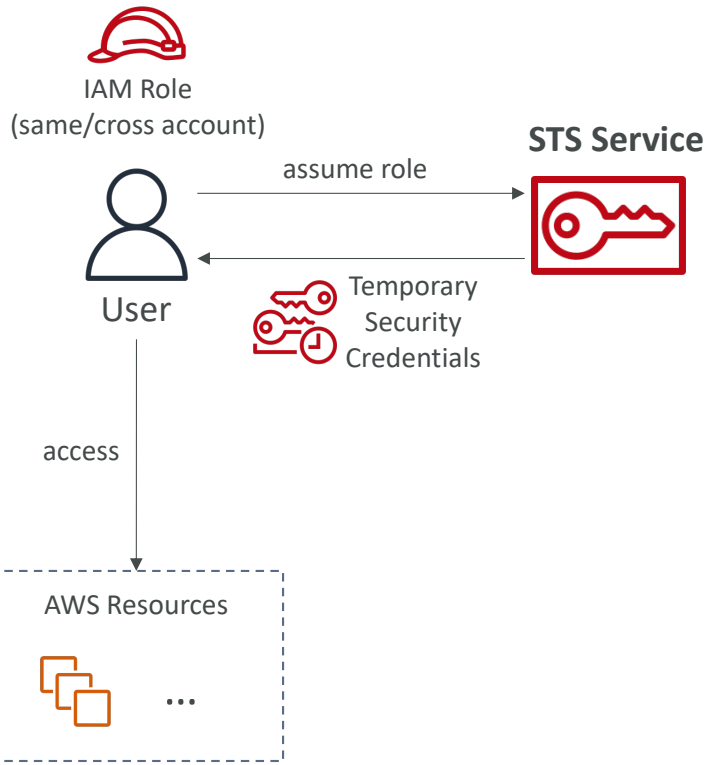
Advanced Identity Section

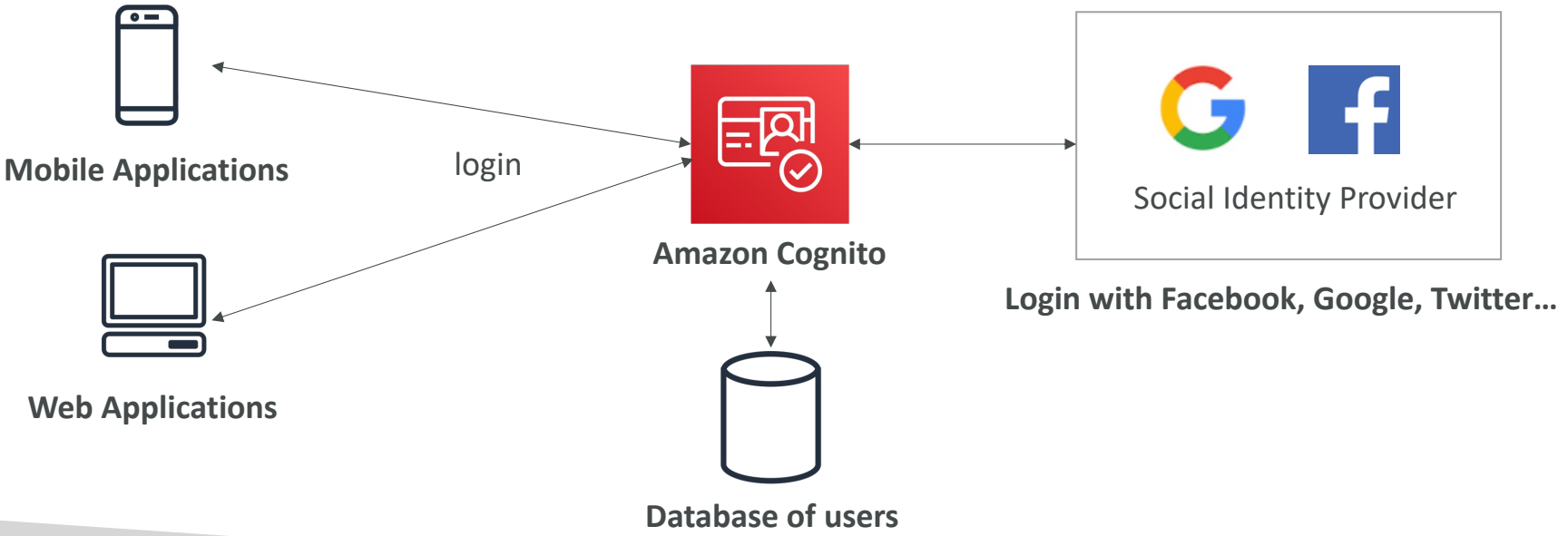
AWS STS (Security Token Service)

