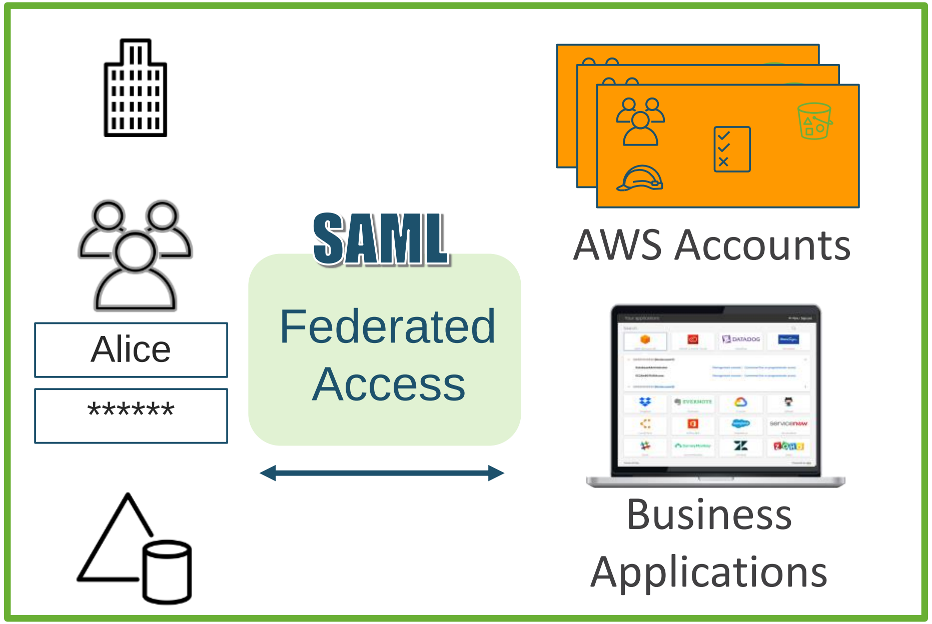
How to use your Azure Active Directory with AWS SSO

Lior Pollack
Solutions Architect, AWS

Yuri Duchovny
Solutions Architect, AWS

February 27th, 2020

Typical types of identities



Alice

******

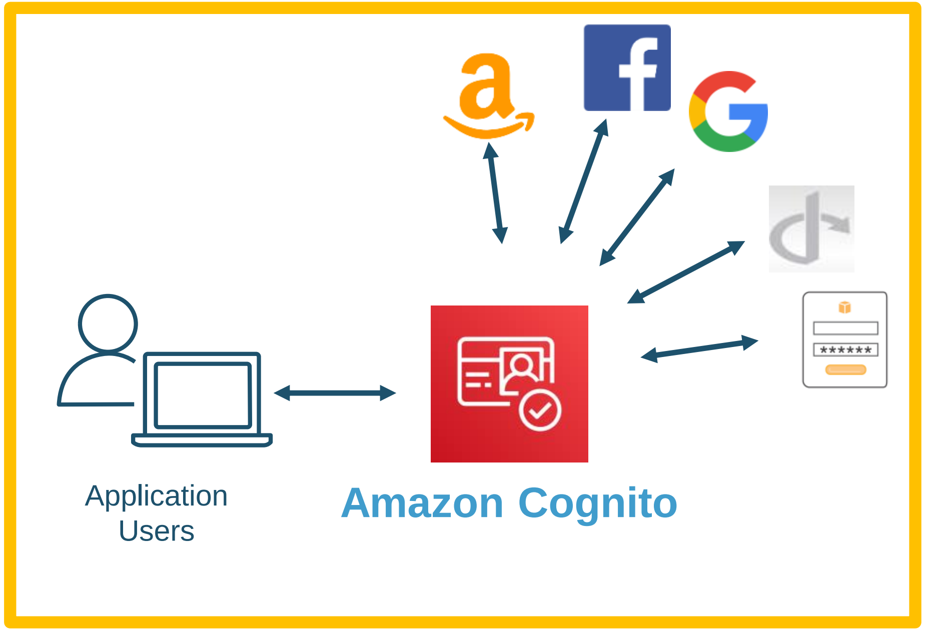
SAML

Federated Access

AWS Accounts

Business Applications

Workforce Identity



Application Users

Amazon Cognito

Application Identity

AWS Single Sign-On

Choose identity source

Manage access centrally

Increase CLI security, productivity

Browser and mobile portal access to accounts/roles/apps

SAML

Security Assertion Markup Language

SCIM

System for Cross-domain Identity Management

Agenda

AWS Identity and Access Management (IAM)

