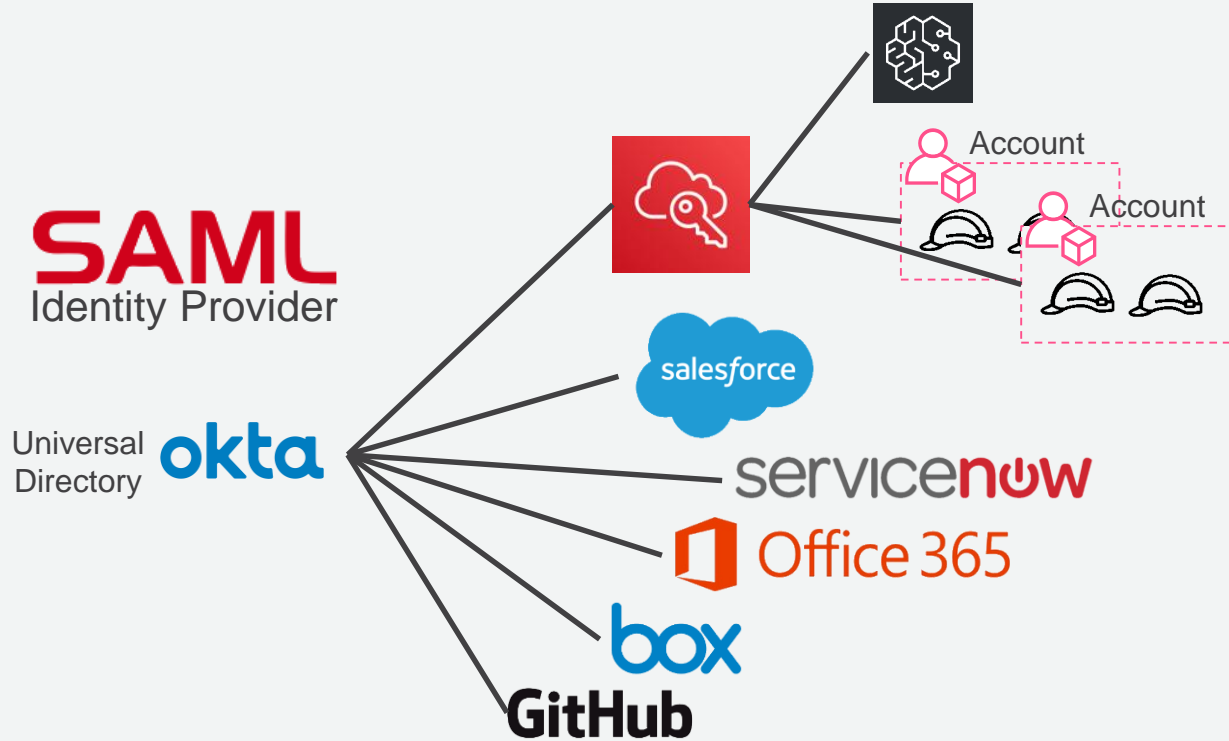


When migrating Active Directory workloads...

