Reference Architecture for Identity and Access Management

Role Data Pattern Distribution in AWS
What we’ll cover

• How you can set up and use consistent user roles across *many* AWS Accounts

• Use your existing company identity store

• Deploy Multi-Factor Auth (MFA) as well
• Using Cloud can mean it is *harder* to do some of the same stuff

• Add ‘Cloud’... and the Security Question:
  • “Who is doing, or did what....” is simple to ask, but complex to answer

Why are we looking at this
• Our IAM team thought this was worth looking at
• Some Patents popped out
  • Sent the plaque to my mom
  • Solution components were developed that *could* solve the problem
    • Hadn’t really seen it deployed
• Using Ephemeral Users (AWS STS) and

• Knowing what a user did or can do is powerful.
  • (attribution / logging)

• Saves administration (creating IAM users in AWS)
  • Shows ‘who did what’ for Compliance/Security/Audit

• Decreases risk
In the meantime, lots of work was being done to

- Use a corporate identity Store (AD/Ping/Okta)
  - Use Multi-Factor Authentication
  - Log into an AWS Account and sub-account with an STS User
  - And log activity tied to the person who used it
Azure Enterprise App
SAML Integration

On premise
Active Directory
Azure
https://adfs.examplecloud.com
Azure Active Directory + Azure MFA
Azure AD Sync

Redirect
SAML / Identity provider integration

User
Login

AWS environment
https://console.aws.amazon.com
AWS ORG account
AWS Role

AWS Sub Account1
AWS Role
AWS Sub Account1
AWS Role

Bolted together it looks like this....
Establishing Azure AD Group to AWS Role Mapping

A little Pre-Config
Managing roles in an AWS Org Acct

Using StackSets to manage Sub-Account AWS Roles
Step 1: Logging into your Identity Store (O365 in this case)
Running AD Federation Services Takes you to this Screen

Step 2: Console Sign in
Here is your Multi-Factor Authentication Step

Step 3: MFA (Very Important)
First look at AWS Org-Level Account

Step 4: Into AWS!!!!!
Step 5: Switch Role to Sub-Account

Sub-Account Role Access
CloudTrail showing STS User, Azure-role and actions tied together
Cloudtrail showing Sub-Account User, Role and actions tied together
SAML response to get API Key

Consuming SAML Response from Azure AD, generating STS API Keys
CloudTrail log on API Key use

Audit Log on the API Key movement
Questions...