- ✓ overview
- ✓ federation with Azure AD

AWS Single Sign On (SSO)

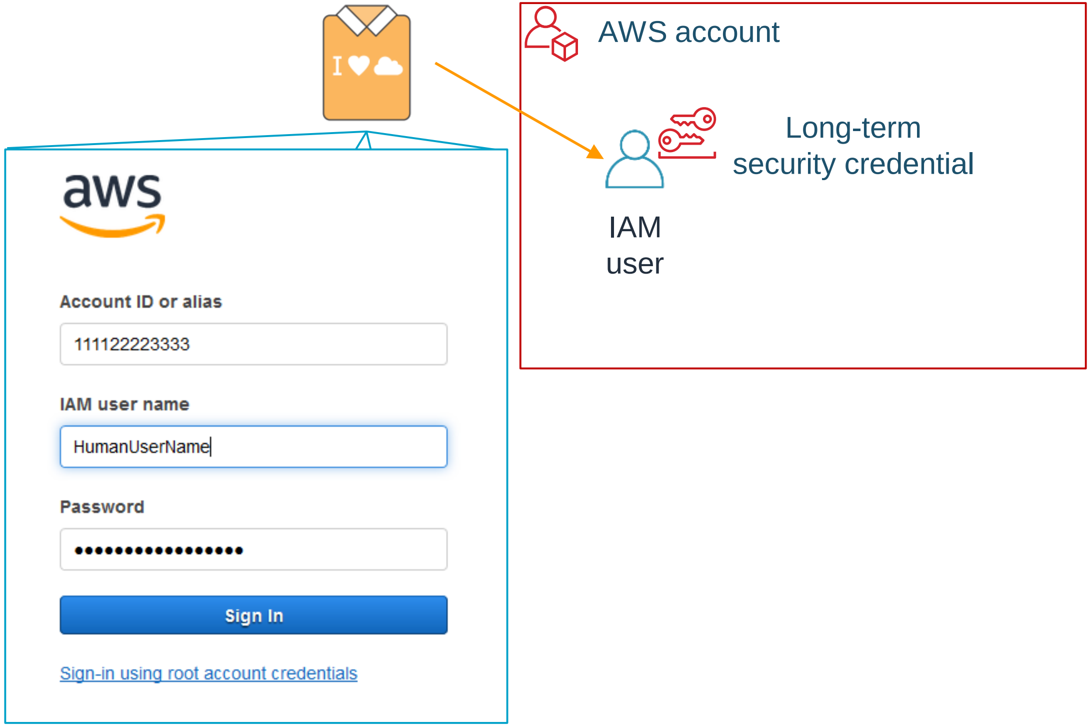
- ✓ multi-account access and governance
- ✓ simplifying multi-account access with existing Azure AD identities

AWS Identity and Access Management

AWS IAM

- **What it is**
  - I – Authentication: Support for human and application caller identities
  - AM – Authorization: Powerful, flexible permissions language for controlling access to cloud resources
- **Why it matters to you**: Every AWS service uses IAM to authenticate and authorize API calls