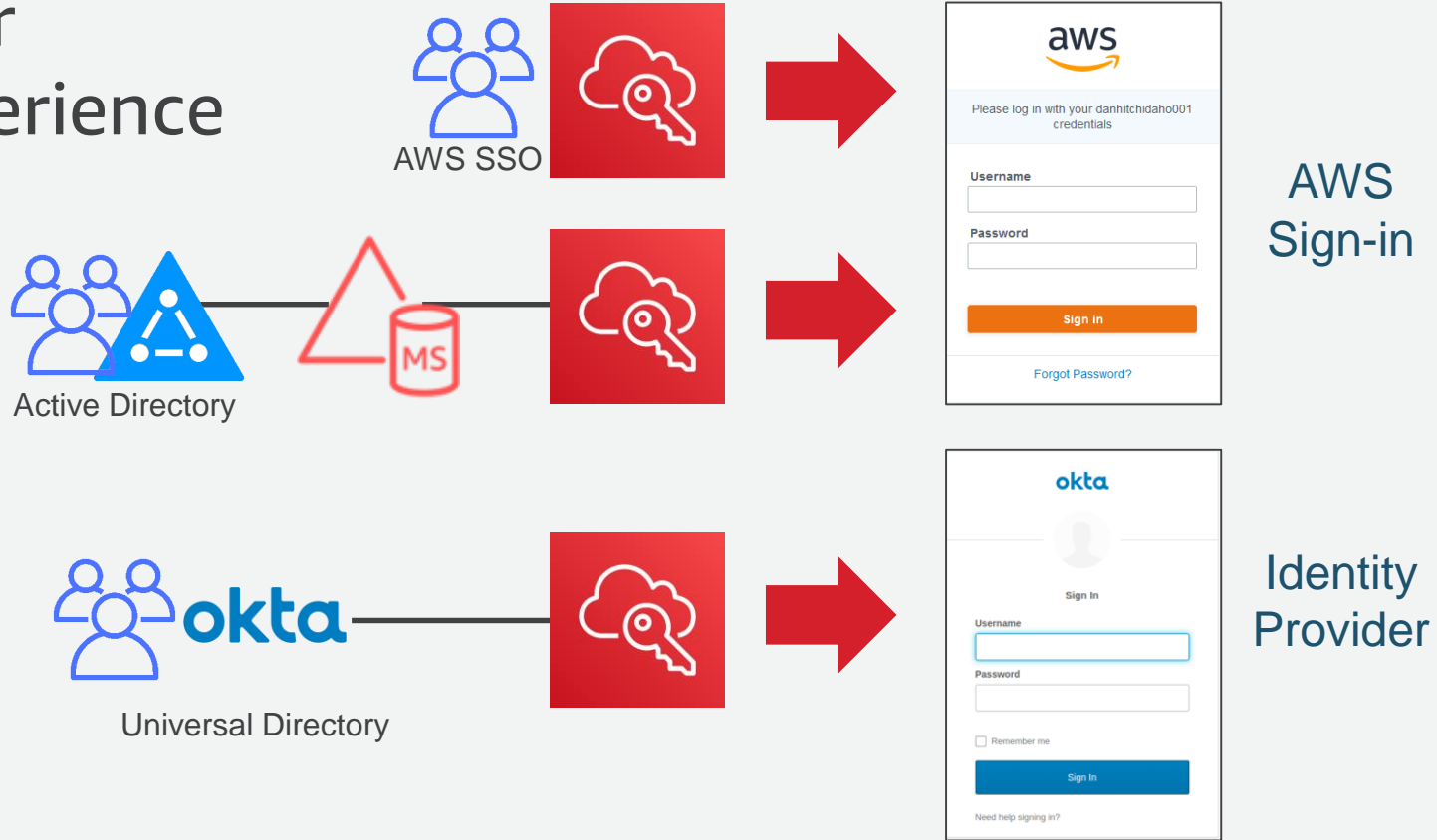
use Active Directory via AWS Directory Service for Microsoft AD or AD Connector



