WIN303

# AWS Directory Service for Microsoft Active Directory Deep Dive

Ron Cully
Principal Product Manager

November 26, 2018

# What we will cover

- What AWS Managed Microsoft AD is
- Key use cases
  - How applications use AWS Managed Microsoft AD
  - Deployment models (user vs. resource forest)
- How to install, administer, and configure
- Supported trust models
- Security event logging
- Directory sharing

# What AWS Managed Microsoft AD is

# AWS Directory Service for Microsoft Active Directory

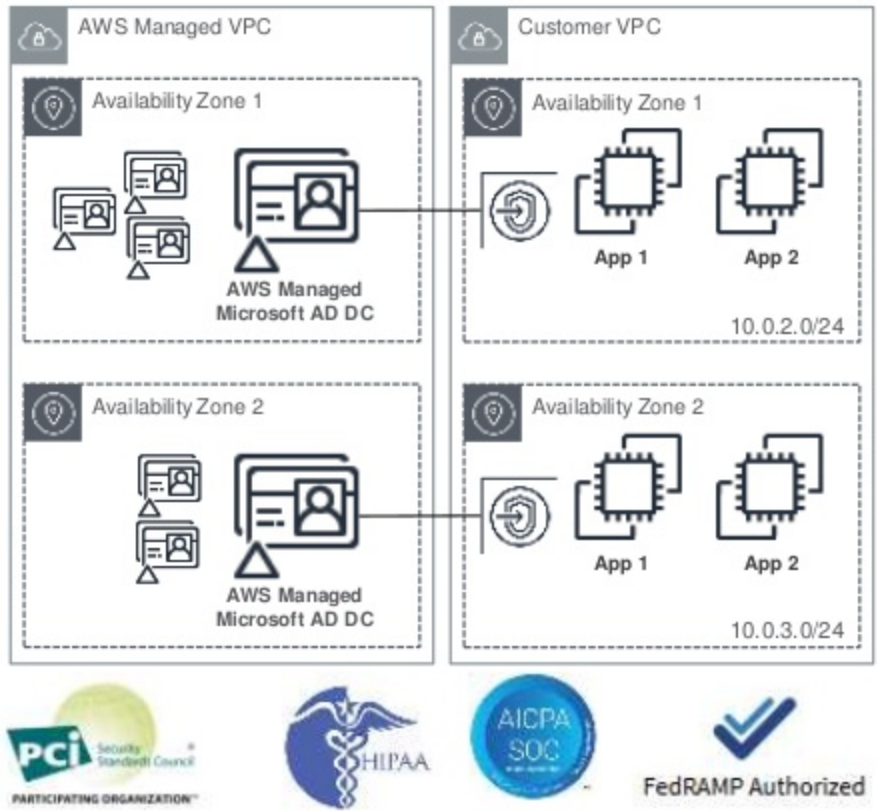
"AWS Managed Microsoft AD"

# AWS Directory Service for Microsoft Active Directory

"AWS Managed Microsoft AD"

**Domain controllers are exclusively yours**

**Compliance audited**



# AWS Directory Service for Microsoft Active Directory

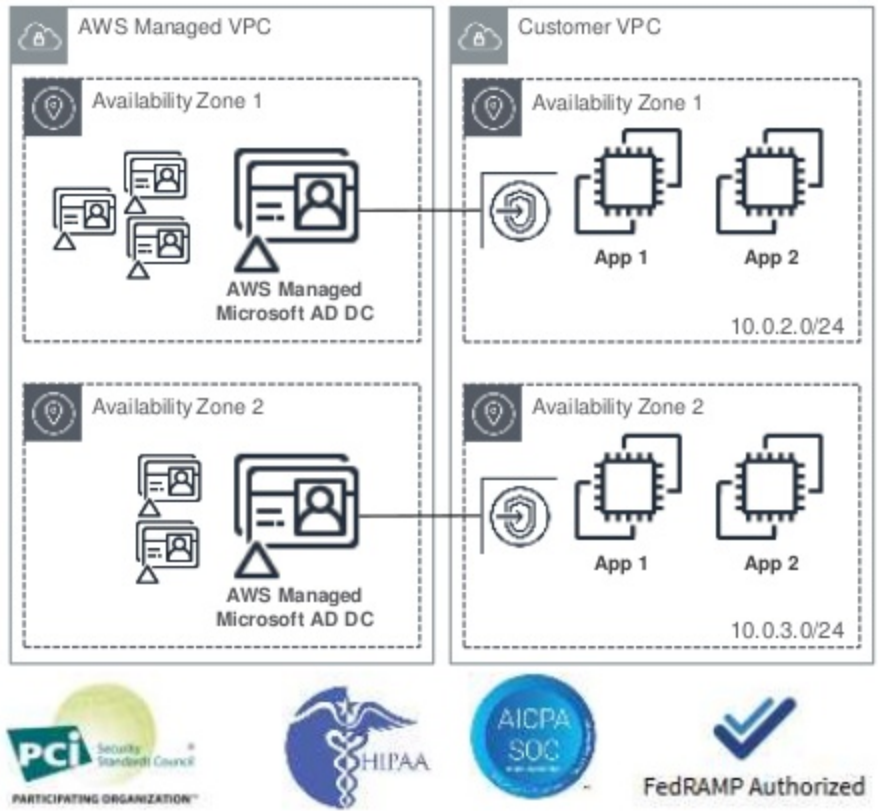
"AWS Managed Microsoft AD"

## Amazon—operates

- Multi-AZ deployment, patch, monitor, DC recovery, instance rotation, snapshot, restore

## Customer—administer and configure

- Administer users, groups, GPOs, other AD content
  - Administration via Active Directory Users and Computers (ADUC) and other standard AD tools
- Configure password policies
- Add domain controllers as needed
- Configure trusts (resource forest deployment)
- Configure certificate authorities (for LDAPS)
- Configure federation



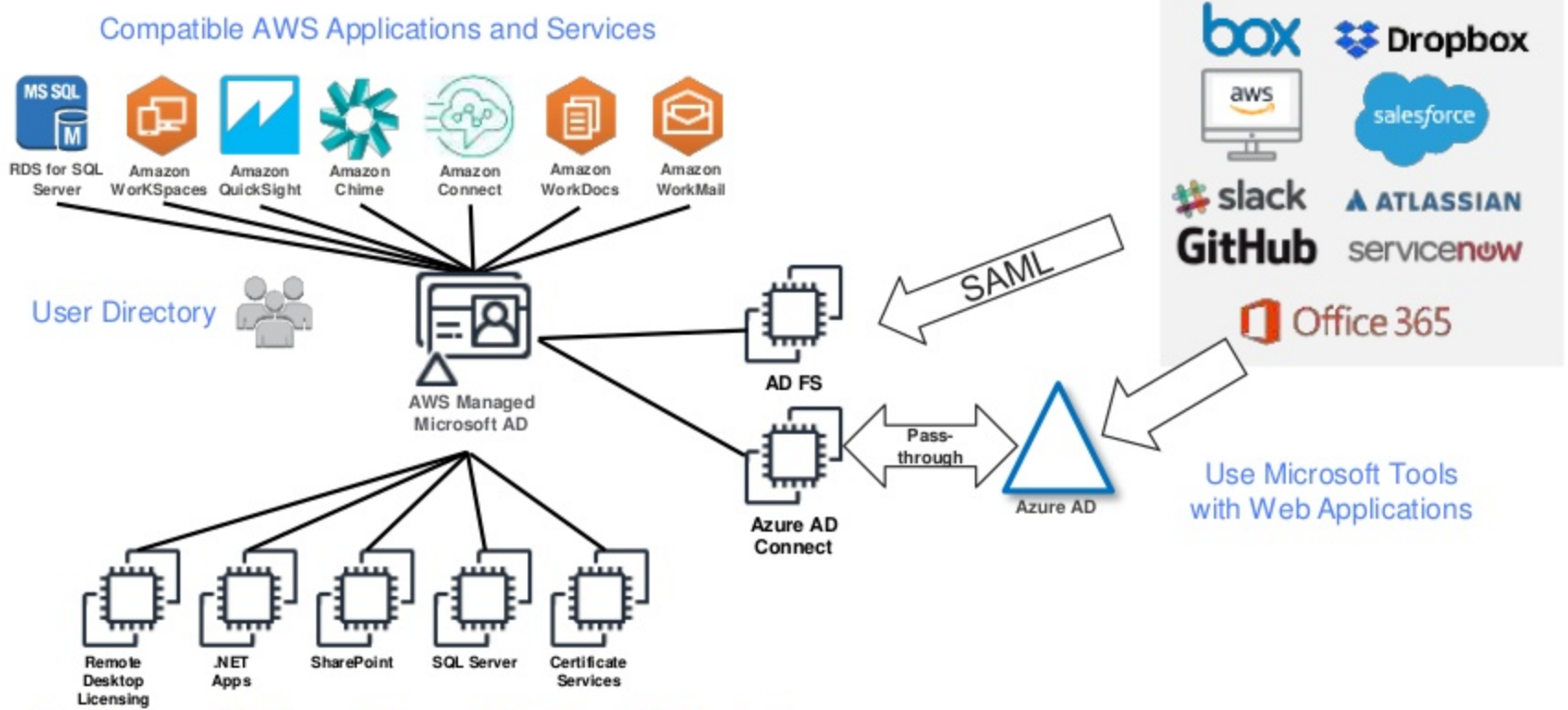
# AWS Directory Service for Microsoft Active Directory

"AWS Managed Microsoft AD"

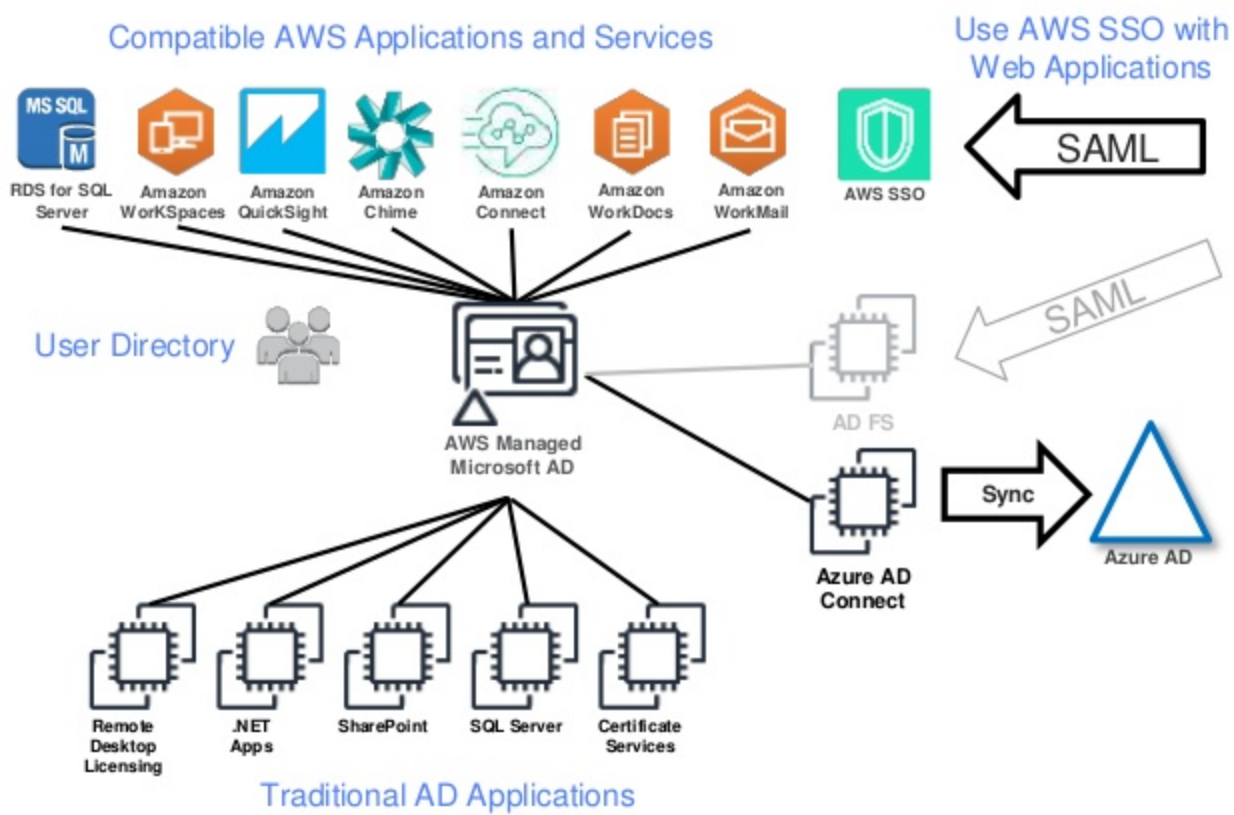
| | Standard Edition | Enterprise Edition |
|---|---|---|
| Storage Capacity | 1GB | 17GB |
| Performance Optimized | ~5,000 employees | Over 5,000 employees |

