AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC206-R2

Integrating your workforce identity with AWS

Dennis Rothmel
Senior Product Manager, AWS Identity
AWS

Vladimir Provorov
Senior Solutions Architect, AWS Identity
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- AWS services for workforce identity
- AWS Managed Microsoft AD and integration
- Picking the right services
- Security best practices
- Using AWS Single Sign-On for managing access to applications

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS services for workforce identity



AWS Identity and Access Management (IAM)

- Create and manage AWS users and groups
- Use permissions to allow and deny access to AWS resources



AWS Directory Service

- Use managed Active Directory in the AWS Cloud
- Connect AWS applications to self-managed Active Directory



AWS SSO

- Centrally manage access to multiple AWS accounts and resources
- Single sign-on access to hundreds of business applications using SAML 2.0

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Managed Microsoft AD

Managed service for actual Active Directory

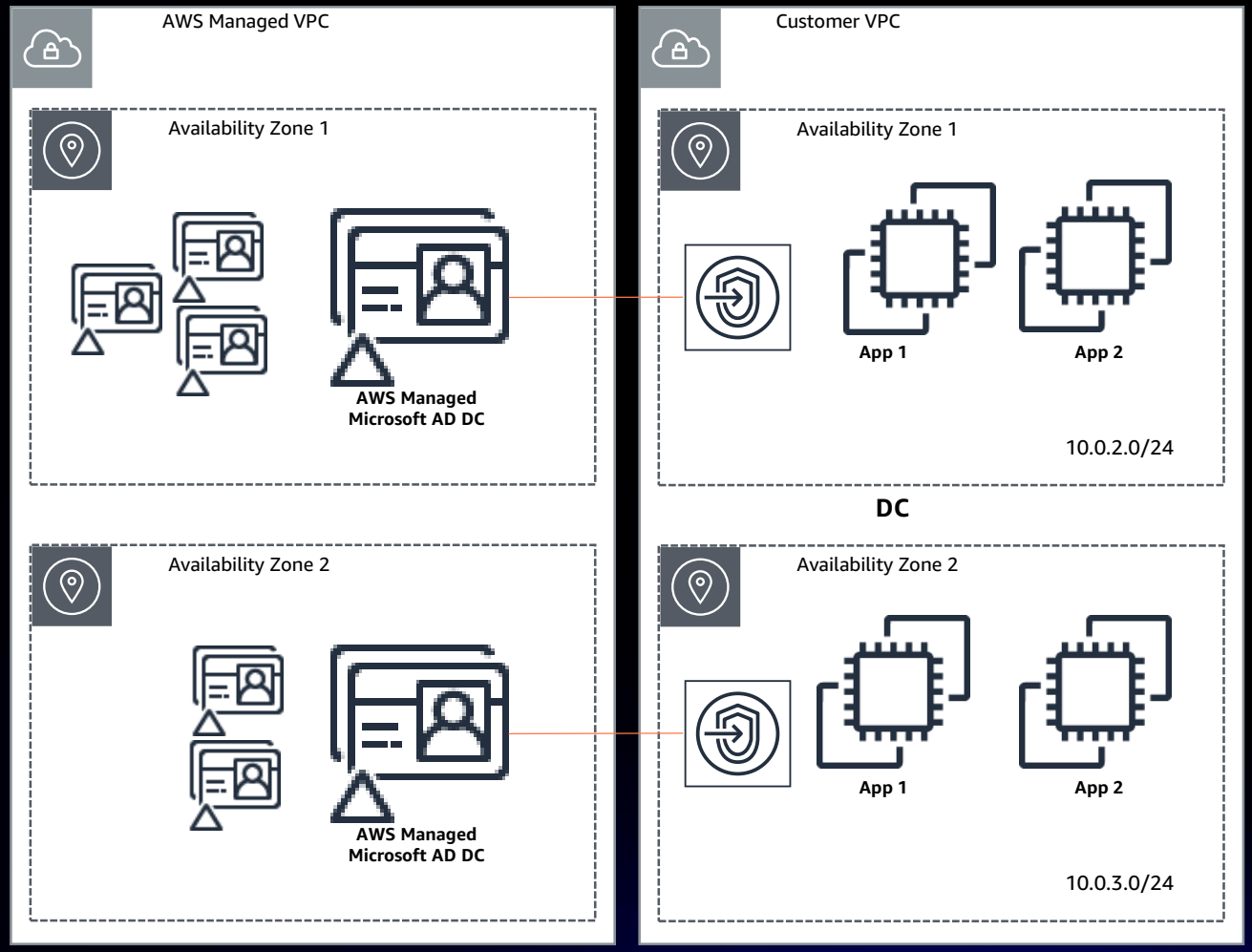
- Multi-AZ, multi-Region
- Supports PCI, HIPAA, SOC, and FedRAMP compliance standards

