Red Hat Enterprise Linux 7

Windows 통합 가이드

Linux 시스템을 Active Directory 환경과 통합

Last Updated: 2023-03-18

Red Hat Enterprise Linux 7 Windows 통합 가이드

Linux 시스템을 Active Directory 환경과 통합

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

법적 공지

초록

이기종 IT 환경에는 원활한 통신이 필요한 다양한 도메인 및 운영 체제가 포함되어 있는 경우가 많습니다. Red Hat Enterprise Linux는 Microsoft Windows의 Active Directory (AD)와 Linux 도메인을 긴밀하게 통합할 수 있는 다양한 방법을 제공합니다. 사용자, 그룹, 서비스 또는 시스템을 포함하는 다른 도메인 개체에서 통합이 가능합니다. 이 가이드에서는 경량 AD 패스스루 인증에서 완전한 Kerberos 신뢰할 수 있는 영역에 이르기까지 다양한 통합 시나리오를 다룹니다. 본 가이드 외에도 Red Hat Enterprise Linux Identity Management와 관련된 기타 기능 및 서비스에 대한 설명서를 다음 가이드에서 확인할 수 있습니다. Linux 도메인 ID, 인증 및 정책 가이드문서 Red Hat Identity Management 문서 ID 저장소 및 Linux 기반 도메인에서 인증 및 권한 부여 정책을 관리하는 중앙 집중식 통합 방법을

제공하는 솔루션입니다. 시스템 수준 인증 가이드에서는 authconfig유틸리티, SSSD(System Security Services Daemon) 서비스, PAM(Pluggable Authentication Module) 프레임워크, Kerberos, certmonger유틸리티 및 애플리케이션에 대한 SSO(Single Sign-On) 등 로컬 시스템에서 인증을 구성할 수 있는 다양한 애플리케이션 및 서비스를 문서화합니다.

차례

1장. ACTIVEACTIVE DIRECTORY HAT;DIRECTORY 및 LINUX 환경 통합 방법

IT 환경에는 구성이 있습니다. 이러한 시스템은 목적에 따라 조정됩니다. 두 개의 개별 인프라를 통합하려면 각 환경의 용도를 평가하고 상호 작용하는 방법과 위치를 파악해야 합니다.

1.1. WINDOWS 통합 정의

Windows 통합은 Linux 환경과 Windows 환경 간의 필요한 상호 작용에 따라 매우 다른 것을 의미할 수 있습니다. 개별 Linux 시스템이 Windows 도메인에 등록되어 있거나 Linux 도메인이 Windows 도메인에 대한 피어가 되도록 구성되었거나 환경 간에 정보가 복사됨을 의미할 수 있습니다.

Windows 도메인과 Linux 시스템 간에는 몇 가지 연락처가 있습니다. 이러한 각 포인트는 서로 다른 도메인 개체(사용자, 그룹, 시스템, 서비스)와 해당 식별에 사용되는 서비스를 식별합니다.

사용자 **ID** 및 인증

- Windows(AD 도메인)에서 실행되는 중앙 인증 시스템 또는 Linux에서 실행되는 중앙 ID 및 인증 서버에서 사용자 계정이 위치합니까?
- Linux 시스템에서 인증된 사용자(로컬 Linux 인증 시스템 또는 Windows에서 실행되는 중앙 인증 시스템을 통해)는 무엇입니까?
- 사용자에 대해 그룹 멤버십이 어떻게 구성되어 있습니까? 그룹 멤버십이 어떻게 결정됩니까?
- 사용자는 사용자 이름/암호 쌍, Kerberos 티켓, 인증서 또는 방법 조합을 사용하여 인증합니까?
- Linux 시스템에서 서비스에 액세스하려면 POSIX 속성이 필요합니다. 이러한 속성은 어떻게 저장됩니까: Windows 도메인에 설정되었거나, Linux 시스템에서 로컬로 구성되거나, 동적으로 매핑(UID/GID 번호 및 Windows SIDs)으로 구성됩니까?
- 어떤 사용자가 어떤 리소스에 액세스합니까? Windows 정의 사용자는 Linux 리소스에 액세스합니까? Linux 정의 사용자는 Windows 리소스에 액세스합니까?

대부분의 환경에서 ActiveActive Directory HAT;Directory 도메인은 사용자 정보를 위한 중앙 허브이며, 이는 Linux 시스템이 인증 요청을 위해 해당 사용자 정보에 액세스할 수 있는 방법이 있어야 함을 의미합니다. 그런 다음 실제 문제는 해당 사용자 정보와 외부 시스템에서 사용할 수 있는 정보의 양을 얻는 방법입니다. *또한 Linux 시스템(POSIX 속성)과 Linux 사용자(애플리케이션 관리자)에 필요한 정보와 해당 정보를 관리하는 방법 간의 균형이 있어야 합니다.*

호스트 및 서비스 주체

- *어떤 리소스에 액세스됩니까?*
- *어떤 인증 프로토콜이 필요합니까?*
- *Kerberos 티켓은 어떻게 받을 수 있습니까? SSL 인증서를 요청하거나 확인하는 방법은 무엇입니까?*
- *사용자는 단일 도메인 또는 Linux 및 Windows 도메인에 모두 액세스해야 합니까?*

***DNS** 도메인, 쿼리 및 이름 확인*

- *DNS 구성은 무엇입니까?*
- *단일 DNS 도메인이 있습니까? 하위 도메인이 있습니까?*

- *시스템 호스트 이름은 어떻게 해결됩니까?*
- *서비스 검색을 어떻게 구성할 수 있습니까?*

보안 정책

- *Access Control instructions는 어디에 설정되어 있습니까?*
- *각 도메인에 대해 어떤 관리자가 구성되어 있습니까?*

변경 관리

- *시스템이 도메인에 얼마나 자주 추가됩니까?*
- *Windows 통합과 관련된 기본 구성이 변경되면(예: DNS 서비스) 이러한 변경 사항은 어떻게 전파됩니까?*
- *도메인 관련 도구 또는 프로비저닝 시스템을 통해 구성이 유지 관리됩니까?*
- *통합 경로에 Windows 서버에서 추가 애플리케이션 또는 구성이 필요합니까?*

도메인의 어떤 요소가 통합되는지와 마찬가지로 중요한 것은 통합을 유지하는 방법입니다. 특정 통합 장치가 매우 수동적이면 환경에 자주 업데이트되는 많은 시스템이 있는 경우 유지 관리 관점에서 해당 환경에서 작동하지 않을 수 있습니다.

다음 섹션에서는 Windows와의 통합의 주요 시나리오를 간략하게 설명합니다. 직접 통합에서 Linux 시스템은 추가 중개체 없이 Active Directory에 연결됩니다. 반면 간접 통합에는 Linux 시스템을 중앙에서 관리하고 전체 환경을 서버-서버 수준의 Active Directory에 연결하는 ID 서버가 포함됩니다.

1.2. 직접 통합

Linux 시스템을 AD(Active Directory)에 연결하려면 다음 두 가지 구성 요소가 필요합니다. 한 구성 요소는 중앙 ID 및 인증 소스와 상호 작용합니다. 이 경우 AD입니다. 다른 구성 요소는 사용 가능한 도메인을 감지하고 올바른 ID 소스를 사용하도록 첫 번째 구성 요소를 구성합니다. 정보를 검색하고 AD에 대한 인증을 수행하는 데 사용할 수 있는 다양한 옵션이 있습니다. 그 중에는 다음과 같습니다.

기본 LDAP 및 Kerberos PAM 및 NSS 모듈

*이러한 모듈 중에는 **nss_ldap**,**pam_ldap**, interval **_krb5** 입니다. PAM 및 NSS 모듈이 모든 애플리케이션 프로세스에 로드되므로 실행 환경에 직접적인 영향을 미칩니다. 캐싱, 오프라인 지원 또는 액세스 자격 증명을 충분히 보호하지 않으면 NSS에 대한 기본 LDAP 및 Kerberos 모듈을 사용하는 것이 제한적인 기능으로 인해 권장되지 않습니다.*

Samba Winbind

Samba Winbind는 Linux 시스템을 AD에 연결하는 기존의 방법이었습니다. winbind는 Linux 시스템에서 Windows 클라이언트를 에뮬레이션하고 AD 서버와 통신할 수 있습니다.

다음 사항에 유의하십시오.

- *Samba를 도메인 멤버로 구성한 경우 Winbind 서비스가 실행 중이어야 합니다.*
- *다중forest AD 설정에서 Winbind와 직접 통합하려면 양방향 신뢰가 필요합니다.*
- *Remote forests는 **idmap_ad** 플러그인이 원격 추정 사용자를 올바르게 처리할 수 있도록 로컬 오레스트를 신뢰해야 합니다.*

SSSD(System Security Services Daemon)

SSSD의 주요 기능은 시스템에 캐싱 및 오프라인 지원을 제공하는 공통 프레임워크를 통해 원격 ID 및 인증 리소스에 액세스하는 것입니다. SSSD는 구성 가능합니다. 로컬 사용자를 저장할 PAM 및 NSS 통합 및 중앙 서버에서 검색된 코어 및 확장 사용자 데이터를 저장하는 데이터베이스를 제공합니다. SSSD는 Linux 시스템을 선택한 ID 서버에 연결하는 것이 좋습니다. Red Hat Enterprise Linux의 Active Directory, IdM(Identity Management) 또는 일반 LDAP 또는 Kerberos 서버여야 합니다.

다음 사항에 유의하십시오.

- SSSD와의 직접 통합은 기본적으로 단일 AD forest 내에서만 작동합니다.
- Remote forests는 **idmap_ad** 플러그인이 원격 추정 사용자를 올바르게 처리할 수 있도록 로컬 오레스트를 신뢰해야 합니다.

Winbind에서 SSSD로 전환해야 하는 주요 이유는 SSSD를 직접 및 간접 통합에 사용할 수 있고 상당한 마이그레이션 비용 없이 한 통합 방법에서 다른 통합 방식으로 전환할 수 있다는 것입니다. Linux 시스템을 AD와 직접 통합하기 위해 SSSD 또는 Winbind를 구성하는 가장 편리한 방법은 **realmd** 서비스를 사용하는 것입니다. 호출자가 표준 방식으로 네트워크 인증 및 도메인 멤버십을 구성할 수 있습니다. **realmd** 서비스는 액세스 가능한 도메인 및 영역에 대한 정보를 자동으로 검색하고 도메인 또는 영역에 조인하기 위해 고급 구성이 필요하지 않습니다.

직접 통합은 Linux 시스템을 AD 환경에 도입하는 간단한 방법입니다. 그러나 Linux 시스템의 공유가 증가함에 따라 배포에서는 일반적으로 호스트 기반 액세스 제어, sudo 또는 SELinux 사용자 매핑과 같은 ID 관련 정책의 중앙 집중식 관리가 필요합니다. 처음에는 Linux 시스템의 이러한 측면의 구성을 로컬 구성 파일에서 유지 관리할 수 있습니다. 시스템 수가 증가함에 따라 Red Hat Satellite와 같은 프로비저닝 시스템을 사용하면 구성 파일의 배포 및 관리를 더 쉽게 수행할 수 있습니다. 이 방법을 사용하면 구성 파일을 변경한 다음 배포하는 오버헤드가 생성됩니다. 직접 통합이 더 이상 확장되지 않으면 다음 섹션에서 설명하는 간접 통합을 고려하는 것이 더 좋습니다.

1.2.1. 직접 통합을 위해 지원되는 Windows 플랫폼

다음 마스트 및 도메인 기능 수준을 사용하는 Linux 머신을 Active Directory 마이그레이드와 직접 통합할 수 있습니다.

- 포리스트 기능 수준 범위: Windows Server 2008 - Windows Server 2016[1]
- 도메인 기능 수준 범위: Windows Server 2008 - Windows Server 2016[1]

언급된 기능 수준을 사용하여 다음과 같은 지원되는 운영 체제에서 직접 통합이 테스트되었습니다.

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

1.3. 간접 통합

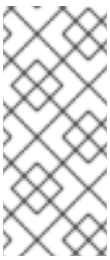
간접 통합의 주요 장점은 해당 시스템과 관련된 정책을 중앙에서 관리하는 동시에 AD(Active Directory) 도메인에서 Linux 시스템 및 서비스에 투명하게 액세스할 수 있도록 하는 것입니다. 간접 통합에는 두 가지 방법이 있습니다.

신뢰할 수 있는 솔루션

Red Hat Enterprise Linux의 IdM(Identity Management)을 중앙 서버로 활용하여 Linux 시스템을 제어한 다음 AD에서 교차 영역 Kerberos 트러스트를 구축할 수 있으므로 AD의 사용자가 SSO(Single Sign-

On)를 사용하여 Linux 시스템 및 리소스에 액세스할 수 있도록 하는 것이 좋습니다. 이 솔루션은 Kerberos 기능을 사용하여 서로 다른 ID 소스 간에 신뢰를 설정합니다. IdM은 AD에 별도의 오스트로 표시하며 AD에서 지원하는 스트레스트 수준 신뢰를 활용합니다.

복잡한 환경에서 단일 IdM 포리스트를 여러 AD 포리스트에 연결할 수 있습니다. 이 설정을 사용하면 조직의 다양한 기능에 대한 작업을 보다 효과적으로 분리할 수 있습니다. AD 관리자는 Linux 인프라를 완전히 제어하는 동안 사용자와 관련된 사용자 및 정책에 중점을 둘 수 있습니다. 이러한 경우 IdM에서 제어하는 Linux 영역은 AD 리소스 도메인 또는 영역과 유사하지만 Linux 시스템과 유사합니다.



참고

Windows에서 모든 도메인은 Kerberos 영역과 동시에 DNS 도메인입니다. 도메인 컨트롤러에서 관리하는 모든 도메인에는 자체 전용 DNS 영역이 있어야 합니다. IdM이 마이그레이드와 AD가 신뢰할 때에도 동일하게 적용됩니다. AD는 IdM에 자체 DNS 도메인이 있을 것으로 예상합니다. 신뢰 설정이 작동하려면 DNS 도메인이 Linux 환경 전용이어야 합니다.

신뢰 환경에서 IdM을 사용하면 ID 뷰 를 사용하여 IdM 서버에서 AD 사용자의 POSIX 속성을 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 8 장. Active Directory 환경에서 ID 뷰 사용
- 시스템 수준 인증 가이드 의 SSSD 클라이언트 측 뷰

동기화 기반 솔루션

신뢰 기반 솔루션의 대안은 IdM 또는 Red Hat Directory Server(RHDS)에서도 사용할 수 있는 사용자 동기화 기능을 활용하여 사용자 계정(및 RHDS를 사용하여 계정)을 AD에서 IdM 또는 RHDS로 동기화할 수 있도록 하는 것입니다. 그러나 반대 방향은 아닙니다. 사용자 동기화에는 다음을 포함한 특정 제한 사항이 있습니다.

- 사용자 중복
- AD 도메인의 모든 도메인 컨트롤러에 특수 구성 요소가 필요한 암호를 동기화해야 합니다.
- 비밀번호를 캡처하려면 모든 사용자가 먼저 수동으로 변경해야 합니다.
- 동기화는 단일 도메인만 지원
- AD에서 하나의 도메인 컨트롤러만 사용하여 데이터를 IdM 또는 RHDS 인스턴스 한 개와 동기화할 수 있습니다.

일부 통합 시나리오에서 사용자 동기화는 사용 가능한 유일한 옵션일 수 있지만 일반적으로 동기화 접근 방식을 사용하는 것은 교차 영역 신뢰 기반 통합을 권장하지 않습니다.

---

[1] Windows Server 2019는 새로운 기능 수준을 도입하지 않습니다. 가장 높은 기능 수준의 Windows Server 2019는 Windows Server 2016 입니다.

I 부. ACTIVE DIRECTORY 도메인에 단일 LINUX 시스템 추가

*이 부분에서는**SSSD**(System Security Services Daemon)가 Active Directory(**AD**) 도메인과 함께 작동하는 방법, **realmd** 시스템을 사용하여 직접 도메인 통합을 달성하는 방법, 마지막으로 **AD** 통합을 위해 **Samba**를 사용하는 방법에 대해 설명합니다.*

2 장. SSSD 의 ID 공급자로 ACTIVE DIRECTORY 사용

SSSD(System Security Services Daemon)는 원격 디렉터리 및 인증 메커니즘에 액세스하는 시스템 서비스입니다. 로컬 시스템(SSSD 클라이언트)을 외부 백엔드 시스템(도메인)에 연결합니다. 이를 통해 SSSD 클라이언트에 SSSD 공급자를 사용하여 ID 및 인증 원격 서비스에 액세스할 수 있습니다. 예를 들어 이러한 원격 서비스에는 LDAP 디렉터리, IdM(Identity Management) 또는 AD(Active Directory) 도메인 또는 Kerberos 영역 등이 있습니다.

AD 통합을 위해 ID 관리 서비스로 사용되는 경우 SSSD 는 NIS 또는 Winbind 와 같은 서비스에 대한 대안입니다. 이 장에서는 SSSD 가 AD 에서 작동하는 방식을 설명합니다. SSSD 에 대한 자세한 내용은 System-Level Authentication Guide 를 참조하십시오.

2.1. AD PROVIDER 가 신뢰할 수 있는 도메인을 처리하는 방법

이 섹션에서는 **/etc/sssd/sssd.conf** 파일에 **id_provider = ad** 를 설정하는 경우 SSSD 에서 신뢰할 수 있는 도메인을 처리하는 방법을 설명합니다.

- SSSD 는 단일 ActiveActive Directory Long;Directory domain 의 도메인만 지원합니다. SSSD 가 여러 오레인의 여러 도메인에 액세스해야 하는 경우 SSSD 대신 신뢰할 수 있는(기본 설정) 또는 **winbindd** 서비스를 사용하는 것이 좋습니다.

- 기본적으로 SSSD 는 오스트레드의 모든 도메인을 검색하고 신뢰할 수 있는 도메인의 객체 요청이 도달하면 SSSD 에서 이를 해결하려고 합니다.

  신뢰할 수 있는 도메인에 도달할 수 없거나 지리적으로 멀리 떨어져 있는 경우 **/etc/sssd/sssd.conf** 에서 **ad_enabled_domains** 매개 변수를 설정하여 신뢰할 수 있는 도메인 SSSD 에서 오브젝트를 확인할 수 있습니다.

- 기본적으로 정규화된 사용자 이름을 사용하여 신뢰할 수 있는 도메인에서 사용자를 확인해야 합니다.

2.2. SSSD 의 AD 공급자 구성

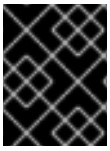
AD 공급자를 통해 SSSD 는 AD 환경의 최적화를 통해 LDAP ID 공급자와 Kerberos 인증 공급자를 사용할 수 있습니다.

2.2.1. 통합 옵션 개요

Linux 및 Windows 시스템은 사용자 및 그룹에 대해 서로 다른 식별자를 사용합니다.

- Linux 는 UID(사용자 ID) 및 그룹 ID (GID) 를 사용합니다. 시스템 관리자 가이드의 사용자 및 그룹 관리를 참조하십시오. Linux UID 및 GID 는 POSIX 표준을 준수합니다.

- Windows 에서 보안 ID (SID) 를 사용합니다.



중요

Windows 및 ActiveActive Directory Long;Directory 에서 동일한 사용자 이름을 사용하지 마십시오.

AD 사용자를 포함하여 Red Hat Enterprise Linux 시스템에 인증하는 사용자는 UID 및 GID 가 할당되어 있어야 합니다. SSSD 는 다음과 같은 통합 옵션을 제공합니다.

AD 사용자의 새 UID 및 GID 자동 생성

SSSD는 AD 사용자의 SID를 사용하여 ID 매핑 이라는 프로세스에서 POSIX ID를 알고리즘적으로 생성할 수 있습니다. ID 매핑은 AD의 SID와 Linux의 ID 간에 맵을 생성합니다.

- SSSD가 새 AD 도메인을 감지하면 사용 가능한 ID 범위를 새 도메인에 할당합니다. 따라서 각 AD 도메인은 모든 SSSD 클라이언트 시스템에서 동일한 ID 범위를 갖습니다.
- AD 사용자가 SSSD 클라이언트 시스템에 처음 로그인하면 SSSD에서 해당 도메인의 id 범위를 기반으로 UID를 포함하여 SSSD 캐시에 사용자에 대한 항목을 만듭니다.
- AD 사용자의 ID는 동일한 SID에서 일관된 방식으로 생성되므로 사용자는 Red Hat Enterprise Linux 시스템에 로그인할 때 동일한 UID 및 GID를 갖습니다.

2.2.2절. "SSSD의 공급자로 ID 매핑을 사용하여 AD 도메인 구성" 을 참조하십시오.

참고

모든 클라이언트 시스템이 SSSD를 사용하여 Multus를 Linux ID에 매핑하면 매핑이 일관되게 유지됩니다. 일부 클라이언트가 다른 소프트웨어를 사용하는 경우 다음 중 하나를 선택합니다.

- 모든 클라이언트에서 동일한 매핑 알고리즘이 사용되는지 확인합니다.
- AD에 정의된 POSIX 속성 사용 에 설명된 대로 명시적 POSIX 특성을 사용합니다.

AD에 정의된 POSIX 속성 사용

AD는 **uidNumber**,**gidNumber**,**unixHomeDirectory** 또는 **loginShell** 과 같은 POSIX 속성을 생성 및 저장할 수 있습니다.

AD 사용자의 새 UID 및 GID 자동 생성 에 설명된 ID 매핑을 사용하는 경우 SSSD는 새 UID와 GID를 생성하여 AD에 정의된 값을 덮어씁니다. AD 정의 값을 유지하려면 SSSD에서 ID 매핑을 비활성화해야 합니다.

2.2.3절. "AD에서 POSIX 속성을 사용하도록 SSSD 구성" 을 참조하십시오.

2.2.2. SSSD의 공급자로 ID 매핑을 사용하여 AD 도메인 구성

사전 요구 사항
AD 시스템과 Linux 시스템이 모두 올바르게 구성되어 있는지 확인합니다.

- 이름 확인을 위한 구성을 확인합니다. 특히 DNS SRV 레코드를 확인합니다. 예를 들어 이름이 **ad.example.com** 인 도메인의 경우:
  - DNS SRV LDAP 레코드를 확인하려면 다음을 수행합니다.

```
# dig -t SRV _ldap._tcp.ad.example.com
```

  - AD 레코드를 확인하려면 다음을 수행합니다.

```
# dig -t SRV _ldap._tcp.dc._msdcs.ad.example.com
```

나중에 SSSD를 특정 AD 도메인 컨트롤러에 연결하는 경우 DNS SRV 레코드를 확인할 필요가 없습니다.

- 두 시스템의 시스템 시간이 동기화되었는지 확인합니다. 이렇게 하면 Kerberos가 제대로 작동할 수 있습니다.
- AD 도메인 컨트롤러에서 다음 포트가 열려 있고 RHEL 호스트에서 액세스할 수 있는지 확인합니다.

표 2.1. SSSD를 사용하여 AD로 Linux 시스템의 직접 통합에 필요한 포트

Service	포트	프로토콜	참고
DNS	53	UDP 및 TCP	
LDAP	389	UDP 및 TCP	
Kerberos	88	UDP 및 TCP	
Kerberos	464	UDP 및 TCP	kadmin에서 암호 설정 및 변경에 사용
LDAP 글로벌 카탈로그	3268	TCP	**id_provider = ad** 옵션이 사용 중인 경우
NTP	123	UDP	선택 사항
Samba	445	UDP 및 TCP	AD Group Policy Objects(GPO)의 경우

로컬 시스템 구성
Red Hat은 **realm join** 명령을 사용하여 시스템을 구성하는 것이 좋습니다. 3장. **realmd** 를 사용하여 Active Directory 도메인에 연결을 참조하십시오. **realmd** Suite는 필요한 모든 구성 파일을 자동으로 편집합니다. 예를 들면 다음과 같습니다.

```
# realm join ad.example.com
```

realmd 를 사용하지 않으려면 시스템을 수동으로 구성할 수 있습니다. Red Hat Kernel;Hat Knowledgebase의 Active Directory 도메인에 SSSD 클라이언트 수동 연결을 참조하십시오.

선택 사항: 사용자 홈 디렉터리 및 쉘 구성
사용자가 Linux 시스템에 처음 로그인하면 **pam_oddjob_mkhomedir.so** 라이브러리에서 홈 디렉터리를 자동으로 생성합니다. 기본적으로 SSSD는 AD ID 공급자에서 홈 디렉터리의 형식을 검색합니다. Linux 클라이언트에서 디렉터리 형식을 사용자 지정하려면 다음을 수행합니다.

1. **/etc/sssd/sssd.conf** 파일을 엽니다.
2. **[domain]** 섹션에서 다음 옵션 중 하나를 사용합니다.
   - **fallback_homedir** 은 홈 디렉터리가 AD에 정의되어 있지 않은 경우에만 사용되는 대체 홈 디렉터리 형식을 설정합니다.
   - **override_homedir** 은 홈 디렉터리 템플릿을 설정하며, 이 템플릿은 항상 AD에 정의된 홈 디렉터리를 덮어씁니다.

   예를 들어 **/home/domain_name/user_name** 형식을 항상 사용하려면 다음을 실행합니다.

```
[domain/EXAMPLE]
[... file truncated ...]
override_homedir = /home/%d/%u
```

자세한 내용은 sssd.conf(5) 도움말 페이지를 참조하십시오.

기본적으로 SSSD는 AD에 구성된 **loginShell** 매개 변수에서 사용자 쉘에 대한 정보를 검색합니다. Linux 클라이언트에서 사용자 쉘 설정을 사용자 지정하려면 다음을 수행합니다.

1. **/etc/sssd/sssd.conf** 파일을 엽니다.
2. 다음 옵션을 사용하여 필요한 사용자 쉘 설정을 정의합니다.
   - **shell_fallback** 은 대체 값을 설정합니다. 이 값은 AD에 쉘이 정의되지 않은 경우에만 사용됩니다.
   - **override_shell** 은 항상 AD에 정의된 쉘을 재정의하는 값을 설정합니다.
   - **default_shell** 은 기본 쉘 값을 설정
   - **allowed_shells** 및 **vetoed_shells** set lists of allowed or blacklisted shells

   자세한 내용은 sssd.conf(5) 도움말 페이지를 참조하십시오.

새 설정 로드

- 설정 파일을 변경한 후 SSSD를 다시 시작합니다.

```
# systemctl restart sssd.service
```

추가 리소스

- LDAP 및 Kerberos 공급자에 대한 기타 구성 옵션은 sssd-ldap(5) 및 sssd-krb5(5) 도움말 페이지를 참조하십시오.
- AD 공급자의 기타 구성 옵션은 sssd-ad(5) 도움말 페이지를 참조하십시오.

2.2.3. AD에서 POSIX 속성을 사용하도록 SSSD 구성

참고

이전에는 사용자 계정에 POSIX 속성을 제공하는 데 UNIX용 Identity Management 확장을 사용할 수 있었습니다. 이제 확장 기능이 더 이상 사용되지 않습니다. 자세한 내용은 Microsoft 개발자 네트워크를 참조하십시오.

UNIX용 Identity Management를 사용 중인 경우 자주 묻는 질문에 대한 답변은 이 지식베이스 문서를 참조하십시오.

Unix용 Identity Management for Unix 및 Services for Unix 패키지를 참조하는 이전 프로시저는 다음과 같은 Red Hat Red Hat qcow;Hat 지식 베이스 문서를 참조하십시오.

- POSIX 속성을 사용하여 Active Directory 도메인 구성
- Active Directory를 LDAP 도메인으로 구성

권장 사항
최상의 성능을 위해 AD 글로벌 카탈로그에 POSIX 특성을 게시합니다. 글로벌 카탈로그에 POSIX 속성이 없는 경우 SSSD는 LDAP 포트에서 직접 개별 도메인 컨트롤러에 연결합니다.

***Linux** 시스템을 **AD** 도메인에 연결*
2.2.2절. "SSSD의 공급자로 ID 매핑을 사용하여 AD 도메인 구성" 의 단계를 따르십시오.

***SSSD**에서 **ID** 매핑 비활성화*

1. ***/etc/sssd/sssd.conf** 파일을 엽니다.*
2. *AD 도메인 섹션에서 **ldap_id_mapping = false** 설정을 추가합니다.*

참고

***realm** 유틸리티를 사용하여 도메인에 참여하고 **--automatic-id-mapping=no** 스위치를 추가한 경우 **realm** 유틸리티에서 **ldap_id_mapping = false** 를 사용하여 SSSD를 이미 설정했습니다.*

3. *이전에 기본 ID 매핑 구성을 가진 사용자를 요청한 경우 SSSD 캐시를 제거하십시오.*

```
rm -f /var/lib/sss/db/*
```

SSSD는 이제 로컬로 생성하는 대신 AD의 POSIX 속성을 사용합니다.

추가 리소스
*ID 매핑 및 **ldap_id_mapping** 매개변수에 대한 자세한 내용은 sssd-ldap(8) 도움말 페이지를 참조하십시오.*

2.3. 자동 KERBEROS 호스트 키 탭 업데이트

adcli 패키지가 설치된 경우 SSSD에서 AD 환경에서 Kerberos 호스트 키탭 파일을 자동으로 갱신합니다. 데몬은 시스템 계정 암호가 구성된 값보다 오래된 경우 매일 확인하고 필요한 경우 갱신합니다.

기본 갱신 간격은 30일입니다. 기본값을 변경하려면 다음을 수행합니다.

1. ***/etc/sssd/sssd.conf** 파일의 AD 공급자에 다음 매개 변수를 추가합니다.*

```
ad_maximum_machine_account_password_age = value_in_days
```

2. *SSSD를 다시 시작:*

```
# systemctl restart sssd
```

*자동 Kerberos 호스트 키탭 갱신을 비활성화하려면 **ad_maximum_machine_account_password_age = 0** 을 설정합니다.*

2.4. 동적 DNS 업데이트 활성화

AD를 사용하면 클라이언트가 DNS 레코드를 자동으로 새로 고칠 수 있습니다. 또한 AD는 DNS 레코드를 적극적으로 유지하여 타이밍 아웃(고정) 및 비활성 레코드 제거(scavenging)를 포함하여 업데이트가 있는지 확인합니다. DNS 감시는 AD 측에서 기본적으로 활성화되어 있지 않습니다.

SSSD를 사용하면 Linux 시스템에서 DNS 레코드를 새로 고침하여 Windows 클라이언트를 모방하여 레코드가 비활성 상태로 표시되어 DNS 레코드에서 제거되지 않도록 할 수 있습니다. 동적 DNS 업데이트가 활성화되면 클라이언트의 DNS 레코드가 새로 고쳐집니다.

- ID 공급자가 온라인 상태가 되면 (거의)
- Linux 시스템이 재부팅되는 경우(주로)
- 기본적으로 AD 공급자는 DNS 레코드를 24시간마다 업데이트합니다.

  이 동작을 DHCP 리스와 동일한 간격으로 설정할 수 있습니다. 이 경우 리스가 갱신된 후 Linux 클라이언트가 갱신됩니다.

DNS 업데이트는 DNS(GSS-TSIG)용 Kerberos/GSSAPI를 사용하여 AD 서버로 전송됩니다. 즉 보안 연결만 활성화해야 합니다.

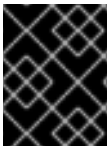
각 도메인에 대해 동적 DNS 구성이 설정됩니다. 예를 들면 다음과 같습니다.

```
[domain/ad.example.com]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad

ldap_schema = ad

dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600
```

이러한 옵션에 대한 자세한 내용은 sssd-ad(5) 도움말 페이지를 참조하십시오.

2.5. SSSD에서 범위 검색 사용

SSSD에서는 범위 검색 기능을 사용하여 AD의 Searching 기능을 지원합니다. 범위 검색에 대한 자세한 내용은 Microsoft 개발자 네트워크를 참조하십시오.



중요

그룹 또는 검색 기반에서 사용자 지정 필터를 설정하면 대규모 그룹에서 필터가 제대로 작동하지 않을 수 있습니다.

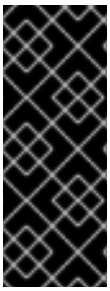
2.6. 그룹 정책 개체 액세스 제어

그룹 정책은 관리자가 AD(Active Directory) 환경에서 사용자 및 컴퓨터에 대한 정책을 중앙에서 관리할 수 있는 Microsoft Windows 기능입니다. 그룹 정책 개체 (GPO)는 도메인 컨트롤러(DC)에 저장되며 컴퓨터 및 사용자와 같은 정책 대상에 적용할 수 있는 정책 설정 컬렉션입니다. Windows 로그온 권한과 관련된 rootfs 정책 설정은 AD 환경에서 컴퓨터 기반 액세스 제어를 관리하는 데 일반적으로 사용됩니다.

2.6.1. SASL 액세스 제어에서 SSSD 작동 방식

rootfs 액세스 제어를 적용하도록 SSSD를 구성하면 SSSD는 호스트 시스템 및 AD 사용자에게 적용되는 rootfs를 검색합니다. 검색된 rootfs 구성에 따라 SSSD는 사용자가 특정 호스트에 로그인할 수 있는지 여

부를 결정합니다. 이를 통해 관리자는AD 도메인 컨트롤러를 중앙에서 사용하는Linux 및Windows 클라이언트가 제공한 로그인 정책을 정의할 수 있습니다.



중요

보안 필터링은 보안 필터에 나열하여 특정 사용자, 그룹 또는 호스트에 대해iLO 액세스 제어 범위를 추가로 제한할 수 있는 기능입니다. 그러나SSSD는 보안 필터의 사용자와 그룹만 지원합니다. SSSD는 보안 필터의 호스트 항목을 무시합니다.

SSSD가 특정 시스템에iLO 액세스 제어를 적용하도록 하려면AD 도메인에 새OU를 만들고 시스템을OU로 이동한 다음IMG를 이OU에 연결합니다.

2.6.2. SSSD에서 지원하는 rootfs 설정

표 2.2. SSSD에 의해 검색 된 access control 옵션

rootfs 옵션 [a]	해당 sssd.conf 옵션 [b]
로컬에서 로그 허용 로컬에서 로그 거부	***ad_gpo_map_interactive***
원격 데스크탑 서비스를 통해 로그 허용 Remote Desktop Services를 통해 로그 거부	***ad_gpo_map_remote_interactive***
네트워크에서 이 컴퓨터에 액세스 네트워크에서 이 컴퓨터에 대한 액세스 거부	***ad_gpo_map_network***
배치 작업으로 로그 허용 배치 작업으로 에서 로그 거부	***ad_gpo_map_batch***
서비스로 로그 허용 서비스로의 로그 거부	***ad_gpo_map_service***

[a] Windows의 그룹 정책 관리 편집기에서 이름이 지정된 대로입니다.

[b] 이러한 옵션에 대한 자세한 내용은 sssd-ad(5) 도움말 페이지를 참조하십시오. 기본적으로 해당 옵션이 매핑되는PAM(플러블 인증 모듈) 서비스 목록은 도움말 페이지를 참조하십시오.

2.6.3. SSSD에 대한 rootfs 기반 액세스 제어 구성

*rootfs 기반 액세스 제어는 **/etc/sssd/sssd.conf** 파일에서 구성할 수 있습니다. **ad_gpo_access_control** 옵션은 grant-based 액세스 제어가 실행되는 모드를 지정합니다. 다음 값으로 설정할 수 있습니다.*

ad_gpo_access_control = permissive

*Permissive 값은 grant-based access control이 평가되고 적용되지 않음을 지정합니다. 액세스 권한이 거부될 때마다 **syslog** 메시지가 기록됩니다.* ***이 설정은 기본 설정입니다.***

ad_gpo_access_control = enforcing

enforcing 값은 grant-based access control이 평가되고 적용되도록 지정합니다.

ad_gpo_access_control = disabled

disabled 값은 iLO 기반 액세스 제어가 평가되거나 적용되지 않도록 지정합니다.

중요

grant-based 액세스 제어를 사용하고 ad_gpo_access_control 을 enforcing 모드로 설정하기 전에 ad_gpo_access_control 을 허용 모드로 설정하고 로그를 검사하는 것이 좋습니다. syslog 메시지를 검토하여 마지막으로 강제 모드를 설정하기 전에 필요에 따라 현재 rootfs 설정을 테스트하고 조정할 수 있습니다.

rootfs 기반 액세스 제어와 관련된 다음 매개변수도 sssd.conf 파일에 지정할 수 있습니다.

- *ad_gpo_map_* 옵션과 ad_gpo_default_right 옵션은 특정 Windows 로그온 권한에 매핑되는 PAM 서비스를 구성합니다.*

  특정 rsh 설정에 매핑된 PAM 서비스의 기본 목록에 PAM 서비스를 추가하거나 목록에서 서비스를 제거하려면 ad_gpo_map_* 옵션을 사용합니다. 예를 들어 대화형 로그인(GPO 설정)에 매핑된 PAM 서비스 목록에서 su 서비스를 제거하려면 로컬에 로그를 허용하고 로컬에서 로그인할 수 있습니다.

  ```
  ad_gpo_map_interactive = -su
  ```

- *ad_gpo_cache_timeout 옵션은 후속 액세스 제어 요청이 DC anew에서 저장된 파일을 검색하는 대신 캐시에 저장된 파일을 재사용할 수 있는 간격을 지정합니다.*

사용 가능한 rootfs 매개변수와 해당 설명 및 기본값의 자세한 목록은 sssd-ad(5) 도움말 페이지를 참조하십시오.

2.6.4. 추가 리소스

- VDDKs와 함께 작동하도록 SSSD를 구성하는 방법에 대한 자세한 내용은 Red Hat qcow;Hat Knowledgebase에서 Active Directory SSH 또는 Console/GUI NetNamespaces를 준수하도록 SSSD 구성을 참조하십시오.

2.7. SSSD를 자동으로 사용하여 사용자 개인 그룹 생성

AD에 직접 통합된 SSSD 클라이언트는 검색된 모든 AD 사용자에 대해 사용자 개인 그룹을 자동으로 생성할 수 있으므로 GID 번호를 아직 사용하지 않는 한 GID가 사용자의 UID와 일치하도록 합니다. 충돌을 방지하려면 사용자 UID와 동일한 GID가 있는 그룹이 서버에 있는지 확인합니다.

GID는 AD에 저장되지 않습니다. 이렇게 하면 AD 사용자에게 그룹 기능의 이점이 있지만 LDAP 데이터베이스에 불필요한 빈 그룹이 포함되어 있지 않습니다.

2.7.1. AD 사용자의 사용자 개인 그룹 자동 생성 활성화

AD 사용자에 대한 사용자 개인 그룹 자동 생성을 활성화하려면 다음을 수행합니다.

1. /etc/sssd/sssd.conf 파일을 편집하여 [domain/LDAP] 섹션에 추가합니다.

```
auto_private_groups = true
```

2. sssd 서비스를 다시 시작하여 sssd 데이터베이스를 제거합니다.

```
# service sssd stop ; rm -rf /var/lib/sss/db/* ; service sssd start
```

이 절차를 수행한 후 모든 AD 사용자에게 UID와 동일한 GID가 있습니다.

```
# id ad_user1
uid=121298(ad_user1) gid=121298(ad_user1) groups=121298(ad_user1),10000(Group1)
# id ad_user2
uid=121299(ad_user2) gid=121299(ad_user2) groups=121299(ad_user2),10000(Group1)
```

2.7.2. AD 사용자에 대한 사용자 개인 그룹 자동 생성 비활성화

AD 사용자에 대한 사용자 개인 그룹의 자동 생성을 비활성화하려면 다음을 수행합니다.

1. /etc/sssd/sssd.conf 파일을 편집하여 [domain/LDAP] 섹션에 추가합니다.

```
auto_private_groups = false
```

2. sssd 서비스를 다시 시작하여 sssd 데이터베이스를 제거합니다.

```
# service sssd stop ; rm -rf /var/lib/sss/db/* ; service sssd start
```

이 절차를 수행한 후 모든 AD 사용자에게 동일한 일반 GID가 있습니다.

```
# id ad_user1
uid=121298(ad_user1) gid=10000(group1) groups=10000(Group1)
# id ad_user2
uid=121299(ad_user2) gid=10000(group1) groups=10000(Group1)
```

2.8. SSSD 클라이언트 및 ACTIVE DIRECTORY DNS 사이트 자동 검색

Active Directory Lakes는 다양한 도메인 컨트롤러, 도메인 및 하위 도메인 및 물리적 사이트와 함께 매우 커질 수 있습니다. Active Directory는 사이트의 개념을 사용하여 도메인 컨트롤러의 물리적 위치를 식별합니다. 이를 통해 클라이언트는 지리적으로 가장 가까운 도메인 컨트롤러에 연결할 수 있으므로 클라이언트 성능이 향상됩니다.

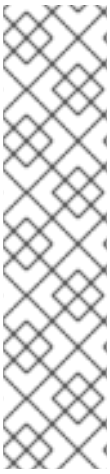
기본적으로 SSSD 클라이언트는 autodiscovery를 사용하여 AD 사이트를 찾고 가장 가까운 도메인 컨트롤러에 연결합니다. 프로세스는 다음 단계로 구성됩니다.

1.

SSSD는 AD forest에 있는 DNS 서버에서 SRV 레코드를 쿼리합니다. 반환된 레코드에는 Pod의 DC 이름이 포함됩니다.

2. SSSD는 이러한 각 DC에 LDAP ping을 보냅니다. DC가 구성된 간격 내에 응답하지 않으면 요청 시간 초과 및 SSSD가 LDAP ping을 다음 간격으로 보냅니다. 연결에 성공하면 응답에 SSSD 클라이언트가 속한 AD 사이트에 대한 정보가 포함됩니다.

3. 그런 다음 SSSD는 DNS 서버에서 SRV 레코드를 쿼리하여 속한 사이트 내에서 DC를 찾고 그 중 하나에 연결합니다.



참고

SSSD는 기본적으로 AD 사이트임을 기억합니다. 이러한 방식으로 SSSD는 자동 검색 프로세스 중에 이 사이트의 DC에 LDAP ping을 직접 전송하여 사이트 정보를 새로 고칠 수 있습니다. 따라서 시간 초과가 정상적으로 발생하지 않기 때문에 자동 검색 절차가 매우 빠릅니다.

사이트가 더 이상 존재하지 않거나 클라이언트가 다른 사이트에 할당되면 SSSD는 마스트에서 SRV 레코드 쿼리를 시작하고 전체 프로세스를 다시 시작합니다.

