



관리 설명서

AWS Directory Service



버전 1.0

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directory Service: 관리 설명서

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

이게 뭐야 AWS Directory Service?	1
무엇을 선택할 것인가	1
AWS Directory Service 옵션	2
Amazon EC2에서의 작업	5
시작하기	7
가입하여 다음을 수행하십시오. AWS 계정	7
관리 액세스 권한이 있는 사용자 생성	7
추가 정보	9
AWS 매니지드 마이크로소프트 AD	10
시작하기	12
AWS 관리형 Microsoft AD 사전 요구 사항	12
AWS 관리형 Microsoft AD 만들기	14
AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목	16
관리자 계정 권한	23
핵심 개념	26
Active Directory 스키마	26
패치 적용 및 유지 관리	27
그룹 관리형 서비스 계정	28
Kerberos 제한된 위임	28
모범 사례	29
설정: 사전 조건	29
설정: 디렉터리 생성	31
디렉터리 사용	32
디렉터리 관리	33
애플리케이션 프로그래밍	36
사용 사례	37
사용 사례 1: Active Directory 자격 증명을 사용하여 AWS 응용 프로그램 및 서비스에 로그인	38
사용 사례 2: Amazon EC2 인스턴스 관리	42
사용 사례 3: Active Directory를 인식하는 워크로드에 디렉터리 서비스를 제공합니다.	43
사용 사례 4: Office 365 및 기타 클라우드 응용 프로그램으로 AWS IAM Identity Center	43
사용 사례 5: 온-프레미스 Active Directory를 클라우드로 확장 AWS	43
사용 사례 6: 디렉터리를 공유하여 계정 간에 Amazon EC2 인스턴스를 도메인에 원활하게 도입합니다. AWS	44

방법.....	44
디렉터리 보안 유지	45
디렉터리 모니터링	90
다중 리전 복제 구성	103
디렉터리 공유	111
AWS 관리형 Microsoft AD에 인스턴스를 조인합니다.	124
사용자 및 그룹 관리	180
기존 액티브 디렉터리 인프라를 연결하세요	192
AWS 관리형 Microsoft AD를 다음으로 연결하세요. Microsoft Entra Connect Sync	215
스키마 확장	221
디렉터리 유지 관리	229
AWS 리소스에 대한 액세스 권한 부여	237
AWS 애플리케이션 및 서비스에 대한 액세스 지원	243
AWS Management Console에 대한 액세스 활성화	254
추가 도메인 컨트롤러 배포	256
AD에서 AWS Managed Microsoft AD로 사용자 마이그레이션	259
할당량	259
애플리케이션 호환성	260
호환성 지침	262
호환되지 않는 것으로 알려진 애플리케이션	263
AWS 관리형 Microsoft AD 테스트 랩 튜토리얼	263
자습서: 기본 AWS 관리형 Microsoft AD 테스트 랩 설정	264
자습서: AWS 관리형 Microsoft AD에서 EC2의 자체 관리형 AD 설치에 대한 트러스트 생성 ..	281
문제 해결	292
AWS 관리형 Microsoft AD와 관련된 문제	292
Netlogon 및 보안 채널 통신 관련 문제	292
암호 복구	292
추가 리소스	293
Microsoft 이벤트 뷰어로 DNS 서버 모니터링	293
Linux 도메인 조인 오류	294
사용 가능한 스토리지 공간 부족	297
스키마 확장 오류	300
신뢰 생성 상태 이유	302
AD Connector	307
시작하기	308
AD Connector 사전 조건	308

AD Connector 생성	323
AD 커넥터로 생성되는 항목	325
방법	325
디렉터리 보안 유지	326
디렉터리 모니터링	347
Amazon EC2 인스턴스를 다음 인스턴스에 연결하세요. Active Directory	350
디렉터리 유지 관리	365
AWS 애플리케이션 및 서비스에 대한 액세스 지원	368
AD Connector의 DNS 주소 업데이트	369
모범 사례	370
설정: 사전 조건	370
애플리케이션 프로그래밍	372
디렉터리 사용	372
할당량	373
애플리케이션 호환성	373
문제 해결	375
생성 문제	375
연결 문제	376
인증 문제	377
유지 관리 문제	381
AD Connector를 삭제할 수 없는 경우	382
Simple AD	383
시작하기	384
간단한 AD 사전 조건	384
나만의 Simple AD 만들기 Active Directory	386
Simple AD로 생성되는 콘텐츠 Active Directory	388
Simple AD용 DNS 구성	389
방법	389
사용자 및 그룹 관리	390
디렉터리 모니터링	401
Simple AD에 인스턴스 연결	404
디렉터리 유지 관리	437
AWS 애플리케이션 및 서비스에 대한 액세스 지원	442
AWS Management Console에 대한 액세스 활성화	452
튜토리얼: 단순 AD 만들기 Active Directory	454
자습서 사전 요구 사항	454

모범 사례	457
설정: 사전 조건	457
설정: 디렉터리 생성	459
애플리케이션 프로그래밍	459
할당량	460
애플리케이션 호환성	461
문제 해결	461
암호 복구	462
사용자를 Simple AD에 추가할 때 "KDC가 요청한 선택을 수행할 수 없음"이라는 오류가 발생 하는 경우	462
내 도메인에 조인된 인스턴스의 DNS 이름이나 IP 주소를 업데이트 할 수 없는 경우 (DNS 동 적 업데이트)	463
SQL Server 계정을 사용해 SQL Server에 로그인할 수 없는 경우	463
디렉터리가 "Requested" 상태에 멈춰있는 경우	463
디렉터를 생성할 때 "AZ Constrained" 오류 메시지가 표시되는 경우	463
일부 사용자들이 내 디렉터를 통해 인증을 할 수 없는 경우	463
추가적인 리소스	293
디렉터리 상태 사유	464
보안	468
자격 증명 및 액세스 관리	469
인증	470
액세스 제어	470
액세스 관리 개요	470
자격 증명 기반 정책(IAM 정책) 사용	474
AWS Directory Service API 권한 참조	483
애플리케이션 및 서비스 승인 및 인증 취소 AWS	483
로그 및 모니터링	485
규정 준수 확인	485
복원력	486
인프라 보안	487
교차 서비스 혼동된 대리인 방지	487
AWS PrivateLink	490
고려 사항	491
가용성	491
인터페이스 엔드포인트 생성	491
엔드포인트 정책을 생성	491

서비스 수준 계약	493
리전 가용성	494
브라우저 호환성	500
TLS란 무엇입니까?	500
IAM Identity Center에서 지원하는 TLS 버전	500
지원되는 TLS 버전을 브라우저에서 활성화하는 방법	501
문서 기록	502
.....	dv

이게 뭐야 AWS Directory Service?

AWS Directory Service 는 다른 AWS 서비스와 함께 Microsoft Active Directory (AD) 를 사용하는 여러 가지 방법을 제공합니다. 디렉터리에는 사용자, 그룹 및 장치에 대한 정보가 저장되며 관리자는 이를 사용하여 정보 및 리소스에 대한 액세스를 관리합니다. AWS Directory Service Microsoft클라우드에서 기존 AD 또는 경량 디렉터리 액세스 프로토콜 (LDAP) 인식 애플리케이션을 사용하려는 고객에게 다양한 디렉터리 옵션을 제공합니다. 또한 사용자, 그룹, 디바이스 및 액세스 권한을 관리하기 위해 디렉터리가 필요한 개발자에게도 동일한 선택 옵션을 제공합니다.

무엇을 선택할 것인가

요구 사항에 가장 적합한 기능 및 확장성을 갖춘 디렉터리 서비스를 선택할 수 있습니다. 다음 표를 참조하면 조직에 가장 적합한 AWS Directory Service 디렉터리 옵션을 결정하는 데 도움이 됩니다.

필요한 작업	권장 AWS Directory Service 옵션
클라우드상의 애플리케이션을 위해 Active Directory 또는 LDAP가 필요	<p>WorkSpaces Amazon QuickSight 및 Amazon과 같은 애플리케이션 및 서비스나 AWS 애플리케이션 및 서비스를 지원하는 Active Directory 실제 Microsoft Active Directory AWS 클라우드가 필요하거나 Linux 애플리케이션에 대한 LDAP 지원이 필요한 경우 Microsoft Active Directory용 Directory Service (스탠다드 에디션 또는 엔터프라이즈 에디션) 를 사용하십시오AWS .</p> <p>온-프레미스 사용자가 Active Directory 자격 증명으로 AWS 응용 프로그램 및 서비스에 로그인할 수만 있도록 허용해야 하는 경우에는 AD Connector를 사용하십시오. 또한 AD Connector를 사용하여 Amazon EC2 인스턴스를 기존 Active Directory 도메인에 결합할 수 있습니다.</p> <p>Samba 4 호환 애플리케이션을 지원하는 기본 Active Directory 호환성을 갖춘 소규모의 저렴한 디렉터리가 필요하거나 LDAP 인식 애플리케이션을 위한 LDAP 호환성이 필요한 경우 Simple AD를 사용하십시오.</p>

필요한 작업	권장 AWS Directory Service 옵션
SaaS 애플리케이션을 개발	대규모 SaaS 애플리케이션 개발자이며 가입자를 관리 및 인증하고 소셜 미디어 자격 증명과 연동하는 확장 가능한 디렉터리가 필요한 경우 Amazon Cognito를 사용합니다.

[디렉터리 옵션에 대한 자세한 내용은 솔루션 선택 방법을 참조하십시오. AWS Directory ServiceActive DirectoryAWS](#)

AWS Directory Service 옵션

AWS Directory Service 선택할 수 있는 여러 디렉터리 유형이 포함되어 있습니다. 자세한 정보를 알고 싶다면 다음 탭 중 하나를 선택하세요.

AWS Directory Service for Microsoft Active Directory

AWS 관리형 Microsoft AD라고도 하는 Microsoft Active AWS Directory용 디렉터리 서비스는 AWS 클라우드에서 관리하는 실제 Microsoft Windows Server Active Directory (AD) AWS 에 의해 구동됩니다. 이를 통해 광범위한 Active Directory 인식 애플리케이션을 클라우드로 마이그레이션할 수 있습니다. AWS 관리형 Microsoft AD는 올웨이즈 온 가용성 그룹 및 여러 .NET 응용 프로그램과 함께 Microsoft SharePoint 사용할 수 있습니다. Microsoft SQL Server 또한 [아마존 WorkSpaces](#), [아마존](#), [아마존](#), [아마존 차임](#), [아마존 커넥트 WorkDocs QuickSight](#), [아마존 관계형 데이터베이스 서비스 \(Microsoft SQL ServerAmazon RDS 전용SQL Server, Amazon RDS Oracle for PostgreSQL용\)](#) 를 포함한 AWS 관리형 애플리케이션 및 서비스도 지원합니다.

[AWS Managed Microsoft AD는 디렉터리에 대한 규정 준수를 활성화하면 미국 건강 보험 이전 및 책임법 \(HIPAA\) 또는 결제 카드 산업 데이터 보안 표준 \(PCI DSS\) 준수가 적용되는 AWS 클라우드 내 애플리케이션에 대해 승인됩니다.](#)

호환되는 모든 애플리케이션은 AWS Managed Microsoft AD에 저장한 사용자 자격 증명으로 작동하거나, 신뢰를 통해 [기존 AD 인프라에 연결하고](#) 온프레미스 또는 EC2 Windows에서 Active Directory 실행 중인 자격 증명을 사용할 수 있습니다. [EC2 인스턴스를 AWS 관리형 Microsoft AD에 연결하면](#) 사용자는 온프레미스 네트워크의 워크로드에 액세스할 때와 동일한 Windows 싱글 사인온 (SSO) AWS 환경에서 클라우드의 Windows 워크로드에 액세스할 수 있습니다.

AWS 관리형 Microsoft AD는 Active Directory 자격 증명을 사용하는 페더레이션 사용 사례도 지원합니다. AWS 관리형 Microsoft AD를 통해서만 에 로그인할 수 [AWS Management Console](#)있

습니다. 를 사용하면 AWS SDK 및 CLI와 함께 사용할 단기 자격 증명을 얻고 사전 구성된 SAML 통합을 사용하여 여러 클라우드 애플리케이션에 로그인할 수 있습니다. [AWS IAM Identity Center](#) 이전에는 ADFS Microsoft Entra Connect (페더레이션 서비스 Azure Active Directory Connect) 를 추가하고 선택적으로 Active Directory 페더레이션 서비스 (ADFS) 를 추가하면 Managed AWS Microsoft AD에 저장된 자격 증명을 사용하여 다른 클라우드 응용 프로그램에 로그인할 수 있습니다. Microsoft Office 365

이 서비스에는 [스키마 확장](#), [암호 정책 관리](#), [Secure Socket Layer\(SSL\)/전송 계층 보안\(TLS\)을 통한 보안 LDAP 통신](#) 같은 주요 기능이 포함됩니다. 또한 [AWS Managed Microsoft AD에 대한 다단계 인증 \(MFA\) 을 활성화하여](#) 사용자가 인터넷에서 애플리케이션에 AWS 액세스할 때 추가 보안 계층을 제공할 수 있습니다. Active Directory는 LDAP 디렉토리이기 때문에 Linux 보안 셸 (SSH) 인증 및 기타 LDAP 지원 응용 프로그램에 관리형 AWS Microsoft AD를 사용할 수도 있습니다.

AWS 서비스의 일부로 모니터링, 일일 스냅샷 및 복구를 제공합니다. 관리형 Microsoft AD에 [사용자 및 그룹을 추가하고 관리형 AWS Microsoft AD](#) 도메인에 연결된 Windows 컴퓨터에서 실행되는 친숙한 Active Directory 도구를 사용하여 그룹 정책을 관리할 수 있습니다. 또한 [추가 도메인 컨트롤러를 배포해](#) 디렉토리를 확장하고, 다수의 도메인 컨트롤러에 요청을 분산해 애플리케이션 성능을 개선할 수도 있습니다.

AWS 관리형 Microsoft AD는 스탠다드와 엔터프라이즈라는 두 가지 에디션으로 제공됩니다.

- Standard Edition: AWS Managed Microsoft AD(Standard Edition)는 직원이 5,000명 이하인 중소기업의 기본 디렉터리로 최적화되어 있습니다. 이 에디션은 사용자, 그룹, 컴퓨터 등 디렉터리 객체를 최대 30,000*개까지 지원하는 데 충분한 스토리지 용량을 제공합니다.
- Enterprise Edition: AWS Managed Microsoft AD(Enterprise Edition)는 최대 500,000개의* 디렉터리 객체를 보유한 엔터프라이즈 조직을 지원하도록 설계되었습니다.

* 상한은 근사치입니다. 디렉터리가 지원할 수 있는 디렉터리 객체 수는 객체 크기와 애플리케이션의 동작 및 성능 요구 사항에 따라 변동할 수 있습니다.

사용해야 하는 경우

AWS Amazon Relational Database Service for 등 AWS 애플리케이션 또는 Windows 워크로드를 지원하는 실제 Active Directory 기능이 필요한 경우 관리형 Microsoft AD를 선택하는 것이 가장 좋습니다. Microsoft SQL Server 또한 Office 365를 지원하는 AWS 클라우드의 독립 Active Directory 실행형을 원하거나 Linux 애플리케이션을 지원하는 LDAP 디렉터리가 필요한 경우에도 가장 좋습니다. 자세한 정보는 [AWS 매니지드 마이크로소프트 AD](#)을 참조하세요.

AD Connector

AD Connector는 Amazon, Amazon, Windows Server 인스턴스용 [Amazon WorkSpaces EC2](#)와 같은 호환 가능한 AWS 애플리케이션을 기존 온프레미스에 쉽게 연결할 수 있는 방법을 제공하는 프록시 서비스입니다. QuickSight Microsoft Active Directory AD Connector를 사용하면 [서비스 계정 하나를 간단히 추가할 수 있습니다](#) Active Directory. 또한 AD Connector를 사용하면 디렉터리 동기화가 필요하지 않으며 페더레이션 인프라를 호스팅하는 데 드는 비용과 복잡성이 없어집니다.

QuickSight Amazon과 같은 AWS 애플리케이션에 사용자를 추가하면 AD Connector가 기존 Active Directory 데이터를 읽고 선택할 사용자 및 그룹 목록을 생성합니다. 사용자가 AWS 응용 프로그램에 로그인하면 AD Connector는 인증을 위해 로그인 요청을 온-프레미스 Active Directory 도메인 컨트롤러로 전달합니다. [AD Connector는 아마존 WorkSpaces, 아마존, 아마존, 아마존차임 WorkDocs, 아마존커넥트 QuickSight, 아마존 등 다양한 AWS 애플리케이션 및 서비스와 호환됩니다.](#) [WorkMail 또한 원활한 도메인 조인을 사용하여 AD Connector를 통해 EC2 Windows 인스턴스를 온프레미스 Active Directory 도메인에 조인할 수 있습니다.](#) 또한 AD Connector를 사용하면 사용자가 기존 Active Directory 자격 증명으로 로그인하여 AWS 리소스에 AWS Management Console 액세스하고 리소스를 관리할 수 있습니다. AD Connector는 RDS SQL 서버와 호환되지 않습니다.

AD Connector를 사용하여 기존 RADIUS 기반 MFA 인프라에 AWS 연결하여 애플리케이션 사용자를 위한 [멀티 팩터 인증 \(MFA\) 을 활성화할](#) 수도 있습니다. 그러면 사용자가 AWS 애플리케이션에 액세스할 때 추가 보안 계층이 제공됩니다.

AD Connector를 사용하면 Active Directory 지금처럼 계속해서 관리할 수 있습니다. 예를 들어 Active Directory 온-프레미스의 표준 Active Directory 관리 도구를 사용하여 새 사용자 및 그룹을 추가하고 암호를 업데이트합니다. 이를 통해 사용자가 온프레미스에서 리소스에 액세스하던 클라우드에서 리소스에 액세스하던 관계없이 암호 만료, 암호 기록, 계정 잠금과 같은 보안 정책을 일관되게 적용할 수 있습니다. AWS

사용해야 하는 경우

AD Connector는 호환되는 AWS 서비스와 함께 기존 온-프레미스 디렉터리를 사용하려는 경우에 가장 적합합니다. 자세한 정보는 [AD Connector](#)을 참조하세요.

Simple AD

Simple AD는 Microsoft Active Directory Samba 4에서 AWS Directory Service 제공하는 호환 가능한 디렉터리입니다. Simple AD는 사용자 계정, 그룹 멤버십, Linux 도메인 가입 또는 Windows 기반 EC2 인스턴스, Kerberos 기반 SSO 및 그룹 정책과 같은 기본 Active Directory 기능을 지원합니다. AWS 서비스의 일부로 모니터링, 일일 스냅샷 및 복구를 제공합니다.

Simple AD는 클라우드상의 독립 실행형 디렉터리로, 여기서 사용자 자격 증명을 생성 및 관리하고 애플리케이션 액세스 권한을 관리할 수 있습니다. 기본 기능이 필요한 친숙하고 Active Directory 인식이 가능한 응용 프로그램 및 도구를 많이 사용할 수 있습니다. Active Directory [Simple AD는 아마존 WorkSpaces, 아마존, 아마존 WorkDocs QuickSight, 아마존 등의 AWS 애플리케이션과 WorkMail 호환됩니다.](#) Simple AD 사용자 계정으로 로그인하여 AWS 리소스를 관리할 수도 있습니다. AWS Management Console

Simple AD는 다단계 인증 (MFA), 신뢰 관계, DNS 동적 업데이트, 스키마 확장, LDAPS를 통한 통신 PowerShell , AD cmdlet 또는 FSMO 역할 전송을 지원하지 않습니다. Simple AD는 RDS SQL 서버와 호환되지 않습니다. 실제 Microsoft Active Directory 기능이 필요하거나 RDS SQL Server 와 함께 디렉터리를 사용하려는 고객은 관리형 AWS Microsoft AD를 대신 사용해야 합니다. Simple AD를 사용하기 전에 필수 애플리케이션이 Samba 4와 완벽하게 호환 가능한지 확인하세요. 자세한 내용은 <https://www.samba.org>를 참조하세요.

사용해야 하는 경우

Simple AD를 클라우드의 독립형 디렉터리로 사용하여 기본 Active Directory 기능, 호환 가능한 AWS 애플리케이션이 필요한 Windows 워크로드를 지원하거나 LDAP 서비스가 필요한 Linux 워크로드를 지원할 수 있습니다. 자세한 정보는 [Simple AD](#)을 참조하세요.

Amazon Cognito

[Amazon Cognito](#)는 Amazon Cognito 사용자 풀을 사용해 모바일 앱 또는 웹 애플리케이션에 가입 및 로그인을 추가하는 사용자 디렉터리입니다.

사용해야 하는 경우

사용자 지정 등록 필드를 생성하고 사용자 디렉터리에 해당 메타데이터를 저장해야 할 때 Amazon Cognito를 사용할 수도 있습니다. 이 완전한 관리형 서비스는 수억 명의 사용자를 지원하도록 확장됩니다. 자세한 내용은 Amazon Cognito 개발자 안내서의 [Amazon Cognito 사용자 풀](#)을 참조하세요.

리전별로 지원되는 디렉터리 유형 목록은 [지역 이용 가능 여부 AWS Directory Service](#) 단원을 참고하세요.

Amazon EC2에서의 작업

AWS Directory Service를 사용하기 위해서는 Amazon EC2에 대한 기본적인 이해가 필요합니다. 다음 주제들을 읽고 시작하면 도움이 됩니다.

- [Windows 인스턴스용 Amazon EC2 사용 설명서](#)의 Amazon EC2란 무엇인가요?
- [Windows 인스턴스용 Amazon EC2 사용 설명서](#)의 EC2 인스턴스 시작하기.
- Windows 인스턴스용 Amazon EC2 사용 설명서의 [보안 그룹](#)
- Amazon VPC 사용 설명서의 [Amazon VPC란 무엇인가요?](#)
- Amazon VPC 사용 설명서의 [VPC에 하드웨어 가상 프라이빗 게이트웨이 추가하기](#).

시작하기 AWS Directory Service

아직 계정을 만들지 않았다면 AWS 계정을 만들고 AWS Identity and Access Management 서비스를 사용하여 액세스를 제어해야 합니다.

를 사용하려면 Microsoft Active Directory AWS Directory Service, AD Connector 또는 Simple AD 용 디렉터리 서비스에 대한 사전 요구 사항을 충족해야 합니다. 자세한 내용은 [AWS 관리형 Microsoft AD 사전 요구 사항](#), [AD Connector 사전 조건](#) 또는 [간단한 AD 사전 조건](#)를 참조하세요.

가입하여 다음을 수행하십시오. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. <https://portal.aws.amazon.com/billing/signup>을 여세요.
2. 온라인 지시 사항을 따르세요.

등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례로, 사용자에게 관리자 액세스 권한을 할당하고 루트 사용자 [액세스가 필요한 작업을 수행할 때는 루트 사용자만](#) 사용하십시오.

AWS 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 <https://aws.amazon.com/>으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리 액세스 권한이 있는 사용자 생성

가입한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오. AWS 계정 루트 사용자

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 [AWS Management Console](#)소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

루트 사용자를 사용하여 로그인하는 데 도움이 필요하다면 [AWS 로그인 사용 설명서의 루트 사용자 로 로그인](#)을 참조하세요.

2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

지침은 IAM [사용 설명서의 AWS 계정 루트 사용자 \(콘솔\)에 대한 가상 MFA 디바이스 활성화를 참조](#)하십시오.

관리 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [AWS IAM Identity Center 설정](#)을 참조하세요.

2. IAM ID 센터에서 사용자에게 관리 액세스 권한을 부여하십시오.

를 ID 소스로 사용하는 방법에 대한 자습서는 사용 [설명서의 기본값으로 IAM Identity Center 디렉터리 사용자 액세스 구성](#)을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

관리 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM IDentity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

IAM Identity Center 사용자를 사용하여 [로그인하는 데 도움이 필요하다면 사용 설명서의 AWS 액세스 포털에 로그인](#)을 참조하십시오. AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

지침은 사용 설명서의 [권한 집합 생성](#)을 참조하십시오. AWS IAM Identity Center

2. 사용자를 그룹에 배정한 다음 그룹에 Single Sign-On 액세스 권한을 할당하십시오.

자세한 지침은 사용 설명서의 [그룹 추가](#)를 참조하십시오. AWS IAM Identity Center

추가 정보

- IAM ID 센터 AWS Management Console 사용자로 로그인하는 방법에 대한 자세한 내용은 IAM ID 센터 [액세스 포털에 로그인](#)을 참조하십시오.
- IAM AWS Management Console 사용자로 로그인하는 방법에 대한 자세한 내용은 IAM AWS Management Console 사용자로 [로그인](#)을 참조하십시오.
- IAM 정책을 사용하여 AWS Directory Service 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 [ID 기반 정책 \(IAM 정책\) 사용 대상 AWS Directory Service](#) 을 참조하십시오.

AWS 매니지드 마이크로소프트 AD

AWS Directory Service Microsoft Active Directory(AD) 를 관리형 서비스로 실행할 수 있습니다. AWS 마이크로소프트 액티브 디렉터리용 디렉터리 서비스 (AWS 매니지드 마이크로소프트 AD라고도 함) 는 Windows 서버 2019에서 제공합니다. 이 디렉터리 유형을 선택하고 실행하면 가상 사설 클라우드 (Amazon VPC) 에 연결된 고가용성 도메인 컨트롤러 쌍으로 생성됩니다. 도메인 컨트롤러는 선택한 리전의 다른 가용 영역에서 실행됩니다. 호스트 모니터링 및 복구, 데이터 복제, 스냅샷, 소프트웨어 업데이트가 자동으로 구성 및 관리됩니다.

AWS 관리형 Microsoft AD를 사용하면 사용자 지정.NET Microsoft SharePoint 및 SQL Server 기반 애플리케이션을 비롯한 디렉터리 인식 워크로드를 AWS 클라우드에서 실행할 수 있습니다. 또한 AWS 클라우드의 AWS Managed Microsoft AD와 기존 온-프레미스 Microsoft Active Directory 간에 신뢰 관계를 구성하여 사용자와 그룹이 를 사용하여 AWS IAM Identity Center 두 도메인 중 하나의 리소스에 액세스할 수 있도록 할 수 있습니다.

AWS Directory Service AWS 클라우드에서 디렉터리를 쉽게 설정 및 실행하거나 AWS 리소스를 기존 온-프레미스와 연결할 수 있습니다. Microsoft Active Directory 생성된 디렉터리는 다양한 작업에서 사용할 수 있습니다.

- 사용자 및 그룹 관리
- 애플리케이션 및 서비스에 Single Sign-On를 제공
- 그룹 정책 생성 및 적용
- 클라우드 기반 Linux 및 워크로드의 배포 및 관리를 간소화합니다. Microsoft Windows
- AWS Managed Microsoft AD를 사용하면 기존 RADIUS 기반 MFA 인프라와 통합하여 다단계 인증을 활성화하여 사용자가 애플리케이션에 액세스할 때 추가 보안 계층을 제공할 수 있습니다. AWS
- Amazon EC2 리눅스 및 인스턴스에 안전하게 연결 Windows

Note

AWS 사용자 대신 Windows 서버 인스턴스의 라이선스를 관리합니다. 사용한 인스턴스에 대한 비용을 지불하기만 하면 됩니다. 또한 액세스 권한이 가격에 포함되어 있으므로 Windows Server CAL(클라이언트 액세스 라이선스)을 추가로 구매할 필요가 없습니다. 각 인스턴스에는 관리 목적으로만 사용할 수 있는 두 개의 원격 연결이 제공됩니다. 연결이 2개 이상 필요하거나 관리자 이외의 용도로 연결이 필요한 경우 AWS에서 사용할 추가 원격 데스크톱 서비스 CAL을 가져와야 할 수 있습니다.

AWS 관리형 Microsoft AD 디렉터리를 만들고, 관리형 Microsoft AD와 온-프레미스 디렉터리 간에 신뢰 관계를 만들고, AWS 관리형 Microsoft AD 스키마를 확장하려면 이 섹션의 항목을 읽어보세요.

AWS

주제

- [AWS 매니지드 마이크로소프트 AD 시작하기](#)
- [AWS Managed Microsoft AD의 주요 개념](#)
- [AWS 관리형 Microsoft AD의 모범 사례](#)
- [AWS 관리형 Microsoft AD의 사용 사례](#)
- [AWS 관리형 Microsoft AD를 관리하는 방법](#)
- [AWS Managed Microsoft AD 할당량](#)
- [AWS 관리형 Microsoft AD를 위한 애플리케이션 호환성](#)
- [AWS 관리형 Microsoft AD 테스트 랩 튜토리얼](#)
- [AWS 관리형 Microsoft AD 문제 해결](#)

관련 보안 블로그 기사 AWS

- [AWS 관리형 Microsoft AD 디렉터리의 관리를 온-프레미스 Active Directory 사용자에게 위임하는 방법](#)
- [AWS 관리형 Microsoft AD를 사용하여 AWS Directory Service 보안 표준을 충족하는 데 도움이 되도록 더욱 강력한 암호 정책을 구성하는 방법](#)
- [도메인 컨트롤러를 추가하여 관리형 AWS Microsoft AD의 이중화 및 성능을 높이는 방법 AWS Directory Service](#)
- [관리형 Microsoft AD에 Microsoft 원격 데스크톱 라이선싱 관리자를 배포하여 원격 데스크톱을 사용할 수 있도록 하는 AWS 방법](#)
- [AWS 관리형 Microsoft AD 및 온-프레미스 자격 증명을 AWS Management Console 사용하여 액세스하는 방법](#)
- [AWS 관리형 Microsoft AD 및 온-프레미스 자격 AWS 증명을 사용하여 서비스에 대한 다단계 인증을 활성화하는 방법](#)
- [온-프레미스 Active Directory를 사용하여 AWS 서비스에 쉽게 로그인하는 방법](#)

AWS 매니지드 마이크로소프트 AD 시작하기

AWS 관리형 Microsoft AD는 Windows 서버 Microsoft Active Directory 2019에 의해 구동되는 완전 관리형 Microsoft AD를 생성하며 2012 R2 포리스트 및 도메인 기능 수준에서 작동합니다. AWS 클라우드 AWS Managed Microsoft AD를 사용하여 디렉터리를 만드는 경우 도메인 컨트롤러 두 개를 AWS Directory Service 만들고 사용자 대신 DNS 서비스를 추가합니다. 도메인 컨트롤러는 Amazon VPC의 여러 서브넷에 생성됩니다. 이러한 중복성은 장애가 발생하더라도 디렉터리에 계속 액세스할 수 있도록 합니다. 더 많은 도메인 컨트롤러가 필요할 경우 나중에 추가할 수 있습니다. 자세한 정보는 [추가 도메인 컨트롤러 배포](#)를 참조하세요.

주제

- [AWS 관리형 Microsoft AD 사전 요구 사항](#)
- [AWS 관리형 Microsoft AD 만들기](#)
- [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)
- [관리자 계정에 대한 권한](#)

AWS 관리형 Microsoft AD 사전 요구 사항

AWS 관리형 Microsoft AD를 생성하려면 다음과 Active Directory 같은 기능을 갖춘 Amazon VPC가 필요합니다.

- 최소 2개의 서브넷. 각 서브넷은 서로 다른 가용 영역에 있어야 합니다.
- VPC는 기본 하드웨어 테넌시를 가지고 있어야 합니다.
- 198.18.0.0/15 주소 공간의 주소를 사용하여 VPC에서 AWS 관리형 Microsoft AD를 만들 수는 없습니다.

AWS 관리형 Microsoft AD 도메인을 기존 온-프레미스 Active Directory 도메인과 통합해야 하는 경우 온프레미스 도메인의 포리스트 및 도메인 기능 수준을 Windows Server 2003 이상으로 설정해야 합니다.

AWS Directory Service 두 개의 VPC 구조를 사용합니다. 디렉터리를 구성하는 EC2 인스턴스는 AWS 계정 외부에서 실행되며 에서 관리합니다. AWSETH0 및 ETH1라는 2개의 어댑터가 있습니다. ETH0는 관리 어댑터로써 계정 외부에 위치합니다. ETH1는 계정 내부에서 생성됩니다.

디렉터리 ETH0 네트워크의 관리 IP 범위는 198.18.0.0/15입니다.

AWS IAM Identity Center 사전 요구 사항

AWS 관리형 Microsoft AD와 함께 IAM ID 센터를 사용하려는 경우 다음 사항이 해당되는지 확인해야 합니다.

- AWS 관리되는 Microsoft AD 디렉터리는 AWS 조직의 관리 계정에 설정되어 있습니다.
- IAM ID 센터의 인스턴스는 AWS 관리형 Microsoft AD 디렉터리가 설정된 지역과 동일한 지역에 있습니다.

자세한 내용은 사용 설명서의 [IAM ID 센터 사전 요구 사항을](#) 참조하십시오. AWS IAM Identity Center

다중 인증 사전 조건

AWS 관리형 Microsoft AD 디렉터를 사용하여 다단계 인증을 지원하려면 다음과 같은 방식으로 온-프레미스 또는 클라우드 기반 [원격 인증 전화 접속 사용자 서비스 \(RADIUS\)](#) 서버를 구성하여 에서 관리형 AWS Microsoft AD 디렉터리의 요청을 수락할 수 있도록 해야 합니다. AWS

1. RADIUS 서버에서 AWS 관리되는 Microsoft AD 도메인 컨트롤러 (DC) 를 모두 나타내는 두 개의 RADIUS 클라이언트를 만드십시오. AWS아래의 공통 파라미터를 이용해 두 클라이언트를 모두 구성해야 합니다(RADIUS 서버는 다를 수 있음).
 - 주소 (DNS 또는 IP): AWS 관리형 Microsoft AD DC 중 하나의 DNS 주소입니다. 두 DNS 주소 모두 MFA를 사용하려는 AWS 관리형 Microsoft AD AWS 디렉터리의 세부 정보 페이지에 있는 디렉터리 서비스 콘솔에서 찾을 수 있습니다. 표시된 DNS 주소는 에서 사용하는 AWS 관리형 Microsoft AD DC의 두 IP 주소를 나타냅니다. AWS

Note

RADIUS 서버가 DNS 주소를 지원하는 경우에는 오직 한 개의 RADIUS 클라이언트 구성만 생성해야 합니다. 그렇지 않으면 각 AWS Managed Microsoft AD DC마다 한 개의 RADIUS 클라이언트 구성을 생성해야 합니다.

- 포트 번호: RADIUS 서버가 RADIUS 클라이언트 연결을 수락하는 포트 번호를 설정합니다. 표준 RADIUS 포트는 1812입니다.
- 공유 보안: RADIUS 클라이언트를 연결하기 위해 RADIUS 서버가 사용할 공유 보안을 입력하거나 생성합니다.
- 프로토콜: AWS 관리되는 Microsoft AD DC와 RADIUS 서버 간에 인증 프로토콜을 구성해야 할 수 있습니다. 지원 프로토콜로는 PAP, CHAP MS-CHAPv1, MS-CHAPv2이 있습니다. MS-CHAPv2는 세 가지 옵션을 가진 가장 강력한 보안을 제공한다는 점에서 권장됩니다.

- 애플리케이션 이름: 일부 RADIUS 서버에서는 옵션일 수 있으며, 보통 메시지나 보고서에서 애플리케이션을 식별합니다.
2. RADIUS 클라이언트 (AWS 관리형 Microsoft AD DC DNS 주소, 1단계 참조) 에서 RADIUS 서버 포트로 향하는 인바운드 트래픽을 허용하도록 기존 네트워크를 구성합니다.
 3. 관리형 AWS Microsoft AD 도메인의 Amazon EC2 보안 그룹에 이전에 정의된 RADIUS 서버 DNS 주소 및 포트 번호로부터의 인바운드 트래픽을 허용하는 규칙을 추가합니다. 자세한 내용은 EC2 사용 설명서의 [보안 그룹에 규칙 추가](#)를 참조하세요.

AWS 관리형 Microsoft AD를 MFA와 함께 사용하는 방법에 대한 자세한 내용은 [을 참조하십시오. AWS 관리형 Microsoft AD에 대한 다중 요소 인증을 활성화합니다.](#)

AWS 관리형 Microsoft AD 만들기

디렉터리를 새로 생성하려면 다음 단계를 수행합니다. 이 절차를 시작하기 전에 [AWS 관리형 Microsoft AD 사전 요구 사항](#)에 나와 있는 선행 조건을 충족했는지 확인합니다.

AWS 관리형 Microsoft AD 디렉터리를 만들려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택한 후 디렉터리 설정을 선택합니다.
2. Select directory type(디렉터리 유형 선택) 페이지에서 AWS Managed Microsoft AD를 선택하고 Next(다음)를 선택합니다.
3. 디렉터리 정보 입력 페이지에서 다음 정보를 제공합니다.

에디션

AWS 관리형 Microsoft AD의 스탠다드 에디션 또는 엔터프라이즈 에디션 중에서 선택하세요. 에디션에 대한 자세한 내용은 [AWS Directory Service for Microsoft Active Directory](#)를 참조하세요.

디렉터리 DNS 이름

디렉터리를 위한 정규화된 이름(예: corp.example.com)입니다.

Note

DNS용 Amazon Route 53을 사용할 계획이라면 AWS 관리형 Microsoft AD의 도메인 이름은 Route 53 도메인 이름과 달라야 합니다. Route 53과 AWS 관리형 Microsoft AD가 동일한 도메인 이름을 공유하는 경우 DNS 확인 문제가 발생할 수 있습니다.

디렉터리 NetBIOS 이름

디렉터리의 짧은 이름(예: CORP)입니다.

디렉터리 설명

디렉터리에 대한 선택적 설명을 입력합니다.

관리자 암호

디렉터리 관리자의 암호입니다. 디렉터리 생성 프로세스에서는 사용자 이름 Admin와 이 암호를 사용하여 관리자 계정을 생성합니다.

암호에 "admin"이라는 말을 포함할 수 없습니다.

디렉터리 관리자 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 또한 다음 네 범주 중 세 개에 해당하는 문자를 1자 이상 포함해야 합니다.

- 소문자(a-z)
- 대문자(A-Z)
- 숫자(0-9)
- 영숫자 외의 특수 문자(~!@#\$%^&* _+=`\|(){}[]:;'"<>.,?/)

[Confirm password]

관리자 암호를 다시 입력합니다.

4. VPC 및 서브넷 선택 페이지에서 다음 정보를 제공한 후 다음을 선택합니다.

VPC

디렉터리에 대한 VPC입니다.

서브넷

도메인 컨트롤러에 대한 서브넷을 선택합니다. 두 서브넷이 서로 다른 가용 영역에 있어야 합니다.

5. 검토 및 생성 페이지에서 디렉터리 정보를 검토하고 필요한 사항을 변경합니다. 정보가 올바르면 디렉터리 생성을 선택합니다. 디렉터리 생성은 20~40분 정도 걸립니다. 생성이 완료되면 상태 값이 활성 상태로 변경됩니다.

AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목

AWS 관리형 Microsoft AD를 사용하여 Active Directory를 만드는 경우 사용자를 대신하여 다음 작업을 AWS Directory Service 수행합니다.

- ENI(탄력적 네트워크 인터페이스)를 자동으로 생성하여 각 도메인 컨트롤러에 연결합니다. 각 ENI는 AWS Directory Service VPC와 도메인 컨트롤러 간의 연결에 필수적이며 절대 삭제해서는 안 됩니다. “디렉터리 id에 대해AWS 생성된 네트워크 인터페이스”라는 AWS Directory Service 설명으로 사용하도록 예약된 모든 네트워크 인터페이스를 식별할 수 있습니다. 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [엘라스틱 네트워크 인터페이스](#)를 참조하십시오. AWS 관리형 Microsoft AD의 기본 DNS 서버는 클래스 없는 도메인 간 라우팅 (CIDR) +2에 있는 VPC DNS Active Directory 서버입니다. 자세한 내용은 Amazon VPC의 [Amazon DNS 서버](#) 사용 설명서를 참조하십시오.

Note

도메인 컨트롤러는 기본적으로 한 지역의 두 가용 영역에 배포되며 Amazon VPC (VPC)에 연결됩니다. 백업은 하루에 한 번 자동으로 수행되며 Amazon EBS (EBS) 볼륨은 암호화되어 저장된 데이터를 안전하게 보호합니다. 장애가 발생한 도메인 컨트롤러는 동일한 IP 주소를 사용하여 동일한 가용 영역에서 자동으로 교체되며, 최신 백업을 사용하여 전체 재해 복구를 수행할 수 있습니다.

- 내결함성 및 고가용성을 위해 두 개의 도메인 컨트롤러를 사용하여 VPC 내에서 Active Directory를 프로비저닝합니다. 디렉터리가 성공적으로 생성되고 [활성 상태](#)가 되면 복원력 및 성능을 높이기 위해 더 많은 도메인 컨트롤러를 프로비저닝할 수 있습니다. 자세한 정보는 [추가 도메인 컨트롤러 배포](#)를 참조하세요.

Note

AWS AWS 관리형 Microsoft AD 도메인 컨트롤러에 모니터링 에이전트를 설치할 수 없습니다.

- 도메인 컨트롤러에서 들어오고 나가는 트래픽에 대한 네트워크 규칙을 설정하는 [AWS 보안 그룹](#)을 생성합니다. 기본 아웃바운드 규칙은 생성된 AWS 보안 그룹에 연결된 모든 트래픽 ENI 또는 인스턴스를 허용합니다. 기본 인바운드 규칙은 임의의 소스(0.0.0.0/0)에서 Active Directory에 필요한 포트를 통해 전달되는 트래픽만 허용합니다. 0.0.0.0/0 규칙은 도메인 컨트롤러에 대한 트래픽이 사용자 VPC, 다른 피어링된 VPC 또는 Transit AWS Direct Connect Gateway 또는 가상 사설망을 사용하여 연결한 네트워크에서 오는 트래픽으로 제한되므로 보안 취약성을 유발하지 않습니다. AWS 보안을

강화하기 위해 생성된 ENI에는 탄력적 IP가 연결되어 있지 않으며 사용자에게 해당 ENI에 탄력적 IP를 연결할 수 있는 권한이 없습니다. 따라서 AWS 관리형 Microsoft AD와 통신할 수 있는 유일한 인바운드 트래픽은 로컬 VPC 및 VPC 라우팅 트래픽입니다. 이러한 규칙을 변경하면 도메인 컨트롤러와 통신하지 못할 수도 있으므로 특히 주의하세요. 자세한 정보는 [AWS 관리형 Microsoft AD의 모범 사례](#)를 참조하세요. 기본적으로 다음과 같은 AWS 보안 그룹 규칙이 생성됩니다.

인바운드 규칙

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
ICMP	N/A	0.0.0.0/0	Ping	LDAP Keep Alive, DFS
TCP 및 UDP	53	0.0.0.0/0	DNS	사용자 및 컴퓨터 인증, 이름 확인, 신뢰
TCP 및 UDP	88	0.0.0.0/0	Kerberos	사용자 및 컴퓨터 인증, 포리스트 수준 신뢰
TCP 및 UDP	389	0.0.0.0/0	LDAP	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP 및 UDP	445	0.0.0.0/0	SMB/CIFS	복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP 및 UDP	464	0.0.0.0/0	Kerberos 암호 변경/설정	복제, 사용자 및 컴퓨터 인증, 신뢰
TCP	135	0.0.0.0/0	복제	RPC, EPM

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP	636	0.0.0.0/0	LDAP SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP	1024~65535	0.0.0.0/0	RPC	복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP	3268 - 3269	0.0.0.0/0	LDAP GC 및 LDAP GC SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
UDP	123	0.0.0.0/0	Windows 시간	Windows 시간, 신뢰
UDP	138	0.0.0.0/0	DFSN 및 NetLogon	DFS, 그룹 정책
모두	모두	sg-##### #####	모든 트래픽	

아웃바운드 규칙

프로토콜	포트 범위	대상	트래픽 유형	Active Directory 사용
모두	모두	sg-##### #####	모든 트래픽	

- Active Directory에서 사용하는 포트 및 프로토콜에 대한 자세한 내용은 Microsoft 설명서의 [Windows 용 서비스 개요 및 네트워크 포트 요구 사항](#)을 참조하세요.

- 사용자 이름 Admin과 지정된 암호를 사용하여 디렉터리 관리자 계정을 생성합니다. 이 계정은 사용자 OU(예: Corp > 사용자) 아래에 있습니다. 이 계정을 사용하여 클라우드에서 디렉터리를 관리합니다. AWS 자세한 정보는 [관리자 계정에 대한 권한](#)을 참조하세요.

Important

이 비밀번호를 꼭 저장해 두세요. AWS Directory Service 이 암호는 저장되지 않으며 검색할 수 없습니다. 하지만 AWS Directory Service 콘솔에서 또는 [ResetUserPassword](#) API를 사용하여 비밀번호를 재설정할 수 있습니다.

- 도메인 루트 아래에 다음 3개의 조직 단위(OU)를 생성합니다.

OU 이름	설명
AWS 위임된 그룹	사용자에게 AWS 특정 권한을 위임하는 데 사용할 수 있는 모든 그룹을 저장합니다.
AWS 예약됨	모든 AWS 관리별 계정을 저장합니다.
<yourdomainname>	<p>이 OU의 이름은 디렉터리 생성 시 입력한 NetBIOS 이름에 근거를 둡니다. NetBIOS 이름을 지정하지 않을 경우 Directory DNS 이름의 첫 부분으로 기본 설정됩니다. 예를 들어, corp.example.com의 경우 NetBIOS 이름은 corp입니다. 이 OU는 모든 관련 디렉터리 개체가 소유하고 AWS 있으며 모든 AWS 관련 디렉터리 개체를 포함하고 있으며 사용자에게 전체 제어 권한이 부여됩니다. 이 OU에는 기본적으로 컴퓨터와 사용자라는 하위 OU가 있습니다.</p> <p>예:</p> <ul style="list-style-type: none"> • Corp <ul style="list-style-type: none"> • 컴퓨터 • 사용자

- AWS 위임된 그룹 OU에 다음 그룹을 생성합니다.

그룹 이름	설명
AWS 위임 계정 운영자	이 보안 그룹의 멤버는 암호 재설정 등의 제한된 계정 관리 기능을 갖습니다.
AWS 위임된 Active Directory 기반 활성화 관리자	이 보안 그룹의 멤버는 Active Directory 볼륨 라이선스 정품 인증 객체를 생성할 수 있습니다. 그러면 기업에서 이 객체를 사용하여 도메인 연결을 통해 컴퓨터를 정품 인증할 수 있습니다.
AWS 도메인 사용자에게 워크스테이션 위임 추가	이 보안 그룹의 멤버는 10개의 컴퓨터를 도메인에 조인할 수 있습니다.
AWS 위임된 관리자	이 보안 그룹의 구성원은 AWS Managed Microsoft AD를 관리하고, OU의 모든 개체를 완전히 제어하고, AWS 위임된 그룹 OU에 포함된 그룹을 관리할 수 있습니다.
AWS 위임: 개체 인증이 허용됨	이 보안 그룹의 구성원에게는 AWS 예약된 OU의 컴퓨터 리소스에 인증할 수 있는 기능이 제공됩니다 (선택적 인증이 활성화된 트러스트가 있는 온-프레미스 개체에만 필요).
AWS 도메인 컨트롤러에 위임 인증 허용	이 보안 그룹의 멤버에게는 도메인 컨트롤러 OU의 컴퓨터 리소스에 대해 인증할 수 있는 기능이 제공됩니다(선택적 인증이 설정된 신뢰가 있는 온프레미스 객체에만 필요).
AWS 위임된 삭제 객체 평생 관리자	이 보안 그룹의 구성원은 삭제된 DeletedObjectLifetime 개체를 AD 휴지통에서 복구할 수 있는 기간을 정의하는 MSDs-개체를 수정할 수 있습니다.
AWS 위임된 분산 파일 시스템 관리자	이 보안 그룹의 멤버는 FRS, DFS-R 및 DFS 이름 공간을 추가하고 제거할 수 있습니다.

그룹 이름	설명
AWS 위임된 도메인 이름 시스템 관리자	이 보안 그룹의 멤버는 Active Directory 통합 DNS를 관리할 수 있습니다.
AWS 위임된 동적 호스트 구성 프로토콜 관리자	이 보안 그룹의 멤버는 기업의 Windows DHCP 서버에 권한을 부여할 수 있습니다.
AWS 위임된 엔터프라이즈 인증 기관 관리자	이 보안 그룹의 멤버는 Microsoft Enterprise Certificate Authority 인프라를 배포하고 관리할 수 있습니다.
AWS 위임된 세분화된 암호 정책 관리자	이 보안 그룹의 멤버는 사전에 생성된 세분화된 암호 정책을 수정할 수 있습니다.
AWS 위임된 FSx 관리자	이 보안 그룹의 멤버에게는 Amazon FSx 리소스를 관리하는 기능이 제공됩니다.
AWS 위임된 그룹 정책 관리자	이 보안 그룹의 멤버는 그룹 정책 관리 작업(생성, 편집, 삭제, 연결)을 수행할 수 있습니다.
AWS 위임된 Kerberos 위임 관리자	이 보안 그룹의 멤버는 컴퓨터 및 사용자 계정 객체에 대한 위임을 활성화할 수 있습니다.
AWS 위임된 관리 서비스 계정 관리자	이 보안 그룹의 멤버는 관리형 서비스 계정을 생성하고 삭제할 수 있습니다.
AWS 위임된 MS-NPRC 비준수 장치	이 보안 그룹의 구성원은 도메인 컨트롤러와의 보안 채널 통신 요구 대상에서 제외됩니다. 이 그룹은 컴퓨터 계정용입니다.
AWS 위임된 원격 액세스 서비스 관리자	이 보안 그룹의 멤버는 RAS 및 IAS 서버 그룹에서 RAS 서버를 추가하고 제거할 수 있습니다.
AWS 위임된 복제 디렉터리 변경 관리자	이 보안 그룹의 구성원은 Active Directory의 프로필 정보를 서버와 동기화할 수 있습니다. SharePoint

그룹 이름	설명
AWS 위임된 서버 관리자	이 보안 그룹의 멤버는 모든 도메인 조인 컴퓨터의 로컬 관리자 그룹에 포함됩니다.
AWS 위임된 사이트 및 서비스 관리자	이 보안 그룹의 멤버는 Active Directory 사이트 및 서비스에서 Default-First-Site-Name 객체의 이름을 변경할 수 있습니다.
AWS 위임된 시스템 관리 관리자	이 보안 그룹의 멤버는 시스템 관리 컨테이너에서 객체를 생성하고 관리할 수 있습니다.
AWS 위임된 터미널 서버 라이선스 관리자	이 보안 그룹의 멤버는 터미널 서버 라이선스 서버 그룹에서 터미널 서버 라이선스 서버를 추가하고 제거할 수 있습니다.
AWS 위임된 사용자 계정 이름 접미사 관리자	이 보안 그룹의 멤버는 사용자 보안 주체 이름 접미사를 추가하고 제거할 수 있습니다.

- 다음 GPO(그룹 정책 객체)를 생성하고 적용합니다.

Note

사용자는 이러한 GPO를 삭제, 수정, 연결 해제할 권한이 없습니다. 이는 사용하도록 예약되어 있으므로 의도적으로 설계된 것입니다. AWS 필요한 경우 제어하는 OU에 연결할 수 있습니다.

그룹 정책 이름	적용 대상	설명
기본 도메인 정책	도메인	도메인 암호 및 Kerberos 정책을 포함합니다.
ServerAdmins	모든 비도메인 컨트롤러 컴퓨터 계정	AWS '위임된 서버 관리자'를 BUILTIN/Administrators 그룹의 구성원으로 추가합니다.

그룹 정책 이름	적용 대상	설명
AWS 예약 정책:사용자	AWS 예약된 사용자 계정	AWS 예약된 OU의 모든 사용자 계정에 대한 권장 보안 설정을 설정합니다.
AWS 관리형 액티브 디렉터리 정책	모든 도메인 컨트롤러	모든 도메인 컨트롤러에 대해 권장되는 보안 설정을 지정합니다.
TimePolicyNT5DS	모든 비PDCe 도메인 컨트롤러	모든 비PDCe 도메인 컨트롤러 시간 정책에서 Windows 시간(NT5DS)을 사용하도록 설정합니다.
TimePolicyPDC	PDCe 도메인 컨트롤러	PDCe 도메인 컨트롤러의 시간 정책에서 NTP(Network Time Protocol)를 사용하도록 설정합니다.
기본 도메인 컨트롤러 정책	사용되지 않습니다	도메인 생성 중에 AWS 프로비전되는 관리형 Active Directory 정책이 대신 사용됩니다.

각 GPO의 설정을 보려면 [GPMC\(그룹 정책 관리 콘솔\)](#)를 활성화한 상태에서 도메인에 조인된 Windows 인스턴스에서 해당 설정을 볼 수 있습니다.

관리자 계정에 대한 권한

Microsoft Active AWS Directory용 디렉터리 서비스를 만들면 AWS 관련된 모든 그룹과 계정을 저장할 OU (조직 구성 단위)가 AWS 만들어집니다. 이 OU에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)를 참조하세요. 여기에는 관리자 계정이 포함됩니다. 관리자 계정은 해당 OU에 대해 다음과 같은 일반적인 관리 활동을 수행하는 권한을 가집니다.

- 사용자, 그룹 및 컴퓨터를 추가하거나 업데이트하거나 삭제합니다. 자세한 정보는 [AWS Managed Microsoft AD에서의 사용자 및 그룹 관리](#)을 참조하세요.

- 도메인(예: 파일 또는 인쇄 서버)에 리소스를 추가한 다음 OU 내의 사용자 및 그룹에 해당 리소스에 대한 권한 할당.
- 추가 OU 및 컨테이너 생성.
- 추가 OU 및 컨테이너의 권한을 위임합니다. 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.
- 그룹 정책 생성 및 연결.
- Active Directory 휴지통에서 삭제된 객체 복원.
- 액티브 디렉터리 웹 서비스에서 액티브 디렉터리 및 DNS Windows PowerShell 모듈을 실행합니다.
- 그룹 관리형 서비스 계정을 생성하고 구성합니다. 자세한 정보는 [그룹 관리형 서비스 계정](#)을 참조하세요.
- Kerberos 제한된 위임을 구성합니다. 자세한 정보는 [Kerberos 제한된 위임](#)을 참조하세요.

또한 관리자 계정은 다음과 같은 도메인 차원 활동을 수행할 권한이 있습니다.

- DNS 구성 관리(레코드, 영역 및 전달자 추가, 제거 또는 업데이트)
- DNS 이벤트 로그 보기
- 보안 이벤트 로그 보기

여기 나열된 작업만 관리자 계정에 허용됩니다. 관리자 계정은 특정 OU(예: 상위 OU) 외부의 디렉터리 관련 작업들에 대한 권한이 없습니다.

Important

AWS 도메인 관리자는 호스팅되는 모든 도메인에 대한 전체 관리 액세스 권한을 AWS가 집니다. 디렉터리 정보를 포함하여 AWS 시스템에 저장하는 콘텐츠를 AWS 처리하는 방법에 대한 자세한 내용은 계약 AWS 및 [AWS 데이터 보호 FAQ](#)를 참조하십시오.

Note

이 계정을 삭제하거나 이름을 바꾸지 않는 것이 좋습니다. 계정을 더 이상 사용하지 않으려면 긴 암호(64자 이하의 임의 문자)를 설정한 다음 계정을 비활성화하는 것이 좋습니다.

엔터프라이즈 및 도메인 관리자 권한 계정

AWS 기본 제공 관리자 암호를 90일마다 임의 암호로 자동 교체합니다. 사람이 사용할 수 있도록 기본 제공되는 관리자 암호를 요청할 때마다 AWS 티켓이 생성되어 AWS Directory Service 팀에 기록됩니다. 보안 인증 정보는 암호화되어 보안 채널을 통해 처리됩니다. 또한 관리자 계정 자격 증명은 AWS Directory Service 관리팀만 요청할 수 있습니다.

디렉토리의 운영 관리를 수행하기 위해 엔터프라이즈 관리자 및 도메인 관리자 권한이 있는 계정을 독점적으로 관리합니다. AWS 여기에는 Active Directory 관리자 계정에 대한 독점적 제어가 포함됩니다. AWS 암호 저장소를 사용하여 암호 관리를 자동화하여 이 계정을 보호합니다. 관리자 암호가 자동으로 교체되는 동안는 임시 사용자 계정을 AWS 만들고 이 계정에 도메인 관리자 권한을 부여합니다. 이 임시 계정은 관리자 계정에서 암호 교체 실패 시 백업으로 사용됩니다. 관리자 암호를 AWS 성공적으로 교체한 후 임시 관리자 계정을 AWS 삭제합니다.

일반적으로 디렉터리 전체를 자동화를 통해 AWS 운영합니다. 자동화 프로세스로 운영 문제를 해결할 AWS 수 없는 경우 지원 엔지니어가 도메인 컨트롤러 (DC) 에 로그인하여 진단을 수행하도록 해야 할 수 있습니다. 드문 경우이긴 하지만 예서는 액세스 권한을 부여하는 요청/알림 시스템을 AWS 구현합니다. 이 프로세스에서 AWS 자동화를 통해 디렉터리에 도메인 관리자 권한이 있는 기간 제한 사용자 계정이 생성됩니다. AWS 사용자 계정을 디렉터리에서 작업하도록 배정된 엔지니어와 연결합니다. AWS 이 연결을 로그 시스템에 기록하고 엔지니어에게 사용할 자격 증명을 제공합니다. 엔지니어가 취하는 모든 행동은 Windows 이벤트 로그에 기록됩니다. 할당된 시간이 경과되면 자동화에서는 사용자 계정을 삭제합니다.

디렉터리에서 로그 전송 기능을 사용하여 관리자 계정을 모니터링할 수 있습니다. 이 기능을 사용하면 AD Security 이벤트를 CloudWatch 시스템에 전달하여 모니터링 솔루션을 구현할 수 있습니다. 자세한 정보는 [로그 전송 활성화](#)를 참조하세요.

누군가가 대화식으로 DC에 로그인하면 보안 이벤트 ID 4624, 4672, 4648이 모두 기록됩니다. 도메인에 조인된 Windows 컴퓨터에서 이벤트 뷰어 Microsoft Management Console(MMC)을 사용하여 각 DC의 Windows 보안 이벤트 로그를 볼 수 있습니다. 모든 보안 이벤트 로그를 계정의 Logs (로그) [로그 전송 활성화](#) 로 CloudWatch 보낼 수도 있습니다.

AWS 예약된 OU 내에서 사용자가 생성되고 삭제되는 경우가 간혹 있을 수 있습니다. AWS 사용자에게 액세스 및 관리 권한을 위임하지 않은 이 OU와 기타 OU 또는 컨테이너에 있는 모든 개체의 관리 및 보안을 책임집니다. 해당 OU에서 생성 및 삭제를 확인할 수 있습니다. 이는 자동화를 AWS Directory Service 사용하여 도메인 관리자 암호를 정기적으로 교체하기 때문입니다. 암호가 교체되면 교체가 실패할 경우를 대비하여 백업이 생성됩니다. 교체가 성공하면 백업 계정이 자동으로 삭제됩니다. 또한 문제 해결을 위해 DC에 대화형 액세스가 필요한 드문 경우에도 AWS Directory Service 엔지니어가 사용할 임시 사용자 계정을 생성합니다. 엔지니어가 작업을 완료하면 임시 사용자 계정이 삭제됩니다. 디렉

터리에 대한 대화형 자격 증명이 요청될 때마다 AWS Directory Service 관리 팀에 알림이 전송된다는 점에 유의하세요.

AWS Managed Microsoft AD의 주요 개념

다음 주요 개념을 익히면 AWS Managed Microsoft AD를 최대한 활용할 수 있습니다.

주제

- [Active Directory 스키마](#)
- [AWS Managed Microsoft AD에 대한 패치 적용 및 유지 관리](#)
- [그룹 관리형 서비스 계정](#)
- [Kerberos 제한된 위임](#)

Active Directory 스키마

스키마는 분산형 디렉터리의 일부인 속성 및 클래스 정의로서, 데이터베이스의 필드 및 테이블과 유사합니다. 스키마에는 데이터베이스에 추가 또는 포함할 수 있는 데이터의 유형 및 형식을 결정하는 규칙 세트가 포함되어 있습니다. 사용자 클래스는 데이터베이스에 저장된 클래스의 한 예입니다. 몇 가지 예제의 사용자 클래스 속성에는 사용자의 이름, 성, 전화 번호 등이 포함될 수 있습니다.

스키마 요소

속성, 클래스 및 객체는 스키마에서 객체를 정의하는 데 사용되는 기본 요소입니다. 아래에는 AWS Managed Microsoft AD 스키마를 확장하기 위한 프로세스를 시작하기 전에 반드시 알아야 할 스키마 요소에 대한 세부 사항이 나와 있습니다.

Attributes

데이터베이스의 필드와 유사한 각 스키마 속성은 속성의 특성을 정의하는 몇 가지 프로퍼티 (property)를 가지고 있습니다. 예를 들면 속성에 대한 읽기 및 쓰기 작업을 위해 LDAP 클라이언트가 사용하는 프로퍼티는 LDAPDisplayName입니다. LDAPDisplayName 프로퍼티는 모든 속성 및 클래스에서 고유해야 합니다. 속성 특성에 대한 전체 목록은 MSDN 웹사이트의 [속성의 특성](#)을 참조하세요. 새 속성을 생성하는 방법에 대한 추가 지침은 MSDN 웹사이트의 [새 속성 정의](#)를 참조하세요.

클래스

클래스는 데이터베이스의 테이블과 유사하며 몇 가지 프로퍼티가 정의되어 있습니다. 예를 들어 objectClassCategory는 클래스 카테고리를 정의합니다. 클래스 특성에 대한 전체 목록은

MSDN 웹사이트의 [객체 클래스의 특성](#)을 참조하세요. 새 클래스를 생성하는 방법은 MSDN 웹사이트의 [새 클래스 정의](#)를 참조하세요.

객체 식별자(OID)

각 클래스와 속성은 모든 객체에 대해 고유한 OID를 가져야 합니다. 고유성을 보장하려면 소프트웨어 벤더들이 자체 OID를 획득해야 합니다. 고유성은 1개 이상의 애플리케이션에서 서로 다른 용도로 동일한 속성이 사용될 때 충돌을 방지합니다. 고유성 보장을 위해 ISO 이름 등록 권한으로부터 루트 OID를 획득할 수 있습니다. 또는 Microsoft로부터 기본 OID를 획득할 수 있습니다. OID 및 OID 획득 방법에 대한 자세한 내용은 MSDN 웹사이트의 [객체 식별자](#)를 참조하세요.

스키마에 링크 연결된 속성

몇몇 속성들은 전방 링크와 후방 링크를 통해 2개의 클래스 간에 연결됩니다. 대표적인 예가 그룹입니다. 그룹을 검색하면 그룹의 멤버를 알 수 있고, 사용자를 검색하면 그룹의 소속을 알 수 있습니다. 그룹에 사용자를 추가하면 Active Directory가 그룹에 대한 전방 링크를 생성합니다. 그런 다음, Active Directory가 그룹에서 사용자로 이어지는 후방 링크를 추가합니다. 링크로 연결될 속성을 생성할 때 고유 링크 ID를 생성해야 합니다. 자세한 내용은 MSDN 웹사이트의 [링크 연결 속성](#)을 참조하세요.

관련 주제

- [AWS Managed Microsoft AD 스키마를 확장해야 하는 경우](#)
- [자습서: AWS 관리형 Microsoft AD 스키마 확장](#)

AWS Managed Microsoft AD에 대한 패치 적용 및 유지 관리

AWS용 AWS DS라고도 하는 AWS Directory Service for Microsoft Active Directory는 사실상 관리형 서비스로 제공되는 Microsoft Active Directory Domain Services(AD DS)입니다. 이 시스템은 도메인 컨트롤러(DC)에서 Microsoft Windows Server 2019를 사용하고, AWS는 서비스 관리를 목적으로 DC에 소프트웨어를 추가합니다. AWS는 DC를 업데이트(패치)하여 새 기능을 추가하고 Microsoft Windows Server 소프트웨어를 업데이트 상태로 유지합니다. 패치 프로세스 중에도 디렉터리는 계속 사용할 수 있습니다.

가용성 보장

기본적으로 각 디렉터리는 두 개의 DC로 이루어져 있으며, 각 DC는 서로 다른 가용 영역에 설치되어 있습니다. 필요에 따라 DC를 추가하여 가용성을 더욱 높일 수 있습니다.고가용성과 내결함성이 필요한 중요 환경의 경우 DC를 추가로 배포하는 것이 좋습니다. AWSDC에 순차적으로 패치를 적용하

는데, 이 기간 동안에는 현재 패치를 적용하고 있는 DC를 사용할 수 없습니다. AWS 하나 이상의 DC가 일시적으로 사용 불가능한 상태인 경우에는 디렉터리에서 작동 중인 DC가 최소 두 개가 될 때까지 AWS가 패치를 연기합니다. 이렇게 하면 패치 프로세스 동안에도 작동 중인 다른 DC를 사용할 수 있습니다. 여기에 걸리는 시간은 각기 다를 수 있지만 보통 30~45분이 소요됩니다. 하나 이상의 DC가 패치를 포함해 어떤 이유로든 사용 불가능한 상태일 때 애플리케이션이 작동 중인 DC에 도달할 수 있도록 하려면 애플리케이션이 정적 DC 주소가 아닌, Windows DC 로케이터 서비스를 사용해야 합니다.

패치 적용 일정 파악

AWS는 DC에서 Microsoft Windows Server 소프트웨어를 최신 상태로 유지하기 위해 Microsoft 업데이트를 사용합니다. Microsoft는 월별 롤업 패치를 Windows Server에서 지원하기 때문에 AWS는 3주 내에 테스트를 거쳐 모든 고객 DC에 롤업을 적용하기 위해 노력합니다. 뿐만 아니라 AWS는 DC에 대한 적용 가능성과 긴급성에 따라 월별 롤업 외에 Microsoft가 발표하는 업데이트를 검토합니다. Microsoft가 중대 또는 중요로 평가하고 DC와 관련이 있는 보안 패치의 경우, AWS는 5일 내에 패치를 테스트하여 배포하기 위해 노력합니다.

그룹 관리형 서비스 계정

Windows Server 2012에서 Microsoft는 관리자가 그룹 관리형 서비스 계정(gMSA)이라는 서비스 계정을 관리하는 데 사용할 수 있는 새로운 방법을 도입했습니다. gMSA를 사용하면 서비스 인스턴스 간 암호 동기화를 더 이상 서비스 관리자가 수동으로 관리할 필요가 없습니다. 대신, 관리자가 Active Directory에 gMSA를 생성한 후 이 단일 gMSA를 사용하는 여러 서비스 인스턴스를 구성하면 됩니다.

AWS Managed Microsoft AD에서 사용자가 gMSA를 생성할 수 있도록 권한을 부여하려면, 사용자의 계정을 AWS위임 관리형 서비스 계정 관리자 보안 그룹의 멤버로 추가해야 합니다. 기본적으로 관리자 계정은 이 그룹의 멤버입니다. GMSA에 대한 자세한 내용은 Microsoft 웹 사이트의 [그룹 관리 서비스 계정 개요를 참조하십시오](#). TechNet

관련 AWS 보안 블로그 게시물

- [AWS관리형 Microsoft AD를 사용하여 배포를 간편하게 수행하고 Active Directory-Integrated .NET 애플리케이션의 보안을 강화하는 방법](#)

Kerberos 제한된 위임

Kerberos 제한 위임은 Windows Server의 새 기능입니다. 이 기능은 서비스 관리자에게 애플리케이션 서비스가 사용자 대신 작동할 수 있는 범위를 제한하여 애플리케이션 신뢰 경계를 지정 및 시행할 수 있는 능력을 제공합니다. 이 기능은 어느 프론트 엔드 서비스 계정이 백엔드 서비스에 위임할 수 있는

지 구성해야 할 때 유용할 수 있습니다. 또한 Kerberos 제한된 위임은 gMSA가 Active Directory 사용자 대신 어떠한 서비스에도 연결하는 것을 방지하여 악의의 개발자에 의해 남용될 가능성을 배제합니다.

예를 들어 사용자 jsmith가 HR 애플리케이션에 로그인한다고 가정합니다. SQL Server가 jsmith의 데이터베이스 권한을 적용하기를 원합니다. 그러나 기본적으로 SQL Server는 jsmith의 구성된 권한 대신 hr-app-service의 권한을 적용하는 서비스 계정 자격 증명을 사용하여 데이터베이스 연결을 엽니다. HR 급여 애플리케이션이 jsmith의 자격 증명을 사용하여 SQL Server 데이터베이스에 액세스할 수 있도록 해야 합니다. 이렇게 하려면 관리형 AWS Microsoft AD 디렉터리의 hr-app-service 서비스 계정에 대해 Kerberos 제한 위임을 사용하도록 설정합니다. AWS jsmith가 로그인하면 Active Directory는 jsmith가 네트워크에서 다른 서비스에 액세스하려고 시도할 경우 Windows가 자동으로 사용하는 Kerberos 티켓을 제공합니다. Kerberos 위임을 통해 해당 hr-app-service 계정은 데이터베이스에 액세스할 때 jsmith Kerberos 티켓을 재사용할 수 있으므로 데이터베이스 연결을 열 때 jsmith에만 해당하는 권한이 적용됩니다.

AWS Managed Microsoft AD의 사용자가 Kerberos 제한 위임을 구성할 수 있는 권한을 부여하려면, 해당 사용자의 계정을 AWS 위임 Kerberos 위임 관리자 보안 그룹의 멤버로 추가해야 합니다. 기본적으로 관리자 계정은 이 그룹의 멤버입니다. Kerberos 제한된 위임에 대한 자세한 내용은 Microsoft 웹 사이트의 [Kerberos 제한된 위임](#) 개요를 참조하십시오. TechNet

[리소스 기반 제한된 위임](#)은 Windows Server 2012에서 도입되었습니다. 이 위임은 백엔드 서비스 관리자에게 서비스에 대한 제한된 위임을 구성할 수 있는 기능을 제공합니다.

AWS 관리형 Microsoft AD의 모범 사례

다음은 문제를 방지하고 AWS 관리형 Microsoft AD를 최대한 활용하기 위해 고려해야 할 몇 가지 제안 및 지침입니다.

설정: 사전 조건

디렉터리를 생성하기 전에 여기 나온 가이드라인을 고려하세요.

디렉터리 유형이 올바른지 확인

AWS Directory Service 다른 AWS 서비스와 Microsoft Active Directory 함께 사용할 수 있는 여러 가지 방법을 제공합니다. 예산에 맞는 비용으로 필요한 기능을 갖춘 디렉터리 서비스를 선택할 수 있습니다.

- AWS Microsoft Active Directory용 디렉터리 서비스는 클라우드에서 Microsoft Active Directory 호스팅되는 기능이 풍부한 관리형 서비스입니다. AWS 사용자 5,000명 이상이고 AWS 호스팅된

디렉터리와 온-프레미스 디렉터리 간에 신뢰 관계를 설정해야 하는 경우 관리형 Microsoft AD를 사용하는 것이 가장 좋습니다.

- AD Connector는 단순히 기존 Active Directory 온-프레미스에 AWS연결합니다. AD Connector는 AWS 서비스와 함께 기존의 온프레미스 디렉터리를 사용하고 싶을 때 가장 적합한 옵션입니다.
- Simple AD는 기본 Active Directory 호환성을 갖춘 소규모의 저렴한 디렉토리입니다. 5,000명 이하의 사용자, Samba 4 호환 애플리케이션, LDAP 인식 애플리케이션을 위한 LDAP 호환성을 지원합니다.

AWS Directory Service 옵션에 대한 자세한 비교는 [여기](#)를 참조하십시오. [무엇을 선택할 것인가](#)

VPC와 인스턴스가 올바르게 구성되도록 보장

디렉터리를 연결, 관리 및 사용하려면 디렉터리와 연관이 있는 VPC를 제대로 구성해야 합니다.

VPC 보안 및 네트워킹 요건에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 사전 요구 사항](#), [AD Connector 사전 조건](#) 또는 [간단한 AD 사전 조건](#) 섹션을 참조하세요.

도메인에 인스턴스를 추가하는 경우에는 [Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory](#)에 설명된 대로 인스턴스에 대한 연결 및 원격 액세스가 가능한지 확인하세요.

한도에 유의

특정 디렉터리 유형에 대한 다양한 제한에 대해 알아보십시오. 가용 스토리지와 객체의 전체 크기가 디렉터리에 저장할 수 있는 객체 수에 대한 유일한 제한입니다. 선택한 디렉터리에 대한 자세한 내용은 [AWS Managed Microsoft AD 할당량](#), [AD Connector 할당량](#) 또는 [Simple AD 할당량](#) 섹션을 참조하세요.

디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오.

AWS [보안 그룹](#)을 생성하여 디렉터리의 도메인 컨트롤러 [엘라스틱 네트워크 인터페이스](#)에 연결합니다. 이 보안 그룹은 도메인 컨트롤러로의 불필요한 트래픽을 차단하고 Active Directory 통신에 필요한 트래픽을 허용합니다. AWS는 Active Directory 통신에 필요한 포트만 열도록 보안 그룹을 구성합니다. 기본 구성에서 보안 그룹은 모든 IP 주소에서 이러한 포트에 들어오는 트래픽을 수락합니다. AWS [피어링되거나 크기가 조정된 VPC 내에서 액세스할 수 있는 도메인 컨트롤러의 인터페이스에 보안 그룹을 연결합니다](#). 이러한 인터페이스는 사용자가 라우팅 테이블을 수정하고, VPC에 대한 네트워크 연결을 변경하고, [NAT 게이트웨이 서비스](#)를 구성하더라도 인터넷에서 액세스할 수 없습니다. 따라서 VPC로의 네트워크 경로가 있는 인스턴스 및 컴퓨터만 디렉터리에 액세스할 수 있습니다. 그러면 특정 주소 범위를 구성할 필요가 없어져 설정이 간소화됩니다. 대신, 신뢰할 수 있는 인스턴스 및 컴퓨터에서 전송되는 트래픽만 허용하는 VPC로 라우팅 및 보안 그룹을 구성합니다.

디렉터리 보안 그룹 수정

디렉터리의 보안 그룹에 대한 보안을 개선하려면 보다 제한적 목록의 IP 주소로부터의 트래픽을 수락하도록 보안 그룹을 수정할 수 있습니다. 예를 들어 수락된 주소를 0.0.0.0/0에서 단일 서브넷 또는 컴퓨터에 고유한 CIDR 범위로 변경할 수 있습니다. 또는 도메인 컨트롤러가 통신할 수 있는 대상 주소를 제한하도록 선택할 수도 있습니다. 단, 보안 그룹 필터링이 어떻게 작동하는지 완전히 이해하는 경우에만 이렇게 변경하세요. 자세한 내용은 Amazon EC2 사용 설명서의 [Linux 인스턴스용 Amazon EC2 보안 그룹](#)을 참조하세요. 잘못 변경하면 의도한 컴퓨터 및 인스턴스와의 통신이 끊길 수 있습니다. AWS 도메인 컨트롤러에 포트를 추가로 열려고 하면 디렉터리 보안이 저하되므로 사용하지 않는 것이 좋습니다. [AWS 공동 책임 모델](#)을 자세히 검토하세요.

Warning

디렉터리가 사용하는 보안 그룹을 생성하는 EC2 인스턴스에 연결하는 것이 기술적으로 가능합니다. 하지만 이 AWS 방법을 사용하지 않는 것이 좋습니다. AWS 관리 디렉터리의 기능 또는 보안 요구 사항을 해결하기 위해 사전 공지 없이 보안 그룹을 수정해야 할 이유가 있을 수 있습니다. 이러한 변경은 디렉터리 보안 그룹과 연결된 모든 인스턴스에 영향을 미칩니다. 또한 디렉터리 보안 그룹을 EC2 인스턴스와 연결하면 EC2 인스턴스에 잠재적 보안 위험이 생깁니다. 디렉터리 보안 그룹은 필요한 Active Directory 포트에서 모든 IP 주소로부터 전송된 트래픽을 수락합니다. 이 보안 그룹을 인터넷에 연결된 퍼블릭 IP 주소를 갖는 EC2 인스턴스와 연결할 경우 인터넷 상의 모든 컴퓨터가 개방된 포트에서 EC2 인스턴스와 통신할 수 있습니다.

설정: 디렉터리 생성

여기에는 디렉터리를 생성할 때 고려해야 할 몇 가지 제안이 나와 있습니다.

관리자 ID 및 암호를 기억

디렉터리를 설정할 때 관리자 계정에 대한 암호를 제시합니다. 해당 계정 ID는 AWS 관리형 Microsoft AD의 관리자입니다. 이 계정에 대해 생성한 암호를 기억하세요. 그렇지 않으면 디렉터리에 객체를 추가할 수 없습니다.

DHCP 옵션 세트 생성

디렉터리에 대한 DHCP 옵션 세트를 생성하고 AWS Directory Service 디렉터리가 있는 VPC에 DHCP 옵션 세트를 할당하는 것이 좋습니다. 이렇게 해야 해당 VPC의 모든 인스턴스가 지정된 도메인을 가리키고 DNS 서버가 도메인 이름을 해석할 수 있습니다.

DHCP 옵션 세트에 대한 자세한 내용은 [DHCP 옵션 세트 생성 또는 변경](#)를 참조하세요.

조건부 전달자 설정 활성화

다음 조건부 전달 설정 이 조건부 전달자를 Active Directory에 저장하고 다음과 같이 복제하십시오. 활성화해야 합니다. 이러한 설정을 사용하면 인프라 장애 또는 과부하 장애로 인해 노드가 교체될 때 조건부 전달자 설정이 사라지는 것을 방지할 수 있습니다.

추가 도메인 컨트롤러 배포

기본적으로는 별도의 가용 영역에 있는 두 개의 도메인 컨트롤러를 AWS 생성합니다. 이렇게 하면 소프트웨어 패칭 및 하나의 도메인 컨트롤러를 연결 또는 사용 불가로 만들 수 있는 다른 이벤트 중 결합 복원력이 제공됩니다. [추가 도메인 컨트롤러를 배포](#)하여 도메인 컨트롤러 또는 가용 영역에 대한 액세스에 영향을 미치는 장기 이벤트 발생 시 회복성을 한층 높이고 확장 성능을 확보할 것을 권장합니다.

자세한 정보는 [Windows DC 로케이터 서비스 사용](#)을 참조하세요.

AWS 애플리케이션에 대한 사용자 이름 제한 이해

AWS Directory Service 사용자 이름 구성에 사용할 수 있는 대부분의 문자 형식을 지원합니다. 그러나 Amazon WorkMail, WorkSpaces WorkDocs Amazon 또는 Amazon과 같은 AWS 애플리케이션에 로그인하는 데 사용되는 사용자 이름에는 문자 제한이 적용됩니다. QuickSight 이러한 제한 때문에 다음 문자는 사용할 수 없습니다.

- 공백
- 멀티바이트 문자
- !"#%&'()*+/,/;<=>?@[]^_{}`~

Note

@ 기호는 UPN 접미사 앞에서만 허용됩니다.

디렉터리 사용

여기에는 디렉터리를 사용할 때 고려해야 할 몇 가지 제안이 나와 있습니다.

사전 정의된 사용자, 그룹, 조직 단위를 변경하지 말 것

를 AWS Directory Service 사용하여 디렉터리를 시작하면 디렉터리의 모든 개체가 포함된 OU (조직 구성 단위) 가 AWS 생성됩니다. 디렉터리를 만들 때 입력한 NetBIOS 이름을 가진 이 OU는 도메인 루

트에 있습니다. 도메인 루트는 에서 소유하고 관리합니다 AWS. 몇몇 그룹 및 관리 사용자도 생성됩니다.

이렇게 사전 정의된 객체들은 어떤 방식으로든 이동, 삭제 또는 변경해서는 안 됩니다. 이렇게 하면 본인과 AWS사용자 모두 디렉터리에 액세스할 수 없게 될 수 있습니다. 자세한 정보는 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)을 참조하세요.

도메인을 자동 조인

AWS Directory Service 도메인에 속할 Windows 인스턴스를 시작할 때는 나중에 인스턴스를 수동으로 추가하는 것보다 인스턴스 생성 프로세스의 일부로 도메인에 가입하는 것이 가장 쉬운 경우가 많습니다. 새로운 인스턴스를 시작할 때 [Domain join directory]에 대한 올바른 디렉터리를 선택하기만 하면 도메인을 자동으로 조인할 수 있습니다. [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#)에서 자세한 내용을 확인할 수 있습니다.

신뢰를 올바르게 설정

AWS 관리형 Microsoft AD 디렉터리와 다른 디렉터리 간에 신뢰 관계를 설정할 때는 다음 지침을 염두에 두십시오.

- 신뢰 유형이 양쪽에서 일치해야 합니다(포리스트 또는 외부).
- 단방향 신뢰를 사용하는 경우 신뢰 방향이 올바르게 설정되었는지 확인합니다(신뢰하는 도메인에서 발신, 신뢰된 도메인에서 수신).
- FQDN(정규화된 도메인 이름)과 NetBIOS 이름은 모두 포리스트/도메인 간에 고유해야 합니다.

신뢰 관계 설정에 대한 세부적인 내용과 구체적인 지침은 [신뢰 관계 생성](#)를 참조하세요.

디렉터리 관리

디렉터리 관리 시 이러한 제안들을 고려하세요.

도메인 컨트롤러 성능 추적

규모 조정 결정을 최적화하고 디렉터리 복원력 및 성능을 개선하려면 CloudWatch 메트릭을 사용하는 것이 좋습니다. 자세한 정보는 [성능 지표로 도메인 컨트롤러 모니터링](#)을 참조하세요.

CloudWatch 콘솔을 사용하여 도메인 컨트롤러 메트릭을 설정하는 [방법에 대한 지침은 AWS 보안 블로그의 사용자 지표를 기반으로 AWS Managed Microsoft AD 조정을 자동화하는 방법](#)을 참조하십시오.

스키마 확장을 위한 면밀한 계획

스키마 확장을 신중하게 적용하여 중요하고 빈번한 쿼리에 대한 디렉터리를 인덱싱하세요. 인덱스는 디렉터리 공간을 사용하고 빠르게 변화하는 인덱싱 값으로 인해 성능에 문제가 발생할 수 있으므로 디렉터리를 지나치게 인덱싱하지 않도록 조심하세요. 인덱스를 추가하려면 LDAP(Lightweight Directory Access Protocol) LDIF(Lightweight Directory Interchange Format) 파일을 생성하고 스키마 변경을 확장해야 합니다. 자세한 정보는 [스키마 확장](#)을 참조하세요.

로드 밸런서 소개

AWS 관리형 Microsoft AD 엔드포인트 앞에는 로드 밸런서를 사용하지 마십시오. Microsoft는 외부 로드 밸런싱 없이 반응성이 뛰어난 운영 도메인 컨트롤러(DC)를 검색하는 DC 검색 알고리즘과 함께 사용할 수 있는 Active Directory(AD)를 설계하였습니다. 외부 네트워크 로드 밸런서에서는 활성 DC를 부정확하게 감지하므로 현재 제공되고 있고 있긴 하나 사용할 준비가 안 된 DC로 애플리케이션이 전송되는 일이 발생할 수 있습니다. 자세한 내용은 외부 [로드 밸런서를 구현하는 대신 Active Directory를 올바르게 사용하도록 응용 프로그램을 수정하도록 TechNet 권장하는 Microsoft의 Active Directory와 로드 밸런서를 참조하십시오.](#)

인스턴스의 백업 만들기

기존 AWS Directory Service 도메인에 인스턴스를 수동으로 추가하려는 경우 먼저 해당 인스턴스를 백업하거나 스냅샷을 만드십시오. 이 기능은 특히 Linux 인스턴스를 조인할 때 중요합니다. 인스턴스 추가에 사용되는 일부 절차들로 인해(올바르게 수행되지 않은 경우) 인스턴스 접속이나 사용이 불가능해질 수 있습니다. 자세한 정보는 [디렉터리 스냅샷 또는 복구](#)을 참조하세요.

SNS 메시징 설정

Amazon Simple Notification Service (Amazon SNS)에서는 디렉터리 상태가 바뀔 때 이메일 또는 텍스트(SMS) 메시지를 수신할 수 있습니다. 디렉터리가 [Active] 상태에서 [Impaired] 또는 [Inoperable] 상태로 바뀔 경우 알림을 받게 됩니다. 디렉터리가 Active 상태로 돌아갈 때도 알림을 받게 됩니다.

또한 메시지를 수신하는 SNS 주제가 있는 경우 Amazon SNS 콘솔에서 AWS Directory Service 해당 주제를 삭제하기 전에 디렉토리를 다른 SNS 주제와 연결해야 합니다. 그렇지 않으면 중요한 디렉터리 상태 메시지가 누락될 위험이 있습니다. Amazon SNS 설정 방법에 대한 자세한 내용은 [Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.](#) 단원을 참조하세요.

디렉터리 서비스 설정 적용

AWS 관리형 Microsoft AD를 사용하면 규정 준수 및 보안 요구 사항에 맞게 보안 구성을 조정할 수 있습니다. AWS Managed Microsoft AD는 새 지역이나 도메인 컨트롤러를 추가하는 경우를 포함하여 디

렉터리의 모든 도메인 컨트롤러에 구성을 배포하고 유지 관리합니다. 모든 새 디렉터리와 기존 디렉터리에 대해 이러한 보안 설정을 구성하고 적용할 수 있습니다. 콘솔에서 API의 단계를 [디렉터리 보안 설정 편집](#) 따르거나 [UpdateSettings API](#)를 통해 이 작업을 수행할 수 있습니다.

자세한 정보는 [보안 설정 구성](#)을 참조하세요.

디렉터리를 삭제하기 전에 Amazon 엔터프라이즈 애플리케이션을 제거

Amazon WorkSpaces 애플리케이션 관리자, Amazon WorkSpaces, Amazon 또는 Amazon RDS (Amazon RDS)와 같은 하나 이상의 Amazon WorkMail 엔터프라이즈 애플리케이션과 연결된 디렉터리를 삭제하기 전에 먼저 각 애플리케이션을 제거해야 합니다. WorkDocs AWS Management Console 애플리케이션 제거 방법에 관한 자세한 내용은 [AWS 관리형 Microsoft AD 삭제](#) 단원을 참조하세요.

SYSVOL 및 NETLOGON 공유에 액세스할 때 SMB 2.x 클라이언트 사용

클라이언트 컴퓨터는 SMB (서버 메시지 블록)를 사용하여 관리형 AWS Microsoft AD 도메인 컨트롤러의 SYSVOL 및 NETLOGON 공유에 액세스하여 그룹 정책, 로그인 스크립트 및 기타 파일에 액세스합니다. AWS 관리형 Microsoft AD는 SMB 버전 2.0 (SMBv2) 이상만 지원합니다.

SMBv2 및 최신 버전 프로토콜에는 클라이언트 성능을 개선하고 도메인 컨트롤러와 클라이언트의 보안을 향상시키는 여러 가지 기능이 추가되었습니다. 이러한 변경 사항은 SMBv1을 비활성화하라는 [미국 컴퓨터 비상 준비 팀](#)과 [Microsoft](#)의 권장 사항을 따릅니다.

Important

현재 SMBv1 클라이언트를 사용하여 도메인 컨트롤러의 SYSVOL 및 NETLOGON 공유에 액세스하고 있는 경우에는 SMBv2 이상을 사용하도록 해당 클라이언트를 업데이트해야 합니다. 디렉터리는 제대로 작동하지만 SMBv1 클라이언트가 AWS 관리형 Microsoft AD 도메인 컨트롤러의 SYSVOL 및 NETLOGON 공유에 연결되지 않고 그룹 정책도 처리할 수 없게 됩니다.

SMBv1 클라이언트는 사용 중인 다른 SMBv1 호환 파일 서버에서 작동합니다. 하지만 모든 SMB AWS 서버 및 클라이언트를 SMBv2 이상으로 업데이트하는 것이 좋습니다. [시스템에서 SMBv1을 비활성화하고 최신 SMB 버전으로 업데이트하는 방법에 대한 자세한 내용은 Microsoft 및 Support에 게시된 이 게시물을 참조하십시오. TechNet](#)

SMBv1 원격 연결 추적

관리형 AWS Microsoft AD 도메인 컨트롤러에 원격으로 연결하는 Microsoft-Windows-SMBServer/Audit Windows 이벤트 로그를 검토할 수 있습니다. 이 로그의 모든 이벤트는 SMBv1 연결을 나타냅니다. 다음은 이러한 로그 중 하나에서 볼 수 있는 정보의 예입니다.

SMB1 액세스

클라이언트 주소: ###.###.###.###

지침:

이 이벤트는 클라이언트가 SMB1을 사용하여 서버 액세스를 시도했음을 나타냅니다. SMB1 액세스 감사를 중지하려면 Windows PowerShell SmbServerConfiguration cmdlet Set-를 사용하십시오.

애플리케이션 프로그래밍

애플리케이션을 프로그래밍하기 전에 다음 사항을 고려하세요.

Windows DC 로케이터 서비스 사용

응용 프로그램을 개발할 때는 Windows DC 로케이터 서비스를 사용하거나 관리형 AWS Microsoft AD의 동적 DNS (DDNS) 서비스를 사용하여 도메인 컨트롤러 (DC) 를 찾을 수 있습니다. 애플리케이션을 DC의 주소로 하드 코딩해서는 안 됩니다. DC 로케이터 서비스를 사용하면 디렉터리 로드를 확실히 분산할 수 있고 도메인 컨트롤러를 해당 배포에 추가하여 수평 조정을 활용할 수 있습니다. 애플리케이션을 고정 DC에 결합하고 이 DC가 패치 적용 또는 복구 과정을 거치는 경우, 애플리케이션은 남은 DC 중 하나를 사용하는 대신에 DC에 액세스할 수 있는 권한을 상실하게 됩니다. 뿐만 아니라 DC를 하드 코딩하면 단일 DC에 핫스팟이 발생할 수 있습니다. 심한 경우에는 핫스팟으로 인해 DC가 반응하지 않을 수 있습니다. 또한 이러한 경우 AWS 디렉터리 자동화로 인해 디렉터리가 손상된 것으로 표시되고 응답하지 않는 DC를 대체하는 복구 프로세스가 트리거될 수 있습니다.

프로덕션 단계로 넘어가기 전에 로드 테스트 실시

프로덕션 워크로드를 대표하는 객체 및 요청에 대해 랩 테스트를 실시하여 디렉터리가 애플리케이션의 로드에게 맞게 조정되는지 확인해야 합니다. 추가 용량이 필요하다면 DC 간에 요청을 분배하는 중에 추가 DC를 테스트합니다. 자세한 정보는 [추가 도메인 컨트롤러 배포](#)을 참조하세요.

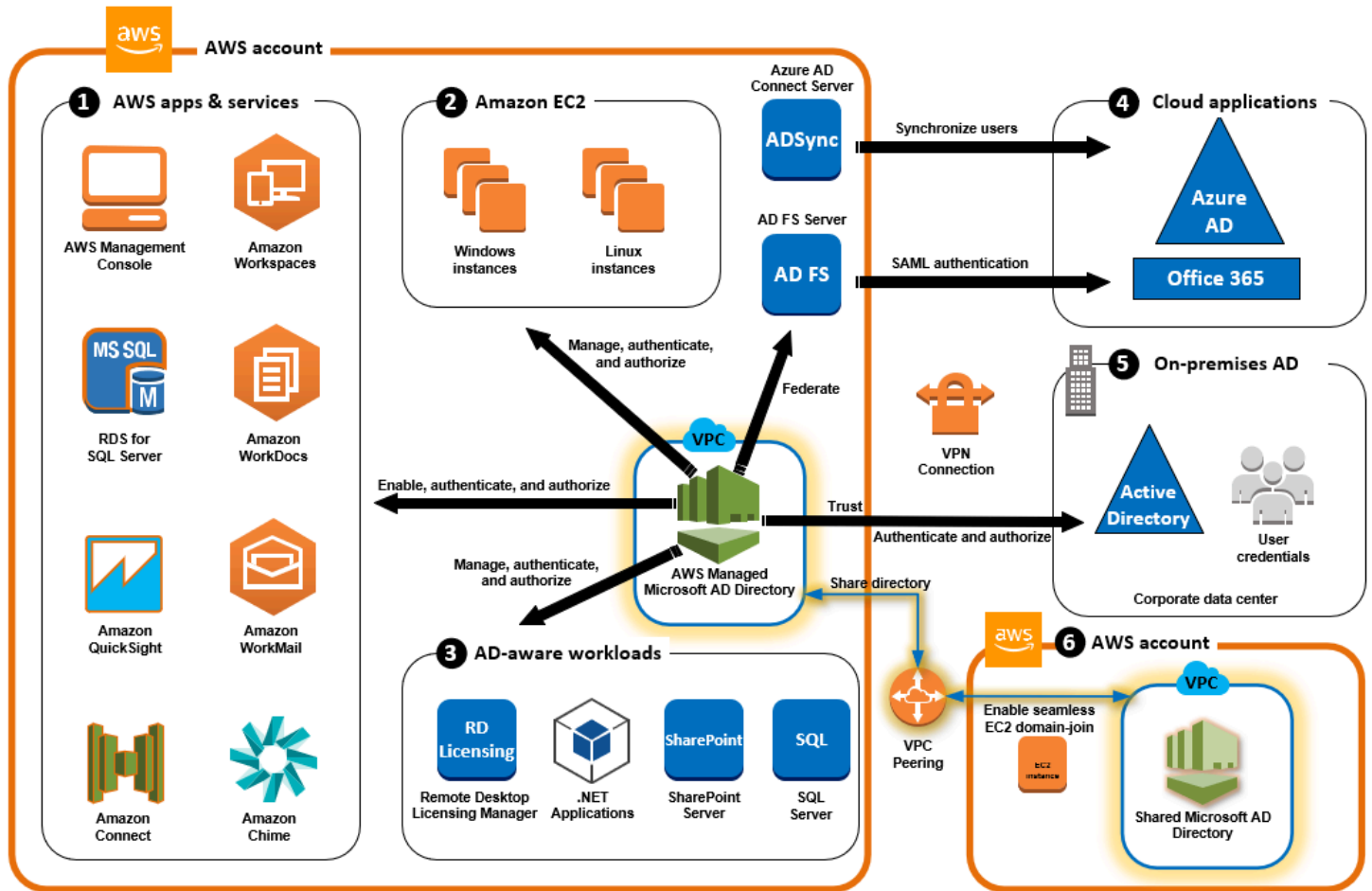
효율적인 LDAP 쿼리 사용

수십만 개의 객체에서 도메인 컨트롤러에 광범위한 LDAP 쿼리를 수행하면 단일 DC에서 상당히 많은 CPU 주기가 사용되면서 핫스팟이 발생할 수 있습니다. 이는 쿼리 중에 동일한 DC를 공유하는 애플리케이션에 부정적인 영향을 미칠 수 있습니다.

AWS 관리형 Microsoft AD의 사용 사례

AWS 관리형 Microsoft AD를 사용하면 단일 디렉터리를 공유하여 여러 사용 사례를 처리할 수 있습니다. 예를 들어 디렉터리를 공유하여 .NET 애플리케이션에 대한 액세스를 인증하고 권한을 부여할 수 있으며, [Windows 인증](#)이 활성화된 [Amazon RDS for SQL Server](#), 메시징 및 화상 회의용 [Amazon Chime](#)을 공유할 수 있습니다.

다음 다이어그램은 AWS 관리형 Microsoft AD 디렉터리의 몇 가지 사용 사례를 보여줍니다. 여기에는 사용자에게 외부 클라우드 애플리케이션에 대한 액세스 권한을 부여하는 기능과 온-프레미스 Active Directory 사용자가 AWS 클라우드의 리소스를 관리하고 액세스할 수 있도록 허용하는 기능이 포함됩니다.



다음 비즈니스 사용 사례 중 하나에 AWS 관리형 Microsoft AD를 사용하십시오.

주제

- [사용 사례 1: Active Directory 자격 증명을 사용하여 AWS 응용 프로그램 및 서비스에 로그인](#)
- [사용 사례 2: Amazon EC2 인스턴스 관리](#)

- [사용 사례 3: Active Directory를 인식하는 워크로드에 디렉터리 서비스를 제공합니다.](#)
- [사용 사례 4: Office 365 및 기타 클라우드 응용 프로그램으로 AWS IAM Identity Center](#)
- [사용 사례 5: 온-프레미스 Active Directory를 클라우드로 확장 AWS](#)
- [사용 사례 6: 디렉터리를 공유하여 계정 간에 Amazon EC2 인스턴스를 도메인에 원활하게 조인합니다. AWS](#)

사용 사례 1: Active Directory 자격 증명을 사용하여 AWS 응용 프로그램 및 서비스에 로그인

„ [Amazon Chime, Amazon Connect AWS Client VPN, AWS Management Console, Amazon FSx, AWS IAM Identity Center](#) <https://aws.amazon.com/single-sign-on/>, [Amazon, QuickSight, SQL Server용 Amazon RDS, Amazon, Amazon, Amazon](#)과 같은 여러 AWS 애플리케이션 및 서비스를 활성화하고 관리형 Microsoft AD, WorkSpaces, 디렉터리를 사용할 수 있습니다. [WorkDocs, WorkMail](#) AWS 디렉터리에서 AWS 애플리케이션 또는 서비스를 활성화하면 사용자가 Active Directory 자격 증명을 사용하여 애플리케이션 또는 서비스에 액세스할 수 있습니다.

예를 들어, 사용자가 [Active Directory 자격 증명을 AWS Management Console 사용하여 로그인](#) 하도록 할 수 있습니다. 이렇게 하려면 디렉터리에서 AWS Management Console 애플리케이션으로 활성화한 다음 Active Directory 사용자 및 그룹을 IAM 역할에 할당해야 합니다. 사용자가 AWS Management Console로 로그인하면 리소스를 관리하는 AWS IAM 역할을 맡습니다. 이로써 별도의 SAML 인프라를 구성 및 관리하지 않고도 사용자에게 AWS Management Console에 액세스 권한을 손쉽게 부여할 수 있습니다.

최종 사용자 경험을 더욱 향상시키기 위해 WorkDocs Amazon용 [Single Sign-On](#) 기능을 활성화하면 사용자가 자격 증명을 별도로 입력할 필요 없이 디렉터리에 연결된 WorkDocs 컴퓨터에서 Amazon에 액세스할 수 있습니다.

디렉터리나 온프레미스 Active Directory의 사용자 계정에 액세스 권한을 부여하면 기존 사용자 계정에 IAM 역할을 직접 할당하여 기존 자격 증명 및 권한을 AWS CLI 사용하여 AWS 리소스를 관리할 수 있도록 디렉터리 AWS Management Console 또는 온프레미스 Active Directory의 사용자 계정에 액세스 권한을 부여할 수 있습니다.

윈도우용 FSx 파일 AWS 서버와 관리형 마이크로소프트 AD의 통합

Windows File Server용 FSx를 관리형 Microsoft AWS AD와 통합하면 완전 관리형 기본 Microsoft Windows 기반 SMB (서버 메시지 블록) 프로토콜 파일 시스템이 제공되므로 공유 파일 스토리지를 사용하는 Windows 기반 응용 프로그램 및 클라이언트를 쉽게 이동할 수 있습니다. AWS FSx for

Windows File Server를 자체 관리형 Microsoft Active Directory와 통합할 수 있지만, 여기서는 이러한 해당 시나리오에 대해서는 설명하지 않습니다.

일반적인 Amazon FSx 사용 사례 및 리소스

이 섹션에서는 Windows File Server용 일반적인 FSx와 관리형 Microsoft AD 사용 사례 통합에 대한 리소스를 제공합니다. 이 섹션의 각 사용 사례는 기본적인 AWS Managed Microsoft AD 및 FSx for Windows File Server의 구성으로 시작합니다. 이러한 구성을 생성하는 방법에 대한 자세한 내용은 다음 단원을 참조하세요.

- [AWS 매니지드 마이크로소프트 AD 시작하기](#)
- [Amazon FSx 시작하기](#)

Windows 컨테이너의 영구 스토리지로서의 FSx for Windows File Server

[Amazon Elastic Container Service\(ECS\)](#)는 이제 Amazon ECS 최적화 Windows AMI로 시작되는 컨테이너 인스턴스에서 Windows 컨테이너를 지원합니다. Windows 컨테이너 인스턴스는 자체 Amazon ECS 컨테이너 에이전트 버전을 사용합니다. Amazon ECS 최적화 Windows AMI에서 Amazon ECS 컨테이너 에이전트는 호스트에서 서비스로 실행됩니다.

Amazon ECS는 그룹 관리형 서비스 계정(gMSA)이라는 특수한 종류의 서비스 계정을 통해 Windows 컨테이너에 대한 Active Directory 인증을 지원합니다. Windows 컨테이너는 도메인에 가입할 수 없으므로 gMSA와 함께 실행되도록 Windows 컨테이너를 구성해야 합니다.

관련 항목

- [Windows 컨테이너의 영구 스토리지로 FSx for Windows File Server 사용하기](#)
- [그룹 관리형 서비스 계정](#)

아마존 AppStream 2.0 지원

[Amazon AppStream 2.0](#)은 완전 관리형 애플리케이션 스트리밍 서비스입니다. 사용자가 애플리케이션을 통해 데이터를 저장하고 액세스할 수 있는 다양한 솔루션을 제공합니다. Amazon FSx 2.0 버전은 Amazon FSx를 AppStream 사용하여 개인용 영구 스토리지 드라이브를 제공하며, 공통 파일에 액세스할 수 있는 공유 폴더를 제공하도록 구성할 수 있습니다.

관련 항목

- [연습 4: 아마존 2.0에서 아마존 FSx 사용하기 AppStream](#)

- [아마존 2.0과 아마존 FSx 사용하기 AppStream](#)
- [2.0에서 액티브 디렉터리 사용 AppStream](#)

Microsoft SQL Server 지원

FSx for Windows File Server는 Microsoft SQL Server 2012(2012 버전 11.x부터) 및 최신 시스템 데이터베이스(Master, Model, MSDB, TempDB 등) 및 데이터베이스 엔진 사용자 데이터베이스의 스토리지 옵션으로 사용할 수 있습니다.

관련 항목

- [SMB 파일 공유 스토리지와 함께 SQL Server 설치](#)
- [FSx for Windows File Server를 사용하여 Microsoft SQL Server 배포 단순화](#)
- [그룹 관리형 서비스 계정](#)

홈 폴더 및 로밍 사용자 프로필 지원

FSx for Windows File Server를 사용하여 Active Directory 사용자 홈 폴더와 내 문서의 데이터를 중앙 위치에 저장할 수 있습니다. FSx for Windows File Server를 사용하여 로밍 사용자 프로필의 데이터를 저장할 수도 있습니다.

관련 항목

- [Amazon FSx로 더 쉬워진 Windows 홈 디렉터리](#)
- [로밍 사용자 프로필 배포하기](#)
- [Windows File Server용 FSx를 다음과 함께 사용 WorkSpaces](#)

네트워크 파일 공유 지원

FSx for Windows File Server의 네트워크 파일 공유는 관리되고 확장 가능한 파일 공유 솔루션을 제공합니다. 한 가지 사용 사례는 수동으로 또는 그룹 정책을 통해 생성될 수 있는 클라이언트용 매핑 드라이브입니다.

관련 항목

- [연습 6: 샤드를 통한 스케일 아웃](#)
- [드라이브 매핑](#)

- [Windows File Server용 FSx를 다음과 함께 사용 WorkSpaces](#)

그룹 정책 소프트웨어 설치 지원

SYSVOL 폴더의 크기와 성능이 제한되므로 소프트웨어 설치 파일과 같은 데이터를 해당 폴더에 저장하지 않는 것이 좋습니다. 이에 대한 가능한 해결책으로 그룹 정책을 사용하여 설치된 모든 소프트웨어 파일을 저장하도록 FSx for Windows File Server를 구성할 수 있습니다.

관련 항목

- [그룹 정책을 사용하여 Windows Server 2008과 Windows Server 2003에서 소프트웨어를 원격으로 설치하는 방법](#)

Windows Server 백업 대상 지원

UNC 파일 공유를 사용하여 Windows Server 백업에서 FSx for Windows File Server를 대상 드라이브로 구성할 수 있습니다. 이 경우 연결된 EBS 볼륨 대신 FSx for Windows File Server의 UNC 경로를 지정해야 합니다.

관련 항목

- [서버의 시스템 상태 복구 수행](#)

Amazon FSx는 AWS 관리형 마이크로소프트 AD 디렉터리 공유도 지원합니다. 자세한 내용은 다음을 참조하세요.

- [디렉터리 공유](#)
- [다른 VPC 또는 계정에서 AWS 관리형 Microsoft AD와 함께 Amazon FSx 사용](#)

Amazon RDS와 AWS 관리형 마이크로소프트 AD의 통합

Amazon RDS에서는 Kerberos 및 Microsoft Active Directory를 사용하여 데이터베이스 사용자의 외부 인증을 지원합니다. Kerberos는 티켓과 대칭 키 암호화를 사용하여 네트워크를 통해 암호를 전송할 필요가 없는 네트워크 인증 프로토콜입니다. Kerberos 및 Active Directory에 대한 Amazon RDS의 지원은 데이터베이스 사용자에게 SSO(Single Sign-On) 및 중앙 집중식 인증의 이점을 제공하므로 사용자 보안 인증 정보를 Active Directory에 보관할 수 있습니다.

이 사용 사례를 시작하려면 먼저 AWS 관리형 Microsoft AD 및 Amazon RDS의 기본 구성을 설정해야 합니다.

- [AWS 매니지드 마이크로소프트 AD 시작하기](#)
- [Amazon RDS 시작하기](#)

아래에 언급된 모든 사용 사례는 기본 AWS 관리형 Microsoft AD 및 Amazon RDS로 시작하여 Amazon RDS를 관리형 AWS Microsoft AD와 통합하는 방법을 다룹니다.

- [Amazon RDS for SQL Server DB 인스턴스와 함께 Windows 인증 사용하기](#)
- [MySQL에 Kerberos 인증 사용하기](#)
- [Amazon RDS for Oracle과 함께 Kerberos 인증 사용하기](#)
- [Amazon RDS for PostgreSQL과 함께 Kerberos 인증 사용하기](#)

Amazon RDS는 AWS 관리형 Microsoft AD 디렉터리 공유도 지원합니다. 자세한 내용은 다음을 참조하세요.

- [디렉터리 공유](#)
- [여러 계정의 Amazon RDS DB 인스턴스를 단일 공유 도메인에 조인](#)

Amazon RDS for SQL Server를 Active Directory에 조인하는 방법에 대한 자세한 내용은 [Amazon RDS for SQL Server를 자체 관리형 Active Directory에 조인](#)을 참조하세요.

그룹 관리 서비스 계정과 함께 Amazon RDS for SQL Server를 사용하는 .NET 애플리케이션

Amazon RDS for SQL Server를 기본 .NET 애플리케이션 및 그룹 관리형 서비스 계정(gMSA)과 통합할 수 있습니다. 자세한 내용은 [AWS 관리형 Microsoft AD를 통해 Active Directory—통합 .NET 응용 프로그램의 배포를 단순화하고 보안을 향상시키는 방법](#)을 참조하십시오.

사용 사례 2: Amazon EC2 인스턴스 관리

친숙한 Active Directory 관리 도구를 사용하면 인스턴스를 [AWS 관리형 Microsoft AD 도메인에 조인함으로써 Active Directory 그룹 정책 개체 \(GPO\)를 적용하여 Windows 또는 Linux용 Amazon EC2 인스턴스를 중앙에서 관리할 수](#) 있습니다.

또한 사용자는 Active Directory 자격 증명을 사용하여 인스턴스에 로그인할 수 있습니다. 따라서 개별 인스턴스 자격 증명을 사용하거나 프라이빗 키(PEM) 파일을 배포할 필요가 없습니다. 이렇게 하면 이미 사용하고 있는 Active Directory 사용자 관리 도구를 사용하여 사용자에게 액세스 권한을 즉시 부여하거나 취소하기가 더 쉬워집니다.

사용 사례 3: Active Directory를 인식하는 워크로드에 디렉터리 서비스를 제공합니다.

AWS Managed Microsoft AD는 [원격 데스크톱 라이선싱 관리자](#), [Microsoft 및 Microsoft SQL Server Always On 더 클라우드](#)와 같은 기존의 액티브 디렉터리 인식 워크로드를 실행할 수 있는 실제 Microsoft Active Directory입니다. SharePoint AWS AWS 또한 관리형 Microsoft AD를 사용하면 [그룹 관리 서비스 계정 \(GMSA\)](#) 및 [Kerberos 제한 위임 \(KCD\)](#) 을 사용하여 Active Directory 통합 .NET 응용 프로그램의 보안을 단순화하고 개선할 수 있습니다.

사용 사례 4: Office 365 및 기타 클라우드 응용 프로그램으로 AWS IAM Identity Center

AWS 관리형 Microsoft AD를 사용하여 클라우드 애플리케이션을 제공할 AWS IAM Identity Center 수 있습니다. Microsoft Entra Connect(이전 명칭) 를 사용하여 사용자를 (이전에는 AD Azure Active Directory Connect) 로 동기화한 다음 Azure AD FS Microsoft Entra (Active Directory 페더레이션 서비스) 를 사용하여 사용자가 Active Directory 자격 증명을 사용하여 [Microsoft Office 365](#) 및 기타 SAML 2.0 클라우드 응용 프로그램에 액세스할 수 있도록 할 수 있습니다. Azure Active Directory

[AWS 관리형 Microsoft AD를 IAM ID 센터와 통합하면 관리형 AWS Microsoft AD 및/또는 온프레미스의 신뢰할 수 있는 도메인에 SAML 기능이 추가됩니다.](#) 일단 통합되면 사용자는 SAML 인프라를 구성하지 않고도 Office 365, Concur, AWS Management Console Salesforce와 같은 타사 클라우드 애플리케이션을 비롯한 SAML을 지원하는 서비스와 함께 IAM ID 센터를 사용할 수 있습니다. 온프레미스 사용자가 IAM Identity Center를 사용하도록 허용하는 프로세스에 대한 데모는 다음 비디오를 참조하십시오. YouTube

Note

AWS 싱글 사인온은 IAM ID 센터로 이름이 변경되었습니다.

사용 사례 5: 온-프레미스 Active Directory를 클라우드로 확장 AWS

이미 Active Directory 인프라가 있고 Active Directory 인식 워크로드를 AWS 클라우드로 마이그레이션할 때 사용하려는 경우 관리형 AWS Microsoft AD가 도움이 될 수 있습니다. [Active Directory 트러스트](#) 를 사용하여 AWS 관리형 Microsoft AD를 기존 Active Directory에 연결할 수 있습니다. 즉, 사용자는 사

용자, 그룹 또는 암호를 동기화할 필요 없이 온-프레미스 Active Directory 자격 증명을 사용하여 Active Directory 인식 및 AWS 애플리케이션에 액세스할 수 있습니다.

예를 들어, 사용자는 기존 Active Directory 사용자 이름과 암호를 사용하여 WorkSpaces Amazon에 로그인할 수 있습니다. AWS Management Console 또한 SharePoint 관리형 AWS Microsoft AD와 같은 Active Directory 인식 애플리케이션을 사용하는 경우 로그인한 Windows 사용자는 자격 증명을 다시 입력할 필요 없이 이러한 애플리케이션에 액세스할 수 있습니다.

Active Directory 마이그레이션 [도구 키트 \(ADMT\)](#) 와 [암호 내보내기 서비스 \(PES\)](#) 를 사용하여 [Active Directory 인프라의 운영 부담을 없애기 AWS 위해 온-프레미스 Active Directory 도메인을 마이그레이션하여 마이그레이션을 수행할](#) 수도 있습니다.

사용 사례 6: 디렉터리를 공유하여 계정 간에 Amazon EC2 인스턴스를 도메인에 원활하게 조인합니다. AWS

여러 AWS 계정에서 디렉터리를 공유하면 각 계정 및 VPC별로 디렉터리를 운영할 필요 없이 [Amazon EC2](#)와 같은 AWS 서비스를 쉽게 관리할 수 있습니다. AWS 리전 내 모든 [Amazon VPC](#)와 모든 AWS 계정의 디렉터리를 사용할 수 있습니다. 모든 계정과 VPC에서 단일 디렉터리로 디렉터리 인식 워크로드를 더 쉽게, 그리고 더 비용 효과적으로 관리할 수 있는 기능입니다. 예를 들어, 이제 단일 AWS Managed Microsoft AD 디렉터리를 사용하여 여러 계정 및 VPC에 걸쳐 EC2 인스턴스에 배포된 [Windows 워크로드](#)를 쉽게 관리할 수 있습니다.

AWS 관리형 Microsoft AD 디렉터리를 다른 AWS 계정과 공유하는 경우 Amazon EC2 콘솔을 사용하거나 계정 및 지역 내의 모든 Amazon VPC에서 인스턴스를 원활하게 조인할 수 있습니다. [AWS Systems Manager](#) AWS 또한 수동으로 인스턴스를 도메인에 조인하거나 각 계정과 VPC의 디렉터리에 배포할 필요 없이, 신속하게 디렉터리 인식 워크로드를 EC2 인스턴스에 배포할 수 있습니다. 자세한 내용은 [디렉터리 공유](#)(를) 참조하세요.

AWS 관리형 Microsoft AD를 관리하는 방법

이 섹션에는 AWS 관리형 Microsoft AD 환경을 운영 및 유지 관리하기 위한 모든 절차가 나열되어 있습니다.

주제

- [AWS Managed Microsoft AD 디렉터리 보안 유지](#)
- [AWS Managed Microsoft AD 모니터링](#)
- [다중 리전 복제](#)

- [디렉터리 공유](#)
- [Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory](#)
- [AWS Managed Microsoft AD에서의 사용자 및 그룹 관리](#)
- [기존 액티브 디렉터리 인프라에 연결](#)
- [AWS 관리형 Microsoft AD를 다음으로 연결하세요. Microsoft Entra Connect Sync](#)
- [스키마 확장](#)
- [AWS 관리형 Microsoft AD 디렉터리 유지 관리](#)
- [사용자 및 그룹에게 AWS 리소스에 대한 액세스 권한 부여](#)
- [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#)
- [AD 보안 인증을 사용한 AWS Management Console 액세스 활성화](#)
- [추가 도메인 컨트롤러 배포](#)
- [Active Directory에서 AWS Managed Microsoft AD로 사용자 마이그레이션](#)

AWS Managed Microsoft AD 디렉터리 보안 유지

이 단원에서는 AWS Managed Microsoft AD 환경의 보안을 유지하기 위한 고려 사항을 설명합니다.

주제

- [AWS 관리형 Microsoft AD에 대한 암호 정책 관리](#)
- [AWS 관리형 Microsoft AD에 대한 다중 요소 인증을 활성화합니다.](#)
- [보안 LDAP 또는 LDAPS 활성화](#)
- [AWS 관리형 Microsoft AD에 대한 규정 준수 관리](#)
- [AWS Managed Microsoft AD 네트워크 보안 구성 강화](#)
- [보안 설정 구성](#)
- [AD용 AWS Private CA 커넥터 설정](#)

AWS 관리형 Microsoft AD에 대한 암호 정책 관리

AWS 관리형 Microsoft AD를 사용하면 관리형 Microsoft AD 도메인에서 관리하는 사용자 그룹에 대해 다양한 암호 및 계정 잠금 정책 ([세분화된 암호 정책이라고도 함](#)) 을 정의하고 할당할 수 있습니다. AWS 관리형 Microsoft AD 디렉터리를 만들면 기본 도메인 정책이 생성되어 적용됩니다. 이 정책에는 다음 설정이 포함되어 있습니다.

정책	설정
암호 기록 강제 시행	24개 암호 저장
최대 암호 수명	42일 *
최소 암호 수명	1일
최소 암호 길이	7자
암호가 복잡성 요구 사항을 충족해야 함	활성화됨
해독 가능한 암호화를 사용하여 암호 저장	Disabled(비활성)

* 참고: 최대 42일의 암호 수명에는 admin 암호가 포함됩니다.

예를 들어 중요도가 낮은 정보에만 액세스할 수 있는 직원에게 덜 엄격한 정책 설정을 할당할 수 있습니다. 정기적으로 기밀 정보에 액세스하는 고위 관리자에 대해서는 더 엄격한 설정을 적용할 수 있습니다.

다음은 Microsoft Active Directory 세분화된 암호 정책 및 보안 정책에 대해 자세히 알아볼 수 있는 리소스입니다.

- [보안 정책 설정을 구성합니다.](#)
- [암호 복잡성 요구 사항](#)
- [암호 복잡성, 보안 고려 사항](#)

AWS 는 사용자가 구성하고 그룹에 할당할 수 있는 관리형 AWS Microsoft AD의 세분화된 암호 정책 세트를 제공합니다. [정책을 구성하려면 관리 센터와 같은 Active Directory 표준 Microsoft 정책 도구를 사용할 수 있습니다.](#) Microsoft정책 도구를 시작하려면 [을 참조하십시오](#)[AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치.](#)

암호 정책 적용 방법

암호를 재설정했는지 아니면 암호를 변경했는지에 따라 세분화된 암호 정책이 적용되는 방식이 달라 집니다. 도메인 사용자는 자신의 암호를 변경할 수 있습니다. 필요한 권한이 있는 Active Directory 관리자나 사용자는 사용자 [암호를 재설정할](#) 수 있습니다. 자세한 내용은 다음 차트를 참조하십시오.

정책	비밀번호 재설정	비밀번호 변경
암호 기록 강제 시행	 아니요	 예
최대 암호 수명	 예	 예
최소 암호 수명	 아니요	 예
최소 암호 길이	 예	 예
암호가 복잡성 요구 사항을 충족해야 함	 예	 예

이러한 차이는 보안에 영향을 미칩니다. 예를 들어 사용자 암호를 재설정할 때마다 암호 기록 적용 및 최소 암호 사용 기간 정책이 적용되지 않습니다. 자세한 내용은 [암호 기록 적용 및 최소 암호 사용 기간 정책](#)과 관련된 보안 고려 사항에 대한 Microsoft 설명서를 참조하십시오.

주제

- [지원되는 정책 설정](#)
- [암호 정책을 관리할 수 있는 사용자 위임](#)
- [사용자에게 암호 정책 할당](#)

관련 AWS 보안 블로그 기사

- [AWS 관리형 Microsoft AD를 사용하여 AWS Directory Service 보안 표준을 충족하는 데 도움이 되도록 더욱 강력한 암호 정책을 구성하는 방법](#)

지원되는 정책 설정

AWS 관리형 Microsoft AD에는 편집할 수 없는 우선 순위 값을 가진 5개의 세분화된 정책이 포함되어 있습니다. 각 정책에서 다수의 속성을 구성하여 암호 강도와 로그인 실패 시 계정 잠금 동작을 적용할 수 있습니다. 정책을 0개 이상의 Active Directory 그룹에 할당할 수 있습니다. 최종 사용자가 여러 그룹의 멤버이고 복수의 암호 정책을 할당 받은 경우 Active Directory가 가장 낮은 우선 순위 값의 정책을 적용합니다.

AWS 사전 정의된 암호 정책

다음 표에는 AWS 관리형 Microsoft AD 디렉터리에 포함된 다섯 가지 정책과 할당된 우선 순위 값이 나와 있습니다. 자세한 정보는 [우선 순위](#)를 참조하세요.

정책 이름	우선 순위
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

암호 정책 속성

비즈니스 요구 사항을 충족하는 규정 준수 표준을 준수하기 위해 암호 정책에서 다음 속성을 편집할 수 있습니다.

- 정책 이름
- [암호 기록 강제 시행](#)
- [최소 암호 길이](#)

- [최소 암호 수명](#)
- [최대 암호 수명](#)
- [해독 가능한 암호화를 사용하여 암호 저장](#)
- [암호가 복잡성 요구 사항을 충족해야 함](#)

이러한 정책에서 우선 순위 값을 수정할 수 없습니다. 이러한 설정이 암호 적용에 미치는 영향에 대한 자세한 내용은 Microsoft [웹 사이트의 AD DS: 세분화된 암호 정책](#)을 참조하십시오. TechNet 이러한 정책에 대한 일반 정보는 Microsoft TechNet 웹 사이트의 [암호 정책](#)을 참조하십시오.

계정 잠금 정책

암호 정책에서 다음 속성을 수정하여 로그인 실패 시 Active Directory가 계정을 잠글지 여부 및 방법을 지정할 수도 있습니다.