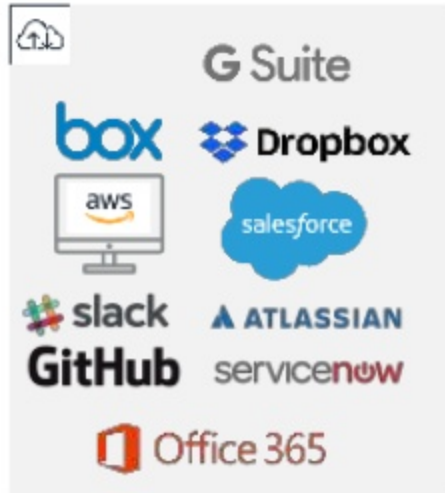
# Key use cases

# AWS Managed Microsoft AD use cases



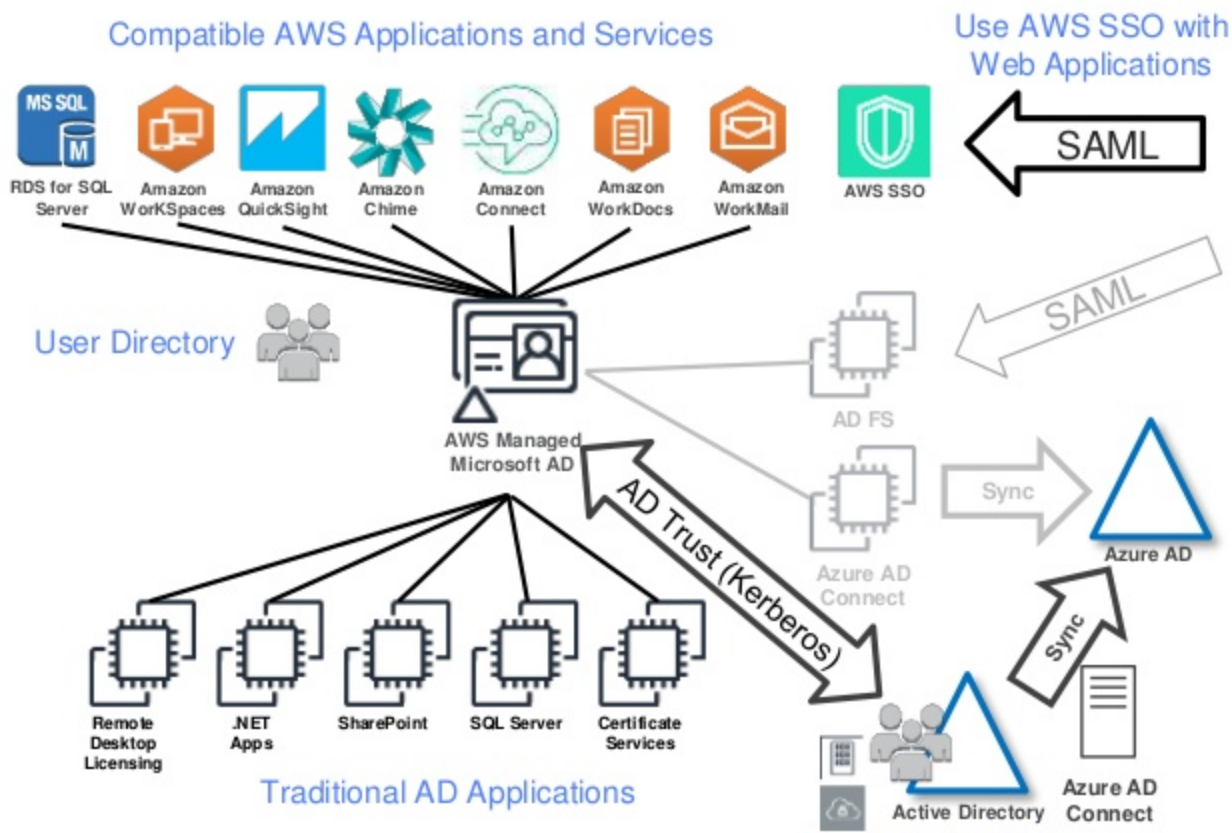
# AWS Managed Microsoft AD use cases

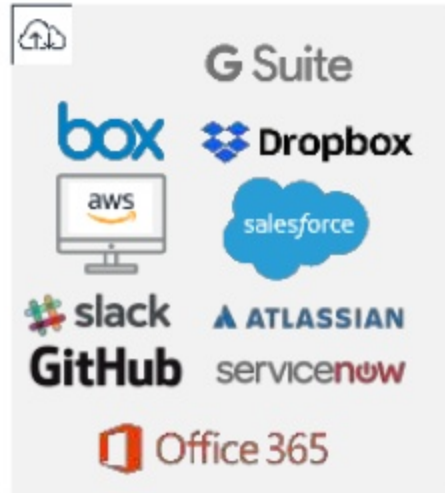



Use Microsoft Tools with Web Applications

# AWS Managed Microsoft AD use cases



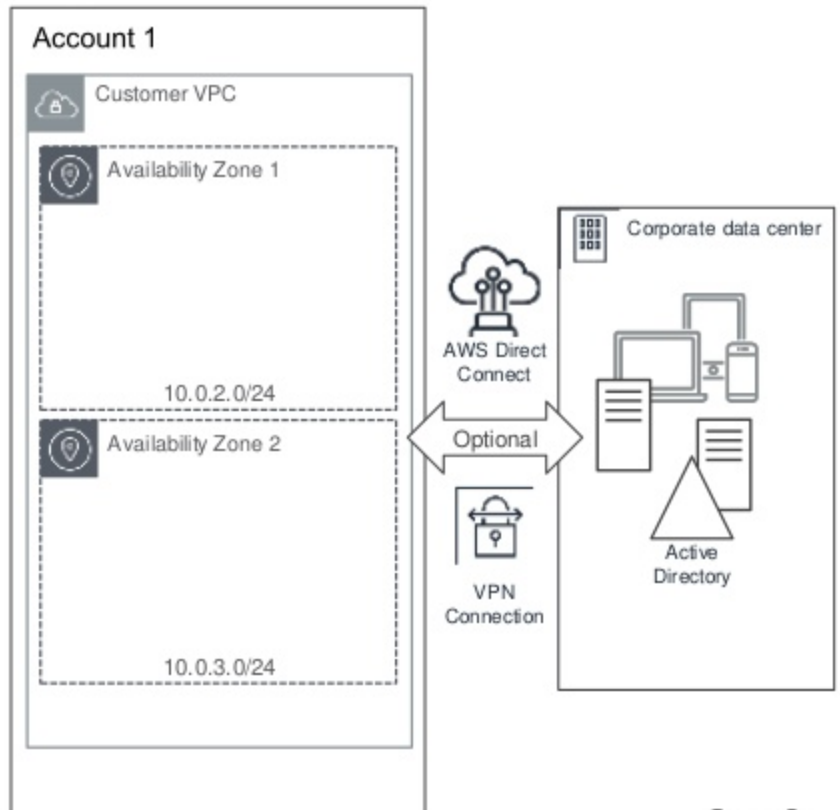

Use Microsoft Tools with Web Applications

# How to install, administer, and configure

# Prerequisites you must create

docs.aws.amazon.com/directoryservice/latest/admin-guide/tutorials_ad_test_labs.html

- Virtual Private Cloud (VPC)
- Two subnets in different AZs
- Optional on-premises link
  - Amazon Direct Connect or Virtual Private Network (VPN)
  - Optional AD on-premises

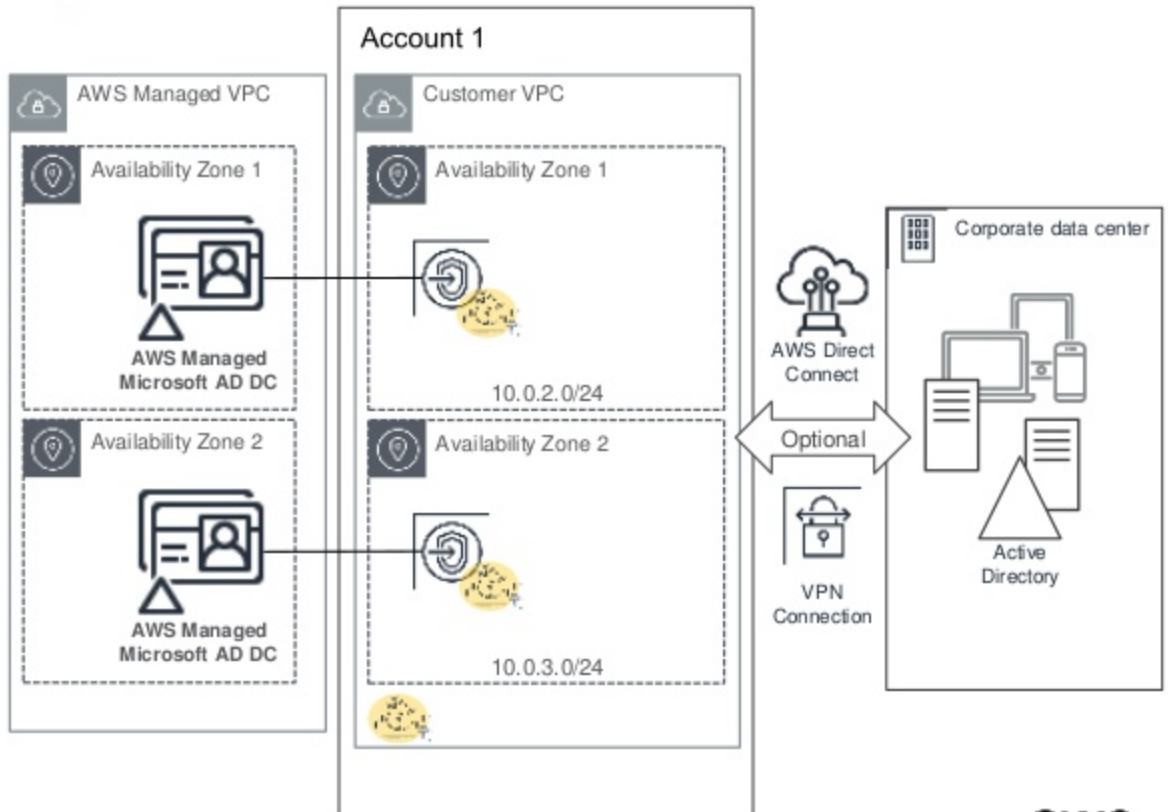


# During creation AWS creates

docs.aws.amazon.com/directoryservice/latest/admin-guide/tutorials_ad_test_labs.html