자동 검색을 재정의하려면 /etc/sssd/sssd.conf 파일의 [domain] 섹션에 ad_site 옵션을 사용하여 클라이언트가 연결하려는 AD 사이트를 지정합니다.

추가 리소스

- ad_site 에 대한 자세한 내용은 sssd-ad(5) 도움말 페이지를 참조하십시오.
- ID 관리 및 Active Directory 간의 신뢰가 있는 환경은 5.6절. "신뢰할 수 있는 Active Directory 도메인에서 ID 관리 또는 SSSD를 선택한 Active Directory 서버 또는 사이트로 제한"를 참조하십시오.

2.9. SSSD 문제 해결

SSSD 문제 해결에 대한 자세한 내용은 System-Level Authentication Guide 의 SSSD 문제 해결 부록을 참조하십시오.

3장. REALMD 를 사용하여 ACTIVE DIRECTORY 도메인에 연결

realmd 시스템은 직접 도메인 통합을 수행하기 위해 ID 도메인을 검색하고 결합할 수 있는 명확하고 간단한 방법을 제공합니다. 도메인에 연결하기 위해 SSSD 또는 Winbind와 같은 기본 Linux 시스템 서비스를 구성합니다.

2장. SSSD의 ID 공급자로 Active Directory 사용 로컬 시스템에서 SSSD(System Security Services Daemon)를 백엔드 ID 공급자로 사용하는 방법에 대해 설명합니다. 시스템이 이 작업에 맞게 올바르게 구성되었는지 확인하는 것은 복잡한 작업일 수 있습니다. 가능한 각 ID 공급자와 SSSD 자체에 대해 다양한 구성 매개변수가 많이 있습니다. 또한 모든 도메인 정보는 미리 사용 가능한 다음 SSSD에서 로컬 시스템을 AD와 통합하기 위해 SSSD 구성에 올바르게 포맷해야 합니다.

realmd 시스템은 해당 구성을 간소화합니다. 검색 검색을 실행하여 사용 가능한 AD 및 Identity Management 도메인을 확인한 다음 시스템을 도메인에 조인하고 지정된 ID 도메인에 연결하고 사용자 액세스를 관리하는 데 사용되는 필수 클라이언트 서비스를 설정할 수 있습니다. 또한 기본 서비스인 SSSD는 여러 도메인을 지원하므로 영역 도 여러 도메인을 검색하고 지원할 수 있습니다.

3.1. 지원되는 도메인 유형 및 클라이언트

realmd 시스템은 다음과 같은 도메인 유형을 지원합니다.

- Microsoft Active Directory
- Red Hat Enterprise Linux Identity Management

다음 도메인 클라이언트가 realmd 에서 지원합니다.

- Red Hat Enterprise Linux Identity Management 및 Microsoft Active Directory용 SSSD
- Microsoft Active Directory에 대한 winbind

3.2. REALMD사용을 위한 사전 요구 사항

realmd 시스템을 사용하려면 realmd 패키지를 설치합니다.

-

```
# yum install realmd
```

또한 **oddjob , oddjob -mkhomedir,sssd, adcli** 패키지가 설치되어 있는지 확인합니다. 이러한 패키지는 **realmd** 를 사용하여 시스템을 관리할 수 있어야 합니다.

참고

3.4절. "ID 도메인 검색 및 연결" 에서 언급한 대로, **realmd** 를 사용하여 설치할 패키지를 찾을 수 있습니다.

3.3. REALMD 명령

realmd 시스템에는 두 가지 주요 작업 영역이 있습니다.

- 도메인에서 시스템 등록 관리
- 로컬 시스템 리소스에 액세스할 수 있는 도메인 사용자 설정

realm d 의 중앙 유틸리티는 영역(**zone**)이라고 합니다. 대부분의 **realm** 명령에는 유틸리티에서 수행해야 하는 작업과 작업을 수행할 도메인 또는 사용자 계정과 같은 엔티티를 지정해야 합니다.

```
realm command arguments
```

예를 들면 다음과 같습니다.

```
realm join ad.example.com
realm permit user_name
```

표 **3.1. realmd** 명령

명령	설명
영역 명령	
discover	네트워크에서 도메인에 대한 검색 검사를 실행합니다.
join	시스템을 지정된 도메인에 추가합니다.

명령	설명
leave	지정된 도메인에서 시스템을 제거합니다.
list	시스템 또는 검색되고 구성된 모든 도메인에 대해 구성된 모든 도메인을 나열합니다.
로그인 명령	
허용	지정된 사용자 또는 구성된 도메인 내의 모든 사용자에 대해 액세스를 활성화하여 로컬 시스템에 액세스할 수 있습니다.
deny	지정된 사용자에 대한 액세스 권한 또는 구성된 도메인 내의 모든 사용자에 대해 로컬 시스템에 대한 액세스를 제한합니다.

realm 명령에 대한 자세한 내용은 realm(8) 도움말 페이지를 참조하십시오.

3.4. ID 도메인 검색 및 연결

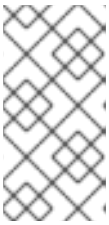
realm discover 명령은 전체 도메인 구성과 시스템을 도메인에 등록하기 위해 설치해야 하는 패키지 목록을 반환합니다.

그러면 realm join 명령은 로컬 시스템 서비스와 ID 도메인의 항목을 모두 구성하여 지정된 도메인과 함께 사용할 로컬 시스템을 설정합니다. 영역 참여 에서 실행되는 프로세스는 다음 단계를 따릅니다.

1. *지정된 도메인에 대한 검색 검사 실행.*

2. *시스템을 도메인에 연결하는 데 필요한 패키지 자동 설치.*

여기에는 SSSD 및 PAM 홈 디렉터리 작업 패키지가 포함됩니다. 패키지의 자동 설치에는 PackageKit 제품군이 실행 중이어야 합니다.



참고

PackageKit 이 비활성화된 경우 시스템은 누락된 패키지를 입력하라는 메시지를 표시하고 yum 유틸리티를 사용하여 수동으로 설치해야 합니다.

3. *디렉터리에 시스템에 대한 계정 항목을 생성하여 도메인에 가입합니다.*

4. */etc/krb5.keytab 호스트 키탭 파일 만들기.*

5. ***SSSD**에서 도메인을 구성하고 서비스를 다시 시작합니다.*

6. ***PAM** 구성 및 **/etc/nsswitch.conf** 파일에서 시스템 서비스에 대한 도메인 사용자를 활성화합니다.*

도메인 검색

*옵션 없이 실행하면 **realm discover** 명령은 **DHCP(Dynamic Host Configuration Protocol)**를 통해 할당된 도메인인 기본 **DNS** 도메인에 대한 정보를 표시합니다.*

```
# realm discover
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common
```

*특정 도메인에 대한 검색을 실행할 수도 있습니다. 이렇게 하려면 **realm discover** 를 실행하고 검색할 도메인의 이름을 추가합니다.*

```
# realm discover ad.example.com
```

*그러면 **realmd** 시스템은 **DNS SRV** 조회를 사용하여 이 도메인의 도메인 컨트롤러를 자동으로 찾습니다.*

참고

***realm discover** 명령을 실행하려면 **NetworkManager**가 실행 중이어야 합니다. 특히 **NetworkManager**의 **D-Bus** 인터페이스에 따라 다릅니다. 시스템에서 **NetworkManager** 를 사용하지 않는 경우 항상 **realm discover** 명령에 도메인 이름을 지정합니다.*

***realmd** 시스템은 **Active Directory** 및 **Identity Management** 도메인을 모두 검색할 수 있습니다. 두 도메인이 모두 사용자 환경에 있는 경우 **--server-software** 옵션을 사용하여 검색 결과를 특정 유형의 서버로 제한할 수 있습니다. 예를 들면 다음과 같습니다.*

```
# realm discover --server-software=active-directory
```

*검색 검색에서 반환된 속성 중 하나는 **login-policy** 이며, 도메인 사용자가 가입이 완료되는 즉시 로그인할 수 있는지 표시됩니다. 기본적으로 로그인이 허용되지 않는 경우 **realm permit** 명령을 사용하여 수동으로 허용할 수 있습니다. 자세한 내용은 **3.7**절. "도메인 사용자에 대한 로그인 권한 관리"의 내용을 참조하십시오.*

***realm discover** 명령에 대한 자세한 내용은 **realm(8)** 도움말 페이지를 참조하십시오.*

도메인 가입

중요

***Active Directory** 도메인을 사용하려면 고유한 컴퓨터 이름이 필요합니다. **ResourceOverride** 컴퓨터 이름과 **DNS** 호스트 이름은 모두 고유하게 정의되고 서로 일치해야 합니다.*

*시스템을 **ID** 도메인에 참여하려면 **realm join** 명령을 사용하여 도메인 이름을 지정합니다.*

```
# realm join ad.example.com
realm: Joined ad.example.com domain
```

*기본적으로 조인은 도메인 관리자로 수행됩니다. **AD**의 경우 관리자 계정을 **Administrator; IdM**의 경우 **admin** 이라고 합니다. 다른 사용자로 연결하려면 **-U** 옵션을 사용합니다.*

```
# realm join ad.example.com -U user
```

명령은 먼저 자격 증명 없이 연결을 시도하지만 필요한 경우 암호를 입력하라는 메시지가 표시됩니다.

Kerberos가 Linux 시스템에 올바르게 구성된 경우 인증을 위해 Kerberos 티켓으로 조인을 수행할 수도 있습니다. Kerberos 주체를 선택하려면 -U 옵션을 사용합니다.

```
# kinit user
 # realm join ad.example.com -U user
```

realm join 명령은 다른 여러 구성 옵션을 허용합니다. realm join 명령에 대한 자세한 내용은 realm(8) 도움말 페이지를 참조하십시오.

예 3.1. 시스템을 도메인에 등록하는 절차의 예

1. *realm discover 명령을 실행하여 도메인에 대한 정보를 표시합니다.*

```
# realm discover ad.example.com
ad.example.com
 type: kerberos
 realm-name: AD.EXAMPLE.COM
 domain-name: ad.example.com
 configured: no
 server-software: active-directory
 client-software: sssd
```

2. *realm join 명령을 실행하고 도메인 이름을 명령에 전달합니다. 시스템에 묻는 메시지가 표시되면 관리자 암호를 입력합니다.*

```
 # realm join ad.example.com
Password for Administrator: password
```

도메인을 검색하거나 결합할 때 realmd 는 DNS SRV 레코드를 확인합니다.

- *_LDAP._tcp.domain.example.com. Identity Management 레코드*
- *Active Directory 레코드에 대한 _LDAP._tcp.dc._msdcs.domain.example.com.*

레코드는 AD가 구성되면 기본적으로 생성되며 서비스 검색에서 찾을 수 있습니다.

도메인에 가입한 후 시스템 구성 테스트

시스템이 도메인에 성공적으로 등록되어 있는지 테스트하려면 도메인에서 사용자로 로그인할 수 있고 사용자 정보가 올바르게 표시되는지 확인합니다.

1. ***id 사용자@domain_name** 명령을 실행하여 도메인의 사용자에 대한 정보를 표시합니다.*

```
# id user@ad.example.com
uid=1348601103(user@ad.example.com) gid=1348600513(domain
group@ad.example.com) groups=1348600513(domain group@ad.example.com)
```

2. ***ssh** 유틸리티를 사용하여 동일한 사용자로 로그인합니다.*

```
# ssh -l user@ad.example.com linux-client.ad.example.com
user@ad.example.com@linux-client.ad.example.com's password:
Creating home directory for user@ad.example.com.
```

3. ***pwd** 유틸리티에서 사용자의 홈 디렉터리를 출력하는지 확인합니다.*

```
$ pwd
/home/ad.example.com/user
```

4. ***id** 유틸리티가 첫 번째 단계의 **id 사용자@domain_name**명령과 동일한 정보를 출력하는지 확인합니다.*

```
$ id
uid=1348601103(user@ad.example.com) gid=1348600513(domain
group@ad.example.com) groups=1348600513(domain group@ad.example.com)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

*또한 **kinit** 유틸리티는 도메인 조인이 성공적인지 테스트할 때 유용합니다. 유틸리티를 사용하려면 **KnativeServing 5-octets** 패키지가 설치되어 있어야 합니다.*

3.5. ID 도메인에서 시스템 제거

***ID** 도메인에서 시스템을 제거하려면 **realm leave** 명령을 사용합니다. 이 명령은 **SSSD** 및 로컬 시스템에서 도메인 구성을 제거합니다.*

```
# realm leave ad.example.com
```

기본적으로 제거는 기본 관리자로 수행됩니다. **AD**의 경우 관리자 계정을 **Administrator; IdM**의 경우 **admin** 이라고 합니다. 다른 사용자가 도메인에 가입하는 데 사용된 경우 해당 사용자로 제거를 수행해야 할 수 있습니다. 다른 사용자를 지정하려면 **-U** 옵션을 사용합니다.

```
# realm leave ad.example.com -U 'AD.EXAMPLE.COM\user'
```

명령은 먼저 자격 증명 없이 연결을 시도하지만 필요한 경우 암호를 입력하라는 메시지가 표시됩니다.

클라이언트가 도메인을 벗어나면 컴퓨터 계정이 디렉터리에서 삭제되지 않으며 로컬 클라이언트 구성은 제거됩니다. 컴퓨터 계정을 삭제하려면 지정된 **--remove** 옵션을 사용하여 명령을 실행합니다.

realm leave 명령에 대한 자세한 내용은 **realm(8)** 도움말 페이지를 참조하십시오.

3.6. 도메인 나열

realm list 명령은 시스템에 구성된 모든 도메인과 해당 도메인에 대한 전체 세부 정보 및 기본 구성을 나열합니다. 이는 영역 검색 명령에서 이미 시스템 구성에 있는 도메인에 대해서만 반환되는 것과 동일한 정보입니다.

```
# realm list --all --name-only
ad.example.com
```

영역 목록에서 사용할 수 있는 가장 주목할 만한 옵션은 다음과 같습니다.

--all

--all 옵션은 검색된 모든 도메인(구성 및 구성 없음)을 나열합니다.

--name-only

name -only 옵션은 결과를 도메인 이름으로 제한하며 도메인 구성 세부 정보를 표시하지 않습니다.

realm list 명령에 대한 자세한 내용은 **realm(8)** 도움말 페이지를 참조하십시오.

3.7. 도메인 사용자에 대한 로그인 권한 관리

기본적으로 도메인 측 액세스 제어가 적용되므로 도메인 사용자에 대한 로그인 정책이 도메인 자체에서 정의됩니다. 클라이언트 측 액세스 제어가 사용되도록 이 기본 동작을 재정의할 수 있습니다. 클라이언트 측 액세스 제어를 사용하면 로컬 정책에 의해서만 로그인 권한이 정의됩니다.

*도메인이 클라이언트 측 액세스 제어를 적용하면 **realmd** 시스템을 사용하여 해당 도메인에서 사용자에 대한 기본 허용 또는 액세스 규칙을 구성할 수 있습니다. 이러한 액세스 규칙은 시스템의 모든 서비스에 대한 액세스를 허용하거나 거부합니다. 특정 시스템 리소스 또는 도메인에 대해 보다 구체적인 액세스 규칙을 설정해야 합니다.*

액세스 규칙을 설정하려면 다음 두 명령을 사용하십시오.

realm deny

***realm deny** 명령은 도메인 내의 모든 사용자에 대한 액세스를 거부하기만 합니다. **--all** 옵션과 함께 이 명령을 사용합니다.*

영역 허용

***realm permit** 명령을 사용하여 다음을 수행할 수 있습니다.*

- *예를 들어 **--all** 옵션을 사용하여 모든 사용자에게 액세스 권한을 부여합니다.*

```
$ realm permit --all
```

- *예를 들어 지정된 사용자에게 액세스 권한을 부여합니다.*

```
$ realm permit user@example.com
$ realm permit 'AD.EXAMPLE.COM\user'
```

- *예를 들어 **-x** 옵션을 사용하여 지정된 사용자에 대한 액세스를 거부합니다.*

```
$ realm permit -x 'AD.EXAMPLE.COM\user'
```

*현재 액세스를 허용하는 것은 신뢰할 수 있는 도메인의 사용자가 아닌 기본 도메인의 사용자만 작동합니다. 이는 사용자 로그인에 도메인 이름이 포함되어야 하지만 현재 **SSSD**는 영역의 사용 가능한 하위 도메인에 대한 정보를 제공할 수 없기 때문입니다.*

중요

특히 선택된 사용자 또는 그룹에 대한 액세스 권한을 일부 사용자에게 거부하는 것보다는 액세스를 허용하는 것이 더 안전합니다. 따라서 영역 허용 **-x**를 사용하여 지정된 사용자에게만 권한을 거부하는 동안 기본적으로 모든 액세스를 허용하지 않는 것이 좋습니다. 대신 **Red Hat**은 모든 사용자에게 기본 액세스 정책을 유지하고 영역 허용 을 사용하여 선택한 사용자에게만 액세스 권한을 부여할 것을 권장합니다.

영역 거부 및 영역 허용 명령에 대한 자세한 내용은 **realm(8)** 도움말 페이지를 참조하십시오.

3.8. 기본 사용자 구성 변경

realmd 시스템은 기본 사용자 홈 디렉터리 및 쉘 **POSIX** 속성 수정을 지원합니다. 예를 들어 **Windows** 사용자 계정에 일부 **POSIX** 속성이 설정되지 않았거나 이러한 속성이 로컬 시스템에 있는 다른 사용자의 **POSIX** 속성과 다른 경우 이 속성이 필요할 수 있습니다.

중요

이 섹션에 설명된 대로 구성을 변경할 때는 **realm join** 명령이 아직 실행되지 않은 경우에만 작동합니다. 시스템이 이미 가입한 경우 "선택 사항: 사용자 홈 디렉터리 및 쉘 구성"에 설명된 대로 **/etc/sssd/sssd.conf** 파일의 기본 홈 디렉터리 및 쉘을 변경합니다.

기본 홈 디렉터리 및 쉘 **POSIX** 속성을 재정의하려면 **/etc/realmd.conf** 파일의 **[users]** 섹션에 다음 옵션을 지정합니다.

default-home

default-home 옵션은 홈 디렉터리가 명시적으로 설정되지 않은 계정의 홈 디렉터리를 생성하는 템플릿을 설정합니다. 일반적인 형식은 **/home/%d/%u** 입니다. 여기서 **%d** 는 도메인 이름이고 **%u** 는 사용자 이름입니다.

default-shell

default-shell 옵션은 기본 사용자 쉘을 정의합니다. 지원되는 모든 시스템 쉘을 허용합니다.

예를 들면 다음과 같습니다.

```
[users]
default-home = /home/%u
default-shell = /bin/bash
```

옵션에 대한 자세한 내용은 **realmd.conf(5)** 도움말 페이지를 참조하십시오.

3.9. ACTIVEACTIVE DIRECTORY FAMILIAR;DIRECTORY DOMAIN ENTRY에 대한 추가 구성

개별 도메인에 대한 사용자 지정 설정은 **/etc/realmd.conf** 파일에 정의할 수 있습니다. 각 도메인에는 자체 구성 섹션이 있을 수 있습니다. 섹션 이름은 도메인 이름과 일치해야 합니다. 예를 들면 다음과 같습니다.

```
[ad.example.com]
attribute = value
attribute = value
```

중요

이 섹션에 설명된 대로 구성을 변경할 때는 **realm join** 명령이 아직 실행되지 않은 경우에만 작동합니다. 시스템이 이미 가입한 경우 이러한 설정을 변경해도 효과가 없습니다. 이러한 상황에서는 **3.5절. "ID 도메인에서 시스템 제거"** 에 설명된 대로 도메인을 그대로 두고 **"도메인 가입"** 에 설명된 대로 다시 가입해야 합니다. 가입하려면 도메인 관리자의 자격 증명이 필요합니다.

도메인 구성을 변경하려면 **/etc/realmd.conf** 에서 해당 섹션을 편집합니다. 다음 예제에서는 **ad.example.com** 도메인의 **ID** 매핑을 비활성화하고, 호스트 주체를 설정하고, 시스템을 지정된 하위 트리에 추가합니다.

```
[ad.example.com]
computer-ou = ou=Linux Computers,DC=domain,DC=example,DC=com
user-principal = host/linux-client@AD.EXAMPLE.COM
automatic-id-mapping = no
```

"도메인 가입" 에 설명된 **realm join** 명령을 사용하여 시스템을 도메인에 조인할 때 동일한 구성을 설정할 수도 있습니다.

```
# realm join --computer-ou="ou=Linux Computers,dc=domain,dc=com" --automatic-id-mapping=no --
user-principal=host/linux-client@AD.EXAMPLE.COM
```

표 3.2. "영역 구성 옵션" **/etc/realmd.conf** 의 도메인 기본 섹션에서 설정할 수 있는 가장 주목할 만한 옵션을 나열합니다. 사용 가능한 구성 옵션에 대한 자세한 내용은 **realmd.conf(5)** 도움말 페이지를 참조

하십시오.

표 3.2. 영역 구성 옵션

옵션	설명
computer-ou	도메인에 컴퓨터 계정을 추가할 디렉터리 위치를 설정합니다. 루트 항목을 기준으로 전체 DN 또는 RDN일 수 있습니다. 하위 트리가 이미 있어야 합니다.
user-principal	컴퓨터 계정의 **userPrincipalName** 특성 값을 제공된 Kerberos 주체로 설정합니다.
automatic-id-mapping	동적 ID 매핑을 활성화하거나 매핑을 비활성화하고 Active Directory에 구성된 POSIX 속성을 사용할지 여부를 설정합니다.

4장. ACTIVE DIRECTORY 통합에 SAMBA 사용

Samba는 Red Hat Enterprise Linux에서 SMB(Server Message Block) 프로토콜을 구현합니다. SMB 프로토콜은 파일 공유 및 공유 프린터와 같은 서버의 리소스에 액세스하는 데 사용됩니다.

Samba를 사용하여 Active Directory(AD) 도메인 사용자를 도메인 컨트롤러(DC)에 인증할 수 있습니다. 또한 Samba를 사용하여 네트워크의 다른 SMB 클라이언트에 프린터 및 로컬 디렉토리를 공유할 수 있습니다.

4.1. 인증 도메인 사용자에 WINBINDD 사용

Samba의 winbindd 서비스는 NSS(Name Service Switch)에 대한 인터페이스를 제공하고 도메인 사용자가 로컬 시스템에 로그인할 때 AD에 인증할 수 있도록 합니다.

winbindd 를 사용하면 추가 소프트웨어를 설치하지 않고도 디렉터리 및 프린터를 공유하도록 구성을 개선할 수 있는 이점이 있습니다. 자세한 내용은 Red Hat 시스템 관리자 가이드의 Samba에 대한 섹션을 참조하십시오.

4.1.1. AD 도메인 연결

AD 도메인에 참여하고 Winbind 서비스를 사용하려면 realm join --client-software=winbind domain_name 명령을 사용합니다. realm 유틸리티는 Samba, Kerberos, PAM에 대한 구성 파일과 같은 구성 파일을 자동으로 업데이트합니다.

자세한 내용과 예제는 Red Hat 시스템 관리자 가이드의 Domain Member로 Samba 설정 섹션을 참조하십시오.

4.2. SSSD 및 WINBIND에서 SMB 공유 사용

이 섹션에서는 SSSD 클라이언트를 사용하여 CIFS(Common Internet File System) 프로토콜이라고도 하는 Server Message Block(SMB) 프로토콜에 따라 공유에 액세스하고 완전히 사용할 수 있는 방법을 설명합니다.

중요

IdM 또는 ActiveActive Directory 6.7 도메인의 클라이언트로 SSSD를 사용하면 특정 제한 사항이 있으며 Red Hat은 Winbind의 ID 매핑 플러그인으로 SSSD를 사용하지 않는 것이 좋습니다. 자세한 내용은 "IdM 클라이언트에서 실행 중인 Samba 파일 서버의 지원 상태 정보 또는 SSSD가 클라이언트 데몬 문서로 사용되는 직접 등록된 AD 클라이언트를" 참조하십시오.

SSSD는 Winbind에서 제공하는 모든 서비스를 지원하지 않습니다. 예를 들어 SSSD는 NT LAN Manager(NTLM) 또는ResourceOverride 이름 조회를 사용한 인증을 지원하지 않습니다. 이러한 서비스가 필요한 경우 Winbind를 사용합니다. ID 관리 도메인에서는 Kerberos 인증 및 DNS 이름 조회를 동일한 용도로 사용할 수 있습니다.

4.2.1. SSSD가 SMB에서 작동하는 방식

SMB 파일 공유 프로토콜은 Windows 머신에서 널리 사용됩니다. Identity Management와 Active Directory의 신뢰가 있는 Red Hat Enterprise Linux 환경에서 SSSD는 마치 표준 Linux 파일 시스템인 것처럼 SMB를 원활하게 사용할 수 있도록 지원합니다.

SMB 공유에 액세스하려면 시스템 호출을 Linux POSIX UID 및 GID로 변환할 수 있어야 합니다. SSSD 클라이언트는 이 ID 매핑을 가능하게 하는 SID-to-ID 또는 InstallPlan-to-name 알고리즘을 사용합니다.

4.2.2. SMB Shared Access의 SSSD 및 Winbind 간 전환

이 절차에서는 SSSD 클라이언트와 SSSD 클라이언트의 SMB 공유에 액세스하는 데 사용되는 SSSD와 Winbind 플러그인을 전환할 수 있는 방법을 설명합니다. Winbind가 SMB 공유에 액세스할 수 있으려면 클라이언트에 cifs-utils 패키지가 설치되어 있어야 합니다. cifs-utils 가 시스템에 설치되어 있는지 확인하려면 다음을 수행하십시오.

```
$ rpm -q cifs-utils
```

1. 선택사항입니다. SSSD 또는 Winbind를 사용하여 SSSD 클라이언트의 SMB 공유에 액세스할 수 있는지 여부를 확인합니다.

```
# alternatives --display cifs-idmap-plugin
cifs-idmap-plugin - status is auto.
 link currently points to /usr/lib64/cifs-utils/cifs_idmap_sss.so
```

```
/usr/lib64/cifs-utils/cifs_idmap_sss.so - priority 20
/usr/lib64/cifs-utils/idmapwb.so - priority 10
Current `best' version is /usr/lib64/cifs-utils/cifs_idmap_sss.so.
```

SSSD 플러그인**(cifs_idmap_ss.so)**이 설치된 경우 기본적으로 **Winbind** 플러그인 **(idmapwb.so)**보다 우선 순위가 높습니다.

2. **Winbind** 플러그인으로 전환하기 전에 시스템에서 **Winbind**가 실행되고 있는지 확인합니다.

```
# systemctl is-active winbind.service
active
```

SSSD 플러그인으로 전환하기 전에 시스템에서 **SSSD**가 실행되고 있는지 확인합니다.

```
# systemctl is-active sssd.service
active
```

3. 다른 플러그인으로 전환하려면 **alternatives --set cifs-idmap-plugin** 명령을 사용하고 필수 플러그인의 경로를 지정합니다. 예를 들어 **Winbind**로 전환하려면 다음을 수행합니다.

```
# alternatives --set cifs-idmap-plugin /usr/lib64/cifs-utils/idmapwb.so
```

참고

RHEL 7의 **i686**과 같은 **32**비트 버전 플랫폼은 **/usr/lib/cifs-utils/** 디렉터리를 **/usr/lib64/cifs-utils/** 대신 사용합니다.

4.3. 추가 리소스

Samba에 대한 자세한 내용은 **Red Hat** 시스템 관리자 가이드의 해당 섹션을 참조하십시오.

II 부. LINUX 도메인과 ACTIVE DIRECTORY 도메인 통합: 가장 안전한 보안

이 부분에서는 가장 간 신뢰 환경을 생성, 구성 및 관리하여 Linux 도메인을 Active Directory 도메인과 통합하는 것이 좋습니다.

5장. ACTIVEACTIVE DIRECTORY LONG;DIRECTORY AND IDENTITY IDENTITY MANAGEMENT {{;MANAGEMENT를 사용하여 CROSS-FOREST TRUSTS 생성

이 장에서는 ActiveActive Directory Long;Directory 및 IdentityIdentity Management qcow;Management 사이에 가장 많은 트러스트를 생성하는 방법을 설명합니다. 조직 간 신뢰는 ID 관리 및 AD(Active Directory) 환경을 간접적으로 통합하는 두 가지 방법 중 하나입니다. 다른 방법은 synchronization입니다. 환경에 대해 어떤 방법을 선택할 수 있는지 확실하지 않은 경우 1.3절. “간접 통합” 를 참조하십시오.

Kerberos는 신뢰 의 개념을 구현합니다. 신뢰에서 한 Kerberos 영역의 주체는 다른 Kerberos 영역의 서비스에 대한 티켓을 요청할 수 있습니다. 이 티켓을 사용하여 보안 주체는 다른 영역에 속하는 머신의 리소스에 대해 인증할 수 있습니다.

Kerberos는 또한 서로 다른 두 가지 Kerberos 영역 간의 관계를 만드는 기능도 있습니다. 즉 교차 영역 (cross-realm trust)이 있습니다. 신뢰의 일부인 영역은 티켓과 키의 공유 쌍을 사용합니다. 한 영역의 멤버는 두 영역의 멤버로 간주합니다.

Red Hat Identity Management는 IdM 도메인과 Active Directory 도메인 간 신뢰 구성을 지원합니다.

5.1. CROSS-FOREST TRUST 소개

Kerberos 영역만 인증 관련입니다. 기타 서비스 및 프로토콜은 Kerberos 영역의 시스템에서 실행되는 리소스에 대한 ID 및 권한 부여를 보완하는 것과 관련이 있습니다.

따라서 Kerberos 교차 영역의 설정만으로는 한 영역의 사용자가 다른 영역의 리소스에 액세스할 수 있도록 하는 것만으로는 충분하지 않으며 다른 수준의 통신에서도 지원이 필요합니다.

5.1.1. 신뢰 관계의 아키텍처

ActiveActive Directory QCOW;Directory 및 IdentityIdentity Management numerous;Management는 Kerberos, LDAP, DNS 또는 인증서 서비스와 같은 다양한 핵심 서비스를 관리합니다. 이 두 가지 다양한 환경을 투명하게 통합하려면 모든 핵심 서비스가 서로 원활하게 상호 작용해야 합니다.

Active Directory 보안, Forests, cross-forest Trusts

Kerberos 교차 영역 신뢰는 Active Directory 환경 간의 인증에 중요한 역할을 합니다. 신뢰할 수 있는 AD 도메인의 사용자 및 그룹 이름을 해결하기 위한 모든 활동에는 액세스 수행 방법에 관계없이 인증이 필요합니다. 즉, LDAP 프로토콜 사용 또는 SSMA(Server Message Block) 프로토콜의 상단에 DCE/RPC(Distributed Computing Environment/RPC)의 일부로 사용됩니다. 서로 다른 Active

Directory 도메인 간 액세스를 구성하는 데 더 많은 프로토콜이 포함되어 있으므로 신뢰 관계에는 더 일반적인 이름인 Active Directory 트러스트 가 있습니다.

여러 AD 도메인을 Active Directory 트리로 함께 구성할 수 있습니다. 하이스트의 루트 도메인은 제네스트에서 생성된 첫 번째 도메인입니다. ID 관리 도메인은 기존 AD gateway의 일부가 될 수 없으므로 항상 별도의 스트레스트로 표시됩니다.

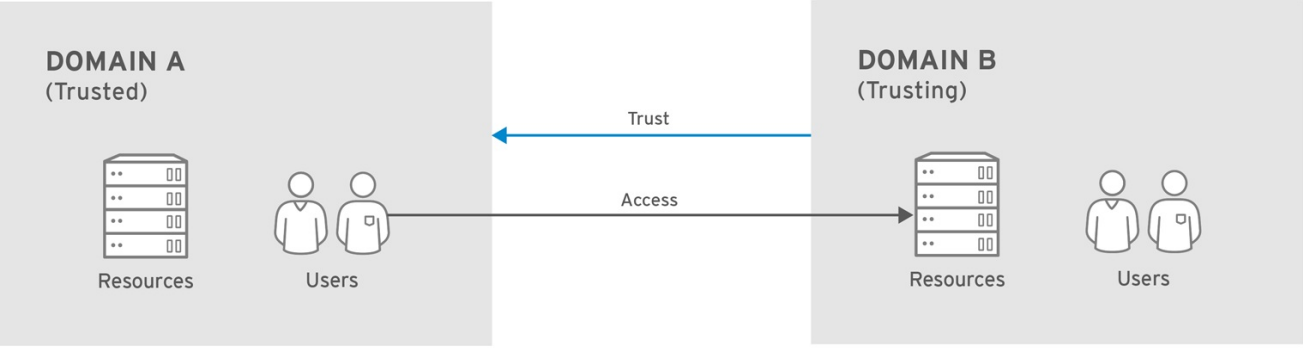
서로 다른 AD forest 루트 도메인의 사용자와 서비스를 통해 신뢰 관계가 설정된 경우, 신뢰를 Active Directory cross-forest trust 라고 합니다.

신뢰 흐름 및 단방향 신뢰

신뢰는 두 도메인 간의 액세스 관계를 설정합니다. ActiveActive Directory QCOW;Directory 환경은 복잡할 수 있으므로 하위 도메인, 루트 도메인 또는 서점 간에 ActiveActive Directory HAT;Directory 트러스트를 위한 다양한 유형과 배열이 있습니다. 신뢰는 하나의 도메인에서 다른 도메인으로의 경로입니다. 도메인 간 ID와 정보를 이동하는 방식을 신뢰 흐름 이라고 합니다.

신뢰할 수 있는 도메인에 는 사용자가 포함되어 있으며 신뢰할 수 있는 도메인에서 리소스에 액세스할 수 있습니다. 양방향 신뢰에서 신뢰는 한 방향으로만 이동합니다. 즉 사용자가 신뢰할 수 있는 도메인의 리소스에 액세스할 수 있지만 신뢰할 수 있는 도메인의 사용자는 신뢰할 수 있는 도메인의 리소스에 액세스할 수 없습니다. 그림 5.1. "단방향 신뢰" 에서 도메인 A는 도메인 B에서 신뢰하지만 도메인 B는 도메인 A에서 신뢰하지 않습니다.

그림 5.1. 단방향 신뢰

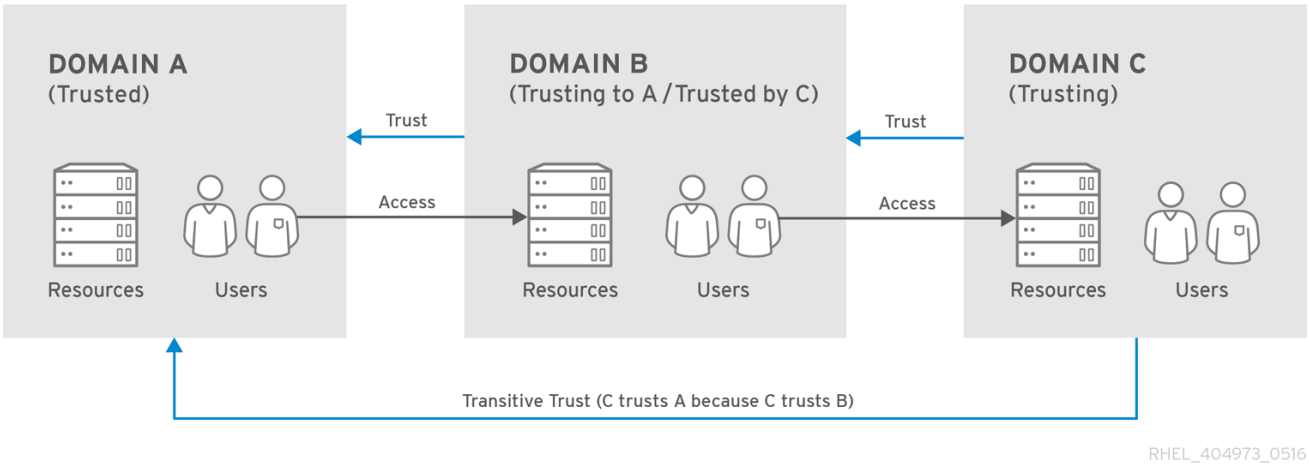


IdM을 사용하면 관리자가 단방향 및 양방향 신뢰를 모두 구성할 수 있습니다. 자세한 내용은 5.1.4절. "one-Way and two-Way Trusts"의 내용을 참조하십시오.

양도할 수 없는 신뢰할 수 있습니다.

신뢰는 도메인이 다른 도메인과 두 번째 도메인에서 신뢰하는 다른 도메인을 신뢰하도록 전송 될 수 있습니다.

그림 5.2. 연속 신뢰



신뢰는 또한 양도할 수 없으므로 명시적으로 포함된 도메인으로만 신뢰가 제한됩니다.

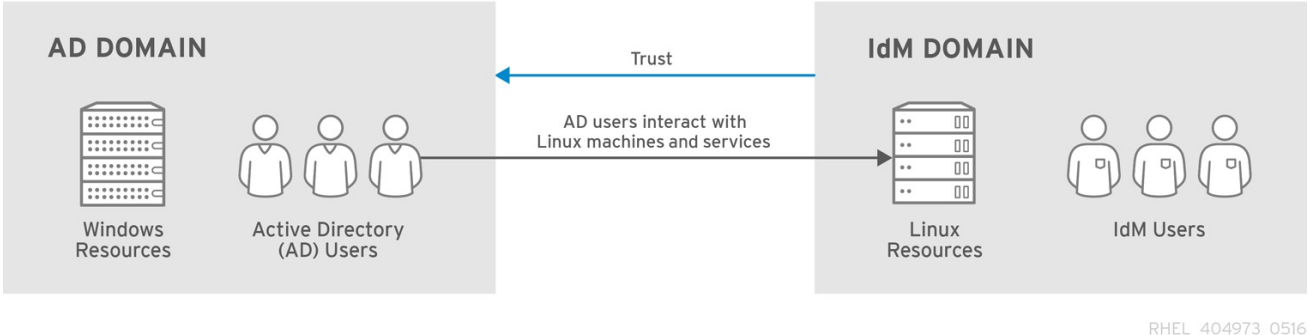
Active Directory 및 Identity Management의 가장 안전한 신뢰

***Active Directory** 하이징 내에서 도메인 간의 신뢰는 일반적으로 기본적으로 양방향과 전환이 가능합니다.*

*두 **AD Lake**의 신뢰는 두 개의 차선 루트 도메인 간의 신뢰이므로 양방향 또는 단방향일 수도 있습니다. 가장 큰 신뢰의 전이성은 명시적입니다:림프레드의 루트 도메인으로 이어지는 모든 도메인 신뢰는 가장 높은 신뢰를 통해 전진됩니다. 그러나 별도의 교차 마스트 신뢰는 전환되지 않습니다. 각 **AD forest** 루트 도메인 간에 명시적인 **cross-forest** 트러스트를 다른 **AD forest** 루트 도메인으로 설정해야 합니다.*

***AD**의 관점에서 **Identity Management**는 단일 **AD** 도메인을 사용하여 별도의 **AD** 오스트리드를 나타냅니다. **AD** 포리스트 루트 도메인과 **IdM** 도메인 간 크로스 포리스트 신뢰가 설정된 경우 **AD**프로브레이션 도메인의 사용자는 **IdM** 도메인의 **Linux** 시스템 및 서비스와 상호 작용할 수 있습니다.*

그림 5.3. 신뢰할 수 있는 직접



5.1.2. Active Directory 보안 개체 및 신뢰

Active Directory 글로벌 카탈로그

글로벌 카탈로그에는 ActiveActive Directory 6.7;Directory의 개체에 대한 정보가 포함되어 있습니다. 자체 도메인에 개체의 전체 사본을 저장합니다. ActiveActive Directory Long;Directory forest에 있는 다른 도메인의 오브젝트에서 일반적으로 검색되는 특성의 부분 복사본만 글로벌 카탈로그에 저장됩니다. 또한 일부 유형의 그룹은 특정 범위 내에서만 유효하며 글로벌 카탈로그의 일부가 아닐 수도 있습니다.

가장 큰 신뢰 컨텍스트는 단일 도메인보다 넓습니다. 따라서 신뢰할 수 있는 보호 대상의 서버-로컬 또는 도메인 로컬 보안 그룹 멤버십 중 일부는 IdM 서버에 표시되지 않을 수 있습니다.

글로벌 카탈로그 및 POSIX 속성

ActiveActive Directory QCOW;Directory는 기본 설정으로 POSIX 속성을 복제하지 않습니다. AD Red Hat에 정의된 POSIX 속성을 사용해야 하는 경우 이를 글로벌 카탈로그 서비스에 복제하는 것이 좋습니다.

5.1.3. IdM의 신뢰 아키텍처

IdentityIdentity Management {{;Management 측에서 IdM 서버는 ActiveActive Directory qcow;Directory ID를 인식할 수 있어야 하며 액세스 제어에 대한 그룹 멤버십을 적절하게 처리할 수 있어야 합니다. Microsoft PAC(MS-PAC, Privilege Account Certificate)에는 사용자에 대한 필수 정보(보안 ID, 도메인 사용자 이름, 그룹 멤버십)가 포함되어 있습니다. IdentityIdentity Management {{;Management에는 Kerberos 티켓의 PAC에서 데이터를 분석하는 두 가지 구성 요소가 있습니다.

- *SSSD: ActiveActive Directory etcdctl;Directory에서 ID 조회를 수행하고 권한 부여를 위한 사용자 및 그룹 보안 식별자(SID)를 검색합니다. SSSD는 또한 사용자에 대한 사용자, 그룹 및 티켓 정보를 캐시하고 Kerberos 및 DNS 도메인을 매핑합니다.*

- *IdM 정책 및 액세스를 위한 ActiveActive Directory}};Directory 사용자를 IdM policies 및 액세스를 위한an IdMseparated;IdM 그룹과 연결할 수 있도록 IdentityIdentity Management(Linux 도메인 관리)(Linux 도메인 관리)*

참고

SELinux, sudo 및 호스트 기반 액세스 제어와 같은 Linux 도메인 관리에 대한 액세스 제어 규칙 및 정책은 IdentityIdentity ManagementProvision;Management를 통해 정의 및 적용됩니다. ActiveActive Directory HAT;Directory 측에 설정된 모든 액세스 제어 규칙은 IdM에서 평가하거나 사용하지 않습니다. 그룹 멤버십과 관련된 ActiveActive Directory Ben;Directory 구성만 사용됩니다.

다른 Active Directory Forests와의 신뢰

IdM은 다른 AD forests와의 신뢰 관계의 일부일 수도 있습니다. 신뢰가 수립되면 동일한 명령 및 절차에 따라 다른 모순에 대한 추가 신뢰를 나중에 추가할 수 있습니다. IdM은 서로 관련이 없는 여러 개의 서로 관련이 없는 간호를 동시에 신뢰할 수 있으므로, 관련 없는 AD 포스트의 사용자가 동일한 공유 IdM 도메인의 리소스에 액세스할 수 있습니다.

5.1.3.1. ActiveActive Directory HAT;Directory PACs 및 IdM 티켓

ActiveActive Directory HAT;Directory의 그룹 정보는 Privilege Attribute Certificate (MS-PAC 또는 PAC) 데이터 세트의 식별자 목록에 저장됩니다. PAC에는 그룹 멤버십 또는 추가 자격 증명 정보와 같은 다양한 권한 부여 정보가 포함되어 있습니다. 또한 Active Directory 도메인에 있는 사용자 및 그룹의 SID(Security Identifiers)가 포함되어 있습니다. GovCloudS는 Active Directory 사용자 및 그룹을 생성할 때 할당된 식별자입니다. 신뢰 환경에서 그룹 멤버는 이름 또는 DN이 아닌 SIDs로 식별됩니다.

PAC는 Active Directory 사용자의 Kerberos 서비스 요청 티켓에 Windows 도메인의 다른 Windows 클라이언트 및 서버에 엔터티를 식별하는 방법으로 포함됩니다. IdM은 PAC의 그룹 정보를 ActiveActive Directory 6.7;Directory 그룹에 매핑한 다음 해당 IdM 그룹에 매핑하여 액세스를 결정합니다.

ActiveActive Directory {{;Directory 사용자가 IdM 리소스에 대한 서비스 티켓을 요청하는 경우 프로세스는 다음과 같습니다.

1. 서비스에 대한 요청에는 사용자의 PAC가 포함됩니다. IdM Kerberos 배포 센터(KDC)는 Active Directory 그룹 목록을 IdM 그룹의 멤버십과 비교하여 PAC를 분석합니다.

2. MS-PAC에 정의된 Kerberos 보안 주체의 InstallPlans의 경우 IdMNetworkPolicy는 IdM LDAP에 정의된 외부 그룹 멤버십을 평가합니다. FlexVolume에 대한 추가 매핑을 사용할 수 있는 경우, SID가 속한 IdM 그룹의 다른 InstallPlan을 사용하여 MS-PAC 레코드를 확장할 수 있습니다. 결과 MS-PAC는 IdMNetworkPolicy에 의해 서명됩니다.

3. 서비스 티켓은 IdM 6443에서 서명한 업데이트된 PAC가 있는 사용자에게 반환됩니다. IdM 도메인에 속하는 AD 그룹에 속하는 사용자는 서비스 티켓의 MS-PAC 콘텐츠를 기반으로 IdM 클라이언트에서 실행되는 SSSD에서 인식할 수 있습니다. 이를 통해 IdM 클라이언트의 그룹 멤버십을 검색하도록 ID 트래픽을 줄일 수 있습니다.

IdM 클라이언트가 서비스 티켓을 평가할 때 프로세스에는 다음 단계가 포함됩니다.

1. 평가 프로세스에 사용되는 Kerberos 클라이언트 라이브러리는 PAC 데이터를 SSSD PAC 응답자에게 보냅니다.

2. PAC 응답자는 PAC에서 그룹 SIDs를 확인하고 사용자를 SSSD 캐시의 해당 그룹에 추가합니다. SSSD는 새 서비스에 액세스할 때 각 사용자에 대해 여러 TGT 및 티켓을 저장합니다.

3. 이제 확인된 그룹에 속하는 사용자는 IdM 측에서 필요한 서비스에 액세스할 수 있습니다.

5.1.3.2. Active Directory 사용자 및 ID 관리 그룹

Active Directory 사용자 및 그룹을 관리할 때 개별 AD 사용자 및 전체 AD 그룹을 Identity Management 그룹에 추가할 수 있습니다.

AD 사용자에 대해 IdM 그룹을 구성하는 방법에 대한 자세한 내용은 5.3.3절. “ActiveActive Directory HAT;Directory 사용자를 위한 IdM 그룹 생성” 을 참조하십시오.

비POSIX 외부 그룹 및 InstallPlan 매핑

IdM LDAP의 그룹 멤버십은 그룹 멤버인 LDAP 오브젝트의 고유 이름(DN)을 지정하여 표시됩니다. AD 항목이 동기화되지 않거나 IdM에 복사되지 않습니다. 즉, AD 사용자 및 그룹에 IdM LDAP에 LDAP 오브젝트가 없습니다. 따라서 IdM LDAP에서 그룹 멤버십을 표현하는 데 직접 사용할 수 없습니다.

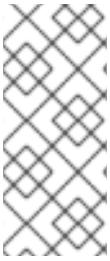
이러한 이유로 IdM은 비POSIX 외부 그룹을 생성합니다. 즉 AD 사용자 및 그룹의 InstallPlans에 대한 참조가 포함된 프록시 LDAP 오브젝트를 문자열로 생성합니다. 그런 다음, IdM이 아닌 외부 그룹을 일반 IdM LDAP 오브젝트로 참조하여 IdM의 AD 사용자 및 그룹의 그룹 멤버십을 식별합니다.

POSIX 이외의 외부 그룹은 SSSD에 의해 처리됩니다. SSSD는 AD 사용자가 IdM의 POSIX 그룹에 속하는 그룹의 InstallPlan을 매핑합니다. AD 측의 InstallPlan은 사용자 이름과 연결되어 있습니다. IdM 리소스에 액세스하는 데 사용자 이름을 사용하는 경우, IdM의 SSSD는 사용자 이름을 SID로 해석한 다음, 5.1.3.1절. “ActiveActive Directory HAT;Directory PACs 및 IdM 티켓” 에 설명된 대로 AD 도메인 내의 해당 FlexVolume에 대한 정보를 조회합니다.

ID 범위

Linux에서 사용자가 생성되면 사용자 ID 번호가 할당됩니다. 또한 사용자를 위해 개인 그룹이 생성됩니다. 개인 그룹 ID 번호는 사용자 ID 번호와 동일합니다. Linux 환경에서는 충돌이 발생하지 않습니다. 그러나 Windows에서는 도메인의 모든 오브젝트에 대해 보안 ID 번호가 고유해야 합니다.

신뢰할 수 있는 AD 사용자에게는 Linux 시스템에서 UID 및 GID 번호가 필요합니다. IdM을 통해 이 UID 및 GID 번호를 생성할 수 있지만 AD 항목에 이미 할당된 UID와 GID 번호가 할당되어 있는 경우 다른 번호를 할당하면 충돌이 발생합니다. 이러한 충돌을 방지하려면 UID 및 GID 번호 및 기본 로그인 쉘을 포함하여 AD 정의 POSIX 속성을 사용할 수 있습니다.



참고

AD는 global catalog 에 있는 모든 객체에 대한 정보의 서브 세트를 저장합니다. 글로벌 카탈로그에는 마스트의 모든 도메인에 대한 모든 항목이 포함되어 있습니다. AD 정의 POSIX 속성을 사용하려면 먼저 속성을 글로벌 카탈로그에 복제하는 것이 좋습니다.

신뢰가 생성되면 IdM은 사용할 ID 범위를 자동으로 감지하고 신뢰에 추가된 AD 도메인의 고유 ID 범위를 생성합니다. 다음 옵션 중 하나를 ipa trust-add 명령에 전달하여 수동으로 선택할 수도 있습니다.

ipa-ad-trust

이 범위 옵션은 SID를 기반으로 IdM에서 생성한 ID 알고리즘에 사용됩니다.

IdM에서 SID-to-POSIX ID 매핑을 사용하여 SID를 생성하는 경우 AD 및 IdM 사용자 및 그룹의 ID 범위가 고유하고 겹치지 않는 ID 범위를 사용할 수 있어야 합니다.

ipa-ad-trust-posix

이 범위 옵션은 AD 항목의 POSIX 특성에 정의된 ID에 사용됩니다.

IdM은 AD의 글로벌 카탈로그 또는 디렉터리 컨트롤러에서 uidNumber 및 gidNumber 를 비롯한 POSIX 속성을 가져옵니다. AD 도메인이 올바르게 관리되고 ID 충돌이 없는 경우 이러한 방식으로 생성된 ID 번호가 고유합니다. 이 경우 ID 검증 또는 ID 범위가 필요하지 않습니다.

예를 들면 다음과 같습니다.