- 로그인 시도 실패 허용 횟수
- 계정 잠금 기간
- 일정 기간 후 로그인 시도 실패 횟수 재설정

이러한 정책에 대한 일반 정보는 Microsoft TechNet 웹 사이트의 [계정 잠금 정책](#)을 참조하십시오.

우선 순위

우선 순위 값이 낮은 정책일수록 우선 순위가 높아집니다. Active Directory 보안 그룹에 암호 정책을 할당합니다. 단일 보안 그룹에 단일 정책을 적용해야 하지만 단일 사용자가 복수의 암호 정책을 할당 받을 수 있습니다. 예를 들어 jsmith가 HR 그룹의 멤버이자 MANAGERS 그룹의 멤버라고 가정합니다. CustomerPSO-05(우선 순위 값 50)를 HR 그룹에 할당하고 CustomerPSO-04(우선 순위 값 40)를 MANAGERS에 할당한 경우, CustomerPSO-04의 우선 순위가 더 높으므로 Active Directory가 이 정책을 jsmith에 적용합니다.

특정 사용자 또는 그룹에 여러 정책을 할당하는 경우 Active Directory는 다음과 같이 적용할 정책을 결정합니다.

1. 사용자 객체에 직접 할당한 정책이 적용됩니다.
2. 사용자 객체에 직접 할당된 정책이 없는 경우 그룹 멤버십으로 인해 사용자에게 할당된 모든 정책 중 우선 순위 값이 가장 낮은 정책이 적용됩니다.

자세한 내용은 Microsoft 웹 [사이트의 AD DS: 세분화된 암호 정책](#)을 참조하십시오. TechNet

암호 정책을 관리할 수 있는 사용자 위임

고급 암호 정책 위임 관리자 보안 그룹에 계정을 추가하여 AWS 관리형 Microsoft AD에서 만든 특정 사용자 계정에 암호 정책을 관리하는 권한을 AWS 위임할 수 있습니다. 이 그룹의 멤버가 된 계정에는 [이전](#)에 나열된 모든 암호 정책을 편집 및 구성할 수 있는 권한이 부여됩니다.

암호 정책을 관리할 수 있는 권한을 위임하려면

1. 관리형 AWS Microsoft AD 도메인에 가입한 모든 관리형 EC2 인스턴스에서 [Active Directory 관리 센터 \(ADAC\)](#) 를 시작합니다.
2. 트리 보기로 전환하여 AWS Delegated Groups(위임 그룹) OU로 이동합니다. 이 OU에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)를 참조하세요.
3. AWS Delegated Fine Grained Password Policy Administrators(위임 세분화된 암호 정책 관리자) 사용자 그룹을 찾습니다. 도메인의 사용자 또는 그룹을 이 그룹에 추가합니다.

사용자에게 암호 정책 할당

AWS AS Delegated Fine Grained Password Policy Administrators(위임 세분화된 암호 정책 관리자) 보안 그룹의 멤버인 사용자 계정은 다음 절차를 사용하여 사용자 및 보안 그룹에 정책을 할당할 수 있습니다.

사용자에게 암호 정책을 할당하려면

1. 관리형 AWS Microsoft AD 도메인에 가입한 모든 관리형 EC2 인스턴스에서 [Active Directory 관리 센터 \(ADAC\)](#) 를 시작합니다.
2. [Tree View]로 전환하여 [System>Password Settings Container]로 이동합니다.
3. 편집하려는 세분화된 정책을 두 번 클릭합니다. [Add]를 클릭하여 정책 속성을 편집하고 사용자 또는 보안 그룹을 정책에 추가합니다. AWS Managed Microsoft AD에서 제공하는 기본 세분화 정책에 관한 자세한 내용은 [AWS 사전 정의된 암호 정책](#) 단원을 참조하세요.
4. 암호 정책이 적용되었는지 확인하려면 다음 PowerShell 명령을 실행합니다.

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

Note

결과가 정확하지 않을 수 있으므로 net user 명령을 사용하지 마세요.

AWS 관리형 Microsoft AD 디렉터리에서 다섯 가지 암호 정책을 구성하지 않으면 Active Directory는 기본 도메인 그룹 정책을 사용합니다. 암호 설정 컨테이너 사용에 대한 자세한 내용은 이 [Microsoft 블로그 게시물](#)을 참조하세요.

AWS 관리형 Microsoft AD에 대한 다중 요소 인증을 활성화합니다.

사용자가 액세스할 AD 자격 증명을 지정할 때 AWS 관리형 Microsoft AD 디렉터리에 대한 MFA (다단계 인증)를 활성화하여 보안을 강화할 수 있습니다. [지원되는 Amazon Enterprise 애플리케이션](#) MFA를 활성화하면 사용자는 평소 대로 사용자 이름 및 암호(첫 번째 요소)를 입력하는 것 외에도 가상 또는 하드웨어 MFA 솔루션에서 얻는 인증 코드(두 번째 요소)를 입력해야 합니다. 이들 요소는 사용자가 유효한 사용자 자격 증명과 유효 MFA 코드를 제공하지 않는 경우 Amazon 엔터프라이즈 애플리케이션에 대한 액세스를 금지하여 보안을 강화합니다.

MFA를 사용하려면 [원격 인증 전화 접속 사용자 서비스\(RADIUS\)](#) 서버인 MFA 솔루션이 있거나 사용자의 온프레미스 인프라에 이미 구현된 RADIUS 서버에 대한 MFA 플러그인이 있어야 합니다. MFA 솔루션에서는 사용자가 하드웨어 디바이스나 휴대전화 등의 기기에서 실행되는 소프트웨어에서 얻는 일회용 암호(OTP)를 사용할 수 있어야 합니다.

RADIUS는 사용자가 네트워크 서비스에 연결할 수 있도록 인증, 권한 부여, 계정 관리 서비스를 제공하는 업계 표준 클라이언트/서버 프로토콜입니다. AWS 관리형 Microsoft AD에는 MFA 솔루션을 구현한 RADIUS 서버에 연결하는 RADIUS 클라이언트가 포함되어 있습니다. RADIUS 서버에서는 사용자 이름과 OTP 코드를 확인합니다. RADIUS 서버가 사용자의 유효성을 성공적으로 검증하면 AWS 관리형 Microsoft AD는 Active Directory에 대해 사용자를 인증합니다. Active Directory 인증에 성공하면 사용자는 애플리케이션에 액세스할 수 있습니다. AWS 관리형 Microsoft AD RADIUS 클라이언트와 RADIUS 서버 간의 통신을 위해서는 포트 1812를 통한 통신을 가능하게 하는 AWS 보안 그룹을 구성해야 합니다.

다음 절차를 수행하여 AWS 관리형 Microsoft AD 디렉터리에 대한 다단계 인증을 활성화할 수 있습니다. RADIUS 서버가 AWS Directory Service 및 MFA에서 작동하도록 구성하는 자세한 방법은 [다중 인증 사전 조건](#) 단원을 참조하세요.

고려 사항

다음은 AWS 관리형 Microsoft AD의 다중 요소 인증에 대한 몇 가지 고려 사항입니다.

- Simple AD에는 다중 인증을 사용할 수 없습니다. 그러나 AD Connector 디렉터리에는 MFA를 사용할 수 있습니다. 자세한 정보는 [AD Connector에 대한 다중 인증 활성화](#)을 참조하세요.
- MFA는 관리형 AWS Microsoft AD의 지역별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)을 참조하세요.

- 외부 통신에 AWS Managed Microsoft AD를 사용하려는 경우 이러한 통신을 위해 네트워크 외부에 NAT (네트워크 주소 변환) Internet Gateway 또는 Internet Gateway를 구성하는 것이 좋습니다. AWS
- AWS 관리형 Microsoft AD와 AWS 네트워크에서 호스팅되는 RADIUS 서버 간의 외부 통신을 지원하려면 문의하세요 [AWS Support](#).

AWS 관리형 Microsoft AD에 대한 다중 요소 인증을 활성화합니다.

다음 절차는 AWS 관리형 Microsoft AD에 대한 다중 요소 인증을 활성화하는 방법을 보여줍니다.

1. RADIUS MFA 서버 및 관리형 AWS Microsoft AD 디렉터리의 IP 주소를 식별하십시오.
2. VPC (가상 사설 클라우드) 보안 그룹을 편집하여 관리형 AWS Microsoft AD IP 엔드포인트와 RADIUS MFA 서버 간에 포트 1812를 통한 통신을 활성화할 수 있습니다.
3. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
4. AWS 관리형 Microsoft AD 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
5. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 MFA를 활성화할 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
6. 다중 인증 섹션에서 작업을 선택한 다음 활성화를 선택합니다.
7. Enable multi-factor authentication (MFA)(다중 인증(MFA) 활성화) 페이지에서 다음 값을 제공합니다.

레이블 표시

레이블 이름을 제공합니다.

RADIUS 서버 DNS 이름 또는 IP 주소

RADIUS 서버 엔드포인트의 IP 주소 또는 RADIUS 서버 로드 밸런서의 IP 주소입니다. 쉼표로 구분하여 여러 IP 주소를 입력할 수 있습니다(예: 192.0.0.0, 192.0.0.12).

Note

RADIUS MFA는 Amazon 또는 Amazon Chime과 같은 아마존 엔터프라이즈 애플리케이션 및 서비스 또는 서비스에 대한 액세스를 인증하는 데만 적용됩니다. AWS Management Console WorkSpaces QuickSight EC2 인스턴스에서 실행되거나 EC2

인스턴스에 로그인하는 Windows 워크로드에는 MFA를 제공하지 않습니다. AWS Directory Service RADIUS 챌린지/응답 인증은 지원하지 않습니다. 사용자는 사용자 이름과 암호를 입력할 때 MFA 코드를 알고 있어야 합니다. 또는 사용자에 대한 SMS 텍스트 out-of-band 검증과 같은 MFA를 수행하는 솔루션을 사용해야 합니다. out-of-band MFA 솔루션에서는 RADIUS 제한 시간 값을 솔루션에 맞게 설정해야 합니다. out-of-band MFA 솔루션을 사용하는 경우 로그인 페이지에서 사용자에게 MFA 코드를 입력하라는 메시지가 표시됩니다. 이 경우, 사용자는 암호 필드와 MFA 필드 모두에 암호를 입력해야 합니다.

포트

RADIUS 서버에서 통신용으로 사용 중인 포트입니다. 온프레미스 네트워크는 서버에서 기본 RADIUS 서버 포트 (UDP:1812) 를 통한 인바운드 트래픽을 허용해야 합니다. AWS Directory Service

Shared secret code

RADIUS 엔드포인트가 생성될 때 지정된 공유 보안 코드입니다.

Confirm shared secret code

RADIUS 엔드포인트의 공유 보안 코드를 확인합니다.

프로토콜

RADIUS 엔드포인트가 생성될 때 지정된 프로토콜을 선택합니다.

서버 제한 시간(초)

RADIUS 서버에서 응답을 대기할 시간(초)입니다. 이 값은 1~50이어야 합니다.

Note

RADIUS 서버 제한 시간은 20초 이하로 구성하는 것이 좋습니다. 제한 시간이 20초를 초과하면 시스템에서 다른 RADIUS 서버로 재시도할 수 없어 시간 초과 실패가 발생할 수 있습니다..

최대 RADIUS 요청 재시도

RADIUS 서버와 통신을 시도하는 횟수입니다. 이 값은 0~10이어야 합니다.

[RADIUS Status]가 [Enabled]로 변경되면 다중 인증을 사용할 수 있습니다.

8. 활성화를 선택합니다.

지원되는 Amazon Enterprise 애플리케이션

Amazon, Amazon WorkSpaces, Amazon을 비롯한 모든 Amazon Enterprise IT 애플리케이션은 MFA와 함께 AWS 관리형 Microsoft AD 및 AD Connector를 AWS IAM Identity Center 사용할 때 액세스가 AWS Management Console 지원되며 QuickSight, 이러한 애플리케이션은 Amazon, Amazon, Amazon을 비롯한 모든 Amazon Enterprise IT 애플리케이션을 사용할 수 있습니다. WorkDocs WorkMail

Amazon Enterprise 애플리케이션, Single AWS Sign-On 및 AWS Management Console 사용에 AWS Directory Service대한 기본 사용자 액세스를 구성하는 방법에 대한 자세한 내용은 [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#), [AD 보안 인증을 사용한 AWS Management Console 액세스 활성화](#)

관련 AWS 보안 블로그 기사

- [AWS 관리형 Microsoft AD 및 온-프레미스 자격 AWS 증명을 사용하여 서비스에 대한 다단계 인증을 활성화하는 방법](#)

보안 LDAP 또는 LDAPS 활성화

LDAP(Lightweight Directory Access Protocol)는 Active Directory에서 데이터를 읽고 쓰는 데 사용되는 표준 통신 프로토콜입니다. 일부 애플리케이션은 LDAP를 사용하여 Active Directory에서 사용자 및 그룹을 추가, 제거 또는 검색하거나 Active Directory에서 사용자를 인증하기 위한 자격 증명을 전송합니다. 모든 LDAP 통신에는 클라이언트(예: 애플리케이션)와 서버(예: Active Directory)가 포함됩니다.

기본적으로 LDAP를 통한 통신은 암호화되지 않습니다. 그러므로 악성 사용자가 네트워크 모니터링 소프트웨어를 사용하여 유선으로 전송되는 데이터 패킷을 볼 수 있습니다. 이 때문에 일반적으로 많은 기업 보안 정책은 조직이 모든 LDAP 통신을 암호화하도록 요구하고 있습니다.

이러한 형태의 데이터 노출을 줄이기 위해 AWS 관리형 Microsoft AD는 다음과 같은 옵션을 제공합니다. LDAPS라고도 하는 SSL (보안 소켓 계층) /TLS (전송 계층 보안) 를 통한 LDAP를 사용할 수 있습니다. LDAPS를 사용하면 유선 보안을 개선할 수 있습니다. 또한 LDAP 지원 애플리케이션과 관리형 AWS Microsoft AD 간의 모든 통신을 암호화하여 규정 준수 요구 사항을 충족할 수 있습니다.

AWS 관리형 Microsoft AD는 다음과 같은 배포 시나리오에서 LDAPS에 대한 지원을 제공합니다.

- 서버측 LDAPS는 상용 또는 자체 개발된 LDAP 인식 애플리케이션 (LDAP 클라이언트 역할) 과 관리형 Microsoft AD (LDAP 서버 역할) 간의 LDAP 통신을 암호화합니다. AWS 자세한 정보는 [관리형 AWS Microsoft AD를 사용하여 서버측 LDAPS를 활성화합니다.](#)을 참조하세요.
- 클라이언트측 LDAPS는 (LDAP 클라이언트 역할을 함) 및 자체 관리형 (온-프레미스) Active Directory WorkSpaces (LDAP 서버 역할) 와 같은 AWS 애플리케이션 간의 LDAP 통신을 암호화합니다. 자세한 내용은 [관리형 AWS Microsoft AD를 사용하여 클라이언트측 LDAPS를 활성화합니다.](#)을(를) 참조하세요.

주제

- [관리형 AWS Microsoft AD를 사용하여 서버측 LDAPS를 활성화합니다.](#)
- [관리형 AWS Microsoft AD를 사용하여 클라이언트측 LDAPS를 활성화합니다.](#)

관리형 AWS Microsoft AD를 사용하여 서버측 LDAPS를 활성화합니다.

서버측 경량 디렉터리 액세스 프로토콜 SSL (보안 소켓 계층) /TLS (전송 계층 보안) (LDAPS) 지원은 상용 또는 자체 개발된 LDAP 인식 응용 프로그램과 관리형 Microsoft AD 디렉터리 간의 LDAP 통신을 암호화합니다. AWS 이렇게 하면 Secure Sockets Layer(SSL) 암호화 프로토콜을 사용하여 유선 보안을 개선하고 규정 준수 요구 사항을 충족할 수 있습니다.

서버 측 LDAPS 활성화

서버측 LDAPS 및 CA (인증 기관) 서버를 설정하고 구성하는 방법에 대한 자세한 지침은 보안 블로그의 [AWS 관리형 Microsoft AD 디렉터리에 대해 서버측 LDAPS를 활성화하는 방법을](#) 참조하십시오.

AWS

대부분의 설정은 AWS Managed Microsoft AD 도메인 컨트롤러를 관리하는 데 사용하는 Amazon EC2 인스턴스로부터 수행해야 합니다. 다음 단계는 클라우드에서 도메인의 LDAPS를 활성화하는 방법을 안내합니다. AWS

자동화를 사용하여 PKI 인프라를 설정하려면 [Microsoft 공개 키 인프라 on AWS QuickStart Guide](#)를 사용할 수 있습니다. 특히 안내서의 지침에 따라 [AWS의 기존 VPC에 Microsoft PKI 배포](#)를 위한 템플릿을 로드하는 것이 좋습니다. 템플릿을 로드한 후에는 Active Directory 도메인 서비스 유형 옵션으로 이동하면 **AWSManaged**를 선택해야 합니다. QuickStart 가이드를 사용한 경우 바로 이동할 [3단계: 인증서 템플릿 생성](#) 수 있습니다.

주제

- [1단계: LDAPS를 활성화할 수 있는 사용자 위임](#)

- [2단계: 인증 기관 설정](#)
- [3단계: 인증서 템플릿 생성](#)
- [4단계: 보안 그룹 규칙 추가](#)

1단계: LDAPS를 활성화할 수 있는 사용자 위임

서버측 LDAPS를 활성화하려면 관리형 AWS Microsoft AD 디렉터리의 관리자 또는 AWS 위임된 엔터프라이즈 인증 기관 관리자 그룹의 구성원이어야 합니다. 또는 기본 관리 사용자(관리자 계정)여야 합니다. 원하는 경우 관리자 계정 설정 LDAPS 이외의 사용자가 있을 수 있습니다. 이 경우 관리형 AWS Microsoft AD 디렉터리의 관리자 또는 AWS 위임된 엔터프라이즈 인증 기관 관리자 그룹에 해당 사용자를 추가하세요.

2단계: 인증 기관 설정

서버 측 LDAPS를 활성화하려면 먼저 인증서를 만들어야 합니다. 이 인증서는 AWS 관리형 Microsoft AD 도메인에 가입된 Microsoft 엔터프라이즈 CA 서버에서 발급해야 합니다. 생성된 인증서는 해당 도메인의 각 도메인 컨트롤러에 설치해야 합니다. 이 인증서는 도메인 컨트롤러 상의 LDAP 서비스가 LDAP 클라이언트로부터의 SSL 연결을 수신 대기하고 자동으로 수락할 수 있게 허용합니다.

Note

관리형 AWS Microsoft AD를 사용하는 서버측 LDAPS는 독립 실행형 CA에서 발급한 인증서를 지원하지 않습니다. 타사 인증 기관에서 발급한 인증서도 지원하지 않습니다.

비즈니스 필요에 따라 다음과 같이 도메인에서 CA를 설정 또는 연결할 수 있는 옵션이 있습니다.

- 하위 Microsoft 엔터프라이즈 CA 생성 - (권장) 이 옵션을 사용하면 클라우드에 하위 Microsoft 엔터프라이즈 CA 서버를 배포할 수 있습니다. AWS 서버에서는 Amazon EC2를 사용하여 기존 루트 Microsoft CA로 작업할 수 있습니다. 하위 Microsoft 엔터프라이즈 CA를 설정하는 방법에 대한 자세한 내용은 [관리되는 AWS Microsoft AD 디렉터리의 서버측 LDAPS를 활성화하는 방법에서 4단계: AWS Microsoft AD 디렉터리에 Microsoft 엔터프라이즈 CA 추가](#)를 참조하십시오.
- 루트 Microsoft 엔터프라이즈 CA 생성 — 이 옵션을 사용하면 Amazon EC2를 사용하여 AWS 클라우드에서 루트 Microsoft 엔터프라이즈 CA를 생성하고 관리형 AWS Microsoft AD 도메인에 가입할 수 있습니다. 이 루트 CA는 도메인 컨트롤러에 인증서를 발급합니다. 새 루트 CA 설정에 대한 자세한 내용은 [관리되는 AWS Microsoft AD 디렉터리의 서버측 LDAPS를 사용하도록 설정하는 방법에서 3단계: 오프라인 CA 설치 및 구성](#)을 참조하십시오.

EC2 인스턴스를 도메인에 조인하는 방법에 대한 자세한 내용은 [Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory](#) 단원을 참조하세요.

3단계: 인증서 템플릿 생성

엔터프라이즈 CA를 설정한 후 Kerberos 인증 인증서 템플릿을 구성할 수 있습니다.

인증서 템플릿을 생성하려면

1. Microsoft Windows Server Manager를 시작합니다. 도구 > 인증 기관을 선택합니다.
2. 인증 기관 창에서 왼쪽 창의 인증 기관 트리를 확장합니다. Certificate Templates를 마우스 오른쪽 버튼으로 클릭하고 Manage를 선택합니다.
3. Certificate Templates Console 창에서 Kerberos Authentication을 마우스 오른쪽 버튼으로 클릭하고 Duplicate Template을 선택합니다.
4. 새 템플릿의 속성 창이 나타납니다.
5. 새 템플릿 속성 창에서 호환성 탭으로 이동한 후 다음을 수행합니다.
 - a. 인증 기관을 CA와 일치하는 OS로 변경합니다.
 - b. 변경 결과 창이 나타나면 확인을 선택합니다.
 - c. 인증 수신자를 Windows 10/ Windows Server 2016으로 변경하십시오.

Note

AWS 매니지드 마이크로소프트 AD는 윈도우 서버 2019에 의해 구동됩니다.

- d. 변경 결과 창이 나타나면 확인을 선택합니다.
6. 일반 탭을 클릭하고 템플릿 표시 이름을 LDApoverssl 또는 원하는 다른 이름으로 변경합니다.
7. 보안 탭을 클릭하고 그룹 또는 사용자 이름 섹션에서 도메인 컨트롤러를 선택합니다. 도메인 컨트롤러에 대한 권한 섹션에서 읽기, 등록, 자동 등록에 대한 허용 확인란이 선택되어 있는지 확인합니다.
8. 확인을 선택하여 LDApoverSSL(또는 앞서 지정한 이름) 인증서 템플릿을 생성합니다. 인증서 템플릿 콘솔 창을 닫습니다.
9. Certificate Authority 창에서 Certificate Templates를 마우스 오른쪽 버튼으로 클릭하고 New > Certificate Template to Issue를 선택합니다.
10. 인증서 템플릿 사용 창에서 LDApoverSL(또는 앞서 지정한 이름)을 선택한 다음 확인을 선택합니다.

4단계: 보안 그룹 규칙 추가

마지막 단계에서 Amazon EC2 콘솔을 열고 보안 그룹 규칙을 추가해야 합니다. 이러한 규칙을 사용하면 도메인 컨트롤러가 엔터프라이즈 CA에 연결하여 인증서를 요청할 수 있습니다. 이렇게 하려면 엔터프라이즈 CA가 도메인 컨트롤러로부터 수신 트래픽을 수락할 수 있도록 인바운드 규칙을 추가합니다. 그런 다음 도메인 컨트롤러에서 엔터프라이즈 CA로 가는 트래픽을 허용하도록 아웃바운드 규칙을 추가합니다.

두 규칙이 모두 구성되면 도메인 컨트롤러가 자동으로 엔터프라이즈 CA에 인증서를 요청하고 디렉터리에 대해 LDAPS를 활성화합니다. 이제 도메인 컨트롤러의 LDAP 서비스가 LDAPS 연결을 수락할 준비가 되었습니다.

보안 그룹 규칙을 구성하려면

1. Amazon EC2 콘솔 <https://console.aws.amazon.com/ec2>로 이동하여 관리자 보안 인증 정보로 로그인합니다.
2. 탐색 창의 Network & Security에서 Security Groups를 선택합니다.
3. 기본 창에서 CA의 AWS 보안 그룹을 선택합니다.
4. 인바운드(Inbound) 탭을 선택한 후 편집(Edit)을 선택합니다.
5. [Edit inbound rules] 대화 상자에서 다음을 수행합니다.
 - 규칙 추가(Add Rule)를 선택합니다.
 - 유형에서 모든 트래픽을 선택하고 소스로 사용자 지정을 선택합니다.
 - 소스 옆의 상자에 디렉터리의 AWS 보안 그룹 (예: sg-123456789) 을 입력합니다.
 - 저장을 선택합니다.
6. 이제 AWS 관리형 Microsoft AD 디렉터리의 AWS 보안 그룹을 선택합니다. [Outbound] 탭을 선택하고 [Edit]를 선택합니다.
7. [Edit outbound rules] 대화 상자에서 다음을 수행합니다.
 - 규칙 추가(Add Rule)를 선택합니다.
 - 유형에서 모든 트래픽을 선택하고 대상에서 사용자 지정을 선택합니다.
 - 대상 옆의 상자에 CA의 AWS 보안 그룹을 입력합니다.
 - 저장을 선택합니다.

LDP 도구를 사용하여 AWS 관리형 Microsoft AD 디렉터리에 대한 LDAPS 연결을 테스트할 수 있습니다. LDP 도구는 Active Directory 관리 도구에 포함되어 있습니다. 자세한 정보는 [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)을 참조하세요.

Note

LDAPS 연결을 테스트하기 전에 하위 CA가 도메인 컨트롤러에 인증서를 발급할 때까지 최대 30분간 기다려야 합니다.

서버측 LDAPS에 대한 자세한 내용과 설정 방법에 [대한 예제 사용 사례를 보려면 보안 블로그의 AWS 관리형 Microsoft AD 디렉터리에 대해 서버측 LDAPS를 활성화하는 방법을 참조하십시오.](#) AWS

관리형 AWS Microsoft AD를 사용하여 클라이언트측 LDAPS를 활성화합니다.

Managed AWS Microsoft AD의 클라이언트측 경량 디렉터리 액세스 프로토콜 SSL (보안 소켓 계층) / TLS (전송 계층 보안) (LDAPS) 지원은 자체 관리형 (온-프레미스) Microsoft Active Directory (AD) 와 응용 프로그램 간의 통신을 암호화합니다. AWS 이러한 애플리케이션의 예로는 WorkSpaces AWS IAM Identity Center QuickSight, Amazon 및 Amazon Chime이 있습니다. 이 암호화를 통해 조직의 자격 증명 데이터에 대한 보안을 강화하고 보안 요구 사항을 충족할 수 있습니다.

필수 조건

클라이언트 측 LDAPS를 활성화하려면 먼저 다음 요구 사항을 충족해야 합니다.

주제

- [AWS 관리형 Microsoft AD와 자체 관리형 AD 간에 신뢰 관계를 구축하십시오. Microsoft Active Directory](#)
- [Active Directory에 서버 인증서 배포](#)
- [인증 기관 인증서 요구 사항](#)
- [네트워킹 요구 사항](#)

AWS 관리형 Microsoft AD와 자체 관리형 AD 간에 신뢰 관계를 구축하십시오. Microsoft Active Directory

먼저, 클라이언트측 LDAPS를 Microsoft Active Directory 활성화하려면 AWS 관리형 Microsoft AD와 자체 관리형 AD 간에 신뢰 관계를 설정해야 합니다. 자세한 정보는 [the section called “신뢰 관계 생성”](#)을 참조하세요.

Active Directory에 서버 인증서 배포

클라이언트 측 LDAPS를 활성화하려면 Active Directory의 각 도메인 컨트롤러에 대한 서버 인증서를 가져와 설치해야 합니다. LDAP 서비스에서는 이러한 인증서를 사용하여 LDAP 클라이언트로부터의 SSL 연결을 수신하고 자동으로 수락합니다. 사내 Active Directory 인증서 서비스(ADCS) 배포에서 발급하거나 상업용 발급자로부터 구매한 SSL 인증서를 사용할 수 있습니다. Active Directory 서버 인증서 요구 사항에 대한 자세한 내용은 Microsoft 웹 사이트의 [LDAP over SSL \(LDAPS\) Certificate](#)를 참조하세요.

인증 기관 인증서 요구 사항

클라이언트 측 LDAPS 작업에는 서버 인증서의 발급자를 나타내는 인증 기관(CA) 인증서가 필요합니다. CA 인증서는 LDAP 통신을 암호화하기 위해 Active Directory 도메인 컨트롤러에서 제공하는 서버 인증서와 일치합니다. 다음 CA 인증서 요구 사항에 유의하세요.

- 클라이언트 측 LDAPS를 활성화하려면 엔터프라이즈 인증 기관 (CA) 이 필요합니다. Active Directory 인증서 서비스, 타사 상용 인증 기관 또는 둘 중 하나를 사용할 수 있습니다. [AWS Certificate Manager](#) Microsoft 엔터프라이즈 인증 기관에 대한 자세한 내용은 [Microsoft 설명서](#)를 참조하십시오.
- 인증서를 등록하려면 만료일까지 90일 이상 남아 있어야 합니다.
- 인증서는 PEM(Privacy-Enhanced Mail) 형식이어야 합니다. Active Directory 내부에서 CA 인증서를 내보내는 경우 내보내기 파일 형식으로 base64로 인코딩된 X.509(.CER)를 선택합니다.
- AWS 관리형 Microsoft AD 디렉터리당 최대 5개의 CA 인증서를 저장할 수 있습니다.
- RSASSA-PSS 서명 알고리즘을 사용하는 인증서는 지원되지 않습니다.
- 신뢰할 수 있는 모든 도메인의 모든 서버 인증서에 연결되는 CA 인증서를 등록해야 합니다.

네트워킹 요구 사항

AWS 애플리케이션 LDAP 트래픽은 LDAP 포트 389로 대체되지 않고 TCP 포트 636에서만 독점적으로 실행됩니다. 그러나 복제, 신뢰 등을 지원하는 Windows LDAP 통신은 Windows 기본 보안과 함께 LDAP 포트 389를 계속 사용합니다. 관리형 AWS Microsoft AD (아웃바운드) 및 자체 관리형 Active Directory (인바운드) 의 포트 636에서 TCP 통신을 허용하도록 AWS 보안 그룹과 네트워크 방화벽을 구성합니다. AWS Managed Microsoft AD 및 자체 관리형 Active Directory 간에 LDAP 포트 389를 열어 둡니다.

클라이언트 측 LDAPS 활성화

클라이언트 측 LDAPS를 활성화하려면 인증 기관(CA) 인증서를 AWS Managed Microsoft AD로 가져온 다음 디렉터리에서 LDAPS를 활성화합니다. 활성화하면 AWS 애플리케이션과 자체 관리형 Active Directory 간의 모든 LDAP 트래픽이 Secure Sockets Layer(SSL) 채널 암호화를 통해 흐릅니다.

두 가지 방법을 사용하여 디렉터리에 대해 클라이언트 측 LDAPS를 활성화할 수 있습니다. 방법 또는 방법 중 하나를 사용할 수 있습니다. AWS Management Console AWS CLI

Note

클라이언트 측 LDAPS는 관리형 AWS Microsoft AD의 지역별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)을 참조하세요.

주제

- [1단계: 인증서 등록 AWS Directory Service](#)
- [2단계: 등록 상태 확인](#)
- [3단계: 클라이언트 측 LDAPS 활성화](#)
- [4단계: LDAPS 상태 확인](#)

1단계: 인증서 등록 AWS Directory Service

다음 방법 중 하나를 사용하여 인증서를 등록하십시오 AWS Directory Service.

방법 1: AWS Directory Service (AWS Management Console) 에 인증서를 등록하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 인증서를 등록할 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션에서 작업 메뉴를 선택한 다음 인증서 등록을 선택합니다.
5. CA 인증서 등록 대화 상자에서 찾아보기를 선택한 다음 인증서를 선택하고 열기를 선택합니다.

6. 인증서 등록을 선택합니다.

방법 2: AWS Directory Service (AWS CLI) 에 인증서 등록하기

- 다음 명령을 실행합니다. 인증서 데이터의 경우 CA 인증서 파일의 위치를 가리킵니다. 응답에 인증서 ID가 제공됩니다.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data  
file://your_file_path
```

2단계: 등록 상태 확인

인증서 등록 상태 또는 등록된 인증서 목록을 보려면 다음 명령을 사용합니다.

방법 1: AWS Directory Service (AWS Management Console) 에서 인증서 등록 상태 확인하기

- Directory details(디렉터리 세부 정보) 페이지의 클라이언트측 LDAPS 섹션으로 이동합니다.
- 등록 상태 열 아래 표시되는 현재 인증서 등록 상태를 검토합니다. 등록 상태 값이 등록됨으로 변경되면 인증서가 성공적으로 등록된 것입니다.

방법 2: AWS Directory Service (AWS CLI) 에서 인증서 등록 상태 확인하기

- 다음 명령을 실행합니다. 상태 값이 Registered를 반환하면 인증서가 성공적으로 등록된 것입니다.

```
aws ds list-certificates --directory-id your_directory_id
```

3단계: 클라이언트 측 LDAPS 활성화

다음 방법 중 하나를 사용하여 클라이언트측 LDAPS를 활성화하십시오. AWS Directory Service

Note

클라이언트 측 LDAPS를 활성화하려면 인증서를 하나 이상 등록해야 합니다.

방법 1: () 에서 클라이언트측 LDAPS를 활성화하려면 AWS Directory ServiceAWS Management Console

1. Directory details(디렉터리 세부 정보) 페이지의 클라이언트측 LDAPS 섹션으로 이동합니다.
2. 활성화를 선택합니다. 이 옵션을 사용할 수 없는 경우, 유효한 인증서가 성공적으로 등록되었는지 확인한 다음 다시 시도하세요.
3. 클라이언트 측 LDAPS 활성화 대화 상자에서 활성화를 선택합니다.

방법 2: () 에서 클라이언트측 LDAPS를 활성화하려면 AWS Directory ServiceAWS CLI

- 다음 명령을 실행합니다.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

4단계: LDAPS 상태 확인

다음 방법 중 하나를 사용하여 에서 LDAPS 상태를 확인합니다. AWS Directory Service

방법 1: () 에서 AWS Directory Service LDAPS 상태를 확인하려면AWS Management Console

1. Directory details(디렉터리 세부 정보) 페이지의 클라이언트측 LDAPS 섹션으로 이동합니다.
2. 상태 값이 활성화됨으로 표시되면 LDAPS가 성공적으로 구성된 것입니다.

방법 2: () 에서 AWS Directory Service LDAPS 상태를 확인하려면AWS CLI

- 다음 명령을 실행합니다. 상태 값이 Enabled을 반환하면 LDAPS가 성공적으로 구성된 것입니다.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

클라이언트 측 LDAPS 관리

LDAPS 구성을 관리하려면 다음 명령을 사용합니다.

두 가지 방법을 사용하여 클라이언트 측 LDAPS 설정을 관리할 수 있습니다. AWS Management Console 메서드 또는 메서드 중 하나를 사용할 수 있습니다 AWS CLI .

인증서 세부 정보 보기

다음 방법 중 하나를 사용하여 인증서가 만료되도록 설정된 시기를 확인합니다.

방법 1: AWS Directory Service (AWS Management Console) 에서 인증서 세부 정보를 보려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 인증서를 보려는 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션의 CA 인증서 아래에 인증서에 대한 정보가 표시됩니다.

방법 2: AWS Directory Service (AWS CLI) 에서 인증서 세부 정보를 보려면

- 다음 명령을 실행합니다. 인증서 ID의 경우 register-certificate 또는 list-certificates에서 반환한 식별자를 사용합니다.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

인증서 등록 취소

다음 방법 중 하나를 사용하여 인증서 등록을 취소합니다.

Note

인증서가 하나만 등록된 경우 먼저 LDAPS를 비활성화해야 인증서의 등록을 취소할 수 있습니다.

방법 1: AWS Directory Service (AWS Management Console)에서 인증서 등록을 취소하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.

- 다중 리전 복제에 여러 리전이 표시된 경우 인증서 등록을 취소할 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션에서 작업을 선택한 다음 인증서 등록 취소를 선택합니다.
 5. CA 인증서 등록 취소 대화 상자에서 등록 취소를 선택합니다.

방법 2: () 에서 AWS Directory Service 인증서 등록 취소하기AWS CLI

- 다음 명령을 실행합니다. 인증서 ID의 경우 register-certificate 또는 list-certificates에서 반환한 식별자를 사용합니다.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

클라이언트 측 LDAPS 비활성화

다음 방법 중 하나를 사용하여 클라이언트 측 LDAPS를 비활성화합니다.

방법 1: () 에서 클라이언트 측 LDAPS를 비활성화하려면 AWS Directory ServiceAWS Management Console

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 클라이언트 측 LDAPS를 사용하지 않도록 설정할 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션에서 비활성화를 선택합니다.
5. 클라이언트 측 LDAPS 비활성화 대화 상자에서 비활성화를 선택합니다.

방법 2: () 에서 클라이언트 측 LDAPS를 비활성화하려면 AWS Directory ServiceAWS CLI

- 다음 명령을 실행합니다.


```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

인증서 등록 문제

AWS 관리형 Microsoft AD 도메인 컨트롤러를 CA 인증서에 등록하는 프로세스에는 최대 30분이 소요될 수 있습니다. 인증서 등록에 문제가 발생하여 관리형 AWS Microsoft AD 도메인 컨트롤러를 다시 시작하려는 경우 문의할 수 있습니다. AWS Support 지원 사례를 만들려면 지원 사례 [만들기 및 사례 관리](#)를 참조하십시오.

AWS 관리형 Microsoft AD에 대한 규정 준수 관리

AWS 관리형 Microsoft AD를 사용하여 AWS 클라우드에서 다음 규정 준수 요구 사항이 적용되는 Active Directory 인식 애플리케이션을 지원할 수 있습니다. 하지만 Simple AD를 사용하는 경우 애플리케이션이 규정 준수 요건을 충족하지 않습니다.

지원되는 규정 준수 표준

AWS Managed Microsoft AD는 다음 표준에 대한 감사를 거쳤으며 규정 준수 인증을 받아야 하는 솔루션의 일부로 사용할 수 있습니다.



AWS 관리형 Microsoft AD는 연방 위험 및 권한 부여 관리 프로그램 (FedRAMP) 보안 요구 사항을 충족하며 FedRAMP 보통/상한 기준에 따라 FedRAMP 공동 승인 위원회 (JAB) 잠정 운영 권한 (P-ATO) 를 받았습니다. FedRAMP에 대한 자세한 내용은 [FedRAMP 규정 준수](#)를 참조하십시오.



AWS 관리형 Microsoft AD는 서비스 제공업체 레벨 1의 PCI (지불 카드 산업) DSS (데이터 보안 표준) 버전 3.2에 대한 규정 준수를 입증했습니다. AWS 제품 및 서비스를 사용하여 카드 소지자 데이터를 저장, 처리 또는 전송하는 고객은 자체 PCI DSS 규정 준수 인증을 관리할 때 AWS Managed Microsoft AD를 사용할 수 있습니다.

[PCI AWS 컴플라이언스 패키지의 사본을 요청하는 방법을 포함하여 PCI DSS에 대한 자세한 내용은 PCI DSS 레벨 1을 참조하십시오.](#) 중요한 것은 관리형 AWS Microsoft AD에서 PCI DSS 버전 3.2 표준과 일치하도록 세분화된 암호 정책을 구성해야 한다는 것입니다. 적용해야 하는 정책에 대한 자세한 내용은 관리형 AWS Microsoft AD 디렉터리에 대한 PCI 규정 준수 활성화라는 제목의 아래 섹션을 참조하십시오.



AWS는 [건강 보험 양도 및 책임에 관한 법률 \(HIPAA\) 규정 준수 프로그램을 확장하여 관리형 AWS Microsoft AD를 HIPAA 적격 서비스로 포함시켰습니다.](#) BAA (비즈니스 제휴 계약)를 체결한 경우 AWS 관리형 Microsoft AD를 사용하여 HIPAA 준수 애플리케이션을 구축할 수 있습니다. AWS

AWS 의료 정보의 처리 및 저장에 활용할 AWS 수 있는 방법에 대해 자세히 알고 싶은 고객을 위해 [HIPAA에 초점을 맞춘 백서](#)를 제공합니다. 자세한 내용은 [HIPAA 규정 준수를 참조](#)하십시오.

공동 책임

FedRAMP, HIPAA 및 PCI 규정 준수를 비롯해 보안은 [공동 책임](#)입니다. AWS Managed Microsoft AD 규정 준수 상태는 AWS 클라우드에서 실행하는 애플리케이션에 자동으로 적용되지 않는다는 점을 이해하는 것이 중요합니다. AWS 서비스 사용이 표준을 준수하는지 확인해야 합니다.

AWS Managed Microsoft AD가 지원하는 다양한 AWS 규정 준수 프로그램의 전체 목록은 규정 [준수 프로그램별 범위 내 AWS 서비스](#)를 참조하십시오.

AWS 관리형 Microsoft AD 디렉터리에 대해 PCI 규정 준수를 활성화합니다.

AWS 관리형 Microsoft AD 디렉터리에 대해 PCI 규정 준수를 활성화하려면 에서 제공하는 PCI DSS AOC (규정 준수 증명) 및 책임 요약 문서에 지정된 대로 세분화된 암호 정책을 구성해야 합니다. AWS Artifact

세분화된 암호 정책 사용에 대한 자세한 내용은 [AWS 관리형 Microsoft AD에 대한 암호 정책 관리](#) 단원을 참조하세요.

AWS Managed Microsoft AD 네트워크 보안 구성 강화

AWS Managed Microsoft AD 디렉터리에 대해 프로비저닝된 AWS 보안 그룹은 AWS Managed Microsoft AD 디렉터리에 대해 알려진 모든 사용 사례를 지원하는 데 필요한 최소 인바운드 네트워크 포트로 구성됩니다. 프로비저닝된 AWS 보안 그룹에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#) 단원을 참조하세요.

AWS Managed Microsoft AD 디렉터리의 네트워크 보안을 더욱 강화하기 위해 아래 나열된 일반적인 시나리오에 따라 AWS 보안 그룹을 수정할 수 있습니다.

주제

- [AWS 애플리케이션 전용 지원](#)
- [신뢰 지원만 있는 AWS 애플리케이션](#)
- [AWS 애플리케이션 및 네이티브 Active Directory 워크로드 지원](#)
- [신뢰 지원과 함께 AWS 애플리케이션 및 네이티브 Active Directory 워크로드 지원](#)


AWS 애플리케이션 전용 지원

모든 사용자 계정은 다음과 같이 지원되는 AWS 애플리케이션과 함께 사용할 수 있도록 사용자의 AWS Managed Microsoft AD에서만 프로비저닝됩니다.

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- AWS Client VPN

- AWS Management Console

다음 AWS 보안 그룹 구성을 사용하여 AWS Managed Microsoft AD 도메인 컨트롤러에 대한 필수적이 아닌 모든 트래픽을 차단할 수 있습니다.

 Note

- 다음은 이 AWS 보안 그룹 구성과 호환되지 않습니다.
 - Amazon EC2 인스턴스
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Active Directory 신뢰
 - 도메인에 조인된 클라이언트 또는 서버

인바운드 규칙

없음.

아웃바운드 규칙

없음.

신뢰 지원만 있는 AWS 애플리케이션

모든 사용자 계정은 다음과 같이 지원되는 AWS 애플리케이션에서 사용할 수 있도록 사용자의 AWS Managed Microsoft AD 또는 신뢰할 수 있는 Active Directory에서 프로비저닝됩니다.

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center

- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

프로비저닝된 AWS 보안 그룹 구성을 수정하여 AWS Managed Microsoft AD 도메인 컨트롤러에 대한 필수적이 아닌 모든 트래픽을 차단할 수 있습니다.

Note

- 다음은 이 AWS 보안 그룹 구성과 호환되지 않습니다.
 - Amazon EC2 인스턴스
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Active Directory 신뢰
 - 도메인에 조인된 클라이언트 또는 서버
- 이 구성을 사용하려면 “온프레미스 CIDR” 네트워크가 안전한지 확인해야 합니다.
- TCP 445는 신뢰 생성에만 사용되며 신뢰가 설정된 후에 제거할 수 있습니다.
- TCP 636은 LDAP over SSL이 사용 중인 경우에만 필요합니다.

인바운드 규칙

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP 및 UDP	53	온프레미스 CIDR	DNS	사용자 및 컴퓨터 인증, 이름 확인, 신뢰
TCP 및 UDP	88	온프레미스 CIDR	Kerberos	사용자 및 컴퓨터 인증, 포리스트 수준 신뢰
TCP 및 UDP	389	온프레미스 CIDR	LDAP	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP 및 UDP	464	온프레미스 CIDR	Kerberos 암호 변경/설정	복제, 사용자 및 컴퓨터 인증, 신뢰
TCP	445	온프레미스 CIDR	SMB/CIFS	복제, 사용자 및 컴퓨터 인증, 그룹 정책 신뢰
TCP	135	온프레미스 CIDR	복제	RPC, EPM
TCP	636	온프레미스 CIDR	LDAP SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP	49152 - 65535	온프레미스 CIDR	RPC	복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP	3268 - 3269	온프레미스 CIDR	LDAP GC 및 LDAP GC SSL	디렉터리, 복제, 사용자 및 컴퓨터

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
				인증 그룹 정책, 신뢰
UDP	123	온프레미스 CIDR	Windows 시간	Windows 시간, 신뢰

아웃바운드 규칙

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
모두	모두	온프레미스 CIDR	모든 트래픽	

AWS 애플리케이션 및 네이티브 Active Directory 워크로드 지원

사용자 계정은 다음과 같이 지원되는 AWS 애플리케이션과 함께 사용할 수 있도록 사용자의 AWS Managed Microsoft AD에서만 프로비저닝됩니다.

- Amazon Chime
- Amazon Connect
- Amazon EC2 인스턴스
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail

- WorkSpaces
- AWS Client VPN
- AWS Management Console

프로비저닝된 AWS 보안 그룹 구성을 수정하여 AWS Managed Microsoft AD 도메인 컨트롤러에 대한 필수적이 아닌 모든 트래픽을 차단할 수 있습니다.

Note

- Active Directory 신뢰는 사용자의 AWS 디렉터리와 온프레미스 도메인 간에 생성 및 유지 관리할 수 없습니다.
- “클라이언트 CIDR” 네트워크가 안전한지 확인해야 합니다.
- TCP 636은 LDAP over SSL이 사용 중인 경우에만 필요합니다.
- 이 구성에서 엔터프라이즈 CA를 사용하려면 아웃바운드 규칙 “TCP, 443, CA CIDR”을 생성해야 합니다.

인바운드 규칙

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP 및 UDP	53	클라이언트 CIDR	DNS	사용자 및 컴퓨터 인증, 이름 확인, 신뢰
TCP 및 UDP	88	클라이언트 CIDR	Kerberos	사용자 및 컴퓨터 인증, 포리스트 수준 신뢰
TCP 및 UDP	389	클라이언트 CIDR	LDAP	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP 및 UDP	445	클라이언트 CIDR	SMB/CIFS	복제, 사용자 및 컴퓨터 인증, 그룹 정책 신뢰
TCP 및 UDP	464	클라이언트 CIDR	Kerberos 암호 변경/설정	복제, 사용자 및 컴퓨터 인증, 신뢰
TCP	135	클라이언트 CIDR	복제	RPC, EPM
TCP	636	클라이언트 CIDR	LDAP SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP	49152 - 65535	클라이언트 CIDR	RPC	복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP	3268 - 3269	클라이언트 CIDR	LDAP GC 및 LDAP GC SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP	9389	클라이언트 CIDR	SOAP	AD DS 웹 서비스
UDP	123	클라이언트 CIDR	Windows 시간	Windows 시간, 신뢰
UDP	138	클라이언트 CIDR	DFSN 및 NetLogon	DFS, 그룹 정책

아웃바운드 규칙

없음.

신뢰 지원과 함께 AWS 애플리케이션 및 네이티브 Active Directory 워크로드 지원

모든 사용자 계정은 다음과 같이 지원되는 AWS 애플리케이션에서 사용할 수 있도록 사용자의 AWS Managed Microsoft AD 또는 신뢰할 수 있는 Active Directory에서 프로비저닝됩니다.

- Amazon Chime
- Amazon Connect
- Amazon EC2 인스턴스
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

프로비저닝된 AWS 보안 그룹 구성을 수정하여 AWS Managed Microsoft AD 도메인 컨트롤러에 대한 필수적이 아닌 모든 트래픽을 차단할 수 있습니다.

Note

- 그러려면 “온프레미스 CIDR” 및 “클라이언트 CIDR” 네트워크가 안전한지 확인해야 합니다.
- “온프레미스 CIDR”이 있는 TCP 445는 신뢰 생성에만 사용되며 신뢰가 설정된 후에 제거할 수 있습니다.
- “클라이언트 CIDR”이 있는 TCP 445는 그룹 정책 처리에 필요한 대로 열려 있어야 합니다.
- TCP 636은 LDAP over SSL이 사용 중인 경우에만 필요합니다.

- 이 구성에서 엔터프라이즈 CA를 사용하려면 아웃바운드 규칙 "TCP, 443, CA CIDR"을 생성해야 합니다.

인바운드 규칙

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP 및 UDP	53	온프레미스 CIDR	DNS	사용자 및 컴퓨터 인증, 이름 확인, 신뢰
TCP 및 UDP	88	온프레미스 CIDR	Kerberos	사용자 및 컴퓨터 인증, 포리스트 수준 신뢰
TCP 및 UDP	389	온프레미스 CIDR	LDAP	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP 및 UDP	464	온프레미스 CIDR	Kerberos 암호 변경/설정	복제, 사용자 및 컴퓨터 인증, 신뢰
TCP	445	온프레미스 CIDR	SMB/CIFS	복제, 사용자 및 컴퓨터 인증, 그룹 정책 신뢰
TCP	135	온프레미스 CIDR	복제	RPC, EPM
TCP	636	온프레미스 CIDR	LDAP SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP	49152 - 65535	온프레미스 CIDR	RPC	복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP	3268 - 3269	온프레미스 CIDR	LDAP GC 및 LDAP GC SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
UDP	123	온프레미스 CIDR	Windows 시간	Windows 시간, 신뢰
TCP 및 UDP	53	클라이언트 CIDR	DNS	사용자 및 컴퓨터 인증, 이름 확인, 신뢰
TCP 및 UDP	88	클라이언트 CIDR	Kerberos	사용자 및 컴퓨터 인증, 포리스트 수준 신뢰
TCP 및 UDP	389	클라이언트 CIDR	LDAP	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP 및 UDP	445	클라이언트 CIDR	SMB/CIFS	복제, 사용자 및 컴퓨터 인증, 그룹 정책 신뢰
TCP 및 UDP	464	클라이언트 CIDR	Kerberos 암호 변경/설정	복제, 사용자 및 컴퓨터 인증, 신뢰
TCP	135	클라이언트 CIDR	복제	RPC, EPM

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
TCP	636	클라이언트 CIDR	LDAP SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP	49152 - 65535	클라이언트 CIDR	RPC	복제, 사용자 및 컴퓨터 인증, 그룹 정책, 신뢰
TCP	3268 - 3269	클라이언트 CIDR	LDAP GC 및 LDAP GC SSL	디렉터리, 복제, 사용자 및 컴퓨터 인증 그룹 정책, 신뢰
TCP	9389	클라이언트 CIDR	SOAP	AD DS 웹 서비스
UDP	123	클라이언트 CIDR	Windows 시간	Windows 시간, 신뢰
UDP	138	클라이언트 CIDR	DFSN 및 NetLogon	DFS, 그룹 정책

아웃바운드 규칙

프로토콜	포트 범위	소스	트래픽 유형	Active Directory 사용
모두	모두	온프레미스 CIDR	모든 트래픽	

보안 설정 구성

운영 워크로드를 늘리지 않고도 규정 준수 및 보안 요구 사항을 충족하도록 AWS Managed Microsoft AD에 대한 세분화된 디렉터리 설정을 구성할 수 있습니다. 디렉터리 설정에서, 디렉터리에 사용되는 프로토콜 및 암호의 보안 채널 구성을 업데이트할 수 있습니다. 예를 들어 RC4 또는 DES와 같은 개별 레거시 암호와 SSL 2.0/3.0 및 TLS 1.0/1.1과 같은 프로토콜을 유연하게 비활성화할 수 있습니다. AWS 그런 다음 Managed Microsoft AD는 디렉터리 내의 모든 도메인 컨트롤러에 구성을 배포하고, 도메인 컨트롤러 재부팅을 관리하며, 스케일 아웃하거나 추가 AWS 리전을 배포할 때 이 구성을 유지합니다. 사용 가능한 모든 설정에 대한 세부 정보는 [디렉터리 보안 설정 목록](#) 단원을 참조하세요.

디렉터리 보안 설정 편집

모든 디렉터리의 설정을 구성하고 편집할 수 있습니다.

디렉터리 설정을 편집하려면

1. AWS 관리형 콘솔에 로그인하여 <https://console.aws.amazon.com/directoryservicev2/>에서 AWS Directory Service 콘솔을 엽니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Networking & security(네트워킹 및 보안)에서 Directory settings(디렉터리 설정)을 찾은 다음 Edit settings(설정 편집)을 선택합니다.
4. Edit settings(설정 편집)에서 편집하려는 설정의 Value(값)을 변경합니다. 설정을 편집하면 상태가 Default(기본값) 에서 Ready to Update(업데이트 준비 완료)로 바뀝니다. 이전에 설정을 편집한 경우 상태가 Updated(업데이트됨)에서 Ready to Update(업데이트 준비 완료)로 바뀝니다. 그런 다음 검토를 선택합니다.
5. 설정 검토 및 업데이트에서 디렉터리 설정을 참조하여 새 값이 모두 올바른지 확인합니다. 기타 설정을 변경하려면 설정 편집을 선택합니다. 변경 사항에 만족하고 새 값을 적용할 준비가 되면 설정 업데이트를 선택합니다. 그러면 디렉터리 ID 페이지로 다시 이동됩니다.

Note

디렉터리 설정에서 업데이트된 설정의 상태를 볼 수 있습니다. 설정이 구현되는 동안에는 상태가 업데이트 중으로 표시됩니다. 설정에서 상태에 업데이트 중이 표시되는 동안에는 다른 설정을 편집할 수 없습니다. 편집한 내용으로 설정이 성공적으로 업데이트되면 상태가 업데이트됨으로 표시됩니다. 편집 내용으로 설정이 업데이트되지 않으면 상태가 실패로 표시됩니다.

디렉터리 보안 설정 실패

설정 업데이트 중에 오류가 발생하는 경우 상태가 실패로 표시됩니다. 실패 상태에서는 설정이 새 값으로 업데이트되지 않고 원래 값이 구현된 상태로 유지됩니다. 이러한 설정을 다시 업데이트를 시도하거나 이전 값으로 되돌릴 수 있습니다.

업데이트된 설정 실패 문제를 해결하려면

- 디렉터리 설정에서 실패한 설정 해결을 선택합니다. 그런 다음, 다음 중 하나를 수행합니다.
 - 설정을 실패 상태 이전의 원래 값으로 되돌리려면 실패한 설정 되돌리기를 선택합니다. 그런 다음 팝업 모드에서 되돌리기를 선택합니다.
 - 디렉터리 설정 업데이트를 재시도하려면 실패한 설정 재시도를 선택합니다. 실패한 업데이트를 다시 시도하기 전에 디렉터리 설정을 추가로 변경하려면 편집 계속을 선택합니다. 실패한 업데이트 검토 및 다시 시도에서 설정 업데이트를 선택합니다.

디렉터리 보안 설정 목록

다음 목록에는 사용 가능한 모든 디렉터리 보안 설정의 유형, 설정 이름, API 이름, 잠재적 값, 설정 설명이 나와 있습니다.

다른 모든 보안 설정을 사용하지 않도록 설정한 경우 TLS 1.2 및 AES 256/256이 기본 디렉터리 보안 설정입니다. 이들은 비활성화할 수 없습니다.

유형	설정 이름	API 이름	잠재적 가치	설정 설명
인증서 기반 인증	인증서 백데이팅 보정	인증서_백데이팅_보정	연: 0~50	인증서를 Active Directory에서 사용자보다 먼저 사용하고 Active Directory에서 인증에 계속 사용할 수 있는 기간을 나타내는 값을 지정합
			월: 0~11	
			일: 0~30	
			시: 0~23	
			분: 0~59	
초: 0~59				

유형	설정 이름	API 이름	잠재적 가치	설정 설명
				<p>니다. 기본값은 10분입니다. 이 값은 1초에서 50년까지 설정할 수 있습니다.</p> <p>이 설정을 구성하려면 강력한 인증서 바인딩 적용에 대한 호환성 유형을 선택해야 합니다.</p> <p>자세한 내용은 Microsoft 지원 설명서에서 KB5014754 - Windows 도메인 컨트롤러의 인증서 기반 인증 변경을 참조 하세요.</p>

유형	설정 이름	API 이름	잠재적 가치	설정 설명
	인증서 강력한 적용	인증서_강력한_적용	호환성, 전체 적용	<p>다음 적용 유형 중 하나를 지정합니다.</p> <ul style="list-style-type: none"> 호환성(기본 값): 인증서가 사용자에게 강력하게 매핑될 수 없는 경우 인증이 허용됩니다. 인증서가 Active Directory의 사용자 계정보다 이전인 경우 인증서 백데이팅 보정도 설정해야 합니다. 그렇지 않으면 인증이 실패합니다. 호환성(기본 값): 인증서가 사용자에게 강력하게 매핑될 수 없는 경우 인증이 허용됩니다. 이 적용 유형을 선택하면 인증서 백데이팅 보정을

유형	설정 이름	API 이름	잠재적 가치	설정 설명
				<p>구성할 수 없습니다.</p> <p>자세한 내용은 Microsoft 지원 설명서에서 KB5014754 - Windows 도메인 컨트롤러의 인증서 기반 인증 변경을 참조 하세요.</p>
보안 채널: 암호	AES 128/128	AES_128_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 AES 128/128 암호화 암호를 활성화 또는 비활성화 합니다.
	DES 56/56	DES_56_56	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 DES 56/56 암호화 암호를 활성화 또는 비활성화 합니다.

유형	설정 이름	API 이름	잠재적 가치	설정 설명
	RC2_40/128	RC2_40_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC2_40/128 암호화 암호를 활성화 또는 비활성화합니다.
	RC2_56/128	RC2_56_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC2_56/128 암호화 암호를 활성화 또는 비활성화합니다.
	RC2_128/128	RC2_128_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC2_128/128 암호화 암호를 활성화 또는 비활성화합니다.

유형	설정 이름	API 이름	잠재적 가치	설정 설명
	RC4 40/128	RC4_40_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC4 40/128 암호화 암호를 활성화 또는 비활성화 합니다.
	RC4 56/128	RC4_56_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC4 56/128 암호화 암호를 활성화 또는 비활성화 합니다.
	RC4 64/128	RC4_64_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC4 64/128 암호화 암호를 활성화 또는 비활성화 합니다.

유형	설정 이름	API 이름	잠재적 가치	설정 설명
보안 채널: 프로 토콜	RC4 128/128	RC4_128_128	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 RC4 128/128 암호화 암호를 활성화 또는 비활성화합니다.
	트리플 DES 168/168	3DES_168_168	Enable, Disable	디렉터리의 도메인 컨트롤러 간 보안 채널 통신을 위해 트리플 DES 168/168 암호화 암호를 활성화 또는 비활성화합니다.
	PCT 1.0	PCT_1_0	Enable, Disable	디렉터리의 도메인 컨트롤러에서 보안 채널 통신(서버 및 클라이언트)을 위한 PCT 1.0 프로토콜을 활성화 또는 비활성화합니다.

유형	설정 이름	API 이름	잠재적 가치	설정 설명
	SSL 2.0	SSL_2_0	Enable, Disable	디렉터리의 도메인 컨트롤러에서 보안 채널 통신(서버 및 클라이언트)을 위한 SSL 2.0 프로토콜을 활성화 또는 비활성화합니다.
	SSL 3.0	SSL_3_0	Enable, Disable	디렉터리의 도메인 컨트롤러에서 보안 채널 통신(서버 및 클라이언트)을 위한 SSL 3.0 프로토콜을 활성화 또는 비활성화합니다.
	TLS 1.0	TLS_1_0	Enable, Disable	디렉터리의 도메인 컨트롤러에서 보안 채널 통신(서버 및 클라이언트)을 위한 TLS 1.0 프로토콜을 활성화 또는 비활성화합니다.

유형	설정 이름	API 이름	잠재적 가치	설정 설명
	TLS 1.1	TLS_1_1	Enable, Disable	디렉터리의 도메인 컨트롤러에서 보안 채널 통신(서버 및 클라이언트)을 위한 TLS 1.1 프로토콜을 활성화 또는 비활성화합니다.

AD용 AWS Private CA 커넥터 설정

AWS 관리형 Microsoft AD를 AWS Private Certificate Authority (CA) 와 통합하여 Active Directory 도메인에 가입된 사용자, 그룹 및 컴퓨터에 대한 인증서를 발급하고 관리할 수 있습니다. AWS Private CA Active Directory용 커넥터를 사용하면 로컬 에이전트 또는 프록시 서버를 배포, 패치 또는 업데이트할 필요 없이 자체 관리형 엔터프라이즈 CA의 완전 관리형 AWS Private CA 그룹인 대체 기능을 사용할 수 있습니다.

Note

Active Directory용 커넥터를 사용하는 AWS 관리형 Microsoft AD 도메인 AWS Private CA 컨트롤러에 대한 서버측 LDAPS 인증서 등록은 지원되지 않습니다. 디렉터리에 대해 서버측 LDAPS를 활성화하려면 관리형 Microsoft AD 디렉터리에 대해 [서버측 LDAPS를 활성화하는 방법을](#) 참조하십시오. AWS

디렉터리 서비스 콘솔, Active Directory용 AWS Private CA 커넥터 콘솔 또는 [CreateTemplateAPI](#) 호출을 통해 디렉터리와의 AWS Private CA 통합을 설정할 수 있습니다. Active Directory용 AWS Private CA 커넥터 콘솔을 통해 사설 CA 통합을 설정하려면 [커넥터 템플릿 만들기를](#) 참조하십시오. AWS Directory Service 콘솔에서 이 통합을 설정하는 방법에 대한 단계는 아래를 참조하십시오.

AD용 AWS Private CA 커넥터를 설정하려면

1. [에](https://console.aws.amazon.com/directoryservicev2/) AWS Management Console 로그인하고 AWS Directory Service 콘솔을 엽니다 <https://console.aws.amazon.com/directoryservicev2/>.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 네트워크 및 보안 탭의 AD용AWS Private CA 커넥터에서 AD용 AWS Private CA 커넥터 설정을 선택합니다. 사설 CA 인증서 생성 대상 페이지가 Active Directory 나타납니다. 콘솔의 단계에 따라 Active Directory 커넥터용 사설 CA를 생성하여 사설 CA에 등록하십시오. 자세한 내용은 [커넥터 생성](#)을 참조하세요.
4. 커넥터를 생성한 후 아래 단계에 따라 커넥터 상태 및 연결된 프라이빗 CA의 상태를 비롯한 세부 정보를 확인하세요.

AD용 AWS Private CA 커넥터를 보려면

1. [에](https://console.aws.amazon.com/directoryservicev2/) AWS Management Console 로그인하고 AWS Directory Service 콘솔을 엽니다 <https://console.aws.amazon.com/directoryservicev2/>.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 네트워크 및 보안의 AD용AWS Private CA 커넥터에서 프라이빗 CA 커넥터 및 연결된 프라이빗 CA를 볼 수 있습니다. 기본적으로 다음 필드가 표시됩니다.
 - a. AWS Private CA 커넥터 ID - 커넥터의 고유 식별자입니다. AWS Private CA 클릭하면 해당 AWS Private CA 커넥터의 세부 정보 페이지로 이동합니다.
 - b. AWS Private CA 제목 — CA의 고유 이름에 대한 정보입니다. 클릭하면 해당 AWS Private CA 세부 정보 페이지로 이동합니다.
 - c. 상태 — AWS Private CA 커넥터 및 커넥터의 상태 확인을 기반으로 AWS Private CA합니다. 두 확인에 모두 통과하면 Active(활성)가 표시됩니다. 확인 중 하나에 실패하면 1/2 checks failed(1/2 확인 실패)가 표시됩니다. 두 확인에 모두 실패하면 Failed(실패)가 표시됩니다. 실패 상태에 대한 자세한 정보는 하이퍼링크에 마우스를 올리면 실패한 확인을 알아 볼 수 있습니다. 콘솔의 지침에 따라 문제를 해결합니다.
 - d. 생성 날짜 - AWS Private CA 커넥터가 생성된 날짜입니다.

자세한 내용은 [커넥터 세부 정보 보기](#)를 참조하세요.

AWS Managed Microsoft AD 모니터링

다음 방법을 사용하여 AWS Managed Microsoft AD 디렉터리를 모니터링할 수 있습니다.

주제

- [디렉터리 상태 이해](#)
- [Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.](#)
- [AWS Managed Microsoft AD 디렉터리 로그 검토](#)
- [로그 전송 활성화](#)
- [성능 지표로 도메인 컨트롤러 모니터링](#)

디렉터리 상태 이해

다음은 디렉터리에 대한 다양한 상태입니다.

활성

디렉터리가 정상적으로 작동하고 있습니다. 디렉터리에서 AWS Directory Service 가 어떤 문제도 탐지하지 않았습니다.

[생성 중]

디렉터리가 현재 생성되는 중입니다. 디렉터리 생성에는 보통 20~45분이 소요되지만, 시스템 로드 에 따라 달라질 수 있습니다.

Deleted

디렉터리가 삭제되었습니다. 디렉터를 위한 모든 리소스들이 해제되었습니다. 디렉터리가 이 상태에 들어오면 복구가 불가능합니다.

[삭제 중]

디렉터리가 현재 삭제되는 중입니다. 디렉터리는 완전히 삭제될 때까지 이 상태를 유지하게 됩니다. 디렉터리가 이 상태에 들어가면 삭제 작업을 취소할 수 없고 디렉터를 복구할 수 없습니다.

실패

디렉터리 생성이 불가능했습니다. 이 디렉터를 삭제하세요. 이 문제가 계속되면 [AWS Support 센터](#)에 문의하세요.

[Impaired]

디렉터리가 성능 저하 상태에서 실행 중입니다. 1개 이상의 문제가 탐지되었고, 모든 디렉터리 작업이 전체 운영 용량에서 실행되지 못할 수 있습니다. 디렉터리가 이 상태가 되는 가능한 이유는 여러 가지입니다. 여기에는 패치 적용 또는 EC2 인스턴스 교체와 같은 정상적인 운영 유지 관리 활동, 도메인 컨트롤러 중 하나에서 애플리케이션에 의한 일시적 핫스팟 발생 또는 사용자가 네트워크를 변경하는 과정에서 잘못 발생한 디렉터리 통신 중단이 포함됩니다. 자세한 내용은 [AWS 관리형 Microsoft AD 문제 해결](#), [문제 해결 AD Connector](#) 또는 [Simple AD 문제 해결](#) 단원을 참조하세요. 일반적인 유지 관리 관련 문제의 경우 40분 이내에 이러한 문제를 AWS 해결합니다. 문제 해결 주제를 검토한 후 디렉터리가 40분 이상 Impaired 상태를 지속할 경우 [AWS Support 센터](#)에 문의하는 것이 좋습니다.

Important

디렉터리가 Impaired 상태일 동안에는 스냅샷을 복원하지 마세요. 장애를 해결하기 위해 스냅샷 복원이 필요한 경우는 드뭅니다. 자세한 정보는 [디렉터리 스냅샷 또는 복구](#)를 참조하세요.

[Requested]

디렉터리를 생성하라는 요청이 현재 보류 중입니다.

RestoreFailed

스냅샷에서 디렉터리 복원이 실패했습니다. 복원 작업을 다시 시도하세요. 이 문제가 계속되면 다른 스냅샷을 시도하거나 [AWS Support Center](#)에 문의하세요.

복원 중

자동 또는 수동 스냅샷에서 디렉터리가 현재 복원 중입니다. 스냅샷의 디렉터리 데이터 크기에 따라 스냅샷에서 디렉터리를 복원하는 데 보통 몇 분이 소요됩니다.

Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.

Amazon Simple Notification Service(Amazon SNS)를 사용하면 디렉터리 상태가 바뀔 때 이메일 또는 텍스트(SMS) 메시지를 수신할 수 있습니다. 디렉터리가 활성 상태에서 [장애 상태로](#) 전환되면 알림을 받게 됩니다. 디렉터리가 Active 상태로 돌아갈 때도 알림을 받게 됩니다.

작동 방식

Amazon SNS는 "주제"를 사용해 메시지를 수집 및 배포합니다. 각 주제마다 1명 이상의 구독자가 해당 주제에 게시된 메시지를 수신합니다. 아래 단계를 사용하여 Amazon SNS 주제에 AWS Directory Service 게시자로 추가할 수 있습니다. 디렉터리 상태의 변화를 AWS Directory Service 감지하면 해당 주제에 메시지를 게시하고, 이 메시지는 주제 구독자에게 전송됩니다.

여러 디렉터를 게시자로서 단일 주제에 연결할 수 있습니다. Amazon SNS에서 이전에 생성했던 주제에 디렉터리 상태 메시지를 추가할 수도 있습니다. 주제를 게시하거나 구독할 수 있는 사람을 세부적으로 제어할 수 있습니다. Amazon SNS에 대한 전체 내용은 [Amazon SNS란 무엇인가요?](#) 단원을 참조하세요.

Note

디렉터리 상태 알림은 AWS 관리형 Microsoft AD의 지역별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)를 참조하세요.

디렉터리에 대해 SNS 메시지를 활성화하는 방법

1. 에 AWS Management Console 로그인하고 [AWS Directory Service 콘솔](#)을 엽니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 SNS 메시징을 활성화할 리전을 선택한 다음 유지 관리 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 유지 관리 탭을 선택합니다.
4. 디렉터리 모니터링 섹션에서 작업을 선택한 후 알림 생성을 선택합니다.
5. 알림 생성 페이지에서 Choose a notification type(알림 유형 선택)을 선택한 후 새 알림 생성을 선택합니다. 또는, 기존 SNS 주제를 이미 가지고 있는 경우 기존 SNS 주제 연결을 선택하여 이 디렉터리에서 해당 주제로 상태 메시지를 전송할 수 있습니다.

Note

새 알림 생성을 선택하지만, 이미 존재하는 SNS 주제에 대해 동일한 주제 이름을 사용하는 경우에는 Amazon SNS가 새 주제를 생성하지 않고 기존 주제에 새 구독 정보를 추가만 합니다.

기존 SNS 주제 연결을 선택하는 경우 디렉터리와 동일한 리전에 있는 SNS 주제만 선택할 수 있습니다.

6. 수신자 유형을 선택하고 수신자 연락처 정보를 입력합니다. SMS에 사용할 전화 번호를 입력할 때는 숫자만 사용합니다. 대시, 공백, 괄호를 사용하지 마세요.
7. (선택 사항) 주제 이름과 SNS 표시 이름을 제공합니다. 표시 이름은 이 주제에서 모든 SMS 메시지에 포함시킬 짧은 이름(최대 10자)입니다. SMS 옵션을 사용할 때 표시 이름이 필요합니다.

Note

[DirectoryServiceFullAccess](#) 관리형 정책만 적용되는 IAM 사용자 또는 역할을 사용하여 로그인한 경우 주제 이름은 "DirectoryMonitoring" 로 시작해야 합니다. 사용자가 주제 이름을 추가로 정의하고 싶으면 SNS에 대한 추가 권한이 필요합니다.

8. 생성을 선택합니다.

[추가 이메일 주소, Amazon SQS 대기열 AWS Lambda등 추가 SNS 구독자를 지정하려는 경우 Amazon SNS 콘솔에서 지정할 수 있습니다.](#)

주제에서 디렉터리 상태 메시지를 삭제하는 방법

1. [예 AWS Management Console 로그인하고 콘솔을 엽니다.AWS Directory Service](#)
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 상태 메시지를 제거할 리전을 선택한 다음 유지 관리 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 유지 관리 탭을 선택합니다.
4. 디렉터리 모니터링 섹션의 목록에서 SNS 주제 이름을 선택하고 작업을 선택한 후 제거를 선택합니다.
5. 제거를 선택합니다.

이렇게 하면 선택한 SNS 주제에 대한 게시자 역할을 하는 디렉터리가 삭제됩니다. 전체 주제를 삭제하려면 [Amazon SNS 콘솔에서](#) 삭제할 수 있습니다.

Note

디렉터리가 해당 주제에 상태 메시지를 전송하고 있지 않아야만 SNS 콘솔을 이용해 Amazon SNS 주제를 삭제할 수 있습니다.

SNS 콘솔을 사용해 Amazon SNS 주제를 삭제하면 이러한 변경이 Directory Services 콘솔 내에 즉각 반영되지 않습니다. 디렉터리의 모니터링 탭에서 주제를 찾을 수 없음을 알리는 상태 업데이트를 확인한 경우에는 다음 번에 디렉터리가 삭제된 주제에 알림을 게시할 때만 알림을 받게 됩니다.

따라서 중요한 디렉터리 상태 메시지를 놓치지 않으려면 메시지를 받는 주제를 삭제하기 전에 디렉터리를 다른 Amazon SNS 주제와 연결하십시오. AWS Directory Service

AWS Managed Microsoft AD 디렉터리 로그 검토

AWS Managed Microsoft AD 도메인 컨트롤러 인스턴스의 보안 로그는 1년간 보관됩니다. 도메인 컨트롤러 로그가 실시간에 가까운 속도로 Amazon CloudWatch Logs로 전송되도록 AWS Managed Microsoft AD 디렉터리를 구성할 수도 있습니다. 자세한 내용은 [로그 전송 활성화](#) 섹션을 참조하세요.

AWS는 규정 준수를 위해 다음 이벤트를 기록합니다.

모니터링 범주	정책 설정	감사 상태
계정 로그인	자격 증명 확인 감사	성공, 실패
	기타 계정 로그인 이벤트 감사	성공, 실패
계정 관리	컴퓨터 계정 관리 감사	성공, 실패
	기타 계정 관리 이벤트 감사	성공, 실패
	보안 그룹 관리 감사	성공, 실패
세부 추적	사용자 계정 관리 감사	성공, 실패
	DPAPI 활동 감사	성공, 실패
	PNP 활동 감사	성공
	프로세스 생성 감사	성공, 실패

모니터링 범주	정책 설정	감사 상태
DS 액세스	디렉터리 서비스 액세스 감사	성공, 실패
	디렉터리 서비스 변경 감사	성공, 실패
로그인/로그아웃	계정 잠금 감사	성공, 실패
	로그아웃 감사	성공
	로그인 감사	성공, 실패
객체 액세스	기타 로그온/로그오프 이벤트 감사	성공, 실패
	특별 로그인 감사	성공, 실패
	기타 객체 액세스 이벤트 감사	성공, 실패
정책 변경	이동식 스토리지 감사	성공, 실패
	중앙 액세스 정책 스테이징 감사	성공, 실패
	정책 변경 감사	성공, 실패
권한 사용	인증 정책 변경 감사	성공, 실패
	권한 부여 정책 변경 감사	성공, 실패
	MPSSVC 규칙 수준 정책 변경 감사	성공
시스템	기타 정책 변경 이벤트 감사	결함
	중요 권한 사용 감사	성공, 실패
시스템	IPsec 드라이버 감사	성공, 실패
	기타 시스템 이벤트 감사	성공, 실패
	보안 상태 변경 감사	성공, 실패

모니터링 범주	정책 설정	감사 상태
	보안 시스템 확장 감사	성공, 실패
	시스템 무결성 감사	성공, 실패

로그 전송 활성화

AWS Directory Service 콘솔이나 API를 이용해 도메인 컨트롤러 보안 이벤트 로그를 Amazon CloudWatch Logs에 전송할 수 있습니다. 이는 디렉터리의 보안 이벤트에 대한 투명성을 제공하여 보안 모니터링, 감사 및 로그 보존 정책 요구 사항을 충족하는 데 도움이 됩니다.

CloudWatch Logs를 사용하면 이러한 이벤트를 다른 AWS 계정, AWS 서비스, 타사 애플리케이션으로 전달할 수 있습니다. 따라서 비정상적인 활동을 거의 실시간으로 탐지하고 선제적으로 대응하도록 중앙 집중식으로 알림을 모니터링 및 구성하기가 좀 더 쉽습니다.

활성화된 후, CloudWatch Logs 콘솔을 사용해 서비스를 활성화할 때 지정한 로그 그룹에서 데이터를 가져올 수 있습니다. 이 로그 그룹에는 도메인 컨트롤러의 보안 로그가 포함됩니다.

이 그룹에 대한 자세한 정보 및 해당 데이터를 읽는 방법은 Amazon CloudWatch Logs 사용 설명서의 [로그 그룹 및 로그 스트림 작업](#)을 참조하세요.

Note

로그 전달은 AWS Managed Microsoft AD의 리전별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 내용은 [글로벌 기능과 리전별 기능 비교](#) 섹션을 참조하세요.

로그 전송을 활성화

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 공유하려는 AWS Managed Microsoft AD 디렉터리의 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 로그 전달을 활성화할 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.

4. 로그 전송 섹션에서 활성화를 선택합니다.
5. CloudWatch로 로그 전송 활성화 대화 상자에서 다음 옵션 중 하나를 선택합니다.
 - a. 새 CloudWatch 로그 그룹 생성을 선택하고, CloudWatch 로그 그룹 이름에서 CloudWatch Logs에서 참조할 수 있는 이름을 지정합니다.
 - b. Choose an existing CloudWatch log group(기존 CloudWatch 로그 그룹 선택)을 선택하고, 기존 CloudWatch 로그 그룹 아래의 메뉴에서 로그 그룹을 선택합니다.
6. 요금 정보와 링크를 검토한 후 활성화를 선택합니다.

로그 전송 비활성화

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 공유하려는 AWS Managed Microsoft AD 디렉터리의 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 로그 전달을 비활성화할 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 로그 전송 섹션에서 비활성화를 선택합니다.
5. Disable log forwarding(로그 전송 비활성화) 대화창의 정보를 읽은 후 비활성화를 선택합니다.

CLI를 사용하여 로그 전송 활성화

`ds create-log-subscription` 명령을 사용하기 전에 Amazon CloudWatch 로그 그룹을 생성한 후 해당 그룹에 필요한 권한을 부여하는 IAM 리소스 정책을 생성해야 합니다. CLI를 사용하여 로그 전송을 활성화하려면 아래 단계를 모두 완료하세요.

1단계: CloudWatch Logs의 로그 그룹 생성

도메인 컨트롤러에서 보안 로그를 수신하는 데 사용할 로그 그룹을 생성합니다. 필수는 아니지만, 이름 앞에 `/aws/directoryservice/`를 추가하는 것이 좋습니다. 예:

CLI 명령 예

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-9876543210'
```


POWERSHELL 명령 예

```
New-CWLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

CloudWatch Logs 그룹을 생성하는 방법에 대한 지침은 Amazon CloudWatch Logs 사용 설명서의 [CloudWatch Logs에서 로그 그룹 생성](#)을 참조하세요.

2단계: IAM에서 CloudWatch Logs 리소스 정책 생성

1단계에서 생성한 새 로그 그룹에 로그를 추가할 AWS Directory Service 권한을 부여하는 CloudWatch Logs 리소스 정책을 생성합니다. 로그 그룹에 정확한 ARN을 지정하여 AWS Directory Service의 액세스를 다른 로그 그룹으로 제한하거나, 와일드카드를 사용하여 모든 로그 그룹을 포함할 수 있습니다. 다음 샘플 정책에서는 와일드카드 메서드를 사용하여 디렉터리가 있는 AWS 계정에 대해 /aws/directoryservice/로 시작하는 모든 로그 그룹을 포함하도록 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/directoryservice/*"
    }
  ]
}
```

CLI에서 실행해야 하므로 이 정책을 로컬 워크스테이션에 텍스트 파일(예: DSPolicy.json)로 저장해야 합니다. 예:

CLI 명령 예

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document file://DSPolicy.json
```

POWERSHELL 명령 예

```
$PolicyDocument = Get-Content .\DSPolicy.json -Raw
```

```
Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument  
$PolicyDocument
```

3단계: AWS Directory Service 로그 구독 생성

이 마지막 단계에서는 로그 구독을 생성하여 로그 전송 활성화를 계속 진행할 수 있습니다. 예:

CLI 명령 예

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-  
name '/aws/directoryservice/d-9876543210'
```

POWERSHELL 명령 예

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/  
directoryservice/d-9876543210'
```

성능 지표로 도메인 컨트롤러 모니터링

AWS Directory Service Amazon과 CloudWatch 통합하여 각 도메인 컨트롤러에 대한 중요한 성능 지표를 제공하는 데 도움이 됩니다. Active Directory. 즉, CPU 및 메모리 사용률과 같은 도메인 컨트롤러 성능 카운터를 모니터링할 수 있습니다. 또한 사용률이 높은 기간에 대응하도록 경보를 구성하고 자동화된 작업을 시작할 수 있습니다. 예를 들어 도메인 컨트롤러 CPU 사용률이 70%를 초과하는 경우 경보를 구성하고 이러한 상황이 발생할 때 알려주는 SNS 주제를 만들 수 있습니다. 이 SNS 주제를 사용하여 AWS Lambda 기능 등의 자동화를 시작하여 도메인 컨트롤러의 수를 늘릴 수 있습니다. Active Directory

도메인 컨트롤러 모니터링에 대한 자세한 내용은 [CloudWatch 메트릭과 함께 도메인 컨트롤러를 추가할 시기를 결정하세요](#)를 참조하세요.

Amazon과 관련된 수수료가 CloudWatch 있습니다. 자세한 내용은 [CloudWatch 청구 및 비용을](#) 참조하십시오.

Important

캐나다 서부 (캘거리) 지역에서는 도메인 컨트롤러 성능 메트릭을 사용할 수 없습니다.
CloudWatch

도메인 컨트롤러 성능 메트릭은 다음에서 찾을 수 있습니다. CloudWatch

Amazon CloudWatch 콘솔에서는 해당 서비스의 지표가 먼저 서비스의 네임스페이스별로 그룹화됩니다. 해당 네임스페이스에 종속되는 지표 필터를 추가할 수 있습니다. 다음 절차를 사용하여 관리형 AWS Microsoft AD 도메인 컨트롤러 메트릭을 설정하는 데 필요한 올바른 네임스페이스와 하위 메트릭을 찾을 수 있습니다. CloudWatch

콘솔에서 도메인 컨트롤러 메트릭을 찾으려면 CloudWatch

1. <https://console.aws.amazon.com/cloudwatch/> 에서 AWS Management Console 로그인하고 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표(Metrics)를 선택합니다.
3. 지표 목록에서 디렉터리 서비스 네임스페이스를 선택한 다음, 목록에서, AWS Managed Microsoft AD 지표를 선택합니다.

CloudWatch 콘솔을 사용하여 도메인 컨트롤러 메트릭을 설정하는 [방법에 대한 지침은 AWS 보안 블로그의 사용자 지표를 기반으로 AWS Managed Microsoft AD 조정을 자동화하는 방법을 참조하십시오](#).

CloudWatch 메트릭과 함께 도메인 컨트롤러를 추가할 시기를 결정하세요.

모든 도메인 컨트롤러의 부하 분산은 도메인 컨트롤러의 복원력과 성능에 중요합니다. Active Directory AWS Managed Microsoft AD에서 도메인 컨트롤러의 성능을 최적화하려면 먼저 중요한 메트릭을 CloudWatch 모니터링하여 기준을 형성하는 것이 좋습니다. 이 프로세스에서는 시간 경과에 Active Directory 따른 사용률을 분석하여 평균 및 최대 Active Directory 사용률을 파악합니다. 기준을 결정한 후에는 이러한 지표를 정기적으로 모니터링하여 도메인 컨트롤러를 추가할 시기를 결정할 수 있습니다.

다음 지표는 정기적으로 모니터링하는 것이 중요합니다. 에서 CloudWatch 사용 가능한 도메인 컨트롤러 메트릭의 전체 목록은 [AWS 관리형 Microsoft AD 성능 카운터](#).

- 다음과 같은 도메인 컨트롤러별 지표:
 - 처리자
 - 메모리
 - 논리적 디스크
 - 네트워크 인터페이스
- AWS 관리되는 Microsoft AD 디렉터리별 메트릭은 다음과 같습니다.

- LDAP 검색
- 바인드
- DNS 쿼리
- 디렉터리 읽기
- 디렉터리 쓰기

CloudWatch 콘솔을 사용하여 도메인 컨트롤러 메트릭을 설정하는 [방법에 대한 지침은 AWS 보안 블로그의 사용률 지표를 기반으로 AWS Managed Microsoft AD 조정을 자동화하는 방법을 참조](#) 하십시오. 의 CloudWatch 지표에 대한 일반 정보는 [Amazon 사용 CloudWatch 설명서의 Amazon CloudWatch 지표 사용](#)을 참조하십시오.

도메인 컨트롤러 계획에 대한 일반적인 내용은 Microsoft 웹 사이트의 [Active Directory도메인 서비스 용량 계획](#)을 참조하십시오.

AWS 관리형 Microsoft AD 성능 카운터

다음 표에는 AWS Managed Microsoft AD의 도메인 컨트롤러 및 디렉터리 성능을 CloudWatch 추적하기 위해 Amazon에서 사용할 수 있는 모든 성능 카운터가 나와 있습니다.

지표 범주	지표 이름
데이터베이스 => 인스턴스(NTDSA)	데이터베이스 캐시 적중률(%)
	I/O 데이터베이스 읽기 평균 대기 시간
	I/O 데이터베이스 읽기/초
	I/O 로그 쓰기 평균 대기 시간
DirectoryServices (NTDS)	LDAP 바인딩 시간
	DRA에서 보류 중인 복제 작업
	DRA에서 보류 중인 복제 동기화
DNS	재귀 쿼리/초
	재귀 쿼리 실패/초

지표 범주	지표 이름
	TCP 쿼리 수신/초
	총 쿼리 수신/초
	발송된 총 응답/초
	수신된 UDP 쿼리/초
LogicalDisk	평균 디스크 대기열 길이
	% 여유 공간
메모리	% Committed Bytes in Use
	장기 평균 대기 캐시 수명(초)
네트워크 인터페이스	발송된 바이트/초
	Bytes Received/sec
	현재 대역폭
NTDS	ATQ 예상 대기열 지연
	ATQ 요청 지연 시간
	DS 디렉터리 읽기/초
	DS 디렉터리 검색/초
	DS 디렉터리 쓰기/초
	LDAP 클라이언트 세션
	LDAP 검색/초
	LDAP 바인드 성공/초
처리자	% 프로세서 시간

지표 범주	지표 이름
보안 시스템 전체 통계	Kerberos 인증
	IAM 인증

다중 리전 복제

다중 지역 복제를 사용하면 관리형 AWS Microsoft AD 디렉터리 데이터를 여러 곳에 자동으로 복제할 수 있습니다. AWS 리전이 복제를 통해 지리적으로 분산된 위치에 있는 사용자와 응용 프로그램의 성능을 개선할 수 있습니다. AWS 관리형 Microsoft AD는 네이티브 Active Directory 복제를 사용하여 디렉터리의 데이터를 새 지역에 안전하게 복제합니다.

다중 지역 복제는 AWS 관리형 Microsoft AD의 엔터프라이즈 에디션에서만 지원됩니다.

AWS Managed Microsoft AD를 사용할 수 있는 대부분의 리전에서 자동 다중 리전 복제를 사용할 수 있습니다.

Important

다음과 같은 옵트인 지역에서는 다중 지역 복제를 사용할 수 없습니다.

- 아프리카(케이프타운) af-south-1
- 아시아 태평양(홍콩) ap-east-1
- 아시아 태평양(하이데라바드) ap-south-2
- 아시아 태평양(자카르타) ap-southeast-3
- 아시아 태평양(멜버른) ap-southeast-4
- 캐나다 서부 (캘거리) ca-west-1
- 유럽(밀라노) eu-south-1
- 유럽(스페인) 리전(eu-south-2)
- 유럽(취리히) eu-central-2
- 이스라엘 (텔아비브) il-센트럴-1
- 중동(바레인) me-south-1
- 중동(UAE) me-central-1

옵트인 지역 및 활성화 방법에 대한 자세한 내용은 가이드에서 사용할 수 있는 [AWS 리전 계정 지정](#)을 참조하십시오. [AWS Account Management](#)

이점

AWS 관리형 Microsoft AD의 다중 지역 복제를 사용하면 Active Directory 인식 애플리케이션은 고성능을 위해 로컬 디렉터리를 사용하고 복원성을 위해 다중 지역 기능을 사용합니다. SQL Server Always On과 같은 액티브 디렉터리 인식 애플리케이션뿐만 아니라 SQL Server용 Amazon RDS SharePoint 및 Windows File Server용 FSx와 같은 AWS 서비스와 함께 다중 지역 복제를 사용할 수 있습니다. 다음은 다중 리전 복제로 얻을 수 있는 추가 이점입니다.

- 이를 통해 단일 AWS 관리형 Microsoft AD 인스턴스를 전 세계에 신속하게 배포할 수 있으며 글로벌 Active Directory 인프라를 자체 관리하는 번거로움을 없애줍니다.
- 이를 통해 여러 AWS 지역에서 Windows 및 Linux 워크로드를 더 쉽고 비용 효율적으로 배포하고 관리할 수 있습니다. 자동화된 다중 지역 복제를 통해 글로벌 Active Directory 인식 애플리케이션에서 최적의 성능을 발휘할 수 있습니다. Windows 또는 Linux 인스턴스에 배포된 모든 애플리케이션은 해당 지역의 로컬에서 AWS Managed Microsoft AD를 사용하므로 가능한 가장 가까운 지역의 사용자 요청에 응답할 수 있습니다.
- 이는 다중 리전 복원력을 제공합니다. 가용성이 높은 AWS 관리형 인프라에 AWS 배포되는 관리형 Microsoft AD는 모든 지역에서 기본 Active Directory 인프라의 자동 소프트웨어 업데이트, 모니터링, 복구 및 보안을 처리합니다. 따라서 애플리케이션 구축에 집중할 수 있습니다.

주제

- [글로벌 기능과 리전별 기능 비교](#)
- [기본 리전과 추가 리전의 비교](#)
- [다중 리전 복제 작동 방식](#)
- [복제된 리전 추가](#)
- [복제된 리전 삭제](#)

글로벌 기능과 리전별 기능 비교

다중 AWS 지역 복제를 사용하여 디렉터리에 지역을 추가하면 모든 기능의 범위가 AWS Directory Service 향상되어 지역을 인식할 수 있습니다. AWS Directory Service 콘솔에서 디렉터리의 ID를 선택

하면 나타나는 세부 정보 페이지의 다양한 탭에 이러한 기능이 나열되어 있습니다. 즉, 콘솔의 다중 리전 복제 섹션에서 선택한 리전을 기반으로 모든 기능을 활성화, 구성, 관리할 수 있습니다. 각 리전의 기능에 대한 변경 사항은 전 세계적으로 또는 리전별로 적용됩니다.

다중 지역 복제는 AWS 관리형 Microsoft AD의 엔터프라이즈 에디션에서만 지원됩니다.

글로벌 기능

[기본 리전](#)을 선택한 상태에서 글로벌 기능을 변경하면 모든 리전에 걸쳐 적용됩니다.

디렉터리 세부 정보 페이지에서 전 세계적으로 사용되는 기능을 식별할 수 있는데, 그 이유는 옆에 복제된 모든 리전에 적용됨이 표시되기 때문입니다. 또는 목록에서 기본 리전이 아닌 다른 리전을 선택한 경우 해당 기능에는 기본 리전에서 상속됨이 표시되므로 전체적으로 사용되는 기능을 식별할 수 있습니다.

리전별 기능

[추가 리전](#)에서 기능에 적용한 모든 변경 사항은 해당 리전에만 적용됩니다.

디렉터리 세부 정보 페이지에서 리전별 기능을 식별할 수 있습니다. 그 이유는 해당 기능 옆에 복제된 모든 리전에 적용됨 또는 기본 리전에서 상속됨이 표시되지 않기 때문입니다.

기본 리전과 추가 리전의 비교

다중 지역 복제의 경우 AWS Managed Microsoft AD는 다음 두 가지 유형의 지역을 사용하여 디렉터리 전체에 글로벌 또는 지역 기능을 적용하는 방법을 구분합니다.

기본 리전

디렉터리를 처음 생성한 초기 리전을 기본 리전이라고 합니다. Active Directory 신뢰 관계를 만들고 기본 리전에서 AD 스키마를 업데이트하는 등의 글로벌 디렉터리 수준 작업만 수행할 수 있습니다.

기본 리전은 항상 다중 리전 복제 섹션의 목록 상단에 표시되는 첫 번째 리전으로 식별될 수 있으며, - Primary(기본)으로 끝납니다. 예: 미국 동부(버지니아 북부) - Primary.

기본 리전을 선택한 상태에서 [글로벌 기능](#)에 수행한 변경 사항은 모든 리전에 적용됩니다.

기본 리전을 선택한 경우에만 리전을 추가할 수 있습니다. 자세한 설명은 [복제된 리전 추가](#) 섹션을 참조하세요.

추가 리전

디렉터리에 추가한 모든 리전을 추가 리전이라고 합니다.

일부 기능은 모든 리전에 대해 전 세계적으로 관리할 수 있지만, 다른 기능은 리전별로 개별적으로 관리됩니다. 추가 리전(기본 리전이 아닌 리전)의 기능을 관리하려면 먼저 디렉터리 세부 정보 페이지의 다중 리전 복제 섹션에 있는 목록에서 추가 리전을 선택해야 합니다. 그런 다음 기능 관리를 진행할 수 있습니다.

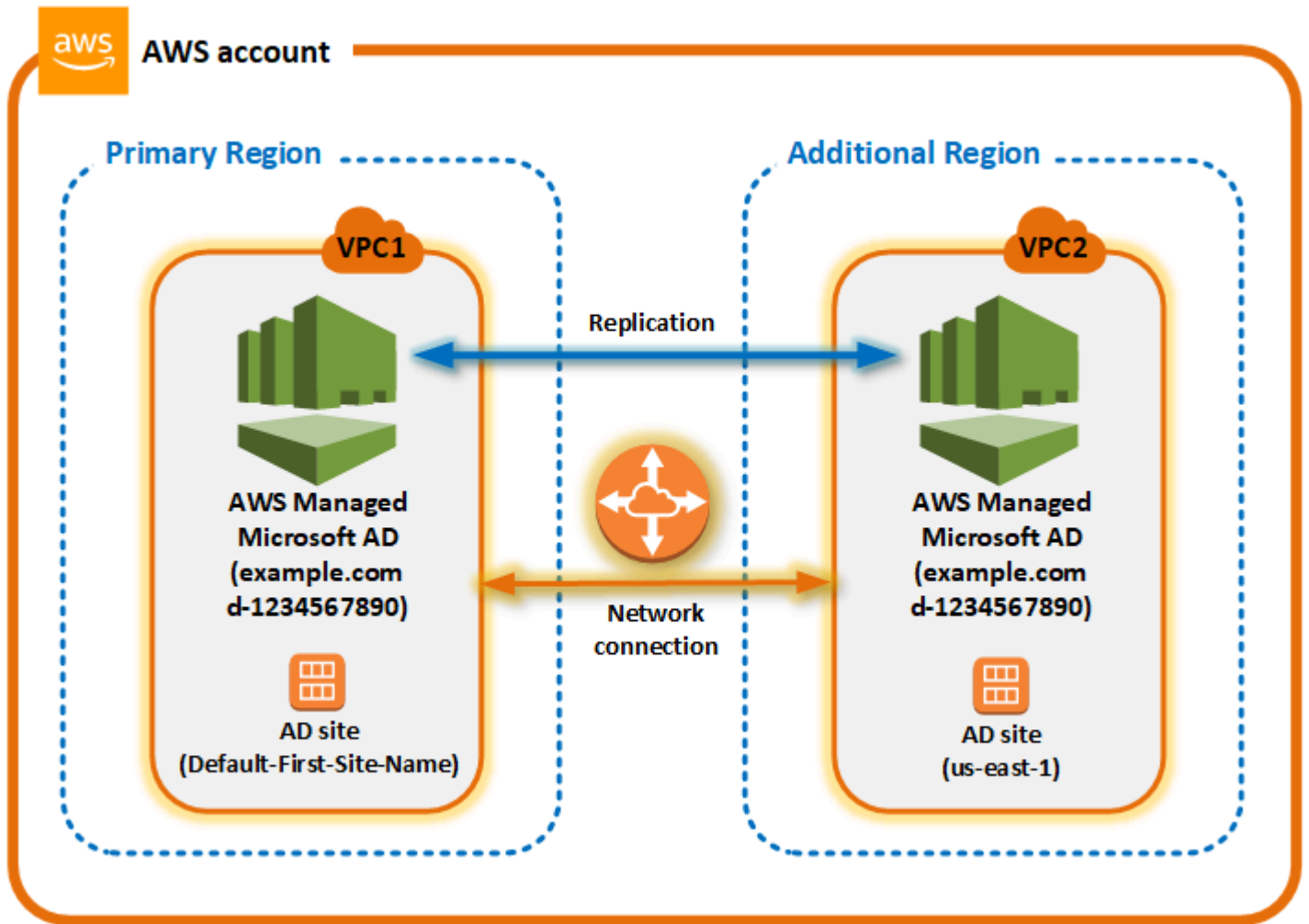
추가 리전을 선택한 상태에서 [리전별 기능](#)에 수행한 변경 사항은 해당 리전에만 적용됩니다.

다중 리전 복제 작동 방식

다중 지역 복제 기능을 사용하면 AWS 관리형 Microsoft AD를 사용하면 글로벌 Active Directory 인프라를 관리해야 하는 차별화되지 않은 번거로움을 없앨 수 있습니다. 구성된 경우 사용자, 그룹, 그룹 정책 및 스키마를 포함한 모든 고객 디렉터리 데이터를 여러 지역에 AWS 복제합니다. AWS

새 리전이 추가되면 그림에 나와 있는 것과 같이 다음 작업이 자동으로 수행됩니다.

- AWS 관리형 Microsoft AD는 선택한 VPC에 두 개의 도메인 컨트롤러를 생성하여 동일한 계정의 새 지역에 배포합니다. AWS 디렉터리 식별자(directory_id)는 모든 리전에서 동일하게 유지됩니다. 원한다면 나중에 도메인 컨트롤러를 추가할 수 있습니다.
- AWS 관리형 Microsoft AD는 기본 지역과 새 지역 간의 네트워크 연결을 구성합니다.
- AWS 관리형 Microsoft AD는 새 액티브 디렉터리 사이트를 만들고 해당 사이트에 해당 지역과 동일한 이름 (예: us-east-1) 을 지정합니다. 나중에 Active Directory 사이트 및 서비스 도구를 사용하여 이 이름을 바꿀 수도 있습니다.
- AWS 관리형 Microsoft AD는 사용자, 그룹, 그룹 정책, Active Directory 트러스트, 조직 단위 및 Active Directory 스키마를 포함하여 모든 Active Directory 개체 및 구성을 새 지역에 복제합니다. Active Directory 사이트 링크는 [변경 알림](#)을 사용하도록 구성되어 있습니다. 사이트 간 변경 알림을 사용하도록 설정하면 긴급 복제가 필요한 변경 내용을 포함하여 변경 내용이 소스 사이트 내에서 전파되는 빈도와 동일한 빈도로 원격 사이트에 전파됩니다.
- 이 지역을 처음 추가한 경우 AWS 관리형 Microsoft AD는 모든 기능을 다중 지역을 인식합니다. 자세한 설명은 [글로벌 기능과 리전별 기능 비교](#) 섹션을 참조하세요.



Active Directory 사이트

다중 지역 복제는 여러 Active Directory 사이트 (지역당 Active Directory 사이트 하나) 를 지원합니다. 새 리전이 추가되면 해당 리전은 리전(예: us-east-1)으로 이름이 동일하게 지정됩니다. 나중에 Active Directory 사이트 및 서비스를 사용하여 이 이름을 바꿀 수도 있습니다.

AWS 서비스

AWS SQL Server용 Amazon RDS 및 Amazon FSx와 같은 서비스는 글로벌 디렉터리의 로컬 인스턴스에 연결됩니다. 이를 통해 사용자는 어느 지역에서든 Amazon RDS for SQL Server와 같은 AWS 서비스뿐만 아니라 실행되는 Active Directory 인식 애플리케이션에 한 번 로그인할 수 있습니다. AWS 이렇게 하려면 관리형 Microsoft AD와 신뢰를 맺고 있는 사용자에게 AWS 관리형 Microsoft AD 또는 온-프레미스 Active Directory의 자격 증명이 필요합니다. AWS

다중 지역 복제 기능과 함께 다음 AWS 서비스를 사용할 수 있습니다.

- Amazon EC2

- FSx for Windows File Server
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora MySQL
- Amazon Aurora for PostgreSQL

장애 조치

한 지역의 모든 도메인 컨트롤러가 다운되는 경우 AWS Managed Microsoft AD는 도메인 컨트롤러를 복구하고 디렉터리 데이터를 자동으로 복제합니다. 한편 다른 리전의 도메인 컨트롤러는 계속 가동됩니다.

복제된 리전 추가

이 [다중 리전 복제](#) 기능을 사용하여 지역을 추가하면 AWS 관리형 Microsoft AD는 선택한 AWS 지역에 Amazon VPC (가상 사설 클라우드)와 서브넷이라는 두 개의 도메인 컨트롤러를 생성합니다. AWS 또한 관리형 Microsoft AD는 Windows 워크로드를 새 지역의 디렉터리에 연결할 수 있도록 관련 보안 그룹을 생성합니다. 또한 디렉터리가 이미 배포된 계정과 동일한 AWS 계정을 사용하여 이러한 리소스를 생성합니다. 이렇게 하려면 리전을 선택하고, VPC를 지정하며, 새 리전에 대한 구성을 제공하면 됩니다.

다중 지역 복제는 AWS 관리형 Microsoft AD의 엔터프라이즈 에디션에서만 지원됩니다.

필수 조건

새 복제 리전 추가 단계를 진행하기 전에 먼저 다음 사전 조건 작업을 검토하는 것이 좋습니다.

- 디렉터리를 복제하려는 새 지역에 필요한 AWS Identity and Access Management (IAM) 권한, Amazon VPC 설정 및 서브넷 설정이 있는지 확인하십시오.
- 기존 온-프레미스 Active Directory 자격 증명을 사용하여 에서 AWS Active Directory 인식 워크로드에 액세스하고 관리하려면 관리형 AWS Microsoft AD와 온-프레미스 AD 인프라 간에 Active Directory 트러스트를 만들어야 합니다. 신뢰에 대한 자세한 내용은 [기존 액티브 디렉터리 인프라에 연결](#) 단원을 참조하세요.

- 온프레미스 Active Directory 간에 기존 신뢰 관계가 있고 복제된 지역을 추가하려는 경우, 디렉터리를 복제하려는 새 지역에 필요한 Amazon VPC 및 서브넷 설정이 있는지 확인해야 합니다.

리전 추가

다음 절차를 사용하여 AWS 관리형 Microsoft AD 디렉터리에 복제된 지역을 추가할 수 있습니다.

복제된 리전을 추가하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지의 다중 리전 복제에서 기본 리전을 목록에서 선택한 다음 리전 추가를 선택합니다.

Note

기본 리전을 선택한 경우에만 리전을 추가할 수 있습니다. 자세한 설명은 [기본 리전](#) 섹션을 참조하세요.

4. 리전 추가 페이지의 리전에서 추가하려는 리전을 목록에서 선택합니다.
5. VPC에서 이 리전에 사용할 VPC를 선택합니다.

Note

이 VPC에는 이 디렉터리에서 사용하는 VPC와 중복되는 Classless Inter-Domain Routing(CIDR)이 다른 리전에 없어야 합니다.

6. Subnets에서 이 리전에 사용할 서브넷을 선택합니다.
7. Pricing(요금)에서 해당 정보를 검토한 다음 Add(추가)를 선택합니다.
8. AWS 관리형 Microsoft AD에서 도메인 컨트롤러 배포 프로세스를 완료하면 해당 지역에 활성 상태가 표시됩니다. 이제 필요에 따라 이 리전을 업데이트할 수 있습니다.

다음 단계

새 리전을 추가한 후에는 다음 후속 단계를 수행하는 것을 고려해야 합니다.

- 필요에 따라 새 리전에 추가 도메인 컨트롤러(최대 20개)를 배포합니다. 새 리전을 추가할 때 기본적으로 도메인 컨트롤러의 수는 2개이며, 이는 내결함성 및고가용성을 위해 필요한 최소 개수입니다. 자세한 설명은 [추가 도메인 컨트롤러 추가 또는 제거](#) 섹션을 참조하세요.
- 지역별로 더 많은 AWS 계정과 디렉터리를 공유하세요. 디렉터리 공유 구성은 기본 리전으로부터 자동으로 복제되지 않습니다. 자세한 설명은 [디렉터리 공유](#) 섹션을 참조하세요.
- 새 지역의 Amazon CloudWatch Logs를 사용하여 디렉터리의 보안 로그를 검색하려면 로그 전달을 활성화하십시오. 로그 전달을 활성화할 때는 디렉터리를 복제했던 각 리전의 로그 그룹 이름을 제공해야 합니다. 자세한 설명은 [로그 전송 활성화](#) 섹션을 참조하세요.
- 새 리전에 대한 Amazon Simple Notification Service(Amazon SNS) 모니터링을 활성화하여 리전별로 디렉터리 상태를 추적할 수 있습니다. 자세한 설명은 [Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.](#) 섹션을 참조하세요.

복제된 리전 삭제

AWS 관리형 Microsoft AD 디렉터리의 지역을 삭제하려면 다음 절차를 사용하십시오. 리전을 삭제하기 전에 다음 중 하나가 없는지 확인합니다.

- 승인된 애플리케이션이 연결되어 있음.
- 이와 관련된 공유 디렉터리.

복제된 리전을 삭제하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. 탐색 모음에서 Regions(리전) 선택기를 선택한 다음 디렉터리가 저장된 리전을 선택합니다.
3. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
4. 디렉터리 세부정보 페이지의 다중 리전 복제에서 리전 삭제를 선택합니다.
5. 리전 삭제 대화 상자에서 해당 정보를 검토한 다음 리전 이름을 입력하여 확인합니다. 그런 다음 삭제를 선택합니다.

Note

리전을 삭제하는 동안에는 리전을 업데이트할 수 없습니다.

디렉터리 공유

AWS Managed Microsoft AD는 여러 AWS 계정에서 원활하게 디렉터리를 공유할 수 있도록 AWS Organizations과 통합되어 있습니다. 같은 조직 내부의 신뢰할 수 있는 다른 AWS 계정과 디렉터리 1개를 공유하거나, 조직 외부의 다른 AWS 계정과 해당 디렉터리를 공유할 수 있습니다. 또한 AWS 계정이 조직에 속하지 않은 경우에도 디렉터리를 공유할 수 있습니다.

Note

AWS 디렉터리 공유에는 추가 요금이 부과됩니다. 자세한 내용은 AWS Directory Service 웹사이트의 [요금](#) 페이지를 참조하세요.

디렉터리 공유를 이용하면 AWS Managed Microsoft AD를 여러 계정 및 VPC에서 Amazon EC2와 통합하는 보다 비용 효율적인 방법으로 사용할 수 있습니다. [AWS Managed Microsoft AD가 제공되는 모든 AWS 리전](#)에서 디렉터리 공유를 사용할 수 있습니다.

Note

AWS 중국(닝샤) 리전의 경우, [AWS System Manager\(SSM\)](#)을 이용해 원활하게 Amazon EC2 인스턴스에 조인할 수 있는 경우에만 이 기능을 사용할 수 있습니다.

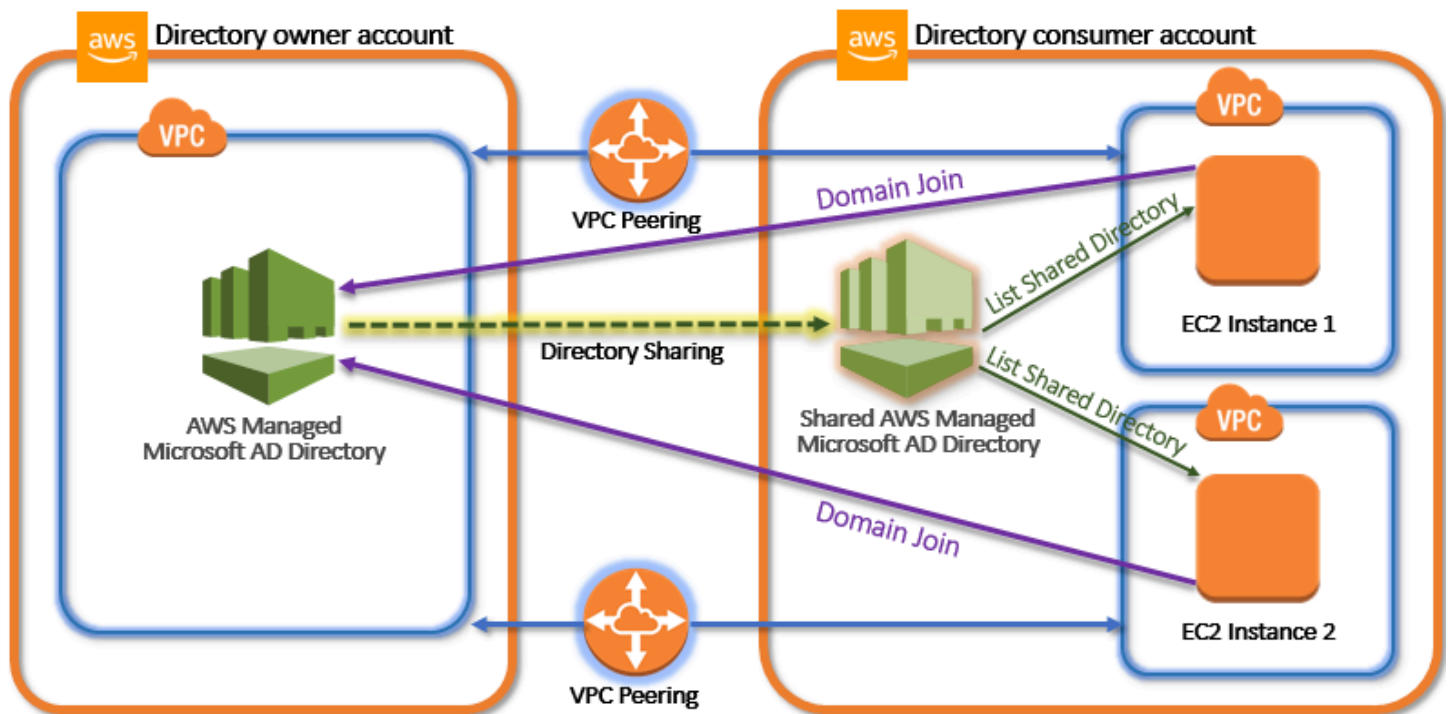
디렉터리 공유 및 AWS 계정 경계를 넘어 내 AWS Managed Microsoft AD 디렉터리의 도달 범위를 확대하는 방법에 대한 자세한 내용은 다음 주제를 참조하세요.

주제

- [디렉터리 공유의 주요 개념](#)
- [자습서: 원활한 EC2 도메인 가입을 위한 AWS 관리형 Microsoft AD 디렉터리 공유](#)
- [디렉터리 공유 해제](#)

디렉터리 공유의 주요 개념

다음 주요 개념을 익히면 디렉터리 공유 기능을 최대한 활용할 수 있습니다.



디렉터리 소유자 계정

디렉터리 소유자는 공유한 디렉터리 관계에서 시작 디렉터를 소유한 AWS 계정 소유자입니다. 이 계정은 관리자가 디렉터리가 공유할 AWS 계정을 지정해 디렉터리 공유 워크플로우를 시작합니다. 디렉터리 소유자는 AWS Directory Service 콘솔에서 지정된 디렉터리의 Scale & Share(스케일 및 공유) 탭을 사용하여 디렉터를 공유한 사람을 확인할 수 있습니다.

디렉터리 소비자 계정

공유 디렉터리 관계에서 디렉터리 소비자는 디렉터리 소유자가 디렉터를 공유한 AWS 계정 소유자입니다. 사용한 공유 방법에 따라, 이 계정의 관리자가 공유 디렉터리 사용을 시작하기 전에 디렉터리 소유자의 초대를 수락해야 할 수도 있습니다.

디렉터리 공유 프로세스는 디렉터리 소비자 계정에 공유 디렉터를 생성합니다. 이 공유 디렉터리에는 디렉터리 소유자 계정의 시작 디렉터리가 위치한 도메인에 원활하게 조인할 수 있도록 EC2 인스턴스를 활성화시키는 메타데이터가 포함되어 있습니다. 디렉터리 소비자 계정의 각 공유 디렉터리에는 고유 식별자(Shared directory ID(공유 디렉터리 ID))가 있습니다.

공유 방법

AWS Managed Microsoft AD는 다음 두 가지 디렉터리 공유 방법을 제공합니다.

- AWS Organizations - 이 방법을 사용하면 디렉터리 소비자 계정을 찾아보고 검증할 수 있으므로 조직 내에서 디렉터를 더 쉽게 공유할 수 있습니다. 이 옵션을 사용하려면 조직에서 모든 기능을 활

성화시켜야 하며, 디렉터리가 조직의 관리 계정 내에 있어야 합니다. 디렉터리 소비자 공유 계정이 디렉터리 공유 요청을 수락할 필요가 없기 때문에 설정이 간편한 공유 방법입니다. 콘솔에서는 이 방법을 조직 내부의 AWS 계정과 이 디렉터리 공유라고 합니다.

- Handshake(핸드셰이크) - AWS Organizations를 사용하지 않을 때 디렉터리 공유를 활성화하는 방법입니다. 핸드셰이크 방법의 경우, 디렉터리 소비자 계정이 디렉터리 공유 요청을 수락해야 합니다. 콘솔에서는 이 방법을 조직 내부의 다른 AWS 계정과 이 디렉터리 공유라고 합니다.

네트워크 연결

네트워크 연결은 AWS 계정 간에 디렉터리 공유 관계를 사용하기 위한 사전 조건입니다. AWS는 VPC를 연결하는 많은 솔루션을 지원하며, 이 중 일부에는 [VPC 피어링](#), [전송 게이트웨이](#), [VPN](#)이 포함됩니다. 시작하려면 [자습서: 원활한 EC2 도메인 가입을 위한 AWS 관리형 Microsoft AD 디렉터리 공유](#) 섹션을 참조하세요.

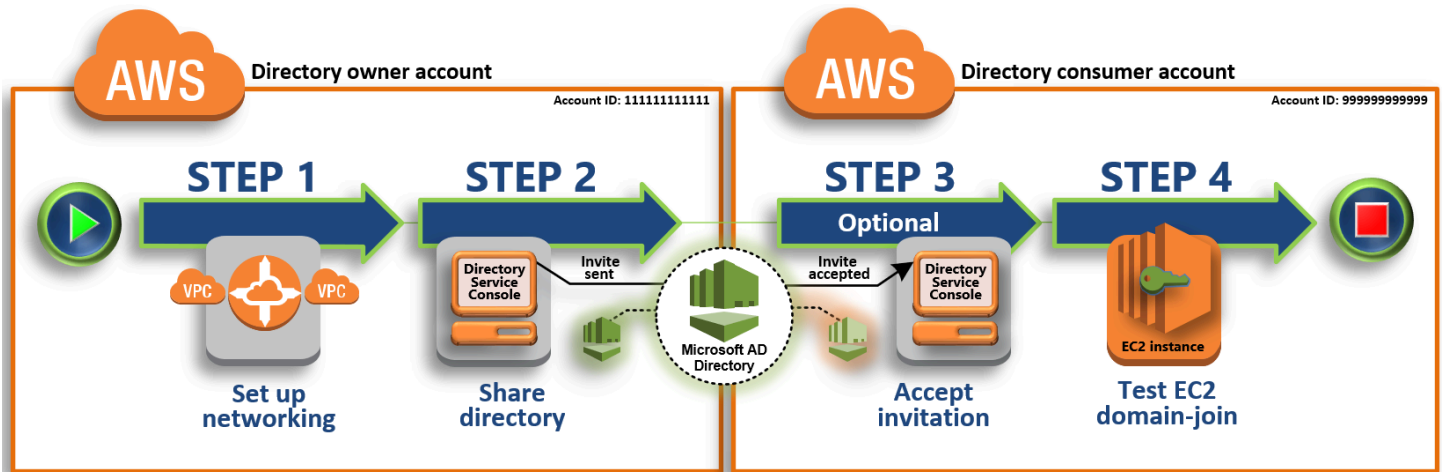
자습서: 원활한 EC2 도메인 가입을 위한 AWS 관리형 Microsoft AD 디렉터리 공유

이 자습서에서는 AWS Managed Microsoft AD 디렉터리 (디렉터리 소유자 계정) 를 다른 사용자 AWS 계정 (디렉터리 소비자 계정) 와 공유하는 방법을 보여줍니다. 네트워킹 사전 요구 사항이 완료되면 둘 사이에서 디렉터리를 공유하게 됩니다. AWS 계정 이후 EC2 인스턴스를 디렉터리 소비자 계정의 도메인에 원활하게 조인하는 방법을 알아봅니다.

이 자습서에 대한 학습을 시작하기 전에 디렉터리 공유와 관련된 주요 개념과 사용 사례에 대한 내용을 검토하는 것이 좋습니다. 자세한 정보는 [디렉터리 공유의 주요 개념](#)을 참조하세요.

디렉터리를 공유하는 프로세스는 디렉터리를 같은 AWS 조직의 다른 AWS 계정 사람과 공유하는지 아니면 조직 외부의 계정과 공유하는지에 따라 달라집니다. AWS 공유 원리에 대한 자세한 내용은 [공유 방법](#)을 참조하세요.

이 워크플로우는 네 가지 기본 단계로 이루어집니다.



1단계: 네트워킹 환경 설정

디렉터리 소유자 계정에서 디렉터리 공유 프로세스에 필요한 모든 네트워킹 사전 조건에 대해 설정을 합니다.

2단계: 내 디렉터리를 공유

디렉터리 소유자 관리자 자격 증명으로 로그인을 해서 AWS Directory Service 콘솔을 열고, 디렉터리 소비자 계정에 초대장을 보내는 공유 디렉터리 워크플로우를 시작합니다.

3단계: 공유 디렉터리 초대 수락 - 선택 사항

디렉터리 소비자 관리자 자격 증명으로 로그인한 상태에서 AWS Directory Service 콘솔을 열고 디렉터리 공유 초대를 수락합니다.

4 단계: Windows 서버용 EC2 인스턴스를 도메인에 원활하게 조인하는 것을 테스트

마지막으로 디렉터리 소비자 관리자로 EC2 인스턴스를 도메인에 조인하는 시도를 하고, 작동을 하는지 확인합니다.

추가 리소스

- [사용 사례: AWS 계정의 특정 도메인에 원활하게 Amazon EC2 인스턴스를 조인할 수 있도록 내 디렉터리를 공유](#)
- [AWS 보안 블로그 기사: 여러 계정 및 VPC의 Amazon EC2 인스턴스를 단일 관리형 AWS Microsoft AD 디렉터리로 조인하는 방법](#)

1단계: 네트워킹 환경 설정

이 자습서의 단계들을 시작하기 전에 다음 작업을 수행해야 합니다.

- 동일한 지역에서 테스트 AWS 계정 목적으로 두 개를 새로 생성하십시오. 를 생성하면 각 계정에 전용 가상 사설 클라우드 (VPC) 가 자동으로 생성됩니다. AWS 계정 각 계정의 VPC ID를 기록해둡니다. 나중에 필요하게 될 정보입니다.
- 이 단계의 절차를 사용, 각 계정에서 두 VPC 간 VPC 피어링 연결을 생성합니다.

Note

디렉터리 소유자와 디렉터리 소비자 계정 VPC를 연결하는 방법은 여러 가지가 있지만 이 자습서에서는 VPC 피어링 방법을 사용합니다. 추가 VPC 연결 옵션은 [네트워크 연결](#) 단원을 참조하세요.

디렉터리 소유자와 디렉터리 소비자 계정 간 VPC 피어링 연결 구성

디렉터리 소비자와 디렉터리 소유자 VPC 간 VPC 피어링 연결을 생성합니다. 이 단계에 따라 디렉터리 소비자 계정을 연결할 VPC 피어링 연결을 구성합니다. 이렇게 연결을 하면 프라이빗 IP 주소를 사용해 두 VPC 간 트래픽을 라우팅할 수 있습니다.

