
AWS
re:Inforce
JULY 26 – 27, 2022 | BOSTON, MA

IAM203

Deploy and secure Active Directory with AWS Managed Microsoft AD

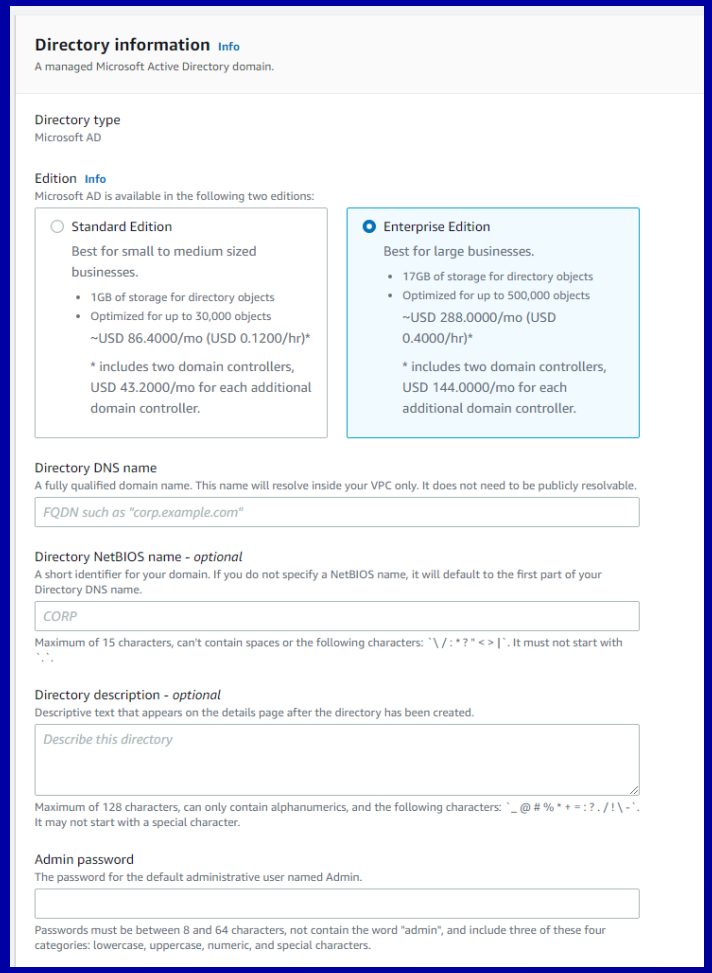
Dennis Rothmel (he/him)
Sr. Product Manager
AWS