```
[root@ipaserver ~]# ipa trust-add name_of_the_trust --range-type=ipa-ad-trust-posix
```

다른 ID 범위를 사용하여 신뢰 재생성

생성된 신뢰의 ID 범위가 배포에 적합하지 않으면 다른 --range-type 옵션을 사용하여 신뢰를 다시 만들 수 있습니다.

1. 현재 사용 중인 모든 ID 범위를 확인합니다.

```
[root@ipaserver ~]# ipa idrange-find
```

목록에서 ipa trust-add 명령으로 생성된 ID 범위의 이름을 확인합니다. ID 범위 이름의 첫

*번째 부분은 **trust: name_of_the_trust_id_range**의 이름입니다(예: **ad.example.com**).*

2. *(선택 사항) 어떤 **--range-type** 옵션, **ipa-ad-trust** 또는 **ipa-ad-trust-posix** 을(를) 모르는 경우, 신뢰할 수 있는 경우 옵션을 확인합니다.*

```
[root@ipaserver ~]# ipa idrange-show name_of_the_trust_id_range
```

5단계에서 새 신뢰에 대한 반대의 유형을 선택하도록 유형을 기록해 두십시오.

3. ***ipa trust-add** 명령으로 생성된 범위를 제거합니다.*

```
[root@ipaserver ~]# ipa idrange-del name_of_the_trust_id_range
```

4. *신뢰를 제거하십시오.*

```
[root@ipaserver ~]# ipa trust-del name_of_the_trust
```

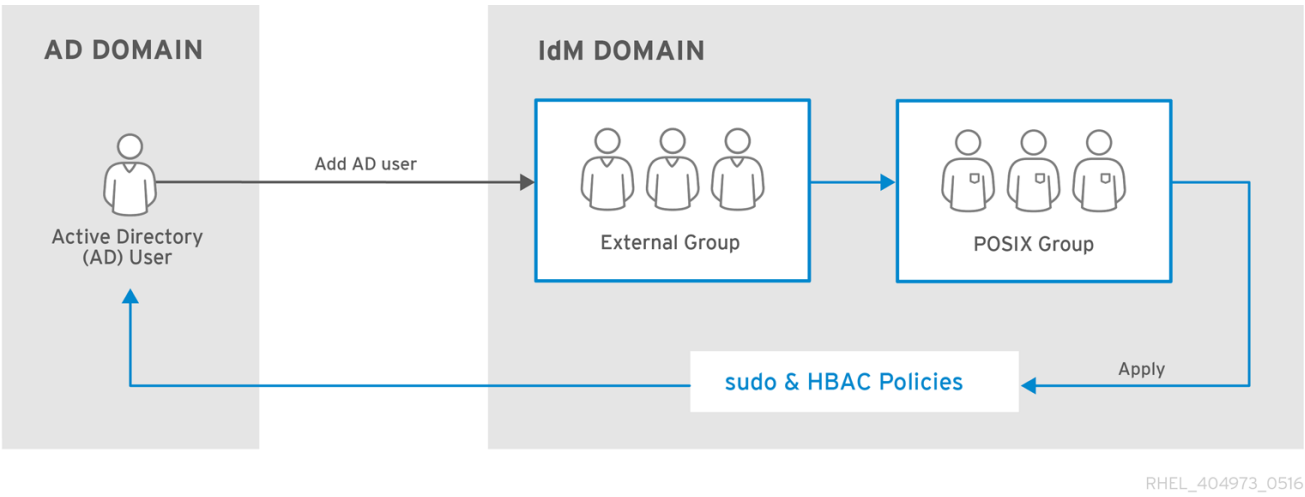
5. *올바른 **--range-type** 옵션을 사용하여 새 신뢰를 생성합니다. 예를 들면 다음과 같습니다.*

```
[root@ipaserver ~]# ipa trust-add name_of_the_trust --range-type=ipa-ad-trust
```

5.1.3.3. Active Directory 사용자 및 IdM 정책 및 구성

***SELinux**, 호스트 기반 액세스 제어, **sudo** 및 **netgroups**와 같은 여러 **IdM** 정책 정의는 사용자 그룹에 의존하여 정책 적용 방법을 식별합니다.*

그림 5.4. ActiveActive DirectoryDirectory 사용자 및 IdM 그룹 및 정책



Active Directory 사용자는 IdM 도메인 외부에 있지만 해당 그룹이 5.1.3.2절. “Active Directory 사용자 및 ID 관리 그룹” 에 설명된 외부 그룹으로 구성된 한 IdM 그룹에 그룹 멤버로 추가할 수 있습니다. 이러한 경우 sudo, 호스트 기반 액세스 제어 및 기타 정책이 외부 POSIX 그룹에 적용되며 궁극적으로 IdM 도메인 리소스에 액세스할 때 AD 사용자에게 적용됩니다.

티켓의 PAC의 사용자 6.7이 AD ID로 확인됩니다. 즉, ActiveActive Directory HAT;Directory 사용자는 정규화된 사용자 이름 또는 해당 SID를 사용하여 그룹 멤버로 추가할 수 있습니다.

5.1.4. one-Way and two-Way Trusts

IdM은 IdM에서 서비스 연결을 설정할 수 있는 엔티티가 AD로만 제한되거나 IdM 엔티티를 포함할 수 있는지에 따라 두 가지 유형의 신뢰 계약을 지원합니다.

단방향 신뢰

AD 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있지만 다른 방법은 액세스할 수 없습니다. IdM 도메인은 AD 포리스트를 신뢰하지만 AD 포리스트에서는 IdM 도메인을 신뢰하지 않습니다.

단방향 신뢰는 신뢰를 생성하기 위한 기본 모드입니다.

양방향 신뢰

AD 사용자 및 그룹은 양방향 신뢰를 통해 IdM의 리소스에 액세스할 수 있습니다. 신뢰할 수 있도록 S4U2Self 및 S4U2Proxy Microsoft 확장 기능을 사용하는 Microsoft SQL Server와 같은 솔루션에 대해 양방향 신뢰를 구성해야 합니다. RHEL IdM 호스트의 애플리케이션에서 AD 사용자에 대한 Active Directory 도메인 컨트롤러에서 S4U2Self 또는 S4U2Proxy 정보를 요청할 수 있으며 양방향 신뢰는 이 기능을 제공합니다.

이 양방향 신뢰 기능은 IdM 사용자가 Windows 시스템에 로그인할 수 없으며 IdM의 양방향 신뢰는 사용자에게 AD의 단방향 신뢰 솔루션에 비해 추가 권한을 부여하지 않습니다.

단방향 및 양방향 신뢰에 대한 자세한 내용은 5.1.1절. “신뢰 관계의 아키텍처” 를 참조하십시오.

신뢰를 설정한 후에는 유형을 변경할 수 없습니다. 다른 유형의 신뢰가 필요한 경우 ipa trust-add 명령을 다시 실행합니다. 이렇게 하면 기존 신뢰를 삭제하고 새 신뢰를 설정할 수 있습니다.

5.1.5. ActiveActive Directory illustrated;Directory에 대한 외부 신뢰

외부 신뢰는 다른 마스트에 있는 도메인 간의 신뢰 관계입니다. Forlege 신뢰는 항상 ActiveActive Directory HAT;Directory forests의 루트 도메인 간의 신뢰를 설정하는 데 필요한 반면, 섬 내의 모든 도메인에 대한 외부 신뢰를 설정할 수 있습니다.

외부 신뢰는 양도할 수 없습니다. 따라서 다른 ActiveActive Directory 6.7;Directory 도메인의 사용자 및 그룹은 IdM 리소스에 액세스할 수 없습니다. 자세한 내용은 “양도할 수 없는 신뢰할 수 있습니다.” 에서 참조하십시오.

5.1.6. 신뢰 컨트롤러 및 신뢰 에이전트

IdM은 ActiveActive Directory illustrated;Directory에 대한 신뢰를 지원하는 다음과 같은 유형의 IdM 서버를 제공합니다.

신뢰 컨트롤러

신뢰할 수 있고 ActiveActive Directory Long;Directory 도메인 컨트롤러 (DC)에 대해 ID 조회를 수행할 수 있는 IdM 서버입니다. ActiveActive Directory qcow;Directory 도메인 컨트롤러는 ActiveActive Directory qcow;Directory에 대한 트러스트를 설정 및 확인할 때 신뢰 컨트롤러에 연결합니다. 신뢰를 구성할 때 첫 번째 신뢰 컨트롤러가 생성됩니다.

IdM 서버를 신뢰 컨트롤러로 구성하는 방법에 대한 자세한 내용은 5.2.2절. “신뢰 생성” 을 참조하십시오.

신뢰 컨트롤러는 신뢰 에이전트에 비해 더 많은 양의 네트워크 연결 서비스를 실행하므로 잠재적인 침입자에 대한 더 큰 공격 면적을 제공합니다.

신뢰 에이전트

ActiveActive Directory etcdctl;Directory 도메인 컨트롤러에 대해 ID 조회를 수행할 수 있는 IdM 서버입니다.

IdM 서버를 신뢰 에이전트로 구성하는 방법에 대한 자세한 내용은 5.2.2.1.1절. "신뢰를 위한 IdM 서버 준비" 을 참조하십시오.

IdM 도메인에는 신뢰 컨트롤러 및 에이전트 외에도 역할이 없는 복제본을 포함할 수 있습니다. 그러나 이러한 서버는 ActiveActive Directory Long;Directory와 통신하지 않습니다. 따라서 이러한 서버와 통신하는 클라이언트는 ActiveActive Directory 6.7;Directory 사용자 및 그룹을 확인하거나 ActiveActive Directory HAT;Directory 사용자를 인증하고 권한을 부여할 수 없습니다.

표 5.1. 신뢰 컨트롤러 및 신뢰 에이전트에서 제공하는 기능 비교

기능	신뢰 컨트롤러	신뢰 에이전트
ActiveActive Directorysetup;Directory 사용자 및 그룹 해결	있음	있음
신뢰할 수 있는 ActiveActive Directory Long;Directory forests에서 사용자가 액세스할 수 있는 서비스를 실행하는 IdM 클라이언트 등록	있음	있음
신뢰 관리 (예: 신뢰 계약 추가)	있음	없음

신뢰 컨트롤러 및 신뢰 에이전트의 배포를 계획할 때 다음 지침을 고려하십시오.

- *Identity Management 배포당 두 개 이상의 신뢰 컨트롤러를 구성합니다.*
- *각 데이터 센터에 두 개 이상의 신뢰 컨트롤러를 구성합니다.*

추가 신뢰 컨트롤러를 생성하거나 기존 신뢰 컨트롤러가 실패하는 경우 신뢰 에이전트 또는 복제본을 승격하여 새 신뢰 컨트롤러를 생성합니다. 이렇게 하려면 5.2.2.1.1절. "신뢰를 위한 IdM 서버 준비" 에 설명된 대로 IdM 서버에서 ipa-adtrust-install 유틸리티를 사용하십시오.

중요

기존 신뢰 컨트롤러를 신뢰 에이전트로 다운그레이드할 수 없습니다. 설치 후 신뢰 컨트롤러 서버 역할은 토폴로지에서 제거할 수 없습니다.

5.2. 대만의 신뢰 생성

5.2.1. 환경 및 머신 요구 사항

신뢰 계약을 구성하기 전에 **ActiveActive DirectoryDirectory** 및 **Identity Management** 서버, 시스템 및 환경이 이 섹션에 설명된 요구 사항과 설정을 모두 충족하는지 확인하십시오.

5.2.1.1. 지원되는 Windows 플랫폼

다음과 같은 섬기 및 도메인 기능 수준을 사용하는 **ActiveActive Directory Long;Directory forests** 와의 신뢰 관계를 설정할 수 있습니다.

- 포리스트 기능 수준 범위: **Windows Server 2008 - Windows Server 2016**
- 도메인 기능 수준 범위: **Windows Server 2008 - Windows Server 2016**

다음과 같은 운영 체제가 언급 된 기능 수준을 사용하여 신뢰를 설정하기 위해 지원 및 테스트됩니다.

- **Windows Server 2012 R2**
- **Windows Server 2016**

이전 버전의 **Windows Server**는 신뢰를 설정하는 데 지원되지 않습니다.

5.2.1.2. DNS 및 realm 설정

신뢰를 구축하기 위해 **Active Directory** 및 **Identity Management**에는 특정 **DNS** 구성이 필요합니다.

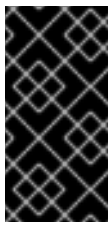
고유한 기본 **DNS** 도메인

각 시스템에는 고유한 기본 **DNS** 도메인이 구성되어 있어야 합니다. 예를 들면 다음과 같습니다.

- **ad.example.com for AD** 및 **idm.example.com for IdM**

- *AD의 경우 example.com 및 IdM용 idm.example.com*

- *ad.example.com for AD 및 example.com for IdM*



중요

IdM 도메인이 AD 도메인의 상위 도메인인 경우 IdM 서버를 Red Hat Enterprise Linux 7.5 이상에서 실행해야 합니다.

가장 편리한 관리 솔루션은 각 DNS 도메인이 통합된 DNS 서버에서 관리되지만 다른 표준 호환 DNS 서버도 사용할 수 있는 환경입니다.

ID 관리를 위해 AD 또는 IdM이 기본 DNS 도메인을 다른 시스템과 공유할 수 없습니다. 자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드 의 호스트 이름 및 DNS 구성 요구 사항에 대한 설명서를 참조하십시오.

Kerberos 영역 이름: 기본 DNS 도메인 이름의 대문자 버전

Kerberos 영역 이름은 모든 문자 대문자와 기본 DNS 도메인 이름과 동일해야 합니다. 예를 들어 도메인 이름이 AD용 ad.example.com 이고 IdM용 idm.example.com 인 경우 Kerberos 영역 이름은 AD.EXAMPLE.COM 및 IDM.EXAMPLE.COM 여야 합니다.

신뢰의 모든 DNS 도메인에서 DNS 레코드를 확인할 수 있음

모든 머신은 신뢰 관계에 관련된 모든 DNS 도메인의 DNS 레코드를 확인할 수 있어야 합니다.

- *IdM DNS를 구성할 때 IdM 도메인 내에서 DNS 서비스 구성 및 Linux 도메인 ID, 인증 및 정책 가이드에서 DNS 전달 관리 섹션 의 섹션에 설명된 지침을 따르십시오.*

- *통합된 DNS 없이 IdM을 사용하는 경우 Linux 도메인 ID, 인증 및 정책 가이드에 통합된 DNS 없이 서버 설치를 설명하는 섹션에 설명된 지침을 따르십시오.*

IdM과 AD DNS 도메인 간의 중복 없음

IdM에 연결된 시스템은 여러 DNS 도메인에 배포할 수 있습니다. IdM 클라이언트를 포함하는 DNS 도메인은 AD에 연결된 시스템이 포함된 DNS 도메인과 겹치지 않아야 합니다. 기본 IdM DNS 도메인에는 AD 트러스트를 지원하기 위해 적절한 SRV 레코드가 있어야 합니다.

참고

IdM과 ActiveActive Directory 6.7;Directory 간의 신뢰가 있는 일부 환경에서는 ActiveActive Directory HAT;Directory DNS 도메인의 일부인 호스트에 IdM 클라이언트를 설치할 수 있습니다. 그러면 호스트는 Linux 중심 IdM 기능을 활용할 수 있습니다. 이는 권장되는 구성이 아니며 몇 가지 제한 사항이 있습니다. Red Hat은 항상 ActiveActive Directory illustrated;Directory가 소유한 것과 다른 DNS 영역에 IdM 클라이언트를 배포하고 IdM 호스트 이름을 통해 IdM 클라이언트에 액세스하는 것이 좋습니다.

$ ipa dns-update-system- records --dry-run 명령을 실행하여 시스템 설정과 관련된 필수 SRV 레코드 목록을 가져올 수 있습니다.

생성된 목록은 다음과 같이 나타날 수 있습니다.

```
$ ipa dns-update-system-records --dry-run
 IPA DNS records:
 _kerberos-master._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos-master._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos.example.com. 86400 IN TXT "EXAMPLE.COM"
 _kpasswd._tcp.example.com. 86400 IN SRV 0 100 464 server.example.com.
 _kpasswd._udp.example.com. 86400 IN SRV 0 100 464 server.example.com.
 _ldap._tcp.example.com. 86400 IN SRV 0 100 389 server.example.com.
 _ntp._udp.example.com. 86400 IN SRV 0 100 123 server.example.com.
```

동일한 IdM 영역에 속하는 다른 DNS 도메인의 경우 AD에 대한 신뢰가 구성될 때 SRV 레코드를 구성할 필요가 없습니다. 이유는 AD 도메인 컨트롤러에서 SRV 레코드를 사용하여 KDC 레코드를 검색하는 대신 신뢰의 이름 접미사 라우팅 정보를 KDC 검색에 기반하기 때문입니다.

DNS 구성 확인

신뢰를 구성하기 전에 Identity Management 및 Active Directory 서버가 서로 해결할 수 있는지 확인합니다.

아래에 설명된 명령을 실행해도 예상 결과가 표시되지 않으면 명령이 실행된 호스트에서 DNS 구성을 검사합니다. 호스트 구성이 올바르면 상위 도메인에서 하위 도메인으로 DNS 위임이 올바르게 설정되어 있는지 확인합니다.

따라서 AD는 DNS 조회 결과를 캐시하고 DNS에서 변경한 내용이 즉시 표시되지 않는 경우가 있습니다. ipconfig /flushdns 명령을 실행하여 현재 캐시를 삭제할 수 있습니다.

*신뢰 설정에 사용되는 **IdM** 도메인 서버에서 **IdM** 호스트 서비스를 확인할 수 있는지 확인합니다.*

1. ***UDP**를 통한 **Kerberos** 및 **TCP** 서비스 레코드를 통해 **LDAP**에 대한 **DNS** 쿼리를 실행합니다.*

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.ipa.example.com.
0 100 88 ipamaster1.ipa.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.ipa.example.com.
0 100 389 ipamaster1.ipa.example.com.
```

*명령에는 모든 **IdM** 서버가 나열되어야 합니다.*

2. ***IdM Kerberos** 영역 이름으로 **TXT** 레코드에 대한 **DNS** 쿼리를 실행합니다. 얻은 값은 **IdM**을 설치할 때 지정한 **Kerberos** 영역과 일치해야 합니다.*

```
[root@ipaserver ~]# dig +short -t TXT _kerberos.ipa.example.com.
IPA.EXAMPLE.COM
```

3. *5.2.2.1.1절. “신뢰를 위한 IdM 서버 준비” 에 설명된 대로 **ipa-adtrust-install** 유틸리티를 실행한 후 **UDP** 및 **LDAP over TCP** 서비스 레코드에 대한 **DNS** 쿼리를 실행합니다.*

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.ipa.example.com.
0 100 88 ipamaster1.ipa.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ipa.example.com.
0 100 389 ipamaster1.ipa.example.com.
```

*명령은 **ipa-adtrust-install** 이 실행된 모든 **IdM** 서버를 나열해야 합니다. 일반적으로 첫 번째 신뢰 관계를 구축하기 전에 **ipa-adtrust-install** 이 **IdM** 서버에서 실행되지 않은 경우 출력이 비어 있습니다.*

***IdM**이 **AD**의 서비스 레코드를 확인할 수 있는지 확인*

***UDP**를 통한 **Kerberos** 및 **TCP** 서비스 레코드를 통해 **LDAP**에 대한 **DNS** 쿼리를 실행합니다.*

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

이러한 명령은 **AD** 도메인 컨트롤러의 이름을 반환해야 합니다.

AD 서버에서 **IdM** 호스트 서비스를 확인할 수 있는지 확인합니다.

1. **AD** 서버에서 서비스 레코드를 조회하도록 **nslookup.exe** 유틸리티를 설정합니다.

```
C:\>nslookup.exe
> set type=SRV
```

2. **UDP**를 통한 **Kerberos**의 도메인 이름과 **TCP** 서비스 레코드를 통한 **LDAP**를 입력합니다.

```
> _kerberos._udp.ipa.example.com.
_kerberos._udp.ipa.example.com.       SRV service location:
    priority       = 0
    weight         = 100
    port           = 88
    svr hostname   = ipamaster1.ipa.example.com
> _ldap._tcp.ipa.example.com
_ldap._tcp.ipa.example.com       SRV service location:
    priority       = 0
    weight         = 100
    port           = 389
    svr hostname   = ipamaster1.ipa.example.com
```

예상되는 출력에는 *신뢰 설정에 사용되는 IdM 도메인 서버에서 IdM 호스트 서비스를 확인할 수 있는지 확인합니다.* 에 표시된 것과 동일한 **IdM** 서버 세트가 포함되어 있습니다.

3. 서비스 유형을 **TXT**로 변경하고 **IdM Kerberos** 영역 이름을 사용하여 **TXT** 레코드에 대한 **DNS** 쿼리를 실행합니다.

```
C:\>nslookup.exe
> set type=TXT
> _kerberos.ipa.example.com.
_kerberos.ipa.example.com.       text =

    "IPA.EXAMPLE.COM"
```

출력에는 *신뢰 설정에 사용되는 IdM 도메인 서버에서 IdM 호스트 서비스를 확인할 수 있는지 확인합니다.* 에 표시된 값과 동일한 값이 포함되어야 합니다.

4. *5.2.2.1.1절. “신뢰를 위한 IdM 서버 준비”* 에 설명된 대로 **ipa-adtrust-install** 유틸리

*티를 실행한 후 **UDP** 및 **LDAP over TCP** 서비스 레코드에 대한 **DNS** 쿼리를 실행합니다.*

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.ipa.example.com.
_kerberos._udp.dc._msdcs.ipa.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = ipamaster1.ipa.example.com
> _ldap._tcp.dc._msdcs.ipa.example.com.
_ldap._tcp.dc._msdcs.ipa.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = ipamaster1.ipa.example.com
```

*명령은 **ipa-adtrust-install** 유틸리티가 실행된 모든 **IdM** 서버를 나열해야 합니다. 일반적으로 첫 번째 신뢰 관계를 구축하기 전에 **ipa-adtrust-install** 이 **IdM** 서버에서 실행되지 않은 경우 출력이 비어 있습니다.*

***AD** 서버에서 **AD** 서비스를 확인할 수 있는지 확인합니다.*

1. *AD 서버에서 서비스 레코드를 조회하도록 **nslookup.exe** 유틸리티를 설정합니다.*

```
C:\>nslookup.exe
> set type=SRV
```

2. *UDP를 통한 Kerberos의 도메인 이름과 TCP 서비스 레코드를 통한 LDAP를 입력합니다.*

```
> _kerberos._udp.dc._msdcs.ad.example.com.
_kerberos._udp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = addc1.ad.example.com
> _ldap._tcp.dc._msdcs.ad.example.com.
_ldap._tcp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = addc1.ad.example.com
```

*예상되는 출력에는 **IdM이 AD의 서비스 레코드를 확인할 수 있는지 확인** 에 표시된 것과 동일한 **AD** 서버 세트가 포함되어 있습니다.*

5.2.1.3. NetBIOS Names

<.> name은 ActiveActive Directory Long;Directory (AD) 도메인을 식별하고 IdM 도메인 및 서비스를 식별하기 위해 AD로 구성된 신뢰가 있는 경우 중요합니다. 따라서est 신뢰를 설정하려는 AD 도메인에 사용된 수행하려면 IdM 도메인에 대해 다른ResourceOverride 이름을 사용해야 합니다.

ActiveActive Directory we;Directory 또는 IdM 도메인은 일반적으로 해당 DNS 도메인의 far-left 구성 요소입니다. 예를 들어 DNS 도메인이 ad.example.com 이면 일반적으로 AD 입니다.For example, if the DNS domain is ad.example.com.

참고

name의 최대 길이는 15자입니다.

5.2.1.4. 방화벽 및 포트

AD 도메인 컨트롤러와 IdM 서버 간의 통신을 활성화하려면 다음 포트 요구 사항을 충족해야 합니다.

- IdM 서버에서 AD 서버, IdM 서버에서 AD 도메인 컨트롤러로의 모든 AD 도메인 컨트롤러에 필요한 IdM 서버 및 모든 AD 도메인 컨트롤러에 필요한 포트를 엽니다.

- 신뢰할 수 있는 AD 마이스트의 모든 AD 도메인 컨트롤러에 대한 AD 신뢰에서 IdM 클라이언트에 필요한 포트를 엽니다. IdM 클라이언트에서 포트가 발신 방향으로 열려 있는지 확인합니다(Linux 도메인 ID, 인증 및 정책 가이드에 클라이언트 설치 사전 요구 사항 참조).

표 5.2. AD Trust에 필요한 포트

Service	포트	프로토콜
끝점 확인 포트 매퍼	135	TCP
NetBIOS-DGM	138	TCP 및 UDP
NetBIOS-SSN	139	TCP 및 UDP
Microsoft-DS	445	TCP 및 UDP
끝점 매퍼 리스너 범위	1024-1300	TCP
AD 글로벌 카탈로그	3268	TCP

Service	포트	프로토콜
LDAP	389	TCP [a] 및 UDP
[a] 신뢰를 위해 IdM 서버에서 TCP 포트 389를 열 필요는 없지만 IdM 서버와 통신하는 클라이언트는 필요합니다.		

표 5.3. 보안에서 IdM 서버에서 필요한 포트

Service	포트	프로토콜
Kerberos	*Linux 도메인 ID, 인증 및 정책 가이드*의 포트 요구 사항을 참조하십시오.	
LDAP		
DNS		

표 5.4. AD Trust에서 IdM 클라이언트가 필요로 하는 포트

Service	포트	프로토콜	참고
Kerberos	88	UDP 및 TCP	**libkrb5** 라이브러리는 UDP를 사용하고 Kerberos 배포 센터(KDC)에서 전송된 데이터가 너무 크면 TCP 프로토콜로 대체됩니다. ActiveActive Directory HAT;Directory는 Kerberos 티켓에 Privilege Attribute 인증서 (PAC)를 첨부하여 크기를 늘리고 대부분의 경우 TCP 프로토콜을 사용해야 합니다. Red Hat Enterprise Linux 7.4의 SSSD는 기본적으로 사용자 인증에 TCP를 사용합니다. **libkrb5** 가 TCP를 사용하기 전에 크기를 구성하려면 **/etc/krb.5.conf** 파일에 ***udp_preference_limit*** 를 설정합니다. 자세한 내용은 krb5.conf(5) 도움말 페이지를 참조하십시오.

추가 리소스

- *필요한 포트를 여는 방법에 대한 자세한 내용은 **Linux** 도메인 **ID,** 인증 및 정책 가이드 의 포트 요구 사항을 참조하십시오.*

5.2.1.5. IPv6 설정

***IdM** 시스템에는 커널에서 **IPv6** 프로토콜이 활성화되어 있어야 합니다. **IPv6**이 비활성화되면 **IdM** 서비스에서 사용하는 **CLDAP** 플러그인이 초기화되지 않습니다.*

5.2.1.6. 클럭 설정

***ActiveActive Directory QCOW;Directory** 서버와 **IdM** 서버에 시계가 동기화되어 있어야 합니다.*

5.2.1.7. AD에서 IdM 도메인용 Conditional Forwarder 생성

IdM 도메인에 대한 쿼리를 IdM DNS 서버로 전달하도록 AD DNS 서버를 준비합니다.

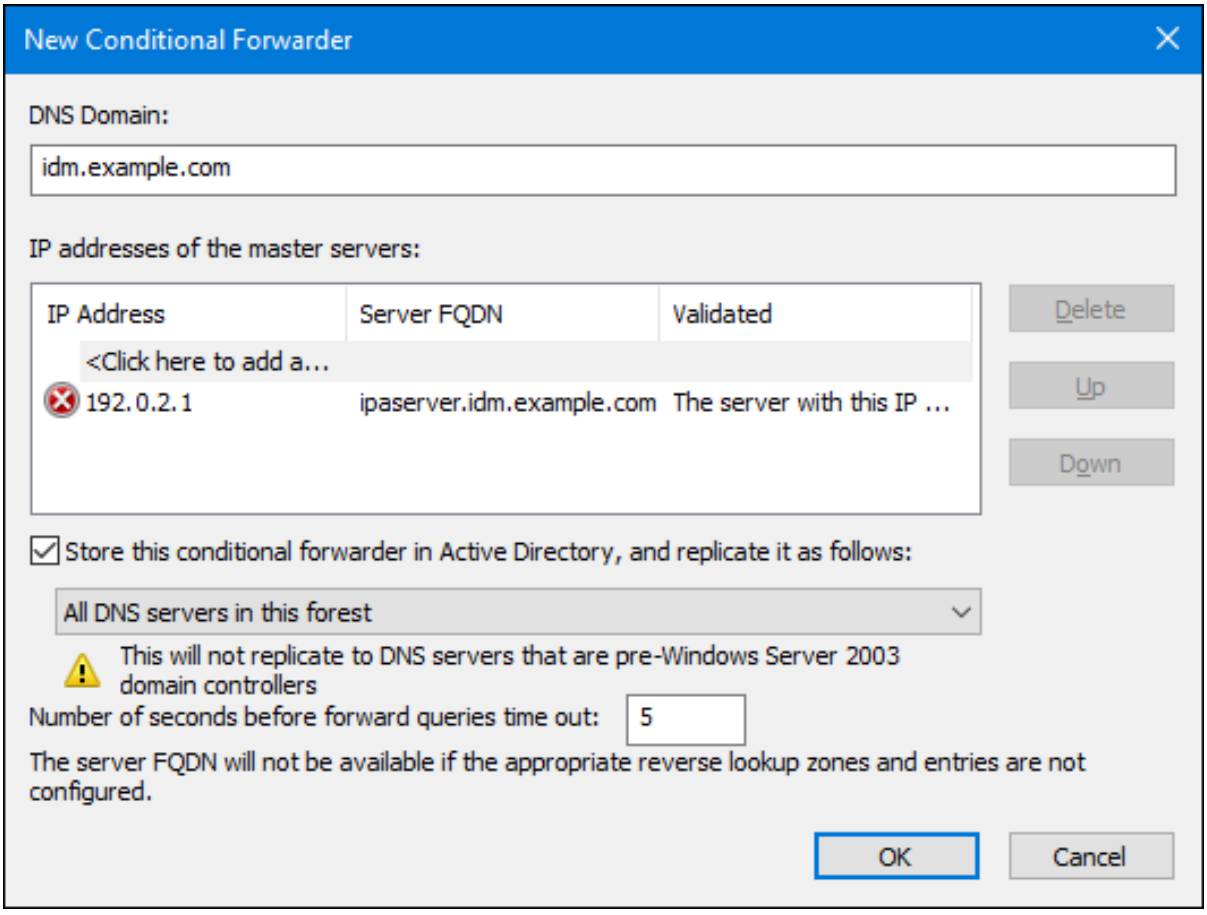
1. **Windows AD 도메인 컨트롤러에서 AD(Active Directory) DNS 콘솔을 엽니다.**

2. **Conditional Forwarder 를 마우스 오른쪽 버튼으로 클릭하고 New Conditional Forwarder 를 선택합니다.**

3. **IdM DNS 도메인 이름 및 IdM DNS 서버의 IP 주소를 입력하십시오.**

4. **Active Directory에서 이 조건부 전달자를 저장하고 다음과 같이 복제 한 다음 환경과 일치하는 복제 설정을 선택합니다.**

5. **OK를 클릭합니다.**



6.

AD 도메인 컨트롤러(DC)가 IdM 도메인에서 DNS 항목을 확인할 수 있는지 확인하려면 명령 프롬프트를 열고 다음을 입력합니다.

```
C:\> nslookup server.idm.example.com
```

명령에서 IdM 서버의 IP 주소를 반환하는 경우 조건부 전달자가 올바르게 작동합니다.

5.2.1.8. IdM에서 AD 도메인의 앞으로 영역 생성

AD 도메인에 대한 쿼리를 AD DNS 서버로 전달하려면 IdM DNS 서버를 준비합니다.

1. IdM 서버에서 AD DNS 도메인에 대한 전달 영역 항목을 생성합니다. IdM에서 DNS 전달 영역 생성에 대한 자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드 의 전달 영역 구성 섹션을 참조하십시오.

2. AD DNS 서버가 DNSSEC를 지원하지 않는 경우 IdM 서버에서 DNSSEC 검증을 비활성화합니다.

   a. /etc/named.conf 파일을 편집하고 dnssec-validation 매개변수를 no 로 설정합니다.

   ```
   dnssec-validation no;
   ```

   b. named-pkcs11 서비스를 다시 시작하십시오.

   ```
   # systemctl restart named-pkcs11
   ```

3. IdM 서버가 AD 도메인의 DNS 항목을 확인할 수 있는지 확인하려면 다음을 입력합니다.

```
# host server.ad.example.com
```

명령이 AD DC의 IP 주소를 반환하면 전달 영역이 올바르게 작동합니다.

5.2.1.9. 지원되는 사용자 이름 형식

IdM은 로컬 SSSD 클라이언트에서 사용자 이름 매핑을 수행합니다. SSSD에서 지원하는 신뢰할 수 있는 도메인에서 사용자의 기본 출력 사용자 이름 형식은 user_name@domain 입니다. ActiveActive

Directory HAT;Directory는 user_name , user_name @DOMAIN_NAME 및 DOMAIN_NAME\user_name 등 다양한 종류의 이름 형식을 지원합니다.

사용자는 사용자 이름(user_name) 또는 정규화된 사용자 이름(user_name@domain_name)만 사용하여 시스템에 인증할 수 있습니다.

주의

보다 바람직하게는 동일한 사용자 이름이 여러 도메인에 있는 경우 충돌을 피하기 위해 정규화된 사용자 이름을 사용합니다.

