Red Hat Enterprise Linux 8

Identity Management 설치

Identity Management 사용 시작하기

Last Updated: 2022-08-16

Red Hat Enterprise Linux 8 Identity Management 설치

Identity Management 사용 시작하기

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

이 문서 수집에서는 RHEL(Red Hat Enterprise Linux 8)에 Identity Management를 설치하는 방법에 대한 지침을 제공합니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

Identity Management에서 용어 교체는 다음과 같습니다.

- *블랙리스트*를 ***블록 목록***으로 대체
- *화이트리스트*를 ***허용 목록***으로 대체
- *슬레이브*를 ***보조***로 대체
- 컨텍스트에 따라 *마스터*라는 단어가 보다 정확한 용어로 교체되고 있습니다.
  - *IdM 마스터*를 ***IdM 서버***로 대체
  - *CA 갱신 마스터*를 ***CA 갱신 서버***로 대체
  - *CRL 마스터*를 ***CRL 게시자 서버***로 대체
  - *multi-master*를 ***multi-supplier***로 교체

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. Red Hat이 어떻게 이를 개선할 수 있는지 알려 주십시오.

- 특정 문구에 대한 간단한 의견 작성 방법은 다음과 같습니다.
  1. 문서가 *Multi-page HTML* 형식으로 표시되는지 확인합니다. 또한 문서 오른쪽 상단에 **피드백** 버튼이 있는지 확인합니다.
  2. 마우스 커서를 사용하여 주석 처리하려는 텍스트 부분을 강조 표시합니다.
  3. 강조 표시된 텍스트 아래에 표시되는 **피드백 추가** 팝업을 클릭합니다.
  4. 표시된 지침을 따릅니다.
- Bugzilla를 통해 피드백을 제출하려면 새 티켓을 생성하십시오.
  1. Bugzilla 웹 사이트로 이동하십시오.
  2. 구성 요소로 **문서**를 사용합니다.
  3. **설명** 필드에 문서 개선을 위한 제안 사항을 기입하십시오. 관련된 문서의 해당 부분 링크를 알려주십시오.
  4. **버그 제출**을 클릭합니다.

1장. 이 가이드를 사용하는 방법

IdM(Identity Management) 도메인에는 복제 및 IdM 클라이언트라고도 하는 IdM 서버가 포함되어 있습니다. IdM 배포를 설치하는 것은 항상 기본 IdM 서버 설치에서 시작되지만 다음 설치 단계의 순서는 대상 토폴로지에 따라 다릅니다. 예를 들어 IdM 클라이언트를 설치하기 전이나 후에 IdM 복제본을 설치할 수 있습니다. 또한 특정 IdM 배포에 는 Active Directory에 대한 신뢰가 필요하지만 다른 IdM 배포에는 신뢰할 수 없습니다.

I 부. IDENTITY MANAGEMENT 설치

2장. IDM 서버 설치를 위한 시스템 준비

다음 섹션에서는 IdM(Identity Management) 서버를 설치하는 요구 사항을 나열합니다. 설치하기 전에 시스템이 이러한 요구 사항을 충족하는지 확인하십시오.

2.1. 사전 요구 사항

- 호스트에 IdM(Identity Management) 서버를 설치하려면 **root** 권한이 필요합니다.

2.2. 하드웨어 권장 사항

RAM은 적절한 크기 조정에 가장 중요한 하드웨어 기능입니다. 시스템에 사용 가능한 RAM이 충분한지 확인합니다. 일반적인 RAM 요구 사항은 다음과 같습니다.

- 10,000명의 사용자 및 100개의 그룹: 최소 4GB의 RAM 및 4GB 스왑 공간
- 사용자 100,000명 및 50,000개 그룹의 경우: 최소 16GB의 RAM 및 4GB의 스왑 공간

대규모 배포의 경우 대부분의 데이터가 캐시에 저장되므로 디스크 공간을 늘리는 것보다 RAM을 늘리는 것이 더 효율적입니다. 일반적으로 RAM을 추가하면 캐싱으로 인해 대규모 배포를 위해 성능이 향상됩니다.

참고

기본 사용자 항목 또는 인증서가 있는 간단한 호스트 항목은 약 5개입니다.크기가 10KB입니다.

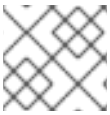
2.3. IDM의 사용자 정의 설정 요구 사항

DNS, Kerberos, Apache 또는 Directory Server와 같은 서비스에 대한 사용자 정의 구성 없이 정리 시스템에 IdM(Identity Management) 서버를 설치합니다.

IdM 서버 설치에서는 시스템 파일을 덮어써서 IdM 도메인을 설정합니다. IdM은 원본 시스템 파일을 **/var/lib/ipa/sysrestore/**에 백업합니다. 라이프사이클이 끝날 때 IdM 서버가 설치 제거되면 이러한 파일이 복원됩니다.

IdM의 IPv6 요구 사항

IdM 시스템에는 커널에 IPv6 프로토콜이 활성화되어 있어야 합니다. IPv6를 비활성화하면 IdM 서비스에서 사용하는 CLDAP 플러그인이 초기화되지 않습니다.