Jeremy Girven (he/him)
Solutions Architect
AWS

Some backstory

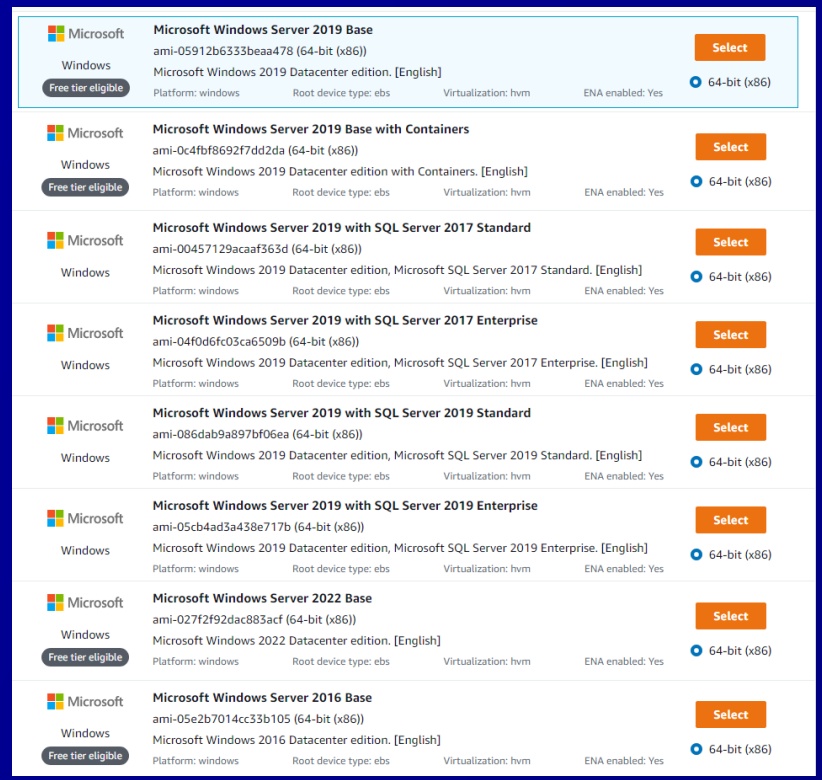
2000

Some backstory



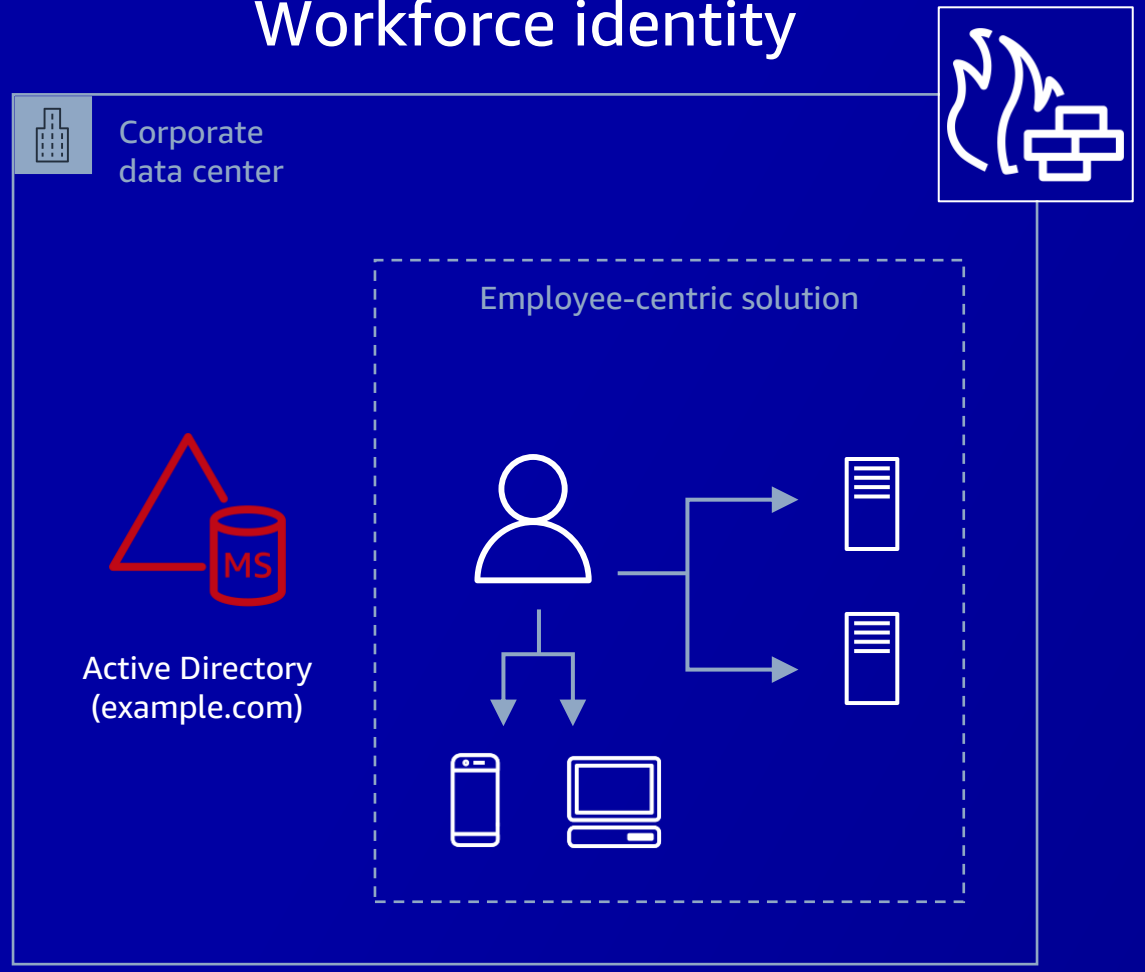
2022

OR

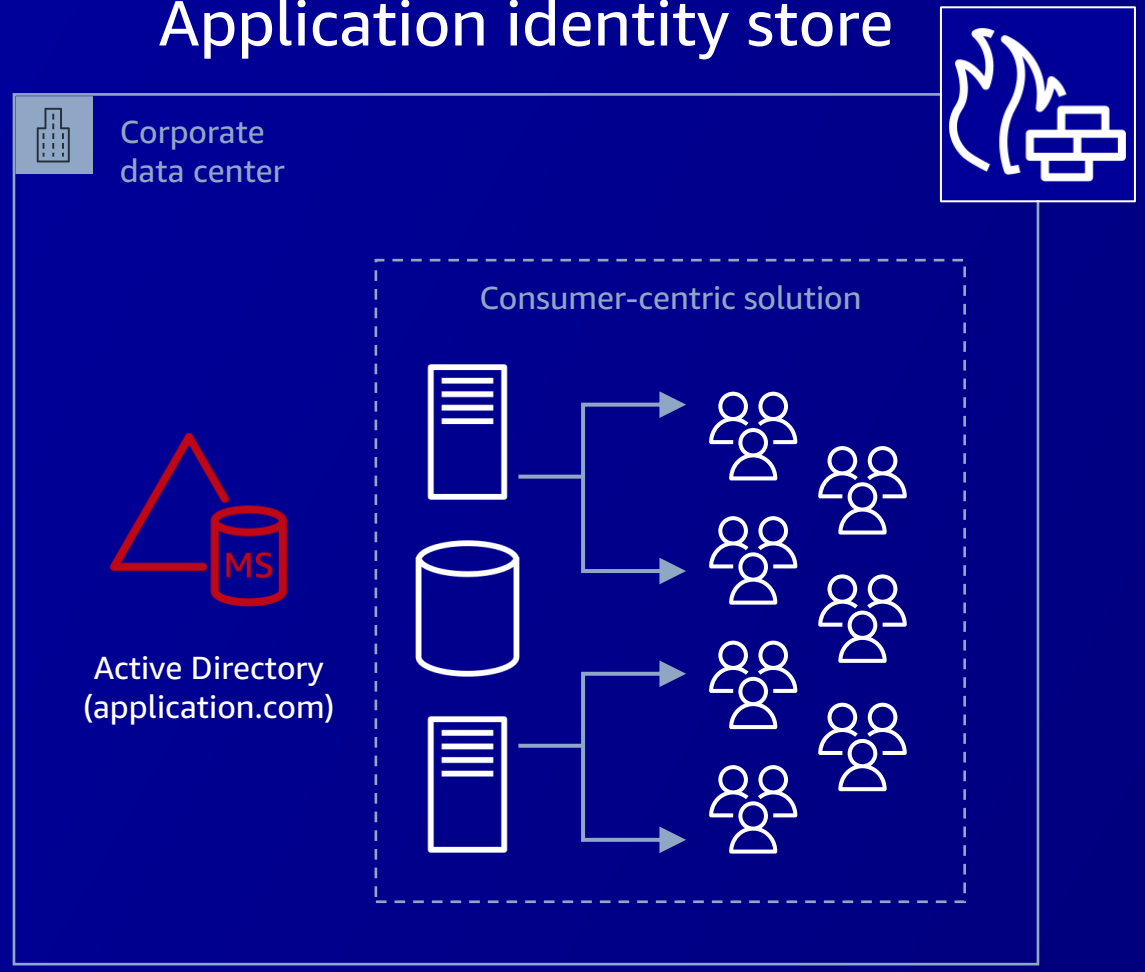


AD use cases

Workforce identity



Application identity store



So . . . why should I move?