사용자가 도메인을 제외한 사용자 이름만 지정하는 경우 SSSD는 /etc/sssd/sssd.conf 파일과 신뢰할 수 있는 도메인에 구성된 모든 도메인에서 계정을 검색합니다. 8.5.3절. "IdM 클라이언트의 도메인 확인 순서 구성" 에 설명된 도메인 확인 순서를 구성한 경우 SSSD는 정의된 순서로 사용자를 검색합니다. 어떠한 경우에도 SSSD는 발견된 첫 번째 항목을 사용합니다. 이로 인해 여러 도메인에 동일한 사용자 이름이 있고 발견된 첫 번째 항목이 예상되지 않은 경우 문제가 발생하거나 혼동될 수 있습니다.

기본적으로 SSSD는 항상 정규화된 형식으로 사용자 이름을 표시합니다. 형식 변경에 대한 자세한 내용은 5.5절. "SSSD로 표시되는 사용자 이름 형식 변경" 을 참조하십시오.

SSSD는 사용자 이름과 사용자 이름이 속하는 도메인을 식별하기 위해 re_expression 옵션에 정의된 정규식을 사용합니다. 정규식은 IdM 백엔드 또는 AD 백엔드에 사용되며 언급된 모든 형식을 지원합니다.

```
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
```

5.2.2. 신뢰 생성

다음 섹션에서는 다양한 구성 시나리오에서 신뢰 생성에 대해 설명합니다. 5.2.2.1절. "명령줄에서 신뢰 생성" 에는 명령줄에서 신뢰를 구성하기 위한 전체 절차가 포함되어 있습니다. 다른 섹션에서는 이 기본 구성 시나리오와 다른 단계를 설명하고 다른 모든 단계에 대한 기본 절차를 참조합니다.

참고

기존 신뢰 환경에서 복제본을 설정하면 복제본이 신뢰 컨트롤러로 자동 구성되지 않습니다. 복제본을 추가 신뢰 컨트롤러로 구성하려면 이 섹션의 절차를 따르십시오.

신뢰를 생성한 후 5.2.3절. “cross-forest Trusts에 대한 설치 후 고려 사항” 를 참조하십시오.

5.2.2.1. 명령줄에서 신뢰 생성

IdM과 Active Directory Kerberos 영역 간의 신뢰 관계를 생성하려면 다음 단계가 포함됩니다.

1. 신뢰할 수 있도록 IdM 서버 준비 5.2.2.1.1절. “신뢰를 위한 IdM 서버 준비”
2. 에 설명된 신뢰 계약서 만들기 5.2.2.1.2절. “신뢰 계약 생성”
3. 에 설명된 Kerberos 구성 확인 5.2.2.1.3절. “Kerberos 구성 확인”

5.2.2.1.1. 신뢰를 위한 IdM 서버 준비

AD와의 신뢰 관계를 위해 IdM 서버를 설정하려면 다음 단계를 따르십시오.

1. 필요한 IdM, 신뢰 및 Samba 패키지를 설치합니다.

```
[root@ipaserver ]# yum install ipa-server ipa-server-trust-ad samba-client
```

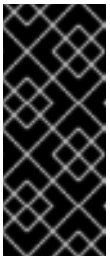
2. 신뢰할 수 있는 서비스를 활성화하도록 IdM 서버를 구성합니다. ipa-replica-install --setup-adtrust 명령을 사용하여 서버를 설치한 경우 이 단계를 건너뛸 수 있습니다.

   a. ipa-adtrust-install 유틸리티를 실행합니다.

```
[root@ipaserver ]# ipa-adtrust-install
```

유틸리티는 AD 신뢰에 필요한 DNS 서비스 레코드를 추가합니다. IdM이 통합된 DNS 서버와 함께 설치된 경우 이러한 레코드는 자동으로 생성됩니다.

*통합 **DNS** 서버 없이 **IdM**을 설치한 경우 **ipa-adtrust-install** 은 계속 진행하기 전에 **DNS**에 수동으로 추가해야 하는 서비스 레코드 목록을 출력합니다.*



중요

***Red Hat**은 특히 **IdM** 또는 **AD**가 통합 **DNS** 서버를 사용하지 않는 경우, 특히 **ipa-adtrust-install** 을 실행한 후 "DNS 구성 확인" 에 설명된 **DNS** 구성을 확인하는 것이 좋습니다.*

b.

*스크립트는 이전 **Linux** 클라이언트가 신뢰할 수 있는 사용자와 함께 작업할 수 있는 호환성 플러그인인 **slapi-nis** 플러그인을 구성하라는 메시지를 표시합니다.*

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted
users.

Enable trusted domains support in slapi-nis? [no]: y
```

c.

*디렉터리가 처음 설치될 때 하나 이상의 사용자(**IdM** 관리자)가 존재합니다. **InstallPlan** 생성 작업은 기존 사용자가 신뢰 환경을 지원할 수 있는 **SID**를 생성할 수 있습니다. 이는 리소스를 많이 사용하는 작업입니다. 많은 사용자의 경우 별도로 실행할 수 있습니다.*

```
Do you want to run the ipa-sidgen task? [no]: yes
```

3. *5.2.1.2절. "DNS 및 realm 설정" 에 설명된 대로 **DNS**가 올바르게 구성되었는지 확인합니다.*

4. ***ClusterRole** 서비스를 시작합니다.*

```
[root@ipaserver ~]# systemctl start smb
```

5. *필요한 경우 시스템이 부팅될 때 **xfs** 서비스가 자동으로 시작되도록 구성합니다.*

```
[root@ipaserver ~]# systemctl enable smb
```

6.

선택적으로 **KubeMacPool client** 유틸리티 를 사용하여 **Samba**가 **IdM** 측의 **Kerberos** 인증에 응답하는지 확인합니다.

```
[root@ipaserver ~]# smbclient -L ipaserver.ipa.example.com -k
lp_load_ex: changing to config backend registry

 Sharename       Type      Comment
 ---------       ----      -------
 IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.

 Server               Comment
 ---------            -------

 Workgroup            Master
 ---------            -------
```

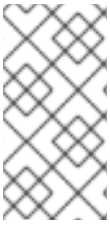
5.2.2.1.2. 신뢰 계약 생성

ipa trust-add 명령을 사용하여 **Active Directory** 도메인 및 **IdM** 도메인에 대한 신뢰 계약을 생성합니다.

```
# ipa trust-add --type=type ad_domain_name --admin ad_admin_username --password
```

ipa trust-add 명령은 기본적으로 단방향 신뢰를 설정합니다. **RHEL 7**에서 양방향 신뢰를 설정할 수 없습니다.

외부 신뢰를 설정하려면 **--external=true** 옵션을 **ipa trust-add** 명령에 전달합니다. 자세한 내용은 **5.1.5절. "ActiveActive Directory illustrated;Directory에 대한 외부 신뢰"** 을 참조하십시오.



참고

ipa trust-add 명령은 기본적으로 서버를 신뢰 컨트롤러로 구성합니다. 자세한 내용은 **5.1.6절. "신뢰 컨트롤러 및 신뢰 에이전트"** 을 참조하십시오.

다음 예제에서는 **--two-way=true** 옵션을 사용하여 양방향 신뢰를 설정합니다.

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --admin Administrator --password --
two-way=true
Active Directory domain administrator's password:
-------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
-------------------------------------------------------
```

```
Realm-Name: ad.example.com
Domain NetBIOS name: AD
Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11, S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19,
                S-1-5-18
SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11, S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19,
                S-1-5-18
Trust direction: Two-way trust
Trust type: Active Directory domain
Trust status: Established and verified
```

5.2.2.1.3. Kerberos 구성 확인

Kerberos 구성을 확인하려면 **IdM** 사용자에 대한 티켓을 받을 수 있는지 여부와 **IdM** 사용자가 서비스 티켓을 요청할 수 있는지 테스트합니다.

양방향 신뢰를 확인하려면 다음을 수행하십시오.

1. **IdM** 사용자에 대한 티켓을 요청합니다.

```
[root@ipaserver ~]# kinit user
```

2. **IdM** 도메인 내의 서비스에 대한 서비스 티켓을 요청하십시오.

```
[root@ipaserver ~]# kvno -S host ipaserver.example.com
```

3. **AD** 도메인 내에서 서비스에 대한 서비스 티켓을 요청합니다.

```
[root@ipaserver ~]# kvno -S cifs adserver.example.com
```

AD 서비스 티켓이 성공적으로 승인되면 요청된 다른 모든 티켓과 함께 **TGT(Cross-realm ticket-granting ticket)**가 표시됩니다. **TGT**의 이름은 **RHEA t finish/AD.DOMAIN@IPA.DOMAIN** 입니다.

```
[root@ipaserver ]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: user@IPA.DOMAIN
```

```
Valid starting     Expires           Service principal
06/15/12 12:13:04  06/16/12 12:12:55  krbtgt/IPA.DOMAIN@IPA.DOMAIN
06/15/12 12:13:13  06/16/12 12:12:55  host/ipaserver.ipa.example.com@IPA.DOMAIN
06/15/12 12:13:23 06/16/12 12:12:55 krbtgt/AD.DOMAIN@IPA.DOMAIN
06/15/12 12:14:58  06/15/12 22:14:58  cifs/adserver.ad.example.com@AD.DOMAIN
```

IdM 측에서 단방향 트러스트를 확인하려면 다음을 수행하십시오.

1. **ActiveActive Directory HAT;Directory 사용자에 대한 티켓을 요청하십시오.**

```
[root@ipaserver ~]# kinit user@AD.DOMAIN
```

2. **IdM 도메인 내의 서비스에 대한 서비스 티켓을 요청하십시오.**

```
[root@ipaserver ~]# kvno -S host ipaserver.example.com
```

AD 서비스 티켓이 성공적으로 승인되면 요청된 다른 모든 티켓과 함께 TGT(Cross-realm ticket-granting ticket)가 표시됩니다. TGT의 이름은 RHEA t finish/IPA.DOMAIN@AD.DOMAIN 입니다.

```
[root@ipaserver ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.DOMAIN

Valid starting       Expires             Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/ipaserver.ipa.example.com@IPA.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IPA.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
```

localauth 플러그인은 Kerberos 사용자를 로컬 SSSD 사용자 이름에 매핑합니다. 이를 통해 AD 사용자는 Kerberos 인증을 사용하고 Linux 서비스에 액세스하여 GSSAPI 인증을 직접 지원할 수 있습니다.

참고

플러그인에 대한 자세한 내용은 **5.3.7.2절. “암호가 없는 SSH 사용”** 을 참조하십시오.

5.2.2.2. 공유 보안을 사용하여 보안 생성

공유 보안은 신뢰할 수 있는 피어로 알려진 암호로, 다른 도메인에서 신뢰에 참여하는 데 사용할 수 있습니다. 공유 시크릿은 **Active Directory(AD)** 내에서 단방향 및 양방향 신뢰를 모두 구성할 수 있습니다. **AD**에서 공유 보안은 신뢰 구성 내의 신뢰할 수 있는 도메인 오브젝트 **(TDO)**로 저장됩니다.

IdM은 **AD** 관리자 자격 증명 대신 공유 시크릿을 사용하여 단방향 또는 양방향 신뢰 생성을 지원합니다. 이러한 신뢰를 설정하려면 관리자가 **AD**에서 공유 보안을 생성하고 **AD** 측에 대한 신뢰를 수동으로 검증해야 합니다.

5.2.2.2.1. 공유 보안을 사용하여 2-Way 보안 생성

Microsoft Windows Server 2012, 2012 R2 또는 **2016**과 함께 공유 보안을 사용하여 양방향 신뢰를 만들려면 다음을 수행합니다.

1. 5.2.2.1.1절. “신뢰를 위한 IdM 서버 준비” 에 설명된 대로 신뢰할 수 있도록 **IdM** 서버를 준비합니다.

2. **IdM** 및 **AD** 호스트가 두 도메인을 모두 확인할 수 없는 **DNS** 서버를 사용하는 경우 **DNS** 영역에 대한 전달을 설정합니다.

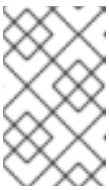
   a. **IdM** 도메인에 대한 쿼리를 **IdM DNS** 서버로 전달하도록 **AD DNS** 서버를 준비합니다. 자세한 내용은 5.2.1.7절. “AD에서 IdM 도메인용 Conditional Forwarder 생성”의 내용을 참조하십시오.

   b. **AD** 도메인에 대한 쿼리를 **AD DNS** 서버로 전달하도록 **IdM DNS** 서버를 준비합니다. 자세한 내용은 5.2.1.8절. “IdM에서 AD 도메인의 앞으로 영역 생성”의 내용을 참조하십시오.

3. **Active Directory** 도메인 및 신뢰 콘솔에 대한 신뢰 구성. 특히 중요한 요인은 다음과 같습니다.

   - 새로운 신뢰를 만듭니다.
   - 신뢰에 **IdM** 도메인 이름(예: **idm.example.com**)을 지정합니다.

- *이 값이 신뢰의 보호 유형임을 지정합니다.*
- *이 값이 양방향 유형의 신뢰임을 지정합니다.*
- *이 인증이 하이그 전체 인증임을 지정합니다.*
- *신뢰 암호 를 설정합니다.*



참고

***IdM**에서 신뢰를 구성할 때 동일한 암호를 사용해야 합니다.*

들어오는 트러스트를 확인하라는 메시지가 표시되면 아니요 를 선택합니다.

4. *5.2.2.1.2절. "신뢰 계약 생성" 에 설명된 대로 신뢰 계약을 만듭니다. **ipa trust-add** 명령을 실행하는 경우 **--type,--trust-secret** 및 **--two-way=True** 옵션을 사용하고 **--admin** 옵션을 생략합니다. 예를 들면 다음과 같습니다.*

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --trust-secret --two-way=True
Shared secret for the trust:
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19, S-1-5-18
  SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19, S-1-5-18
  Trust direction: Trusting forest
  Trust type: Active Directory domain
  Trust status: Waiting for confirmation by remote side
```

5. *도메인 목록을 검색합니다.*

```
[root@ipaserver ~]# ipa trust-fetch-domains ad_domain
```

6. **IdM 서버에서 ipa trust-show 명령을 사용하여 신뢰 관계가 설정되어 있는지 확인합니다.**

```
[root@ipaserver ~]# ipa trust-show ad.example.com

 Domain NetBIOS name: AD
 Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
 Trust direction: Trusting forest
 Trust type: Active Directory domain
```

7. **선택적으로 신뢰할 수 있는 도메인을 검색합니다.**

```
[root@ipaserver ~]# ipa trustdomain-find ad.example.com
Domain name: ad.example.com
Domain NetBIOS name: AD
Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
Domain enabled: True
```

8. **5.2.2.1.3절. "Kerberos 구성 확인" 에 설명된 대로 Kerberos 구성을 확인합니다.**

5.2.2.2.2. 공유 보안을 사용하여 일대일 신뢰 생성

Microsoft Windows Server 2012, 2012 R2 또는 2016과 함께 공유 보안을 사용하여 양방향 신뢰를 만들려면 다음을 수행합니다.

1. **5.2.2.1.1절. "신뢰를 위한 IdM 서버 준비" 에 설명된 대로 신뢰할 수 있도록 IdM 서버를 준비합니다.**

2. **IdM 및 AD 호스트가 두 도메인을 모두 확인할 수 없는 DNS 서버를 사용하는 경우 DNS 영역에 대한 전달을 설정합니다.**

   a. **IdM 도메인에 대한 쿼리를 IdM DNS 서버로 전달하도록 AD DNS 서버를 준비합니다. 자세한 내용은 5.2.1.7절. "AD에서 IdM 도메인용 Conditional Forwarder 생성"의 내용을 참조하십시오.**

   b. **AD 도메인에 대한 쿼리를 AD DNS 서버로 전달하도록 IdM DNS 서버를 준비합니다. 자세한 내용은 5.2.1.8절. "IdM에서 AD 도메인의 앞으로 영역 생성"의 내용을 참조하십시오.**

3. ***Active Directory** 도메인 및 신뢰 콘솔에서 신뢰를 구성합니다.*

   a. *도메인 이름을 마우스 오른쪽 버튼으로 클릭하고 속성 을 선택합니다.*

   b. *신뢰 탭에서 새 신뢰를 클릭합니다.*

   c. ***IdM** 도메인 이름을 입력하고 **Next** 를 클릭합니다.*

   d. ***Forest trust** 를 선택하고 **Next** 를 클릭합니다.*

   e. *단방향: 수신 을 선택하고 다음을 클릭합니다.*

   f. *이 도메인만 선택하고 다음을 클릭합니다.*

   g. *공유 시크릿(**trust password**)을 입력하고 **Next** 를 클릭합니다.*

   h. *설정을 확인하고 **Next** 를 클릭합니다.*

   i. *시스템이 들어오는 신뢰를 확인할지 묻는 메시지가 표시되면 **No**를 선택하고 들어오는 트러스트를 확인하지 말고 **Next** 를 클릭합니다.*

   j. *완료를 클릭합니다.*

4. *신뢰 계약을 생성합니다.*

```
[root@ipaserver ~]# ipa trust-add --type=ad --trust-secret ad.example.com
Shared secret for the trust: password
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-1762709870-351891212-3141221786
```

```
Trust direction: Trusting forest
Trust type: Active Directory domain
Trust status: Waiting for confirmation by remote side
```

AD Domains and Trusts 콘솔에 설정한 공유 시크릿을 입력합니다.

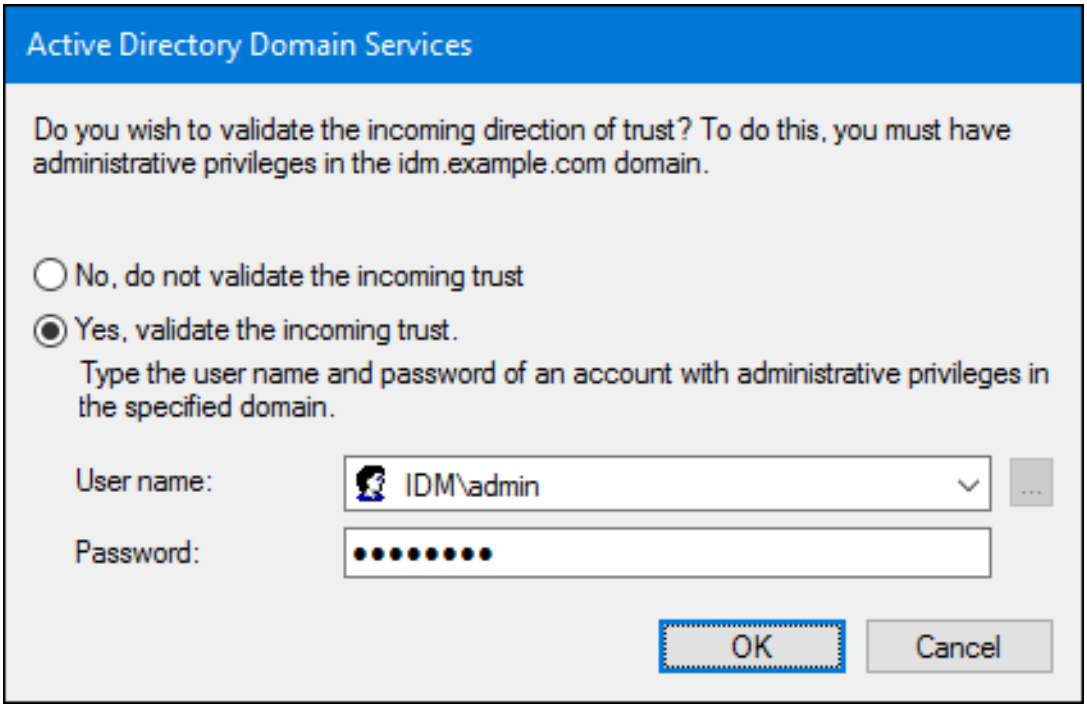
5. **Active Directory** 도메인 및 신뢰 콘솔에서 신뢰를 검증합니다.

   a. 도메인 이름을 마우스 오른쪽 버튼으로 클릭하고 속성 을 선택합니다.

   b. 신뢰 탭에서 이 도메인(다음 신뢰) 창을 신뢰하는 도메인에서 도메인을 선택하고 속성 을 클릭합니다.

   c. **Validate** (유효성 검사) 버튼을 클릭합니다.

   d. **Yes**를 선택하고 들어오는 신뢰를 검증 하고 **IdM** 관리자 사용자의 자격 증명을 입력합니다.



6. 신뢰할 수 있는 도메인 목록을 업데이트합니다.

```
[root@ipaserver ~]# ipa trust-fetch-domains ad.example.com
--------------------------------------------------------------------------------
```

```
List of trust domains successfully refreshed. Use trustdomain-find command to list them.
----------------------------------------------------------------------------------------
----------------------------
Number of entries returned 0
----------------------------
```

7. *신뢰할 수 있는 도메인을 나열합니다.*

```
[root@ipaserver ~]# ipa trustdomain-find ad.example.com
  Domain name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-1762709870-351891212-3141221786
  Domain enabled: True
----------------------------
Number of entries returned 1
----------------------------
```

8. *선택적으로 **IdM** 서버가 **AD** 도메인에서 사용자 정보를 검색할 수 있는지 확인합니다.*

```
[root@ipaserver ~]# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:610600500:610600500:Administrator:/home/ad.example.co
m/administrator:
```

5.2.2.3. ID 매핑 확인

***ID** 매핑을 확인하려면 다음을 수행합니다.*

1. *가장 높은 **ID**를 나열하려면 **Windows Active Directory 6.7;Directory** 도메인 컨트롤러 **(DC)**에서 다음 명령을 실행합니다.*

```
C:\> dcdiag /v /test:ridmanager /s:ad.example.com
...
Available RID Pool for the Domain is 1600 to 1073741823
...
```

2. ***IdM** 서버의 **ID** 범위를 나열합니다.*

```
[root@ipaserver ~]# ipa idrange-find
----------------
1 range matched
----------------
  Range name: AD.EXAMPLE.COM_id_range
  First Posix ID of the range: 610600000
  Number of IDs in the range: 200000
```

```
  First RID of the corresponding RID range: 0
  Domain SID of the trusted domain: S-1-5-21-796215754-1239681026-23416912
  Range type: Active Directory domain range
----------------------------
Number of entries returned 1
----------------------------
```

*이후 단계에서 첫 번째 **POSIX ID** 값이 필요합니다.*

3.

***ActiveActive Directory {{;Directory DC**에서 보안 식별자(**SID**) 또는 사용자를 표시합니다. 예를 들어, **Administrator**의 **SID**를 표시하려면 다음을 수행합니다.*

```
C:\> wmic useraccount where name="administrator" get sid
S-1-5-21-796215754-1239681026-23416912-500
```

***SID**의 마지막 부분은 **RID(relative identifier)**입니다. 다음 단계에서 사용자의 **RID**가 필요합니다.*

참고

***RID**가 기본 **ID** 범위(**200000**)보다 큰 경우 **ipa idrange-mod** 명령을 사용하여 범위를 확장합니다. 예를 들면 다음과 같습니다.*

```
# ipa idrange-mod --range-size=1000000 AD.EXAMPLE.COM_id_range
```

4.

***IdM** 서버에 동일한 사용자의 사용자 **ID**를 표시합니다.*

```
[root@ipaserver ~]# id ad\\administrator
uid=610600500(administrator@ad.example.com)...
```

5.

*첫 번째 **POSIX ID** 값(**610600000**)을 **RID**(**500**)에 추가하는 경우 **IdM** 서버(**610600500**)에 표시된 사용자 **ID**와 일치해야 합니다.*

5.2.2.4. 기존 IdM 인스턴스에 대한 신뢰 생성

*기존 **IdM** 인스턴스에 대한 신뢰를 구성할 때 도메인 내의 **IdM** 서버 및 항목에 대한 특정 설정이 이미 구성되어 있습니다. 그러나 **Active Directory** 도메인의 **DNS** 구성을 설정하고 **Active Directory GovClouds**를 기존 **IdM** 사용자 및 그룹에 모두 할당해야 합니다.*

1. *5.2.2.1.1절. "신뢰를 위한 IdM 서버 준비" 에 설명된 대로 신뢰할 수 있도록 IdM 서버를 준비합니다.*

2. *5.2.2.1.2절. "신뢰 계약 생성" 에 설명된 대로 신뢰 계약을 만듭니다.*

3. *각 IdM 사용자에 대해 InstallPlan을 생성합니다.*

참고

ipa-adtrust-install 유틸리티를 사용하여 신뢰를 설정할 때 SIDs가 생성된 경우 이 단계를 수행하지 마십시오.

a. *백엔드 LDAP 디렉터리에서 ipa-sidgen-task 작업을 실행하여 각 항목에 대해 InstallPlan을 포함하는 새 ipaNTSecurityIdentifier 특성을 추가합니다.*

```
[root@ipaserver ]# ldapmodify -x -H ldap://ipaserver.ipa.example.com:389 -D
"cn=directory manager" -w password

dn: cn=sidgen,cn=ipa-sidgen-task,cn=tasks,cn=config
changetype: add
objectClass: top
objectClass: extensibleObject
cn: sidgen
nsslapd-basedn: dc=ipadomain,dc=com
delay: 0

adding new entry "cn=sidgen,cn=ipa-sidgen-task,cn=tasks,cn=config"
```

b. *작업이 성공적으로 완료되면 InstallPlan 생성 작업(Sidgen 작업)이 0(0) 상태로 완료된다는 오류 로그에 메시지가 기록됩니다.*

```
[root@ipaserver ]# grep "sidgen_task_thread" /var/log/dirsrv/slapd-IDM-EXAMPLE-
COM/errors
[20/Jul/2012:18:17:16 +051800] sidgen_task_thread - [file ipa_sidgen_task.c, line 191]:
Sidgen task starts ...
[20/Jul/2012:18:17:16 +051800] sidgen_task_thread - [file ipa_sidgen_task.c, line 196]:
Sidgen task finished [0].
```

4. *5.2.2.1.3절. "Kerberos 구성 확인" 에 설명된 대로 Kerberos 구성을 확인합니다.*

5.2.2.5. 두 번째 신뢰 추가

이미 신뢰 계약이 구성된 IdM 서버에 대한 신뢰를 추가할 때 신뢰 관련 패키지 설치 또는 Multus 구성과 같은 특정 일반 IdM 신뢰 설정은 더 이상 필요하지 않습니다. 추가 신뢰를 추가하려면 DNS만 구성하고 신뢰 계약을 설정해야 합니다.

1. 5.2.1.2절. "DNS 및 realm 설정" 에 설명된 대로 DNS가 올바르게 구성되었는지 확인합니다.

2. 5.2.2.1.2절. "신뢰 계약 생성" 에 설명된 대로 신뢰 계약을 만듭니다.

5.2.2.6. 웹 UI에서 신뢰 생성

웹 UI에 신뢰를 생성하기 전에 신뢰할 수 있도록 IdM 서버를 준비합니다. 이 신뢰 구성은 5.2.2.1.1절. "신뢰를 위한 IdM 서버 준비" 에 설명된 대로 명령줄에서 쉽게 수행할 수 있습니다.

초기 구성이 설정되면 IdM 웹 UI에 신뢰 계약을 추가할 수 있습니다.

1. IdM 웹 UI를 엽니다.

```
https://ipaserver.example.com
```

2. IPA 서버 메인 탭을 열고 트러스트 하위 탭을 선택합니다.

3. Trusts tab에서 Add 를 클릭하여 새 신뢰 구성 창을 엽니다.

4. 신뢰에 대한 필요한 정보를 입력하십시오:

   a. Domain 필드에 AD 도메인 이름을 제공합니다.

   b. 신뢰를 양방향으로 설정하려면 양방향 신뢰 확인란을 선택합니다. 신뢰를 단방향으로 설정하려면 양방향 신뢰를 선택하지 않고 남겨 둡니다.

단방향 및 양방향 신뢰에 대한 자세한 내용은 5.1.4절. "one-Way and two-Way Trusts" 를 참조하십시오.

c.

*다른 **Kubernetes**의 도메인에 대한 외부 신뢰를 설정하려면 외부 신뢰 확인란을 선택합니다.*

자세한 내용은 5.1.5절. "ActiveActive Directory illustrated;Directory에 대한 외부 신뢰"의 내용을 참조하십시오.

d.

*섹션을 사용하여 **Establish** 는 신뢰를 설정하는 방법을 정의합니다.*

- *AD 관리자의 사용자 이름 및 암호를 사용하여 신뢰를 설정하려면 관리 계정을 선택하고 필요한 자격 증명을 제공합니다.*

- *또는 공유 암호를 사용하여 신뢰를 설정하려면 **Pre-shared** 암호를 선택하고 신뢰 암호 를 제공합니다.*

e.

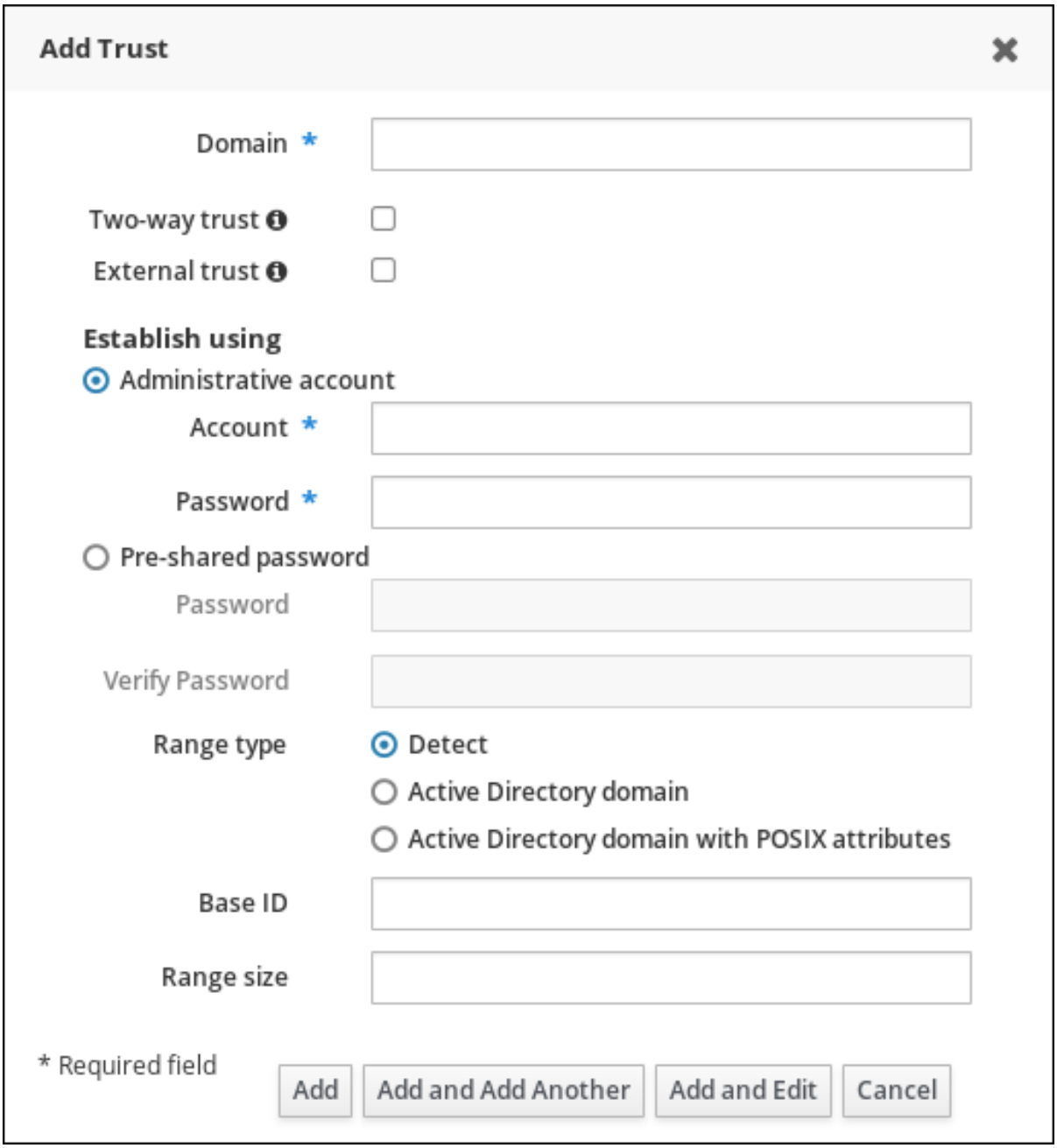
*신뢰의 **ID** 구성을 정의합니다.*

- *Range 유형 옵션을 사용하면 ID 범위 유형을 선택할 수 있습니다. IdM에서 사용할 ID 범위를 자동으로 감지하려면 Detect 를 선택합니다.*

- *ID 범위의 시작 ID를 정의하려면 기본 ID 필드를 사용합니다. ID 범위의 크기를 정의하려면 Range size 필드를 사용합니다. IdM에서 ID 범위에 기본값을 사용하려면 이러한 옵션을 지정하지 마십시오.*

ID 범위에 대한 자세한 내용은 "ID 범위" 을 참조하십시오.

그림 5.5. 웹 UI에서 신뢰 추가



5. *추가 를 클릭하여 새 신뢰를 저장합니다.*

이 후 5.2.2.1.3절. "Kerberos 구성 확인" 에 설명된 대로 Kerberos 구성을 확인합니다.

5.2.3. cross-forest Trusts에 대한 설치 후 고려 사항

5.2.3.1. Active Directory Trust 관련 잠재적인 동작 문제

5.2.3.1.1. Active Directory 사용자 및 IdM 관리

현재 AD(Active Directory) 사용자와 관리자는 IdM 웹 UI에 로그인한 후 셀프 서비스 페이지만 볼 수

있습니다. AD 관리자는 IdM 웹 UI의 관리자 보기에 액세스할 수 없습니다. 자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드 의 AD 사용자로 IdM 웹 UI 인증을 참조하십시오.

또한 현재 AD 사용자는 자체 ID 재정의를 관리할 수 없습니다. IdM 사용자만 ID 재정의를 추가하고 관리할 수 있습니다.

5.2.3.1.2. 삭제된 ActiveActive Directoryfqdn;Directory 사용자 인증

기본적으로 모든 IdM 클라이언트는 SSSD 서비스를 사용하여 사용자 ID 및 자격 증명을 캐시합니다. IdM 또는 AD 백엔드 공급자를 일시적으로 사용할 수 없는 경우 SSSD를 사용하면 로컬 시스템에서 성공적으로 로그인한 사용자의 ID를 참조할 수 있습니다.

SSSD는 로컬로 사용자 목록을 유지 관리하므로 백엔드에 적용된 변경 사항은 SSSD를 오프라인으로 실행하는 클라이언트에 즉시 표시되지 않을 수 있습니다. 이러한 클라이언트에서 IdM 리소스에 로그인했으며 해시된 암호가 SSSD 캐시에 저장된 사용자는 AD에서 사용자 계정이 삭제된 경우에도 다시 로그인할 수 있습니다.

위의 조건이 충족되면 사용자 ID가 SSSD에 캐시되고 사용자 계정이 AD를 삭제하더라도 AD 사용자는 IdM 리소스에 로그인할 수 있습니다. 이 문제는 SSSD가 온라인 상태가 되고 AD 도메인 컨트롤러에 대해 AD 사용자 로그온을 확인할 수 있을 때까지 지속됩니다.

클라이언트 시스템이 SSSD를 온라인으로 실행하는 경우 사용자가 제공하는 암호는 AD 도메인 컨트롤러에서 검증합니다. 이렇게 하면 삭제된 AD 사용자가 로그인할 수 없습니다.

5.2.3.1.3. 자격 증명 캐시 컬렉션 및 ActiveActive Directory Long;Directory principals 선택

Kerberos 자격 증명 캐시는 다음 순서에 따라 서버 주체와 서버 주체와 일치하려고 합니다.

1. 서비스 이름
2. 호스트 이름
3. 영역 이름

클라이언트 및 서버 매핑이 호스트 이름 또는 실제 이름 및 자격 증명 캐시 컬렉션을 기반으로 하는 경우 AD 사용자로 바인딩할 때 예기치 않은 동작이 발생할 수 있습니다. 이는 ActiveActive Directory

etcdctl;Directory 사용자의 영역 이름이 IdM 시스템의 영역 이름과 다르기 때문입니다.

AD 사용자가 kinit 유틸리티를 사용하여 티켓을 얻은 다음 SSH를 사용하여 anan IdM adm;IdM 리소스에 연결하면 보안 주체가 리소스 티켓에 대해 선택되지 않습니다. IdM principal가 리소스의 영역 이름과 일치하므로 IdM principal가 리소스의 영역 이름과 일치하기 때문에 보안 주체가 사용됩니다.

예를 들어 AD 사용자가 Administrator 이고 도메인이 ADEXAMPLE.ADREALM 인 경우 보안 주체는 Administrator@ADEXAMPLE.ADREALM 입니다.

```
[root@server ~]# kinit Administrator@ADEXAMPLE.ADREALM
Password for Administrator@ADEXAMPLE.ADREALM:
[root@server ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@ADEXAMPLE.ADREALM

Valid starting       Expires              Service principal
27.11.2015 11:25:23  27.11.2015 21:25:23
krbtgt/ADEXAMPLE.ADREALM@ADEXAMPLE.ADREALM
 renew until 28.11.2015 11:25:16
```

이는 ActiveActive Directory 6.7;Directory 티켓 캐시의 기본 주체로 설정됩니다. 그러나 IdM 사용자에게 Kerberos 티켓(예: admin)도 있는 경우, anan IdMrng;IdM 기본 주체가 있는 별도의 IdM 인증 정보 캐시가 있습니다. ActiveActive Directory advised;Directory 사용자가 SSH를 사용하여 리소스에 연결하는 경우 호스트 티켓에 대해 IdM 기본 주체가 선택됩니다.

```
[root@vm-197 ~]# ssh -l Administrator@adexample.adrealm ipaclient.example.com
Administrator@adexample.adrealm@ipaclient.example.com's password:

[root@vm-197 ~]# klist -A
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@ADEXAMPLE.ADREALM

Valid starting       Expires              Service principal
27.11.2015 11:25:23  27.11.2015 21:25:23
krbtgt/ADEXAMPLE.ADREALM@ADEXAMPLE.ADREALM
 renew until 28.11.2015 11:25:16

Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EXAMPLE.COM >>>>> IdM user

Valid starting       Expires              Service principal
27.11.2015 11:25:18  28.11.2015 11:25:16  krbtgt/EXAMPLE.COM@EXAMPLE.COM
27.11.2015 11:25:48 28.11.2015 11:25:16 host/ipaclient.example.com@EXAMPLE.COM >>>>> host
principal
```

이는 IdM 주체의 영역 이름이 IdM 리소스의 영역과 일치하기 때문입니다.

5.2.3.1.4. 그룹 6.7s 해결

***Kerberos** 티켓 손실*

***net getlocalsid** 또는 **net getdomainsid.NET getdomainsid** 와 같은 **Samba** 서비스에서 **SID**를 가져오려면 **Kerberos** 캐시의 기존 **admin** 티켓을 제거합니다.*

참고

***Active Directory** 트러스트를 사용하려면 **net getlocalsid** 또는 **net getdomainsid** 와 같은 명령을 실행할 필요가 없습니다.*

사용자 그룹 멤버십을 확인할 수 없음

*특정 신뢰할 수 있는 사용자가 특정 **IdM** 그룹, 외부 또는 **POSIX**와 연결되어 있는지 확인할 수 없습니다.*

***ActiveActive Directory HAT;Directory** 사용자에 대한 원격 **ActiveActive Directory qcow;Directory** 그룹 멤버십을 표시할 수 없습니다.*

중요

***IdM** 서버와 클라이언트가 **Red Hat Enterprise Linux 7.1** 이상에서 실행되는 경우 이 문제는 더 이상 발생하지 않습니다.*

***id** 유틸리티를 사용하여 **Linux** 시스템 사용자의 로컬 그룹 연결을 표시할 수 있습니다. 그러나 **id** 는 **Samba** 도구가 표시하더라도 **Active Directory** 사용자에 대한 **Active Directory** 그룹 멤버십이 표시되지 않습니다.*

*이 문제를 해결하려면 **ssh** 유틸리티를 사용하여 지정된 **AD** 사용자로 **IdMseparated;IdM** 클라이언트 시스템에 로그인할 수 있습니다. **AD** 사용자가 처음으로 로그인하면 **id** 검색에서 **AD** 그룹 멤버십을 감지하고 표시합니다.*

```
[root@ipaserver ~]# id ADDOMAIN\user
uid=1921801107(user@ad.example.com) gid=1921801107(user@ad.example.com)
groups=1921801107(user@ad.example.com),129600004(ad_users),1921800513(domain
users@ad.example.com)
```

5.2.3.2. 신뢰 에이전트 구성

*신뢰 환경에서 새 복제본을 설정한 후에는 복제본에 **AD** 신뢰 에이전트 역할이 자동으로 설치되지 않습니다. 복제본을 신뢰 에이전트로 구성하려면 다음을 수행합니다.*

1. 기존 신뢰 컨트롤러에서 **ipa-adtrust-install --add-agents** 명령을 실행합니다.

