

The background of the image is a vibrant blue with a complex, abstract pattern of overlapping, curved lines that create a sense of depth and movement. The lines are in various shades of blue and purple, with some areas appearing more saturated than others. The overall effect is a dynamic, almost architectural feel.

AWS re:Inforce

JULY 26 – 27, 2022 | BOSTON, MA

I AM 203

Deploy and secure Active Directory with AWS Managed Microsoft AD

Dennis Rothmel (he/him)

Sr. Product Manager
AWS

Jeremy Girven (he/him)

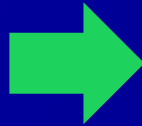
Solutions Architect
AWS



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Some backstory

2000



Some backstory

2022

OR

Directory information [Info](#)

A managed Microsoft Active Directory domain.

Directory type

Microsoft AD

Edition [Info](#)

Microsoft AD is available in the following two editions:

☐ Standard Edition

Best for small to medium sized businesses.

- 1GB of storage for directory objects
- Optimized for up to 30,000 objects

~USD 86.4000/mo (USD 0.1200/hr)*

* includes two domain controllers, USD 43.2000/mo for each additional domain controller.

☒ Enterprise Edition

Best for large businesses.

- 17GB of storage for directory objects
- Optimized for up to 500,000 objects

~USD 288.0000/mo (USD 0.4000/hr)*

* includes two domain controllers, USD 144.0000/mo for each additional domain controller.

Directory DNS name

A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

FQDN such as "corp.example.com"

Directory NetBIOS name - optional

A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.

CORP

Maximum of 15 characters, can't contain spaces or the following characters: ` \ / : * ? " < > | ` . It must not start with ` .` .

Directory description - optional

Descriptive text that appears on the details page after the directory has been created.









Describe this directory

Maximum of 128 characters, can only contain alphanumerics, and the following characters: ` _ @ # % * + = : ? . / ! \ - ` . It may not start with a special character.

Admin password

The password for the default administrative user named Admin.

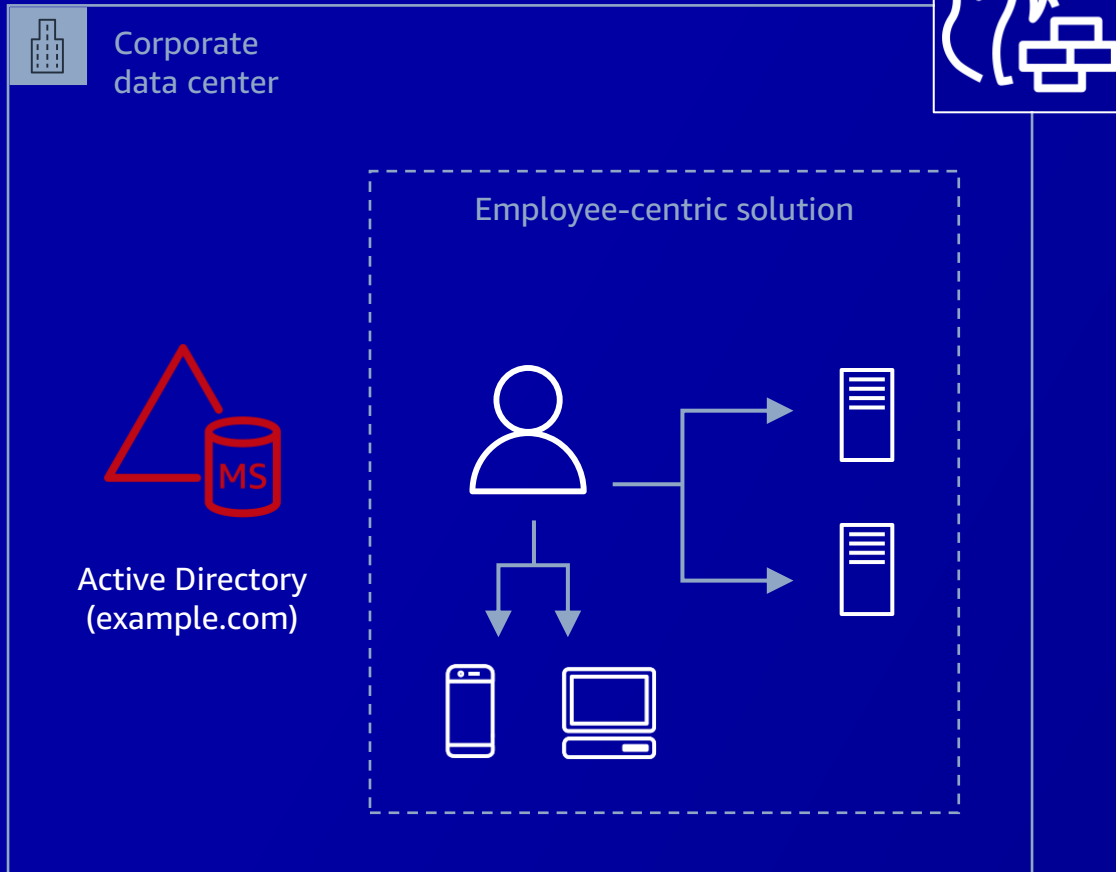
Passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.