디렉터리 소유자와 디렉터리 소비자 계정 간 VPC 피어링 연결 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요. 디렉터리 소유자 계정에서 관리자 자격 증명을 가진 사용자로 로그인합니다.
2. 탐색 창에서 [Peering Connections]를 선택합니다. 그런 다음 Create Peering Connection(피어링 연결 생성)을 선택합니다.
3. 다음 정보를 구성합니다.
 - Peering connection name tag(피어링 연결 이름 태그): 디렉터리 소비자 계정에서 이 VPC 연결을 확실히 식별할 수 있는 이름을 부여합니다.
 - VPC(요청자): 디렉터리 소유자 계정의 VPC ID를 선택합니다.
 - 피어링할 다른 VPC 선택에서 내 계정 및 This region(이 리전)이 선택되어 있는지 확인합니다.
 - VPC(수락자): 디렉터리 소비자 계정의 VPC ID를 선택합니다.
4. 피어링 연결 생성을 선택합니다. 확인 대화 상자에서 [OK]를 선택합니다.

두 VPC가 동일한 리전에 있기 때문에 VPC 피어링을 요청한 디렉터리 소유자 계정의 관리자가 디렉터리 소비자 계정을 대신해 피어링 요청을 수락할 수도 있습니다.

디렉터리 소비자 계정을 대신해 피어링 요청을 수락

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Peering Connections]를 선택합니다.
3. 대기 중인 VPC 피어링 연결을 선택합니다. (상태가 수락 대기 중.) 작업과 요청 수락을 선택합니다.
4. 확인 대화 상자에서 [Yes, Accept]를 선택합니다. 다음 확인 대화 상자에서 지금 내 라우팅 테이블 수정을 선택해 라우팅 테이블 페이지로 이동합니다.

VPC 피어링 연결이 활성 상태이므로, 디렉터리 소유자 계정의 VPC 라우팅 테이블에 항목을 추가해야 합니다. 이렇게 해야 디렉터리 소비자 계정의 VPC로 트래픽이 전송됩니다.

디렉터리 소유자 계정의 VPC 라우팅 테이블에 항목 추가

1. Amazon VPC 콘솔의 라우팅 테이블 섹션에서 디렉터리 소유자 VPC의 라우팅 테이블을 선택합니다.
2. 경로(Routes) 탭을 선택하고, 경로 편집(Edit routes) 및 경로 추가(Add route)를 차례로 선택합니다.
3. Destination(대상) 열에서 디렉터리 소비자 VPC에 대한 CIDR 블록을 입력합니다.
4. Target(대상) 열에서 앞서 디렉터리 소유자 계정에 생성한 피어링 연결에 대한 VPC 피어링 연결 ID(예: **pcx-123456789abcde000**)를 입력합니다.
5. 변경 사항 저장률 선택합니다.

디렉터리 소비자 계정의 VPC 라우팅 테이블에 항목 추가

1. Amazon VPC 콘솔의 라우팅 테이블 섹션에서 디렉터리 소비자 VPC의 라우팅 테이블을 선택합니다.
2. Routes(경로) 탭을 선택하고, Edit routes(경로 편집) 및 Add route(경로 추가)를 차례로 선택합니다.
3. Destination(대상) 열에서 디렉터리 소유자 VPC에 대한 CIDR 블록을 입력합니다.
4. Target(대상) 열에서 앞서 디렉터리 소비자 계정에 생성한 피어링 연결에 대한 VPC 피어링 연결 ID(예: **pcx-123456789abcde001**)를 입력합니다.
5. 변경 사항 저장률 선택합니다.

디렉터리 소비자 VPC 보안 그룹에서 아웃바운드 규칙 테이블에 대한 포트와 Active Directory 프로토콜을 추가해 아웃바운드 트래픽이 활성화되도록 구성합니다. 자세한 내용은 [VPC의 보안 그룹 및 AWS Managed Microsoft AD 사전 조건](#)을 참조하세요.

다음 단계

[2단계: 내 디렉터리를 공유](#)

2단계: 내 디렉터리를 공유

다음 절차를 사용해 디렉터리 소유자 계정 내부의 디렉터리 공유 워크플로우를 시작합니다.

Note

디렉터리 공유는 AWS 관리형 Microsoft AD의 지역별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)을 참조하세요.

디렉터리 소유자 계정의 내 디렉터리를 공유

1. 디렉터리 소유자 계정의 관리자 자격 증명으로 로그인하고 <https://console.aws.amazon.com/directoryservicev2/>에서 [AWS Directory Service 콘솔](#)을 엽니다. AWS Management Console
2. 탐색 창에서 디렉터리를 선택합니다.
3. 공유하려는 AWS 관리형 Microsoft AD 디렉터리의 디렉터리 ID를 선택합니다.
4. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 디렉터리를 공유할 리전을 선택한 다음 Scale & share(스케일 및 공유) 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 Scale & share(스케일 및 공유) 탭을 선택합니다.
5. Shared directories(공유 디렉터리) 섹션에서 작업을 선택한 다음 Create new shared directory(새 공유 디렉터리 생성)를 선택합니다.
6. 공유할 대상 선택 페이지에서 비즈니스 요구 사항에 따라 다음 공유 방법 중 하나를 선택합니다.

AWS 계정

 - a. 이 디렉터리를 조직 내부와 공유 — 이 옵션을 AWS 계정 사용하면 AWS 조직 AWS 계정 내부의 모든 정보가 표시된 목록에서 디렉터리를 공유할 대상을 선택할 수 있습니다. AWS 계정

디렉터리를 공유하려면 AWS Directory Service 먼저 신뢰할 수 있는 액세스를 활성화해야 합니다. 자세한 내용은 [신뢰할 수 있는 액세스 활성화 및 비활성화 방법](#)을 참조하세요.

Note

이 옵션을 사용하려면 조직에서 모든 기능을 활성화해야 하며, 디렉터리가 조직의 관리 계정 내에 있어야 합니다.

- i. 조직AWS 계정 내에서 디렉터리를 공유할 대상을 선택하고 추가를 클릭합니다. AWS 계정
 - ii. 요금 내역을 검토한 후 공유를 선택합니다.
 - iii. 이 가이드의 [4단계](#)로 넘어가세요. AWS 계정 모두 같은 조직에 속해 있기 때문에 3단계를 따를 필요는 없습니다.
- b. 이 디렉터를 다른 사용자와 공유 AWS 계정 - 이 옵션을 사용하면 AWS 조직 내부 또는 외부 계정과 디렉터를 공유할 수 있습니다. 디렉터리가 AWS 조직의 구성원이 아니고 다른 사람과 공유하려는 경우에도 이 옵션을 사용할 수 AWS 계정있습니다.
- i. AWS 계정 ID에, 디렉터를 공유할 모든 AWS 계정 ID를 입력한 후 추가를 클릭합니다.
 - ii. Send a note(노트 전송)에 다른 AWS 계정관리자에게 보낼 메시지를 입력합니다.
 - iii. 요금 내역을 검토한 후 공유를 선택합니다.
 - iv. 3단계로 이동합니다.

다음 단계

[3단계: 공유 디렉터리 초대 수락 - 선택 사항](#)

3단계: 공유 디렉터리 초대 수락 - 선택 사항

앞서 절차에서 Share this directory with other AWS 계정(핸드셰이크 방법) 옵션을 선택한 경우, 공유 디렉터리 워크플로우 완료에 이 절차를 사용해야 합니다. 이 디렉터를 조직 AWS 계정 내부와 공유 옵션을 선택한 경우 이 단계를 건너뛰고 4단계로 진행하십시오.

공유 디렉터리 초대 수락

1. 디렉터리 소비자 계정에서 관리자 자격 증명으로 로그인하고 <https://console.aws.amazon.com/directoryservicev2/> 에서 [AWS Directory Service 콘솔](#)을 엽니다. AWS Management Console

2. 탐색 창에서 Directories shared with me(내가 공유한 디렉터리)를 선택합니다.
3. 공유 디렉터리 ID 열에서 수락 대기 중 상태인 디렉터리 ID를 선택합니다.
4. Shared directory details(공유 디렉터리 세부 정보) 페이지에서 검토를 선택합니다.
5. Pending shared directory invitation(대기 중인 공유 디렉터리 초대) 대화 상자에서 노트와 디렉터리 소유자 세부 정보, 요금 정보를 검토합니다. 동의를 할 경우, 수락을 선택해 디렉터리를 사용하기 시작합니다.

다음 단계

4 단계: Windows 서버용 EC2 인스턴스를 도메인에 원활하게 조인하는 것을 테스트

4 단계: Windows 서버용 EC2 인스턴스를 도메인에 원활하게 조인하는 것을 테스트

EC2 인스턴스에서 도메인에 원활하게 조인하는지 테스트하기 위해 다음 두 방법 중 하나를 사용할 수 있습니다.

방법 1: Amazon EC2 콘솔을 사용하여 도메인 조인을 테스트

디렉터리 소비자 계정에 이들 방법을 사용합니다.

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 표시줄에서 기존 디렉터리와 AWS 리전 동일한 디렉터리를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Windows EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지(Amazon Machine Image) 섹션의 빠른 시작 창에서 Windows를 선택합니다. Amazon Machine Image(AMI) 드롭다운 목록에서 Windows Amazon Machine Image(AMI)를 변경할 수 있습니다.
7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다.
 - a. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다.

- b. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다.
- c. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다.
- d. Create key pair(키 페어 생성)를 선택합니다.
- e. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

 Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.


- 9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
- 10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



- 11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

- 12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
- 13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
- 14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

 Note

도메인 조인 디렉터를 선택하면 다음이 표시될 수 있습니다.

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로파일의 경우 기존 IAM 인스턴스 프로파일을 선택하거나 새 프로파일을 생성할 수 있습니다. IAM 인스턴스 프로파일 드롭다운 목록에서 AmazonSSM ManagedInstanceCore 및 AmazonSSM의 AWS 관리형 정책이 DirectoryServiceAccess 연결된 IAM 인스턴스 프로파일을 선택합니다. 새 프로파일을 생성하려면 새 IAM 프로파일 생성 링크를 선택한 후 다음을 수행하십시오.

1. 역할 생성을 선택합니다.
2. Select trusted entity(신뢰할 수 있는 엔터티 선택)에서 AWS Service를 선택합니다.
3. 사용 사례에서 EC2를 선택합니다.
4. 권한 추가의 정책 목록에서 AmazonSSM 및 AmazonSSM ManagedInstanceCore 정책을 선택합니다. DirectoryServiceAccess 목록을 필터링하려면 검색 상자에 **SSM**을(를) 입력합니다. 다음을 선택합니다.

Note

AmazonSSM은 인스턴스를 관리자에 조인할 수 있는 DirectoryServiceAccess 권한을 제공합니다. Active Directory AWS Directory Service AmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는 기타 권한 및 정책에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

5. Name, review, and create(이름, 검토 및 생성) 페이지에서 Role name(역할 이름)을 입력합니다. EC2 인스턴스에 연결하려면 이 역할 이름이 필요합니다.
6. (선택 사항) 설명 필드에 IAM 인스턴스 프로파일에 대한 설명을 입력할 수 있습니다.
7. 역할 생성을 선택합니다.

8. 인스턴스 시작 페이지로 돌아가서 IAM 인스턴스 프로파일 옆에 있는 새로 고침 아이콘을 선택합니다. 새 IAM 인스턴스 프로파일은 IAM 인스턴스 프로파일 드롭다운 목록에 표시되어야 합니다. 새 프로파일을 선택하고 나머지 설정은 기본값으로 유지합니다.

16. 인스턴스 시작을 선택합니다.

방법 2: 를 사용하여 도메인 가입 테스트 AWS Systems Manager

디렉터리 소비자 계정에 이들 방법을 사용합니다. 이 절차를 완료하려면 디렉터리 ID, 디렉터리 이름, DNS IP 주소 등 디렉터리 소유자 계정에 대한 몇 가지 정보가 필요합니다.

사전 조건

- 설정 AWS Systems Manager.
 - Systems Manager에 대한 자세한 내용은 [AWS Systems Manager에 대한 일반 설정](#)을 참조하세요.
- AWS 관리형 Microsoft Active Directory 도메인에 가입하려는 인스턴스에는 AmazonSSM ManagedInstanceCore 및 AmazonSSM 관리형 정책이 포함된 IAM 역할이 연결되어 있어야 합니다. DirectoryServiceAccess
 - 이러한 관리형 정책 및 Systems Manager의 IAM 인스턴스 프로파일에 연결할 수 있는 기타 정책에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager에 대한 IAM 인스턴스 프로파일 생성](#)을 참조하세요. 관리형 정책에 대한 자세한 정보는 IAM 사용 설명서에서 [AWS 관리형 정책](#)을 참조하세요.

Systems Manager를 사용하여 EC2 인스턴스를 AWS 관리형 Microsoft Active Directory 도메인에 조인하는 방법에 대한 자세한 내용은 [실행 중인 EC2 Windows 인스턴스를 AWS 디렉터리 서비스 도메인에 가입하는 AWS Systems Manager 데 사용하려면 어떻게 해야 하나요?](#) 를 참조하십시오. .

1. 에서 AWS Systems Manager 콘솔을 엽니다 <https://console.aws.amazon.com/systems-manager/>.
2. 탐색 창의 노드 관리에서 명령 실행을 선택합니다.
3. Run command(Run 명령)를 선택합니다.
4. 명령 실행 페이지에서 AWS-JoinDirectoryServiceDomain을(를) 검색합니다 해당 내용이 검색 결과에 표시되면 AWS-JoinDirectoryServiceDomain 옵션을 선택합니다.
5. Command parameters(명령 파라미터) 섹션으로 스크롤을 내립니다. 다음 파라미터를 제공해야 합니다.

Note

AWS Directory Service 콘솔로 돌아가서 나와 공유한 디렉터리를 선택하고 디렉터리를 선택하면 디렉터리 ID, 디렉터리 이름, DNS IP 주소를 찾을 수 있습니다. 디렉터리 ID는 공유 디렉터리 세부 정보 섹션에서 찾을 수 있습니다. 디렉터리 이름 및 DNS IP 주소 값은 Owner directory details(소유자 디렉터리 세부 정보) 섹션에서 찾을 수 있습니다.

- 디렉터리 ID에는 AWS 관리되는 Microsoft Active Directory의 이름을 입력합니다.
 - 디렉터리 이름에 AWS Managed Microsoft Active Directory의 이름(디렉터리 소유자 계정용)을 입력합니다.
 - DNS IP 주소의 경우 AWS 관리형 Microsoft 액티브 디렉터리 (디렉터리 소유자 계정의 경우)에 있는 DNS 서버의 IP 주소를 입력합니다.
6. 대상의 경우 인스턴스 수동 선택을 선택한 다음 도메인에 조인하려는 인스턴스를 선택합니다.
 7. 양식의 나머지 부분을 기본 값으로 유지한 다음 페이지를 아래로 스크롤해 실행을 선택합니다.
 8. 인스턴스가 도메인에 성공적으로 조인되면 명령 상태가 보류 중에서 성공으로 변경됩니다. 도메인에 조인한 인스턴스의 인스턴스 ID를 선택하고 출력 보기를 선택하여 명령 출력을 볼 수 있습니다.

이러한 단계들 중 하나를 완료하면 EC2 인스턴스를 도메인에 조인할 수 있습니다. 이렇게 하면 AWS 관리형 Microsoft AD 사용자 계정의 자격 증명으로 RDP (원격 데스크톱 프로토콜) 클라이언트를 사용하여 인스턴스에 로그인할 수 있습니다.

디렉터리 공유 해제

AWS Managed Microsoft AD 디렉터리의 공유를 해제하려면 다음 절차에 따르세요.

디렉터리 공유를 해제하려면

1. [AWS Directory Service 콘솔](#) 탐색 창의 Active Directory에서 디렉터리를 선택합니다.
2. 공유 해제하려는 AWS Managed Microsoft AD 디렉터리의 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 디렉터리를 공유 해제할 리전을 선택한 다음 크기 조정 및 공유 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.

- 다중 리전 복제에 리전이 표시되지 않는 경우 크기 조정 및 공유 탭을 선택합니다.
4. 공유 디렉터리 섹션에서 공유 해제할 공유 디렉터를 선택하고 작업과 공유 해제를 차례로 선택합니다.
 5. Unshare directory(디렉터리 공유 해제) 대화 상자에서 공유 해제를 선택합니다.

추가 리소스

- [사용 사례: AWS계정](#)의 도메인에 원활하게 Amazon EC2 인스턴스를 조인할 수 있도록 내 디렉터를 공유
- [AWS 보안 블로그 기사: 여러 계정과 VPC의 Amazon EC2 인스턴스를 단일 AWS Managed Microsoft AD 디렉터리에 조인하는 방법](#)
- [여러 계정의 Amazon RDS DB 인스턴스를 단일 공유 도메인에 조인](#)

Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory

인스턴스가 시작되면 Amazon EC2 인스턴스를 도메인에 원활하게 조인할 Active Directory 수 있습니다. 자세한 정보는 [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#)을 참조하세요. 또한 자동화를 통해 AWS Directory Service 콘솔에서 직접 EC2 인스턴스를 시작하고 Active Directory 도메인에 조인할 수 있습니다. [AWS Systems Manager](#)

EC2 인스턴스를 Active Directory 도메인에 수동으로 조인해야 하는 경우 적절한 지역 및 보안 그룹 또는 서브넷에서 인스턴스를 시작한 다음 인스턴스를 도메인에 조인해야 합니다.

이러한 인스턴스에 원격 연결이 가능하려면 연결 중인 네트워크에서 인스턴스로의 IP 연결이 있어야 합니다. 대부분의 경우, 이를 위해서는 인터넷 게이트웨이가 VPC에 연결되고 인스턴스가 퍼블릭 IP 주소를 가지고 있어야 합니다.

주제

- [AWS 관리형 Microsoft AD에서 디렉터리 관리 인스턴스를 시작합니다. Active Directory](#)
- [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#)
- [Amazon EC2 Windows 인스턴스를 관리형 AWS Microsoft AD에 수동으로 조인합니다. Active Directory](#)

- [Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD 액티브 디렉터리에 원활하게 조인합니다.](#)
- [Amazon EC2 Linux 인스턴스를 관리형 AWS Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.](#)
- [Winbind를 사용하여 Amazon EC2 Linux 인스턴스를 관리형 AWS Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.](#)
- [Amazon EC2 Mac 인스턴스를 관리형 AWS Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.](#)
- [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)
- [DHCP 옵션 세트 생성 또는 변경](#)

AWS 관리형 Microsoft AD에서 디렉터리 관리 인스턴스를 시작합니다. Active Directory

이 절차는 AWS Systems Manager 자동화를 AWS Management Console 사용하여 디렉터리를 관리하는 Amazon EC2 디렉터리 관리 Windows 인스턴스를 시작합니다. 자동화 콘솔에서 자동화 [AWS ManagementInstance>CreateDS](#)를 직접 실행하여 이 작업을 수행할 수도 있습니다. AWS Systems Manager

필수 조건

콘솔에서 디렉터리 관리 EC2 인스턴스를 시작하려면 계정에서 다음 권한을 활성화해야 합니다.

- ds:DescribeDirectories
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2>DeleteSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeKeyPairs
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile

- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam>DeleteInstanceProfile
- iam>DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam>ListAttachedRolePolicies
- iam>ListInstanceProfiles
- iam>ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm>DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm>ListCommandInvocations
- ssm>ListCommands
- ssm>ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:GetDocument

디렉터리 관리 EC2 인스턴스를 시작하려면 AWS Management Console

1. [AWS Directory Service 콘솔](#)에 로그인합니다.
2. Active Directory에서 디렉터리를 선택합니다.

3. 디렉터리 관리 EC2 인스턴스를 시작하려는 디렉터리의 디렉터리 ID를 선택합니다.
4. 디렉터리 페이지의 오른쪽 상단에서 작업을 선택합니다.
5. 작업 드롭다운 목록에서 디렉터리 관리 EC2 인스턴스 시작을 선택합니다.
6. 디렉터리 관리 EC2 인스턴스 시작 페이지의 입력 파라미터에서 필드를 작성합니다.
 - a. (선택 사항) 인스턴스에 키 페어를 제공할 수 있습니다. 키 페어 이름 - 옵션 드롭다운 목록에서 키 페어를 선택합니다.
 - b. (선택 사항) 이 자동화를 AWS CLI 실행하기 위해 사용하는 예제를 보려면 보기 AWS CLI 명령을 선택합니다.
7. 제출을 선택합니다.
8. 디렉터리 페이지로 다시 이동됩니다. 화면 상단에 성공적으로 시작을 시작했음을 나타내는 녹색 플래시바가 표시됩니다.

디렉터리 관리 (EC2 인스턴스) 를 보려면

디렉터리에 대해 EC2 인스턴스를 시작하지 않은 경우 디렉터리 관리 EC2 인스턴스에 대시(-)가 표시됩니다.

1. Active Directory에서 디렉터리를 선택하고 보려는 디렉터리를 선택합니다.
2. 디렉터리 세부 정보의 디렉터리 관리 EC2 인스턴스에서 보려는 인스턴스를 하나 또는 모두 선택합니다.
3. 인스턴스를 선택하면 원격 데스크톱을 인스턴스에 연결할 수 있는 EC2 Connect to instance 페이지로 라우팅됩니다.

Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다.


Active Directory

이 절차는 Amazon Windows EC2 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결합니다. 여러 AWS 계정개에서 원활한 도메인 조인을 수행해야 하는 경우 을 참조하십시오. [자습서: 원활한 EC2 도메인 가입을 위한 AWS 관리형 Microsoft AD 디렉터리 공유](#) Amazon SNS에 대한 자세한 내용은 [Amazon EC2란 무엇인가요?](#) 단원을 참조하세요.

Amazon Windows EC2 인스턴스에 원활하게 가입하려면

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 Amazon EC2 콘솔을 엽니다.

2. 탐색 표시줄에서 기존 디렉터리와 AWS 리전 동일한 디렉터를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Windows EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지(Amazon Machine Image) 섹션의 빠른 시작 창에서 Windows를 선택합니다. Amazon Machine Image(AMI) 드롭다운 목록에서 Windows Amazon Machine Image(AMI)를 변경할 수 있습니다.
7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다.
 - a. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다.
 - b. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다.
 - c. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다.
 - d. Create key pair(키 페어 생성)를 선택합니다.
 - e. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

 Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.

9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

Note

도메인 조인 디렉터를 선택하면 다음이 표시될 수 있습니다.

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로파일의 경우 기존 IAM 인스턴스 프로파일을 선택하거나 새 프로파일을 생성할 수 있습니다. IAM 인스턴스 프로파일 드롭다운 목록에서 AmazonSSM ManagedInstanceCore 및 AmazonSSM의 AWS 관리형 정책이 DirectoryServiceAccess 연결된 IAM 인스턴스 프로파일을 선택합니다. 새 프로파일을 생성하려면 새 IAM 프로파일 생성 링크를 선택하고 다음을 수행하십시오.
 1. 역할 생성을 선택합니다.
 2. Select trusted entity(신뢰할 수 있는 엔터티 선택)에서 AWS Service를 선택합니다.
 3. 사용 사례에서 EC2를 선택합니다.
 4. 권한 추가의 정책 목록에서 AmazonSSM 및 AmazonSSM ManagedInstanceCore 정책을 선택합니다. DirectoryServiceAccess 목록을 필터링하려면 검색 상자에 **SSM**을(를) 입력합니다. 다음을 선택합니다.

Note

AmazonSSM은 인스턴스를 관리자에 조인할 수 있는 DirectoryServiceAccess 권한을 제공합니다. Active Directory AWS Directory ServiceAmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는 기타 권한 및 정책에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

5. Name, review, and create(이름, 검토 및 생성) 페이지에서 Role name(역할 이름)을 입력합니다. EC2 인스턴스에 연결하려면 이 역할 이름이 필요합니다.
 6. (선택 사항) 설명 필드에 IAM 인스턴스 프로파일에 대한 설명을 입력할 수 있습니다.
 7. 역할 생성을 선택합니다.
 8. 인스턴스 시작 페이지로 돌아가서 IAM 인스턴스 프로파일 옆에 있는 새로 고침 아이콘을 선택합니다. 새 IAM 인스턴스 프로파일은 IAM 인스턴스 프로파일 드롭다운 목록에 표시되어야 합니다. 새 프로파일을 선택하고 나머지 설정은 기본값으로 유지합니다.
16. 인스턴스 시작을 선택합니다.

Amazon EC2 Windows 인스턴스를 관리형 AWS Microsoft AD에 수동으로 조인합니다. Active Directory

기존 Amazon EC2 Windows 인스턴스를 관리형 AWS Microsoft Active Directory AD에 수동으로 조인하려면 에 지정된 파라미터를 사용하여 인스턴스를 시작해야 합니다. [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#)

AWS 관리형 Microsoft AD DNS 서버의 IP 주소가 필요합니다. 이 정보는 디렉터리 서비스 > 디렉터리 > 디렉터리의 디렉터리 ID 링크 > 디렉터리 세부 정보 및 네트워킹 및 보안 섹션에서 찾을 수 있습니다.

The screenshot displays the AWS Directory Service console for a directory instance named 'd-1234567890'. The left sidebar shows navigation options for 'Active Directory' and 'Cloud Directory'. The main content area is divided into sections: 'Directory details' and 'Networking details'. The 'Directory details' section lists the following information:

- Directory type: Microsoft AD
- Edition: Standard
- Operating system version: Windows Server 2019
- Directory DNS name: corp.example.com
- Directory NetBIOS name: corp
- Directory administration EC2 instance(s): -

The 'Networking details' section shows the VPC and Subnets. The DNS address is highlighted as 192.0.2.1 and 198.51.100.1.

Windows 인스턴스를 AWS 관리형 Microsoft AD에 조인하려면 Active Directory

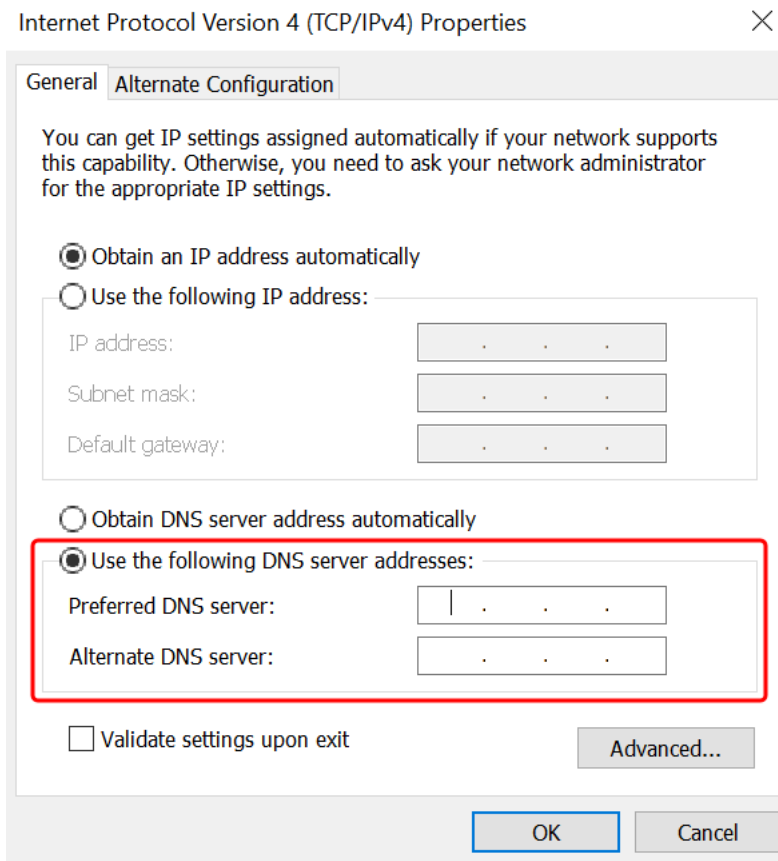
1. 원격 데스크톱 프로토콜 클라이언트를 사용해 인스턴스를 연결합니다.
2. 인스턴스에서 TCP/IPv4 속성 대화 상자를 엽니다.
 - a. 네트워크 연결 대화 상자를 엽니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 네트워크 연결 대화 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. 활성화된 네트워크 연결에 대한 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) [Properties]를 선택합니다.
 - c. 연결 속성 대화 상자에서 인터넷 프로토콜 버전 4를 엽니다(더블 클릭).
3. 다음 DNS 서버 주소 사용을 선택하고 기본 설정 DNS 서버 및 대체 DNS 서버 주소를 Microsoft AD에서 제공하는 AWS 관리형 DNS 서버의 IP 주소로 변경한 다음 확인을 선택합니다.



- 인스턴스에 대한 [System Properties] 대화 상자를 열고 [Computer Name] 탭을 선택한 다음, [Change]를 선택합니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 시스템 속성 대화 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

- 구성원 필드에서 도메인을 선택하고 AWS 관리형 Microsoft AD Active Directory의 정식 이름을 입력한 다음 확인을 선택합니다.
- 도메인 관리자의 이름과 암호를 묻는 메시지가 표시되면 도메인 조인 권한을 가진 계정의 사용자 이름과 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

Note

도메인의 전체 이름 또는 NetBIOS 이름, 백슬래시 (\), 사용자 이름 순으로 입력할 수 있습니다. 사용자 이름은 Admin입니다. 예: **corp.example.com\admin** 또는 **corp\admin**.

7. 도메인에 온 것을 환영하는 메시지를 받은 후에 인스턴스를 재시작해야 변경 사항이 적용됩니다.

이제 인스턴스가 AWS 관리형 Microsoft AD Active Directory 도메인에 가입되었으므로 해당 인스턴스에 원격으로 로그인하여 디렉터리를 관리하는 유틸리티 (예: 사용자 및 그룹 추가) 를 설치할 수 있습니다. Active Directory 관리 도구를 사용하여 사용자와 그룹을 만들 수 있습니다. 자세한 정보는 [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)을 참조하세요.

Note

Amazon EC2 인스턴스의 DNS 주소를 수동으로 변경하는 대신 Amazon Route 53을 사용하여 DNS 쿼리를 처리할 수도 있습니다. 자세한 내용은 [디렉터리 서비스의 DNS 확인 통합 Amazon Route 53 Resolver 및 네트워크로 아웃바운드 DNS 쿼리 전달](#)을 참조하십시오.

Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD 액티브 디렉터리에 원활하게 조인합니다.

이 절차는 Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD Active Directory에 원활하게 연결합니다. [여러 AWS 계정에서 원활한 도메인 조인을 수행해야 하는 경우 디렉터리 공유를 활성화하도록 선택할 수도 있습니다.](#)

다음과 같은 Linux 인스턴스 배포판과 버전이 지원됩니다.

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2(64비트 x86)
- Red Hat Enterprise Linux 8(HVM)(64비트 x86)
- Ubuntu Server 18.04 LTS 및 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

Ubuntu 14 및 Red Hat Enterprise Linux 7 이전의 배포판은 원활한 도메인 조인 기능을 지원하지 않습니다.

Linux 인스턴스를 AWS 관리형 Microsoft AD Active Directory에 원활하게 연결하는 프로세스에 대한 데모는 다음 YouTube 비디오를 참조하십시오.

[Linux용 Amazon EC2 원활한 AD 도메인 조인 데모](#)

필수 조건

Linux 인스턴스에 원활한 도메인 가입을 설정하려면 먼저 이 섹션의 절차를 완료해야 합니다.

원활한 도메인 가입 서비스 계정을 선택합니다

Linux 컴퓨터를 AWS 관리형 Microsoft AD Active Directory 도메인에 원활하게 가입할 수 있습니다. 이렇게 하려면 컴퓨터 계정 생성 권한이 있는 사용자 계정을 사용하여 컴퓨터를 도메인에 조인해야 합니다. AWS 위임된 관리자 또는 다른 그룹의 구성원은 컴퓨터를 도메인에 조인할 수 있는 충분한 권한을 가질 수 있지만, 이러한 권한은 사용하지 않는 것이 좋습니다. 가장 좋은 방법은 컴퓨터를 도메인에 조인하는 데 필요한 최소 권한이 있는 서비스 계정을 사용하는 것입니다.

컴퓨터를 도메인에 가입시키는 데 필요한 최소 권한이 있는 계정을 위임하려면 다음 PowerShell 명령을 실행할 수 있습니다. 도메인에 조인된 Windows 컴퓨터에 [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)(가) 설치되어 있는 상태에서 이러한 명령을 실행해야 합니다. 또한 컴퓨터 OU 또는 컨테이너에 대한 권한을 수정할 권한이 있는 계정을 사용해야 합니다. 이 PowerShell 명령은 서비스 계정이 도메인의 기본 컴퓨터 컨테이너에 컴퓨터 개체를 만들 수 있도록 권한을 설정합니다.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
    'schemaNamingContext'
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
    -Filter { LDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
```

```
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
    $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
in the Computers container.
$AddAccessRule = New-Object -TypeName
    'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
    'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

GUI(그래픽 사용자 인터페이스)를 선호하는 경우 [서비스 계정에 관한 위임](#)에서 설명하는 수동 프로세스를 사용할 수 있습니다.

도메인 서비스 계정을 저장할 보안 암호 생성

를 AWS Secrets Manager 사용하여 도메인 서비스 계정을 저장할 수 있습니다.

보안 암호를 만들고 도메인 서비스 계정 정보를 저장하려면

1. <https://console.aws.amazon.com/secretsmanager/> 에서 AWS Management Console 로그인하고 AWS Secrets Manager 콘솔을 엽니다.
2. 새 보안 암호 저장(Store a new secret)을 선택합니다.
3. 새 보안 암호 저장(Store a new secret) 페이지에서 다음을 수행합니다.
 - a. 암호 유형에서 다른 암호 유형을 선택합니다.
 - b. 키값 쌍에서 다음을 수행하십시오.
 - i. 첫 번째 상자에 **awsSeamlessDomainUsername**를 입력합니다. 같은 행의 다음 상자에 서비스 계정의 사용자 이름을 입력합니다. 예를 들어 이전에 PowerShell 명령을 사용한 경우 서비스 계정 이름은 다음과 같습니다**awsSeamlessDomain**.

Note

있는 그대로 **awsSeamlessDomainUsername**을 입력해야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 조인에 실패합니다.

The screenshot shows the AWS Secrets Manager console interface for creating a new secret. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows the progress: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The main content area is titled 'Choose secret type' and contains three sections: 'Secret type', 'Key/value pairs', and 'Encryption key'. In the 'Secret type' section, 'Other type of secret' is selected. In the 'Key/value pairs' section, a row is added with the key 'awsSeamlessDomainUsername'. In the 'Encryption key' section, 'aws/secretsmanager' is selected. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. Add row(행 추가)를 선택합니다.
- iii. 새 행의 첫 번째 상자에 **awsSeamlessDomainPassword**를 입력합니다. 같은 행의 다음 상자에 서비스 계정의 암호를 입력합니다.

Note

있는 그대로 **awsSeamlessDomainPassword**을 입력해야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 조인에 실패합니다.

- iv. 암호화 키에서 기본값을 그대로 유지합니다 `aws/secretsmanager`. AWS Secrets Manager 이 옵션을 선택하면 항상 암호를 암호화합니다. 사용자가 생성한 키를 선택할 수도 있습니다.

Note

사용하는 비밀번호에 따라 수수료가 부과됩니다. AWS Secrets Manager 현재 기준의 전체적인 요금 목록은 [AWS Secrets Manager 요금](#)을 참조하세요. Secrets Manager에서 생성한 AWS 관리 키를 `aws/secretsmanager` 사용하여 비밀을 무료로 암호화할 수 있습니다. 자체 KMS 키를 생성하여 암호를 암호화하는 경우 현재 요율로 AWS 요금이 부과됩니다. AWS KMS 자세한 내용은 [AWS Key Management Service 요금](#)을 참조하십시오.

v. 다음을 선택합니다.

- 비밀 이름에 다음 형식을 사용하여 디렉터리 ID가 포함된 비밀 이름을 입력합니다. 이때 `d-xxxxxxxxxx#` 디렉터리 ID로 대체합니다.

```
aws/directory-services/d-xxxxxxxx/seamless-domain-join
```

이는 애플리케이션에서 보안 암호를 검색하는 데 사용됩니다.

Note

있는 그대로 `aws/directory-services/d-xxxxxxxx/seamless-domain-join`를 입력해야 하지만, `d-xxxxxxxxxxxx`를 디렉터리 ID로 바꿔야 합니다. 선행 공백이나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 가입에 실패합니다.

The screenshot shows the 'Configure secret' page in AWS Secrets Manager. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The page is divided into four steps: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The 'Secret name and description' section is active, showing a text input for the secret name with the value 'aws/directory-services/d-xxxxxxx/seamless-domain-join'. Below the name is a description text area containing 'Access to MYSQL prod database for my AppBeta'. There are also sections for 'Tags - optional' (no tags), 'Resource permissions - optional' (with an 'Edit permissions' button), and 'Replicate secret - optional'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

5. 다른 모든 항목은 기본값으로 설정한 후 Next(다음)를 선택합니다.
6. Configure automatic rotation(자동 교체 구성)을 Disable automatic rotation(자동 교체 사용 안 함)으로 선택하고 Next(다음)를 선택합니다.

이 암호를 저장한 후 해당 암호에 대한 로테이션을 켤 수 있습니다.

7. 설정을 검토한 다음 Store(저장)를 선택하여 변경 내용을 저장합니다. 이제 Secrets Manager 콘솔에서 새 보안 암호가 목록에 포함된 계정의 보안 암호 목록으로 돌아갑니다.
8. 목록에서 새로 생성한 보안 암호 이름을 선택하고 보안 암호 ARN 값을 기록해 둡니다. 다음 단원에서 이 값을 사용하게 됩니다.

도메인 서비스 계정 비밀번호에 대한 로테이션을 켜세요.

보안 태세를 개선하려면 정기적으로 암호를 교체하는 것이 좋습니다.

도메인 서비스 계정 비밀번호에 대한 순환 기능을 켜려면

- 사용 AWS Secrets Manager 설명서의 AWS Secrets Manager [암호 자동 교체 설정의](#) 지침을 따르십시오.

5단계의 경우 사용 AWS Secrets Manager 설명서의 [Microsoft Active Directory 순환 템플릿 자격 증명을](#) 사용하십시오.

도움이 필요하면 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager [순환 문제 해결을](#) 참조하십시오.

필요한 IAM policy 정책 및 역할 생성

다음 사전 필수 단계를 사용하여 Secrets Manager 원활한 도메인 가입 암호 (이전에 생성함) 에 대한 읽기 전용 액세스를 허용하는 사용자 지정 정책을 생성하고 새 DomainJoin LinuxEC2 IAM 역할을 생성합니다.

Secrets Manager IAM 읽기 정책 생성

IAM 콘솔을 사용하여 Secrets Manager 보안 암호에 대한 읽기 전용 액세스 권한을 부여하는 정책을 생성합니다.

Secrets Manager IAM 읽기 정책을 생성하려면

1. IAM 정책을 생성할 권한이 있는 AWS Management Console 사용자로 로그인합니다. 그런 다음 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창의 액세스 관리에서 정책을 선택합니다.
3. 정책 생성(Create policy)을 선택합니다.
4. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 그런 다음 JSON 텍스트 상자에 붙여 넣습니다.

Note

지역 및 리소스 ARN을 이전에 생성한 암호의 실제 지역 및 ARN으로 교체해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. 마쳤으면 [Next]를 선택합니다. 정책 검사기가 모든 구문 오류를 보고합니다. IAM 검증 정책에 대한 자세한 내용은 [Validating IAM policies](#)를 참조하세요.
6. Review policy(정책 검토) 페이지에서 **SM-Secret-Linux-DJ-d-xxxxxxxx-Read**와 같은 정책의 이름을 입력합니다. Summary(요약)을 검토하여 정책이 부여하는 권한을 확인합니다. 그런 다음 Create policy(정책 생성)를 선택하여 변경 내용을 저장합니다. 새로운 정책이 관리형 정책 목록에 나타나며 ID 연결 준비가 완료됩니다.

Note

보안 암호당 정책을 하나씩 생성하는 것이 좋습니다. 이렇게 하면 인스턴스가 적절한 보안 암호에만 액세스할 수 있고 인스턴스가 손상될 경우 미치는 영향이 최소화됩니다.

Linux/EC2 역할을 생성하십시오. DomainJoin

IAM 콘솔을 사용하여 Linux EC2 인스턴스를 도메인에 조인하는 데 사용할 역할을 생성합니다.

Linux/EC2 역할을 만들려면 DomainJoin

1. IAM 정책을 생성할 권한이 있는 AWS Management Console 사용자로 로그인합니다. 그런 다음 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.

2. 탐색 창의 액세스 관리에서 역할을 선택합니다.
3. 콘텐츠 창에서 Create role(역할 생성)을 선택합니다.
4. 신뢰할 수 있는 엔티티 유형 선택 아래에서 AWS 서비스를 선택합니다.
5. 사용 사례에서 EC2를 선택한 후 다음을 선택합니다.

The screenshot shows the 'Select trusted entity' page in the AWS IAM console. The page is divided into two main sections: 'Trusted entity type' and 'Use case'.

Trusted entity type: This section contains five radio button options:

- AWS service** (selected): Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.

Use case: This section contains a dropdown menu for 'Service or use case' with 'EC2' selected. Below it, there are several radio button options for 'Use case':

- EC2** (selected): Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager: Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role: Allows EC2 Spot Fleet to request and terminate Spot instances on your behalf.
- EC2 - Spot Fleet Auto Scaling: Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging: Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances: Allows EC2 Spot instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet: Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled instances: Allows EC2 Scheduled instances to manage instances on your behalf.

6. Filter policies(필터 정책)의 경우 다음을 수행합니다.
 - a. **AmazonSSMManagedInstanceCore**을 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - b. **AmazonSSMDirectoryServiceAccess**을 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - c. **SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read**(또는 이전 절차에서 생성한 IAM 정책의 이름)을(를) 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - d. 위에 나열된 세 가지 정책을 추가한 후 역할 생성을 선택합니다.

Note

AmazonSSM은 인스턴스를 DirectoryServiceAccess 관리자에 조인할 수 있는 Active Directory 권한을 제공합니다. AWS Directory Service AmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는

기타 권한 및 정책에 관한 정보에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

7. 새 역할의 이름 (예: 역할 이름) 필드에 원하는 다른 이름을 입력합니다. **LinuxEC2DomainJoin**
8. (선택 사항)역할 설명에 설명을 입력합니다.
9. (선택 사항) 3단계: 태그를 추가할 태그 추가에서 새 태그 추가를 선택합니다. 태그 키-값 쌍은 이 역할에 대한 액세스를 구성, 추적 또는 제어하는 데 사용됩니다.
10. 역할 생성을 선택합니다.

Linux 인스턴스에 원활하게 가입하세요.

이제 필수 작업을 모두 구성했으므로 다음 절차를 사용하여 EC2 Linux 인스턴스를 원활하게 연결할 수 있습니다.

Linux 인스턴스를 원활하게 연결하려면

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/)에서 [Amazon EC2 콘솔을 엽니다.](#)
2. 탐색 표시줄의 지역 선택기에서 기존 디렉토리와 AWS 리전 동일한 디렉토리를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Linux EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지 (Amazon 머신 이미지) 섹션에서 시작하려는 Linux AMI를 선택합니다.

Note

사용되는 AMI에는 AWS Systems Manager (SSM 에이전트) 버전 2.3.1644.0 이상이 있어야 합니다. AMI에서 인스턴스를 시작하여 AMI에 설치된 SSM 에이전트 버전을 확인하려면 [현재 설치된 SSM 에이전트 버전 가져오기](#)를 참조하세요. SSM 에이전트를 업그레이드해야 하는 경우 [Linux용 EC2 인스턴스에 SSM 에이전트 설치 및 구성](#)을 참조하세요. SSM은 Linux 인스턴스를 도메인에 aws:domainJoin 조인할 때 플러그인을 사용합니다. Active Directory ##### Linux ##### ### ### EC2AMAZ- XXXXXXXX #####

#. 에 대한 자세한 내용은 사용 `aws:domainJoin` 설명서의 [AWS Systems Manager 명령 문서 플러그인 참조](#)를 참조하십시오. AWS Systems Manager

7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다. Create key pair(키 페어 생성)를 선택합니다. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.

9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

Note

도메인 조인 디렉터를 선택하면 다음이 표시될 수 있습니다.

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로필의 경우 사전 요구 사항 섹션 2단계: LinuxEC2 역할 생성에서 이전에 생성한 IAM 역할을 선택합니다. DomainJoin
16. 인스턴스 시작을 선택합니다.

Note

SUSE Linux로 원활한 도메인 조인을 수행하는 경우 인증이 작동하려면 재부팅해야 합니다. Linux 터미널에서 SUSE를 재부팅하려면 `sudo reboot`를 입력합니다.

Amazon EC2 Linux 인스턴스를 관리형 AWS Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.

Amazon EC2 Windows 인스턴스 외에도 특정 Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD 액티브 디렉터리에 조인할 수 있습니다. 다음과 같은 Linux 인스턴스 배포판과 버전이 지원됩니다.

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2(64비트 x86)
- 아마존 리눅스 2023 AMI
- Red Hat Enterprise Linux 8(HVM)(64비트 x86)
- Ubuntu Server 18.04 LTS 및 Ubuntu Server 16.04 LTS

- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

기타 Linux 배포판 및 버전은 작동이 가능할 수도 있지만, 테스트는 거치지 않았습니다.

Linux 인스턴스를 AWS 관리형 Microsoft AD에 연결

디렉터리에 Amazon Linux 혹은 CentOS, Red Hat, Ubuntu 인스턴스를 조인하려면 [Linux 인스턴스에 원활하게 가입하세요](#)에 지정된 대로 인스턴스를 먼저 시작해야 합니다.

Important

아래의 일부 절차들로 인해(올바르게 수행되지 않은 경우) 인스턴스 접속이나 사용이 불가능해질 수 있습니다. 따라서 이러한 절차를 수행하기 전에 인스턴스에 대한 백업을 생성하거나 스냅샷을 만드는 것이 좋습니다.

디렉터리에 Linux 인스턴스 조인

다음 탭 중 하나를 이용해 특정 Linux 인스턴스의 단계를 수행합니다.

Amazon Linux

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Amazon Linux - 64비트 인스턴스가 업데이트되었는지 확인합니다.

```
sudo yum -y update
```

4. Linux 인스턴스에 필요한 Amazon Linux 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

Note

사용 중인 Amazon Linux 버전을 확인하는 데 도움이 필요하면 Linux 인스턴스용 Amazon EC2 사용 설명서에서 [Amazon Linux 이미지 식별](#)을 참조하세요.

- 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

도메인 조인 권한을 가진 *example.com* 도메인의 계정입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...
* Successfully enrolled machine in realm
```

- 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - 텍스트 편집기에서 `/etc/ssh/sshd_config` 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

7. 인스턴스가 재시작된 후 SSH 클라이언트를 사용하여 인스턴스에 연결하고 다음 단계를 수행하여 sudoers 목록에 AWS 위임된 관리자 그룹을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "\<space>"를 사용합니다.

CentOS

- SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
- 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. AWS Directory Service VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
- CentOS 7 인스턴스가 업데이트되었는지 확인합니다.

```
sudo yum -y update
```

- Linux 인스턴스에 필요한 CentOS 7 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

- 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

도메인 조인 권한을 가진 *example.com* 도메인의 계정입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...
* Successfully enrolled machine in realm
```

- 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - 텍스트 편집기에서 `/etc/ssh/sshd_config` 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- PasswordAuthentication 설정값을 `yes`로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

7. 인스턴스가 다시 시작된 후 SSH 클라이언트를 사용하여 인스턴스에 연결하고 다음 단계를 수행하여 sudoers 목록에 AWS 위임된 관리자 그룹을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "\<space>"를 사용합니다.

Red Hat

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. AWS Directory Service VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Red Hat - 64비트 인스턴스가 업데이트되었는지 확인합니다.

```
sudo yum -y update
```

4. Linux 인스턴스에 필요한 Red Hat 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -v -U join_account example.com --install=/  
join_account
```

join_account

도메인 가입 AccountName 권한이 있는 **example.com** 도메인 계정의 SAM입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...  
* Successfully enrolled machine in realm
```

6. 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
- 텍스트 편집기에서 `/etc/ssh/sshd_config` 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- PasswordAuthentication 설정값을 `yes`로 설정합니다.

```
PasswordAuthentication yes
```

- SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

7. 인스턴스가 재시작된 후 SSH 클라이언트를 사용하여 인스턴스에 연결하고 다음 단계를 수행하여 sudoers 목록에 AWS 위임된 관리자 그룹을 추가합니다.

a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "\<space>"를 사용합니다.

SUSE

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service가 제공하는 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS Knowledge Center의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. SUSE Linux 15 인스턴스가 최신 버전인지 확인합니다.
 - a. 패키지 리포지토리를 연결합니다.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

b. SUSE를 업데이트합니다.

```
sudo zypper update -y
```

4. Linux 인스턴스에 필요한 SUSE Linux 15 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
```

5. 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account example.com --verbose
```

join_account

도메인 가입 권한이 AccountName 있는 *example.com* ##### SAM. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름입니다.

```
...
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

다음 두 가지 반환이 예상됩니다.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. PAM에서 SSSD를 수동으로 활성화합니다.

```
sudo pam-config --add --sss
```

7. nsswitch.conf에서 SSSD를 활성화하도록 nsswitch.conf를 편집합니다.

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. /etc/pam.d/common-session에 다음 줄을 추가하여 초기 로그인 시 홈 디렉터리를 자동으로 생성합니다.

```
sudo vi /etc/pam.d/common-session
```

```
session optional          pam_mkhomedir.so skel=/etc/skel umask=077
```

9. 인스턴스를 재부팅하여 도메인 조인 프로세스를 완료합니다.

```
sudo reboot
```

- 10.SSH 클라이언트를 사용하여 인스턴스에 다시 연결하여 도메인 조인이 성공적으로 완료되었는지 확인하고 추가 단계를 완료합니다.

- a. 인스턴스가 도메인에 등록되었는지 확인하려면

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

- b. SSSD 데몬의 상태를 확인하려면


```
systemctl status sssd
```

```

sssd.service - System Security Services Daemon
  Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor
  preset: disabled)
  Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
  Main PID: 479 (sss)
  Tasks: 4
  CGroup: /system.slice/sss.service
          ##479 /usr/sbin/sss -i --logger=files
          ##505 /usr/lib/sss/sss_be --domain example.com --uid 0 --gid 0 --
  logger=files
          ##548 /usr/lib/sss/sss_nss --uid 0 --gid 0 --logger=files
          ##549 /usr/lib/sss/sss_pam --uid 0 --gid 0 --logger=files

```

11.SSH 및 콘솔을 통해 사용자 액세스를 허용하려면

```
sudo realm permit join_account@example.com
```

SSH 및 콘솔을 통해 도메인 그룹 액세스를 허용하려면

```
sudo realm permit -g 'AWS Delegated Administrators'
```

또는 모든 사용자 액세스를 허용하려면

```
sudo realm permit --all
```

12.암호 인증을 허용하도록 SSH 서비스를 설정합니다.

a. 텍스트 편집기에서 /etc/ssh/sshd_config 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

13.13. 인스턴스가 재시작된 후 SSH 클라이언트를 사용하여 인스턴스에 연결하고 다음 단계를 수행하여 sudoers 목록에 AWS 위임된 관리자 그룹을 추가합니다.

a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "Domain Admins" group from the awsad.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. AWS Directory Service VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Ubuntu - 64비트 인스턴스가 업데이트되었는지 확인합니다.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Linux 인스턴스에 필요한 Ubuntu 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 역방향 DNS 확인을 비활성화하고 기본 영역을 도메인의 FQDN으로 설정합니다. 영역이 작동하려면 Ubuntu 인스턴스가 DNS에서 역 확인이 가능해야 합니다. 그렇지 않을 경우 다음과 같이 /etc/krb5.conf에서 역 DNS를 비활성해야 합니다.

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

도메인 가입 AccountName 권한이 있는 *example.com* 도메인 계정의 SAM입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...
* Successfully enrolled machine in realm
```

7. 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - a. 텍스트 편집기에서 /etc/ssh/sshd_config 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

8. 인스턴스가 재시작된 후 SSH 클라이언트를 사용하여 인스턴스에 연결하고 다음 단계를 수행하여 sudoers 목록에 AWS 위임된 관리자 그룹을 추가합니다.

a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "`\<space>`"를 사용합니다.

계정 로그인 액세스 제한

모든 계정을 Active Directory에 정의하면 기본으로 디렉토리의 모든 사용자는 인스턴스에 로그인할 수 있습니다. 특정 사용자만 sssd.conf의 ad_access_filter으로 인스턴스에 로그인할 수 있습니다. 예:

```
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

memberOf

특정 그룹의 멤버인 사용자는 반드시 인스턴스에 액세스할 수 있어야 한다는 뜻입니다.

cn

액세스해야 하는 그룹의 일반 이름입니다. 이 예제에서 그룹 이름은 *admins*입니다.

ou

위의 그룹이 위치해 있는 조직 단위(OU)입니다. 이 예제에서 OU는 *Testou*입니다.

dc

도메인의 도메인 구성 요소입니다. 이 예제에서는 *example*입니다.

dc

추가적인 도메인 구성 요소입니다. 이 예제에서는 *com*입니다.

현재 사용자는 `ad_access_filter`를 `/etc/sss/sss.conf`에 수동으로 추가해야 합니다.

텍스트 편집기에서 `/etc/sss/sss.conf` 파일을 엽니다.

```
sudo vi /etc/sss/sss.conf
```

추가를 하고 나면 `sss.conf`가 다음과 같이 보일 수 있습니다.

```
[sss]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@d
access_provider = ad
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

이 구성이 활성화되려면 `sss` 서비스를 재시작해야 합니다.

```
sudo systemctl restart sss.service
```

또는 다음 작업을 사용할 수 있습니다.

```
sudo service sss restart
```

모든 계정을 Active Directory에 정의하면 기본으로 디렉토리의 모든 사용자는 인스턴스에 로그인할 수 있습니다. 특정 사용자만 `sssd.conf`의 `ad_access_filter`으로 인스턴스에 로그인할 수 있습니다.

예:

```
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

memberOf

특정 그룹의 멤버인 사용자는 반드시 인스턴스에 액세스할 수 있어야 한다는 뜻입니다.

cn

액세스해야 하는 그룹의 일반 이름입니다. 이 예제에서 그룹 이름은 *admins*입니다.

ou

위의 그룹이 위치해 있는 조직 단위(OU)입니다. 이 예제에서 OU는 *Testou*입니다.

dc

도메인의 도메인 구성 요소입니다. 이 예제에서는 *example*입니다.

dc

추가적인 도메인 구성 요소입니다. 이 예제에서는 *com*입니다.

현재 사용자는 `ad_access_filter`를 `/etc/sss/sss.conf`에 수동으로 추가해야 합니다.

1. 텍스트 편집기에서 `/etc/sss/sss.conf` 파일을 엽니다.

```
sudo vi /etc/sss/sss.conf
```

2. 추가를 하고 나면 `sss.conf`가 다음과 같이 보일 수 있습니다.

```
[sss]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
```

```
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. 이 구성이 활성화되려면 sssd 서비스를 재시작해야 합니다.

```
sudo systemctl restart sssd.service
```

또는 다음 작업을 사용할 수 있습니다.

```
sudo service sssd restart
```

ID 매핑

Unix/Linux 사용자 식별자 (UID) 와 GID (그룹 식별자), Windows 및 SID (Active Directory보안 식별자) ID 간에 통합된 환경을 유지하기 위해 두 가지 방법으로 ID 매핑을 수행할 수 있습니다.

1. 중앙 집중식
2. 분산형

Note

중앙 집중식 사용자 ID 매핑에는 휴대용 운영 체제 인터페이스 또는 POSIX가 Active Directory 필요합니다.

중앙 집중식 사용자 ID 매핑

Active Directory또는 다른 경량 디렉터리 액세스 프로토콜 (LDAP) 서비스는 Linux 사용자에게 UID 및 GID를 제공합니다. Active Directory에서는 이러한 식별자가 사용자 속성에 저장됩니다.

- UID - 리눅스 사용자 이름 (문자열)

- UID 번호 - 리눅스 사용자 ID 번호 (정수)
- GID 번호 - 리눅스 그룹 ID 번호 (정수)

의 UID와 GID를 사용하도록 리눅스 인스턴스를 구성하려면 `sssd.conf` Active Directory `ldap_id_mapping = False` 파일에서 설정하십시오. 이 값을 설정하기 전에 사용자 및 그룹에 UID, UID 번호 및 GID 번호를 추가했는지 확인하십시오. Active Directory

분산 사용자 ID 매핑

POSIX 확장이 없거나 ID 매핑을 중앙에서 관리하지 않기로 선택한 경우 Linux에서 UID 및 GID 값을 계산할 수 있습니다. Active Directory Linux는 일관성을 유지하기 위해 사용자의 고유한 SID (보안 식별자)를 사용합니다.

분산 사용자 ID 매핑을 구성하려면 `ldap_id_mapping = True` `sssd.conf` 파일에서 설정합니다.

Linux 인스턴스에 연결

SSH 클라이언트를 사용하여 인스턴스 연결을 하면 사용자 이름을 입력하라는 메시지가 나타납니다. 사용자는 `username@example.com` 또는 `EXAMPLE\username` 형식으로 사용자 이름을 입력할 수 있습니다. 사용 중인 Linux 배포판에 따라 다음과 비슷한 응답이 나타납니다.

Amazon Linux, Red Hat Enterprise Linux, CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```


Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Sat Apr 18 22:03:35 UTC 2020

System load:  0.01          Processes:            102
Usage of /:   18.6% of 7.69GB Users logged in:      2
Memory usage: 16%          IP address for eth0: 10.24.34.1
Swap usage:   0%
```

Winbind를 사용하여 Amazon EC2 Linux 인스턴스를 관리형 AWS Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.

Winbind 서비스를 사용하여 Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD Active Directory 도메인에 수동으로 조인할 수 있습니다. 이렇게 하면 기존 온프레미스 Active Directory 사용자가 AWS 관리형 Microsoft AD Active Directory에 연결된 Linux 인스턴스에 액세스할 때 Active Directory 자격 증명을 사용할 수 있습니다. 다음과 같은 Linux 인스턴스 배포판과 버전이 지원됩니다.

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2(64비트 x86)
- 아마존 리눅스 2023 AMI
- Red Hat Enterprise Linux 8(HVM)(64비트 x86)
- Ubuntu Server 18.04 LTS 및 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

기타 Linux 배포판 및 버전은 작동이 가능할 수도 있지만, 테스트는 거치지 않았습니다.

AWS 관리형 Microsoft AD 액티브 디렉터리에 Linux 인스턴스를 조인합니다.

Important

아래의 일부 절차들로 인해(올바르게 수행되지 않은 경우) 인스턴스 접속이나 사용이 불가능해질 수 있습니다. 따라서 이러한 절차를 수행하기 전에 인스턴스에 대한 백업을 생성하거나 스냅샷을 만드는 것이 좋습니다.

디렉터리에 Linux 인스턴스 조인

다음 탭 중 하나를 이용해 특정 Linux 인스턴스의 단계를 수행합니다.

Amazon Linux/CENTOS/REDHAT

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service가 제공하는 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS Knowledge Center의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Linux 인스턴스가 최신 버전인지 확인합니다.

```
sudo yum -y update
```

4. Linux 인스턴스에 필요한 Samba/Winbind 패키지를 설치합니다.

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
```

5. 오류가 발생할 경우 되돌릴 수 있도록 기본 smb.conf 파일을 백업해 두세요.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 텍스트 편집기에서 저장된 원본 파일[/etc/samba/smb.conf]을 엽니다.

```
sudo vim /etc/samba/smb.conf
```

아래 예와 같이 Active Directory 도메인 환경 정보를 입력합니다.

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. 텍스트 편집기에서 호스트 파일[/etc/hosts]을 엽니다.

```
sudo vim /etc/hosts
```

다음과 같이 Linux 인스턴스 프라이빗 IP 주소를 추가합니다.

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

/etc/hosts 파일에 IP 주소를 지정하지 않은 경우 인스턴스를 도메인에 조인하는 동안 다음 DNS 오류가 발생할 수 있습니다.

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

이 오류는 조인에 성공했지만 [net ads] 명령으로 DNS에 DNS 레코드를 등록할 수 없었음을 의미합니다.

8. net 유틸리티를 사용하여 Linux 인스턴스를 Active Directory에 조인합니다.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

도메인 조인 권한을 가진 *example.com* 도메인의 계정입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. PAM 구성 파일을 수정하고, 아래 명령을 사용하여 winbind 인증에 필요한 항목을 추가합니다.

```
sudo authconfig --enablewinbind --enablewinbindauth --enablemkhomedir --update
```

10./etc/ssh/sshd_config 파일을 편집하여 암호 인증을 허용하도록 SSH 서비스를 설정합니다.

a. 텍스트 편집기에서 /etc/ssh/sshd_config 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

11.인스턴스가 재시작되고 나면 SSH 클라이언트에 이를 연결하고 다음 단계를 수행하여 sudoers 목록에 도메인 사용자 또는 그룹에 대한 루트 권한을 추가합니다.

a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. 신뢰하는(Trusting) 또는 신뢰할 수 있는(Trusted) 도메인에서 필요한 그룹 또는 사용자를 다음과 같이 추가한 다음 저장합니다.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "\<space>"를 사용합니다.

SUSE

- SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
- AWS Directory Service가 제공하는 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS Knowledge Center의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
- SUSE Linux 15 인스턴스가 최신 버전인지 확인합니다.
 - 패키지 리포지토리를 연결합니다.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

- b. SUSE를 업데이트합니다.

```
sudo zypper update -y
```

- Linux 인스턴스에 필요한 Samba/Winbind 패키지를 설치합니다.

```
sudo zypper in -y samba samba-winbind
```

- 오류가 발생할 경우 되돌릴 수 있도록 기본 smb.conf 파일을 백업해 두세요.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 텍스트 편집기에서 저장된 원본 파일[/etc/samba/smb.conf]을 엽니다.

```
sudo vim /etc/samba/smb.conf
```

아래 예와 같이 Active Directory 도메인 환경 정보를 입력합니다.

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. 텍스트 편집기에서 호스트 파일[/etc/hosts]을 엽니다.

```
sudo vim /etc/hosts
```

다음과 같이 Linux 인스턴스 프라이빗 IP 주소를 추가합니다.

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

/etc/hosts 파일에 IP 주소를 지정하지 않은 경우 인스턴스를 도메인에 조인하는 동안 다음 DNS 오류가 발생할 수 있습니다.

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

이 오류는 조인에 성공했지만 [net ads] 명령으로 DNS에 DNS 레코드를 등록할 수 없었음을 의미합니다.

8. 다음 명령을 통해 디렉터리에 Linux 인스턴스를 조인합니다.

```
sudo net ads join -U join_account@example.com
```

join_account

도메인 가입 AccountName 권한이 있는 *example.com* 도메인의 SaM 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름입니다.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. PAM 구성 파일을 수정하고, 아래 명령을 사용하여 Winbind 인증에 필요한 항목을 추가합니다.

```
sudo pam-config --add --winbind --mkhomedir
```

10. 텍스트 편집기에서 Name Service Switch 구성 파일[/etc/nsswitch.conf]을 엽니다.

```
vim /etc/nsswitch.conf
```

아래에 나와 있는 것과 같이 Winbind 지시문을 추가합니다.

```
passwd: files winbind
shadow: files winbind
group: files winbind
```

11. /etc/ssh/sshd_config 파일을 편집하여 암호 인증을 허용하도록 SSH 서비스를 설정합니다.

a. 텍스트 편집기에서 /etc/ssh/sshd_config 파일을 엽니다.

```
sudo vim /etc/ssh/sshd_config
```

b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

12. 인스턴스가 재시작되고 나면 SSH 클라이언트에 이를 연결하고 다음 단계를 수행하여 sudoers 목록에 도메인 사용자 또는 그룹에 대한 루트 권한을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. 신뢰하는(Trusting) 또는 신뢰할 수 있는(Trusted) 도메인에서 필요한 그룹 또는 사용자를 다음과 같이 추가한 다음 저장합니다.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "\<space>"를 사용합니다.

Ubuntu

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service가 제공하는 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동으로 설정하려면 [AWS 지식 센터의 프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법을 참조하여 특정 Linux 배포 및 버전에 맞게 영구 DNS 서버를 설정하는 방법](#)을 참조하십시오.

3. Linux 인스턴스가 최신 버전인지 확인합니다.

```
sudo yum -y update
```

```
sudo apt-get -y upgrade
```

4. Linux 인스턴스에 필요한 Samba/Winbind 패키지를 설치합니다.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. 오류가 발생할 경우 되돌릴 수 있도록 기본 smb.conf 파일을 백업해 두세요.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 텍스트 편집기에서 저장된 원본 파일[/etc/samba/smb.conf]을 엽니다.

```
sudo vim /etc/samba/smb.conf
```

아래 예와 같이 Active Directory 도메인 환경 정보를 입력합니다.

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. 텍스트 편집기에서 호스트 파일[/etc/hosts]을 엽니다.

```
sudo vim /etc/hosts
```

다음과 같이 Linux 인스턴스 프라이빗 IP 주소를 추가합니다.

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

/etc/hosts 파일에 IP 주소를 지정하지 않은 경우 인스턴스를 도메인에 조인하는 동안 다음 DNS 오류가 발생할 수 있습니다.

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
이 오류는 조인에 성공했지만 [net ads] 명령으로 DNS에 DNS 레코드를 등록할 수 없었
음을 의미합니다.
```

8. net 유틸리티를 사용하여 Linux 인스턴스를 Active Directory에 조인합니다.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

도메인 조인 권한을 가진 *example.com* 도메인의 계정입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. PAM 구성 파일을 수정하고, 아래 명령을 사용하여 Winbind 인증에 필요한 항목을 추가합니다.

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. 텍스트 편집기에서 Name Service Switch 구성 파일[/etc/nsswitch.conf]을 엽니다.

```
vim /etc/nsswitch.conf
```

아래에 나와 있는 것과 같이 Winbind 지시문을 추가합니다.

```
passwd: compat winbind
group:  compat winbind
```

```
shadow: compat winbind
```

11. /etc/ssh/sshd_config 파일을 편집하여 암호 인증을 허용하도록 SSH 서비스를 설정합니다.

- a. 텍스트 편집기에서 /etc/ssh/sshd_config 파일을 엽니다.

```
sudo vim /etc/ssh/sshd_config
```

- b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

12. 인스턴스가 재시작되고 나면 SSH 클라이언트에 이를 연결하고 다음 단계를 수행하여 sudoers 목록에 도메인 사용자 또는 그룹에 대한 루트 권한을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. 신뢰하는(Trusting) 또는 신뢰할 수 있는(Trusted) 도메인에서 필요한 그룹 또는 사용자를 다음과 같이 추가한 다음 저장합니다.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "`\<space>`"를 사용합니다.

Linux 인스턴스에 연결

SSH 클라이언트를 사용하여 인스턴스 연결을 하면 사용자 이름을 입력하라는 메시지가 나타납니다. 사용자는 `username@example.com` 또는 `EXAMPLE\username` 형식으로 사용자 이름을 입력할 수 있습니다. 사용 중인 Linux 배포판에 따라 다음과 비슷한 응답이 나타납니다.

Amazon Linux, Red Hat Enterprise Linux, CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)
```

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

```
System information as of Sat Apr 18 22:03:35 UTC 2020
```

```
System load:  0.01          Processes:            102
Usage of /:   18.6% of 7.69GB Users logged in:       2
Memory usage: 16%          IP address for eth0: 10.24.34.1
Swap usage:   0%
```

Amazon EC2 Mac 인스턴스를 관리형 AWS Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.

이 절차는 Amazon EC2 Mac 인스턴스를 AWS 관리형 Microsoft AD 액티브 디렉터리에 수동으로 조인합니다.

필수 조건

- Amazon EC2 Mac 인스턴스에는 [Amazon EC2 전용 호스트가](#) 필요합니다. 전용 호스트를 할당하고 호스트에서 인스턴스를 시작해야 합니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서에서 [Mac 인스턴스 시작을](#) 참조하십시오.
- AWS 관리형 Microsoft AD 액티브 디렉터리에 대한 DHCP 옵션 세트를 만드는 것이 좋습니다. 이렇게 하면 Amazon VPC의 모든 인스턴스가 지정된 도메인을 가리키고 DNS 서버가 해당 도메인 이름을 확인할 수 있습니다. 자세한 정보는 [DHCP 옵션 세트 생성 또는 변경을](#) 참조하세요.

Note

전용 호스팅 요금은 선택한 결제 옵션에 따라 다릅니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 [요금 및 청구를](#) 참조하십시오.

Mac 인스턴스를 수동으로 조인하려면

1. 다음 SSH 명령어를 사용하여 Mac 인스턴스에 연결합니다. Mac 인스턴스 연결에 대한 자세한 내용은 [Mac 인스턴스에 연결을](#) 참조하십시오.

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

2. Mac 인스턴스에 연결한 후 다음 명령을 사용하여 *ec2-user* 계정의 비밀번호를 생성합니다.

```
sudo passwd ec2-user
```

3. 명령줄에 메시지가 표시되면 *ec2-user* 계정의 암호를 입력합니다. Linux 인스턴스용 Amazon EC2 사용 설명서의 [운영 체제 및 소프트웨어 업데이트에](#) 나와 있는 절차에 따라 운영 체제와 소프트웨어를 업데이트할 수 있습니다.
4. 다음 *dsconfigad ### #### Mac ##### ### AWS Microsoft AD* 액티브 디렉터리 도메인에 가입할 수 있습니다. 도메인 이름, 컴퓨터 이름 및 조직 구성 단위를 AWS 관리형 Microsoft

AD Active Directory 도메인 정보로 바뀌어야 합니다. 자세한 내용은 Apple 웹 사이트의 [Mac용 디렉터리 유틸리티에서 도메인 액세스 구성을 참조하십시오.](#)

Warning

컴퓨터 이름에는 하이픈이 없어야 합니다. 하이픈으로 인해 관리형 AWS Microsoft AD Active Directory에 대한 바인딩이 차단될 수 있습니다.

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

다음 예는 도메인에 이름이 지정된 **myec2mac01** Mac 인스턴스의 관리자 사용자를 참여시킬 때 표시되는 명령의 **example.com** 모습입니다.

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

- 다음 명령을 사용하여 AWS 위임된 관리자를 Mac 인스턴스의 관리자 사용자에게 추가합니다.

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators"
```

- 다음 명령을 사용하여 AWS 관리형 Microsoft AD Active Directory 도메인 가입이 성공했는지 확인하십시오.

```
dsconfigad -show
```

Mac 인스턴스를 AWS 관리형 Microsoft AD Active Directory에 성공적으로 연결했습니다. 이제 AWS 관리형 Microsoft AD Active Directory 자격 증명을 사용하여 Mac 인스턴스에 로그인할 수 있습니다.

Mac 인스턴스에 처음 로그인할 때 “기타” 사용자로 로그인할 수 있는 옵션이 제공되어야 합니다. 이제 Active Directory 도메인 자격 증명을 사용하여 Mac 인스턴스에 로그인할 수 있습니다. 이 단계를 완료한 후에도 로그인 화면에 “기타”가 표시되지 않으면 ec2-user로 로그인한 다음 로그아웃하십시오.

도메인 사용자와 그래픽 사용자 인터페이스를 사용하여 로그인하려면 Linux 인스턴스용 Amazon EC2 사용 설명서에서 [인스턴스의 그래픽 사용자 인터페이스 \(GUI\) 연결에](#) 나와 있는 단계를 따르십시오.

AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임

컴퓨터를 디렉터리에 조인하려면 해당 권한을 가진 계정이 필요합니다.

Microsoft Active AWS Directory용 디렉터리 서비스를 사용하면 관리자 및 AWS 위임된 서버 관리자 그룹의 구성원이 이러한 권한을 가집니다.

그러나 가장 좋은 방법은 필요한 최소 권한만을 가진 계정을 사용하는 것입니다. 다음 절차에서는 **Joiners**라는 새 그룹을 생성하고 이 그룹에 컴퓨터를 디렉터리에 조인하는 데 필요한 권한을 위임하는 방법을 보여줍니다.

이 절차는 디렉터리에 조인된 컴퓨터상에서 수행해야 하며, Active Directory User and Computers MMC 스냅인이 설치되어 있어야 합니다. 또한 도메인 관리자로 로그인해야 합니다.

AWS 관리형 Microsoft AD에 대한 조인 권한을 위임하려면

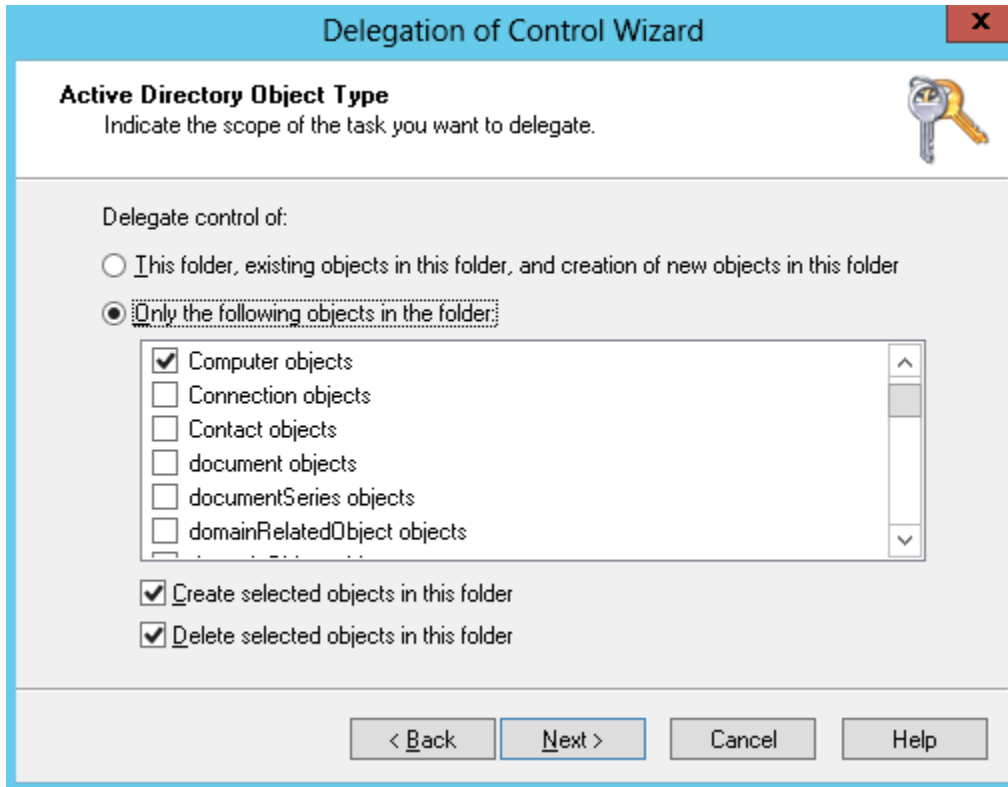
1. [Active Directory User and Computers] 페이지를 열고 탐색 트리에서 입력한 NetBIOS 이름을 가진 OU(조직 단위)를 선택한 다음, [Users] OU를 선택합니다.

Important

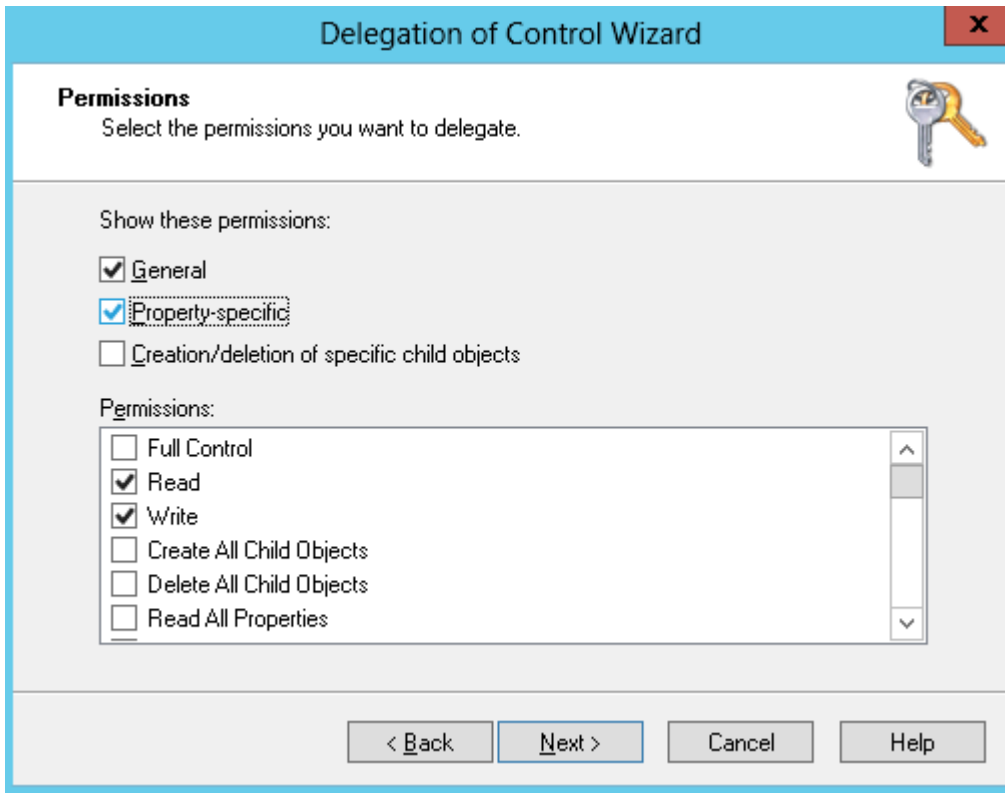
Microsoft Active AWS Directory용 디렉터리 서비스를 시작하면 디렉터리의 모든 개체가 포함된 OU (조직 구성 단위)가 AWS 만들어집니다. 디렉터리를 만들 때 입력한 NetBIOS 이름을 가진 이 OU는 도메인 루트에 있습니다. 도메인 루트는 에서 소유하고 관리합니다 AWS. 도메인 루트 자체는 변경이 불가능하기 때문에 입력한 NetBIOS 이름을 가진 OU 내에 **Joiners** 그룹을 생성해야 합니다.

2. [Users]에 대한 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭), [New]를 선택한 다음, [Group]을 선택합니다.
3. [New Object - Group] 상자에서 다음을 입력하고 [OK]를 선택합니다.
 - 그룹 이름에 **Joiners**를 입력합니다.
 - [Group scope]에서 [Global]을 선택합니다.
 - [Group type]에서 [Security]를 선택합니다.
4. 탐색 창에서 입력한 NetBIOS 이름 아래에 있는 [Computers] 컨테이너를 선택합니다. [Action] 메뉴에서 [Delegate Control]을 선택합니다.
5. [Delegation of Control Wizard] 페이지에서 Next를 선택한 후 [Add]를 선택합니다.

6. [Select Users, Computers, or Groups] 상자에 Joiners를 입력하고 [OK]를 선택합니다. 객체가 여러 개 있는 경우 위에서 생성한 Joiners 그룹을 선택합니다. 다음을 선택합니다.
7. [Tasks to Delegate] 페이지에서 [Create a custom task to delegate]를 선택한 후 [Next]를 선택합니다.
8. [Only the following objects in the folder]를 선택한 후 [Computer objects]를 선택합니다.
9. [Create selected objects in this folder]를 선택한 후 [Delete selected objects in this folder]를 선택합니다. 다음을 선택합니다.



10. [Read] 및 [Write]를 선택한 후 [Next]를 선택합니다.



11. [Completing the Delegation of Control Wizard] 페이지에서 정보를 확인하고 [Finish]를 선택합니다.
12. 강력한 암호를 사용하여 사용자를 생성하고 해당 사용자를 Joiners 그룹에 추가합니다. 이 사용자는 입력한 NetBIOS 이름 아래에 있는 [Users] 컨테이너에 있어야 합니다. 이 사용자는 인스턴스를 디렉터리에 연결할 수 있는 충분한 권한을 가집니다.

DHCP 옵션 세트 생성 또는 변경

AWS 디렉터리에 대한 DHCP 옵션 세트를 생성하고 AWS Directory Service 디렉터리가 있는 VPC에 DHCP 옵션 세트를 할당하는 것이 좋습니다. 이렇게 해야 해당 VPC의 모든 인스턴스가 지정된 도메인을 가리키고 DNS 서버가 도메인 이름을 해석할 수 있습니다.

DHCP 옵션 세트에 대한 자세한 정보는 Amazon VPC 사용 설명서의 [DHCP 옵션 세트](#)를 참조하세요.

디렉터리에 대한 DHCP 옵션 세트를 생성하는 방법

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 [DHCP Options Sets]를 선택한 후 [Create DHCP options set]를 선택합니다.
3. DHCP 옵션 세트 생성 페이지에서 디렉터리에 대해 다음 값을 입력합니다.

이름

옵션 세트를 위한 옵션 태그입니다.

도메인 이름

corp.example.com 등 디렉터리의 정규화된 이름.

도메인 이름 서버

AWS제공된 디렉터리의 DNS 서버 IP 주소.

Note

[AWS Directory Service 콘솔](#) 탐색 창으로 가서 디렉터리를 선택한 후 올바른 디렉터리 ID를 선택하면 이들 주소를 찾을 수 있습니다.

NTP 서버

이 필드는 비워둡니다.

NetBIOS 이름 서버

이 필드는 비워둡니다.

NetBIOS 노드 유형

이 필드는 비워둡니다.

4. [Create DHCP options set]를 선택합니다. 새 DHCP 옵션 세트가 DHCP 옵션 목록에 나타납니다.
5. 새로운 DHCP 옵션 세트의 ID를 기록해 두세요(dopt-xxxxxxxx). 새 옵션 세트를 VPC와 연결할 때 필요합니다.

VPC와 연결된 DHCP 옵션 세트를 변경하려면

DHCP 옵션 세트를 생성한 후에는 이 옵션 세트를 수정할 수 없습니다. VPC에서 다른 DHCP 옵션 세트를 사용하도록 하려면 새 세트를 생성하여 VPC와 연결해야 합니다. DHCP 옵션을 전혀 사용하지 않도록 VPC를 설정할 수도 있습니다.

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 사용자 VPC(Your VPCs)를 선택합니다.

3. VPC를 선택한 다음 작업, VPC 설정 편집을 선택합니다.
4. DHCP 옵션 세트에서 옵션 세트를 선택하거나 DHCP 옵션 세트 없음을 선택한 후 저장을 선택합니다.

명령줄을 사용하여 VPC와 연결된 DHCP 옵션 세트를 변경하려면 다음을 참조하십시오.

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

AWS Managed Microsoft AD에서의 사용자 및 그룹 관리

사용자는 디렉터리에 액세스할 수 있는 개별 사용자 또는 개체를 나타냅니다. 그룹은 개별 사용자에게 권한을 적용할 필요 없이 사용자 그룹에 권한을 부여하거나 거부하는 데 매우 유용합니다. 사용자가 다른 조직으로 이동할 경우 해당 사용자를 다른 그룹으로 이동하면 새 조직에 필요한 권한이 사용자에게 자동으로 부여됩니다.

AWS Directory Service 디렉터리에서 사용자 및 그룹을 생성하려면 AWS Directory Service 디렉터리에 조인된 인스턴스(온프레미스 또는 EC2)에 연결하고, 사용자 및 그룹 생성 권한이 있는 사용자로 로그인해야 합니다. 또한 Active Directory 사용자 및 컴퓨터 스냅인을 사용하여 사용자 및 그룹을 추가할 수 있도록 EC2 인스턴스에 Active Directory 도구도 설치해야 합니다.

관리 콘솔에서 AWS Directory Service 사전 설치된 Active Directory 관리 도구를 사용하여 사전 구성된 EC2 인스턴스를 배포할 수 있습니다. 자세한 내용은 [AWS 관리형 Microsoft AD에서 디렉터리 관리 인스턴스를 시작합니다. Active Directory](#) 섹션을 참조하세요.

관리 도구를 사용하여 자체 관리형 EC2 인스턴스를 배포하고 필요한 도구를 설치해야 하는 경우 [3단계: Amazon EC2 인스턴스를 배포하여 관리형 AWS Microsoft AD 액티브 디렉터리를 관리합니다.](#)을 (를) 참조하세요.

Note

사용자 계정에서 Kerberos 사전 인증이 활성화되어 있어야 합니다. 이것이 새 사용자 계정에 대한 기본 설정이며 이를 변경해서는 안 됩니다. 이 설정에 대한 자세한 정보는 Microsoft TechNet의 [사전 인증](#)을 참조하세요.

다음 항목에서는 사용자와 그룹을 생성하고 관리하는 방법을 설명합니다.

주제

- [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)
- [사용자 생성](#)
- [사용자 삭제](#)
- [사용자 암호 재설정](#)
- [그룹 생성](#)
- [그룹에 사용자 추가](#)

AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치

Amazon EC2 Windows Server 인스턴스에서 인스턴스를 관리하려면 인스턴스에 을 설치해야 합니다 Active Directory Domain Services and Active Directory Lightweight Directory Services Tools. Active Directory 다음 절차를 사용하여 EC2 Windows Server 인스턴스에 이러한 도구를 설치할 수 있습니다.

필수 조건

이 절차를 시작하기 전에 다음을 완료하십시오.

1. AWS 관리형 Microsoft AD를 만드세요Active Directory. 자세한 정보는 [AWS 관리형 Microsoft AD 만들기](#)을 참조하세요.
2. EC2 Windows Server 인스턴스를 시작하고 AWS 관리형 Microsoft AD Active Directory에 연결합니다. EC2 인스턴스에 사용자 및 그룹을 생성하려면 다음과 같은 정책이 필요합니다. **AWSManagedInstanceCore** 및 **AmazonSSMDirectoryServiceAccess** 자세한 내용은 [AWS 관리형 Microsoft AD에서 디렉터리 관리 인스턴스를 시작합니다. Active Directory](#) 및 [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#) 섹션을 참조하세요.
3. Active Directory도메인 관리자의 자격 증명이 필요합니다. 이러한 자격 증명은 AWS 관리형 Microsoft AD를 만들 때 만들어졌습니다. 의 절차를 따랐다면 관리자 사용자 이름에는 NetBIOS 이름 () 이 포함됩니다. [AWS 관리형 Microsoft AD 만들기](#) **corp\admin**

EC2 Windows Server 인스턴스에 액티브 디렉터리 관리 도구를 설치합니다.

EC2 Windows Server 인스턴스에 Active Directory 관리 도구를 설치하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.

2. Amazon EC2 Console에서 Instances를 선택하고, Windows Server 인스턴스를 선택한 다음 Connect를 선택합니다.
3. 인스턴스에 연결 페이지에서 RDP 클라이언트를 선택합니다.
4. RDP 클라이언트 탭에서 원격 데스크톱 파일 다운로드를 선택한 다음 암호 가져오기를 선택하여 암호를 검색합니다.
5. Windows 암호 가져오기에서 프라이빗 키 파일 업로드를 선택합니다. Windows Server 인스턴스와 연결된.pem 프라이빗 키 파일을 선택합니다. 프라이빗 키 파일을 업로드한 후 암호 해독을 선택합니다.
6. Windows 보안 대화 상자에서 로그인할 Windows Server 컴퓨터의 로컬 관리자 자격 증명을 복사합니다. 사용자 이름은 다음 형식일 수 있습니다 **DNS-Name\admin**. **NetBIOS-Name\admin** 또는. 예를 들어, **corp\admin** 의 절차를 따랐다면 사용자 이름이 될 [AWS 관리형 Microsoft AD 만들기](#) 것입니다.
7. Windows Server 인스턴스에 로그인한 후 [시작] 메뉴에서 [서버 관리자] 를 선택하여 [서버 관리자] 를 엽니다.
8. 서버 관리자 대시보드에서 역할 및 기능 추가를 선택합니다.
9. 역할 및 기능 추가 마법사에서 설치 유형을 선택하고 역할 기반 또는 기능 기반 설치를 선택한 후 다음을 선택합니다.
10. 서버 선택에서 로컬 서버가 선택되었는지 확인하고 왼쪽 탐색 창에서 기능을 선택합니다.
11. 기능 트리에서 원격 서버 관리 도구, 역할 관리 도구를 열고 AD DS 및 AD LDS 도구를 선택하고 엽니다. AD DS 및 AD LDS 도구를 선택하면 Active Directory모듈 대상, AD DS 도구Windows PowerShell, AD LDS 스냅인 및 명령줄 도구가 선택됩니다. 아래로 스크롤하여 DNS 서버 도구를 선택한 후 다음을 선택합니다.

Select features

DESTINATION SERVER

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

<input type="checkbox"/>	Remote Differential Compression
<input checked="" type="checkbox"/>	Remote Server Administration Tools
▸ <input type="checkbox"/>	Feature Administration Tools
<input checked="" type="checkbox"/>	Role Administration Tools
▸ <input checked="" type="checkbox"/>	AD DS and AD LDS Tools
<input checked="" type="checkbox"/>	Active Directory module for Windows PowerShell
▸ <input checked="" type="checkbox"/>	AD DS Tools
<input checked="" type="checkbox"/>	AD LDS Snap-Ins and Command-Line Tools
▸ <input type="checkbox"/>	Hyper-V Management Tools
▸ <input type="checkbox"/>	Remote Desktop Services Tools
▸ <input type="checkbox"/>	Windows Server Update Services Tools
▸ <input type="checkbox"/>	Active Directory Certificate Services Tools
▸ <input type="checkbox"/>	Active Directory Rights Management Services Tools
▸ <input type="checkbox"/>	DHCP Server Tools
<input checked="" type="checkbox"/>	DNS Server Tools
▸ <input type="checkbox"/>	Fax Server Tools
▸ <input type="checkbox"/>	File Services Tools
▸ <input type="checkbox"/>	Network Controller Management Tools
▸ <input type="checkbox"/>	Network Policy and Access Services Tools

Description

Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.

< Previous

Next >

Install

Cancel

12. 정보를 검토한 후 설치를 선택합니다. 기능 설치가 완료되면 관리 도구 폴더의 시작 메뉴에서 Active Directory 도메인 서비스와 Active Directory Lightweight Directory Services 도구를 사용할 수 있습니다.

EC2 Windows Server 인스턴스에 액티브 디렉터리 관리 도구를 설치하는 다른 방법

- Active Directory 관리 도구를 설치하는 몇 가지 다른 방법은 다음과 같습니다.
 - 를 사용하여 Active Directory 관리 도구를 설치하도록 선택할 수도 Windows PowerShell 있습니다. 예를 들어 를 사용하여 PowerShell 프롬프트에서 Active Directory 원격 관리 도구를 설치할 수 Install-WindowsFeature RSAT-ADDS 있습니다. 자세한 내용은 Microsoft 웹 [WindowsFeature사이트에 설치](#)를 참조하십시오.
 - 의 절차에 따라 Active Directory 도메인 서비스 및 Active Directory 경량 디렉터리 서비스 도구가 이미 설치되어 AWS Management Console 있는 에서 [AWS 관리형 Microsoft AD에서 디렉터리 관리 인스턴스를 시작합니다](#). [Active Directory](#) 디렉터리 관리 EC2 인스턴스를 시작할 수도 있습니다.

사용자 생성

AWS Managed Microsoft AD 디렉터리에 조인된 EC2 인스턴스에서 사용자를 생성하려면 다음 절차를 사용합니다. 사용자를 만들려면 먼저 [Active Directory 관리 도구 설치](#)의 절차를 완료해야 합니다.

다음 방법 중 하나를 사용하여 사용자를 생성할 수 있습니다.

- Active Directory관리 도구
- Windows PowerShell

Active Directory관리 도구를 사용하여 사용자 만들기

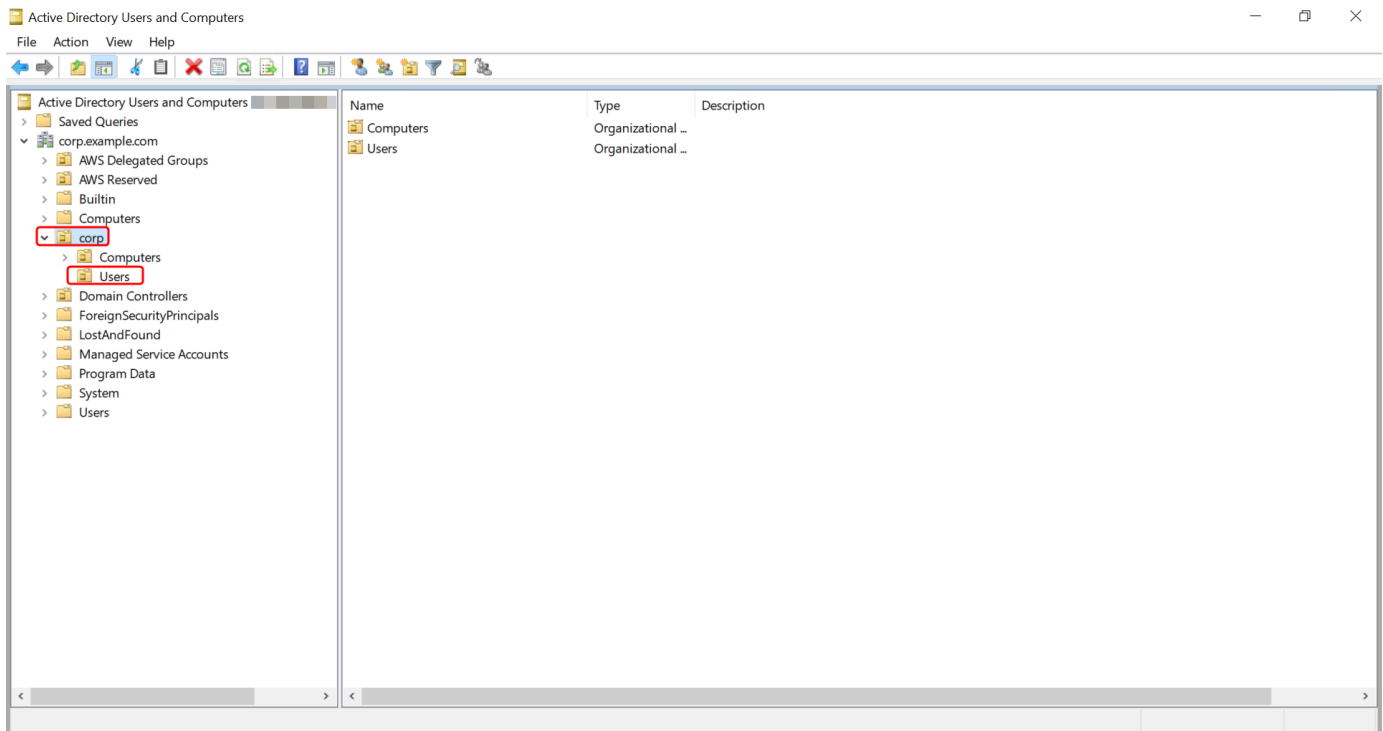
1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
2. Windows 시작 메뉴에서 Active Directory 사용자 및 컴퓨터 도구를 엽니다. Windows 관리 도구 폴더에 이 도구의 바로 가기가 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서 디렉터리의 NetBIOS 이름 OU에서 사용자를 저장할 OU (예:) 를 선택합니다. **corp\Users** 의 디렉터리에서 AWS사용되는 OU 구조에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#) 을 참조하십시오.



4. 작업 메뉴에서 새로 만들기를 클릭한 후 사용자를 선택하여 새 사용자 마법사를 엽니다.
5. 마법사의 첫 페이지에서 다음 필드에 값을 입력하고 다음을 선택합니다.
 - 이름
 - 성
 - 사용자 로그인 이름
6. 마법사의 두 번째 페이지에서 암호와 암호 확인에 임시 암호를 입력합니다. 다음 로그인할 때 반드시 암호 변경 옵션이 선택되어 있는지 확인합니다. 다른 옵션들 중 어떤 것도 선택해서는 안 됩니다. 다음을 선택합니다.
7. 마법사의 세 번째 페이지에서 새 사용자 정보가 올바른지 확인한 후 마침을 선택합니다. 새 사용자가 사용자 폴더에 나타납니다.

에서 사용자 생성 Windows PowerShell

1. Active Directory관리자로 Active Directory 도메인에 가입된 인스턴스에 연결합니다.
2. Windows PowerShell를 엽니다.
3. 다음 명령을 입력하여 사용자 이름을 **jane.doe** 생성하려는 사용자의 사용자 이름으로 대체합니다. 새 사용자의 비밀번호를 입력하라는 메시지가 표시됩니다. Windows PowerShell Active

Directory 암호 복잡성 요구 사항에 대한 자세한 내용은 [Microsoft 설명서를 참조하십시오.](#) [New-ADUser 명령에 대한 자세한 내용은 설명서를 참조하십시오.](#) [Microsoft](#)

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString 'Password')
```

사용자 삭제

AWS 관리형 Microsoft AD에 가입한 사용자를 삭제하려면 다음 절차를 사용하십시오 Active Directory.

다음 방법 중 하나를 사용하여 사용자를 삭제할 수 있습니다.

- Active Directory 관리 도구
- Windows PowerShell

Active Directory 관리 도구를 사용하여 사용자 삭제

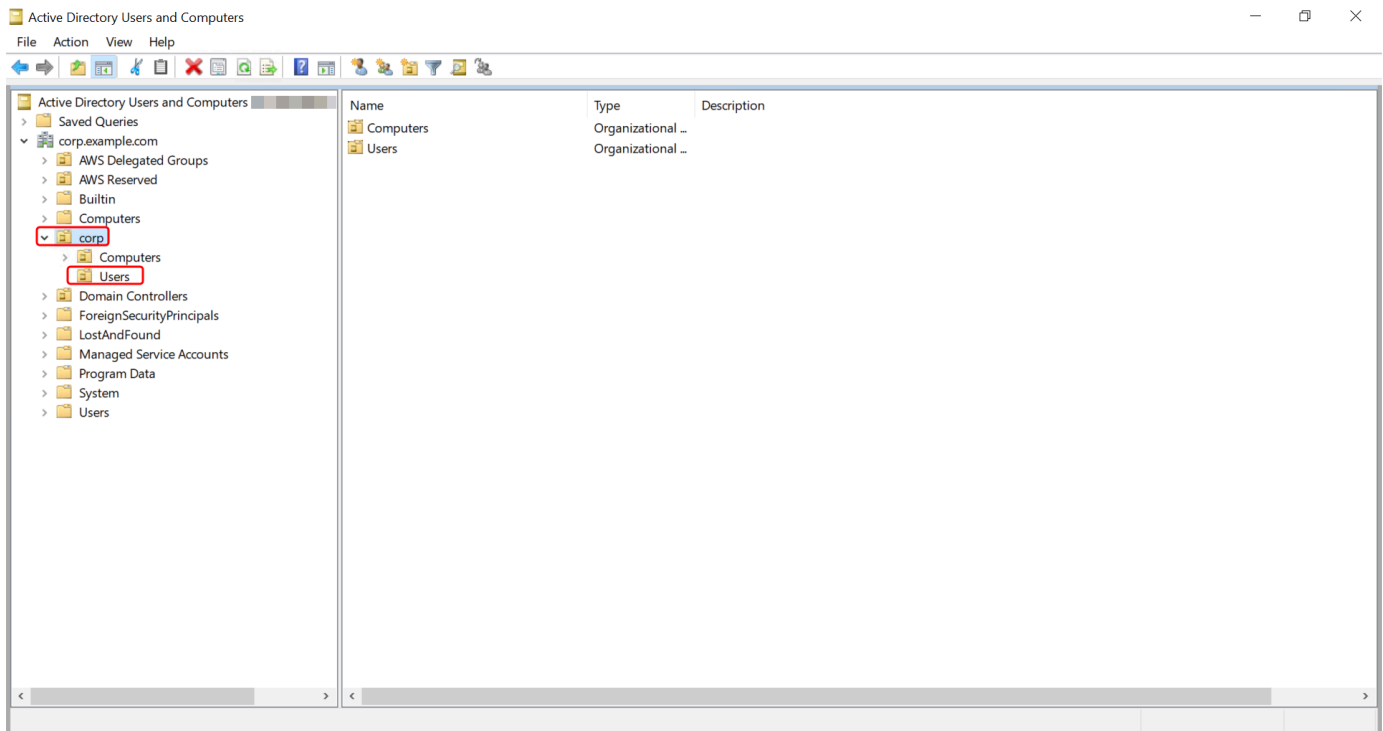
1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
2. Windows 시작 메뉴에서 Active Directory 사용자 및 컴퓨터 도구를 엽니다. Windows 관리 도구 폴더에 이 도구의 바로 가기가 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서 삭제하려는 사용자가 들어 있는 OU (예: **corp\Users**) 를 선택합니다.



4. 삭제하려는 사용자를 선택합니다. Action 메뉴에서 Delete를 선택합니다.
5. 사용자를 삭제할 것인지 확인하라는 대화 상자가 나타납니다. 사용자를 삭제하려면 예를 선택합니다. 그러면 선택한 사용자가 영구적으로 삭제됩니다.

에서 사용자 삭제 Windows PowerShell

1. Active Directory관리자로 Active Directory 도메인에 가입된 인스턴스에 연결합니다.
2. Windows PowerShell를 엽니다.
3. 다음 명령을 입력하여 사용자 이름을 **jane.doe** 삭제하려는 사용자의 사용자 이름으로 대체합니다. [Remove-ADUser 명령에 대한 자세한 내용은 설명서를 참조하십시오. Microsoft](#)

```
Remove-ADUser -Identity "jane.doe"
```

AD 휴지통 고려 사항

삭제된 사용자는 AD 휴지통에 임시로 저장됩니다. AD 휴지통에 대한 자세한 내용은 디렉토리 서비스 팀에 문의하기 블로그의 [AD 휴지통: 이해, 구현, 모범 사례 및 문제 해결](#)을 참조하십시오. Microsoft

사용자 암호 재설정

사용자는 에 정의된 암호 정책을 준수해야 합니다Active Directory. 이 경우 Active Directory 관리자를 비롯한 사용자가 자신의 비밀번호를 잊어버릴 수 있어 문제가 발생할 수 있습니다. 이 경우 사용자가 AWS 관리형 Microsoft AD에 상주하는 AWS Directory Service 경우 를 사용하여 사용자 암호를 빠르게 재설정할 수 있습니다.

암호를 재설정하는 데 필요한 권한이 있는 사용자로 로그인해야 합니다. 권한에 대한 자세한 내용은 [AWS Directory Service 리소스에 대한 액세스 권한 관리 개요](#) 섹션을 참조하세요.

다음과 같은 경우를 제외하고 내 모든 사용자의 암호를 재설정할 수 있습니다. Active Directory

- OU (조직 구성 단위) 내 모든 사용자의 암호를 재설정할 수 있습니다. 이 암호는 OU (조직 구성 단위) 를 만들 때 사용한 NetBIOS 이름을 기반으로 합니다. Active Directory 예를 들어 NetBIOS 이름의 절차를 따르면 CORP가 되고 재설정할 수 있는 사용자 암호는 Corp/Users OU의 구성원이 됩니다. [AWS 관리형 Microsoft AD 만들기](#)
- OU를 만들 때 사용한 NetBIOS 이름을 기반으로 하는 OU 외부 사용자의 암호는 재설정할 수 없습니다. Active Directory 예를 들어 AWS 예약된 OU의 사용자 암호는 재설정할 수 없습니다. AWS 관리형 Microsoft AD의 OU 구조에 대한 자세한 내용은 을 참조하십시오 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#).

AWS 관리형 Microsoft AD에서 암호를 다시 설정할 때 암호 정책이 적용되는 방법에 대한 자세한 내용은 을 참조하십시오 [암호 정책 적용 방법](#).

다음 방법 중 하나를 사용하여 사용자 암호를 재설정할 수 있습니다.

- AWS Management Console
- AWS CLI
- Windows PowerShell

에서 사용자 암호를 재설정합니다. AWS Management Console

1. [AWS Directory Service 콘솔](#) 탐색 창의 디렉터리에서 디렉토리를 선택한 다음 목록에서 사용자 암호를 재설정하려는 디렉토리를 선택합니다. Active DirectoryActive Directory
2. Directory details(디렉터리 세부 정보) 페이지에서 Actions(작업), Reset user password(사용자 암호 재설정)를 차례로 선택합니다.
3. 사용자 암호 재설정 대화 상자의 사용자 이름에 암호를 변경해야 하는 사용자의 사용자 이름을 입력합니다.

4. 새 암호와 암호 확인에 암호를 입력한 후 암호 재설정을 선택합니다.

에서 사용자 암호를 재설정하세요. AWS CLI

1. 를 설치하려면 [의 최신 버전 설치 또는 업데이트를](#) 참조하십시오 AWS CLI. AWS CLI
2. 를 엽니다 AWS CLI.
3. 다음 명령을 입력하고 디렉터리 ID **jane.doe**, 사용자 이름 및 비밀번호를 디렉터리 ID 및 원하는 자격 **P@ssw0rd** 증명으로 바꿉니다. Active Directory 자세한 내용은 AWS CLI 명령 참조를 참조하십시오 [reset-user-password](#).