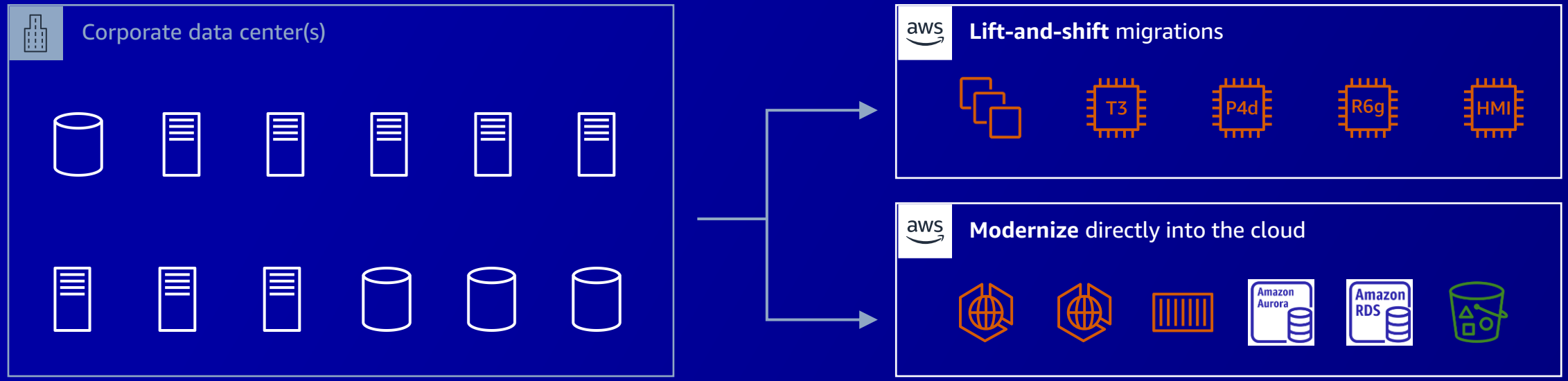
Migration and modernization driven by

Technology and security

- Enable work from anywhere
- Identity as the new security perimeter

Business agility and innovation

- Grow faster and save costs
- Innovate with new tools/capabilities



AWS Directory Service

AD Connector

Directory gateway that can redirect requests to your on-premises Active Directory without caching any information in the cloud

- Bring AD accounts to AWS services
- Hosted in AWS
- Connects to on-premises AD
- 1 Connector, 1 Active Directory

AWS Managed Microsoft AD

Fully managed service providing a new Active Directory domain in AWS to host your users and groups and support your AD-dependent apps

- Standalone as-a-service AD domain
- Integrates with AWS applications and services
- Connects to on-premises AD
- Automated operations provided by AWS

AWS Managed Microsoft AD

Managed service for Windows Active Directory

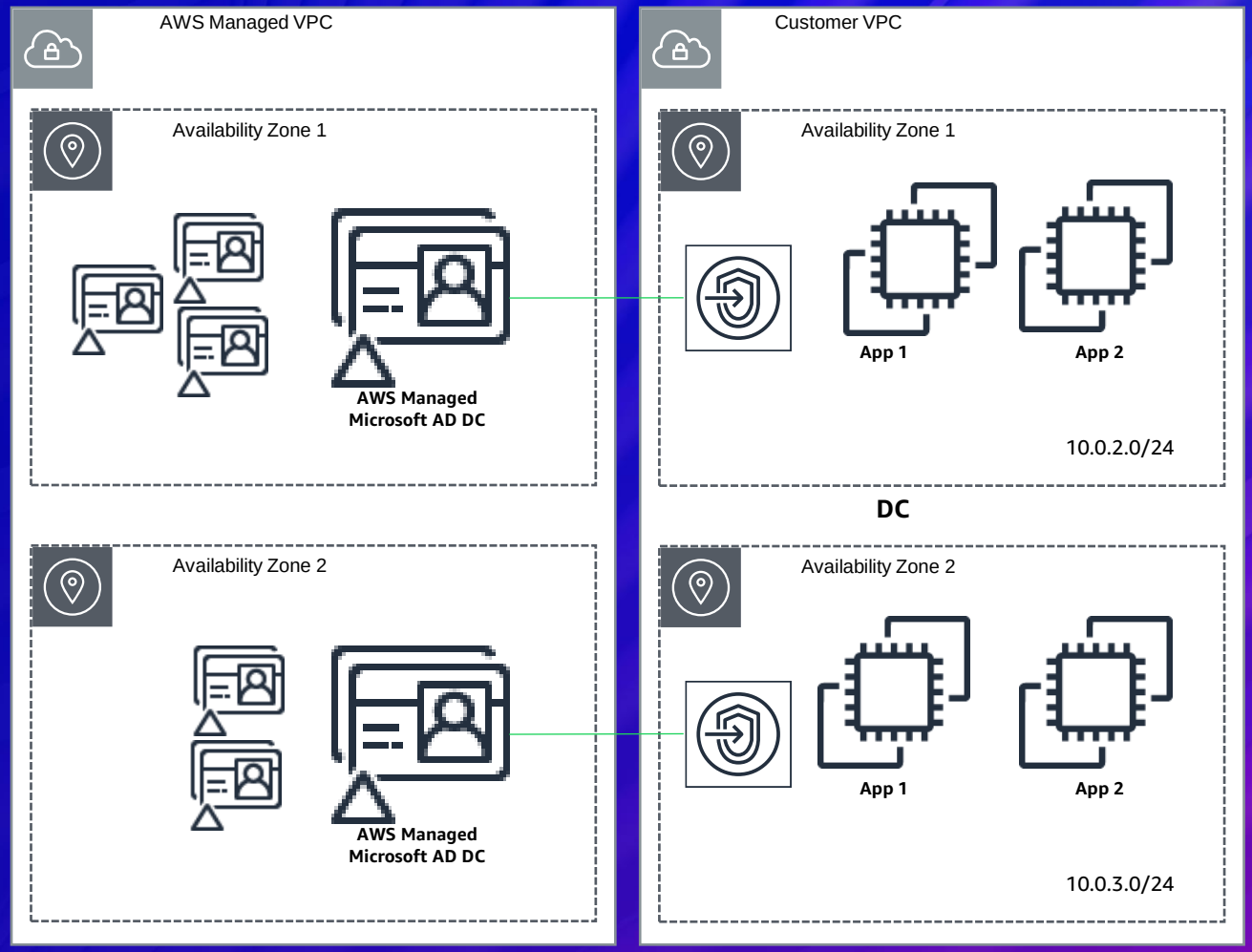
- Single tenant domain (single forest, single domain)
- Multi-AZ, multi-region
- Default 2x domain controllers, can scale out per Region
- Compliances: PCI, HIPAA-eligible, SOC, FedRAMP