	Microsoft Windows Server 2019 Base ami-05912b6333beaa478 (64-bit (x86)) Microsoft Windows 2019 Datacenter edition. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2019 Base with Containers ami-0c4fbf8692f7dd2da (64-bit (x86)) Microsoft Windows 2019 Datacenter edition with Containers. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2019 with SQL Server 2017 Standard ami-00457129acaaf363d (64-bit (x86)) Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2017 Standard. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2019 with SQL Server 2017 Enterprise ami-04f0d6fc03ca6509b (64-bit (x86)) Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2017 Enterprise. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2019 with SQL Server 2019 Standard ami-086dab9a897bf06ea (64-bit (x86)) Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2019 Standard. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2019 with SQL Server 2019 Enterprise ami-05cb4ad3a438e717b (64-bit (x86)) Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2019 Enterprise. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2022 Base ami-027f2f92dac883acf (64-bit (x86)) Microsoft Windows 2022 Datacenter edition. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>
	Microsoft Windows Server 2016 Base ami-05e2b7014cc33b105 (64-bit (x86)) Microsoft Windows 2016 Datacenter edition. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<div>Select</div> <div>Free tier eligible</div> <div>64-bit (x86)</div>

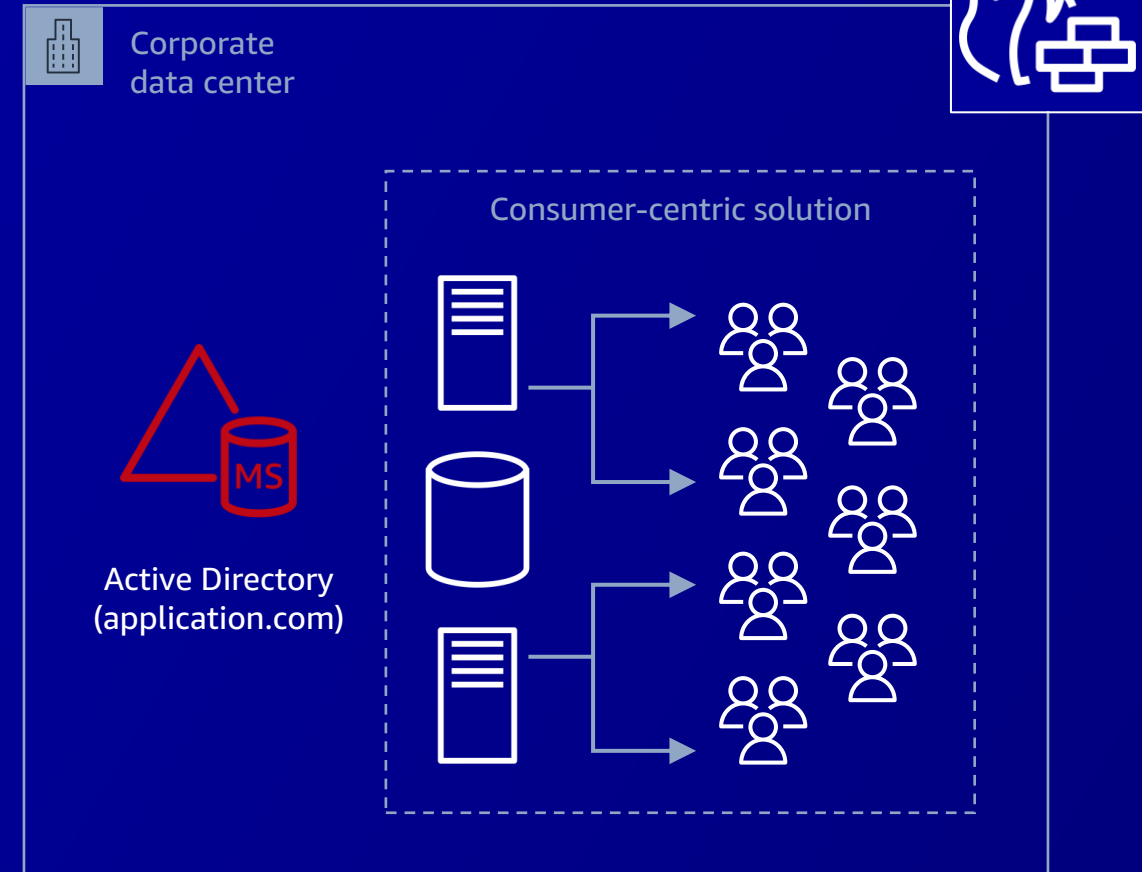


AD use cases

Workforce identity



Application identity store



So . . . **why** should I move?