```
[root@existing_trust_controller]# ipa-adtrust-install --add-agents
```

명령은 대화식 구성 세션을 시작하고 에이전트를 설정하는 데 필요한 정보를 입력하라는 메시지를 표시합니다.

--add-agents 옵션에 대한 자세한 내용은 **ipa-adtrust-install(1)** 도움말 페이지를 참조하십시오.

2. 새 복제본에서 다음을 수행합니다.

   a. **IdM** 서비스를 다시 시작하십시오.

   ```
   [root@new_trust_controller]# ipactl restart
   ```

   b. **SSSD** 캐시에서 모든 항목을 제거합니다.

   ```
   [root@new_trust_controller]# sssctl cache-remove
   ```

   참고

   sssctl 명령을 사용하려면 **sssd-tools** 패키지가 설치되어 있어야 합니다.

   c. 필요한 경우 복제본에 **AD** 신뢰 에이전트 역할이 설치되어 있는지 확인합니다.

   ```
   [root@new_trust_controller]# ipa server-show new_replica.idm.example.com
   ...
   Enabled server roles: CA server, NTP server, AD trust agent
   ```

5.3. CROSS-FOREST TRUST 환경 관리 및 구성

5.3.1. 신뢰할 수 있는 도메인 환경에서 사용자 계정 이름

IdM은 사용자 주체 이름(UPN)을 사용하여 로그인을 지원합니다. UPN은 인증할 사용자 이름의 대안이며 username@KERBEROS-REALM 형식입니다. ActiveActive Directory Long;Directory forest에서 추가 UPN 접미사를 구성할 수 있습니다. 이러한 엔터프라이즈 주체 이름은 기본 UPN에 대체 로그인을 제공하는 데 사용됩니다.

예를 들어, 회사에서 Kerberos 영역 AD.EXAMPLE.COM 을 사용하는 경우 사용자의 기본 UPN은 user@ad.example.com 입니다. 그러나 종종 회사에서 사용자가 user@example.com 와 같이 이메일 주소를 사용하여 로그인할 수 있기를 원합니다. 이 경우 관리자는 추가 UPN 접미사 example.com 을 ActiveActive Directory qcow;Directory forest에 추가하고 사용자 계정 속성에 새 접미사를 설정합니다.

AD forest 루트에 정의된 경우에만 IdM에 UPN 접미사가 표시됩니다. AD 관리자는 Active Directory 도메인 및 신뢰 유틸리티 또는 PowerShell 명령줄 도구를 사용하여 UPN을 정의할 수 있습니다.

참고

사용자에 대한 UPN 접미사를 구성하기 위해 Red Hat은 Active Directory 도메인 및 신뢰 유틸리티와 같은 오류 유효성 검사를 수행하는 툴을 사용할 것을 권장합니다.

Active Directory가 해당 작업의 유효성을 검사하지 않으므로 ldapmodify 명령을 사용하여 사용자에 대한 userPrincipalName 특성을 설정하는 등 낮은 수준의 수정을 통해 UPN을 구성하는 것이 좋습니다.

신뢰할 수 있는 AD forest에서 UPN 접미사를 추가하거나 제거하는 경우 IdM 마스터에서 신뢰할 수 있는 추정에 대한 정보를 새로 고쳐야 합니다.

```
[root@ipaserver ~]# ipa trust-fetch-domains
Realm-Name: ad.example.com
--------------------------------
No new trust domains were found
--------------------------------
----------------------------
Number of entries returned 0
----------------------------
```

다음을 실행하여 대체 UPN이 가져왔는지 확인합니다.

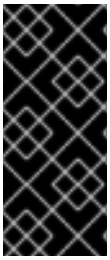
```
[root@ipaserver ~]# ipa trust-show
Realm-Name: ad.example.com
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
```

```
Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
Trust direction: Two-way trust
Trust type: Active Directory domain
UPN suffixes: example.com
```

도메인의 **UPN** 접미사는 **cn=trusted_domain_name,cn=ad,cn=trusts,dc=idm,dc=example,dc=com** 하위 트리의 다중 값 속성 **ipaNT additionalSuffixes** 에 저장됩니다.

5.3.2. ActiveActive Directory HAT;Directory DNS 도메인의 IdM 클라이언트

IdM과 **ActiveActive Directory 6.7;Directory** 간의 신뢰가 있는 일부 환경에서는 **ActiveActive Directory HAT;Directory DNS** 도메인의 일부인 호스트에 **IdM** 클라이언트를 설치할 수 있습니다. 그러면 호스트는 **Linux** 중심 **IdM** 기능을 활용할 수 있습니다.



중요

이는 권장되는 구성이 아니며 몇 가지 제한 사항이 있습니다. **Red Hat**은 항상 **ActiveActive Directory illustrated;Directory**가 소유한 것과 다른 **DNS** 영역에 **IdM** 클라이언트를 배포하고 **IdM** 호스트 이름을 통해 **IdM** 클라이언트에 액세스하는 것이 좋습니다.

5.3.2.1. IdM 클라이언트의 Kerberos Single Sign-on이 필요하지 않음

ActiveActive Directory HAT;Directory DNS 도메인에 설정된 **IdM** 클라이언트의 경우, 이 **IdM** 호스트의 리소스에 액세스할 수 있는 암호 인증만 사용할 수 있습니다. 이 시나리오에 맞게 클라이언트를 구성하려면 다음을 수행합니다.

1. 클라이언트의 **SSSD(System Security Service Daemon)**가 **IdM** 서버와 통신할 수 있도록 **--domain=IPA_DNS_Domain** 옵션으로 **IdM** 클라이언트를 설치합니다.

```
[root@idm-client.ad.example.com ~]# ipa-client-install --domain=idm.example.com
```

이 옵션은 **ActiveActive Directory qcow;Directory DNS** 도메인에 대한 **SRV** 레코드 자동 감지를 비활성화합니다.

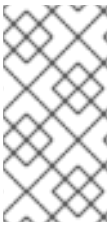
2. **/etc/krb5.conf** 구성 파일의 **[domain_realm]** 섹션에서 **ActiveActive Directory HAT;Directory** 도메인의 기존 매핑을 찾습니다.

```
.ad.example.com = IDM.EXAMPLE.COM
ad.example.com = IDM.EXAMPLE.COM
```

*두 행을 **ActiveActive Directory HAT;Directory DNS** 영역의 **Linux** 클라이언트 **FQDN(정규화된 도메인 이름)**의 매핑 항목으로 바꿉니다.*

```
idm-client.ad.example.com = IDM.EXAMPLE.COM
```

*기본 매핑을 대체하면 **Kerberos**가 **ActiveActive Directory QCOW;Directory** 도메인에 대한 요청을 **IdM Kerberos** 배포 센터**(KDC)**로 전송하지 않습니다. 대신 **Kerberos**는 **SRV DNS** 레코드를 통한 자동 검색을 사용하여 **KDC**를 찾습니다. 추가된 호스트 **idm-client.ad.example.com**에만 **IdMNetworkPolicy**가 설정됩니다.*



참고

***IdM** 소유 **DNS** 영역에 없는 클라이언트의 리소스에 인증하는 것은 사용자 이름과 암호를 사용하는 경우에만 가능합니다.*

***SSL** 인증서 처리*

***SSL** 기반 서비스에는 원본**(A/AAAA)**과 **CNAME** 레코드가 모두 인증서에 있어야 하므로 모든 시스템 호스트 이름을 포함하는 **dNSName** 확장 레코드가 있는 인증서가 필요합니다. 현재 **IdM**은 **IdM** 데이터베이스의 오브젝트를 호스트하는 인증서만 발행합니다.*

***Single Sign-On**을 사용할 수 없는 설정에서 **IdM**에는 이미 데이터베이스의 **FQDN**에 대한 호스트 오브젝트가 있으며 **certmonger** 는 이 이름에 대한 인증서를 요청할 수 있습니다.*

```
[root@idm-client.ad.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=ipa-client.ad.example.com \
    -D ipa-client.ad.example.com \
    -K host/idm-client.ad.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

***certmonger** 서비스는 **/etc/krb5.keytab** 파일에 저장된 기본 호스트 키를 사용하여 **IdM CA(인증 기관)**에 인증합니다.*

5.3.2.2. IdM 클라이언트에 Kerberos Single Sign-On이 필요합니다.

***IdM** 클라이언트의 리소스에 액세스하기 위해 **Kerberos Single Sign-on**이 필요한 경우 클라이언트는 **IdM DNS** 도메인**(예: idm-client.idm.example.com)** 내에 있어야 합니다. **IdM** 클라이언트의 **A/AAAA** 레코드를 가리키는 **ActiveActive Directory 6.7;Directory DNS** 도메인에 **CNAME** 레코드 **idm-client.ad.example.com** 을 생성해야 합니다.*

Kerberos 기반 애플리케이션 서버의 경우 MIT Kerberos는 애플리케이션의 키 탭에서 사용 가능한 호스트 기반 주체를 수락할 수 있는 방법을 지원합니다. Kerberos 서버를 대상으로 하는 Kerberos 주체에 대한 엄격한 확인을 비활성화하려면 /etc/krb5.conf 구성 파일의 [libdefaults] 섹션에 다음 옵션을 설정합니다.

```
ignore_acceptor_hostname = true
```

SSL 인증서 처리

SSL 기반 서비스에는 원본(A/AAAA)과 CNAME 레코드가 모두 인증서에 있어야 하므로 모든 시스템 호스트 이름을 포함하는 dNSName 확장 레코드가 있는 인증서가 필요합니다. 현재 IdM은 IdM 데이터베이스의 오브젝트를 호스트하는 인증서만 발행합니다.

Single Sign-On을 사용할 수 없는 설정에서 IdM에는 이미 데이터베이스의 FQDN에 대한 호스트 오브젝트가 있으며 certmonger 는 이 이름에 대한 인증서를 요청할 수 있습니다.

1. *새 호스트 오브젝트를 생성합니다.*

```
[root@idm-server.idm.example.com ~]# ipa host-add idm-client.ad.example.com --force
```

호스트 이름은 A/AAAA 레코드가 아닌 CNAME이므로 --force 옵션을 사용합니다.

2. *IdM DNS 호스트 이름을 사용하여 IdM 데이터베이스의 ActiveActive Directory 6.7;Directory 호스트 항목을 관리할 수 있습니다.*

```
[root@idm-server.idm.example.com ~]# ipa host-add-managedby idm-client.ad.example.com
\
    --hosts=idm-client.idm.example.com
```

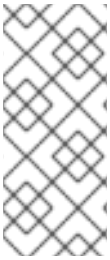
이 설정을 사용하면 IdM 클라이언트에서 ActiveActive Directory HAT;Directory DNS 도메인 내의 호스트 이름에 대한 dNSName 확장 레코드가 있는 SSL 인증서를 요청할 수 있습니다.

```
[root@idm-client.idm.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=`hostname --fqdn` \
    -D `hostname --fqdn` \
    -D idm-client.ad.example.com \
    -K host/idm-client.idm.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

5.3.3. ActiveActive Directory HAT;Directory 사용자를 위한 IdM 그룹 생성

사용자 그룹은 IdM 사용자에게 액세스 권한, 호스트 기반 액세스 제어, sudo 규칙 및 기타 제어를 설정하는 데 필요합니다. 이러한 그룹은 IdM 도메인 리소스에 대한 액세스 권한 부여 및 액세스 제한입니다.

AD 사용자 및 AD 그룹 모두 IdM 사용자 그룹에 직접 추가할 수 있습니다. 이를 위해 먼저 AD 사용자 또는 그룹을 비POSIX IdM 외부 그룹에 추가한 다음 로컬 IdM POSIX 그룹에 추가합니다. 그런 다음 POSIX 그룹을 AD 사용자의 사용자 및 역할 관리에 사용할 수 있습니다. IdM에서 비POSIX 그룹을 처리하는 원칙에 대한 내용은 5.1.3.2절. “Active Directory 사용자 및 ID 관리 그룹” 에 설명되어 있습니다.



참고

IdM 외부 그룹에 멤버로 AD 사용자 그룹을 추가할 수도 있습니다. 이렇게 하면 단일 AD 영역 내에서 사용자 및 그룹 관리를 유지하여 Windows 사용자에 대한 정책을 더 쉽게 정의할 수 있습니다.

1. 선택 사항: IdM 영역에서 AD 사용자를 관리하는 데 사용할 AD 도메인에서 그룹을 생성하거나 선택합니다. IdM 측의 여러 그룹을 사용하고 다양한 그룹에 추가할 수 있습니다.

2. ipa group-add 명령에 --external 옵션을 추가하여 ActiveActive Directory 6.7;Directory 사용자의 IdM 도메인에 외부 그룹을 생성합니다. external 옵션 은 이 그룹에 IdM 도메인 외부의 멤버가 포함되어 있음을 나타냅니다. 예를 들면 다음과 같습니다.

```
[root@ipaserver ~]# ipa group-add --desc='AD users external map' ad_users_external --
external
-------------------------------
Added group "ad_users_external"
-------------------------------
  Group name: ad_users_external
  Description: AD users external map
```

참고

외부 그룹은 사용자의 기본 그룹이 아닌 추가 사용자 그룹에 연결되어 있어야 합니다. ActiveActive Directory QCOW;Directory는 그룹 속성에 그룹 멤버 를 저장하고, IdM은 이 특성을 사용하여 멤버를 확인합니다. 그러나 ActiveActive Directory {{;Directory는 해결되지 않은 사용자 항목의 primaryGroupID 속성에 사용자 그룹을 저장합니다.

3. 새 IdM POSIX 그룹을 생성하거나 IdM 정책을 관리할 기존 그룹을 선택합니다. 예를 들어 새 그룹을 생성하려면 다음을 실행합니다.

```
[root@ipaserver ~]# ipa group-add --desc='AD users' ad_users
----------------------
Added group "ad_users"
----------------------
  Group name: ad_users
  Description: AD users
  GID: 129600004
```

4. **IdM 외부 그룹에 AD 사용자 또는 그룹을 외부 멤버로 추가합니다. AD 멤버는 DOMAIN\group_name 또는 DOMAIN\username 과 같은 정규화된 이름으로 식별됩니다. 그러면 AD ID가 사용자 또는 그룹의 ActiveActive Directory Long;Directory SID에 매핑됩니다.**

   예를 들어 **AD** 그룹의 경우 다음을 수행합니다.

```
[root@ipaserver ~]# ipa group-add-member ad_users_external --external "AD\Domain
Users"
 [member user]:
 [member group]:
  Group name: ad_users_external
  Description: AD users external map
  External member: S-1-5-21-3655990580-1375374850-1633065477-513
SID_DOM_GROUP (2)
-------------------------
Number of members added 1
-------------------------
```

5. 외부 **IdM** 그룹을 **POSIX IdM** 그룹에 멤버로 추가합니다. 예를 들면 다음과 같습니다.

```
[root@ipaserver ~]# ipa group-add-member ad_users --groups ad_users_external
  Group name: ad_users
  Description: AD users
  GID: 129600004
  Member groups: ad_users_external
-------------------------
Number of members added 1
-------------------------
```

5.3.4. 신뢰 유지 관리

신뢰 관리에는 글로벌 신뢰 구성, **Kerberos** 신뢰 구성, **DNS** 영역 구성 또는 **Active Directory** 사용자에 대한 **ID** 범위 할당과 같은 여러 영역이 포함됩니다.

5.3.4.1. 글로벌 신뢰 구성 편집

ipa-adtrust-install 유틸리티는 IdM 도메인에 대한 백그라운드 정보를 자동으로 구성합니다. 이 정보는 ActiveActive Directory qcow;Directory 도메인을 사용하여 신뢰를 생성하는 데 필요합니다.

글로벌 신뢰 구성에는 다음 5가지 속성이 포함되어 있습니다.

- *Windows 스타일의 보안 ID(SID): 이 특성은 자동 생성되므로 수정할 수 없습니다.*
- *도메인 GUID; 이 속성은 자동으로 생성되었으며 수정할 수 없습니다.*
- *Kerberos 도메인 이름. 이 속성은 IdM 구성에서 제공되며 수정할 수 없습니다.*
- *IdM 사용자를 추가할 기본 그룹; 이 속성을 수정할 수 있습니다.*
- *mirror name; 이 특성을 수정하지 않는 것이 좋습니다.*

신뢰 구성은 cn=도메인,cn=ad,cn=etc,dc=example,dc=com 하위 트리에 저장됩니다.

5.3.4.1.1. ResourceOverride 이름 변경

중요

대부분의 경우ResourceOverride 이름을 변경하려면 기존 모든 신뢰를 다시 설정해야 합니다. 따라서 Red Hat은 특성을 변경하지 않는 것이 좋습니다.

ipa-adtrust-install 유틸리티를 실행할 때 Active Directory 토폴로지에서 compatible within an Active Directory topology is configured for the IdM server when running the ipa-adtrust-install 유틸리티를 실행합니다. 나중에 변경하려면 ipa-adtrust-install 을 다시 실행하고 --netbios-name 옵션을 사용하여 새 redfish 이름을 지정합니다.

```
[root@ipaserver ]# ipa-adtrust-install --netbios-name=NEWBIOSNAME
```

5.3.4.1.2. Windows 사용자의 기본 그룹 변경

Identity Management가 Active Directory 마이그레이드를 신뢰하도록 구성되면 IdM 사용자의

Kerberos 티켓에 MS-PAC 레코드가 추가됩니다. MS-PAC 레코드에는 IdM 사용자가 속한 그룹의 SID(보안 식별자)가 포함되어 있습니다. IdM 사용자의 기본 그룹에 6.7이 할당되지 않은 경우 기본 SMB 그룹에 대해 정의된 보안 식별자의 값이 사용됩니다. AD 도메인 컨트롤러에서 IdM 신뢰 컨트롤러에서 사용자 정보를 요청할 때 Samba 제품군에서 동일한 논리를 적용합니다.

기본 SMB 그룹은 ipa-adtrust-install 유틸리티에서 자동으로 생성된 대체 그룹입니다. 기본 그룹은 삭제할 수 없지만 글로벌 신뢰 구성을 사용하여 IdM 사용자 기본 그룹의 폴백으로 사용할 다른 IdM 그룹을 지정할 수 있습니다.

명령줄에서 기본 그룹을 설정하려면 ipa trustconfig-mod 명령을 사용합니다.

```
[root@server ~]# kinit admin
[root@server ~]# ipa trustconfig-mod --fallback-primary-group="Example Windows Group"
```

IdM 웹 UI에서 기본 그룹을 설정하려면 다음을 수행합니다.

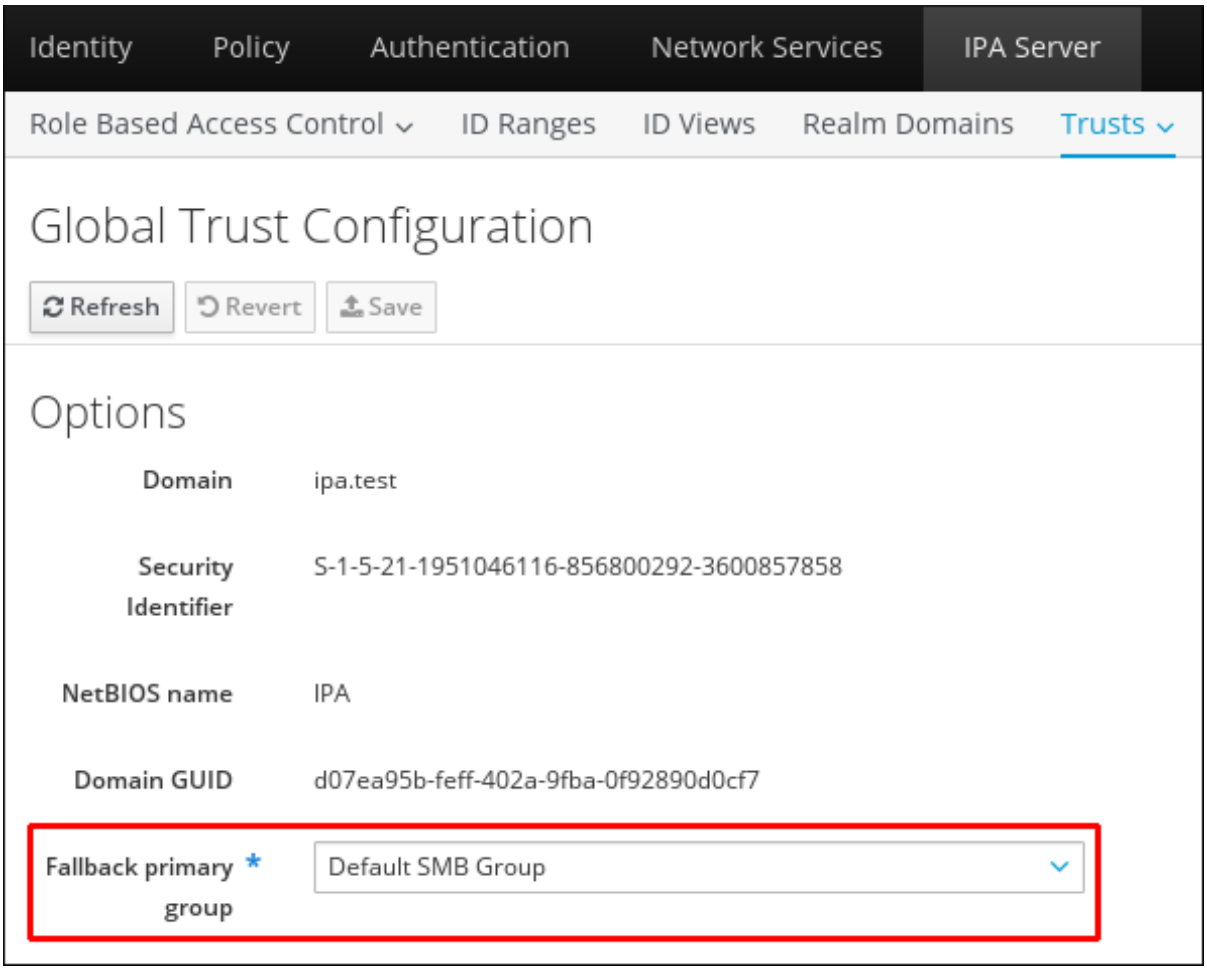
1. *IdM 웹 UI를 엽니다.*

   ```
   https://ipaserver.example.com
   ```

2. *IPA 서버 메인 탭에서 보안 하위 탭을 선택한 다음 글로벌 구성 섹션을 엽니다.*

3. *Fallback 기본 그룹 드롭다운 목록에 있는 모든 IdM 그룹에서 새 그룹을 선택합니다.*

그림 5.6. Windows 사용자의 기본 그룹 구성



4. *저장을 클릭하여 새 구성을 저장합니다.*

5.3.4.2. 보안 도메인 검색, 활성화 및 비활성화

통과된 신뢰는 신뢰 경로가 도메인 체인을 따를 수 있음을 의미합니다. 자세한 내용은 5.1.1절. "신뢰 관계의 아키텍처" 에서 참조하십시오.

***IdM**은 산림의 루트 도메인에 대한 신뢰를 가지고 있으며, 전송 기능 때문에 동일한 스트레인의 모든 하위 도메인과 기타 도메인은 암시적으로 해당 신뢰에 포함됩니다. **IdM**은 마스트의 모든 위치에서 **Windows** 사용자로 토폴로지를 따라 **IdM** 리소스에 액세스합니다. 각 도메인 및 하위 도메인은 **IdM** 신뢰 구성에서 신뢰 도메인 입니다. 각 도메인은 **trusts** 하위 트리의 고유한 항목인 **cn=**하위 도메인 **,cn=trust_name,cn=ad,cn=trusts,dc=example,dc=com** 에 저장됩니다.*

***IdM**은 신뢰가 처음 구성될 때 전체 **ActiveActive Directory qcow;Directory** 토폴로지를 검색하고 매핑하려고 시도하지만 경우에 따라 또는 해당 토폴로지를 수동으로 검색하는 것이 좋습니다. 이 작업은 **trust-fetch-domains** 명령으로 수행됩니다.*

```
[root@ipaserver ~]# kinit admin
```

```
[root@ipaserver ~]# ipa trust-fetch-domains ad.example.com
-----------------------------------------
List of trust domains successfully refreshed
-----------------------------------------
  Realm name: test.ad.example.com
  Domain NetBIOS name: TEST
  Domain Security Identifier: S-1-5-21-87535643-5658642561-5780864324

  Realm name: users.ad.example.com
  Domain NetBIOS name: USERS
  Domain Security Identifier: S-1-5-21-91314187-2404433721-1858927112

  Realm name: prod.ad.example.com
  Domain NetBIOS name: PROD
  Domain Security Identifier: S-1-5-21-46580863-3346886432-4578854233
----------------------------
Number of entries returned 3
----------------------------
```

참고

*공유 시크릿을 사용하여 신뢰를 추가할 때 **AD forest**의 토폴로지를 수동으로 검색해야 합니다. **ipa trust-add ad.domain --trust-secret** 명령을 실행한 후 **AD Domains** 및 **Trusts** 도구의**est trust** 속성을 사용하여 **AD side**에서 들어오는 신뢰를 검증합니다. 그런 다음 **ipa trust-fetch-domains ad.domain** 명령을 실행합니다. **IdM**은 신뢰에 대한 정보를 수신하여 사용할 수 있습니다.*

*토폴로지가 자동 또는 수동 검색을 통해 검색되면 해당 토폴로지의 개별 도메인 및 하위 도메인을 **IdM** 신뢰 구성 내에서 완전히 활성화, 비활성화 또는 제거할 수 있습니다.*

*예를 들어 특정 하위 도메인의 사용자가 **IdM** 리소스 사용을 허용하지 않도록 하려면 해당 신뢰 도메인을 비활성화합니다.*

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trustdomain-disable test.ad.example.com
-----------------------------------------
Disabled trust domain "test.ad.example.com"
-----------------------------------------
```

*해당 신뢰 도메인은 **trustdomain-enable** 명령을 사용하여 다시 활성화할 수 있습니다.*

*도메인이 토폴로지에서 영구적으로 제거되어야 하는 경우 **IdM** 신뢰 구성에서 삭제할 수 있습니다.*

```
[root@ipaserver ~]# kinit admin
```

```
[root@ipaserver ~]# ipa trustdomain-del prod.ad.example.com
---------------------------------------------------------------
Removed information about the trusted domain " "prod.ad.example.com"
---------------------------------------------------------------
```

5.3.4.3. IdM Kerberos 영역과 관련된 도메인 보기 및 관리

IdM Kerberos 영역과 관련된 도메인은 **IdM** 디렉터리의 **cn=Realm Domains,cn=ipa,cn=etc,dc=example,dc=com** 하위 트리에 저장됩니다. 도메인 목록은 **Active Directory**와의 신뢰를 설정하는 경우 **IdM**에서 사용됩니다. **IdM**에서 관리하는 도메인의 전체 목록을 파악하면 **AD** 도메인 컨트롤러에서 **IdMmtls**로 라우팅할 인증 요청을 확인할 수 있습니다. **IdM** 영역과 관련된 구성된 도메인 목록은 **realmdomains-show** 명령을 사용하여 표시할 수 있습니다.

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa realmdomains-show
Domain: ipa.example.org, ipa.example.com, example.com
```

통합된 DNS가 포함된 **IdM** 설정에서 다음을 수행하십시오.

- **ipa dnszone-add** 명령을 사용하여 새 **DNS** 영역을 **IdM**에 추가한 후 도메인 목록에 자동으로 도메인이 추가됩니다. **ipa realmdomains-show** 를 실행하면 **IdM NetNamespace**에서 제어하는 도메인 목록에 새 도메인이 표시됩니다.

  ```
  # kinit admin
  # ipa dnszone-add ipa2.example.com
  # ipa realmdomains-show
  Domain: ipa.example.org, ipa.example.com, example.com, ipa2.example.com
  ```

  IdM Kerberos 영역과 관련된 도메인 삭제 및 기타 유형의 수정도 자동으로 처리됩니다.

통합된 DNS가 없는 **IdM** 설정에서 다음을 수행하십시오.

- **IdM Kerberos** 영역에 포함된 **DNS** 영역이 추가된 경우 새 도메인을 **IdMReplicas**의 제어 아래에 있는 도메인의 **IdM** 목록에 수동으로 추가해야 합니다. **ipa realmdomains-mod** 명령을 **--add-domain** 옵션과 함께 사용하여 새 도메인을 추가합니다.

  ```
  [root@ipaserver ~]# kinit admin
  [root@ipaserver ~]# ipa realmdomains-mod --add-domain=ipa2.example.com
  Domain: ipa.example.org, ipa.example.com, example.com, ipa2.example.com
  ```

  DNS 영역이 삭제된 경우 **IdM Kerberos** 영역과 연결된 도메인을 수동으로 삭제해야 합니다.

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa realmdomains-mod --del-domain=ipa2.example.com
Domain: ipa.example.org, ipa.example.com, example.com
```

도메인 목록에 여러 변경 사항을 적용하면 목록 자체를 수정하고 **--domain** 옵션을 사용하여 교체할 수 있습니다.

```
[root@ipaserver ~]# ipa realmdomains-mod --domain={ipa.example.org,ipa2.example.com}
```

5.3.4.4. Transitive Trust에서 UID 및 GID 번호의 범위 추가

신뢰가 원래 구성된 시점에 **ID** 범위를 생성하는 방법은 *"ID 범위"* 에 설명되어 있습니다. 나중에 **ID** 범위를 추가하려면 다음 옵션과 함께 **ipa idrange-add** 명령을 사용하십시오.

- **base -id** 옵션은 시작 번호인 **POSIX** 범위의 기본 **ID**를 설정합니다.
- **--range-size** 옵션은 **IdM**에서 사용하는 **POSIX ID** 범위 크기를 설정합니다. **IdM**은 신뢰할 수 있는 **AD** 도메인의 사용자 및 그룹의 **RID**를 **POSIX ID**에 매핑합니다. **--range-size** 옵션은 **IdM**에서 생성하는 최대 **ID** 수를 정의합니다. **AD**는 사용자가 생성한 각 사용자와 그룹에 대해 새 **RID**를 사용합니다. 사용자 또는 그룹을 삭제하면 **AD**는 향후 **AD** 항목에 대해 **RID**를 다시 사용하지 않습니다. 따라서 이 범위는 **IdM**이 기존 **AD** 사용자 및 그룹 각각에 **ID**를 할당하고 향후 생성하는 **ID**를 할당할 수 있을 만큼 커야 합니다. 예를 들어, 관리자가 **50000**명의 **AD** 사용자를 삭제하고 이 기간 동안 **10000**개의 새 계정을 생성하는 경우 범위는 **60000**으로 설정해야 합니다. 그러나 범위에 충분한 예약이 포함되어 있어야 합니다. 대규모 환경에서는 기본값 **(200000)** 범위 크기가 충분하지 않다고 예상되는 대규모 환경에서는 **--range-size** 를 더 높은 값으로 설정합니다.
- **--rid-base** 옵션은 **InstallPlan**의 가장 오른쪽 숫자인 **RID**의 시작 번호를 설정합니다. 값은 충돌을 방지하기 위해 기본 **ID**에 추가할 범위를 나타냅니다.
- **--dom-sid** 옵션은 신뢰용으로 구성된 도메인이 여러 개 있을 수 있으므로 도메인 **GovCloud**를 설정합니다.

다음 예에서 기본 **ID**는 **1,200,000**이고 **RID**는 **1,000**입니다. 결과 **ID** 번호는 **1,201,000**입니다.

```
[root@server ~]$ kinit admin
[root@server ~]$ ipa idrange-add --base-id=1200000 --range-size=200000 --rid-base=0 --dom-
sid=S-1-5-21-123-456-789 trusted_dom_range
```

중요

*수동으로 정의한 **ID** 범위가 **IdM**에서 사용하는 **ID** 범위와 겹치지 않는지 확인합니다.*

5.3.4.5. NV ID 범위 수동 조정

*경우에 따라 기존 복제본에 대해 **DCN(Distributed Numeric Assignment) ID** 범위를 수동으로 조정하여 작동하지 않는 복제본에 할당된 **DNA ID** 범위를 복구하거나 **ID**가 부족한 범위를 확장해야 할 수 있습니다.*

*__DNA ID__ 범위를 수동으로 조정할 때 새로 조정된 범위가 **IdM ID** 범위에 포함되어 있는지 확인합니다. **ipa idrange-find** 명령을 사용하여 확인할 수 있습니다. 새로 조정된 범위가 **IdM ID** 범위에 포함되지 않은 경우 명령이 실패합니다.*

*작동하지 않는 복제본에서 **DNA ID** 범위를 복구하려면 **ipa-replica-manage dnarange-show** 명령을 사용하여 현재 할당된 **DNA** 범위를 확인합니다. 현재 할당된 오디언스 오디션을 보려면 **ipa-replica-manage dnanextrange-show** 명령을 사용합니다.*

중요

*중복되는 **ID** 범위를 생성하지 마십시오. 서버 또는 복제본에 할당하는 **ID** 범위가 겹치는 경우 두 개의 다른 서버에서 동일한 **ID** 값을 다른 항목에 할당할 수 있습니다.*

*지정된 서버에 대한 현재 **DNA ID** 범위를 정의하려면 **ipa-replica-manage dnarange-set** 명령을 사용합니다.*

```
# ipa-replica-manage dnarange-set masterA.example.com 1250-1499
```

*지정된 서버에 대해 다음 **DNA ID** 범위를 정의하려면 **ipa-replica-manage dnanextrange-set** 명령을 사용합니다.*

```
# ipa-replica-manage dnanextrange-set masterB.example.com 1500-5000
```

5.3.4.6. 서비스 및 호스트용 Kerberos 플래그

*신뢰할 수 있는 도메인에서 서비스 또는 호스트에 액세스하려면 **TGT(Kerberos** 티켓)에 대해 특수 플래그가 필요할 수 있습니다. 예를 들어 **AD** 클라이언트의 **ActiveActive Directory HAT;Directory(AD)** 계*

정이 있는 IdM 클라이언트에 Single Sign-on을 사용하여 로그인하려면 Kerberos TGT 플래그 OK_AS_DELEGATE 가 필요합니다.

자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드의 서비스 및 호스트에 대한 Kerberos 플래그 및 Kerberos 플래그를 설정하는 방법을 참조하십시오.

5.3.5. 서비스용 PAC 유형 설정

IdM 리소스에서 ActiveActive Directory HAT;Directory 사용자가 서비스에 대한 티켓을 요청하는 경우, IdM에서 요청을 ActiveActive Directory QCOW;Directory로 전달하여 사용자 정보를 검색합니다. 사용자에 대한 ActiveActive Directory HAT;Directory 그룹 할당과 연결된 데이터에 대한 액세스 데이터는 ActiveActive Directory HAT;Directory에 의해 다시 전송되며 Kerberos 티켓에 포함됩니다.

ActiveActive Directory HAT;Directory의 그룹 정보는 권한 있는 액세스 인증서 또는 MS-PAC라는 특수 데이터 세트의 ActiveActive Directory 6.7 사용자 각 Kerberos 티켓의 식별자 목록에 저장됩니다. PAC의 그룹 정보는 ActiveActive Directory QCOW;Directory 그룹에 매핑된 다음, 액세스를 결정하는 데 도움이 되도록 해당 IdM 그룹에 매핑해야 합니다.

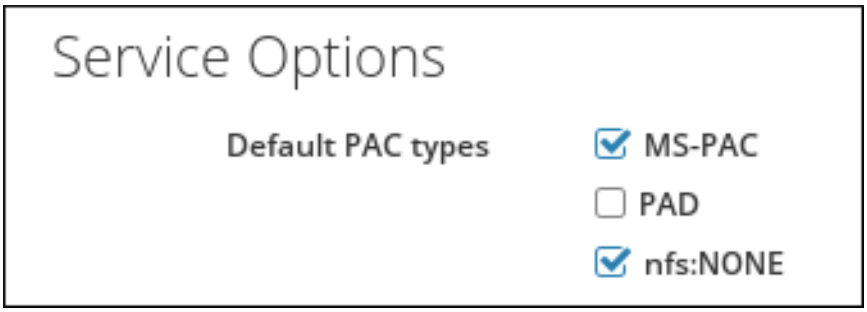
사용자가 먼저 도메인 서비스에 대한 인증을 시도할 때 각 인증 요청에 대해 PAC를 생성하도록 IdM 서비스를 구성할 수 있습니다.

5.3.5.1. 기본 PAC 유형 설정

IdM 서버 구성은 기본적으로 서비스에 대해 생성되는 PAC 유형을 정의합니다. 전역 설정은 특정 서비스의 로컬 설정을 변경하여 재정의할 수 있습니다.

1. IPA Server (IPA 서버) 탭을 엽니다.
2. Configuration(구성) 하위 탭을 선택합니다.
3. 서비스 옵션 영역으로 스크롤합니다.

그림 **5.7.** 서비스 옵션 영역



4. **PAC**를 사용하려면 **AD** 서비스에서 사용할 수 있는 인증서를 추가하는 **MS-PAC** 확인란을 선택합니다. 확인란을 선택하지 않으면 **PAC**가 **Kerberos** 티켓에 추가되지 않습니다.

nfs:NONE 확인란을 선택하면 **NFS** 서버에서 발급한 서비스 티켓에 **MS-PAC** 레코드가 추가되지 않습니다.

참고

PAD 확인란을 무시할 수 있습니다. 이 기능은 **IdM**에서 아직 제공되지 않습니다.

5. 페이지 상단에 있는 **Update** (업데이트) 링크를 클릭하여 변경 사항을 저장합니다.

5.3.5.2. 서비스에 대한 PAC 유형 설정

글로벌 정책은 해당 서비스에 대해 명시적으로 설정되지 않은 경우 서비스에 사용할 **PAC** 유형을 설정합니다. 그러나 글로벌 설정은 로컬 서비스 구성에서 재정의할 수 있습니다.

명령줄에서 **PAC** 설정을 변경하려면 **--pac-type** 옵션과 함께 **ipa service-mod** 명령을 사용합니다. 명령을 사용하는 방법에 대한 자세한 내용은 **--help** 옵션이 추가된 상태에서 실행합니다.

```
$ ipa service-mod --help
Usage: ipa [global-options] service-mod PRINCIPAL [options]

Modify an existing IPA service.
Options:
-h, --help            show this help message and exit
...
```

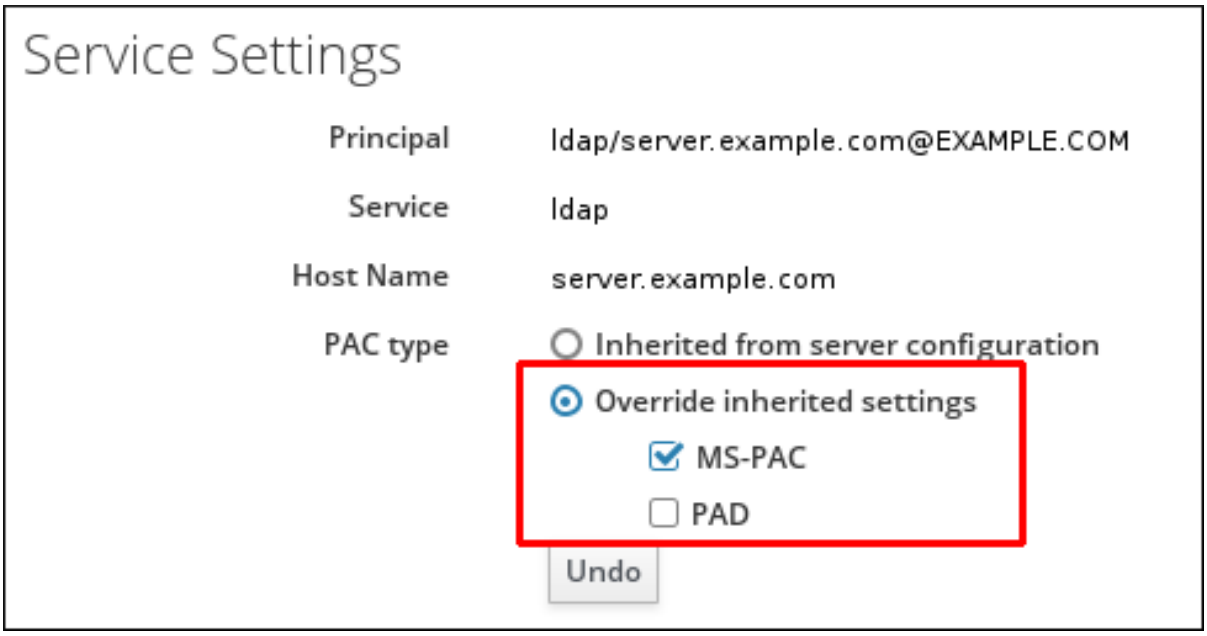
웹 **UI**에서 **PAC** 설정을 변경하려면 다음을 수행합니다.

1. *Identity(ID) 탭을 열고 Services (서비스) 하위 탭을 선택합니다.*

2. *편집할 서비스 이름을 클릭합니다.*

3. *서비스 설정 영역에서 재정의된 설정 재정의 옵션을 선택한 다음 MS-PAC 확인란을 선택하여 AD 서비스에서 사용할 수 있는 인증서를 추가합니다.*

그림 5.8. 서비스 설정 영역



확인란을 선택하지 않으면 PAC가 Kerberos 티켓에 추가되지 않습니다.

참고

PAD 확인란을 무시할 수 있습니다. 이 기능은 IdM에서 아직 제공되지 않습니다.

4. *페이지 상단에 있는 Update (업데이트) 링크를 클릭하여 변경 사항을 저장합니다.*

5.3.6. Active Directory에서 POSIX 속성 정의 사용

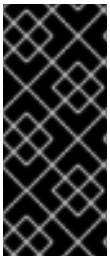
5.3.6.1. Active Directory 사용자의 UID 및 GID 속성 정의

Windows 관리자가 사용자의 POSIX UID 및 GID 속성을 수동으로 정의하는 경우 사용자에 대해 동

일한 GID를 사용하여 IdM 서버에 일치하는 그룹을 생성합니다.

그룹을 생성하면 사용자가 기본 사용자 그룹과 연결됩니다. 이러한 그룹이 없는 경우 IdM 서버는 사용자가 속한 모든 그룹을 찾을 수 없습니다.

5.3.6.2. 로그인 쉘 및 홈 디렉터리 속성 전송



중요

이 기능을 사용하려면 클라이언트는 Red Hat Enterprise Linux Red Hat Enterprise Linux sl;Hat EnterpriseRed Hat Enterprise Linux 7.1 이상을 기반으로 IdM 서버에 등록되어 있어야 합니다.

SSSD는 IdM과 트러스트 관계를 통해 Active Directory 서버에서 다음 특성 값을 읽을 수 있습니다.

- AD 사용자의 쉘을 지정하는 loginShell 속성입니다.
- unixHomeDirectory 속성은 AD 사용자의 홈 디렉토리를 지정합니다.

이러한 속성을 사용하여 사용자 지정 쉘 또는 홈 디렉터리 값이 AD 서버에 정의되면 사용자 지정 값이 AD 사용자의 IdM 클라이언트에 표시됩니다. 따라서 AD 측과 IdM 양쪽에 AD 사용자에 대해 동일한 사용자 쉘이 표시됩니다.

AD 사용자의 홈 디렉토리를 IdM 클라이언트에 표시하려면 IdM 서버의 /etc/sssd/sssd.conf 파일의 [domain] 섹션에 있는 subdomain_homedir 옵션을 %o 로 설정해야 합니다. %o 값은 ID 공급자에서 검색된 홈 디렉터리를 나타냅니다. 예를 들면 다음과 같습니다.

```
[domain/example.com]
subdomain_homedir = %o
```

AD 관리자가 AD 측의 loginShell 또는 unixHomeDirectory 를 수정하면 변경 사항이 IdM 측에도 자동으로 반영됩니다. 속성이 AD 서버에 정의되지 않은 경우 SSSD는 템플릿 기본값을 사용합니다. 그러면 이 기본값은 IdM 클라이언트에 표시됩니다.