- Enables you to create **temporary, limited-privileges credentials** to access your AWS resources
- Short-term credentials: you configure expiration period
- Use cases
  - **Identity federation:** manage user identities in external systems, and provide them with STS tokens to access AWS resources
  - **IAM Roles for cross/same account access**
  - **IAM Roles for Amazon EC2:** provide temporary credentials for EC2 instances to access AWS resources



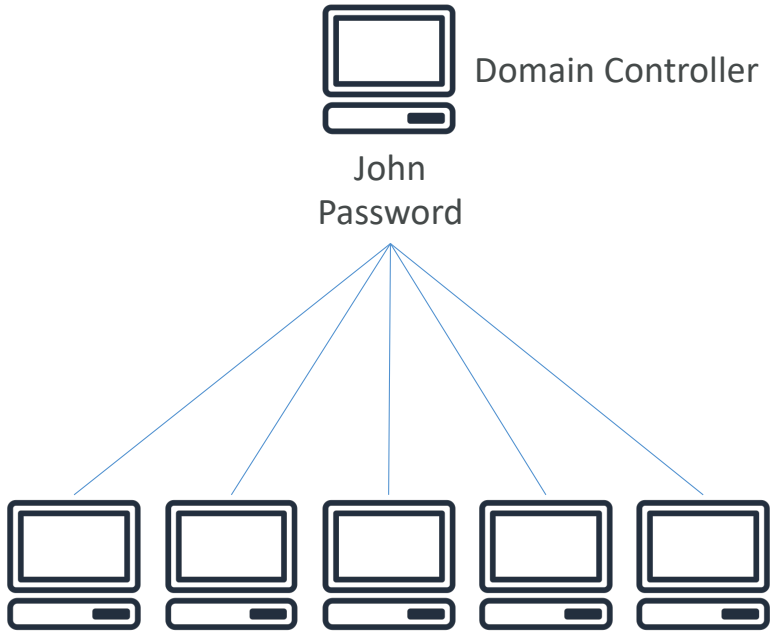
Amazon Cognito (simplified)

- Identity for your Web and Mobile applications users (potentially millions)
- Instead of creating them an IAM user, you create a user in Cognito



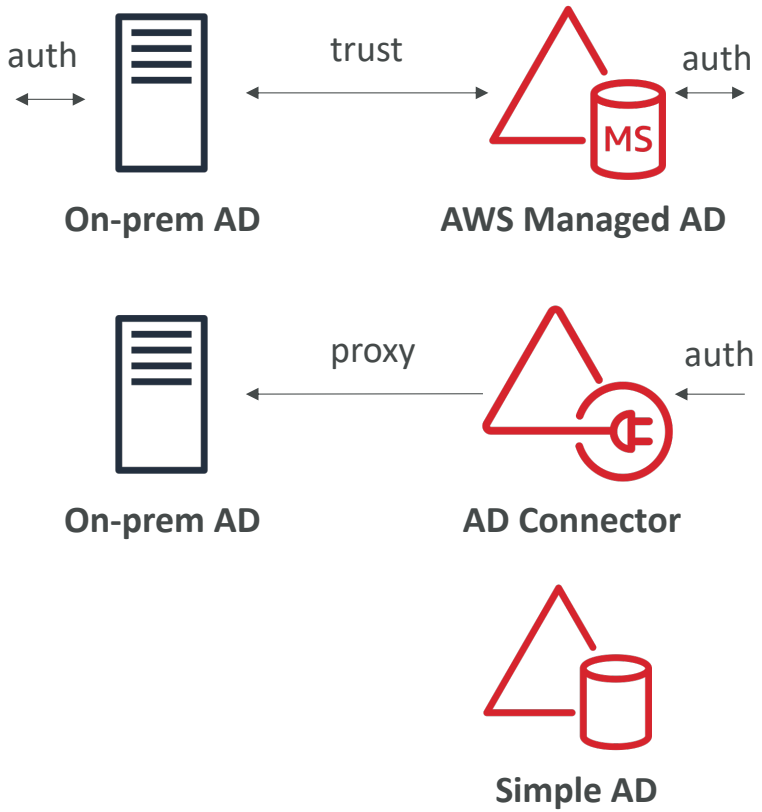
What is Microsoft Active Directory (AD)?