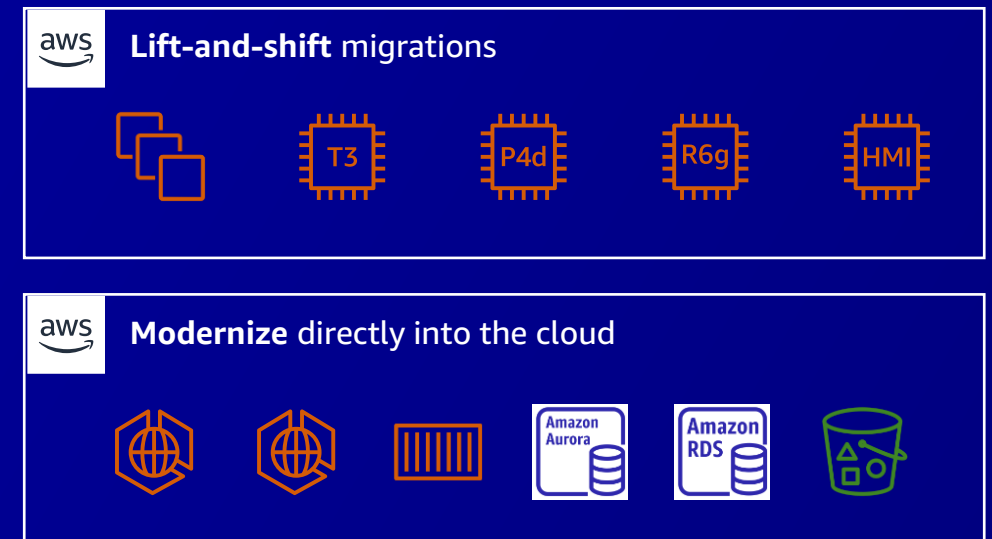
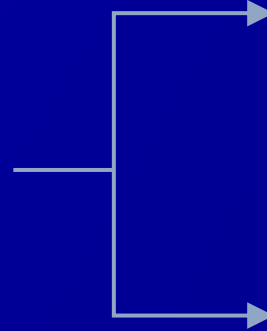
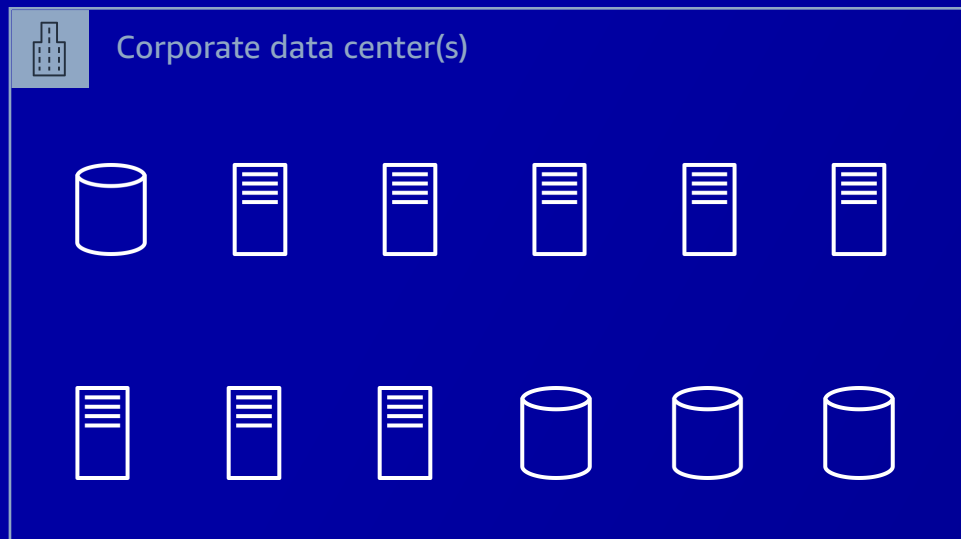
Migration and modernization driven by

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

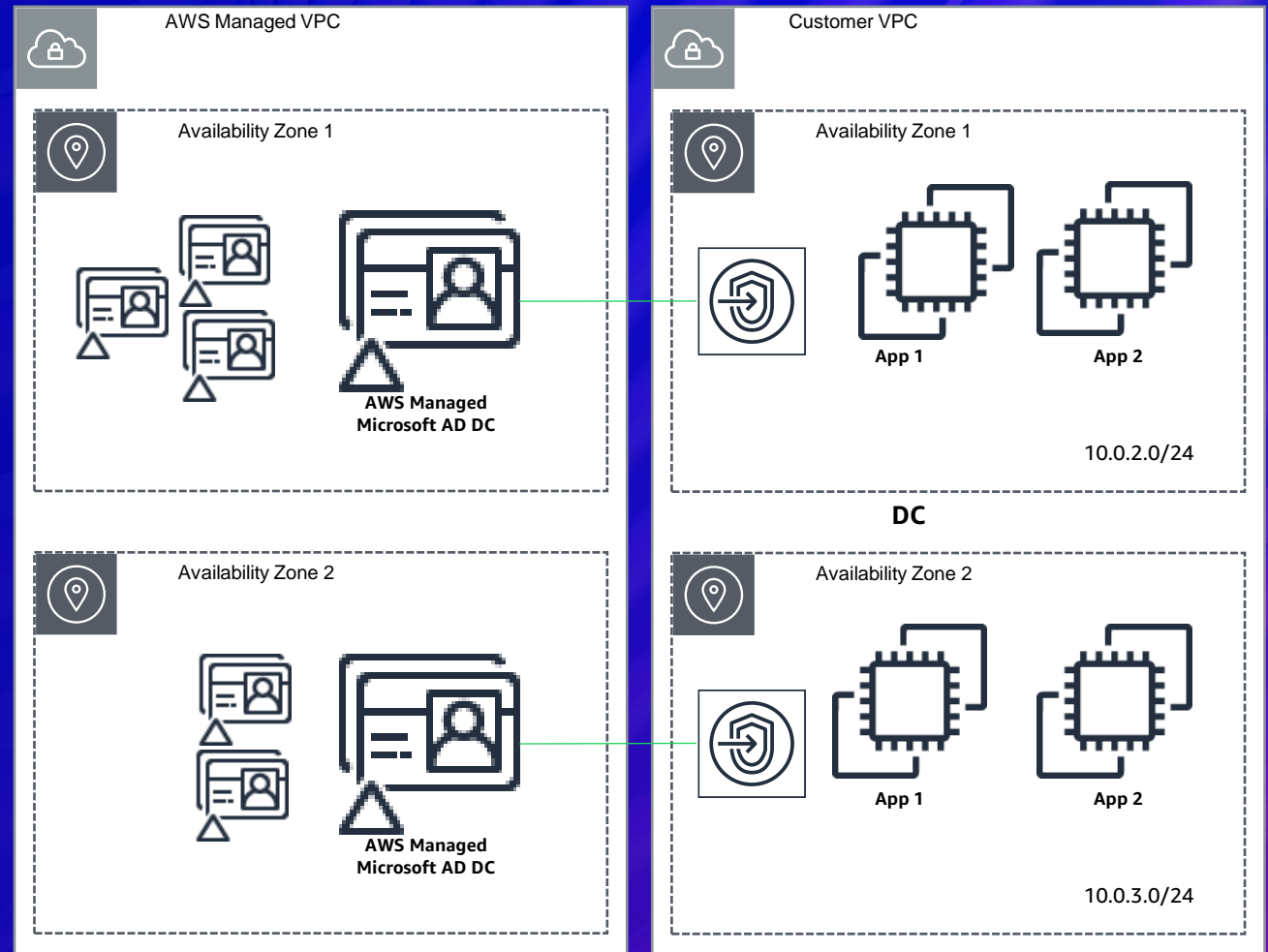
- Single tenant domain (single forest, single domain)
- Multi-AZ, multi-region
- Default 2x domain controllers, can scale out per Region
- Compliances: PCI, HIPAA-eligible, SOC, FedRAMP