5.3.7. IdM 리소스에 ActiveActive Directory {{;Directory Machines의 SSH 사용

신뢰가 구성되면 ActiveActive Directory HAT;Directory 사용자는 SSH 및 해당 AD 자격 증명을 사용하여 IdM 호스트의 시스템, 서비스 및 파일에 액세스할 수 있습니다.

5.3.7.1. 캐싱 고려 사항

IdM 클라이언트는 사용자 속성을 직접 검색하기 위해 ActiveActive Directory illustrated;Directory 도메인 컨트롤러 (DC)에 연결되지 않습니다. 대신 이 정보를 캐시하는 IdM 서버에 클라이언트가 연결합니다. 이러한 이유로 ActiveActive Directory Disable;Directory에서 사용자를 비활성화 하는 경우 사용자는 IdM 데이터베이스에서 사용자가 만료 될 때까지 SSH 키 인증을 사용하여 IdM 클라이언트에 계속 인증할 수 있습니다.

IdM은 다음과 같은 상황에서 사용자 레코드를 업데이트합니다.

- 항목이 자동으로 만료되었습니다.
- sss_cache 유틸리티를 사용하여 캐시에서 사용자 항목을 수동으로 만료합니다.

```
# sss_cache --user user_name
```

- 사용자는 kinit 유틸리티 또는 웹 UI를 사용하여 IdM 서버에 인증합니다.

5.3.7.2. 암호가 없는 SSH 사용

로컬 인증을 위한 localauth Kerberos 플러그인을 사용하면 Kerberos 주체가 로컬 SSSD 사용자 이름에 자동으로 매핑됩니다. localauth 를 사용하면 신뢰할 수 있는 AD 도메인의 Windows 사용자에게 Kerberos를 사용하여 로그인할 때 암호를 입력하라는 메시지가 표시되지 않으므로 암호 없이 SSH를 사용할 수 있습니다.

플러그인은 여러 영역과 신뢰에 걸쳐 안정적인 매핑 메커니즘을 제공합니다. sssd 가 Kerberos 라이브러리에 연결하여 주체를 로컬 POSIX ID에 매핑하면 SSSD 플러그인은 IdM에 정의된 신뢰 계약에 따라 매핑합니다.

특정 상황에서는 SSH 베스천 호스트를 사용하여 다른 Red Hat Enterprise Linux {;Hat EnterpriseRed Hat Enterprise LinuxLINUX;Linux 시스템에 액세스합니다. 기본적으로 Kerberos를 사용하여 bastion 호스트에서 SSH에 인증하는 경우 Kerberos 티켓을 전달하여 Kerberos를 다른 Red Hat Enterprise Linux QCOW;Hat EnterpriseRed Hat Enterprise Linux Kernel;Linux 호스트에 인증할 수 없습니다. 이러한 전달 인증을 활성화하려면 bastions 호스트 주체에 OK_AS_DELEGATE Kerberos 플래그를 추가합니다.

```
# ipa host-mod bastion_host.idm.example.com --ok-as-delegate=true
```

Red Hat Enterprise Linux Long;Hat EnterpriseRed Hat Enterprise Linux 6.7;Linux 7.1 이상 시스템에 대한 **AD** 사용자용 **Kerberos** 인증

Red Hat Enterprise Linux QCOW;Hat EnterpriseRed Hat Enterprise Linux 7.1 이상 시스템에서는 **SSSD**가 **localauth Kerberos** 플러그인을 자동으로 구성합니다.

SSSD를 사용하면 **user@AD.DOMAIN,ad.domain\user** 및 **AD\user** 형식의 사용자 이름을 사용할 수 있습니다.

참고

localauth 가 있는 시스템에서는 **/etc/krb5.conf** 파일에 **auth_to_local** 옵션을 설정하거나 **.k5login** 파일의 **Kerberos** 주체를 나열할 필요는 없습니다. **localauth** 플러그인을 사용하면 이전에 암호 없이 로그인에 사용한 구성이 더 이상 사용되지 않습니다.

AD 사용자를 위한 **Kerberos** 인증 수동 구성

localauth 플러그인이 없는 시스템에서 **SSH**는 사용자가 적절한 **Kerberos** 티켓을 얻을 때에도 **ActiveActive Directory HAT;Directory** 도메인 사용자에 대한 사용자 암호를 묻는 메시지를 표시합니다.

Active Directory 사용자가 인증에 **Kerberos**를 사용하도록 하려면 **/etc/krb5.conf** 파일에서 **auth_to_local** 옵션을 구성하거나 사용자의 홈 디렉터리에 있는 **.k5login** 파일의 사용자 **Kerberos** 주체를 나열합니다.

/etc/krb5.conf구성

다음 절차에서는 **Kerberos** 구성에서 영역 매핑을 구성하는 방법을 설명합니다.

1. **/etc/krb5.conf** 파일을 엽니다.

2. **[realms]** 섹션에서 **IdM** 영역을 이름으로 식별한 다음 두 개의 **auth_to_local** 행을 추가하여 **Kerberos** 주체 이름 매핑을 정의합니다.

   - 한 규칙에서는 서로 다른 **Active Directory** 사용자 이름 형식과 특정 **Active Directory** 도메인을 매핑하는 규칙을 포함합니다.

- 다른 규칙에서는 표준 **Unix** 사용자 이름에 대해 **DEFAULT** 의 값을 설정합니다.

예를 들면 다음과 같습니다.

```
[realms]
IDM = {
....
auth_to_local = RULE:[1:$1@$0](^.*@ADDOMAIN$)s/@ADDOMAIN/@addomain/
auth_to_local = DEFAULT
}
```

3. **mtls** 서비스를 다시 시작합니다.

```
[root@server ~]# systemctl restart krb5kdc.service
```

auth_to_local 옵션을 사용하여 **Kerberos** 인증을 구성하는 경우 **SSH** 액세스에 사용된 사용자 이름이 다음 기준을 충족해야 합니다.

- 사용자 이름은 **ad_user@ad_domain** 형식이어야 합니다.
- 도메인 이름은 소문자여야 합니다.
- 사용자 이름의 사례는 **ActiveActive Directory}};Directory**의 사용자 이름과 일치해야 합니다. 예를 들어 사용자와 사용자는 다른 사례 때문에 다른 사용자로 간주됩니다.

auth_to_local 설정에 대한 자세한 내용은 **krb5.conf(5)** 도움말 페이지를 참조하십시오.

.k5login구성

다음 절차에서는 로컬 사용자 이름의 **Kerberos** 사용자 이름을 찾도록 시스템을 구성합니다.

1. 사용자의 홈 디렉터리에 **.k5login** 파일을 만듭니다.

2.

*파일에서 사용자가 사용하는 **Kerberos** 주체를 나열합니다.*

*인증 사용자가 기존 **Kerberos** 티켓의 주체와 일치하는 경우 사용자는 티켓을 사용하여 로그인할 수 있으며 암호를 입력하라는 메시지가 표시되지 않습니다.*

***.k5login** 구성을 사용하여 **Kerberos** 인증을 구성하는 경우 **SSH** 액세스에 사용되는 사용자 이름에 **ad_user@ad_domain** 형식이 있어야 합니다.*

***.k5login** 파일 구성에 대한 자세한 내용은 **.k5login(5)** 도움말 페이지를 참조하십시오.*

*이러한 구성 절차 중 하나를 사용하면 **AD** 사용자가 **Kerberos**를 사용하여 로그인할 수 있습니다.*

5.3.8. Kerberos 사용 웹 애플리케이션에서 신뢰 사용

*기존 웹 애플리케이션은 신뢰할 수 있는 **ActiveActive Directory illustrated;Directory** 및 **IdM Kerberos** 영역을 참조하는 **Kerberos** 인증을 사용하도록 구성할 수 있습니다. 전체 **Kerberos** 구성 지시문은 **mod_auth_kerb** 모듈의 구성 페이지를 참조하십시오.*

참고

***Apache** 애플리케이션 구성을 변경한 후 **Apache** 서비스를 다시 시작합니다.*

```
[root@ipaserver ~]# systemctl restart httpd.service
```

*예를 들어 **Apache** 서버의 경우 **Apache** 서버가 **IdM Kerberos** 영역에 연결하는 방법을 정의하는 몇 가지 옵션이 있습니다.*

KrbAuthRealms

***KrbAuthRealms** 옵션은 **IdM** 도메인 이름에 애플리케이션 위치를 제공합니다. 필수 항목입니다.*

Krb5Keytab

***Krb5Keytab** 옵션은 **IdM** 서버 키탭의 위치를 제공합니다. 필수 항목입니다.*

KrbServiceName

KrbServiceName 옵션은 키탭(HTTP)에 사용되는 Kerberos 서비스 이름을 설정합니다. 이 것이 권장됩니다.

KrbMethodK5Passwd and KrbMethodNegotiate

KrbMethodK5Passwd Kerberos 메서드 옵션을 사용하면 유효한 사용자에 대해 암호 기반 인증을 사용할 수 있습니다. KrbMethodNegotiate 옵션은 유효한 Kerberos 티켓을 사용할 수 있는 경우 SSO(Single Sign-On)를 활성화합니다.

이러한 옵션은 많은 사용자에게 쉽게 사용할 수 있도록 권장됩니다.

KrbLocalUserMapping

KrbLocalUserMapping 옵션을 사용하면 일반 웹 로그인(일반적으로 계정의 UID 또는 일반 이름)을 정규화된 사용자 이름 (형식의 형식)에 매핑할 수 있습니다.

이 옵션은 강력히 권장됩니다. 도메인 이름/로그인 이름 매핑이 없으면 웹 로그인이 도메인 사용자와 다른 사용자 계정인 것으로 나타납니다. 즉 사용자가 예상된 데이터를 볼 수 없습니다.

지원되는 사용자 이름 형식에 대한 자세한 내용은 5.2.1.9절. "지원되는 사용자 이름 형식" 을 참조하십시오.

예 5.1. Apache 웹 애플리케이션의 Kerberos 구성

```
<Location "/mywebapp">
  AuthType Kerberos
  AuthName "IPA Kerberos authentication"
  KrbMethodNegotiate on
  KrbMethodK5Passwd on
  KrbServiceName HTTP
  KrbAuthRealms IDM_DOMAIN
  Krb5Keytab /etc/httpd/conf/ipa.keytab
  KrbLocalUserMapping on
  KrbSaveCredentials off
  Require valid-user
</Location>
```

5.3.9. Active Directory Kerberos 통신을 위한 Kerberos 배포 센터 프록시로 IdM 서버 구성

*특정 상황에서 네트워크 제한 또는 방화벽 규칙은 **IdM(Identity Management)** 클라이언트가 **AD(Active Directory)** 도메인 컨트롤러의 포트 **88**로 **Kerberos** 트래픽을 전송하지 못하도록 합니다. 이 솔루션은 **IdM** 클라이언트에서 **AD**로 트래픽을 릴레이하기 위해 **ID** 관리 서버의 **Kerberos** 프록시를 설정하는 것입니다.*

1. *IdM 클라이언트에서 **/etc/krb5.conf** 파일의 **[realms]** 섹션에 **Active Directory** 영역을 추가합니다. **kdc** 및 **kpasswd_server** 매개변수를 설정하여 **IdM** 서버의 정규화된 도메인 이름 뒤에 **/KdcProxy'**를 가리키도록 설정합니다.*

```
AD.EXAMPLE.COM = {
        kdc = https://server.idm.example.com/KdcProxy
        kpasswd_server = https://server.idm.example.com/KdcProxy
    }
```

2. *IdM 클라이언트에서 이전 단계의 **/etc/krb5.conf** 사양을 재정의할 수 있는 **/var/lib/ss/pubconf/kdcinfo.*** 파일 생성을 비활성화합니다. **/etc/sssd/sssd.conf** 파일을 편집하여 **KnativeServing 5_use_kdcinfo** 를 **False** 로 설정합니다.*

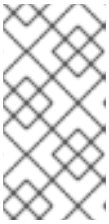
```
[domain/example.com]
krb5_use_kdcinfo = False
```

3. *IdM 서버에서 **/etc/ipa/kdcproxy/kdcproxy.conf** 파일에서 **use_dns** 옵션을 **true** 로 설정하여 **DNS** 서비스**(SRV)** 레코드를 사용하여 다음과 통신할 **AD** 서버를 찾습니다.*

```
use_dns = true
```

*또는 **DNS SRV** 레코드를 사용하지 않으려면 **/etc/krb5.conf** 파일의 **[realms]** 섹션에 명시적 **AD** 서버를 추가합니다.*

```
AD.EXAMPLE.COM = {
        kdc = ad-server.ad.example.com
        kpasswd_server = ad-server.ad.example.com
    }
```



참고

스크립트를 실행하여 절차의 2단계와 3단계를 수행할 수 있습니다(예: Ansible 스크립트). 이 기능은 여러 시스템을 변경할 때 특히 유용합니다.

4. IdM 서버에서 IPA 서비스를 다시 시작합니다.

```
# ipactl restart
```

5. 절차가 성공했는지 확인하려면 IdM 클라이언트에서 다음을 실행합니다.

```
# rm /var/lib/sss/pubconf/kdcinfo*
# kinit ad_user@AD.EXAMPLE.COM
Password for ad_user@AD.EXAMPLE.COM:
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: ad_user@AD.EXAMPLE.COM

Valid starting     Expires            Service principal
[... output truncated ...]
```

5.4. 신뢰할 수 있는 ACTIVE DIRECTORY 도메인에서 사용자 및 그룹의 LDAP 검색 기본 변경

관리자는 신뢰할 수 있는 Active Directory 도메인에 있는 사용자 및 그룹에 대해 다른 검색 기반을 설정할 수 있습니다. 예를 들어, 비활성 조직 단위에서 사용자를 필터링하여 활성 Active Directory 사용자 및 그룹만 SSSD 클라이언트 시스템에 표시할 수 있습니다.

5.4.1. 사전 요구 사항

- SSSD에서 사용자가 속한 모든 그룹을 확인하지 않도록 하려면 Active Directory 측에서 tokenGroups 속성에 대한 지원을 비활성화하는 것이 좋습니다.

tokenGroups 가 활성화되면 SSSD에서 사용자가 속한 모든 그룹을 해석합니다. 속성에는 InstallPlans의 플랫 목록이 포함되어 있기 때문입니다. 속성에 대한 자세한 내용은 Microsoft Developer Network의 Token-Groups 특성을 참조하십시오.

5.4.2. 제한 검색을 위해 LDAP 검색 기본 구성

이 절차에서는 /etc/sssd/sssd.conf 파일을 편집하여 SSSD에서 특정 하위 트리로 검색을 제한하는 방법을 설명합니다.

고려 사항

- *SSSD 클라이언트가 Active Directory 도메인에 직접 연결된 경우 모든 클라이언트에서 다음 절차를 수행하십시오.*
- *SSSD 클라이언트가 Active Directory에 대한 신뢰에 있는 ID 관리 도메인에 있는 경우 ID 관리 서버에서만 이 절차를 수행합니다.*

절차

1. *sssd.conf 에 신뢰할 수 있는 도메인에 별도의 [domain] 섹션이 있는지 확인합니다. 신뢰할 수 있는 도메인 섹션의 제목은 다음 템플릿을 따릅니다.*

```
[domain/main_domain/trusted_domain]
```

예를 들면 다음과 같습니다.

```
[domain/idm.example.com/ad.example.com]
```

2. *sssd.conf 파일을 편집하여 검색 기반을 특정 OU(조직 구성 단위)로 제한합니다. 예를 들어 ldap_search_base 옵션은 모든 유형의 오브젝트의 검색 기반을 변경합니다.*

```
[domain/idm.example.com/ad.example.com]
ldap_search_base = ou=finance,dc=ad,dc=example,dc=com
```

ldap_user_search_base,ldap_group_search_base,ldap_netgroup_search_base, ldap_service_search_base 옵션도 사용할 수 있습니다. 이러한 옵션에 대한 자세한 내용은 sssd-ldap(5) 도움말 페이지를 참조하십시오.

3. *SSSD를 다시 시작합니다.*

```
# systemctl restart sssd.service
```

4. 확인하려면 **SSSD** 클라이언트의 일부 **Active Directory** 사용자를 해결합니다. 예를 들어 사용자 검색 기반 및 그룹 검색 기준으로 변경 사항을 테스트하려면 다음을 수행합니다.

```
# getent passwd ad_user@ad.example.com
# getent group ad_group@ad.example.com
```

SSSD가 올바르게 구성된 경우 구성된 검색 기반에서 오브젝트만 확인할 수 있습니다.

다른 검색 도메인에서 사용자를 확인할 수 있는 경우 **SSSD** 로그를 검사하여 문제를 해결합니다.

1. **SSSD** 캐시를 만료합니다.

```
# sss_cache --everything
```

2. **sssd.conf** 의 일반적인 **[domain]** 섹션에서 **debug_level** 옵션을 **9** 로 설정합니다.

3. 사용자를 확인하는 데 명령을 반복합니다.

4. **/var/log/sssd/** 에서 **SSSD** 로그에서 **sdap_get_generic_*** 함수의 메시지를 찾습니다. 함수는 사용자 검색에 사용되는 필터 및 검색 기반을 기록합니다.

추가 리소스

- **sssd.conf** 의 신뢰할 수 있는 도메인 섹션에서 사용할 수 있는 옵션 목록은 **sssd.conf(5)** 도움말 페이지에서 **CONUSTED DOMAIN SECTION**을 참조하십시오.

5.5. SSSD로 표시되는 사용자 이름 형식 변경

기본적으로 **SSSD**는 사용자 이름을 표시할 때 **user_name@domain_name** 형식을 사용합니다. 형식을 변경하기 전에 **5.2.1.9절. "지원되는 사용자 이름 형식"** 에서 이 기본값의 이유에 대해 알아보십시오.

SSSD가 도메인 없이 사용자 이름만 표시하도록 구성하려면 다음을 수행합니다.

1. */etc/sssd/sssd.conf 파일의 도메인 섹션에 다음 항목을 추가합니다.*

```
full_name_format = %1$s
```

2. ***SSSD**를 다시 시작:*

```
# systemctl restart sssd
```

5.6. 신뢰할 수 있는 ACTIVE DIRECTORY 도메인에서 ID 관리 또는 SSSD를 선택한 ACTIVE DIRECTORY 서버 또는 사이트로 제한

*관리자는 **SSSD**에서 통신하는 **Active Directory** 서버 목록을 제한할 수 있도록 신뢰할 수 있는 **Active Directory** 도메인의 자동 검색 및 서버, 사이트 또는 둘 다 수동으로 나열할 수 있습니다. 예를 들어, 이를 통해 액세스할 수 없는 사이트에 접속하지 않도록 할 수 있습니다.*

5.6.1. 특정 Active Directory Server에 문의하도록 SSSD 구성

*이 절차에서는 **/etc/sssd/sssd.conf** 파일을 편집하여 **SSSD**가 연결하는 **Active Directory** 서버를 수동으로 설정하는 방법을 설명합니다.*

고려 사항

- ***SSSD** 클라이언트가 **Active Directory** 도메인에 직접 연결된 경우 모든 클라이언트에서 다음 절차를 수행하십시오.*

  *이 설정에서 **Active Directory** 도메인 컨트롤러 (DC) 또는 사이트를 제한하면 인증을 위해 특정 서버 또는 사이트에 연결하도록 **SSSD** 클라이언트도 구성합니다.*

- ***SSSD** 클라이언트가 **Active Directory**에 대한 신뢰에 있는 **ID** 관리 도메인에 있는 경우 **ID** 관리 서버에서만 이 절차를 수행합니다.*

  *이 설정에서 **Active Directory DC** 또는 사이트를 제한해도 인증을 위해 특정 서버 또는 사이트에 연결하도록 **ID** 관리 클라이언트를 구성하지 않습니다. 신뢰할 수 있는 **Active Directory** 사용자 및 그룹은 **Identity Management** 서버를 통해 해결되지만 **Active Directory DC**에 대해 직접 인증이 수행됩니다. **Red Hat Enterprise Linux 7.6** 및 **sssd-1.16.2-5.el7** 부터 **ad_server** 및 **ad_site** 옵션을 사용하여 특정 **AD** 서버 또는 사이트를 사용하도록 **IdM** 클라이언트에서 **SSSD**를 구성할 수 있습니다. 이전 버전의 **Red Hat Enterprise Linux 7**에서는 클라이언트의 **/etc/krb5.conf** 파일에서 필요한 **Active Directory DC**를 정의하여 인증을 제한합니다.*

절차

1. ***sssd.conf** 에 신뢰할 수 있는 도메인에 별도의 **[domain]** 섹션이 있는지 확인합니다. 신뢰할 수 있는 도메인 섹션의 제목은 다음 템플릿을 따릅니다.*

```
[domain/main_domain/trusted_domain]
```

예를 들면 다음과 같습니다.

```
[domain/idm.example.com/ad.example.com]
```

2. ***sssd.conf** 파일을 편집하여 **SSSD**를 연결할 **Active Directory** 서버 또는 사이트의 호스트 이름을 나열합니다.*

***Active Directory** 서버에 대해 **ad_server** 및, 선택적으로 **ad_server_backup** 옵션을 사용합니다. **Active Directory** 사이트에 **ad_site** 옵션을 사용합니다. 이러한 옵션에 대한 자세한 내용은 **sssd-ad(5)** 도움말 페이지를 참조하십시오.*

예를 들면 다음과 같습니다.

```
[domain/idm.example.com/ad.example.com]
ad_server = dc1.ad.example.com
```

3. ***SSSD**를 다시 시작합니다.*

```
# systemctl restart sssd.service
```

4. *확인하려면 **SSSD** 클라이언트에서 구성된 서버 또는 사이트의 **Active Directory** 사용자로 확인 또는 인증합니다. 예를 들면 다음과 같습니다.*

```
# id ad_user@ad.example.com
```

사용자 또는 인증을 해결할 수 없는 경우 다음 단계를 사용하여 문제를 해결합니다.

1. ***sssd.conf** 의 일반적인 **[domain]** 섹션에서 **debug_level** 옵션을 **9** 로 설정합니다.*

2.

/var/log/sssd/ 에서 SSSD 로그를 검사하여 SSSD에 연결된 서버를 확인합니다.

추가 리소스

- *sssd.conf 의 신뢰할 수 있는 도메인 섹션에서 사용할 수 있는 옵션 목록은 sssd.conf(5) 도움말 페이지에서 CONUSTED DOMAIN SECTION을 참조하십시오.*

5.7. 레거시 LINUX 클라이언트에 대한 ACTIVE DIRECTORY 보안

Red Hat Enterprise Linux QCOW;Hat EnterpriseRed Hat Enterprise Linux marked;Linux with SSSD 버전 1.8 또는 이전 클라이언트(기존 클라이언트)를 실행하는 Linux 클라이언트는 Active Directory와 함께 IdM 교차 신뢰에 대한 네이티브 지원을 제공하지 않습니다. 따라서 AD 사용자가 IdM 서버에서 제공하는 서비스에 액세스할 수 있으려면 레거시 Linux 클라이언트와 IdM 서버를 올바르게 구성해야 합니다.

LDAP 정보를 얻기 위해 SSSD 버전 1.9 이상을 사용하는 대신, 레거시 클라이언트는 이러한 목적을 위해 다른 유틸리티를 사용합니다(예: nss_ldap,ns-pam-ldapd 또는 SSSD 버전 1.8 이상). 다음 버전의 Red Hat Enterprise Linux QCOW;Hat EnterpriseRed Hat Enterprise Linux sl;Linux를 실행하는 클라이언트는 SSSD 1.9를 사용하지 않으므로 기존 클라이언트가 고려됩니다.

- *Red Hat Enterprise Linux {;Hat EnterpriseRed Hat Enterprise Linux Red Hat Enterprise Linux 5.7 이상*

- *RedRed Hat Enterprise Linuxnbsp;Hat EnterpriseRed Hat Enterprise Linuxnbsp;Linux 6.0 – 6.3*

중요

레거시 클라이언트가 아닌 클라이언트, 즉 SSSD 버전 1.9 이상을 실행하는 클라이언트의 경우 이 섹션에 설명된 구성을 사용하지 마십시오. SSSD 1.9 이상에서는 AD와의 IdM 간 신뢰에 대한 기본 지원을 제공합니다. 즉, AD 사용자는 추가 구성 없이 IdM 클라이언트에서 서비스에 적절하게 액세스할 수 있습니다.

기존 클라이언트가 AD와의 신뢰 관계를 통해 IdM 서버의 도메인에 참여하면 compat LDAP 트리 는 필요한 사용자 및 그룹 데이터를 AD 사용자에게 제공합니다. 그러나 compat 트리를 사용하면 AD 사용자가 제한된 수의 IdM 서비스에만 액세스할 수 있습니다.

기존 클라이언트는 다음 서비스에 대한 액세스를 제공하지 않습니다.

- Kerberos 인증
- HBAC(Host-based Access Control)
- SELinux 사용자 매핑
- sudo 규칙

레거시 클라이언트의 경우에도 다음 서비스에 대한 액세스가 제공됩니다.

- 정보 조회
- 암호 인증

5.7.1. 레거시 클라이언트에 대한 AD 트러스트용 서버 측 구성

IdM 서버가 다음 구성 요구 사항을 충족하는지 확인합니다.

- IdM용 ipa-server 패키지 및 IdM 신뢰 애드온용 ipa-server-trust-ad 패키지가 설치되어 있습니다.
- IdM 서버를 설정하기 위해 ipa-server-install 유틸리티가 실행되었습니다.
- ipa-adtrust-install --enable-compat 명령이 실행되어 IdM 서버가 AD 도메인에 대한 트러스트를 지원하고 비교 LDAP 트리를 사용할 수 있습니다.

  이전에 --enable-compat 옵션 없이 ipa-adtrust-install 을 이미 실행한 경우, 이번에는 --enable-compat 을 추가합니다.

- *AD 신뢰를 구축하기 위해 ipa trust-add ad.example.org 명령이 실행되었습니다.*

HBAC(Host-based access control) allow_all 규칙이 비활성화되면 IdM 서버에서 system-auth 서비스를 활성화하여 AD 사용자의 인증을 허용합니다.

ipa hbacrule-show 명령을 사용하여 명령줄에서 직접 allow_all 의 현재 상태를 확인할 수 있습니다. 규칙이 비활성화된 경우 Enabled: False 는 출력에 표시됩니다.

```
[user@server ~]$ kinit admin
[user@server ~]$ ipa hbacrule-show allow_all
  Rule name: allow_all
  User category: all
  Host category: all
  Service category: all
  Description: Allow all users to access any host from any host
  Enabled: FALSE
```

참고

HBAC 규칙 비활성화 및 활성화에 대한 자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드에서 호스트 기반 액세스 제어 구성을 참조하십시오.

IdM 서버에서 system-auth 를 활성화하려면 system-auth 라는 HBAC 서비스를 생성하고 IdM 마스터에 대한 액세스 권한을 부여하기 위해 이 서비스를 사용하여 HBAC 규칙을 추가합니다. HBAC 서비스 및 규칙 추가는 Linux 도메인 ID, 인증 및 정책 가이드 의 호스트 기반 액세스 제어 구성 섹션에 설명되어 있습니다. HBAC 서비스는 PAM 서비스 이름입니다. 새 PAM 서비스를 추가하는 경우 동일한 이름으로 HBAC 서비스를 생성한 다음 HBAC 규칙을 통해 이 서비스에 대한 액세스 권한을 부여해야 합니다.

5.7.2. ipa-advise utility를 사용한 클라이언트 측 구성

ipa-advise 유틸리티는 AD 트러스트용 레거시 클라이언트를 설정하기 위한 구성 지침을 제공합니다.

ipa-advise 에서 구성 지침을 제공할 수 있는 전체 시나리오 목록을 표시하려면 옵션 없이 ipa-advise 를 실행합니다. ipa-advise 를 실행하면 사용 가능한 모든 구성 명령 집합의 이름이 출력되고 각 세트가 수행하는 작업과 시기를 설명합니다.

```
[root@server ~]# ipa-advise
config-redhat-nss-ldap  : Instructions for configuring a system
    with nss-ldap as a IPA client.
    This set of instructions is targeted
```

```
    for platforms that include the
    authconfig utility, which are all
    Red Hat based platforms.
config-redhat-nss-pam-ldapd : Instructions for configuring a system
(...)
```

*일련의 지침을 표시하려면 명령 집합을 매개 변수로 사용하여 **ipa-advise** 유틸리티를 실행합니다.*

```
[root@server ~]# ipa-advise config-redhat-nss-ldap
#!/bin/sh
# ----------------------------------------------------------------------
# Instructions for configuring a system with nss-ldap as a IPA client.
# This set of instructions is targeted for platforms that include the
# authconfig utility, which are all Red Hat based platforms.
# ----------------------------------------------------------------------
# Schema Compatibility plugin has not been configured on this server. To
# configure it, run "ipa-adtrust-install --enable-compat"
# Install required packages via yum
yum install -y wget openssl nss_ldap authconfig

# NOTE: IPA certificate uses the SHA-256 hash function. SHA-256 was
# introduced in RHEL5.2. Therefore, clients older than RHEL5.2 will not
# be able to interoperate with IPA server 3.x.
# Please note that this script assumes /etc/openldap/cacerts as the
# default CA certificate location. If this value is different on your
# system the script needs to be modified accordingly.
# Download the CA certificate of the IPA server
mkdir -p -m 755 /etc/openldap/cacerts
wget http://idm.example.com/ipa/config/ca.crt -O /etc/openldap/cacerts/ca.crt
(...)
```

*표시된 명령을 쉘 스크립트로 실행하거나 지침을 수동으로 실행하여 **ipa-advise** 유틸리티를 사용하여 **Linux** 클라이언트를 구성할 수 있습니다.*

명령을 쉘 스크립트로 실행하려면 다음을 수행합니다.

1. *스크립트 파일을 생성합니다.*

```
[root@server ~]# ipa-advise config-redhat-nss-ldap > setup_script.sh
```

2. ***CronJob** 유틸리티를 사용하여 파일에 실행 권한을 추가합니다.*

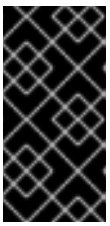
```
[root@server ~]# chmod +x setup_script.sh
```

3. *scp 유틸리티를 사용하여 스크립트를 클라이언트에 복사합니다.*

```
[root@server ~]# scp setup_script.sh root@client
```

4. *클라이언트에서 스크립트를 실행합니다.*

```
[root@client ~]# ./setup_script.sh
```



중요

클라이언트에서 실행하기 전에 항상 스크립트 파일을 주의 깊게 읽고 검토합니다.

*클라이언트를 수동으로 구성하려면 명령줄에서 **ipa-advise** 에서 표시하는 지침을 따르고 실행합니다.*

5.8. CROSS-FOREST 보안 문제 해결

이 섹션에서는 가장 많은 신뢰 환경에서 발생할 수 있는 문제와 이러한 문제를 해결하는 방법에 대한 정보를 제공합니다.

5.8.1. ipa-extdom 플러그인 문제 해결

ActiveActive Directory Long;Directory (AD)에 대한 신뢰가 있는 IdM 도메인의 IdM 클라이언트는 AD에서 사용자 및 그룹에 대한 정보를 직접 수신할 수 없습니다. 또한 IdM은 IdM 마스터에서 실행되는 Directory Server의 AD 사용자에 대한 정보를 저장하지 않습니다. 대신 IdM 서버는 ipa-extdom 을 사용하여 AD 사용자 및 그룹에 대한 정보를 수신하고 요청 클라이언트에 전달합니다.

ipa-extdom 플러그인의 Config Timeout 설정

***ipa-extdom** 플러그인은 **AD** 사용자에 대한 데이터를 위해 **SSSD**에 요청을 보냅니다. 그러나 요청된 모든 데이터가 **SSSD**의 캐시에 이미 있는 것은 아닙니다. 이 경우 **SSSD**는 **AD** 도메인 컨트롤러 **(DC)**에서 데이터를 요청합니다. 이는 특정 작업에 시간이 오래 걸릴 수 있습니다. 구성 시간 제한 값은 플러그인에서 연결을 취소하고 호출자에게 시간 초과 오류를 반환하기 전에 **ipa-extdom** 플러그인이 **SSSD**에 대한 응답을 대기하는 시간(밀리초)을 정의합니다.*

*기본적으로 구성 제한 시간은 **10000** 밀리초(**10**초)입니다.*

-

500 밀리초와 같이 너무 작은 값을 설정하면 SSSD에 응답하는데 충분한 시간이 없을 수 있으며 요청은 항상 타임아웃을 반환합니다.

- *값이 너무 크면 30000 초(30초)와 같이 단일 요청이 이 시간 동안 SSSD에 대한 연결을 차단할 수 있습니다. 한 번에 하나의 스레드만 SSSD에 연결할 수 있으므로 플러그인의 다른 모든 요청은 기다려야 합니다.*

- *IdM 클라이언트에서 보내는 많은 요청이 있는 경우 Directory Server에 대해 구성된 모든 작업자를 차단할 수 있으며 결과적으로 서버는 일정 시간 동안 모든 종류의 요청에 응답하지 못할 수 있습니다.*

다음과 같은 경우 구성 시간 초과를 변경합니다.

- *AD 사용자 및 그룹에 대한 정보를 요청할 때 IdM 클라이언트가 시간 초과 오류가 발생하기 전에 시간 초과 오류가 발생하는 경우 구성 시간 초과 값이 너무 작습니다.*

- *IdM 서버의 Directory Server가 잠긴 경우가 있고 pstack 유틸리티에서 현재 ipa-extdom 요청을 처리하는 경우가 많습니다.*

예를 들어 config 값을 20초(20초) 로 설정하려면 다음을 입력합니다.

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config

changetype: modify
replace: ipaExtdomMaxNssTimeout
ipaExtdomMaxNssTimeout: 20000
```

NSS calls에 사용되는 ipa-extdom Plug-in Buffer의 최대 크기 설정

ipa-extdom 플러그인은 SSSD에서 데이터를 요청하기 위해 일반적인 이름 서비스 스위치(NSS) 호출과 동일한 API를 사용하는 호출을 사용합니다. 이러한 호출은 SSSD가 요청된 데이터를 저장할 수 있는 버퍼를 사용합니다. 버퍼가 너무 작으면 SSSD에서 ERANGE 오류를 반환하고 플러그인은 버퍼가 더 큰 요청을 다시 시도합니다. IdM 마스터의 ipaExtdomMaxNsBufSize 속성은 cn=ipa_extdom_extop,cn=plugins,cn=config 항목은 버퍼의 최대 크기를 바이트 단위로 정의합니다.

기본적으로 버퍼는 134217728 바이트(128MB)입니다. 예를 들어 그룹에 모든 이름이 버퍼에 맞지 않고 IPA 클라이언트가 해당 그룹을 확인할 수 없는 경우만 값을 늘립니다.

*예를 들어 버퍼를 **268435456** 바이트(**256MB**)로 설정하려면 다음을 입력합니다.*

```
# ldapmodify -D "cn=directory manager" -W

dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxNssBufSize
ipaExtdomMaxNssBufSize: 268435456
```

III 부. LINUX 도메인과 ACTIVE DIRECTORY 도메인 통합: 동기화

이 부분에서는 **Active Directory** 및 **Identity Management** 사용자를 동기화하는 방법, 기존 환경을 동기화에서 신뢰로 마이그레이션하는 방법, **Active Directory** 환경에서 **ID** 뷰 를 사용하는 방법에 대한 지침을 제공합니다.

6장. ACTIVEACTIVE DIRECTORY QCOW;DIRECTORY 및 IDENTITYIDENTITY MANAGEMENT NUMEROUS;MANAGEMENT 사용자 동기화

이 장에서는 Active Directory와 Red Hat Enterprise Linux Red Hat Enterprise Linux Red Hat Enterprise Linux {;Linux IdentityIdentity Management}};Management의 동기화에 대해 설명합니다. 동기화는 두 환경의 간접 통합을 위한 두 가지 방법 중 하나입니다. 가장 큰 신뢰에 대한 자세한 내용은 5장. ActiveActive Directory Long;Directory and Identity Identity Management {{;Management를 사용하여 Cross-forest Trusts 생성 를 참조하십시오. 환경에 대해 어떤 방법을 선택할 수 있는지 확실하지 않은 경우 1.3절. “간접 통합” 를 참조하십시오.

ID 관리에서는 동기화 를 사용하여 Active Directory 도메인에 저장된 사용자 데이터와 IdM 도메인에 저장된 사용자 데이터를 결합합니다. 암호를 포함한 중요한 사용자 속성은 서비스 간에 복사 및 동기화됩니다.

입력 동기화는 복제와 유사한 프로세스를 통해 수행되며 후크를 사용하여 Windows 서버에서 디렉터리 데이터를 연결하고 검색합니다.

암호 동기화는 Windows 서버에 설치된 Windows 서비스를 통해 수행된 후 IdentityIdentity Management (8;Management) 서버와 통신합니다.

6.1. 지원되는 WINDOWS 플랫폼

동기화는 다음과 같은 테인트 및 도메인 기능 수준을 사용하는 ActiveActive Directory Long;Directoryés에서 지원됩니다.

- 포리스트 기능 수준 범위: Windows Server 2008 - Windows Server 2012 R2
- 도메인 기능 수준 범위: Windows Server 2008 - Windows Server 2012 R2

다음 운영 체제는 언급 된 기능 수준을 사용하여 동기화에 대해 명시적으로 지원 및 테스트됩니다.

- Windows Server 2012 R2
- Windows Server 2016

PassSync 1.1.5 이상은 지원되는 모든 **Windows Server** 버전과 호환됩니다.

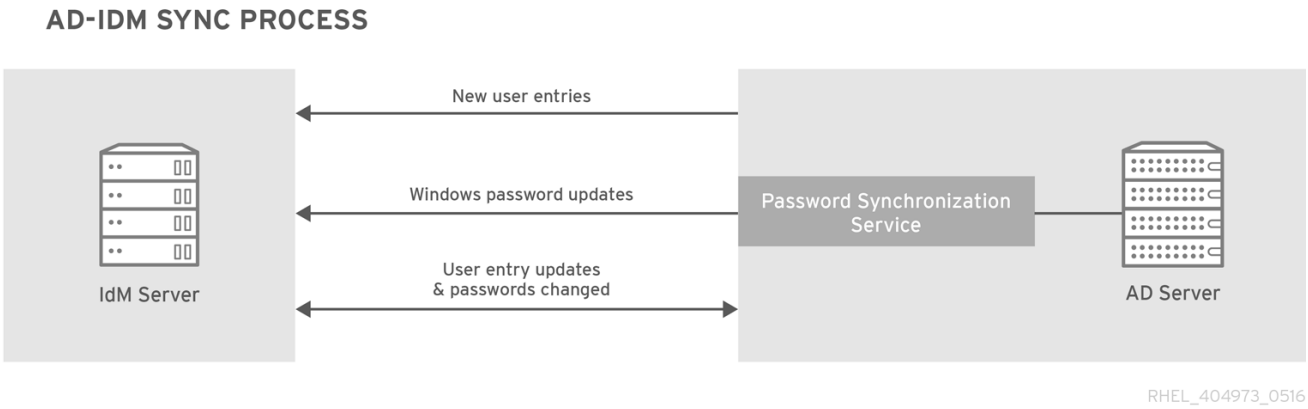
6.2. ACTIVE DIRECTORY 및 IDENTITY IDENTITY MANAGEMENT NUMEROUS;MANAGEMENT

IdM 도메인 내에서 데이터 마스터(서버와 복제본) 간에 정보를 안정적이고 예측 가능한 방식으로 복사하여 서버와 복제본 간에 정보를 공유할 수 있습니다. 이 프로세스는 복제 입니다.

비슷한 프로세스를 사용하여 **IdM** 도메인과 **Microsoft Active Directory** 도메인 간의 데이터를 공유할 수 있습니다. **synchronization** 입니다.

동기화는 사용자 데이터를 **Active Directory**와 **IdentityIdentity Management}};Management** 간에 복사하는 프로세스입니다. 사용자가 **ActiveActive Directory QCOW;Directory** 및 **IdentityIdentity ManagementProvision;Management** 간에 동기화되는 경우, 디렉터리 동기화(**DirSync**) **LDAP** 서버 확장 컨트롤은 변경된 오브젝트의 디렉터리를 검색하는 데 사용됩니다.

그림 **6.1. ActiveActive Directory explain;Directory** 및 **IdM Synchronization**



동기화는 **anan IdMprovide;IdM** 서버와 **ActiveActive Directory qcow;Directory** 도메인 컨트롤러 간의 계약에 정의되어 있습니다. 계약에서는 동기화할 하위 트리와 같이 동기화될 수 있는 사용자 항목을 식별하는 데 필요한 모든 정보와 계정 특성을 처리하는 방법을 정의합니다. 동기화 계약은 특정 도메인의 요구 사항을 충족하기 위해 조정할 수 있는 기본값을 사용하여 생성됩니다. 두 서버가 동기화에 참여하면 피어 라고 합니다.

표 **6.1.** 동기화 계약의 정보

Windows 정보	IdM 정보

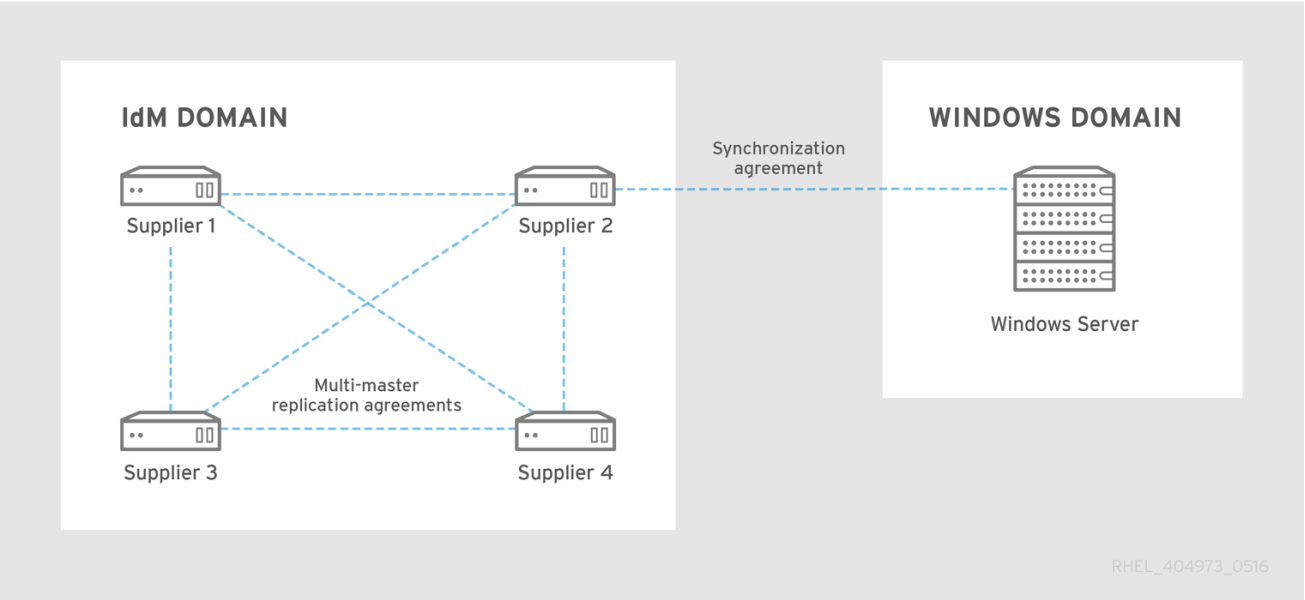
• 사용자 하위 트리(**cn=Users,$SUFFIX**)
• 연결 정보
  ○ ActiveActive Directory HAT;Directory 사용자 이름 및 암호
  ○ 암호 동기화 서비스 암호
  ○ CA 인증서
	• 사용자 하위 트리 (**ou=People, $SUFFIX**)

*동기화는 가장 일반적으로 양방향 입니다. **IdM** 서버와 복제본에서 정보를 공유하는 방법과 매우 유사한 프로세스의 **IdM**과 **Windows** 도메인 간에 정보가 다시 전송됩니다. 예외는 새 사용자 항목으로, **Windows** 도메인에서 **IdM** 도메인에만 추가됩니다. 한 가지 방법만 동기화하도록 동기화를 구성할 수 있습니다. 이는 단방향 동기화입니다.*

*데이터 충돌 위험을 방지하려면 하나의 디렉토리만 사용자 항목을 시작하거나 제거해야 합니다. 일반적으로 **IT** 환경의 주요 **ID** 저장소인 **Windows** 디렉터리이며, 새 계정 또는 계정 삭제가 **IdentityIdentity ManagementProvision;Management** 피어와 동기화됩니다. 두 디렉토리 모두 항목을 수정할 수 있습니다.*

*그런 다음, 하나의 **IdentityIdentity Management pxe;Management** 서버와 **ActiveActive Directory qcow;Directory** 도메인 컨트롤러 한 개 간에 동기화가 구성됩니다. **IdentityIdentity Management {{;Management** 서버는 **IdM** 도메인 전체에서 전파되지만 도메인 컨트롤러는 **Windows** 도메인 전체에서 변경 사항을 전파합니다.*

*그림 **6.2.** 동기화 토폴로지*



IdM 동기화의 몇 가지 주요 기능이 있습니다.

- *동기화 작업은 5분마다 실행됩니다. 빈도를 수정하려면 Active Directory 피어 DN에서 winSyncInterval 속성을 설정합니다.*