참고

네트워크에서 IPv6를 활성화할 필요가 없습니다.

IdM의 암호화 유형 지원

RHEL(Red Hat Enterprise Linux)은 AES(Advanced Encryption Standard), Camellia 및 Data Encryption Standard(DES)와 같은 암호화 유형을 지원하는 Kerberos 프로토콜의 버전 5를 사용합니다.

지원되는 암호화 유형 목록

IdM 서버 및 클라이언트의 Kerberos 라이브러리는 더 많은 암호화 유형을 지원할 수 있지만 IdM Kerberos Distribution Center(KDC)는 다음 암호화 유형만 지원합니다.

- **aes256-cts:normal**
- **aes256-cts:special** (기본값)
- **aes128-cts:normal**
- **aes128-cts:special** (기본값)
- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**
- **camellia128-cts-cmac:normal**
- **camellia128-cts-cmac:special**
- **camellia256-cts-cmac:normal**
- **camellia256-cts-cmac:special**

RC4 암호화 유형은 기본적으로 비활성화되어 있습니다.

다음 RC4 암호화 유형은 최신 AES-128 및 AES-256 암호화 유형보다 덜 안전한 것으로 간주되므로 RHEL 8에서 기본적으로 더 이상 사용되지 않거나 비활성화되어 있습니다.

- **arcfour-hmac:normal**
- **arcfour-hmac:special**

RC4에서 이전 Active Directory 환경과의 호환성을 수동으로 지원하는 방법에 대한 자세한 내용은 AD 및 RHEL의 일반적인 암호화 유형에 대한 지원 활성화를 참조하십시오.

DES 및 3DES 암호화 지원이 제거되었습니다.

보안상의 이유로 RHEL 7에서는 DES 알고리즘 지원이 더 이상 사용되지 않습니다. RHEL 8.3.0의 Kerberos 패키지 리베이스는 RHEL 8의 단일DES(DES) 및 threele-DES(DES) 암호화 유형에 대한 지원을 제거합니다.

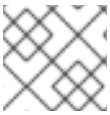
참고

표준 RHEL 8 IdM 설치는 기본적으로 DES 또는 3DES 암호화 유형을 사용하지 않으며 Kerberos 업그레이드의 영향을 받지 않습니다.

DES 또는 3DES 암호화(예: 레거시 클라이언트) **만** 사용하도록 서비스 또는 사용자를 수동으로 구성한 경우 다음과 같은 최신 Kerberos 패키지로 업데이트한 후 서비스 중단이 발생할 수 있습니다.

- Kerberos 인증 오류
- **unknown enctype** 암호화 오류
- DES로 암호화된 Database Master Keys(**K/M**)가 있는 KDC를 시작할 수 없습니다.

사용자 환경에서 DES 또는 3DES 암호화를 사용하지 않는 것이 좋습니다.



참고

환경을 사용하도록 구성된 경우 DES 및 3DES 암호화 유형만 비활성화해야 합니다.

IdM에서 시스템 전체 암호화 정책 지원

IdM은 **DEFAULT** 시스템 전체 암호화 정책을 사용합니다. 이 정책은 현재 위협 모델에 대한 보안 설정을 제공합니다. 이 보안 설정은 TLS 1.2 및 1.3 프로토콜과 IKEv2 및 SSH2 프로토콜을 허용합니다. RSA 키와 Diffie-Hellman 매개변수는 2048비트 이상인 경우 허용됩니다. 이 정책은 DES, 3DES, RC4, DSA, TLS v1.0 및 기타 Weaker 알고리즘을 허용하지 않습니다.

참고

FUTURE 시스템 전체 암호화 정책을 사용하는 동안에는 IdM 서버를 설치할 수 없습니다. IdM 서버를 설치할 때 **DEFAULT** 시스템 전체 암호화 정책을 사용하고 있는지 확인합니다.

추가 리소스

- 시스템 전체 암호화 정책

2.4. FIPS 컴플라이언스

RHEL 8.3.0 이상에서는 새 IdM 서버를 설치하거나 연방 정보 처리 표준(FIPS) 모드가 활성화된 시스템에 IdM 서버를 설치할 수 있습니다.

FIPS를 사용하여 IdM을 설치하려면 먼저 호스트에서 FIPS 모드를 활성화한 다음 IdM을 설치하십시오. IdM 설치 스크립트는 FIPS가 활성화되어 있는지 감지하고 FIPScabundle와 호환되는 암호화 유형만 사용하도록 IdM을 구성합니다.

- **aes256-cts:normal**
- **aes256-cts:special**
- **aes128-cts:normal**
- **aes128-cts:special**
- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**

IdM 환경이 FIPS와 호환되려면 **모든** IdM 복제본이 FIPS 모드를 활성화해야 합니다.

특히 이러한 클라이언트를 IdM 복제본으로 승격할 수 있는 경우 IdM 클라이언트에서 FIPS를 활성화하는 것이 좋습니다. 궁극적으로 FIPS 요구 사항을 충족하는 방법을 결정하는 것은 관리자에게 달려 있습니다. Red Hat은 FIPS 기준을 강제하지 않습니다.