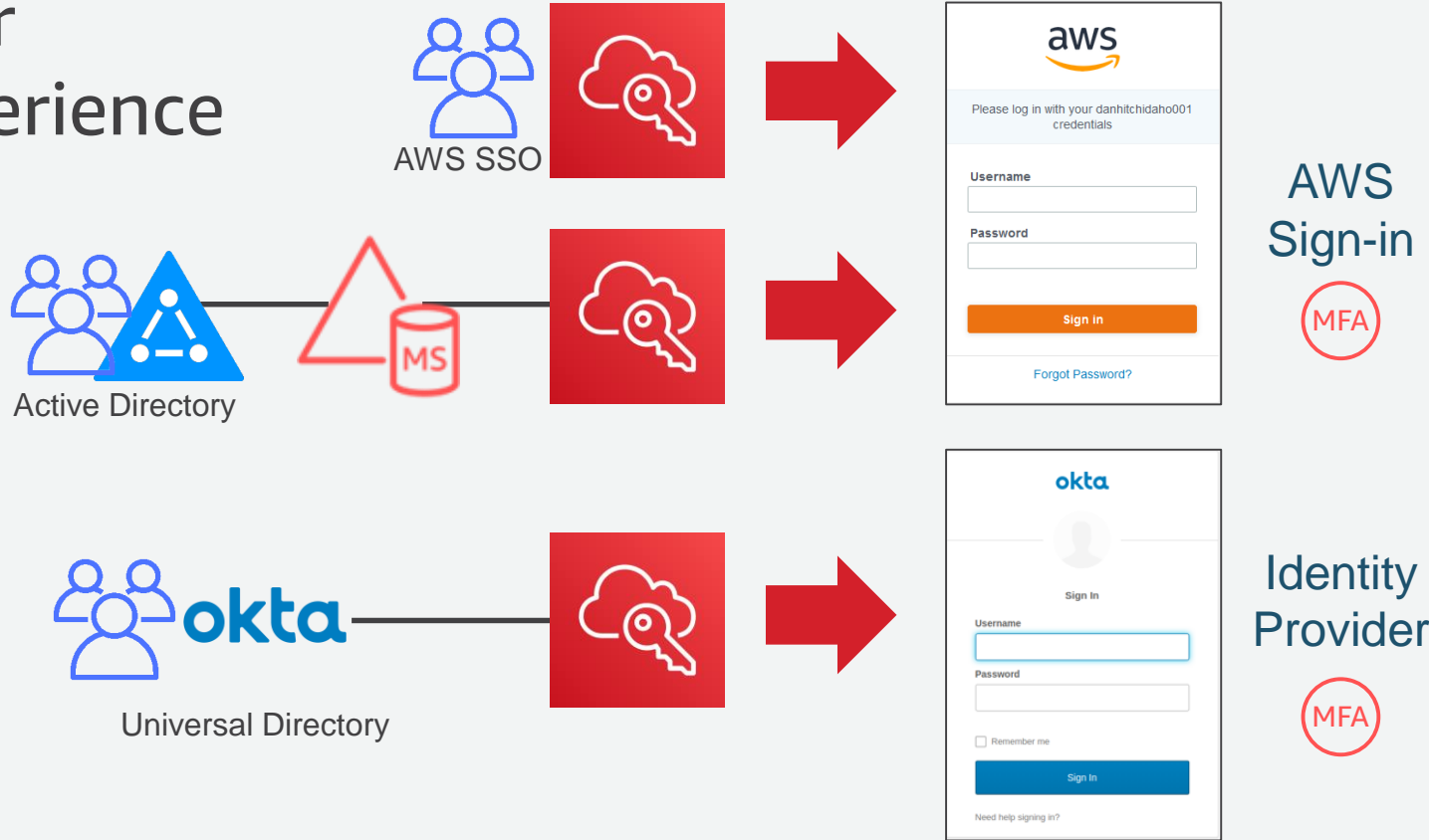
When using an existing identity provider (IdP)...