AWS responsibility

- Deployment
- Patch
- Monitor
- Snapshot/restore

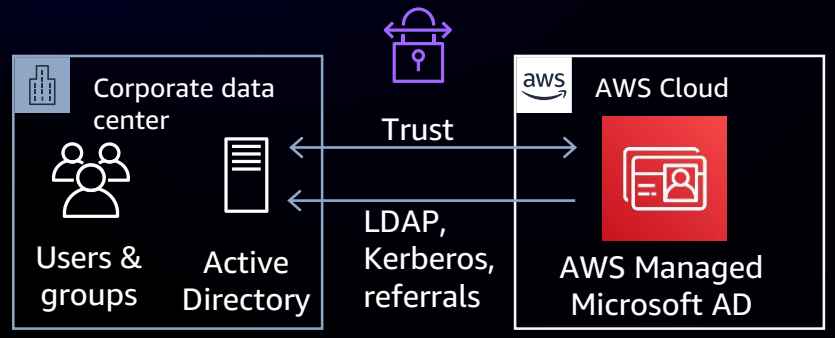
Customer responsibility

- Administer users, groups, GPOs, etc.
- Password policies
- Trust relationships

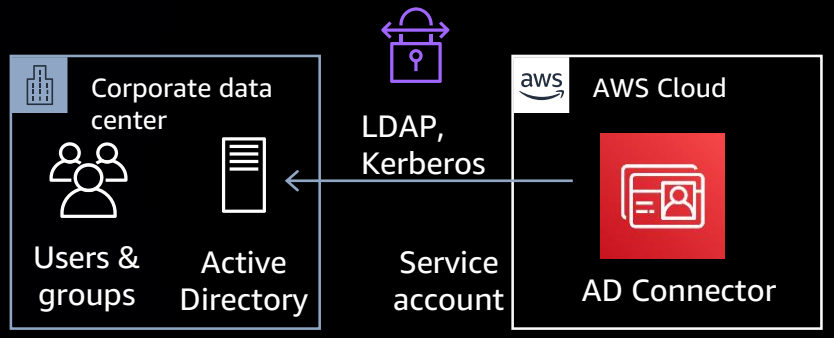


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

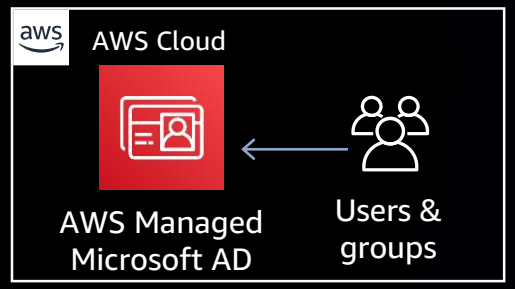
Establishing Active Directory in AWS



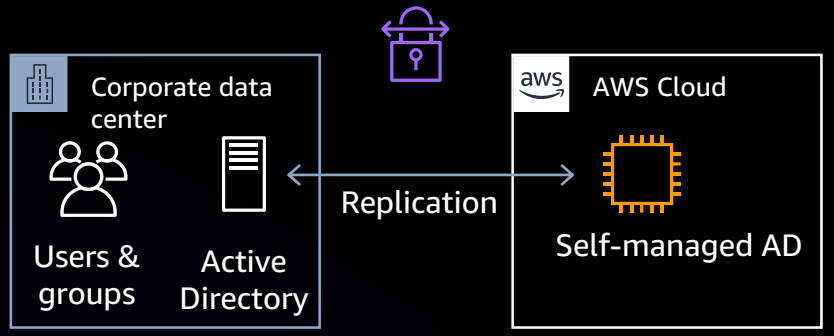
Option 1: AWS Managed Microsoft AD with trust