- 2 DCs with Dynamic DNS
- Elastic network interface in your subnets
- One AWS security group

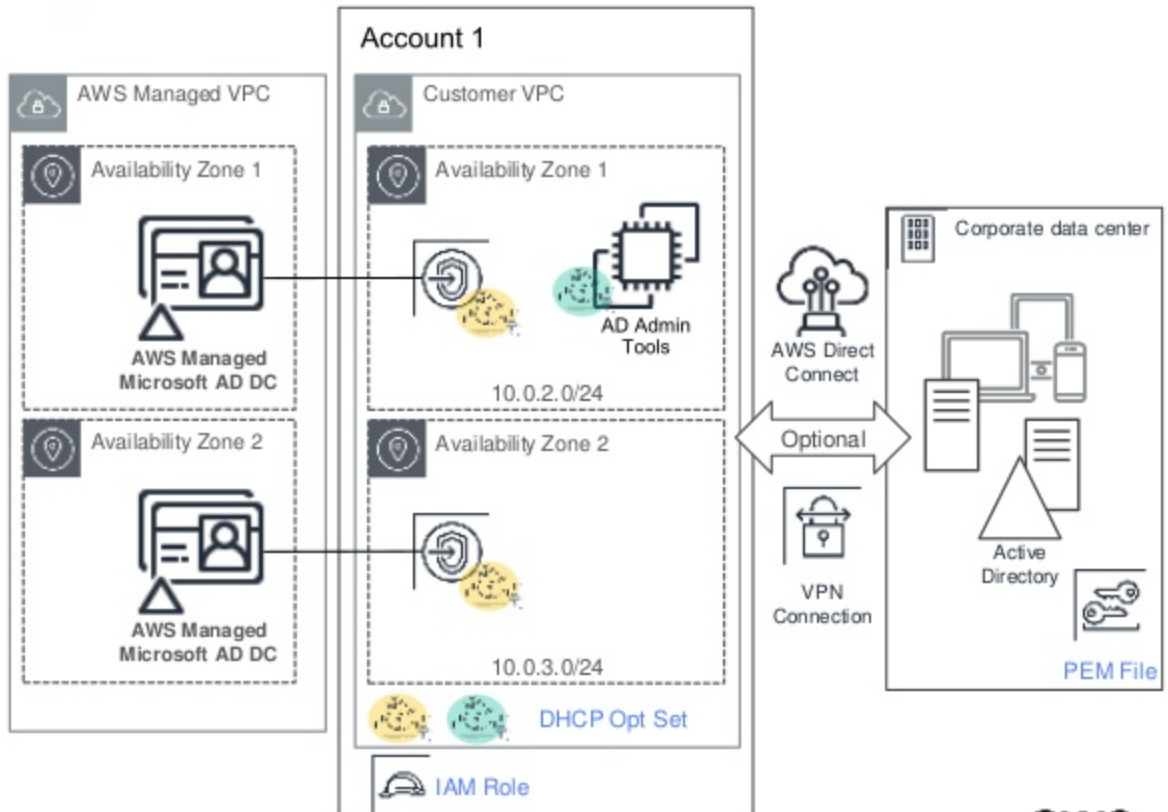
Use extreme caution modifying the security groups!



# Best practice after creation

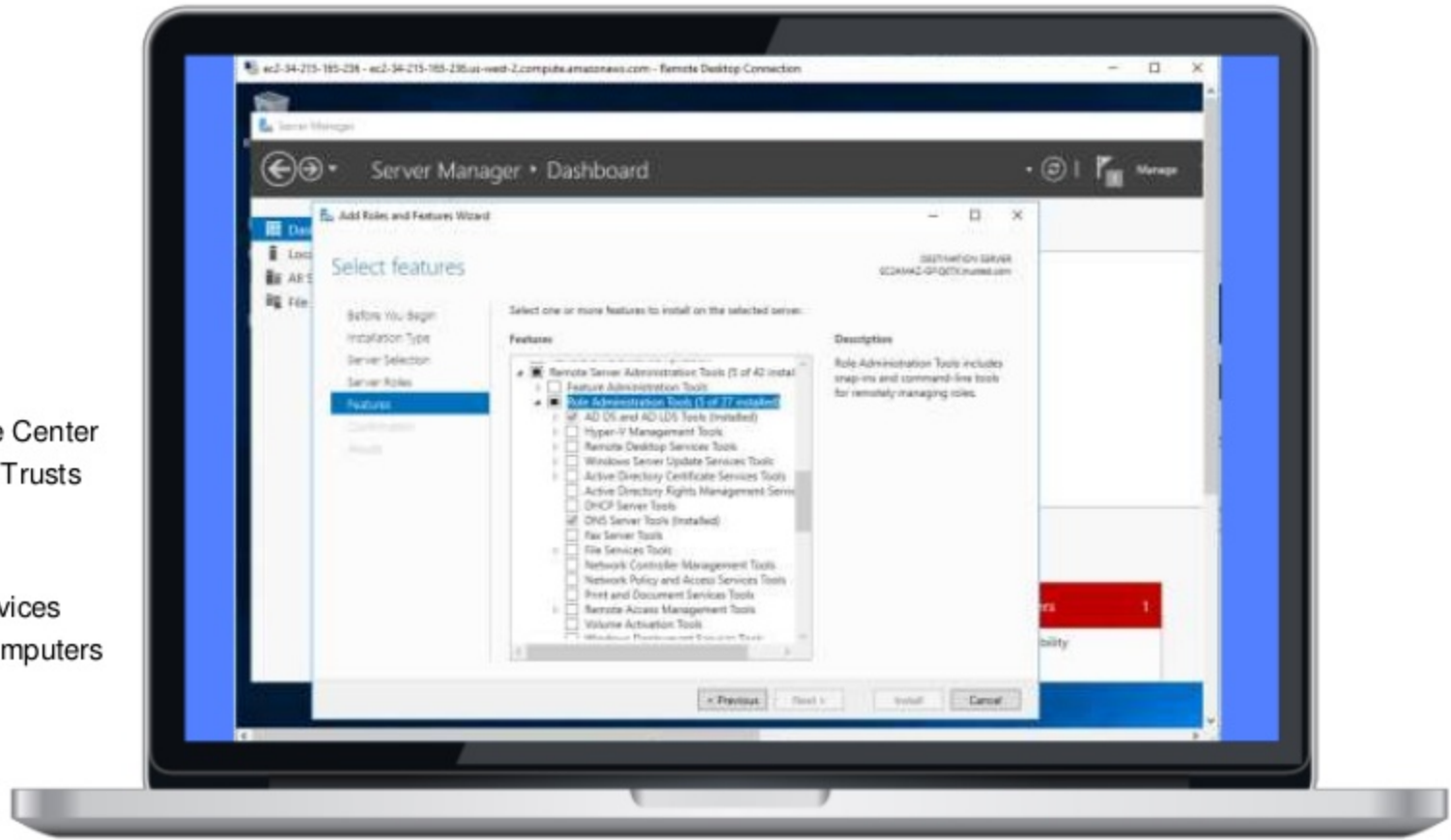
docs.aws.amazon.com/directoryservice/latest/admin-guide/tutorials_ad_test_labs.html

- DHCP option sets
- AWS security group
  (for your EC2 creations)
- IAM role/policy for EC2
  (AmazonEC2RoleforSSM)
- Key-pair (PEM) file
- EC2 Windows
  (Install AD Administration Tools)

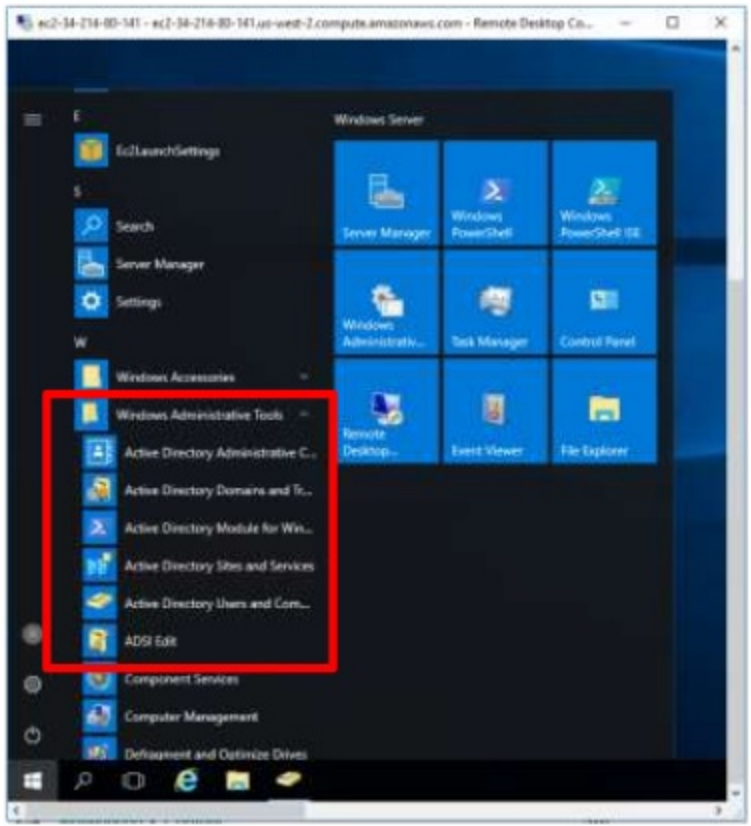


# Configure administration instance

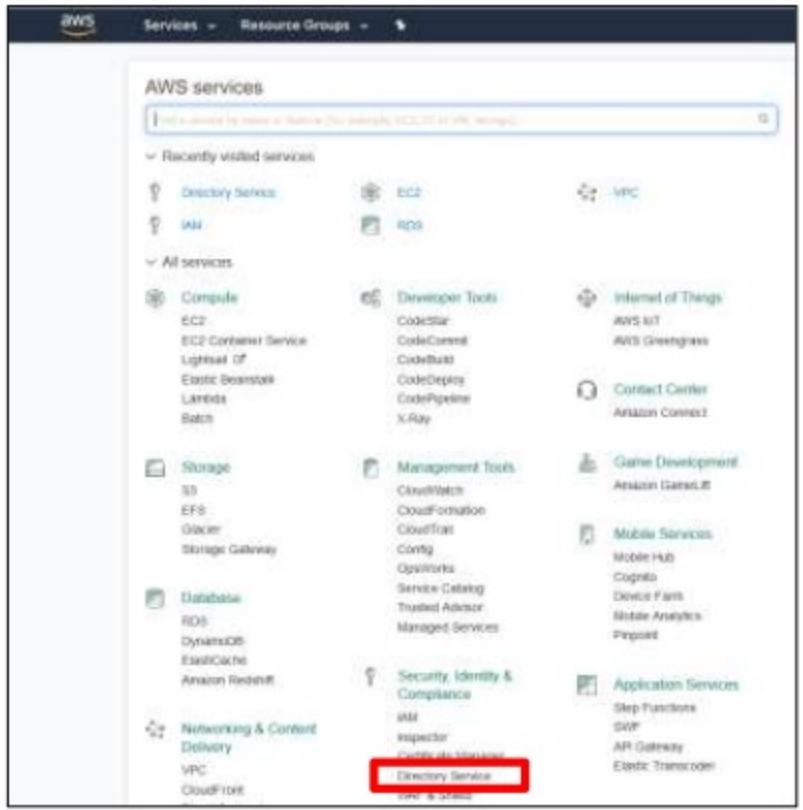
1. RDP to Instance
   yourdomain\admin
2. Add Features
   - ☑ Group Policy Management
   - ☑ AD DS and AD LDS Tools
   - ☑ DNS Server Tools
3. Verify Tools Added
   - ☑ Active Directory Administrative Center
   - ☑ Active Directory Domains and Trusts
   - ☑ Active Directory Module for Windows PowerShell
   - ☑ Active Directory Sites and Services
   - ☑ Active Directory Users and Computers
   - ☑ ADSI Edit
   - ☑ DNS
   - ☑ Group Policy Management