2.5. FIPS 모드가 활성화된 교차 포리스트 신뢰 지원

FIPS 모드가 활성화된 동안 AD(Active Directory) 도메인을 사용하여 교차 트러스트를 설정하려면 다음 요구 사항을 충족해야 합니다.

- IdM 서버는 RHEL 8.4.0 이상에 있습니다.
- 신뢰를 설정할 때 AD 관리 계정으로 인증해야 합니다. FIPS 모드가 활성화된 동안 공유 보안을 사용하여 신뢰를 설정할 수 없습니다.

중요

RADIUS 프로토콜은 MD5 해시 함수를 사용하여 클라이언트와 서버 간 암호를 암호화하고 FIPS 모드에서는 MD5 다이제스트 알고리즘의 사용을 비활성화하므로 RADIUS 인증이 FIPS와 호환되지 않습니다. 그러나 RADIUS 서버가 IdM 서버와 동일한 호스트에서 실행 중인 경우 문제를 해결하고 FIPS 모드에서 FreeRADIUS 인증을 구성하는 방법에 설명된 단계를 수행하여 MD5를 활성화할 수 있습니다.

추가 리소스

- RHEL 운영 체제에서 FIPS 모드를 활성화하려면 *Security Hardening* 가이드에서 시스템을 FIPS 모드로 전환합니다.
- FIPSRegistryLogin에 대한 자세한 내용은 NIST(National Labs of Standards and Technology) 웹 사이트에서 암호화 모듈에 대한 보안 요구 사항 을 참조하십시오.

2.6. IDM에서 CHRONYD를 동기화하는 방법

이 섹션에서는 **chronyd**를 사용하여 IdM 호스트를 중앙 시간 소스와 동기화합니다.

IdM의 기본 인증 메커니즘인 Kerberos는 타임스탬프를 프로토콜의 일부로 사용합니다. IdM 클라이언트의 시스템 시간이 KDC(Key Distribution Center) 시스템 시간과 5분 이상 다른 경우 Kerberos 인증이 실패합니다.

IdM 서버 및 클라이언트가 중앙 시간 소스와 동기화되도록 IdM 설치 스크립트는 **chronyd** 네트워크 시간 프로토콜(NTP) 클라이언트 소프트웨어를 자동으로 구성합니다.

IdM 설치 명령에 NTP 옵션을 전달하지 않으면 설치 프로그램이 네트워크에서 NTP 서버를 가리키는 **_ntp._udp** DNS 서비스(SRV) 레코드를 검색하고 해당 IP 주소로 **chrony**를 구성합니다. **_ntp._udp** SRV 레코드가 없는 경우 **chronyd** 는 **chrony** 패키지와 함께 제공되는 설정을 사용합니다.

참고

ntpd는 RHEL 8에서 **chronyd** 보다 더 이상 사용되지 않기 때문에 IdM 서버는 더 이상 NTP(Network Time Protocol) 서버로 구성되지 않으며 NTP 클라이언트로만 구성됩니다. RHEL 8에서는 RHEL 7 **NTP Server** IdM 서버 역할도 더 이상 사용되지 않습니다.

추가 리소스

- NTP 구현
- Chrony 모음을 사용하여 NTP 구성

2.7. IDM 설치 명령의 NTP 구성 옵션 목록

이 섹션에서는 **chronyd**를 사용하여 IdM 호스트를 중앙 시간 소스와 동기화된 상태로 유지하는 방법에 대해 설명합니다.

설치 중에 **chronyd** 클라이언트 소프트웨어를 구성하기 위해 IdM 설치 명령(**ipa-server-install**,**ipa-replica-install**,**ipa-client-install**)을 사용하여 다음 옵션을 지정할 수 있습니다.

표 2.1. IdM 설치 명령의 NTP 구성 옵션 목록

옵션	동작
--ntp-server	이를 사용하여 하나의 NTP 서버를 지정합니다. 여러 번 사용하여 여러 서버를 지정할 수 있습니다.
--ntp-pool	이를 사용하여 하나의 호스트 이름으로 확인된 여러 NTP 서버 풀을 지정합니다.
-N, **--no-ntp**	**chronyd** 를 구성, 시작 또는 활성화하지 마십시오.

추가 리소스

- NTP 구현
- Chrony 모음을 사용하여 NTP 구성

2.8. IDM에서 NTP 시간 서버를 참조할 수 있는지 확인

이 절차에서는 IdM이 NTP(Network Time Protocol) 시간 서버와 동기화되는 데 필요한 구성이 있는지 확인합니다.

사전 요구 사항

- 환경에 NTP 시간 서버를 구성했습니다. 이 예에서 이전에 구성된 시간 서버의 호스트 이름은 **ntpserver.example.com**입니다.

절차

1. DNS 서비스(SRV) 레코드 환경에서 NTP 서버를 검색합니다.

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

2. 이전 **dig** 검색에서 시간 서버를 반환하지 않으면 포트 **123**에서 시간 서버를 가리키는 **_ntp._udp** SRV 레코드를 추가합니다. 이 프로세스는 DNS 솔루션에 따라 다릅니다.