Option 2: AD Connector with service principal



Option 3: Stand-alone AWS Managed Microsoft AD

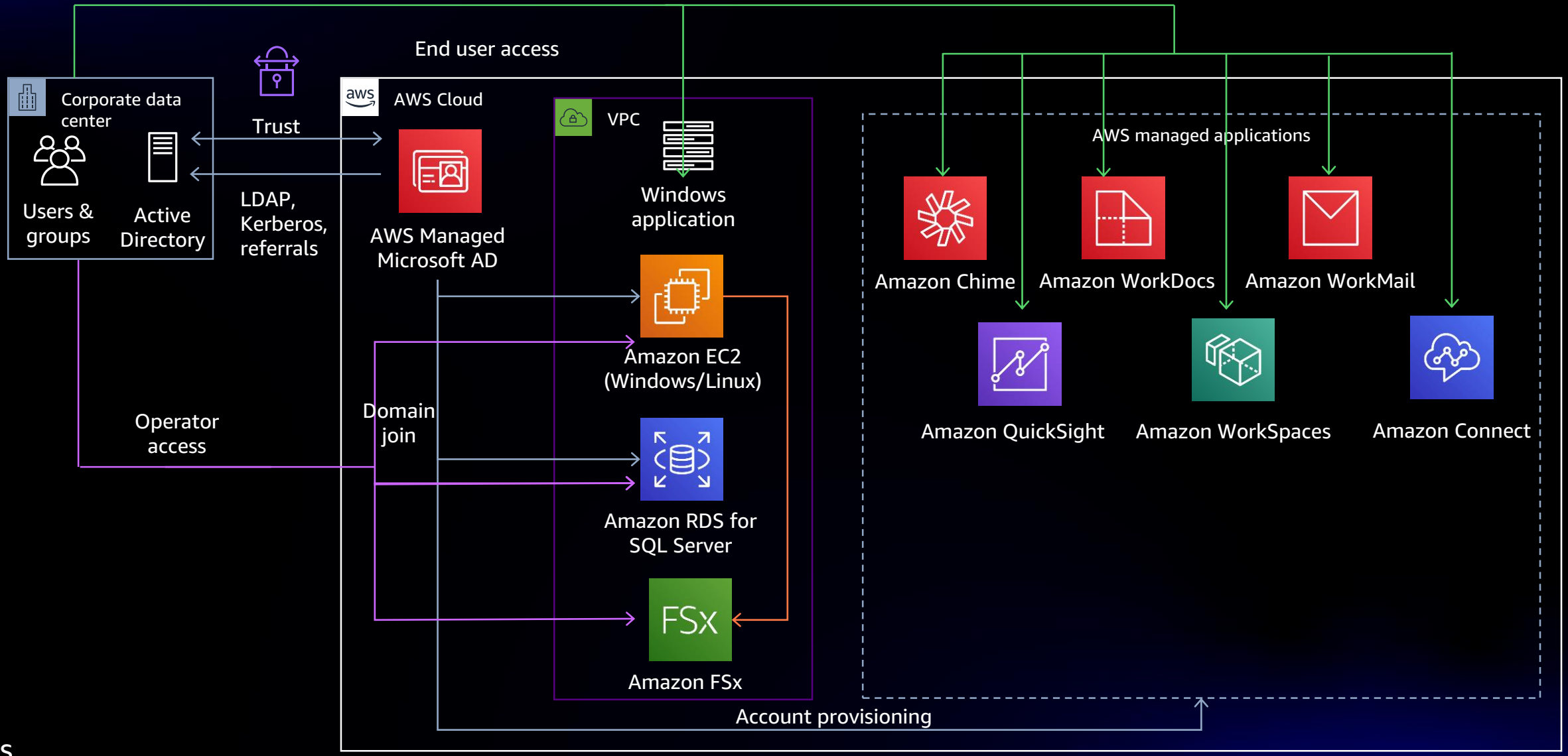


Option 4: AD on Amazon EC2 with replication

Option X: Combinations of the above

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Leveraging Active Directory in AWS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