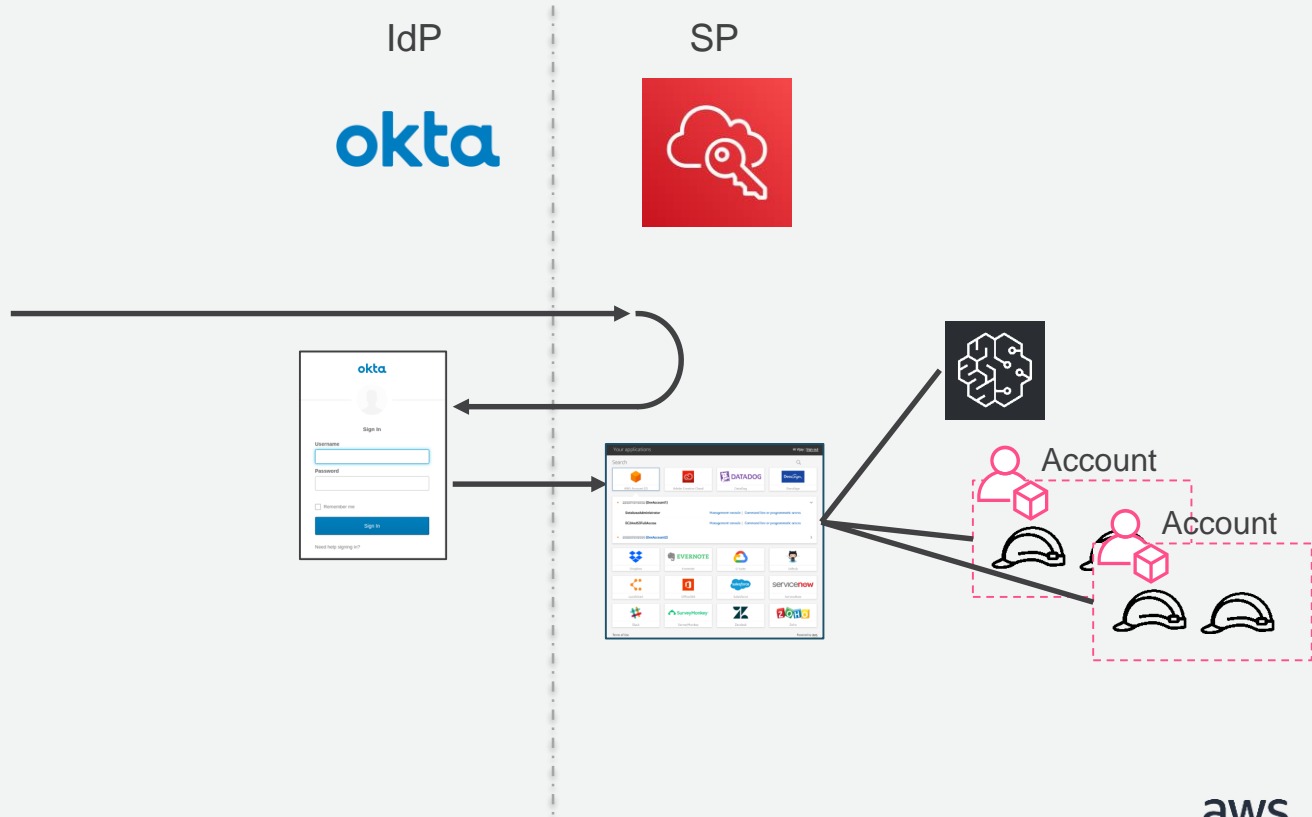
User experience



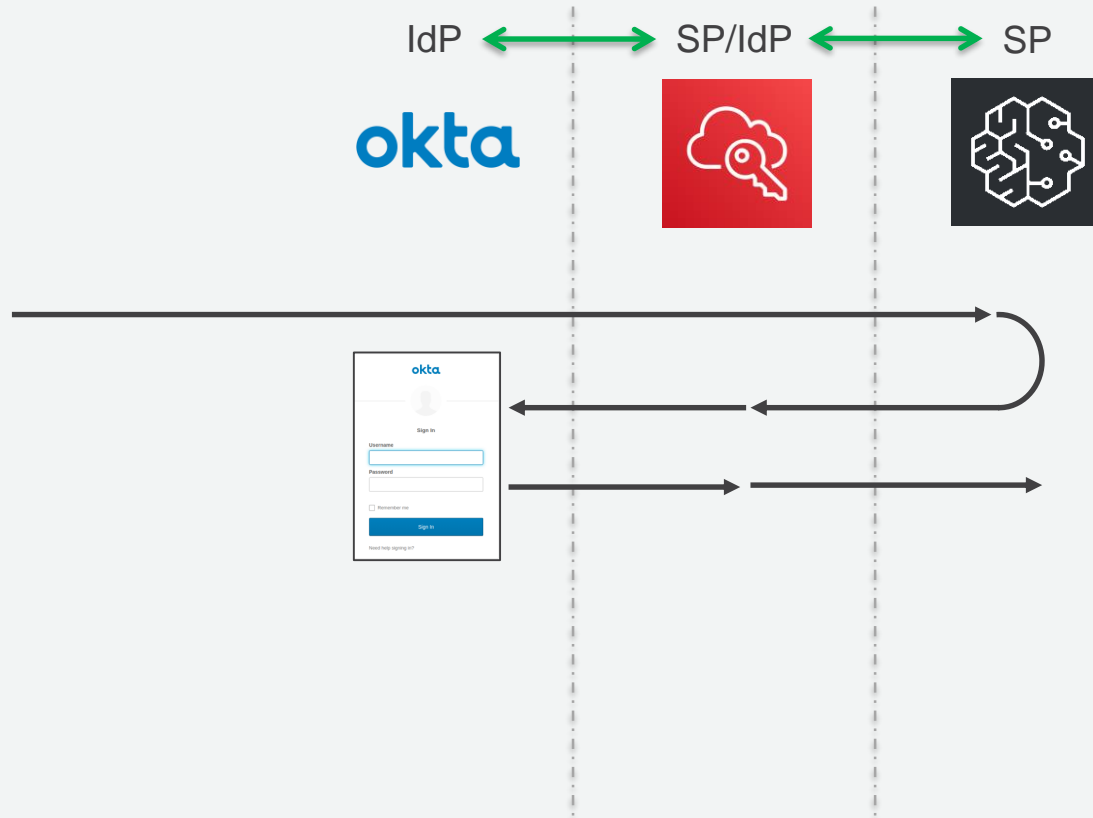
User experience



Sign-in flows: SP initiated authentication