검증 단계

- **_ntp._udp** SRV 레코드를 검색할 때 DNS가 포트 **123**에서 시간 서버에 대한 항목을 반환하는지 확인합니다.

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

추가 리소스

- NTP 구현

- Chrony 모음을 사용하여 NTP 구성

2.9. IDM의 호스트 이름 및 DNS 요구 사항

이 섹션에는 서버 및 복제본 시스템에 대한 호스트 이름 및 DNS 요구 사항이 나열됩니다. 또한 시스템이 요구 사항을 충족하는지 확인하는 방법도 보여줍니다.

이 섹션의 요구 사항은 통합된 DNS 및 통합 DNS가 없는 IdM(Identity Management) 서버에 적용됩니다.

주의

LDAP 디렉터리 서비스, Kerberos 및 Active Directory 통합 실행을 포함하여 거의 모든 IdM 도메인 기능에 DNS 레코드가 중요합니다. 신중하게 다음 사항을 확인하십시오.

- 테스트되고 기능적인 DNS 서비스를 사용할 수 있습니다.
- 서비스가 올바르게 구성되어 있습니다.

이 요구 사항은 통합된 DNS가 있는 IdM 서버에 적용됩니다.

서버 호스트 이름 확인

호스트 이름은 ***server.idm.example.com*** 과 같은 정규화된 도메인 이름이어야 합니다.

중요

단일 레이블 도메인 이름(예: .company): IdM 도메인은 하나 이상의 하위 도메인과 최상위 도메인(예: example.com 또는 company.example.com)으로 구성되어야 합니다.

정규화된 도메인 이름은 다음 조건을 충족해야 합니다.

- **유효한 DNS 이름이며 숫자, 영문자 및 하이픈(-)만 허용됩니다. 호스트 이름에 밑줄(_)과 같은 기타 문자는 DNS 오류가 발생합니다.**
- **모두 소문자이어야 합니다. 대문자는 사용할 수 없습니다.**
- **루프백 주소로 확인되지 않습니다. 127.0.0.1 이 아닌 시스템의 공용 IP 주소로 확인되어야 합니다.**

호스트 이름을 확인하려면 설치하려는 시스템에서 hostname 유틸리티를 사용합니다.

```
# hostname
server.idm.example.com
```

hostname의 출력은 localhost 또는 localhost6이 아니어야 합니다.

정방향 및 역방향 DNS 구성 확인

1. **서버의 IP 주소를 가져옵니다.**

a. **ip addr show** 명령은 IPv4 및 IPv6 주소를 모두 표시합니다. 다음 예에서 범위가 전역이므로 관련 IPv6 주소는 **2001:DB8::1111** 입니다.

```
[root@server ~]# ip addr show
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
 link/ether 00:1a:4a:10:4e:33 brd ff:ff:ff:ff:ff:ff
 inet 192.0.2.1/24 brd 192.0.2.255 scope global dynamic eth0
  valid_lft 106694sec preferred_lft 106694sec
 inet6 2001:DB8::1111/32 scope global dynamic
   valid_lft 2591521sec preferred_lft 604321sec
 inet6 fe80::56ee:75ff:fe2b:def6/64 scope link
       valid_lft forever preferred_lft forever
...
```

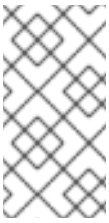
2. **dig** 유틸리티를 사용하여 정방향 DNS 구성을 확인합니다.

a. **dig +short *server.idm.example.com*** 명령을 실행합니다. 반환된 IPv4 주소는**ip addr show** 에서 반환된 IP 주소와 일치해야 합니다.

```
[root@server ~]# dig +short server.idm.example.com A
192.0.2.1
```

b. **dig +short *server.idm.example.com* AAAA** 명령을 실행합니다. 주소를 반환하는 경우**ip addr show**:에서 반환한 IPv6 주소와 일치해야합니다.

```
[root@server ~]# dig +short server.idm.example.com AAAA
2001:DB8::1111
```



참고

dig 에서 AAAA 레코드에 대한 출력을 반환하지 않으면 잘못된 구성이 표시되지 않습니다. 출력은 단지 시스템의 DNS에 IPv6 주소가 구성되어 있지 않음을 의미합니다. 네트워크에서 IPv6 프로토콜을 사용하지 않으려면 이 상황에서 설치를 진행할 수 있습니다.