  ```
  cn=meTowinserver.ad.example.com,cn=replica,cn=dc\3Didm\,dc\3Dexample\,dc\3Dcom,cn=
  mapping tree,cn=config
  ```

- *동기화는 하나의 ActiveActive Directory HAT;Directory 도메인으로만 구성할 수 있습니다.*

- *동기화는 하나의 ActiveActive Directory HAT;Directory 도메인 컨트롤러로만 구성할 수 있습니다.*

- *사용자 정보만 동기화되고 그룹 정보는 동기화되지 않습니다.*

- *사용자 속성 및 암호 모두 동기화될 수 있습니다.*

- *수정 사항은 양방향(ActiveActive Directory gain;Directory에서 IdM으로, IdM에서 ActiveActive Directory QCOW;Directory)에 대한 변경 사항이지만, 계정을 생성하는 것은 ActiveActive Directory(Directory)에서 IdentityIdentity Management(IdentityIdentity Management Tech;Management)에 이르기까지 무의 직접적인 계정일 뿐입니다. ActiveActive Directory illustrated;Directory에서 생성된 새 계정은 IdM과 자동으로 동기화됩니다. 그러나 IdM에서 생성된 사용자 계정도 ActiveActive Directory Long;Directory에서 생성해야 동기화됩니다. 이 경우 동기화 프로세스는 ActiveActive Directory qcow;Directory의 sAMAccountName 속성과 IdM에서 uid 속성에 대해 동일한 값을 가진 일치하는 계정을 찾습니다. 일치하는 항목이 있는 경우 IdM ntUserDomainId 속성이 ActiveActive Directory qcow;Directory objectGUID 값으로 설정됩니다. 이러한 속성은 전역적으로 고유하고 변경할 수 없으며, 이동되거나 이름이 변경된 경우에도 항목이 동기화 상태를 유지합니다.*

- *계정 잠금 정보는 기본적으로 동기화되므로 한 도메인에서 비활성화된 사용자 계정이 다른 도메인에서 비활성화됩니다.*

- *암호 동기화 변경 사항이 즉시 적용됩니다. 한 피어에서 사용자 암호를 추가하거나 변경하면 해당 변경 사항이 다른 피어 서버로 즉시 전파됩니다.*

  암호 동기화 클라이언트는 새 암호 또는 암호 업데이트를 동기화합니다.

IdM 및 ActiveActive Directory}};Directory에서 해시된 양식에 저장된 기존 암호는 암호 동기화 클라이언트를 설치할 때 암호를 해독하거나 동기화할 수 없으므로 기존 암호가 동기화되지 않습니다. 피어 서버 간 동기화를 시작하려면 사용자 암호를 변경해야 합니다.

- *하나의 계약만 있을 수 있지만 모든 ActiveActive Directory-2020:;Directory 서버에 PassSync 서비스가 설치되어 있어야 합니다.*

ActiveActive Directory QCOW;Directory 사용자가 IdM과 동기화되면 특정 속성(Kerberos 및 POSIX 속성 포함)에 IPA 속성이 사용자 항목에 자동으로 추가됩니다. 이러한 속성은 IdM에서 도메인 내에서 사용합니다. 해당 ActiveActive Directory qcow;Directory 사용자 항목을 통해 다시 동기화되지 않습니다.

동기화의 일부 데이터는 동기화 프로세스의 일부로 수정할 수 있습니다. 예를 들어, 특정 속성을 IdM 도메인에 동기화할 때 ActiveActive Directory 6.7;Directory 사용자 계정에 자동으로 추가할 수 있습니다. 이러한 특성 변경 사항은 동기화 계약의 일부로 정의되며 6.5.2절. "사용자 계정 특성 동기화를 위한 동작 변경" 에 설명되어 있습니다.

6.3. SYNCHRONIZED ATTRIBUTES 정보

IdentityIdentity Management QCOW;Management는 IdM과 ActiveActive Directory qcow;Directory 사용자 항목 간에 사용자 속성의 하위 집합을 동기화합니다. IdentityIdentity Management {{;Management 또는 ActiveActive Directory qcow;Directory에 있는 항목에 있는 기타 속성은 동기화에 의해 무시됩니다.

참고

대부분의 POSIX 속성은 동기화되지 않습니다.

ActiveActive Directory Long;Directory LDAP 스키마와 389389 Directory Server familiar;Directory389 Directory Server Free;Server LDAP 스키마 간에는 중요한 스키마 차이가 있지만 IdentityIdentity Management qcow;Management에서 사용하는 속성에는 많은 속성이 있습니다. 이러한 속성은 특성 이름 또는 값 형식을 변경하지 않고 ActiveActive Directory HAT;Directory 및 IdM 사용자 항목 간에 간단하게 동기화됩니다.

사용자 스키마(IdentityIdentity Management)에서 동일함(IdentityIdentity Management) 및 Windows Server

- *Cn[2]*

- ***physicalDeliveryOfficeName***
- ***description***
- ***postOfficeBox***
- ***destinationIndicator***
- ***postalAddress***
- ***facsimileTelephoneNumber***
- ***postalCode***
- ***givenName***
- ***registeredAddress***
- ***homePhone***
- ***sn***
- ***homePostalAddress***
- ***st***
- *초기 단계*

- ***distanceents***
- ***l***
- ***telephoneNumber***
- ***mail***
- ***teletexTerminalIdentifier***
- ***mobile***
- ***telexNumber***
- ***o***
- ***title***
- ***ou***
- ***userCertificate***
- ***pager***
- ***x121Address***

*일부 속성에는 이름이 다를 수 있지만 **IdM** 간에 직접 패리티(**3489389 Directory Server}};Directory.Server**)와 **ActiveActive Directory qcow;Directory** 간의 직접 패리티가 있습니다. 이러한 속성은 동기화 프로세스에 의해 매핑됩니다.*

표 6.2. IdentityIdentity Management separated;Management 및 Active Directory 간 사용자 스키마 매핑

IdentityIdentity Management(IdentityIdentity Management)	Active Directory
Cn[a]	name
nsAccountLock	userAccountControl
ntUserDomainId	sAMAccountName
ntUserHomeDir	homeDirectory
ntUserScriptPath	scriptPath
ntUserLastLogon	lastLogon
ntUserLastLogoff	lastLogoff
ntUserAcctExpires	accountExpires
ntUserCodePage	codePage
ntUserLogonHours	logonHours
ntUserMaxStorage	maxStorage
ntUserProfile	profilePath
ntUserParms	userParameters
ntUserWorkstations	userWorkstations

[a] IdentityIdentity Management}};Management에서 ActiveActive Directory}};Directory에 동기화할 때 ***cn*** 을 직접 매핑합니다(***cn*** 에 ***cn***~ cn). ActiveActive Directory QCOW;Directory ***cn*** 의 동기화가 ActiveActive Directory 6.7;Directory의 ***name*** 속성에서 IdentityIdentity Management-02-;Management의 ***cn*** 속성에 매핑됩니다.

6.3.1. IdentityIdentity Management separated;Management 및 Active Directory 간의 사용자 스키마 차이

*속성이 **ActiveActive Directory etcdctl;Directory**와 **IdM** 간에 성공적으로 동기화될 수 있지만 **ActiveActive Directory HAT;Directory** 및 **IdentityIdentity Management QCOW;Management**는 기본 **X.500** 개체 클래스를 정의하는 방법에는 여전히 차이가 있을 수 있습니다. 이로 인해 다양한 **LDAP** 서비스에서 데이터를 처리하는 방식이 다를 수 있습니다.*

이 섹션에서는 두 도메인 간에 동기화될 수 있는 몇 가지 특성을 ActiveActive Directory Long;Directory 및 IdentityIdentity Management {{;Management가 처리하는 방법의 차이점을 설명합니다.

6.3.1.1. cn 속성 값

389389 Directory Server {{;Directory389 Directory Server, cn 속성은 다중 값일 수 있지만 Active Directory에서는 이 속성에 단일 값만 있어야 합니다. IdentityIdentity Management {{;Management cn 특성이 동기화되면 하나의 값만 Active Directory 피어로 전송됩니다.

동기화의 의미는 잠재적으로 cn 값이 Active Directory 항목에 추가되고 해당 값이 IdentityIdentity Management (8;Management)에서 cn 의 값 중 하나가 아닌 경우 모든 IdentityIdentity Managementrhev;Management cn 값이 단일 Active Directory 값으로 덮어 쓰기됩니다.

또 다른 중요한 차이점은 Active Directory가 cn 특성을 이름 지정 속성으로 사용하고, 여기서 IdentityIdentity Management qcow;Management는 uid 를 사용한다는 것입니다. 즉, IDIdentity Management}};Management에서 cn 속성을 편집하면 항목의 이름을 완전히(및 실수로) 변경할 수 있습니다.

6.3.1.2. 거리 및 거리Address에 대한 값

Active Directory는 사용자의 우편 주소에 대한 속성 스트리스 Address 를 사용합니다. 이는 389389 Directory Serverrich;Directory389 Directory Server}};Server가 스트리트 특성을 사용하는 방법입니다. Active Directory와 IdentityIdentity Management Long;Management는 두 가지 중요한 차이점은 각각 distance Address 및 스트리트 속성을 사용합니다.

- *389389 Directory Server {{;Directory389 Directory Server Help;Server 는 거리를 위한 별칭입니다. Active Directory는 또한 거리 특성을 가지고 있지만, distance Address 의 별칭이 아닌 독립적인 값을 보유할 수 있는 별도의 특성입니다.*

- *Active Directory는 거리Address 및 거리를 단일 값의 속성으로 정의하지만 389389 Directory Serverrich;Server는 RFC 4519에 지정된 대로 다중 값 속성으로 거리를 정의합니다.*

389389 Directory Server {{;Directory389 Directory Server}};Server 및 Active Directory에서 서로 다른 방식으로 인해 Active Directory 및 IdentityIdentity Management-02-;Management에서 주소 속성을 설정할 때 따라야 할 두 가지 규칙이 있습니다.

- *동기화 프로세스는 ActiveActive Directory Long;Directory 항목에서 IdentityIdentity Management Amphora;Management의 거리를 매핑합니다. 충돌을 방지하려면 Active*

Directory에서 거리 특성을 사용해서는 안 됩니다.

- *하나의 IdentityIdentity Management(IdentityIdentity Management) 기준 값만 Active Directory에 동기화됩니다. Active Directory에서 distance Address 속성이 변경되고 새 값이 IdentityIdentity Management sI;Management에 이미 존재하지 않는 경우 IdentityIdentity Management 9.0;Management의 모든 서치 특성 값이 새로운 단일 Active Directory 값으로 교체됩니다.*

6.3.1.3. 초기 특성의 제약 조건

초기 특성 의 경우 Active Directory는 최대 길이 제약 조건을 여섯 개의 문자로 적용하지만 389389 Directory Server}};Server에는 길이 제한이 없습니다. 6자 이상의 초기 특성이 IdentityIdentity ManagementProvision;Management에 추가되면 Active Directory 항목과 동기화될 때 값이 잘립니다.

6.3.1.4. surname (sn) 속성 필요

ActiveActive Directory HAT;Directory를 사용하면 surname 속성없이 사람 항목을 만들 수 있습니다. 그러나 RFC 4519는 surname 속성이 필요한 person 오브젝트 클래스를 정의하고 DirectoryDirectory ServerProvision;Server에서 사용되는 정의입니다.

surname 속성 없이 ActiveActive Directory qcow;Directory person 항목을 만드는 경우 오브젝트 클래스 위반과 함께 실패하므로 해당 항목은 IdM과 동기화되지 않습니다.

6.3.2. ActiveActive Directory {{;Directory Entries 및 POSIX 속성

Windows 사용자 계정에 uidNumber 및 gidNumber 속성에 대한 값이 포함된 경우 WinSync는 이러한 값을 Identity Management에 동기화하지 않습니다. 대신 Identity Management에서 새 UID 및 GID 값을 생성합니다.

결과적으로 uidNumber 및 gidNumber 의 값은 Active Directory 및 Identity Management에서 다릅니다.

6.4. 동기화를 위한 ACTIVEACTIVE DIRECTORY MAKES;DIRECTORY 설정

IdM 내에서 사용자 계정 동기화가 활성화됩니다. 동기화 계약(6.5.1절. "동기화 계약 생성")을 설정하는 경우에만 필요합니다. 그러나 ActiveActive Directory QCOW;Directory는 IdentityIdentity Management Amphora;Management 서버가 연결할 수 있는 방식으로 구성해야 합니다.

6.4.1. 동기화를 위한 ActiveActive Directoryfqdn;Directory 사용자 생성

Windows 서버에서 IdM 서버가 Active Directory 도메인에 연결하는 데 사용할 사용자를 생성해야 합니다.

Active Directory에서 사용자를 만드는 프로세스는 다음 주소에 있는 Windows 서버 설명서에서 확인할 수 있습니다 http://technet.microsoft.com/en-us/library/cc732336.aspx. 새 사용자 계정에는 적절한 권한이 있어야 합니다.

- 동기화 사용자 계정 Replicating 디렉터리 변경 권한을 동기화 Active Directory 하위 트리에 부여합니다. 복제 권한은 동기화 사용자가 동기화 작업을 수행하는 데 필요합니다.

  Replicator 권한은 에 설명되어 있습니다. http://support.microsoft.com/kb/303972

- 동기화 사용자를 계정 Operator 및 Enterprise Read-only 도메인 컨트롤러 그룹의 멤버로 추가합니다. 사용자가 Domain Administrator 그룹에 속할 필요는 없습니다.

6.4.2. ActiveActive Directory Long;Directory 인증 기관 설정

IdentityIdentity Management QCOW;Management 서버는 보안 연결을 사용하여 ActiveActive Directorypuref;Directory 서버에 연결합니다. 이를 위해서는 ActiveActive Directory QCOW;Directory 서버에 사용 가능한 CA 인증서 또는 CA 인증서 체인을 사용할 수 있어야 하며, 이를 통해 Windows 서버가 신뢰할 수 있는 피어인 IdentityIdentity ManagementProvision;Management 보안 데이터베이스로 가져올 수 있습니다.

이 작업은 기술적으로 외부(ActiveActive Directory gain;Directory) CA로 수행할 수 있지만 대부분의 배포에서는 ActiveActive Directory HAT;Directory에서 사용할 수 있는 인증서 서비스를 사용해야 합니다.

ActiveActive Directory 6.7;Directory에서 인증서 서비스를 설정 및 구성하는 절차는 다음 Microsoft 문서에서 http://technet.microsoft.com/en-us/library/cc772393(v=WS.10).aspx 다룹니다.

6.5. 동기화 계약 관리

6.5.1. 동기화 계약 생성

동기화 계약은 ActiveActive Directory qcow;Directory 도메인에 대한 연결을 생성하기 때문에 ipa-replica-manage connect 명령을 사용하여 IdM 서버에 생성됩니다. ActiveActive Directory HAT;Directory에 대한 암호화된 연결을 설정하려면 IdM에서 Windows CA 인증서를 신뢰해야 합니다.

1. *루트 **CA**(인증 기관) 인증서를 **IdM** 서버에 복사합니다.*

   a. ***ActiveActive Directory {{;Directory CA** 인증서가 자체 서명된 경우:*

      i. ***Windows** 서버에서 **ActiveActive Directory QCOW;Directory CA** 인증서를 내보냅니다.*

         A. ***Super** 키**+R** 조합을 눌러 실행 대화 상자를 엽니다.*

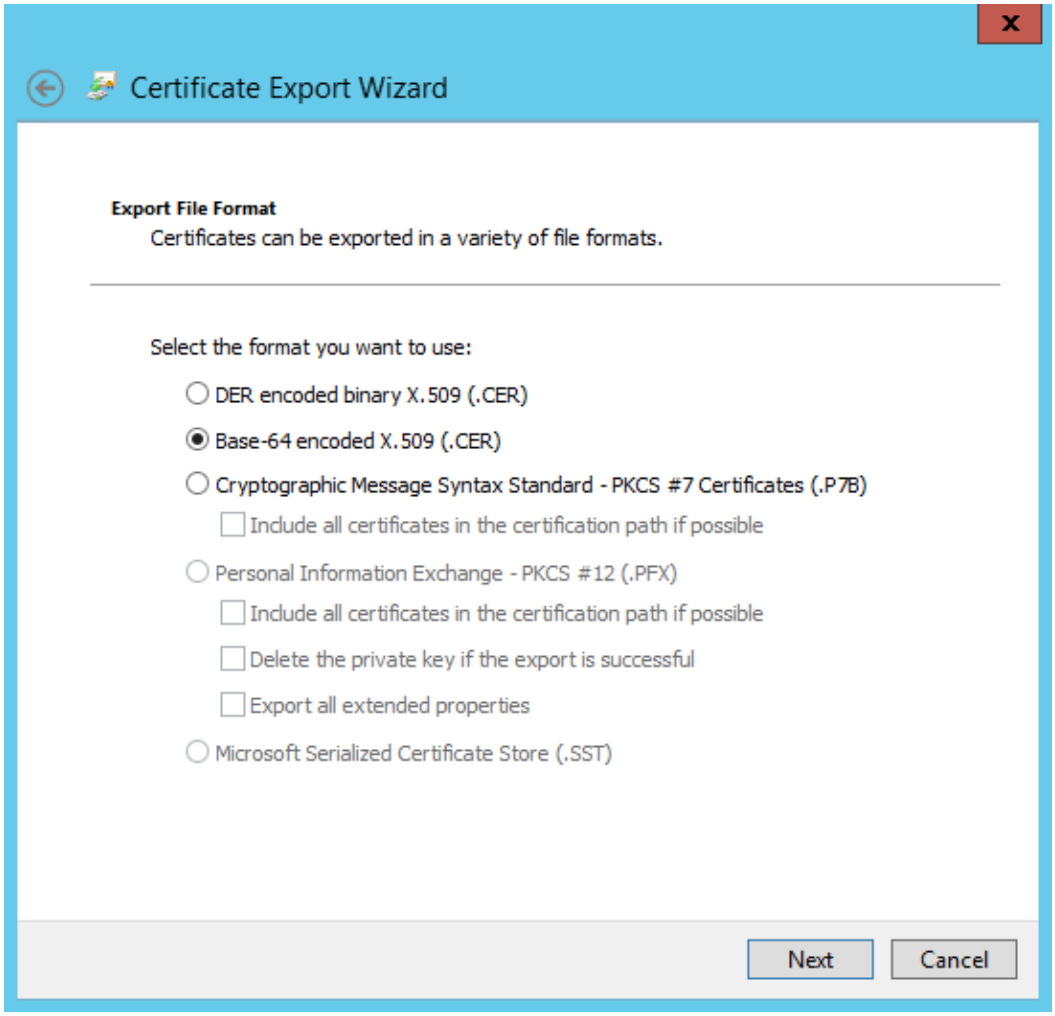
         B. ***certsrv.msc** 를 입력하고 **OK** 를 클릭합니다.*

         C. *로컬 인증 기관의 이름을 마우스 오른쪽 버튼으로 클릭하고 **Properties** 를 선택합니다.*

         D. *일반 탭에서 **CA** 인증서 필드에서 내보낼 인증서를 선택하고 **View Certificate** 를 클릭합니다.*

         E. *세부 정보 탭에서 파일 복사를 클릭하여 인증서 내보내기 마법사 를 시작합니다.*

         F. *다음을 클릭한 다음 **Base-64**로 인코딩된 **X.509(.CER)** 를 선택합니다.*



G.

내보낸 파일에 적합한 디렉터리 및 파일 이름을 지정합니다. 다음을 클릭하여 인증서를 내보낸 다음 완료 를 클릭합니다.

H.

*내보낸 인증서를 **IdM** 서버 시스템에 복사합니다.*

b.

***ActiveActive Directorysetup;Directory CA** 인증서가 외부 **CA**에서 서명한 경우:*

i.

***CA** 루트 인증서가 무엇인지 확인하려면 인증서 체인을 표시합니다.*

```
# openssl s_client -connect adserver.example.com:636
CONNECTED(00000003)
depth=1 C = US, O = Demo Company, OU = IT, CN = Demo CA-28
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/O=Demo Company/OU=IT/CN=adserver.example.com
```

```
 i:/C=US/O=Demo Company/OU=IT/CN=Demo CA-1
1 s:/C=US/O=Demo Company/OU=IT/CN=Demo CA-1
 i:/C=US/O=Demo Company/OU=IT/CN=Demo Root CA 2
```

*이전 예에서는 **CN=Demo Root CA 2** 에 의해 서명되는 **CN=Demo CA-1** 에 의해 **ActiveActive** 디렉터리의 **CA** 인증서가 서명되었음을 보여줍니다. 즉, **CN=Demo Root CA 2** 는 루트 **CA**입니다.*

ii. ***CA** 인증서를 **IdM** 서버에 복사합니다.*

2. ***IdM** 서버의 기존 **Kerberos** 자격 증명을 제거합니다.*

```
$ kdestroy
```

3. ***ipa-replica-manage** 명령을 사용하여 **Windows** 동기화 계약을 생성합니다. 이를 위해서는 **--winsync** 옵션이 필요합니다. 암호와 사용자 계정이 동기화되는 경우 **--passsync** 옵션도 사용하고 암호 동기화에 사용할 암호를 설정합니다.*

***--binddn** 및**--bindpw** 옵션은 **IdM**이 **ActiveActive Directory HAT;Directory** 서버에 연결하는 데 사용할 **ActiveActive Directory HAT;Directory** 서버에서 시스템 계정의 사용자 이름과 암호를 제공합니다.*

```
$ ipa-replica-manage connect --winsync \
 --binddn cn=administrator,cn=users,dc=example,dc=com \
 --bindpw Windows-secret \
 --passsync secretpwd \
 --cacert /etc/openldap/cacerts/windows.cer \
 adserver.example.com -v
```

- ***--winsync:** 이를 **Windows** 동기화 계약으로 식별합니다.*
- ***--binddn: IdM**은 **ActiveActive Directory HAT;Directory** 계정의 **DN**을 사용하여 원격 디렉터리에 바인딩하고 속성을 동기화합니다.*
- ***--bindpw:** 동기화 계정의 암호입니다.*
- ***--cacert:** 전체 경로 및 파일 이름:*

- *CA가 자체 서명된 경우 ActiveActive Directory QCOW;Directory CA 인증서입니다.*

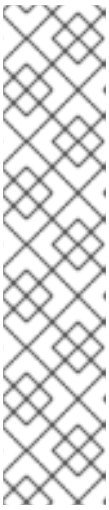
- *ActiveActive Directory HAT;Directory CA가 외부 CA에서 서명한 경우 외부 CA 인증서를 사용합니다.*

- *--win-subtree: 동기화할 사용자가 포함된 Windows 디렉터리 하위 트리의 DN입니다. 기본값은 cn=Users,$SUFFIX 입니다.*

- *AD_server_name: ActiveActive Directory etcdctl;Directory 도메인 컨트롤러의 정규화된 도메인 이름(FQDN)입니다.*

4. *메시지가 표시되면 Directory Manager 암호를 입력합니다.*

5. *선택 사항: 6.6.2절. "암호 동기화 설정" 에서와 같이 암호 동기화를 구성합니다. 암호 동기화 클라이언트가 없으면 사용자 속성이 피어 서버 간에 동기화되지만 암호는 동기화되지 않습니다.*



참고

Password Synchronization 클라이언트는 암호 변경 사항을 캡처한 다음 ActiveActive Directory {{;Directory와 IdM 간에 동기화합니다. 즉, 새 암호 또는 암호 업데이트를 동기화합니다.

IdM 및 ActiveActive Directory}};Directory에서 해시된 양식에 저장된 기존 암호는 암호 동기화 클라이언트를 설치할 때 암호를 해독하거나 동기화할 수 없으므로 기존 암호가 동기화되지 않습니다. 피어 서버 간 동기화를 시작하려면 사용자 암호를 변경해야 합니다.

6.5.2. 사용자 계정 특성 동기화를 위한 동작 변경

동기화 연결이 생성되면 동기화 프로세스에서 동기화 중에 사용자 계정 속성을 처리하는 방법에 대해 정의된 특정 기본 동작이 있습니다. 동작 유형은 잠금 속성을 처리하는 방법이나 다른 DN 형식을 처리하는 방법과 같습니다. 이 동작은 동기화 계약을 편집하여 변경할 수 있습니다.

동기화 계약은 LDAP 서버의 특수 플러그인 항목으로 존재하며 각 특성 동작은 LDAP 특성을 통해 설정됩니다. 동기화 동작을 변경하려면 ldap modify 명령을 사용하여 LDAP 서버 항목을 직접 수정합니다.

*예를 들어 계정 잠금 기능은 기본적으로 **IdM**과 **ActiveActive Directory Long;Directory** 간에 동기화되지만 **ipaWinSyncAcctDisable** 속성을 편집하여 비활성화할 수 있습니다. (이를 변경하면 **ActiveActive Directory advised;Directory**에서 계정이 비활성화 된 경우, **IdM**에서 계속 활성 상태이며 그 반대의 경우도 마찬가지입니다.)*

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -w password

dn: cn=ipa-winsync,cn=plugins,cn=config
changetype: modify
replace: ipaWinSyncAcctDisable
ipaWinSyncAcctDisable: none

modifying entry "cn=ipa-winsync,cn=plugins,cn=config"
```

다음은 동기화 설정 속성의 개요입니다.

일반 사용자 계정 매개변수

- ***ipaWinSyncNewEntryFilter:** 새 사용자 항목에 추가할 오브젝트 클래스 목록이 포함된 항목을 찾는 데 사용할 검색 필터를 설정합니다.*

  *기본값: **(cn=ipaConfig)***

- ***ipaWinSyncNewUserOCAttr:** 새 사용자 항목에 추가할 오브젝트 클래스 목록을 실제로 포함하는 구성 항목의 속성을 설정합니다.*

  *기본값: **ipauserobjectclasses***

- ***ipaWinSyncHomeDirAttr: POSIX** 홈 디렉터리의 기본 위치가 포함된 항목의 속성을 식별합니다.*

  *기본값: **ipaHomesRootDir***

- ***ipaWinSyncUserAttr: ActiveActive Directory HAT;Directory** 도메인의 동기화를 수행할 때 **ActiveActive Directory 6.7;Directory** 사용자에게 추가할 특정 값이 있는 추가 특성을 설정합니다. 속성이 다중값인 경우 여러 번 설정할 수 있으며 동기화 프로세스는 모든 값을 항목에 추가합니다.*

예: ipaWinSyncUserAttr: attributeName attributeValue

참고

*항목에 해당 특성이 없는 경우에만 특성 값을 설정합니다. 속성이 있는 경우 **ActiveActive Directory illustrated;Directory** 항목이 동기화될 때 항목의 값이 사용됩니다.*

- *ipaWinSyncForceSync: 기존 **AD** 사용자와 일치하는 기존 **IdM** 사용자를 동기화해야 하는지 여부를 설정합니다. **true** 로 설정하면 이러한 **IdM** 사용자가 동기화되도록 자동으로 편집됩니다.*

  *가능한 값: **true | false***

  *anan IdMprovide;IdM 사용자 계정에 **uid** 매개변수가 있는 경우 기존 **ActiveActive Directory qcow;Directory** 사용자의 **sAMAccountName** 과 동일한 **uid** 매개 변수가 있는 경우 해당 계정은 기본적으로 동기화 되지 않습니다. 이 속성은 동기화 서비스에 **ntUser** 및 **ntUserDomainId** 를 **IdM** 사용자 항목에 자동으로 추가하여 동기화할 수 있도록 지시합니다.*

사용자 계정 잠금 매개변수

- *ipaWinSyncAcctDisable: 계정 잠금 속성을 동기화하는 방법을 설정합니다. 적용되는 계정 잠금 설정을 제어할 수 있습니다. 예를 들어 **to_ad** 는 **IdM**에 계정 잠금 해제 속성이 설정되어 있을 때 해당 값은 **ActiveActive Directory}};Directory**에 대해 동기화되고 로컬 **ActiveActive Directorytekton;Directory** 값을 덮어씁니다. 기본적으로 계정 잠금 속성은 두 도메인에서 동기화됩니다.*

  *가능한 값: 둘 다 (기본값), **to_ad,to_ds,none***

- *ipaWinSyncInactivatedFilter: 사용자를 비활성화(비활성화)하는 데 사용되는 그룹의 **DN** 을 찾는 데 사용할 검색 필터를 설정합니다. 대부분의 배포에서는 이 값을 변경할 필요가 없습니다.*

  *기본값: **(&(cn=inactivated)(objectclass=groupOfNames)***

그룹 매개 변수

-

ipaWinSyncDefaultGroupAttr: 새 사용자 계정의 속성을 참조하도록 설정하여 사용자의 기본 그룹을 확인합니다. 그런 다음 항목의 그룹 이름이 사용자 계정의 gidNumber 를 찾는 데 사용됩니다.

기본값: ipaDefaultPrimaryGroup

- *ipaWinSyncDefaultGroupFilter: 새 사용자 계정의 속성을 참조하도록 설정하여 사용자의 기본 그룹을 확인합니다. 그런 다음 항목의 그룹 이름이 사용자 계정의 gidNumber 를 찾는 데 사용됩니다.*

  기본값: ipaDefaultPrimaryGroup

영역 매개 변수

- *ipaWinSyncRealmAttr: realm 항목의 영역 이름을 포함하는 속성을 설정합니다.*

  기본값: cn

- *ipaWinSyncRealmFilter: IdM 영역 이름이 포함된 항목을 찾는 데 사용할 검색 필터를 설정합니다.*

  기본값: (objectclass=krbRealmContainer)

6.5.3. 동기화된 Windows 하위 트리 변경

동기화 계약을 생성하면 동기화된 사용자 데이터베이스로 사용할 두 하위 트리가 자동으로 설정됩니다. IdM에서 기본값은 cn=users,cn=accounts,$SUFFIX, ActiveActive Directory HAT;Directory의 경우 기본값은 CN=Users,$SUFFIX 입니다.

--win-subtree 옵션을 사용하여 동기화 계약을 생성할 때 ActiveActive Directory QCOW;Directory 하위 트리의 값을 기본값이 아닌 값으로 설정할 수 있습니다. 계약이 생성되면 ldapmodify 명령을 사용하여 동기화 계약 항목의 nsds7WindowsReplicaSubtree 값을 편집하여 ActiveActive Directory qcow;Directory 하위 트리를 변경할 수 있습니다.

1. *ldapsearch 를 사용하여 동기화 계약의 이름을 가져옵니다. 이 검색은 전체 항목 대신 dn 및 nsds7WindowsReplicaSubtree 속성에 대한 값만 반환합니다.*

```
[jsmith@ipaserver ~]$ ldapsearch -xLLL -D "cn=directory manager" -w password -p 389 -h
ipaserver.example.com -b cn=config objectclass=nsdswindowsreplicationagreement dn
nsds7WindowsReplicaSubtree

dn:
cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
nsds7WindowsReplicaSubtree: cn=users,dc=example,dc=com

... 8< ...
```

2. *동기화 계약 수정*

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -W -p 389 -h
ipaserver.example.com <<EOF
 dn:
cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
 changetype: modify
 replace: nsds7WindowsReplicaSubtree
 nsds7WindowsReplicaSubtree: cn=alternateusers,dc=example,dc=com
 EOF

 modifying entry
"cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config"
```

새 하위 트리 설정은 즉시 적용됩니다. 동기화 작업이 현재 실행 중인 경우 현재 작업이 완료되는 즉시 적용됩니다.

6.5.4. Uni-directional Synchronization 구성

*기본적으로 모든 수정 및 삭제는 양방향입니다. **ActiveActive Directory qcow;Directory**의 변경 사항은 **IdentityIdentity Management Long;Management**와 동기화되며 **IdentityIdentity Management (8;Management)**의 항목 변경은 **ActiveActive Directory qcow;Directory**로 동기화됩니다. 이는 기본적으로 **ActiveActive Directory HAT;Directory** 및 **IdentityIdentity ManagementProvision;Management**는 동기화의 피어이고 데이터 마스터 모두와 동일한 쿼리인 **equitable**의 다중 마스터 관계입니다.*

*그러나 하나의 도메인은 데이터 마스터여야 하고 다른 도메인은 업데이트를 수락해야 하는 일부 데이터 구조 또는 **IT** 설계가 있을 수 있습니다. 이렇게 하면 다중 마스터 관계(피어 서버가 동일한 경우)의 동기화 관계가 마스터 소비자 관계로 변경됩니다.*

*이 작업은 동기화 계약에 **oneWaySync** 매개변수를 설정하여 수행됩니다. 가능한 값은 **fromWindows (Active Directory etcdctl;Directory**에서 **Identity Management {{;Management** 동기화*

*에 대한) 및 **toWindows (IdentityIdentity Management 9.0;Management**에서 **ActiveActive Directorytekton;Directory** 동기화에 대한)입니다.*

*예를 들어 **ActiveActive Directory HAT;Directory**에서 **IdentityIdentity Management {{;Management**에 대한 변경 사항을 동기화하려면 다음을 수행합니다.*

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -w password -p 389 -h
ipaserver.example.com

dn: cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
changetype: modify
add: oneWaySync
oneWaySync: fromWindows
```

중요

*리디렉션 동기화를 사용하도록 설정하면 동기화되지 않은 서버에서 자동으로 변경되지 않으며 동기화 업데이트 간의 동기화 피어 간 불일치가 발생할 수 있습니다. 예를 들어, 단방향 동기화는 **ActiveActive Directory Long;Directory**에서 **IdentityIdentity Management HAT;Management**로 이동하도록 구성되어 있으므로 **ActiveActive Directory QCOW;Directory**는 (중요한) 데이터 마스터입니다. **IdentityIdentity Management 6.7;Management**에서 항목이 수정되거나 삭제된 경우 **IdentityIdentity Management qcow;Management** 정보는 서로 다른 경우 정보와 변경 사항은 **ActiveActive Directory HAT;Directory**로 전달되지 않습니다. 다음 동기화 업데이트 중에 **DirectoryDirectory Server Long;Server**에서 편집 내용이 다시 추가되고 삭제된 항목이 다시 추가됩니다.*

6.5.5. 동기화 계약 삭제

***IdM** 및 **ActiveActive Directory qcow;Directory** 서버의 연결을 끊는 동기화를 삭제하여 동기화를 중지할 수 있습니다. 동기화 계약 생성과 반대로 동기화 계약을 삭제하면 **ipa-replica-manage disconnect** 명령을 사용한 다음 **ActiveActive Directory qcow;Directory** 서버의 호스트 이름을 사용합니다.*

1. *동기화 계약을 삭제합니다.*

```
# ipa-replica-manage disconnect adserver.ad.example.com
```

2. ***IdM** 디렉터리 인증서 데이터베이스의 인증서를 나열합니다.*

```
# certutil -L -d /etc/dirsrv/slapd-IDM-EXAMPLE-COM/
Certificate Nickname                    Trust Attributes
                                        SSL,S/MIME,JAR/XPI
```

```
IDM.EXAMPLE.COM IPA CA                  CT,C,C
CN=adserver,DC=ad,DC=example,DC=com     C,,
Server-Cert                             u,u,u
```

3. **IdM** 서버 데이터베이스에서 **ActiveActive Directory {{;Directory CA** 인증서를 삭제합니다.

```
# certutil -D -d /etc/dirsrv/slapd-IDM-EXAMPLE-COM/ -n
"CN=adserver,DC=ad,DC=example,DC=com"
```

6.5.6. WinSync 계약 오류

ActiveActive Directory qcow;Directory 서버에 연결할 수 없기 때문에 동기화 계약이 실패합니다.

가장 일반적인 동기화 계약 실패 중 하나는 **IdM** 서버가 **ActiveActive Directory qcow;Directory** 서버에 연결할 수 없다는 것입니다.

```
"Update failed! Status: [81  - LDAP error: Can't contact LDAP server]
```

이 문제는 계약이 생성될 때 **ActiveActive Directory HAT;Directory CA** 인증서가 지정 된 경우 발생할 수 있습니다. 그러면 가져온 **CA**라는 이름으로 **IdM LDAP** 데이터베이스(**/etc/dirsrv/slapd-DOMAIN/** 디렉터리에 있음)에 중복 인증서가 생성됩니다. **certutil:**을 사용하여 확인할 수 있습니다.

```
$ certutil -L -d /etc/dirsrv/slapd-DOMAIN/

Certificate Nickname                        Trust Attributes
SSL,S/MIME,JAR/XPI

CA certificate                             CTu,u,Cu
Imported CA                                 CT,,C
Server-Cert                                u,u,u
Imported CA                                 CT,,C
```

이 문제를 해결하려면 인증서 데이터베이스에서 **CA** 인증서를 제거하십시오.

```
# certutil -d /etc/dirsrv/slapd-DOMAIN-NAME -D -n "Imported CA"
```

항목이 존재하지 않기 때문에 암호가 동기화되지 않음을 나타내는 오류가 있습니다.

사용자 데이터베이스의 일부 항목에 대해 항목이 이미 있으므로 암호가 재설정되지 않는다는 정보 오류 메시지가 있을 수 있습니다.

> *"Windows PassSync entry exists, not resetting password"*

*이는 오류가 아닙니다. 이 메시지는 예외 사용자 암호 동기화 사용자가 변경되지 않을 때 발생합니다. 암호 동기화 사용자는 서비스에서 **IdM**의 암호를 변경하는 데 사용하는 운영 사용자입니다.*

6.6. 암호 동기화 관리

*사용자 항목 동기화는 동기화 계약으로 구성됩니다. 그러나 **ActiveActive Directory QCOW;Directory** 및 **IdentityIdentity Management Long;Management**의 암호는 일반 사용자 동기화 프로세스의 일부가 아닙니다. 사용자 계정이 생성되거나 암호가 변경되므로 별도의 클라이언트를 **ActiveActive Directory qcow;Directory** 서버에 설치하여 암호를 변경한 다음 동기화된 업데이트를 사용하여 암호 정보를 전달해야 합니다.*

참고

***Password Synchronization** 클라이언트는 암호 변경 사항을 캡처한 다음 **ActiveActive Directory {{;Directory**와 **IdM** 간에 동기화합니다. 즉, 새 암호 또는 암호 업데이트를 동기화합니다.*

***IdM** 및 **ActiveActive Directory}};Directory**에서 해시된 양식에 저장된 기존 암호는 암호 동기화 클라이언트를 설치할 때 암호를 해독하거나 동기화할 수 없으므로 기존 암호가 동기화되지 않습니다. 피어 서버 간 동기화를 시작하려면 사용자 암호를 변경해야 합니다.*

6.6.1. 암호 동기화를 위한 Windows Server 설정

암호를 동기화하려면 다음과 같은 작업이 필요합니다.

- ***ActiveActive Directory HAT;Directory**가 **SSL**에서 실행 중이어야 합니다.*

참고

Microsoft 인증서 시스템을 엔터프라이즈 루트 모드로 설치합니다. 그러면 ActiveActive Directory explain;Directory가 자동으로 등록하여 SSL 서버 인증서를 검색합니다.

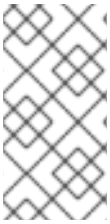
- Password Synchronization Service는 각 ActiveActive Directory 6.7;Directory 도메인 컨트롤러에 설치되어 있어야 합니다. Windows의 암호를 동기화하려면 PassSync 서비스는 보안 연결을 통해 IdM과 동기화하기 위해 암호화되지 않은 암호에 액세스해야 합니다. 사용자는 모든 도메인 컨트롤러에서 암호를 변경할 수 있으므로 각 도메인 컨트롤러에서 PassSync 서비스를 설치해야 합니다.