AWS identities for human callers: IAM users



Account ID or alias

111122223333

IAM user name

HumanUserName

Password

•••••••••••••••••

Sign In

Sign-in using root account credentials

AWS identities for non-human callers

Amazon EC2 instance

AWS Lambda function

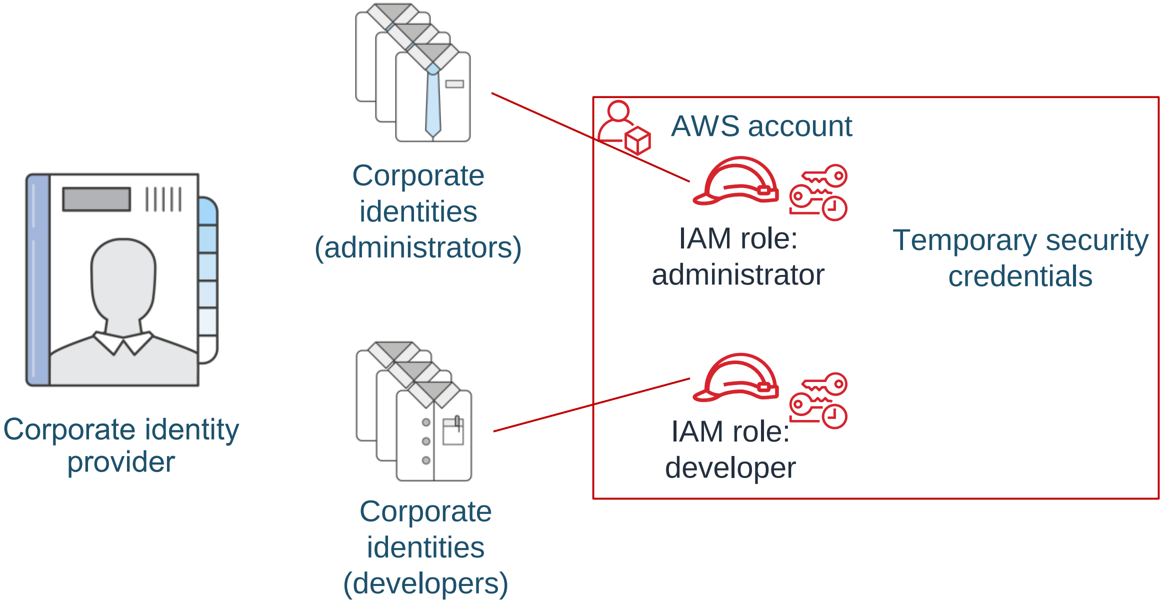
Amazon SageMaker notebook

AWS Glue crawler

Amazon ECS task

…and many others

AWS identities for human callers: Federated identities



Corporate identity provider

Corporate identities (administrators)

Corporate identities (developers)

AWS account

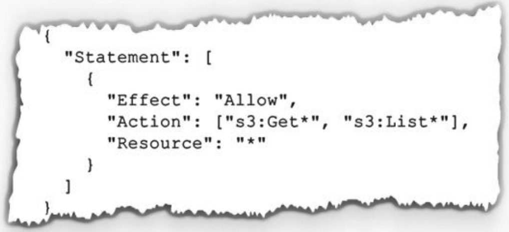
IAM role: administrator

IAM role: developer

Temporary security credentials

What are IAM policies?

Policies provide authorization to AWS services and resources



```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:Get*", "s3:List*"],
      "Resource": "*"
    }
  ]
}
```

Two parts:

- **Specification**: *Defining* access policies
- **Enforcement**: *Evaluating* policies

When you *define* access policies. You specify which IAM principals are allowed to perform which actions on specific AWS resources and under which conditions.

IAM enforces this access by *evaluating* the AWS request and the policies you defined and returns either yes or no answer.

IAM policies enable granular access controls

```
{
 "Statement":[{
   "Effect":"effect",
   "Principal":"principal",
   "Action":"action",
   "Resource":"arn",
   "Condition":{
     "condition":{
       "key":"value" }
      }
    }
  ]
 }
```

Principal: The entity that is allowed or denied access

"Principal":"AWS":"arn:aws:iam::123456789012:user/username"