3. 역방향 DNS 구성(PTR 레코드)을 확인합니다. **dig** 유틸리티를 사용하여 IP 주소를 추가합니다. 아래 명령에서 다른 호스트 이름 또는 호스트 이름이 없으면 역방향 DNS 구성이 올바르지 않습니다.

a. **dig +short -x *IPv4_address*** 명령을 실행합니다. 출력에 서버 호스트 이름이 표시되어야 합니다. 예를 들어 다음과 같습니다.

```
[root@server ~]# dig +short -x 192.0.2.1
server.idm.example.com
```

b. 이전 단계에서 **dig +short -x *server.example.com* AAAA** 명령이 IPv6 주소를 반환한 경우 **dig** 를 사용하여 IPv6 주소를 쿼리합니다. 출력에 서버 호스트 이름이 표시되어야 합니다. 예를 들어 다음과 같습니다.

```
[root@server ~]# dig +short -x 2001:DB8::1111
server.idm.example.com
```

참고

이전 단계에서 **dig +short *server.idm.example.com* AAAA** 가 IPv6 주소를 표시하지 않으면 AAAA 레코드를 쿼리해도 아무 것도 출력되지 않습니다. 이 경우 정상적인 동작이며 잘못된 구성이 표시되지 않습니다.

주의

역방향 DNS(PTR 레코드) 검색에서 여러 호스트 이름, **httpd** 및 IdM과 관련된 기타 소프트웨어에서 예기치 않은 동작이 표시될 수 있습니다. Red Hat은 IP당 하나의 PTR 레코드만 구성하는 것이 좋습니다.

DNS 전달자의 표준 준수 확인 (통합 DNS에만 필요)

IdM DNS 서버와 함께 사용하려는 모든 DNS 전달자가 DNS (Extension Mechanisms for DNS (EDNS0) 및 DNS Security Extensions) 표준을 준수하는지 확인하십시오. 이렇게 하려면 각 전달자에 대해 다음 명령의 출력을 검사합니다.

```
$ dig +dnssec @IP_address_of_the_DNS_forwarder . SOA
```

명령에서 표시되는 예상 출력에는 다음 정보가 포함됩니다.

- 상태: **NOERROR**
- 플래그: **ra**
- EDNS 플래그: **do**
- **RRSIG** 레코드가 **ANSWER** 섹션에 있어야 합니다.

출력에서 이러한 항목 중 하나라도 없으면 DNS 전달자의 설명서를 검사하고 EDNS0 및 DNSSEC가 지원되는지 확인합니다. 최신 버전의 BIND 서버에서 **dnssec-enable yes;** 옵션은 **/etc/named.conf** 파일에 설정해야 합니다.

dig에서 생성된 예상 출력 예:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48655
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; ANSWER SECTION:
. 31679 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2015100701 1800 900 604800
86400
. 31679 IN RRSIG SOA 8 0 86400 20151017170000 20151007160000 62530 . GNVz7SQs [...]
```

/etc/hosts 파일 확인

/etc/hosts 파일이 다음 조건 중 하나를 충족하는지 확인합니다.

- 파일에는 호스트에 대한 항목이 포함되어 있지 않습니다. 호스트의 IPv4 및 IPv6 localhost 항목만 나열합니다.
- 파일에는 호스트에 대한 항목이 포함되어 있으며 파일은 다음 조건을 모두 이행합니다.
  - 처음 두 항목은 IPv4 및 IPv6 localhost 항목입니다.
  - 다음 항목은 IdM 서버 IPv4 주소와 호스트 이름을 지정합니다.
  - IdM 서버의 **FQDN**은 IdM 서버의 짧은 이름 앞에 옵니다.
  - IdM 서버 호스트 이름은 localhost 항목에 포함되지 않습니다.

다음은 올바르게 구성된 **/etc/hosts** 파일의 예입니다.

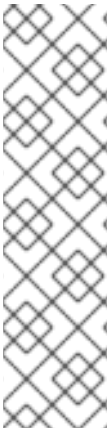
```
127.0.0.1   localhost localhost.localdomain \
localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain \
localhost6 localhost6.localdomain6
192.0.2.1 server.idm.example.com server
2001:DB8::1111 server.idm.example.com server
```

2.10. IDM의 포트 요구 사항

IdM(Identity Management)은 여러 포트를 사용하여 해당 서비스와 통신합니다. 이러한 포트가 열려 있어야 하며 IdM 서버 작동을 위해 IdM 서버에 대한 수신 연결에 사용할 수 있어야 합니다. 현재 다른 서비스에서 사용하거나 방화벽에 의해 차단되어서는 안 됩니다.

표 2.2. IdM 포트

서비스	포트	프로토콜
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP 및 UDP
DNS	53	TCP 및 UDP (선택 사항)
NTP	123	UDP (선택 사항)



참고

IdM은 포트 80 및 389를 사용합니다. 이 방법은 다음과 같은 안전 조치를 취하기 때문에 안전한 방법입니다.

- IdM은 일반적으로 포트 80에 도달하는 요청을 포트 443으로 리디렉션합니다. 포트 80(HTTP)은 OCSP(Online Certificate Status Protocol) 응답 및 CRL(Certificate Revocation Lists)을 제공하는 데만 사용됩니다. 둘 다 디지털 서명되어 있으므로 메시지 가로채기(man-in-the-middle) 공격으로부터 보호됩니다.
- 포트 389(LDAP)는 암호화를 위해 nfsnobodyTLS 및 Generic Security Services API(GSSAPI)를 사용합니다.

또한 포트 8080, 8443 및 749는 내부적으로 사용 가능해야 합니다. 이러한 포트를 열지 말고 방화벽에 의해 차단된 상태로 둡니다.

표 2.3. **firewalld** 서비스

서비스 이름	자세한 내용은 다음을 참조하십시오.
freeipa-ldap	**/usr/lib/firewalld/services/freeipa-ldap.xml**
freeipa-ldaps	**/usr/lib/firewalld/services/freeipa-ldaps.xml**
dns	**/usr/lib/firewalld/services/dns.xml**

2.11. IDM에 필요한 포트 열기

절차

1. **firewalld** 서비스가 실행 중인지 확인합니다.
   - **firewalld** 가 현재 실행되고 있는지 확인하려면 다음을 수행합니다.

     ```
     # systemctl status firewalld.service
     ```

   - **firewalld** 를 시작하고 시스템이 부팅될 때 자동으로 시작하도록 구성하려면 다음을 수행합니다.

     ```
     # systemctl start firewalld.service
     # systemctl enable firewalld.service
     ```

2. **firewall-cmd** 유틸리티를 사용하여 필요한 포트를 엽니다. 다음 옵션 중 하나를 선택합니다.
   a. **firewall-cmd --add-port** 명령을 사용하여 방화벽에 개별 포트를 추가합니다. 예를 들어 기본 영역에서 포트를 엽니다.

      ```
      # firewall-cmd --permanent --add-port=
      {80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp,123/udp}
      ```

   b. **firewall-cmd --add-service** 명령을 사용하여 방화벽에 **firewalld** 서비스를 추가합니다. 예를 들어 기본 영역에서 포트를 엽니다.