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

The screenshot shows the 'Create an AWS Managed Microsoft AD' page in the AWS console. It includes sections for 'Directory information', 'Directory type' (Microsoft AD), 'Edition' (Standard or Enterprise), 'Directory DNS name', 'Directory NetBIOS name', 'Directory description', and 'Admin password'.

Directory information [info](#)
A managed Microsoft Active Directory domain.

Directory type
Microsoft AD

Edition [info](#)
Microsoft AD is available in the following two editions:

- ☐ **Standard Edition**
Best for small to medium sized businesses.
 - 1GB of storage for directory objects
 - Optimized for up to 30,000 objects
 - ~USD 86.4000/mo (USD 0.1200/hr)*
 - * includes two domain controllers, USD 43.2000/mo for each additional domain controller.
- ☒ **Enterprise Edition**
Best for large businesses.
 - 17GB of storage for directory objects
 - Optimized for up to 500,000 objects
 - ~USD 288.0000/mo (USD 0.4000/hr)*
 - * includes two domain controllers, USD 144.0000/mo for each additional domain controller.

Directory DNS name
A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

Directory NetBIOS name - optional
A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.

Maximum of 15 characters, can't contain spaces or the following characters: '\\ / : * ? \" < > |'. It must not start with '.'.

Directory description - optional
Descriptive text that appears on the details page after the directory has been created.

Maximum of 128 characters, can only contain alphanumerics, and the following characters: '_ @ # % * + = : ? , / \ ^ ~'. It may not start with a special character.

Admin password
The password for the default administrative user named Admin.

Passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.

2) AWS CloudFormation/Terraform/AWS CDK

The screenshot shows the 'Create an AWS Managed Microsoft AD' page in the AWS CloudFormation console. It displays the JSON and YAML templates for the stack.

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)

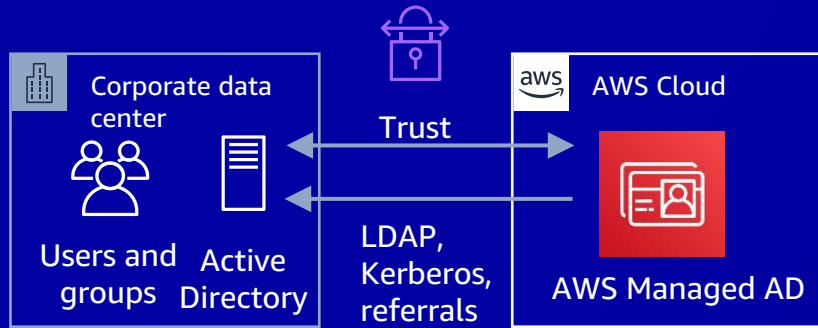
That's it! You're good to go!

3) Command line interface

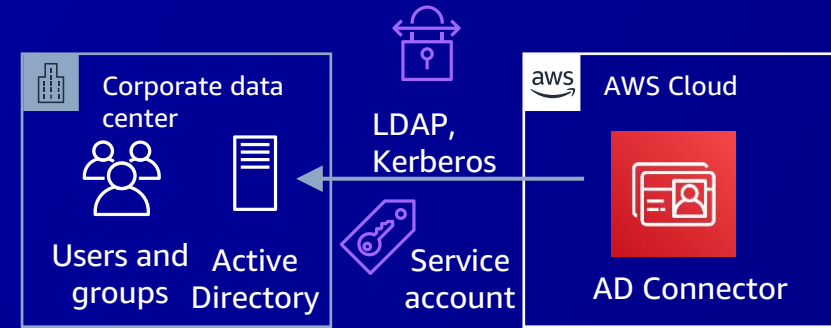
```
aws ds create-microsoft-ad --name example.com --password ExamplePassword  
--vpc-settings VpcId=abc12345,SubnetIds=abc12345,def67890
```