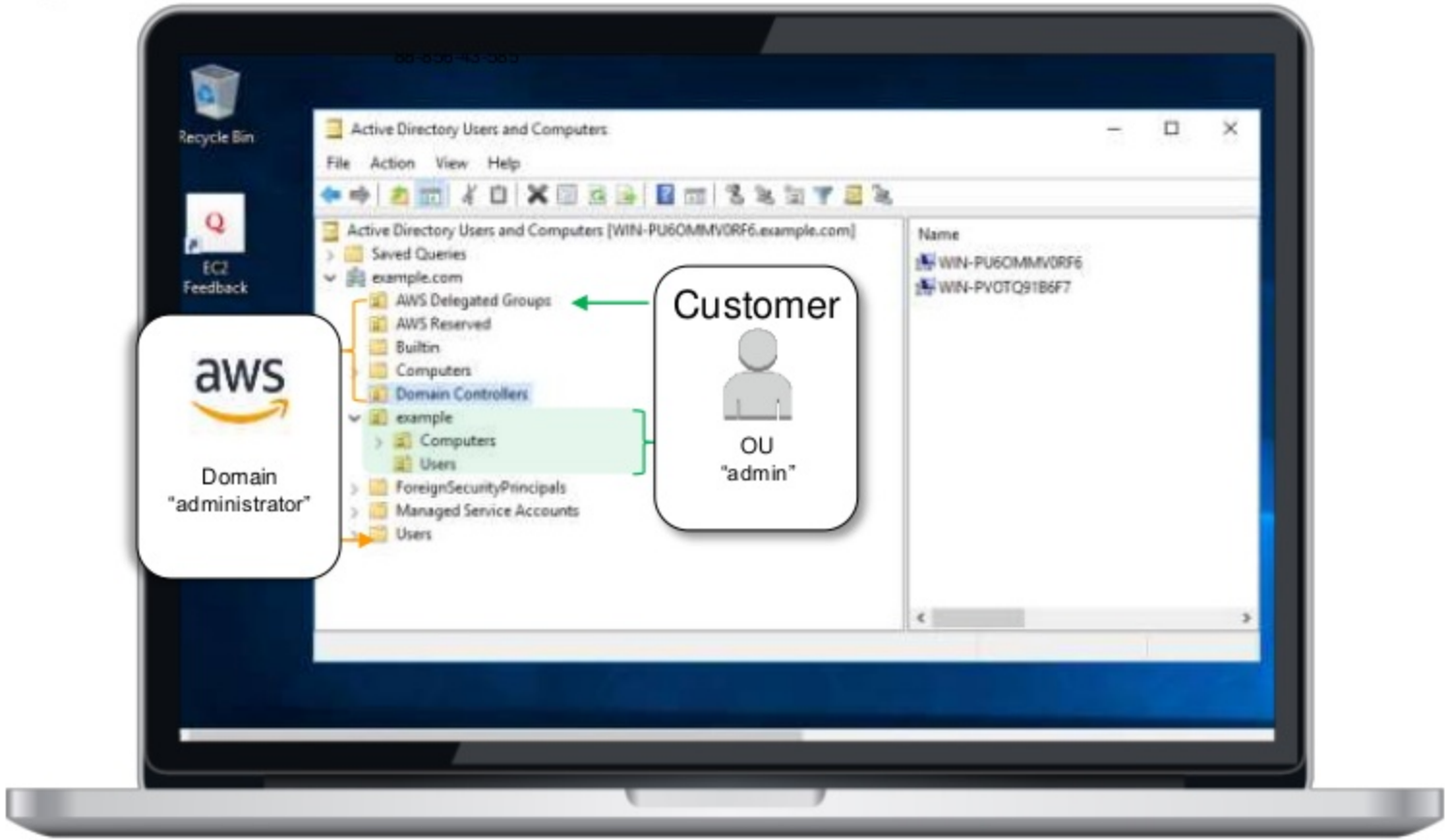
## Administer with AD tools



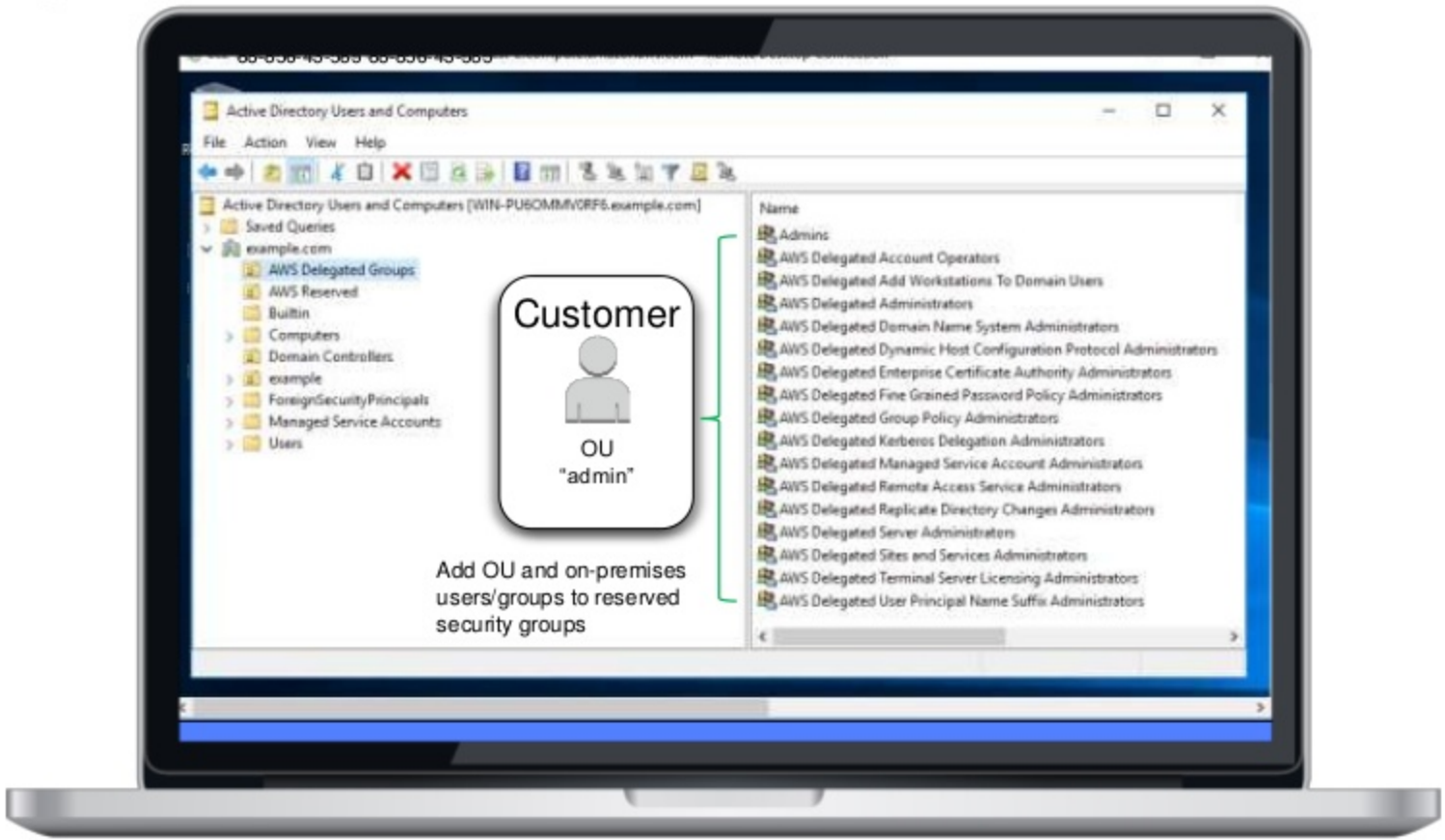

## Configure from AWS Console



# Managing from AD Administration Tools



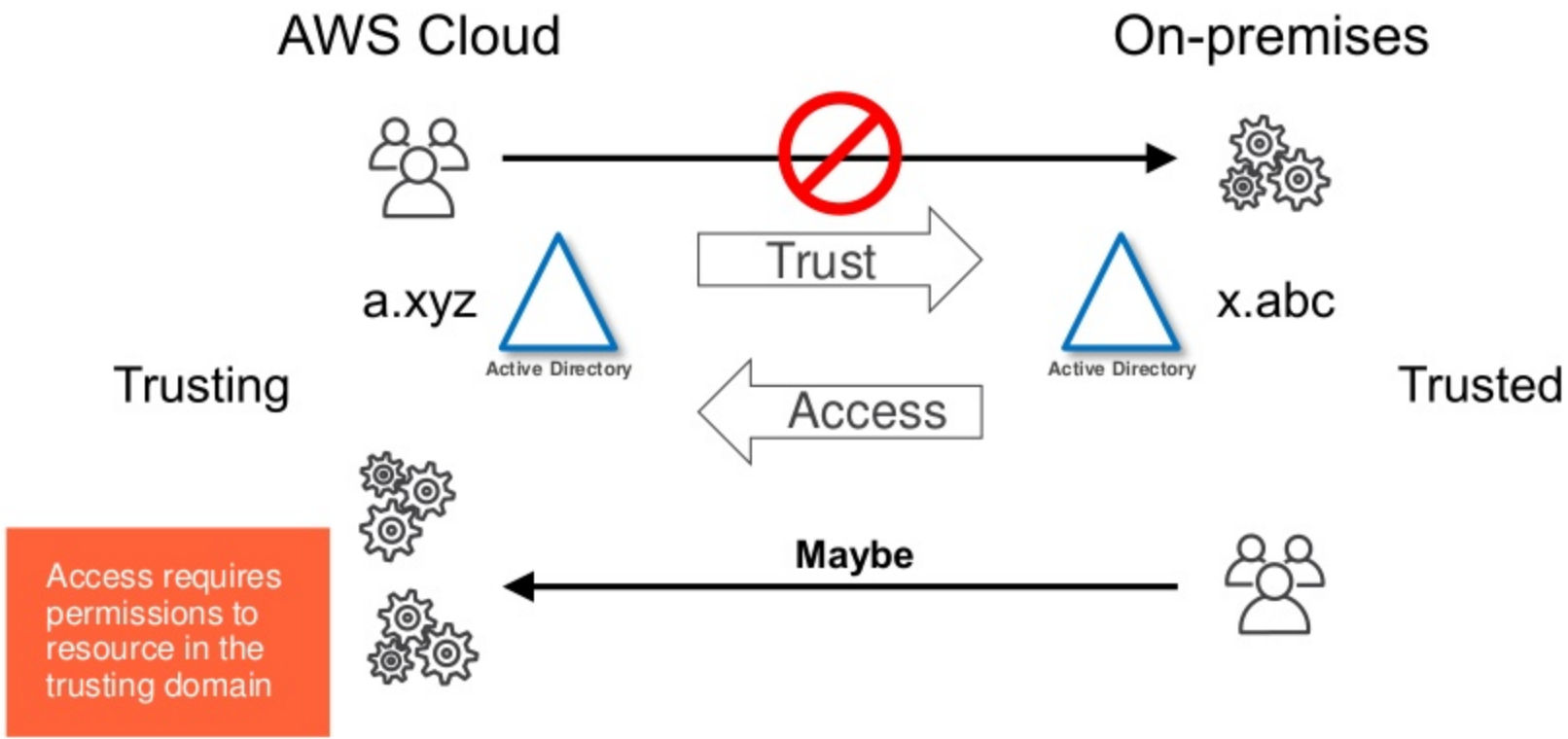
# Managing from AD Administration Tools



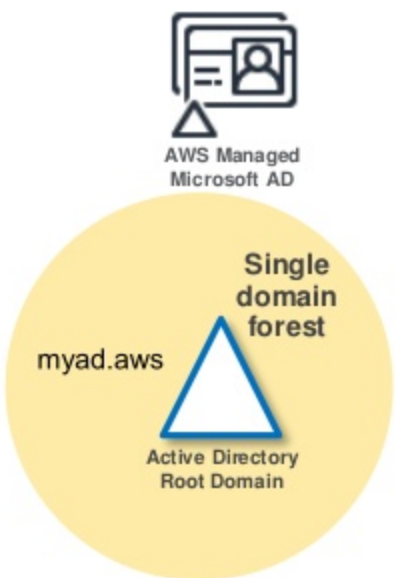
# Demo:
# Configuring AWS Managed Microsoft AD