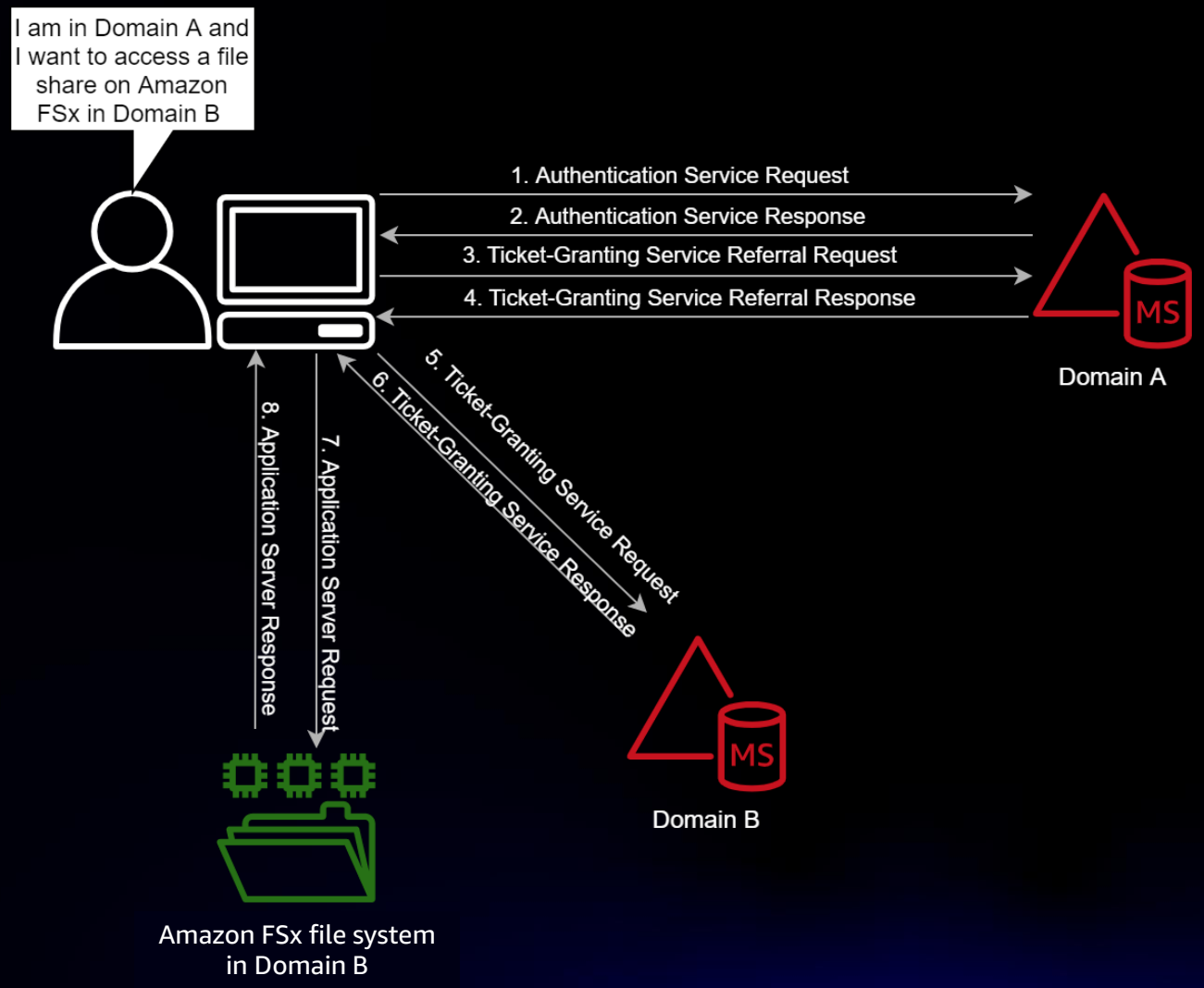
When is two-way trust required?