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

에서 사용자 암호를 재설정하세요. Windows PowerShell

1. Active Directory관리자로 Active Directory 도메인에 가입된 인스턴스에 연결합니다.
2. Windows PowerShell를 엽니다.
3. 다음 명령을 입력하여 사용자 이름, 디렉터리 ID **jane.doe**, 비밀번호를 디렉터리 ID 및 원하는 자격 **P@ssw0rd** 증명으로 대체합니다. Active Directory 자세한 내용은 [Reset-DS UserPassword Cmdlet](#)을 참조하십시오.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword "P@ssw0rd"
```

그룹 생성

다음 절차를 사용하여 AWS 관리형 Microsoft AD 디렉터리에 연결된 EC2 인스턴스로 보안 그룹을 만들 수 있습니다. 보안 그룹을 만들려면 먼저 [Active Directory 관리 도구 설치](#)에서 절차를 완료해야 합니다.

Windows PowerShell명령을 사용하여 그룹을 생성할 수도 있습니다. 자세한 내용은 [Windows Server 2022의 새 광고 그룹 설명서](#)를 참조하십시오. PowerShell

그룹을 생성하려면

1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.

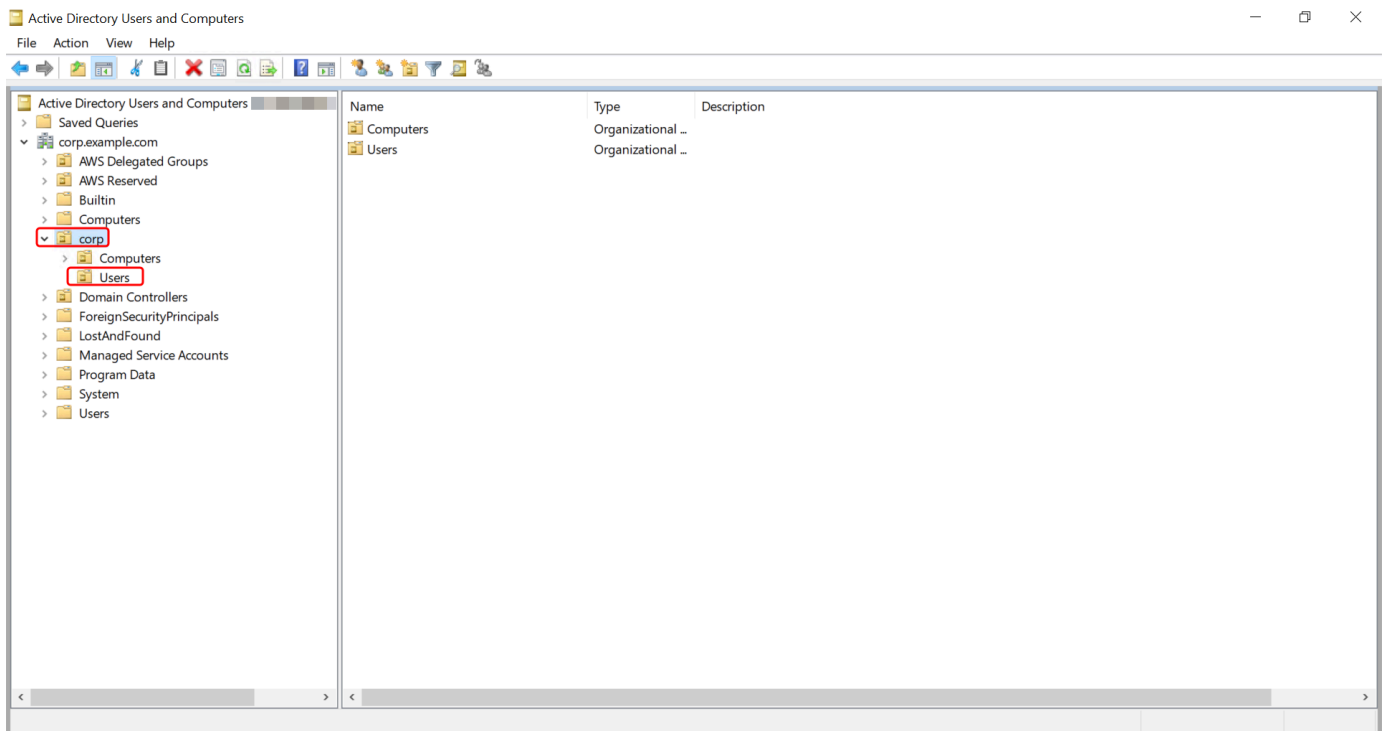
2. Active Directory 사용자 및 컴퓨터 도구를 엽니다. 이 도구에 대한 바로 가기는 관리 도구 폴더에 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서, 디렉터리의 NetBIOS 이름 OU 아래에서 그룹을 저장할 OU를 선택합니다 (예: Corp\Users). 의 디렉터리에서 사용하는 OU 구조에 대한 자세한 내용은 [AWS AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)을 참조하십시오.



4. 작업 메뉴에서 새로 만들기를 클릭한 후 그룹을 클릭하여 새 그룹 마법사를 엽니다.
5. 그룹 이름에 그룹 이름을 입력하고 필요에 맞는 그룹 범위를 선택한 다음 그룹 유형으로 보안을 선택합니다. Active Directory 그룹 범위 및 보안 그룹에 대한 자세한 내용은 Microsoft Windows Server 설명서의 [Active Directory 보안 그룹](#)을 참조하세요.
6. 확인을 클릭합니다. 사용자 폴더에 새 보안 그룹이 나타납니다.

그룹에 사용자 추가

AWS Managed Microsoft AD 디렉터리에 조인된 EC2 인스턴스에서 사용자를 보안 그룹에 추가하려면 다음 절차를 사용합니다.

그룹에 사용자를 추가하는 방법

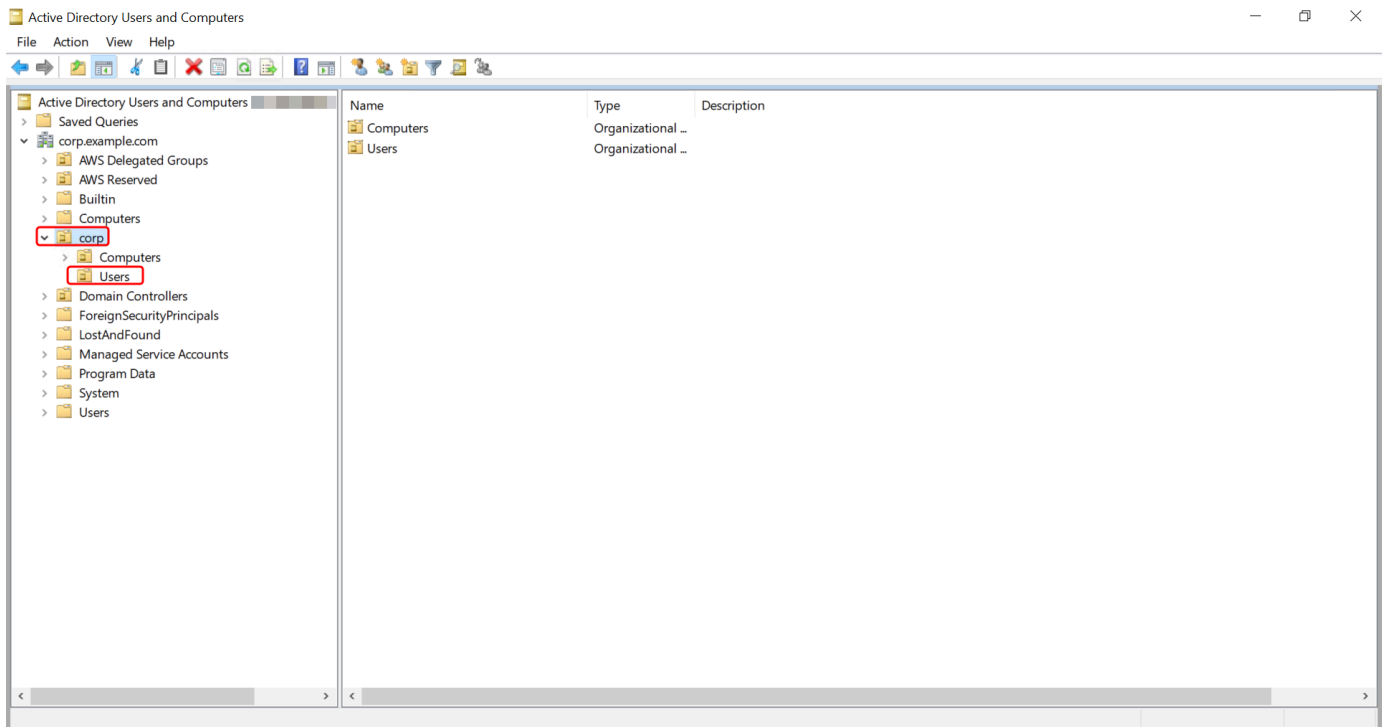
1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
2. Active Directory 사용자 및 컴퓨터 도구를 엽니다. 이 도구에 대한 바로 가기는 관리 도구 폴더에 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서, 디렉터리의 NetBIOS 이름 OU 아래에서 그룹을 저장한 OU를 선택하고 사용자를 추가하려는 그룹을 선택합니다.



4. 작업 메뉴에서 속성을 클릭하여 그룹의 속성 대화 상자를 엽니다.

5. 구성원 탭을 선택하고 추가를 클릭합니다.
6. 선택할 객체 이름 입력에 추가하려는 사용자 이름을 입력하고 확인을 클릭합니다. 구성원 목록에 이름이 표시됩니다. 확인을 다시 선택하여 그룹 멤버십을 업데이트합니다.
7. 사용자 폴더에서 사용자를 선택하고 작업 메뉴에서 속성을 클릭하여 속성 대화 상자를 열고 해당 사용자가 그룹의 구성원인지 확인합니다. 소속 그룹 탭을 선택합니다. 사용자가 속한 그룹의 이름이 목록에 표시됩니다.

기존 액티브 디렉터리 인프라에 연결

이 섹션에서는 AWS 관리형 Microsoft AD와 기존 Active Directory 인프라 간의 신뢰 관계를 구성하는 방법에 대해 설명합니다.

주제

- [신뢰 관계 생성](#)
- [퍼블릭 IP 주소를 사용할 때 IP 루트 추가](#)
- [자습서: AWS Managed Microsoft AD 디렉터리와 자체 관리형 Active Directory 도메인 간에 신뢰 관계를 생성합니다](#)
- [자습서: 두 AWS Managed Microsoft AD 도메인 간의 신뢰 관계 만들기](#)

신뢰 관계 생성

Microsoft Active Directory용 AWS 디렉터리 서비스와 자체 관리형 (온-프레미스) 디렉터리 간뿐만 아니라 클라우드의 여러 관리형 AWS Microsoft AD 디렉터리 간에도 단방향 및 양방향 외부 및 포리스트 트러스트 관계를 구성할 수 있습니다. AWS 관리형 Microsoft AD는 수신, 발신 및 양방향 (양방향) 의 세 가지 신뢰 관계 방향을 모두 지원합니다.

신뢰 관계에 대한 자세한 내용은 [AWS 관리형 Microsoft AD를 통한 트러스트에 대해 알고 싶었던 모든 것을](#) 참조하십시오.

Note

신뢰 관계를 설정할 때는 자체 관리형 디렉터리가 s와 호환되고 계속 AWS Directory Service호환되는지 확인해야 합니다. 책임 사항에 대한 자세한 내용은 [공동 책임 모델](#)을 참조하세요.

AWS 관리형 Microsoft AD는 외부 트러스트와 포리스트 트러스트를 모두 지원합니다. 포리스트 신뢰를 생성하는 방법을 보여주는 예제를 따라가려면 [자습서: AWS Managed Microsoft AD 디렉터리와 자체 관리형 Active Directory 도메인 간에 신뢰 관계를 생성합니다](#)을 참조하세요.

Amazon Chime, Amazon Connect, Amazon, Amazon, Amazon AWS IAM Identity Center WorkDocs WorkMail, QuickSight WorkSpaces Amazon 등과 같은 AWS 엔터프라이즈 앱에는 양방향 신뢰가 필요합니다. AWS Management Console AWS 관리형 Microsoft AD는 자체 Active Directory 관리형의 사용자 및 그룹을 쿼리할 수 있어야 합니다.

Amazon EC2, Amazon RDS, Amazon FSx는 단방향 또는 양방향 신뢰를 사용할 수 있습니다.

필수 조건

몇 가지 단계만 거치면 신뢰 생성이 가능하지만, 신뢰 설정에 앞서 먼저 몇 가지 선행 단계를 완료해야 합니다.

Note

AWS 관리형 Microsoft AD는 [단일 레이블 도메인과의](#) 트러스트를 지원하지 않습니다.

VPC 연결

자체 관리형 디렉터리와 신뢰 관계를 만들려면 먼저 자체 관리형 네트워크를 관리형 Microsoft AD가 포함된 Amazon VPC에 연결해야 합니다. AWS 자체 관리형 및 AWS 관리형 Microsoft AD 네트워크용 방화벽에는 Microsoft 설명서의 [WindowsServer 2008 이상 버전에](#) 나열된 네트워크 포트가 열려 있어야 합니다.

WorkDocs Amazon QuickSight 또는 Amazon과 AWS 같은 애플리케이션에서 인증할 때 전체 도메인 이름 대신 NetBIOS 이름을 사용하려면 포트 9389를 허용해야 합니다. Active Directory 포트 및 프로토콜에 대한 자세한 내용은 설명서의 [서비스 개요 및 네트워크 포트 요구 사항을](#) 참조하십시오. Windows Microsoft

이들은 디렉터리 연결 능력이 필요한 최소 포트입니다. 특정 구성에서는 추가 포트를 개방해야 하는 경우도 있습니다.

VPC 구성

관리형 AWS Microsoft AD가 포함된 VPC에는 적절한 아웃바운드 및 인바운드 규칙이 있어야 합니다.

VPC 아웃바운드 규칙을 구성하는 방법

1. [AWS Directory Service 콘솔의](#) 디렉터리 세부 정보 페이지에서 AWS 관리되는 Microsoft AD 디렉터리 ID를 기록해 둡니다.
2. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
3. [Security Groups]를 선택합니다.
4. AWS 관리형 Microsoft AD 디렉터리 ID를 검색하세요. 검색 결과에서 “디렉터리 ID 디렉터리 컨트롤러용으로 AWS 생성된 보안 그룹”이라는 설명이 있는 항목을 선택합니다.

Note

선택된 보안 그룹은 처음 디렉터리를 생성할 때 자동으로 생성된 보안 그룹입니다.

5. 해당 보안 그룹의 [Outbound Rules] 탭으로 이동합니다. [Edit]와 [Add another rule]을 차례로 선택합니다. 새 규칙에서 아래 값을 입력합니다.
 - [Type]: 모든 트래픽
 - [Protocol]: 모두
 - Destination(대상)은 도메인 컨트롤러에서 나가는 트래픽과 자체 관리형 네트워크상의 트래픽 대상을 결정합니다. 단일 IP 주소 또는 CIDR 표기법으로 된 IP 주소 범위(예: 203.0.113.5/32)를 지정합니다. 또한 동일 리전 내 다른 보안 그룹의 이름이나 ID를 지정할 수도 있습니다. 자세한 정보는 [디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오.](#)을 참조하세요.
6. 저장을 선택합니다.

Kerberos 사전 인증 활성화

사용자 계정에서 Kerberos 사전 인증이 활성화되어 있어야 합니다. 이 설정에 대한 자세한 내용은 TechNet Microsoft의 [사전 인증](#)을 참조하십시오.

자체 관리형 도메인에서의 DNS 조건부 전달자 구성

자체 관리형 도메인에서 DNS 조건부 전달자를 설정해야 합니다. [조건부 전달자에 대한 자세한 내용은 Microsoft의 도메인 이름에 TechNet 대한 조건부 전달자 할당을](#) 참조하십시오.

다음 단계를 수행하려면 자체 관리형 도메인에서 아래 Windows Server 도구들에 액세스할 권한이 있어야 합니다.

- AD DS 및 AD LDS 도구

• DNS

자체 관리형 도메인에서 조건부 전달자를 구성하려면

1. 먼저 AWS 관리형 Microsoft AD에 대한 몇 가지 정보를 얻어야 합니다. AWS Management Console 에 로그인한 다음 [AWS Directory Service 콘솔](#)을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. AWS 관리형 Microsoft AD의 디렉터리 ID를 선택합니다.
4. 디렉터리의 FQDN(Fully Qualified Domain Name)과 DNS 주소를 기록해 둡니다.
5. 이제 자체 관리형 도메인 컨트롤러로 돌아갑니다. 서버 관리자를 엽니다.
6. [Tools] 메뉴에서 [DNS]를 선택합니다.
7. 콘솔 트리에서 신뢰를 설정 중인 도메인의 DNS 서버를 확장합니다.
8. 콘솔 트리에서 [Conditional Forwarders]를 선택합니다.
9. [Action] 메뉴에서 [New conditional forwarder]를 선택합니다.
10. DNS 도메인에는 앞서 언급한 관리형 AWS Microsoft AD의 FQDN (정규화된 도메인 이름) 을 입력합니다.
11. 마스터 서버의 IP 주소를 선택하고 앞서 언급한 AWS 관리형 Microsoft AD 디렉터리의 DNS 주소를 입력합니다.

DNS 주소를 입력하고 나면 "timeout" 또는 "unable to resolve"라는 오류 메시지가 나타날 수 있습니다. 보통 이러한 오류 메시지는 무시해도 좋습니다.

12. [Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain]을 선택합니다. 확인을 선택합니다.

신뢰 관계 암호

기존 도메인과의 신뢰 관계를 설정 중이라면 Windows Server Administration 도구를 사용해 해당 도메인에서 신뢰 관계를 설정합니다. 이때, 사용한 신뢰 암호를 적어둡니다. AWS 관리형 Microsoft AD에서 신뢰 관계를 설정할 때도 이와 동일한 암호를 사용해야 합니다. 자세한 내용은 TechNet Microsoft에서의 [트러스트 관리를](#) 참조하십시오.

이제 AWS 관리형 Microsoft AD에서 신뢰 관계를 만들 준비가 되었습니다.

NetBIOS 및 도메인 이름

NetBIOS와 도메인 이름은 고유해야 하며 신뢰 관계를 설정하기 위해 동일할 수 없습니다.


신뢰 관계의 설정, 확인, 삭제

Note

신뢰 관계는 AWS 관리형 Microsoft AD의 글로벌 기능입니다. [다중 리전 복제](#)를 사용하는 경우 [기본 리전](#)에서 다음 절차를 수행해야 합니다. 변경은 복제된 모든 리전에 자동으로 적용됩니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)를 참조하세요.

AWS 관리형 Microsoft AD와 신뢰 관계를 만들려면

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. 디렉터리 페이지에서 AWS 관리되는 Microsoft AD ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 신뢰 관계 섹션에서 작업을 선택한 후 신뢰 관계 추가를 선택합니다.
5. 신뢰 관계 추가 페이지에서 신뢰 유형, 신뢰 관계가 설정된 도메인의 FQDN(정규화된 도메인 이름), 신뢰 암호 및 신뢰 방향을 포함한 필수 정보를 제공합니다.
6. (선택 사항) 인증된 사용자만 AWS Managed Microsoft AD 디렉터리의 리소스에 액세스하도록 허용하려는 경우 선택적 인증 확인란을 선택할 수 있습니다. 선택적 인증에 대한 일반 정보는 TechNet Microsoft의 [트러스트에 대한 보안 고려 사항을](#) 참조하십시오.
7. Conditional forwarder(조건부 전달자)의 경우 자체 관리형 DNS 서버의 IP 주소를 입력합니다. 이미 조건부 전달자를 생성한 경우에는 DNS IP 주소 대신 자체 관리형 도메인의 FQDN을 입력할 수 있습니다.
8. (선택 사항) Add another IP address(다른 IP 주소 추가)를 선택하고 추가적인 자체 관리형 DNS 서버의 IP 주소를 입력합니다. 해당되는 각 DNS 서버 주소(총 4개의 주소)에 대해 이 단계를 반복할 수 있습니다.
9. 추가를 선택합니다.
10. 자체 관리형 도메인에 대한 DNS 서버 또는 네트워크가 퍼블릭(RFC를 제외한 1918) IP 주소 공간을 사용하는 경우에는 IP 라우팅 섹션으로 이동하여 작업을 선택한 후 라우팅 추가를 선택합니다. CIDR 형식을 이용해 DNS 서버 또는 자체 관리형 네트워크의 IP 주소 블록을 입력합니다(예: 203.0.113.0/24). DNS 서버와 자체 관리형 네트워크가 모두 RFC 1918 IP 주소 공간을 사용하는 경우에는 이 단계가 필요하지 않습니다.

 Note

퍼블릭 IP 주소 공간을 사용하는 경우에는 [AWS IP 주소 범위](#)를 사용할 수 없으므로 절대로 사용해서는 안 됩니다.

11. (선택 사항) 라우팅 추가 페이지에서 Add routes to the security group for this directory's VPC(이 디렉터리의 VPC에 대해 보안 그룹에 라우팅 추가)도 선택할 것을 권장합니다. 이렇게 하면 "Configure your VPC"에서 위에 설명한 보안 그룹이 구성됩니다. 이러한 보안 규칙은 공개되지 않은 내부 네트워크 인터페이스에 영향을 미칩니다. 이 옵션을 사용할 수 없는 경우에는 대신에 보안 그룹을 이미 사용자 지정했음을 알리는 메시지가 표시될 것입니다.

두 도메인 모두에서 신뢰 관계를 설정해야 합니다. 이 관계는 상호 보완적이어야 합니다. 예를 들어 한 도메인에서 아웃바운드 신뢰를 설정했다면 다른 도메인에는 인바운드 신뢰를 설정해야 합니다.

기존 도메인과의 신뢰 관계를 설정 중이라면 Windows Server Administration 도구를 사용해 해당 도메인에서 신뢰 관계를 설정합니다.

AWS 관리형 Microsoft AD와 다양한 Active Directory 도메인 간에 여러 트러스트를 만들 수 있습니다. 그러나 한번에 쌍당 오직 한 개의 신뢰 관계만 존재할 수 있습니다. 예를 들어 이미 "인바운드 방향"의 단방향 신뢰가 있지만 "아웃바운드 방향"의 또 다른 신뢰 관계를 설정하고 싶은 경우에는 기존의 신뢰 관계를 삭제하고 "양방향" 신뢰를 새로 설정해야 합니다.

아웃바운드 신뢰 관계를 확인하는 방법

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. 디렉터리 페이지에서 AWS 관리되는 Microsoft AD ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 신뢰 관계 섹션에서 확인하려는 신뢰 관계를 선택하고 작업을 선택한 후 신뢰 관계 확인을 선택합니다.

이 프로세스는 양방향 트러스트의 발신 방향만 확인합니다. AWS 들어오는 트러스트의 검증은 지원하지 않습니다. 자체 관리형 Active Directory와의 신뢰 여부를 확인하는 방법에 대한 자세한 내용은 TechNet Microsoft의 [신뢰 확인](#)을 참조하십시오.

기존 신뢰 관계를 삭제하는 방법

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. 디렉터리 페이지에서 AWS 관리되는 Microsoft AD ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 신뢰 관계 섹션에서 삭제하려는 신뢰 관계를 선택하고 작업을 선택한 후 신뢰 관계 삭제를 선택합니다.
5. 삭제를 선택합니다.

퍼블릭 IP 주소를 사용할 때 IP 루트 추가

AWS Directory Service for Microsoft Active Directory를 사용해 다른 디렉터리와의 신뢰 관계 설정 등 강력한 Active Directory 기능을 활용할 수 있습니다. 그러나 다른 디렉터리의 네트워크를 위한 DNS 서버가 퍼블릭(RFC를 제외한 1918) IP 주소를 가지고 있는 경우에는 신뢰 관계를 설정하는 과정에서 이러한 IP 주소들을 지정해야 합니다. 이에 대한 지침은 [신뢰 관계 생성](#)에서 확인하실 수 있습니다.

마찬가지로 AWS의 AWS Managed Microsoft AD에서 피어 AWS VPC로 트래픽을 라우팅할 때 IP 주소 정보도 입력해야 합니다(VPC가 퍼블릭 IP 범위를 사용하는 경우).

[신뢰 관계 생성](#)에서 설명한 대로, IP 주소를 추가할 때 [Add routes to the security group for this directory's VPC]를 선택합니다. 아래와 같이 필요한 트래픽을 허용하도록 [보안 그룹](#)을 사전에 사용자 지정하지 않는 한, 반드시 이 옵션을 선택해야 합니다. 자세한 내용은 [디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오](#). 섹션을 참조하세요.

자습서: AWS Managed Microsoft AD 디렉터리와 자체 관리형 Active Directory 도메인 간에 신뢰 관계를 생성합니다

이 자습서에서는 AWS Directory Service for Microsoft Active Directory와 온프레미스 Microsoft Active Directory 간에 신뢰 관계를 설정하는 데 필요한 모든 단계를 안내합니다. 몇 가지 단계만 거치면 신뢰 생성이 가능하지만, 먼저 다음 필수 선행 단계를 완료해야 합니다.

주제

- [필수 조건](#)
- [1단계: 자체 관리형 AD 도메인 준비](#)
- [2단계: AWS Managed Microsoft AD 준비](#)
- [3단계: 신뢰 관계 만들기](#)

참고 항목

[신뢰 관계 생성](#)

필수 조건

이 자습서에서는 다음을 이미 완료했다고 가정합니다.

Note

AWS Managed Microsoft AD는 [단일 레이블 도메인](#)과의 신뢰를 지원하지 않습니다.

- AWS에 생성된 AWS Managed Microsoft AD 디렉터리. 이와 관련해 도움이 필요할 경우 [AWS 매니지드 마이크로소프트 AD 시작하기](#)를 참조하세요.
- Windows를 실행하는 EC2 인스턴스가 해당 AWS Managed Microsoft AD에 추가되어 있습니다. 이와 관련해 도움이 필요할 경우 [Amazon EC2 Windows 인스턴스를 관리형 AWS Microsoft AD에 수동으로 조인합니다. Active Directory](#)를 참조하세요.

Important

AWS Managed Microsoft AD를 위한 관리자 계정은 이 인스턴스에 관리자 권한으로 액세스할 수 있어야 합니다.

- 다음 Windows Server 도구들이 해당 인스턴스에 설치되어 있습니다.
 - AD DS 및 AD LDS 도구
 - DNS

이와 관련해 도움이 필요할 경우 [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)를 참조하세요.

- 자체 관리형(온프레미스) Microsoft Active Directory

이 디렉터리에 관리자로서 액세스할 수 있는 권한을 가지고 있어야 합니다. 위에 나열된 것과 동일한 Windows Server 도구들을 이 디렉터리에서 사용할 수 있어야 합니다.

- 자체 관리형 네트워크와 AWS Managed Microsoft AD가 포함된 VPC 간의 활성 연결. 이와 관련해 도움이 필요하면 [Amazon 가상 프라이빗 클라우드 연결 옵션](#)을 참조하세요.
- 올바르게 설정된 로컬 보안 정책. Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously를 점검하여 다음과 같이 명명된 파이프가 3개 이상 포함되어 있는지 확인합니다.
 - netlogon
 - samr
 - lsarpc
- NetBIOS와 도메인 이름은 고유해야 하며 신뢰 관계를 설정하기 위해 동일할 수 없습니다

신뢰 관계를 만들기 위한 사전 조건에 대한 자세한 내용은 [신뢰 관계 생성](#) 단원을 참조하세요.

자습서 구성

이 자습서에서는 이미 AWS Managed Microsoft AD와 자체 관리형 도메인을 만들었습니다. 자체 관리형 네트워크는 AWS Managed Microsoft AD의 VPC에 연결됩니다. 다음은 두 디렉터리의 속성입니다.

AWS에서 실행되는 AWS Managed Microsoft AD

- 도메인 이름(FQDN): MyManagedAD.example.com
- NetBIOS 이름: MyManagedAD
- DNS 주소: 10.0.10.246, 10.0.20.121
- VPC CIDR: 10.0.0.0/16

AWS Managed Microsoft AD는 VPC ID인 vpc-12345678에 있습니다.

자체 관리형 또는 AWS Managed Microsoft AD 도메인

- 도메인 이름(FQDN): corp.example.com
- NetBIOS 이름: CORP
- DNS 주소: 172.16.10.153
- 자체 관리형 CIDR: 172.16.0.0/16

다음 단계

[1단계: 자체 관리형 AD 도메인 준비](#)

1단계: 자체 관리형 AD 도메인 준비

먼저 자체 관리형(온프레미스) 도메인에서 몇 가지 사전 조건 단계를 완료해야 합니다.

자체 관리형 방화벽 구성

관리형 Microsoft AD가 포함된 VPC에서 사용하는 모든 서브넷의 CIDR에 대해 다음 포트가 열리도록 자체 관리형 방화벽을 구성해야 합니다. AWS 이 자습서에서는 다음 포트에서 10.0.0.0/16 (관리형 AWS Microsoft AD VPC의 CIDR 블록) 에서 들어오는 트래픽과 나가는 트래픽을 모두 허용합니다.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 인증
- TCP/UDP 389 - 경량 디렉터리 액세스 프로토콜 (LDAP)
- TCP 445 - 서버 메시지 블록 (SMB)
- TCP 9389 - Active Directory 웹 서비스 (ADWS) (선택 사항 - AWS Amazon 또는 Amazon과 같은 애플리케이션에서 인증할 때 전체 도메인 이름 대신 NetBIOS 이름을 사용하려면 이 포트를 열어야 합니다.) WorkDocs QuickSight

Note

더 이상 SMBv1이 지원되지 않습니다.

이들은 자체 관리형 디렉터리에 VPC를 연결하기 위해 필요한 최소 포트입니다. 특정 구성에서는 추가 포트를 개방해야 하는 경우도 있습니다.

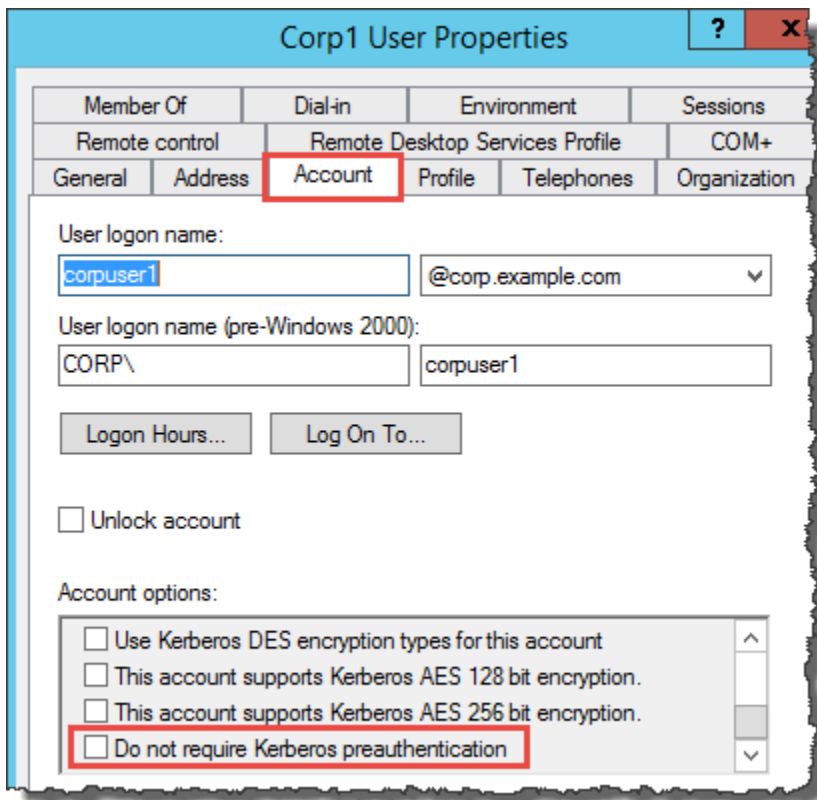
Kerberos 사전 인증이 활성화되었는지 확인

두 디렉터리 모두의 사용자 계정이 Kerberos 사전 인증을 활성화해야 합니다. 이것이 기본 설정이지만, 변경되지 않았는지 확인하기 위해 임의 사용자의 속성을 확인합니다.

사용자의 Kerberos 설정을 보려면

1. 자체 관리형 도메인 컨트롤러에서 서버 관리자를 엽니다.
2. [Tools] 메뉴에서 [Active Directory Users and Computers]를 선택합니다.

3. 사용자 폴더를 선택해 컨텍스트 메뉴를 엽니다(마우스 오른쪽 버튼 클릭). 오른쪽 창에 나열된 임의의 사용자 계정을 선택합니다. 속성을 선택합니다.
4. [Account] 탭을 선택합니다. [Account options] 목록을 아래로 스크롤해서 [Do not require Kerberos preauthentication]가 선택되지 않았는지 확인합니다.



자체 관리형 도메인을 위한 DNS 조건부 전달자 구성

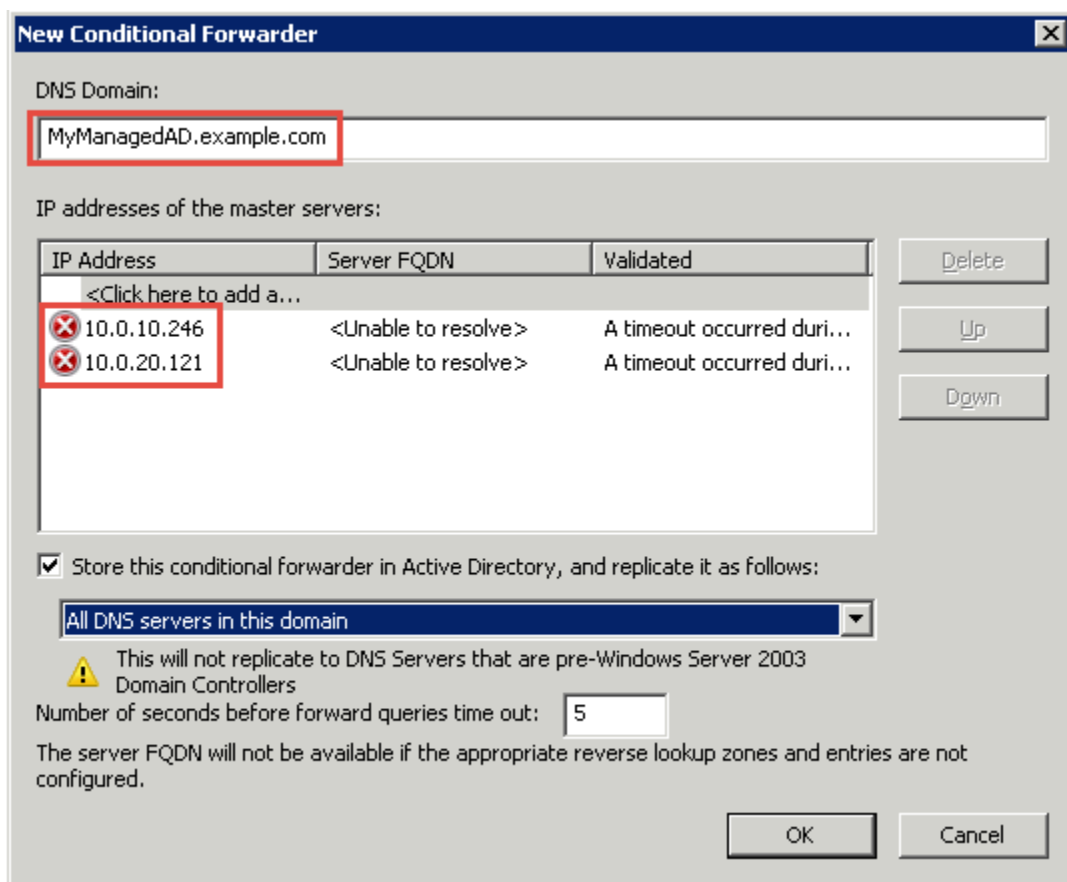
각 도메인에서 DNS 조건부 전달자를 설정해야 합니다. 자체 관리형 도메인에서 이 작업을 수행하기 전에 먼저 관리형 Microsoft AD에 대한 몇 가지 정보를 얻게 됩니다. AWS

자체 관리형 도메인에서 조건부 전달자를 구성하려면

1. AWS Management Console 로그인하고 [AWS Directory Service 콘솔](#)을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. AWS 관리형 Microsoft AD의 디렉터리 ID를 선택합니다.
4. 세부 정보 페이지에 표시된 디렉터리 이름의 값과 디렉터리의 DNS 주소를 적어둡니다.
5. 이제 자체 관리형 도메인 컨트롤러로 돌아갑니다. 서버 관리자를 엽니다.
6. [Tools] 메뉴에서 [DNS]를 선택합니다.

7. 콘솔 트리에서 신뢰를 설정 중인 도메인의 DNS 서버를 확장합니다. 서버는 WIN-5V70CN7VJ0.corp.example.com입니다.
8. 콘솔 트리에서 [Conditional Forwarders]를 선택합니다.
9. [Action] 메뉴에서 [New conditional forwarder]를 선택합니다.
10. DNS 도메인에는 앞서 언급한 관리형 AWS Microsoft AD의 FQDN (정규화된 도메인 이름) 을 입력합니다. 이 예시에서는 FQDN이 AD.Example.com입니다. MyManaged
11. 마스터 서버의 IP 주소를 선택하고 앞서 언급한 AWS 관리형 Microsoft AD 디렉터리의 DNS 주소를 입력합니다. 이 예제에서 DNS 주소는 10.0.10.246, 10.0.20.121입니다.

DNS 주소를 입력하고 나면 "timeout" 또는 "unable to resolve"라는 오류 메시지가 나타날 수 있습니다. 보통 이러한 오류 메시지는 무시해도 좋습니다.



12. [Store this conditional forwarder in Active Directory, and replicate it as follows]를 선택합니다.
13. [All DNS servers in this domain]을 선택하고 [OK]를 선택합니다.

다음 단계

[2단계: AWS Managed Microsoft AD 준비](#)

2단계: AWS Managed Microsoft AD 준비

이제 신뢰할 수 있는 관계를 구축할 수 있도록 AWS 관리형 Microsoft AD를 준비해 보겠습니다. 다음 단계들은 자체 관리형 도메인에서 완료한 단계들과 거의 동일합니다. 하지만 이번에는 AWS 관리형 Microsoft AD를 사용하고 계실 것입니다.

VPC 서브넷 및 보안 그룹 구성

자체 관리형 네트워크에서 관리형 Microsoft AD가 포함된 AWS VPC로의 트래픽을 허용해야 합니다. 이렇게 하려면 Managed AWS Microsoft AD를 배포하는 데 사용되는 서브넷과 연결된 ACL과 도메인 컨트롤러에 구성된 보안 그룹 규칙이 모두 트러스트를 지원하는 데 필요한 트래픽을 허용하는지 확인해야 합니다.

포트 요구 사항은 신뢰 관계를 사용하게 될 서비스나 애플리케이션, 도메인 컨트롤러가 사용하는 Windows Server 버전에 따라 크게 달라집니다. 이 자습서 목적 상 지금은 다음 포트를 엽니다.

인바운드

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 인증
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Kerberos 인증
- TCP 636 - LDAPS(LDAP over TLS/SSL)
- TCP 3268-3269 - 글로벌 카탈로그
- TCP/UDP 49152-65535 - RPC용 휘발성 포트

Note

더 이상 SMBv1이 지원되지 않습니다.

아웃바운드

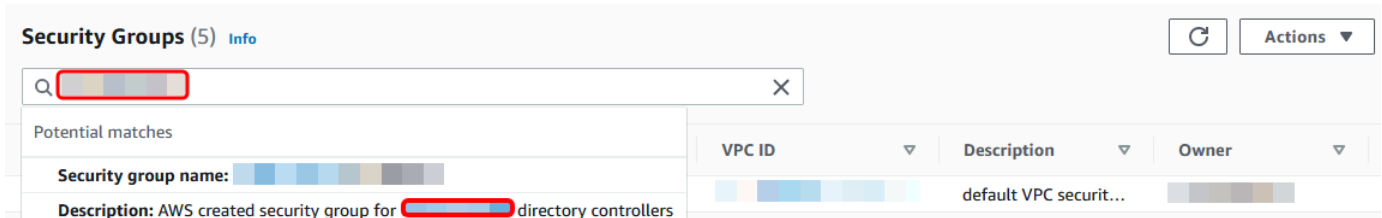
- ALL

Note

이들은 VPC와 자체 관리형 디렉터리를 연결하기 위해 필요한 최소 포트입니다. 특정 구성에서는 추가 포트를 개방해야 하는 경우도 있습니다.

AWS 관리형 Microsoft AD 도메인 컨트롤러 아웃바운드 및 인바운드 규칙을 구성하려면

1. [AWS Directory Service 콘솔](#)로 돌아갑니다. 디렉터리 목록에서 AWS 관리형 Microsoft AD 디렉터리의 디렉터리 ID를 기록해 둡니다.
2. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
3. 탐색 창에서 보안 그룹(Security Groups)을 선택합니다.
4. 검색 상자를 사용하여 AWS 관리형 Microsoft AD 디렉터리 ID를 검색할 수 있습니다. 검색 결과에서 설명이 포함된 보안 그룹을 선택합니다 **AWS created security group for *yourdirectoryID* directory controllers.**



5. 해당 보안 그룹의 [Outbound Rules] 탭으로 이동합니다. 아웃바운드 규칙 편집을 선택한 다음 규칙 추가를 선택합니다. 새 규칙에서 아래 값을 입력합니다.
 - [Type]: 모든 트래픽
 - [Protocol]: 모두
 - [Destination]은 도메인 컨트롤러에서 나가는 트래픽과 트래픽 대상을 결정합니다. 단일 IP 주소 또는 CIDR 표기법으로 된 IP 주소 범위(예: 203.0.113.5/32)를 지정합니다. 또한 동일 리전 내 다른 보안 그룹의 이름이나 ID를 지정할 수도 있습니다. 자세한 정보는 [디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오.](#)을 참조하세요.
6. 규칙 저장을 선택합니다.

Edit outbound rulesinfo

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rulesinfo

Security group rule ID	Type	Protocol	Port range	Destination	Description - optional	
	All traffic	All	All	Anywhere...		Delete

0.0.0.0/0 X

Add rule

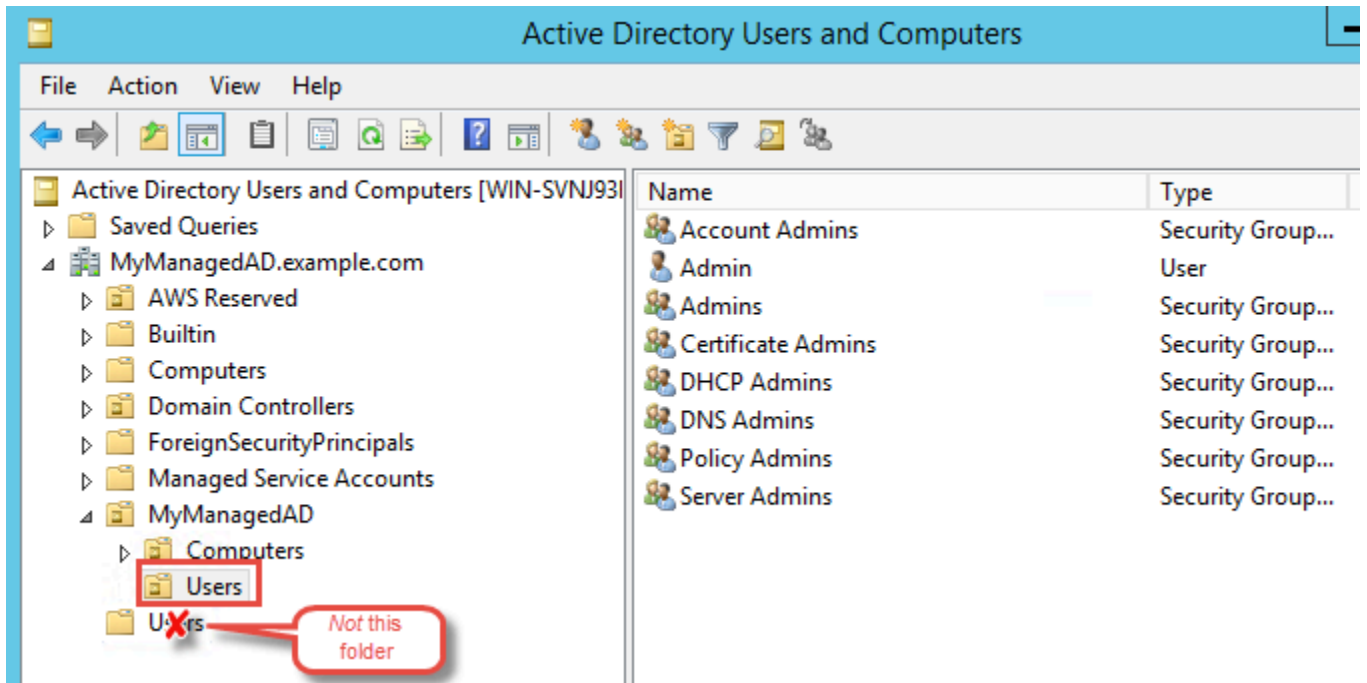
Cancel Preview changes **Save rules**

Kerberos 사전 인증이 활성화되었는지 확인

이제 AWS 관리형 Microsoft AD의 사용자에게도 Kerberos 사전 인증이 활성화되어 있는지 확인해야 합니다. 자체 관리형 디렉터리에서 완료한 것과 동일한 프로세스입니다. 이것이 기본 설정이지만, 어떤 것도 변경되지 않았는지 확인합니다.

사용자 Kerberos 설정을 보려면

1. 도메인용 또는 도메인의 사용자 관리 권한을 위임받은 계정을 사용하여 AWS Managed Microsoft AD 디렉터리의 구성원인 인스턴스에 로그인합니다. [관리자 계정에 대한 권한](#)
2. 아직 설치가 되지 않았다면 Microsoft Active Directory 사용자 및 컴퓨터 도구와 DNS 도구를 설치합니다. [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)에서 이들 도구를 설치하는 방법을 확인합니다.
3. 서버 관리자를 엽니다. [Tools] 메뉴에서 [Active Directory Users and Computers]를 선택합니다.
4. 도메인에서 [Users] 폴더를 선택합니다. 이는 NetBIOS 이름 아래에 있는 사용자 폴더이며 FQDN(정규화된 도메인 이름) 아래에 있는 사용자 폴더가 아니라는 점에 유의하세요.



5. 사용자 목록에서 사용자를 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.
6. [Account] 탭을 선택합니다. [Account options] 목록에서 [Do not require Kerberos preauthentication]가 선택되지 않았는지 확인합니다.

다음 단계

3단계: 신뢰 관계 만들기

3단계: 신뢰 관계 만들기

준비 작업이 완료되었으므로 마지막 단계로 신뢰 관계를 설정합니다. 먼저 자체 관리형 도메인에서 신뢰 관계를 생성한 다음 AWS Managed Microsoft AD에 신뢰 관계를 생성합니다. 신뢰 관계를 생성하는 과정에서 문제가 발생한 경우에는 [신뢰 생성 상태 이유](#)를 참조하세요.

자체 관리형 Active Directory에 신뢰 관계 구성

이 자습서에서는 양방향 포리스트 신뢰를 구성합니다. 하지만 단방향 포리스트 신뢰를 설정하는 경우에는 각 도메인의 신뢰 방향이 상호 보완적이라는 점에 유의하세요. 예를 들어 한 자체 관리형스 도메인에서 단방향 아웃바운드 신뢰 관계를 설정했다면 AWS Managed Microsoft AD에서는 단방향 인바운드 신뢰를 설정해야 합니다.

Note

AWS Managed Microsoft AD는 외부 신뢰 관계도 지원합니다. 그렇지만 이 자습서의 목적상 여기에서는 양방향 포리스트 신뢰만 구성합니다.

자체 관리형 Active Directory에서 신뢰를 구성하려면

1. 서버 관리자를 열고 [Tools] 메뉴에서 [Active Directory Domains and Trusts]를 선택합니다.
2. 도메인에 대한 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼을 클릭) [Properties]를 선택합니다.
3. [Trusts] 탭을 선택하고 [New trust]를 선택합니다. AWS Managed Microsoft AD의 이름을 입력하고 다음을 선택합니다.
4. [Forest trust]를 선택합니다. 다음을 선택합니다.
5. [Two-way]를 선택합니다. 다음을 선택합니다.
6. [This domain only]를 선택합니다. 다음을 선택합니다.
7. [Forest-wide authentication]을 선택합니다. 다음을 선택합니다.
8. [Trust password]를 입력합니다. AWS Managed Microsoft AD에서 신뢰 관계를 설정할 때 필요하므로 이 암호를 반드시 기억해야 합니다.
9. 다음 대화 상자에서 설정을 확인하고 [Next]를 선택합니다. 신뢰 관계가 성공적으로 설정되었는지 확인하고 다시 [Next]를 선택합니다.
10. [No, do not confirm the outgoing trust]를 선택합니다. 다음을 선택합니다.
11. [No, do not confirm the incoming trust]를 선택합니다. 다음을 선택합니다.

AWS Managed Microsoft AD 디렉터리에서 신뢰 관계 구성

마지막으로 AWS Managed Microsoft AD 디렉터리에서 포리스트 신뢰 관계를 구성합니다. 자체 관리형 도메인에서 양방향 포리스트 신뢰 관계를 생성했으므로 AWS Managed Microsoft AD 디렉터를 사용해 양방향 신뢰 관계도 생성합니다.

Note

신뢰 관계는 AWS Managed Microsoft AD의 글로벌 기능입니다. [다중 리전 복제](#)를 사용하는 경우 [기본 리전](#)에서 다음 절차를 수행해야 합니다. 변경은 복제된 모든 리전에 자동으로 적용됩니다. 자세히 알아보려면 [글로벌 기능과 리전별 기능 비교](#)의 내용을 참조하세요.

AWS Managed Microsoft AD 디렉터리에 신뢰 관계를 구성하는 방법

1. [AWS Directory Service 콘솔](#)로 돌아갑니다.
2. 디렉터리 페이지에서 AWS Managed Microsoft AD ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세히 알아보려면 [기본 리전과 추가 리전의 비교](#)의 내용을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 신뢰 관계 섹션에서 작업을 선택한 후 신뢰 관계 추가를 선택합니다.
5. 신뢰 관계 추가 페이지에서 신뢰 유형을 지정합니다. 이 경우에는 포리스트 신뢰를 선택합니다. 자체 관리형 도메인의 FQDN을 입력합니다(이 자습서 **corp.example.com**에서는). 자체 관리형 도메인에서 신뢰 관계를 설정할 때 사용한 것과 동일한 신뢰 암호를 입력합니다. 방향을 지정합니다. 이 경우 Two-way를 선택합니다.
6. Conditional forwarder 필드에서 자체 관리형 DNS 서버의 IP 주소를 입력합니다. 이 예에서는 172.16.10.153를 입력합니다.
7. (선택 사항) Add another IP address(다른 IP 주소 추가)를 선택하고 자체 관리형 DNS 서버의 두 번째 IP 주소를 입력합니다. 최대 4개의 DNS 서버를 지정할 수 있습니다.
8. 추가를 선택합니다.

축하합니다. 이제 자체 관리형 도메인 (corp.example.com) 과 관리형 AWS Microsoft AD (AD.example.com) 간에 신뢰 관계가 생겼습니다. MyManaged 이 둘 두 도메인 간에 오직 한 개의 관계만 설정할 수 있습니다. 예를 들어 신뢰 방향을 단방향으로 변경하고 싶은 경우에는 먼저 기존의 신뢰 관계를 삭제하고 새 관계를 설정해야 합니다.

지침을 포함해 신뢰 확인 또는 삭제에 대한 자세한 내용은 [신뢰 관계 생성](#)를 참조하세요.

자습서: 두 AWS Managed Microsoft AD 도메인 간의 신뢰 관계 만들기

이 자습서에서는 두 AWS Directory Service for Microsoft Active Directory 간에 신뢰 관계를 설정하는데 필요한 모든 단계를 안내합니다.

주제

- [1단계: AWS Managed Microsoft AD 준비](#)
- [2단계: 다른 AWS Managed Microsoft AD 도메인과 신뢰 관계 만들기](#)

참고 항목

[신뢰 관계 생성](#)

1단계: AWS Managed Microsoft AD 준비

이 섹션에서는 관리형 Microsoft AD를 다른 AWS 관리형 Microsoft AD와 신뢰 관계를 맺을 수 있도록 준비할 수 있습니다. 다음 단계 중 다수가 [자습서: AWS Managed Microsoft AD 디렉터리와 자체 관리형 Active Directory 도메인 간에 신뢰 관계를 생성합니다](#)에서 완료한 단계와 거의 동일합니다. 하지만 이번에는 AWS 관리형 Microsoft AD 환경을 서로 연동하도록 구성하고 있습니다.

VPC 서브넷 및 보안 그룹 구성

한 AWS 관리형 Microsoft AD 네트워크에서 다른 AWS 관리형 Microsoft AD를 포함하는 VPC로의 트래픽을 허용해야 합니다. 이렇게 하려면 Managed AWS Microsoft AD를 배포하는 데 사용되는 서브넷과 연결된 ACL과 도메인 컨트롤러에 구성된 보안 그룹 규칙이 모두 트러스트를 지원하는 데 필요한 트래픽을 허용하는지 확인해야 합니다.

포트 요구 사항은 신뢰 관계를 사용하게 될 서비스나 애플리케이션, 도메인 컨트롤러가 사용하는 Windows Server 버전에 따라 크게 달라집니다. 이 자습서 목적 상 지금은 다음 포트를 엽니다.

인바운드

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 인증
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

Note

더 이상 SMBv1이 지원되지 않습니다.

- TCP/UDP 464 - Kerberos 인증
- TCP 636 - LDAPS(LDAP over TLS/SSL)
- TCP 3268-3269 - 글로벌 카탈로그

- TCP/UDP 1024-65535 - RPC용 휘발성 포트

아웃바운드

- ALL

Note

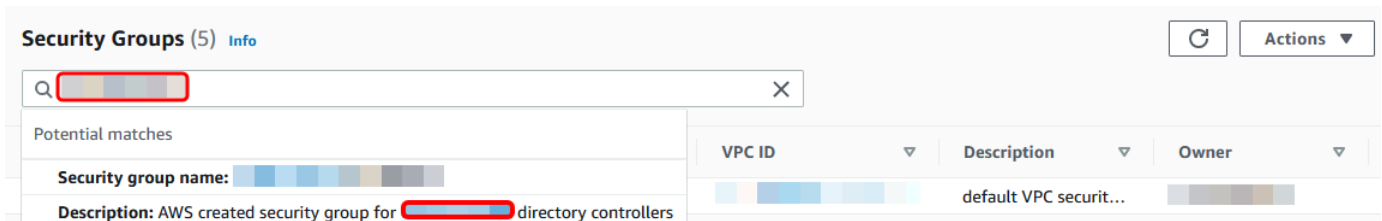
이들 포트는 AWS Managed Microsoft AD에서 모두 VPC를 연결하는 데 필요한 최소 포트입니다. 특정 구성에서는 추가 포트를 개방해야 하는 경우도 있습니다. 자세한 내용은 Microsoft 웹 사이트에서 [Active Directory 도메인 및 신뢰를 위한 방화벽을 구성하는 방법](#)을 참조하세요.

AWS 관리형 Microsoft AD 도메인 컨트롤러 아웃바운드 규칙을 구성하려면

Note

각 디렉터리에 대해 아래의 1~6단계를 반복합니다.

1. [AWS Directory Service 콘솔](#)로 이동합니다. 디렉터리 목록에서 AWS 관리형 Microsoft AD 디렉터리의 디렉터리 ID를 기록해 둡니다.
2. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
3. 탐색 창에서 보안 그룹(Security Groups)을 선택합니다.
4. 검색 상자를 사용하여 AWS 관리형 Microsoft AD 디렉터리 ID를 검색할 수 있습니다. 검색 결과에서 설명이 있는 항목을 선택합니다 **AWS created security group for *yourdirectoryID* directory controllers.**



5. 해당 보안 그룹의 [Outbound Rules] 탭으로 이동합니다. [Edit]를 선택한 후 [Add another rule]을 선택합니다. 새 규칙에서 아래 값을 입력합니다.

- [Type]: 모든 트래픽

- [Protocol]: 모두
- [Destination]은 도메인 컨트롤러에서 나가는 트래픽과 트래픽 대상을 결정합니다. 단일 IP 주소 또는 CIDR 표기법으로 된 IP 주소 범위(예: 203.0.113.5/32)를 지정합니다. 또한 동일 리전 내 다른 보안 그룹의 이름이나 ID를 지정할 수도 있습니다. 자세한 정보는 [디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오](#)을 참조하세요.

6. 저장을 선택합니다.

Edit outbound rules info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules info

Security group rule ID	Type <small>info</small>	Protocol <small>info</small>	Port range <small>info</small>	Destination <small>info</small>	Description - optional <small>info</small>
	All traffic	All	All	Anywhere...	

0.0.0.0/0 X

Add rule

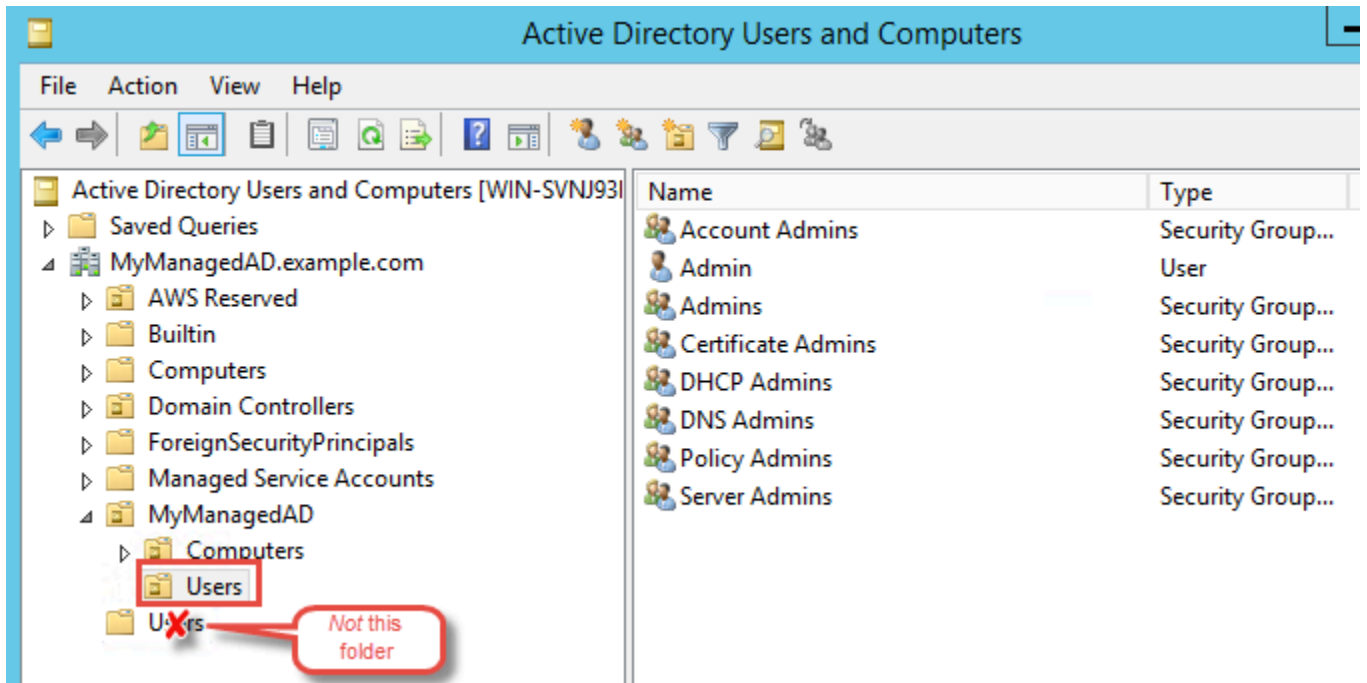
Cancel Preview changes Save rules

Kerberos 사전 인증이 활성화되었는지 확인

이제 AWS 관리형 Microsoft AD의 사용자에게도 Kerberos 사전 인증이 활성화되어 있는지 확인해야 합니다. 온프레미스 디렉터리에서 완료한 것과 동일한 프로세스입니다. 이것이 기본 설정이지만, 어떤 것도 변경되지 않았는지 확인합니다.

사용자 Kerberos 설정을 보려면

1. 도메인용 또는 도메인의 사용자 관리 권한을 위임받은 계정을 사용하여 AWS Managed Microsoft AD 디렉터리의 구성원인 인스턴스에 로그인합니다. [관리자 계정에 대한 권한](#)
2. 아직 설치가 되지 않았다면 Microsoft Active Directory 사용자 및 컴퓨터 도구와 DNS 도구를 설치합니다. [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#)에서 이들 도구를 설치하는 방법을 확인합니다.
3. 서버 관리자를 엽니다. [Tools] 메뉴에서 [Active Directory Users and Computers]를 선택합니다.
4. 도메인에서 [Users] 폴더를 선택합니다. 이는 NetBIOS 이름 아래에 있는 사용자 폴더이며 FQDN(정규화된 도메인 이름) 아래에 있는 사용자 폴더가 아니라는 점에 유의하세요.



5. 사용자 목록에서 사용자를 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.
6. [Account] 탭을 선택합니다. [Account options] 목록에서 [Do not require Kerberos preauthentication]가 선택되지 않았는지 확인합니다.

다음 단계

2단계: 다른 AWS Managed Microsoft AD 도메인과 신뢰 관계 만들기

2단계: 다른 AWS Managed Microsoft AD 도메인과 신뢰 관계 만들기

준비 작업이 완료되었으므로 마지막 단계는 두 AWS Managed Microsoft AD 도메인 간의 신뢰 관계를 만드는 것입니다. 신뢰 관계를 생성하는 과정에서 문제가 발생한 경우에는 [신뢰 생성 상태 이유](#)를 참조하세요.

첫 번째 AWS Managed Microsoft AD 도메인에서 신뢰 관계 구성

이 자습서에서는 양방향 포리스트 신뢰를 구성합니다. 하지만 단방향 포리스트 신뢰를 설정하는 경우에는 각 도메인의 신뢰 방향이 상호 보완적이라는 점에 유의하세요. 예를 들어 이 첫 번째 도메인에서 단방향 아웃바운드 신뢰 관계를 설정했다면 두 번째 AWS Managed Microsoft AD 도메인에서는 단방향 인바운드 신뢰 관계를 설정해야 합니다.

Note

AWS Managed Microsoft AD는 외부 신뢰 관계도 지원합니다. 그렇지만 이 자습서의 목적상 여기에서는 양방향 포리스트 신뢰만 구성합니다.

첫 번째 AWS Managed Microsoft AD 도메인에서 신뢰 관계 구성

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. 디렉터리 페이지에서 첫 번째 AWS Managed Microsoft AD ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 Networking & security(네트워킹 및 보안) 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 Networking & security(네트워킹 및 보안) 탭을 선택합니다.
4. 신뢰 관계 섹션에서 작업을 선택한 후 신뢰 관계 추가를 선택합니다.
5. 신뢰 관계 추가 페이지에서 두 번째 AWS Managed Microsoft AD 도메인의 FQDN을 입력합니다. AWS Managed Microsoft AD에서 신뢰 관계를 설정할 때 필요하므로 이 암호를 반드시 기억해야 합니다. 방향을 지정합니다. 이 경우 Two-way를 선택합니다.
6. Conditional forwarder 필드에서 두 번째 AWS Managed Microsoft AD DNS 서버의 IP 주소를 입력합니다.
7. (선택 사항) Add another IP address(다른 IP 주소 추가)를 선택하고 두 번째 AWS Managed Microsoft AD DNS 서버의 두 번째 IP 주소를 입력합니다. 최대 4개의 DNS 서버를 지정할 수 있습니다.
8. 추가(Add)를 선택합니다. 이 시점에서 신뢰는 신뢰 관계의 반대편을 만들 때까지 실패할 것으로 예상됩니다.

두 번째 AWS Managed Microsoft AD 도메인에서 신뢰 관계 구성

마지막으로 AWS Managed Microsoft AD 디렉터리에서 포리스트 신뢰 관계를 구성합니다. 첫 번째 AWS Managed Microsoft AD 도메인에서 양방향 포리스트 신뢰 관계를 만들었으므로 이 AWS Managed Microsoft AD 도메인을 사용하여 양방향 신뢰관계도 만듭니다.

두 번째 AWS Managed Microsoft AD 도메인에서 신뢰 관계 구성

1. [AWS Directory Service 콘솔](#)로 돌아갑니다.
2. 디렉터리 페이지에서 두 번째 AWS Managed Microsoft AD ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 Networking & security(네트워킹 및 보안) 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 Networking & security(네트워킹 및 보안) 탭을 선택합니다.
4. 신뢰 관계 섹션에서 작업을 선택한 후 신뢰 관계 추가를 선택합니다.
5. 신뢰 관계 추가 페이지에서 첫 번째 AWS Managed Microsoft AD 도메인의 FQDN을 입력합니다. 온프레미스 도메인에서 신뢰 관계를 설정할 때 사용한 것과 동일한 신뢰 암호를 입력합니다. 방향을 지정합니다. 이 경우 Two-way를 선택합니다.
6. Conditional forwarder 필드에서 첫 번째 AWS Managed Microsoft AD DNS 서버의 IP 주소를 입력합니다.
7. (선택 사항) Add another IP address(다른 IP 주소 추가)를 선택하고 첫 번째 AWS Managed Microsoft AD DNS 서버의 두 번째 IP 주소를 입력합니다. 최대 4개의 DNS 서버를 지정할 수 있습니다.
8. 추가(Add)를 선택합니다. 신뢰는 잠시 후 확인되어야 합니다.
9. 이제 첫 번째 도메인에서 만든 신뢰로 돌아가서 신뢰 관계를 다시 확인합니다.

축하합니다. 이제 두 개의 AWS Managed Microsoft AD 도메인 간에 신뢰 관계가 생겼습니다. 이들 두 도메인 간에 오직 한 개의 관계만 설정할 수 있습니다. 예를 들어 신뢰 방향을 단방향으로 변경하고 싶은 경우에는 먼저 기존의 신뢰 관계를 삭제하고 새 관계를 설정해야 합니다.

AWS 관리형 Microsoft AD를 다음으로 연결하세요. Microsoft Entra Connect Sync

이 자습서에서는 AWS 관리형 Microsoft AD에 [Microsoft Entra Connect Sync](#) 동기화하기 위해 설치하는 [Microsoft Entra ID](#) 데 필요한 단계를 안내합니다.

이 자습서에서는 다음 작업을 수행합니다.

1. AWS 관리형 Microsoft AD 도메인 사용자를 생성합니다.

2. Entra Connect Sync를 다운로드합니다.
3. 스크립트를 Windows PowerShell 실행하여 새로 만든 사용자에게 적절한 권한을 제공하는 데 사용합니다.
4. Entra Connect Sync을 설치합니다.

필수 조건

이 자습서를 완료하려면 다음이 필요합니다.

- AWS 관리형 마이크로소프트 AD. 자세한 정보는 [the section called “AWS 관리형 Microsoft AD 만들기”](#)을 참조하세요.
- 관리형 AWS 마이크로소프트 AD에 연결된 Amazon EC2 Windows 서버 인스턴스. 자세한 정보는 [Windows 인스턴스에 원활하게 조인을](#) 참조하세요.
- AWS 관리형 Microsoft AD를 관리하기 위해 Active Directory Administration Tools 설치된 EC2 Windows 서버 자세한 정보는 [the section called “AWS 관리형 Microsoft AD용 AD 관리 도구 설치”](#)을 참조하세요.

1단계: Active Directory 도메인 사용자 생성

이 자습서에서는 AWS 관리형 Microsoft AD와 EC2 Windows 서버 인스턴스가 이미 설치되어 있다고 가정합니다. Active Directory Administration Tools 자세한 정보는 [the section called “AWS 관리형 Microsoft AD용 AD 관리 도구 설치”](#)을 참조하세요.

1. 설치된 인스턴스에 연결합니다. Active Directory Administration Tools
2. AWS 관리형 Microsoft AD 도메인 사용자를 생성합니다. 이 사용자가 Fors가 Active Directory Directory Service (AD DS) Connector account 됩니다Entra Connect Sync. 이 프로세스에 대한 자세한 단계는 을 참조하십시오[the section called “사용자 생성”](#).

2단계: 다운로드 Entra Connect Sync

- [Microsoft웹 Entra Connect Sync](#) 사이트에서 AWS 관리형 Microsoft AD 관리자인 EC2 인스턴스로 다운로드합니다.

⚠ Warning

Entra Connect Sync 지금은 열거나 실행하지 마십시오. 다음 단계에서는 1단계에서 생성한 도메인 사용자에게 필요한 권한을 제공합니다.

3단계: Windows PowerShell 스크립트 실행

- [PowerShell관리자로 열고](#) 다음 스크립트를 실행합니다. 스크립트가 실행되는 동안 1단계에서 새로 만든 도메인 사용자의 [AccountNameSaM](#)을 입력하라는 메시지가 표시됩니다.

```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig\AdSyncConfig.psm1"

try {
    # Attempt to import the module
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
    Import-Module $modulePath -ErrorAction Stop
    Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'
```



```

Try {
    $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
'DistinguishedName'
} Catch [System.Exception] {
    Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
}

Try {
    $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
Stop | Select-Object -ExpandProperty 'DistinguishedName'
} Catch [System.Exception] {
    Write-Output "Failed to get service account DN $_"
}

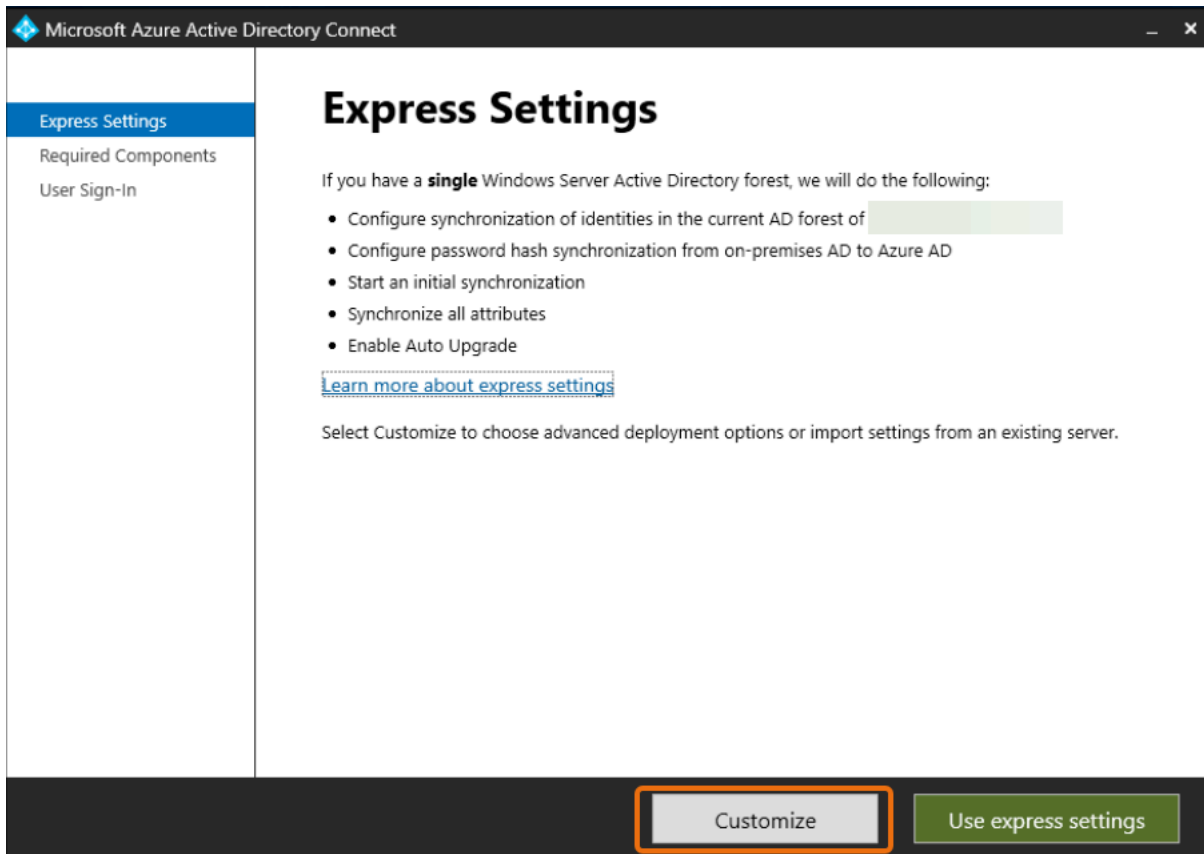
Foreach ($OU in $OUs) {
    try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
$ADConnectorAccountDN -ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
$ADConnectorAccountDN on OU $OU : $_"
    }
}
}

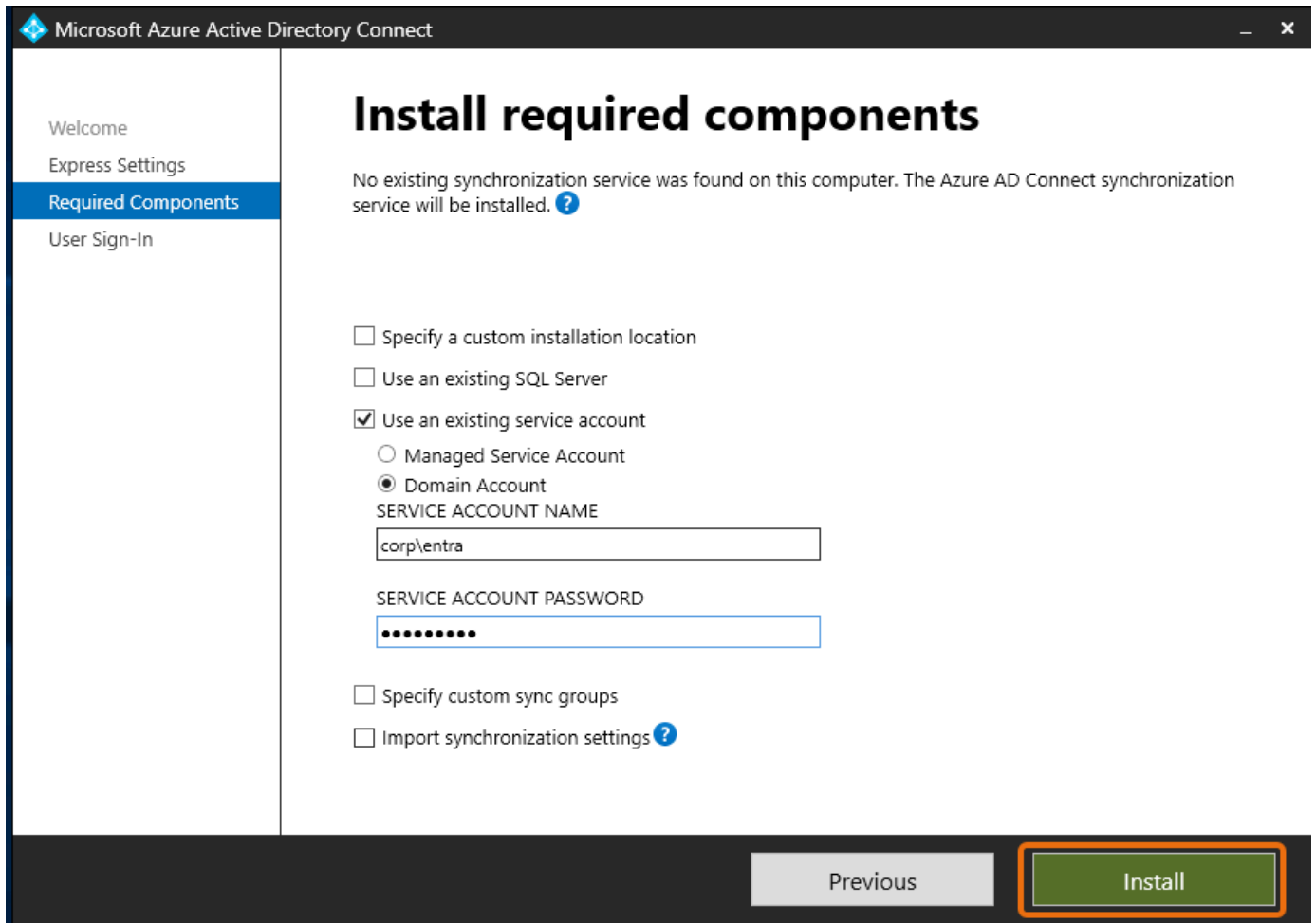
```

4단계: 설치 Entra Connect Sync

1. 스크립트가 완료되면 다운로드한 Microsoft Entra Connect (이전 명칭 Azure Active Directory Connect) 구성 파일을 실행할 수 있습니다.
2. 이전 단계의 구성 파일을 실행한 후 Microsoft Azure Active Directory Connect 창이 열립니다. 익스프레스 설정 창에서 사용자 지정을 선택합니다.

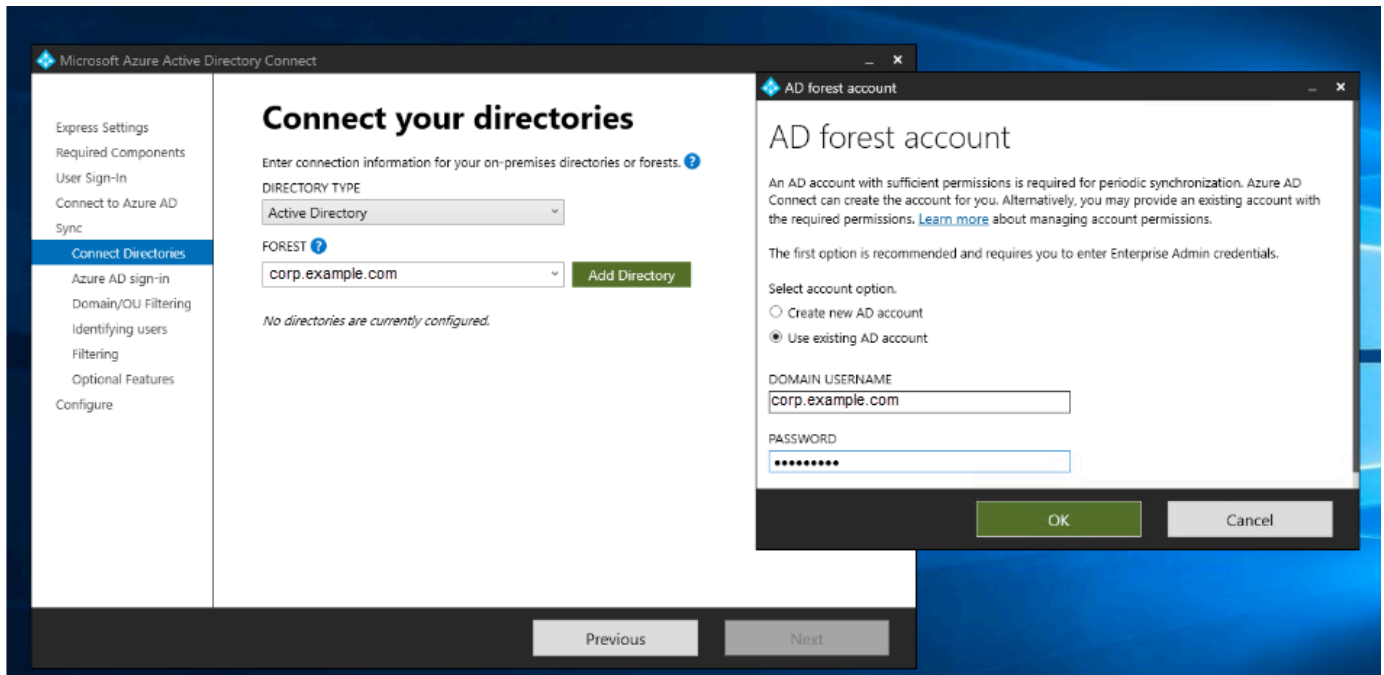


- 필수 구성 요소 설치 창에서 기존 서비스 계정 사용 확인란을 선택합니다. 서비스 계정 이름 및 서비스 계정 암호에 1단계에서 만든 사용자의 AD DS Connector account 이름과 암호를 입력합니다. 예를 들어, AD DS Connector account 이름이 인 entra 경우 계정 이름은 다음과 같습니다corp\entra. 그런 다음 설치를 선택합니다.



4. 사용자 로그인 창에서 다음 옵션 중 하나를 선택합니다.
 - a. [패스스루 인증](#) - 이 옵션을 사용하면 사용자 이름과 Active Directory 비밀번호로 로그인할 수 있습니다.
 - b. 구성 안 함 - 이렇게 하면 페더레이션 로그인 Microsoft Entra (이전 명칭 (AD)) 을 사용하거나 사용할 수 있습니다. Azure Active Directory Azure Office 365

그런 후 다음을 선택합니다.
5. Connect to Azure 창에서 [글로벌 관리자](#) 사용자 이름과 암호를 입력하고 다음을 선택합니다.
Entra ID
6. 디렉터리 연결 창에서 디렉터리 유형을 선택합니다 Active Directory. FOREST용 AWS 관리형 Microsoft AD의 포리스트를 선택하십시오. 그런 다음 디렉터리 추가를 선택합니다.
7. 계정 옵션을 요청하는 팝업 상자가 나타납니다. 기존 AD 계정 사용을 선택합니다. 1단계에서 만든 AD DS Connector account 사용자 이름과 암호를 입력한 다음 확인을 선택합니다. 그런 후 다음을 선택합니다.



8. Azure AD로그인 창에서 확인된 베니티 도메인이 추가되지 않은 경우에만 모든 UPN 접미사를 확인된 도메인과 일치시키지 않고 계속을 선택합니다. Entra ID 그런 후 다음을 선택합니다.
9. 도메인/OU 필터링 창에서 필요에 맞는 옵션을 선택합니다. 자세한 내용은 설명서의 [필터링 구성을 Entra Connect Sync 참조하십시오](#). Microsoft 그런 후 다음을 선택합니다.
10. 사용자 식별, 필터링 및 선택적 기능 창에서 기본값을 유지하고 다음을 선택합니다.
11. 구성 창에서 구성 설정을 검토하고 구성을 선택합니다. 설치 Entra Connect Sync 양식이 완료되고 사용자가 동기화하기 시작합니다. Microsoft Entra ID

스키마 확장

AWS Managed Microsoft AD는 디렉터리 데이터가 저장되는 방법을 구성하고 시행하기 위해 스키마를 사용합니다. 스키마에 정의를 추가하는 프로세스를 “스키마 확장”이라고 합니다. 스키마 확장을 사용하면 올바른 LDIF(LDAP Data Interchange Format) 파일을 사용하여 AWS Managed Microsoft AD 디렉터리의 스키마를 수정할 수 있습니다. AD 스키마와 스키마 확장 방법에 대한 자세한 내용은 아래 나와 있는 주제들을 참조하세요.

주제

- [AWS Managed Microsoft AD 스키마를 확장해야 하는 경우](#)
- [자습서: AWS 관리형 Microsoft AD 스키마 확장](#)

AWS Managed Microsoft AD 스키마를 확장해야 하는 경우

새 객체 클래스와 속성을 추가하여 AWS Managed Microsoft AD 스키마를 확장할 수 있습니다. 예를 들어 Single Sign-On 기능을 지원하기 위해 스키마를 변경해야 하는 애플리케이션이 있는 경우에 이렇게 할 수 있습니다.

특정 Active Directory 객체 클래스 및 속성을 사용하는 애플리케이션을 지원하기 위해 스키마 확장을 사용할 수도 있습니다. 이 확장 기능은 AWS Managed Microsoft AD에 의존하는 기업 애플리케이션을 AWS클라우드로 마이그레이션해야 하는 경우에 특히 유용할 수 있습니다.

기존 Active Directory 스키마에 추가되는 각 속성 또는 클래스는 고유 ID를 갖도록 정의해야 합니다. 이런 식으로 기업이 스키마 확장을 수행하면 고유성을 보장하여 상호 충돌을 방지할 수 있습니다. 이러한 ID를 AD 객체 식별자(OID)라고 하며 AWS Managed Microsoft AD에 저장됩니다.

시작하려면 [자습서: AWS 관리형 Microsoft AD 스키마 확장](#) 섹션을 참조하세요.

관련 주제

- [스키마 확장](#)
- [스키마 요소](#)

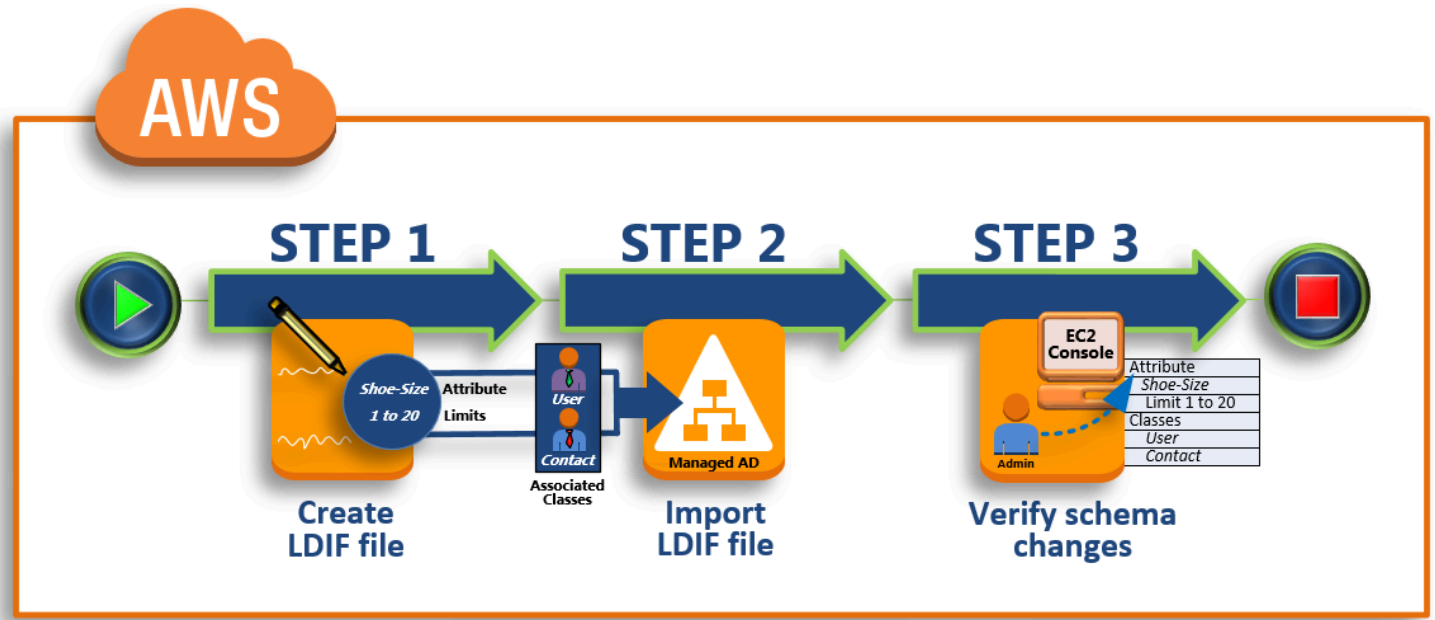
자습서: AWS 관리형 Microsoft AD 스키마 확장

이 자습서에서는 특정 요구 사항을 충족하는 고유한 특성과 클래스를 추가하여 AWS 관리형 Microsoft AD라고도 하는 Microsoft Active Directory 디렉터리용 디렉터리 서비스의 스키마를 확장하는 방법을 알아봅니다. AWS 관리되는 Microsoft AD 스키마 확장은 유효한 LDIF (경량 디렉터리 교환 형식) 스크립트 파일을 사용해서만 업로드하고 적용할 수 있습니다.

속성(attributeSchema)은 데이터베이스의 필드를 정의하고, 클래스(classSchema)는 데이터베이스의 테이블을 정의합니다. 예를 들어 Microsoft Active Directory의 모든 사용자 객체들은 스키마 계층 User가 정의하고, 이메일 주소나 전화 번호 같은 사용자의 개별 속성들은 속성이 각기 정의합니다.

과거에는 신발 사이즈와 같은 새 속성을 추가하고 싶은 경우에 정수 유형의 속성을 새로 정의했습니다. 또한 1~20 같이 하한선과 상한선도 정의할 수 있습니다. 신발 사이즈 attributeSchema 객체가 생성되고 나면 해당 속성이 포함된 사용자 classSchema 객체를 변경했습니다. 속성은 여러 클래스에 링크 연결이 가능합니다. 또한 신발 사이즈를 연락처 같은 클래스에 추가할 수 있습니다. Microsoft Active Directory 스키마에 대한 자세한 내용은 [AWS Managed Microsoft AD 스키마를 확장해야 하는 경우](#)를 참조하세요.

이 워크플로우는 세 가지 기본 단계로 이루어집니다.



1단계: LDIF 파일 생성

먼저, LDIF 파일을 생성하고 새 속성과 속성을 추가해야 하는 클래스를 정의합니다. 워크플로우의 다음 단계에서 이 파일을 사용합니다.

2단계: LDIF 파일 가져오기

이 단계에서는 AWS Directory Service 콘솔을 사용하여 LDIF 파일을 Microsoft Active Directory 환경으로 가져옵니다.

3단계: 스키마 확장이 성공적이었는지 확인

마지막으로 관리자는 EC2 인스턴스를 사용해 새 확장 스키마가 Microsoft Active Directory Schema Snap-in에 나타나는지 확인합니다.

1단계: LDIF 파일 생성

LDIF 파일은 [LDAP](#)(Lightweight Directory Access Protocol) 디렉터리 콘텐츠 및 업데이트 요청을 표현하기 위한 표준 일반 텍스트 데이터 교환 형식입니다. LDIF는 레코드 세트(객체 또는 엔트리당 한 개의 레코드)로서 디렉터리 콘텐츠를 전달합니다. 또한 추가, 수정, 삭제, 이름 바꾸기와 같은 업데이트 요청들을 레코드 세트(업데이트 요청당 한 개의 레코드)로서 표현합니다.

는 관리형 AWS Microsoft AD 디렉터리에서 `ldifde.exe` 응용 프로그램을 실행하여 스키마 변경 사항과 함께 LDIF 파일을 AWS Directory Service 가져옵니다. 따라서 LDIF 스크립트 구문을 이해하는 데 도움이 될 것입니다. 자세한 내용은 [LDIF 스크립트](#)를 참조하세요.

몇몇 타사 LDIF 도구들은 스키마 업데이트를 추출, 정리 및 업데이트할 수 있습니다. 사용하는 도구에 관계 없이 LDIF 파일에서 사용되는 모든 식별자들이 고유해야 한다는 것을 이해하는 것이 중요합니다.

LDIF 파일을 생성하기 앞서 아래의 개념과 팁을 검토하는 것이 좋습니다.

- 스키마 요소 – 속성, 클래스, 객체 ID, 링크 연결된 속성 같은 스키마 요소를 확인합니다. 자세한 정보는 [스키마 요소](#)를 참조하세요.
- 항목 순서 – LDIF 파일의 항목이 레이아웃된 순서가 [DIT\(Directory Information Tree\)](#)를 완벽하게 따르는지 확인합니다. LDIF 파일에 대한 일반적인 시퀀싱 규칙에는 다음 정보가 포함됩니다.
 - 빈 줄로 항목들을 분리합니다.
 - 상위 항목 이후의 하위 항목을 나열합니다.
 - 속성이나 객체 클래스 같은 항목들이 스키마에 존재하는지 확인합니다. 존재하지 않을 경우 먼저 스키마에 추가해야 사용할 수 있습니다. 예를 들어 클래스에 속성을 할당할 수 있으려면 먼저 속성을 생성해야 합니다.
- DN의 형식 – LDIF 파일의 새 명령 각각에 대해 명령의 첫 번째 줄로 고유 이름(DN)을 정의합니다. DN은 Microsoft Active Directory 객체의 트리 내에서 Microsoft Active Directory 객체를 식별하고 디렉터리에 대한 도메인 구성 요소를 포함하고 있어야 합니다. 예를 들어 이 자습서의 디렉터리에 대한 도메인 구성 요소는 DC=example,DC=com입니다.

또한 DN에는 Microsoft Active Directory 객체의 일반 이름(CN)이 포함되어 있어야 합니다. 첫 번째 CN 엔트리는 속성이나 클래스 이름입니다. 그 다음부터는 CN=Schema,CN=Configuration를 사용해야 합니다. 이 CN은 Microsoft Active Directory 스키마를 확장할 수 있도록 해줍니다. 앞서 설명한 바와 같이, Microsoft Active Directory 객체의 콘텐츠를 추가 또는 수정할 수 없습니다. DN을 위한 일반 형식은 다음과 같습니다.

```
dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
```

이 자습서에서 새 신발 사이즈 속성에 대한 DN은 다음과 같을 것입니다.

```
dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
```

- 경고 – 스키마를 확장하기 전에 아래 경고를 검토합니다.
 - Microsoft Active Directory 스키마를 확인하기 앞서 이 작업의 영향에 대해 Microsoft의 경로를 검토하는 것이 중요합니다. 자세한 내용은 [스키마를 확장하기 전에 알아야 할 것](#)을 참조하세요.

- 스키마 속성이나 클래스를 삭제할 수 없습니다. 따라서 실수를 하거나 백업에서 복구를 원하지 않는 경우에는 간단히 객체를 비활성화할 수 있습니다. 자세한 내용은 [기존 클래스 및 속성 비활성화](#)를 참조하세요.
- 에 대한 defaultSecurityDescriptor 변경은 지원되지 않습니다.

LDIF 파일 구성 방법에 대한 자세한 내용과 관리형 Microsoft AD 스키마 확장을 테스트하는 데 사용할 수 있는 샘플 LDIF 파일을 보려면 보안 블로그의 [관리형 AWSAWS Microsoft AD 디렉터리 스키마를 확장하는 방법](#) 문서를 참조하십시오. AWS

다음 단계

[2단계: LDIF 파일 가져오기](#)

2단계: LDIF 파일 가져오기

AWS Directory Service 콘솔에서 LDIF 파일을 가져오거나 API를 사용하여 스키마를 확장할 수 있습니다. 스키마 확장 API로 이런 작업을 하는 방법에 대한 자세한 내용은 [AWS Directory Service API 참조](#) 단원을 참조하세요. 현재로는 AWS가 스키마 업데이트를 직접 수행하기 위해 Microsoft Exchange 같은 외부 애플리케이션을 지원하지 않습니다.

Important

AWS 관리형 Microsoft AD 디렉터리 스키마를 업데이트하면 작업이 되돌릴 수 없습니다. 즉, 일단 새 클래스나 속성이 생성되면 Microsoft Active Directory가 이를 제거하도록 허용하지 않습니다. 그러나 비활성화는 가능합니다.

스키마 변경을 삭제해야 하는 경우에는 이전 스냅샷에서 디렉터리를 복구하는 것도 하나의 방법입니다. 스냅샷을 복구하면 단순히 스키마가 아니라 이전 지점으로 스키마와 디렉터리가 모두 롤백됩니다. 스냅샷의 최대 지원 기간은 180일입니다. 자세한 내용은 Microsoft 웹 사이트에서 [Active Directory의 시스템 상태 백업의 유효 수명](#)을 참조하세요.

업데이트 프로세스가 시작되기 전에 AWS Managed Microsoft AD는 스냅샷을 생성하여 디렉터리의 현재 상태를 보존합니다.

Note

스키마 확장은 AWS 관리형 Microsoft AD의 글로벌 기능입니다. [다중 리전 복제](#)를 사용하는 경우 [기본 리전](#)에서 다음 절차를 수행해야 합니다. 변경은 복제된 모든 리전에 자동으로 적용됩니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)를 참조하세요.

LDIF 파일을 가져오는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - Multi-Region replication(다중 리전 복제)에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 Maintenance(유지 관리) 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - Multi-Region replication(다중 리전 복제)에 표시된 리전이 없는 경우 Maintenance(유지 관리) 탭을 선택합니다.
4. 스키마 확장 섹션에서 작업을 선택한 후 스키마 업로드 및 업데이트를 선택합니다.
5. 대화 상자에서 [Browse]를 클릭하고 유효한 LDIF 파일을 선택한 후 설명을 입력하고 나서 [Update Schema]를 선택합니다.

Important

스키마 확장은 중요한 작업입니다. 개발 또는 테스트 환경의 애플리케이션에서 먼저 테스트를 해보기 전에 프로덕션 환경에서 스키마 업데이트를 적용하지 않도록 합니다.

LDIF 파일이 적용되는 방법

Managed AWS Microsoft AD는 LDIF 파일이 업로드된 후 다음 순서대로 변경 내용을 적용하므로 디렉터리를 오류로부터 보호하기 위한 조치를 취합니다.

1. LDIF 파일을 검사합니다. LDIF 스크립트는 도메인의 모든 개체를 조작할 수 있으므로 Managed AWS Microsoft AD는 업로드 직후 검사를 실행하여 가져오기 작업이 실패하지 않도록 합니다. 여기에는 다음을 확인하기 위한 점검이 포함됩니다.
 - 업데이트할 객체는 스키마 컨테이너에만 보관

- 도메인 컨트롤러(DC) 부분은 LDIF 스크립트가 실행 중인 도메인의 이름과 일치합니다.
2. 디렉터리의 스냅샷을 가져옵니다. 스키마를 업데이트한 후 애플리케이션에서 문제가 발생하는 경우에는 스냅샷을 사용해 디렉터리를 복구할 수 있습니다.
 3. 변경 내용을 단일 DC에 적용합니다. AWS 관리형 Microsoft AD는 DC 중 하나를 분리하고 LDIF 파일의 업데이트를 격리된 DC에 적용합니다. 그런 다음, 스키마 마스터 역할을 할 DC를 하나 선택하고 디렉터리 복제본에서 해당 DC를 제거한 후, Ldifde.exe를 사용해 LDIF 파일을 적용합니다.
 4. 복제는 모든 DC에 이루어집니다. AWS 관리형 Microsoft AD는 격리된 DC를 복제에 다시 추가하여 업데이트를 완료합니다. 이 모든 작업이 진행되는 동안 디렉터리는 중단 없이 애플리케이션에 Microsoft Active Directory 서비스를 계속 제공합니다.

다음 단계

[3단계: 스키마 확장이 성공적이었는지 확인](#)

3단계: 스키마 확장이 성공적이었는지 확인

가져오기 프로세스가 완료되고 나면 스키마 업데이트가 디렉터리에 적용되었는지 반드시 확인합니다. 이는 특히 스키마 업데이트에 상주하는 애플리케이션을 마이그레이션 또는 업데이트하기 전에 중요합니다. 이를 위해 다양한 LDAP 도구를 사용하거나 해당되는 LDAP 명령을 발급하는 테스트 도구를 개발할 수 있습니다.

이 절차에서는 Active Directory 스키마 PowerShell 스냅인을 사용하거나 스키마 업데이트가 적용되었는지 확인합니다. AWS 관리형 Microsoft AD에 도메인으로 가입된 컴퓨터에서 이러한 도구를 실행해야 합니다. 가상 프라이빗 클라우드(VPC)에 액세스하거나 가상 프라이빗 네트워크(VPN) 연결을 통해 온프레미스 네트워크에서 실행 중인 Windows 서버가 여기에 해당될 수 있습니다. Amazon EC2 Windows 인스턴스에서 이러한 도구를 실행할 수도 있습니다([도메인 조인이 원활한 상태에서 새 EC2 인스턴스를 시작하는 방법](#) 참조).

Microsoft Active Directory Schema Snap-in 사용을 확인하는 방법

1. [TechNet](#) 웹 사이트의 지침에 따라 Active Directory 스키마 스냅인을 설치합니다.
2. Microsoft Management Console (MMC)을 열고 디렉터리에서 AD 스키마 트리를 확장합니다.
3. 이전에 수행한 스키마 변경을 찾을 때까지 Classes 및 Attributes 폴더를 탐색합니다.

사용을 확인하려면 PowerShell

1. PowerShell 창을 엽니다.

2. 아래 나와 있는 Get-ADObject cmdlet를 사용해 스키마 변경을 확인합니다. 예:

```
get-adobject -Identity 'CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

옵션 단계

[새 속성에 값 추가 - 선택 사항](#)

새 속성에 값 추가 - 선택 사항

새 특성을 만들고 AWS 관리형 Microsoft AD 디렉터리의 속성에 새 값을 추가하려는 경우 이 선택적 단계를 사용하십시오.

속성에 값을 추가하는 방법

1. Windows PowerShell 명령줄 유틸리티를 열고 다음 명령을 사용하여 새 특성을 설정합니다. 이 예제에서는 특정 컴퓨터에서 새 EC2InstanceID 값을 속성에 추가해 보겠습니다.

```
PS C:\> set-adcomputer -Identity computer name -add @{example-EC2InstanceID = 'EC2 instance ID'}
```

2. 아래 명령을 실행해서 EC2InstanceID 값이 컴퓨터 객체에 추가되었는지 확인할 수 있습니다.

```
PS C:\> get-adcomputer -Identity computer name -Property example-EC2InstanceID
```

관련 리소스

아래 리소스 링크는 Microsoft 웹사이트에 위치에 있으며 관련 정보를 제공합니다.

- [스키마 확장 \(Windows\)](#)
- [Active Directory 스키마 \(Windows\)](#)
- [Microsoft Active Directory 스키마](#)
- [Windows 관리: Microsoft Active Directory 스키마 확장](#)
- [스키마 확장에 대한 제약 \(Windows\)](#)
- [Ldifde](#)

AWS 관리형 Microsoft AD 디렉터리 유지 관리

이 섹션에서는 AWS 관리형 Microsoft AD 환경에 대한 일반적인 관리 작업을 유지 관리하는 방법에 대해 설명합니다.

주제

- [대체 UPN 접미사 추가](#)
- [AWS 관리형 Microsoft AD 삭제](#)
- [디렉터리의 사이트 이름 변경](#)
- [디렉터리 스냅샷 또는 복구](#)
- [AWS 관리형 Microsoft AD를 업그레이드하세요](#)
- [디렉터리 정보 보기](#)

대체 UPN 접미사 추가

AWS Managed Microsoft AD 디렉터리에 대체 UPN(사용자 보안 주체 이름) 접미사를 추가하여 Active Directory(AD) 로그인 이름 관리를 간소화하고 사용자 로그인 환경을 개선할 수 있습니다. 이렇게 하려면 Admin 계정 또는 AWS Delegated User Principal Name Suffix Administrators 그룹의 구성원인 계정으로 로그인되어 있어야 합니다. 이 그룹에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#) 단원을 참조하세요.

대체 UPN 접미사를 추가하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. AWS Managed Microsoft AD 디렉터리에 조인된 Amazon EC2 인스턴스를 찾으세요. 찾은 인스턴스를 선택한 다음 [Connect]를 선택합니다.
3. [Server Manager] 창에서 [Tools]를 선택합니다. 그런 다음 [Active Directory Domains and Trusts]를 선택합니다.
4. 왼쪽 창에서 Active Directory Domains and Trusts(Active Directory 도메인 및 신뢰 관계)를 마우스 오른쪽 버튼으로 클릭한 후 속성을 선택합니다.
5. UPN Suffixes(UPN 접미사) 탭에서 대체 UPN 접미사(예: **sales.example.com**)를 입력합니다. 추가를 선택한 후 적용을 선택합니다.
6. 대체 UPN 접미사를 추가해야 한다면 필요한 UPN 접미사를 얻을 때까지 5단계를 반복합니다.

AWS 관리형 Microsoft AD 삭제

AWS 관리형 Microsoft AD를 삭제하면 디렉터리 데이터와 스냅샷이 모두 삭제되며 복구할 수 없습니다. 디렉터리가 삭제된 후에도 디렉터리에 조인된 모든 인스턴스는 변동 없이 보관됩니다. 그러나 디렉터리 자격 증명을 사용해서 이러한 인스턴스에 로그인할 수 없습니다. 인스턴스에 로컬인 사용자 계정을 통해 이러한 인스턴스에 로그인해야 합니다.

디렉터리를 삭제하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다. 현재 배포된 AWS 리전 위치에 Active Directory 있는지 확인하십시오. 자세한 내용은 [지역 선택](#)을 참조하십시오.
2. 삭제하려는 디렉터리에 대해 활성화된 AWS 응용 프로그램이 없는지 확인하십시오. 활성화된 AWS 응용 프로그램을 사용하면 AWS 관리형 Microsoft AD 또는 Simple AD를 삭제할 수 없습니다.
 - a. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
 - b. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다. AWS 앱 및 서비스 섹션에서 디렉터리에 사용할 수 있는 AWS 애플리케이션을 확인할 수 있습니다.
 - AWS Management Console 액세스를 비활성화합니다. 자세한 정보는 [AWS Management Console 액세스 비활성화](#)을 참조하세요.
 - WorkSpacesAmazon을 비활성화하려면 WorkSpaces 콘솔의 디렉터리에서 서비스 등록을 취소해야 합니다. 자세한 내용은 Amazon WorkSpaces 관리 가이드의 [디렉터리 등록 취소](#)를 참조하십시오.
 - WorkDocsAmazon을 비활성화하려면 Amazon WorkDocs 콘솔에서 Amazon WorkDocs 사이트를 삭제해야 합니다. 자세한 내용은 Amazon WorkDocs 관리 가이드의 [사이트 삭제](#)를 참조하십시오.
 - WorkMailAmazon을 비활성화하려면 Amazon WorkMail 콘솔에서 Amazon WorkMail 조직을 제거해야 합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 [조직 제거](#)를 참조하십시오.
 - Amazon FSx for Windows File Server를 비활성화하려면 도메인에서 Amazon FSx 파일 시스템을 제거해야 합니다. 자세한 내용은 Windows File Server용 Amazon [FSx 사용 설명서의 Windows File Server용 FSx 사용 설명서의 Windows](#) 파일 서버용 FSx 사용을 참조하십시오. Active Directory
 - Amazon 관계형 데이터베이스 서비스를 비활성화하려면 도메인에서 Amazon RDS 인스턴스를 제거해야 합니다. 자세한 내용은 Amazon RDS 사용 설명서의 [도메인에서 DB 인스턴스 관리하기](#) 단원을 참조하세요.

- AWS Client VPN 서비스를 비활성화하려면 Client VPN 엔드포인트에서 디렉터리 서비스를 제거해야 합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Active Directory [인증을](#) 참조하십시오.
- Amazon Connect를 비활성화하려면 Amazon Connect 인스턴스를 삭제해야 합니다. 자세한 정보는 Amazon Connect 관리자 안내서의 [Amazon Connect 인스턴스 삭제하기](#)를 참조하십시오.
- Amazon을 QuickSight 비활성화하려면 Amazon 구독을 취소해야 합니다. QuickSight 자세한 내용은 Amazon QuickSight 사용 설명서의 Amazon QuickSight [계정](#) 해지를 참조하십시오.

Note

삭제하려는 AWS Managed Microsoft AD 디렉터를 사용 AWS IAM Identity Center 중이고 이전에 연결한 적이 있는 경우 삭제하려면 먼저 ID 소스를 변경해야 합니다. 자세한 내용은 IAM Identity Center 사용 설명서의 [ID 소스 변경](#)을 참조하십시오.

3. 탐색 창에서 디렉터를 선택합니다.
4. 삭제할 디렉터리만 선택하고 [Delete]를 클릭합니다. 디렉터를 삭제하는 데 몇 분 정도 걸립니다. 삭제된 디렉터리는 디렉터리 목록에서 제거됩니다.

디렉터리의 사이트 이름 변경

AWS Managed Microsoft AD 디렉터리의 기본 사이트 이름을 변경하여 기존 Microsoft Active Directory(AD) 사이트 이름과 일치시킬 수 있습니다. 이렇게 하면 AWS Managed Microsoft AD에서 온프레미스 디렉터리에 있는 기존 AD 사용자를 더 빨리 검색하고 인증할 수 있습니다. 그 결과 AWS Managed Microsoft AD 디렉터리에 조인한 [Amazon EC2](#) 및 [Amazon RDS for SQL Server](#) 인스턴스와 같이 AWS 리소스에 로그인하는 사용자의 경험이 개선됩니다.

이렇게 하려면 관리자 계정 또는 AWS 위임 사이트 및 서비스 관리자 그룹의 멤버인 계정으로 로그인 되어 있어야 합니다. 이 그룹에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#) 단원을 참조하십시오.

신뢰와 관련하여 사이트 이름을 바꾸는 데 대한 추가 이점은 Microsoft 웹 사이트에서 [Domain Locator Across a Forest Trust\(포리스트 신뢰에서 도메인 로케이터\)](#)를 참조하십시오.

AWS Managed Microsoft AD 사이트 이름을 변경하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. AWS Managed Microsoft AD 디렉터리에 연결된 Amazon EC2 인스턴스를 찾습니다. 찾은 인스턴스를 선택한 다음 [Connect]를 선택합니다.
3. [Server Manager] 창에서 [Tools]를 선택합니다. 그런 다음 [Active Directory Sites and Services]를 선택합니다.
4. 왼쪽 창에 있는 [Sites] 폴더를 펼쳐 사이트 이름(기본값은 Default-Site-Name)을 마우스 오른쪽 버튼으로 클릭한 다음 [Rename]을 선택합니다.
5. 새로운 사이트 이름을 입력하고 [Enter]를 선택합니다.

디렉터리 스냅샷 또는 복구

AWS Directory Service 자동 일일 스냅샷을 제공하고 관리형 AWS Microsoft AD Active Directory에 대한 데이터의 수동 스냅샷을 생성하는 기능을 제공합니다. 이러한 스냅샷을 사용하여 Active Directory를 point-in-time 복원할 수 있습니다. 각 AWS 관리형 Microsoft AD Active Directory에 대한 수동 스냅샷은 5개로 제한됩니다. 이미 제한 값에 도달한 경우에는 기존의 수동 스냅샷 중 하나를 삭제해야만 또 다른 스냅샷을 생성할 수 있습니다. AD Connector 디렉터리의 스냅샷은 가져올 수 없습니다.

Note

스냅샷은 AWS Managed Microsoft AD의 글로벌 기능입니다. [다중 리전 복제](#)를 사용하는 경우 [기본 리전](#)에서 다음 절차를 수행해야 합니다. 변경은 복제된 모든 리전에 자동으로 적용됩니다. 자세히 알아보려면 [글로벌 기능과 리전별 기능 비교](#)의 내용을 참조하세요.

주제

- [디렉터리의 스냅샷 생성](#)
- [스냅샷에서 디렉터리 복원](#)
- [스냅샷 삭제](#)

디렉터리의 스냅샷 생성

스냅샷은 스냅샷을 가져왔던 시점의 상태로 디렉터를 복원하는 데 사용할 수 있습니다. 디렉터리의 수동 스냅샷을 생성하려면 다음 단계를 수행합니다.

Note

각 디렉터리에 대한 수동 스냅샷은 수가 5개로 제한되어 있습니다. 이미 제한 값에 도달한 경우에는 기존의 수동 스냅샷 중 하나를 삭제해야만 또 다른 스냅샷을 생성할 수 있습니다.

수동 스냅샷을 생성하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 유지 관리 탭을 선택합니다.
4. 스냅샷섹션에서 작업을 선택한 후 스냅샷 생성을 선택합니다.
5. 원하는 경우 디렉터리 스냅샷 생성 대화 상자에 스냅샷 이름을 제공합니다. 준비가 되면 생성을 선택합니다.

디렉터리 크기에 따라 스냅샷 생성에 몇 분 정도 걸릴 수 있습니다. 스냅샷이 준비가 되면 상태 값이 Completed로 바뀝니다.

스냅샷에서 디렉터리 복원

스냅샷에서 디렉터리를 복원하는 것은 디렉터리를 시간을 되돌려 놓는 것과 같습니다. 디렉터리 스냅샷은 생성된 디렉터리 고유의 것입니다. 스냅샷이 생성된 디렉터리에만 스냅샷을 저장할 수 있습니다. 또한 수동 스냅샷의 최대 지원 기간은 180일입니다. 자세한 내용은 Microsoft 웹 사이트에서 [Active Directory의 시스템 상태 백업의 유효 수명](#)을 참조하세요.

Warning

스냅샷 복원을 수행하기 전에 [AWS Support 센터](#)에 문의하시는 것이 좋습니다. 문의하시면 스냅샷 복원이 필요하지 않도록 도와드릴 수 있습니다. 스냅샷 복원은 특정 시점이므로 데이터 손실이 발생할 수 있습니다. 복원 작업이 완료될 때까지 디렉터리에 연결된 모든 DC 및 DNS 서버가 오프라인 상태가 된다는 점에 유의하세요.

스냅샷에서 디렉터리를 복원하려면 다음 단계를 수행합니다.

스냅샷에서 디렉터리를 복원하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.

2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 유지 관리 탭을 선택합니다.
4. 스냅샷 섹션의 목록에서 스냅샷을 선택하고 작업을 선택한 후 스냅샷 복원을 선택합니다.
5. Restore directory snapshot(디렉터리 스냅샷 복원) 대화 상자에서 정보를 검토하고 복원을 선택합니다.

AWS Managed Microsoft AD 디렉터리의 경우 디렉터리를 복원하는 데 2~3시간이 걸릴 수 있습니다. 성공적으로 복원되면 디렉터리의 상태 값이 Active로 바뀝니다. 디렉터리에 대한 모든 변경은 스냅샷 날짜가 덮어쓰기된 이후에 이루어집니다.

스냅샷 삭제

스냅샷을 삭제하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 유지 관리 탭을 선택합니다.
4. 스냅샷 섹션에서 작업을 선택한 후 스냅샷 삭제를 선택합니다.
5. 스냅샷을 삭제할지 확인한 다음 삭제를 선택합니다.

AWS 관리형 Microsoft AD를 업그레이드하세요

AWS Support문의하여 스탠다드 에디션 AWS 관리형 Microsoft Active Directory AD를 엔터프라이즈 에디션으로 업그레이드할 수 있습니다. 자세한 내용은 AWS Support 사용 설명서에서 [지원 사례 생성 및 사례 관리](#)를 참조하십시오.

Note

다중 지역 복제는 다음 지역의 AWS 관리형 Microsoft AD Enterprise 에디션에서만 사용할 수 있습니다.

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오레곤)
- 아프리카(케이프타운)

- 아시아 태평양(홍콩)
- 아시아 태평양(뭄바이)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(오사카)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 캐나다 서부(캘거리)
- 중국(베이징)
- 중국(닝샤)
- 유럽(프랑크푸르트)
- 유럽(취리히)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(파리)
- 유럽(스톡홀름)
- 유럽(밀라노)
- 유럽(스페인)
- 이스라엘(텔아비브)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- AWS GovCloud (미국 서부)
- AWS GovCloud (미국 동부)

AWS 관리형 Microsoft AD를 업그레이드할 때 알아두어야 할 몇 가지 제한 사항이 있습니다. 스크립트는 다음과 같습니다.

- 업그레이드 시 추가 비용이 발생합니다. 자세한 내용은 [AWS Directory Service 요금](#)을 참조하십시오.
- Active Directory를 업그레이드한 후에는 이전 버전으로 되돌릴 수 없습니다.
- 이전 스냅샷은 업그레이드된 Active Directory 후의 복원에 사용할 수 없습니다.
- 업그레이드는 합의된 AWS Support예정된 날짜 및 시간에 이루어집니다. 업그레이드는 태평양 표준시 기준 월요일에서 금요일, 오전 9시부터 오후 5시 사이에 이루어집니다.
- 업그레이드 프로세스에는 4~5시간이 소요됩니다.
- 업그레이드 프로세스 중에 AWS 관리형 Microsoft AD의 도메인 컨트롤러가 한 번에 하나씩 업그레이드됩니다. 이로 인해 성능이 저하되고 유지 관리 기간 중에 다운타임이 발생할 수 있습니다.
- 애플리케이션이 Active Directory의 도메인 이름 대신 도메인 컨트롤러의 호스트 이름 또는 IP 주소를 사용하는 경우 이러한 애플리케이션을 업데이트해야 합니다.
- LDAPS (SSL을 통한 경량 디렉터리 액세스 프로토콜) 를 사용하는 경우 도메인 컨트롤러에 새 인증서가 필요합니다.

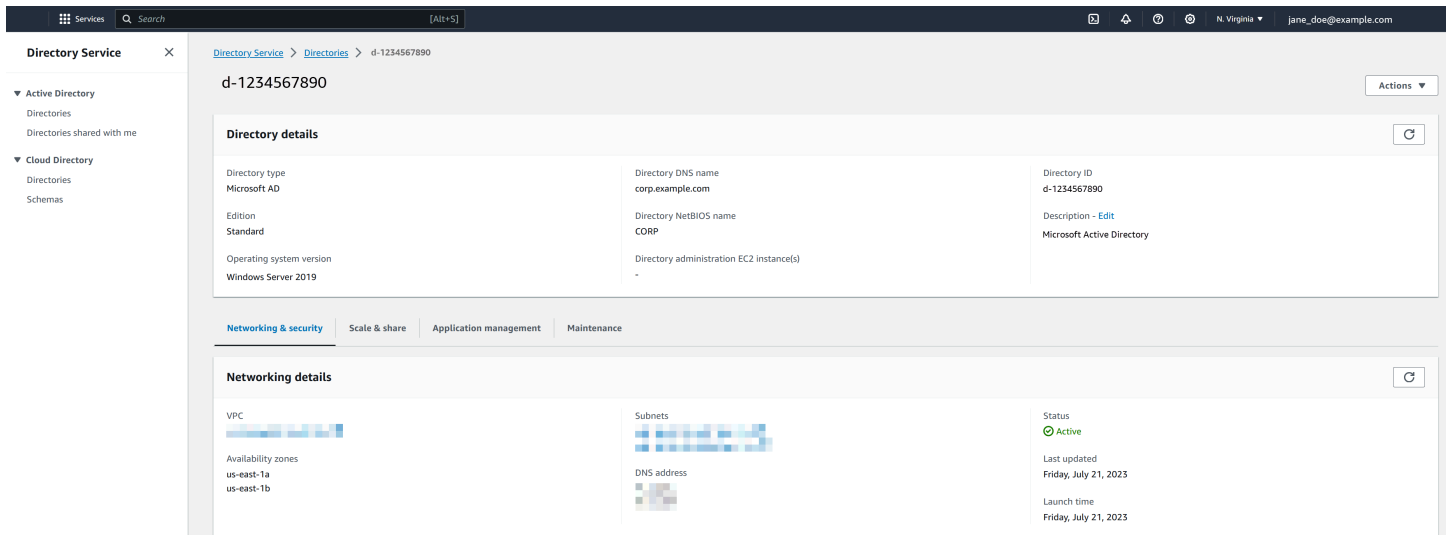
디렉터리 정보 보기

디렉터리에 대한 세부 정보를 볼 수 있습니다.

디렉터리에 대한 세부 정보 보기

1. [AWS Directory Service 콘솔](#) 탐색 창의 아래에서 Active Directory디렉터를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 클릭합니다. 디렉터리에 대한 정보가 디렉터리 세부 정보 페이지에 표시됩니다.

상태 필드에 대한 자세한 내용은 [디렉터리 상태 이해](#) 단원을 참조하세요.



사용자 및 그룹에게 AWS 리소스에 대한 액세스 권한 부여

AWS Directory Service 디렉터리 사용자 및 그룹에 Amazon EC2 콘솔 액세스와 같은 AWS 서비스 및 리소스에 대한 액세스 권한을 부여하는 기능을 제공합니다. 에 설명된 대로 IAM 사용자에게 디렉터리 관리 액세스 권한을 부여하는 것과 마찬가지로 [자격 증명 기반 정책\(IAM 정책\)](#), 디렉터리의 사용자가 Amazon EC2와 같은 다른 AWS 리소스에 액세스할 수 있으려면 해당 사용자 및 그룹에 IAM 역할 및 정책을 할당해야 합니다. 자세한 내용은 IAM 사용 설명서에서 [IAM 역할](#)을 참조하세요.

사용자에게 에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [AWS Management Console AD 보안 인증을 사용한 AWS Management Console 액세스 활성화](#)

주제

- [새 역할 생성](#)
- [기존 역할에서 신뢰 관계를 편집](#)
- [기존 역할에 사용자 또는 그룹 할당](#)
- [역할에 할당된 사용자 및 그룹 보기](#)
- [역할에서 사용자 또는 그룹 제거](#)
- [AWS Directory Service에서의 AWS 관리형 정책 사용](#)

새 역할 생성

에서 사용할 새 IAM 역할을 생성해야 하는 경우 IAM 콘솔을 사용하여 생성해야 합니다. AWS Directory Service 역할을 생성한 후에는 해당 역할과 신뢰 관계를 설정해야 콘솔에서 해당 AWS Directory Service 역할을 확인할 수 있습니다. 자세한 정보는 [기존 역할에서 신뢰 관계를 편집](#)을 참조하세요.

Note

이 작업을 수행하고 있는 사용자는 아래 IAM 작업을 수행할 수 있는 권한을 가지고 있어야 합니다. 자세한 정보는 [자격 증명 기반 정책\(IAM 정책\)](#)을 참조하세요.

- iam: PassRole
- 목표: GetRole
- 목표: CreateRole
- 목표: PutRolePolicy

IAM 콘솔에서 새 역할을 생성하려면

1. IAM 콘솔의 탐색 창에서 역할을 선택합니다. 자세한 내용은 IAM 사용 설명서의 [역할\(AWS Management Console\) 생성](#)을 참조하세요.
2. 역할 생성을 선택합니다.
3. Choose the service that will use this role(이 역할을 사용할 서비스 선택)에서 Directory Service(디렉터리 서비스)를 선택하고 Next(다음)를 선택합니다.
4. 디렉터리 사용자에게 적용할 정책 (예: AmazonEC2 FullAccess) 옆의 확인란을 선택한 후 다음을 선택합니다.
5. 필요한 경우 태그를 역할에 추가하고 Next(다음)를 선택합니다.
6. Role name(역할 이름)과 선택 사항인 Description(설명)을 입력한 다음 Create role(역할 생성)을 선택합니다.

예제: 역할을 생성하여 AWS Management Console 액세스 활성화

다음 체크리스트는 특정 디렉터리 사용자에게 Amazon EC2 콘솔에 대한 액세스를 부여하는 새 역할을 생성하기 위해 완료해야 하는 작업의 예를 제공합니다.

1. 위의 절차를 사용하여 IAM 콘솔에서 역할을 생성합니다. 정책을 입력하라는 메시지가 표시되면 AmazonEC2를 선택합니다. FullAccess
2. [기존 역할에서 신뢰 관계를 편집](#)의 단계를 사용하여 방금 생성한 역할을 편집한 다음, 필요한 신뢰 관계 정보를 정책 문서에 추가합니다. 다음 단계에서 액세스를 활성화한 후 역할이 즉시 표시되면 이 단계가 필요합니다. AWS Management Console
3. [AD 보안 인증을 사용한 AWS Management Console 액세스 활성화](#)의 단계에 따라 AWS Management Console에 대한 일반 액세스를 구성합니다.

4. [기존 역할에 사용자 또는 그룹 할당](#)의 단계에 따라 EC2 리소스에 액세스해야 하는 사용자를 새 역할에 추가합니다.

기존 역할에서 신뢰 관계를 편집

기존 IAM 역할을 AWS Directory Service 사용자 및 그룹에 할당할 수 있습니다. 하지만 이렇게 하려면 역할이 신뢰 관계를 AWS Directory Service가 가져야 합니다. 이 절차를 사용하여 역할을 생성하는 [새 역할 생성](#) 경우 이 신뢰 관계가 자동으로 설정됩니다. AWS Directory Service AWS Directory Service가 생성하지 않은 IAM 역할에서 이러한 신뢰 관계를 설정하기만 하면 됩니다.

기존 역할에 대한 신뢰 관계를 설정하려면 AWS Directory Service

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창의 액세스 관리에서 역할을 선택합니다.

콘솔에 계정에 대한 역할이 표시됩니다.

3. 수정하려는 역할의 이름을 선택하고 역할의 페이지에서 Trust relationships(신뢰 관계) 탭을 선택합니다.
4. 신뢰 정책 편집을 선택합니다.
5. Edit trust policy(신뢰 정책 편집)에서 다음을 붙여 넣은 다음 Update policy(정책 업데이트)를 선택합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS CLI를 사용하여 이 정책 문서를 업데이트할 수도 있습니다. 자세한 내용은 AWS CLI Command Reference(명령 참조)의 [update-trust](#)를 참조하세요.

기존 역할에 사용자 또는 그룹 할당

기존 IAM 역할을 AWS Directory Service 사용자 또는 그룹에 할당할 수 있습니다. 이렇게 하려면 다음 작업을 완료해야 합니다.

필수 조건

- [AWS 관리형 Microsoft AD를 만드세요.](#)
- [사용자를 만들거나 그룹을 만드세요.](#)
- 신뢰 관계가 [있는 역할을 AWS Directory Service 생성하십시오.](#) [기존 역할의 신뢰 관계를 편집할 수](#) 있습니다.

Note

디렉터리 내의 중첩 그룹 사용자를 위한 액세스는 지원되지 않습니다. 상위 그룹 멤버는 콘솔 액세스 권한이 있지만, 하위 그룹 멤버는 없습니다.

기존 IAM 역할에 사용자나 그룹을 할당하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창의 Active Directory에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 할당할 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
4. AWS Management Console 섹션으로 스크롤하여 '작업'과 '활성화'를 선택합니다.
5. 콘솔 액세스 위임 섹션에서 사용자에게 할당하려는 기존 IAM 역할의 IAM 역할 이름을 선택합니다.
6. Selected role(선택한 역할) 페이지의 Manage users and groups for this role(이 역할에 대한 사용자 및 그룹 관리)에서 추가를 선택합니다.
7. Add users and groups to the role(역할에 사용자 및 그룹 추가) 페이지의 Select Active Directory Forest(Active Directory 포리스트 선택)에서 AWS Managed Microsoft AD 포리스트(이 포리스트) 또는 온프레미스 포리스트(신뢰할 수 있는 포리스트) 중 AWS Management Console에 대한 액세스 권한이 필요한 계정이 포함된 것을 선택합니다. 신뢰할 수 있는 포리스트 설정 방법에 대한 자

세한 내용은 [자습서: AWS Managed Microsoft AD 디렉터리와 자체 관리형 Active Directory 도메인 간에 신뢰 관계를 생성합니다](#) 단원을 참조하세요.

8. Specify which users or groups to add(추가할 사용자 또는 그룹 지정)에서 Find by user(사용자별 찾기) 또는 Find by group(그룹별 찾기)을 선택한 후 사용자 또는 그룹의 이름을 입력합니다. 가능한 매치 목록에서 추가하고자 하는 사용자나 그룹을 선택합니다.
9. [Add]를 선택해 역할에 사용자 및 그룹을 할당하는 작업을 완료합니다.

역할에 할당된 사용자 및 그룹 보기

역할에 할당된 사용자 및 그룹을 보려면 다음 절차를 수행합니다.

필수 조건

- [사용자 또는 그룹을 기존 역할에 할당합니다](#).

역할에 할당된 사용자 및 그룹을 보는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창의 Active Directory에서 디렉터를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 할당을 보려는 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.
4. Delegate Console Access(위임 콘솔 액세스) 섹션에서 보려는 IAM 역할을 선택합니다.
5. Selected role(선택한 역할) 페이지의 Manage users and groups for this role(이 역할에 대한 사용자 및 그룹 관리) 섹션에서 역할에 할당된 사용자 및 그룹을 볼 수 있습니다.

역할에서 사용자 또는 그룹 제거

역할에서 사용자 또는 그룹을 제거하려면 다음 단계를 수행합니다.

역할에서 사용자 또는 그룹을 제거하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.

3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 할당을 제거하려는 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.
4. AWS Management Console 섹션에서 보려는 역할을 선택합니다.
5. Selected role(선택한 역할) 페이지의 Manage users and groups for this role(이 역할에 대한 사용자 및 그룹 관리)에서 역할을 제거할 사용자 또는 그룹을 선택한 후 제거를 선택합니다. 지정된 사용자 및 그룹에서 역할이 제거되지만, 계정에서는 해당 역할이 제거되지 않습니다.

AWS Directory Service에서의 AWS 관리형 정책 사용

AWS Directory Service에서는 사용자와 그룹에게 AWS 서비스 및 리소스에 대한 액세스 권한(예: Amazon EC2 콘솔에 대한 액세스 권한)을 부여하는 다음과 같은 AWS 관리형 정책을 제공합니다. 이러한 정책을 보려면 AWS Management Console에 로그인해야 합니다.

- [읽기 전용 액세스](#)
- [파워 유저 액세스](#)
- [AWS Directory Service 전체 액세스](#)
- [AWS Directory Service 읽기 전용 액세스](#)
- [Amazon Cloud Directory 전체 액세스](#)
- [Amazon Cloud Directory 읽기 전용 액세스](#)
- [Amazon EC2 전체 액세스](#)
- [Amazon EC2 읽기 전용 액세스](#)
- [Amazon VPC 전체 액세스](#)
- [Amazon VPC 읽기 전용 액세스](#)
- [Amazon RDS 전체 액세스](#)
- [Amazon RDS 읽기 전용 액세스](#)
- [Amazon DynamoDB 전체 액세스](#)
- [Amazon DynamoDB 읽기 전용 액세스](#)
- [Amazon S3 전체 액세스](#)
- [Amazon S3 읽기 전용 액세스](#)
- [AWS CloudTrail 전체 액세스](#)

- [AWS CloudTrail 읽기 전용 액세스](#)
- [Amazon CloudWatch 전체 액세스](#)
- [Amazon CloudWatch 읽기 전용 액세스](#)
- [Amazon CloudWatch Logs 전체 액세스](#)
- [Amazon CloudWatch Logs 읽기 전용 액세스](#)

자체 정책을 생성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [AWS리소스 관리를 위한 예제 정책](#)을 참조하세요.

AWS 애플리케이션 및 서비스에 대한 액세스 지원

사용자는 AWS 관리형 Microsoft AD에 WorkSpaces Amazon과 같은 AWS 애플리케이션 및 서비스에 액세스 권한을 부여할 수 있는 권한을 부여할 수 있습니다Active Directory. AWS 관리형 Microsoft AD와 함께 작동하도록 다음 AWS 응용 프로그램 및 서비스를 활성화하거나 비활성화할 수 있습니다.

AWS 애플리케이션/ 서비스	추가 정보...
Amazon Chime	자세한 내용은 Amazon Chime 관리 안내서 를 참조하세요.
Amazon Connect	자세한 내용은 Amazon Connect 관리 안내서 를 참조하세요.
Amazon FSx for Windows File Server	자세한 내용은 Microsoft Active Directory용 디렉터리 AWS 서비스와 함께 Amazon FSx 사용을 참조하십시오 .
아마존 QuickSight	자세한 내용은 Amazon QuickSight 사용 설명서 를 참조하십시오.
Amazon Relational Database Service	자세한 내용은 Amazon RDS 사용 설명서 를 참조하세요.
아마존 WorkDocs	자세한 내용은 Amazon WorkDocs 관리 안내서 를 참조하십시오.
아마존 WorkMail	자세한 내용은 Amazon WorkMail 관리자 안내서 를 참조하십시오.

AWS 애플리케이션/ 서비스	추가 정보...
아마존 WorkSpaces	에서 직접 Simple AD, AWS 관리형 Microsoft AD 또는 AD 커넥터를 만들 수 WorkSpaces 있습니다. Workspace를 생성할 때 고급 설정을 시작하면 됩니다. 자세한 내용은 Amazon WorkSpaces 관리 안내서 를 참조하십시오.
AWS Client VPN	자세한 내용은 AWS Client VPN 사용 설명서 를 참조하십시오.
AWS IAM Identity Center	자세한 내용은 AWS IAM Identity Center 사용 설명서 를 참조하십시오.
AWS License Manager	자세한 설명은 License Manager 사용자 가이드 를 참조하세요.
AWS Management Console	자세한 정보는 AD 보안 인증을 사용한 AWS Management Console 액세스 활성화 를 참조하세요.
AWS Private Certificate Authority	자세한 내용은 AWS Private CA 커넥터를 참조하십시오 Active Directory.
AWS Transfer Family	자세한 내용은 AWS Transfer Family 사용 설명서 를 참조하십시오.

일단 활성화가 되면 디렉터리에 대한 액세스 권한을 부여하고자 하는 애플리케이션 또는 서비스의 콘솔에서 디렉터리에 대한 액세스를 관리합니다. AWS Directory Service 콘솔에서 위에서 설명한 AWS 응용 프로그램 및 서비스 링크를 찾으려면 다음 단계를 수행하십시오.

디렉터리에서 애플리케이션 및 서비스를 표시하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.

4. AWS apps & services(앱 및 서비스) 섹션에서 목록을 검토합니다.

를 사용하여 AWS AWS Directory Service 응용 프로그램 및 서비스를 승인하거나 권한 부여를 해제하는 방법에 대한 자세한 내용은 [을 참조하십시오. 를 사용하는 AWS 애플리케이션 및 서비스에 대한 권한 부여 AWS Directory Service](#)

주제

- [액세스 URL 생성하기](#)
- [Single Sign-On](#)

액세스 URL 생성하기

액세스 URL은 디렉터리에 연결된 로그인 페이지에 도달하기 위해 Amazon WorkDocs 등의 AWS 애플리케이션 및 서비스에서 사용됩니다. URL은 전역적으로 고유해야 합니다. 다음 단계를 수행하여 디렉터리에 대한 액세스 URL을 생성할 수 있습니다.

Warning

이 디렉터리에 대한 애플리케이션 액세스 URL을 생성한 후에는 변경할 수 없습니다. 액세스 URL이 생성되고 난 후에는 다른 계정에서 이를 사용할 수 없습니다. 디렉터리를 삭제하면 액세스 URL 역시 삭제가 되면서 다른 계정이 사용할 수 있게 됩니다.

Note

다중 리전 디렉터리를 사용하는 경우 기본 리전에서만 액세스 URL을 구성할 수 있습니다.

액세스 URL 생성 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.

4. 액세스 URL이 디렉터리에 할당되지 않은 경우 애플리케이션 액세스 URL 섹션에 생성 버튼이 표시됩니다. 디렉터리 별칭을 입력하고 생성을 선택합니다. 개체 이미 존재 오류가 반환되면 지정된 디렉터리 별칭이 이미 할당되었다는 뜻입니다. 또 다른 별칭을 선택하고 이 절차를 반복합니다.

액세스 URL이 *<alias>.awsapps.com* 형식으로 표시됩니다. 기본적으로 이 URL을 클릭하면 Amazon WorkDocs의 로그인 페이지로 이동합니다.

Single Sign-On

AWS Directory Service 사용자가 자격 증명을 별도로 입력할 필요 없이 디렉터리에 연결된 WorkDocs 컴퓨터에서 Amazon에 액세스할 수 있도록 하는 기능을 제공합니다.

Single Sign-On 기능을 활성화하려면 추가 단계를 수행하여 사용자의 웹 브라우저가 Single Sign-On을 지원하도록 해야 합니다. 사용자는 웹 브라우저 설정을 변경하여 Single Sign-On을 활성화해야 할 수도 있습니다.

Note

Single Sign-On은 AWS Directory Service 디렉터리에 조인된 컴퓨터에 사용할 때만 작동합니다. 이 디렉터리에 조인되지 않은 컴퓨터에서는 사용할 수 없습니다.

디렉터리가 AD Connector 디렉터리이고 AD Connector 서비스 계정에 서비스 보안 주체 이름 속성을 추가하거나 제거할 권한이 없는 경우 아래의 5단계와 6단계에 대해 두 가지 옵션이 있습니다.