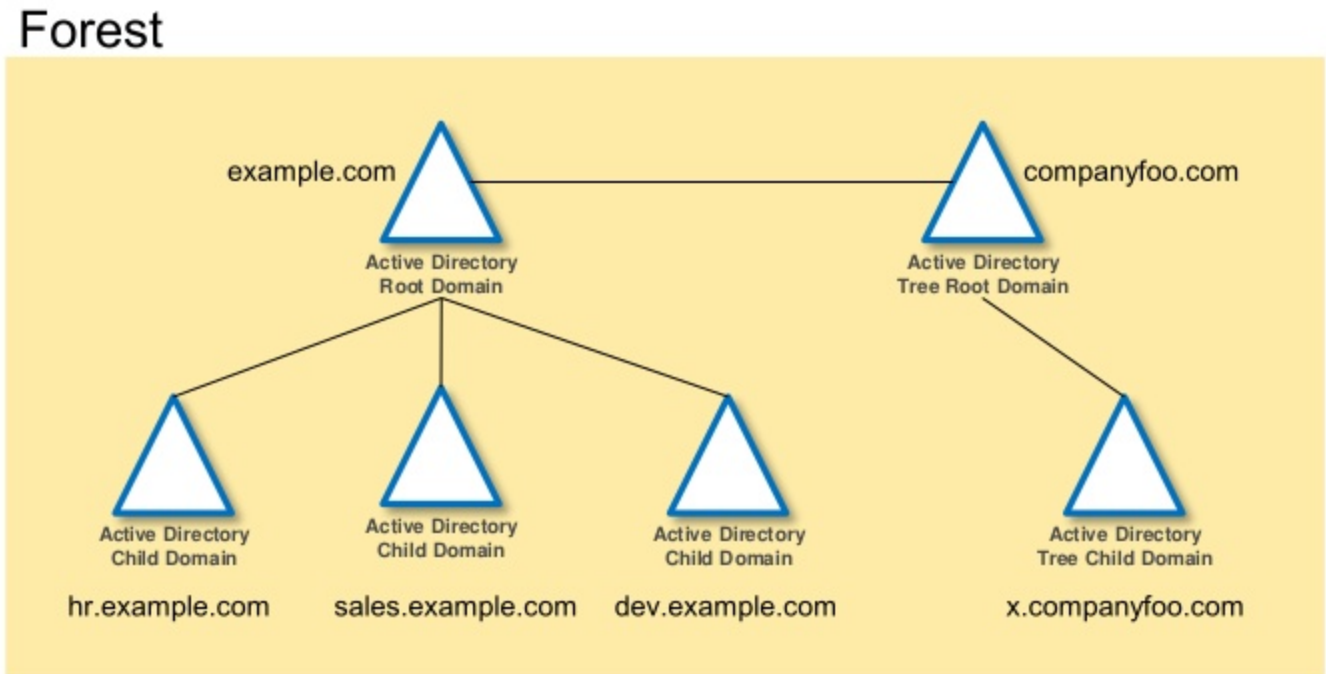
# Supported trust models

# Trusts

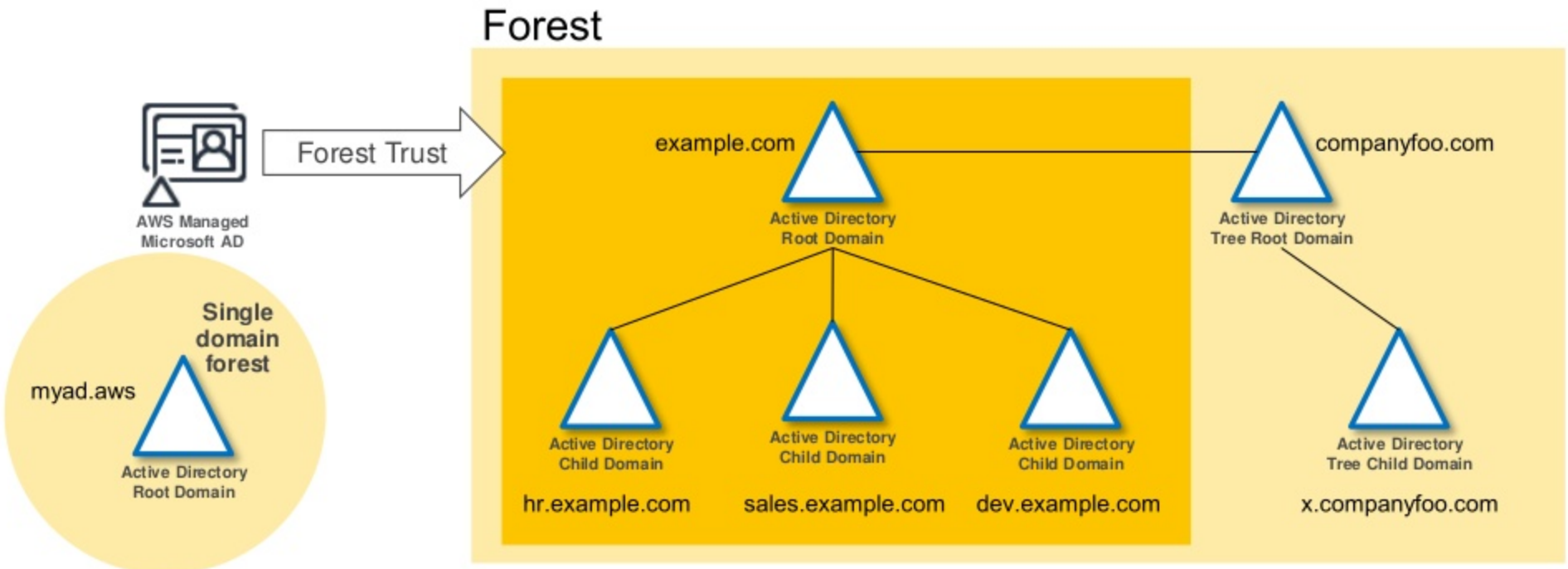


# Forests, domains, tree domains

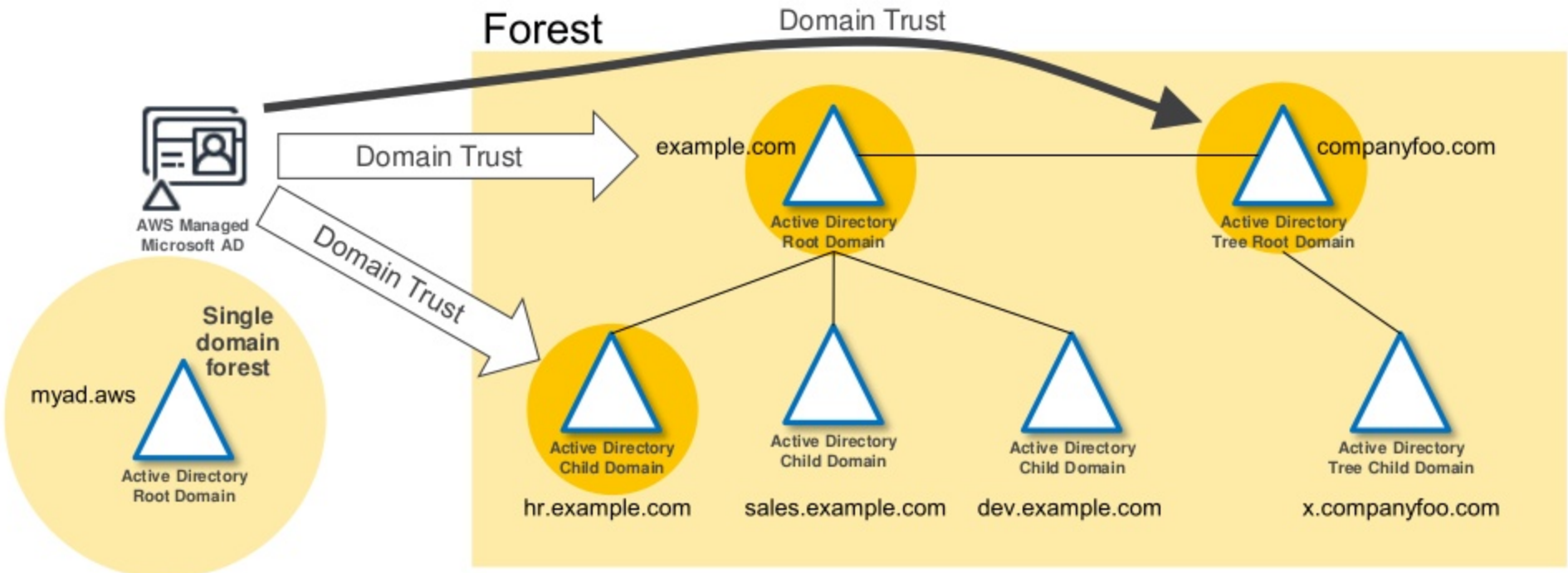


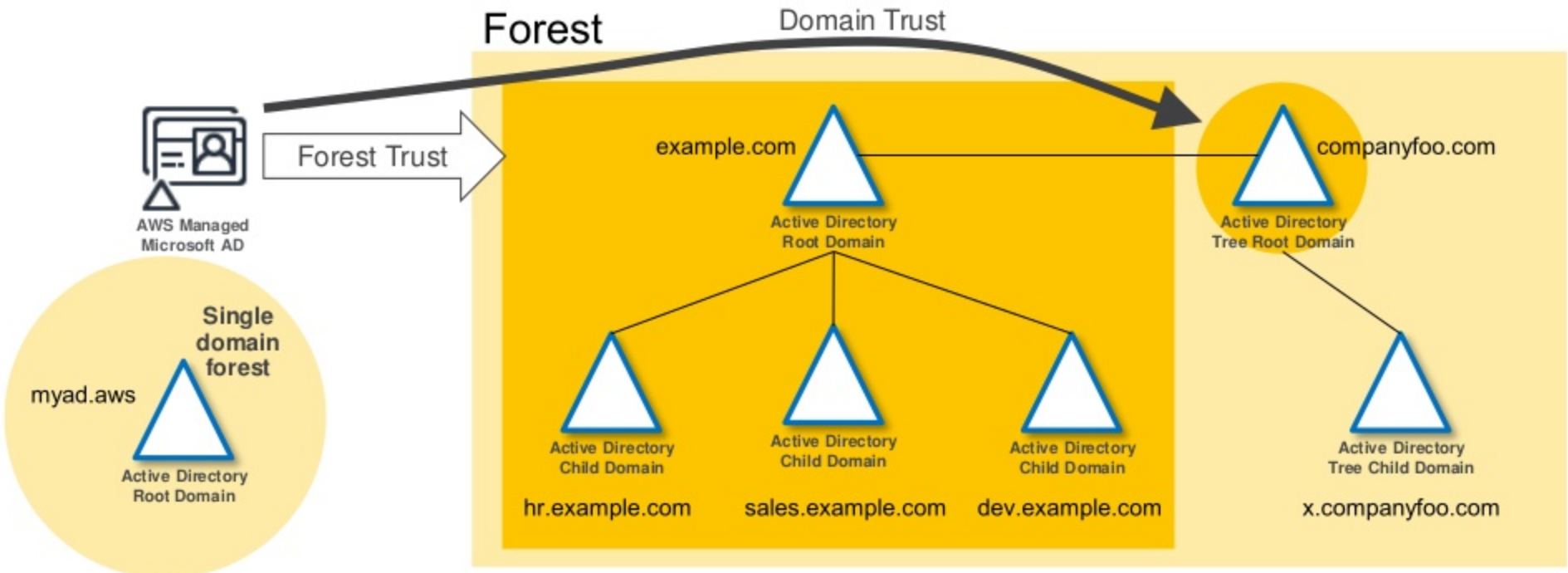
# AWS Managed Microsoft AD forest trust support



# AWS Managed Microsoft AD domain trust support

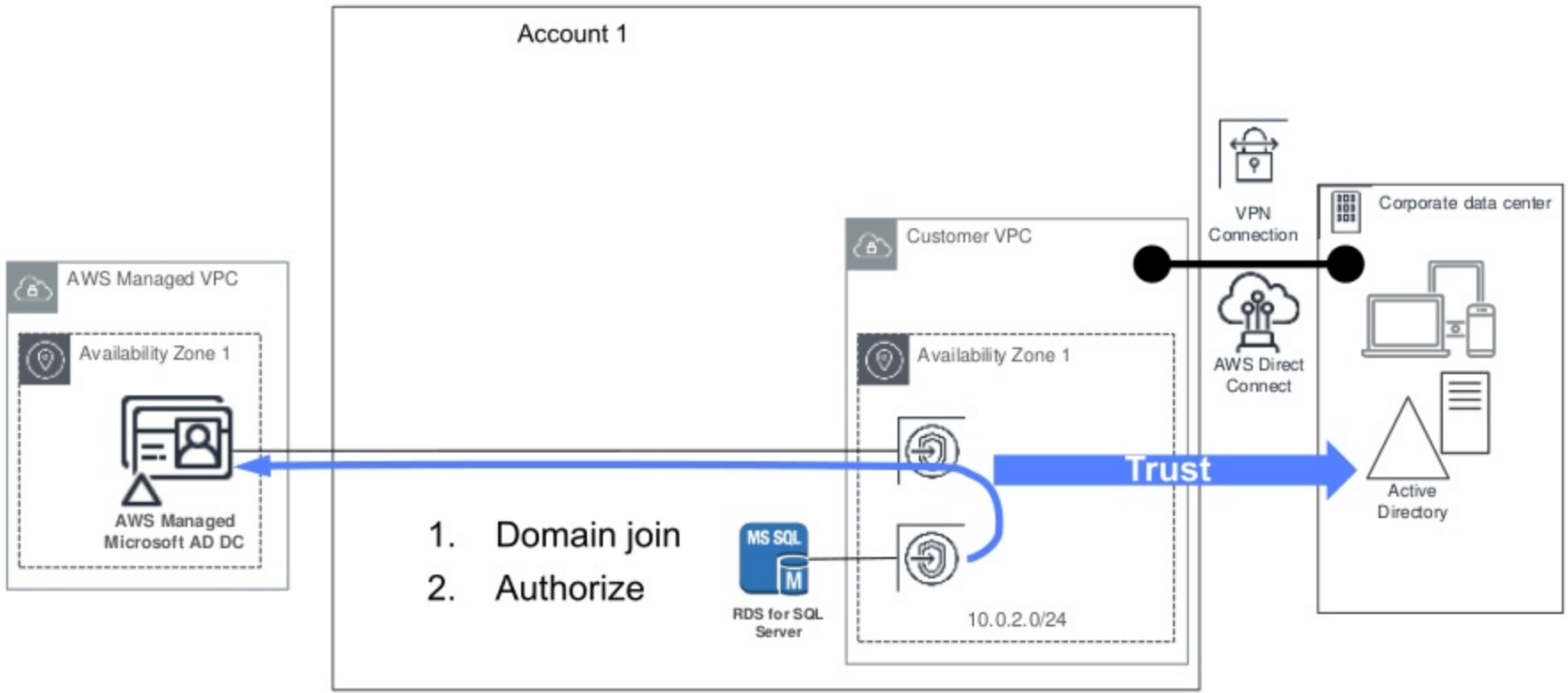


# AWS Managed Microsoft AD mixed trust support



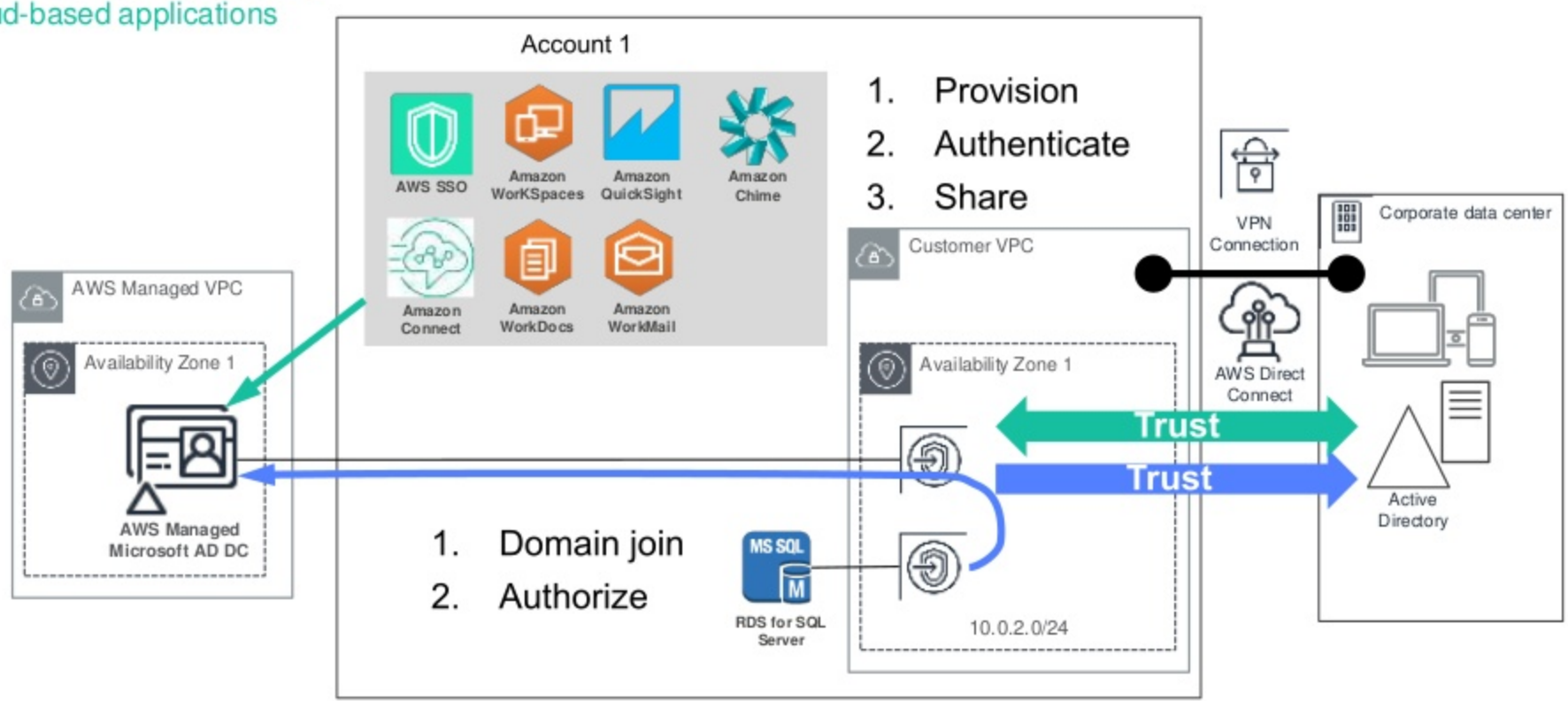
# AWS applications and trusts for hybrid IT use cases