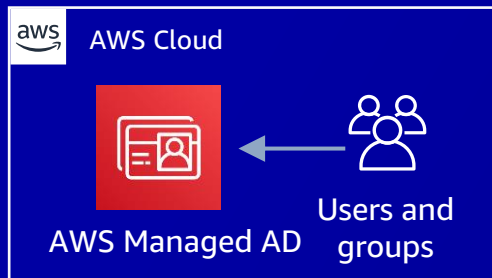
AWS Managed Microsoft AD patterns



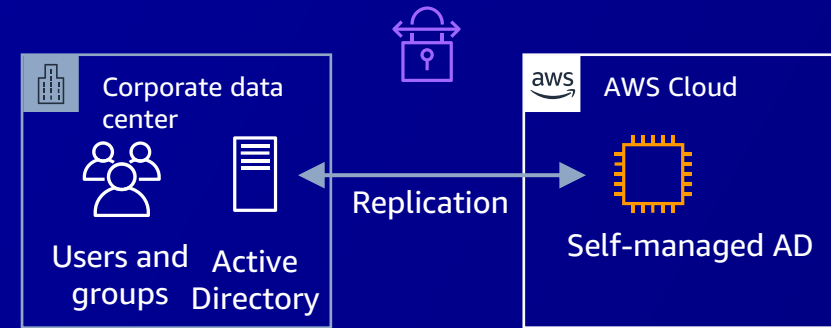
Option 1: AWS Managed AD with trust



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

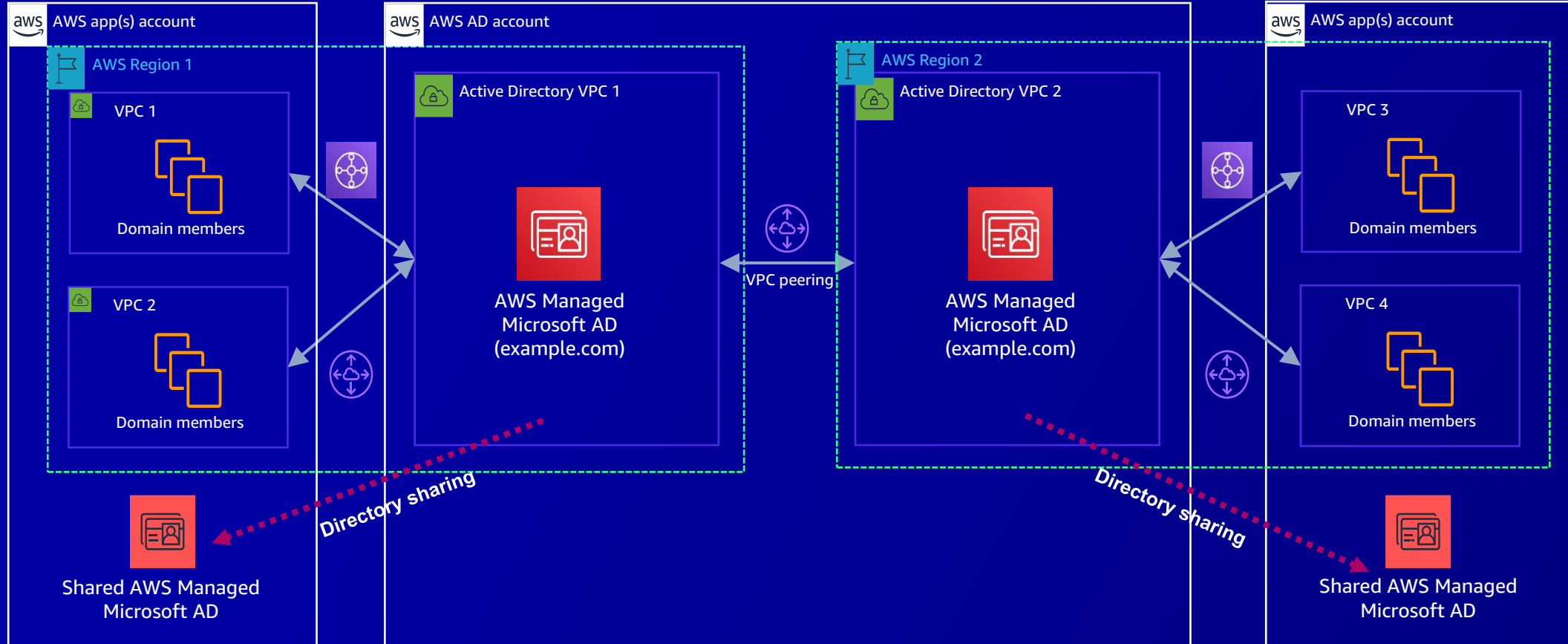
AWS Managed Microsoft AD multi-Region

- 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

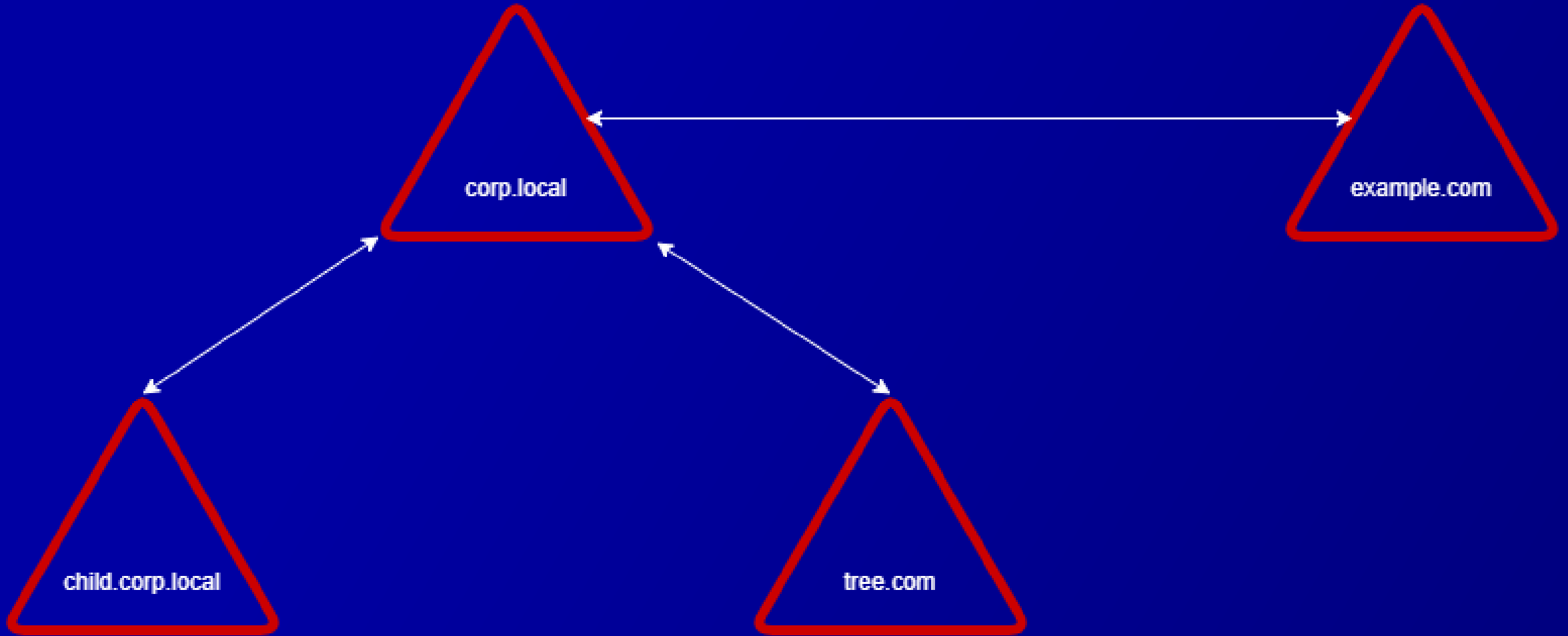