1. 계속 진행하면 AD Connector 서비스 계정에 서비스 보안 주체 이름 속성을 추가하거나 제거할 권한이 있는 디렉터리 사용자의 사용자 이름과 암호를 묻는 메시지가 표시됩니다. 이러한 자격 증명은 Single Sign-On을 활성화하는 목적으로만 사용되며 서비스에 저장되지 않습니다. AD Connector 서비스 계정 사용 권한은 변경되지 않습니다.
2. AD Connector 서비스 계정이 자체적으로 서비스 주체 이름 특성을 추가 또는 제거할 수 있도록 권한을 위임할 수 있습니다. AD Connector 서비스 계정에 대한 사용 권한을 수정할 권한이 있는 계정을 사용하여 도메인에 가입된 컴퓨터에서 아래 PowerShell 명령을 실행할 수 있습니다. 아래 명령은 AD Connector 서비스 계정에 서비스 보안 주체 이름 속성을 추가 및 제거할 수 있는 기능을 제공합니다.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
```

```
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
  $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
  Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
  $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
  Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
  'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
  'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Amazon에서 싱글 사인온을 활성화 또는 비활성화하려면 WorkDocs

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. 애플리케이션 액세스 URL 섹션에서 활성화를 선택하여 Amazon용 싱글 사인온을 활성화합니다.
WorkDocs

활성화 버튼이 보이지 않으면 먼저 액세스 URL을 생성해야 이 옵션이 표시됩니다. 액세스 URL을 생성하는 자세한 방법은 [액세스 URL 생성하기](#)를 참조하세요.

5. 이 디렉터리에 대해 SSO(Single-Sign-On)를 활성화하시겠습니까? 대화 상자에서 활성화를 선택합니다. Single Sign-On이 디렉터리에서 활성화됩니다.
6. 나중에 WorkDocs Amazon에서의 SSO (Single Sign-On) 를 비활성화하려면 [Disable] 을 선택한 다음 [이 디렉터리에 대한 Single Sign-On 비활성화] 대화 상자에서 [비활성화] 를 다시 선택합니다.

주제

- [IE 및 Chrome에서의 Single Sign-On](#)

- [Firefox에서의 Single Sign-On](#)

IE 및 Chrome에서의 Single Sign-On

Microsoft Internet Explorer(IE) 및 Google Chrome 브라우저가 Single Sign-On을 지원하도록 하려면 클라이언트 컴퓨터에서 아래 절차를 수행해야 합니다.

- 액세스 URL(예: <https://<alias>.awsapps.com>)을 Single Sign-On이 승인된 사이트 목록에 추가합니다.
- 액티브 스크립팅을 활성화합니다 (). JavaScript
- 자동 로그인을 허용합니다.
- 통합 인증을 활성화합니다.

도메인 관리자나 사용자가 이러한 작업을 수동으로 수행하거나, 도메인 관리자가 그룹 정책 설정을 이용해 이러한 설정값을 변경할 수 있습니다.

주제

- [Windows에서의 Single Sign-On을 위한 수동 업데이트](#)
- [OS X에서 Single Sign-On의 수동 업데이트](#)
- [Single Sign-On을 위한 그룹 정책 설정](#)

Windows에서의 Single Sign-On을 위한 수동 업데이트

Windows 컴퓨터에서 Single Sign-On을 수동으로 활성화하려면 해당 컴퓨터에서 다음 단계를 수행합니다. 이러한 설정값 중 일부는 이미 올바르게 설정되어 있을 수 있습니다.

Windows에서 IE 또는 Chrome을 위한 Single Sign-On을 수동으로 활성화하는 방법

1. 인터넷 속성 대화 상자를 열려면 시작 메뉴를 선택하고 검색 상자에 Internet Options를 입력한 후 인터넷 옵션을 선택합니다.
2. 다음 단계를 수행하여 Single Sign-On이 승인된 사이트 목록에 액세스 URL을 추가합니다.
 - a. 인터넷 속성 대화 상자에서 보안 탭을 선택합니다.
 - b. 로컬 인트라넷을 선택하고 사이트를 선택합니다.
 - c. 로컬 인트라넷 대화 상자에서 고급을 선택합니다.
 - d. 웹 사이트 목록에 액세스 URL을 추가하고 닫기를 선택합니다.

- e. 로컬 인트라넷 대화 상자에서 확인을 선택합니다.
3. 액티브 스크립팅을 활성화하려면 다음 단계를 수행합니다.
 - a. 인터넷 속성 대화 상자의 보안 탭에서 사용자 지정 수준을 선택합니다.
 - b. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 스크립팅까지 아래로 스크롤한 다음 액티브 스크립팅에서 활성화를 선택합니다.
 - c. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 확인을 선택합니다.
4. 자동 로그인을 활성화하려면 다음 단계를 수행합니다.
 - a. 인터넷 속성 대화 상자의 보안 탭에서 사용자 지정 수준을 선택합니다.
 - b. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 사용자 인증까지 아래로 스크롤한 다음 로그인에서 인트라넷 영역에서만 자동 로그인을 선택합니다.
 - c. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 확인을 선택합니다.
 - d. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 확인을 선택합니다.
5. 통합 인증을 활성화하려면 다음 단계를 수행합니다.
 - a. 인터넷 속성 대화 상자에서 고급 탭을 선택합니다.
 - b. 보안으로 스크롤하여 통합된 Windows 인증 사용을 선택합니다.
 - c. 인터넷 속성 대화 상자에서 확인을 선택합니다.
6. 이러한 변경 사항이 적용되도록 브라우저를 닫았다가 다시 엽니다.

OS X에서 Single Sign-On의 수동 업데이트

OS X에서 Chrome을 위해 Single Sign-On을 수동으로 활성화하려면 해당 컴퓨터에서 다음 단계를 수행합니다. 이 단계를 완료하려면 컴퓨터에서 관리자 권한이 필요합니다.

OS X 기반 Chrome에서 Single Sign-On을 수동으로 활성화하는 방법

1. 다음 명령을 실행하여 [AuthServerAllowlist](#) 정책에 액세스 URL을 추가합니다.

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```


2. 시스템 기본 설정을 열고 프로필 패널로 이동하여 Chrome Kerberos Configuration 프로필을 삭제합니다.
3. Chrome을 다시 시작하고 Chrome에서 chrome://policy을 열어 새로운 설정이 올바르게 되었는지 확인합니다.

Single Sign-On을 위한 그룹 정책 설정

도메인 관리자는 그룹 정책 설정을 실행하여 도메인에 조인된 클라이언트 컴퓨터에서 Single Sign-On을 변경할 수 있습니다.

Note

Chrome 정책을 사용하여 도메인의 컴퓨터에서 Chrome 웹 브라우저를 관리하는 경우 [AuthServerAllowlist](#) 정책에 액세스 URL을 추가해야 합니다. Chrome 정책 설정에 대한 자세한 내용은 [Chrome의 정책 설정](#)을 참조하세요.

그룹 정책 설정을 사용하여 IE 또는 Chrome을 위한 Single Sign-On 활성화하는 방법

1. 다음 단계를 수행하여 그룹 정책 객체를 새로 생성합니다.
 - a. 그룹 정책 관리 도구를 열고 도메인을 탐색한 후 그룹 정책 객체를 선택합니다.
 - b. 메인 메뉴에서 작업을 선택한 후 새로 만들기를 선택합니다.
 - c. 새 GPO 대화 상자에서 그룹 정책 객체를 설명하는 이름(예: IAM Identity Center Policy)을 입력하고 원본 스타터 GPO 설정은 (없음)으로 유지합니다. 확인을 클릭합니다.
2. 다음 단계를 수행하여 Single Sign-On이 승인된 사이트 목록에 액세스 URL을 추가합니다.
 - a. 그룹 정책 관리 도구에서 도메인을 탐색한 후 그룹 정책 객체를 선택하고 IAM Identity Center 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열어 편집을 선택합니다.
 - b. 정책 트리에서 사용자 구성 > 기본 설정 > Windows 설정으로 이동합니다.
 - c. Windows 설정 목록에서 레지스트리의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 새 레지스트리 항목을 선택합니다.
 - d. 새 레지스트리 속성 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.

Action

Update

Hive

HKEY_CURRENT_USER

경로

Software\Microsoft\Windows\CurrentVersion\Internet Settings
 \ZoneMap\Domains\awsapps.com*<alias>*

*<alias>*의 값은 액세스 URL에서 파생됩니다. 액세스 URL이 https://
 examplecorp.awsapps.com이면 별칭이 examplecorp이고 레지스트리 키가
 Software\Microsoft\Windows\CurrentVersion\Internet Settings
 \ZoneMap\Domains\awsapps.com\examplecorp가 됩니다.

값 이름

https

값 유형

REG_DWORD

값 데이터

1

3. 액티브 스크립팅을 활성화하려면 다음 단계를 수행합니다.
 - a. 그룹 정책 관리 도구에서 도메인을 탐색한 후 그룹 정책 객체를 선택하고 IAM Identity Center 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열어 편집을 선택합니다.
 - b. 정책 트리에서 컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > Internet Explorer > 인터넷 제어판 > 보안 페이지 > 인트라넷 영역으로 이동합니다.
 - c. 인트라넷 영역 목록에서 액티브 스크립팅 허용의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 편집을 선택합니다.
 - d. 액티브 스크립팅 허용 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.
 - 사용 라디오 버튼을 선택합니다.
 - 옵션에서 액티브 스크립팅 허용을 사용으로 설정합니다.
4. 자동 로그인을 활성화하려면 다음 단계를 수행합니다.
 - a. 그룹 정책 관리 도구를 열고 도메인을 탐색한 다음, 그룹 정책 객체를 선택하고 SSO 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 편집을 선택합니다.

- b. 정책 트리에서 컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > Internet Explorer > 인터넷 제어판 > 보안 페이지 > 인트라넷 영역으로 이동합니다.
 - c. 인트라넷 영역 목록에서 로그인 옵션의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 편집을 선택합니다.
 - d. 로그인 옵션 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.
 - 사용 라디오 버튼을 선택합니다.
 - 옵션에서 로그인 옵션을 인트라넷 영역에서만 자동으로 로그인으로 설정합니다.
5. 통합 인증을 활성화하려면 다음 단계를 수행합니다.
- a. 그룹 정책 관리 도구에서 도메인을 탐색한 후 그룹 정책 객체를 선택하고 IAM Identity Center 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열어 편집을 선택합니다.
 - b. 정책 트리에서 사용자 구성 > 기본 설정 > Windows 설정으로 이동합니다.
 - c. Windows 설정 목록에서 레지스트리의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 새 레지스트리 항목을 선택합니다.
 - d. 새 레지스트리 속성 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.

Action

Update

Hive

HKEY_CURRENT_USER

경로

Software\Microsoft\Windows\CurrentVersion\Internet Settings

값 이름

EnableNegotiate

값 유형

REG_DWORD

값 데이터

1

6. 그룹 정책 관리 편집기 창이 아직 열려 있으면 닫습니다.

7. 이 단계에 따라 도메인에 새 정책을 할당합니다.
 - a. 그룹 정책 관리 트리에서 도메인의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 기존 GPO 연결을 선택합니다.
 - b. 그룹 정책 객체 목록에서 IAM Identity Center 정책을 선택하고 확인을 선택합니다.

다음에 클라이언트에서 그룹 정책이 업데이트되고 나서, 또는 다음에 사용자가 로그인을 할 때 이러한 변경 사항이 적용됩니다.

Firefox에서의 Single Sign-On

Mozilla Firefox 브라우저가 Single Sign-On을 지원하도록 하려면 액세스 URL(예: <https://<alias>.awsapps.com>)을 Single Sign-On이 승인된 사이트 목록에 추가합니다. 수동 추가나 스크립트를 통한 자동 추가가 가능합니다.

주제

- [Single Sign-On의 수동 업데이트](#)
- [Single Sign-On의 자동 업데이트](#)

Single Sign-On의 수동 업데이트

Firefox에서 승인된 사이트 목록에 액세스 URL을 수동으로 추가하려면 클라이언트 컴퓨터에서 다음 단계를 수행합니다.

Firefox에서 승인된 사이트 목록에 액세스 URL을 수동으로 추가하는 방법

1. Firefox를 열고 `about:config` 페이지를 엽니다.
2. `network.negotiate-auth.trusted-uris` 기본 설정을 열고 사이트 목록에 액세스 URL을 추가합니다. 쉼표(,)를 사용해 여러 항목을 구분합니다.

Single Sign-On의 자동 업데이트

도메인 관리자는 스크립트를 사용해 네트워크 상의 모든 컴퓨터에서 Firefox `network.negotiate-auth.trusted-uris` 사용자 기본 설정에 액세스 URL을 추가할 수 있습니다. 자세한 내용은 <https://support.mozilla.org/en-US/questions/939037>을 참조하세요.

AD 보안 인증을 사용한 AWS Management Console 액세스 활성화

AWS Directory Service는 디렉터리 멤버에게 AWS Management Console에 대한 액세스 권한을 부여할 수 있도록 허용합니다. 기본적으로 디렉터리 멤버는 AWS 리소스에 액세스할 수 있는 권한이 없습니다. 디렉터리 멤버에게 IAM 역할을 할당하여 다양한 AWS 서비스 및 리소스에 대한 액세스 권한을 제공합니다. IAM 역할은 디렉터리 멤버가 보유하고 있는 서비스, 리소스, 액세스 수준을 정의합니다.

디렉터리 멤버에게 콘솔 액세스 권한을 부여할 수 있으려면 디렉터리가 액세스 URL을 가지고 있어야 합니다. 디렉터리 세부 정보를 확인하고 액세스 URL을 얻을 수 있는 자세한 방법은 [디렉터리 정보 보기](#)를 참조하세요. 액세스 URL을 생성하는 자세한 방법은 [액세스 URL 생성하기](#)를 참조하세요.

IAM 역할을 생성해서 디렉터리 멤버에게 할당하는 자세한 방법은 [사용자 및 그룹에게 AWS 리소스에 대한 액세스 권한 부여](#) 단원을 참조하세요.

주제

- [AWS Management Console 액세스 활성화](#)
- [AWS Management Console 액세스 비활성화](#)
- [로그인 세션 길이 설정](#)

관련 AWS 보안 블로그 문서

- [AWS Managed Microsoft AD 및 온프레미스 보안 인증을 사용하여 AWS Management Console에 액세스하는 방법](#)

Note

AWS Management Console에 대한 액세스는 AWS Managed Microsoft AD의 리전별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 내용은 [글로벌 기능과 리전별 기능 비교](#) 섹션을 참조하세요.

AWS Management Console 액세스 활성화

기본적으로 디렉터리에서는 콘솔 액세스가 활성화되어 있지 않습니다. 디렉터리 사용자 및 그룹에 대해 콘솔 액세스를 활성화하려면 다음 단계를 수행합니다.

콘솔 액세스 활성화

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 AWS Management Console에 대한 액세스를 활성화할 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.
4. AWS Management Console 섹션에서 활성화를 선택합니다. 콘솔 액세스는 현재 디렉터리에서 활성화되어 있습니다.

사용자가 액세스 URL을 통해 콘솔에 로그인할 수 있으려면 우선 역할에 사용자를 추가해야 합니다. IAM 역할에 사용자를 할당하는 방법은 [기존 역할에 사용자 또는 그룹 할당](#) 단원을 참조하세요. IAM 역할이 할당되고 나면 사용자는 액세스 URL을 이용해 콘솔에 액세스할 수 있습니다. 예를 들어 디렉터리 액세스 URL이 example-corp.awsapps.com이면 콘솔에 액세스하기 위한 URL은 https://example-corp.awsapps.com/console/입니다.

AWS Management Console 액세스 비활성화

디렉터리 사용자 및 그룹에 대해 콘솔 액세스를 비활성화하려면 다음 단계를 수행합니다.

콘솔 액세스를 비활성화하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 AWS Management Console에 대한 액세스를 비활성화할 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.
4. AWS Management Console 섹션에서 비활성화를 선택합니다. 콘솔 액세스는 현재 디렉터리에서 비활성화되어 있습니다.
5. 디렉터리 내 사용자나 그룹에 IAM 역할이 할당된 경우, 비활성화 버튼을 사용할 수 없을 수 있습니다. 이 경우 계속 진행하기 전에 디렉터리에 대한 모든 IAM 역할 할당을 제거해야 합니다. 여기에

는 디렉터리에서 삭제된 사용자 또는 그룹에 대한 할당(삭제된 사용자 또는 삭제된 그룹으로 표시됨)이 포함됩니다.

할당된 모든 IAM 역할이 삭제되고 나면 위의 단계들을 반복합니다.

로그인 세션 길이 설정

기본적으로 콘솔에 성공적으로 로그인하면 로그아웃이 되기 전까지 1시간 동안 세션을 이용할 수 있습니다. 그 이후에는 다시 로그인을 해야 다음 세션을 1시간 동안 이용할 수 있고, 1시간이 지나면 다시 로그아웃이 됩니다. 아래 절차를 통해 세션당 최대 12시간까지 연장이 가능합니다.

로그인 세션 길이를 설정하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 로그인 세션 길이를 설정할 리전을 선택한 다음 애플리케이션 관리 탭을 선택합니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.
 - 다중 리전 복제에 표시된 리전이 없는 경우 애플리케이션 관리 탭을 선택합니다.
4. AWS 앱 및 서비스 섹션에서 AWSManagement Console(관리 콘솔)을 선택합니다.
5. AWS 리소스에 대한 액세스 관리 대화 상자에서 계속을 선택합니다.
6. IAM 역할에 사용자 및 그룹 할당 페이지의 로그인 세션 길이 설정에서 번호가 매겨진 값을 편집한 다음 저장을 선택합니다.

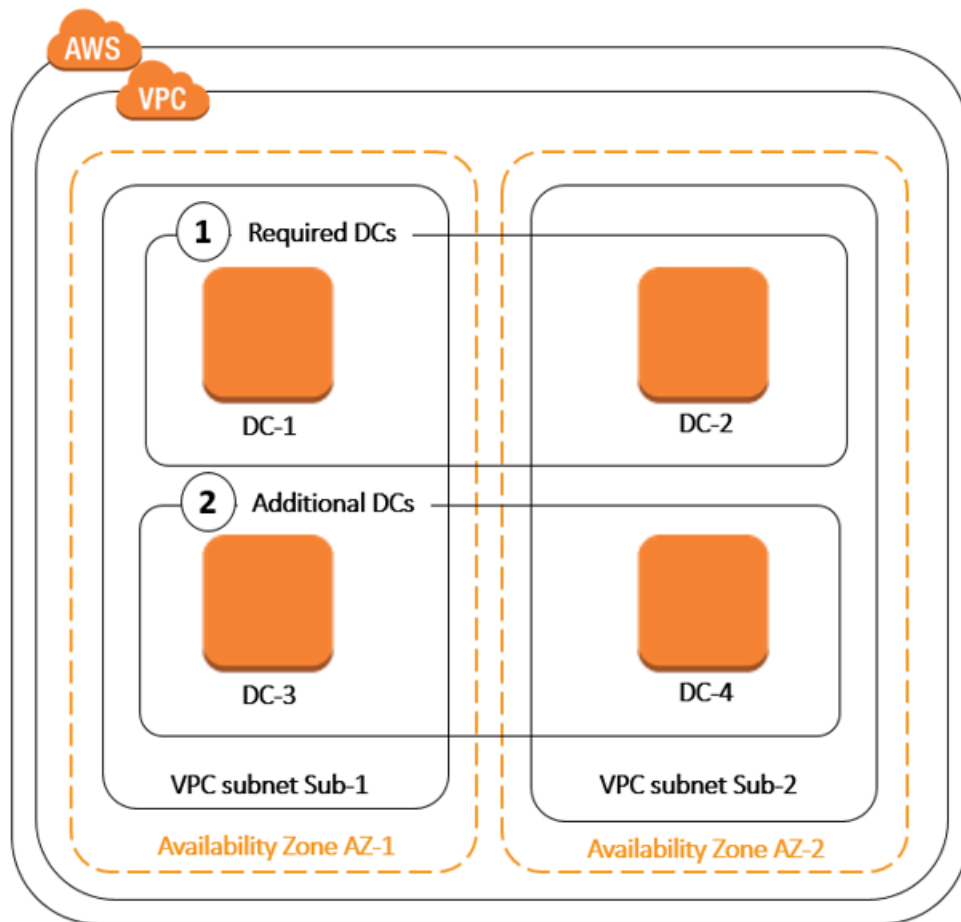
추가 도메인 컨트롤러 배포

추가 도메인 컨트롤러를 배포하면 중복성이 증가하여 복원성 및 가용성이 한층 향상됩니다. 또한 더 많은 수의 Active Directory 요청을 지원하여 디렉터리 성능이 개선됩니다. 예를 들어, 이제 AWS 관리형 Microsoft AD를 사용하여 SQL Server용 Amazon EC2 및 Amazon RDS의 대규모 인스턴스에 배포되는 여러 .NET 애플리케이션을 지원할 수 있습니다.

디렉터를 처음 만들면 AWS Managed Microsoft AD는 여러 가용 영역에 두 개의 도메인 컨트롤러를 배포하며, 이는 고가용성을 위해 필요합니다. 나중에 원하는 도메인 컨트롤러의 총 개수만 지정하면 AWS Directory Service 콘솔을 통해 추가 도메인 컨트롤러를 쉽게 배포할 수 있습니다. AWS 관리형

Microsoft AD는 디렉터리가 실행되는 가용 영역 및 Amazon VPC 서브넷에 추가 도메인 컨트롤러를 배포합니다.

예를 들어 아래 그림에서, DC-1 및 DC-2는 디렉터리와 함께 원래 생성된 2개의 도메인 컨트롤러를 나타냅니다. AWS Directory Service 콘솔에서는 이러한 기본 도메인 컨트롤러를 필수라고 합니다. AWS Managed Microsoft AD는 디렉터리 생성 프로세스 중에 의도적으로 이러한 각 도메인 컨트롤러를 별도의 가용 영역에 배치합니다. 나중에 로그인 피크 시간대에 인증 부하를 분산시키기 위해 두 개의 도메인 컨트롤러를 추가해야 할 수도 있습니다. DC-3 및 DC-4는 모두 새 도메인 컨트롤러를 나타냅니다. 콘솔에는 이제 Additional로 지칭됩니다. 이전과 마찬가지로 AWS Managed Microsoft AD는 새 도메인 컨트롤러를 다른 가용 영역에 자동으로 배치하여 도메인의고가용성을 보장합니다.



이 프로세스에서는 추가 도메인 컨트롤러에 대해 디렉터리 데이터 복제, 자동 일별 스냅샷 또는 모니터링을 수동으로 구성할 필요가 없습니다. 자체 Active Directory 인프라를 배포하고 유지 관리할 필요 없이 보다 용이하게 미션 크리티컬 Active Directory 통합 워크로드를 AWS 클라우드로 마이그레이션 및 실행할 수도 있습니다. [UpdateNumberOfDomainControllers](#) API를 사용하여 AWS 관리형 Microsoft AD 용 추가 도메인 컨트롤러를 배포하거나 제거할 수도 있습니다.

Note

추가 도메인 컨트롤러는 AWS 관리형 Microsoft AD의 지역별 기능입니다. [다중 리전 복제](#)를 사용하는 경우 다음 절차를 각 리전에 별도로 적용해야 합니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)를 참조하세요.

추가 도메인 컨트롤러 추가 또는 제거

도메인 컨트롤러를 추가하거나 제거하기 전에 도메인 컨트롤러 요구 사항에 대한 자세한 내용은 다음과 같습니다.

- 추가 도메인 컨트롤러를 배포한 후, 도메인 컨트롤러를 2개로 줄일 수 있습니다. 2개는 내결함성 및 고가용성 목적에 필요한 최소 개수입니다.
- 삭제된 도메인 컨트롤러는 추가 도메인 컨트롤러 목록에서 삭제됩니다. 주 도메인 컨트롤러와 보조 도메인 컨트롤러는 필수이며 삭제할 수 없습니다.
- LDAPS를 활성화하도록 AWS 관리형 Microsoft AD를 구성한 경우 추가하는 모든 추가 도메인 컨트롤러에도 LDAPS가 자동으로 활성화됩니다. 자세한 정보는 [보안 LDAP 또는 LDAPS 활성화](#)를 참조하세요.

다음 절차를 사용하여 AWS Managed Microsoft AD 디렉터리에서 추가 도메인 컨트롤러를 배포하거나 제거할 수 있습니다.

추가 도메인 컨트롤러를 추가 또는 제거하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되어 있는 경우 도메인 컨트롤러를 추가하거나 제거할 리전을 선택한 다음 Scale & share(크기 조정 및 공유) 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 Scale & share(크기 조정 및 공유) 탭을 선택합니다.
4. Domain controllers(도메인 컨트롤러) 섹션에서 편집을 선택합니다.
5. 디렉터리에서 추가 또는 제거할 도메인 컨트롤러 수를 지정하고 수정을 선택합니다.

6. AWS 관리형 Microsoft AD가 배포 프로세스를 완료하면 모든 도메인 컨트롤러가 활성 상태로 표시되고 할당된 가용 영역과 Amazon VPC 서브넷이 모두 표시됩니다. 새 도메인 컨트롤러는 디렉터리가 이미 배포된 가용 영역 및 서브넷에 고르게 분산됩니다.

관련 보안 블로그 기사 [AWS](#)

- [도메인 컨트롤러를 추가하여 관리형 AWS Microsoft AD의 중복성 및 성능을 높이는 방법 AWS Directory Service](#)

Active Directory에서 AWS Managed Microsoft AD로 사용자 마이그레이션

암호 내보내기 서비스 (PES) 와 함께 Active Directory 마이그레이션 툴킷 (ADMT) 을 사용하여 자체 관리형 Active Directory에서 관리형 AWS Microsoft AD 디렉터리로 사용자를 마이그레이션할 수 있습니다. 이를 통해 사용자를 위해 Active Directory 개체 및 암호화된 암호를 보다 쉽게 마이그레이션할 수 있습니다.

자세한 지침은 AWS 보안 블로그에서 [ADMT를 사용하여 온프레미스 도메인을 AWS Managed Microsoft AD로 마이그레이션하는 방법](#)을 참조하세요.

AWS Managed Microsoft AD 할당량

다음은 AWS Managed Microsoft AD의 기본 할당량입니다. 별도로 명시되지 않는 한 각 할당량은 리전 별입니다.

AWS Managed Microsoft AD 할당량

리소스	기본 할당량
AWS Managed Microsoft AD 디렉터리	20
수동 스냅샷 *	AWS Managed Microsoft AD당 5
수동 스냅샷 기간	180일
디렉터리당 최대 도메인 컨트롤러 수	20
Standard Microsoft AD당 공유 도메인 ***	5
Enterprise Microsoft AD당 공유 도메인 ***	125

리소스	기본 할당량
디렉터리당 등록된 인증 기관(CA) 인증서의 최대 수	5
단일 AWS Managed Microsoft AD(Enterprise Edition) 디렉터리의 최대 총 AWS 리전 수 ****	5

* 수동 스냅샷 할당량은 변경할 수 없습니다.

** 수동 스냅샷의 최대 지원 기간은 180일이며 변경할 수 없습니다. 이는 Active Directory의 시스템 상태 백업의 유효 수명을 정의하는 삭제된 객체의 삭제 표시-수명 속성 때문입니다. 180일이 지난 스냅샷에서는 복구할 수 없습니다. 자세한 내용은 Microsoft 웹 사이트에서 [Active Directory의 시스템 상태 백업의 유효 수명](#)을 참조하세요.

*** 공유 도메인 기본 할당량은 개별 디렉터리를 공유할 수 있는 계정 수를 나타냅니다.

**** 여기에는 기본 리전 1개와 추가 리전 최대 4개가 포함됩니다. 자세한 내용은 [기본 리전과 추가 리전의 비교](#) 섹션을 참조하세요.

Note

AWS 탄력적 네트워크 인터페이스(ENI)에는 퍼블릭 IP 주소를 연결할 수 없습니다.

애플리케이션 설계 및 로드 분산에 관한 정보는 [애플리케이션 프로그래밍](#)을 참조하세요.

스토리지 및 객체 할당량은 [AWS Directory Service 요금](#) 페이지의 비교표를 참조하세요.

AWS 관리형 Microsoft AD를 위한 애플리케이션 호환성

AWS Microsoft Active Directory용 디렉터리 서비스 (AWS 관리형 Microsoft AD) 는 여러 AWS 서비스 및 타사 응용 프로그램과 호환됩니다.

다음은 호환되는 AWS 응용 프로그램 및 서비스 목록입니다.

- Amazon Chime - 세부 지침은 [Active Directory 연결](#)을 참조하세요.
- Amazon Connect - 자세한 내용은 [How Amazon Connect works](#)를 참조하세요.

- Amazon EC2 - 자세한 내용은 [Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory](#)를 참조하세요.
- Amazon QuickSight - 자세한 내용은 [Amazon QuickSight 엔터프라이즈 에디션의 사용자 계정 관리를 참조하십시오.](#)
- Amazon RDS for MySQL - 자세한 내용은 [MySQL용 Kerberos 인증 사용](#)을 참조하세요.
- Amazon RDS for Oracle - 자세한 내용은 [Amazon RDS for Oracle과 함께 Kerberos 인증 사용](#)을 참조하세요.
- Amazon RDS for PostgreSQL - 자세한 내용은 [Amazon RDS for PostgreSQL과 함께 Kerberos 인증 사용](#)을 참조하세요.
- Amazon RDS for SQL Server - 자세한 내용은 [Amazon RDS Microsoft SQL Server DB 인스턴스에서 Windows 인증 사용](#)을 참조하세요.
- Amazon WorkDocs - 자세한 지침은 [AWS 관리형 Microsoft AD를 사용하여 온프레미스 디렉터리에 연결](#)을 참조하십시오.
- Amazon WorkMail - 자세한 지침은 [Amazon을 기존 WorkMail 디렉터리와 통합 \(표준 설정\)](#) 을 참조하십시오.
- AWS Client VPN - 자세한 지침은 [클라이언트 인증 및 권한 부여](#)를 참조하십시오.
- AWS IAM Identity Center - 자세한 지침은 [IAM ID 센터를 온프레미스 Active Directory에 연결](#) 섹션을 참조하십시오.
- AWS License Manager - 자세한 내용은 의 [사용자 기반](#) 구독을 참조하십시오. AWS License Manager
- AWS Management Console — 자세한 내용은 을 참조하십시오. [AD 보안 인증을 사용한 AWS Management Console 액세스 활성화](#)
- FSx for Windows File Server – 자세한 정보는 [FSx for Windows File Server란 무엇인가요?](#)를 참조하세요.
- WorkSpaces - 자세한 지침은 [AWS 관리형 Microsoft AD를 Workspace 사용하여 실행](#)을 참조하십시오.

Active Directory를 사용하는 사용자 지정 및 상용 off-the-shelf 응용 프로그램의 규모 때문에 Microsoft Active Directory용 AWS Directory Service (AWS 관리형 Microsoft AD) 와의 타사 응용 프로그램 호환성에 대한 형식적 또는 광범위한 검증을 수행하지 AWS 않으며 수행할 수도 없습니다. 고객이 직면할 수 있는 잠재적인 응용 프로그램 설치 문제를 해결하기 위해 고객과 AWS 협력하고 있지만, 모든 응용 프로그램이 AWS Managed Microsoft AD와 호환되거나 계속 호환될 것이라고 보장할 수는 없습니다.

AWS 관리형 Microsoft AD와 호환되는 타사 애플리케이션은 다음과 같습니다.

- Active Directory 기반 정품 인증(ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server(.NET)
- Microsoft Entra(이전의 명칭은 Azure Active Directory (AzureAD))
- Microsoft Entra Connect(이전 명칭) Azure Active Directory Connect
- 분산 파일 시스템 복제(DFSR)
- 분산 파일 시스템 네임스페이스(DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(SQL Server 올웨이즈 온 가용성 그룹 포함)
- Microsoft System Center Configuration Manager(SCCM) - SCCM을 배포하는 사용자는 AWS 위임 시스템 관리 관리자 그룹의 구성원이어야 합니다.
- Microsoft Windows and Windows Server OS
- Office 365

이러한 애플리케이션의 모든 구성이 지원되지 않을 수 있다는 점에 유의하세요.

호환성 지침

애플리케이션에 호환되지 않는 구성이 있다 하더라도 애플리케이션 배포 구성을 통해 비호환성을 해결할 수 있는 경우가 많습니다. 다음은 애플리케이션이 호환되지 않는 가장 흔한 이유를 설명한 것입니다. 고객은 이 정보를 사용하여 원하는 애플리케이션의 호환성 관련 특성을 조사하고 있을 수 있는 배포 변경 사항을 알아낼 수 있습니다.

- 도메인 관리자 또는 기타 특권 – 일부 애플리케이션에서 도메인 관리자의 자격으로 설치해야 한다고 지시하는 경우가 있습니다. Active Directory를 관리형 서비스로 제공하려면 이 권한 수준을 독점적으로 AWS 제어해야 하므로 이러한 응용 프로그램을 설치하는 도메인 관리자 역할을 할 수는 없습니다. 하지만 설치 수행자에게 권한이 낮고 AWS 지원되는 특정 권한을 위임하여 이러한 응용 프로그램을 설치할 수 있는 경우가 많습니다. 애플리케이션에 필요한 권한이 정확히 무엇인지에 관한 세부 정보는 해당 애플리케이션 공급자에게 문의하세요. AWS 위임할 수 있는 권한에 대한 자세한 내용은 참조하십시오. [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)

- 권한이 있는 Active Directory 컨테이너에 대한 액세스 — AWS 관리형 Microsoft AD는 디렉터리 내에서 사용자가 모든 관리 권한을 갖는 조직 구성 단위 (OU) 를 제공합니다. 권한을 생성하거나 작성할 필요가 없고 Active Directory 트리에서 사용자의 OU보다 상위에서 있는 컨테이너에 대한 읽기 권한이 제한될 수 있습니다. 사용자에게 권한이 없는 컨테이너를 생성하거나 그러한 컨테이너에 액세스하는 애플리케이션은 작동하지 않을 수 있습니다. 그러나 그러한 애플리케이션은 사용자가 대체 방법으로 OU에 생성하는 컨테이너를 사용할 수 있는 경우가 많습니다. 해당 애플리케이션 공급자에게 문의하여 대체 방법으로 OU에 컨테이너를 생성하여 사용할 수 있는 방법을 찾으세요. OU 관리에 관한 자세한 내용은 [AWS 관리형 Microsoft AD를 관리하는 방법](#) 단원을 참조하세요.
- 설치 워크플로 중 스키마 변경 - 일부 Active Directory 응용 프로그램에서는 기본 Active Directory 스키마를 변경해야 하며 이러한 변경 내용을 응용 프로그램 설치 워크플로의 일부로 설치하려고 할 수 있습니다. 스키마 확장의 권한 특성으로 인해 콘솔 AWS Directory Service, CLI 또는 SDK를 통해서만 경량 디렉터리 교환 형식 (LDIF) 파일을 가져와서 이를 AWS 가능하게 합니다. 이러한 응용 프로그램에는 스키마 업데이트 프로세스를 통해 디렉토리에 적용할 수 있는 LDIF 파일이 함께 제공되는 경우가 많습니다. AWS Directory Service LDIF 가져오기 프로세스 작동 방식에 관한 자세한 내용은 [자습서: AWS 관리형 Microsoft AD 스키마 확장](#) 단원을 참조하세요. 설치 프로세스 중에 스키마 설치를 무시하는 방식으로 애플리케이션을 설치할 수 있습니다.

호환되지 않는 것으로 알려진 애플리케이션

다음은 AWS 관리형 Microsoft AD와 호환되는 구성을 찾지 못했지만 일반적으로 요청되는 상용 off-the-shelf 응용 프로그램 목록입니다. AWS 비생산적인 작업을 피할 수 있도록 편의를 위해 단독 재량에 따라 이 목록을 수시로 업데이트합니다. AWS 현재 또는 미래의 호환성에 대한 보증이나 클레임 없이 이 정보를 제공하십시오.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

AWS 관리형 Microsoft AD 테스트 랩 튜토리얼

이 섹션에서는 AWS Managed Microsoft AD를 실험해 볼 수 있는 AWS 있는 테스트 랩 환경을 구축하는 데 도움이 되는 일련의 가이드 자습서를 제공합니다.

주제

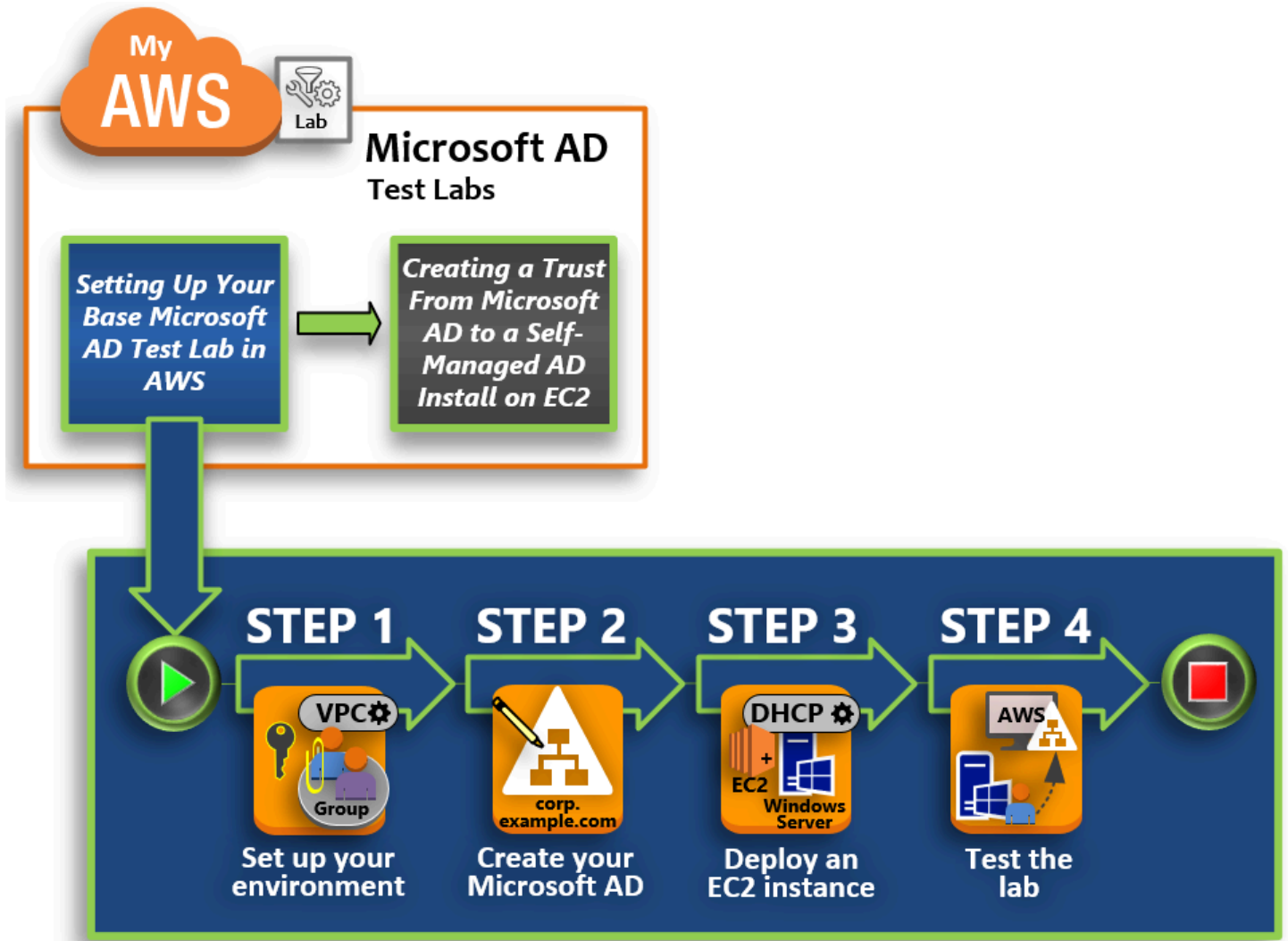
- [자습서: 기본 AWS 관리형 Microsoft AD 테스트 랩 설정하기 AWS](#)

- [자습서: AWS 관리형 Microsoft AD에서 Amazon EC2에 설치된 자체 관리형 Active Directory로의 트러스트 생성](#)

자습서: 기본 AWS 관리형 Microsoft AD 테스트 랩 설정하기 AWS

이 자습서에서는 Windows Server 2019를 실행하는 새 Amazon EC2 인스턴스를 사용하는 새로운 AWS 관리형 Microsoft AD 설치를 준비하기 위한 AWS 환경을 설정하는 방법을 설명합니다. 그런 다음 일반적인 Active Directory 관리 도구를 사용하여 EC2 Windows 인스턴스에서 AWS 관리형 Microsoft AD 환경을 관리하는 방법을 설명합니다. 자습서를 완료할 때쯤이면 네트워크 사전 요구 사항을 설정하고 새 관리형 AWS Microsoft AD 포리스트를 구성한 것입니다.

다음 그림에서 볼 수 있듯이 이 자습서에서 만든 실습은 관리형 AWS Microsoft AD에 대한 실습을 위한 기본 구성 요소입니다. 더 많은 실무 경험이 필요할 경우 나중에 선택적 자습서를 추가할 수 있습니다. 이 자습서 시리즈는 AWS Managed Microsoft AD를 처음 접하고 평가용으로 테스트 랩을 원하는 사람에게 이상적입니다. 이 자습서는 완료하는데 약 1시간이 걸립니다.



1단계: AWS 관리형 Microsoft AD 액티브 디렉터리를 위한 AWS 환경 설정

필수 작업을 완료한 후 EC2 인스턴스에서 Amazon VPC를 생성하고 구성합니다.

2단계: AWS 관리형 Microsoft AD 액티브 디렉터리 만들기

이 단계에서는 처음으로 AWS 관리형 Microsoft AD를 설정합니다. AWS

3단계: Amazon EC2 인스턴스를 배포하여 관리형 AWS Microsoft AD 액티브 디렉터리를 관리합니다.

여기서 클라이언트 컴퓨터가 새 도메인에 연결하고 EC2에서 새 Windows Server 시스템을 설정하는 데 필요한 다양한 배포 후 작업을 살펴보겠습니다.

4단계: 기본 테스트 랩이 작동하는지 확인

마지막으로 관리자로서 EC2 내 Windows Server 시스템에 로그인하여 AWS Managed Microsoft AD에 연결할 수 있는지 확인합니다. 테스트에서 랩이 작동하는지 성공적으로 확인되면 계속해서 다른 테스트 랩 가이드 모듈을 추가할 수 있습니다.

필수 조건

이 자습서의 UI 단계를 사용하여 테스트 랩을 생성할 계획이면 이 사전 요구 사항 단원을 건너뛰고 1단계로 넘어갈 수 있습니다. 하지만 AWS CLI 명령어나 AWS Tools for Windows PowerShell 모듈을 사용하여 테스트 랩 환경을 만들려면 먼저 다음을 구성해야 합니다.

- 액세스 및 비밀 액세스 키가 있는 IAM 사용자 — AWS CLI 또는 AWS Tools for Windows PowerShell 모듈을 사용하려면 액세스 키가 있는 IAM 사용자가 필요합니다. 액세스 키가 없는 경우 [액세스 키 생성, 수정, 확인\(AWS Management Console\)](#) 단원을 참조하세요.
- AWS Command Line Interface (선택 사항) — [AWS CLI Windows에서 다운로드 및 설치합니다.](#) 설치가 완료되면 명령 프롬프트 또는 Windows PowerShell 창을 연 다음 다음을 입력합니다 `aws configure`. 설정을 완료하려면 액세스 키와 보안 키가 필요합니다. 이렇게 하는 방법은 첫 번째 사전 요구 사항을 참조하세요. 다음과 같은 메시지가 표시됩니다.
 - AWS 액세스 키 ID [없음]: AKIAIOSFODNN7EXAMPLE
 - AWS 비밀 액세스 키 [없음]: wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
 - Default Region name [None]: us-west-2
 - Default output format [None]: json
- AWS Tools for Windows PowerShell (선택 사항) — <https://aws.amazon.com/powershell/>에서 AWS Tools for Windows PowerShell 의 최신 버전을 다운로드하여 설치한 다음 다음 명령을 실행합니다. 설정을 완료하려면 액세스 키와 보안 키가 필요합니다. 이렇게 하는 방법은 첫 번째 사전 요구 사항을 참조하세요.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJa1rXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

1단계: AWS 관리형 Microsoft AD 액티브 디렉터리를 위한 AWS 환경 설정

AWS 테스트 랩에서 AWS 관리형 Microsoft AD를 생성하려면 먼저 모든 로그인 데이터가 암호화되도록 Amazon EC2 키 쌍을 설정해야 합니다.

키 페어 생성

이미 키 페어가 있다면 이 단계를 생략할 수 있습니다. Amazon EC2 키 페어에 대한 자세한 내용은 키 페어 [생성을](#) 참조하십시오.

키 페어를 생성하는 방법

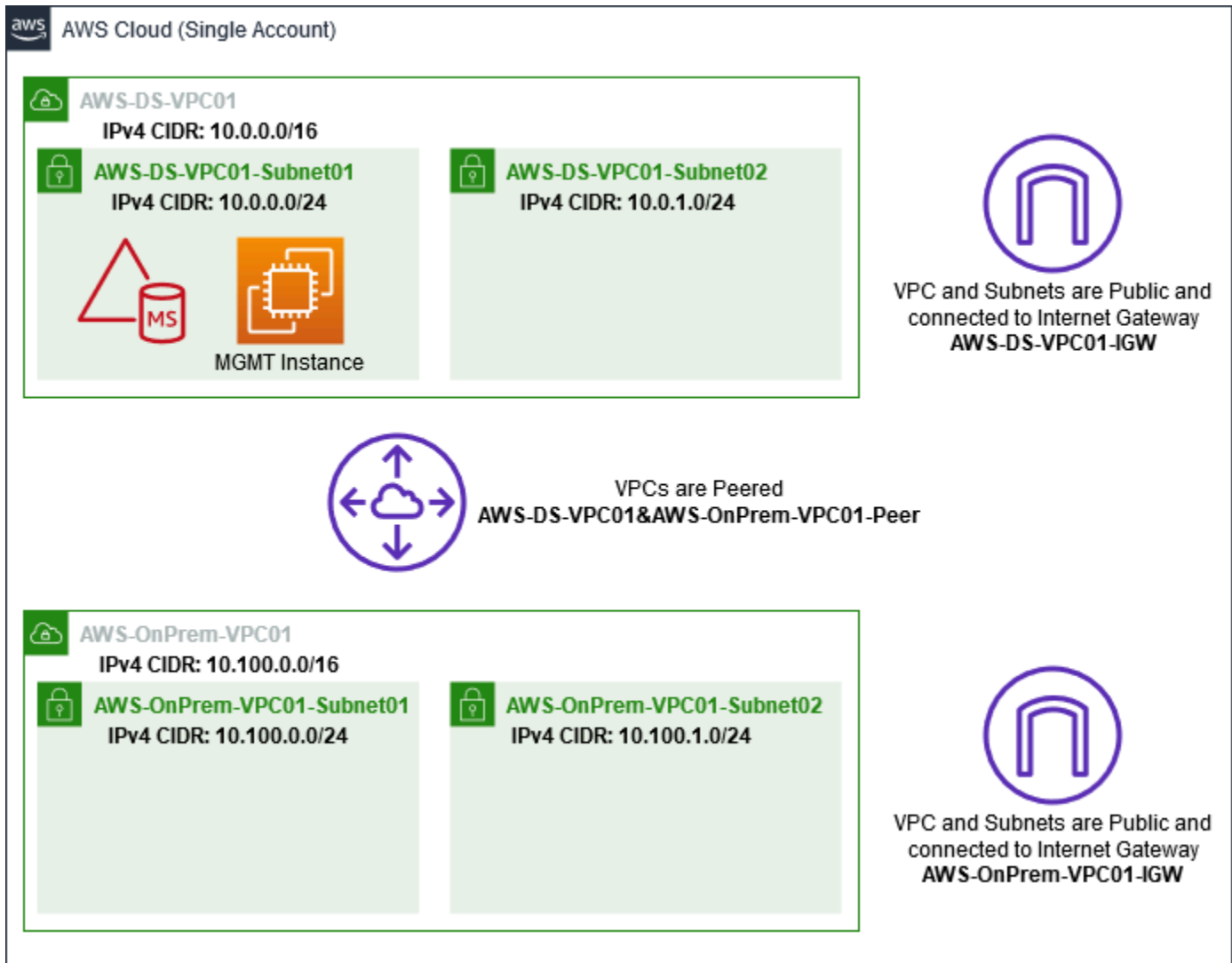
1. AWS Management Console [로그인](#)하고 <https://console.aws.amazon.com/ec2/> 에서 **Amazon EC2 콘솔을 엽니다.**
2. 탐색 창의 [Network & Security]에서 [Key Pairs]를 선택하고 [Create Key Pair]를 선택합니다.
3. 키 페어 이름에 **AWS-DS-KP**를 입력합니다. Key pair file format(키 페어 파일 형식)에 대해 pem을 선택한 다음 생성을 선택합니다.
4. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 파일 이름은 키 페어를 생성할 때 지정한 이름이며 확장명은 .pem입니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다. 인스턴스를 시작할 때 키 페어의 이름을 제공하고, 인스턴스의 암호를 복호화할 때마다 해당 프라이빗 키를 제공해야 합니다.

두 개의 Amazon VPC를 생성, 구성 및 피어링합니다.

다음 그림과 같이 이 다단계 프로세스를 마치면 퍼블릭 VPC 두 개, VPC당 퍼블릭 서브넷 두 개, VPC당 인터넷 게이트웨이 한 개, VPC 간 VPC 피어링 연결 한 개를 생성하고 구성한 것입니다. 단순성 및 비용을 위해 퍼블릭 VPC 및 서브넷을 사용하기로 결정했습니다. 프로덕션 워크로드의 경우 프라이빗 VPC를 사용하는 것이 좋습니다. VPC 보안 향상에 대한 자세한 내용은 [Amazon Virtual Private Cloud의 보안](#)을 참조하세요.



AWS CLI 및 PowerShell 예제는 모두 아래의 VPC 정보를 사용하며 us-west-2에 내장되어 있습니다. 환경을 구축할 [지원되는 리전](#)을 선택할 수 있습니다. 일반적인 내용은 [Amazon VPC란?](#)을 참조하세요.

1단계: 두 개의 VPC 생성

이 단계에서는 다음 표의 지정된 파라미터를 사용하여 동일한 계정에 두 개의 VPC를 생성해야 합니다. AWS 관리형 Microsoft AD는 이 [디렉터리 공유](#) 기능을 통해 별도의 계정을 사용할 수 있도록 지원합니다. 첫 번째 VPC는 관리형 AWS Microsoft AD에 사용됩니다. 두 번째 VPC는 나중에 [자습서: AWS 관리형 Microsoft AD에서 Amazon EC2에 설치된 자체 관리형 Active Directory로의 트러스트 생성](#)에서 사용할 수 있는 리소스에 사용됩니다.

관리형 액티브 디렉터리 VPC 정보	온프레미스 VPC 정보
네임 태그: AWS-DS-VPC01	네임 태그: - -VPC01 AWS OnPrem

관리형 액티브 디렉터리 VPC 정보	온프레미스 VPC 정보
IPv4 CIDR 블록: 10.0.0.0/16	IPv4 CIDR 블록: 10.100.0.0/16
IPv6 CIDR block: No IPv6 CIDR Block	IPv6 CIDR block: No IPv6 CIDR Block
테넌시: 기본값	테넌시: 기본값

자세한 지침은 [VPC 생성](#)을 참조하세요.

2단계: VPC당 두 개의 서브넷 생성

VPC를 생성한 후에는 다음 표의 지정된 파라미터를 사용하여 VPC당 두 개의 서브넷을 생성해야 합니다. 이 테스트 랩의 경우 각 서브넷은 /24가 됩니다. 이렇게 하면 서브넷당 최대 256개의 주소를 발급할 수 있습니다. 각 서브넷은 별도의 AZ에 있어야 합니다. AZ에서 각 서브넷을 별도로 배치하는 것은 [AWS 관리형 Microsoft AD 사전 요구 사항](#) 중 하나입니다.

AWS-DS-VPC01 서브넷 정보:	AWS- -VPC01 서브넷 정보 OnPrem
네임 태그: -DS-VPC01-서브넷01 AWS	네임 태그: - -VPC01-서브넷01 AWS OnPrem
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS	VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem
가용 영역: us-west-2a	가용 영역: us-west-2a
IPv4 CIDR 블록: 10.0.0.0/24	IPv4 CIDR 블록: 10.100.0.0/24
네임 태그: -DS-VPC01-서브넷02 AWS	네임 태그: - -VPC01-서브넷02 AWS OnPrem
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS	VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem
가용 영역: us-west-2b	가용 영역: us-west-2b
IPv4 CIDR 블록: 10.0.1.0/24	IPv4 CIDR 블록: 10.100.1.0/24

자세한 지침은 [VPC에서 서브넷 생성](#)을 참조하세요.

3단계: 인터넷 게이트웨이 생성 및 VPC에 연결

퍼블릭 VPC를 사용하고 있으므로 다음 표의 지정된 파라미터를 사용하여 인터넷 게이트웨이를 생성하고 VPC에 연결해야 합니다. 이렇게 하면 EC2 인스턴스에 연결하고 관리할 수 있습니다.

AWS-DS-VPC01 인터넷 게이트웨이 정보	AWS- OnPrem -VPC01 인터넷 게이트웨이 정보
네임 태그: -DS-VPC01-IGW AWS	네임 태그: - -VPC01-IGW AWS OnPrem
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS	VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem

자세한 지침은 [인터넷 게이트웨이](#)를 참조하세요.

4단계: -DS-VPC01과 AWS- -VPC01 간의 VPC 피어링 연결을 구성합니다. AWS OnPrem

이전에 이미 두 개의 VPC를 생성했으므로 다음 표의 지정된 파라미터를 사용하여 VPC 피어링으로 이 두 VPC를 함께 네트워크로 연결해야 합니다. VPC를 연결하는 방법은 여러 가지가 있지만 이 자습서에서는 VPC 피어링을 사용합니다. AWS [관리형 Microsoft AD는 VPC를 연결하는 다양한 솔루션을 지원하며, 그 중 일부에는 VPC 피어링, Transit Gateway 및 VPN이 포함됩니다.](#)

피어링 연결 네임 태그: -DS-VPC01& - -VPC01-Peer AWSAWS OnPrem
VPC (요청자): vpc-xxxxxxxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS
계정: 내 계정
리전: 이 리전
VPC (수락자): vpc-xxxxxxxxxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

계정에 있는 다른 VPC와의 VPC 피어링 연결을 생성하는 방법에 대한 지침은 [계정에 있는 다른 VPC와의 VPC 피어링 연결 생성](#)을 참조하세요.

5단계: 각 VPC의 기본 라우팅 테이블에 두 개의 라우팅 추가

이전 단계에서 생성된 인터넷 게이트웨이 및 VPC 피어링 연결이 작동하려면 다음 표의 지정된 파라미터를 사용하여 두 VPC의 기본 라우팅 테이블을 업데이트해야 합니다. 라우팅 테이블에 명시적으로 알려지지 않은 모든 대상으로 라우팅되는 0.0.0.0/0과 위에 설정된 VPC 피어링 연결을 통해 각 VPC로 라우팅되는 10.0.0.0/16 또는 10.100.0.0/16인 두 라우팅을 추가합니다.

VPC 이름 태그 (AWS-DS-VPC01 또는 -VPC01) 로 필터링하여 각 VPC에 대한 올바른 라우팅 테이블을 쉽게 찾을 수 있습니다. AWS OnPrem

AWS-DS-VPC01 라우팅 1 정보	AWS-DS-VPC01 라우팅 2 정보	AWS- -VPC01 라우트 1 정보 OnPrem	AWS- OnPrem - VPC01 루트 2 정보
대상 주소: 0.0.0.0/0	대상 주소: 10.100.0.0/16	대상 주소: 0.0.0.0/0	대상 주소: 10.0.0.0/16
대상: igw-xxxxx xxxxxxxxxxxxxxxxx -DS-VPC01-IGW AWS	대상: pcx-xxxxx xxxxxxxxxxxxxxxxx AWS-DS-VPC01& -VPC01-Peer AWS OnPrem	대상: igw-xxxxx xxxxxxxxxxxxxxxxx -AWS온프레미-VPC01	대상: pcx-xxxxx xxxxxxxxxxxxxxxxx -AWS DS-VPC01& -VPC01-Peer AWS OnPrem

VPC 라우팅 테이블에 라우팅을 추가하는 방법에 대한 지침은 [라우팅 테이블에서 라우팅 추가 및 제거](#)를 참조하세요.

Amazon EC2 인스턴스용 보안 그룹 생성

기본적으로 AWS Managed Microsoft AD는 도메인 컨트롤러 간의 트래픽을 관리하는 보안 그룹을 만듭니다. 이 단원에서는 다음 표의 지정된 파라미터를 사용하여 EC2 인스턴스의 VPC 내 트래픽을 관리하는 데 사용할 두 개의 보안 그룹(VPC당 하나씩)을 생성해야 합니다. 또한 모든 위치에서 들어오는 RDP(3389) 트래픽을 허용하고 로컬 VPC에서 들어오는 모든 트래픽 유형을 허용하는 규칙도 추가합니다. 자세한 내용은 [Amazon EC2 Windows 인스턴스에 대한 Amazon EC2 보안 그룹](#) 단원을 참조하세요.

AWS-DS-VPC01 보안 그룹 정보:

보안 그룹 이름: AWS DS Test Lab 보안 그룹

설명: AWS DS 테스트 랩 보안 그룹

VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS

-DS-VPC01에 대한 보안 그룹 인바운드 규칙 AWS

유형	프로토콜	포트 범위	소스	트래픽 유형
사용자 지정 TCP 규칙	TCP	3389	내 IP	원격 데스크톱
모든 트래픽	모두	모두	10.0.0.0/16	모든 로컬 VPC 트래픽

-DS-VPC01에 대한 보안 그룹 아웃바운드 규칙 AWS

유형	프로토콜	포트 범위	대상	트래픽 유형
모든 트래픽	모두	모두	0.0.0.0/0	모든 트래픽

AWS- -VPC01 보안 그룹 정보: OnPrem

보안 그룹 이름: AWS OnPrem 테스트 랩 보안 그룹.

설명: AWS OnPrem 테스트 랩 보안 그룹.

VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem

- -VPC01에 대한 보안 그룹 인바운드 규칙 AWS OnPrem

유형	프로토콜	포트 범위	소스	트래픽 유형
사용자 지정 TCP 규칙	TCP	3389	내 IP	원격 데스크톱
사용자 지정 TCP 규칙	TCP	53	10.0.0.0/16	DNS
사용자 지정 TCP 규칙	TCP	88	10.0.0.0/16	Kerberos

유형	프로토콜	포트 범위	소스	트래픽 유형
사용자 지정 TCP 규칙	TCP	389	10.0.0.0/16	LDAP
사용자 지정 TCP 규칙	TCP	464	10.0.0.0/16	Kerberos 암호 변경/설정
사용자 지정 TCP 규칙	TCP	445	10.0.0.0/16	SMB/CIFS
사용자 지정 TCP 규칙	TCP	135	10.0.0.0/16	복제
사용자 지정 TCP 규칙	TCP	636	10.0.0.0/16	LDAP SSL
사용자 지정 TCP 규칙	TCP	49152 - 65535	10.0.0.0/16	RPC
사용자 지정 TCP 규칙	TCP	3268 - 3269	10.0.0.0/16	LDAP GC 및 LDAP GC SSL
사용자 지정 UDP 규칙	UDP	53	10.0.0.0/16	DNS
사용자 지정 UDP 규칙	UDP	88	10.0.0.0/16	Kerberos
사용자 지정 UDP 규칙	UDP	123	10.0.0.0/16	Windows 시간
사용자 지정 UDP 규칙	UDP	389	10.0.0.0/16	LDAP
사용자 지정 UDP 규칙	UDP	464	10.0.0.0/16	Kerberos 암호 변경/설정
모든 트래픽	모두	모두	10.100.0.0/16	모든 로컬 VPC 트래픽

--VPC01에 대한 보안 그룹 아웃바운드 규칙 AWS OnPrem

유형	프로토콜	포트 범위	대상	트래픽 유형
모든 트래픽	모두	모두	0.0.0.0/0	모든 트래픽

규칙을 생성하고 보안 그룹에 추가하는 방법에 대한 세부 지침은 [보안 그룹 작업을 참조](#)하세요.

2단계: AWS 관리형 Microsoft AD 액티브 디렉터리 만들기

디렉터리를 생성할 수 있는 방법은 세 가지가 있습니다. 이 자습서에서 권장하는 AWS Management Console 절차를 사용하거나 AWS CLI 또는 AWS Tools for Windows PowerShell 절차를 사용하여 디렉터리를 만들 수 있습니다.

방법 1: AWS 관리형 Microsoft AD 디렉터리 (AWS Management Console) 를 만들려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택한 후 디렉터리 설정을 선택합니다.
2. Select directory type(디렉터리 유형 선택) 페이지에서 AWS Managed Microsoft AD를 선택하고 Next(다음)를 선택합니다.
3. Enter directory information(디렉터리 정보 입력) 페이지에서 다음 정보를 입력한 후 다음을 선택합니다.
 - Edition(에디션)에서 Standard Edition 또는 Enterprise Edition을 선택합니다. 에디션에 대한 자세한 내용은 [AWS Directory Service for Microsoft Active Directory](#)를 참조하세요.
 - Directory DNS name(디렉터리 DNS 이름)에 **corp.example.com**를 입력합니다.
 - Directory NetBIOS name(디렉터리 NetBIOS 이름)에 **corp**를 입력합니다.
 - Directory description(디렉터리 설명)에 **AWS DS Managed**를 입력합니다.
 - [Admin password]에 이 계정에서 사용할 암호를 입력한 다음 [Confirm password]에도 다시 입력합니다. 이 Admin 계정은 디렉터리 생성 프로세스 도중 자동으로 생성됩니다. 암호에 admin이라는 말을 포함할 수 없습니다. 디렉터리 관리자 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 또한 다음 네 범주 중 세 개에 해당하는 문자를 1자 이상 포함해야 합니다.
 - 소문자(a-z)
 - 대문자(A-Z)
 - 숫자(0-9)
 - 영숫자 외의 특수 문자(~!@#%&*_+=`|\(){}[]:;'"<>.,?/)

- VPC 및 서브넷 선택 페이지에서 다음 정보를 제공한 후 다음을 선택합니다.
 - VPC에서 AWS-DS-VPC01로 시작하고 (10.0.0.0/16)으로 끝나는 옵션을 선택합니다.
 - 서브넷에서 10.0.0.0/24 및 10.0.1.0/24 퍼블릭 서브넷을 선택합니다.
- 검토 및 생성 페이지에서 디렉터리 정보를 검토하고 필요한 사항을 변경합니다. 정보가 올바르면 디렉터리 생성을 선택합니다. 디렉터리 생성은 20~40분 정도 걸립니다. 생성이 완료되면 상태 값이 활성 상태로 변경됩니다.

방법 2: AWS 관리형 Microsoft AD (Windows PowerShell) 를 만들려면 (선택 사항)

- Windows PowerShell을 엽니다.
- 다음 명령을 입력합니다. 이전 AWS Management Console 절차의 4단계에서 제공된 값을 사용해야 합니다.

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
-Description "AWS DS Managed" - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

방법 3: AWS 관리형 Microsoft AD (AWS CLI) 를 만들려면 (선택 사항)

- 를 엽니다 AWS CLI.
- 다음 명령을 입력합니다. 이전 AWS Management Console 절차의 4단계에서 제공된 값을 사용해야 합니다.

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

3단계: Amazon EC2 인스턴스를 배포하여 관리형 AWS Microsoft AD 액티브 디렉터리를 관리합니다.

이 실습에서는 어디서나 관리 인스턴스에 쉽게 액세스할 수 있도록 퍼블릭 IP 주소가 있는 Amazon EC2 인스턴스를 사용하고 있습니다. 프로덕션 환경에서는 VPN 또는 AWS Direct Connect 링크를 통해서만 액세스할 수 있는 프라이빗 VPC에 있는 인스턴스를 사용할 수 있습니다. 인스턴스가 퍼블릭 IP 주소를 가져야 하는 요구 사항은 없습니다.

이 단원에서는 클라이언트 컴퓨터가 새 EC2 인스턴스에서 Windows Server를 사용하여 도메인에 연결하는 데 필요한 다양한 배포 후 작업을 살펴보겠습니다. 다음 단계에서 Windows Server를 사용하여 랩이 작동하는지 확인합니다.

선택 사항: AWS-DS-VPC01에 디렉터리에 대한 DHCP 옵션 세트를 생성합니다.

이 선택적 절차에서는 VPC의 EC2 인스턴스가 DNS 확인을 위해 관리형 AWS Microsoft AD를 자동으로 사용하도록 DHCP 옵션 범위를 설정합니다. 자세한 내용은 [DHCP 옵션 세트](#) 단원을 참조하세요.

디렉터리에 대한 DHCP 옵션 세트를 생성하는 방법

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 [DHCP Options Sets]를 선택한 후 [Create DHCP options set]를 선택합니다.
3. Create DHCP options set(DHCP 옵션 세트 생성) 페이지에서 디렉터리에 대해 다음 값을 입력합니다.
 - Name에 **AWS DS DHCP**를 입력합니다.
 - 도메인 이름에 **corp.example.com**를 입력합니다.
 - 도메인 이름 서버에 디렉터리의 DNS 서버가 제공하는 AWS의 IP 주소를 입력합니다.

Note

이러한 주소를 찾으려면 AWS Directory Service 디렉터리 페이지로 이동한 다음 해당하는 디렉터리 ID를 선택합니다. 세부 정보 페이지에서 DNS 주소에 표시된 IP를 식별하고 사용합니다.

또는, 이러한 주소를 찾으려면 AWS Directory Service 디렉터리 페이지로 이동하여 해당하는 디렉터리 ID를 선택합니다. 그런 다음 Scale & share(크기 조정 및 공유)를 선택합니다. 도메인 컨트롤러에서 IP 주소에 표시된 IP를 식별하고 사용합니다.

- NTP servers(NTP 서버), NetBIOS name servers(NetBIOS 이름 서버) 및 NetBIOS node type(NetBIOS 노드 유형) 설정은 공란으로 둡니다.
4. Create DHCP options set(DHCP 옵션 세트 생성)를 선택하고, 닫기를 선택합니다. 새 DHCP 옵션 세트가 DHCP 옵션 목록에 나타납니다.
 5. 새로운 DHCP 옵션 세트의 ID를 기록해 두세요(dopt-**xxxxxxxx**). 이 절차의 끝부분에서 새 옵션 세트를 VPC와 연결할 때 이 ID를 사용합니다.

Note

원활한 도메인 조인은 DHCP 옵션 세트를 구성하지 않고도 작동합니다.

6. 탐색 창에서 사용자 VPC(Your VPCs)를 선택합니다.
7. VPC 목록에서, AWS DS VPC, 작업, Edit DHCP Options Set(DHCP 옵션 세트 편집)를 차례대로 선택합니다.
8. Edit DHCP Options Set(DHCP 옵션 세트 편집) 대화 상자에 5단계에서 기록한 옵션 세트를 선택하고 저장을 선택합니다.

Windows 인스턴스를 AWS 관리형 Microsoft AD 도메인에 조인하는 역할을 생성합니다.

이 절차를 사용하여 Amazon EC2 Windows 인스턴스를 도메인에 조인하는 역할을 구성할 수 있습니다. 자세한 정보는 [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#)을 참조하세요.

Windows 인스턴스를 도메인에 조인하기 위해 EC2를 구성하려면

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔티티 유형 선택 아래에서 AWS 서비스를 선택합니다.
4. 이 역할을 사용할 서비스 선택에서 EC2와 다음: 권한을 차례대로 선택합니다.
5. 연결된 권한 정책 페이지에서 다음을 수행합니다.
 - ManagedInstanceCoreAmazonSSM 관리형 정책 옆의 상자를 선택합니다. 이 정책에서는 Systems Manager 서비스 사용에 필요한 최소 권한을 제공합니다.
 - DirectoryServiceAccessAmazonSSM 관리형 정책 옆의 상자를 선택합니다. 이 정책은 AWS Directory Service에 의해 관리되는 Active Directory에 인스턴스를 조인할 수 있는 권한을 제공합니다.

Systems Manager에 대한 IAM 인스턴스 프로파일에 연결할 수 있는 관리형 정책 및 기타 정책에 대한 정보는 AWS Systems Manager 사용 설명서의 [Systems Manager에 대한 IAM 인스턴스 프로파일 생성](#)을 참조하세요. 관리형 정책에 대한 정보는 IAM 사용 설명서에서 [AWS 관리형 정책](#)을 참조하세요.

6. 다음: 태그를 선택합니다.

7. (선택 사항) 이 역할에 대한 액세스를 구성, 추적 또는 제어할 태그-키 값 페어를 하나 이상 추가한 후 다음: 검토를 선택합니다.
8. 역할 이름에 인스턴스를 도메인에 조인하는 데 사용된다고 설명하는 역할 이름 (예: EC2) 을 입력합니다. DomainJoin
9. (선택 사항)역할 설명에 설명을 입력합니다.
10. 역할 생성을 선택합니다. 그러면 역할 페이지로 돌아갑니다.

Amazon EC2 인스턴스를 생성하고 자동으로 디렉터리에 가입합니다.

이 절차에서는 나중에 Active Directory에서 사용자, 그룹 및 정책을 관리하는 데 사용할 수 있는 EC2 인스턴스에 Windows Server 시스템을 설정합니다.

EC2 인스턴스를 생성하고 자동으로 디렉터리를 조인하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 인스턴스 시작을 선택합니다.
3. 1단계 페이지의 Microsoft Windows Server 2019 Base - ami-**xxxxxxxxxxxxxxxxxxxx** 옆에서 선택을 선택합니다.
4. 2단계 페이지에서 t3.micro(이보다 더 큰 인스턴스 유형을 선택할 수 있음)를 선택한 다음 Next: Configure Instance Details(다음: 인스턴스 세부 정보 구성)를 선택합니다.
5. [Step 3] 페이지에서 다음을 수행합니다.
 - 네트워크에서 AWS-DS-VPC01로 끝나는 VPC(예: vpc-**xxxxxxxxxxxxxxxxxxxx** | AWS-DS-VPC01)를 선택합니다.
 - 서브넷에서 Public subnet 1(퍼블릭 서브넷 1)을 선택합니다. 이 서브넷은 선호하는 가용 영역용으로 미리 구성되어야 합니다(예: subnet-**xxxxxxxxxxxxxxxxxxxx** | AWS-DS-VPC01-Subnet01 | **us-west-2a**).
 - [Auto-assign Public IP]에서 [Enable]을 선택합니다(서브넷 설정이 기본적으로 [Enable]로 설정되지 않은 경우).
 - 도메인 조인 디렉터리에서 corp.example.com (d-**xxxxxxxxxx**)을 선택합니다.
 - IAM 역할의 경우 인스턴스 역할에 부여한 이름 (예: EC2) 을 [Windows 인스턴스를 AWS 관리형 Microsoft AD 도메인에 조인하는 역할을 생성합니다.](#) 선택합니다. DomainJoin
 - 나머지 설정은 기본값을 유지합니다.
 - 다음: 스토리지 추가를 선택합니다.
6. [Step 4] 페이지에서 기본 설정을 유지하고 [Next: Add Tags]를 선택합니다.

7. [Step 5] 페이지에서 [Add Tag]를 선택합니다. 키 아래에서 **corp.example.com-mgmt**를 입력하고 Next: Configure Security Group(다음: 보안 그룹 구성)을 선택합니다.
8. Step 6 페이지에서 Select an existing security group을 선택하고 AWS DS RDP Security Group(앞서 [기본 자습서](#)에서 설정한 항목)을 선택한 다음, Review and Launch를 선택하여 인스턴스를 검토합니다.
9. [Step 7] 페이지에서 페이지를 검토한 다음 [Launch]를 선택합니다.
10. [Select an existing key pair or create a new key pair] 대화 상자에서 다음을 수행합니다.
 - [Choose an existing key pair]를 선택합니다.
 - Select a key pair에서 AWS-DS-KP를 선택합니다.
 - [I acknowledge...] 확인란을 선택합니다.
 - 인스턴스 시작(Launch Instances)을 선택합니다.
11. 인스턴스 보기를 선택하여 Amazon EC2 콘솔로 돌아가 배포 상태를 확인합니다.

EC2 인스턴스에 Active Directory 도구 설치

EC2 인스턴스에 Active Directory 도메인 관리 도구를 설치하는 방법은 두 가지가 있습니다. 서버 관리자 UI (이 자습서에서는 권장) 또는 을 사용할 수 있습니다. Windows PowerShell

EC2 인스턴스에 Active Directory 도구를 설치하려면(Server Manager)

1. Amazon EC2 콘솔에서 Instances를 선택하고, 방금 생성한 인스턴스를 선택한 다음 Connect를 선택합니다.
2. 사용자 인스턴스에 연결 대화 상자에서 암호 가져오기를 선택하여 아직 암호를 검색하지 않은 경우 암호를 검색한 다음 원격 데스크톱 파일 다운로드를 선택합니다.
3. Windows Security 대화 상자에서 Windows Server 컴퓨터에 대한 로컬 관리자 자격 증명을 입력하여 로그인합니다(예: **administrator**).
4. [Start] 메뉴에서 [Server Manager]를 선택합니다.
5. [Dashboard]에서 [Add Roles and Features]를 선택합니다.
6. [Add Roles and Features Wizard]에서 [Next]를 선택합니다.
7. [Select installation type] 페이지에서 [Role-based or feature-based installation]을 선택하고 [Next]를 선택합니다.
8. [Select destination server] 페이지에서 로컬 서버가 선택되어 있는지 확인한 다음 [Next]를 선택합니다.

9. [Select server roles] 페이지에서 [Next]를 선택합니다.
10. [Select features] 페이지에서 다음을 수행합니다.
 - [Group Policy Management] 확인란을 선택합니다.
 - [Remote Server Administration Tools]를 확장한 다음 [Role Administration Tools]를 확장합니다.
 - [AD DS and AD LDS Tools] 확인란을 선택합니다.
 - [DNS Server Tools] 확인란을 선택합니다.
 - 다음을 선택합니다.
11. [Confirm installation selections] 페이지에서 정보를 검토하고 [Install]을 선택합니다. 기능 설치가 완료되면 [Start] 메뉴의 [Windows Administrative Tools] 폴더에서 다음과 같은 새 도구 또는 스냅인을 사용할 수 있습니다.
 - Active Directory Administrative Center
 - Active Directory Domains and Trusts
 - 액티브 디렉터리 모듈: Windows PowerShell
 - Active Directory 사이트 및 서비스
 - Active Directory Users and Computers
 - ADSI Edit
 - DNS
 - 그룹 정책 관리

EC2 인스턴스에 Active Directory 도구를 설치하려면 (Windows PowerShell) (선택 사항)

1. Start Windows PowerShell.
2. 다음 명령을 입력합니다.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
```

4단계: 기본 테스트 랩이 작동하는지 확인

추가 테스트 랩 가이드 모듈을 설치하기 전에 다음 절차를 사용하여 테스트 랩이 성공적으로 설정되었는지 확인합니다. 이 절차를 통해 Windows 서버가 적절하게 구성되어 있고 corp.example.com 도메인

에 연결할 수 있으며 관리형 Microsoft AD 포리스트를 관리하는 데 사용할 수 있는지 확인할 수 있습니다. AWS

테스트 랩이 작동하는지 확인하려면

1. 로컬 관리자로 로그인한 EC2 인스턴스에서 로그아웃합니다.
2. Amazon EC2 콘솔로 돌아가 탐색 창에서 Instances를 선택합니다. 그럼 다음 방금 생성한 인스턴스를 선택합니다. 연결을 선택합니다.
3. [Connect To Your Instance] 대화 상자에서 [Download Remote Desktop File]을 선택합니다.
4. Windows Security 대화 상자에서 CORP 도메인에 대한 관리자 자격 증명을 입력하여 로그인합니다(예: **corp\admin**).
5. 로그인 후 [Start] 메뉴의 [Windows Administrative Tools] 아래에서 [Active Directory Users and Computers]를 선택합니다.
6. 새 도메인과 연결된 모든 기본 OU 및 계정과 함께 [corp.example.com]이 표시될 것입니다. 도메인 컨트롤러에서 이 자습서의 2단계에서 AWS 관리형 Microsoft AD를 만들 때 자동으로 생성된 도메인 컨트롤러의 이름을 확인합니다.

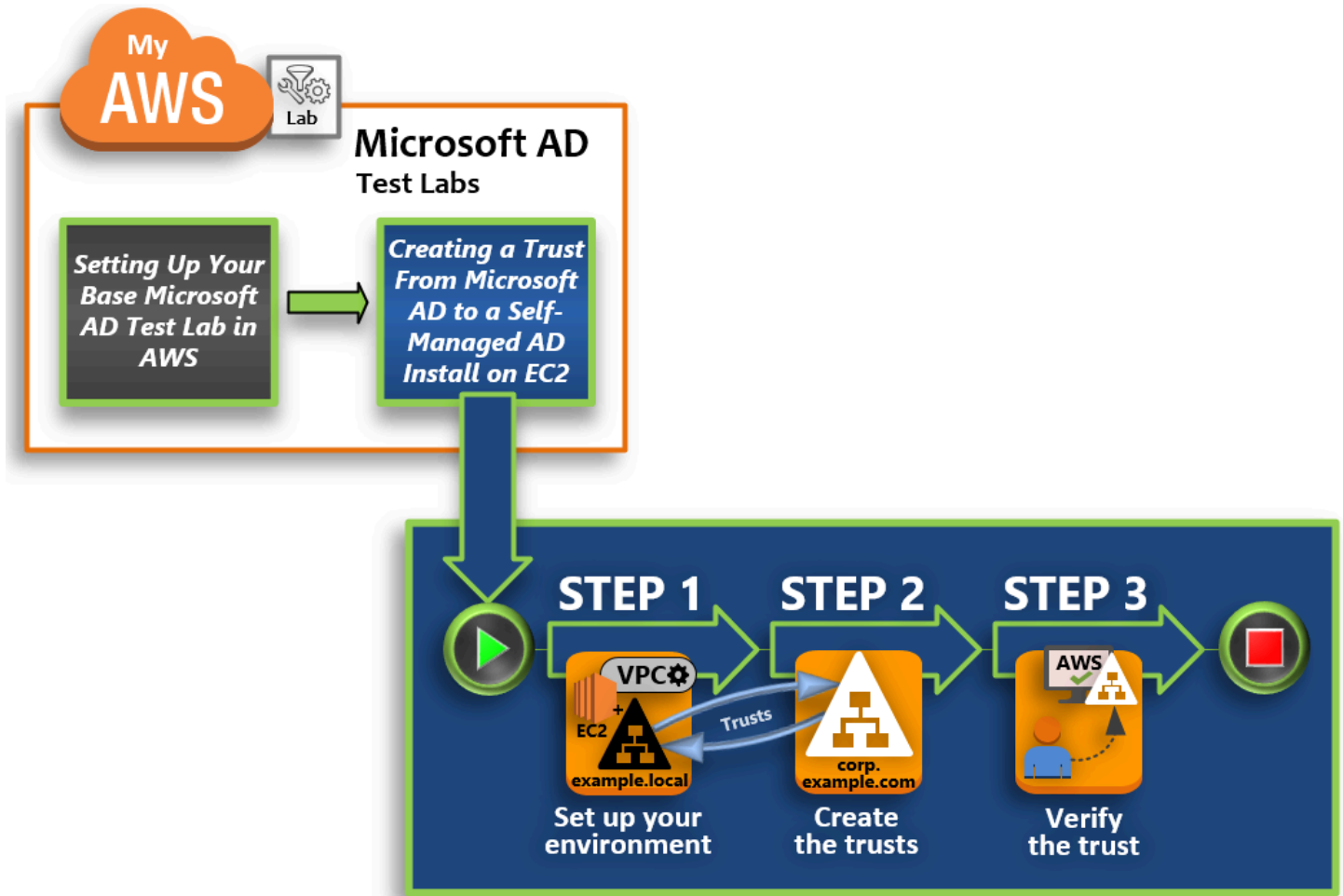
축하합니다! AWS 관리형 Microsoft AD 기본 테스트 랩 환경이 이제 구성되었습니다. 이 시리즈의 다음 테스트 랩을 추가할 준비가 되었습니다.

다음 자습서: [자습서: AWS 관리형 Microsoft AD에서 Amazon EC2에 설치된 자체 관리형 Active Directory로의 트러스트 생성](#)

자습서: AWS 관리형 Microsoft AD에서 Amazon EC2에 설치된 자체 관리형 Active Directory로의 트러스트 생성

이 자습서에서는 [기본 자습서에서](#) 만든 Microsoft Active AWS Directory용 디렉터리 서비스 포리스트 간에 트러스트를 만드는 방법을 알아봅니다. 또한 Amazon EC2 내 Windows Server에서 새 네이티브 Active Directory 포리스트를 생성하는 방법도 알아봅니다. 다음 그림에서 볼 수 있듯이 이 자습서에서 만드는 실습은 완전한 AWS Managed Microsoft AD 테스트 실습을 설정하는 데 필요한 두 번째 구성 요소입니다. 테스트 랩을 사용하여 순수 클라우드 또는 하이브리드 클라우드 AWS 기반 솔루션을 테스트할 수 있습니다.

이 자습서는 한 번만 생성해야 합니다. 그런 다음 더 많은 환경이 필요할 경우 선택적 자습서를 추가할 수 있습니다.



1단계: 신뢰 관계 환경 설정

새 Active Directory 포리스트와 [기본 자습서](#)에서 만든 AWS Managed Microsoft AD 포리스트 간에 신뢰 관계를 설정하려면 먼저 Amazon EC2 환경을 준비해야 합니다. 그러려면 먼저 Windows Server 2019 서버를 생성하고, 해당 서버를 도메인 컨트롤러로 승격한 다음 이에 따라 VPC를 구성합니다.

2단계: 신뢰 관계 생성

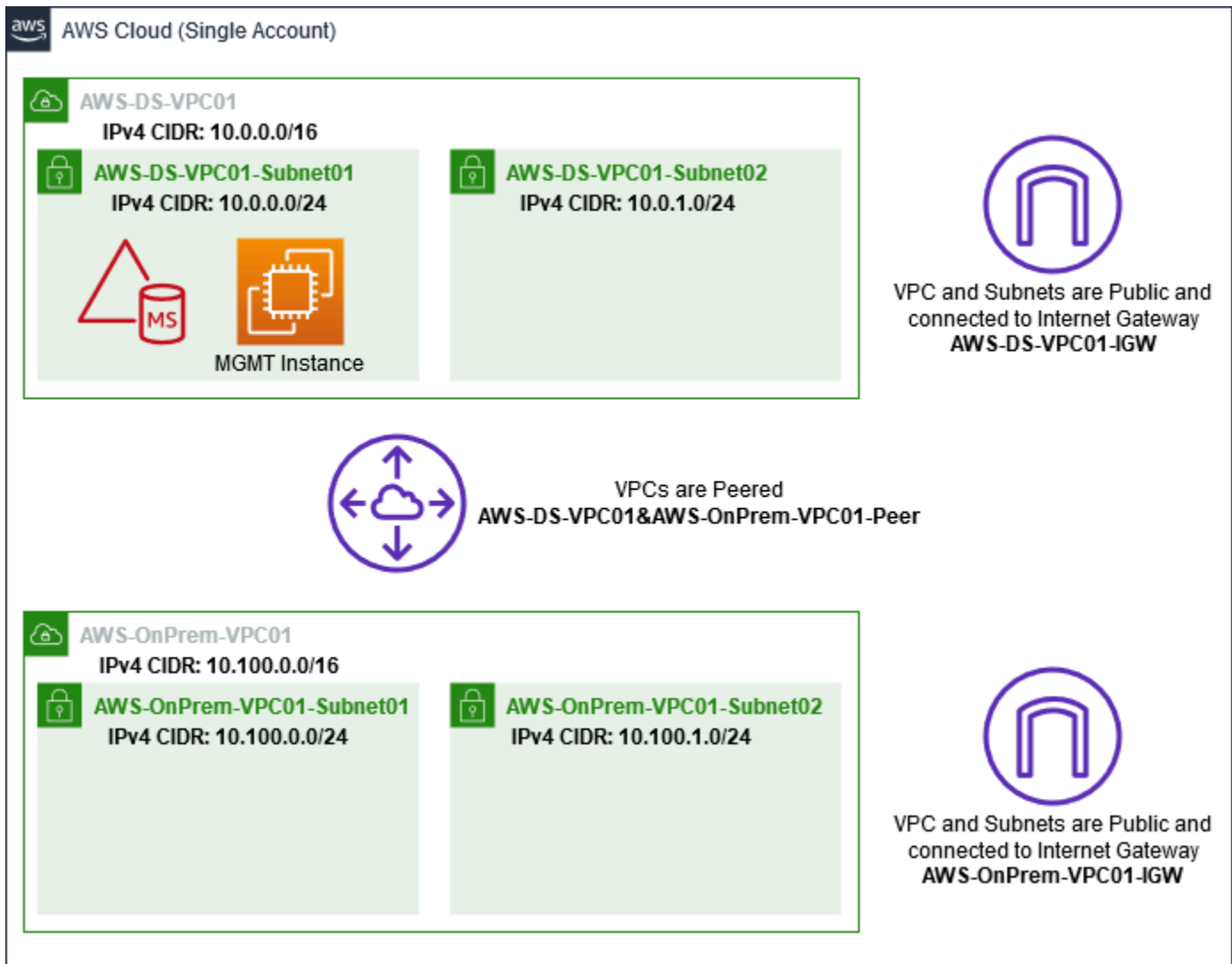
이 단계에서는 Amazon EC2에서 호스팅되는 새로 만든 Active Directory 포리스트와 에서 AWS 호스팅되는 관리형 Microsoft AD 포리스트 간에 양방향 포리스트 신뢰 관계를 생성합니다. AWS

3단계: 신뢰 관계 확인

마지막으로 관리자는 AWS Directory Service 콘솔을 사용하여 새 트러스트가 작동 중인지 확인합니다.

1단계: 신뢰 관계 환경 설정

이 섹션에서는 Amazon EC2 환경을 설정하고, 새 포리스트를 배포하고, VPC를 사용하여 트러스트를 받을 수 있도록 준비합니다. AWS



Windows Server 2019 EC2 인스턴스 생성

다음 절차를 사용하여 Amazon EC2에서 Windows Server 2019 멤버 서버를 생성합니다.

Windows Server 2019 EC2 인스턴스를 생성하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. Amazon EC2 콘솔에서 인스턴스 시작을 선택합니다.
3. 1단계 페이지의 목록에서 Microsoft Windows Server 2019 Base - ami-**xxxxxxxxxxxxxxxxxxxxxx**를 찾습니다. 그런 다음 선택을 선택합니다.

4. [Step 2] 페이지에서 [t2.large]를 선택하고 [Next: Configure Instance Details]를 선택합니다.
5. [Step 3] 페이지에서 다음을 수행합니다.
 - 네트워크에서는 [vpc- xxxxxxxxxxxxxxxxxxxxxxxx AWS- OnPrem -VPC01 \(이전에 기본 자습서에서 설정함\)](#) 을 선택합니다.
 - **#### ## ###- xxxxxxxxxxxxxxxxxxxx | - -VPC01-###01 | - -VPC01# #####.**
AWS OnPrem AWS OnPrem
 - [Auto-assign Public IP] 목록에서 [Enable]을 선택합니다(서브넷 설정이 기본적으로 [Enable]로 설정되지 않은 경우).
 - 나머지 설정은 기본값을 유지합니다.
 - 다음: 스토리지 추가를 선택합니다.
6. [Step 4] 페이지에서 기본 설정을 유지하고 [Next: Add Tags]를 선택합니다.
7. [Step 5] 페이지에서 [Add Tag]를 선택합니다. 키 아래에서 **example.local-DC01**를 입력하고 Next: Configure Security Group(다음: 보안 그룹 구성)을 선택합니다.
8. Step 6 페이지에서 Select an existing security group을 선택하고 AWS On-Prem Test Lab Security Group(앞서 [기본 자습서](#)에서 설정한 항목)을 선택한 다음, Review and Launch를 선택하여 인스턴스를 검토합니다.
9. [Step 7] 페이지에서 페이지를 검토한 다음 [Launch]를 선택합니다.
10. [Select an existing key pair or create a new key pair] 대화 상자에서 다음을 수행합니다.
 - [Choose an existing key pair]를 선택합니다.
 - Select a key pair 아래에서 AWS-DS-KP(앞서 [기본 자습서](#)에서 설정한 항목)를 선택합니다.
 - [I acknowledge...] 확인란을 선택합니다.
 - 인스턴스 시작(Launch Instances)을 선택합니다.
11. 인스턴스 보기를 선택하여 Amazon EC2 콘솔로 돌아가 배포 상태를 확인합니다.

서버를 도메인 컨트롤러로 승격시킵니다

신뢰 관계를 생성하려면 먼저 새 포리스트에 대한 첫 번째 도메인 컨트롤러를 빌드 및 배포해야 합니다. 이 절차에서 새 Active Directory 포리스트를 구성하고, DNS를 설치하고, 이름 확인에 DNS 서버를 사용하도록 이 서버를 설정합니다. 이 절차의 끝부분에서 서버를 다시 부팅해야 합니다.

Note

온프레미스 네트워크와 함께 AWS 복제되는 도메인 컨트롤러를 만들려면 먼저 EC2 인스턴스를 온프레미스 도메인에 수동으로 조인해야 합니다. 그런 다음 서버를 도메인 컨트롤러로 승격할 수 있습니다.

서버를 도메인 컨트롤러로 승격하려면

1. Amazon EC2 콘솔에서 Instances를 선택하고, 방금 생성한 인스턴스를 선택한 다음 Connect를 선택합니다.
2. [Connect To Your Instance] 대화 상자에서 [Download Remote Desktop File]을 선택합니다.
3. Windows Security 대화 상자에서 Windows Server 컴퓨터에 대한 로컬 관리자 자격 증명을 입력하여 로그인합니다(예: **administrator**). 아직 로컬 관리자 암호가 없는 경우 Amazon EC2 콘솔로 돌아가 인스턴스를 마우스 오른쪽 버튼으로 클릭하여 Windows 암호 가져오기를 선택합니다. AWS DS KP.pem 파일 또는 개인 .pem 키로 이동한 다음 [Decrypt Password]를 선택합니다.
4. [Start] 메뉴에서 [Server Manager]를 선택합니다.
5. [Dashboard]에서 [Add Roles and Features]를 선택합니다.
6. [Add Roles and Features Wizard]에서 [Next]를 선택합니다.
7. [Select installation type] 페이지에서 [Role-based or feature-based installation]을 선택하고 [Next]를 선택합니다.
8. [Select destination server] 페이지에서 로컬 서버가 선택되어 있는지 확인한 다음 [Next]를 선택합니다.
9. [Select server roles] 페이지에서 [Active Directory Domain Services]를 선택합니다. [Add Roles and Features Wizard] 대화 상자에서 [Include management tools (if applicable)] 확인란이 선택되어 있는지 확인합니다. [Add Features]를 선택한 다음 [Next]를 선택합니다.
10. [Select features] 페이지에서 [Next]를 선택합니다.
11. [Active Directory Domain Services] 페이지에서 [Next]를 선택합니다.
12. [Confirm installation selections] 페이지에서 [Install]을 선택합니다.
13. Active Directory 바이너리가 설치되면 [Close]를 선택합니다.
14. Server Manager가 열리면 Manage 옆의 상단에서 플래그를 찾습니다. 이 플래그가 노란색으로 바뀌면 서버를 승격할 준비가 된 것입니다.
15. 노란색 플래그를 선택한 다음 [Promote this server to a domain controller]를 선택합니다.

16. [Deployment Configuration] 페이지에서 [Add a new forest]를 선택합니다. Root domain name(루트 도메인 이름)에 **example.local**를 입력하고 다음을 선택합니다.
17. [Domain Controller Options] 페이지에서 다음을 수행합니다.
 - [Forest functional level] 및 [Domain functional level] 모두에서 [Windows Server 2016]을 선택합니다.
 - 도메인 컨트롤러 기능 지정에서 DNS 서버와 글로벌 카탈로그 (GC) 가 모두 선택되어 있는지 확인합니다.
 - DSRM(Directory Services Restore Mode) 암호를 입력하고 확인합니다. 다음을 선택합니다.
18. [DNS Options] 페이지에서 위임에 대한 경고를 무시하고 [Next]를 선택합니다.
19. 추가 옵션 페이지에서 EXAMPLE이 NetBios 도메인 이름으로 나열되어 있는지 확인합니다.
20. [Paths] 페이지에서 기본값을 그대로 두고 [Next]를 선택합니다.
21. [Review Options] 페이지에서 [Next]를 선택합니다. 이제 서버가 도메인 컨트롤러 전제 조건이 모두 충족되었는지 확인합니다. 일부 경고가 표시될 수 있지만 무시해도 무방합니다.
22. 설치를 선택합니다. 설치가 완료되면 서버가 다시 부팅한 후 도메인 컨트롤러가 동작 상태가 됩니다.

VPC 구성

다음 세 절차에서 AWS와 연결을 위해 VPC를 구성하는 단계를 안내합니다.

VPC 아웃바운드 규칙을 구성하는 방법

1. [AWS Directory Service 콘솔에서 이전에 기본 자습서에서 만든 corp.example.com의 AWS 관리형 Microsoft AD 디렉터리 ID를 기록해 둡니다.](#)
2. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
3. 탐색 창에서 보안 그룹(Security Groups)을 선택합니다.
4. AWS 관리형 Microsoft AD 디렉터리 ID를 검색하세요. 검색 결과에서 "AWS created security group for d-xxxxxx directory controllers"라는 설명이 붙은 항목을 선택합니다.

Note

이 보안 그룹은 처음 디렉터리를 생성할 때 자동으로 생성된 것입니다.

5. 해당 보안 그룹 아래에서 [Outbound Rules] 탭을 선택합니다. [Edit]를 선택하고 [Add another rule]을 선택한 후 다음 값을 추가합니다.

- [Type]에서 [All Traffic]을 선택합니다.
- [Destination]에 **0.0.0.0/0**을 입력합니다.
- 나머지 설정은 기본값을 유지합니다.
- 저장을 선택합니다.

Kerberos 사전 인증이 활성화되었는지 확인하려면

1. [example.local] 도메인 컨트롤러에서 Server Manager를 엽니다.
2. [Tools] 메뉴에서 [Active Directory Users and Computers]를 선택합니다.
3. Users 디렉터리로 이동하여 임의의 사용자를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택한 후 계정 탭을 선택합니다. [Account options] 목록을 아래로 스크롤해서 [Do not require Kerberos preauthentication]가 선택되지 않았는지 확인합니다.
4. corp.example.com-mgmt 인스턴스의 corp.example.com 도메인에 대해서도 동일한 단계를 수행합니다.

DNS 조건부 전달자를 구성하려면

Note

조건부 전달자는 쿼리의 DNS 도메인 이름에 따라 DNS 쿼리를 전달하는 데 사용되는 네트워크의 DNS 서버입니다. 예를 들어 widgets.example.com으로 끝나는 이름에 대해 수신하는 모든 쿼리를 특정 DNS 서버의 IP 주소 또는 여러 DNS 서버의 IP 주소로 전달하도록 DNS 서버를 구성할 수 있습니다.

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. AWS 관리형 Microsoft AD의 디렉터리 ID를 선택합니다.
4. 디렉터리의 정규화된 도메인 이름(FQDN) "corp.example.com"과 DNS 주소를 기록해 둡니다.
5. 이제 [example.local] 도메인 컨트롤러로 돌아가 Server Manager를 엽니다.
6. [Tools] 메뉴에서 [DNS]를 선택합니다.
7. 콘솔 트리에서 신뢰 관계를 설정 중인 도메인의 DNS 서버를 확장하고 [Conditional Forwarders]로 이동합니다.

8. [Conditional Forwarders]를 마우스 오른쪽 버튼으로 클릭하고 [New Conditional Forwarder]를 선택합니다.
9. DNS 도메인에 **corp.example.com**를 입력합니다.
10. 마스터 서버의 IP 주소에서 <추가하려면 여기를 클릭하십시오...> 를 선택합니다. >, 이전 절차에서 기록해 둔 AWS 관리형 Microsoft AD 디렉터리의 첫 번째 DNS 주소를 입력한 다음 Enter 키를 누릅니다. 두 번째 DNS 주소에 대해서도 똑같이 합니다. DNS 주소를 입력하고 나면 "timeout" 또는 "unable to resolve"라는 오류 메시지가 나타날 수 있습니다. 보통 이러한 오류 메시지는 무시해도 좋습니다.
11. [Store this conditional forwarder in Active Directory, and replicate as follows] 확인란을 선택합니다. 드롭다운 메뉴에서 [All DNS servers in this Forest]를 선택한 다음 [OK]를 선택하세요.

2단계: 신뢰 관계 생성

이 단원에서는 2개의 포리스트 신뢰 관계를 생성합니다. 하나의 트러스트는 EC2 인스턴스의 Active Directory 도메인에서 생성되고 다른 하나는 AWS 관리형 Microsoft AD에서 AWS 생성됩니다.



EC2 도메인으로부터 AWS 관리형 Microsoft AD로의 트러스트를 생성하려면

1. example.local에 로그인합니다.
2. Server Manager를 열고 콘솔에서 [DNS]를 선택합니다. 서버에 대해 나열된 IPv4 주소를 기록합니다. 다음 단계에서 corp.example.com에서 example.local 디렉터리로 조건부 전달자를 생성할 때 이 값이 필요합니다.
3. [Tools] 메뉴에서 [Active Directory Domains and Trusts]를 선택합니다.
4. 콘솔 트리에서 example.local을 마우스 오른쪽 버튼으로 클릭하고 [Properties]를 선택합니다.
5. [Trusts] 탭에서 [New Trust]를 선택하고 [Next]를 선택합니다.
6. Trust Name(신뢰 관계 이름) 페이지에서 **corp.example.com**를 입력하고 다음을 선택합니다.
7. [Trust Type] 페이지에서 [Forest trust]를 선택하고 [Next]를 선택합니다.

Note

AWS 관리형 Microsoft AD는 외부 트러스트도 지원합니다. 그렇지만 이 자습서의 목적상 여기에서는 양방향 포리스트 신뢰만 구성합니다.

- [Direction of Trust] 페이지에서 [Two-way]를 선택하고 [Next]를 선택합니다.

Note

나중에 단방향 신뢰를 사용하여 이 작업을 시도하기로 결정한 경우 신뢰 방향이 올바르게 설정되었는지 확인합니다(신뢰하는 도메인에서 발신, 신뢰된 도메인에서 수신). 일반적인 내용은 Microsoft 웹 사이트의 [Understanding Trust Direction\(신뢰 방향 이해\)](#)을 참조하세요.

- [Sides of Trust] 페이지에서 [This domain only]를 선택하고 [Next]를 선택합니다.
- [Outgoing Trust Authentication Level] 페이지에서 [Forest-wide authentication]을 선택하고 [Next]를 선택합니다.

Note

옵션을 선택적으로 인증할 수 있지만 이 자습서의 단순성을 위해 여기서는 사용하지 않는 것이 좋습니다. 이를 구성하면 신뢰하는 도메인이나 포리스트에 있는 컴퓨터 객체(리소스 컴퓨터)에 대한 인증 권한이 명시적으로 부여된 신뢰된 도메인 또는 포리스트의 사용자만 외부 또는 포리스트 신뢰에 액세스할 수 있습니다. 자세한 내용은 [선택적 인증 설정 구성](#)을 참조하세요.

- [Trust Password] 페이지에서 신뢰 관계 암호를 두 번 입력하고 [Next]를 선택합니다. 다음 절차에서 이 암호를 다시 사용합니다.
- [Trust Selections Complete] 페이지에서 결과를 검토한 다음 [Next]를 선택합니다.
- [Trust Creation Complete] 페이지에서 결과를 검토한 다음 [Next]를 선택합니다.
- [Confirm Outgoing Trust] 페이지에서 [No, do not confirm the outgoing trust]를 선택합니다. 그런 다음 [Next]를 선택합니다.
- [Confirm Incoming Trust] 페이지에서 [No, do not confirm the incoming trust]를 선택합니다. 그런 다음 [Next]를 선택합니다.
- [Completing the New Trust Wizard] 페이지에서 [Finish]를 선택합니다.

Note

신뢰 관계는 AWS 관리형 Microsoft AD의 글로벌 기능입니다. [다중 리전 복제](#)를 사용하는 경우 [기본 리전](#)에서 다음 절차를 수행해야 합니다. 변경은 복제된 모든 리전에 자동으로 적용됩니다. 자세한 정보는 [글로벌 기능과 리전별 기능 비교](#)를 참조하세요.

AWS 관리형 Microsoft AD에서 EC2 도메인으로의 트러스트를 생성하려면

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. corp.example.com 디렉터리를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)를 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 신뢰 관계 섹션에서 작업을 선택한 후 신뢰 관계 추가를 선택합니다.
5. [Add a trust relationship] 대화 상자에서 다음을 수행합니다.
 - 트러스트 유형에서 Forest trust(포리스트 신뢰)를 선택합니다.

Note

여기서 선택하는 신뢰 유형이 이전 절차 (EC2 도메인에서 AWS 관리형 Microsoft AD로 트러스트를 생성하려면) 에서 구성한 것과 동일한 신뢰 유형과 일치하는지 확인하십시오.

- Existing or new remote domain name(기존 또는 새 원격 도메인 이름)에 example.local을 입력합니다.
- [Trust password]에서 이전 절차에서 입력한 암호를 입력합니다.
- 신뢰 방향에서 양방향을 선택합니다.

Note

- 나중에 단방향 신뢰를 사용하여 이 작업을 시도하기로 결정한 경우 신뢰 방향이 올바르게 설정되었는지 확인합니다(신뢰하는 도메인에서 발신, 신뢰된 도메인에서 수신).

일반적인 내용은 Microsoft 웹 사이트의 [Understanding trust direction\(신뢰 방향 이해\)](#)을 참조하세요.

- 옵션을 선택적으로 인증할 수 있지만 이 자습서의 단순성을 위해 여기서는 사용하지 않는 것이 좋습니다. 이를 구성하면 신뢰하는 도메인이나 포리스트에 있는 컴퓨터 객체(리소스 컴퓨터)에 대한 인증 권한이 명시적으로 부여된 신뢰된 도메인 또는 포리스트의 사용자만 외부 또는 포리스트 신뢰에 액세스할 수 있습니다. 자세한 내용은 [Configuring selective authentication settings\(선택적 인증 설정 구성\)](#)을 참조하세요.

- 조건부 전달자에 example.local 포리스트 내 DNS 서버의 IP 주소(이전 절차에서 기록한 주소)를 입력합니다.

Note

조건부 전달자는 쿼리의 DNS 도메인 이름에 따라 DNS 쿼리를 전달하는 데 사용되는 네트워크의 DNS 서버입니다. 예를 들어 widgets.example.com으로 끝나는 이름에 대해 수신하는 모든 쿼리를 특정 DNS 서버의 IP 주소 또는 여러 DNS 서버의 IP 주소로 전달하도록 DNS 서버를 구성할 수 있습니다.

6. 추가를 선택합니다.

3단계: 신뢰 관계 확인

이 단원에서는 AWS 와 Amazon EC2의 Active Directory 사이에 신뢰 관계가 성공적으로 설정되었는지 여부를 테스트합니다.

신뢰 관계를 확인하려면

1. [AWS Directory Service 콘솔](#)을 엽니다.
2. corp.example.com 디렉터리를 선택합니다.
3. Directory details(디렉터리 세부 정보) 페이지에서 다음 중 하나를 수행합니다.
 - 다중 리전 복제에 여러 리전이 표시되는 경우 기본 리전을 선택한 다음 네트워킹 및 보안 탭을 선택합니다. 자세한 정보는 [기본 리전과 추가 리전의 비교](#)을 참조하세요.
 - 다중 리전 복제에 리전이 표시되지 않는 경우 네트워킹 및 보안 탭을 선택합니다.
4. 신뢰 관계 섹션에서 방금 생성한 신뢰 관계를 선택합니다.
5. [Actions]를 선택하고 [Verify trust relationship]을 선택합니다.

확인이 완료되면 상태 열에 Verified가 표시됩니다.

축하합니다! 이 자습서를 완료했습니다. 이제 완전히 동작하는 다중 포리스트 Active Directory 환경에서 다양한 시나리오를 테스트할 수 있습니다. 추가 테스트 랩 자습서는 2018에 예정되어 있으니 때때로 새 소식을 확인하시기 바랍니다.

AWS 관리형 Microsoft AD 문제 해결

다음은 디렉터리를 생성 또는 사용할 때 발생할 수 있는 일부 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

AWS 관리형 Microsoft AD와 관련된 문제

일부 문제 해결 작업은 다음을 통해서만 완료할 수 AWS Support 있습니다. 다음은 몇 가지 작업입니다.

- AWS Directory Service 제공된 도메인 컨트롤러 재시작.
- [AWS 관리형 Microsoft AD를 업그레이드하세요.](#)

지원 사례를 만들려면 지원 사례 [만들기 및 사례 관리](#)를 참조하십시오.

Netlogon 및 보안 채널 통신 관련 문제

[CVE-2020-1472](#)에 대한 완화 조치로, Microsoft에서는 도메인 컨트롤러에서 Netlogon 보안 채널 통신을 처리하는 방식을 수정하는 패치를 릴리스했습니다. 이러한 보안 Netlogon 변경 사항이 도입된 이후 관리형 Microsoft AD에서 일부 Netlogon 연결 (서버, 워크스테이션 및 신뢰 검증)을 허용하지 않을 수 있습니다. AWS

문제가 Netlogon 또는 보안 채널 통신과 관련이 있는지 확인하려면 Amazon CloudWatch Logs에서 이벤트 ID 5827 (디바이스 인증 관련 문제) 또는 5828 (AD 신뢰 검증 관련 문제)을 검색하십시오. AWS 관리형 Microsoft CloudWatch AD에 대한 자세한 내용은 [로그 전송 활성화](#).

CVE-2020-1472 완화에 대한 자세한 내용은 Microsoft 웹 사이트에서 [CVE-2020-1472 관련 Netlogon 보안 채널 연결의 변경 사항을 관리하는 방법](#)을 참조하세요.

암호 복구

사용자가 암호를 잊어버렸거나 Simple AD 또는 AWS Managed Microsoft AD 디렉터리에 로그인하는데 문제가 있는 경우 AWS Management Console, Windows PowerShell 또는 를 사용하여 암호를 재설정할 수 있습니다. AWS CLI

자세한 정보는 [사용자 암호 재설정](#)을 참조하세요.

추가 리소스

다음 리소스는 작업할 때 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS 지식 센터](#) - 문제 해결에 도움이 되는 FAQ 및 기타 리소스 링크를 찾을 수 있습니다.
- [AWS 지원 센터](#) —기술 지원을 받을 수 있습니다.
- [AWS 프리미엄 지원 센터](#) —프리미엄 기술 지원을 받을 수 있습니다.

다음 리소스는 일반적인 Active Directory 문제를 해결하는 데 도움이 될 수 있습니다.

- [Active Directory 설명서](#)
- [AD DS 문제 해결](#)
- [디렉터리 데이터 문제 해결](#)

주제

- [Microsoft 이벤트 뷰어로 DNS 서버 모니터링](#)
- [Linux 도메인 조인 오류](#)
- [Active Directory 사용 가능한 스토리지 공간 부족](#)
- [스키마 확장 오류](#)
- [신뢰 생성 상태 이유](#)

Microsoft 이벤트 뷰어로 DNS 서버 모니터링

AWS Managed Microsoft AD DNS 이벤트를 감사할 수 있습니다. 이렇게 하면 DNS 관련 문제를 식별하고 해결하기가 쉬워집니다. 예를 들어 DNS 레코드가 누락된 경우 DNS 감사 이벤트 로그를 사용하여 문제의 근본 원인을 파악하고 이를 해결할 수 있습니다. 또한 DNS 감사 이벤트 로그를 사용하여 의심스러운 IP 주소에서 발신된 요청을 감지하여 차단함으로써 보안을 강화할 수 있습니다.

이렇게 하려면 Admin 계정 또는 AWS Domain Name System Administrators 그룹의 구성원인 계정으로 로그인되어 있어야 합니다. 이 그룹에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#) 단원을 참조하세요.

AWS Managed Microsoft AD DNS의 이벤트 뷰어에 액세스하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 인스턴스를 선택합니다.
3. AWS Managed Microsoft AD 디렉터리에 연결된 Amazon EC2 인스턴스를 찾으세요. 찾은 인스턴스를 선택한 다음 [Connect]를 선택합니다.
4. Amazon EC2 인스턴스에 연결되면 시작 메뉴를 열고 Windows 관리 도구 폴더를 선택합니다. 관리 도구 폴더에서 이벤트 뷰어를 선택합니다.
5. [Event Viewer] 창에서 [Action]을 선택한 다음 [Connect to Another Computer]를 선택합니다.
6. Another computer(또 다른 컴퓨터)를 선택하고 AWS Managed Microsoft AD DNS 서버 이름 또는 IP 주소를 입력한 후 확인을 선택합니다.
7. 왼쪽 창에서 [Applications and Services Logs] > [Microsoft] > [Windows] > [DNS-Server]를 선택한 다음 [Audit]을 선택합니다.

Linux 도메인 조인 오류

다음은 AWS Managed Microsoft AD 디렉터리에 EC2 Linux 인스턴스를 조인할 때 직면할 수 있는 오류 메시지 중 일부를 해결하는 데 도움이 될 수 있습니다.

Linux 인스턴스가 도메인에 조인을 할 수 없거나, 인증을 할 수 없는 경우

영역이 Microsoft Active Directory에서 작동하려면 먼저 DNS에서 우분투 14.04, 16.04 및 18.04 인스턴스를 역해석할 수 있어야 합니다. 그렇지 않으면 다음 두 가지 시나리오 중 하나가 발생할 수 있습니다.

시나리오 1: 영역에 아직 조인되지 않은 Ubuntu 인스턴스

영역을 조인하려고 시도 중인 Ubuntu 인스턴스의 경우 `sudo realm join` 명령을 실행하면 도메인을 조인하는 데 필요한 권한이 제공되지 않을 수 있으며 다음 오류가 표시될 수 있습니다.

! Active Directory에 인증할 수 없음: SASL(-1): 일반 실패: GSSAPI 오류: 잘못된 이름이 제공되었음 (성공) adcli: EXAMPLE.COM 도메인에 연결할 수 없음: Active Directory에 인증할 수 없음: SASL(-1): 일반 실패: GSSAPI 오류: 잘못된 이름이 제공되었음 (성공)! 도메인 영역에 조인할 권한 부족: 영역에 조인할 수 없음: 도메인에 조인할 권한 부족

시나리오 2: 영역에 조인된 Ubuntu 인스턴스

이미 Microsoft Active Directory 도메인에 가입된 Ubuntu 인스턴스의 경우 도메인 자격 증명을 사용하여 인스턴스에 SSH로 연결하려고 하면 다음 오류가 발생하면서 실패할 수 있습니다.

```
$ ssh admin@EXAMPLE.COM@198.51.100
```

해당 자격 증명 없음: /Users/username/.ssh/id_ed25519: 해당 파일 또는 디렉터리 없음

admin@EXAMPLE.COM@198.51.100의 암호:

권한이 거부되었습니다. 다시 시도하세요.

admin@EXAMPLE.COM@198.51.100의 암호:

퍼블릭 키를 사용하여 인스턴스에 로그인하고 확인하면/var/log/auth.log 다음과 같이 사용자를 찾을 수 없다는 내용의 오류가 나타날 수 있습니다.

```
5월 12일 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): 인증 실패; logname= uid=0 euid=0  
tty=ssh ruser= rhost=203.0.113.0
```

```
5월 12일 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): 인증 실패; logname= uid=0 euid=0  
tty=ssh ruser= rhost=203.0.113.0 user=admin@EXAMPLE.COM
```

```
5월 12일 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): admin@EXAMPLE.COM 사용자에게  
대해 수신됨: 10 (기본 인증 모듈에서 알 수 없는 사용자)
```

```
5월 12일 01:02:14 ip-192-0-2-0 sshd[2251]: 203.0.113.0 포트 13344 ssh2에서 잘못된 사용자  
admin@EXAMPLE.COM의 암호 실패
```

```
5월 12일 01:02:15 ip-192-0-2-0 sshd[2251]: Connection closed by 203.0.113.0에서 연결 닫  
힘 [preauth]
```

하지만 사용자에게 대한 kinit는 여전히 작동합니다. 이 예제를 참조하세요.

```
ubuntu@ip-192-0-2-0:~$ kinit admin@EXAMPLE.COM admin@EXAMPLE.COM의 암호:  
ubuntu@ip-192-0-2-0:~$ klist 티켓 캐시: FILE:/tmp/krb5cc_1000 기본 보안 주체:  
admin@EXAMPLE.COM
```

차선책

이러한 두 시나리오 모두에 대해 현재 권장되는 해결 방법은 아래와 같이 [libdefaults] 섹션의 /etc/krb5.conf에서 역방향 DNS를 비활성화하는 것입니다.

```
[libdefaults]  
default_realm = EXAMPLE.COM
```

```
rdns = false
```

원활한 도메인 조인 시 단방향 신뢰 인증 문제

관리형 AWS Microsoft AD와 온-프레미스 Active Directory 간에 단방향 발신 트러스트가 설정된 경우, Winbind에서 신뢰할 수 있는 Active Directory 자격 증명을 사용하여 도메인에 가입된 Linux 인스턴스에 대해 인증을 시도할 때 인증 문제가 발생할 수 있습니다.

오류

```
7월 31일 00:00:00 EC2Amaz-LSMWQT sshd [23832]: xxx.xxx.xxx.xxx 포트 18309 ssh2에서
user@corp.example.com 암호 실패
```

```
7월 31일 00:05:00 EC2Amaz-LSMWQT sshd [23832]: pam_winbind (sshd:auth): 암호 얻기
(0x00000390)
```

```
7월 31일 00:05:00 EC2Amaz-LSMWQT sshd [23832]: pam_winbind (sshd:auth): pam_get_item에서
암호를 반환함
```

```
7월 31일 00:05:00 EC2Amaz-LSMWQT sshd [23832]: pam_winbind (sshd:auth): 요청
wbcLogonUser 실패: WBC_ERR_AUTH_ERR, PAM 오류: PAM_SYSTEM_ERR (4), NTSTATUS:
**NT_STATUS_OBJECT_NAME_NOT_FOUND**, 오류 메시지는 다음과 같습니다. 개체 이름은 다음
과 같습니다. 찾을 수 없습니다.
```

```
7월 31일 00:05:00 EC2Amaz-LSMWQT sshd [23832]: pam_winbind (sshd:auth): 내부 모듈 오류
(retval = PAM_SYSTEM_ERR(4), user = 'CORP\user')
```

차선책

이 문제를 해결하려면 다음과 같은 단계를 사용하여 PAM 모듈 구성 파일(/etc/security/pam_winbind.conf)에서 디렉티브를 주석 처리하거나 제거해야 합니다.

1. 텍스트 편집기에서 /etc/security/pam_winbind.conf 파일을 엽니다.

```
sudo vim /etc/security/pam_winbind.conf
```

2. krb5_auth = yes라는 디렉티브를 주석 처리하거나 삭제하세요.

```
[global]
```

```
cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Winbind 서비스를 중지한 다음 다시 시작하세요.

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

Active Directory 사용 가능한 스토리지 공간 부족

Active Directory에서 사용 가능한 스토리지 공간이 부족하여 AWS Managed Microsoft AD가 손상된 경우, 디렉터리를 활성 상태로 되돌리려면 즉각적인 조치가 필요합니다. 이 손상의 가장 일반적인 두 가지 원인은 아래 단원에서 다룹니다.

1. [SYSVOL 폴더가 필수 그룹 정책 객체 이상을 저장하는 중](#)
2. [Active Directory 데이터베이스가 볼륨을 채움](#)

AWS Managed Microsoft AD 스토리지에 대한 요금 정보는 [AWS Directory Service요금](#)을 참조하세요.

SYSVOL 폴더가 필수 그룹 정책 객체 이상을 저장하는 중

이러한 손상의 일반적인 원인은 그룹 정책 처리를 위해 필수적이지 않은 파일을 SYSVOL 폴더에 저장하기 때문입니다. 이러한 필수적이지 않은 파일은 EXE, MSI 또는 그룹 정책에서 처리하는 데 필수적이지 않은 기타 파일일 수 있습니다. 그룹 정책에서 처리할 필수 객체는 그룹 정책 객체, 로그인/오프 스크립트 및 [그룹 정책용 중앙 저장소 객체](#)입니다. 필수적이지 않은 파일은 AWS Managed Microsoft AD 도메인 컨트롤러가 아닌 파일 서버에 저장해야 합니다.

[그룹 정책 소프트웨어 설치용](#) 파일이 필요한 경우, 파일 서버를 사용하여 해당 설치 파일을 저장해야 합니다. 파일 서버를 자체 관리하지 않으려는 경우, AWS는 관리형 파일 서버 옵션인 [Amazon FSx](#)를 제공합니다.

불필요한 파일을 제거하기 위해 범용 명명 규칙(UNC) 경로를 통해 SYSVOL 공유에 액세스할 수 있습니다. 예를 들어 도메인의 정규화된 도메인 이름(FQDN)이 example.com인 경우, SYSVOL의 UNC 경로는 “\\example.local\SYSVOL\example.local”입니다. 그룹 정책에서 디렉터리를 처리하는 데 필수적이지 않은 객체를 찾아서 제거하면 30분 이내에 활성 상태로 돌아갑니다. 30분 후에도 디렉터리가 활성화되지 않으면 AWS Support에 문의하세요.

SYSVOL 공유에 필수 그룹 정책 파일만 저장하면 SYSVOL 부풀림으로 인해 디렉터리가 손상되지 않습니다.

Active Directory 데이터베이스가 볼륨을 채움

이러한 손상의 일반적인 원인은 Active Directory 데이터베이스가 볼륨을 가득 채우기 때문입니다. 이러한 경우인지 확인하기 위해 디렉터리의 총 객체 수를 검토할 수 있습니다. 삭제된 객체는 여전히 디렉터리의 총 개체 수에 포함된다는 점을 이해하실 수 있도록 총계라는 글자를 굵게 표시합니다.

기본적으로 AWS Managed Microsoft AD는 항목이 재활용 객체가 되기 전에 180일 동안 AD 휴지통에 항목을 보관합니다. 객체가 재활용 객체(삭제 표시)가 되면 해당 객체가 디렉터리에서 최종적으로 제거되기 전에 180일 동안 보관됩니다. 따라서 삭제된 객체는 제거되기 전 360일 동안 디렉터리 데이터베이스에 존재합니다. 이 이유 때문에 총 객체 수를 평가해야 합니다.

AWS Managed Microsoft AD 지원 객체 수에 대한 자세한 내용은 [AWS Directory Service요금](#)을 참조하세요.

삭제된 객체가 포함된 디렉터리의 총 객체 수를 가져오려면 도메인이 조인된 Windows 인스턴스에서 다음 PowerShell 명령을 실행하면 됩니다. 관리 인스턴스를 설정하는 방법의 단계는 [AWS Managed Microsoft AD에서의 사용자 및 그룹 관리](#) 단원을 참조하세요.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
Select-Object -Property 'Count'
```

다음은 위 명령의 출력 예입니다.