Action: Type of access that is allowed or denied

*"Action":"*secretsmanager:GetSecretValue*"*

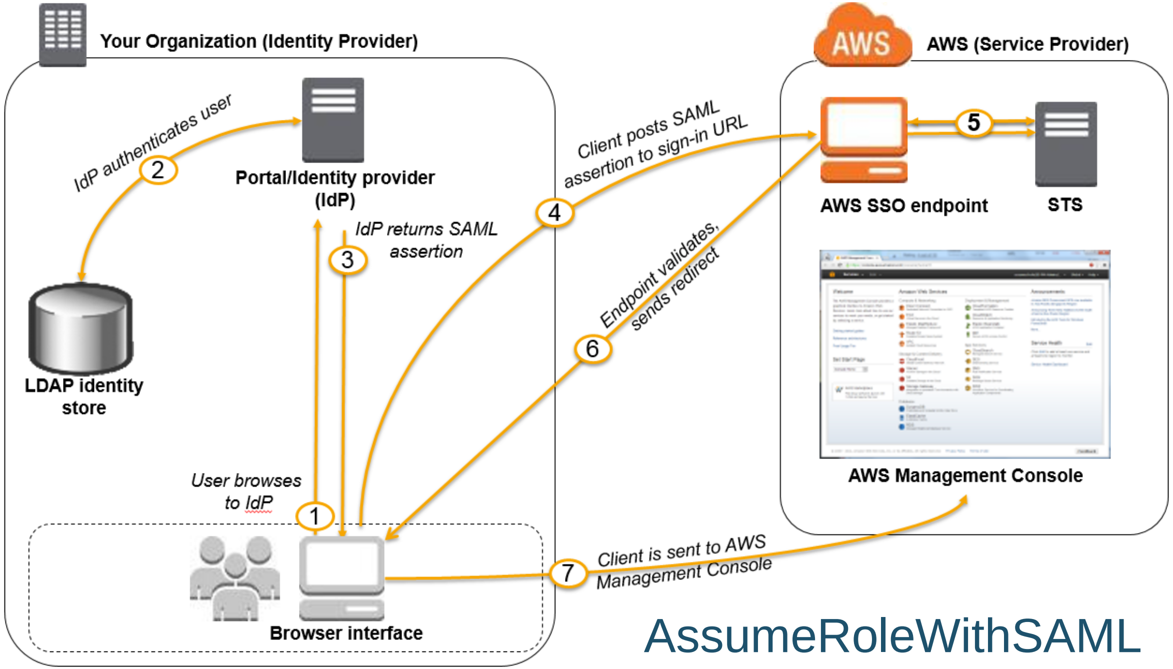
Resource: The Amazon resource(s) the action will act on

"Resource":"arn:aws:secretsmanager:xx-xxxx-xx:xxx:secret:xxx"

Condition: The conditions that are valid under the access defined

"StringEqua": {"secretsmanager:ResourceTag/Project": "Project1"}

SAML 2.0 – based federated users



Your Organization (Identity Provider)
AWS
AWS (Service Provider)
IdP authenticates user
2
Portal/Identity provider (IdP)
IdP returns SAML assertion
3
LDAP identity store
User browses to IdP
1
Browser interface
Client posts SAML assertion to sign-in URL
4
Endpoint validates, sends redirect
6
AWS SSO endpoint
5
STS
AWS Management Console
Client is sent to AWS Management Console
7

AssumeRoleWithSAML

Auth0

ForgeRock®

IBM Security

okta

onelogin

Ping Identity®

RSA

AWS Single Sign On

AWS Single Sign-on

Cloud single sign-on (SSO) service that helps centrally manage SSO access to AWS accounts and business applications.

Centrally manage access to multiple AWS accounts.

Use your existing corporate identities.

Easy to enable and use.

SSO access to business applications.

