Advanced Identity

AWS STS (Security Token Service)

- Provides temporary, limited-privilege credentials to access AWS resources
- Credentials have a configurable expiration period
- Use cases:
  - Identity federation: manage user identities in external systems, providing STS tokens for AWS resource access
  - IAM Roles for cross-account or same-account access
  - IAM Roles for EC2 instances: temporary credentials for EC2 to access AWS resources

Amazon Cognito

- Manages identity for web and mobile application users (potentially millions)
- Instead of creating IAM users, create users in Cognito

Microsoft Active Directory (AD)

- Available on any Windows Server with AD Domain Services
- Database of objects: user accounts, computers, printers, file shares, security groups
- Centralized security management, create accounts, assign permissions

AWS Directory Services

- **AWS Managed Microsoft AD**
  - Create and manage your own AD in AWS, supports MFA
  - Establish trust connections with 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 IAM Identity Center

- Single sign-on (SSO) for:
  - AWS accounts in AWS Organizations
  - Business cloud applications (e.g., Salesforce, Box, Microsoft 365)
  - SAML 2.0-enabled applications
  - EC2 Windows instances
- Identity providers:
  - Built-in identity store in IAM Identity Center

Summary

- **IAM**: Identity and Access Management within your AWS account for trusted users within your company
- **Organizations**: Manage multiple AWS accounts
- **Security Token Service (STS)**: Temporary, limited-privilege credentials for AWS resource access
- **Cognito**: Create a user database for mobile and web applications
- **Directory Services**: Integrate Microsoft Active Directory in AWS
- **IAM Identity Center**: Single login for multiple AWS accounts and applications