When your workload in AWS Managed Microsoft AD needs to access any service secured by your on-premises Active Directory

- Access from a server joined to AWS Managed Microsoft AD to on-premises resources (file shares, SQL databases, etc.)
- Apps requiring searching for AD objects and groups

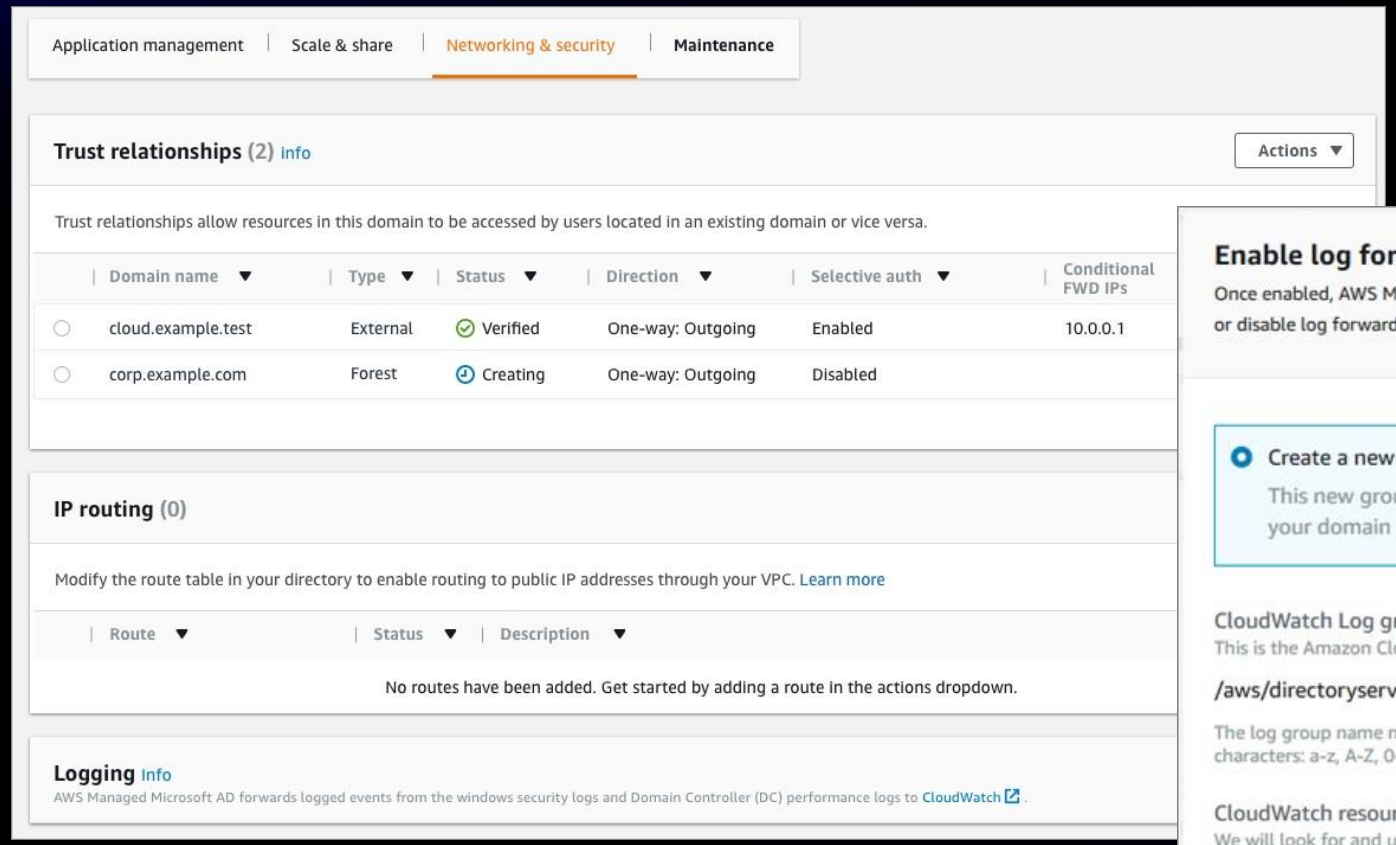
Typical use cases