Sign-in flows: Chained SP initiated

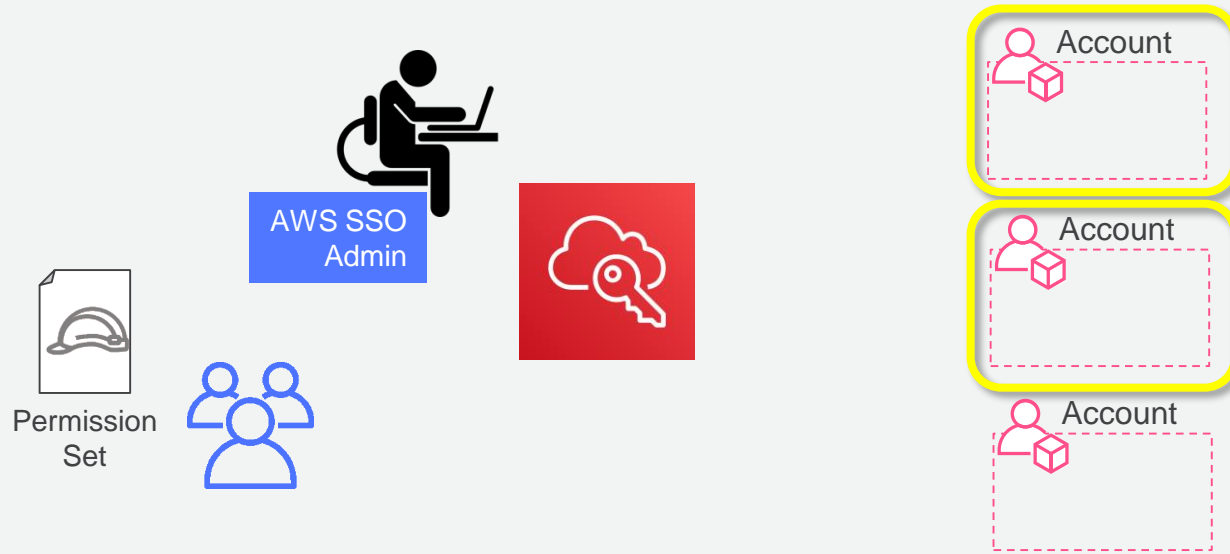


How AWS SSO works with identities to assign access

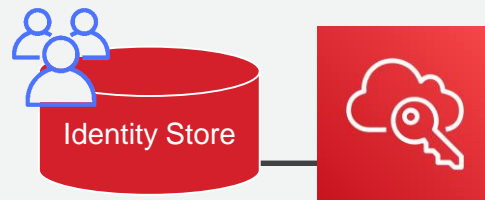
AWS SSO application access assignment