```
Count
10000
```

총 개수가 위의 참고 내용에 나열된 디렉터리 크기에 대해 지원되는 객체 수보다 크면 디렉터리의 용량을 초과한 것입니다.

다음은 이러한 손상을 해결할 수 있는 옵션입니다.

1. AD 정리

- a. 원치 않는 AD 객체를 삭제합니다.
- b. AD 휴지통에서 원하지 않는 객체를 모두 제거합니다. 이 작업은 실행 취소할 수 없으며, 삭제된 객체를 복구할 수 있는 유일한 방법은 디렉터리 복원을 수행하는 것입니다.

c. 다음 명령은 AD 휴지통에서 삭제된 모든 객체를 제거합니다.

Important

이 명령은 실행 취소할 수 없는 명령이며, 삭제된 객체를 복구할 수 있는 유일한 방법은 디렉터리 복원을 수행하는 것이므로 이 명령은 특히 주의해서 사용해야 합니다.

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
{ ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
'*\0ADEL:*') }
ForEach($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
$ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

d. AWS Support에서 사례를 개설하여 AWS Directory Service가 사용 가능한 공간을 회수하도록 요청하세요.

2. 디렉터리 유형이 Standard Edition인 경우, AWS Support에서 디렉터를 Enterprise Edition으로 업그레이드하도록 요청하는 사례를 개설하세요. 이렇게 하면 디렉터리 비용도 증가합니다. 요금 정보는 [AWS Directory Service 요금](#)을 참조하세요.

AWS Managed Microsoft AD에서 AWS 위임 삭제된 객체 수명 관리자 그룹의 멤버는 삭제된 객체가 재활용 객체가 되기 전에 AD 휴지통에 보관되는 시간(일)을 설정하는 msDS-DeletedObjectLifetime 속성을 수정할 수 있습니다.

Note

이는 고급 주제입니다. 부적절하게 구성하면 데이터가 손실될 수 있습니다. 이러한 프로세스를 더 잘 이해하려면 먼저 [AD 휴지통: 이해, 구현, 모범 사례 및 문제 해결](#)을 검토하는 것이 좋습니다.

msDS-DeletedObjectLifetime 속성 값을 더 낮은 숫자로 변경하는 기능은 객체 수가 지원되는 수준을 초과하지 않도록 하는 데 도움이 될 수 있습니다. 이 속성을 설정할 수 있는 가장 낮은 유효 값은 2

일입니다. 이 값을 초과하면 AD 휴지통을 사용하여 삭제된 객체를 더 이상 복구할 수 없습니다. 객체를 복구하려면 스냅샷에서 디렉터리를 복구해야 합니다. 자세한 내용은 [디렉터리 스냅샷 또는 복구](#) 섹션을 참조하세요. 스냅샷 복원은 특정 시점이므로 데이터 손실이 발생할 수 있습니다.

디렉터리의 삭제된 객체 수명을 변경하려면 다음 명령을 실행하세요.

Note

명령을 그대로 실행하면 삭제된 객체 수명 속성 값이 30일로 설정됩니다. 길거나 짧게 만들고 싶다면 "30"을 원하는 숫자로 바꾸세요. 그러나 기본 수인 180보다 높지 않게 설정하는 것이 좋습니다.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{ "msDS-DeletedObjectLifetime" = $DeletedObjectLifetime }
```

스키마 확장 오류

다음은 AWS Managed Microsoft AD 디렉터리에서 스키마를 확장할 때 발생할 수 있는 일부 오류 메시지를 처리하는 데 도움이 될 수 있습니다.

추천

오류

라인 1에서 시작되는 엔트리에 오류 추가: 추천 서버 측 오류: 0x202b 추천이 서버에서 반환되었습니다. 확장 서버 오류: 0000202B: RefErr: DSID-0310082F, 데이터 0, 1 액세스 포인트 \tref 1: 'example.com' 수정된 객체 수: 0

문제 해결

모든 고유 이름 필드가 올바른 도메인 이름을 가지고 있는지 확인합니다. 위의 예제에서 DC=example,dc=com를 cmdlet Get-ADDomain에 표시된 DistinguishedName으로 교체해야 합니다.

가져오기 파일을 읽을 수 없음

오류

가져오기 파일을 읽을 수 없습니다. 수정된 객체 수: 0

문제 해결

가져온 LDIF 파일이 비어 있습니다(0바이트). 올바른 파일이 업로드되었는지 확인합니다.

구문 오류

오류

라인 21에서 실패한 입력 파일에 구문 오류가 있습니다. 마지막 토큰은 'q'로 시작합니다. 수정된 객체 수: 0

문제 해결

라인 21의 텍스트가 올바르게 포맷되지 않았습니다. 유효하지 않은 텍스트의 첫 번째 문자는 A입니다. 라인 21을 유효한 LDIF 구문으로 업데이트합니다. LDIF 파일을 포맷하는 방법에 대한 자세한 내용은 [1단계: LDIF 파일 생성](#)을 참조하세요.

속성 또는 값 있음

오류

라인 1에서 시작되는 엔트리에 오류 추가: 속성 또는 값 있음 서버 측 오류: 0x2083 지정된 값이 이미 존재합니다. 확장 서버 오류: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, 문제 1006 (ATT_OR_VALUE_EXISTS), 데이터 0, Att 20019 (mayContain):len 4 수정된 객체 수: 0

문제 해결

스키마 변경이 이미 적용되었습니다.

이러한 속성 없음

오류

라인 1에서 시작되는 엔트리에 오류 추가: 이러한 속성 없음 서버 측 오류: 0x2085 속성 값은 객체에 존재하지 않으므로 삭제할 수 없습니다. 확장 서버 오류: 00002085: AtrErr: DSID-03152367,

#1: \t0: 00002085: DSID-03152367, 문제 1001 (NO_ATTRIBUTE_OR_VAL), 데이터 0, Att 20019 (mayContain):len 4 수정된 객체 수: 0

문제 해결

LDIF 파일은 클래스에서 속성을 제거하려고 시도하지만, 현재 해당 속성이 클래스에 연결되어 있지 않습니다. 아마도 스키마 변경이 이미 적용되었습니다.

오류

라인 41에서 시작되는 엔트리에 오류 추가: 이러한 속성 없음 0x57 파라미터가 올바르지 않습니다. 확장 서버 오류: 0x208d 디렉터리 객체를 찾을 수 없음. 확장 서버 오류: "00000057: LdapErr: DSID-0C090D8A, 설명: 속성 변환 작업 시 오류, 데이터 0, v2580" 수정된 객체 수: 0

문제 해결

라인 41에 나온 속성이 올바르지 않습니다. 스펠링을 다시 확인합니다.

이러한 객체 없음

오류

라인 1에서 시작되는 엔트리에 오류 추가: 이러한 객체 없음 서버 측 오류: 0x208d 디렉터리 객체를 찾을 수 없음. 확장 서버 오류: 0000208D: NameErr: DSID-03100238, problem 2001 (NO_OBJECT), 데이터 0, best match of: 'CN=Schema,CN=Configuration,DC=example,DC=com' 수정된 객체 수: 0

문제 해결

고유 이름(DN)이 참조한 객체가 존재하지 않습니다.

신뢰 생성 상태 이유

신뢰 생성이 실패하면 디렉터리 상태 메시지에 추가 정보가 포함됩니다. 여기 나온 내용은 이러한 메시지가 의미하는 바를 이해하는 데 도움이 될 것입니다.

액세스 거부됨

신뢰 생성을 시도할 때 액세스가 거부되었습니다. 신뢰 암호가 잘못되었거나 원격 도메인의 보안 설정이 신뢰 구성을 허용하지 않습니다. 이러한 문제를 해결하려면 다음 작업을 시도해 보세요.

- AWS 관리 대상 Microsoft Active Directory AD와 신뢰 관계를 Active Directory 생성하려는 자체 관리형 Microsoft AD의 첫 번째 사이트 이름은 같아야 합니다. 첫 번째 사이트 이름은 로 설정됩니다. Default-First-Site-Name 도메인마다 이름이 다르면 액세스 거부 오류가 발생합니다.
- 원격 도메인에서 해당 신뢰 관계를 생성할 때 사용한 것과 동일한 신뢰 암호를 사용하고 있는지 확인합니다.
- 도메인 보안 설정이 신뢰 관계 생성을 허용하는지 확인합니다.
- 로컬 보안 정책이 올바르게 설정되었는지 확인합니다. Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously를 자세히 점검하여 다음과 같이 명명된 파이프가 3개 이상 포함되어 있는지 확인합니다.
 - netlogon
 - samr
 - lsarpc
- 위의 명명된 파이프가 NullSessionPipes레지스트리 경로 HKLM\SYSTEM\services\Parameters에 있는 레지스트리 키의 값으로 존재하는지 확인하십시오. CurrentControlSet LanmanServer 이러한 값은 구분된 행에 삽입해야 합니다.

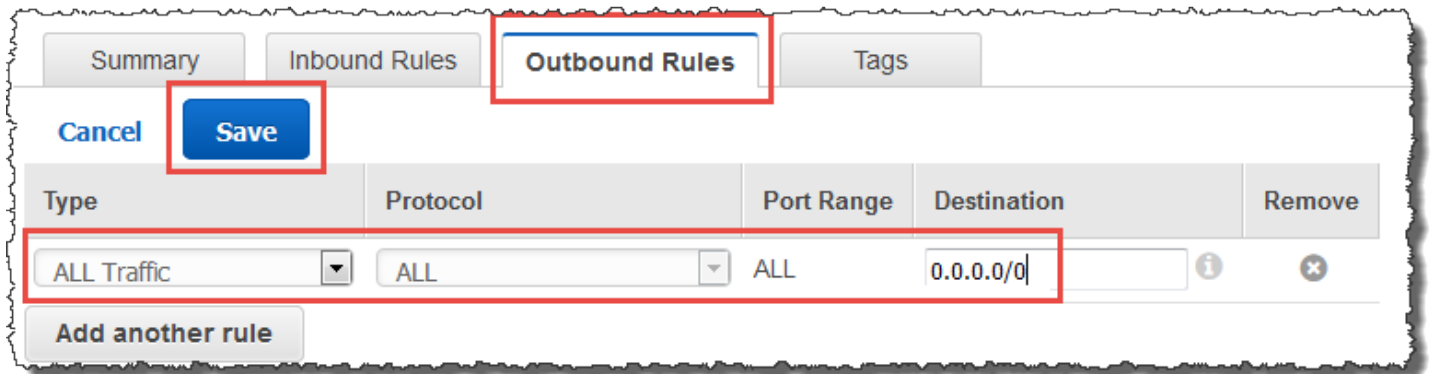
Note

기본적으로 Network access: Named Pipes that can be accessed anonymously는 설정이 되어 있지 않으며 Not Defined라는 메시지가 표시됩니다. Network access: Named Pipes that can be accessed anonymously에 대한 도메인 컨트롤러의 유효 기본 설정이 netlogon, samr, lsarpc이기 때문에 이는 정상적인 상태입니다.

- 기본 도메인 컨트롤러 정책에서 다음 SMB (서버 메시지 블록) 서명 설정을 확인하십시오. 이러한 설정은 컴퓨터 구성 > Windows 설정 > 보안 설정 > 로컬 정책/보안 옵션에서 찾을 수 있습니다. 다음 설정과 일치해야 합니다.
 - Microsoft네트워크 클라이언트: 디지털 서명 통신 (항상): 기본값: 활성화됨
 - Microsoft네트워크 클라이언트: 디지털 서명 통신 (서버가 동의하는 경우): 기본값: 활성화
 - Microsoft네트워크 서버: 디지털 서명 통신 (항상): 활성화됨
 - Microsoft네트워크 서버: 디지털 서명 통신 (클라이언트가 동의하는 경우): 기본값: 활성화

지정된 도메인 이름이 없거나 해당 주소를 찾을 수 없습니다.

이 문제를 해결하려면 도메인을 위한 보안 그룹 설정과 VPC를 위한 액세스 제어 목록(ACL)이 올바른지 확인하고 조건부 전달자에 대한 정보를 정확하게 입력했는지 확인하세요. AWS 은(는) Active Directory 통신에 필요한 포트만 열도록 보안 그룹을 구성합니다. 기본 구성에서 보안 그룹은 모든 IP 주소에서 이러한 포트에 도달하는 트래픽을 수용합니다. 아웃바운드 트래픽은 보안 그룹으로 제한됩니다. 온프레미스 네트워크로의 트래픽을 허용하려면 보안 그룹의 아웃바운드 규칙을 업데이트해야 합니다. 보안 요건에 대한 자세한 내용은 [2단계: AWS Managed Microsoft AD 준비](#)(를) 참조하세요.



다른 디렉터리의 네트워크에 대한 DNS 서버가 공용(RFC 1918이 아닌) IP 주소를 사용하는 경우 디렉터리에 Directory Services 콘솔에서 DNS 서버에 대한 IP 경로를 추가해야 합니다. 자세한 내용은 [신뢰 관계의 설정, 확인, 삭제 및 필수 조건](#) 섹션을 참조하세요.

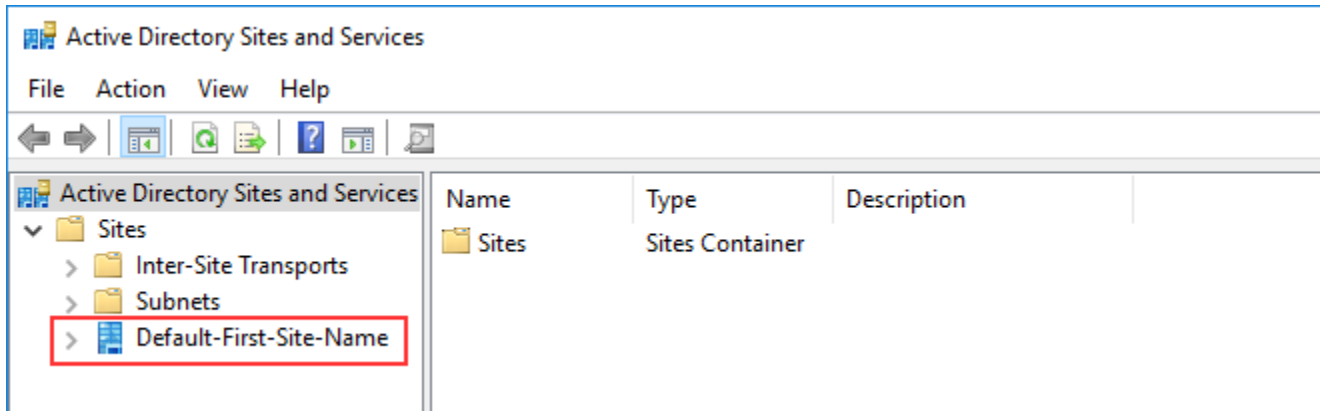
IANA(인터넷 할당 번호 기관)가 다음 세 블록의 IP 주소 공간을 사설 인터넷을 위해 예약했습니다.

- 10.0.0.0 - 10.255.255.255 (10/8 접두사)
- 172.16.0.0 - 172.31.255.255 (172.16/12 접두사)
- 192.168.0.0 - 192.168.255.255 (192.168/16 접두사)

자세한 내용은 <https://tools.ietf.org/html/rfc1918>을 참조하세요.

AWS 관리형 Microsoft AD의 기본 AD 사이트 이름이 온-프레미스 인프라의 기본 AD 사이트 이름과 일치하는지 확인하십시오. 컴퓨터는 사용자 도메인이 아닌 컴퓨터가 구성원으로 속해 있는 도메인을 사용하여 사이트 이름을 결정합니다. 가장 가까운 온프레미스와 일치하도록 사이트 이름을 바꾸면 DC 로케이터가 가장 가까운 사이트의 도메인 컨트롤러를 사용합니다. 이것으로도 문제가 해결되지 않는 경우에는 이전에 생성된 조건부 전달자로부터의 정보가 캐시에 저장되어 새로운 신뢰 생성이 금지되었을 가능성이 있습니다. 몇 분 정도 기다린 다음 신뢰 및 조건부 전달자를 다시 생성하세요.

작동 방식에 대한 자세한 내용은 웹 사이트의 [포리스트 트러스트 전반의 도메인 로케이터](#)를 참조하십시오. Microsoft



이 도메인에서 해당 작업을 수행할 수 없습니다

두 도메인/디렉터리 모두에 중복되는 NETBIOS 이름이 없어야 이 문제를 해결할 수 있습니다. 도메인/디렉터리에 NETBIOS 이름이 겹치는 경우 둘 중 하나를 다른 NETBIOS 이름으로 다시 만든 다음 다시 시도하세요.

“필요하고 유효한 도메인 이름”이라는 오류 때문에 트러스트 생성이 실패하고 있습니다.

DNS 이름에는 영문자(A~Z), 숫자(0~9), 빼기 기호(-) 및 마침표(.)만 포함될 수 있습니다. 마침표 문자는 도메인 스타일 이름의 구성 요소를 구분하는 데 사용하는 경우에만 허용됩니다. 또한, 다음을 고려하세요.

- AWS 관리형 Microsoft AD는 단일 레이블 도메인을 사용하는 트러스트를 지원하지 않습니다. 자세한 내용은 [단일 레이블 도메인 Microsoft 지원](#)을 참조하십시오.
- RFC 1123(<https://tools.ietf.org/html/rfc1123>)에 따르면 DNS 레이블에 사용할 수 있는 유일한 문자는 “A”~“Z”, “a”~“z”, “0”~“9”, 하이픈(“-”)입니다. 마침표[.]는 DNS 이름에도 사용되지만, DNS 레이블 사이와 FQDN 끝에만 사용됩니다.
- RFC 952(<https://tools.ietf.org/html/rfc952>)에 따르면 “이름”(넷, 호스트, 게이트웨이, 도메인 이름)은 알파벳(A~Z), 숫자(0~9), 빼기 기호(-), 마침표(.)에서 가져온 최대 24자의 텍스트 문자열입니다. 마침표는 “도메인 스타일 이름”의 구성 요소를 구분하는 용도로만 사용할 수 있다는 점을 유의하세요.

자세한 내용은 Microsoft 웹 사이트의 [호스트 및 도메인에 대한 이름 제한 준수](#)를 참조하십시오.

신뢰 관계 테스트용 일반 도구

다음은 다양한 신뢰 관련 문제를 해결하는 데 사용할 수 있는 도구입니다.

AWS Systems Manager 자동화 문제 해결 도구

[지원 자동화 워크플로 \(SAW\)](#) 는 AWS Systems Manager 자동화를 활용하여 사전 정의된 런북을 제공합니다. AWS Directory Service [AWSSupport- TroubleshootDirectoryTrust](#) runbook 도구를 사용하면 AWS 관리형 Microsoft AD와 온-프레미스 Microsoft Active Directory 간의 일반적인 신뢰 생성 문제를 진단할 수 있습니다.

DirectoryServicePortTest 도구

[DirectoryServicePortTest](#) 테스트 도구는 AWS 관리형 Microsoft AD와 온-프레미스 Active Directory 간의 신뢰 생성 문제를 해결할 때 유용할 수 있습니다. 도구를 사용하는 방법에 대한 예제는 [AD 커넥터 테스트](#) 단원을 참조하세요.

NETDOM 및 NLTEST 도구

관리자는 Netdom 및 Nltest 명령줄 도구를 모두 사용하여 신뢰를 찾고, 표시하며, 생성하고, 제거하며, 관리할 수 있습니다. 이러한 도구는 도메인 컨트롤러의 LSA 기관과 직접 통신합니다. 이러한 도구를 사용하는 방법에 대한 예는 웹 사이트의 [Netdom](#) 및 [NLTEST](#)를 참조하십시오. Microsoft

패킷 캡처 도구

내장된 Windows 패키지 캡처 유틸리티를 사용하여 잠재적인 네트워크 문제를 조사하고 해결할 수 있습니다. 자세한 내용은 [아무것도 설치하지 않은 채로 네트워크 추적 캡처](#)를 참조하세요.

AD Connector

AD Connector는 클라우드에 정보를 Microsoft Active Directory 캐싱하지 않고도 디렉터리 요청을 온-프레미스로 리디렉션할 수 있는 디렉터리 게이트웨이입니다. AD Connector는 소형 및 대형 두 가지 크기로 제공됩니다. 소형 AD Connector는 소규모 조직을 위해 설계되었으며 초당 적은 수의 작업을 처리하기 위한 것입니다. 대형 AD Connector는 대규모 조직을 위해 설계되었으며 초당 적정 수의 작업에서 많은 수의 작업까지를 처리하기 위한 것입니다. 여러 AD Connector 간에 애플리케이션 로드를 분산하여 성능 필요에 맞게 조정할 수 있습니다. 적용되는 사용자 도는 연결 제한은 없습니다.

AD Connector는 Active Directory 전이적 트러스트를 지원하지 않습니다. AD 커넥터와 온-프레미스 Active Directory 도메인은 일대일 관계입니다. 즉, 인증하려는 Active Directory 포리스트의 하위 도메인을 포함하여 각 온-프레미스 도메인에 대해 고유한 AD Connector를 만들어야 합니다.

Note

AD Connector는 다른 AWS 계정과 공유할 수 없습니다. 이것이 요구 사항인 경우 AWS 관리형 Microsoft AD를 사용하는 것을 고려해 보십시오 [디렉터리 공유](#). 또한 AD Connector는 다중 VPC를 인식하지 못하므로 AD 커넥터와 동일한 VPC에 같은 AWS [WorkSpaces](#) 애플리케이션을 프로비저닝해야 합니다.

AD Connector가 설정되면 다음과 같은 이점이 있습니다.

- 최종 사용자와 IT 관리자는 기존 기업 자격 증명을 사용하여 Amazon WorkDocs 또는 Amazon과 WorkSpaces 같은 AWS 애플리케이션에 로그인할 수 WorkMail 있습니다.
- 에 대한 IAM 역할 기반 액세스를 통해 Amazon EC2 인스턴스 또는 Amazon S3 버킷과 같은 AWS 리소스를 관리할 수 있습니다. AWS Management Console
- 사용자나 IT 관리자가 온프레미스 인프라 또는 클라우드의 리소스에 액세스하는지 여부에 관계없이 기존 보안 정책 (예: 암호 만료, 암호 기록, 계정 잠금) 을 일관되게 적용할 수 있습니다. AWS
- AD Connector를 사용하면 기존 RADIUS 기반 MFA 인프라와 통합하여 사용자가 애플리케이션에 액세스할 때 추가 보안 계층을 제공함으로써 다단계 인증을 활성화할 수 있습니다. AWS

본 섹션의 여러 주제 항목을 계속 읽으면서 디렉터리를 연결하고 AD Connector 기능의 대다수를 생성하는 방법을 알아 보세요.

주제

- [AD Connector와의 연결 시작하기](#)
- [AD Connector 관리 방법](#)
- [AD Connector 모범 사례](#)
- [AD Connector 할당량](#)
- [AD Connector의 애플리케이션 호환성 정책](#)
- [문제 해결 AD Connector](#)

AD Connector와의 연결 시작하기

AD Connector를 사용하여 기존 엔터프라이즈에 AWS Directory Service 연결할 수 Active Directory 있습니다. 기존 디렉터리에 연결하면 모든 디렉터리 데이터가 도메인 컨트롤러에 남아 있습니다. AWS Directory Service 디렉터리 데이터를 복제하지 않습니다.

주제

- [AD Connector 사전 조건](#)
- [AD Connector 생성](#)
- [AD 커넥터로 생성되는 항목](#)

AD Connector 사전 조건

AD Connector를 사용하여 기존 디렉터리에 연결하려면 다음 사항이 필요합니다.

Amazon VPC

다음은 통해 VPC 설정:

- 최소 2개의 서브넷. 각 서브넷은 서로 다른 가용 영역에 있어야 합니다.
- 가상 프라이빗 네트워크(VPN) 연결 또는 AWS Direct Connect을 통해 VPC를 기존 네트워크에 연결해야 합니다.
- VPC는 기본 하드웨어 테넌시를 가지고 있어야 합니다.

AWS Directory Service 두 개의 VPC 구조를 사용합니다. 디렉터리를 구성하는 EC2 인스턴스는 AWS 계정 외부에서 실행되며 에서 관리합니다. AWSETH0 및 ETH1라는 2개의 어댑터가 있습니다. ETH0는 관리 어댑터로써 계정 외부에 위치합니다. ETH1는 계정 내부에서 생성됩니다.

디렉터리의 ETH0 네트워크에서 관리 IP 범위는 디렉터리를 배포할 경우 VPC와 충돌하지 않도록 보장하기 위해 프로그래밍 방식으로 선택합니다. 이 IP 범위는 다음 페어 중 하나일 수 있습니다(디렉터리가 2개의 서브넷에서 실행되기 때문에).

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

ETH1 CIDR의 첫 번째 옥텟을 확인하여 충돌을 방지합니다. 10으로 시작할 경우, 192.168.1.0/24 및 192.168.2.0/24 서브넷의 192.168.0.0/16 VPC를 선택합니다. 첫 번째 옥텟이 10 이외의 수일 경우, 10.0.1.0/24 및 10.0.2.0/24 서브넷의 10.0.0.0/16 VPC를 선택합니다.

선택 알고리즘은 VPC 상의 라우팅을 포함하지 않습니다. 따라서 이 시나리오에서 IP 라우팅 충돌 결과가 있을 수 없습니다.

자세한 내용은 Amazon VPC 사용 설명서에서 다음 주제를 참조하세요.

- [Amazon VPC란 무엇인가?](#)
- [VPC의 서브넷](#)
- [VPC에 하드웨어 가상 프라이빗 게이트웨이 추가](#)

에 대한 AWS Direct Connect 자세한 내용은 [AWS Direct Connect 사용 설명서](#)를 참조하십시오.

기존 Active Directory

Active Directory도메인이 있는 기존 네트워크에 연결해야 합니다.

Note

AD Connector는 [단일 레이블 도메인](#)을 지원하지 않습니다.

이 Active Directory 도메인의 기능 수준은 Windows Server 2003 이상이어야 합니다. AD Connector는 Amazon EC2 인스턴스에 호스팅된 도메인으로의 연결도 지원합니다.

Note

AD Connector는 Amazon EC2 도메인 조인 기능과 조합으로 사용될 경우 RODC(읽기 전용 도메인 컨트롤러)를 지원하지 않습니다.

서비스 계정

다음과 같은 권한이 부여된 기존 디렉터리의 서비스 계정에 대한 자격 증명을 가지고 있어야 합니다.

- 사용자 및 그룹 읽기 - 필수
- 컴퓨터를 도메인에 연결 - 원활한 도메인 가입을 사용하는 경우에만 필요하고 WorkSpaces
- 컴퓨터 개체 생성 - 원활한 도메인 가입을 사용하는 경우에만 필요하고 WorkSpaces
- 서비스 계정 암호는 AWS 암호 요구 사항을 준수해야 합니다. AWS 비밀번호는 다음과 같아야 합니다.
 - 길이 8~128자 (포함)
 - 다음 네 가지 범주 중 세 개의 문자를 하나 이상 포함해야 합니다.
 - 소문자(a~z)
 - 대문자(A-Z)
 - 숫자(0-9)
 - 영숫자 외의 특수 문자(~!@#\$\$%^&* _+=`\|(){}[]:;'"<>.,/?)

자세한 정보는 [서비스 계정에 권한 위임](#)을 참조하세요.

Note

AD Connector는 AWS 애플리케이션의 인증 및 권한 부여에 Kerberos를 사용합니다. LDAP는 사용자 및 그룹 객체 조회(읽기 작업)에만 사용됩니다. LDAP 트랜잭션에서는 아무것도 변경할 수 없으며 보안 인증 정보가 일반 텍스트로 전달되지 않습니다. 인증은 Kerberos 티켓을 사용하여 사용자로서 LDAP 작업을 수행하는 AWS 내부 서비스에 의해 처리됩니다.

사용자 권한

모든 Active Directory 사용자는 자신의 속성을 읽을 수 있는 권한이 있어야 합니다. 다음 속성을 지정합니다.

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName

- UserAccountControl
- MemberOf

기본적으로 Active Directory 사용자는 이러한 속성에 대한 읽기 권한이 부여되어 있습니다. 그러나 관리자가 시간이 지나면 이러한 권한을 수정할 수 있으므로, 처음 AD Connector를 설정하기 전에 사용자가 이러한 읽기 권한을 보유하고 있는지 확인해야 합니다.

IP 주소

기존 디렉터리에서 두 개의 DNS 서버 또는 도메인 컨트롤러의 IP 주소를 가져옵니다.

AD Connector는 디렉터리를 연결할 때 `_ldap._tcp.<DnsDomainName>` 및 `_kerberos._tcp.<DnsDomainName>` SRV 레코드를 획득하므로 이들 서버에는 SRV 레코드가 포함되어야 합니다. AD Connector는 LDAP와 Kerberos 서비스 모두를 제공하는 공통 도메인 컨트롤러를 찾으려고 시도하므로 이들 SRV 레코드에는 적어도 한 개의 공통 도메인 컨트롤러가 포함되어야 합니다. SRV 레코드에 대한 자세한 내용은 Microsoft의 [SRV 리소스 레코드를](#) 참조하십시오. TechNet

서브넷용 포트

AD Connector가 디렉터리 요청을 기존 Active Directory 도메인 컨트롤러로 리디렉션하려면 기존 네트워크의 방화벽에 Amazon VPC의 두 서브넷 모두에 대해 CIDR에 대해 다음과 같은 포트가 열려 있어야 합니다.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 인증
- TCP/UDP 389 - LDAP

이들은 Amazon VPC가 디렉터리에 연결하기 위해 필요한 최소 포트입니다. 특정 구성에서는 추가 포트를 개방해야 하는 경우도 있습니다.

AD Connector와 WorkSpaces Amazon을 사용하려면 도메인 컨트롤러의 DisableVSupportLDAP 속성을 0으로 설정해야 합니다. 도메인 컨트롤러의 기본 설정입니다. DisableVSupportLDAP 속성이 활성화된 경우 AD Connector는 디렉터리의 사용자를 쿼리할 수 없습니다. 이렇게 하면 AD Connector가 작동하지 Amazon WorkSpaces 않습니다.

Note

기존 Active Directory 도메인의 DNS 서버 또는 도메인 컨트롤러 서버가 VPC 내에 있는 경우, 해당 서버와 연결된 보안 그룹은 VPC의 두 서브넷 모두에 대해 위의 포트를 CIDR에 개방해야 합니다.

추가 포트 요구 사항은 설명서의 [AD 및 AD DS](#) 포트 요구 사항을 참조하십시오. Microsoft

Kerberos 사전 인증

사용자 계정에서 Kerberos 사전 인증이 활성화되어 있어야 합니다. 이 설정을 활성화하는 방법에 대한 자세한 지침은 [Kerberos 사전 인증이 활성화되었는지 확인](#) 단원을 참조하세요. 이 설정에 대한 일반적인 내용은 [사전 인증](#) Microsoft TechNet 쉼표를 참조하십시오.

암호화 유형

AD Connector에서는 Kerberos를 통해 Active Directory 도메인 컨트롤러에 인증할 때 다음과 같은 암호 유형을 지원합니다.

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center 사전 요구 사항

AD Connector와 함께 IAM Identity Center를 사용하려는 경우 다음 사항이 맞는지 확인해야 합니다.

- AD Connector는 AWS 조직의 관리 계정에 설정되어 있습니다.
- IAM Identity Center의 인스턴스가 AD Connector가 설정된 동일한 리전에 있습니다.

자세한 내용은 사용 설명서의 [IAM ID 센터 사전 요구 사항을](#) 참조하십시오. AWS IAM Identity Center

다중 인증 사전 조건

AD Connector 디렉터리에서 다중 인증을 지원하려면 다음이 필요합니다.

- 두 개의 클라이언트 엔드포인트가 있는 기존 네트워크의 [RADIUS\(Remote Authentication Dial-In User Service\)](#) 서버입니다. RADIUS 클라이언트 엔드포인트에 대한 요구 사항은 다음과 같습니다.
 - 엔드포인트를 생성하려면 AWS Directory Service 서버의 IP 주소가 필요합니다. 이 IP 주소는 디렉터리 세부 정보의 [Directory IP Address] 필드에서 가져올 수 있습니다.
 - 두 RADIUS 엔드포인트에서 동일한 공유 보안 코드를 사용해야 합니다.
- 기존 네트워크는 서버에서 기본 RADIUS 서버 포트 (1812) 를 통한 인바운드 트래픽을 허용해야 합니다. AWS Directory Service
- RADIUS 서버와 기존 디렉터리 간에 사용자 이름이 동일해야 합니다.

MFA와 AD Connector를 함께 사용하는 방법에 대한 자세한 내용은 [AD Connector에 대한 다중 인증 활성화](#) 단원을 참조하세요.

서비스 계정에 권한 위임

기존 디렉터리에 연결하려면 특정 권한이 위임된 기존 디렉터리의 AD Connector 서비스 계정에 대한 보안 인증이 있어야 합니다. Domain Admins(도메인 관리자) 그룹 멤버라면 이 디렉터리에 연결하기에 충분한 권한이 있지만, 모범 사례에 따르자면 디렉터리 연결에 필요한 최소한의 권한만 가진 서비스 계정을 사용해야 합니다. 다음 절차는 이라는 Connectors 새 그룹을 만들고 이 그룹에 연결하는 AWS Directory Service 데 필요한 권한을 위임한 다음 이 그룹에 새 서비스 계정을 추가하는 방법을 보여줍니다.

이 절차는 디렉터리에 조인된 컴퓨터 상에서 수행해야 하며, [Active Directory User and Computers] MMC 스냅인이 설치되어 있어야 합니다. 또한 도메인 관리자로 로그인해야 합니다.

서비스 계정에 권한을 위임하려면

1. [Active Directory User and Computers]를 열고 탐색 트리에서 도메인 루트를 선택합니다.
2. 왼쪽 창의 목록에서 [Users]를 마우스 오른쪽 버튼으로 클릭하고 [New]와 [Group]을 차례로 선택합니다.
3. [New Object - Group] 대화 상자에서 다음을 입력하고 [OK]를 클릭합니다.

필드	값/선택
그룹 이름	Connectors
[Group scope]	[Global]
[Group type]	보안

4. [Active Directory User and Computers] 탐색 트리에서 도메인 루트를 선택합니다. 메뉴에서 [Action]을 선택한 후 [Delegate Control]을 선택합니다. AD Connector가 AWS 관리형 Microsoft AD에 연결되어 있는 경우 도메인 루트 수준에서 제어를 위임할 수 없습니다. 이 경우 제어를 위임하려면 디렉터리 OU에서 컴퓨터 객체를 만들 OU를 선택하세요.
5. [Delegation of Control Wizard] 페이지에서 Next를 클릭한 후 [Add]를 클릭합니다.
6. [Select Users, Computers, or Groups] 대화 상자에서 Connectors를 입력하고 [OK]를 선택합니다. 객체가 여러 개 있는 경우 위에서 생성한 Connectors 그룹을 선택합니다. 다음을 클릭합니다.

7. [Tasks to Delegate] 페이지에서 [Create a custom task to delegate]를 선택한 후 [Next]를 선택합니다.
8. [Only the following objects in the folder]를 선택한 후 [Computer objects]와 [User objects]를 차례로 선택합니다.
9. [Create selected objects in this folder]를 선택한 후 [Delete selected objects in this folder]를 선택합니다. 다음을 선택합니다.

Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

This folder, existing objects in this folder, and creation of new objects in this folder

Only the following objects in the folder:

- Site Settings objects
- Sites Container objects
- Subnet objects
- Subnets Container objects
- Trusted Domain objects
- User objects

Create selected objects in this folder

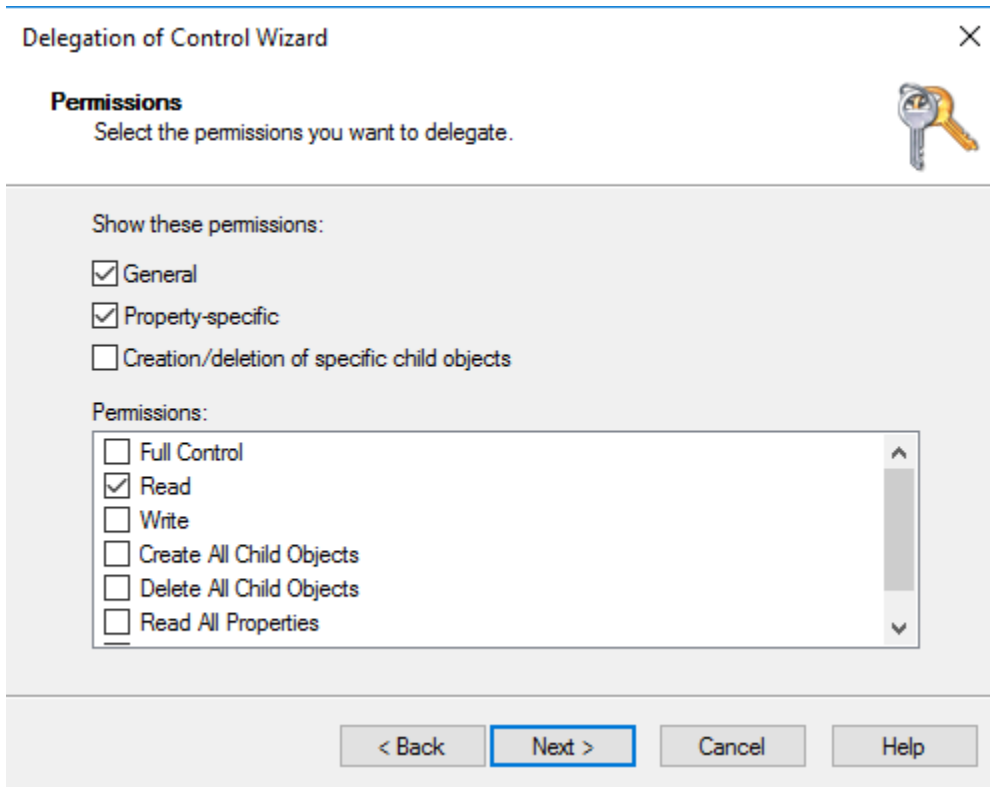
Delete selected objects in this folder

< Back Next > Cancel Help

10. 읽기를 선택한 후 다음을 선택합니다.

Note

원활한 도메인 가입 또는 WorkSpaces 을 사용할 경우 Active Directory에서 컴퓨터 개체를 만들 수 있도록 쓰기 권한도 활성화해야 합니다.



11. [Completing the Delegation of Control Wizard] 페이지에서 정보를 확인하고 [Finish]를 클릭합니다.
12. 강력한 암호로 사용자 계정을 만들고 해당 사용자를 Connectors 그룹에 추가합니다. 이 사용자를 AD Connector 서비스 계정이라고 하며, 이제 이 사용자는 Connectors 그룹의 구성원이 되었으므로 디렉터리에 AWS Directory Service 연결할 수 있는 충분한 권한을 갖게 되었습니다.


AD 커넥터 테스트

AD Connector가 기존 디렉터리에 연결하려면 기존 네트워크의 방화벽에서 특정 포트를 VPC에 있는 두 서브넷의 CIDR에 개방해야 합니다. 이러한 조건이 충족되는지 테스트하려면 다음 단계를 수행하세요.

연결을 테스트하려면


1. VPC에서 Windows 인스턴스를 실행하고 RDP를 통해 연결합니다. 인스턴스가 기존 도메인의 멤버여야 합니다. 나머지 단계들은 이 VPC 인스턴스에서 수행됩니다.

2. [DirectoryServicePortTest](#) 테스트 응용 프로그램을 다운로드하고 압축을 풉니다. 소스 코드 및 Visual Studio 프로젝트 파일이 포함되어 있으므로 원할 경우 테스트 애플리케이션을 수정할 수 있습니다.

 Note

이 스크립트는 Windows Server 2003 이하 OS에서는 지원되지 않습니다.

3. Windows 명령 프롬프트에서 다음 옵션을 사용하여 DirectoryServicePortTest 테스트 애플리케이션을 실행합니다.

 Note

DirectoryServicePortTest 테스트 응용 프로그램은 도메인 및 포리스트 기능 수준이 Windows Server 2012 R2 이하로 설정된 경우에만 사용할 수 있습니다.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
"53,88,389" -udp "53,88,389"
```

<domain_name>

정규화된 도메인 이름이며, 포리스트 및 도메인 기능 수준을 테스트하는 데 사용됩니다. 도메인 이름을 제외하면 기능 수준이 테스트되지 않습니다.

<server_IP_address>

기존 도메인에 있는 도메인 컨트롤러의 IP 주소입니다. 포트가 이 IP 주소에 대해 테스트됩니다. IP 주소를 제외하면 포트가 테스트되지 않습니다.

이 테스트 앱은 VPC에서 도메인까지 필요한 포트들이 열려 있는지 판단하고, 최소한의 포리스트 및 도메인 기능 수준을 확인합니다.

다음과 같은 결과가 출력됩니다.

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
```

```
Domain Functional Level = Windows2008R2Domain : PASSED
```

```
Testing required TCP ports to <server_IP_address>:
```

```
Checking TCP port 53: PASSED
```

```
Checking TCP port 88: PASSED
```

```
Checking TCP port 389: PASSED
```

```
Testing required UDP ports to <server_IP_address>:
```

```
Checking UDP port 53: PASSED
```

```
Checking UDP port 88: PASSED
```

```
Checking UDP port 389: PASSED
```

다음은 DirectoryServicePortTest 애플리케이션에 대한 소스 코드입니다.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
```

```
    if (ParseArgs(args))
    {
        try
        {
            if (_domain.Length > 0)
            {
                try
                {
                    TestForestFunctionalLevel();

                    TestDomainFunctionalLevel();
                }
                catch (ActiveDirectoryObjectNotFoundException)
                {
                    Console.WriteLine("The domain {0} could not be found.\n",
                        _domain);
                }
            }

            if (null != _ipAddr)
            {
                if (_tcpPorts.Count > 0)
                {
                    TestTcpPorts(_tcpPorts);
                }

                if (_udpPorts.Count > 0)
                {
                    TestUdpPorts(_udpPorts);
                }
            }
        }
        catch (AuthenticationException ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
    else
    {
        PrintUsage();
    }

    Console.Write("Press <enter> to continue.");
    Console.ReadLine();
}
```

```
    }

    static void PrintUsage()
    {
        string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
        Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
    }

    static bool ParseArgs(string[] args)
    {
        bool fReturn = false;
        string ipAddress = "";

        try
        {
            _tcpPorts = new List<int>();
            _udpPorts = new List<int>();

            for (int i = 0; i < args.Length; i++)
            {
                string arg = args[i];

                if ("-tcp" == arg | "/tcp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _tcpPorts = ParsePortList(portList);
                }

                if ("-udp" == arg | "/udp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _udpPorts = ParsePortList(portList);
                }

                if ("-d" == arg | "/d" == arg)
                {
                    i++;
                    _domain = args[i];
                }
            }
        }
    }
}
```

```
        if ("-ip" == arg | "/ip" == arg)
        {
            i++;
            ipAddress = args[i];
        }
    }
}
catch (ArgumentOutOfRangeException)
{
    return false;
}

if (_domain.Length > 0 || ipAddress.Length > 0)
{
    fReturn = true;
}

if (ipAddress.Length > 0)
{
    _ipAddr = IPAddress.Parse(ipAddress);
}

return fReturn;
}

static List<int> ParsePortList(string portList)
{
    List<int> ports = new List<int>();

    char[] separators = {',', ';', ':'};

    string[] portStrings = portList.Split(separators);
    foreach (string portString in portStrings)
    {
        try
        {
            ports.Add(Convert.ToInt32(portString));
        }
        catch (FormatException)
        {
        }
    }
}
```

```
        return ports;
    }

    static void TestForestFunctionalLevel()
    {
        Console.WriteLine("Testing forest functional level.");

        DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
        Forest forestContext = Forest.GetForest(dirContext);

        Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

        if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
        {
            Console.WriteLine("PASSED");
        }
        else
        {
            Console.WriteLine("FAILED");
        }

        Console.WriteLine();
    }

    static void TestDomainFunctionalLevel()
    {
        Console.WriteLine("Testing domain functional level.");

        DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
        Domain domainObject = Domain.GetDomain(dirContext);

        Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

        if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
        {
            Console.WriteLine("PASSED");
        }
        else
        {
            Console.WriteLine("FAILED");
        }
    }
}
```



```
        Console.WriteLine();
    }

    static List<int> TestTcpPorts(List<int> portList)
    {
        Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();

        foreach (int port in portList)
        {
            Console.Write("Checking TCP port {0}: ", port);

            TcpClient tcpClient = new TcpClient();

            try
            {
                tcpClient.Connect(_ipAddr, port);

                tcpClient.Close();
                Console.WriteLine("PASSED");
            }
            catch (SocketException)
            {
                failedPorts.Add(port);
                Console.WriteLine("FAILED");
            }
        }

        Console.WriteLine();

        return failedPorts;
    }

    static List<int> TestUdpPorts(List<int> portList)
    {
        Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();

        foreach (int port in portList)
        {
            Console.Write("Checking UDP port {0}: ", port);
```

```
        UdpClient udpClient = new UdpClient();

        try
        {
            udpClient.Connect(_ipAddr, port);
            udpClient.Close();
            Console.WriteLine("PASSED");
        }
        catch (SocketException)
        {
            failedPorts.Add(port);
            Console.WriteLine("FAILED");
        }
    }

    Console.WriteLine();

    return failedPorts;
}
}
```

AD Connector 생성

AD Connector를 사용하여 기존 디렉터리에 연결하려면 다음 단계를 수행합니다. 이 절차를 시작하기 전에 [AD Connector 사전 조건](#)에 나와 있는 선행 조건을 충족했는지 확인합니다.

Note

클라우드 포메이션 템플릿으로는 AD Connector를 만들 수 없습니다.

AD Connector로 연결하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택한 후 디렉터리 설정을 선택합니다.
2. Select directory type(디렉터리 유형 선택) 페이지에서 AD Connector를 선택하고 다음을 선택합니다.
3. Enter AD Connector information(AD Connector 정보 입력) 페이지에서 다음 정보를 입력합니다.

디렉터리 크기

Small(스몰) 또는 Large(라지) 크기 옵션 중에서 선택합니다. 크기에 대한 자세한 내용은 [AD Connector](#) 단원을 참조하세요.

디렉터리 설명

디렉터리에 대한 선택적 설명을 입력합니다.

4. VPC 및 서브넷 선택 페이지에서 다음 정보를 제공한 후 다음을 선택합니다.

VPC

디렉터리에 대한 VPC입니다.

서브넷

도메인 컨트롤러에 대한 서브넷을 선택합니다. 두 서브넷이 서로 다른 가용 영역에 있어야 합니다.

5. Connect to AD(AD에 연결) 페이지에서 다음 정보를 입력합니다.

디렉터리 DNS 이름

기존 디렉터리의 정규화된 이름입니다(예:corp.example.com).

디렉터리 NetBIOS 이름

기존 디렉터리의 약식 이름입니다(예: CORP).

DNS IP 주소

기존 디렉터리에 있는 최소 한 개의 DNS 서버의 IP 주소입니다. 이 서버는 4단계에서 지정된 각 서브넷에서 액세스할 수 있어야 합니다. 지정된 서브넷과 DNS 서버 IP 주소 사이에 네트워크 연결이 있는 한 이러한 서버는 외부에 위치할 수 있습니다. AWS

서비스 계정 사용자 이름

기존 디렉터리에 있는 사용자의 사용자 이름입니다. 이 계정에 대한 자세한 내용은 [AD Connector 사전 조건](#)을 참조하세요.

서비스 계정 암호

기존 사용자 계정의 암호입니다. 이 암호는 대소문자를 구분하며 길이가 8~128자여야 합니다. 또한 다음 네 범주 중 세 개에 해당하는 문자를 1자 이상 포함해야 합니다.

- 소문자(a-z)

- 대문자(A-Z)
- 숫자(0-9)
- 영숫자 외의 특수 문자(~!@#\$\$%^&* _+=`\|(){}[]:;'"<>.,?/)

[Confirm password]

기존 사용자 계정의 암호를 다시 입력합니다.

6. 검토 및 생성 페이지에서 디렉터리 정보를 검토하고 필요한 사항을 변경합니다. 정보가 올바르면 디렉터리 생성을 선택합니다. 디렉터리를 생성하는 데 몇 분 정도 걸립니다. 생성이 완료되면 상태 값이 활성 상태로 변경됩니다.

AD 커넥터로 생성되는 항목

AD 커넥터를 만들면 AWS Directory Service 자동으로 ENI (엘라스틱 네트워크 인터페이스) 를 만들어 각 AD Connector 인스턴스에 연결합니다. 이러한 각 ENI는 VPC와 AD AWS Directory Service 커넥터 간의 연결에 필수적이며 절대 삭제해서는 안 됩니다. “디렉터리 id에 대해AWS 생성된 네트워크 인터페이스”라는 AWS Directory Service 설명으로 사용하도록 예약된 모든 네트워크 인터페이스를 식별할 수 있습니다. 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [탄력적 네트워크 인터페이스](#)를 참조하세요.

Note

AD Connector 인스턴스는 기본적으로 한 리전의 두 가용 영역에 걸쳐 배포되며 Amazon Virtual Private Cloud(VPC)에 연결됩니다. 실패한 AD Connector 인스턴스는 동일한 IP 주소를 사용하여 동일한 가용 영역에서 자동으로 교체됩니다.

AD 커넥터 (AWS IAM Identity Center 포함) 와 통합된 AWS 애플리케이션 또는 서비스에 로그인하면 앱 또는 서비스가 AD Connector로 인증 요청을 전달한 다음 AD Connector는 인증을 위해 자체 관리형 Active Directory의 도메인 컨트롤러에 요청을 전달합니다. 자체 관리형 Active Directory에 성공적으로 인증되면 AD Connector는 앱 또는 서비스에 인증 토큰 (Kerberos 토큰과 유사) 을 반환합니다. 이제 앱 또는 서비스에 액세스할 수 있습니다. AWS

AD Connector 관리 방법

이 단원에서는 AD Connector 환경을 운영하고 유지 관리하기 위한 모든 절차를 나열합니다.

주제

- [AD Connector 디렉터리 보안](#)
- [AD Connector 디렉터리 모니터링](#)
- [Amazon EC2 인스턴스를 다음 인스턴스에 연결하세요. Active Directory](#)
- [AD Connector 디렉터리 유지 관리](#)
- [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#)
- [AD Connector의 DNS 주소 업데이트](#)

AD Connector 디렉터리 보안

이 단원에서는 AD Connector 환경의 보안을 유지하기 위한 고려 사항을 설명합니다.

주제

- [AWS Directory Service에서 AD Connector 서비스 계정 자격 증명을 업데이트](#)
- [AD Connector에 대한 다중 인증 활성화](#)
- [AD Connector를 사용하여 클라이언트 측 LDAPS 활성화](#)
- [스마트 카드와 함께 사용할 수 있도록 AD Connector에서 mTLS 인증 활성화](#)
- [AD용 AWS Private CA 커넥터 설정](#)

AWS Directory Service에서 AD Connector 서비스 계정 자격 증명을 업데이트

AWS Directory Service에서 입력한 AD Connector 보안 인증 정보는 기존의 온프레미스 디렉터리에 액세스하는 데 사용되는 서비스 계정을 나타냅니다. 다음 단계를 수행하여 AWS Directory Service에서 서비스 계정 자격 증명을 수정할 수 있습니다.

Note

디렉터리에서 AWS IAM Identity Center이 활성화된 경우, AWS Directory Service는 현재 서비스 계정에서 새로운 서비스 계정으로 서비스 보안 주체 이름(SPN)을 전달해야 합니다. 현재 서비스 계정에 SPN을 삭제할 수 있는 권한이 없거나 새 서비스 계정에 SPN을 추가할 수 있는 권한이 없는 경우에는 두 작업을 수행하기 위한 권한을 가진 디렉터리 계정에 대한 자격 증명 화면에 나타납니다. 이 자격 증명은 SPN을 전달하는 용도로만 사용되며, 서비스에 저장되지 않습니다.

AWS Directory Service에서 AD Connector 서비스 계정 자격 증명을 업데이트하려면

1. [AWS Directory Service 콘솔](#) 탐색 창의 Active Directory에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 아래로 스크롤하여 서비스 계정 보안 인증 섹션으로 이동합니다.
4. 서비스 계정 자격 증명 섹션에서 업데이트를 선택합니다.
5. 서비스 계정 보안 인증 정보 업데이트 대화 상자에 서비스 계정 사용자 이름과 암호를 입력합니다. 암호를 다시 입력하여 확인한 다음 업데이트를 선택합니다.

AD Connector에 대한 다중 인증 활성화

온프레미스 혹은 EC2 인스턴스로 액티브 디렉터리를 가동하는 경우 AD Connector에 대해 다중 인증을 활성화할 수 있습니다. AWS Directory Service에서 다중 인증 사용에 대한 자세한 내용은 [AD Connector 사전 조건](#) 단원을 참조하세요.

Note

Simple AD에는 다중 인증을 사용할 수 없습니다. 그러나 AWS Managed Microsoft AD 디렉터리에 대해서는 MFA를 활성화할 수 있습니다. 자세히 알아보려면 [AWS 관리형 Microsoft AD에 대한 다중 요소 인증을 활성화합니다.](#)의 내용을 참조하세요.

AD Connector에 대한 다중 인증 활성화

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. AD Connector 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 Networking & security(네트워킹 및 보안) 탭을 선택합니다.
4. 다중 인증 섹션에서 작업을 선택한 다음 활성화를 선택합니다.
5. Enable multi-factor authentication (MFA)(다중 인증(MFA) 활성화) 페이지에서 다음 값을 제공합니다.

레이블 표시

레이블 이름을 제공합니다.

RADIUS 서버 DNS 이름 또는 IP 주소

RADIUS 서버 엔드포인트의 IP 주소 또는 RADIUS 서버 로드 밸런서의 IP 주소입니다. 쉼표로 구분하여 여러 IP 주소를 입력할 수 있습니다(예: 192.0.0.0, 192.0.0.12).

Note

RADIUS MFA는 Amazon 또는 Amazon Chime과 같은 아마존 엔터프라이즈 애플리케이션 및 서비스 또는 서비스에 대한 액세스를 인증하는 데만 적용됩니다. AWS Management Console WorkSpaces QuickSight EC2 인스턴스에서 실행되는 Windows 워크로드 또는 EC2 인스턴스 로그인에 대해서는 MFA를 제공하지 않습니다. AWS Directory Service는 RADIUS 챌린지/응답 인증을 지원하지 않습니다.

사용자는 사용자 이름과 암호를 입력할 때 MFA 코드를 알고 있어야 합니다. 또는 사용자에 대한 SMS 텍스트 out-of-band 검증과 같은 MFA를 수행하는 솔루션을 사용해야 합니다. out-of-band MFA 솔루션에서는 RADIUS 제한 시간 값을 솔루션에 맞게 설정해야 합니다. out-of-band MFA 솔루션을 사용하는 경우 로그인 페이지에서 사용자에게 MFA 코드를 입력하라는 메시지가 표시됩니다. 이 경우, 사용자가 암호 필드와 MFA 필드 모두에 암호를 입력하는 것이 모범 사례입니다.

포트

RADIUS 서버에서 통신용으로 사용 중인 포트입니다. 온프레미스 네트워크는 AWS Directory Service 서버에서 기본 RADIUS 서버 포트(UDP:1812)로 전송되는 인바운드 트래픽을 허용해야 합니다.

Shared secret code

RADIUS 엔드포인트가 생성될 때 지정된 공유 보안 코드입니다.

Confirm shared secret code

RADIUS 엔드포인트의 공유 보안 코드를 확인합니다.

프로토콜

RADIUS 엔드포인트가 생성될 때 지정된 프로토콜을 선택합니다.

서버 제한 시간(초)

RADIUS 서버에서 응답을 대기할 시간(초)입니다. 이 값은 1~50이어야 합니다.

최대 RADIUS 요청 재시도

RADIUS 서버와 통신을 시도하는 횟수입니다. 이 값은 0~10이어야 합니다.

[RADIUS Status]가 [Enabled]로 변경되면 다중 인증을 사용할 수 있습니다.

6. 활성화를 선택합니다.

AD Connector를 사용하여 클라이언트 측 LDAPS 활성화

클라이언트 측 LDAPS는 Microsoft Active Directory(AD)와 AWS 애플리케이션 간의 암호화 통신을 지원합니다. 이러한 애플리케이션의 예로는 WorkSpaces, AWS IAM Identity Center, Amazon QuickSight, Amazon Chime 등이 있습니다. 이 암호화를 통해 조직의 자격 증명 데이터에 대한 보안을 강화하고 보안 요구 사항을 충족할 수 있습니다.

주제

- [필수 조건](#)
- [클라이언트 측 LDAPS 활성화](#)
- [클라이언트 측 LDAPS 관리](#)

필수 조건

클라이언트 측 LDAPS를 활성화하려면 먼저 다음 요구 사항을 충족해야 합니다.

주제

- [Active Directory에 서버 인증서 배포](#)
- [CA 인증서 요구 사항](#)
- [네트워킹 요구 사항](#)

Active Directory에 서버 인증서 배포

클라이언트 측 LDAPS를 활성화하려면 Active Directory의 각 도메인 컨트롤러에 대한 서버 인증서를 가져와 설치해야 합니다. LDAP 서비스에서는 이러한 인증서를 사용하여 LDAP 클라이언트로부터의 SSL 연결을 수신하고 자동으로 수락합니다. 사내 Active Directory 인증서 서비스(ADCS) 배포에서 발급하거나 상업용 발급자로부터 구매한 SSL 인증서를 사용할 수 있습니다. Active Directory 서버 인증서 요구 사항에 대한 자세한 내용은 Microsoft 웹 사이트의 [LDAP over SSL \(LDAPS\) Certificate](#)를 참조하세요.

CA 인증서 요구 사항

클라이언트 측 LDAPS 작업에는 서버 인증서의 발급자를 나타내는 인증 기관(CA) 인증서가 필요합니다. CA 인증서는 LDAP 통신을 암호화하기 위해 Active Directory 도메인 컨트롤러에서 제공하는 서버 인증서와 일치합니다. 다음 CA 인증서 요구 사항에 유의하세요.

- 인증서를 등록하려면 만료일까지 90일 이상 남아 있어야 합니다.
- 인증서는 PEM(Privacy-Enhanced Mail) 형식이어야 합니다. Active Directory 내부에서 CA 인증서를 내보내는 경우 내보내기 파일 형식으로 base64로 인코딩된 X.509(.CER)를 선택합니다.
- AD Connector 디렉터리당 최대 5개의 CA 인증서를 저장할 수 있습니다.
- RSASSA-PSS 서명 알고리즘을 사용하는 인증서는 지원되지 않습니다.

네트워킹 요구 사항

AWS 애플리케이션 LDAP 트래픽은 LDAP 포트 389로 돌아가지 않고 TCP 포트 636에서만 실행됩니다. 그러나 복제, 신뢰 등을 지원하는 Windows LDAP 통신은 Windows 기본 보안과 함께 LDAP 포트 389를 계속 사용합니다. AD Connector(아웃바운드) 및 자체 관리형 Active Directory(인바운드)의 포트 636에서 TCP 통신을 허용하도록 AWS 보안 그룹과 네트워크 방화벽을 구성합니다.

클라이언트 측 LDAPS 활성화

클라이언트 측 LDAPS를 활성화하려면 인증 기관(CA) 인증서를 AD Connector로 가져온 다음 디렉터리에서 LDAPS를 활성화합니다. 활성화하면 AWS 애플리케이션과 자체 관리형 Active Directory 간의 모든 LDAP 트래픽이 Secure Sockets Layer(SSL) 채널 암호화를 통해 흐릅니다.

두 가지 방법을 사용하여 디렉터리에 대해 클라이언트 측 LDAPS를 활성화할 수 있습니다. AWS Management Console 메서드 또는 AWS CLI 메서드를 사용할 수 있습니다.

주제

- [1단계: AWS Directory Service에서 인증서 등록](#)
- [2단계: 등록 상태 확인](#)
- [3단계: 클라이언트 측 LDAPS 활성화](#)
- [4단계: LDAPS 상태 확인](#)

1단계: AWS Directory Service에서 인증서 등록

다음 방법 중 하나를 사용하여 AWS Directory Service에서 인증서를 등록합니다.

방법 1: AWS Directory Service(AWS Management Console)에서 인증서를 등록하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션에서 작업 메뉴를 선택한 다음 인증서 등록을 선택합니다.
5. CA 인증서 등록 대화 상자에서 찾아보기를 선택한 다음 인증서를 선택하고 열기를 선택합니다.
6. 인증서 등록을 선택합니다.

방법 2: AWS Directory Service(AWS CLI)에서 인증서를 등록하려면

- 다음 명령을 실행합니다. 인증서 데이터의 경우 CA 인증서 파일의 위치를 가리킵니다. 응답에 인증서 ID가 제공됩니다.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data  
file://your_file_path
```

2단계: 등록 상태 확인

인증서 등록 상태 또는 등록된 인증서 목록을 보려면 다음 명령을 사용합니다.

방법 1: AWS Directory Service(AWS Management Console)에서 인증서 등록 상태를 확인하려면

1. Directory details(디렉터리 세부 정보) 페이지의 클라이언트측 LDAPS 섹션으로 이동합니다.
2. 등록 상태 열 아래 표시되는 현재 인증서 등록 상태를 검토합니다. 등록 상태 값이 등록됨으로 변경되면 인증서가 성공적으로 등록된 것입니다.

방법 2: AWS Directory Service(AWS CLI)에서 인증서 등록 상태를 확인하려면

- 다음 명령을 실행합니다. 상태 값이 Registered를 반환하면 인증서가 성공적으로 등록된 것입니다.

```
aws ds list-certificates --directory-id your_directory_id
```

3단계: 클라이언트 측 LDAPS 활성화

다음 방법 중 하나를 사용하여 AWS Directory Service에서 클라이언트 측 LDAPS를 활성화합니다.

Note

클라이언트 측 LDAPS를 활성화하려면 인증서를 하나 이상 등록해야 합니다.

방법 1: AWS Directory Service(AWS Management Console)에서 클라이언트 측 LDAPS를 활성화하려면

1. Directory details(디렉터리 세부 정보) 페이지의 클라이언트 측 LDAPS 섹션으로 이동합니다.
2. 활성화를 선택합니다. 이 옵션을 사용할 수 없는 경우, 유효한 인증서가 성공적으로 등록되었는지 확인한 다음 다시 시도하세요.
3. 클라이언트 측 LDAPS 활성화 대화 상자에서 활성화를 선택합니다.

방법 2: AWS Directory Service(AWS CLI)에서 클라이언트 측 LDAPS를 활성화하려면

- 다음 명령을 실행합니다.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

4단계: LDAPS 상태 확인

다음 방법 중 하나를 사용하여 AWS Directory Service에서 LDAPS 상태를 확인합니다.

방법 1: AWS Directory Service(AWS Management Console)에서 LDAPS 상태를 확인하려면

1. Directory details(디렉터리 세부 정보) 페이지의 클라이언트 측 LDAPS 섹션으로 이동합니다.
2. 상태 값이 활성화됨으로 표시되면 LDAPS가 성공적으로 구성된 것입니다.

방법 2: AWS Directory Service(AWS CLI)에서 LDAPS 상태를 확인하려면

- 다음 명령을 실행합니다. 상태 값이 Enabled을 반환하면 LDAPS가 성공적으로 구성된 것입니다.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

클라이언트 측 LDAPS 관리

LDAPS 구성을 관리하려면 다음 명령을 사용합니다.

두 가지 방법을 사용하여 클라이언트 측 LDAPS 설정을 관리할 수 있습니다. AWS Management Console 방법 또는 AWS CLI 방법을 사용할 수 있습니다.

인증서 세부 정보 보기

다음 방법 중 하나를 사용하여 인증서가 만료되도록 설정된 시기를 확인합니다.

방법 1: AWS Directory Service(AWS Management Console)에서 인증서 세부 정보를 보려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션의 CA 인증서 아래에 인증서에 대한 정보가 표시됩니다.

방법 2: AWS Directory Service(AWS CLI)에서 인증서 세부 정보를 보려면

- 다음 명령을 실행합니다. 인증서 ID의 경우 `register-certificate` 또는 `list-certificates`에서 반환한 식별자를 사용합니다.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

인증서 등록 취소

다음 방법 중 하나를 사용하여 인증서 등록을 취소합니다.

Note

인증서가 하나만 등록된 경우 먼저 LDAPS를 비활성화해야 인증서의 등록을 취소할 수 있습니다.

방법 1: AWS Directory Service(AWS Management Console)에서 인증서 등록을 취소하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.

2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션에서 작업을 선택한 다음 인증서 등록 취소를 선택합니다.
5. CA 인증서 등록 취소 대화 상자에서 등록 취소를 선택합니다.

방법 2: AWS Directory Service(AWS CLI)에서 인증서 등록을 취소하려면

- 다음 명령을 실행합니다. 인증서 ID의 경우 `register-certificate` 또는 `list-certificates`에서 반환한 식별자를 사용합니다.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

클라이언트 측 LDAPS 비활성화

다음 방법 중 하나를 사용하여 클라이언트 측 LDAPS를 비활성화합니다.

방법 1: AWS Directory Service(AWS Management Console)에서 클라이언트 측 LDAPS를 비활성화하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 클라이언트 측 LDAPS 섹션에서 비활성화를 선택합니다.
5. 클라이언트 측 LDAPS 비활성화 대화 상자에서 비활성화를 선택합니다.

방법 2: AWS Directory Service(AWS CLI)에서 클라이언트 측 LDAPS를 비활성화하려면

- 다음 명령을 실행합니다.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

스마트 카드와 함께 사용할 수 있도록 AD Connector에서 mTLS 인증 활성화

스마트 카드를 이용한 인증서 기반 상호 전송 계층 보안 (MTL) 인증을 사용하여 자체 관리형 Active Directory (AD) 및 AD Connector를 WorkSpaces 통해 Amazon에 사용자를 인증할 수 있습니다. 활성화 되면 사용자는 사용자 이름과 비밀번호를 사용하는 대신 WorkSpaces 로그인 화면에서 스마트 카드를 선택하고 PIN을 입력하여 인증합니다. 여기에서 Windows 또는 Linux 가상 데스크톱은 스마트 카드를 사용하여 기본 데스크톱 OS에서 AD에 인증합니다.

Note

AD Connector의 스마트 카드 인증은 다음 AWS 리전제품에서만 사용할 수 있으며 다음을 통해서만 사용할 수 WorkSpaces 있습니다. 현재 다른 AWS 애플리케이션은 지원되지 않습니다.

- 미국 동부(버지니아 북부)
- 미국 서부(오리건)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 유럽(아일랜드)
- AWS GovCloud (미국 서부)

주제

- [필수 조건](#)
- [스마트 카드 인증 활성화](#)
- [스마트 카드 인증 설정 관리](#)

필수 조건

Amazon WorkSpaces 클라이언트용 스마트 카드를 사용하여 인증서 기반 상호 전송 계층 보안 (MTL) 인증을 활성화하려면 자체 관리형 시스템과 통합된 운영 스마트 카드 인프라가 필요합니다. Active Directory Amazon에서 스마트 카드 인증을 설정하는 방법에 대한 자세한 내용은 [Amazon WorkSpaces WorkSpaces 관리 안내서](#)를 참조하십시오. Active Directory

에 대한 WorkSpaces 스마트 카드 인증을 활성화하기 전에 다음 고려 사항을 검토하십시오.

- [CA 인증서 요구 사항](#)

- [사용자 인증서 요구 사항](#)
- [인증서 해지 확인 프로세스](#)
- [기타 고려 사항](#)

CA 인증서 요구 사항

AD Connector에는 스마트 카드 인증을 위해 사용자 인증서 발급자를 나타내는 인증 기관(CA) 인증서가 필요합니다. AD Connector는 CA 인증서를 사용자가 스마트 카드로 제시한 인증서와 일치시킵니다. 다음 CA 인증서 요구 사항에 유의하세요.

- CA 인증서를 등록할 수 있으려면 만료일까지 90일 이상 남아 있어야 합니다.
- CA 인증서는 PEM(Privacy-Enhanced Mail) 형식이어야 합니다. Active Directory 내부에서 CA 인증서를 내보내는 경우 내보내기 파일 형식으로 Base64로 인코딩된 X.509(.CER)를 선택합니다.
- 스마트 카드 인증이 성공하려면 발급하는 CA에서 사용자 인증서로 연결되는 모든 루트 및 중간 CA 인증서를 업로드해야 합니다.
- AD Connector 디렉터리당 최대 100개의 CA 인증서를 저장할 수 있습니다
- AD Connector는 CA 인증서에 대한 RSASSA-PSS 서명 알고리즘을 지원하지 않습니다.
- 인증서 전달 서비스가 자동으로 설정되어 실행 중인지 확인하십시오.

사용자 인증서 요구 사항

다음은 사용자 인증서에 대한 몇 가지 요구 사항입니다.

- 사용자의 스마트 카드 인증서에는 사용자 (UPN) 의 주체 대체 이름 userPrincipalName (SAN) 이 있습니다.
- 사용자의 스마트 카드 인증서에는 스마트 카드 로그인 (1.3.6.1.4.1.311.20.2.2) 클라이언트 인증 (1.3.6.1.5.5.7.3.2) 과 같은 고급 키 사용이 있습니다.
- 사용자 스마트 카드 인증서에 대한 OCSP (온라인 인증서 상태 프로토콜) 정보는 기관 정보 액세스의 액세스 방법=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) 이어야 합니다.

AD Connector 및 스마트 카드 인증 요구 사항에 대한 자세한 내용은 Amazon WorkSpaces 관리 안내서의 [요구 사항을](#) 참조하십시오. 로그인 WorkSpaces, 암호 재설정 또는 연결과 같은 Amazon WorkSpaces 문제를 [해결하는 데 도움이 필요하다면 Amazon WorkSpaces User Guide의 WorkSpaces 클라이언트 문제 해결을](#) 참조하십시오. WorkSpaces

인증서 해지 확인 프로세스

스마트 카드 인증을 수행하려면 AD Connector가 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 사용자 인증서의 해지 상태를 확인해야 합니다. 인증서 해지 확인을 수행하려면 OCSP 응답자 URL이 인터넷에서 액세스할 수 있어야 합니다. DNS 이름을 사용하는 경우 OCSP 응답자 URL은 IANA([인터넷 할당 번호 기관](#)) [루트 영역 데이터베이스](#)에 있는 최상위 도메인을 사용해야 합니다.

AD Connector 인증서 해지 확인에서는 다음 프로세스를 사용합니다.

- AD Connector는 OCSP 응답자 URL에 대한 사용자 인증서의 AIA(기관 정보 액세스) 확장을 확인해야 합니다. 그러면 AD Connector는 URL을 사용하여 해지를 확인합니다.
- AD Connector가 사용자 인증서 AIA 확장에 있는 URL을 확인할 수 없거나 사용자 인증서에서 OCSP 응답자 URL을 찾을 수 없는 경우 AD Connector는 루트 CA 인증서 등록 중에 제공된 선택적 OCSP URL을 사용합니다.

사용자 인증서 AIA 확장의 URL이 확인되지만 응답하지 않는 경우 사용자 인증이 실패합니다.

- 루트 CA 인증서 등록 중에 제공된 OCSP 응답자 URL이 확인되지 않거나 응답하지 않거나 제공된 OCSP 응답자 URL이 없는 경우 사용자 인증이 실패합니다.
- [OCSP 서버는 RFC 6960을 준수해야 합니다](#). 또한 OCSP 서버는 총 255바이트 이하의 요청에 대해 GET 메서드를 사용하는 요청을 지원해야 합니다.

Note

AD Connector에는 OCSP 응답자 URL에 대한 HTTP URL이 필요합니다.

기타 고려 사항

AD Connector에서 스마트 카드 인증을 사용하도록 설정하기 전에 다음 항목을 고려하세요.

- AD Connector는 인증서 기반 상호 전송 계층 보안 인증(상호 TLS)을 사용하여 하드웨어 또는 소프트웨어 기반 스마트 카드 인증서를 사용하여 Active Directory에 사용자를 인증합니다. 현재는 CAC(일반 액세스 카드) 및 PIV(개인 신원 확인) 카드만 지원됩니다. 다른 유형의 하드웨어 또는 소프트웨어 기반 스마트 카드는 작동할 수 있지만 스트리밍 프로토콜과 함께 사용하도록 테스트되지는 않았습니다. WorkSpaces
- 스마트 카드 인증은 사용자 이름 및 암호 인증을 로 대체합니다. WorkSpaces

스마트 카드 인증을 사용하도록 AD Connector 디렉터리에 다른 AWS 응용 프로그램을 구성한 경우에도 해당 응용 프로그램에는 여전히 사용자 이름 및 암호 입력 화면이 표시됩니다.

- 스마트 카드 인증을 활성화하면 사용자 세션 길이가 Kerberos 서비스 티켓의 최대 수명으로 제한됩니다. 그룹 정책을 사용하여 이 설정을 구성할 수 있으며 기본적으로 10시간으로 설정되어 있습니다. 이 설정에 대한 자세한 내용은 [Microsoft 설명서](#)를 참조하세요.
- AD Connector 서비스 계정의 지원되는 Kerberos 암호화 유형은 도메인 컨트롤러에서 지원하는 각 Kerberos 암호화 유형과 일치해야 합니다.

스마트 카드 인증 활성화

AD 커넥터에서 스마트 카드 인증을 활성화하려면 먼저 CA (인증 기관) 인증서를 AD Connector로 가져와야 합니다. WorkSpaces AWS Directory Service 콘솔, [API](#) 또는 [CLI](#)를 사용하여 AD 커넥터로 CA 인증서를 가져올 수 있습니다. 다음과 같은 단계를 사용하여 CA 인증서를 가져온 다음 스마트 카드 인증을 활성화합니다.

주제

- [1단계: AD Connector 서비스 계정에 대해 Kerberos 제한된 위임 활성화](#)
- [2단계: AD Connector에 CA 인증서 등록](#)
- [3단계: 지원되는 AWS 애플리케이션 및 서비스에 대한 스마트 카드 인증 활성화](#)

1단계: AD Connector 서비스 계정에 대해 Kerberos 제한된 위임 활성화

AD Connector를 통한 스마트 카드 인증을 사용하려면 자체 관리형 AD 디렉터리의 LDAP 서비스에 대한 AD Connector 서비스 계정에 대해 Kerberos 제한된 위임(KCD)을 사용하도록 설정해야 합니다.

Kerberos 제한된 위임은 Windows Server의 새 기능입니다. 이 기능은 관리자에게 애플리케이션 서비스가 사용자 대신 작동할 수 있는 범위를 제한하여 애플리케이션 신뢰 경계를 지정 및 시행할 수 있는 능력을 제공합니다. 자세한 내용은 [Kerbero 제한된 위임](#)을 참조하세요.

Note

Kerberos 제한 위임 (KCD) 을 사용하려면 AD Connector 서비스 계정의 사용자 이름 부분이 동일한 AccountName 사용자의 SaM과 일치해야 합니다. AccountName sAM은 20자로 제한됩니다. AccountName sAM은 이전 버전의 Windows 클라이언트 및 서버의 로그인 이름으로 사용되는 Microsoft Active Directory 속성입니다.

1. SetSpn 명령을 사용하여 자체 관리형 AD에서 AD Connector 서비스 계정의 SPN(서비스 보안 주체 이름)을 설정합니다. 이렇게 하면 서비스 계정을 위임 구성에 사용할 수 있습니다.

SPN은 모든 서비스 또는 이름 조합일 수 있지만, 기존 SPN과 중복될 수는 없습니다. -s에서는 중복이 있는지 확인합니다.

```
setspn -s my/spn service_account
```

2. AD 사용자 및 컴퓨터에서 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 다음 AD Connector 서비스 계정을 선택하고 Properties(속성)를 선택합니다.
3. Delegation(위임) 탭을 선택합니다.
4. 지정된 서비스에만 위임할 수 있도록 이 사용자를 신뢰를 선택하고 모든 인증 프로토콜 사용 옵션을 선택합니다.
5. 추가를 선택한 다음 사용자 또는 컴퓨터를 선택하여 도메인 컨트롤러를 찾습니다.
6. 확인을 선택하면 위임에 사용할 수 있는 서비스 목록이 표시됩니다.
7. ldap 서비스 역할 유형을 선택한 후 확인을 선택합니다.
8. 확인을 선택하여 새 구성을 저장합니다.
9. Active Directory의 다른 도메인 컨트롤러에 대해서도 이 프로세스를 반복합니다. 를 사용하여 프로세스를 자동화할 수도 PowerShell 있습니다.

2단계: AD Connector에 CA 인증서 등록

다음 방법 중 하나를 사용하여 AD Connector 디렉터리의 CA 인증서를 등록합니다.

방법 1: AD Connector(AWS Management Console)에서 인증서를 등록하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 스마트 카드 인증 섹션에서 작업을 선택한 다음 인증서 등록을 선택합니다.
5. 인증서 등록 대화 상자에서 파일 선택을 선택한 다음 인증서를 선택하고 열기를 선택합니다. OCSP(온라인 인증서 상태 프로토콜) 응답자 URL을 제공하여 이 인증서에 대한 해지 확인을 수행하도록 선택할 수도 있습니다. OCSP에 대한 자세한 내용은 [인증서 해지 확인 프로세스](#) 단원을 참조하세요.
6. 인증서 등록을 선택합니다. 인증서 상태가 등록으로 변경되면 등록 프로세스가 성공적으로 완료된 것입니다.

방법 2: AD Connector(AWS CLI)에서 CA 인증서를 등록하려면

- 다음 명령을 실행합니다. 인증서 데이터의 경우 CA 인증서 파일의 위치를 가리킵니다. 보조 OCSP 응답자 주소를 제공하려면 선택적 ClientCertAuthSettings 객체를 사용합니다.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data file://your_file_path --type ClientCertAuth --client-cert-auth-settings OCSPUrl=http://your_OCSP_address
```

성공하면 응답은 인증서 ID를 제공합니다. 다음 CLI 명령을 실행하여 CA 인증서가 성공적으로 등록되었는지 확인할 수도 있습니다.

```
aws ds list-certificates --directory-id your_directory_id
```

상태 값이 Registered를 반환하면 인증서가 성공적으로 등록된 것입니다.

3단계: 지원되는 AWS 애플리케이션 및 서비스에 대한 스마트 카드 인증 활성화

다음 방법 중 하나를 사용하여 AD Connector 디렉터리의 CA 인증서를 등록할 수 있습니다.

방법 1: AD Connector(AWS Management Console) 에서 스마트 카드 인증을 활성화하려면

- 디렉터리 세부 정보 페이지의 스마트 카드 인증 섹션으로 이동한 다음 활성화를 선택합니다. 이 옵션을 사용할 수 없는 경우, 유효한 인증서가 성공적으로 등록되었는지 확인한 다음 다시 시도하세요.
- 스마트 카드 인증 활성화 대화 상자에서 활성화를 선택합니다.

방법 2: AD Connector(AWS CLI)에서 스마트 카드 인증을 활성화하려면

- 다음 명령을 실행합니다.

```
aws ds enable-client-authentication --directory-id your_directory_id --type SmartCard
```

성공하면 AD Connector는 HTTP 본문이 비어 있는 HTTP 200 응답을 반환합니다.

스마트 카드 인증 설정 관리

두 가지 방법을 사용하여 스마트 카드 설정을 관리할 수 있습니다. AWS Management Console 방법 또는 방법 중 하나를 사용할 수 있습니다. AWS CLI

주제

- [인증서 세부 정보 보기](#)
- [인증서 등록 취소](#)
- [스마트 카드 인증 비활성화](#)

인증서 세부 정보 보기

다음 방법 중 하나를 사용하여 인증서가 만료되도록 설정된 시기를 확인합니다.

방법 1: AWS Directory Service (AWS Management Console) 에서 인증서 세부 정보를 보려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. AD Connector 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 스마트 카드 인증 섹션의 CA 인증서에서 인증서 ID를 선택하여 해당 인증서에 대한 세부 정보를 표시합니다.

방법 2: AWS Directory Service (AWS CLI) 에서 인증서 세부 정보를 보려면

- 다음 명령을 실행합니다. 인증서 ID의 경우 `register-certificate` 또는 `list-certificates`에서 반환한 식별자를 사용합니다.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

인증서 등록 취소

다음 방법 중 하나를 사용하여 인증서 등록을 취소합니다.

Note

인증서가 하나만 등록된 경우 먼저 스마트 카드 인증을 비활성화해야 인증서의 등록을 취소할 수 있습니다.

방법 1: AWS Directory Service ()AWS Management Console에서 인증서 등록을 취소하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. AD Connector 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 스마트 카드 인증 섹션의 CA 인증서에서 등록 취소하려는 인증서를 선택하고 작업을 선택한 다음 인증서 등록 취소를 선택합니다.

Important

등록 취소하려는 인증서가 활성 상태가 아니거나 현재 스마트 카드 인증을 위한 CA 인증서 체인의 일부로 사용되고 있는지 확인하세요.

5. CA 인증서 등록 취소 대화 상자에서 등록 취소를 선택합니다.

방법 2: () 에서 AWS Directory Service 인증서 등록 취소하기AWS CLI

- 다음 명령을 실행합니다. 인증서 ID의 경우 register-certificate 또는 list-certificates에서 반환한 식별자를 사용합니다.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

스마트 카드 인증 비활성화

다음 방법 중 하나를 사용하여 스마트 카드 인증을 비활성화합니다.

방법 1: AWS Directory Service ()AWS Management Console에서 스마트 카드 인증을 비활성화하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. AD Connector 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.

3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 스마트 카드 인증 섹션에서 비활성화를 선택합니다.
5. 스마트 카드 인증 비활성화 대화 상자에서 비활성화를 선택합니다.

방법 2: AWS Directory Service (AWS CLI) 에서 스마트 카드 인증을 비활성화하려면

- 다음 명령을 실행합니다.

```
aws ds disable-client-authentication --directory-id your_directory_id --type SmartCard
```

AD용 AWS Private CA 커넥터 설정

자체 관리형 Active Directory (AD) 를 AD Connector를 AWS Private Certificate Authority (CA) 와 통합하여 AD 도메인에 가입된 사용자, 그룹 및 컴퓨터에 대한 인증서를 발급하고 관리할 수 있습니다. AWS Private CA AD용 커넥터를 사용하면 로컬 에이전트 또는 프록시 서버를 배포, 패치 또는 업데이트할 필요 없이 자체 관리형 엔터프라이즈 CA의 완전 관리형 AWS Private CA 드롭인 대체 기능을 사용할 수 있습니다.

디렉터리 서비스 콘솔, AD용 AWS Private CA 커넥터 콘솔 또는 [CreateTemplate](#) API 호출을 통해 디렉터리와의 AWS Private CA 통합을 설정할 수 있습니다. Active Directory용 AWS Private CA 커넥터 콘솔을 통해 사실 CA 통합을 설정하려면 Active [Directory용 AWS Private CA 커넥터를](#) 참조하십시오. AWS Directory Service 콘솔에서 이 통합을 설정하는 방법에 대한 단계는 아래를 참조하십시오.

필수 조건

AD Connector를 사용하는 경우 서비스 계정에 추가 권한을 위임해야 합니다. 서비스 계정에 액세스 제어 목록(ACL)을 설정하여 다음 작업을 수행할 수 있도록 하세요.

- 서비스 보안 주체 이름(SPN) 을 자체 추가 및 제거합니다.
- 다음 컨테이너에서 인증 기관을 생성하고 업데이트합니다.

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- 아래 예와 같이 NT AuthCertificates 인증 기관 개체를 만들고 업데이트하십시오. NT AuthCertificates 인증 기관 개체가 있는 경우 해당 개체에 대한 권한을 위임해야 합니다. 객체가 없는 경우 퍼블릭 키 서비스 컨테이너에 하위 객체를 생성할 권한을 위임해야 합니다.

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

Note

AWS 관리형 Microsoft AD를 사용하는 경우 디렉터리를 사용하여 AD용 AWS Private CA 커넥터 서비스를 승인하면 추가 권한이 자동으로 위임됩니다.

다음 PowerShell 스크립트를 사용하여 추가 권한을 위임하고 NT AuthCertificates 인증 기관 개체를 만들 수 있습니다. 'myconnectoraccount'를 서비스 계정 이름으로 대체하세요.

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE

# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
    $AccountProperties.SID.Value
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
    $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
    Properties 'schemaIDGUID').schemaIDGUID
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
    Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
    'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
    'Allow', $ServicePrincipalNameGuid, 'None'
```

```

$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"

# Add ACLs allowing AD Connector service account the ability to create certification
  authorities
[System.Guid]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
  $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'certificationAuthority' }
  -Properties 'schemaIDGUID').schemaIDGUID
$CAAccessRule = New-Object -TypeName
  'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
  'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
  $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
  $($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
  $($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
  Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
  Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
  @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
  -Path "CN=Public Key Services,CN=Services,CN=Configuration,
  $($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.Guid]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
  'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
  'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'

```



```
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

AD용 AWS Private CA 커넥터를 설정하려면

1. [에](https://console.aws.amazon.com/directoryservicev2/) AWS Management Console 로그인하고 AWS Directory Service 콘솔을 엽니다 <https://console.aws.amazon.com/directoryservicev2/>.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 네트워크 및 보안 탭의 AD용 AWS Private CA 커넥터에서 AD용 AWS Private CA 커넥터 설정을 선택합니다. 사설 CA 인증서 생성 대상 페이지가 Active Directory 나타납니다. 콘솔의 단계에 따라 Active Directory 커넥터용 사설 CA를 생성하여 사설 CA에 등록하십시오. 자세한 내용은 [커넥터 생성](#)을 참조하세요.
4. 커넥터를 생성한 후 아래 단계에 따라 커넥터 상태 및 연결된 프라이빗 CA의 상태를 비롯한 세부 정보를 확인하세요.

AD용 AWS Private CA 커넥터를 보려면

1. [에](https://console.aws.amazon.com/directoryservicev2/) AWS Management Console 로그인하고 AWS Directory Service 콘솔을 엽니다 <https://console.aws.amazon.com/directoryservicev2/>.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 네트워크 및 보안의 AD용 AWS Private CA 커넥터에서 프라이빗 CA 커넥터 및 연결된 프라이빗 CA를 볼 수 있습니다. 기본적으로 다음 필드가 표시됩니다.
 - a. AWS Private CA 커넥터 ID - 커넥터의 고유 식별자입니다. AWS Private CA 클릭하면 해당 AWS Private CA 커넥터의 세부 정보 페이지로 이동합니다.
 - b. AWS Private CA 제목 — CA의 고유 이름에 대한 정보입니다. 클릭하면 해당 AWS Private CA 세부 정보 페이지로 이동합니다.
 - c. 상태 — AWS Private CA 커넥터 및 커넥터의 상태 확인을 기반으로 AWS Private CA합니다. 두 확인에 모두 통과하면 Active(활성)가 표시됩니다. 확인 중 하나에 실패하면 1/2 checks failed(1/2 확인 실패)가 표시됩니다. 두 확인에 모두 실패하면 Failed(실패)가 표시됩니다. 실패 상태에 대한 자세한 정보는 하이퍼링크에 마우스를 올리면 실패한 확인을 알아 볼 수 있습니다. 콘솔의 지침에 따라 문제를 해결합니다.
 - d. 생성 날짜 - AWS Private CA 커넥터가 생성된 날짜.

자세한 내용은 [커넥터 세부 정보 보기](#)를 참조하세요.

AD Connector 디렉터리 모니터링

다음 방법을 사용하여 AD Connector 디렉터를 모니터링할 수 있습니다.

주제

- [디렉터리 상태 이해](#)
- [Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.](#)

디렉터리 상태 이해

다음은 디렉터리에 대한 다양한 상태입니다.

활성

디렉터리가 정상적으로 작동하고 있습니다. 디렉터리에서 AWS Directory Service 가 어떤 문제도 탐지하지 않았습니

[생성 중]

디렉터리가 현재 생성되는 중입니다. 디렉터리 생성에는 보통 20~45분이 소요되지만, 시스템 로드 에 따라 달라질 수 있습니다.

Deleted

디렉터리가 삭제되었습니다. 디렉터를 위한 모든 리소스들이 해제되었습니다. 디렉터리가 이 상태에 들어오면 복구가 불가능합니다.

[삭제 중]

디렉터리가 현재 삭제되는 중입니다. 디렉터리는 완전히 삭제될 때까지 이 상태를 유지하게 됩니다. 디렉터리가 이 상태에 들어가면 삭제 작업을 취소할 수 없고 디렉터를 복구할 수 없습니다.

실패

디렉터리 생성이 불가능했습니다. 이 디렉터를 삭제하세요. 이 문제가 계속되면 [AWS Support 센터](#)에 문의하세요.

[Impaired]

디렉터리가 성능 저하 상태에서 실행 중입니다. 1개 이상의 문제가 탐지되었고, 모든 디렉터리 작업이 전체 운영 용량에서 실행되지 못할 수 있습니다. 디렉터리가 이 상태가 되는 가능한 이유는 여

러 가지입니다. 여기에는 패치 적용 또는 EC2 인스턴스 교체와 같은 정상적인 운영 유지 관리 활동, 도메인 컨트롤러 중 하나에서 애플리케이션에 의한 일시적 핫스팟 발생 또는 사용자가 네트워크를 변경하는 과정에서 잘못 발생한 디렉터리 통신 중단이 포함됩니다. 자세한 내용은 [AWS 관리형 Microsoft AD 문제 해결](#), [문제 해결 AD Connector](#) 또는 [Simple AD 문제 해결](#) 단원을 참조하세요. 일반적인 유지 관리 관련 문제의 경우 40분 이내에 이러한 문제를 AWS 해결합니다. 문제 해결 주제를 검토한 후 디렉터리가 40분 이상 Impaired 상태를 지속할 경우 [AWS Support 센터](#)에 문의하는 것이 좋습니다.

Important

디렉터리가 Impaired 상태일 동안에는 스냅샷을 복원하지 마세요. 장애를 해결하기 위해 스냅샷 복원이 필요한 경우는 드뭅니다. 자세한 정보는 [디렉터리 스냅샷 또는 복구](#)를 참조하세요.

Inoperable

디렉터리가 작동하지 않습니다. 모든 디렉터리 엔드포인트가 문제를 보고했습니다.

[Requested]

디렉터리를 생성하라는 요청이 현재 보류 중입니다.

Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.

Amazon Simple Notification Service(Amazon SNS)를 사용하면 디렉터리 상태가 바뀔 때 이메일 또는 텍스트(SMS) 메시지를 수신할 수 있습니다. 디렉터리 상태가 활성 상태에서 [손상됨 또는 작동 불가 상태](#)로 바뀌면 알림을 받게 됩니다. 디렉터리가 Active 상태로 돌아갈 때도 알림을 받게 됩니다.

작동 방식

Amazon SNS는 "주제"를 사용해 메시지를 수집 및 배포합니다. 각 주제마다 1명 이상의 구독자가 해당 주제에 게시된 메시지를 수신합니다. 아래 단계를 사용하여 Amazon SNS 주제에 AWS Directory Service 게시자로 추가할 수 있습니다. 디렉터리 상태의 변화를 AWS Directory Service 감지하면 해당 주제에 메시지를 게시하고, 이 메시지는 주제 구독자에게 전송됩니다.

여러 디렉터를 게시자로서 단일 주제에 연결할 수 있습니다. Amazon SNS에서 이전에 생성했던 주제에 디렉터리 상태 메시지를 추가할 수도 있습니다. 주제를 게시하거나 구독할 수 있는 사람을 세부적으로 제어할 수 있습니다. Amazon SNS에 대한 전체 내용은 [Amazon SNS란 무엇인가요?](#) 단원을 참조하세요.

디렉터리에 대해 SNS 메시지를 활성화하는 방법

1. [에 AWS Management Console 로그인하고 콘솔을 엽니다.AWS Directory Service](#)
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 유지 관리 탭을 선택합니다.
4. 디렉터리 모니터링 섹션에서 작업을 선택한 후 알림 생성을 선택합니다.
5. 알림 생성 페이지에서 Choose a notification type(알림 유형 선택)을 선택한 후 새 알림 생성을 선택합니다. 또는, 기존 SNS 주제를 이미 가지고 있는 경우 기존 SNS 주제 연결을 선택하여 이 디렉터리에서 해당 주제로 상태 메시지를 전송할 수 있습니다.

Note

새 알림 생성을 선택하지만, 이미 존재하는 SNS 주제에 대해 동일한 주제 이름을 사용하는 경우에는 Amazon SNS가 새 주제를 생성하지 않고 기존 주제에 새 구독 정보를 추가만 합니다.

기존 SNS 주제 연결을 선택하는 경우 디렉터리와 동일한 리전에 있는 SNS 주제만 선택할 수 있습니다.

6. 수신자 유형을 선택하고 수신자 연락처 정보를 입력합니다. SMS에 사용할 전화 번호를 입력할 때는 숫자만 사용합니다. 대시, 공백, 괄호를 사용하지 마세요.
7. (선택 사항) 주제 이름과 SNS 표시 이름을 제공합니다. 표시 이름은 이 주제에서 모든 SMS 메시지에 포함시킬 짧은 이름(최대 10자)입니다. SMS 옵션을 사용할 때 표시 이름이 필요합니다.

Note

[DirectoryServiceFullAccess](#)관리형 정책만 적용되는 IAM 사용자 또는 역할을 사용하여 로그인한 경우 주제 이름은 "DirectoryMonitoring" 로 시작해야 합니다. 사용자가 주제 이름을 추가로 정의하고 싶으면 SNS에 대한 추가 권한이 필요합니다.

8. 생성을 선택하세요.

[추가 이메일 주소, Amazon SQS 대기열 AWS Lambda등 추가 SNS 구독자를 지정하려는 경우 Amazon SNS 콘솔에서 지정할 수 있습니다.](#)

주제에서 디렉터리 상태 메시지를 삭제하는 방법

1. [에 AWS Management Console 로그인하고 콘솔을 엽니다.AWS Directory Service](#)

2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 유지 관리 탭을 선택합니다.
4. 디렉터리 모니터링 섹션의 목록에서 SNS 주제 이름을 선택하고 작업을 선택한 후 제거를 선택합니다.
5. 제거를 선택합니다.

이렇게 하면 선택한 SNS 주제에 대한 게시자 역할을 하는 디렉터리가 삭제됩니다. 전체 주제를 삭제하려면 [Amazon SNS 콘솔에서](#) 삭제할 수 있습니다.

Note

디렉터리가 해당 주제에 상태 메시지를 전송하고 있지 않아야만 SNS 콘솔을 이용해 Amazon SNS 주제를 삭제할 수 있습니다.

SNS 콘솔을 사용해 Amazon SNS 주제를 삭제하면 이러한 변경이 Directory Services 콘솔 내에 즉각 반영되지 않습니다. 디렉터리의 모니터링 탭에서 주제를 찾을 수 없음을 알리는 상태 업데이트를 확인한 경우에는 다음 번에 디렉터리가 삭제된 주제에 알림을 게시할 때만 알림을 받게 됩니다.

따라서 중요한 디렉터리 상태 메시지를 놓치지 않으려면 메시지를 받는 주제를 삭제하기 전에 디렉터를 다른 Amazon SNS 주제와 연결하십시오. AWS Directory Service

Amazon EC2 인스턴스를 다음 인스턴스에 연결하세요. Active Directory

AD Connector는 클라우드에 정보를 Microsoft Active Directory 캐싱하지 않고도 디렉터리 요청을 온-프레미스로 리디렉션할 수 있는 디렉터리 게이트웨이입니다. Amazon EC2를 Active Directory 도메인에 조인하는 방법에 대한 자세한 내용은 다음과 같습니다.

- 인스턴스가 시작되면 Amazon EC2 인스턴스를 도메인에 원활하게 조인할 Active Directory 수 있습니다. 자세한 정보는 [AD Connector를 사용하여 Amazon Windows EC2 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결할 수 있습니다.](#)을 참조하세요.
- EC2 인스턴스를 Active Directory 도메인에 수동으로 조인해야 하는 경우 적절한 AWS 리전 보안 그룹 또는 서브넷에서 인스턴스를 시작한 다음 인스턴스를 도메인에 조인해야 합니다. Active Directory
- 이러한 인스턴스에 원격 연결이 가능하려면 연결 중인 네트워크에서 인스턴스로의 IP 연결이 있어야 합니다. 대부분의 경우, 이를 위해서는 인터넷 게이트웨이가 Amazon VPC에 연결되고 인스턴스가 퍼블릭 IP 주소를 가지고 있어야 합니다. 인터넷 게이트웨이를 사용하여 인터넷에 연결하는 것에 대

한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.

Note

인스턴스를 자체 관리형 Active Directory (온프레미스) 에 연결하면 인스턴스가 AD Connector 와 직접 Active Directory 통신하고 AD Connector를 우회합니다.

주제

- [AD Connector를 사용하여 Amazon Windows EC2 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결할 수 있습니다.](#)
- [AD Connector를 사용하여 Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결할 수 있습니다.](#)

AD Connector를 사용하여 Amazon Windows EC2 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결할 수 있습니다.

이 절차는 Amazon Windows EC2 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결합니다.
Active Directory

EC2 인스턴스에 원활하게 연결하려면 Windows

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 표시줄에서 기존 디렉터리와 AWS 리전 동일한 디렉터리를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Windows EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지(Amazon Machine Image) 섹션의 빠른 시작 창에서 Windows를 선택합니다. Amazon Machine Image(AMI) 드롭다운 목록에서 Windows Amazon Machine Image(AMI)를 변경할 수 있습니다.

7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다.
 - a. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다.
 - b. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다.
 - c. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다.
 - d. Create key pair(키 페어 생성)를 선택합니다.
 - e. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

⚠ Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.

9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

i Note

도메인 조인 디렉터리를 선택하면 다음이 표시될 수 있습니다.


 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로파일의 경우 기존 IAM 인스턴스 프로파일을 선택하거나 새 프로파일을 생성할 수 있습니다. IAM 인스턴스 프로파일 드롭다운 목록에서 AmazonSSM ManagedInstanceCore 및 AmazonSSM의 AWS 관리형 정책이 DirectoryServiceAccess 연결된 IAM 인스턴스 프로파일을 선택합니다. 새 프로파일을 생성하려면 새 IAM 프로파일 생성 링크를 선택한 후 다음을 수행하십시오.

1. 역할 생성을 선택합니다.
2. Select trusted entity(신뢰할 수 있는 엔터티 선택)에서 AWS Service를 선택합니다.
3. 사용 사례에서 EC2를 선택합니다.
4. 권한 추가의 정책 목록에서 AmazonSSM 및 AmazonSSM ManagedInstanceCore 정책을 선택합니다. DirectoryServiceAccess 목록을 필터링하려면 검색 상자에 **SSM**을(를) 입력합니다. 다음을 선택합니다.

 Note

AmazonSSM은 인스턴스를 관리자에 조인할 수 있는 DirectoryServiceAccess 권한을 제공합니다. Active Directory AWS Directory Service AmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는 기타 권한 및 정책에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

5. Name, review, and create(이름, 검토 및 생성) 페이지에서 Role name(역할 이름)을 입력합니다. EC2 인스턴스에 연결하려면 이 역할 이름이 필요합니다.
 6. (선택 사항) 설명 필드에 IAM 인스턴스 프로파일에 대한 설명을 입력할 수 있습니다.
 7. 역할 생성을 선택합니다.
 8. 인스턴스 시작 페이지로 돌아가서 IAM 인스턴스 프로파일 옆에 있는 새로 고침 아이콘을 선택합니다. 새 IAM 인스턴스 프로파일은 IAM 인스턴스 프로파일 드롭다운 목록에 표시되어야 합니다. 새 프로파일을 선택하고 나머지 설정은 기본값으로 유지합니다.
16. 인스턴스 시작을 선택합니다.

AD Connector를 사용하여 Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결할 수 있습니다.

이 절차는 Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD 디렉터리에 원활하게 연결합니다.

다음과 같은 Linux 인스턴스 배포판과 버전이 지원됩니다.

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2(64비트 x86)
- Red Hat Enterprise Linux 8(HVM)(64비트 x86)
- Ubuntu Server 18.04 LTS 및 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

Ubuntu 14 및 Red Hat Enterprise Linux 7 이전의 배포판은 원활한 도메인 조인 기능을 지원하지 않습니다.

필수 조건

EC2 Linux 인스턴스에 원활한 도메인 조인을 설정하려면 먼저 이 섹션의 절차를 완료해야 합니다.

원활한 도메인 가입 서비스 계정을 선택합니다

AD Connector를 통해 Linux 컴퓨터를 온-프레미스 Active Directory 도메인에 원활하게 연결할 수 있습니다. 이렇게 하려면 컴퓨터 계정 만들기 권한이 있는 사용자 계정을 만들어 컴퓨터를 도메인에 조인해야 합니다. 원하는 경우 AD Connector 서비스 계정을 사용할 수 있습니다. 또는 컴퓨터를 도메인에 조인할 수 있는 충분한 권한이 있는 다른 계정을 사용할 수 있습니다. Domain Admins 또는 다른 그룹의 구성원이 컴퓨터를 도메인에 조인할 충분한 권한을 가지고 있을 수 있지만, 이러한 권한은 사용하지 않는 것이 좋습니다. 모범 사례로, 컴퓨터를 도메인에 조인하는 데 필요한 최소 권한이 있는 서비스 계정을 사용하는 것이 좋습니다.

컴퓨터를 도메인에 가입시키는 데 필요한 최소 권한이 있는 계정을 위임하려면 다음 명령을 실행할 수 있습니다. PowerShell 도메인에 가입되어 있고 설치된 Windows 컴퓨터에서 이러한 명령을 실행해야 합니다. [AWS 관리형 Microsoft AD용 액티브 디렉터리 관리 도구 설치](#) 또한 컴퓨터 OU 또는 컨테이너에 대한 권한을 수정할 권한이 있는 계정을 사용해야 합니다. 이 PowerShell 명령은 서비스 계정인 도메인의 기본 컴퓨터 컨테이너에 컴퓨터 개체를 만들 수 있도록 하는 권한을 설정합니다. GUI(그래픽 사용자 인터페이스)를 선호하는 경우 [서비스 계정에 권한 위임](#)에서 설명하는 수동 프로세스를 사용할 수 있습니다.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
    'schemaNamingContext'
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
    -Filter { LDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
    $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
    in the Computers container.
$AddAccessRule = New-Object -TypeName
    'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
    'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
```

```
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```


GUI(그래픽 사용자 인터페이스)를 선호하는 경우 [서비스 계정에 권한 위임](#)에서 설명하는 수동 프로세스를 사용할 수 있습니다.

도메인 서비스 계정을 저장할 보안 암호 생성

를 AWS Secrets Manager 사용하여 도메인 서비스 계정을 저장할 수 있습니다.

보안 암호를 만들고 도메인 서비스 계정 정보를 저장하려면

1. <https://console.aws.amazon.com/secretsmanager/> 에서 AWS Management Console 로그인하고 AWS Secrets Manager 콘솔을 엽니다.
2. 새 보안 암호 저장(Store a new secret)을 선택합니다.
3. 새 보안 암호 저장(Store a new secret) 페이지에서 다음을 수행합니다.
 - a. 암호 유형에서 다른 암호 유형을 선택합니다.
 - b. 키값 쌍에서 다음을 수행하십시오.
 - i. 첫 번째 상자에 **awsSeamlessDomainUsername**를 입력합니다. 같은 행의 다음 상자에 서비스 계정의 사용자 이름을 입력합니다. 예를 들어 이전에 PowerShell 명령을 사용한 경우 서비스 계정 이름은 다음과 같습니다**awsSeamlessDomain**.

 Note

있는 그대로 **awsSeamlessDomainUsername**을 입력해야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 조인에 실패합니다.

The screenshot shows the AWS Secrets Manager console interface for creating a new secret. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The wizard is in 'Step 1: Choose secret type'. On the left, there are four steps: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The main area is titled 'Choose secret type' and contains three sections: 'Secret type', 'Key/value pairs', and 'Encryption key'. In the 'Secret type' section, four options are listed: 'Credentials for Amazon RDS database', 'Credentials for Amazon DocumentDB database', 'Credentials for Amazon Redshift cluster', and 'Other type of secret' (which is selected and highlighted with a red box). The 'Key/value pairs' section has two tabs: 'Key/value' and 'Plaintext'. Under the 'Key/value' tab, there is one row with the key 'awsSeamlessDomainUsername' (highlighted with a red box) and an empty value field. Below this is a '+ Add row' button. The 'Encryption key' section has a dropdown menu with 'aws/secretsmanager' selected and a refresh button. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. Add row(행 추가)를 선택합니다.
- iii. 새 행의 첫 번째 상자에 **awsSeamlessDomainPassword**를 입력합니다. 같은 행의 다음 상자에 서비스 계정의 암호를 입력합니다.

Note

있는 그대로 **awsSeamlessDomainPassword**을 입력해야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 조인에 실패합니다.

- iv. 암호화 키에서 기본값을 그대로 유지합니다 `aws/secretsmanager`. AWS Secrets Manager 이 옵션을 선택하면 항상 암호를 암호화합니다. 사용자가 생성한 키를 선택할 수도 있습니다.

Note

사용하는 비밀번호에 따라 수수료가 부과됩니다. AWS Secrets Manager 현재 기준의 전체적인 요금 목록은 [AWS Secrets Manager 요금](#)을 참조하세요. Secrets Manager에서 생성한 AWS 관리 키를 `aws/secretsmanager` 사용하여 비밀을 무료로 암호화할 수 있습니다. 자체 KMS 키를 생성하여 암호를 암호화하는 경우 현재 요율로 AWS 요금이 부과됩니다. AWS KMS 자세한 내용은 [AWS Key Management Service 요금](#)을 참조하십시오.

v. 다음을 선택합니다.

- 비밀 이름에 다음 형식을 사용하여 디렉터리 ID가 포함된 비밀 이름을 입력합니다. 이때 `d-xxxxxxxxxx#` 디렉터리 ID로 대체합니다.

```
aws/directory-services/d-xxxxxxxx/seamless-domain-join
```

이는 애플리케이션에서 보안 암호를 검색하는 데 사용됩니다.

Note

있는 그대로 `aws/directory-services/d-xxxxxxxx/seamless-domain-join`를 입력해야 하지만, `d-xxxxxxxxxxxxx`를 디렉터리 ID로 바꿔야 합니다. 선행 공백이나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 가입에 실패합니다.

The screenshot shows the 'Configure secret' page in AWS Secrets Manager. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The page is divided into four steps: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The 'Secret name and description' section is highlighted with a red box around the secret name 'aws/directory-services/d-xxxxxxx/seamless-domain-join'. Below the secret name is a description field containing 'Access to MYSQL prod database for my AppBeta'. The 'Tags' section shows 'No tags associated with the secret.' and an 'Add' button. The 'Resource permissions' section has an 'Edit permissions' button. The 'Replicate secret' section is optional. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

5. 다른 모든 항목은 기본값으로 설정한 후 Next(다음)를 선택합니다.
6. Configure automatic rotation(자동 교체 구성)을 Disable automatic rotation(자동 교체 사용 안 함)으로 선택하고 Next(다음)를 선택합니다.

저장한 후 이 비밀의 로테이션을 켤 수 있습니다.

7. 설정을 검토한 다음 Store(저장)를 선택하여 변경 내용을 저장합니다. 이제 Secrets Manager 콘솔에서 새 보안 암호가 목록에 포함된 계정의 보안 암호 목록으로 돌아갑니다.
8. 목록에서 새로 생성한 보안 암호 이름을 선택하고 보안 암호 ARN 값을 기록해 둡니다. 다음 단원에서 이 값을 사용하게 됩니다.

도메인 서비스 계정 비밀번호에 대한 로테이션을 켜세요.

보안 태세를 개선하려면 정기적으로 암호를 교체하는 것이 좋습니다.

도메인 서비스 계정 비밀번호에 대한 순환 기능을 켜려면

- 사용 AWS Secrets Manager 설명서의 AWS Secrets Manager [암호 자동 교체 설정의](#) 지침을 따르십시오.

5단계의 경우 사용 AWS Secrets Manager 설명서의 [Microsoft Active Directory 순환 템플릿 자격 증명을](#) 사용하십시오.

도움이 필요하면 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager [순환 문제 해결을](#) 참조하십시오.

필요한 IAM policy 정책 및 역할 생성

다음 사전 요구 사항 단계를 사용하여 Secrets Manager 원활한 도메인 가입 암호 (이전에 생성함) 에 대한 읽기 전용 액세스를 허용하는 사용자 지정 정책을 생성하고 새 DomainJoin LinuxEC2 IAM 역할을 생성합니다.

Secrets Manager IAM 읽기 정책 생성

IAM 콘솔을 사용하여 Secrets Manager 보안 암호에 대한 읽기 전용 액세스 권한을 부여하는 정책을 생성합니다.

Secrets Manager IAM 읽기 정책을 생성하려면

1. IAM 정책을 생성할 권한이 있는 AWS Management Console 사용자로 로그인합니다. 그런 다음 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창의 액세스 관리에서 정책을 선택합니다.
3. 정책 생성(Create policy)을 선택합니다.
4. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 그런 다음 JSON 텍스트 상자에 붙여 넣습니다.

Note

지역 및 리소스 ARN을 이전에 생성한 암호의 실제 지역 및 ARN으로 교체해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. 마쳤으면 [Next]를 선택합니다. 정책 검사기가 모든 구문 오류를 보고합니다. IAM 검증 정책에 대한 자세한 내용은 [Validating IAM policies](#)를 참조하세요.
6. Review policy(정책 검토) 페이지에서 **SM-Secret-Linux-DJ-d-xxxxxxxx-Read**와 같은 정책의 이름을 입력합니다. Summary(요약)을 검토하여 정책이 부여하는 권한을 확인합니다. 그런 다음 Create policy(정책 생성)를 선택하여 변경 내용을 저장합니다. 새로운 정책이 관리형 정책 목록에 나타나며 ID 연결 준비가 완료됩니다.

Note

보안 암호당 정책을 하나씩 생성하는 것이 좋습니다. 이렇게 하면 인스턴스가 적절한 보안 암호에만 액세스할 수 있고 인스턴스가 손상될 경우 미치는 영향이 최소화됩니다.

Linux/EC2 역할을 생성하십시오. DomainJoin

IAM 콘솔을 사용하여 Linux EC2 인스턴스를 도메인에 조인하는 데 사용할 역할을 생성합니다.

Linux/EC2 역할을 만들려면 DomainJoin

1. IAM 정책을 생성할 권한이 있는 AWS Management Console 사용자로 로그인합니다. 그런 다음 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.

2. 탐색 창의 액세스 관리에서 역할을 선택합니다.
3. 콘텐츠 창에서 Create role(역할 생성)을 선택합니다.
4. 신뢰할 수 있는 엔티티 유형 선택 아래에서 AWS 서비스를 선택합니다.
5. 사용 사례에서 EC2를 선택한 후 다음을 선택합니다.

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected.

6. Filter policies(필터 정책)의 경우 다음을 수행합니다.
 - a. **AmazonSSManagedInstanceCore**을 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - b. **AmazonSSMDirectoryServiceAccess**을 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - c. **SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read**(또는 이전 절차에서 생성한 IAM 정책의 이름)을(를) 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - d. 위에 나열된 세 가지 정책을 추가한 후 역할 생성을 선택합니다.

Note

AmazonSSM은 인스턴스를 DirectoryServiceAccess 관리자에 조인할 수 있는 Active Directory 권한을 제공합니다. AWS Directory Service AmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는

기타 권한 및 정책에 관한 정보에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

7. 새 역할의 이름 (예: 역할 이름) 필드에 원하는 다른 이름을 입력합니다. **LinuxEC2DomainJoin**
8. (선택 사항)역할 설명에 설명을 입력합니다.
9. (선택 사항) 3단계: 태그를 추가할 태그 추가에서 새 태그 추가를 선택합니다. 태그 키-값 쌍은 이 역할에 대한 액세스를 구성, 추적 또는 제어하는 데 사용됩니다.
10. 역할 생성을 선택합니다.

Amazon EC2 Linux 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 연결합니다. Active Directory

필수 작업을 모두 구성했으므로 이제 다음 절차를 사용하여 EC2 Linux 인스턴스를 원활하게 연결할 수 있습니다.

Linux 인스턴스를 원활하게 연결하려면

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 [Amazon EC2 콘솔을 엽니다.](#)
2. 탐색 표시줄의 지역 선택기에서 기존 디렉토리와 AWS 리전 동일한 디렉토리를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Linux EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지 (Amazon 머신 이미지) 섹션에서 시작하려는 Linux AMI를 선택합니다.

Note

사용되는 AMI에는 AWS Systems Manager (SSM 에이전트) 버전 2.3.1644.0 이상이 있어야 합니다. AMI에서 인스턴스를 시작하여 AMI에 설치된 SSM 에이전트 버전을 확인하려면 [현재 설치된 SSM 에이전트 버전 가져오기](#)를 참조하세요. SSM 에이전트를 업그레이드해야 하는 경우 [Linux용 EC2 인스턴스에 SSM 에이전트 설치 및 구성](#)을 참조하세요. SSM은 Linux 인스턴스를 도메인에 aws:domainJoin 조인할 때 플러그인을 사용합니다. Active Directory ##### Linux ##### ### ## EC2AMAZ- XXXXXXXX #####

#. 에 대한 자세한 내용은 사용 `aws:domainJoin` 설명서의 [AWS Systems Manager 명령 문서 플러그인 참조](#)를 참조하십시오. AWS Systems Manager

7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다. Create key pair(키 페어 생성)를 선택합니다. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.

9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

Note

도메인 조인 디렉터를 선택하면 다음이 표시될 수 있습니다.

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로파일의 경우 사전 요구 사항 섹션 2단계: LinuxEC2 역할 생성에서 이전에 생성한 IAM 역할을 선택합니다. DomainJoin
16. 인스턴스 시작을 선택합니다.

Note

SUSE Linux로 원활한 도메인 조인을 수행하는 경우 인증이 작동하려면 재부팅해야 합니다. Linux 터미널에서 SUSE를 재부팅하려면 `sudo reboot`를 입력합니다.

AD Connector 디렉터리 유지 관리

이 단원에서는 AD Connector 환경에 대해 일반적으로 실시되는 관리 작업을 유지 관리하는 방법을 설명합니다.

주제

- [AD Connector 삭제](#)
- [디렉터리 정보 보기](#)

AD Connector 삭제

AD Connector가 삭제되어도 온프레미스 디렉터리는 그대로 유지됩니다. 디렉터리에 조인된 모든 인스턴스도 변동 없이 보관되며, 온프레미스 디렉터리에 조인된 상태가 유지됩니다. 여전히 디렉터리 자격 증명을 사용해 이러한 인스턴스에 로그인할 수 있습니다.

AD Connector를 삭제하려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다. AD Connector가 배포된 AWS 리전 위치에 있는지 확인하십시오. 자세한 내용은 [지역 선택](#)을 참조하십시오.
2. 삭제하려는 AD Connector에 대해 활성화된 AWS 응용 프로그램이 없는지 확인하십시오. 활성화된 AWS 응용 프로그램을 사용하면 AD Connector를 삭제할 수 없습니다.
 - a. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
 - b. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다. AWS 앱 및 서비스 섹션에서 AD Connector에 사용할 수 있는 AWS 애플리케이션을 확인할 수 있습니다.
 - AWS Management Console 액세스를 비활성화합니다. 자세한 정보는 [AWS Management Console 액세스 비활성화](#)을 참조하세요.
 - WorkSpacesAmazon을 비활성화하려면 WorkSpaces 콘솔의 디렉터리에서 서비스 등록을 취소해야 합니다. 자세한 내용은 Amazon WorkSpaces 관리 가이드의 [디렉터리 등록 취소](#)를 참조하십시오.
 - WorkDocsAmazon을 비활성화하려면 Amazon WorkDocs 콘솔에서 Amazon WorkDocs 사이트를 삭제해야 합니다. 자세한 내용은 Amazon WorkDocs 관리 가이드의 [사이트 삭제](#)를 참조하십시오.
 - WorkMailAmazon을 비활성화하려면 Amazon WorkMail 콘솔에서 Amazon WorkMail 조직을 제거해야 합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 [조직 제거](#)를 참조하십시오.
 - Amazon FSx for Windows File Server를 비활성화하려면 도메인에서 Amazon FSx 파일 시스템을 제거해야 합니다. 자세한 내용은 Windows File Server용 Amazon [FSx 사용 설명서의 Windows File Server용 FSx 사용 설명서의 Windows](#) 파일 서버용 FSx 사용을 참조하십시오. Active Directory
 - Amazon 관계형 데이터베이스 서비스를 비활성화하려면 도메인에서 Amazon RDS 인스턴스를 제거해야 합니다. 자세한 내용은 Amazon RDS 사용 설명서의 [도메인에서 DB 인스턴스 관리하기](#) 단원을 참조하세요.

- AWS Client VPN 서비스를 비활성화하려면 Client VPN 엔드포인트에서 디렉터리 서비스를 제거해야 합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Active Directory [인증](#)을 참조하십시오.
- Amazon Connect를 비활성화하려면 Amazon Connect 인스턴스를 삭제해야 합니다. 자세한 정보는 Amazon Connect 관리자 안내서의 [Amazon Connect 인스턴스 삭제하기](#)를 참조하십시오.
- Amazon을 QuickSight 비활성화하려면 Amazon 구독을 취소해야 합니다. QuickSight 자세한 내용은 Amazon QuickSight 사용 설명서의 Amazon QuickSight [계정](#) 해지를 참조하십시오.

Note

삭제하려는 AWS Managed Microsoft AD 디렉터리를 사용 AWS IAM Identity Center 중이고 이전에 연결한 적이 있는 경우 삭제하려면 먼저 ID 소스를 변경해야 합니다. 자세한 내용은 IAM Identity Center 사용 설명서의 [ID 소스 변경](#)을 참조하십시오.

3. 탐색 창에서 디렉터리를 선택합니다.
4. 삭제할 AD Connector 디렉터리만 선택하고 Delete(삭제)를 클릭합니다. AD Connector를 삭제하는 데 몇 분 정도 걸립니다. AD Connector가 삭제되면 디렉터리 목록에서 제거됩니다.

디렉터리 정보 보기

디렉터리에 대한 세부 정보를 볼 수 있습니다.

디렉터리에 대한 세부 정보 보기

1. [AWS Directory Service 콘솔](#) 탐색 창의 아래에서 Active Directory 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 클릭합니다. 디렉터리에 대한 정보가 디렉터리 세부 정보 페이지에 표시됩니다.

상태 필드에 대한 자세한 내용은 [디렉터리 상태 이해](#) 단원을 참조하십시오.

AWS 애플리케이션 및 서비스에 대한 액세스 지원

사용자는 AD Connector를 승인하여 WorkSpaces Amazon과 같은 AWS 애플리케이션 및 서비스에 액세스 권한을 부여할 수 있습니다Active Directory. AD Connector와 함께 작동하도록 다음 AWS 응용 프로그램 및 서비스를 활성화하거나 비활성화할 수 있습니다.

AWS 애플리케이션/서비스	추가 정보...
Amazon Chime	자세한 내용은 Amazon Chime 관리 안내서 를 참조하세요.
Amazon Connect	자세한 내용은 Amazon Connect 관리 안내서 를 참조하세요.
아마존 WorkDocs	자세한 내용은 Amazon WorkDocs 관리 안내서 를 참조하십시오.
아마존 WorkMail	자세한 내용은 Amazon WorkMail 관리자 안내서 를 참조하십시오.
아마존 WorkSpaces	<p>에서 직접 Simple AD, AWS 관리형 Microsoft AD 또는 AD 커넥터를 만들 수 WorkSpaces 있습니다. Workspace를 생성할 때 고급 설정을 시작하면 됩니다.</p> <p>자세한 내용은 Amazon WorkSpaces 관리 안내서를 참조하십시오.</p>
AWS Client VPN	자세한 내용은 AWS Client VPN 사용 설명서 를 참조하십시오.
AWS IAM Identity Center	자세한 내용은 AWS IAM Identity Center 사용 설명서 를 참조하십시오.
AWS Management Console	자세한 설명은 AD 보안 인증을 사용한 AWS Management Console 액세스 활성화 섹션을 참조하세요.

AWS 애플리케이션/서비스	추가 정보...
AWS Transfer Family	자세한 내용은 AWS Transfer Family 사용 설명서 를 참조하십시오.

일단 활성화가 되면 디렉터리에 대한 액세스 권한을 부여하고자 하는 애플리케이션 또는 서비스의 콘솔에서 디렉터리에 대한 액세스를 관리합니다. AWS Directory Service 콘솔에서 위에서 설명한 AWS 애플리케이션 및 서비스 링크를 찾으려면 다음 단계를 수행하십시오.

디렉터리에서 애플리케이션 및 서비스를 표시하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. AWS apps & services(앱 및 서비스) 섹션에서 목록을 검토합니다.

를 사용하여 AWS AWS Directory Service 응용 프로그램 및 서비스를 승인하거나 권한 부여를 해제하는 방법에 대한 자세한 내용은 [을 참조하십시오. 를 사용하는 AWS 애플리케이션 및 서비스에 대한 권한 부여 AWS Directory Service](#)

AD Connector의 DNS 주소 업데이트

다음 단계에 따라 AD Connector가 가리키고 있는 DNS 주소를 업데이트합니다.

Note

진행 중인 업데이트가 있을 경우, 업데이트가 완료될 때까지 기다렸다가 또 다른 업데이트를 제출하셔야 합니다.

AD Connector와 함께 WorkSpaces를 사용하는 경우 WorkSpaces의 DNS 주소도 업데이트해야 합니다. 자세한 내용은 [WorkSpaces의 DNS 서버 업데이트](#)를 참조하세요.

AD Connector의 DNS 설정을 업데이트하려면

1. [AWS Directory Service 콘솔](#) 탐색 창의 Active Directory에서 디렉터를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 선택합니다.

3. 디렉터리 세부 정보 페이지에서 네트워킹 및 보안 탭을 선택합니다.
4. 기존 DNS 설정 섹션으로 스크롤하여 업데이트를 선택합니다.
5. Update existing DNS addresses(기존 DNS 주소 업데이트) 대화 상자에 업데이트된 DNS IP 주소를 입력하고 업데이트를 선택합니다.

AD Connector 문제 해결에 대한 자세한 내용은 [AD Connector 문제 해결](#)을 참조하세요.

AD Connector 모범 사례

여기에는 문제를 방지하고 AD Connector를 최대한 활용하기 위해 반드시 고려해야 할 몇 가지 제안 및 가이드라인이 나와 있습니다.

설정: 사전 조건

디렉터리를 생성하기 전에 여기 나온 가이드라인을 고려하세요.

디렉터리 유형이 올바른지 확인

AWS Directory Service 다른 AWS 서비스와 Microsoft Active Directory 함께 사용할 수 있는 다양한 방법을 제공합니다. 예산에 맞는 비용으로 필요한 기능을 갖춘 디렉터리 서비스를 선택할 수 있습니다.

- AWS Microsoft Active Directory용 디렉터리 서비스는 클라우드에서 Microsoft Active Directory 호스팅되는 기능이 풍부한 관리형 서비스입니다. AWS 사용자 수가 5,000명 이상이고 AWS 호스팅된 디렉터리와 온-프레미스 디렉터리 간에 신뢰 관계를 설정해야 하는 경우 관리형 Microsoft AD를 사용하는 것이 가장 좋습니다.
- AD Connector는 단순히 기존 Active Directory 온-프레미스에 AWS 연결합니다. AD Connector는 AWS 서비스와 함께 기존의 온프레미스 디렉터리를 사용하고 싶을 때 가장 적합한 옵션입니다.
- Simple AD는 기본 Active Directory 호환성을 갖춘 소규모의 저렴한 디렉터리입니다. 5,000명 이하의 사용자, Samba 4 호환 애플리케이션, LDAP 인식 애플리케이션을 위한 LDAP 호환성을 지원합니다.

AWS Directory Service 옵션에 대한 자세한 비교는 [여기](#)를 참조하십시오. [무엇을 선택할 것인가](#)

VPC와 인스턴스가 올바르게 구성되도록 보장

디렉터리를 연결, 관리 및 사용하려면 디렉터리와 연관이 있는 VPC를 제대로 구성해야 합니다.

VPC 보안 및 네트워킹 요건에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 사전 요구 사항](#), [AD Connector 사전 조건](#) 또는 [간단한 AD 사전 조건](#) 섹션을 참조하세요.

도메인에 인스턴스를 추가하는 경우에는 [Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory](#)에 설명된 대로 인스턴스에 대한 연결 및 원격 액세스가 가능한지 확인하세요.

한도에 유의

특정 디렉터리 유형에 대한 다양한 제한에 대해 알아봅니다. 가용 스토리지와 객체의 전체 크기가 디렉터리에 저장할 수 있는 객체 수에 대한 유일한 제한입니다. 선택한 디렉터리에 대한 자세한 내용은 [AWS Managed Microsoft AD 할당량](#), [AD Connector 할당량](#) 또는 [Simple AD 할당량](#) 섹션을 참조하세요.

디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오.

AWS [보안 그룹을 생성하여 피어링되거나 크기가 조정된 VPC 내에서 액세스할 수 있는 디렉터리의 엘라스틱 네트워크 인터페이스에 연결합니다](#). AWS 디렉터리로 들어오는 불필요한 트래픽을 차단하고 필요한 트래픽을 허용하도록 보안 그룹을 구성합니다.

디렉터리 보안 그룹 수정

디렉터리의 보안 그룹에 대해 보안을 수정하고 싶으면 수정할 수 있습니다. 단, 보안 그룹 필터링이 어떻게 작동하는지 완전히 이해하는 경우에만 이렇게 변경하세요. 자세한 내용은 Amazon EC2 사용 설명서의 [Linux 인스턴스용 Amazon EC2 보안 그룹](#)을 참조하세요. 잘못 변경하면 의도한 컴퓨터 및 인스턴스와의 통신이 끊길 수 있습니다. AWS 디렉터리에 포트를 추가로 열려고 하면 디렉터리 보안이 저하되므로 사용하지 않는 것이 좋습니다. [AWS 공동 책임 모델](#)을 자세히 검토하세요.

Warning

디렉터리의 보안 그룹을 사용자가 생성한 다른 EC2 인스턴스에 연결하는 것은 기술적으로 가능합니다. 하지만 이 AWS 방법을 사용하지 않는 것이 좋습니다. AWS 관리 디렉터리의 기능 또는 보안 요구 사항을 해결하기 위해 사전 공지 없이 보안 그룹을 수정해야 할 이유가 있을 수 있습니다. 그러한 변경은 디렉터리 보안 그룹과 연결된 모든 인스턴스에 영향을 미치며, 연결된 인스턴스의 작동이 중단될 수 있습니다. 또한 디렉터리 보안 그룹을 EC2 인스턴스와 연결하면 EC2 인스턴스에 잠재적 보안 위험이 생길 수 있습니다.

AD Connector를 사용할 때 온프레미스 사이트 및 서브넷을 올바르게 구성

온프레미스 네트워크에서 Microsoft Active Directory 사이트가 정의되어 있는 경우에는 AD Connector가 상주하는 VPC의 서브넷이 Microsoft Active Directory 사이트에 정의되어 있도록 하고 VPC의 서브넷과 다른 사이트의 서브넷 간에 충돌이 존재하지 않도록 해야 합니다.

도메인 컨트롤러를 검색하기 위해 AD Connector는 서브넷 IP 주소 범위가 AD Connector를 포함하는 VPC의 범위와 근접한 Microsoft Active Directory 사이트를 사용합니다. 사이트에서 서브넷이 VPC와 동일한 IP 주소 범위를 가지고 있는 경우에는 AD Connector가 리전과 물리적으로 근접하지 않을 수 있는 해당 사이트에서 도메인 컨트롤러를 검색합니다.

AWS 애플리케이션의 사용자 이름 제한을 이해하십시오.

AWS Directory Service 사용자 이름 구성에 사용할 수 있는 대부분의 문자 형식을 지원합니다. 그러나 Amazon WorkMail, WorkSpaces WorkDocs Amazon 또는 Amazon과 같은 AWS 애플리케이션에 로그인하는 데 사용되는 사용자 이름에는 문자 제한이 적용됩니다. QuickSight 이러한 제한 때문에 다음 문자는 사용할 수 없습니다.

- 공백
- 멀티바이트 문자
- !"#%&'()*+,-/;<=>?@[]^_{}~

Note

@ 기호는 UPN 접미사 앞에서만 허용됩니다.

애플리케이션 프로그래밍

애플리케이션을 프로그래밍하기 전에 다음 사항을 고려하세요.

프로덕션 단계로 넘어가기 전에 로드 테스트 실시

프로덕션 워크로드를 대표하는 애플리케이션 및 요청에 대해 랩 테스트를 실시하여 디렉터리 규모가 애플리케이션 로드와 맞게 조정되는지 확인해야 합니다. 용량이 더 필요한 경우, AD Connector 디렉터리 여러 개에 로드를 분산하세요.

디렉터리 사용

여기에는 디렉터리를 사용할 때 고려해야 할 몇 가지 제안이 나와 있습니다.

정기적으로 Admin 보안 인증 정보 교체

AD Connector 서비스 계정 Admin 암호를 정기적으로 변경하고, 암호가 기존 Active Directory 암호 정책과 일관되는지 확인하세요. 서비스 계정 암호를 변경하는 방법에 대한 지침은 [AWS Directory Service에서 AD Connector 서비스 계정 자격 증명을 업데이트](#) 단원을 참조하세요.

각 도메인에 고유한 AD Connector 사용

AD Connector와 온프레미스 AD 도메인은 1대1 관계를 가집니다. 따라서 AD 포리스트의 하위 도메인을 포함하여 인증 받으려는 각 온프레미스 도메인에서 고유 AD Connector를 생성해야 합니다. 생성된 각각의 AD Connector는 동일한 디렉터리에 연결이 되더라도 서로 다른 서비스 계정을 사용해야 합니다.

호환성 점검

AD Connector를 사용할 때는 온-프레미스 디렉터리가 AWS Directory Service s와 호환되고 계속 호환되는지 확인해야 합니다. 책임 사항에 대한 자세한 내용은 [공동 책임 모델](#)을 참조하세요.

AD Connector 할당량

다음은 AD Connector의 기본 할당량입니다. 별도로 명시되지 않는 한 각 할당량은 리전별입니다.

AD Connector 할당량

리소스	기본 할당량
AD Connector 디렉터리	10
디렉터리당 등록된 인증 기관(CA) 인증서의 최대 수	5

AD Connector의 애플리케이션 호환성 정책

AWS Directory Service for Microsoft Active Directory([AWS 매니지드 마이크로소프트 AD](#))의 대안으로, AD Connector는 AWS에서 만든 애플리케이션 및 서비스에만 사용할 수 있는 Active Directory 프록시입니다. 지정된 Active Directory 도메인을 사용하도록 프록시를 구성합니다. 애플리케이션에서 Active Directory의 사용자 또는 그룹을 검색할 때 AD Connector에서는 디렉터리에 요청을 위임합니다. 이와 마찬가지로 사용자가 애플리케이션에 로그인하면 AD Connector에서는 디렉터리에 인증 요청을 위임합니다. AD Connector와 연동되는 타사 애플리케이션은 없습니다.

호환되는 AWS 애플리케이션 및 서비스는 다음과 같습니다.

- Amazon Chime - 세부 지침은 [Active Directory 연결](#)을 참조하세요.
- Amazon Connect - 자세한 내용은 [How Amazon Connect works](#)를 참조하세요.
- Windows 또는 Linux용 Amazon EC2 — Amazon EC2 Windows 또는 Linux의 원활한 Active Directory 도메인 조인 기능을 사용하여 자체 관리형 Active Directory (온프레미스) 에 인스턴스를 조인할 수 있습니다. 조인되면 해당 인스턴스는 Active Directory와 직접 통신하고 AD Connector를 우회합니다. 자세히 알아보려면 [Amazon EC2 인스턴스를 다음 인스턴스에 연결하세요. Active Directory](#)의 내용을 참조하세요.
- AWS Management Console – AD Connector를 사용하면 SAML 인프라를 설정하지 않고도 Active Directory 보안 인증을 통해 AWS Management Console 사용자를 인증할 수 있습니다. 자세히 알아보려면 [AD 보안 인증을 사용한 AWS Management Console 액세스 활성화](#)의 내용을 참조하세요.
- Amazon QuickSight - 자세한 내용은 [Amazon QuickSight 엔터프라이즈 에디션의 사용자 계정 관리를 참조하십시오.](#)
- AWS IAM Identity Center - 세부 지침은 [IAM ID 센터를 온프레미스 Active Directory에 연결](#)을 참조하세요.
- AWS Transfer Family - 세부 지침은 [Microsoft Active Directory용 AWS Directory Service 사용](#)을 참조하세요.
- AWS - 세부 지침은 [클라이언트 인증 및 권한 부여](#)를 참조하세요.
- Amazon WorkDocs - 자세한 지침은 [AD Connector를 사용하여 온프레미스 디렉터리에 연결](#)을 참조하십시오.
- Amazon WorkMail - 자세한 지침은 [Amazon을 기존 WorkMail 디렉터리와 통합 \(표준 설정\)](#)을 참조하십시오.
- WorkSpaces - 자세한 지침은 [AD Connector를 Workspace 사용하여 실행](#)을 참조하십시오.

Note

Amazon RDS는 AWS Managed Microsoft AD와만 호환되며 AD Connector와는 호환되지 않습니다. 자세한 내용은 [AWS Directory Service FAQ](#) 페이지의 AWS 관리형 Microsoft AD 섹션을 참조하십시오.

문제 해결 AD Connector

다음은 AD Connector를 만들거나 사용할 때 발생할 수 있는 몇 가지 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

주제

- [생성 문제](#)
- [연결 문제](#)
- [인증 문제](#)
- [유지 관리 문제](#)
- [AD Connector를 삭제할 수 없는 경우](#)

생성 문제

다음은 AD Connector의 일반적인 생성 문제입니다.

- [디렉터리를 생성할 때 "AZ Constrained" 오류 메시지가 표시됩니다.](#)
- [AD Connector를 만들려고 할 때 "연결 문제가 감지되었습니다." 오류 메시지가 나타납니다.](#)

디렉터리를 생성할 때 "AZ Constrained" 오류 메시지가 표시됩니다.

2012년 이전에 생성된 일부 AWS 계정은 디렉터리를 지원하지 AWS Directory Service 앵는 미국 동부 (버지니아 북부), 미국 서부 (캘리포니아 북부) 또는 아시아 태평양 (도쿄) 지역의 가용 영역에 액세스할 수 있습니다. 를 생성할 때 이와 같은 오류가 발생하면 다른 Active Directory 가용 영역에 있는 서브넷을 선택하고 디렉터리를 다시 생성해 보십시오.

AD Connector를 만들려고 할 때 "연결 문제가 감지되었습니다." 오류 메시지가 나타납니다.

AD 커넥터를 만들려고 할 때 "연결 문제가 발견됨" 오류가 표시되면 포트 가용성 또는 AD Connector 암호의 복잡성 때문일 수 있습니다. AD 커넥터의 연결을 테스트하여 다음 포트를 사용할 수 있는지 확인할 수 있습니다.

- 53(DNS)
- 88(Kerberos)
- 389(LDAP)

연결을 테스트하려면 을 참조하십시오 [AD 커넥터 테스트](#). AD 커넥터의 IP 주소가 연결된 두 서브넷에 연결된 인스턴스에서 연결 테스트를 수행해야 합니다.

연결 테스트에 성공하고 인스턴스가 도메인에 가입하면 AD 커넥터의 비밀번호를 확인하십시오. AD Connector는 AWS 암호 복잡성 요구 사항을 충족해야 합니다. 자세한 내용은 의 서비스 계정을 참조하십시오 [AD Connector 사전 조건](#).

AD Connector가 이러한 요구 사항을 충족하지 않는 경우 이러한 요구 사항을 준수하는 암호로 AD Connector를 다시 만드십시오.

연결 문제

다음은 AD Connector의 일반적인 연결 문제입니다.

- [내 온프레미스 디렉터리에 연결할 때 "Connectivity issues detected" 오류가 표시되는 경우](#)
- [온프레미스 디렉터리에 연결할 때 "DNS unavailable" 오류가 표시되는 경우](#)
- [내 온프레미스 디렉터리에 연결할 때 "SRV record" 오류가 표시되는 경우](#)

내 온프레미스 디렉터리에 연결할 때 "Connectivity issues detected" 오류가 표시되는 경우

온프레미스 디렉터리에 연결할 때 다음과 비슷한 오류 메시지가 표시됩니다.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
Kerberos/authentication unavailable (TCP port 88) for IP: <IP address> Please ensure
that the listed ports are available and retry the operation.
```

AD Connector에서 다음 포트를 통해 TCP 및 UDP를 경유하여 온프레미스 도메인 컨트롤러와 통신할 수 있어야 합니다. 보안 그룹 및 온프레미스 방화벽에서 이러한 포트를 통한 TCP 및 UDP 통신을 허용하는지 확인합니다. 자세한 정보는 [AD Connector 사전 조건](#)을 참조하세요.