Multi-Region and directory sharing



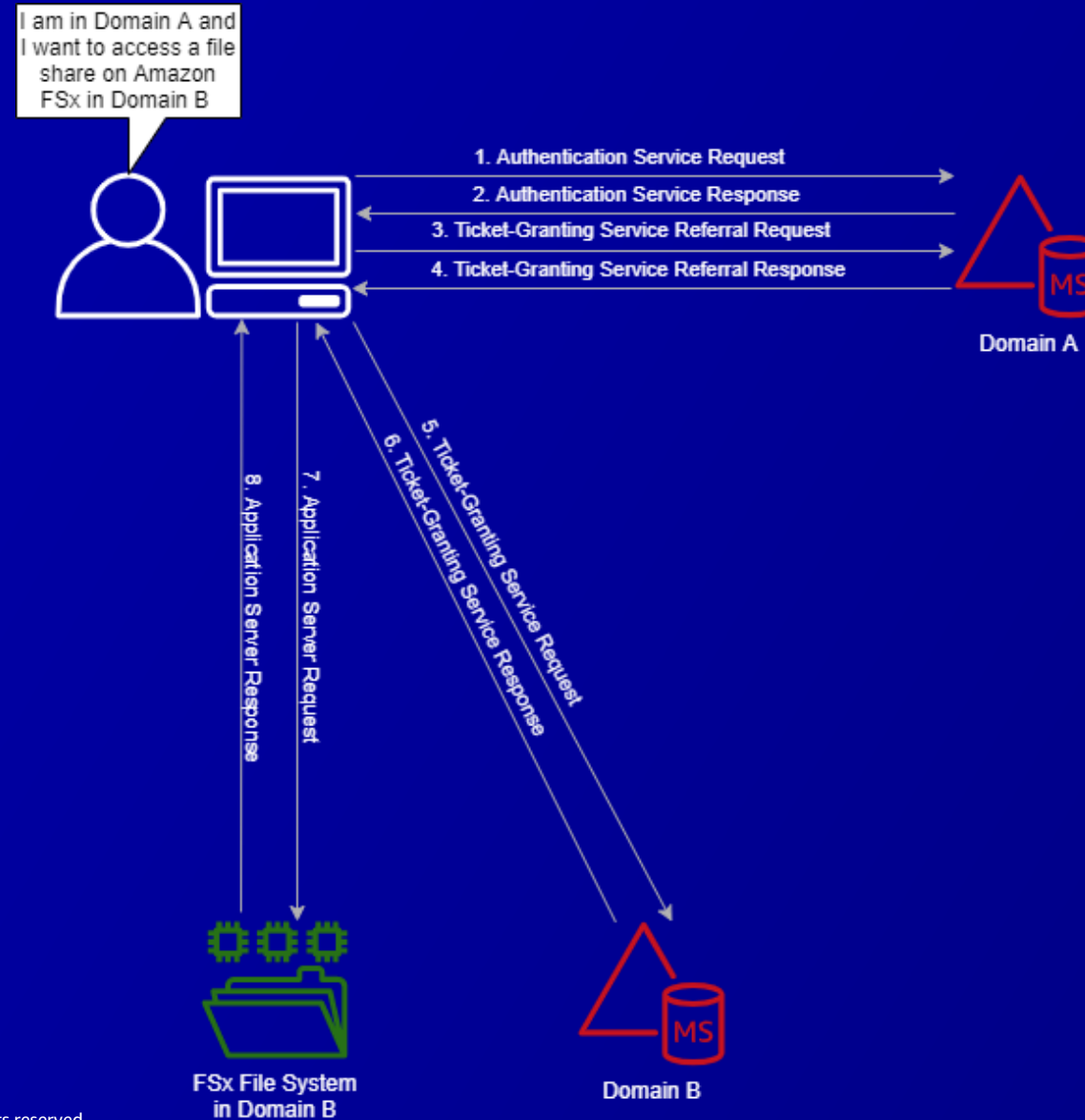
AWS Managed Microsoft AD trust types

Type	Direction	Transitivity	Auth type	MAD sup
Forest	One- or two-way	Transitive	Kerberos V5 or NTLM	<input checked="" type="checkbox"/>
External	One- or two-way	Nontransitive	NTLM	<input checked="" type="checkbox"/>
Realm	One- or two-way	Transitive or nontransitive	Kerberos V5	