- Found on any Windows Server with AD Domain Services
- Database of **objects**: User Accounts, Computers, Printers, File Shares, Security Groups
- Centralized security management, create account, assign permissions



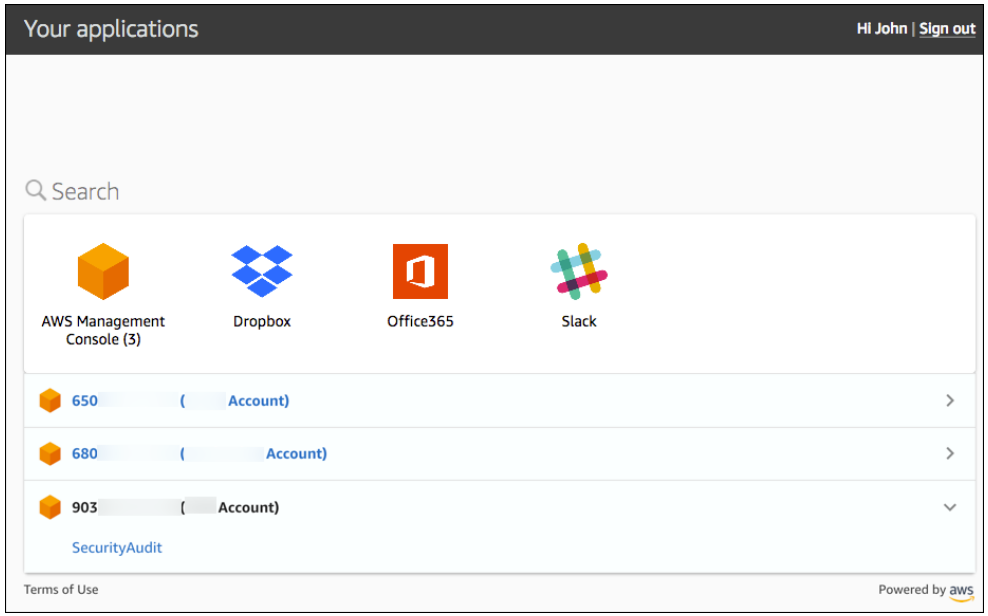
AWS Directory Services

- AWS Managed Microsoft AD
  - Create your own AD in AWS, manage users locally, supports MFA
  - Establish "trust" connections with your on-premise AD
- AD Connector
  - Directory Gateway (proxy) to redirect to on-premise AD, supports MFA
  - Users are managed on the on-premise AD
- Simple AD
  - AD-compatible managed directory on AWS
  - Cannot be joined with on-premise AD



AWS Single Sign-On (SSO)

- Centrally manage Single Sign-On to access **multiple accounts** and **3rd-party business applications.**
- Integrated with **AWS Organizations**
- **Supports SAML 2.0** markup
- Integration with on-premise **Active Directory**



https://aws.amazon.com/blogs/security/introducing-aws-single-sign-on/

AWS Single Sign-On (SSO) – Setup with AD

Advanced Identity - Summary

- IAM
  - Identity and Access Management inside your AWS account
  - For users that you trust and belong to your company
- **Organizations**: manage multiple AWS accounts
- **Security Token Service (STS):** temporary, limited-privileges credentials to access AWS resources
- **Cognito**: create a database of users for your mobile & web applications
- **Directory Services**: integrate Microsoft Active Directory in AWS
- **Single Sign-On (SSO):** one login for multiple AWS accounts & applications