- 88(Kerberos)
- 389(LDAP)

필요에 따라 추가 TCP/UDP 포트가 필요할 수 있습니다. 이러한 포트 중 일부에 대해서는 다음 목록을 참조하십시오. 에서 사용하는 포트에 대한 자세한 내용은 Microsoft 설명서의 [Active Directory도메인 및 트러스트용 방화벽을 구성하는 방법을](#) 참조하십시오. Active Directory

- 135 (RPC 엔드포인트 매퍼)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

온프레미스 디렉터리에 연결할 때 "DNS unavailable" 오류가 표시되는 경우

온프레미스 디렉터리에 연결할 때 다음과 비슷한 오류 메시지가 표시됩니다.

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector에서 포트 53을 통해 TCP 및 UDP를 경유하여 온프레미스 DNS 서버와 통신할 수 있어야 합니다. 보안 그룹 및 온프레미스 방화벽에서 이 포트를 통한 TCP 및 UDP 통신을 허용하는지 확인합니다. 자세한 정보는 [AD Connector 사전 조건](#)을 참조하세요.

내 온프레미스 디렉터리에 연결할 때 "SRV record" 오류가 표시되는 경우

온프레미스 디렉터리에 연결할 때 다음 중 하나 이상과 비슷한 오류 메시지가 표시됩니다.

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos does not exist for IP: <DNS IP address>
```

AD Connector는 디렉터리에 연결할 때 `_ldap._tcp.<DnsDomainName>` 및 `_kerberos._tcp.<DnsDomainName>` SRV 레코드를 가져와야 합니다. 서비스에서 디렉터리에 연결할 때 지정한 DNS 서버로부터 이러한 레코드를 가져올 수 없는 경우에 이 오류가 표시됩니다. 이러한 SRV 레코드에 대한 자세한 내용은 [SRV record requirements](#)을 참조하세요.

인증 문제

AD Connector와 관련된 몇 가지 일반적인 인증 문제는 다음과 같습니다.

- [스마트 카드로 로그인하려고 Amazon WorkSpaces 하면 '인증서 유효성 검증에 실패했습니다' 오류 메시지가 나타납니다.](#)
- [AD Connector에서 사용되는 서비스 계정이 인증을 시도할 때 "Invalid Credentials" 오류가 표시되는 경우](#)
- [AWS 애플리케이션을 사용하여 사용자 또는 그룹을 검색할 때 "인증할 수 없음" 오류 메시지가 나타납니다.](#)

- [AD Connector 서비스 계정을 업데이트하려고 하면 디렉터리 자격 증명에 대한 오류 메시지가 나타납니다.](#)
- [일부 사용자들이 내 디렉터리를 통해 인증을 할 수 없는 경우](#)

스마트 카드로 로그인하려고 Amazon WorkSpaces 하면 '인증서 유효성 검증에 실패했습니다' 오류 메시지가 나타납니다.

스마트 WorkSpaces 카드로 로그인하려고 하면 다음과 비슷한 오류 메시지가 나타납니다.

ERROR: Certificate Validation failed. Please try again by restarting your browser or application and make sure you select the correct certificate.

스마트 카드의 인증서가 인증서를 사용하는 클라이언트에 제대로 저장되지 않은 경우 오류가 발생합니다. AD Connector 및 스마트 카드 요구 사항에 대한 자세한 내용은 [필수 조건](#)을 참조하십시오.

다음 절차를 사용하여 사용자의 인증서 저장소에 인증서를 저장하는 스마트 카드의 기능 문제를 해결하십시오.

1. 인증서에 액세스하는 데 문제가 있는 장치에서 Microsoft Management Console (MMC)에 액세스합니다.

Important

진행하기 전에 스마트 카드 인증서의 사본을 만드십시오.

2. MMC의 인증서 저장소로 이동합니다. 인증서 저장소에서 사용자의 스마트 카드 인증서를 삭제합니다. MMC의 인증서 저장소를 보는 방법에 대한 자세한 내용은 설명서의 [방법: MMC 스냅인을 사용하여 인증서 보기를](#) 참조하십시오. Microsoft
3. 스마트 카드를 제거합니다.
4. 사용자의 인증서 저장소에 있는 스마트 카드 인증서를 다시 채울 수 있도록 스마트 카드를 다시 삽입합니다.

Warning

스마트 카드가 사용자 저장소에 인증서를 다시 채우지 않는 경우 스마트 카드 인증에 사용할 수 없습니다. WorkSpaces

AD 커넥터의 서비스 계정에는 다음이 있어야 합니다.

- my/spn서비스 원칙 이름에 추가됨
- LDAP 서비스를 위임받았습니다.

스마트 카드에 인증서를 다시 채운 후에는 온프레미스 도메인 컨트롤러를 검사하여 해당 도메인 컨트롤러가 주체 대체 이름에 대한 UPN (사용자 계정 이름) 매핑에서 차단되었는지 확인해야 합니다. 이 변경 사항에 대한 자세한 내용은 설명서에서 UPN [매핑의 주체 대체 이름을 비활성화하는 방법을 참조](#)하십시오. Microsoft

다음 절차를 사용하여 도메인 컨트롤러의 레지스트리 키를 확인하십시오.

1. 레지스트리 편집기에서 다음 하이브 키로 이동합니다.

HKEY_LOCAL_MACHINE\SYSTEM\ 서비스\ Kdc\ CurrentControlSet UseSubjectAltName

2. UseSubjectAltName선택. 값이 0으로 설정되어 있는지 확인합니다.

Note

온-프레미스 도메인 컨트롤러에서 레지스트리 키를 설정하면 AD Connector가 사용자를 찾을 수 없어 위와 같은 오류 메시지가 표시됩니다. Active Directory

CA (인증 기관) 인증서를 AD Connector 스마트 카드 인증서에 업로드해야 합니다. 인증서에는 OCSP 정보가 포함되어야 합니다. 다음은 CA에 대한 추가 요구 사항 목록입니다.

- 인증서는 도메인 컨트롤러의 신뢰할 수 있는 루트 기관, 인증 기관 서버 및 에 있어야 WorkSpaces 합니다.
- 오프라인 및 루트 CA 인증서에는 OSCP 정보가 포함되지 않습니다. 이러한 인증서에는 해지에 대한 정보가 들어 있습니다.
- 스마트 카드 인증에 타사 CA 인증서를 사용하는 경우 CA 및 중간 인증서를 Active Directory NAuth 저장소에 게시해야 합니다. 모든 도메인 컨트롤러, 인증 기관 서버 및 기타 서버의 신뢰할 수 있는 루트 기관에 설치해야 합니다. WorkSpaces
 - 다음 명령을 사용하여 인증서를 Active Directory NTAAuth 저장소에 게시할 수 있습니다.

```
certutil -dspublish -f Third_Party_CA.cer NTAAuthCA
```

인증서를 NTAAuth 스토어에 게시하는 방법에 대한 자세한 내용은 공용 액세스 카드를 사용하여 [Access Amazon의 엔터프라이즈 NTAAuth 스토어로 발급 CA 인증서 가져오기](#) 설치 WorkSpaces 가이드를 참조하십시오.

다음 절차에 따라 OCSP에서 사용자 인증서 또는 CA 체인 인증서를 확인했는지 확인할 수 있습니다.

1. C: 드라이브와 같은 로컬 컴퓨터의 위치로 스마트 카드 인증서를 내보냅니다.
2. 명령줄 프롬프트를 열고 내보낸 스마트 카드 인증서가 저장된 위치를 탐색합니다.
3. 다음 명령을 입력합니다.

```
certutil -URL Certificate_name.cer
```

4. 명령 다음에 팝업 창이 나타나야 합니다. 오른쪽 모서리에서 OCSP 옵션을 선택하고 검색을 선택합니다. 상태가 확인된 상태로 돌아와야 합니다.

[certutil 명령에 대한 자세한 내용은 설명서의 certutil을 참조하십시오.](#) Microsoft

AD Connector에서 사용되는 서비스 계정이 인증을 시도할 때 "Invalid Credentials" 오류가 표시되는 경우

도메인 컨트롤러 상의 하드 드라이브에 공간이 부족할 경우 이러한 오류가 발생할 수 있습니다. 도메인 컨트롤러의 하드 드라이브가 가득 차지 않았는지 확인합니다.

AWS 애플리케이션을 사용하여 사용자 또는 그룹을 검색할 때 “인증할 수 없음” 오류 메시지가 나타납니다.

AD Connector 상태가 활성 상태인 경우에도 Amazon WorkSpaces QuickSight 등의 AWS 애플리케이션을 사용하는 동안 사용자를 검색할 때 오류가 발생할 수 있습니다. 보안 인증이 만료되면 AD Connector가 Active Directory의 객체에 대한 쿼리를 완료하지 못할 수 있습니다. 에 제공된 순서에 따라 서비스 계정의 비밀번호를 업데이트하십시오 [Amazon EC2 인스턴스에 대한 원활한 도메인 조인이 작동함을 멈춥니다.](#)

AD Connector 서비스 계정을 업데이트하려고 하면 디렉터리 자격 증명에 대한 오류 메시지가 나타납니다.

AD Connector 서비스 계정을 업데이트하려고 할 때 다음 중 하나 이상과 비슷한 오류 메시지가 나타납니다.

```
Message:An Error Has Occurred
```

Your directory needs a credential update. Please update the directory credentials.

An Error Has Occurred

Your directory needs a credential update. Please update the directory credentials following Update your AD Connector Service Account Credentials

Message:

An Error Has Occurred

Your request has a problem. Please see the following details.

There was an error with the service account/password combination

시간 동기화 및 Kerberos에 문제가 있을 수 있습니다. AD Connector는 에 Kerberos 인증 요청을 보냅니다. Active Directory 이러한 요청은 시간에 민감하며 요청이 지연되면 실패합니다. 이 문제를 해결하려면 설명서의 [권장 사항 - 신뢰할 수 있는 시간 소스로 루트 PDC를 구성하고 시간 왜곡이 확산되지 않도록](#) 하기 항목을 참조하십시오. Microsoft 시간 서비스 및 동기화에 대한 자세한 내용은 아래를 참조하십시오.

- [Windows시간 서비스 작동 방식](#)
- [컴퓨터 시계 동기화의 최대 허용 오차](#)
- [Windows시간 서비스 도구 및 설정](#)

일부 사용자들이 내 디렉터리를 통해 인증을 할 수 없는 경우

사용자 계정에서 Kerberos 사전 인증이 활성화되어 있어야 합니다. 이것이 새 사용자 계정에 대한 기본 설정이며 이를 변경해서는 안 됩니다. 이 설정에 대한 자세한 내용은 [사전 인증](#) Microsoft TechNet 쉼표를 참조하십시오.

유지 관리 문제

다음은 AD Connector의 일반적인 유지 관리 문제입니다.

- 디렉터리가 "Requested" 상태에 멈춰있는 경우
- Amazon EC2 인스턴스에 대한 원활한 도메인 조인이 작동을 멈춥니다.

디렉터리가 "Requested" 상태에 멈춰있는 경우

"Requested" 상태에 5분 이상 멈춰있는 디렉터리가 있으면 이를 삭제하고 다시 생성해보세요. 문제가 지속될 경우 [AWS Support](#)에 문의하세요.

Amazon EC2 인스턴스에 대한 원활한 도메인 조인이 작동을 멈췄습니다.

AD Connector가 활성 상태인데 EC2 인스턴스의 원활한 도메인 조인이 잘 작동하다가 멈췄다면 AD Connector 서비스 계정의 자격 증명이 만료되었을 수 있습니다. 자격 증명이 만료되면 AD Connector에서 컴퓨터 개체를 만들지 못할 수 Active Directory 있습니다.

이 문제를 해결하려면 서비스 계정 암호를 다음 순서로 업데이트하여 암호가 서로 일치하게 하세요.

1. 에 있는 서비스 계정의 암호를 업데이트하십시오. Active Directory
2. 에서 AD Connector의 서비스 계정 암호를 업데이트하십시오 AWS Directory Service. 자세한 정보는 [AWS Directory Service에서 AD Connector 서비스 계정 자격 증명을 업데이트](#)를 참조하세요.

Important

에서만 암호를 업데이트하면 암호 변경 내용이 기존 온-프레미스로 푸시되지 AWS Directory Service Active Directory 않으므로 이전 절차에 표시된 순서대로 변경하는 것이 중요합니다.

AD Connector를 삭제할 수 없는 경우

AD Connector가 작동 불가능 상태로 전환되면 도메인 컨트롤러에 더 이상 액세스할 수 없습니다. AD Connector에 연결된 애플리케이션이 있는 경우 해당 애플리케이션 중 하나가 여전히 디렉터리를 사용하고 있을 수 있으므로 AD Connector의 삭제를 차단합니다. AD Connector를 삭제하기 위해 비활성화해야 하는 응용 프로그램 목록은 을 참조하십시오 [AD Connector 삭제](#). 그래도 AD Connector를 삭제할 수 없는 경우 를 통해 도움을 요청할 수 [AWS Support](#) 있습니다.

Simple AD

Simple AD는 Samba 4 Active Directory 호환 서버를 기반으로 하는 독립 관리형 디렉터리입니다. 두 가지 크기를 사용할 수 있습니다.

- 소형 - 최대 500명의 사용자(사용자, 그룹 및 컴퓨터를 포함한 약 2,000개의 객체)를 지원합니다.
- 대형 - 최대 5,000명의 사용자(사용자, 그룹 및 컴퓨터를 포함한 약 20,000개의 객체)를 지원합니다.

Simple AD는 사용자 계정 및 그룹 멤버십을 관리하고, 그룹 정책을 생성 및 적용하고, Amazon EC2 인스턴스에 안전하게 연결하고, Kerberos 기반 싱글 사인온 (SSO) 을 제공하는 기능을 포함하여 AWS 관리형 Microsoft AD에서 제공하는 기능 중 일부를 제공합니다. 하지만 Simple AD는 다중 요소 인증 (MFA), 다른 도메인과의 신뢰 관계, Active Directory 관리 센터, 지원, Active Directory 휴지통 PowerShell , 그룹 관리 서비스 계정, POSIX 및 Microsoft 응용 프로그램의 스키마 확장과 같은 기능을 지원하지 않는다는 점에 유의하십시오.

Simple AD는 다음과 같은 많은 이점을 제공합니다.

- Simple AD를 사용하면 [Linux 및 Windows를 실행하는 Amazon EC2 인스턴스를 더 쉽게 관리하고](#) AWS 클라우드에 Windows 애플리케이션을 배포할 수 있습니다.
- Microsoft Active Directory 지원을 요구하는 기존의 많은 애플리케이션과 도구를 Simple AD에서 사용할 수 있습니다.
- Simple AD의 사용자 계정을 사용하면 Amazon WorkDocs 또는 Amazon과 WorkSpaces 같은 AWS 애플리케이션에 액세스할 수 WorkMail 있습니다.
- 에 대한 IAM 역할 기반 액세스를 통해 AWS 리소스를 관리할 수 있습니다. AWS Management Console
- 매일 자동 스냅샷을 생성하면 복구가 가능합니다. point-in-time

Simple AD는 다음을 지원하지 않습니다.

- 아마존 AppStream 2.0
- Amazon Chime
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- AWS IAM Identity Center
- 다른 도메인과의 신뢰 관계

- Active Directory Administrative Center
- PowerShell
- Active Directory 휴지통
- 그룹 관리형 서비스 계정
- POSIX 및 Microsoft 애플리케이션용 스키마 확장

이 섹션의 주제를 통해 자체 Simple AD를 생성하는 방법을 알아 보세요.

주제

- [Simple AD로 시작하기](#)
- [Simple AD 관리 방법](#)
- [튜토리얼: 단순 AD 만들기 Active Directory](#)
- [Simple AD 모범 사례](#)
- [Simple AD 할당량](#)
- [Simple AD에 대한 애플리케이션 호환성 정책](#)
- [Simple AD 문제 해결](#)

Simple AD로 시작하기

Simple AD는 클라우드에 완전히 관리되는 Samba 기반 디렉터리를 생성합니다. AWS Simple AD로 디렉터리를 만들면 사용자를 대신하여 두 개의 도메인 컨트롤러와 DNS 서버가 AWS Directory Service 생성됩니다. 도메인 컨트롤러는 Amazon VPC의 여러 서브넷에 생성됩니다. 이러한 중복성은 장애가 발생하더라도 디렉터리에 계속 액세스할 수 있도록 합니다.


주제

- [간단한 AD 사전 조건](#)
- [나만의 Simple AD 만들기 Active Directory](#)
- [Simple AD로 생성되는 콘텐츠 Active Directory](#)
- [Simple AD용 DNS 구성](#)

간단한 AD 사전 조건

Simple AD를 생성하려면 다음과 Active Directory 같은 기능을 갖춘 Amazon VPC가 필요합니다.

- VPC는 기본 하드웨어 테넌시를 가지고 있어야 합니다.
- VPC를 다음 [VPC 엔드포인트](#)로 구성해서는 안 됩니다.
 - *.amazonaws.com에 대한 DNS 조건부 재정의의 포함하는 [Route53 VPC 엔드포인트](#)는 퍼블릭 IP 주소가 아닌 주소로 확인됩니다. AWS
 - [CloudWatch VPC 엔드포인트](#)
 - [Systems Manager VPC 엔드포인트](#)
 - [보안 토큰 서비스 VPC 엔드포인트](#)
- 서로 다른 두 가용 영역에 있는 최소 두 개의 서브넷. 서브넷은 동일한 클래스 없는 도메인 간 라우팅 (CIDR) 범위에 있어야 합니다. 디렉터리의 VPC를 확장하거나 크기를 변경하고 싶다면, 확장된 VPC CIDR 범위에 맞는 도메인 컨트롤러 서브넷 2개를 선택해야 합니다. Simple AD를 만들면 사용자를 대신하여 두 개의 도메인 컨트롤러와 DNS 서버를 AWS Directory Service 생성합니다.
- CIDR 범위에 대한 자세한 내용은 Amazon VPC [사용 설명서의 VPC 및 서브넷의 IP 주소 지정](#)을 참조하십시오.
- Simple AD에서 LDAPS 지원이 필요한 경우 포트 389에 연결된 Network Load Balancer를 사용하여 구성하는 것이 좋습니다. 이 모델에서는 LDAPS 연결 시 강력한 인증서를 사용할 뿐만 아니라 단일 NLB IP 주소를 통해 LDAPS에 간편하게 액세스하고 NLB를 통해 자동 장애 조치를 구현할 수 있습니다. Simple AD는 포트 636에서 자체 서명된 인증서 사용을 지원하지 않습니다. Simple AD를 사용하여 LDAPS를 구성하는 방법에 대한 자세한 내용은 AWS 보안 블로그의 [Simple AD용 LDAPS 엔드포인트 구성 방법](#)을 참조하세요.
- 디렉터리에서 다음 암호화 유형을 활성화해야 합니다.
 - RC4_HMAC_MD5
 - AES128_HMAC_SHA1
 - AES256_HMAC_SHA1
 - 향후의 암호화 유형

 Note

위의 암호화 유형을 비활성화하면 RSAT(Remote Server Administration Tools)와 통신 문제를 초래하여 가용성이나 디렉터리에 영향을 끼칠 수 있습니다.

- 자세한 내용은 Amazon VPC 사용 설명서의 [Amazon VPC란 무엇인가요?](#)를 참조하세요.

AWS Directory Service 두 개의 VPC 구조를 사용합니다. 디렉터리를 구성하는 EC2 인스턴스는 AWS 계정 외부에서 실행되며 에서 관리합니다. AWSETH0 및 ETH1라는 2개의 어댑터가 있습니다. ETH0는 관리 어댑터로써 계정 외부에 위치합니다. ETH1는 계정 내부에서 생성됩니다.

디렉터리의 ETH0 네트워크에서 관리 IP 범위는 디렉터리를 배포할 경우 VPC와 충돌하지 않도록 보장하기 위해 프로그래밍 방식으로 선택합니다. 이 IP 범위는 다음 페어 중 하나일 수 있습니다(디렉터리가 2개의 서브넷에서 실행되기 때문에).

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

ETH1 CIDR의 첫 번째 옥텟을 확인하여 충돌을 방지합니다. 10으로 시작할 경우, 192.168.1.0/24 및 192.168.2.0/24 서브넷의 192.168.0.0/16 VPC를 선택합니다. 첫 번째 옥텟이 10 이외의 수일 경우, 10.0.1.0/24 및 10.0.2.0/24 서브넷의 10.0.0.0/16 VPC를 선택합니다.

선택 알고리즘은 VPC 상의 라우팅을 포함하지 않습니다. 따라서 이 시나리오에서 IP 라우팅 충돌 결과가 있을 수 없습니다.

나만의 Simple AD 만들기 Active Directory

새 Simple Active Directory AD를 만들려면 다음 단계를 수행하십시오. 이 절차를 시작하기 전에 [간단한 AD 사전 조건](#)에 나와 있는 선행 조건을 충족했는지 확인합니다.

Simple AD를 만들려면 Active Directory

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택한 후 디렉터리 설정을 선택합니다.
2. Select directory type(디렉터리 유형 선택) 페이지에서 Simple AD를 선택하고 다음을 선택합니다.
3. 디렉터리 정보 입력 페이지에서 다음 정보를 제공합니다.

디렉터리 크기

Small(스몰) 또는 Large(라지) 크기 옵션 중에서 선택합니다. 크기에 대한 자세한 내용은 [Simple AD](#) 단원을 참조하세요.

조직 이름

클라이언트 장치를 등록하는 데 사용할 디렉터리에 대한 고유한 조직 이름입니다.

이 필드는 시작 과정에서 디렉터리를 만드는 경우에만 사용할 수 WorkSpaces 있습니다.

디렉터리 DNS 이름

디렉터리를 위한 정규화된 이름(예: corp.example.com)입니다.

디렉터리 NetBIOS 이름

디렉터리의 짧은 이름(예: CORP)입니다.

관리자 암호

디렉터리 관리자의 암호입니다. 디렉터리 생성 프로세스에서는 사용자 이름 Administrator와 이 암호를 사용하여 관리자 계정을 생성합니다.

디렉터리 관리자 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 또한 다음 네 범주 중 세 개에 해당하는 문자를 1자 이상 포함해야 합니다.

- 소문자(a-z)
- 대문자(A-Z)
- 숫자(0-9)
- 영숫자 외의 특수 문자(~!@#\$\$%^&* _-+=`\|(){}[]:;'"<>.,./?)

[Confirm password]

관리자 암호를 다시 입력합니다.

디렉터리 설명

디렉터리에 대한 선택적 설명을 입력합니다.

4. VPC 및 서브넷 선택 페이지에서 다음 정보를 제공한 후 다음을 선택합니다.

VPC

디렉터리에 대한 VPC입니다.

서브넷

도메인 컨트롤러에 대한 서브넷을 선택합니다. 두 서브넷이 서로 다른 가용 영역에 있어야 합니다.

5. 검토 및 생성 페이지에서 디렉터리 정보를 검토하고 필요한 사항을 변경합니다. 정보가 올바르면 디렉터리 생성을 선택합니다. 디렉터리를 생성하는 데 몇 분 정도 걸립니다. 생성이 완료되면 상태 값이 활성 상태로 변경됩니다.

Simple AD로 생성되는 콘텐츠 Active Directory

Simple AD를 Active Directory 사용하여 생성하는 경우 사용자를 대신하여 다음 작업을 AWS Directory Service 수행합니다.

- VPC 내에서 Samba 기반 디렉터리를 설정합니다.
- 사용자 이름 Administrator 과 지정된 암호를 사용하여 디렉터리 관리자 계정을 생성합니다. 이 계정을 사용하여 디렉터리를 관리할 수 있습니다.

Important

이 비밀번호는 반드시 저장해 두십시오. AWS Directory Service 이 암호는 저장되지 않으며 검색할 수 없습니다. 하지만 AWS Directory Service 콘솔에서 또는 [ResetUserPasswordAPI](#) 를 사용하여 비밀번호를 재설정할 수 있습니다.

- 디렉터리 컨트롤러에 대한 보안 그룹을 만듭니다.
- 도메인 관리 권한을 가진 AWSAdminD-**xxxxxxxx**라는 이름의 계정을 생성합니다. 이 계정은 디렉터리 스냅샷 생성 및 FSMO 역할 전송과 같은 디렉터리 유지 관리 작업을 위한 자동화된 작업을 수행하는 데 사용됩니다. AWS Directory Service 이 계정에 대한 자격 증명은 AWS Directory Service에서 안전하게 저장됩니다.
- ENI(탄력적 네트워크 인터페이스)를 자동으로 생성하여 각 도메인 컨트롤러에 연결합니다. 각 ENI는 AWS Directory Service VPC와 도메인 컨트롤러 간의 연결에 필수적이며 절대 삭제해서는 안 됩니다. “디렉터리 id에 대해AWS 생성된 네트워크 인터페이스”라는 AWS Directory Service 설명으로 사용하도록 예약된 모든 네트워크 인터페이스를 식별할 수 있습니다. 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [엘라스틱 네트워크 인터페이스](#)를 참조하십시오. AWS 관리형 Microsoft AD의 기본 DNS 서버는 클래스 없는 도메인 간 라우팅 (CIDR) +2에 있는 VPC DNS Active Directory 서버입니다. 자세한 내용은 Amazon VPC의 [Amazon DNS 서버](#) 사용 설명서를 참조하십시오.

Note

도메인 컨트롤러는 기본적으로 한 리전의 두 가용 영역에 배포되며 Amazon Virtual Private Cloud(VPC)에 연결됩니다. 백업은 하루에 한 번 자동으로 수행되며 Amazon Elastic Block Store(EBS) 볼륨이 암호화되어 저장된 데이터를 안전하게 보호합니다. 장애가 발생한 도메인 컨트롤러는 동일한 IP 주소를 사용하여 동일한 가용 영역에서 자동으로 교체되며, 최신 백업을 사용하여 전체 재해 복구를 수행할 수 있습니다.

Simple AD용 DNS 구성

Simple AD는 VPC에서 Amazon이 제공하는 DNS 서버의 IP 주소에 대한 DNS 요청을 Amazon VPC에 전달합니다. 이러한 DNS 서버는 Amazon Route 53 프라이빗 호스팅 영역에서 구성된 이름을 해석하게 됩니다. 이제, Simple AD로 온프레미스 컴퓨터를 지정하여 프라이빗 호스팅 영역에 대한 DNS 요청을 해석할 수 있게 되었습니다. Route 53에 대한 자세한 내용은 [Route 53이란 무엇입니까?](#)를 참조하세요.

Simple AD가 외부 DNS 쿼리에 응답하도록 하려면 VPC 밖에서 트래픽이 허용하도록 Simple AD를 포함한 VPC에 대한 네트워크 액세스 제어 목록(ACL)을 구성해야 합니다.

- Route 53 프라이빗 호스팅 영역을 사용하고 있지 않은 경우에는 퍼블릭 DNS 서버로 DNS 요청이 전달됩니다.
- VPC 외부에 있는 사용자 지정 DNS 서버를 사용 중일 때 프라이빗 DNS를 사용하려면 VPC 내의 EC2 인스턴스에서 사용자 지정 DNS 서버를 사용하도록 재구성해야 합니다. 자세한 내용은 [프라이빗 호스팅 영역 작업](#)을 참조하세요.
- VPC 내부에 있는 DNS 서버와 VPC 외부에 있는 사용자 지정 DNS 서버를 모두 사용하여 Simple AD에서 이름을 해석하고 싶은 경우에는 DHCP 옵션 세트를 이용하면 이것이 가능합니다. 세부적인 예제는 [본 기사](#)를 참조하세요.

Note

Simple AD 도메인에서 DNS 동적 업데이트가 지원되지 않습니다. 도메인에 조인된 인스턴스에서 DNS Manager를 사용해 디렉터리를 연결하는 방식으로 직접 변경을 수행할 수 있습니다.

Simple AD 관리 방법

이 단원에서는 Simple AD 환경을 운영 및 유지 관리하기 위한 모든 절차를 나열합니다.

주제

- [Simple AD에서 사용자 및 그룹 관리](#)
- [Simple AD 디렉터리 모니터링](#)
- [Amazon EC2 인스턴스를 Simple AD Active Directory에 조인합니다.](#)
- [Simple AD 디렉터리 관리](#)
- [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#)

- [AD 보안 인증을 사용한 AWS Management Console에 대한 액세스 활성화](#)

Simple AD에서 사용자 및 그룹 관리

사용자는 디렉터리에 액세스할 수 있는 개별 사용자 또는 개체를 나타냅니다. 그룹은 개별 사용자에게 권한을 적용할 필요 없이 사용자 그룹에 권한을 부여하거나 거부하는 데 매우 유용합니다. 사용자가 다른 조직으로 이동할 경우 해당 사용자를 다른 그룹으로 이동하면 새 조직에 필요한 권한이 사용자에게 자동으로 부여됩니다.

AWS Directory Service 디렉터리에서 사용자 및 그룹을 생성하려면 AWS Directory Service 디렉터리에 조인된 인스턴스(온프레미스 또는 EC2)에 연결하고, 사용자 및 그룹 생성 권한이 있는 사용자로 로그인해야 합니다. 또한 Active Directory 사용자 및 컴퓨터 스냅인을 사용하여 사용자 및 그룹을 추가할 수 있도록 EC2 인스턴스에 Active Directory 도구도 설치해야 합니다. EC2 인스턴스를 설정하고 필요한 도구를 설치하는 방법에 대한 자세한 정보는 [Amazon EC2 인스턴스를 Simple AD Active Directory에 조인합니다](#) 섹션을 참조하세요.

Note

사용자 계정에서 Kerberos 사전 인증이 활성화되어 있어야 합니다. 이것이 새 사용자 계정에 대한 기본 설정이며 이를 변경해서는 안 됩니다. 이 설정에 대한 자세한 내용은 TechNet Microsoft의 [사전 인증](#)을 참조하십시오.

다음 항목에서는 사용자와 그룹을 생성하고 관리하는 방법을 설명합니다.

주제

- [Simple AD용 액티브 디렉터리 관리 도구 설치](#)
- [사용자 생성](#)
- [사용자 삭제](#)
- [사용자 암호 재설정](#)
- [그룹 만들기](#)
- [그룹에 사용자 추가](#)

Simple AD용 액티브 디렉터리 관리 도구 설치

Amazon EC2 Windows Server 인스턴스에서 Active Directory를 관리하려면 인스턴스에 Active Directory 도메인 서비스 및 Active Directory 경량 디렉터리 서비스 도구를 설치해야 합니다. 다음 절차를 사용하여 EC2 Windows Server 인스턴스에 이러한 도구를 설치할 수 있습니다.

필수 조건

이 절차를 시작하기 전에 다음을 완료하십시오.

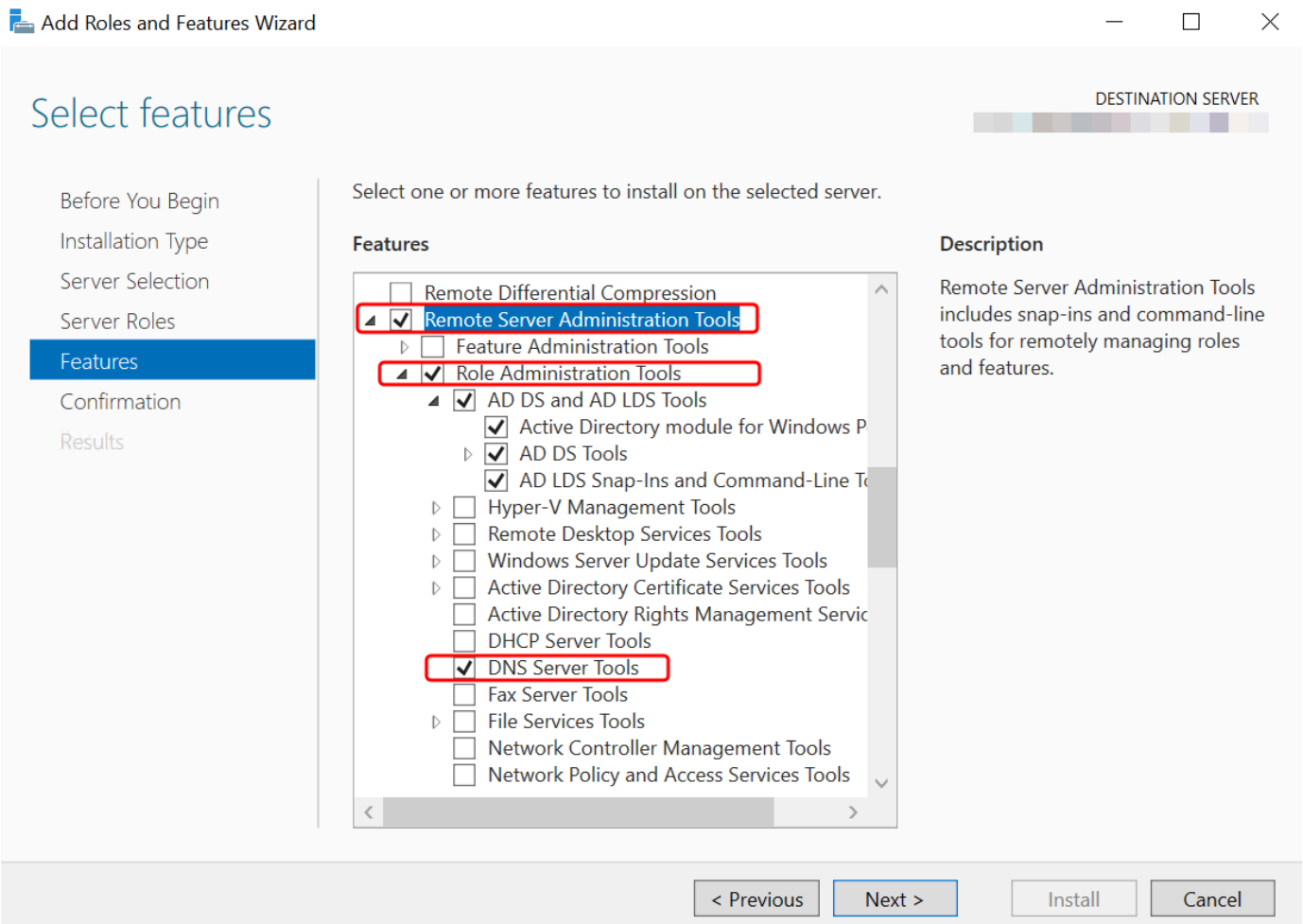
1. 간단한 AD 액티브 디렉터리 만들기 자세한 정보는 [나만의 Simple AD 만들기 Active Directory](#)을 참조하세요.
2. EC2 윈도우 서버 인스턴스를 시작하고 Simple AD Active Directory에 연결합니다. EC2 인스턴스에 사용자 및 그룹을 생성하려면 다음과 같은 정책이 필요합니다. **AWSSSMManagedInstanceCore** 및 **AmazonSSMDirectoryServiceAccess** 자세한 정보는 [Amazon EC2 윈도우 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.](#)을 참조하세요.
3. Active Directory 도메인 관리자의 자격 증명이 필요합니다. 이러한 자격 증명은 Simple AD가 생성될 때 생성되었습니다. 이 절차를 따랐다면 관리자 사용자 이름에는 NetBIOS 이름 () 이 포함됩니다. [나만의 Simple AD 만들기 Active Directory](#) **corp\administrator**

EC2 Windows Server 인스턴스에 액티브 디렉터리 관리 도구를 설치합니다.

EC2 Windows Server 인스턴스에 Active Directory 관리 도구를 설치하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. Amazon EC2 Console에서 Instances를 선택하고, Windows Server 인스턴스를 선택한 다음 Connect를 선택합니다.
3. 인스턴스에 연결 페이지에서 RDP 클라이언트를 선택합니다.
4. RDP 클라이언트 탭에서 원격 데스크톱 파일 다운로드를 선택한 다음 암호 가져오기를 선택하여 암호를 검색합니다.
5. Windows 암호 가져오기에서 프라이빗 키 파일 업로드를 선택합니다. Windows Server 인스턴스와 연결된.pem 프라이빗 키 파일을 선택합니다. 프라이빗 키 파일을 업로드한 후 암호 해독을 선택합니다.
6. Windows 보안 대화 상자에서 로그인할 Windows Server 컴퓨터의 로컬 관리자 자격 증명을 복사합니다. 사용자 이름은 다음 형식일 수 있습니다 **DNS-Name\administrator**. **NetBIOS-Name\administrator** 또는. 예를 들어, **corp\administrator** 이 절차를 따랐다면 사용자 이름이 [나만의 Simple AD 만들기 Active Directory](#) 됩니다.

7. Windows Server 인스턴스에 로그인한 후 [시작] 메뉴에서 [서버 관리자] 를 선택하여 [서버 관리자] 를 엽니다.
8. 서버 관리자 대시보드에서 역할 및 기능 추가를 선택합니다.
9. 역할 및 기능 추가 마법사에서 설치 유형을 선택하고 역할 기반 또는 기능 기반 설치를 선택한 후 다음을 선택합니다.
10. 서버 선택에서 로컬 서버가 선택되었는지 확인하고 왼쪽 탐색 창에서 기능을 선택합니다.
11. 기능 트리에서 원격 서버 관리 도구, 역할 관리 도구를 열고 AD DS 및 AD LDS 도구를 선택하고 엽니다. AD DS 및 AD LDS 도구를 선택하면 Active Directory 모듈 대상, AD DS 도구 Windows PowerShell, AD LDS 스냅인 및 명령줄 도구가 선택됩니다. 아래로 스크롤하여 DNS 서버 도구를 선택한 후 다음을 선택합니다.



12. 정보를 검토한 후 설치를 선택합니다. 기능 설치가 완료되면 관리 도구 폴더의 시작 메뉴에서 Active Directory 도메인 서비스와 Active Directory Lightweight Directory Services 도구를 사용할 수 있습니다.

EC2 Windows Server 인스턴스에 Active Directory 관리 도구를 설치하는 대체 방법

- Active Directory 관리 도구를 설치하는 또 다른 방법은 다음과 같습니다.
 - 를 사용하여 Active Directory 관리 도구를 설치하도록 선택할 수도 Windows PowerShell 있습니다. 예를 들어 를 사용하여 PowerShell 프롬프트에서 Active Directory 원격 관리 도구를 설치할 수 Install-WindowsFeature RSAT-ADDS 있습니다. 자세한 내용은 Microsoft 웹 [WindowsFeature사이트에 설치를](#) 참조하십시오.

사용자 생성

다음 절차를 사용하여 Simple AD 디렉터리에 가입된 EC2 인스턴스에서 사용자를 생성합니다. 사용자를 만들려면 먼저 [Active Directory 관리 도구 설치](#)의 절차를 완료해야 합니다.

Note

Simple AD를 사용할 때 "사용자가 첫 번째 로그인 시 암호를 변경하도록 강제" 옵션을 통해 Linux 인스턴스에서 사용자 계정을 생성한 경우, 사용자가 처음에는 kpasswd를 사용해 암호를 변경할 수 없습니다. 처음으로 암호를 변경하려면 도메인 관리자가 Microsoft Active Directory 관리 도구를 사용해 사용자 암호를 업데이트해야 합니다.

다음 방법 중 하나를 사용하여 사용자를 생성할 수 있습니다.

- Active Directory관리 도구
- Windows PowerShell

Active Directory관리 도구를 사용하여 사용자 만들기

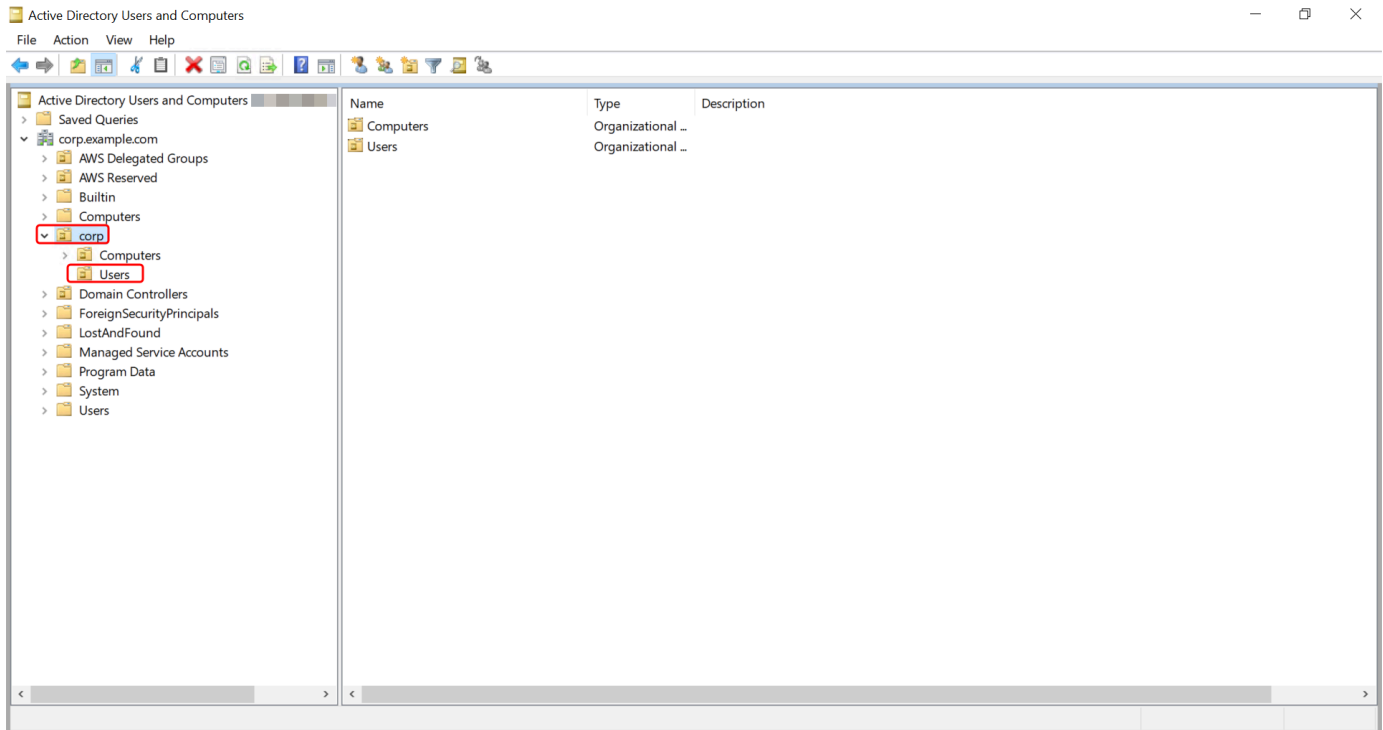
1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
2. Windows 시작 메뉴에서 Active Directory 사용자 및 컴퓨터 도구를 엽니다. Windows 관리 도구 폴더에 이 도구의 바로 가기가 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.


```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서 디렉터리의 NetBIOS 이름 OU에서 사용자를 저장할 OU (예:) 를 선택합니다. **corp\Users** 의 디렉터리에서 AWS사용되는 OU 구조에 대한 자세한 내용은 [을 참조하십시오.](#)
[AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#)



4. 작업 메뉴에서 새로 만들기를 클릭한 후 사용자를 선택하여 새 사용자 마법사를 엽니다.
5. 마법사의 첫 페이지에서 다음 필드에 값을 입력하고 다음을 선택합니다.
 - 이름
 - 성
 - 사용자 로그인 이름
6. 마법사의 두 번째 페이지에서 암호와 암호 확인에 임시 암호를 입력합니다. 다음 로그인할 때 반드시 암호 변경 옵션이 선택되어 있는지 확인합니다. 다른 옵션들 중 어떤 것도 선택해서는 안 됩니다. 다음을 선택합니다.
7. 마법사의 세 번째 페이지에서 새 사용자 정보가 올바른지 확인한 후 마침을 선택합니다. 새 사용자가 사용자 폴더에 나타납니다.

에서 사용자 생성 Windows PowerShell

1. Active Directory관리자로 Active Directory 도메인에 가입된 인스턴스에 연결합니다.
2. Windows PowerShell를 엽니다.
3. 다음 명령을 입력하여 사용자 이름을 **jane.doe** 생성하려는 사용자의 사용자 이름으로 대체합니다. 새 사용자의 비밀번호를 입력하라는 메시지가 표시됩니다. Windows PowerShell Active Directory암호 복잡성 요구 사항에 대한 자세한 내용은 [Microsoft설명서를](#) 참조하십시오. [New-ADUser 명령에 대한 자세한 내용은 설명서를 참조하십시오.](#) [Microsoft](#)

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString 'Password')
```

사용자 삭제

Simple AD 디렉터리에 조인된 EC2 Windows 인스턴스에서 사용자를 삭제하려면 다음 절차를 사용합니다.

다음 방법 중 하나를 사용하여 사용자를 삭제할 수 있습니다.

- Active Directory관리 도구
- Windows PowerShell

Active Directory관리 도구를 사용하여 사용자 삭제

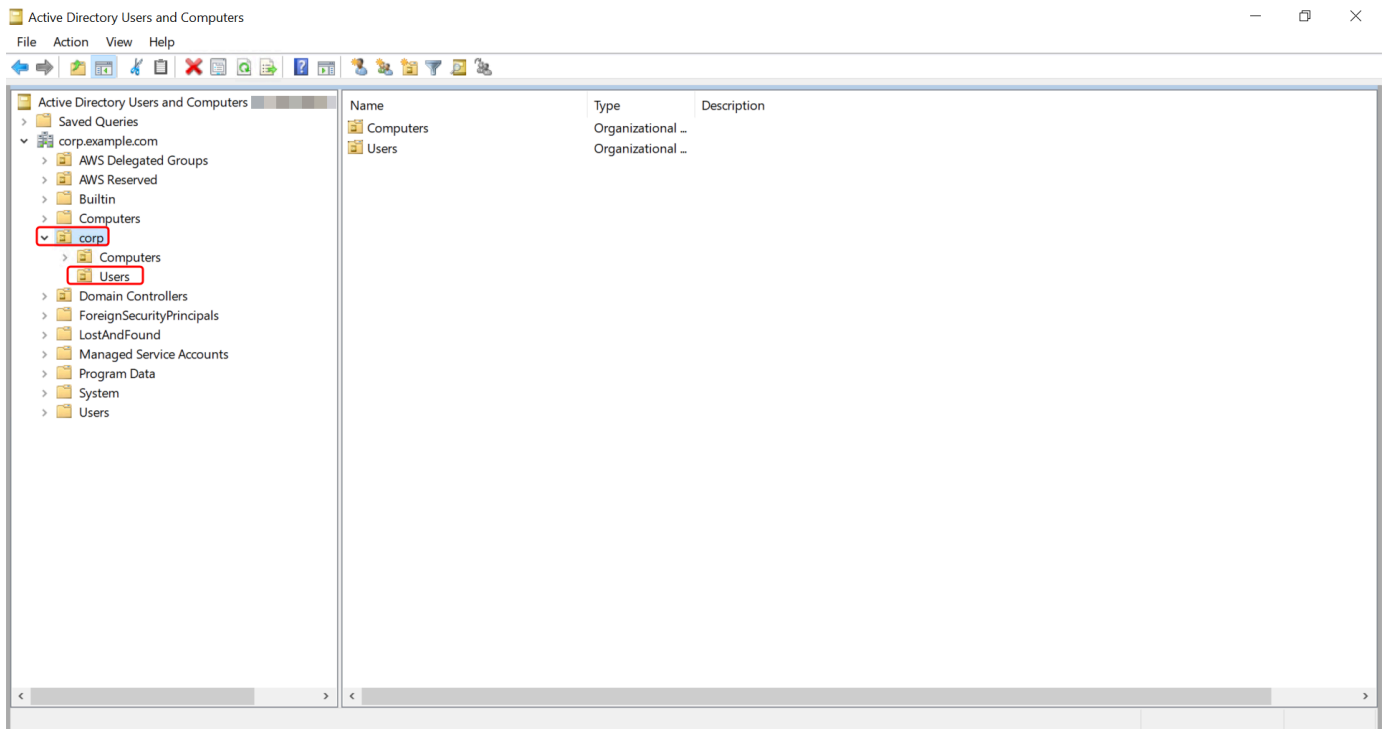
1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
2. Windows 시작 메뉴에서 Active Directory 사용자 및 컴퓨터 도구를 엽니다. Windows 관리 도구 폴더에 이 도구의 바로 가기가 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서 삭제하려는 사용자가 들어 있는 OU (예:**corp\Users**) 를 선택합니다.



4. 삭제하려는 사용자를 선택합니다. Action 메뉴에서 Delete를 선택합니다.
5. 사용자를 삭제할 것인지 확인하라는 대화 상자가 나타납니다. 사용자를 삭제하려면 예를 선택합니다. 그러면 선택한 사용자가 영구적으로 삭제됩니다.

에서 사용자 삭제 Windows PowerShell

1. Active Directory관리자로 Active Directory 도메인에 가입된 인스턴스에 연결합니다.
2. Windows PowerShell를 엽니다.
3. 다음 명령을 입력하여 사용자 이름을 **jane.doe** 삭제하려는 사용자의 사용자 이름으로 대체합니다. [Remove-ADUser 명령에 대한 자세한 내용은 설명서를 참조하십시오. Microsoft](#)

```
Remove-ADUser -Identity "jane.doe"
```

사용자 암호 재설정

사용자는 에 정의된 암호 정책을 준수해야 합니다Active Directory. 이 경우 Active Directory 관리자를 비롯한 사용자가 자신의 비밀번호를 잊어버릴 수 있어 문제가 발생할 수 있습니다. 이 경우 사용자가 Simple AD에 있는 AWS Directory Service 경우 를 사용하여 사용자 암호를 빠르게 재설정할 수 있습니다.

암호를 재설정하는 데 필요한 권한이 있는 사용자로 로그인해야 합니다. 권한에 대한 자세한 내용은 [AWS Directory Service 리소스에 대한 액세스 권한 관리 개요](#) 섹션을 참조하세요.

다음과 같은 경우를 제외하고 내 모든 사용자의 비밀번호를 재설정할 수 Active Directory 있습니다.

- OU (조직 구성 단위) 내 모든 사용자의 암호를 재설정할 수 있습니다. 이 암호는 OU (조직 구성 단위) 를 만들 때 사용한 NetBIOS 이름을 기반으로 합니다. Active Directory 예를 들어, 의 절차를 따랐다면 NetBIOS 이름은 CORP가 되고 재설정할 수 있는 사용자 암호는 Corp/Users OU의 구성원이 됩니다. [나만의 Simple AD 만들기 Active Directory](#)
- OU를 만들 때 사용한 NetBIOS 이름을 기반으로 하는 OU 외부 사용자의 암호는 재설정할 수 없습니다. Active Directory Simple AD의 OU 구조에 대한 자세한 내용은 을 참조하십시오 [Simple AD로 생성되는 콘텐츠 Active Directory](#).
- 두 도메인의 구성원인 사용자의 암호는 재설정할 수 없습니다. 또한 관리자 사용자를 제외하고 도메인 관리자 또는 Enterprise Admins 그룹에 속한 사용자의 비밀번호는 재설정할 수 없습니다.

다음 방법 중 하나를 사용하여 사용자 암호를 재설정할 수 있습니다.

- AWS Management Console
- AWS CLI
- Windows PowerShell

에서 사용자 암호를 재설정합니다. AWS Management Console

1. [AWS Directory Service 콘솔](#) 탐색 창의 디렉토리에서 디렉토리를 선택한 다음 목록에서 사용자 암호를 재설정하려는 디렉토리를 선택합니다. Active DirectoryActive Directory
2. Directory details(디렉터리 세부 정보) 페이지에서 Actions(작업), Reset user password(사용자 암호 재설정)를 차례로 선택합니다.
3. 사용자 암호 재설정 대화 상자의 사용자 이름에 암호를 변경해야 하는 사용자의 사용자 이름을 입력합니다.
4. 새 암호와 암호 확인에 암호를 입력한 후 암호 재설정을 선택합니다.

에서 사용자 암호를 재설정하세요. AWS CLI

1. 를 설치하려면 [의 최신 버전 설치 또는 업데이트를](#) 참조하십시오 AWS CLI. AWS CLI
2. 를 엽니다 AWS CLI.

- 다음 명령을 입력하고 디렉터리 ID `jane.doe`, 사용자 이름 및 비밀번호를 디렉터리 ID 및 원하는 자격 `P@ssw0rd` 증명으로 바꿉니다. Active Directory 자세한 내용은 AWS CLI 명령 참조를 참조하십시오 [reset-user-password](#).

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

에서 사용자 암호를 재설정하세요. Windows PowerShell

- Active Directory관리자로 Active Directory 도메인에 가입된 인스턴스에 연결합니다.
- Windows PowerShell를 엽니다.
- 다음 명령을 입력하여 사용자 이름, 디렉터리 ID `jane.doe`, 비밀번호를 디렉터리 ID 및 원하는 자격 `P@ssw0rd` 증명으로 대체합니다. Active Directory 자세한 내용은 [Reset-DS UserPassword Cmdlet](#)을 참조하십시오.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword "P@ssw0rd"
```

그룹 만들기

다음 절차를 사용하여 Simple AD 디렉터리에 조인된 EC2 인스턴스에서 보안 그룹을 생성합니다. 보안 그룹을 만들려면 먼저 [Active Directory 관리 도구 설치](#)에서 절차를 완료해야 합니다.

그룹을 생성하려면

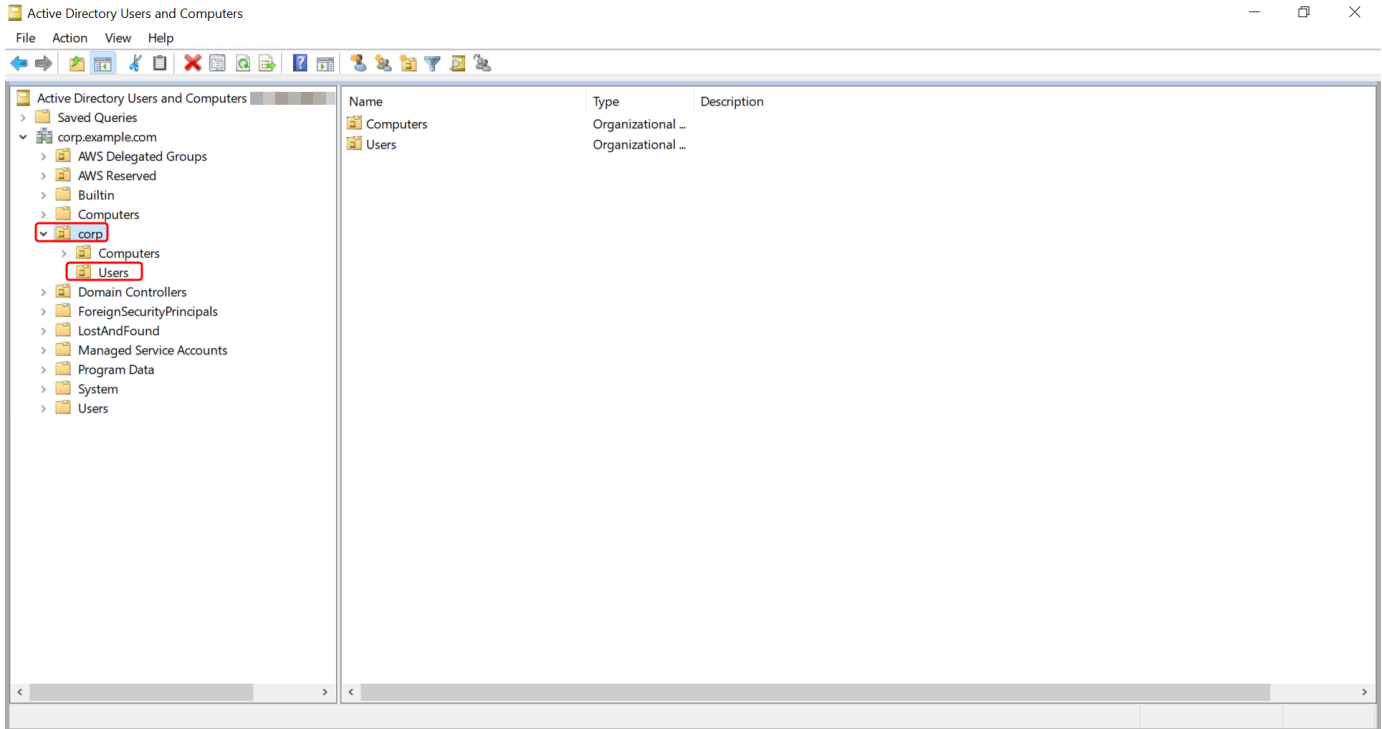
- Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
- Active Directory 사용자 및 컴퓨터 도구를 엽니다. 이 도구에 대한 바로 가기는 관리 도구 폴더에 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서, 디렉터리의 NetBIOS 이름 OU 아래에서 그룹을 저장할 OU를 선택합니다 (예: Corp\Users). AWS에서 디렉터리에 사용되는 OU 구조에 대한 자세한 정보는 [AWS 관리형 Microsoft AD 액티브 디렉터리로 생성되는 항목](#) 단원을 참조하세요.



4. 작업 메뉴에서 새로 만들기를 클릭한 후 그룹을 클릭하여 새 그룹 마법사를 엽니다.
5. 그룹 이름에 그룹 이름을 입력하고 필요에 맞는 그룹 범위를 선택한 다음 그룹 유형으로 보안을 선택합니다. Active Directory 그룹 범위 및 보안 그룹에 대한 자세한 내용은 Microsoft Windows Server 설명서의 [Active Directory 보안 그룹](#)을 참조하세요.
6. 확인을 클릭합니다. 사용자 폴더에 새 보안 그룹이 나타납니다.

그룹에 사용자 추가

Simple AD 디렉터리에 조인된 EC2 인스턴스에서 사용자를 보안 그룹에 추가하려면 다음 절차를 사용합니다.

그룹에 사용자를 추가하는 방법

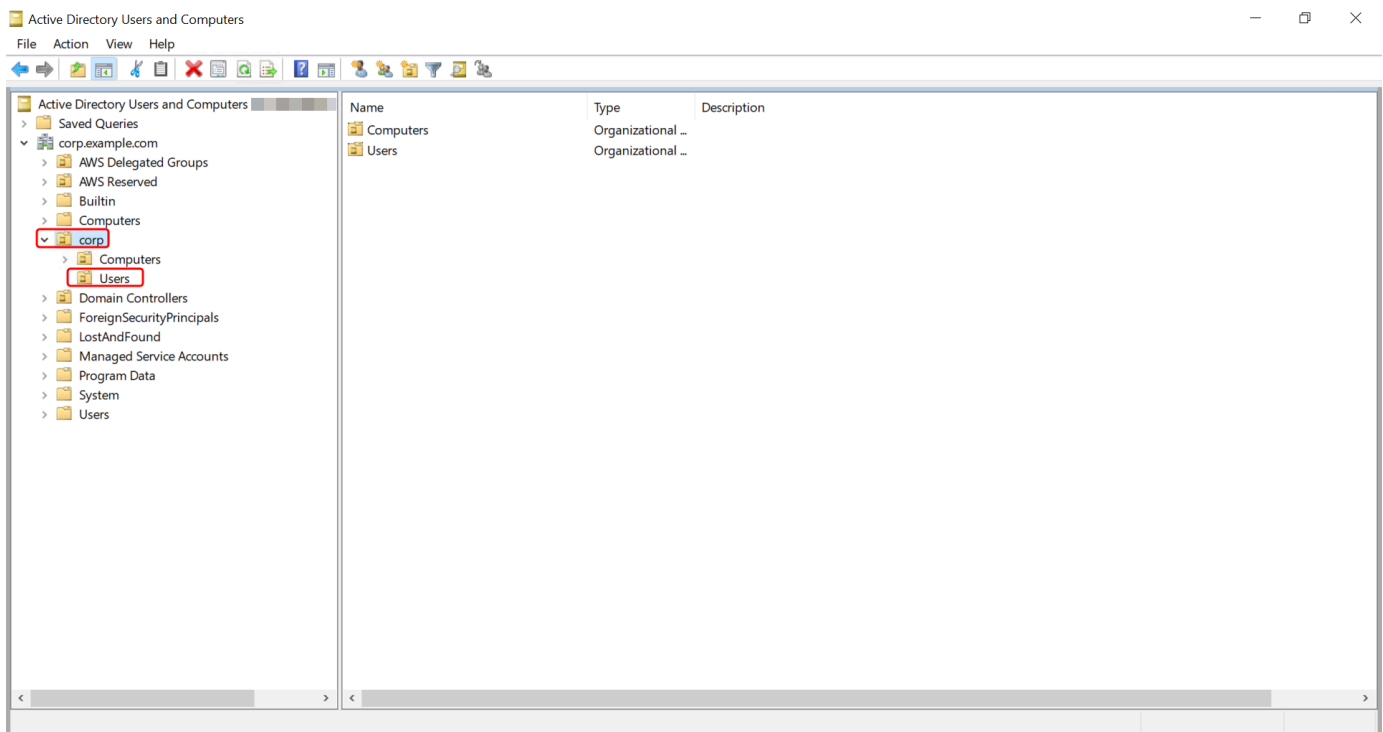
1. Active Directory 관리 도구가 설치된 인스턴스에 연결합니다.
2. Active Directory 사용자 및 컴퓨터 도구를 엽니다. 이 도구에 대한 바로 가기는 관리 도구 폴더에 있습니다.

Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 Active Directory 사용자 및 컴퓨터 도구 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\dsa.msc
```

3. 디렉터리 트리에서, 디렉터리의 NetBIOS 이름 OU 아래에서 그룹을 저장한 OU를 선택하고 사용자를 추가하려는 그룹을 선택합니다.



4. 작업 메뉴에서 속성을 클릭하여 그룹의 속성 대화 상자를 엽니다.
5. 구성원 탭을 선택하고 추가를 클릭합니다.
6. 선택할 객체 이름 입력에 추가하려는 사용자 이름을 입력하고 확인을 클릭합니다. 구성원 목록에 이름이 표시됩니다. 확인을 다시 선택하여 그룹 멤버십을 업데이트합니다.
7. 사용자 폴더에서 사용자를 선택하고 작업 메뉴에서 속성을 클릭하여 속성 대화 상자를 열고 해당 사용자가 그룹의 구성원인지 확인합니다. 소속 그룹 탭을 선택합니다. 사용자가 속한 그룹의 이름이 목록에 표시됩니다.

Simple AD 디렉터리 모니터링

다음 방법을 사용하여 Simple AD 디렉터리를 모니터링할 수 있습니다.

주제

- [디렉터리 상태 이해](#)
- [Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.](#)

디렉터리 상태 이해

다음은 디렉터리에 대한 다양한 상태입니다.

활성

디렉터리가 정상적으로 작동하고 있습니다. 디렉터리에서 AWS Directory Service 가 어떤 문제도 탐지하지 않았습니니다.

[생성 중]

디렉터리가 현재 생성되는 중입니다. 디렉터리 생성에는 보통 20~45분이 소요되지만, 시스템 로드 에 따라 달라질 수 있습니다.

Deleted

디렉터리가 삭제되었습니다. 디렉터리를 위한 모든 리소스들이 해제되었습니다. 디렉터리가 이 상태에 들어오면 복구가 불가능합니다.

[삭제 중]

디렉터리가 현재 삭제되는 중입니다. 디렉터리는 완전히 삭제될 때까지 이 상태를 유지하게 됩니다. 디렉터리가 이 상태에 들어가면 삭제 작업을 취소할 수 없고 디렉터리를 복구할 수 없습니다.

실패

디렉터리 생성이 불가능했습니다. 이 디렉터를 삭제하세요. 이 문제가 계속되면 [AWS Support 센터](#)에 문의하세요.

[Impaired]

디렉터리가 성능 저하 상태에서 실행 중입니다. 1개 이상의 문제가 탐지되었고, 모든 디렉터리 작업이 전체 운영 용량에서 실행되지 못할 수 있습니다. 디렉터리가 이 상태가 되는 가능한 이유는 여러 가지입니다. 여기에는 패치 적용 또는 EC2 인스턴스 교체와 같은 정상적인 운영 유지 관리 활동, 도메인 컨트롤러 중 하나에서 애플리케이션에 의한 일시적 핫스팟 발생 또는 사용자가 네트워크

크를 변경하는 과정에서 잘못 발생한 디렉터리 통신 중단이 포함됩니다. 자세한 내용은 [AWS 관리형 Microsoft AD 문제 해결](#), [문제 해결 AD Connector](#) 또는 [Simple AD 문제 해결](#) 단원을 참조하세요. 일반적인 유지 관리 관련 문제의 경우 40분 이내에 이러한 문제를 AWS 해결합니다. 문제 해결 주제를 검토한 후 디렉터리가 40분 이상 Impaired 상태를 지속할 경우 [AWS Support 센터](#)에 문의하는 것이 좋습니다.

Important

디렉터리가 Impaired 상태일 동안에는 스냅샷을 복원하지 마세요. 장애를 해결하기 위해 스냅샷 복원이 필요한 경우는 드뭅니다. 자세한 정보는 [디렉터리 스냅샷 또는 복구](#)를 참조하세요.

Inoperable

디렉터리가 작동하지 않습니다. 모든 디렉터리 엔드포인트가 문제를 보고했습니다.

[Requested]

디렉터리를 생성하라는 요청이 현재 보류 중입니다.

RestoreFailed

스냅샷에서 디렉터리 복원이 실패했습니다. 복원 작업을 다시 시도하세요. 이 문제가 계속되면 다른 스냅샷을 시도하거나 [AWS Support Center](#)에 문의하세요.

복원 중

자동 또는 수동 스냅샷에서 디렉터리가 현재 복원 중입니다. 스냅샷의 디렉터리 데이터 크기에 따라 스냅샷에서 디렉터리를 복원하는 데 보통 몇 분이 소요됩니다.

자세한 내용은 [Simple AD 디렉터리 상태 사유](#)을(를) 참조하세요.

Amazon SNS를 사용하여 디렉터리 상태 알림을 구성합니다.

Amazon Simple Notification Service(Amazon SNS)를 사용하면 디렉터리 상태가 바뀔 때 이메일 또는 텍스트(SMS) 메시지를 수신할 수 있습니다. 디렉터리 상태가 활성 상태에서 [손상됨 또는 작동 불가 상태](#)로 바뀌면 알림을 받게 됩니다. 디렉터리가 Active 상태로 돌아갈 때도 알림을 받게 됩니다.

작동 방식

Amazon SNS는 "주제"를 사용해 메시지를 수집 및 배포합니다. 각 주제마다 1명 이상의 구독자가 해당 주제에 게시된 메시지를 수신합니다. 아래 단계를 사용하여 Amazon SNS 주제에 AWS Directory

Service 게시자로 추가할 수 있습니다. 디렉터리 상태의 변화를 AWS Directory Service 감지하면 해당 주제에 메시지를 게시하고, 이 메시지는 주제 구독자에게 전송됩니다.

여러 디렉터를 게시자로서 단일 주제에 연결할 수 있습니다. Amazon SNS에서 이전에 생성했던 주제에 디렉터리 상태 메시지를 추가할 수도 있습니다. 주제를 게시하거나 구독할 수 있는 사람을 세부적으로 제어할 수 있습니다. Amazon SNS에 대한 전체 내용은 [Amazon SNS란 무엇인가요?](#) 단원을 참조하세요.

디렉터리에 대해 SNS 메시지를 활성화하는 방법

1. [예 AWS Management Console 로그인하고 콘솔을 엽니다.](#) AWS Directory Service
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 유지 관리 탭을 선택합니다.
4. 디렉터리 모니터링 섹션에서 작업을 선택한 후 알림 생성을 선택합니다.
5. 알림 생성 페이지에서 Choose a notification type(알림 유형 선택)을 선택한 후 새 알림 생성을 선택합니다. 또는, 기존 SNS 주제를 이미 가지고 있는 경우 기존 SNS 주제 연결을 선택하여 이 디렉터리에서 해당 주제로 상태 메시지를 전송할 수 있습니다.

Note

새 알림 생성을 선택하지만, 이미 존재하는 SNS 주제에 대해 동일한 주제 이름을 사용하는 경우에는 Amazon SNS가 새 주제를 생성하지 않고 기존 주제에 새 구독 정보를 추가만 합니다.

기존 SNS 주제 연결을 선택하는 경우 디렉터리와 동일한 리전에 있는 SNS 주제만 선택할 수 있습니다.

6. 수신자 유형을 선택하고 수신자 연락처 정보를 입력합니다. SMS에 사용할 전화 번호를 입력할 때는 숫자만 사용합니다. 대시, 공백, 괄호를 사용하지 마세요.
7. (선택 사항) 주제 이름과 SNS 표시 이름을 제공합니다. 표시 이름은 이 주제에서 모든 SMS 메시지에 포함시킬 짧은 이름(최대 10자)입니다. SMS 옵션을 사용할 때 표시 이름이 필요합니다.

Note

[DirectoryServiceFullAccess](#) 관리형 정책만 적용되는 IAM 사용자 또는 역할을 사용하여 로그인한 경우 주제 이름은 "DirectoryMonitoring" 로 시작해야 합니다. 사용자가 주제 이름을 추가로 정의하고 싶으면 SNS에 대한 추가 권한이 필요합니다.

8. 생성을 선택하세요.

[추가 이메일 주소, Amazon SQS 대기열 AWS Lambda등 추가 SNS 구독자를 지정하려는 경우 Amazon SNS 콘솔에서 지정할 수 있습니다.](#)

주제에서 디렉터리 상태 메시지를 삭제하는 방법

1. [예 AWS Management Console 로그인하고 콘솔을 엽니다.AWS Directory Service](#)
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 유지 관리 탭을 선택합니다.
4. 디렉터리 모니터링 섹션의 목록에서 SNS 주제 이름을 선택하고 작업을 선택한 후 제거를 선택합니다.
5. 제거를 선택합니다.

이렇게 하면 선택한 SNS 주제에 대한 게시자 역할을 하는 디렉터리가 삭제됩니다. 전체 주제를 삭제하려면 [Amazon SNS 콘솔에서](#) 삭제할 수 있습니다.

Note

디렉터리가 해당 주제에 상태 메시지를 전송하고 있지 않아야만 SNS 콘솔을 이용해 Amazon SNS 주제를 삭제할 수 있습니다.

SNS 콘솔을 사용해 Amazon SNS 주제를 삭제하면 이러한 변경이 Directory Services 콘솔 내에 즉각 반영되지 않습니다. 디렉터리의 모니터링 탭에서 주제를 찾을 수 없음을 알리는 상태 업데이트를 확인한 경우에는 다음 번에 디렉터리가 삭제된 주제에 알림을 게시할 때만 알림을 받게 됩니다.

따라서 중요한 디렉터리 상태 메시지를 놓치지 않으려면 메시지를 받는 주제를 삭제하기 전에 디렉터리를 다른 Amazon SNS 주제와 연결하십시오. AWS Directory Service

Amazon EC2 인스턴스를 Simple AD Active Directory에 조인합니다.

인스턴스가 시작되면 Amazon EC2 인스턴스를 도메인에 원활하게 조인할 Active Directory 수 있습니다. 자세한 정보는 [Amazon EC2 윈도우 인스턴스를 AWS 관리형 Microsoft AD에 원활하게 조인합니다. Active Directory](#)을 참조하세요. 또한 자동화를 통해 [AWS Directory Service 콘솔에서 직접 EC2 인스턴스를 시작하고 Active Directory 도메인에 조인할 수 있습니다.AWS Systems Manager](#)

EC2 인스턴스를 Active Directory 도메인에 수동으로 조인해야 하는 경우 적절한 지역 및 보안 그룹 또는 서브넷에서 인스턴스를 시작한 다음 인스턴스를 도메인에 조인해야 합니다.

이러한 인스턴스에 원격 연결이 가능하려면 연결 중인 네트워크에서 인스턴스로의 IP 연결이 있어야 합니다. 대부분의 경우, 이를 위해서는 인터넷 게이트웨이가 VPC에 연결되고 인스턴스가 퍼블릭 IP 주소를 가지고 있어야 합니다.

주제

- [Amazon EC2 윈도우 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.](#)
- [Amazon EC2 Windows 인스턴스를 Simple AD Active Directory에 수동으로 조인합니다.](#)
- [Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.](#)
- [Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 수동으로 조인합니다.](#)
- [Simple AD에 대한 디렉터리 조인 권한 위임](#)
- [DHCP 옵션 세트 생성](#)

Amazon EC2 윈도우 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.

이 절차는 Amazon EC2 Windows 인스턴스를 Simple AD Active Directory에 원활하게 연결합니다.

EC2 Windows 인스턴스에 원활하게 가입하려면

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 [Amazon EC2 콘솔을 엽니다.](#)
2. 탐색 표시줄에서 기존 디렉터리와 AWS 리전 동일한 디렉터를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Windows EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지(Amazon Machine Image) 섹션의 빠른 시작 창에서 Windows를 선택합니다. Amazon Machine Image(AMI) 드롭다운 목록에서 Windows Amazon Machine Image(AMI)를 변경할 수 있습니다.
7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다.
 - a. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다.

- b. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다.
- c. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다.
- d. Create key pair(키 페어 생성)를 선택합니다.
- e. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

 Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.


- 9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
- 10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



- 11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

- 12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
- 13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
- 14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

 Note

도메인 조인 디렉터를 선택하면 다음이 표시될 수 있습니다.

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로파일의 경우 기존 IAM 인스턴스 프로파일을 선택하거나 새 프로파일을 생성할 수 있습니다. IAM 인스턴스 프로파일 드롭다운 목록에서 AmazonSSM ManagedInstanceCore 및 AmazonSSM의 AWS 관리형 정책이 DirectoryServiceAccess 연결된 IAM 인스턴스 프로파일을 선택합니다. 새 프로파일을 생성하려면 새 IAM 프로파일 생성 링크를 선택하고 다음을 수행하십시오.

1. 역할 생성을 선택합니다.
2. Select trusted entity(신뢰할 수 있는 엔터티 선택)에서 AWS Service를 선택합니다.
3. 사용 사례에서 EC2를 선택합니다.
4. 권한 추가의 정책 목록에서 AmazonSSM 및 AmazonSSM ManagedInstanceCore 정책을 선택합니다. DirectoryServiceAccess 목록을 필터링하려면 검색 상자에 **SSM**을(를) 입력합니다. 다음을 선택합니다.

Note

AmazonSSM은 인스턴스를 관리자에 조인할 수 있는 DirectoryServiceAccess 권한을 제공합니다. Active Directory AWS Directory Service AmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는 기타 권한 및 정책에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

5. Name, review, and create(이름, 검토 및 생성) 페이지에서 Role name(역할 이름)을 입력합니다. EC2 인스턴스에 연결하려면 이 역할 이름이 필요합니다.
6. (선택 사항) 설명 필드에 IAM 인스턴스 프로파일에 대한 설명을 입력할 수 있습니다.
7. 역할 생성을 선택합니다.

8. 인스턴스 시작 페이지로 돌아가서 IAM 인스턴스 프로파일 옆에 있는 새로 고침 아이콘을 선택합니다. 새 IAM 인스턴스 프로파일은 IAM 인스턴스 프로파일 드롭다운 목록에 표시되어야 합니다. 새 프로파일을 선택하고 나머지 설정은 기본값으로 유지합니다.

16. 인스턴스 시작을 선택합니다.

Amazon EC2 Windows 인스턴스를 Simple AD Active Directory에 수동으로 조인합니다.

기존 Amazon EC2 Windows 인스턴스를 Simple AD Active Directory에 수동으로 조인하려면 에서 지정한 파라미터를 사용하여 인스턴스를 시작해야 합니다. [Amazon EC2 윈도우 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.](#)

Simple AD DNS 서버의 IP 주소가 필요합니다. 이 정보는 디렉터리 서비스 > 디렉터리 > 디렉터리의 디렉터리 ID 링크 > 디렉터리 세부 정보 및 네트워킹 및 보안 섹션에서 찾을 수 있습니다.

The screenshot displays the AWS Management Console interface for a Simple AD directory instance. The breadcrumb navigation shows 'Directory Service > Directories > d-1234567890'. The main content area is titled 'd-1234567890' and contains two main sections: 'Directory details' and 'Networking details'. The 'Directory details' section lists the following information:

Directory type	Microsoft AD	Directory DNS name	corp.example.com
Edition	Standard	Directory NetBIOS name	corp
Operating system version	Windows Server 2019	Directory administration EC2 instance(s)	-

The 'Networking details' section shows the VPC, availability zones (us-east-2a and us-east-2b), and subnets. The DNS address is highlighted as 192.0.2.1 and 198.51.100.1.

Windows 인스턴스를 Simple AD Active Directory에 조인하려면

1. 원격 데스크톱 프로토콜 클라이언트를 사용해 인스턴스를 연결합니다.
2. 인스턴스에서 TCP/IPv4 속성 대화 상자를 엽니다.

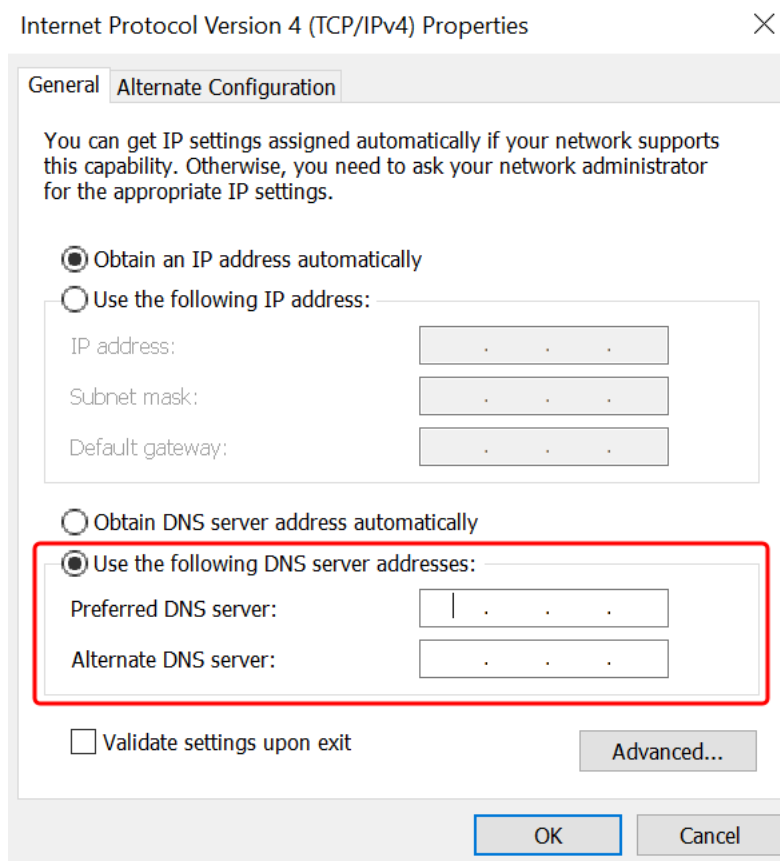
- a. 네트워크 연결 대화 상자를 엽니다.

i Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 네트워크 연결 대화 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. 활성화된 네트워크 연결에 대한 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) [Properties]를 선택합니다.
- c. 연결 속성 대화 상자에서 인터넷 프로토콜 버전 4를 엽니다(더블 클릭).
3. 다음 DNS 서버 주소 사용을 선택하고 기본 DNS 서버 및 대체 DNS 서버 주소를 Simple AD 제공 DNS 서버의 IP 주소로 변경한 다음 확인을 선택합니다.



4. 인스턴스에 대한 [System Properties] 대화 상자를 열고 [Computer Name] 탭을 선택한 다음, [Change]를 선택합니다.

i Tip

인스턴스의 명령 프롬프트에서 다음을 실행하여 시스템 속성 대화 상자를 직접 열 수 있습니다.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

- 구성원 필드에서 도메인을 선택하고 Simple AD Active Directory의 정식 이름을 입력한 다음 확인을 선택합니다.
- 도메인 관리자의 이름과 암호를 묻는 메시지가 표시되면 도메인 조인 권한을 가진 계정의 사용자 이름과 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [Simple AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

i Note

도메인의 전체 이름 또는 NetBIOS 이름, 백슬래시 (\), 사용자 이름 순으로 입력할 수 있습니다. 사용자 이름은 관리자입니다. 예: **corp.example.com\administrator** 또는 **corp\administrator**.

- 도메인에 온 것을 환영하는 메시지를 받은 후에 인스턴스를 재시작해야 변경 사항이 적용됩니다.

이제 인스턴스가 Simple AD Active Directory 도메인에 가입되었으므로 해당 인스턴스에 원격으로 로그인하여 디렉터리를 관리하는 유틸리티 (예: 사용자 및 그룹 추가) 를 설치할 수 있습니다. Active Directory 관리 도구를 사용하여 사용자 및 그룹을 만들 수 있습니다. 자세한 정보는 [Simple AD용 액티브 디렉터리 관리 도구 설치](#)을 참조하세요.


Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.

이 절차는 Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 원활하게 연결합니다.

다음과 같은 Linux 인스턴스 배포판과 버전이 지원됩니다.

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2(64비트 x86)
- Red Hat Enterprise Linux 8(HVM)(64비트 x86)
- Ubuntu Server 18.04 LTS 및 Ubuntu Server 16.04 LTS

- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

 Note

Ubuntu 14 및 Red Hat Enterprise Linux 7 이전의 배포판은 원활한 도메인 조인 기능을 지원하지 않습니다.

필수 조건

Linux 인스턴스에 원활한 도메인 조인을 설정하려면 먼저 이 섹션의 절차를 완료해야 합니다.

원활한 도메인 가입 서비스 계정을 선택합니다

Linux 컴퓨터를 Simple AD 도메인에 원활하게 연결할 수 있습니다. 이렇게 하려면 컴퓨터 계정 만들기 권한이 있는 사용자 계정을 만들어 컴퓨터를 도메인에 조인해야 합니다. Domain Admins 또는 다른 그룹의 구성원이 컴퓨터를 도메인에 조인할 수 있는 충분한 권한을 가지고 있더라도 이 방법은 권장되지 않습니다. 컴퓨터를 도메인에 조인하는 데 필요한 최소 권한이 있는 서비스 계정을 사용하는 것이 가장 좋습니다.

컴퓨터 계정 생성을 위한 권한을 처리하고 서비스 계정에 권한을 위임하는 방법에 대한 자세한 내용은 [서비스 계정에 권한 위임](#)을 참조하세요.

도메인 서비스 계정을 저장할 보안 암호 생성

를 AWS Secrets Manager 사용하여 도메인 서비스 계정을 저장할 수 있습니다.

보안 암호를 만들고 도메인 서비스 계정 정보를 저장하려면

1. <https://console.aws.amazon.com/secretsmanager/> 에서 AWS Management Console 로그인하고 AWS Secrets Manager 콘솔을 엽니다.
2. 새 보안 암호 저장(Store a new secret)을 선택합니다.
3. 새 보안 암호 저장(Store a new secret) 페이지에서 다음을 수행합니다.
 - a. 암호 유형에서 다른 암호 유형을 선택합니다.
 - b. 키/값 쌍에서 다음을 수행하십시오.

- i. 첫 번째 상자에 **awsSeamlessDomainUsername**를 입력합니다. 같은 행의 다음 상자에 서비스 계정의 사용자 이름을 입력합니다. 예를 들어 이전에 PowerShell 명령을 사용한 경우 서비스 계정 이름은 다음과 같습니다**awsSeamlessDomain**.

Note

있는 그대로 **awsSeamlessDomainUsername**을 입력해야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 조인에 실패합니다.

The screenshot shows the AWS Secrets Manager console interface for creating a new secret. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows a progress indicator with four steps: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The main content area is titled 'Choose secret type' and is divided into three sections: 'Secret type', 'Key/value pairs', and 'Encryption key'. In the 'Secret type' section, the 'Other type of secret' option is selected and highlighted with a red box. In the 'Key/value pairs' section, the 'Key/value' tab is active, and a single row is added with the key 'awsSeamlessDomainUsername' highlighted by a red box. The 'Encryption key' section shows 'aws/secretsmanager' selected from a dropdown menu. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. Add row(행 추가)를 선택합니다.
- iii. 새 행의 첫 번째 상자에 **awsSeamlessDomainPassword**를 입력합니다. 같은 행의 다음 상자에 서비스 계정의 암호를 입력합니다.

Note

있는 그대로 **awsSeamlessDomainPassword**을 입력해야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 조인에 실패합니다.

- iv. 암호화 키에서 기본값을 그대로 유지합니다 `aws/secretsmanager`. AWS Secrets Manager 이 옵션을 선택하면 항상 암호를 암호화합니다. 사용자가 생성한 키를 선택할 수도 있습니다.

Note

사용하는 비밀번호에 따라 수수료가 부과됩니다. AWS Secrets Manager 현재 기존의 전체적인 요금 목록은 [AWS Secrets Manager 요금](#)을 참조하세요. Secrets Manager에서 생성한 AWS 관리 키를 `aws/secretsmanager` 사용하여 비밀을 무료로 암호화할 수 있습니다. 자체 KMS 키를 생성하여 암호를 암호화하는 경우 현재 요율로 AWS 요금이 부과됩니다. AWS KMS 자세한 내용은 [AWS Key Management Service 요금](#)을 참조하십시오.

- v. 다음을 선택합니다.

4. 비밀 이름에 다음 형식을 사용하여 디렉터리 ID가 포함된 비밀 이름을 입력합니다. 이때 `d-xxxxxxxxxx#` 디렉터리 ID로 대체합니다.

```
aws/directory-services/d-xxxxxxxx/seamless-domain-join
```

이는 애플리케이션에서 보안 암호를 검색하는 데 사용됩니다.

Note

있는 그대로 **aws/directory-services/d-xxxxxxxx/seamless-domain-join**를 입력해야 하지만, `d-xxxxxxxxxxxx`를 디렉터리 ID로 바꿔야 합니다. 선행 공백이 나 끝 공백이 없어야 합니다. 그렇지 않으면 도메인 가입에 실패합니다.

The screenshot shows the 'Configure secret' page in the AWS Secrets Manager console. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The page is divided into four steps: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The 'Configure secret' section includes:

- Secret name and description**: A text input field for the secret name containing 'aws/directory-services/d-xxxxxxx/seamless-domain-join'. Below it is a description text area containing 'Access to MYSQL prod database for my AppBeta'.
- Tags - optional**: A section indicating no tags are currently associated with the secret, with an 'Add' button.
- Resource permissions - optional**: A section with an 'Edit permissions' button.
- Replicate secret - optional**: A section with a right-pointing arrow and text explaining that it creates read-only replicas in other regions.

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

5. 다른 모든 항목은 기본값으로 설정한 후 Next(다음)를 선택합니다.
6. Configure automatic rotation(자동 교체 구성)을 Disable automatic rotation(자동 교체 사용 안 함)으로 선택하고 Next(다음)를 선택합니다.

이 암호를 저장한 후 해당 암호에 대한 로테이션을 켤 수 있습니다.

7. 설정을 검토한 다음 Store(저장)를 선택하여 변경 내용을 저장합니다. 이제 Secrets Manager 콘솔에서 새 보안 암호가 목록에 포함된 계정의 보안 암호 목록으로 돌아갑니다.
8. 목록에서 새로 생성한 보안 암호 이름을 선택하고 보안 암호 ARN 값을 기록해 둡니다. 다음 단원에서 이 값을 사용하게 됩니다.

도메인 서비스 계정 비밀번호에 대한 로테이션을 켜세요.

보안 태세를 개선하려면 정기적으로 암호를 교체하는 것이 좋습니다.

도메인 서비스 계정 비밀번호에 대한 순환 기능을 켜려면

- 사용 AWS Secrets Manager 설명서의 AWS Secrets Manager [암호 자동 교체 설정의](#) 지침을 따르십시오.

5단계의 경우 사용 AWS Secrets Manager 설명서의 [Microsoft Active Directory 순환 템플릿 자격 증명을](#) 사용하십시오.

도움이 필요하면 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager [순환 문제 해결을](#) 참조하십시오.

필요한 IAM policy 정책 및 역할 생성

다음 사전 필수 단계를 사용하여 Secrets Manager 원활한 도메인 가입 암호 (이전에 생성함) 에 대한 읽기 전용 액세스를 허용하는 사용자 지정 정책을 생성하고 새 DomainJoin LinuxEC2 IAM 역할을 생성합니다.

Secrets Manager IAM 읽기 정책 생성

IAM 콘솔을 사용하여 Secrets Manager 보안 암호에 대한 읽기 전용 액세스 권한을 부여하는 정책을 생성합니다.

Secrets Manager IAM 읽기 정책을 생성하려면

1. IAM 정책을 생성할 권한이 있는 AWS Management Console 사용자로 로그인합니다. 그런 다음 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창의 액세스 관리에서 정책을 선택합니다.
3. 정책 생성(Create policy)을 선택합니다.
4. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 그런 다음 JSON 텍스트 상자에 붙여 넣습니다.

Note

지역 및 리소스 ARN을 이전에 생성한 암호의 실제 지역 및 ARN으로 교체해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. 마쳤으면 [Next]를 선택합니다. 정책 검사기가 모든 구문 오류를 보고합니다. IAM 검증 정책에 대한 자세한 내용은 [Validating IAM policies](#)를 참조하세요.
6. Review policy(정책 검토) 페이지에서 **SM-Secret-Linux-DJ-d-xxxxxxxx-Read**와 같은 정책의 이름을 입력합니다. Summary(요약)을 검토하여 정책이 부여하는 권한을 확인합니다. 그런 다음 Create policy(정책 생성)를 선택하여 변경 내용을 저장합니다. 새로운 정책이 관리형 정책 목록에 나타나며 ID 연결 준비가 완료됩니다.

Note

보안 암호당 정책을 하나씩 생성하는 것이 좋습니다. 이렇게 하면 인스턴스가 적절한 보안 암호에만 액세스할 수 있고 인스턴스가 손상될 경우 미치는 영향이 최소화됩니다.

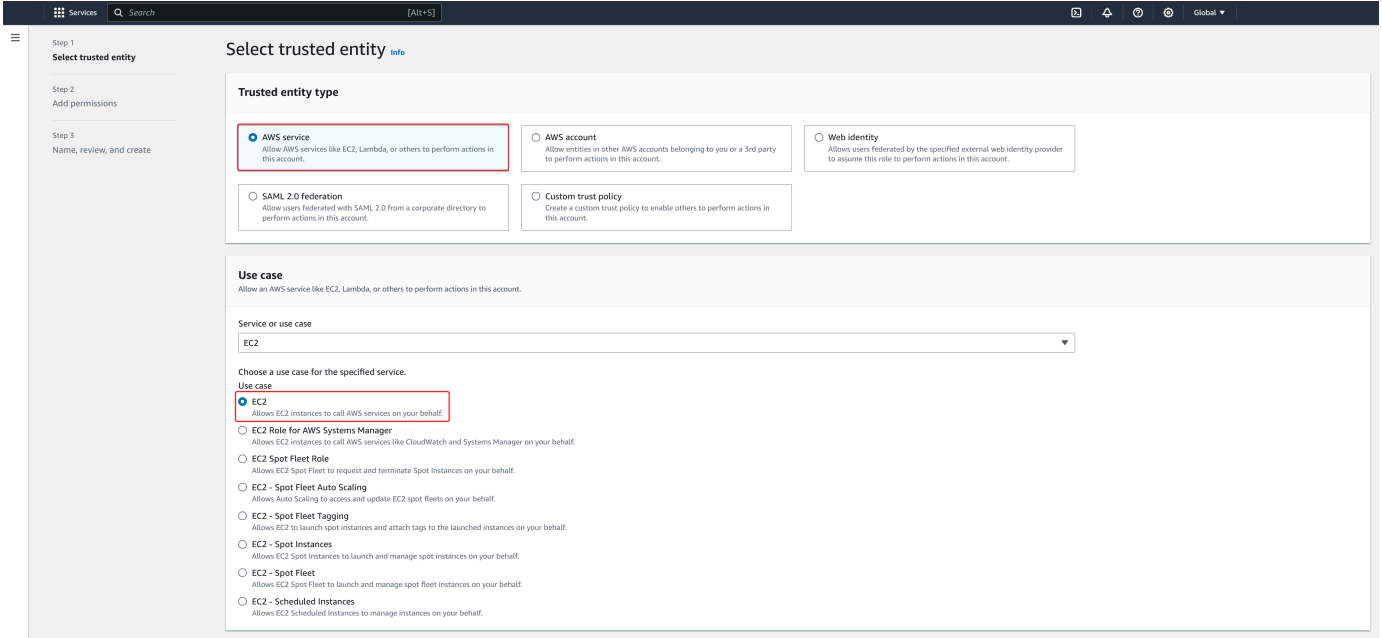
Linux/EC2 역할을 생성하십시오. DomainJoin

IAM 콘솔을 사용하여 Linux EC2 인스턴스를 도메인에 조인하는 데 사용할 역할을 생성합니다.

Linux/EC2 역할을 만들려면 DomainJoin

1. IAM 정책을 생성할 권한이 있는 AWS Management Console 사용자로 로그인합니다. 그런 다음 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.

2. 탐색 창의 액세스 관리에서 역할을 선택합니다.
3. 콘텐츠 창에서 Create role(역할 생성)을 선택합니다.
4. 신뢰할 수 있는 엔티티 유형 선택 아래에서 AWS 서비스를 선택합니다.
5. 사용 사례에서 EC2를 선택한 후 다음을 선택합니다.



6. Filter policies(필터 정책)의 경우 다음을 수행합니다.
 - a. **AmazonSSMManagedInstanceCore**을 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - b. **AmazonSSMDirectoryServiceAccess**을 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - c. **SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read**(또는 이전 절차에서 생성한 IAM 정책의 이름)을(를) 입력합니다. 그런 다음 목록에서 해당 항목의 확인란을 선택합니다.
 - d. 위에 나열된 세 가지 정책을 추가한 후 역할 생성을 선택합니다.

Note

AmazonSSM은 인스턴스를 DirectoryServiceAccess 관리자에 조인할 수 있는 Active Directory 권한을 제공합니다. AWS Directory Service AmazonSSM은 ManagedInstanceCore 서비스를 사용하는 데 필요한 최소 권한을 제공합니다. AWS Systems Manager 이러한 권한으로 역할을 생성하는 방법과 IAM 역할에 할당할 수 있는

기타 권한 및 정책에 관한 정보에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.

7. 새 역할의 이름 (예: 역할 이름) 필드에 원하는 다른 이름을 입력합니다. **LinuxEC2DomainJoin**
8. (선택 사항)역할 설명에 설명을 입력합니다.
9. (선택 사항) 3단계: 태그를 추가할 태그 추가에서 새 태그 추가를 선택합니다. 태그 키-값 쌍은 이 역할에 대한 액세스를 구성, 추적 또는 제어하는 데 사용됩니다.
10. 역할 생성을 선택합니다.

Linux 인스턴스를 Simple AD Active Directory에 원활하게 연결

이제 필수 작업을 모두 구성했으므로 다음 절차를 사용하여 EC2 Linux 인스턴스를 원활하게 연결할 수 있습니다.

Linux 인스턴스를 원활하게 연결하려면

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 [Amazon EC2 콘솔을 엽니다.](#)
2. 탐색 표시줄의 지역 선택기에서 기존 디렉토리와 AWS 리전 동일한 디렉토리를 선택합니다.
3. EC2 대시보드의 시작 인스턴스 섹션에서 인스턴스 시작을 선택합니다.
4. 인스턴스 시작 페이지의 이름 및 태그 섹션에서 Linux EC2 인스턴스에 사용할 이름을 입력합니다.
5. (선택 사항) 추가 태그 추가에서 이 EC2 인스턴스에 대한 액세스를 구성, 추적, 제어할 태그-키 값 페어를 하나 이상 추가합니다.
6. 애플리케이션 및 OS 이미지 (Amazon 머신 이미지) 섹션에서 시작하려는 Linux AMI를 선택합니다.

Note

사용되는 AMI에는 AWS Systems Manager (SSM 에이전트) 버전 2.3.1644.0 이상이 있어야 합니다. AMI에서 인스턴스를 시작하여 AMI에 설치된 SSM 에이전트 버전을 확인하려면 [현재 설치된 SSM 에이전트 버전 가져오기](#)를 참조하세요. SSM 에이전트를 업그레이드해야 하는 경우 [Linux용 EC2 인스턴스에 SSM 에이전트 설치 및 구성](#)을 참조하세요. SSM은 Linux 인스턴스를 도메인에 aws:domainJoin 조인할 때 플러그인을 사용합니다. Active Directory ##### Linux ##### ### ### EC2AMAZ- XXXXXXXX #####

#. 에 대한 자세한 내용은 사용 `aws:domainJoin` 설명서의 [AWS Systems Manager 명령 문서 플러그인 참조](#)를 참조하십시오. AWS Systems Manager

7. 인스턴스 유형 섹션의 인스턴스 유형 드롭다운 목록에서 사용하려는 인스턴스 유형을 선택합니다.
8. 키 페어(로그인) 섹션에서 새 키 페어 생성을 선택하거나 기존 키 페어에서 선택할 수 있습니다. 새로운 키 페어를 생성하려면 새 키 페어 생성을 선택합니다. 키 페어의 이름을 입력하고 키 페어 유형 및 프라이빗 키 파일 형식에 대한 옵션을 선택합니다. OpenSSH에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .pem을 선택합니다. PuTTY에서 사용할 수 있는 형식으로 프라이빗 키를 저장하려면 .ppk를 선택합니다. Create key pair(키 페어 생성)를 선택합니다. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

Important

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다.

9. 인스턴스 시작 페이지의 네트워크 설정 섹션에서 편집을 선택합니다. VPC - 필수 드롭다운 목록에서 디렉터리가 생성된 VPC를 선택합니다.
10. 서브넷 드롭다운 목록에서 VPC의 퍼블릭 서브넷 중 하나를 선택합니다. 선택한 서브넷에서는 인터넷 게이트웨이로 모든 외부 트래픽이 라우팅되어야 합니다. 그렇지 않으면 인스턴스를 원격으로 연결할 수 없게 됩니다.

인터넷 게이트웨이에 연결하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.



11. Auto-assign Public IP(퍼블릭 IP 자동 할당)에서 Enable(활성화)을 선택합니다.

퍼블릭 및 프라이빗 IP 주소 지정에 대한 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 [Amazon EC2 인스턴스 IP 주소 지정](#)을 참조하세요.

12. 방화벽(보안 그룹) 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
13. 스토리지 구성 설정의 경우 기본 설정을 사용하거나 필요에 맞게 변경할 수 있습니다.
14. 고급 세부 정보 섹션을 선택하고 도메인 조인 디렉터리 드롭다운 목록에서 도메인을 선택합니다.

Note

도메인 조인 디렉터를 선택하면 다음이 표시될 수 있습니다.

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

이 오류는 EC2 시작 마법사가 예상치 못한 속성을 가진 기존 SSM 문서를 식별할 때 발생합니다. 다음 중 하나를 수행할 수 있습니다.

- 이전에 SSM 문서를 편집했는데 속성이 예상된 경우 [Close] 를 선택하고 변경 없이 EC2 인스턴스를 시작하십시오.
- SSM 문서를 삭제하려면 여기에서 기존 SSM 문서 삭제 링크를 선택합니다. 이렇게 하면 올바른 속성을 가진 SSM 문서를 만들 수 있습니다. EC2 인스턴스를 시작하면 SSM 문서가 자동으로 생성됩니다.

15. IAM 인스턴스 프로필의 경우 사전 요구 사항 섹션 2단계: LinuxEC2 역할 생성에서 이전에 생성한 IAM 역할을 선택합니다. DomainJoin
16. 인스턴스 시작을 선택합니다.

Note

SUSE Linux로 원활한 도메인 조인을 수행하는 경우 인증이 작동하려면 재부팅해야 합니다. Linux 터미널에서 SUSE를 재부팅하려면 `sudo reboot`를 입력합니다.

Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 수동으로 조인합니다.

Amazon EC2 Windows 인스턴스 외에도 특정 Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 조인할 수 있습니다. 다음과 같은 Linux 인스턴스 배포판과 버전이 지원됩니다.

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2(64비트 x86)
- 아마존 리눅스 2023 AMI
- Red Hat Enterprise Linux 8(HVM)(64비트 x86)
- Ubuntu Server 18.04 LTS 및 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64

- SUSE Linux Enterprise Server 15 SP1

Note

기타 Linux 배포판 및 버전은 작동이 가능할 수도 있지만, 테스트는 거치지 않았습니다.

필수 조건

디렉터리에 Amazon Linux 혹은 CentOS, Red Hat, Ubuntu 인스턴스를 조인하려면 [Amazon EC2 Linux 인스턴스를 Simple AD Active Directory에 원활하게 조인합니다.](#)에 지정된 대로 인스턴스를 먼저 시작해야 합니다.

Important

아래의 일부 절차들로 인해(올바르게 수행되지 않은 경우) 인스턴스 접속이나 사용이 불가능해질 수 있습니다. 따라서 이러한 절차를 수행하기 전에 인스턴스에 대한 백업을 생성하거나 스냅샷을 만드는 것이 좋습니다.

디렉터리에 Linux 인스턴스 조인

다음 탭 중 하나를 이용해 특정 Linux 인스턴스의 단계를 수행합니다.

Amazon Linux

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Amazon Linux - 64비트 인스턴스가 업데이트되었는지 확인합니다.

```
sudo yum -y update
```

4. Linux 인스턴스에 필요한 Amazon Linux 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
krb5-workstation
```

Note

사용 중인 Amazon Linux 버전을 확인하는 데 도움이 필요하면 Linux 인스턴스용 Amazon EC2 사용 설명서에서 [Amazon Linux 이미지 식별](#)을 참조하세요.

- 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

도메인 조인 권한을 가진 *example.com* 도메인의 계정입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...
* Successfully enrolled machine in realm
```

- 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - 텍스트 편집기에서 `/etc/ssh/sshd_config` 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

7. 인스턴스가 재시작되고 나면 다음 단계를 수행하여 SSH 클라이언트에 이를 연결하고 sudoers 목록에 도메인 관리자 그룹을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "`\<space>`"를 사용합니다.

CentOS

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. CentOS 7 인스턴스가 업데이트되었는지 확인합니다.

```
sudo yum -y update
```

4. Linux 인스턴스에 필요한 CentOS 7 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

도메인 조인 권한을 가진 *example.com* 도메인의 계정입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...  
* Successfully enrolled machine in realm
```

6. 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - a. 텍스트 편집기에서 `/etc/ssh/sshd_config` 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 설정값을 `yes`로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

7. 인스턴스가 재시작되고 나면 다음 단계를 수행하여 SSH 클라이언트에 이를 연결하고 sudoers 목록에 도메인 관리자 그룹을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "`<space>`"를 사용합니다.

Red hat

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Red Hat - 64비트 인스턴스가 업데이트되었는지 확인합니다.

```
sudo yum -y update
```

4. Linux 인스턴스에 필요한 Red Hat 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다. 패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

- 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -v -U join_account example.com --install=/  
join_account
```

join_account

도메인 가입 AccountName 권한이 있는 *example.com* 도메인 계정의 SAM입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...  
* Successfully enrolled machine in realm
```

- 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - 텍스트 편집기에서 `/etc/ssh/sshd_config` 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- PasswordAuthentication 설정값을 `yes`로 설정합니다.

```
PasswordAuthentication yes
```

- SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

7. 인스턴스가 재시작되고 나면 다음 단계를 수행하여 SSH 클라이언트에 이를 연결하고 sudoers 목록에 도메인 관리자 그룹을 추가합니다.

a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "<space>"를 사용합니다.

Ubuntu

1. SSH 클라이언트를 사용하여 인스턴스에 연결합니다.
2. AWS Directory Service 제공된 DNS 서버의 DNS 서버 IP 주소를 사용하도록 Linux 인스턴스를 구성합니다. VPC에 연결된 DHCP 옵션 세트에서 이를 설정하거나 인스턴스에서 이를 수동으로 설정하는 방법으로 이러한 구성이 가능합니다. 수동 설정을 원할 경우에는 AWS 지식 센터의 [프라이빗 Amazon EC2 인스턴스에 정적 DNS 서버를 할당하는 방법](#)에서 특정 Linux 배포판 및 버전에서 지속적인 DNS 서버를 설정하는 방법에 대한 지침을 참조하세요.
3. Ubuntu - 64비트 인스턴스가 업데이트되었는지 확인합니다.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Linux 인스턴스에 필요한 Ubuntu 패키지를 설치합니다.

Note

이러한 패키지 중 몇 개는 이미 설치가 되어 있을 수 있습니다.

패키지를 설치할 때 몇 가지 팝업 구성 화면이 나타날 수 있습니다. 보통은 이러한 화면의 필드들을 공백 상태로 남겨둡니다.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 역방향 DNS 확인을 비활성화하고 기본 영역을 도메인의 FQDN으로 설정합니다. 영역이 작동하려면 Ubuntu 인스턴스가 DNS에서 역 확인이 가능해야 합니다. 그렇지 않을 경우 다음과 같이 /etc/krb5.conf에서 역 DNS를 비활성해야 합니다.

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 다음 명령을 통해 디렉터리에 인스턴스를 조인합니다.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

도메인 가입 AccountName 권한이 있는 *example.com* 도메인 계정의 SAM입니다. 메시지가 나타나면 계정에 대한 암호를 입력합니다. 이러한 권한의 위임에 대한 자세한 정보는 [AWS Managed Microsoft AD에 대한 디렉터리 조인 권한 위임](#)을 참조하세요.

example.com

디렉터리의 정규화된 DNS 이름.

```
...
* Successfully enrolled machine in realm
```

7. 암호 인증을 허용하도록 SSH 서비스를 설정합니다.
 - a. 텍스트 편집기에서 /etc/ssh/sshd_config 파일을 엽니다.