AWS responsibility

- Deployment
- Patch
- Monitor
- Snapshot/Restore

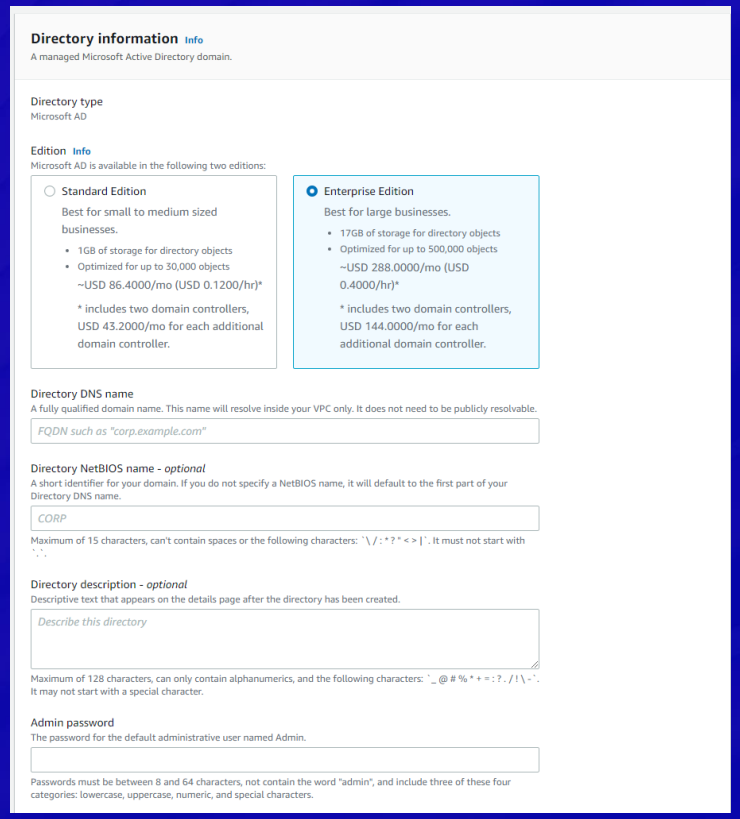
Customer responsibility

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



What are my deployment options?

1) Console deployment



2) AWS CloudFormation/Terraform/AWS CDK

Create an AWS Managed Microsoft AD

JSON

```
"myDirectory" : {
  "Type" : "AWS::DirectoryService::MicrosoftAD",
  "Properties" : {
    "Name" : "corp.example.com",
    "Password" : { "Ref" : "MicrosoftADPW" },
    "ShortName" : { "Ref" : "MicrosoftADShortName" },
    "VpcSettings" : {
      "SubnetIds" : [ { "Ref" : "subnetID1" }, { "Ref" : "subnetID2" } ],
      "VpcId" : { "Ref" : "vpcID" }
    }
  }
}
```

YAML

```
myDirectory:
  Type: AWS::DirectoryService::MicrosoftAD
  Properties:
    Name: "corp.example.com"
    Password:
      Ref: MicrosoftADPW
    ShortName:
      Ref: MicrosoftADShortName
    VpcSettings:
      SubnetIds:
        - Ref: subnetID1
        - Ref: subnetID2
      VpcId:
        Ref: vpcID
```

Required information

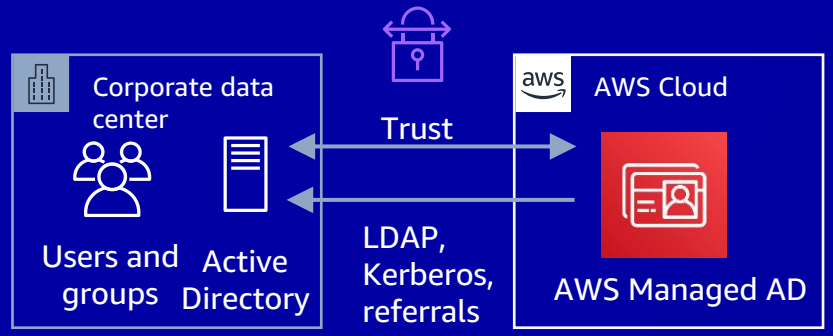
1. Select an Edition
2. Provide a DNS name
3. Set the admin account password
4. Select a VPC and two subnets (in different Availability Zones)

That's it! You're good to go!

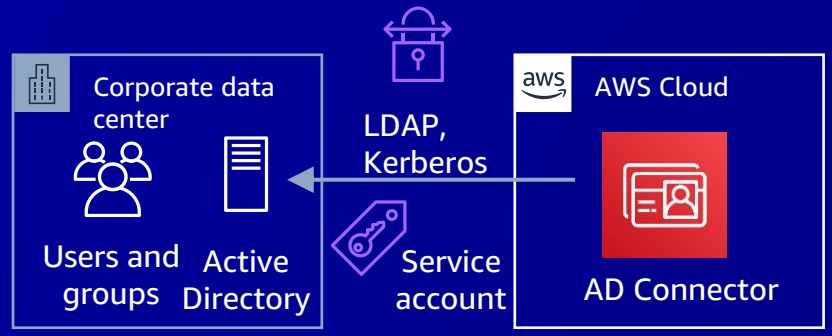
3) Command line interface

```
aws ds create-microsoft-ad --name example.com --password ExamplePassword
--vpc-settings VpcId=abc12345,SubnetIds=abc12345,def67890
```