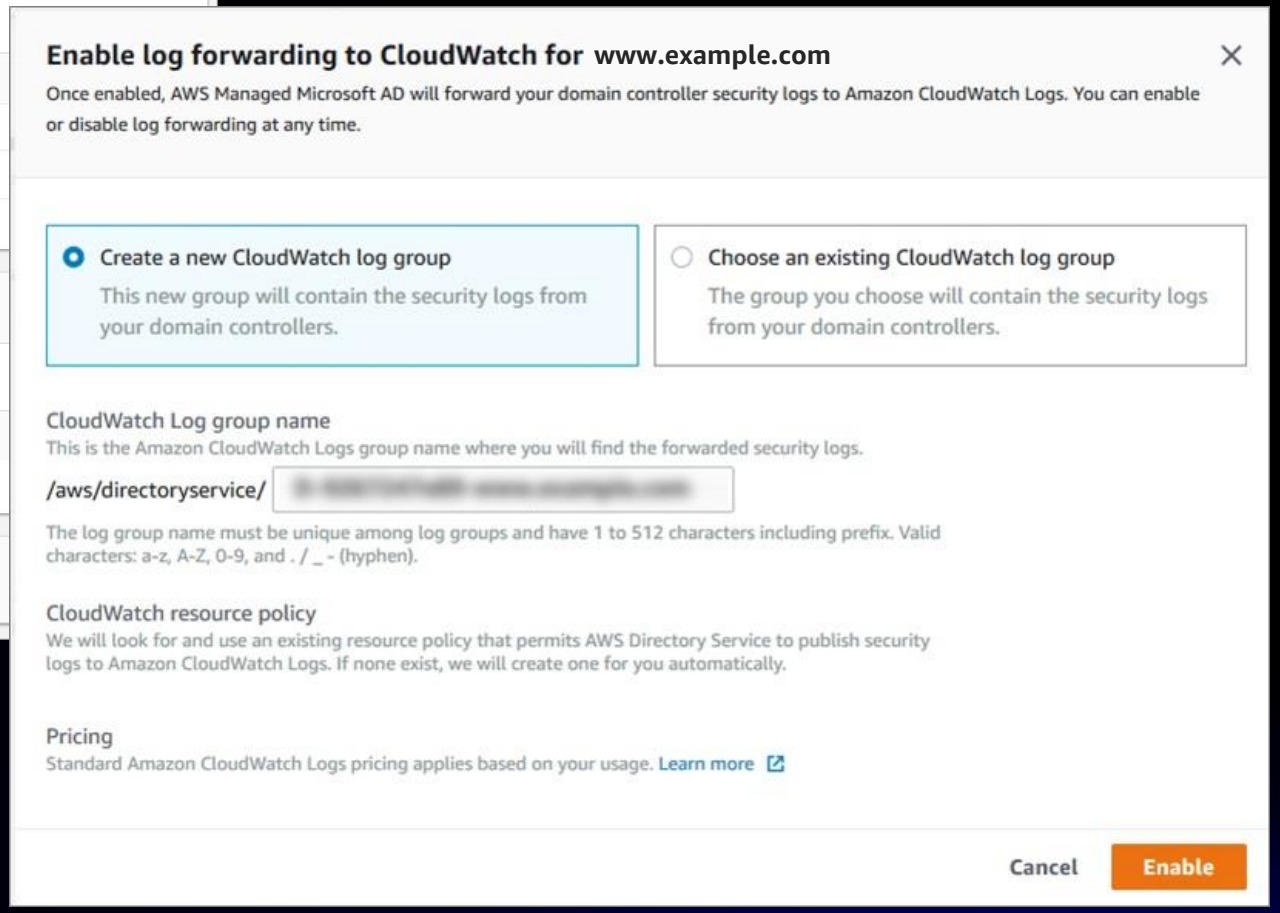
- Accessing Amazon RDS for SQL with on-premises AD credentials – one-way trust is sufficient
- Login to Amazon WorkSpaces deployed in AWS Managed Microsoft AD – one-way trust is sufficient
- Accessing on-premises file share from Amazon WorkSpaces joined to AWS Managed Microsoft AD – two-way trust is needed