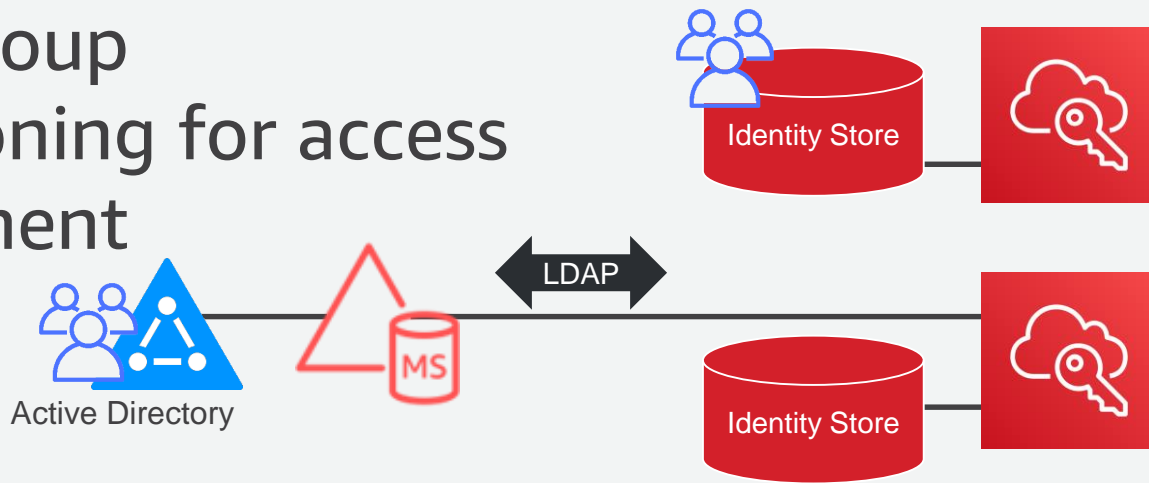
AWS SSO permission set assignment



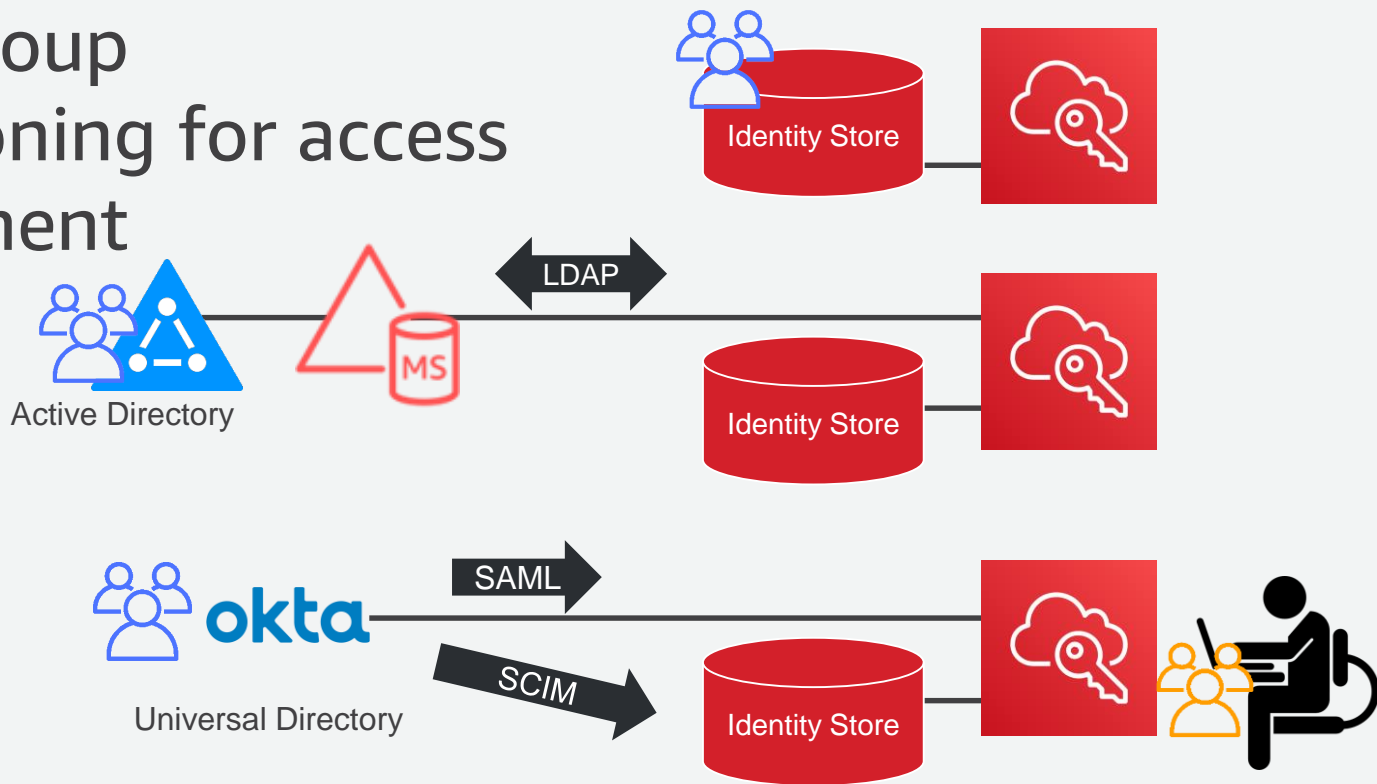
User/group provisioning for access assignment