AWS Account

AWS Account

AWS Account

AWS Account

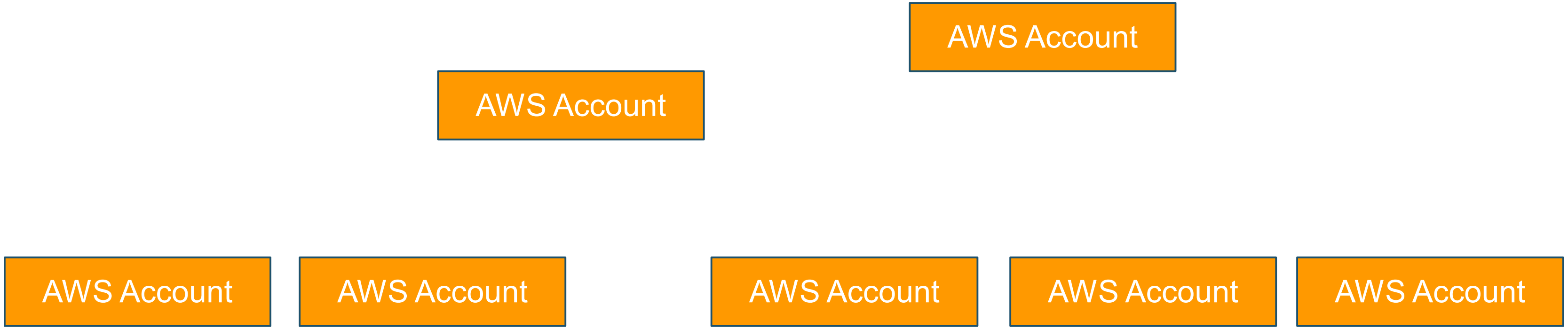
AWS Account

AWS Account

AWS Account

AWS Account

Govern accounts



AWS Account

AWS Account

AWS Account

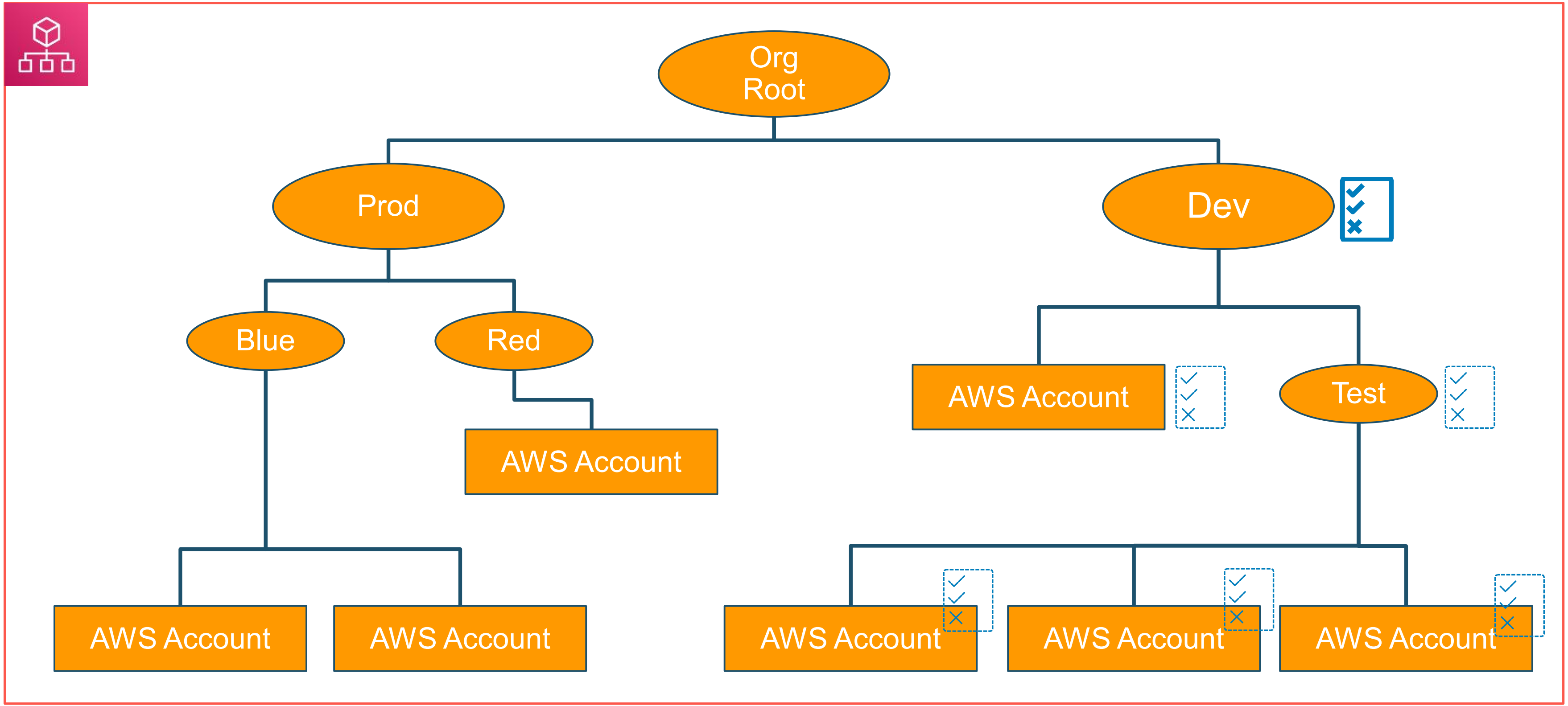
AWS Account

AWS Account

AWS Account

AWS Account

Organization



AWS Organizations

Central governance and management across AWS accounts for a comprehensive multi-account AWS environment