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

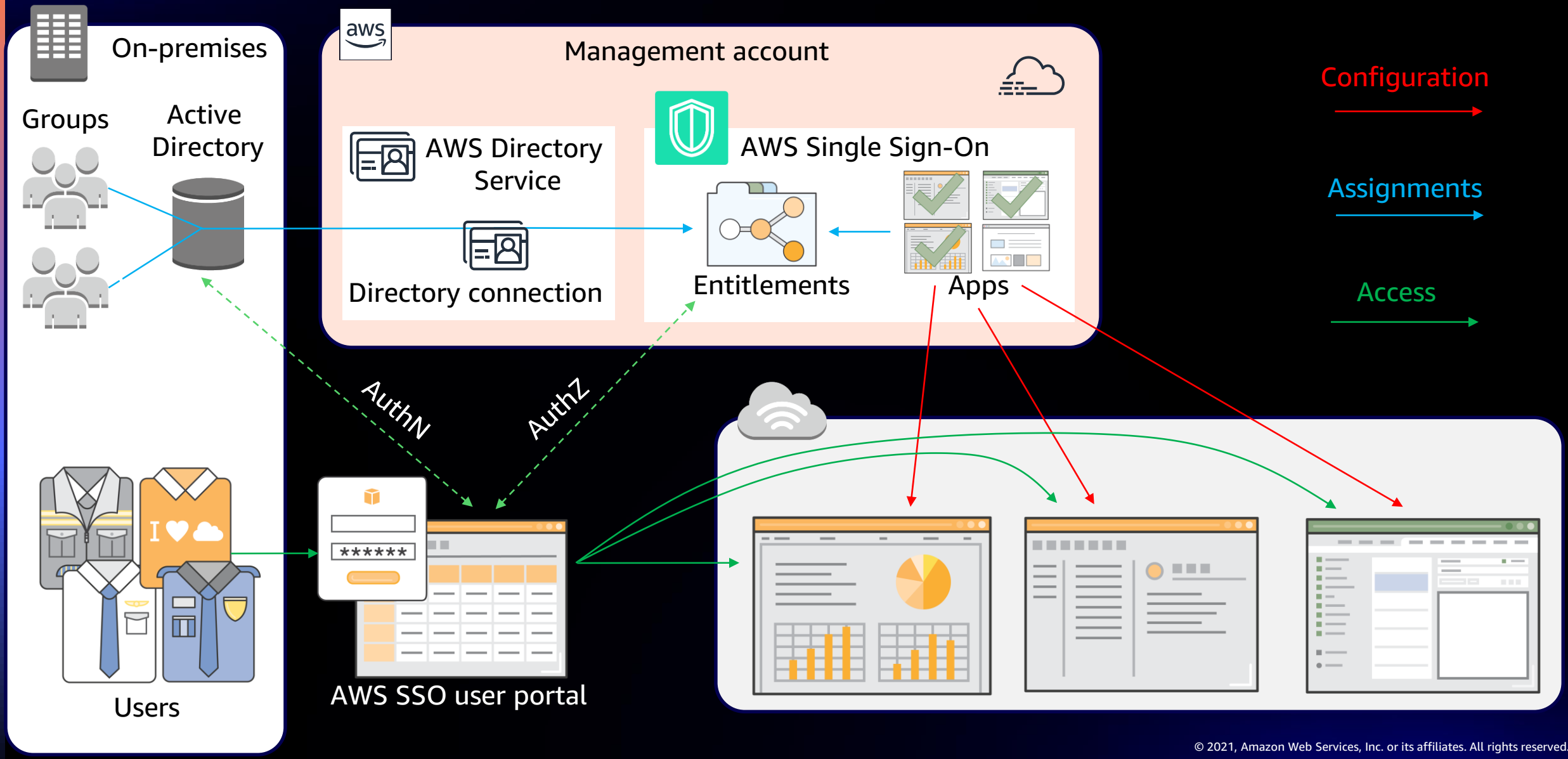
Security event logging to Amazon CloudWatch





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using AWS SSO for managing access to apps