```
# firewall-cmd --permanent --add-service={freeipa-ldap,freeipa-ldaps,dns}
```

firewall-cmd 를 사용하여 시스템에서 포트를 여는 방법에 대한 자세한 내용은firewall-cmd(1) 매뉴얼 페이지를 참조하십시오.

3. **firewall-cmd** 구성을 다시 로드하여 변경 사항이 즉시 수행되었는지 확인합니다.

```
# firewall-cmd --reload
```

프로덕션 환경에서 시스템에서 **firewalld** 를 다시 로드하면 DNS 연결이 시간 초과될 수 있습니다. 필요한 경우 시간 초과를 방지하고 실행 중인 시스템에서 변경 사항을 영구적으로 만들려면 **firewall-cmd** 명령의 **--runtime-to-permanent** 옵션을 사용합니다. 예를 들면 다음과 같습니다.

```
# firewall-cmd --runtime-to-permanent
```

4. 선택 사항: 포트를 사용할 수 있는지 확인하려면**nc,telnet** 또는 **nmap** 유틸리티를 사용하여 포트에 연결하거나 포트 스캔을 실행합니다.

참고

또한 들어오고 나가는 트래픽 모두에 대한 네트워크 기반 방화벽도 열어야 합니다.

2.12. IDM 서버에 필요한 패키지 설치

RHEL8에서는 IdM(Identity Management) 서버를 설치하는 데 필요한 패키지가 모듈로 제공됩니다. IdM 서버 모듈 스트림은 **DL1** 스트림이라고 하며, 이 스트림에서 패키지를 다운로드하기 전에 이 스트림을 활성화해야 합니다. 다음 절차에서는 선택한 IdM 환경을 설정하는 데 필요한 패키지를 다운로드하는 방법을 보여줍니다.

사전 요구 사항

- 새로 설치된 RHEL 시스템이 있습니다.
- 필요한 리포지토리를 사용할 수 있습니다.
  - RHEL 시스템이 클라우드에서 실행되지 않는 경우 RHSM(Red Hat Subscription Manager)에 시스템을 등록합니다. 자세한 내용은 Subscription Manager 명령줄에서 서브스크립션 등록, 연결, 제거를 참조하십시오. IdM에서 사용하는 **BaseOS** 및 **AppStream** 리포지토리도 활성화했습니다.

```
# subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms
# subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms
```

RHSM을 사용하여 특정 리포지토리를 활성화 및 비활성화하는 방법에 대한 자세한 내용은 Red Hat Subscription Manager의 옵션 구성을 참조하십시오.

  - RHEL 시스템이 클라우드에서 실행 중인 경우 등록을 건너뜁니다. 필수 리포지토리는 이미 RHUI(Red Hat Update Infrastructure)를 통해 사용할 수 있습니다.
- 이전에 IdM 모듈 스트림을 활성화하지 않았습니다.

절차

1. **idm:DL1** 스트림을 활성화합니다.

```
# yum module enable idm:DL1
```

2. **idm:DL1** 스트림을 통해 제공되는 RPM으로 전환합니다.

```
# yum distro-sync
```

3. IdM 요구 사항에 따라 다음 옵션 중 하나를 선택합니다.

- 통합 DNS 없이 IdM 서버 설치에 필요한 패키지를 다운로드하려면 다음을 수행하십시오.

```
# yum module install idm:DL1/server
```

- 통합 DNS를 사용하여 IdM 서버를 설치하는 데 필요한 패키지를 다운로드하려면 다음을 수행합니다.