## Traditional AD aware applications



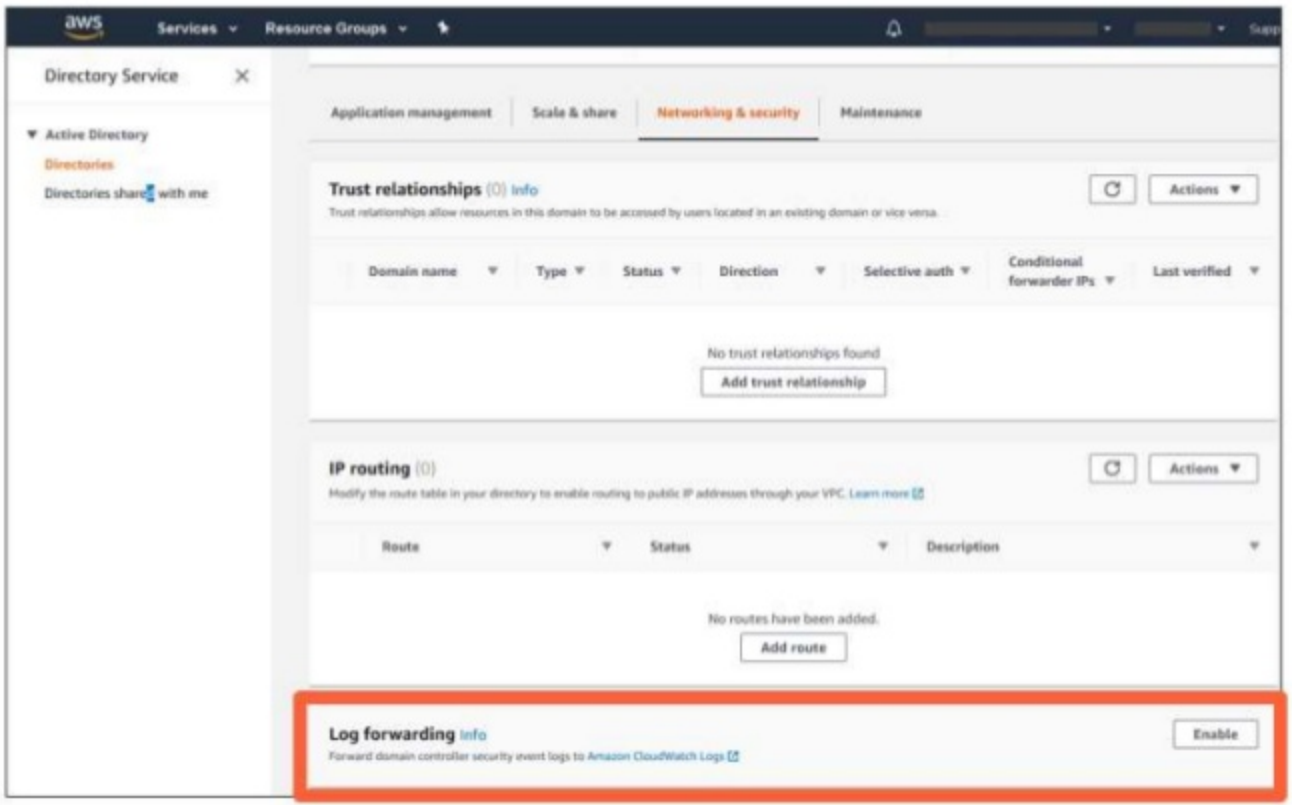
# AWS applications and trusts for hybrid IT use cases