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 설정값을 yes로 설정합니다.

```
PasswordAuthentication yes
```

- c. SSH 서비스를 다시 시작합니다.

```
sudo systemctl restart sshd.service
```

대안:

```
sudo service sshd restart
```

8. 인스턴스가 재시작되고 나면 다음 단계를 수행하여 SSH 클라이언트에 이를 연결하고 sudoers 목록에 도메인 관리자 그룹을 추가합니다.

- a. 다음 명령을 통해 sudoers 파일을 엽니다.

```
sudo visudo
```

- b. sudoers 파일 끝부분에 다음을 추가하고 저장합니다.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

위 예제에서는 Linux 공백 문자를 생성하기 위해 "\<space>"를 사용합니다.

Note

Simple AD를 사용할 때 "사용자가 첫 번째 로그인 시 암호를 변경하도록 강제" 옵션을 통해 Linux 인스턴스에서 사용자 계정을 생성한 경우, 해당 사용자는 처음에는 kpasswd를 사용해 암호를 변경할 수 없습니다. 처음으로 암호를 변경하려면 도메인 관리자가 Microsoft Active Directory 관리 도구를 사용해 사용자 암호를 업데이트해야 합니다.

Linux 인스턴스에서 계정 관리

Linux 인스턴스의 Simple AD 계정을 관리하려면 Linux 인스턴스의 특정 구성 파일을 다음과 같이 업데이트해야 합니다.

1. /etc/sss/sssd.conf 파일에서 krb5_use_kdcinfo를 False로 설정합니다. 예:

```
[domain/example.com]
krb5_use_kdcinfo = False
```

2. 이 구성이 활성화되려면 sssd 서비스를 재시작해야 합니다.

```
$ sudo systemctl restart sssd.service
```

또는 다음 작업을 사용할 수 있습니다.

```
$ sudo service sssd start
```

3. 또한 CentOS Linux 인스턴스에서 사용자를 관리하려면 다음이 포함되도록 /etc/smb.conf를 편집해야 합니다.

```
[global]
workgroup = EXAMPLE.COM
realm = EXAMPLE.COM
netbios name = EXAMPLE
security = ads
```

계정 로그인 액세스 제한

모든 계정을 Active Directory에 정의하면 기본으로 디렉토리의 모든 사용자는 인스턴스에 로그인할 수 있습니다. 특정 사용자만 sssd.conf의 ad_access_filter으로 인스턴스에 로그인할 수 있습니다. 예:

```
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

memberOf

특정 그룹의 멤버인 사용자는 반드시 인스턴스에 액세스할 수 있어야 한다는 뜻입니다.

cn

액세스해야 하는 그룹의 일반 이름입니다. 이 예제에서 그룹 이름은 *admins*입니다.

ou

위의 그룹이 위치해 있는 조직 단위(OU)입니다. 이 예제에서 OU는 *Testou*입니다.

dc

도메인의 도메인 구성 요소입니다. 이 예제에서는 *example*입니다.

dc

추가적인 도메인 구성 요소입니다. 이 예제에서는 *com*입니다.

현재 사용자는 `ad_access_filter`를 `/etc/sssds/sssds.conf`에 수동으로 추가해야 합니다.

텍스트 편집기에서 `/etc/sssds/sssds.conf` 파일을 엽니다.

```
sudo vi /etc/sssds/sssds.conf
```

추가를 하고 나면 `sssds.conf`가 다음과 같이 보일 수 있습니다.

```
[sssds]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@d
access_provider = ad
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

이 구성이 활성화되려면 `sssds` 서비스를 재시작해야 합니다.

```
sudo systemctl restart sssds.service
```

또는 다음 작업을 사용할 수 있습니다.

```
sudo service sssds restart
```

ID 매핑

Unix/Linux 사용자 식별자 (UID) 와 GID (그룹 식별자), Windows 및 SID (Active Directory보안 식별자) ID 간에 통합된 환경을 유지하기 위해 두 가지 방법으로 ID 매핑을 수행할 수 있습니다.

1. 중앙 집중식
2. 분산형

Note

중앙 집중식 사용자 ID 매핑에는 휴대용 운영 체제 인터페이스 또는 POSIX가 Active Directory 필요합니다.

중앙 집중식 사용자 ID 매핑

Active Directory또는 다른 경량 디렉터리 액세스 프로토콜 (LDAP) 서비스는 Linux 사용자에게 UID 및 GID를 제공합니다. Active Directory에서는 이러한 식별자가 사용자 속성에 저장됩니다.

- UID - 리눅스 사용자 이름 (문자열)
- UID 번호 - 리눅스 사용자 ID 번호 (정수)
- GID 번호 - 리눅스 그룹 ID 번호 (정수)

의 UID와 GID를 사용하도록 리눅스 인스턴스를 구성하려면 `sssd.conf` Active Directory `ldap_id_mapping = False` 파일에서 설정하십시오. 이 값을 설정하기 전에 사용자 및 그룹에 UID, UID 번호 및 GID 번호를 추가했는지 확인하십시오. Active Directory

분산 사용자 ID 매핑

POSIX 확장이 없거나 ID 매핑을 중앙에서 관리하지 않기로 선택한 경우 Linux에서 UID 및 GID 값을 계산할 수 있습니다. Active Directory Linux는 일관성을 유지하기 위해 사용자의 고유한 SID (보안 식별자) 를 사용합니다.

분산 사용자 ID 매핑을 구성하려면 `ldap_id_mapping = True` `sssd.conf` 파일에서 설정합니다.

Linux 인스턴스에 연결

SSH 클라이언트를 사용하여 인스턴스 연결을 하면 사용자 이름을 입력하라는 메시지가 나타납니다. 사용자는 `username@example.com` 또는 `EXAMPLE\username` 형식으로 사용자 이름을 입력할 수 있습니다. 사용 중인 Linux 배포판에 따라 다음과 비슷한 응답이 나타납니다.

Amazon Linux, Red Hat Enterprise Linux, CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)
```

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

```
System information as of Sat Apr 18 22:03:35 UTC 2020
```

```
System load:  0.01          Processes:            102
Usage of /:   18.6% of 7.69GB Users logged in:      2
Memory usage: 16%          IP address for eth0: 10.24.34.1
```


Swap usage: 0%

Simple AD에 대한 디렉터리 조인 권한 위임

컴퓨터를 디렉터리에 조인하려면 해당 권한을 가진 계정이 필요합니다.

Simple AD에서는 Domain Admins 그룹의 멤버가 컴퓨터를 디렉터리에 조인할 충분한 권한을 가집니다.


그러나 가장 좋은 방법은 필요한 최소 권한만을 가진 계정을 사용하는 것입니다. 다음 절차에서는 Joiners라는 새 그룹을 생성하고 이 그룹에 컴퓨터를 디렉터리에 조인하는 데 필요한 권한을 위임하는 방법을 보여줍니다.

이 절차는 디렉터리에 조인된 컴퓨터상에서 수행해야 하며, Active Directory User and Computers MMC 스냅인이 설치되어 있어야 합니다. 또한 도메인 관리자로 로그인해야 합니다.

Simple AD에 대한 조인 권한을 위임하려면

1. [Active Directory User and Computers]를 열고 탐색 트리에서 도메인 루트를 선택합니다.
2. 왼쪽 탐색 창에서 [Users]에 대한 컨텍스트 메뉴를 열고 (마우스 오른쪽 버튼 클릭) [New]를 선택한 다음, [Group]을 선택합니다.
3. [New Object - Group] 상자에서 다음을 입력하고 [OK]를 선택합니다.
 - 그룹 이름에 **Joiners**를 입력합니다.
 - [Group scope]에서 [Global]을 선택합니다.
 - [Group type]에서 [Security]를 선택합니다.
4. 탐색 트리에서 도메인 루트를 선택합니다. [Action] 메뉴에서 [Delegate Control]을 선택합니다.
5. [Delegation of Control Wizard] 페이지에서 Next를 선택한 후 [Add]를 선택합니다.
6. [Select Users, Computers, or Groups] 상자에 Joiners를 입력하고 [OK]를 선택합니다. 객체가 여러 개 있는 경우 위에서 생성한 Joiners 그룹을 선택합니다. 다음을 선택합니다.
7. [Tasks to Delegate] 페이지에서 [Create a custom task to delegate]를 선택한 후 [Next]를 선택합니다.
8. [Only the following objects in the folder]를 선택한 후 [Computer objects]를 선택합니다.
9. [Create selected objects in this folder]를 선택한 후 [Delete selected objects in this folder]를 선택합니다. 다음을 선택합니다.

Delegation of Control Wizard ✕

Active Directory Object Type
Indicate the scope of the task you want to delegate. 

Delegate control of:

This folder, existing objects in this folder, and creation of new objects in this folder

Only the following objects in the folder:

Site Settings objects

Sites Container objects

Subnet objects

Subnets Container objects

Trusted Domain objects


User objects

Create selected objects in this folder

Delete selected objects in this folder

10. [Read] 및 [Write]를 선택한 후 [Next]를 선택합니다.

Delegation of Control Wizard ✕

Permissions
Select the permissions you want to delegate. 

Show these permissions:

General

Property-specific

Creation/deletion of specific child objects

Permissions:

Full Control

Read

Write

Create All Child Objects

Delete All Child Objects

Read All Properties

11. [Completing the Delegation of Control Wizard] 페이지에서 정보를 확인하고 [Finish]를 선택합니다.
12. 강력한 암호를 사용하여 사용자를 생성하고 해당 사용자를 Joiners 그룹에 추가합니다. 그러면 사용자는 디렉터리에 연결할 수 있는 충분한 권한을 갖게 됩니다 AWS Directory Service .

DHCP 옵션 세트 생성

AWS 디렉터리에 대한 DHCP 옵션 세트를 생성하고 AWS Directory Service 디렉터리가 있는 VPC에 DHCP 옵션 세트를 할당하는 것이 좋습니다. 이렇게 해야 해당 VPC의 모든 인스턴스가 지정된 도메인을 가리키고 DNS 서버가 도메인 이름을 해석할 수 있습니다.

DHCP 옵션 세트에 대한 자세한 정보는 Amazon VPC 사용 설명서의 [DHCP 옵션 세트](#)를 참조하세요.

디렉터리에 대한 DHCP 옵션 세트를 생성하는 방법

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 [DHCP Options Sets]를 선택한 후 [Create DHCP options set]를 선택합니다.
3. DHCP 옵션 세트 생성 페이지에서 디렉터리에 대해 다음 값을 입력합니다.

이름

옵션 세트를 위한 옵션 태그입니다.

도메인 이름

corp.example.com 등 디렉터리의 정규화된 이름.

도메인 이름 서버

AWS제공된 디렉터리의 DNS 서버 IP 주소.

Note

[AWS Directory Service 콘솔](#) 탐색 창으로 가서 디렉터리를 선택한 후 올바른 디렉터리 ID를 선택하면 이들 주소를 찾을 수 있습니다.

NTP 서버

이 필드는 비워둡니다.

NetBIOS 이름 서버

이 필드는 비워둡니다.

NetBIOS 노드 유형

이 필드는 비워둡니다.

4. [Create DHCP options set]를 선택합니다. 새 DHCP 옵션 세트가 DHCP 옵션 목록에 나타납니다.
5. 새로운 DHCP 옵션 세트의 ID를 기록해 두세요(dopt-xxxxxxxx). 새 옵션 세트를 VPC와 연결할 때 필요합니다.

VPC와 연결된 DHCP 옵션 세트를 변경하려면

DHCP 옵션 세트를 생성한 후에는 이 옵션 세트를 수정할 수 없습니다. VPC에서 다른 DHCP 옵션 세트를 사용하도록 하려면 새 세트를 생성하여 VPC와 연결해야 합니다. DHCP 옵션을 전혀 사용하지 않도록 VPC를 설정할 수도 있습니다.

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 사용자 VPC(Your VPCs)를 선택합니다.
3. VPC를 선택한 다음 작업, VPC 설정 편집을 선택합니다.
4. DHCP 옵션 세트에서 옵션 세트를 선택하거나 DHCP 옵션 세트 없음을 선택한 후 저장을 선택합니다.

명령줄을 사용하여 VPC와 연결된 DHCP 옵션 세트를 변경하려면 다음을 참조하십시오.

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

Simple AD 디렉터리 관리

이 단원에서는 Simple AD 환경에 대해 일반적으로 실시되는 관리 작업을 유지 관리하는 방법을 설명합니다.

주제

- [Simple AD 삭제](#)
- [디렉터리 스냅샷 또는 복구](#)
- [디렉터리 정보 보기](#)

Simple AD 삭제

Simple AD를 삭제하면 디렉터리 데이터와 스냅샷이 모두 삭제되며 복구할 수 없습니다. 디렉터리가 삭제된 후에도 디렉터리에 조인된 모든 인스턴스는 변동 없이 보관됩니다. 그러나 디렉터리 자격 증명을 사용해서 이러한 인스턴스에 로그인할 수 없습니다. 인스턴스에 로컬인 사용자 계정을 통해 이러한 인스턴스에 로그인해야 합니다.

디렉터리를 삭제하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다. 현재 배포된 AWS 리전 위치에 Active Directory 있는지 확인하십시오. 자세한 내용은 [지역 선택](#)을 참조하십시오.
2. 삭제하려는 디렉터리에 대해 활성화된 AWS 응용 프로그램이 없는지 확인하십시오. 활성화된 AWS 응용 프로그램을 사용하면 AWS 관리형 Microsoft AD 또는 Simple AD를 삭제할 수 없습니다.
 - a. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
 - b. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다. AWS 앱 및 서비스 섹션에서 디렉터리에 사용할 수 있는 AWS 애플리케이션을 확인할 수 있습니다.
 - AWS Management Console 액세스를 비활성화합니다. 자세한 정보는 [AWS Management Console 액세스 비활성화](#)을 참조하세요.
 - WorkSpacesAmazon을 비활성화하려면 WorkSpaces 콘솔의 디렉터리에서 서비스 등록을 취소해야 합니다. 자세한 내용은 Amazon WorkSpaces 관리 가이드의 [디렉터리 등록 취소](#)를 참조하십시오.
 - WorkDocsAmazon을 비활성화하려면 Amazon WorkDocs 콘솔에서 Amazon WorkDocs 사이트를 삭제해야 합니다. 자세한 내용은 Amazon WorkDocs 관리 가이드의 [사이트 삭제](#)를 참조하십시오.
 - WorkMailAmazon을 비활성화하려면 Amazon WorkMail 콘솔에서 Amazon WorkMail 조직을 제거해야 합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 [조직 제거](#)를 참조하십시오.
 - Amazon FSx for Windows File Server를 비활성화하려면 도메인에서 Amazon FSx 파일 시스템을 제거해야 합니다. 자세한 내용은 Windows File Server용 Amazon [FSx 사용 설명서의 Windows File Server용 FSx 사용 설명서의 Windows](#) 파일 서버용 FSx 사용을 참조하십시오. Active Directory
 - Amazon 관계형 데이터베이스 서비스를 비활성화하려면 도메인에서 Amazon RDS 인스턴스를 제거해야 합니다. 자세한 내용은 Amazon RDS 사용 설명서의 [도메인에서 DB 인스턴스 관리하기](#) 단원을 참조하세요.

- AWS Client VPN 서비스를 비활성화하려면 Client VPN 엔드포인트에서 디렉터리 서비스를 제거해야 합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Active Directory [인증](#)을 참조하십시오.
- Amazon Connect를 비활성화하려면 Amazon Connect 인스턴스를 삭제해야 합니다. 자세한 정보는 Amazon Connect 관리자 안내서의 [Amazon Connect 인스턴스 삭제하기](#)를 참조하십시오.
- Amazon을 QuickSight 비활성화하려면 Amazon 구독을 취소해야 합니다. QuickSight 자세한 내용은 Amazon QuickSight 사용 설명서의 Amazon QuickSight [계정](#) 해지를 참조하십시오.

Note

삭제하려는 AWS Managed Microsoft AD 디렉터를 사용 AWS IAM Identity Center 중이고 이전에 연결한 적이 있는 경우 삭제하려면 먼저 ID 소스를 변경해야 합니다. 자세한 내용은 IAM Identity Center 사용 설명서의 [ID 소스 변경](#)을 참조하십시오.

3. 탐색 창에서 디렉터를 선택합니다.
4. 삭제할 디렉터리만 선택하고 [Delete]를 클릭합니다. 디렉터를 삭제하는 데 몇 분 정도 걸립니다. 삭제된 디렉터리는 디렉터리 목록에서 제거됩니다.

디렉터리 스냅샷 또는 복구

AWS Directory Service에서는 Simple AD 디렉터리에 대한 데이터의 수동 스냅샷을 만드는 기능을 제공합니다. 이 스냅샷은 디렉터리에 대한 point-in-time 복원을 수행하는 데 사용할 수 있습니다. AD Connector 디렉터리의 스냅샷은 가져올 수 없습니다.

주제

- [디렉터리의 스냅샷 생성](#)
- [스냅샷에서 디렉터리 복원](#)
- [스냅샷 삭제](#)

디렉터리의 스냅샷 생성

스냅샷은 스냅샷을 가져왔던 시점의 상태로 디렉터를 복원하는 데 사용할 수 있습니다. 디렉터리의 수동 스냅샷을 생성하려면 다음 단계를 수행합니다.

Note

각 디렉터리에 대한 수동 스냅샷은 수가 5개로 제한되어 있습니다. 이미 제한 값에 도달한 경우에는 기존의 수동 스냅샷 중 하나를 삭제해야만 또 다른 스냅샷을 생성할 수 있습니다.

수동 스냅샷을 생성하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 유지 관리 탭을 선택합니다.
4. 스냅샷섹션에서 작업을 선택한 후 스냅샷 생성을 선택합니다.
5. 원하는 경우 디렉터리 스냅샷 생성 대화 상자에 스냅샷 이름을 제공합니다. 준비가 되면 생성을 선택합니다.

디렉터리 크기에 따라 스냅샷 생성에 몇 분 정도 걸릴 수 있습니다. 스냅샷이 준비가 되면 상태 값이 Completed로 바뀝니다.

스냅샷에서 디렉터리 복원

스냅샷에서 디렉터리를 복원하는 것은 디렉터리를 시간을 되돌려 놓는 것과 같습니다. 디렉터리 스냅샷은 생성된 디렉터리 고유의 것입니다. 스냅샷이 생성된 디렉터리에만 스냅샷을 저장할 수 있습니다. 또한 수동 스냅샷의 최대 지원 기간은 180일입니다. 자세한 내용은 Microsoft 웹 사이트에서 [Active Directory의 시스템 상태 백업의 유효 수명](#)을 참조하세요.

Warning

스냅샷 복원을 수행하기 전에 [AWS Support 센터](#)에 문의하시는 것이 좋습니다. 문의하시면 스냅샷 복원이 필요하지 않도록 도와드릴 수 있습니다. 스냅샷 복원은 특정 시점이므로 데이터 손실이 발생할 수 있습니다. 복원 작업이 완료될 때까지 디렉터리에 연결된 모든 DC 및 DNS 서버가 오프라인 상태가 된다는 점에 유의하세요.

스냅샷에서 디렉터리를 복원하려면 다음 단계를 수행합니다.

스냅샷에서 디렉터리를 복원하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.

2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 유지 관리 탭을 선택합니다.
4. 스냅샷 섹션의 목록에서 스냅샷을 선택하고 작업을 선택한 후 스냅샷 복원을 선택합니다.
5. Restore directory snapshot(디렉터리 스냅샷 복원) 대화 상자에서 정보를 검토하고 복원을 선택합니다.

디렉터리의 경우 디렉터리를 복원하는 데 몇 분 정도 걸릴 수 있습니다. 성공적으로 복원되면 디렉터리의 상태 값이 Active로 바뀝니다. 디렉터리에 대한 모든 변경은 스냅샷 날짜가 덮어쓰기된 이후에 이루어집니다.

스냅샷 삭제

스냅샷을 삭제하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 유지 관리 탭을 선택합니다.
4. 스냅샷 섹션에서 작업을 선택한 후 스냅샷 삭제를 선택합니다.
5. 스냅샷을 삭제할지 확인한 다음 삭제를 선택합니다.

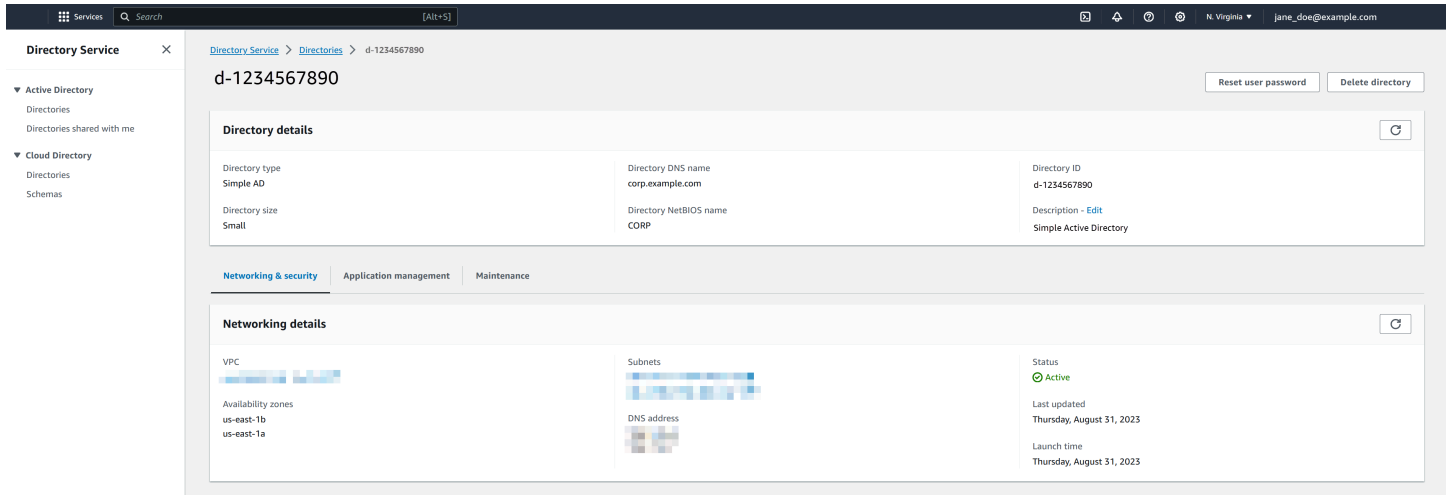
디렉터리 정보 보기

디렉터리에 대한 세부 정보를 볼 수 있습니다.

디렉터리에 대한 세부 정보 보기

1. [AWS Directory Service 콘솔](#) 탐색 창의 아래에서 Active Directory 디렉터리를 선택합니다.
2. 디렉터리에 대한 디렉터리 ID 링크를 클릭합니다. 디렉터리에 대한 정보가 디렉터리 세부 정보 페이지에 표시됩니다.

상태 필드에 대한 자세한 내용은 [디렉터리 상태 이해](#) 단원을 참조하세요.



AWS 애플리케이션 및 서비스에 대한 액세스 지원

사용자는 Simple AD에 WorkSpaces Amazon과 같은 AWS 애플리케이션 및 서비스에 액세스 권한을 부여하도록 승인할 수 있습니다. Active Directory, Simple AD에서 작동하도록 다음 AWS 응용 프로그램 및 서비스를 활성화하거나 비활성화할 수 있습니다.

AWS 애플리케이션/서비스	추가 정보...
Amazon Chime	자세한 내용은 Amazon Chime 관리 안내서 를 참조하세요.
아마존 WorkDocs	자세한 내용은 Amazon WorkDocs 관리 안내서 를 참조하십시오.
아마존 WorkMail	자세한 내용은 Amazon WorkMail 관리자 안내서 를 참조하십시오.
아마존 WorkSpaces	<p>에서 직접 Simple AD, AWS 관리형 Microsoft AD 또는 AD 커넥터를 만들 수 WorkSpaces 있습니다. Workspace를 생성할 때 고급 설정을 시작하면 됩니다.</p> <p>자세한 내용은 Amazon WorkSpaces 관리 안내서를 참조하십시오.</p>

AWS 애플리케이션/서비스	추가 정보...
AWS Management Console	자세한 설명은 AD 보안 인증을 사용한 AWS Management Console 액세스 활성화 섹션을 참조하세요.

일단 활성화가 되면 디렉터리에 대한 액세스 권한을 부여하고자 하는 애플리케이션 또는 서비스의 콘솔에서 디렉터리에 대한 액세스를 관리합니다. AWS Directory Service 콘솔에서 위에서 설명한 AWS 애플리케이션 및 서비스 링크를 찾으려면 다음 단계를 수행하십시오.

디렉터리에서 애플리케이션 및 서비스를 표시하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. AWS apps & services(앱 및 서비스) 섹션에서 목록을 검토합니다.

를 사용하여 AWS AWS Directory Service 응용 프로그램 및 서비스를 승인하거나 권한 부여를 해제하는 방법에 대한 자세한 내용은 [를 사용하는 AWS 애플리케이션 및 서비스에 대한 권한 부여 AWS Directory Service](#)

주제

- [액세스 URL 생성하기](#)
- [Single Sign-On](#)

액세스 URL 생성하기

액세스 URL은 디렉터리에 연결된 로그인 페이지에 도달하기 위해 Amazon WorkDocs 같은 AWS 애플리케이션 및 서비스에서 사용됩니다. URL은 전역적으로 고유해야 합니다. 다음 단계를 수행하여 디렉터리에 대한 액세스 URL을 생성할 수 있습니다.

⚠ Warning

이 디렉터리에 대한 애플리케이션 액세스 URL을 생성한 후에는 변경할 수 없습니다. 액세스 URL이 생성되고 난 후에는 다른 계정에서 이를 사용할 수 없습니다. 디렉터를 삭제하면 액세스 URL 역시 삭제가 되면서 다른 계정이 사용할 수 있게 됩니다.

액세스 URL 생성 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. 액세스 URL이 디렉터리에 할당되지 않은 경우 애플리케이션 액세스 URL 섹션에 생성 버튼이 표시됩니다. 디렉터리 별칭을 입력하고 생성을 선택합니다. 개체 이미 존재 오류가 반환되면 지정된 디렉터리 별칭이 이미 할당되었다는 뜻입니다. 또 다른 별칭을 선택하고 이 절차를 반복합니다.

액세스 URL이 *<alias>.awsapps.com* 형식으로 표시됩니다.

Single Sign-On

AWS Directory Service 사용자가 자격 증명을 별도로 입력할 필요 없이 디렉터리에 연결된 WorkDocs 컴퓨터에서 Amazon에 액세스할 수 있도록 하는 기능을 제공합니다.

Single Sign-On 기능을 활성화하려면 추가 단계를 수행하여 사용자의 웹 브라우저가 Single Sign-On을 지원하도록 해야 합니다. 사용자는 웹 브라우저 설정을 변경하여 Single Sign-On을 활성화해야 할 수도 있습니다.

i Note

Single Sign-On은 AWS Directory Service 디렉터리에 조인된 컴퓨터에 사용할 때만 작동합니다. 이 디렉터리에 조인되지 않은 컴퓨터에서는 사용할 수 없습니다.

디렉터리가 AD Connector 디렉터리이고 AD Connector 서비스 계정에 서비스 보안 주체 이름 속성을 추가하거나 제거할 권한이 없는 경우 아래의 5단계와 6단계에 대해 두 가지 옵션이 있습니다.

1. 계속 진행하면 AD Connector 서비스 계정에 서비스 보안 주체 이름 속성을 추가하거나 제거할 권한이 있는 디렉터리 사용자의 사용자 이름과 암호를 묻는 메시지가 표시됩니다. 이러한 자격 증명은

Single Sign-On을 활성화하는 목적으로만 사용되며 서비스에 저장되지 않습니다. AD Connector 서비스 계정 사용 권한은 변경되지 않습니다.

- AD Connector 서비스 계정이 자체적으로 서비스 주체 이름 특성을 추가 또는 제거할 수 있도록 권한을 위임할 수 있습니다. AD Connector 서비스 계정에 대한 사용 권한을 수정할 권한이 있는 계정을 사용하여 도메인에 가입된 컴퓨터에서 아래 PowerShell 명령을 실행할 수 있습니다. 아래 명령은 AD Connector 서비스 계정에 서비스 보안 주체 이름 속성을 추가 및 제거할 수 있는 기능을 제공합니다.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
  $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
  Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
  $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
  Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
  'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
  'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Amazon에서 싱글 사인온을 활성화 또는 비활성화하려면 WorkDocs

- [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
- [Directories] 페이지에서 디렉터리 ID를 선택합니다.
- 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
- 애플리케이션 액세스 URL 섹션에서 활성화를 선택하여 Amazon용 싱글 사인온을 활성화합니다. WorkDocs

활성화 버튼이 보이지 않으면 먼저 액세스 URL을 생성해야 이 옵션이 표시됩니다. 액세스 URL을 생성하는 자세한 방법은 [액세스 URL 생성하기](#)를 참조하세요.

5. 이 디렉터리에 대해 SSO(Single-Sign-On)를 활성화하시겠습니까? 대화 상자에서 활성화를 선택합니다. Single Sign-On이 디렉터리에서 활성화됩니다.
6. 나중에 WorkDocs Amazon에서의 SSO (Single Sign-On) 를 비활성화하려면 [Disable] 을 선택한 다음 [이 디렉터리에 대한 Single Sign-On 비활성화] 대화 상자에서 [비활성화] 를 다시 선택합니다.

주제

- [IE 및 Chrome에서의 Single Sign-On](#)
- [Firefox에서의 Single Sign-On](#)

IE 및 Chrome에서의 Single Sign-On

Microsoft Internet Explorer(IE) 및 Google Chrome 브라우저가 Single Sign-On을 지원하도록 하려면 클라이언트 컴퓨터에서 아래 절차를 수행해야 합니다.

- 액세스 URL(예: <https://<alias>.awsapps.com>)을 Single Sign-On이 승인된 사이트 목록에 추가합니다.
- 액티브 스크립팅을 활성화합니다 (). JavaScript
- 자동 로그인을 허용합니다.
- 통합 인증을 활성화합니다.

도메인 관리자나 사용자가 이러한 작업을 수동으로 수행하거나, 도메인 관리자가 그룹 정책 설정을 이용해 이러한 설정값을 변경할 수 있습니다.

주제

- [Windows에서의 Single Sign-On을 위한 수동 업데이트](#)
- [OS X에서 Single Sign-On의 수동 업데이트](#)
- [Single Sign-On을 위한 그룹 정책 설정](#)

Windows에서의 Single Sign-On을 위한 수동 업데이트

Windows 컴퓨터에서 Single Sign-On을 수동으로 활성화하려면 해당 컴퓨터에서 다음 단계를 수행합니다. 이러한 설정값 중 일부는 이미 올바르게 설정되어 있을 수 있습니다.

Windows에서 IE 또는 Chrome을 위한 Single Sign-On을 수동으로 활성화하는 방법

1. 인터넷 속성 대화 상자를 열려면 시작 메뉴를 선택하고 검색 상자에 Internet Options를 입력한 후 인터넷 옵션을 선택합니다.
2. 다음 단계를 수행하여 Single Sign-On이 승인된 사이트 목록에 액세스 URL을 추가합니다.
 - a. 인터넷 속성 대화 상자에서 보안 탭을 선택합니다.
 - b. 로컬 인트라넷을 선택하고 사이트를 선택합니다.
 - c. 로컬 인트라넷 대화 상자에서 고급을 선택합니다.
 - d. 웹 사이트 목록에 액세스 URL을 추가하고 닫기를 선택합니다.
 - e. 로컬 인트라넷 대화 상자에서 확인을 선택합니다.
3. 액티브 스크립팅을 활성화하려면 다음 단계를 수행합니다.
 - a. 인터넷 속성 대화 상자의 보안 탭에서 사용자 지정 수준을 선택합니다.
 - b. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 스크립팅까지 아래로 스크롤한 다음 액티브 스크립팅에서 활성화를 선택합니다.
 - c. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 확인을 선택합니다.
4. 자동 로그인을 활성화하려면 다음 단계를 수행합니다.
 - a. 인터넷 속성 대화 상자의 보안 탭에서 사용자 지정 수준을 선택합니다.
 - b. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 사용자 인증까지 아래로 스크롤한 다음 로그인에서 인트라넷 영역에서만 자동 로그인을 선택합니다.
 - c. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 확인을 선택합니다.
 - d. 보안 설정 - 로컬 인트라넷 영역 대화 상자에서 확인을 선택합니다.
5. 통합 인증을 활성화하려면 다음 단계를 수행합니다.
 - a. 인터넷 속성 대화 상자에서 고급 탭을 선택합니다.
 - b. 보안으로 스크롤하여 통합된 Windows 인증 사용을 선택합니다.

- c. 인터넷 속성 대화 상자에서 확인을 선택합니다.
6. 이러한 변경 사항이 적용되도록 브라우저를 닫았다가 다시 엽니다.

OS X에서 Single Sign-On의 수동 업데이트

OS X에서 Chrome을 위해 Single Sign-On을 수동으로 활성화하려면 해당 컴퓨터에서 다음 단계를 수행합니다. 이 단계를 완료하려면 컴퓨터에서 관리자 권한이 필요합니다.

OS X 기반 Chrome에서 Single Sign-On을 수동으로 활성화하는 방법

1. 다음 명령을 실행하여 [AuthServerAllowlist](#) 정책에 액세스 URL을 추가합니다.

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. 시스템 기본 설정을 열고 프로필 패널로 이동하여 Chrome Kerberos Configuration 프로필을 삭제합니다.
3. Chrome을 다시 시작하고 Chrome에서 `chrome://policy`을 열어 새로운 설정이 올바르게 되었는지 확인합니다.

Single Sign-On을 위한 그룹 정책 설정

도메인 관리자는 그룹 정책 설정을 실행하여 도메인에 조인된 클라이언트 컴퓨터에서 Single Sign-On을 변경할 수 있습니다.

Note

Chrome 정책을 사용하여 도메인의 컴퓨터에서 Chrome 웹 브라우저를 관리하는 경우 [AuthServerAllowlist](#) 정책에 액세스 URL을 추가해야 합니다. Chrome 정책 설정에 대한 자세한 내용은 [Chrome의 정책 설정](#)을 참조하세요.

그룹 정책 설정을 사용하여 IE 또는 Chrome을 위한 Single Sign-On 활성화하는 방법

1. 다음 단계를 수행하여 그룹 정책 객체를 새로 생성합니다.
 - a. 그룹 정책 관리 도구를 열고 도메인을 탐색한 후 그룹 정책 객체를 선택합니다.
 - b. 메인 메뉴에서 작업을 선택한 후 새로 만들기를 선택합니다.

- c. 새 GPO 대화 상자에서 그룹 정책 객체를 설명하는 이름(예: IAM Identity Center Policy)을 입력하고 원본 스타터 GPO 설정은 (없음)으로 유지합니다. 확인을 클릭합니다.
2. 다음 단계를 수행하여 Single Sign-On이 승인된 사이트 목록에 액세스 URL을 추가합니다.
 - a. 그룹 정책 관리 도구에서 도메인을 탐색한 후 그룹 정책 객체를 선택하고 IAM Identity Center 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열어 편집을 선택합니다.
 - b. 정책 트리에서 사용자 구성 > 기본 설정 > Windows 설정으로 이동합니다.
 - c. Windows 설정 목록에서 레지스트리의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 새 레지스트리 항목을 선택합니다.
 - d. 새 레지스트리 속성 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.

Action

Update

Hive

HKEY_CURRENT_USER

경로

Software\Microsoft\Windows\CurrentVersion\Internet Settings
 \ZoneMap\Domains\awsapps.com*<alias>*

*<alias>*의 값은 액세스 URL에서 파생됩니다. 액세스 URL이 https://
 examplecorp.awsapps.com이면 별칭이 examplecorp이고 레지스트리 키가
 Software\Microsoft\Windows\CurrentVersion\Internet Settings
 \ZoneMap\Domains\awsapps.com\examplecorp가 됩니다.

값 이름

https

값 유형

REG_DWORD

값 데이터

1

3. 액티브 스크립팅을 활성화하려면 다음 단계를 수행합니다.

- a. 그룹 정책 관리 도구에서 도메인을 탐색한 후 그룹 정책 객체를 선택하고 IAM Identity Center 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열어 편집을 선택합니다.
 - b. 정책 트리에서 컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > Internet Explorer > 인터넷 제어판 > 보안 페이지 > 인트라넷 영역으로 이동합니다.
 - c. 인트라넷 영역 목록에서 액티브 스크립팅 허용의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 편집을 선택합니다.
 - d. 액티브 스크립팅 허용 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.
 - 사용 라디오 버튼을 선택합니다.
 - 옵션에서 액티브 스크립팅 허용을 사용으로 설정합니다.
4. 자동 로그인을 활성화하려면 다음 단계를 수행합니다.
- a. 그룹 정책 관리 도구를 열고 도메인을 탐색한 다음, 그룹 정책 객체를 선택하고 SSO 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 편집을 선택합니다.
 - b. 정책 트리에서 컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > Internet Explorer > 인터넷 제어판 > 보안 페이지 > 인트라넷 영역으로 이동합니다.
 - c. 인트라넷 영역 목록에서 로그온 옵션의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 편집을 선택합니다.
 - d. 로그온 옵션 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.
 - 사용 라디오 버튼을 선택합니다.
 - 옵션에서 로그온 옵션을 인트라넷 영역에서만 자동으로 로그온으로 설정합니다.
5. 통합 인증을 활성화하려면 다음 단계를 수행합니다.
- a. 그룹 정책 관리 도구에서 도메인을 탐색한 후 그룹 정책 객체를 선택하고 IAM Identity Center 정책의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열어 편집을 선택합니다.
 - b. 정책 트리에서 사용자 구성 > 기본 설정 > Windows 설정으로 이동합니다.
 - c. Windows 설정 목록에서 레지스트리의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 새 레지스트리 항목을 선택합니다.
 - d. 새 레지스트리 속성 대화 상자에서 다음 설정을 입력하고 확인을 선택합니다.

Action

Update

Hive

HKEY_CURRENT_USER

경로

Software\Microsoft\Windows\CurrentVersion\Internet Settings

값 이름

EnableNegotiate

값 유형

REG_DWORD

값 데이터

1

6. 그룹 정책 관리 편집기 창이 아직 열려 있으면 닫습니다.
7. 이 단계에 따라 도메인에 새 정책을 할당합니다.
 - a. 그룹 정책 관리 트리에서 도메인의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 기존 GPO 연결을 선택합니다.
 - b. 그룹 정책 객체 목록에서 IAM Identity Center 정책을 선택하고 확인을 선택합니다.

다음에 클라이언트에서 그룹 정책이 업데이트되고 나서, 또는 다음에 사용자가 로그인할 때 이러한 변경 사항이 적용됩니다.

Firefox에서의 Single Sign-On

Mozilla Firefox 브라우저가 Single Sign-On을 지원하도록 하려면 액세스 URL(예: <https://<alias>.awsapps.com>)을 Single Sign-On이 승인된 사이트 목록에 추가합니다. 수동 추가나 스크립트를 통한 자동 추가가 가능합니다.

주제

- [Single Sign-On의 수동 업데이트](#)
- [Single Sign-On의 자동 업데이트](#)

Single Sign-On의 수동 업데이트

Firefox에서 승인된 사이트 목록에 액세스 URL을 수동으로 추가하려면 클라이언트 컴퓨터에서 다음 단계를 수행합니다.

Firefox에서 승인된 사이트 목록에 액세스 URL을 수동으로 추가하는 방법

1. Firefox를 열고 `about:config` 페이지를 엽니다.
2. `network.negotiate-auth.trusted-uris` 기본 설정을 열고 사이트 목록에 액세스 URL을 추가합니다. 쉼표(,)를 사용해 여러 항목을 구분합니다.

Single Sign-On의 자동 업데이트

도메인 관리자는 스크립트를 사용해 네트워크 상의 모든 컴퓨터에서 Firefox `network.negotiate-auth.trusted-uris` 사용자 기본 설정에 액세스 URL을 추가할 수 있습니다. 자세한 내용은 <https://support.mozilla.org/en-US/questions/939037>을 참조하세요.

AD 보안 인증을 사용한 AWS Management Console에 대한 액세스 활성화

AWS Directory Service는 디렉터리 멤버에게 AWS Management Console에 대한 액세스 권한을 부여할 수 있도록 허용합니다. 기본적으로 디렉터리 멤버는 AWS 리소스에 액세스할 수 있는 권한이 없습니다. 디렉터리 멤버에게 IAM 역할을 할당하여 다양한 AWS 서비스 및 리소스에 대한 액세스 권한을 제공합니다. IAM 역할은 디렉터리 멤버가 보유하고 있는 서비스, 리소스, 액세스 수준을 정의합니다.

디렉터리 멤버에게 콘솔 액세스 권한을 부여할 수 있으려면 디렉터리가 액세스 URL을 가지고 있어야 합니다. 디렉터리 세부 정보를 확인하고 액세스 URL을 얻을 수 있는 자세한 방법은 [디렉터리 정보 보기](#)를 참조하세요. 액세스 URL을 생성하는 자세한 방법은 [액세스 URL 생성하기](#)를 참조하세요.

IAM 역할을 생성해서 디렉터리 멤버에게 할당하는 자세한 방법은 [사용자 및 그룹에게 AWS 리소스에 대한 액세스 권한 부여](#) 단원을 참조하세요.

주제

- [AWS Management Console 액세스 활성화](#)
- [AWS Management Console 액세스 비활성화](#)
- [로그인 세션 길이 설정](#)

관련 AWS 보안 블로그 문서

- [AWS Managed Microsoft AD 및 온프레미스 보안 인증을 사용하여 AWS Management Console에 액세스하는 방법](#)

AWS Management Console 액세스 활성화

기본적으로 디렉터리에서는 콘솔 액세스가 활성화되어 있지 않습니다. 디렉터리 사용자 및 그룹에 대해 콘솔 액세스를 활성화하려면 다음 단계를 수행합니다.

콘솔 액세스 활성화

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. AWS Management Console 섹션에서 활성화를 선택합니다. 콘솔 액세스는 현재 디렉터리에서 활성화되어 있습니다.

사용자가 액세스 URL을 통해 콘솔에 로그인할 수 있으려면 우선 역할에 사용자를 추가해야 합니다. IAM 역할에 사용자를 할당하는 방법은 [기존 역할에 사용자 또는 그룹 할당](#) 단원을 참조하세요. IAM 역할이 할당되고 나면 사용자는 액세스 URL을 이용해 콘솔에 액세스할 수 있습니다. 예를 들어 디렉터리 액세스 URL이 example-corp.awsapps.com이면 콘솔에 액세스하기 위한 URL은 <https://example-corp.awsapps.com/console/>입니다.

AWS Management Console 액세스 비활성화

디렉터리 사용자 및 그룹에 대해 콘솔 액세스를 비활성화하려면 다음 단계를 수행합니다.

콘솔 액세스를 비활성화하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. AWS Management Console 섹션에서 비활성화를 선택합니다. 콘솔 액세스는 현재 디렉터리에서 비활성화되어 있습니다.
5. 디렉터리 내 사용자나 그룹에 IAM 역할이 할당된 경우, 비활성화 버튼을 사용할 수 없을 수 있습니다. 이 경우 계속 진행하기 전에 디렉터리에 대한 모든 IAM 역할 할당을 제거해야 합니다. 여기에는 디렉터리에서 삭제된 사용자 또는 그룹에 대한 할당 (삭제된 사용자 또는 삭제된 그룹으로 표시됨)이 포함됩니다.

할당된 모든 IAM 역할이 삭제되고 나면 위의 단계들을 반복합니다.

로그인 세션 길이 설정

기본적으로 콘솔에 성공적으로 로그인하면 로그아웃이 되기 전까지 1시간 동안 세션을 이용할 수 있습니다. 그 이후에는 다시 로그인을 해야 다음 세션을 1시간 동안 이용할 수 있고, 1시간이 지나면 다시 로그아웃이 됩니다. 아래 절차를 통해 세션당 최대 12시간까지 연장이 가능합니다.

로그인 세션 길이를 설정하는 방법

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택합니다.
2. [Directories] 페이지에서 디렉터리 ID를 선택합니다.
3. 디렉터리 세부 정보 페이지에서 애플리케이션 관리 탭을 선택합니다.
4. AWS앱 및 서비스 섹션에서 AWSManagement Console(관리 콘솔)을 선택합니다.
5. AWS 리소스에 대한 액세스 관리 대화 상자에서 계속을 선택합니다.
6. IAM 역할에 사용자 및 그룹 할당 페이지의 로그인 세션 길이 설정에서 번호가 매겨진 값을 편집한 다음 저장을 선택합니다.

튜토리얼: 단순 AD 만들기 Active Directory

다음 자습서에서는 Simple AD Active Directory를 설정하는 데 필요한 모든 단계를 안내합니다. Simple AD를 Active Directory 빠르고 쉽게 시작할 수 있도록 하기 위한 것이지만 대규모 프로덕션 환경에서는 사용할 수 없습니다.

자습서 사전 요구 사항

이 튜토리얼은 다음과 같이 가정합니다.

- 활성 상태가 AWS 계정있습니다.
- Simple AD를 사용하려는 지역의 계정 Amazon VPC 한도에 도달하지 않았습니디. VPC에 대한 자세한 내용은 [Amazon VPC란 무엇입니까?](#) 를 참조하십시오. 및 [VPC의 서브넷은 Amazon VPC 사용 설명서](#)를 참조하십시오.
- 해당 지역에 CIDR이 인 기존 VPC가 없습니다. 10.0.0.0/16

자세한 정보는 [간단한 AD 사전 조건](#)을 참조하세요.

1단계: Simple AD용 Amazon VPC 생성 및 구성 Active Directory

Simple AD와 함께 사용할 Amazon VPC를 생성하고 구성합니다. 이 절차를 시작하기 전에 [자습서 사전 요구 사항](#)을 작성했는지 확인합니다.

Simple AD용 VPC 생성 Active Directory

두 개의 퍼블릭 서브넷이 있는 VPC를 생성합니다. AWS Directory Service VPC에 두 개의 서브넷이 필요하며 각 서브넷은 서로 다른 가용 영역에 있어야 합니다.

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. VPC 대시보드에서 Create VPC(VPC 생성)을 선택합니다.
3. VPC 설정에서 VPC 등을 선택합니다.
4. 이 필드를 다음과 같이 작성합니다.
 - 이름 태그 자동 생성에서 자동 생성을 선택한 상태로 유지합니다. 프로젝트를 ADS VPC로 변경합니다.
 - IPv4 CIDR 블록은 10.0.0.0/16이어야 합니다.
 - No IPv6 CIDR block 옵션을 선택한 상태로 유지합니다.
 - 테넌시는 기본값으로 유지되어야 합니다.
 - 그런 다음 Number of Availability Zones(AZs)에서 2를 선택합니다.
 - 퍼블릭 서브넷 수로 2를 선택합니다. 프라이빗 서브넷 수는 0으로 변경할 수 있습니다.
 - 서브넷 CIDR 블록 사용자 지정을 선택하여 퍼블릭 서브넷 IP 주소 범위를 구성합니다. 퍼블릭 서브넷 CIDR 블록은 10.0.0.0/20 및 10.0.16.0/20이어야 합니다.
5. VPC 생성을 선택합니다. VPC가 생성되는 데 몇 분 정도 걸립니다.

2단계: Simple AD 액티브 디렉터리 만들기

새 Simple AD Active Directory를 만들려면 다음 단계를 수행하십시오. 이 절차를 시작하기 전에 1단계: Simple AD용 Amazon VPC 생성 [자습서 사전 요구 사항](#) 및 구성에 명시된 사전 요구 사항을 완료했는지 확인하십시오. Active Directory

단순 AD 액티브 디렉터리를 만들려면

1. [AWS Directory Service 콘솔](#) 탐색 창에서 디렉터리를 선택한 후 디렉터리 설정을 선택합니다.
2. Select directory type(디렉터리 유형 선택) 페이지에서 Simple AD를 선택하고 다음을 선택합니다.
3. 디렉터리 정보 입력 페이지에서 다음 정보를 제공합니다.

디렉터리 크기

Small(스몰) 또는 Large(라지) 크기 옵션 중에서 선택합니다. 크기에 대한 자세한 내용은 [Simple AD](#) 단원을 참조하세요.

조직 이름

클라이언트 장치를 등록하는 데 사용할 디렉터리에 대한 고유한 조직 이름입니다.

이 필드는 시작 과정에서 디렉터리를 만드는 경우에만 사용할 수 WorkSpaces 있습니다.

디렉터리 DNS 이름

디렉터리를 위한 정규화된 이름(예: corp.example.com)입니다.

디렉터리 NetBIOS 이름

디렉터리의 짧은 이름(예: CORP)입니다.

관리자 암호

디렉터리 관리자의 암호입니다. 디렉터리 생성 프로세스에서는 사용자 이름 Administrator과 이 암호를 사용하여 관리자 계정을 생성합니다.

디렉터리 관리자 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 또한 다음 네 범주 중 세 개에 해당하는 문자를 1자 이상 포함해야 합니다.

- 소문자(a-z)
- 대문자(A-Z)
- 숫자(0-9)
- 영숫자 외의 특수 문자(~!@#\$%^&* _-+=`\|(){}[]:;'"<>,.?/)

[Confirm password]

관리자 암호를 다시 입력합니다.

디렉터리 설명

디렉터리에 대한 선택적 설명을 입력합니다.

4. VPC 및 서브넷 선택 페이지에서 다음 정보를 제공한 후 다음을 선택합니다.

VPC

디렉터리에 대한 VPC입니다

서브넷

도메인 컨트롤러에 대한 서브넷을 선택합니다. 두 서브넷이 서로 다른 가용 영역에 있어야 합니다.

5. 검토 및 생성 페이지에서 디렉터리 정보를 검토하고 필요한 사항을 변경합니다. 정보가 올바르면 디렉터리 생성을 선택합니다. 디렉터리를 생성하는 데 몇 분 정도 걸립니다. 생성이 완료되면 상태 값이 활성 상태로 변경됩니다.

Simple AD 모범 사례

다음은 문제를 방지하고 Simple AD를 최대한 활용하기 위해 고려해야 할 몇 가지 제안 및 지침입니다.

설정: 사전 조건

디렉터리를 생성하기 전에 여기 나온 가이드라인을 고려하세요.

디렉터리 유형이 올바른지 확인

AWS Directory Service 다른 AWS 서비스와 Microsoft Active Directory 함께 사용할 수 있는 다양한 방법을 제공합니다. 예산에 맞는 비용으로 필요한 기능을 갖춘 디렉터리 서비스를 선택할 수 있습니다.

- AWS Microsoft Active Directory용 디렉터리 서비스는 클라우드에서 Microsoft Active Directory 호스팅되는 기능이 풍부한 관리형 서비스입니다. AWS 사용자 5,000명 이상이고 AWS 호스팅된 디렉터리와 온-프레미스 디렉터리 간에 신뢰 관계를 설정해야 하는 경우 관리형 Microsoft AD를 사용하는 것이 가장 좋습니다.
- AD Connector는 단순히 기존 Active Directory 온-프레미스에 AWS 연결합니다. AD Connector는 AWS 서비스와 함께 기존의 온프레미스 디렉터리를 사용하고 싶을 때 가장 적합한 옵션입니다.
- Simple AD는 기본 Active Directory 호환성을 갖춘 소규모의 저렴한 디렉터리입니다. 5,000명 이하의 사용자, Samba 4 호환 애플리케이션, LDAP 인식 애플리케이션을 위한 LDAP 호환성을 지원합니다.

AWS Directory Service 옵션에 대한 자세한 비교는 [여기](#)를 참조하십시오. [무엇을 선택할 것인가](#)

VPC와 인스턴스가 올바르게 구성되도록 보장

디렉터리를 연결, 관리 및 사용하려면 디렉터리와 연관이 있는 VPC를 제대로 구성해야 합니다.

VPC 보안 및 네트워킹 요건에 대한 자세한 내용은 [AWS 관리형 Microsoft AD 사전 요구 사항](#), [AD Connector 사전 조건](#) 또는 [간단한 AD 사전 조건](#) 섹션을 참조하세요.

도메인에 인스턴스를 추가하는 경우에는 [Amazon EC2 인스턴스를 관리형 AWS 마이크로소프트 AD에 연결 Active Directory](#)에 설명된 대로 인스턴스에 대한 연결 및 원격 액세스가 가능한지 확인하세요.

한도에 유의

특정 디렉터리 유형에 대한 다양한 제한에 대해 알아봅니다. 가용 스토리지와 객체의 전체 크기가 디렉터리에 저장할 수 있는 객체 수에 대한 유일한 제한입니다. 선택한 디렉터리에 대한 자세한 내용은 [AWS Managed Microsoft AD 할당량](#), [AD Connector 할당량](#) 또는 [Simple AD 할당량](#) 섹션을 참조하세요.

디렉터리의 AWS 보안 그룹 구성 및 사용에 대해 알아보십시오.

AWS [보안 그룹](#)을 생성하여 디렉터리의 도메인 컨트롤러 [엘라스틱 네트워크 인터페이스](#)에 연결합니다. AWS 디렉터리에 대한 불필요한 트래픽을 차단하고 필요한 트래픽을 허용하도록 보안 그룹을 구성합니다.

디렉터리 보안 그룹 수정

디렉터리의 보안 그룹에 대해 보안을 수정하고 싶으면 수정할 수 있습니다. 단, 보안 그룹 필터링이 어떻게 작동하는지 완전히 이해하는 경우에만 이렇게 변경하세요. 자세한 내용은 Amazon EC2 사용 설명서의 [Linux 인스턴스용 Amazon EC2 보안 그룹](#)을 참조하세요. 잘못 변경하면 의도한 컴퓨터 및 인스턴스와의 통신이 끊길 수 있습니다. AWS 디렉터리에 포트를 추가로 열려고 하면 디렉터리 보안이 저하되므로 사용하지 않는 것이 좋습니다. [AWS 공동 책임 모델](#)을 자세히 검토하세요.

Warning

디렉터리의 보안 그룹을 사용자가 생성한 다른 EC2 인스턴스에 연결하는 것은 기술적으로 가능합니다. 하지만 이 AWS 방법을 사용하지 않는 것이 좋습니다. AWS 관리 디렉터리의 기능 또는 보안 요구 사항을 해결하기 위해 사전 공지 없이 보안 그룹을 수정해야 할 이유가 있을 수 있습니다. 그러한 변경은 디렉터리 보안 그룹과 연결된 모든 인스턴스에 영향을 미치며, 연결된 인스턴스의 작동이 중단될 수 있습니다. 또한 디렉터리 보안 그룹을 EC2 인스턴스와 연결하면 EC2 인스턴스에 잠재적 보안 위험이 생길 수 있습니다.

트러스트가 필요한 경우 AWS 관리형 Microsoft AD 사용

Simple AD는 신뢰 관계를 지원하지 않습니다. AWS Directory Service 디렉터리와 다른 디렉터리 간에 트러스트를 설정해야 하는 경우 Microsoft Active Directory용 AWS 디렉터리 서비스를 사용해야 합니다.

설정: 디렉터리 생성

여기에는 디렉터리를 생성할 때 고려해야 할 몇 가지 제안이 나와 있습니다.

관리자 ID 및 암호를 기억

디렉터리를 설정할 때 관리자 계정에 대한 암호를 제시합니다. 해당 계정 ID는 Simple AD의 관리자입니다. 이 계정에 대해 생성한 암호를 기억하세요. 그렇지 않으면 디렉터리에 객체를 추가할 수 없습니다.

AWS 응용 프로그램의 사용자 이름 제한을 이해하십시오.

AWS Directory Service 사용자 이름 구성에 사용할 수 있는 대부분의 문자 형식을 지원합니다. 그러나 Amazon WorkMail, WorkSpaces WorkDocs Amazon 또는 Amazon과 같은 AWS 애플리케이션에 로그인하는 데 사용되는 사용자 이름에는 문자 제한이 적용됩니다. QuickSight 이러한 제한 때문에 다음 문자는 사용할 수 없습니다.

- 공백
- 멀티바이트 문자
- !"#%&'()*+,-./:;<=>@[]^`{|}~

Note

@ 기호는 UPN 접미사 앞에서만 허용됩니다.

애플리케이션 프로그래밍

애플리케이션을 프로그래밍하기 전에 다음 사항을 고려하세요.

Windows DC 로케이터 서비스 사용

응용 프로그램을 개발할 때는 Windows DC 로케이터 서비스를 사용하거나 관리형 AWS Microsoft AD의 동적 DNS (DDNS) 서비스를 사용하여 도메인 컨트롤러 (DC)를 찾을 수 있습니다. 애플리케이션을 DC의 주소로 하드 코딩해서는 안 됩니다. DC 로케이터 서비스를 사용하면 디렉터리 로드를 확실히 분산할 수 있고 도메인 컨트롤러를 해당 배포에 추가하여 수평 조정을 활용할 수 있습니다. 애플리케이션을 고정 DC에 결합하고 이 DC가 패치 적용 또는 복구 과정을 거치는 경우, 애플리케이션은 남은 DC 중 하나를 사용하는 대신에 DC에 액세스할 수 있는 권한을 상실하게 됩니다. 뿐만 아니라 DC를 하드

코딩하면 단일 DC에 핫스팟이 발생할 수 있습니다. 심한 경우에는 핫스팟으로 인해 DC가 반응하지 않을 수 있습니다. 또한 이러한 경우 AWS 디렉터리 자동화로 인해 디렉터리가 손상된 것으로 표시되고 응답하지 않는 DC를 대체하는 복구 프로세스가 트리거될 수 있습니다.

프로덕션 단계로 넘어가기 전에 로드 테스트 실시

프로덕션 워크로드를 대표하는 객체 및 요청에 대해 랩 테스트를 실시하여 디렉터리가 애플리케이션의 로드와 맞게 조정되는지 확인해야 합니다. 추가 용량이 필요한 경우 고성능을 AWS Directory Service 위해 도메인 컨트롤러를 추가할 수 있는 Microsoft Active Directory를 사용해야 합니다. 자세한 정보는 [추가 도메인 컨트롤러 배포](#)를 참조하세요.

효율적인 LDAP 쿼리 사용

수천 개의 객체에 대해 도메인 컨트롤러에 광범위한 LDAP 쿼리를 수행하면 DC 하나에서 상당히 많은 CPU 주기가 사용되면서 핫스팟이 발생할 수 있습니다. 이는 쿼리 중에 동일한 DC를 공유하는 애플리케이션에 부정적인 영향을 미칠 수 있습니다.

Simple AD 할당량

일반적으로 스몰 Simple AD 디렉터리에는 500명 이상, 라지 Simple AD 디렉터리에는 5,000명을 초과해 사용자를 추가해서는 안 됩니다. 더 유연한 조정 옵션과 추가적인 Active Directory 기능을 원할 경우, 대신 AWS Directory Service for Microsoft Active Directory(Standard Edition 또는 Enterprise Edition) 사용을 고려하세요.

다음은 Simple AD의 기본 할당량입니다. 별도로 명시되지 않는 한 각 할당량은 리전별로 적용됩니다.

Simple AD 할당량

리소스	기본 할당량
Simple AD 디렉터리	10
수동 스냅샷 *	Simple AD당 5

* 수동 스냅샷 할당량은 변경할 수 없습니다.

Note

AWS 탄력적 네트워크 인터페이스(ENI)에는 퍼블릭 IP 주소를 연결할 수 없습니다.

Simple AD에 대한 애플리케이션 호환성 정책

Simple AD는 Samba를 구현한 것으로, Active Directory의 기본 기능 중 여러 가지를 제공합니다. Active Directory를 사용하는 사용자 지정 및 상업용 기성 애플리케이션의 규모가 크기 때문에 AWS에서는 타사 애플리케이션이 Simple AD와 호환되는지 여부에 대한 공식적인 확인이나 광범위한 확인을 수행하지 않으며 수행할 수도 없습니다. AWS는 발생할 수 있는 모든 잠재적 애플리케이션 설치 관련 문제를 해결하기 위해 고객과 협력하기는 하지만, 모든 애플리케이션이 Simple AD와 호환된다고, 또는 앞으로도 계속해서 호환된다고 보장할 수는 없습니다.

다음 타사 애플리케이션은 Simple AD와 호환됩니다.

- 다음 플랫폼을 기반으로 하는 Microsoft Internet Information Services (IIS):
 - Windows Server 2003 R2
 - Windows Server 2008 R1
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
- Microsoft SQL Server:
 - SQL Server 2005 R2 (Express, Web 및 Standard 에디션)
 - SQL Server 2008 R2 (Express, Web 및 Standard 에디션)
 - SQL Server 2012 (Express, Web 및 Standard 에디션)
 - SQL Server 2014 (Express, Web 및 Standard 에디션)
- Microsoft SharePoint:
 - SharePoint 2010 Foundation
 - SharePoint 2010 Enterprise
 - SharePoint 2013 Enterprise

고객은 실제 Active Directory에 기반으로 호환성 수준을 높이기 위해 AWS Microsoft Active Directory를 위한 디렉터리 서비스([AWS 매니지드 마이크로소프트 AD](#))를 사용하는 것을 선택할 수 있습니다.

Simple AD 문제 해결

다음은 디렉터리를 생성 또는 사용할 때 발생할 수 있는 일부 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

주제

- [암호 복구](#)
- [사용자를 Simple AD에 추가할 때 "KDC가 요청한 선택을 수행할 수 없음"이라는 오류가 발생하는 경우](#)
- [내 도메인에 조인된 인스턴스의 DNS 이름이나 IP 주소를 업데이트 할 수 없는 경우 \(DNS 동적 업데이트\)](#)
- [SQL Server 계정을 사용해 SQL Server에 로그인할 수 없는 경우](#)
- [디렉터리가 "Requested" 상태에 멈춰있는 경우](#)
- [디렉터리를 생성할 때 "AZ Constrained" 오류 메시지가 표시되는 경우](#)
- [일부 사용자들이 내 디렉터를 통해 인증을 할 수 없는 경우](#)
- [추가적인 리소스](#)
- [Simple AD 디렉터리 상태 사유](#)

암호 복구

사용자가 암호를 잊어버렸거나 Simple AD 또는 AWS Managed Microsoft AD 디렉터리에 로그인하는데 문제가 있는 경우 AWS Management Console, Windows PowerShell 또는 를 사용하여 암호를 재설정할 수 있습니다. AWS CLI

자세한 정보는 [사용자 암호 재설정](#)을 참조하세요.

사용자를 Simple AD에 추가할 때 "KDC가 요청한 선택을 수행할 수 없음"이라는 오류가 발생하는 경우

Samba CLI 클라이언트가 모든 도메인 컨트롤러에 'net' 명령을 올바르게 전송하지 않았을 때 발생할 수 있는 오류입니다. Simple AD 디렉터리에 사용자를 추가하면서 'net ads' 명령을 사용했을 때 이런 오류 메시지가 표시되었다면, S 인수를 사용하고 도메인 컨트롤러 중 하나의 IP 주소를 지정합니다. 그래도 오류가 발송하면 다른 도메인 컨트롤러를 시도해보세요. 또한 Active Directory 관리 도구를 사용, 디렉터리에 사용자를 추가할 수도 있습니다. 자세한 정보는 [Simple AD용 액티브 디렉터리 관리 도구 설치](#)을 참조하세요.

내 도메인에 조인된 인스턴스의 DNS 이름이나 IP 주소를 업데이트 할 수 없는 경우 (DNS 동적 업데이트)

Simple AD 도메인에서 DNS 동적 업데이트가 지원되지 않습니다. 도메인에 조인된 인스턴스에서 DNS Manager를 사용해 디렉터리를 연결하는 방식으로 직접 변경을 수행할 수 있습니다.

SQL Server 계정을 사용해 SQL Server에 로그인할 수 없는 경우

SQL Server 계정으로 Windows 2012 R2 EC2 인스턴스에서 실행 중인 SQL Server에 로그인하기 위해 SQL Server 계정으로 SSMS(SQL Server Management Studio)를 사용하려고 하면 오류 메시지가 뜰 수 있습니다. SSMS가 도메인 사용자 자격으로 실행이 되면 문제가 발생하고, 이로 인해 유효한 보안 인증이 제공되더라도 "Login failed for user"라는 오류 메시지가 뜰 수 있습니다. 이 문제는 알려진 AWS 문제이며 해결하기 위해 최선을 다하고 있습니다.

문제를 해결하기 위해 SQL Authentication 대신 Windows 인증을 통해 SQL Server에 로그인할 수 있습니다. 또는 Simple AD 도메인 사용자 대신 로컬 사용자 자격으로 SSMS를 시작합니다.

디렉터리가 "Requested" 상태에 멈춰있는 경우

"Requested" 상태에 5분 이상 멈춰있는 디렉터리가 있으면 이를 삭제하고 다시 생성해보세요. 문제가 지속될 경우 [AWS Support 센터](#)에 문의하세요.

디렉터리를 생성할 때 "AZ Constrained" 오류 메시지가 표시되는 경우

2012년 이전에 생성된 일부 AWS 계정은 디렉터리를 지원하지 AWS Directory Service 애플은 미국 동부 (버지니아 북부), 미국 서부 (캘리포니아 북부) 또는 아시아 태평양 (도쿄) 지역의 가용 영역에 액세스할 수 있습니다. 디렉터리를 생성할 때 이와 같은 오류 메시지가 표시되면 다른 가용 영역의 서브넷을 선택하고 디렉터리를 다시 생성해보세요.

일부 사용자들이 내 디렉터리를 통해 인증을 할 수 없는 경우

사용자 계정에서 Kerberos 사전 인증이 활성화되어 있어야 합니다. 이것이 새 사용자 계정에 대한 기본 설정이며 이를 변경해서는 안 됩니다. 이 설정에 대한 자세한 내용은 TechNet Microsoft의 [사전 인증](#)을 참조하십시오.

추가적인 리소스

다음 리소스는 작업할 때 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS 지식 센터](#) - 문제 해결에 도움이 되는 FAQ 및 기타 리소스 링크를 찾을 수 있습니다.
- [AWS 지원 센터](#) —기술 지원을 받을 수 있습니다.
- [AWS Premium 지원 센터](#) —프리미엄 기술 지원을 받을 수 있습니다.

주제

- [Simple AD 디렉터리 상태 사유](#)

Simple AD 디렉터리 상태 사유

디렉터리가 손상되거나 작동 불가능한 상태로 바뀌면 디렉터리 상태 메시지에 추가 정보가 포함됩니다. 상태 메시지는 AWS Directory Service 콘솔에 표시되거나 [DescribeDirectories](#) API에 의해 [DirectoryDescription.StageReason](#) 구성원에게 반환됩니다. 디렉터리 상태에 대한 자세한 내용은 [디렉터리 상태 이해](#)를 참조하세요.

다음은 Simple AD 디렉터리에 대한 상태 메시지입니다.

주제

- [디렉터리 서비스의 탄력적 네트워크 인터페이스가 연결되어 있지 않음](#)
- [인스턴스가 감지한 문제](#)
- [중요한 AWS Directory Service 예약 사용자가 디렉터리에서 누락](#)
- [중요한 AWS Directory Service 예약 사용자가 도메인 관리 그룹에 속해야 함](#)
- [중요 AWS Directory Service 예약 사용자가 비활성됨](#)
- [메인 도메인 컨트롤러가 모든 FSMO 역할을 맡고 있지 않음](#)
- [도메인 컨트롤러 복제 실패](#)

디렉터리 서비스의 탄력적 네트워크 인터페이스가 연결되어 있지 않음

설명

VPC와의 네트워크 연결을 설정하기 위해 디렉터리 생성 중에 자동으로 생성된 중요 ENI(탄력적 네트워크 인터페이스)가 디렉터리 인스턴스에 연결되지 않았습니니다. 이 디렉터리에서 지원하는 AWS 애플리케이션이 작동하지 않습니다. 이 디렉터리는 온프레미스 네트워크에 연결할 수 없습니다.

문제 해결

ENI가 분리되었어도 남아 있는 경우 AWS Support에 문의하세요. ENI를 삭제하면 문제를 해결할 수 없으며 디렉터리를 영구적으로 사용할 수 없습니다. 디렉터리를 삭제하고 새로 생성해야 합니다.

인스턴스가 감지한 문제

설명

이 인스턴스에서 내부 오류를 발견했습니다. 이 경우 일반적으로 모니터링 서비스가 손상된 인스턴스를 적극적으로 복구하려고 함을 나타냅니다.

문제 해결

대부분의 경우 일시적인 문제이며 디렉터리는 결국 활성 상태로 돌아갑니다. 문제가 계속되면 AWS Support에 추가 지원을 요청하세요.

중요한 AWS Directory Service 예약 사용자가 디렉터리에서 누락

설명

Simple AD가 생성되면 AWS Directory Service가 `AWSAdminD-xxxxxxxxxx`라는 이름의 디렉터리에서 서비스 계정을 생성합니다. 이 서비스 계정을 발견할 수 없을 때 이 오류 메시지가 뜹니다. 이 계정이 없으면 디렉터리가 사용 불가 상태가 되면서 AWS Directory Service가 디렉터리에서 관리 기능을 수행할 수 없습니다.

문제 해결

이 문제를 해결하려면 서비스 계정이 삭제되기 전에 생성했던 이전의 스냅샷으로 디렉터를 복구합니다. 하루에 한 번 Simple AD 디렉터리에 대한 스냅샷이 자동 생성됩니다. 계정이 삭제되고 5일이 지난 후부터는 이 계정이 존재하는 스냅샷으로 디렉터를 복구하는 것이 불가능할 수 있습니다. 이 계정이 존재하는 스냅샷에서 디렉터를 복구할 수 없는 경우에는 디렉터리가 영구적으로 사용할 수 없는 상태가 될 수 있습니다. 이때는 디렉터를 삭제하고 새로 생성해야 합니다.

중요한 AWS Directory Service 예약 사용자가 도메인 관리 그룹에 속해야 함

설명

Simple AD가 생성되면 AWS Directory Service가 AWSAdminD-xxxxxxxxxx라는 이름의 디렉터리에서 서비스 계정을 생성합니다. 이 서비스 계정이 Domain Admins 그룹의 멤버가 아니면 이 오류 메시지가 뜹니다. AWS Directory Service에게 유지 관리 및 복구 작업을 수행하는 데 필요한 권한(예: FSMO 역할 이동, 새 디렉터리 컨트롤러의 도메인 조인, 스냅샷에서 복구)을 부여하려면 이 그룹에 대한 멤버십이 필요합니다.

문제 해결

Active Directory 사용자 및 컴퓨터 도구를 사용해 서비스 계정을 Domain Admins 그룹에 다시 추가합니다.

중요 AWS Directory Service 예약 사용자가 비활성됨

설명

Simple AD가 생성되면 AWS Directory Service가 AWSAdminD-xxxxxxxxxx라는 이름의 디렉터리에서 서비스 계정을 생성합니다. 이 서비스 계정이 비활성화될 때 이 오류 메시지가 뜹니다. AWS Directory Service가 디렉터리에 대해 유지 관리 및 복구 작업을 수행할 수 있으려면 이 계정을 활성화해야 합니다.

문제 해결

Active Directory 사용자 및 컴퓨터 도구를 사용해 서비스 계정을 다시 활성화합니다.

메인 도메인 컨트롤러가 모든 FSMO 역할을 맡고 있지 않음

설명

Simple AD 디렉터리 컨트롤러가 모든 FSMO 역할을 맡고 있지는 않습니다. FSMO 역할이 올바른 Simple AD 디렉터리 컨트롤러에 속하지 않을 경우, AWS Directory Service는 특정 동작 및 기능을 보장할 수 없습니다.

문제 해결

Active Directory 도구를 사용해 FSMO 역할을 원래 작동 중인 디렉터리 컨트롤러로 다시 보냅니다. FSMO 역할 이동에 대한 자세한 내용은 <https://docs.microsoft.com/troubleshoot/windows-server/>

[identity/transfer-or-seize-fsmo-roles-in-ad-ds](#) 단원을 참조하세요. 이렇게 해도 문제가 해결되지 않으면 AWS Support에 연락해 도움을 받으세요.

도메인 컨트롤러 복제 실패

설명

Simple AD 디렉터리 컨트롤러를 또 다른 디렉터리로 복제하지 못하고 있습니다. 이 오류는 다음 문제 중 하나 이상으로 인해 발생할 수 있습니다.

- 디렉터리 컨트롤러에 대한 보안 그룹에서 올바른 포트가 열려있지 않습니다.
- 네트워크 ACL이 너무 제한적입니다.
- VPC 라우팅 테이블이 디렉터리 컨트롤러들 간에 네트워크 트래픽을 올바르게 라우팅하지 않습니다.
- 또 다른 인스턴스가 디렉터리의 도메인 컨트롤러로 승격되었습니다.

문제 해결

VPC 네트워크 요건에 대한 자세한 내용은 AWS Managed Microsoft AD [AWS 관리형 Microsoft AD 사전 요구 사항](#), AD Connector [AD Connector 사전 조건](#), Simple AD [간단한 AD 사전 조건](#) 단원을 참조하세요. 디렉터리에 알려지지 않은 도메인 컨트롤러가 있으면 이를 강등시켜야 합니다. VPC 네트워크가 제대로 설정되었는데도 오류가 계속되는 경우에는 AWS Support에 연락해서 도움을 받으세요.

보안 입력 AWS Directory Service

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 [AWS 규정 준수 프로그램](#)의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 [규정 준수 프로그램별 범위 내 AWS 서비스를 참조하십시오](#). AWS Directory Service
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 공동 책임 모델을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 AWS Directory Service됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 AWS Directory Service 충족하도록 구성하는 방법을 보여줍니다. 또한 AWS Directory Service 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

보안 주제

이 섹션에서는 다음 보안 주제를 찾을 수 있습니다.

- [ID 및 액세스 관리 대상 AWS Directory Service](#)
- [로그인 및 모니터링 AWS Directory Service](#)
- [규정 준수 검증의 대상 AWS Directory Service](#)
- [의 레질리언스 AWS Directory Service](#)
- [인프라 보안: AWS Directory Service](#)

추가 보안 주제

이 가이드에서는 다음과 같은 추가 보안 주제를 찾을 수 있습니다.

계정, 트러스트, AWS 리소스 액세스

- [관리자 계정에 대한 권한](#)
- [그룹 관리형 서비스 계정](#)
- [신뢰 관계 생성](#)
- [Kerberos 제한된 위임](#)
- [사용자 및 그룹에게 AWS 리소스에 대한 액세스 권한 부여](#)
- [를 사용하는 AWS 애플리케이션 및 서비스에 대한 권한 부여 AWS Directory Service](#)

디렉터리 보안 유지

- [AWS Managed Microsoft AD 디렉터리 보안 유지](#)
- [AD Connector 디렉터리 보안](#)

로깅 및 모니터링

- [AWS Managed Microsoft AD 모니터링](#)
- [AD Connector 디렉터리 모니터링](#)

복원성

- [AWS Managed Microsoft AD에 대한 패치 적용 및 유지 관리](#)

ID 및 액세스 관리 대상 AWS Directory Service

에 액세스하려면 요청을 인증하는 데 사용할 AWS 수 있는 자격 증명이 AWS Directory Service 필요합니다. 이러한 자격 증명에는 AWS Directory Service 디렉터리와 같은 AWS 리소스에 액세스할 수 있는 권한이 있어야 합니다. 다음 섹션에서는 사용 방법 [AWS Identity and Access Management \(IAM\)](#) 에 대한 세부 정보를 제공하고 리소스에 액세스할 수 있는 사용자를 제어하여 리소스를 보호하는 AWS Directory Service 데 도움이 됩니다.

- [인증](#)
- [액세스 제어](#)

인증

[IAM ID](#)를 AWS 사용하여 액세스하는 방법을 알아보십시오.

액세스 제어

요청을 인증하는 데 필요한 유효한 자격 증명을 보유할 수 있지만 권한이 없으면 리소스를 생성하거나 액세스할 수 없습니다. AWS Directory Service 예를 들어, AWS Directory Service 디렉터리를 만들거나 디렉터리 스냅샷을 만들 수 있는 권한이 있어야 합니다.

다음 섹션에서는 에 대한 권한을 관리하는 방법을 설명합니다 AWS Directory Service. 먼저 개요를 읽어 보면 도움이 됩니다.

- [AWS Directory Service 리소스에 대한 액세스 권한 관리 개요](#)
- [ID 기반 정책 \(IAM 정책\) 사용 대상 AWS Directory Service](#)
- [AWS Directory Service API 권한: 작업, 리소스, 조건 참조](#)

AWS Directory Service 리소스에 대한 액세스 권한 관리 개요

모든 AWS 리소스는 AWS 계정이 소유하며 리소스를 만들거나 액세스할 수 있는 권한은 권한 정책에 의해 관리됩니다. 계정 관리자는 IAM ID (즉, 사용자, 그룹, 역할) 에 권한 정책을 연결할 수 있으며 일부 서비스 (예:) 는 리소스에 권한 정책을 연결하는 것도 지원합니다. AWS Lambda

Note

계정 관리자 또는 관리자 사용자는 관리자 권한이 있는 사용자입니다. 자세한 내용은 IAM 사용 설명서의 [IAM 모범 사례](#)를 참조하십시오.

주제

- [AWS Directory Service 리소스 및 운영](#)
- [리소스 소유권 이해](#)
- [리소스 액세스 관리](#)
- [정책 요소 지정: 작업, 효과, 리소스, 보안 주체](#)
- [정책에서 조건 지정](#)

AWS Directory Service 리소스 및 운영

에서 AWS Directory Service 기본 리소스는 디렉터리입니다. AWS Directory Service 디렉터리 스냅샷 리소스도 지원합니다. 하지만 기존 디렉터리의 컨텍스트에서만 스냅샷을 생성할 수 있습니다. 따라서 스냅샷을 가리켜 하위 리소스라고 합니다.

다음 표에 나와 있는 것처럼 이러한 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결됩니다.

리소스 유형	ARN 형식
디렉터리	arn:aws:ds: <i>region</i> : <i>account-id</i> :directory/ <i>external-directory-id</i>
스냅샷	arn:aws:ds: <i>region</i> : <i>account-id</i> :snapshot/ <i>external-snapshot-id</i>

AWS Directory Service 적절한 리소스로 작업하기 위한 일련의 작업을 제공합니다. 사용 가능한 작업 목록은 [디렉터리 서비스 작업](#)을 참조하세요.

리소스 소유권 이해

리소스 소유자는 리소스를 만든 AWS 계정입니다. 즉, 리소스 소유자는 리소스를 생성하는 요청을 인증하는 보안 주체 (루트 계정, IAM 사용자 또는 IAM 역할) 의 계정입니다. AWS 다음 예에서는 이러한 작동 방식을 설명합니다.

- 계정의 루트 계정 자격 증명을 사용하여 디렉터리와 같은 리소스를 생성하는 경우 해당 AWS 계정이 해당 AWS Directory Service 리소스의 소유자가 됩니다. AWS
- AWS 계정에서 IAM 사용자를 생성하고 해당 사용자에게 AWS Directory Service 리소스를 생성할 권한을 부여하면 사용자도 AWS Directory Service 리소스를 생성할 수 있습니다. 하지만 사용자가 속한 AWS 계정이 리소스를 소유합니다.
- AWS 계정에서 리소스를 생성할 권한이 있는 IAM 역할을 생성하는 경우, 역할을 수입할 수 있는 사람은 누구나 AWS Directory Service 리소스를 생성할 수 있습니다. 역할이 속한 AWS 계정이 리소스를 소유합니다. AWS Directory Service

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 나타냅니다. 다음 섹션에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

Note

이 섹션에서는 다음과 같은 맥락에서 IAM을 사용하는 방법을 설명합니다. AWS Directory Service IAM 서비스에 대한 자세한 정보는 다루지 않습니다. IAM 설명서 전체 내용은 IAM 사용 설명서의 [IAM이란 무엇입니까?](#) 단원을 참조하십시오. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 참조](#)를 참조하세요.

IAM 자격 증명에 연결된 정책을 자격 증명 기반 정책 (IAM 정책) 이라고 하고 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다. AWS Directory Service ID 기반 정책 (IAM 정책) 만 지원합니다.

주제

- [자격 증명 기반 정책\(IAM 정책\)](#)
- [리소스 기반 정책](#)

자격 증명 기반 정책(IAM 정책)

정책을 IAM ID에 연계할 수 있습니다. 예를 들면, 다음을 수행할 수 있습니다:

- 계정 내 사용자 또는 그룹에 권한 정책 연결 — 계정 관리자는 특정 사용자와 관련된 권한 정책을 사용하여 해당 사용자에게 새 디렉터리와 같은 AWS Directory Service 리소스를 생성할 수 있는 권한을 부여할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) – ID 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다.

IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [액세스 관리](#) 단원을 참조하십시오.

다음 권한 정책은 사용자에게 Describe로 시작하는 모든 작업을 실행할 수 있는 권한을 부여합니다. 이러한 작업은 디렉터리 또는 스냅샷과 같은 AWS Directory Service 리소스에 대한 정보를 표시합니다. Resource요소의 와일드카드 문자 (*) 는 해당 계정이 소유한 모든 AWS Directory Service 리소스에 대해 해당 작업이 허용됨을 나타냅니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "*"
    }
  ]
}
```

에서 ID 기반 정책을 사용하는 방법에 대한 자세한 내용은 [AWS Directory Service](#)를 참조하십시오. [ID 기반 정책 \(IAM 정책\) 사용 대상 AWS Directory Service](#) 사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM User Guide의 [Identities \(users, groups, and roles\)](#)를 참조하십시오.

리소스 기반 정책

Amazon S3과 같은 다른 서비스도 리소스 기반 권한 정책을 지원합니다. 예를 들어 정책을 S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. AWS Directory Service 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 작업, 효과, 리소스, 보안 주체

서비스는 각 AWS Directory Service 리소스에 대해 API 작업 세트를 정의합니다. 자세한 정보는 [AWS Directory Service 리소스 및 운영](#)을 참조하십시오. 사용 가능한 API 작업 목록은 [디렉터리 서비스 작업을](#) 참조하십시오.

이러한 API 작업에 대한 권한을 부여하려면 정책에서 지정할 수 있는 작업 세트를 AWS Directory Service 정의하십시오. API 작업을 수행하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

다음은 기본 정책 요소입니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. AWS Directory Service 리소스의 경우 IAM 정책에서는 항상 와일드카드 문자 (*) 를 사용합니다. 자세한 정보는 [AWS Directory Service 리소스 및 운영](#)을 참조하십시오.
- 조치 – 조치 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 예를 들어, `ds:DescribeDirectories` 권한은 사용자에게 AWS Directory Service `DescribeDirectories` 작업 수행 권한을 허용합니다.
- 결과 – 사용자가 특정 작업을 요청할 때 결과를 지정합니다. 이 값은 허용 또는 거부일 수 있습니다. 명시적으로 리소스에 대한 액세스 권한을 부여(허용)하지 않는 경우, 액세스는 묵시적으로 거부됩니다.

다. 다른 정책에서 액세스 권한을 부여하는 경우라도 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 권한을 명시적으로 거부할 수도 있습니다.

- 보안 주체 – ID 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다. 리소스 기반 정책의 경우 권한을 받을 사용자, 계정, 서비스 또는 기타 엔티티를 지정합니다 (리소스 기반 정책에만 적용). AWS Directory Service 리소스 기반 정책을 지원하지 않습니다.

IAM 정책 구문 및 설명에 대해 자세히 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 참조](#) 단원을 참조하세요.

모든 AWS Directory Service API 작업과 해당 작업이 적용되는 리소스를 보여주는 표는 을 참조하십시오. [AWS Directory Service API 권한: 작업, 리소스, 조건 참조](#)

정책에서 조건 지정

권한을 부여할 때 액세스 정책 언어를 사용하여 조건이 적용되는 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 설명은 IAM 사용자 가이드의 [조건](#)을 참조하십시오.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. AWS Directory Service에만 해당되는 특정한 조건 키는 없습니다. 하지만 필요에 따라 사용할 수 있는 AWS 조건 키가 있습니다. 전체 AWS 키 목록은 IAM 사용 설명서의 [사용 가능한 글로벌 조건 키](#)를 참조하십시오.

ID 기반 정책 (IAM 정책) 사용 대상 AWS Directory Service

이 항목에서는 계정 관리자가 IAM 자격 증명(사용자, 그룹, 역할)에 권한 정책을 연결할 수 있는 자격 증명 기반 정책의 예를 제공합니다.

Important

먼저 리소스에 대한 액세스를 관리하는 데 사용할 수 있는 기본 개념과 옵션을 설명하는 소개 주제를 검토하는 것이 좋습니다. AWS Directory Service 자세한 정보는 [AWS Directory Service 리소스에 대한 액세스 권한 관리 개요](#)을 참조하세요.

이 주제의 섹션에서는 다음 내용을 학습합니다.

- [AWS Directory Service 콘솔 사용에 필요한 권한](#)

- [AWS 에 대한 관리형 \(사전 정의된\) 정책 AWS Directory Service](#)
- [고객 관리형 정책 예](#)
- [IAM 정책에 태그 사용](#)

다음은 권한 정책의 예입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDsEc2IamGetRole",
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "iam:GetRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:PutRolePolicy"
      ],
      "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
    },
    {
      "Sid": "AllowPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "cloudwatch.amazonaws.com"
      }
    }
  }
]
}

```

정책에는 다음이 포함되어 있습니다.

- 첫 번째 명령문은 AWS Directory Service 디렉터리 생성 권한을 부여합니다. AWS Directory Service 리소스 수준에서 이 특정 작업에 대한 권한을 지원하지 않습니다. 따라서 정책은 와일드카드 문자(*)를 Resource 값으로 지정합니다.
- 두 번째 설명문은 IAM 작업을 생성할 수 있는 권한을 부여합니다. 사용자 대신 IAM 역할을 읽고 생성하려면 IAM 작업에 대한 액세스 권한이 필요합니다. AWS Directory Service Resource 값의 끝에 있는 와일드카드 문자(*)는 설명문이 모든 IAM 역할에서 IAM 작업에 대한 권한을 허용함을 의미합니다. 이러한 권한을 특정 역할로 제한하려면 리소스 ARN에 있는 와일드카드 문자(*)를 특정 역할 이름으로 대체합니다. 자세한 내용은 [IAM 작업](#)을 참조하세요.
- 세 번째 명령문은 디렉터리 생성, 구성 및 삭제를 허용하는 AWS Directory Service 데 필요한 특정 Amazon EC2 리소스 세트에 권한을 부여합니다. Resource 값의 끝에 있는 와일드카드 문자(*)는 설명문이 모든 EC2 리소스나 하위 리소스에서 EC2 작업에 대한 권한을 허용함을 의미합니다. 이러한 권한을 특정 역할로 제한하려면 리소스 ARN에 있는 와일드카드 문자(*)를 특정 리소스 또는 하위 리소스로 대체합니다. 자세한 내용은 [Amazon EC2 작업](#)을 참조하세요.

ID 기반 정책에서는 권한을 가질 보안 주체를 지정하지 않으므로 이 정책은 Principal 요소를 지정하지 않습니다. 정책을 사용자에게 연결할 경우 사용자는 암시적인 보안 주체입니다. IAM 역할에 권한 정책을 연결할 경우 역할의 신뢰 정책에 식별된 보안 주체는 권한을 가집니다.

모든 AWS Directory Service API 작업과 해당 작업이 적용되는 리소스를 보여주는 표는 을 참조하십시오. [AWS Directory Service API 권한: 작업, 리소스, 조건 참조](#)

AWS Directory Service 콘솔 사용에 필요한 권한

사용자가 AWS Directory Service 콘솔을 사용하려면 이전 정책에 나열된 권한 또는 에 설명된 Directory Service 전체 액세스 역할 또는 Directory Service Read Only 역할에서 [AWS 에 대한 관리형 \(사전 정의된\) 정책 AWS Directory Service](#) 부여한 권한이 있어야 합니다.

최소 필수 권한보다 더 제한적인 IAM 정책을 만들면 콘솔은 해당 IAM 정책에 연결된 사용자에게 대해 의도대로 작동하지 않습니다.

AWS 에 대한 관리형 (사전 정의된) 정책 AWS Directory Service

AWS 에서 생성하고 관리하는 독립형 IAM 정책을 제공하여 많은 일반적인 사용 사례를 해결합니다. AWS 관리형 정책은 사용자가 필요한 권한을 조사할 필요가 없도록 일반 사용 사례에 필요한 권한을 부여합니다. 자세한 내용은 IAM User Guide의 [AWS managed policies](#)를 참조하세요.

계정의 사용자에게 연결할 수 있는 다음과 같은 AWS 관리형 정책은 다음과 같은 경우에만 적용됩니다. AWS Directory Service

- `AWSDirectoryServiceReadOnlyAccess`— 사용자 또는 그룹에게 루트 계정의 모든 AWS Directory Service 리소스, EC2 서브넷, EC2 네트워크 인터페이스, Amazon Simple Notification Service (Amazon SNS) 주제 및 구독에 대한 읽기 전용 액세스 권한을 부여합니다. AWS 자세한 정보는 [AWS Directory Service에서의 AWS 관리형 정책 사용](#)을 참조하세요.
- `AWSDirectoryServiceFullAccess` - 사용자 또는 그룹에 다음을 부여합니다.
 - 전체 액세스 권한: AWS Directory Service
 - 사용하는 데 필요한 주요 Amazon EC2 서비스에 대한 액세스 AWS Directory Service
 - Amazon SNS 주제를 나열할 권한
 - 이름이 "DirectoryMonitoring" 로 시작하는 Amazon SNS 주제를 생성, 관리 및 삭제할 수 있음

자세한 정보는 [AWS Directory Service에서의 AWS 관리형 정책 사용](#)을 참조하세요.

또한 다른 IAM 역할과 함께 사용하기에 적합한 다른 AWS 관리형 정책도 있습니다. 이러한 정책은 AWS Directory Service 디렉터리의 사용자와 관련된 역할에 할당됩니다. 이러한 정책은 해당 사용자가 Amazon EC2와 같은 다른 AWS 리소스에 액세스하는 데 필요합니다. 자세한 정보는 [사용자 및 그룹에게 AWS 리소스에 대한 액세스 권한 부여](#)을 참조하세요.

사용자에게 필요한 API 작업 및 리소스에 액세스하도록 허용하는 사용자 지정 IAM 정책을 생성할 수도 있습니다. 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 사용자 지정 정책을 연결할 수 있습니다.

고객 관리형 정책 예

이 섹션에서는 다양한 AWS Directory Service 작업에 대한 권한을 부여하는 사용자 정책의 예를 확인할 수 있습니다.

Note

모든 예에서는 미국 서부(오리건) 리전(us-west-2)을 사용하며 가상의 계정 ID를 포함합니다.

예제

- [예 1: 사용자가 모든 AWS Directory Service 리소스에서 모든 Describe 작업을 수행하도록 허용](#)
- [예제 2: 사용자에게 디렉터리 생성 허용](#)

예 1: 사용자가 모든 AWS Directory Service 리소스에서 모든 Describe 작업을 수행하도록 허용

다음 권한 정책은 사용자에게 Describe로 시작하는 모든 작업을 실행할 수 있는 권한을 부여합니다. 이러한 작업은 디렉터리 또는 스냅샷과 같은 AWS Directory Service 리소스에 대한 정보를 표시합니다. Resource요소의 와일드카드 문자 (*) 는 해당 계정이 소유한 모든 AWS Directory Service 리소스에 대해 해당 작업이 허용됨을 나타냅니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "*"
    }
  ]
}
```

예제 2: 사용자에게 디렉터리 생성 허용

다음 권한 정책은 사용자가 디렉터리와 스냅샷, 신뢰 같은 기타 모든 관련 리소스를 생성하도록 허용하는 권한을 부여합니다. 이를 위해서는 특정 Amazon EC2 서비스에 대한 권한도 필요합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

        "ds:Create*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource": "*"
  ]
}

```

IAM 정책에 태그 사용

대부분의 API 작업에 사용하는 IAM 정책에서 태그 기반 리소스 수준 권한을 적용할 수 있습니다. AWS Directory Service 이를 통해 사용자가 생성, 수정 또는 사용할 수 있는 리소스를 더욱 정확하게 제어할 수 있습니다. 리소스 태그를 기반으로 사용자 액세스(권한)를 제어하기 위해 IAM 정책에서 다음 조건 컨텍스트 키 및 값과 함께 Condition 요소(Condition 블록)를 사용합니다.

- 특정 태그가 지정된 리소스에 대한 사용자 작업을 허용 또는 거부하려면 `aws:ResourceTag/tag-key: tag-value`를 사용합니다.
- 태그가 허용되는 리소스를 생성하거나 수정하기 위해 API 요청을 할 때 특정 태그를 사용하도록(또는 사용하지 않도록) 요구하려면 `aws:ResourceTag/tag-key: tag-value`를 사용합니다.
- 태그가 허용되는 리소스를 생성하거나 수정하기 위해 API 요청을 할 때 특정한 태그 키 세트를 사용하도록(또는 사용하지 않도록) 요구하려면 `aws:TagKeys: [tag-key, ...]`를 사용합니다.

Note

IAM 정책의 조건 컨텍스트 키와 값은 태깅 가능한 리소스의 ID가 필수 파라미터인 AWS Directory Service 작업에만 적용됩니다.

태그 사용에 대한 자세한 내용은 IAM 사용 설명서의 [Controlling access using tags\(태그를 사용한 액세스 제어\)](#)를 참조하세요. 이 설명서의 [IAM JSON 정책 참조](#) 단원에서는 IAM에서 JSON 정책의 자세한 구문과 설명, 요소의 예, 변수, 평가 로직을 설명합니다.

아래의 태그 정책 예에서는 태그 키값 쌍 "fooKey":"fooValue"가 포함되어 있는 한 모든 ds 호출을 허용합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"VisualEditor0",
      "Effect":"Allow",
      "Action":[
        "ds:*"
      ],
      "Resource":"*",
      "Condition":{"StringEquals":{"aws:ResourceTag/fooKey":"fooValue"}}
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:*"
      ],
      "Resource":"*"
    }
  ]
}
```

아래의 리소스 정책 예에서는 리소스에 디렉터리 ID "d-1234567890"이 포함되어 있는 한 모든 ds 호출을 허용합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"VisualEditor0",
      "Effect":"Allow",
```

```
    "Action":[
      "ds:*"
    ],
    "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
  },
  {
    "Effect":"Allow",
    "Action":[
      "ec2:*"
    ],
    "Resource":"*"
  }
]
```

ARN에 대한 자세한 내용은 [Amazon 리소스 이름 \(ARN\) 및 AWS 서비스 네임스페이스](#)를 참조하십시오.

태그 기반 리소스 수준 권한을 지원하는 AWS Directory Service API 작업의 다음 목록은 다음과 같습니다.

- [AcceptSharedDirectory](#)
- [AddIpRoutes](#)
- [AddTagsToResource](#)
- [CancelSchemaExtension](#)
- [CreateAlias](#)
- [CreateComputer](#)
- [CreateConditionalForwarder](#)
- [CreateSnapshot](#)
- [CreateLogSubscription](#)
- [CreateTrust](#)
- [DeleteConditionalForwarder](#)
- [DeleteDirectory](#)
- [DeleteLogSubscription](#)
- [DeleteSnapshot](#)
- [DeleteTrust](#)

- [DeregisterEventTopic](#)
- [DescribeConditionalForwarders](#)
- [DescribeDomainControllers](#)
- [DescribeEventTopics](#)
- [DescribeSharedDirectories](#)
- [DescribeSnapshots](#)
- [DescribeTrusts](#)
- [DisableRadius](#)
- [DisableSso](#)
- [EnableRadius](#)
- [EnableSso](#)
- [GetSnapshotLimits](#)
- [ListIpRoutes](#)
- [ListSchemaExtensions](#)
- [ListTagsForResource](#)
- [RegisterEventTopic](#)
- [RejectSharedDirectory](#)
- [RemoveIpRoutes](#)
- [RemoveTagsForResource](#)
- [ResetUserPassword](#)
- [RestoreFromSnapshot](#)
- [ShareDirectory](#)
- [StartSchemaExtension](#)
- [UnshareDirectory](#)
- [UpdateConditionalForwarder](#)
- [UpdateNumberOfDomainControllers](#)
- [UpdateRadius](#)
- [UpdateTrust](#)
- [VerifyTrust](#)

AWS Directory Service API 권한: 작업, 리소스, 조건 참조

[액세스 제어](#)를 설정하고 IAM ID에 연결할 수 있는 사용 권한 정책(ID 기반 정책)을 작성할 때 이 [AWS Directory Service API 권한: 작업, 리소스, 조건 참조](#) 표를 참조로 사용할 수 있습니다. 의 각 API 항목에는 다음이 포함됩니다.

- AWS Directory Service API 오퍼레이션의 이름
- 각 작업을 수행할 수 있는 권한을 부여할 수 있는 작업
- 권한을 부여할 수 있는 AWS 리소스

정책의 Action 필드에서 작업을 지정하고 정책의 Resource 필드에서 리소스 값을 지정합니다. 작업을 지정하려면 ds: 접두사 다음에 API 작업 명칭을 사용합니다(예: ds:CreateDirectory). 일부 AWS 애플리케이션은 정책에 ds:AuthorizeApplication, ds:CheckAlias, ds:CreateIdentityPoolDirectory, ds:GetAuthorizedApplicationDetails, ds:UpdateAuthorizedApplication, 및 ds:UnauthorizeApplication 같은 비공개 AWS Directory Service API 작업을 사용해야 할 수 있습니다.

일부 AWS Directory Service API는 를 통해서만 호출할 수 있습니다. AWS Management Console 프로그래밍 방식으로 호출할 수 없고 어떤 SDK에서도 제공되지 않는다는 점에서 퍼블릭 API가 아닙니다. 사용자 자격 증명을 수락합니다. 이러한 API 작업에는 ds:DisableRoleAccess, ds:EnableRoleAccess, 및 가 포함됩니다 ds:UpdateDirectory.

AWS Directory Service 정책에서 AWS 글로벌 조건 키를 사용하여 조건을 표현할 수 있습니다. 전체 AWS 키 목록은 IAM 사용 설명서의 [사용 가능한 글로벌 조건 키](#) 참조하십시오.

관련 항목

- [액세스 제어](#)

를 사용하는 AWS 애플리케이션 및 서비스에 대한 권한 부여 AWS Directory Service

액티브 AWS 디렉터리에서 애플리케이션 권한 부여

AWS Directory Service 응용 프로그램을 승인할 때 선택한 응용 프로그램이 Active Directory와 원활하게 통합될 수 있도록 특정 권한을 부여합니다. AWS 응용 프로그램에는 사용 사례에 필요한 액세스

스 권한만 부여됩니다. 승인 후 애플리케이션 및 Application Manager에게 부여되는 내부 권한 세트는 다음과 같습니다.

Note

새 AWS 애플리케이션을 Active Directory로 승인하려면 `ds:AuthorizationApplication` 권한이 필요합니다. 이 작업에 대한 권한은 Directory Service와의 통합을 구성하는 관리자에게만 제공되어야 합니다.

- AWS 관리형 Microsoft AD, Simple AD, AD Connector 디렉터리의 모든 OU (조직 구성 단위)에 있는 Active Directory 사용자, 그룹, 조직 구성 단위, 컴퓨터 또는 인증 기관 데이터에 대한 읽기 권한 (신뢰 관계에서 허용하는 경우) 및 AWS 관리형 Microsoft AD의 신뢰할 수 있는 도메인에 대한 읽기 액세스 권한
- AWS 관리형 Microsoft AD의 조직 단위에 있는 사용자, 그룹, 그룹 구성원, 컴퓨터 또는 인증 기관 데이터에 대한 쓰기 액세스 권한을 제공합니다. Simple AD의 모든 OU에 대한 쓰기 권한.
- 모든 디렉터리 유형에 대한 Active Directory 사용자의 인증 및 세션 관리.

Amazon RDS 및 Amazon FSx와 같은 일부 AWS 관리형 Microsoft AD 애플리케이션은 직접 네트워크 연결을 통해 액티브 디렉터리에 통합됩니다. 이 경우 디렉터리 상호 작용에는 LDAP 및 Kerberos와 같은 네이티브 Active Directory 프로토콜이 사용됩니다. 이러한 AWS 애플리케이션의 권한은 애플리케이션 인증 중에 AWS 예약 조직 단위 (OU)에서 생성된 디렉터리 사용자 계정에 의해 제어되며, 여기에는 애플리케이션용으로 생성된 사용자 지정 OU에 대한 모든 액세스 권한과 DNS 관리가 포함됩니다. 이 계정을 사용하려면 애플리케이션에서 발신자 보안 인증 또는 IAM 역할을 통해 `ds:GetAuthorizedApplicationDetails` 조치를 취할 수 있는 권한이 필요합니다.

AWS Directory Service API 권한에 대한 자세한 내용은 [을 참조하십시오](#) [AWS Directory Service API 권한: 작업, 리소스, 조건 참조](#).

AWS 관리형 Microsoft AD의 AWS 응용 프로그램 및 서비스 활성화에 대한 자세한 내용은 [을 참조하십시오](#) [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#). AD Connector용 AWS 응용 프로그램 및 서비스 활성화에 대한 자세한 내용은 [을 참조하십시오](#) [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#). Simple AD용 AWS 응용 프로그램 및 서비스 활성화에 대한 자세한 내용은 [을 참조하십시오](#) [AWS 애플리케이션 및 서비스에 대한 액세스 지원](#).

Active Directory에서 AWS 응용 프로그램 인증 해제하기

AWS 애플리케이션이 Active Directory에 액세스할 수 있는 권한을 제거하려면 해당 `ds:UnauthorizedApplication` 권한이 필요합니다. 애플리케이션에서 제공하는 단계에 따라 애플리케이션을 사용하지 않도록 설정합니다.

로그인 및 모니터링 AWS Directory Service

모범 사례로, 조직에서 변경 사항이 기록되고 있는지 모니터링합니다. 이렇게 하면 예상치 못한 변경 사항을 조사하고 원치 않는 변경 사항을 롤백할 수 있습니다. AWS Directory Service 현재 다음 두 AWS 서비스를 지원하므로 조직과 조직 내에서 발생하는 활동을 모니터링할 수 있습니다.

- Amazon CloudWatch - AWS 관리형 Microsoft AD 디렉터리 유형으로 CloudWatch 이벤트를 사용할 수 있습니다. 자세한 정보는 [로그 전송 활성화](#)를 참조하세요. 또한 CloudWatch 메트릭을 사용하여 도메인 컨트롤러 성능을 모니터링할 수 있습니다. 자세한 정보는 [CloudWatch 메트릭과 함께 도메인 컨트롤러를 추가할 시기를 결정하세요](#)를 참조하세요.
- AWS CloudTrail - 모든 AWS Directory Service 디렉터리 유형에 사용할 CloudTrail 수 있습니다. 자세한 내용은 [AWS Directory Service API 호출 로깅](#)을 참조하십시오 CloudTrail.

규정 준수 검증의 대상 AWS Directory Service

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면 AWS 서비스 규정 준수 [프로그램의 AWS 서비스 범위별, 규정](#) 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 [AWS 규정 준수 프로그램 AWS 보증 프로그램 규정 AWS](#) 참조하십시오.

를 사용하여 AWS Artifact 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 <https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html> 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- [보안 및 규정 준수 킷스타트 가이드](#) - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- [Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.](#)

Note

모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 [HIPAA 적격 서비스 참조](#)를 참조하십시오.

- [AWS 규정 준수 리소스AWS](#) — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- [AWS 고객 규정 준수 가이드](#) — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) — 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 [Security Hub 제어 참조](#)를 참조하십시오.
- [Amazon GuardDuty](#) — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- [AWS Audit Manager](#) — 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위협을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

의 레질리언스 AWS Directory Service

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워크로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS [지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS](#).

AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 수동 데이터 스냅샷을 언제든지 만들 수 있는 기능을 AWS Directory Service 제공합니다. 자세한 정보는 [디렉터리 스냅샷 또는 복구](#)를 참조하세요.

인프라 보안: AWS Directory Service

관리형 서비스로서 [Amazon Web Services: 보안 프로세스 개요](#) 백서에 설명된 [AWS 글로벌 네트워크 보안 절차에 따라](#) 보호됩니다. AWS Directory Service

AWS 게시된 API 호출을 사용하여 네트워크를 AWS Directory Service 통해 액세스할 수 있습니다. 클라이언트가 TLS(전송 계층 보안)를 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [Federal Information Processing Standard\(FIPS\) 140-2](#)를 참조하세요.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 [AWS Security Token Service\(AWS STS\)](#)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 예서 크로스 서비스 사칭으로 인해 AWS대리인 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

Microsoft Active Directory용 AWS Directory 서비스가 리소스에 다른 서비스에 부여하는 권한을 제한하려면 리소스 정책의 [aws:SourceArn](#) 및 [aws:SourceAccount](#) 글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. 만약 `aws:SourceArn` 값에 S3 버킷 ARN과 같은 계정 ID가 포함되어 있지 않은 경우, 권한을 제한하려면 두 전역 조건 컨텍스트 키를 모두 사용해야 합니다. 두 전역 조건

컨텍스트 키와 계정을 포함한 `aws:SourceArn` 값을 모두 사용하는 경우, `aws:SourceAccount` 값 및 `aws:SourceArn` 값의 계정은 동일한 정책 명령문에서 사용할 경우 반드시 동일한 계정 ID를 사용해야 합니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 `aws:SourceArn`을 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 `aws:SourceAccount`을 사용하세요.

다음 예제의 경우 의 값은 CloudWatch 로그 `aws:SourceArn` 그룹이어야 합니다.

혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn` 전역 조건 컨텍스트 키를 사용합니다. 예제: `arn:aws:service:*:123456789012:*`.

다음 예제는 AWS Managed Microsoft AD의 `aws:SourceArn` 및 `aws:SourceAccount` 글로벌 조건 컨텍스트 키를 사용하여 혼동되는 대리자 문제를 방지하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
        "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

```
}
}
```

다음 예에서는 `aws:SourceArn`의 값이 계정의 SNS 주제여야 합니다. 예를 들어 “ap-southeast-1”은 사용자 지역, “123456789012”는 고객 ID, “_d-966739499f”는 사용자가 생성한 아마존 SNS 주제 이름인 경우 등을 사용할 수 있습니다. `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` DirectoryMonitoring

혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn` 전역 조건 컨텍스트 키를 사용합니다. 예제: `arn:aws:servicename:*:123456789012:*`.

다음 예제는 AWS Managed Microsoft AD의 `aws:SourceArn` 및 `aws:SourceAccount` 글로벌 조건 컨텍스트 키를 사용하여 혼동되는 대리자 문제를 방지하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": ["SNS:GetTopicAttributes",
      "SNS:SetTopicAttributes",
      "SNS:AddPermission",
      "SNS:RemovePermission",
      "SNS>DeleteTopic",
      "SNS:Subscribe",
      "SNS:ListSubscriptionsByTopic",
      "SNS:Publish"],
    "Resource": [
      "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
          "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
```



```

    "aws:SourceAccount": "123456789012"
  }
}
}
}

```

다음 예는 콘솔 액세스 권한을 위임받은 역할에 대한 IAM 신뢰 정책을 보여줍니다. `aws:SourceArn`의 값은 계정의 디렉터리 리소스여야 합니다. 자세한 내용은 [에서 정의한 리소스 유형을](#) 참조하십시오 AWS Directory Service. 예를 들어, 123456789012이(가) 고객 ID이고 d-1234567890이(가) 디렉터리 ID인 경우 `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890`을(를) 사용할 수 있습니다.

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
      "sts:AssumeRole"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
          "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
}

```

인터페이스 엔드포인트를 사용하여 AWS Directory Service API에 액세스 - AWS PrivateLink

를 AWS PrivateLink 사용하여 VPC와 AWS Directory Service API 간에 프라이빗 연결을 생성할 수 있습니다. 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 연결을 사용하지 않고도 VPC에 있는 것처럼

럼 AWS Directory Service API에 액세스할 수 있습니다. AWS Direct Connect VPC의 인스턴스는 API에 액세스하는 AWS Directory Service 데 퍼블릭 IP 주소가 필요하지 않습니다.

AWS PrivateLink에서 제공되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 이는 AWS Directory Service로 향하는 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다.

자세한 내용은 AWS PrivateLink가이드의 [AWS 서비스AWS PrivateLink 액세스](#)를 참조하십시오.

에 대한 고려 사항 AWS Directory Service

AWS Directory Service API 엔드포인트의 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 [고려 사항](#)을 검토하십시오.

AWS Directory Service 인터페이스 엔드포인트를 통해 모든 API 작업에 대한 호출을 지원합니다.

가용성

AWS Directory Service 다음과 같은 VPC 엔드포인트를 지원합니다. AWS 리전

- 미국 동부(버지니아 북부)
- AWS GovCloud (미국 서부)
- AWS GovCloud (미국 동부)

에 대한 인터페이스 엔드포인트 생성 AWS Directory Service

Amazon VPC 콘솔 또는 AWS Command Line Interface () 를 사용하여 AWS Directory Service API용 인터페이스 엔드포인트를 생성할 수 있습니다. AWS CLI자세한 내용은 AWS PrivateLink 설명서의 [인터페이스 엔드포인트 생성](#)을 참조하십시오.

다음 서비스 이름을 사용하여 AWS Directory Service API용 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.ds
```

인터페이스 엔드포인트에 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 통해 AWS Directory Service API에 대한 전체 액세스를 허

용합니다. VPC에서 AWS Directory Service API에 허용된 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결하십시오.

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체 (AWS 계정, IAM 사용자, IAM 역할)
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은 AWS PrivateLink 가이드의 [엔드포인트 정책을 사용하여 서비스에 대한 액세스 제어를 참조](#)하십시오.

예: API 작업에 대한 AWS Directory Service VPC 엔드포인트 정책

다음은 사용자 지정 엔드포인트 정책의 예입니다. 이 정책을 인터페이스 엔드포인트에 연결하면 모든 리소스의 모든 보안 주체에 대해 나열된 AWS Directory Service 작업에 대한 액세스 권한이 부여됩니다. **##-1**, **##-2**, **##-3** 정책에 포함하려는 AWS Directory Service API에 필요한 권한으로 대체하십시오. 전체 목록은 [AWS Directory Service API 권한: 작업, 리소스, 조건 참조](#) 단원을 참조하십시오.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds:action-1",
        "ds:action-2",
        "ds:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Directory Service에 대한 서비스 수준 계약















AWS Directory Service는고가용성 서비스이며 AWS 관리형 인프라에서 구축됩니다. 이는 당사의 서비스 가용성 정책을 정의하는 서비스 수준 계약에 의해 뒷받침됩니다.

자세한 내용은 [AWS Directory Service에 대한 서비스 수준 계약](#)을 참조하세요.


지역 이용 가능 여부 AWS Directory Service













다음 표는 디렉터리 유형별로 어느 리전 엔드포인트가 지원되는지 설명하는 목록입니다.


지역명	리전	엔드포인트	프로토콜	AWS 관리형 마이크로소프트 AD	AD Connect	Simple AD
미국 동부 (오하이오)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 예	 예	 아 니요
미국 동부 (버지니아 북부)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 예	 예	 예
미국 서부 (캘리포니아 북부)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 예	 예	 아 니요
미국 서부 (오레곤)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 예	 예	 예
아프리카(케이프타운)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 예	 예	 아 니요

지역명	리전	엔드포인트	프로토콜	AWS 관리형 마이크로소프트 AD	AD Connect	Simple AD
아시아 태평양 (홍콩)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS			 아니요
아시아 태평양 (뭄바이)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS			 아니요
아시아 태평양 (하이데라바드)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS			 아니요
아시아 태평양 (오사카)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS			 아니요
아시아 태평양 (서울)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS			 아니요
아시아 태평양 (싱가포르)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS			 예

지역명	리전	엔드포인트	프로토콜	AWS 관리형 마이크로소프트 AD	AD Connect	Simple AD
아시아 태평양 (시드니)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 예	 예	 예
아시아 태평양 (자카르타)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 예	 예	 아니요
아시아 태평양 (멜버른)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 예	 예	 아니요
아시아 태평양 (도쿄)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 예	 예	 예
캐나다 (중부)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 예	 예	 아니요
캐나다 서부 (캘거리)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 예	 예	 아니요
중국 (베이징)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 예	 예	 아니요

지역명	리전	엔드포인트	프로토콜	AWS 관리형 마이크로소프트 AD	AD Connect	Simple AD
중국 (닝샤)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS			 아니요
유럽 (프랑크푸르트)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS			 아니요
유럽 (취리히)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS			 아니요
유럽 (아일랜드)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS			 예
유럽 (런던)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS			 아니요
Europe (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS			 아니요
유럽 (스톡홀름)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS			 아니요

지역명	리전	엔드포인트	프로토콜	AWS 관리형 마이크로소프트 AD	AD Connect	Simple AD
유럽 (밀라노)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS			 아니요
유럽 (스페인)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS			 아니요
이스라엘(텔아비브)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS			 아니요
중동 (바레인)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS			 아니요
중동 (UAE)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS			 아니요
남아메리카 (상파울루)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS			 아니요

지역명	리전	엔드포인트	프로토콜	AWS 관리형 마이크로소프트 AD	AD Connect	Simple AD
AWS GovCloud (미국 서부)	us-gov-west-1	광고. us-gov-west-1.amazonaws.com	HTTPS	 0-	 0-	 아 니요
AWS GovCloud (미국 동부)	us-gov-east-1	광고. us-gov-east-1.amazonaws.com	HTTPS	 0-	 0-	 아 니요

[AWS GovCloud \(미국 서부\) 지역 및 AWS GovCloud \(미국 동부\) AWS Directory Service 지역에서의 사용에 대한 자세한 내용은 서비스 엔드포인트를 참조하십시오.](#)

베이징 및 닝샤 AWS Directory Service 지역에서의 사용에 대한 자세한 내용은 중국 [Amazon Web Services](#)의 [엔드포인트 및 ARN](#)을 참조하십시오.

브라우저 호환성

AWS Amazon, Amazon Connect WorkSpaces WorkMail, Amazon Chime, Amazon 등과 같은 애플리케이션과 서비스는 AWS IAM Identity Center 모두 호환되는 브라우저의 유효한 로그인 자격 증명이 있어야 액세스할 수 있습니다. WorkDocs 다음 테이블에서는 로그인에 대해 호환되는 브라우저 버전과 브라우저만을 설명합니다.

브라우저	버전	호환성
Microsoft Edge	최신 3개 버전	호환됨
Mozilla Firefox	최신 3개 버전	호환됨
Google Chrome	최신 3개 버전	호환됨
Apple Safari	최신 3개 버전	호환됨

지원되는 브라우저 버전을 사용하고 있다는 것을 지금 확인하셨다면, 아래 섹션을 검토하여 사용하고 있는 브라우저가 AWS에서 요구하는 TLS(전송 계층 보안) 설정을 사용하도록 구성되어 있는지 확인해 보실 것을 권장합니다.

TLS란 무엇입니까?

TLS는 네트워크상에서 데이터를 안전하게 교환하기 위해 사용하는 프로토콜 웹 브라우저 및 다른 애플리케이션입니다. TLS는 원격 엔드포인트로의 연결이 암호화 및 엔드포인트 자격 증명 확인을 통해 의도된 엔드포인트 연결인지 확인합니다. 지금까지 TLS 버전은 TLS 1.0, 1.1, 1.2, 1.3입니다.

IAM Identity Center에서 지원하는 TLS 버전

AWS 애플리케이션 및 서비스는 보안 로그인을 위해 TLS 1.1, 1.2 및 1.3을 지원합니다. 2019년 10월 30일자로 TLS 1.0 버전이 더는 지원되지 않습니다. 따라서 모든 브라우저는 TLS 1.1 버전 이상을 지원하도록 구성되어야 합니다. 즉, TLS 1.0을 사용하는 동안에 AWS 애플리케이션 및 서비스에 액세스하는 경우, 로그인할 수 없습니다. 이러한 변경에 있어 지원을 받으려면, 관리자에게 문의하세요.

지원되는 TLS 버전을 브라우저에서 활성화하는 방법

사용하고 있는 브라우저에 따라 달라집니다. 보통 브라우저 설정에 있는 고급 설정 영역에서 이러한 설정을 찾을 수 있습니다. 예를 들어, 인터넷 익스플로러에서는 인터넷 속성, 고급 탭, 보안 섹션에서 다양한 TLS 옵션을 찾아볼 수 있습니다. 브라우저 제조업체 도움말 웹사이트에서 관련 지침을 확인하세요.

문서 기록

다음 표에서는 AWS Directory Service 관리자 가이드의 최신 릴리스 이후 변경된 중요 사항에 대해 설명합니다.

변경 사항	설명	날짜
인증서 기반 인증 설정	AWS 관리형 Microsoft AD의 두 가지 새로운 보안 설정에 대한 콘텐츠가 추가되었습니다.	2023년 4월 11일
AWS PrivateLink	AWS PrivateLink에 대한 콘텐츠를 추가했습니다.	2023년 3월 31일
Simple AD VPC 엔드포인트	구성하지 말아야 할 VPC 엔드포인트에 대한 콘텐츠를 추가했습니다.	2021년 8월 25일
AD Connector VPC 엔드포인트	구성하지 말아야 할 VPC 엔드포인트에 대한 콘텐츠를 추가했습니다.	2021년 8월 25일
스마트 카드 지원	AWS GovCloud (미국 서부) 지역의 스마트 카드 및 Amazon WorkSpaces 애플리케이션 관리자 지원에 대한 콘텐츠 추가	2020년 12월 1일
암호 재설정	AWS Management Console, Windows PowerShell 및 AWS CLI를 사용하여 사용자 암호를 재설정하는 방법에 대한 콘텐츠가 추가되었습니다.	2019년 1월 2일
디렉터리 공유	AWS 관리형 Microsoft AD에서 디렉터리 공유를 사용하는 방법에 대한 콘텐츠가 추가되었습니다.	2018년 9월 25일

콘텐츠를 새 Amazon Cloud Directory 개발자 안내서로 마이그레이션했습니다	Amazon Cloud Directory 콘텐츠를 이 안내서에서 새 Amazon Cloud Directory 개발자 안내서로 이동시켰습니다.	2018년 6월 21일
관리자 안내서 TOC 일괄 점검	고객이 필요한 것을 바로 찾을 수 있도록 목차를 재구성했습니다. 또한 필요한 경우 새 콘텐츠를 추가했습니다.	2018년 5월 4일
AWS 위임된 그룹	온-프레미스 사용자에게 할당할 수 있는 AWS 위임된 그룹 목록이 추가되었습니다.	2018년 3월 8일
세분화된 암호 정책	새로운 암호 정책에 대한 콘텐츠를 추가했습니다.	2017년 7월 5일
추가 도메인 컨트롤러	AWS 관리형 Microsoft AD에서 디렉터리에 도메인 컨트롤러를 추가하는 방법에 대한 콘텐츠가 추가되었습니다.	2017년 6월 30일
자습서	AWS 관리형 Microsoft AD 랩 환경을 테스트하기 위한 새 자습서가 추가되었습니다.	2017년 6월 21일
MFA (매니지드 AWS 마이크로소프트 AD 포함)	관리형 AWS Microsoft AD와 함께 MFA를 사용하는 방법에 대한 콘텐츠가 추가되었습니다.	2017년 2월 13일
Amazon Cloud Directory	새 디렉터리 유형에 대한 콘텐츠를 추가했습니다.	2017년 1월 26일
스키마 확장	Microsoft Active Directory용 AWS 디렉터리 서비스를 사용하여 스키마 확장에 대한 콘텐츠를 추가했습니다.	2016년 11월 14일

AWS Directory Service 관리자 안내서의 주요 개편	고객이 필요한 것을 바로 찾을 수 있도록 목차를 재구성했습니다.	2016년 11월 14일
SNS 알림	SNS 알림에 대한 콘텐츠를 추가했습니다.	2016년 2월 25일
인증 및 권한 부여	IAM을 AWS Directory Service 사용하는 방법에 대한 내용이 추가되었습니다.	2016년 2월 25일
AWS 관리형 마이크로소프트 AD	AWS 관리형 Microsoft AD 및 통합 가이드에 대한 콘텐츠를 단일 가이드에 추가했습니다.	2015년 17월 11일
Linux 인스턴스가 Simple AD 디렉터리에 조인될 수 있도록 허용	Linux 인스턴스를 Simple AD 디렉터리에 조인하는 방법에 대한 콘텐츠를 추가했습니다.	2015년 7월 23일
안내서 분리	AWS Directory Service 관리 안내서를 별도의 안내서로 나누었습니다.	2015년 7월 14일
Single Sign-On 지원	Single Sign-On 지원에 대한 콘텐츠를 추가했습니다.	2015년 3월 31일
새 안내서	이 안내서는 AWS Directory Service 관리 안내서의 첫 번째 릴리스입니다.	2014년 10월 21일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.