```
# yum module install idm:DL1/dns
```

- Active Directory와의 신뢰 관계가 있는 IdM 서버 설치에 필요한 패키지를 다운로드하려면 다음을 수행합니다.

```
# yum module install idm:DL1/adtrust
```

- 여러 프로필에서 패키지를 다운로드하려면 (예: **adtrust** 및 **dns** 프로필)

```
# yum module install idm:DL1/{dns,adtrust}
```

- IdM 클라이언트 설치에 필요한 패키지를 다운로드하려면 다음을 수행합니다.

```
# yum module install idm:DL1/client
```

중요

이미 다른 스트림을 활성화하여 패키지를 다운로드한 후 새 모듈 스트림으로 전환할 때 먼저 관련 설치된 모든 콘텐츠를 명시적으로 제거하고 새 모듈 스트림을 활성화하기 전에 현재 모듈 스트림을 비활성화해야 합니다. 현재 스트림을 비활성화하지 않고 새 스트림을 활성화하면 오류가 발생합니다. 진행 방법에 대한 자세한 내용은 이후 스트림으로 전환을 참조하십시오.

주의

모듈에서 모듈에서 패키지를 개별적으로 설치할 수는 있지만, 해당 모듈의 "API"로 나열되지 않은 모듈에서 패키지를 설치하는 경우 해당 모듈의 컨텍스트에서 Red Hat에서만 지원됩니다. 예를 들어 사용자 지정 389 Directory Server 설정과 함께 사용할 리포지토리에서 직접 **bind-dyndb-ldap** 를 설치하는 경우 IdM에 대해 발생하지 않는 한 발생하는 문제도 무시됩니다.

2.13. IDM 설치에 대한 올바른 파일 모드 생성 마스크 설정

IdM(Identity Management) 설치 프로세스에서 루트 계정에 대해 파일 모드 생성 마스크를**0022** 로 설정해야 합니다. 이렇게 하면 **root** 이외의 사용자가 설치 중에 생성된 파일을 읽을 수 있습니다. 다른 **ServiceAccount** 가 설정되면 **IdM** 서버 설치에 경고가 표시됩니다. 설치를 계속하면 서버의 일부 기능이 제대로 작동하지 않습니다. 예를 들어 이 서버에서 **IdM** 복제본을 설치할 수 없습니다. 설치한 후 **umask** 를 원래 값으로 다시 설정할 수 있습니다.

사전 요구 사항

- 루트 권한이 있어야 합니다.

절차

1. (선택 사항) 현재 **umask** 를 표시합니다.

```
# umask
0027
```

2. **bookinfo**를 **0022** 로 설정합니다.

```
# umask 0022
```

3. (선택 사항) **IdM** 설치가 완료된 후 **CCO**를 원래 값으로 다시 설정합니다.

```
# umask 0027
```

3장. IDM 서버 설치: 통합 DNS 사용, 통합 CA를 루트 CA로 사용

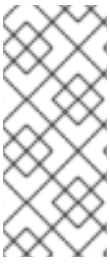
통합된 DNS를 사용하여 새로운 IdM(Identity Management) 서버를 설치하는 경우 다음과 같은 이점이 있습니다.

- 네이티브 IdM 툴을 사용하여 많은 유지 관리 및 DNS 레코드 관리를 자동화할 수 있습니다. 예를 들어 설정 중에 DNS SRV 레코드가 자동으로 생성되고 나중에 이 레코드가 자동으로 업데이트됩니다.
- IdM 서버를 설치하는 동안 글로벌 전달자를 설정하여 나머지 인터넷과 안정적으로 연결할 수 있습니다. 글로벌 전달자는 Active Directory와의 신뢰에도 유용합니다.
- 도메인의 이메일이 IdM 도메인 외부의 이메일 서버에서 스팸으로 간주되지 않도록 DNS 역방향 영역을 설정할 수 있습니다.

통합 DNS로 IdM을 설치하면 다음과 같은 몇 가지 제한 사항이 있습니다.

- IdM DNS는 범용 DNS 서버로 사용할 수 없습니다. 일부 고급 DNS 기능은 지원되지 않습니다.

이 장에서는 루트 CA로 통합된 CA(인증 기관)를 사용하여 새 IdM 서버를 설치하는 방법을 설명합니다.



참고

ipa-server-install 명령의 기본 구성은 루트 CA로 통합된 CA입니다. CA 옵션이 없는 경우(예: --external-ca 또는 --ca-less)가 지정된 경우 통합 CA와 함께 IdM 서버가 설치됩니다.

3.1. 대화형 설치

ipa-server-install 유틸리티를 사용한 대화형 설치 중에 시스템의 기본 구성(예: 영역, 관리자의 암호, Directory Manager의 암호)을 제공해야 합니다.

ipa-server-install 설치 스크립트는 /var/log/ipaserver-install.log에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

절차

1. **ipa-server-install** 유틸리티를 실행합니다.