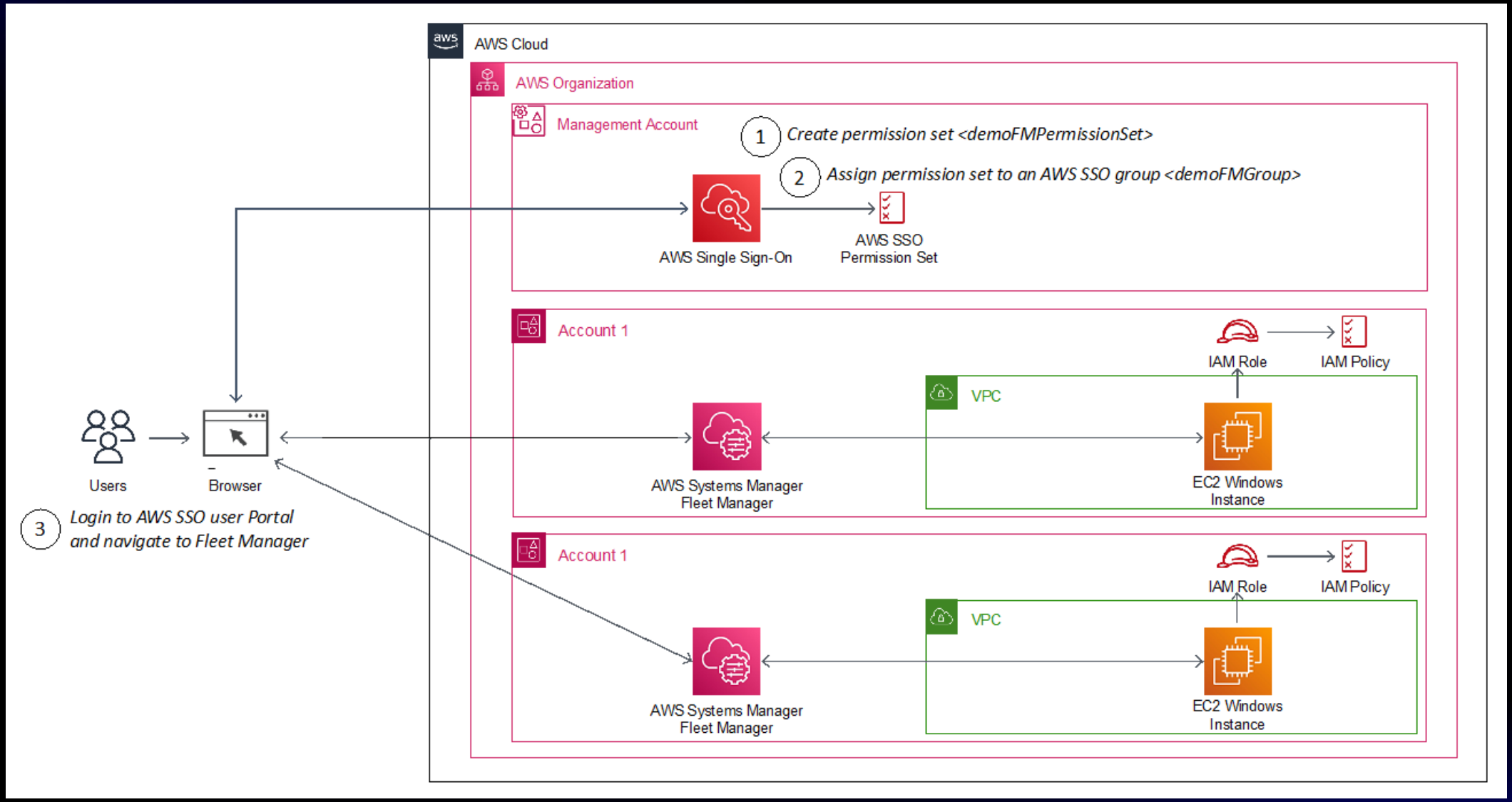
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Single sign-on to Amazon EC2 Windows instances

- New feature in AWS Single Sign-On and AWS Systems Manager Fleet Manager (released 11/29/2021)
- In-browser desktop session to Amazon EC2 Windows instance
- Supports single sign-on, Amazon EC2 key pairs, or username and password credentials
- No open ports, no bastion hosts required!
- Permissions managed with AWS Identity and Access Management (IAM)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Single sign-on to Amazon EC2 Windows instances



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional resources

AWS Directory Service
https://aws.amazon.com/directoryservice

AWS Managed Microsoft AD
https://aws.amazon.com/documentation/directory-service/

AWS Quick Start for Active Directory
https://aws.amazon.com/quickstart/architecture/active-directory-ds/

“AWS for Microsoft Workloads” on YouTube
https://www.youtube.com/playlist?list=PLhr1KZpdzukdJllxulUM7pMB7aJ2_FfTP

“Active Directory Doman Services on AWS” whitepaper
https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf

“AWS Hybrid DNS with Active Directory” whitepaper
https://d1.awsstatic.com/whitepapers/aws-hybrid-dns-with-active-directory.pdf

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.