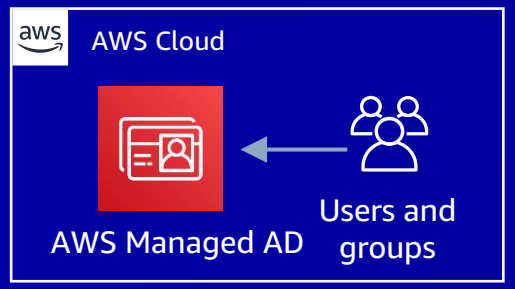
AWS Managed Microsoft AD patterns



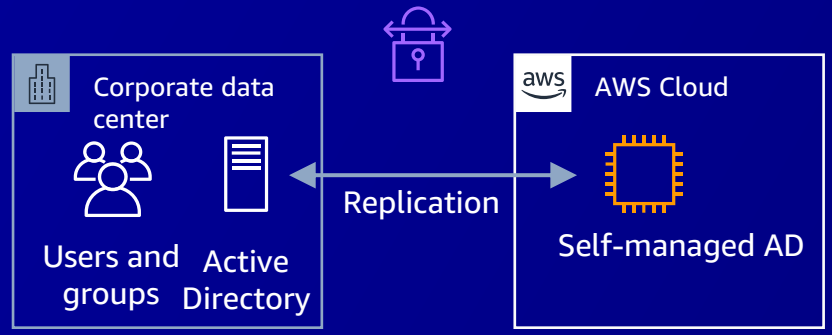
Option 1: AWS Managed AD with trust



Option 2: AD Connector with service principal



Option 3: Standalone AWS Managed AD



Option 4: AD on Amazon EC2 with replication

Option X: Combinations of the above

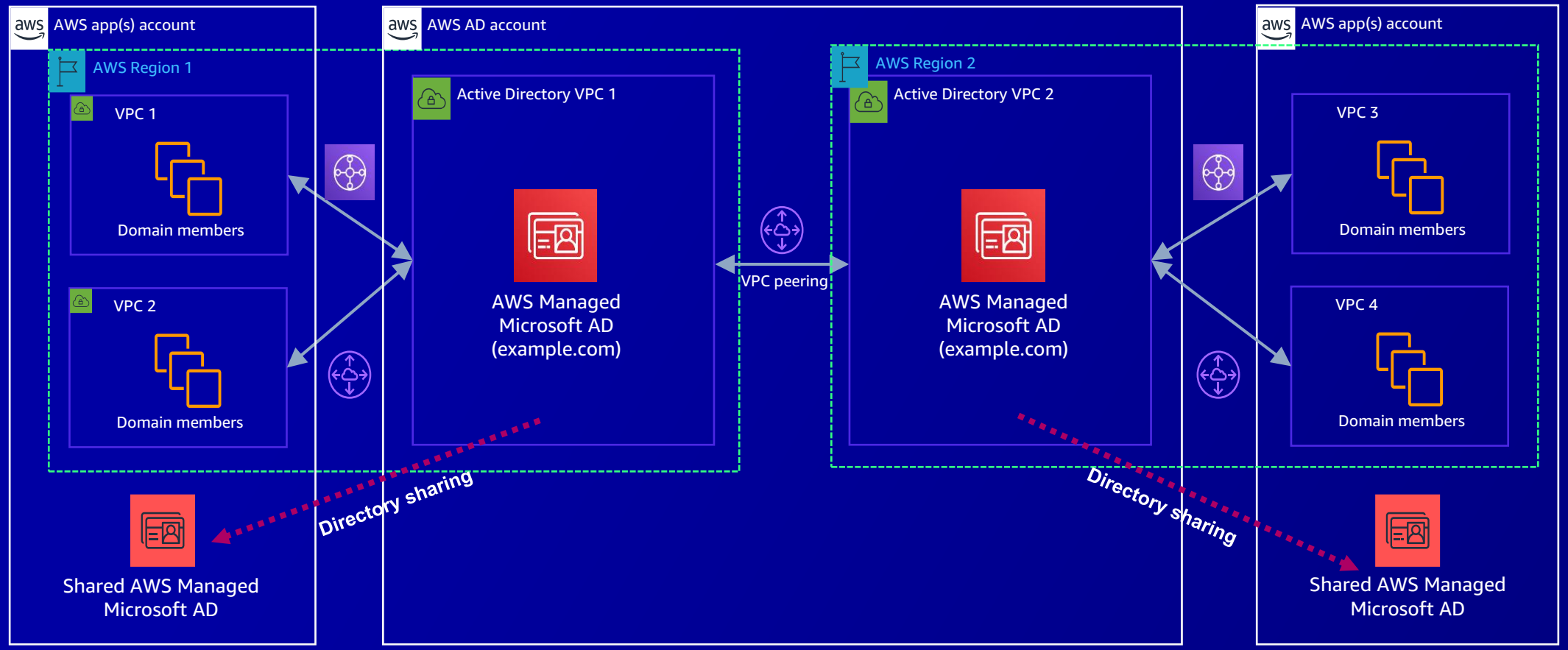
AWS Managed Microsoft AD multi-Region

- Available for **Enterprise Edition** directories
- Deploys domain controllers in Region, scale out per Region
- All replication occurs on the AWS service's VPC
- Change notification is enabled on all site links
- Flexible Single Master Operation (FSMO) roles are located in the primary Region

AWS Managed Microsoft AD sharing

- A single directory, multiple AWS accounts, no additional infrastructure
- Share within your AWS organization or any AWS account (via handshake)
- “Virtual” directory ID links shared accounts to original directory
- Network connectivity between origin VPC and shared account resource VPC
- Directory shares are per Region, keeping network traffic localized