- Manage and define your organization and accounts
- Control access and permissions
- Audit, monitor, and secure your environment for compliance
- Share resources across accounts
- Centrally manage costs and billing

AWS Single Sign-On

Identity Sources

SSO Identity Store

AWS Managed Microsoft AD

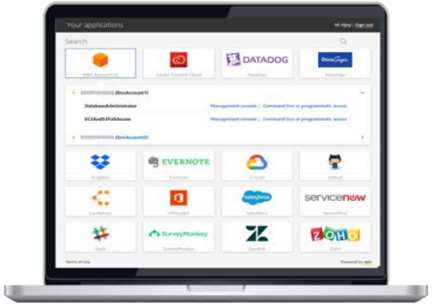
NEW! External Identity Provider

AWS Accounts

AWS Organizations

Permission Sets

Cloud Applications



Your applications

Hi Vijay | Sign out

Search

(DevAccount1)

DatabaseAdministrator — Management console | Command line or programmatic access

EC2AndS3FullAccess — Management console | Command line or programmatic access

(DevAccount2)

Terms of Use

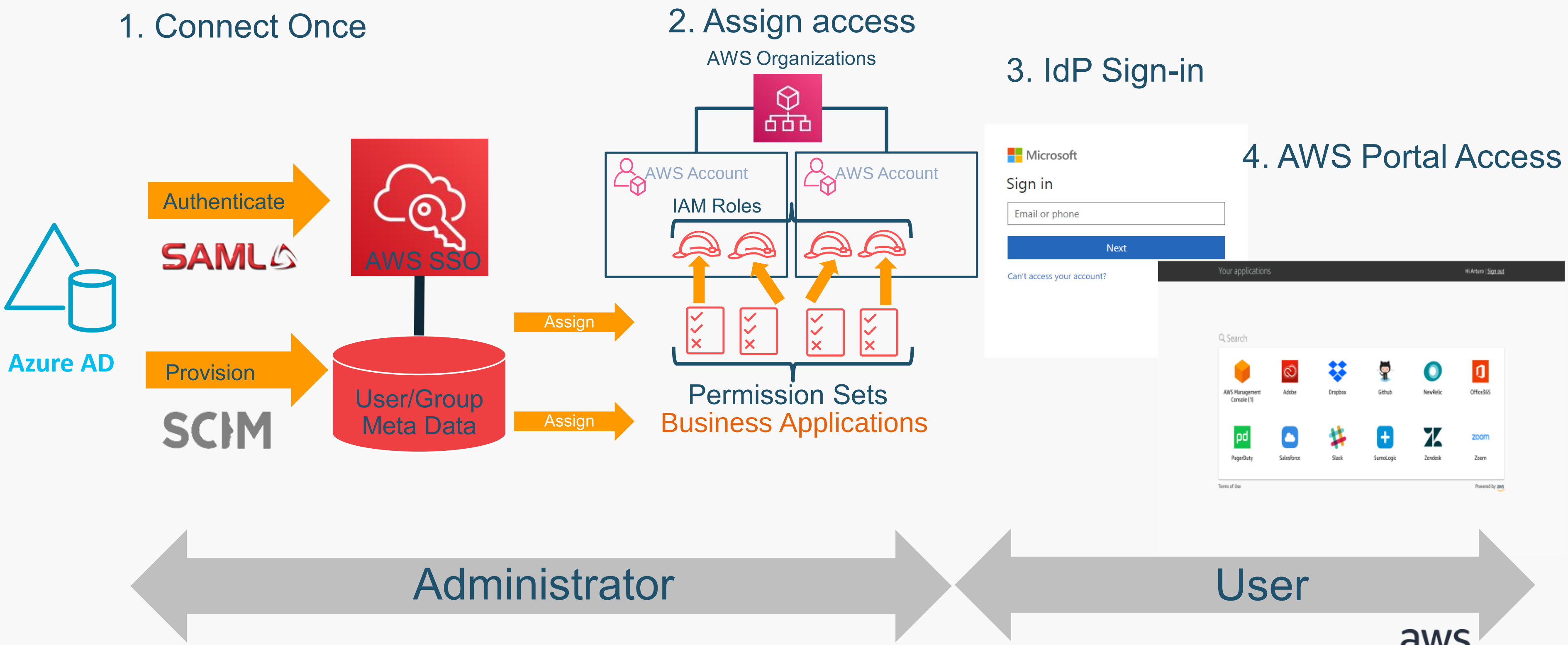
Powered by aws

Demo – SSO Basic Configuration

AWS SSO with external identity provider

AWS Single Sign-On external identity provider support

Standards-based provisioning and authentication



1. Connect Once

2. Assign access

3. IdP Sign-in

4. AWS Portal Access

Microsoft

Sign in

Email or phone

Next

Can't access your account?

Your applications

Hi Arturo | Sign out

Search

AWS Management Console (1)
Adobe
Dropbox
Github
NewRelic