AWS Managed Microsoft AD trust transitivity



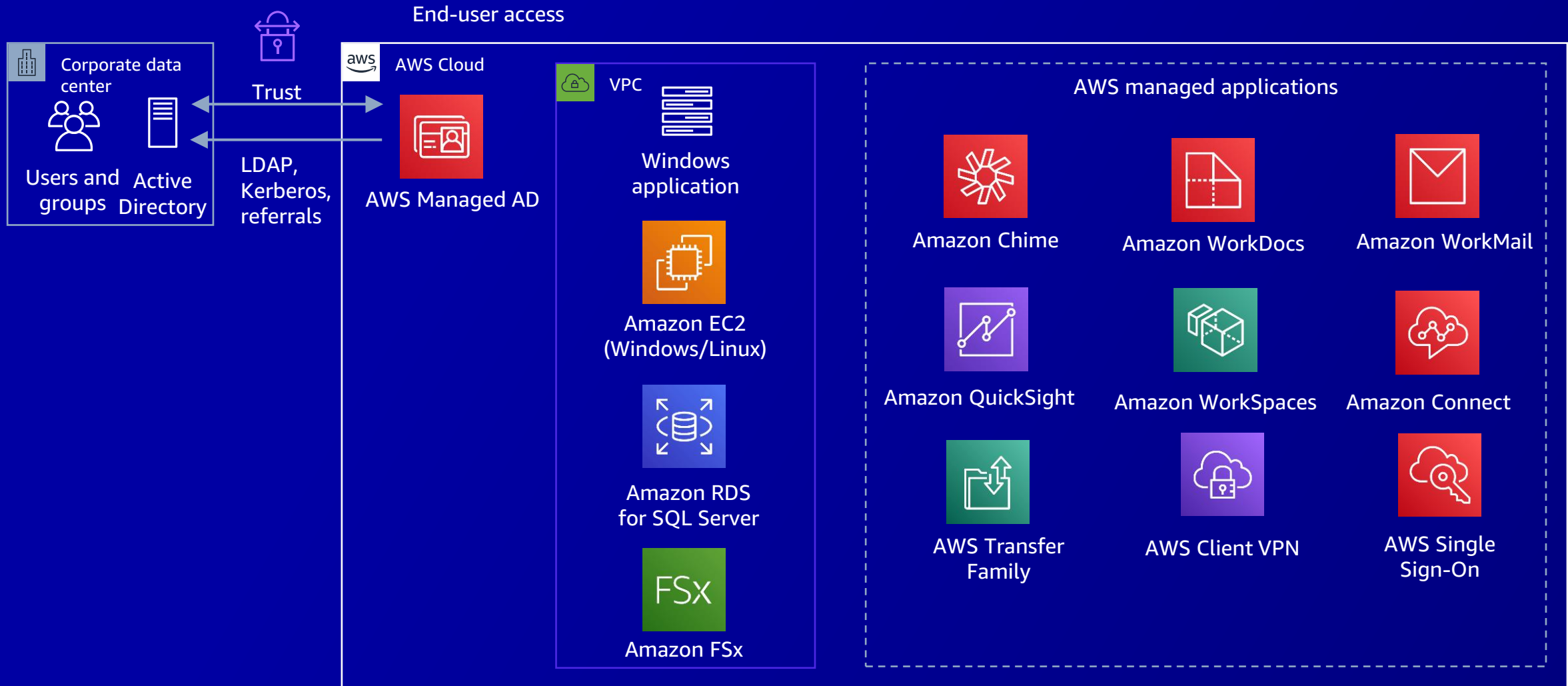
AWS Managed Microsoft AD trust Kerberos



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

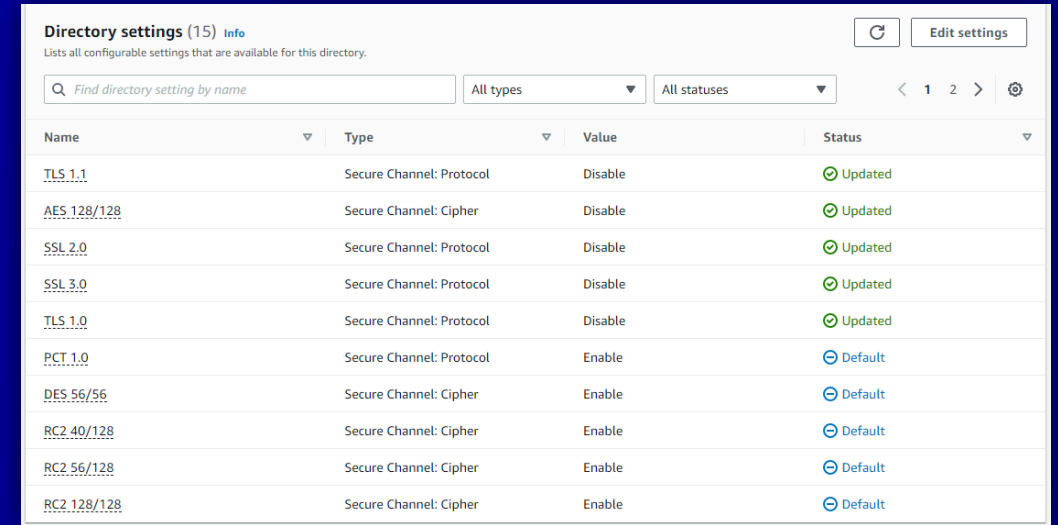
- Most applications without enterprise or domain admin rights requirements
- Microsoft ADFS
- Microsoft PKI
- Microsoft SharePoint
- Microsoft SQL
- Microsoft System Center Suite

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

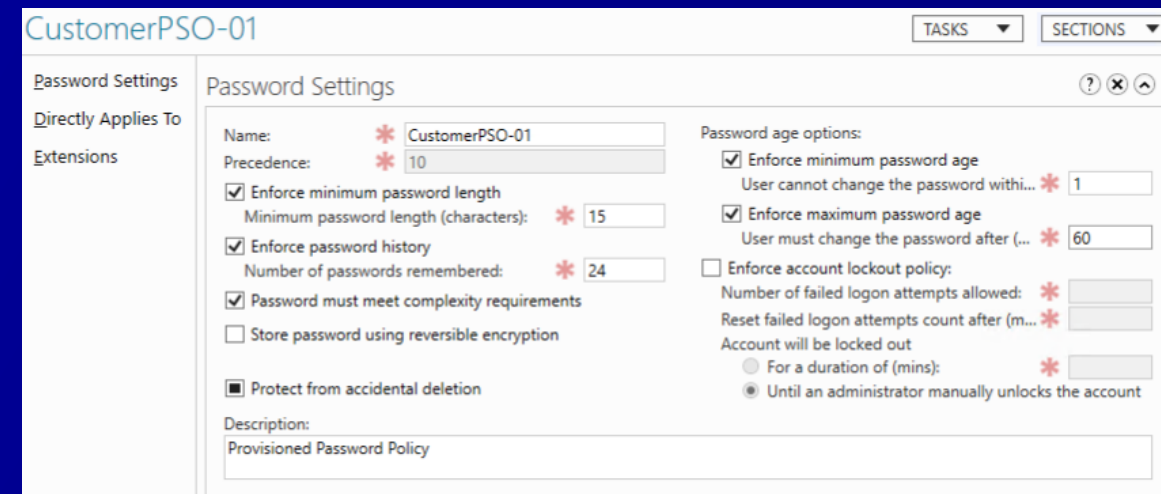


Directory settings (15) Info

Lists all configurable settings that are available for this directory.

Q Find directory setting by name All types All statuses < 1 2 > ⚙

Name	Type	Value	Status
TLS 1.1	Secure Channel: Protocol	Disable	Updated
AES 128/128	Secure Channel: Cipher	Disable	Updated
SSL 2.0	Secure Channel: Protocol	Disable	Updated
SSL 3.0	Secure Channel: Protocol	Disable	Updated
TLS 1.0	Secure Channel: Protocol	Disable	Updated
PCT 1.0	Secure Channel: Protocol	Enable	Default
DES 56/56	Secure Channel: Cipher	Enable	Default
RC4 40/128	Secure Channel: Cipher	Enable	Default
RC2 56/128	Secure Channel: Cipher	Enable	Default
RC2 128/128	Secure Channel: Cipher	Enable	Default



CustomerPSO-01 TASKS SECTIONS

Password Settings

Directly Applies To Extensions

Name: * CustomerPSO-01

Precedence: * 10