- 암호 정책은 IdM 및 ActiveActive Directory Long;Directory 측과 유사하게 설정해야 합니다. 동기화 대상에서 업데이트된 암호를 수신하면 소스의 정책과 일치하도록만 검증되었습니다. 동기화 대상에서 다시 검증되지 않습니다.

ActiveActive Directory qcow;Directory 암호 복잡성 정책이 활성화되어 있는지 확인하려면 ActiveActive Directory qcow;Directory 도메인 컨트롤러에서 다음을 실행합니다.

```
> dsquery * -scope base -attr pwdProperties
  pwdProperties
  1
```

pwdProperties 속성 값이 1 로 설정되면 도메인에 대한 암호 복잡성 정책이 활성화됩니다.



참고

그룹 정책이 조직 단위(ou)에 대한 암호 변경 사항을 정의하는지 확실하지 않은 경우 그룹 정책 관리자에게 문의하십시오.

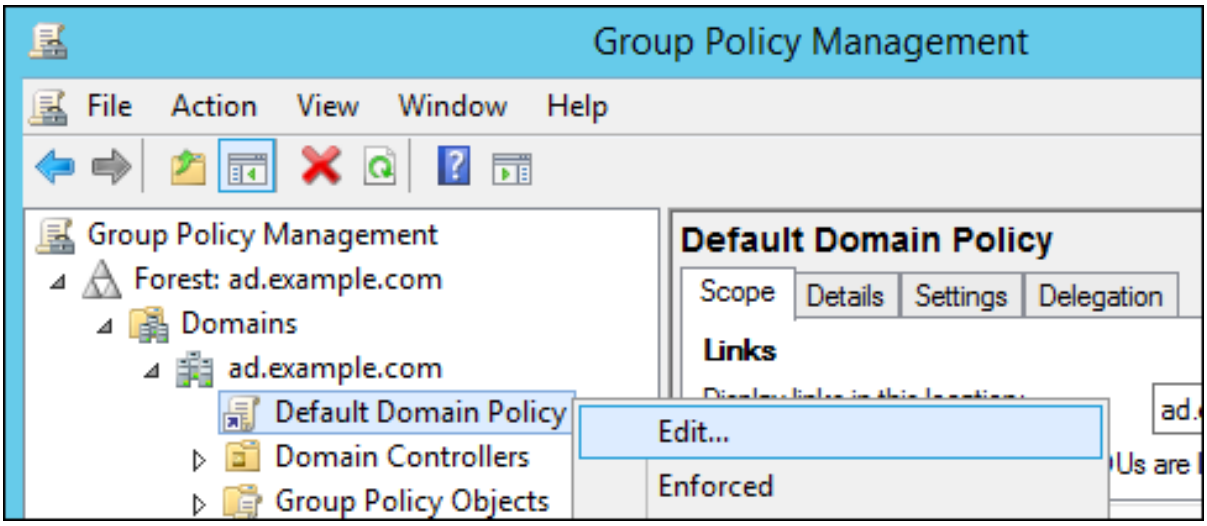
전체 도메인에 대해 ActiveActive Directory Long;Directory 암호 복잡성 설정을 활성화하려면 다음을 수행합니다.

1. 명령줄에서 gpmc.msc 를 실행합니다.

2. *그룹 정책 관리 을 선택합니다.*

3. ***Open Forest: ad.example.com → 도메인 → ad.example.com.***

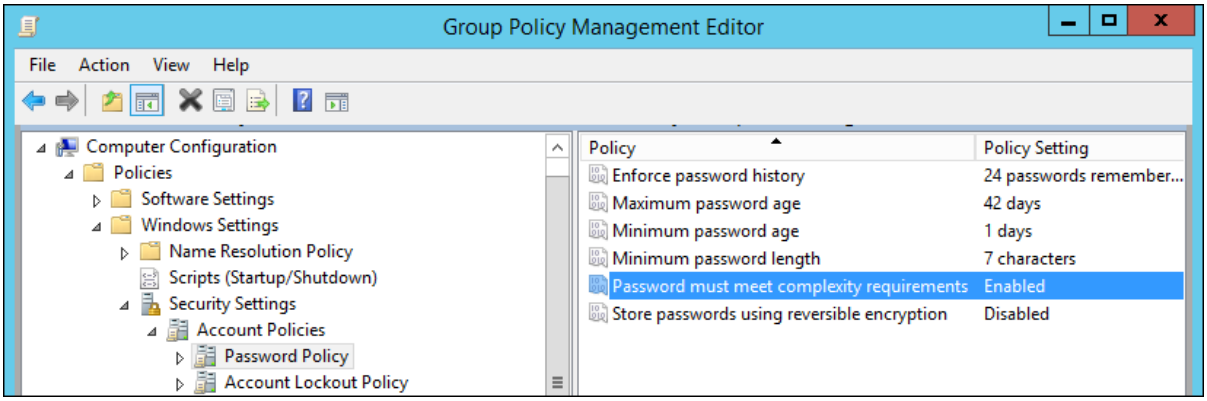
4. ***Default Domain Policy** (기본 도메인 정책) 항목을 마우스 오른쪽 버튼으로 클릭하고 **Edit** 를 선택합니다.*



5. *그룹 정책 관리 편집기 가 자동으로 열립니다.*

6. *컴퓨터 구성 → 정책 → **Windows**설정보안 → 계정정책 정책을 엽니다.*

7. *암호가 복잡성 요구 사항을 충족하고 비용을 절감해야 합니다.*



6.6.2. 암호 동기화 설정

Windows 암호를 동기화하려면 ActiveActive Directory qcow;Directory 도메인의 모든 도메인 컨트롤러에 Password Synchronization Service를 설치합니다.

1. *RedHat-PassSync-*.msi 파일을 Active Directory 도메인 컨트롤러로 다운로드합니다.*

   a. *고객 포털에 로그인합니다.*

   b. *페이지 상단에서 다운로드를 클릭합니다.*

   c. *제품 목록에서 Red Hat Enterprise Linux QCOW;Hat EnterpriseRed Hat Enterprise Linux Kernel;Linux 를 선택합니다.*

   d. *최신 Red Hat Enterprise Linux 기준 Red Hat Enterprise Linux HAT;Hat Enterprise Linux Red Hat Enterprise Linux 6 또는 Red Hat Enterprise Linuxrich;Hat EnterpriseRed Hat Enterprise Linux HAT;Linux 7 및 아키텍처를 선택합니다.*

   e. *지금 다운로드 버튼을 클릭하여 ActiveActive Directory qcow;Directory 도메인 컨트롤러의 아키텍처에 대한 WinSync 설치 프로그램을 다운로드합니다.*

2. *ProfileBundle 파일을 두 번 클릭하여 설치합니다.*

3. *암호 동기화 설정 창이 표시됩니다. 다음을 눌러 설치를 시작합니다.*

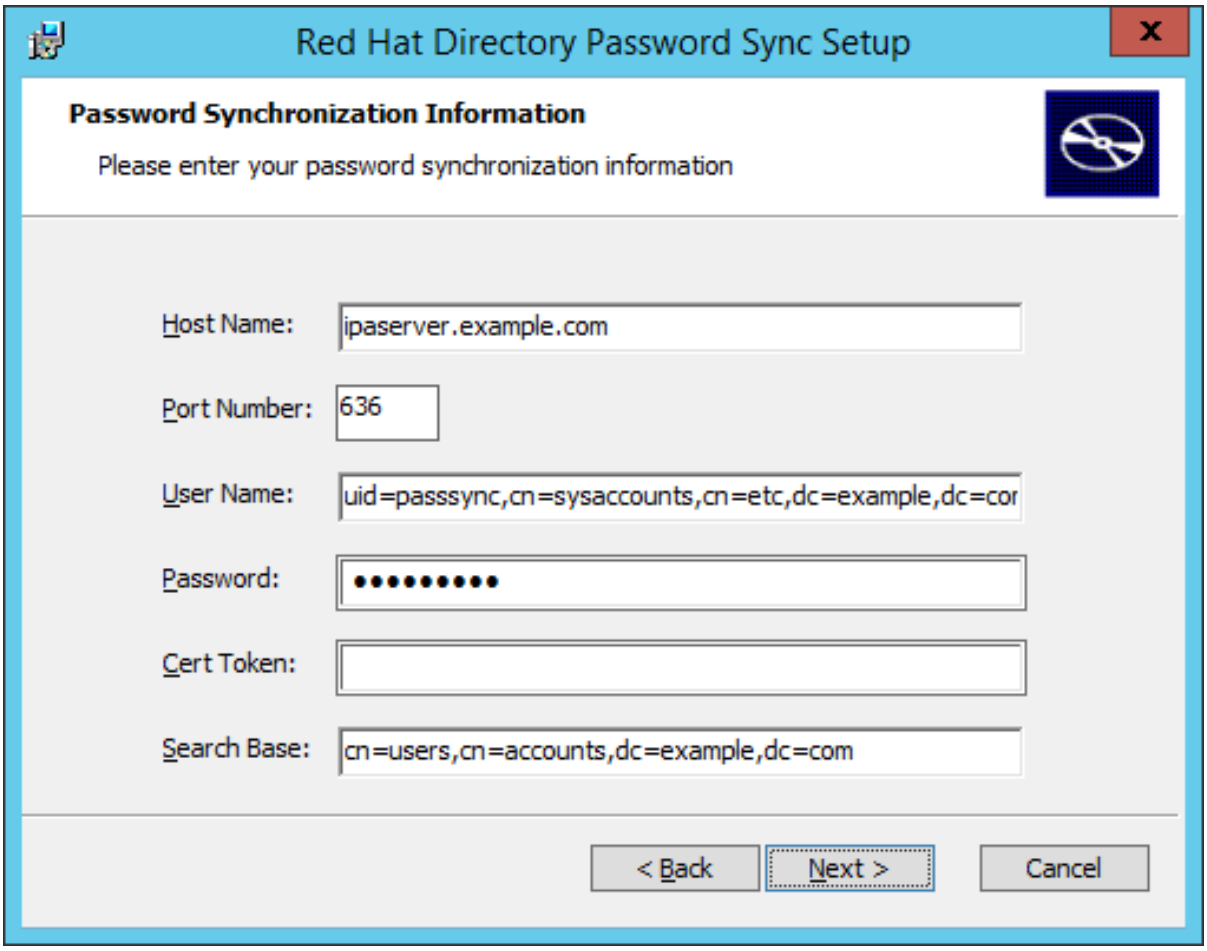
4. *정보를 입력하여 IdM 서버에 대한 연결을 설정합니다.*

   - *호스트 이름 및 보안 포트 번호를 포함한 IdM 서버 연결 정보입니다.*
   - *ActiveActive Directory qcow;Directory에서 IdM 시스템에 연결하는 데 사용하는 시스템 사용자의 사용자 이름입니다. 이 계정은 IdM 서버에 동기화가 구성된 경우 자동으로 구성됩니다. 기본 계정은 uid=passsync,cn=sysaccounts,cn=etc,dc=example,dc=com 입니다.*

- *동기화 계약이 생성된 경우 **--passsync** 옵션에 설정된 암호입니다.*

- *IdM 서버에서 **people** 하위 트리의 검색 기반입니다. **ActiveActive Directory {{;Directory** 서버는 **ldapsearch** 또는 복제 작업과 유사한 **IdM** 서버에 연결하므로 사용자 계정을 찾기 위해 **IdM** 하위 트리의 위치를 알아야 합니다. 사용자 하위 트리는 **cn=users,cn=accounts,dc=example,dc=com** 입니다.*

- *인증서 토큰은 현재 사용되지 않으므로 필드를 비워야 합니다.*



***Next** 를 클릭한 다음 **Finish to install Password Synchronization**을 클릭합니다.*

5. *IdM 서버의 **CA** 인증서를 **PassSync** 인증서 저장소로 가져옵니다.*

   a. *http://ipa.example.com/ipa/config/ca.crt 에서 **IdM** 서버의 **CA** 인증서를 다운로드합니다.*

b.

IdM CA 인증서를 ActiveActive Directory etcdctl;Directory 서버에 복사합니다.

c.

암호 동기화 데이터베이스에 IdM CA 인증서를 설치합니다. 예를 들면 다음과 같습니다.

```
cd "C:\Program Files\Red Hat Directory Password Synchronization"

certutil.exe -d . -A -n "IPASERVER.EXAMPLE.COM IPA CA" -t CT,, -a -i ipaca.crt
```

6.

Windows 머신을 재부팅하여 암호 동기화를 시작합니다.

참고

Windows 머신을 재부팅해야 합니다. 재부팅하지 않으면 PasswordHook.dll 이 활성화되지 않고 암호 동기화가 작동하지 않습니다.

7.

기존 계정의 암호를 동기화해야 하는 경우 사용자 암호를 재설정합니다.

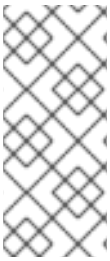
참고

Password Synchronization 클라이언트는 암호 변경 사항을 캡처한 다음 ActiveActive Directory {{;Directory와 IdM 간에 동기화합니다. 즉, 새 암호 또는 암호 업데이트를 동기화합니다.

IdM 및 ActiveActive Directory}};Directory에서 해시된 양식에 저장된 기존 암호는 암호 동기화 클라이언트를 설치할 때 암호를 해독하거나 동기화할 수 없으므로 기존 암호가 동기화되지 않습니다. 피어 서버 간 동기화를 시작하려면 사용자 암호를 변경해야 합니다.

Password Synchronization 애플리케이션이 설치될 때 발생한 암호를 동기화하려는 첫 번째 시도는 DirectoryDirectory Serverprovide;Server 및 Active Directory 동기화 피어 간의 SSL 연결로 인해 항상 실패합니다. 인증서 및 키 데이터베이스를 생성하는 도구는 .msi 와 함께 설치됩니다.

암호 동기화 클라이언트는 IdM admin 그룹의 암호를 동기화할 수 없습니다. 이는 암호 동기화 에이전트 또는 하위 수준 관리자의 암호를 변경하여 최상위 관리자의 암호를 변경하는 것을 방지하기 위한 동작입니다.



참고

*암호는 암호 정책과 일치하도록 동기화 소스에서만 유효성을 검사합니다. **ActiveActive Directory QCOW;Directory** 암호 복잡성 정책을 확인하고 활성화하려면 **6.6.1절. "암호 동기화를 위한 Windows Server 설정"** 을 참조하십시오.*

---

[2]

***cn** 은 다른 동기화된 특성과 다르게 취급됩니다. **IdentityIdentity Management}};Management**에서 **ActiveActive Directory HAT;Directory**에 동기화할 때 직접 매핑(**cn** 에 **cn** ~ **cn**)합니다. **ActiveActive Directory QCOW;Directory**에서 **IdentityIdentity Management(IdentityIdentity Management)**에 동기화되는 경우 **cn** 은 **Windows**의 **name** 속성에서 **IdentityIdentity Managementtekton;Management**의 **cn** 속성에 매핑됩니다.*

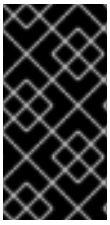
7장. 동기화에서 신뢰로 기존 환경 마이그레이션

동기화 및 신뢰 는 간접 통합에 대한 두 가지 가능한 접근 방식입니다. 동기화는 일반적으로 권장되지 않으며, Red Hat은 AD(Active Directory) 신뢰를 기반으로 한 접근 방식을 대신 사용할 것을 권장합니다. 자세한 내용은 1.3절. “간접 통합” 을 참조하십시오.

이 장에서는 기존 동기화 기반 설정을 AD 신뢰로 마이그레이션하는 방법을 설명합니다. IdM에서 다음 마이그레이션 옵션을 사용할 수 있습니다.

- 7.1절. “ipa-winsync-migrate를 사용하여 자동으로 동기화에서 신뢰로 마이그레이션”
- 7.2절. “동기화에서 ID 뷰를 사용하여 수동으로 신뢰로 마이그레이션”

7.1. IPA-WINSYNC-MIGRATE를 사용하여 자동으로 동기화에서 신뢰로 마이그레이션



중요

ipa-winsync-migrate 유틸리티는 Red Hat Enterprise Linux 7.2 이상을 실행하는 시스템에서만 사용할 수 있습니다.

7.1.1. ipa-winsync-migrate Works를 사용한 마이그레이션 방법

ipa-winsync-migrate 유틸리티는 AD forest에서 동기화된 모든 사용자를 마이그레이션하고 Winsync 환경의 기존 구성을 유지하면서 AD 신뢰로 전송합니다. Winsync 계약에 의해 생성된 각 AD 사용자의 경우 ipa-winsync-migrate 는 기본 신뢰 보기에 ID 재정의를 만듭니다(8.1절. “Active Directory 기본 신뢰 보기”참조).

마이그레이션이 완료된 후 다음을 수행합니다.

- AD 사용자의 ID 재정의에는 Winsync의 원래 항목에서 복사한 다음과 같은 속성이 있습니다.
  - 로그인 이름(uid)

- *UID 번호(uidnumber)*
- *GID 번호(gidnumber)*
- *홈 디렉토리(홈 디렉토리)*
- *GECOS 항목 (gecos)*

- *AD 트러스트의 사용자 계정은 IdM의 원래 구성을 유지합니다. 여기에는 다음이 포함됩니다.*
  - *POSIX 속성*
  - *사용자 그룹*
  - *역할 기반 액세스 제어 규칙*
  - *호스트 기반 액세스 제어 규칙*
  - *SELinux 멤버십*
  - *sudo 규칙*

- *새 AD 사용자가 외부 IdM 그룹의 멤버로 추가됩니다.*

- *원본 Winsync 복제 계약, 동기화된 원본 사용자 계정 및 사용자 계정의 모든 로컬 복사본이 제거됩니다.*

7.1.2. ipa-winsync-migrate를 사용하여 마이그레이션을 마이그레이션하는 방법

시작하기 전에:

- ipa-backup 유틸리티를 사용하여 IdM 설정을 백업합니다. Linux 도메인 ID, 인증 및 정책 가이드의 ID 관리 백업 및 복원을 참조하십시오.

  이유: 마이그레이션은 IdM 구성 및 많은 사용자 계정의 중요한 부분에 영향을 미칩니다. 백업을 만들면 필요한 경우 원래 설정을 복원할 수 있습니다.

마이그레이션하려면 다음을 수행합니다.

1. 동기화된 도메인을 사용하여 신뢰를 만듭니다. 5장. ActiveActive Directory Long;Directory and Identity Identity Management {{;Management를 사용하여 Cross-forest Trusts 생성을 참조하십시오.

2. ipa-winsync-migrate 를 실행하고 AD 도메인 컨트롤러의 호스트 이름과 AD 영역을 지정합니다.

```
# ipa-winsync-migrate --realm example.com --server ad.example.com
```

   ipa-winsync-migrate 에서 생성된 덮어쓰기에서 충돌이 발생하면 충돌이 발생하지만 마이그레이션이 계속됩니다.

3. AD 서버에서 Password Sync 서비스를 설치 제거합니다. 이를 통해 AD 도메인 컨트롤러에서 동기화 계약을 제거합니다.

유틸리티에 대한 자세한 내용은 ipa-winsync-migrate(1) 도움말 페이지를 참조하십시오.

7.2. 동기화에서 ID 뷰를 사용하여 수동으로 신뢰로 마이그레이션

ID 뷰를 사용하여 AD 사용자에게 이전에 생성한 POSIX 속성을 수동으로 변경할 수 있습니다.

1. 동기화된 원본 사용자 또는 그룹 항목의 백업을 만듭니다.

2.

동기화된 도메인을 사용하여 신뢰를 만듭니다. 신뢰 생성에 대한 자세한 내용은 5장. ActiveActive Directory Long;Directory and Identity Identity Management {{;Management를 사용하여 Cross-forest Trusts 생성 을 참조하십시오.

3. 동기화된 모든 사용자 또는 그룹의 경우 다음 중 하나를 수행하여 IdM에서 생성한 UID 및 GID를 유지합니다.

   - 특정 호스트에 적용되는 ID 뷰를 개별적으로 생성하고 보기에 사용자 ID 재정의를 추가합니다.
   - Default Trust View에서 사용자 ID 재정의를 생성합니다.

   자세한 내용은 다른 호스트에서 사용자 계정의 다양한 속성 값 정의를 참조하십시오.

   참고

   IdM 사용자만 ID 보기를 관리할 수 있습니다. AD 사용자는 할 수 없습니다.

4. 동기화된 원본 사용자 또는 그룹 항목을 삭제합니다.

Active Directory 환경에서 ID 뷰를 사용하는 방법에 대한 자세한 내용은 8장. Active Directory 환경에서 ID 뷰 사용 을 참조하십시오.

8장. ACTIVE DIRECTORY 환경에서 ID 뷰 사용

ID 보기를 사용하면 POSIX 사용자 또는 그룹 속성의 새 값을 지정하고 새 값을 적용할 클라이언트 호스트 또는 호스트를 정의할 수 있습니다.

IdM(Identity Management) 이외의 통합 시스템은 IdM에서 사용되는 알고리즘과 다른 알고리즘을 기반으로 UID 및 GID 값을 생성하는 경우가 있습니다. IdM에서 사용된 값과 일치하도록 이전에 생성한 값을 재정의하면 다른 통합 시스템의 멤버로 사용된 클라이언트를 IdM과 완전히 통합할 수 있습니다.

참고

이 장에서는 AD(Active Directory)와 관련된 ID 뷰 기능에 대해서만 설명합니다. ID 뷰에 대한 일반적인 내용은 Linux 도메인 ID, 인증 및 정책 가이드 를 참조하십시오.

다음과 같은 목적으로 AD 환경에서 ID 보기를 사용할 수 있습니다.

POSIX 속성 또는 SSH 로그인 세부 정보와 같은 AD 사용자 속성 덮어쓰기

자세한 내용은 8.3절. “ID 뷰를 사용하여 AD 사용자 속성 정의” 을 참조하십시오.

동기화 기반에서 신뢰 기반 통합으로 마이그레이션

자세한 내용은 7.2절. “동기화에서 ID 뷰를 사용하여 수동으로 신뢰로 마이그레이션” 을 참조하십시오.

IdM 사용자 속성의 호스트별 그룹 덮어쓰기 수행

자세한 내용은 8.4절. “NIS 도메인을 IdM으로 마이그레이션” 을 참조하십시오.

8.1. ACTIVE DIRECTORY 기본 신뢰 보기

8.1.1. 기본 신뢰 보기

기본 신뢰 보기는 항상 신뢰할 수 있는 설정의 AD 사용자 및 그룹에 적용되는 기본 ID 뷰입니다. ipa-adtrust-install 을 사용하여 신뢰를 설정하면 자동으로 생성되며 삭제할 수 없습니다.

Default Trust View를 사용하면 AD 사용자 및 그룹에 대한 사용자 지정 POSIX 속성을 정의하여 AD

에 정의된 값을 재정의할 수 있습니다.

표 8.1. 기본 신뢰 보기 적용

	AD의 값	기본 신뢰 보기		결과
login	ad_user	ad_user	→	ad_user
UID	111	222	→	222
GID	111	(값 없음)	→	111

참고

***Default Trust View**는 **IdM** 사용자 및 그룹이 아닌 **AD** 사용자 및 그룹에 대한 덮어쓰기만 허용합니다. **IdM** 서버 및 클라이언트에 적용되므로 **ActiveActive Directory qcow;Directory** 사용자 및 그룹에 대한 덮어쓰기만 제공해야 합니다.*

8.1.2. 기타 ID 뷰를 사용하여 기본 신뢰 보기 덮어쓰기

*호스트에 적용되는 다른 **ID** 뷰가 **Default Trust View**의 속성 값을 재정의하는 경우 **IdM**은 **Default Trust View** 상단에 있는 호스트별 **ID** 보기의 값을 적용합니다.*

- *호스트별 **ID** 보기에 속성이 정의된 경우 **IdM**은 이 보기의 값을 적용합니다.*
- *호스트별 **ID** 보기에 속성이 정의되지 않은 경우 **IdM**은 **Default Trust View**의 값을 적용합니다.*

*기본 신뢰 보기는 항상 **IdM** 서버 및 복제본과 **AD** 사용자 및 그룹에 적용됩니다. 다른 **ID** 보기를 할당할 수 없습니다. 항상 기본 신뢰 보기의 값을 적용합니다.*

표 8.2. 기본 신뢰 보기 상단에 호스트 관련 ID 보기 적용

	AD의 값	기본 신뢰 보기	host-Specific View		결과
login	ad_user	ad_user	(값 없음)	→	ad_user
UID	111	222	333	→	333
GID	111	(값 없음)	333	→	333

8.1.3. 클라이언트 버전을 기반으로 하는 클라이언트 재정의

IdM 마스터는 IdM 클라이언트가 SSSD를 사용하거나 스키마 호환성 트리 요청을 사용하는 방법에 관계없이 Default Trust View의 ID 재정의를 항상 적용합니다.

그러나 호스트별 ID 보기에서 ID 재정의의 가용성은 제한됩니다.

기존 클라이언트: RHEL 6.3 및 이전 버전 (SSSD 1.8 이상)

클라이언트는 적용할 특정 ID 보기를 요청할 수 있습니다.

기존 클라이언트에서 호스트별 ID 뷰를 사용하려면 클라이언트의 기본 DN을 cn=id_view_name,cn=views,cn=compat,dc=com 로 변경합니다.

RHEL 6.4에서 7.0 (SSSD 1.9 to 1.11)

클라이언트의 호스트별 ID 보기는 지원되지 않습니다.

RHEL 7.1 이상 (SSSD 1.12 이상)

완전 지원.

8.2. ID 충돌 수정

IdM은 ID 범위를 사용하여 다른 도메인에서 POSIX ID의 충돌을 방지합니다. ID 범위에 대한 자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드 의 ID 범위를 참조하십시오.

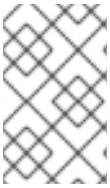
IdM은 다른 종류의 ID 범위와 겹치는 것을 허용해야 하므로 ID 뷰의 POSIX ID 보기에서는 특수 범위 유형을 사용하지 않습니다. 예를 들어 동기화를 통해 생성된 AD 사용자에게는 IdM 사용자와 동일한 ID 범위의 POSIX ID가 있습니다.

POSIX ID는 IdM 측의 ID 보기에서 수동으로 관리됩니다. 따라서 ID 충돌이 발생하면 충돌하는 ID를 변경하여 수정합니다.

8.3. ID 뷰를 사용하여 AD 사용자 속성 정의

ID 뷰를 사용하면 AD에 정의된 사용자 특성 값을 변경할 수 있습니다. 속성의 전체 목록은 ID 보기를 무시할 수 있는 특성을 참조하십시오.

예를 들면 다음과 같습니다. 혼합 Linux-Windows 환경을 관리하고 AD 사용자에 대해 POSIX 속성 또는 SSH 로그인 속성을 수동으로 정의하려는 경우 AD 정책에서 허용하지 않는 경우 ID 뷰를 사용하여 특성 값을 재정의할 수 있습니다. AD 사용자가 SSSD를 실행하는 클라이언트에 인증하거나 비교 LDAP 트리를 사용하여 인증하면 인증 프로세스에서 새 값이 사용됩니다.



참고

IdM 사용자만 ID 보기를 관리할 수 있습니다. AD 사용자는 할 수 없습니다.

특성 값을 재정의하는 프로세스는 다음 단계를 따릅니다.

1. 새 ID 보기를 만듭니다.
2. ID 뷰에 사용자 ID 재정의를 추가하고 require 특성 값을 지정합니다.
3. 특정 호스트에 ID 뷰를 적용합니다.

이러한 단계를 수행하는 방법에 대한 자세한 내용은 Linux 도메인 ID, 인증 및 정책 가이드 의 다양한 호스트에서 사용자 계정의 다양한 속성 값 정의를 참조하십시오.

8.4. NIS 도메인을 IDM으로 마이그레이션

Linux 환경을 관리하고 다른 UID 및 GID가 있는 분산된 NIS 도메인을 최신 ID 관리 솔루션으로 마이그레이션하려는 경우 ID 뷰를 사용하여 기존 호스트에 대한 호스트 특정 UID 및 GID를 설정하여 기존 파일 및 디렉터리에 대한 권한이 변경되지 않도록 할 수 있습니다.

마이그레이션 프로세스는 다음 단계를 따릅니다.

1. IdM 도메인에 사용자 및 그룹을 생성합니다. 자세한 내용은 를 참조하십시오.

- 단계 또는 활성 사용자 추가
- 사용자 그룹 추가 및 제거

2. 기존 호스트에 ID 뷰를 사용하여 사용자 생성 중에 IdM에서 생성한 ID를 덮어씁니다.

    1. 개별 ID 보기를 생성합니다.
    2. ID 보기에 사용자 및 그룹의 ID 재정의를 추가합니다.
    3. 특정 호스트에 ID 뷰를 할당합니다.

    자세한 내용은 다른 호스트에서 사용자 계정의 다양한 속성 값 정의를 참조하십시오.

3. Linux 도메인 ID, 인증 및 정책 가이드에서 ID 관리 클라이언트 설치 및 제거.
4. NIS 도메인 해제.

8.5. 짧은 이름을 사용하여 RESOLVE 및 AUTHENTICATE 사용자 및 그룹 사용에 대한 구성 옵션

이 섹션에서는 AD(Active Directory) 환경에서 사용자 및 그룹을 확인하고 인증하기 위해 user_name@domain 또는 domain\user_name 대신 짧은 사용자 또는 그룹 이름을 사용할 수 있는 구성 옵션에 대해 설명합니다. 다음을 구성할 수 있습니다.

- AD를 신뢰하는 IdM(Identity Management)
- SSSD를 사용하여 AD에 가입한 Red Hat Enterprise Linux

8.5.1. 도메인 확인 작동 방식

도메인 확인 순서 옵션을 사용하여 도메인 목록을 검색하여 지정된 사용자 이름에 대한 일치를 반환하는 순서를 지정할 수 있습니다. 옵션을 설정할 수 있습니다.

- **On the server** 보기:
  - 8.5.2.1절. "도메인 확인 순서(Globally) 설정"
  - 8.5.2.2절. "ID 보기의 도메인 확인 순서 설정"
- **On the client** 보기 8.5.3절. "IdM 클라이언트의 도메인 확인 순서 구성"

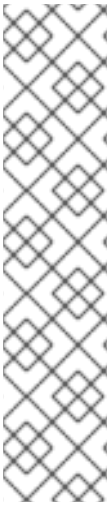
Active Directory 트러스트가 있는 환경에서는 서버 기반 옵션 중 하나 또는 둘 다를 적용하는 것이 좋습니다.

특정 클라이언트의 관점에서 도메인 확인 순서 옵션은 위의 세 위치 중 하나 이상에서 설정할 수 있습니다. 클라이언트가 세 가지 위치를 참조하는 순서는 다음과 같습니다.

1. 로컬 **sssd.conf** 설정
2. **id view** 구성
3. 글로벌 **IdM** 구성

먼저 확인된 도메인 확인 순서 설정만 사용됩니다.

Red Hat Enterprise Linux가 AD에 직접 통합되는 환경에서는 클라이언트에서 도메인 확인 순서만 설정할 수 있습니다.



참고

다음과 같은 경우 정규화된 이름을 사용해야 합니다.

- *여러 도메인에 사용자 이름이 있습니다.*
- *SSSD 설정에는 default_domain_suffix 옵션이 포함되어 있으며 해당 옵션으로 지정되지 않은 도메인에 대한 요청을 하고 싶습니다.*

8.5.2. ID 관리 서버에서 도메인 확인 순서 구성

도메인 또는 하위 도메인의 클라이언트가 동일한 도메인 확인 순서를 사용해야 하는 경우 서버 기반 구성을 선택합니다.

8.5.2.1. 도메인 확인 순서(Globally) 설정

도메인 확인 순서를 신뢰의 모든 클라이언트에 설정하려면 이 옵션을 선택합니다. 이렇게 하려면 ipa config-mod 명령을 사용합니다. 예를 들어 여러 하위 도메인이 있는 AD Lake를 신뢰하는 IdM 도메인에서 다음을 수행합니다.

```
$ ipa config-mod --domain-resolution-order='idm.example.com:ad.example.com:subdomain1.ad.example.com:subdomain2.ad.example.com'
Maximum username length: 32
Home directory base: /home
...
Domain Resolution Order:
idm.example.com:ad.example.com:subdomain1.ad.example.com:subdomain2.ad.example.com
...
```

이러한 방식으로 도메인 확인 순서를 설정하면 IdM 도메인과 신뢰할 수 있는 ADest의 사용자 모두 짧은 이름만 사용하여 로그인할 수 있습니다.

8.5.2.2. ID 보기의 도메인 확인 순서 설정

특정 도메인의 클라이언트에 설정을 적용하려면 이 옵션을 선택합니다.

예를 들어 하위 도메인 서버에서 **server.idm.example.com.com .idm.example.com . subdomain1.ad.example.com** 하위 도메인에서 더 많은 로그인 정보를 확인합니다. 그러나 글로벌 확인 순서는 사용자 이름을 확인할 때 **subdomain1.ad.example.com** 하위 도메인 사용자 데이터베이스가 **subdomain2.ad.example.com** 이전에 시도됨을 나타냅니다. 특정 서버에 대해 다른 순서를 설정하려면 특정 보기에 대한 도메인 확인 순서를 설정합니다.

1. 도메인 확인 순서 옵션이 설정된 **ID** 보기를 생성합니다.

```
$ ipa idview-add example_view --desc "ID view for custom shortname resolution on
server.idm.example.com" --domain-resolution-order
subdomain2.ad.example.com:subdomain1.ad.example.com
---------------------------------
Added ID View "example_view"
---------------------------------
ID View Name: example_view
Description: ID view for custom shortname resolution on server.idm.example.com
Domain Resolution Order: subdomain2.ad.example.com:subdomain1.ad.example.com
```

2. 클라이언트에 뷰를 적용합니다. 예를 들면 다음과 같습니다.

```
$ ipa idview-apply example_view --hosts server.idm.example.com
---------------------------------
Applied ID View "example_view"
---------------------------------
hosts: server.idm.example.com
-----------------------------------------
Number of hosts the ID View was applied to: 1
-----------------------------------------
```

ID 뷰에 대한 자세한 내용은 *8장. Active Directory 환경에서 ID 뷰 사용* 을 참조하십시오.

8.5.3. IdM 클라이언트의 도메인 확인 순서 구성

낮은 수의 클라이언트에서 또는 클라이언트가 **AD**에 직접 연결된 경우 클라이언트의 도메인 확인 순서를 설정합니다.

/etc/sssd/sssd.conf 파일에서 **domain_resolution_order** 옵션을 설정합니다. 예를 들면 다음과 같습니다.

-

domain_resolution_order = *subdomain1.ad.example.com, subdomain2.ad.example.com*

domain_resolution_order *옵션 구성에 대한 자세한 내용은* **sssd.conf(5)** *매뉴얼 페이지를 참조하십시오.*

부록 A. 개정 내역

버전 번호는 Red Hat Enterprise Linux 버전 번호가 아닌 이 설명서의 에디션과 관련이 있습니다.

고침 7.0-51 **Thu Mar 4 2021** **Florian Delehaye**
7.9 GA 가이드 버전입니다. DNA ID 범위를 수동으로 조정하는 데 대한 새 섹션을 추가했습니다.

고침 7.0-50 **Wed May 27 2020** **Florian Delehaye**
몇 가지 수정 및 업데이트

고침 7.0-49 **Tue Aug 06 2019** **Marc Muehlfeld**
7.7 GA 게시용 문서 버전.

고침 7.0-48 **Wed Jun 05 2019** **Marc Muehlfeld**
보안 *에이전트 구성* 업데이트, *AD 공급자가 신뢰할 수 있는 도메인을 처리하는 방법과SSSD에서 표시하는 사용자 이름 형식 변경* 방법이 추가되었습니다.

고침 7.0-47 **Tue Apr 08 2019** **Marc Muehlfeld**
몇 가지 사소한 수정 및 업데이트

고침 7.0-46 **Mon Oct 29 2018** **Filip Hanzelka**
7.6 GA 게시를 위한 문서 준비.

고침 7.0-45 **Mon Jun 25 2018** **Filip Hanzelka**
SMB share Access를 위해 SSSD와 Winbind 간 전환이 추가되었습니다.

고침 7.0-44 **Thu Apr 5 2018** **Filip Hanzelka**
7.5 GA 게시를 위한 문서 준비.

고침 7.0-43 **Wed Feb 28 2018** **Filip Hanzelka**
*SSSD에서 지원하는 관련 설정*업데이트

고침 7.0-42 **Mon Feb 12 2018** **Aneta Šteflová Petrová**
공유 보안을 사용하여 2-Way Trust 생성

고침 7.0-41 **Mon Jan 29 2018** **Aneta Šteflová Petrová**
마이너 픽스.

고침 7.0-40 **Fri Dec 15 2017** **Aneta Šteflová Petrová**
마이너 픽스.

고침 7.0-39 **Mon Dec 6 2017** **Aneta Šteflová Petrová**
Active Directory 통합을 위해 Samba를 사용하여 업데이트.

고침 7.0-38 **Mon Dec 4 2017** **Aneta Šteflová Petrová**
신뢰를 위한 업데이트된 *DNS 및 realm 설정.*

고침 7.0-37 **Mon Nov 20 2017** **Aneta Šteflová Petrová**
공유 보안을 사용하여 2-Way Trust 생성

고침 7.0-36 **Mon Nov 6 2017** **Aneta Šteflová Petrová**

마이너 픽스.

고침 7.0-35 **Mon Oct 23 2017** **Aneta Šteflová Petrová**
업데이트된 *Active Directory 항목 및 POSIX 속성 구성 및 ID 매핑을 사용하여 SSSD의 공급자로 AD 도메인 구성*

고침 7.0-34 **Mon Oct 9 2017** **Aneta Šteflová Petrová**
짧은 이름 사용에 대한 구성 옵션이 추가되었습니다. 업데이트된 *신뢰 컨트롤러 및 신뢰 에이전트.*

고침 7.0-33 **Tue Sep 26 2017** **Aneta Šteflová Petrová**
SSSD 장의 자동 검색 섹션을 업데이트했습니다. 신뢰할 수 있는 도메인 구성에 두 개의 섹션이 추가되었습니다.

고침 7.0-32 **Tue Jul 18 2017** **Aneta Šteflová Petrová**
7.4 GA 게시용 문서 버전.

고침 7.0-31 **Tue May 23 2017** **Aneta Šteflová Petrová**
보안 ID 매핑에 대한 마이너 수정

고침 7.0-30 **Mon Apr 24 2017** **Aneta Šteflová Petrová**
Windows 통합 정의를 위한 작은 수정 사항.

고침 7.0-29 **Mon Apr 10 2017** **Aneta Šteflová Petrová**
업데이트된 직접 통합.

고침 7.0-28 **Mon Mar 27 2017** **Aneta Šteflová Petrová**
사용자가 암호 재설정 활성화로 Linux 도메인 ID 가이드로 다른 사용자의 비밀번호를 변경하도록 허용하도록 허용했습니다. 신뢰를 위해 지원되는 Windows 플랫폼 업데이트 손상된 링크로 인해 문제가 발생했습니다. 기타 마이너 업데이트

고침 7.0-27 **Mon Feb 27 2017** **Aneta Šteflová Petrová**
신뢰를 위한 포트 요구 사항 업데이트 신뢰 및 동기화를 위한 작은 구조 기타 마이너 업데이트

고침 7.0-26 **Wed Nov 23 2016** **Aneta Šteflová Petrová**
ipa-winsync-migrate를 추가했습니다. 신뢰, SSSD 및 동기화 장에 대한 사소한 수정

고침 7.0-25 **Tue Oct 18 2016** **Aneta Šteflová Petrová**
7.3 GA 게시 버전.

고침 7.0-24 **Thu Jul 28 2016** **Marc Muehlfeld**
업데이트된 다이어그램, 서비스 및 호스트에 대한 Kerberos 플래그가 추가됨, 기타 일부 수정 사항.

고침 7.0-23 **Thu Jun 09 2016** **Marc Muehlfeld**
동기화 장을 업데이트했습니다. Kerberos 장을 삭제했습니다. 기타 마이너 픽스.

고침 7.0-22 **Tue Feb 09 2016** **Aneta Petrová**
업데이트된 영역, 제거된 인덱스는 ID 보기의 일부를 Linux 도메인 ID 가이드, 기타 마이너 업데이트로 이동했습니다.

고침 7.0-21 **Fri Nov 13 2015** **Aneta Petrová**
마이너 업데이트가 포함된 7.2 GA 릴리스의 버전입니다.

고침 7.0-20 **Thu Nov 12 2015** **Aneta Petrová**
7.2 GA 릴리스 버전.

고침 7.0-19 **Fri Sep 18 2015** **Tomáš Čapek**
시작 페이지 정렬 순서를 업데이트합니다.

고침 7.0-18 **Thu Sep 10 2015** **Aneta Petrová**
출력 형식을 업데이트했습니다.

고침 7.0-17 **Mon Jul 27 2015** **Aneta Petrová**

grant-based access control, a number of other minor changes를 추가했습니다.

고침 7.0-16 **Thu Apr 02 2015** **Tomáš Čapek**
UNIX 확장용 Identity Management의 admonition을 사용하여 SSSD를 사용하여 확장된 ipa-advise, 확장된 CIFS 공유를 추가했습니다.

고침 7.0-15 **Fri Mar 13 2015** **Tomáš Čapek**
7.1에 대한 최근 편집 작업이 포함된 비동기 업데이트.

고침 7.0-13 **Wed Feb 25 2015** **Tomáš Čapek**
7.1 GA 릴리스의 버전입니다.

고침 7.0-11 **Fri Dec 05 2014** **Tomáš Čapek**
를 다시 빌드하여 시작 페이지의 정렬 순서를 업데이트합니다.

고침 7.0-7 **Mon Sep 15 2014** **Tomáš Čapek**
섹션 5.3 Create Trusts는 콘텐츠 업데이트에 대해 일시적으로 제거되었습니다.

고침 7.0-5 **June 27, 2014** **Ella Deon Ballard**
Samba+Kerberos+Winbind 장을 개선

고침 7.0-4 **June 13, 2014** **Ella Deon Ballard**
Kerberos 영역 추가 장.

고침 7.0-3 **June 11, 2014** **Ella Deon Ballard**
초기 릴리스.