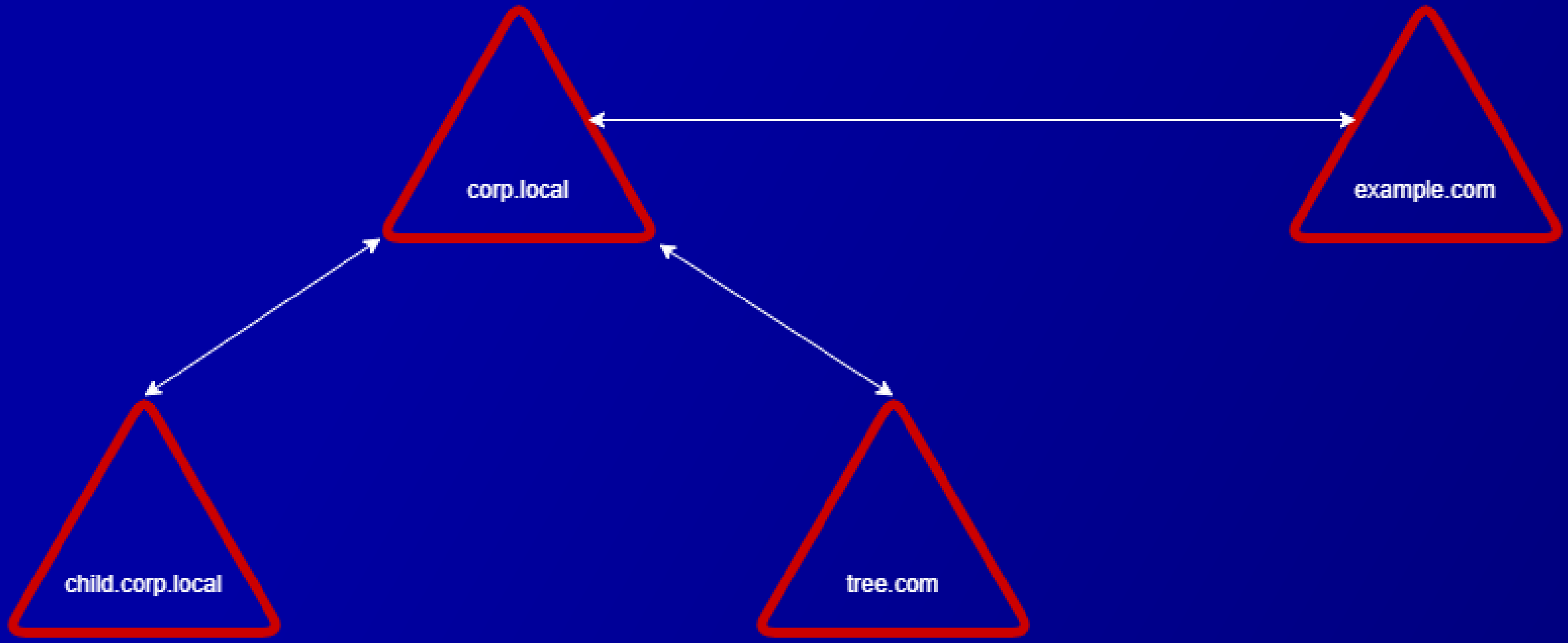
Multi-Region and directory sharing



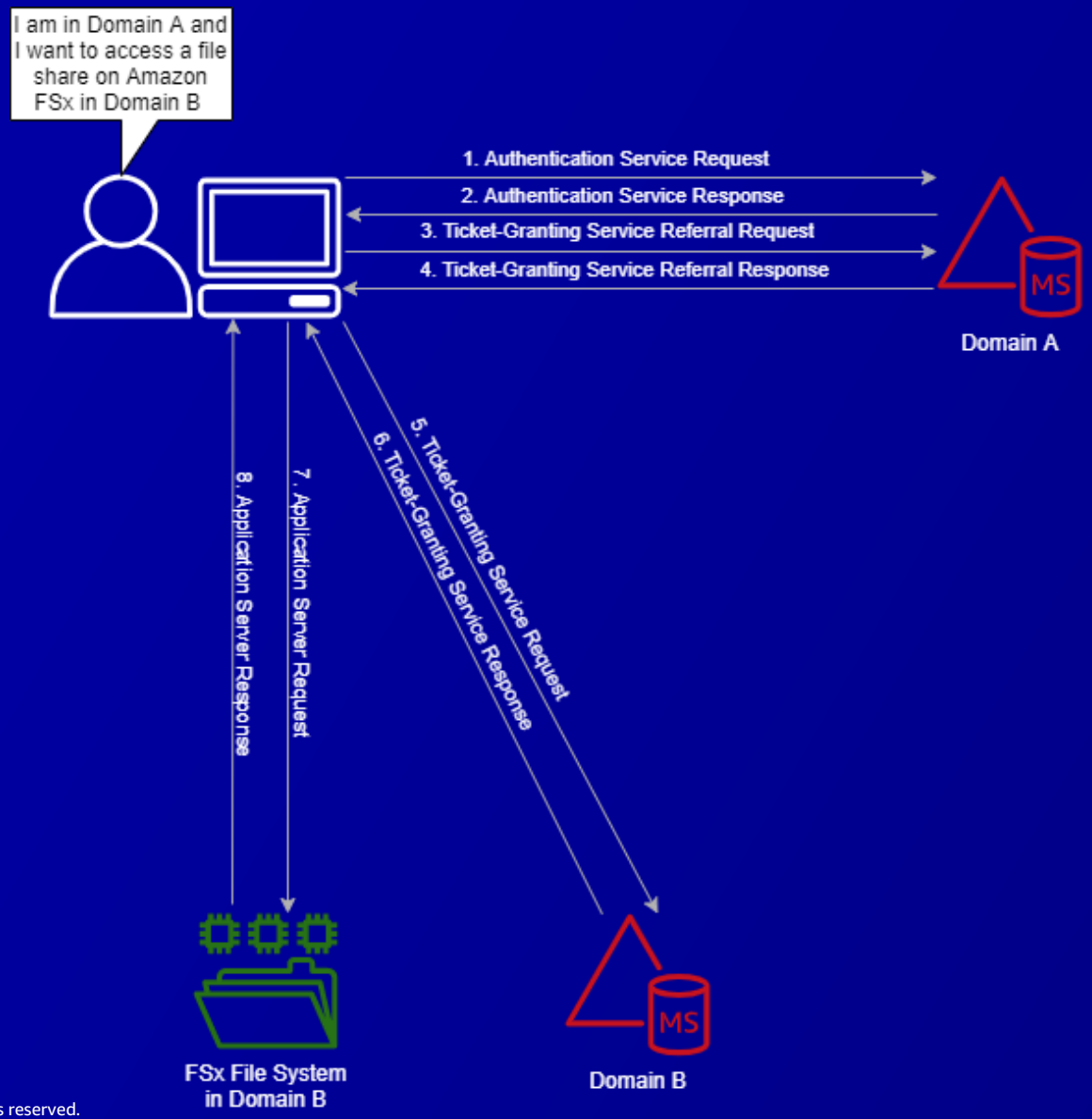
AWS Managed Microsoft AD trust types

Type	Direction	Transitivity	Auth type	MAD sup
Forest	One- or two-way	Transitive	Kerberos V5 or NTLM	☑
External	One- or two-way	Nontransitive	NTLM	☑
Realm	One- or two-way	Transitive or nontransitive	Kerberos V5	