☒ Enforce minimum password length
Minimum password length (characters): * 15

☒ Enforce password history
Number of passwords remembered: * 24

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:
Provisioned Password Policy

Password age options:

☒ Enforce minimum password age
User cannot change the password withi... * 1

☒ Enforce maximum password age
User must change the password after (... * 60

☐ Enforce account lockout policy:

Number of failed logon attempts allowed: *

Reset failed logon attempts count after (m... *

Account will be locked out

☐ For a duration of (mins): *

☒ Until an administrator manually unlocks the account

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

Inbound rules Info					
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	
sgr-00b588b6cf3239c4f	DNS (UDP) ▼	UDP	53	Custom ▼	<input type="text" value="10.0.0.0/16"/> X
sgr-064b70d9e504595a4	Custom UDP ▼	UDP	445	Custom ▼	<input type="text" value="10.0.0.0/16"/> X
sgr-00b7bd8b6d76b1047	Custom TCP ▼	TCP	1024 - 655	Custom ▼	<input type="text" value="10.0.0.0/16"/> X
sgr-0bb3e07ffd644e415	All ICMP - IPv4 ▼	ICMP	All	Custom ▼	<input type="text" value="10.0.0.0/16"/> X

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=PLhr1KZpdzkdJllxulUM7pMB7aJ2_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