User/group provisioning for access assignment



User/group provisioning for access assignment



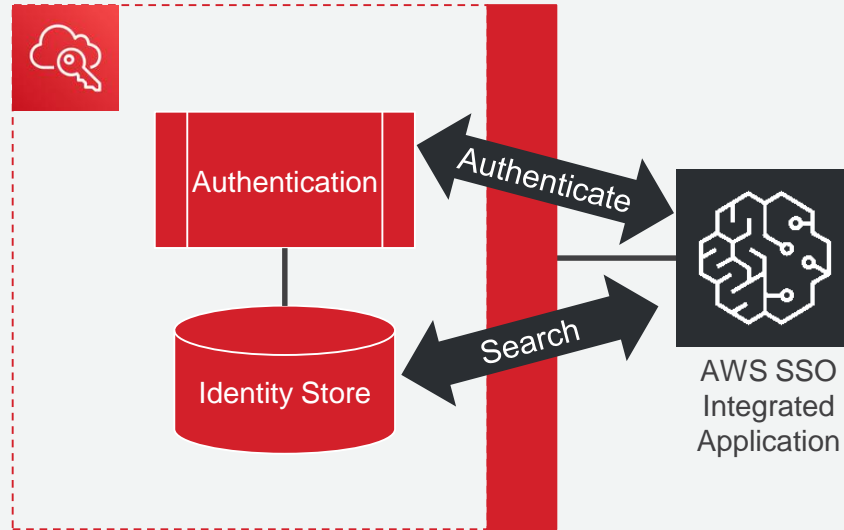
AWS SSO integrated applications

Example: AWS IoT SiteWise Monitor

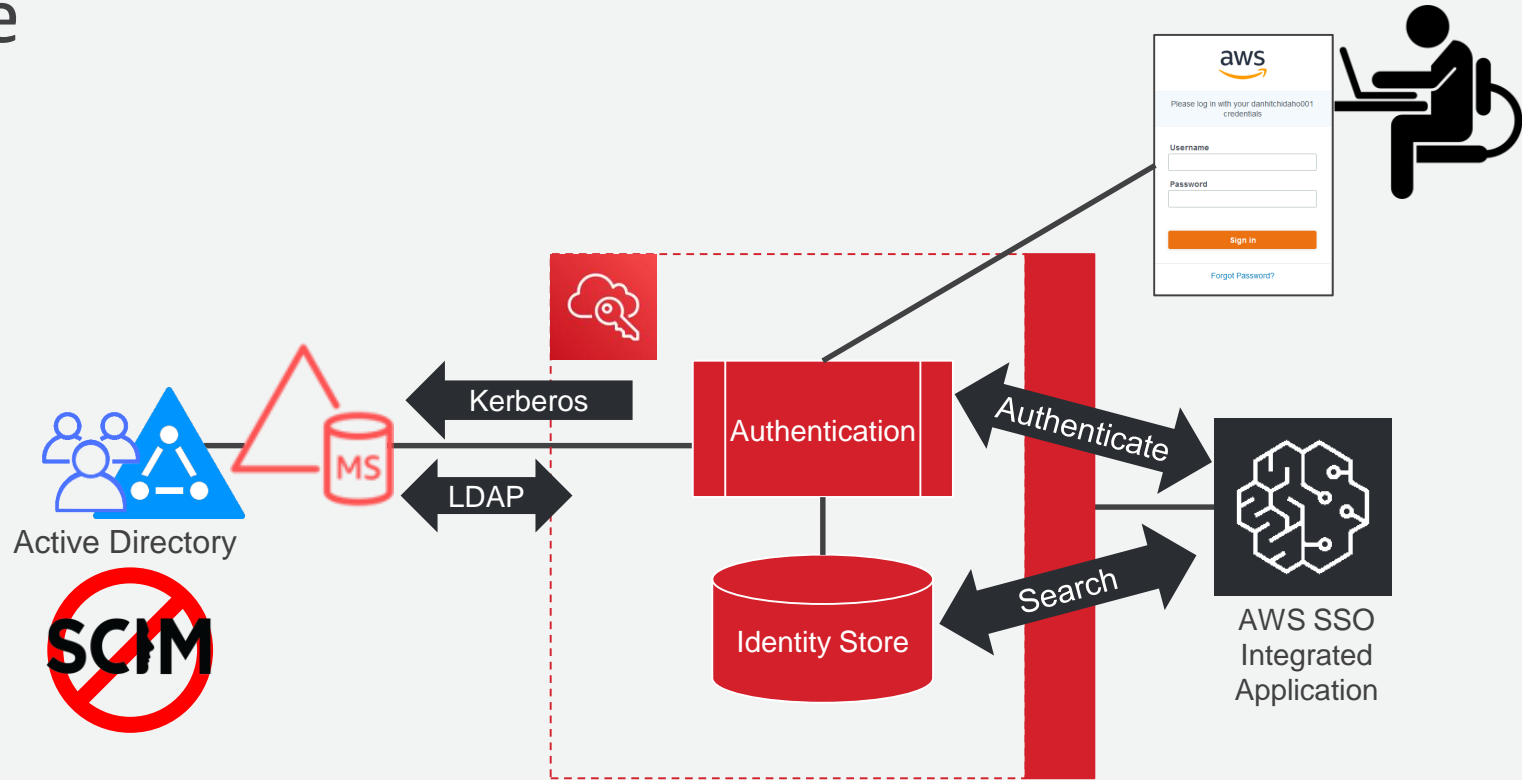
The screenshot displays the AWS SSO console interface for a project. The left sidebar contains navigation options: DevelopmentPortal, Dashboards, Projects, Asset library, Users, D Kamath, English (US), Help, and Log Out. The main content area is divided into two sections: 'Project owners' and 'Project viewers'. The 'Project owners' section includes buttons for 'Send invitations', 'Remove owners', and 'Edit owners', and a table with columns for 'Name' and 'Email'. Below this, a message states: 'You have not invited any other portal users to own this project. Project owners can modify and update dashboards and project viewers. [Learn more](#)'. An 'Add owners' button is also present. The 'Project viewers' section includes buttons for 'Send invitations', 'Remove viewers', and 'Edit viewers', and a table with columns for 'Name' and 'Email'. A red dashed arrow points from the 'Identity Store' icon in the top right to the 'Project viewers' table, indicating the integration of user data from the Identity Store into the application's user list.

<input type="checkbox"/>	Name	Email
<input type="checkbox"/>	Alex Klink	akl@amazon.com
<input type="checkbox"/>	Brian Diehr	diehbria@amazon.com
<input type="checkbox"/>	Hersh Patel	herpatel@amazon.com
<input type="checkbox"/>	Kent Lee	kentlee@amazon.com
<input type="checkbox"/>	Tracy French	tracfren@amazon.com

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

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?