AWS Managed Microsoft AD trust transitivity



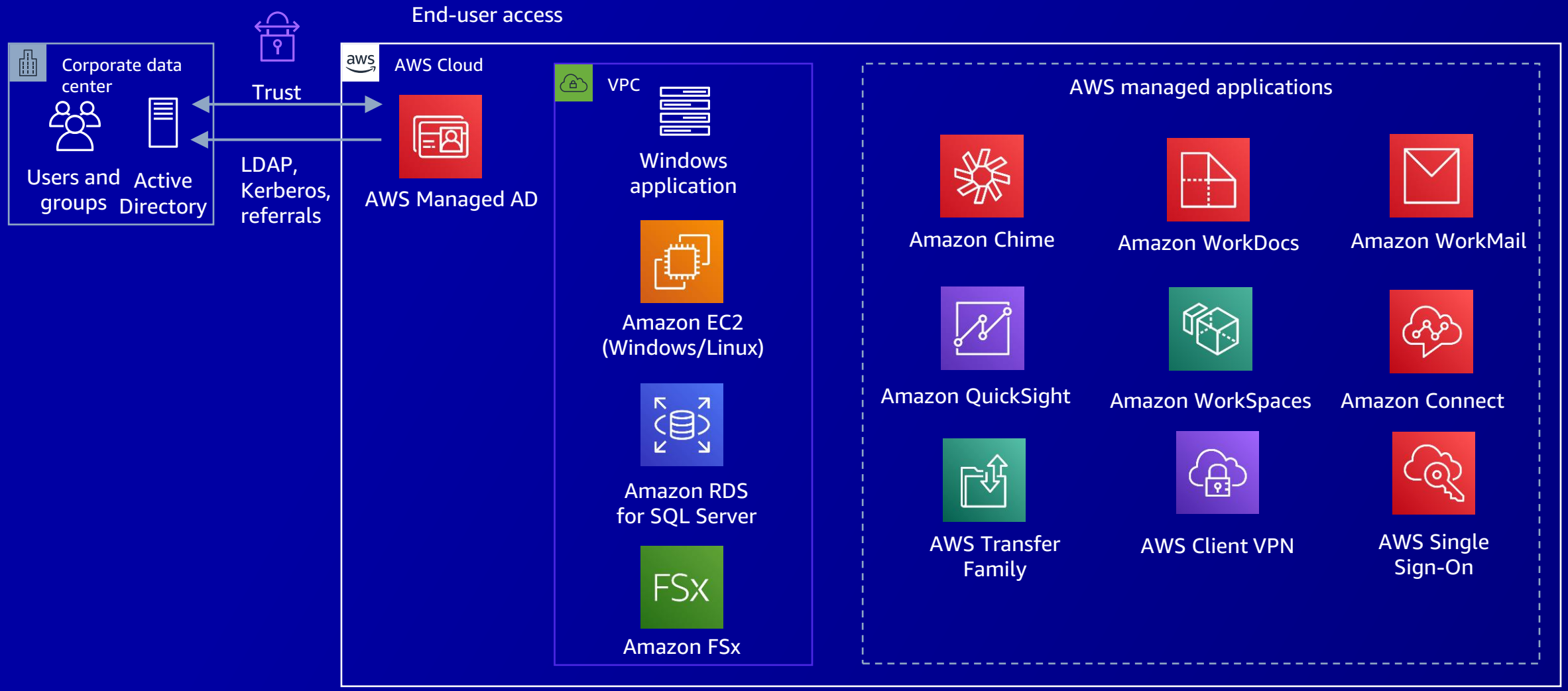
AWS Managed Microsoft AD trust Kerberos



AWS Managed Microsoft AD trust myths

Myth	Fact
Trusts synchronize objects between each domain	False: the only object synchronized is the trust password
Trusts by default are inherently insecure	False: trusts in of themselves are not secure
My password is passed over the trust when authenticating	False: passwords are not passed across the trusts
A one-way trust allows bidirectional authentication	False: a one-way trust is only one-way
When a trust is created, users in the trusted domain are granted permissions to trusting domain	False: permissions are not granted; all write operations must be delegated

AWS Managed Microsoft AD app integration



AWS Managed Microsoft AD app integration

- Amazon AppStream 2.0
- Amazon Aurora MySQL
- Amazon Aurora PostgreSQL
- Amazon Chime
- Amazon Connect
- Amazon EC2 Seamless Domain Join
- Amazon FSx for NetApp ONTAP
- Amazon FSx for Windows File Server
- Amazon MQ
- Amazon QuickSight
- Amazon RDS Custom
- Amazon RDS for MariaDB
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- Amazon WorkSpaces Application Manager
- AWS Client VPN
- AWS Management Console
- AWS Single Sign-On
- AWS Transfer Family

AWS Managed Microsoft AD app integration

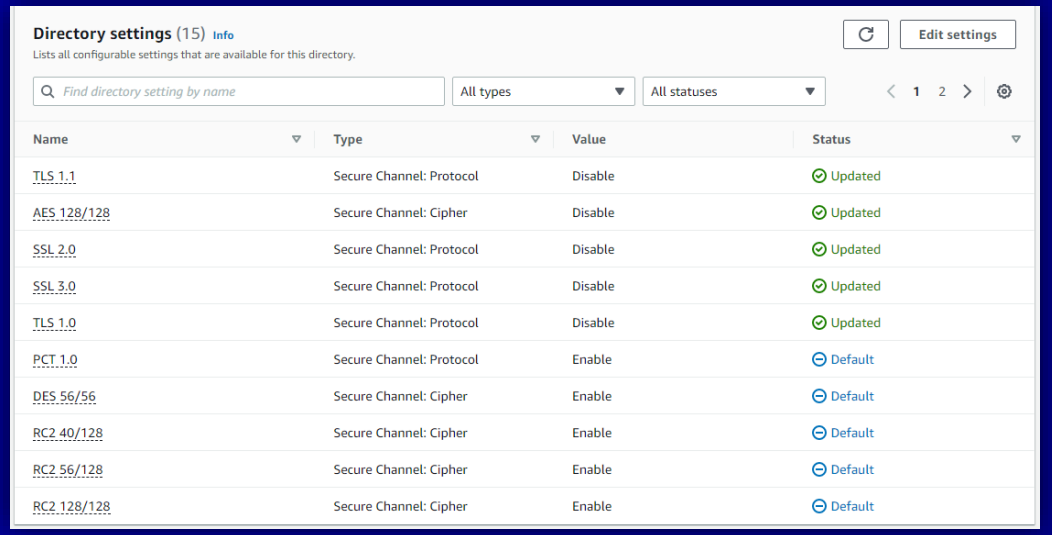
- Most applications without enterprise or domain admin rights requirements
- Microsoft ADFS
- Microsoft PKI
- Microsoft SharePoint
- Microsoft SQL
- Microsoft System Center Suite