Office365
PagerDuty
Salesforce
Slack
SumoLogic
Zendesk
Zoom

Terms of Use

Powered by aws

Demo
Integrating AWS SSO with Azure AD

Demo
Signing into AWS CLIv2

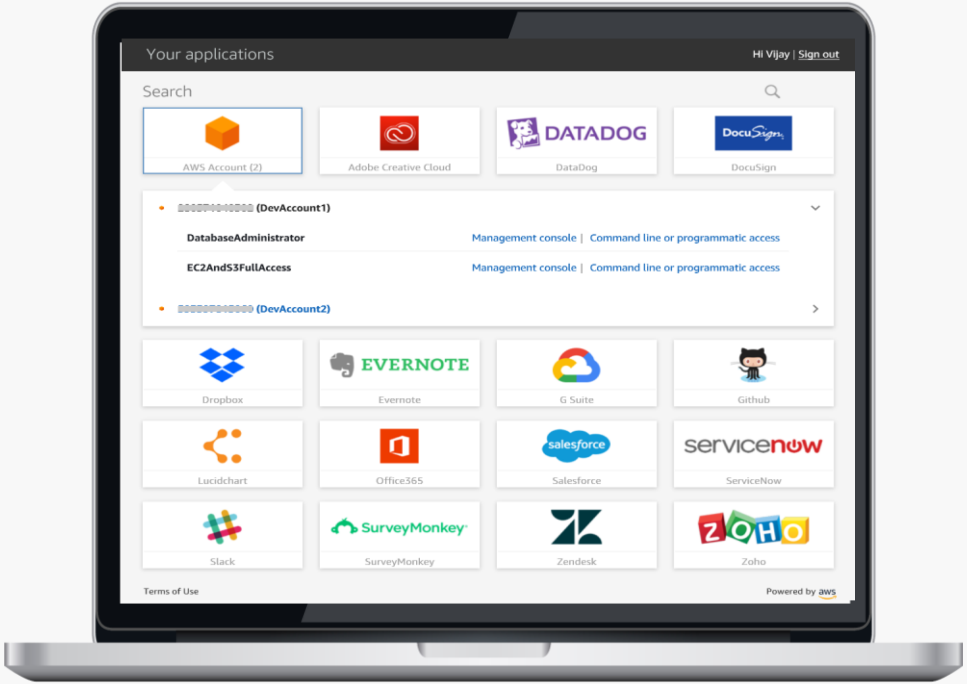
AWS SSO recap

Manage identities:

- Within AWS SSO
- In your on-premises directory
- In a cloud identity provider

AWS SSO supports open standards:

- SAML 2.0 **New!**
- SCIM **New!**


Your applications

Hi Vijay | Sign out

Search

[redacted] (DevAccount1)

DatabaseAdministrator — Management console | Command line or programmatic access

EC2AndS3FullAccess — Management console | Command line or programmatic access

[redacted] (DevAccount2)

Centrally control access across AWS accounts in your organization and business applications.

Additional resources

https://aws.amazon.com/single-sign-on/

https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html

https://aws.amazon.com/about-aws/whats-new/2019/11/manage-access-to-aws-centrally-for-azure-ad-users-with-aws-single-sign-on/

https://aws.amazon.com/blogs/aws/the-next-evolution-in-aws-single-sign-on/

https://aws.amazon.com/iam/

Thank you!

Lior Pollack
Solutions Architect, AWS

Yuri Duchovny
Solutions Architect, AWS