Traditional AD aware applications
AWS cloud-based applications

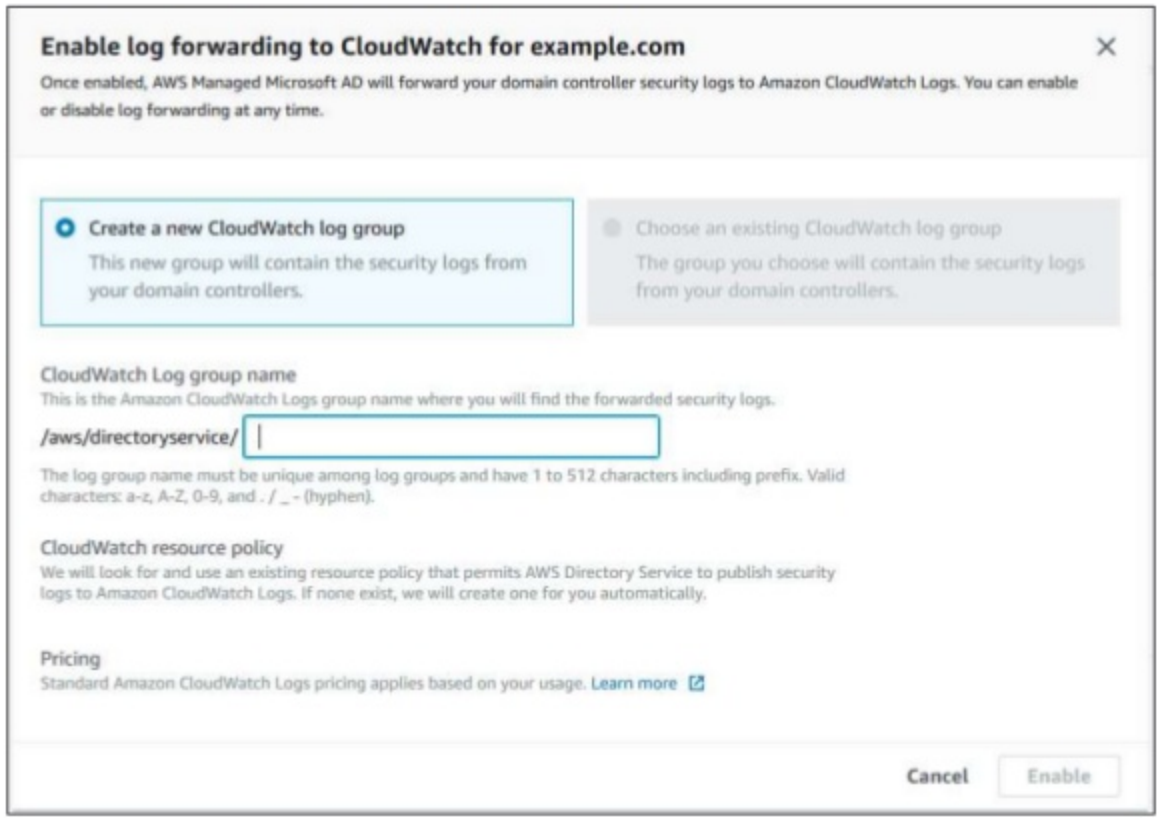


# Security event logging

# Security event logging to CloudWatch

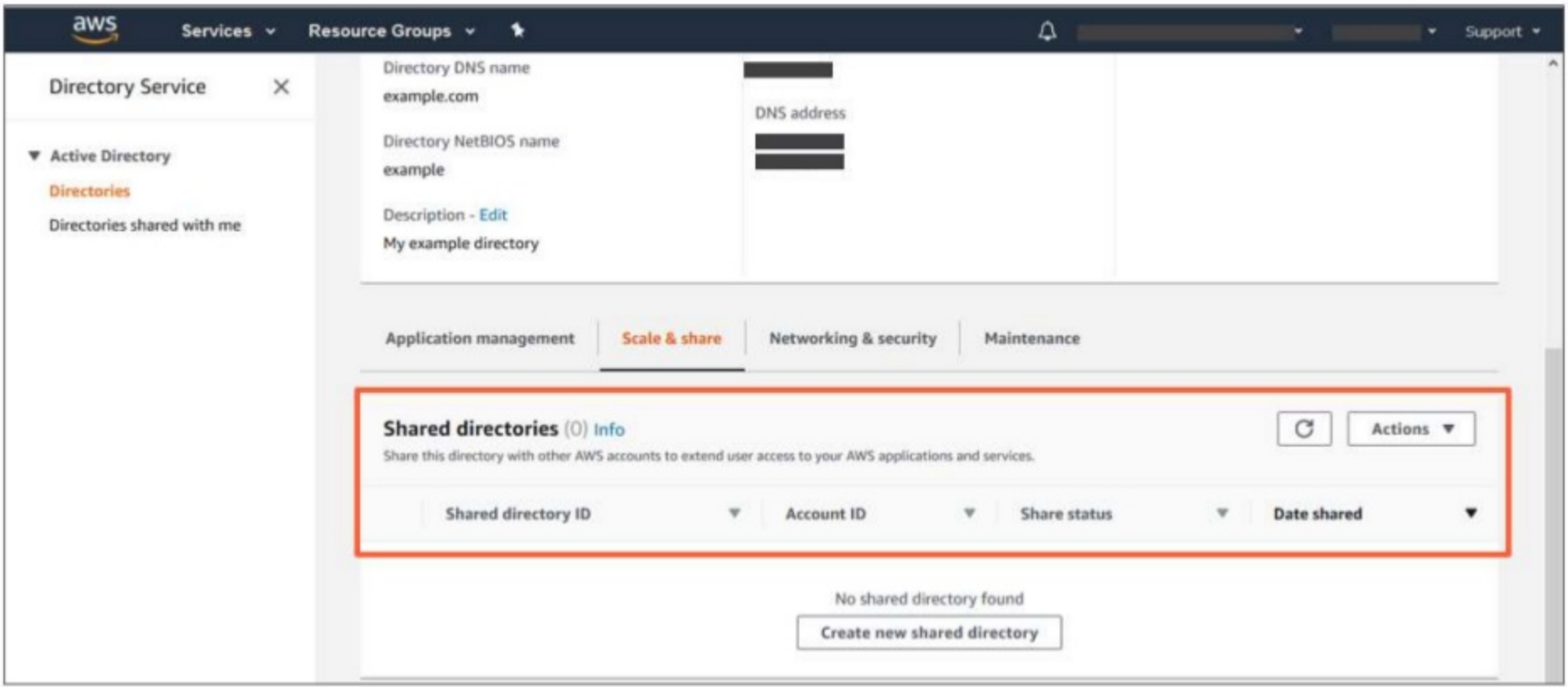



# Use existing or create a new log group

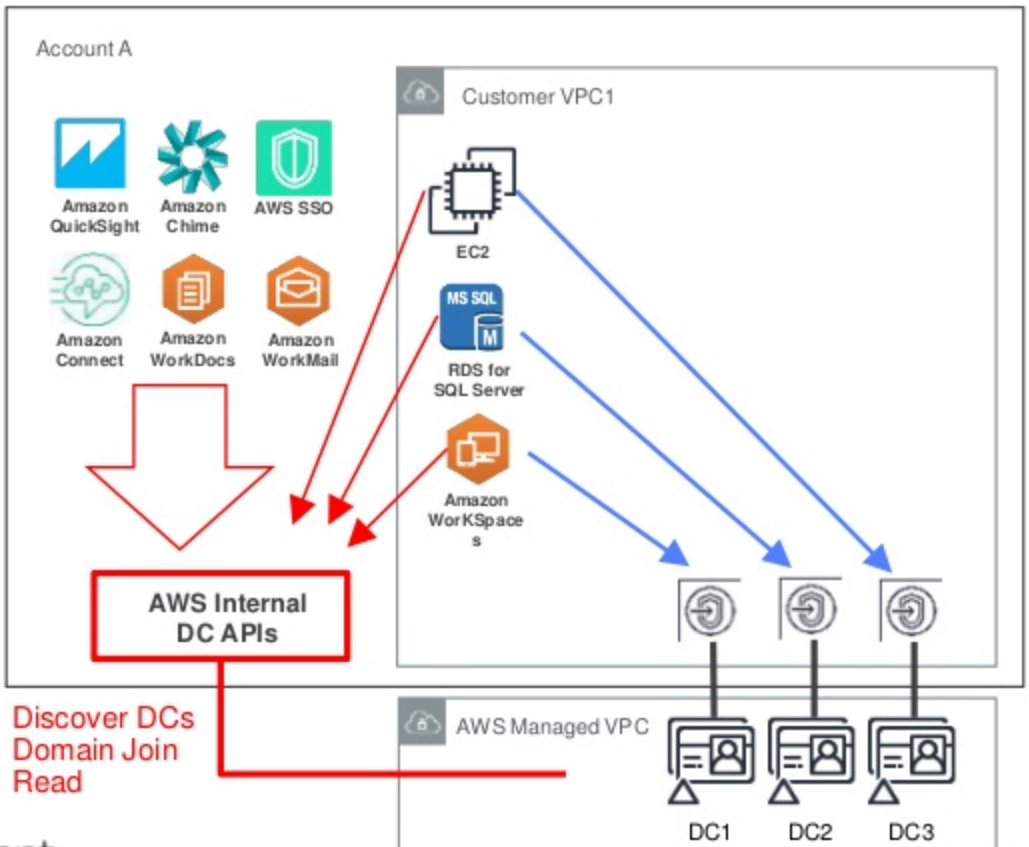


# Directory sharing

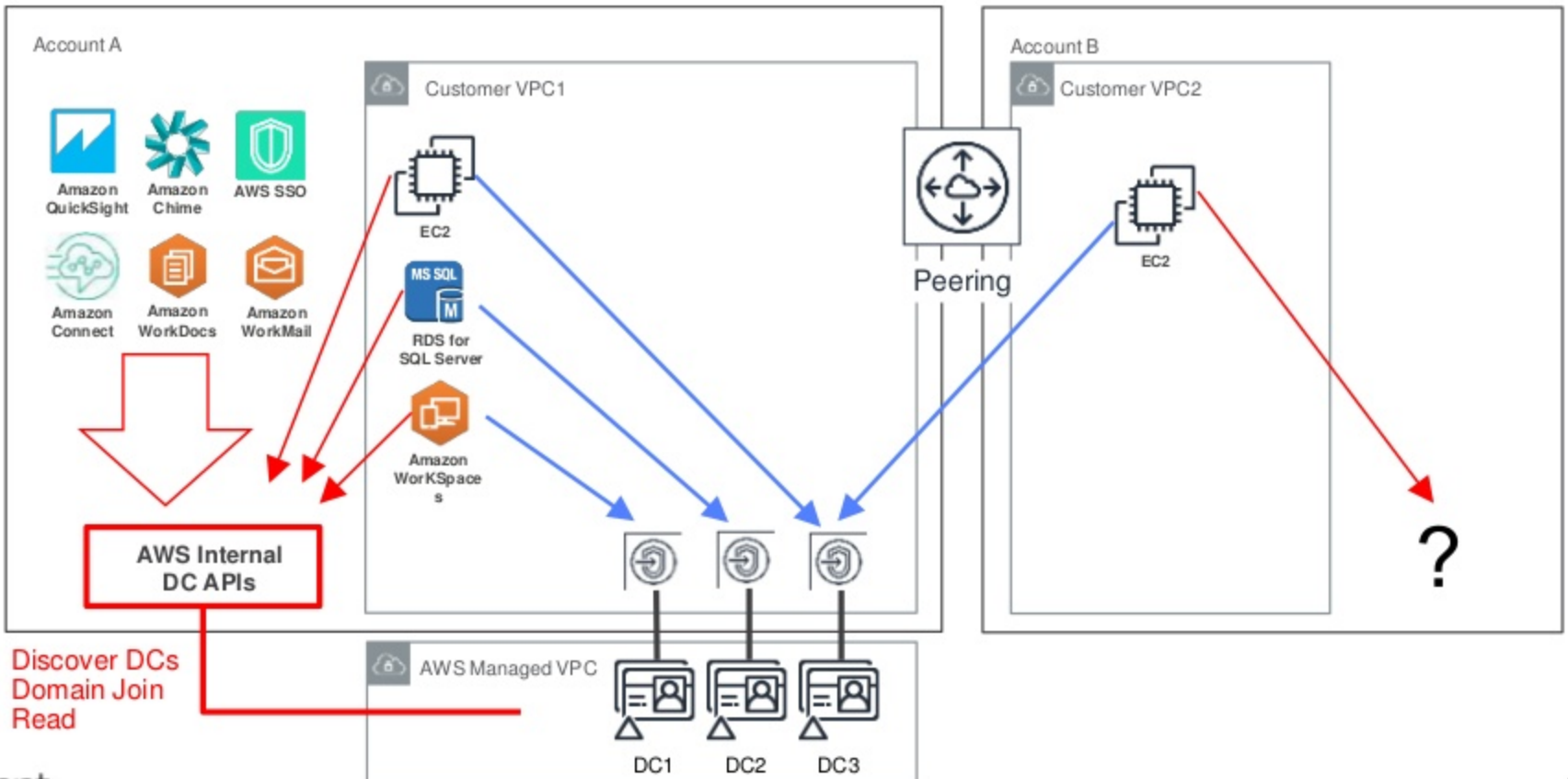
# Cross-account sharing



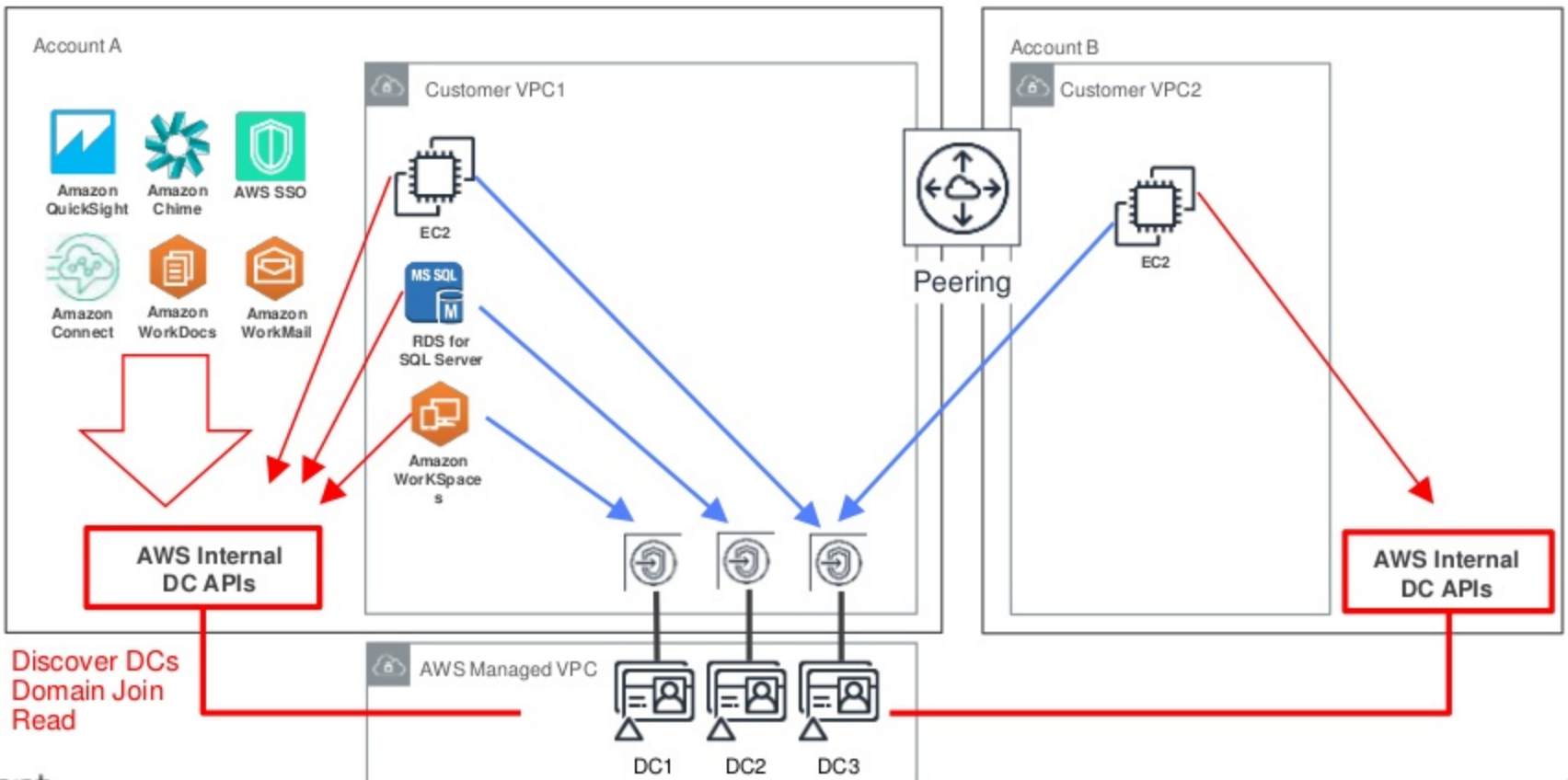
# Communication paths to AWS Managed Microsoft AD



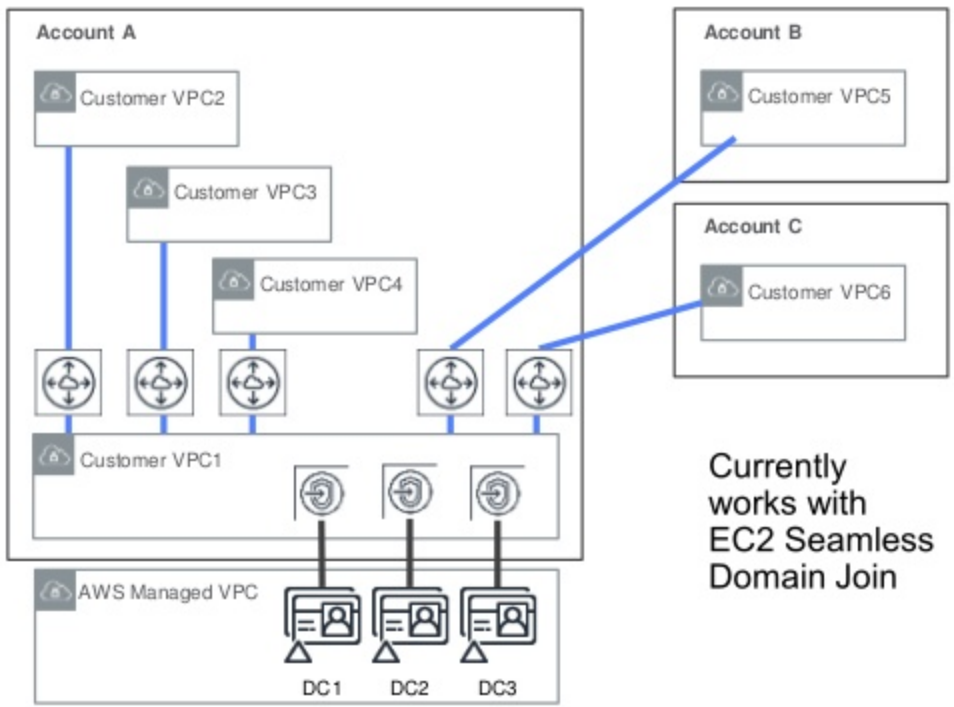
# Internal DC APIs inaccessible in other accounts



# Cross-account directory sharing



# Sharing across multiple VPCs and accounts




Currently works with EC2 Seamless Domain Join

## Sharing model

With accounts within an AWS Organization, no handshake

With accounts outside of AWS Organizations, handshake required

Charges to accounts to which directory is shared

Limited by route table entries

# Recap

- What  AWS Managed Microsoft AD is
- Key use cases
  - How applications use AWS Managed Microsoft AD
  - Deployment models (user vs. resource forest)
- How to install, administer, and configure
- Supported trust models
- Security event logging
- Directory sharing

# Reference information

Documentation

- AWS Directory Service—aws.amazon.com/directoryservice
- AWS Security Blog—aws.amazon.com/blogs/security/ (search for “AWS Managed Microsoft AD”)
- AWS What’s New—aws.amazon.com/new/ (Security, Identity & Compliance)
- AWS Managed Microsoft AD—aws.amazon.com/documentation/directory-service/
- RDS for SQL Server—aws.amazon.com/documentation/rds/

AWS Quick Starts— aws.amazon.com/quickstart/

- Active Directory Domain Services
- Exchange Server 2013
- SharePoint Server 2016 Enterprise
- Lync Server 2013
- SQL Server 2014 AlwaysOn
- Windows PowerShell DSC

Please complete the session survey in the mobile app.

# Thank you!

Thank you!