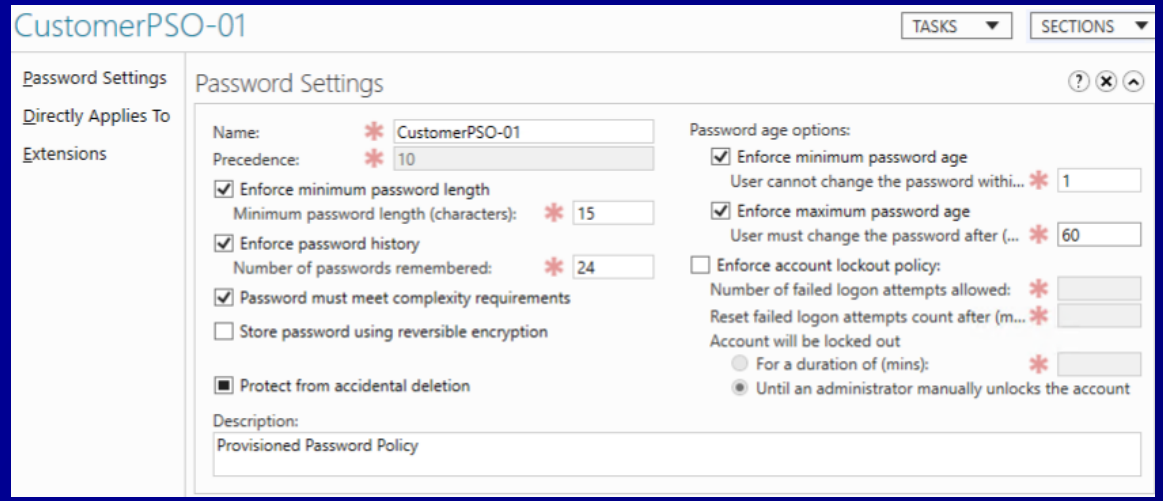
AWS Managed Microsoft AD: Monitoring

- Log forwarding Windows Security event logs to Amazon CloudWatch Logs
  - IAM352-R1/R2 – Anomaly detection and security insights with AWS Managed Microsoft AD
- Amazon Simple Notification Service (Amazon SNS) for status changes
- Logging AWS Directory Service API calls with AWS CloudTrail
- Additional logs available via Microsoft Management Console (MMC)

AWS Managed Microsoft AD security

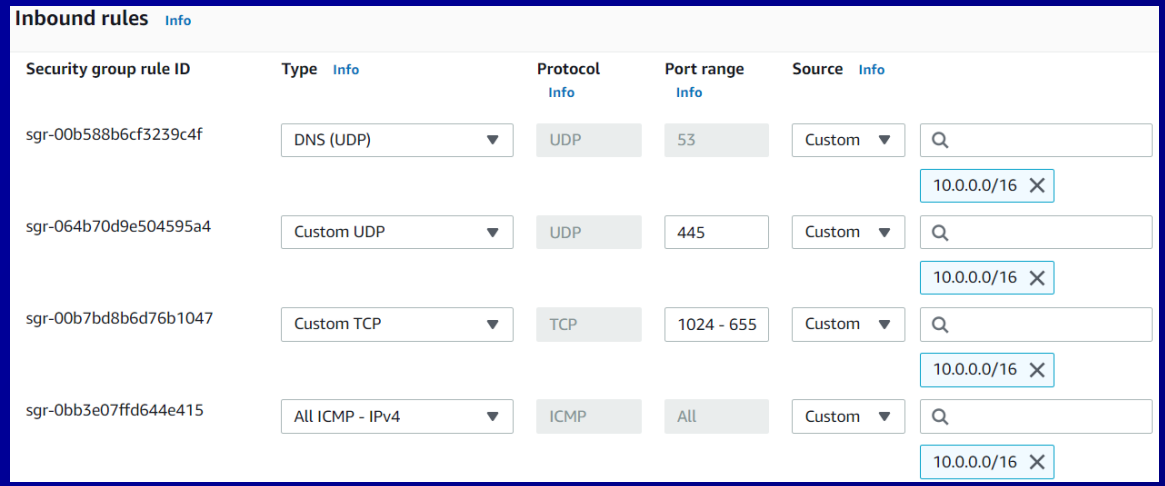
- **New:** Disable legacy network protocols and ciphers
- Remove domain admin and enterprise admin access
- Treat the built-in admin as a break glass account
- Use Managed Service Accounts whenever possible
- Implement restrictive fine-grained password policies for users and service accounts
  - 15 or more characters is recommended





AWS Managed Microsoft AD security

- Use the minimum required trust type
- Implement LDAP over SSL to encrypt LDAP communications
- Implement multifactor authentication for additional layer of security
- Use more restrictive VPC security groups to minimize access to domain controllers
- Plan AWS account placement of AD resources



AWS Managed Microsoft AD – Recap

- Flexible deployment patterns
- Versatile deployment options
- Simple and automated operations
- Secure application and service integrations
- Trust relationships myths dispelled
- Recommended security practices

Additional resources

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

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

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

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

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

- Everything you wanted to know about trusts with AWS Managed Microsoft AD
- https://aws.amazon.com/blogs/security/everything-you-wanted-to-know-about-trusts-with-aws-managed-microsoft-ad/

Thank you!

Dennis Rothmel
@AWSRothmel

Jeremy Girven
girvenj@amazon.com