```
# ipa-server-install
```

2. 스크립트에서 통합 **DNS** 서비스를 구성하라는 메시지가 표시됩니다. **yes** 를 입력합니다.

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

3. 이 스크립트는 몇 가지 필수 설정을 입력하라는 메시지를 표시하고 대괄호에 권장되는 기본 값을 제공합니다.

- 기본값을 허용하려면 **Enter** 를 누릅니다.
- 사용자 지정 값을 제공하려면 필요한 값을 입력합니다.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

주의

이러한 이름을 신중하게 계획하십시오. 설치가 완료된 후에는 변경할 수 없습니다.

4. **Directory Server** 슈퍼 유저(**cn=Directory Manager**)의 암호와 **IdM**(**Identity Management**) 관리 시스템 사용자 계정(**admin**)에 대해 암호를 입력합니다.

```
Directory Manager password:
IPA admin password:
```

5. 스크립트에서 서버별 **DNS** 전달자를 입력하라는 메시지를 표시합니다.

-

```
Do you want to configure DNS forwarders? [yes]:
```

- 서버별 **DNS** 전달자를 구성하려면 **yes** 를 입력한 다음 명령줄의 지침을 따릅니다. 설치 프로세스에서 **IdM LDAP**에 전달자 **IP** 주소를 추가합니다.
  - 전달 정책 기본 설정의 경우 **ipa-dns-install(1)** 도움말 페이지의 **--forward-policy** 설명을 참조하십시오.
- **DNS** 전달을 사용하지 않으려면 **no** 를 입력합니다.

DNS 전달자가 없으면 **IdM** 도메인의 호스트에서 인프라의 다른 내부 **DNS** 도메인의 이름을 확인할 수 없습니다. 호스트는 **DNS** 쿼리를 확인하기 위해 공용 **DNS** 서버에서만 유지됩니다.

6. 스크립트에서 서버와 연결된 **IP** 주소에 대한 **DNS** 역방향**(PTR)** 레코드가 구성되어 있는지 확인하라는 메시지가 표시됩니다.

```
Do you want to search for missing reverse zones? [yes]:
```

검색 및 누락된 역방향 영역을 실행하는 경우 스크립트는 **PTR** 레코드와 함께 역방향 영역을 생성할지 여부를 요청합니다.

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

참고

IdM을 사용하여 역방향 영역을 관리하는 것은 선택 사항입니다. 대신 외부 **DNS** 서비스를 사용할 수 있습니다.

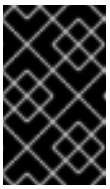
7. **yes** 를 입력하여 서버 구성을 확인합니다.

```
Continue to configure the system with these values? [no]: yes
```

8. 이제 설치 스크립트가 서버를 구성합니다. 작업이 완료될 때까지 기다립니다.

9. 설치 스크립트가 완료되면 다음과 같은 방식으로 **DNS** 레코드를 업데이트합니다.

a. 상위 도메인의 **DNS** 위임을 **IdM DNS** 도메인에 추가합니다. 예를 들어 **IdM DNS** 도메인이 ***idm.example.com*** 인 경우 **example.com** 상위 도메인에 이름 서버(**NS**) 레코드를 추가합니다.



중요

IdM DNS 서버가 설치되면 이 단계를 반복합니다.

b. 시간 서버의 **_ntp._udp** 서비스(**SRV**) 레코드를 **IdM DNS**에 추가합니다. **IdM DNS**에 새로 설치된 **IdM** 서버의 시간 서버에 **SRV** 레코드가 있으면 이 기본 **IdM** 서버에서 사용하는 시간 서버와 동기화되도록 향후 복제본 및 클라이언트 설치가 자동으로 구성됩니다.

3.2. 비대화형 설치

ipa-server-install 설치 스크립트는 **/var/log/ipaserver-install.log**에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

절차

1. 옵션을 사용하여 **ipa-server-install** 유틸리티를 실행하여 필요한 모든 정보를 제공합니다. 비대화형 설치에 필요한 최소 옵션은 다음과 같습니다.

- **--realm: Kerberos** 영역 이름을 제공합니다.
- **--ds-password:** 디렉터리 서버 슈퍼 사용자 디렉터리 관리자(**DM**)의 암호를 제공합니다.
- **--admin-password: admin, IdM(Identity Management)** 관리자의 암호를 제공합니다.
- **--unattended:** 설치 프로세스에서 호스트 이름 및 도메인 이름에 대한 기본 옵션을 선택하도록 합니다.

통합 DNS를 사용하여 서버를 설치하려면 다음 옵션도 추가합니다.

- --setup-dns: 통합 DNS를 구성
- --forwarder 또는 --no-forwarders: DNS 전달자 구성 여부에 따라 사용
- --auto-reverse 또는 --no-reverse: IdM DNS에서 생성해야 하는 역방향 DNS 영역의 자동 탐지를 구성하려는 여부에 따라 또는 역방향 영역 자동 탐지 구성 여부에 따라 기능을 설정 가능

예를 들어 다음과 같습니다.

```
# ipa-server-install --realm IDM.EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended --setup-dns --forwarder 192.0.2.1 --no-reverse
```

2. 설치 스크립트가 완료되면 다음과 같은 방식으로 DNS 레코드를 업데이트합니다.

a. 상위 도메인의 DNS 위임을 IdM DNS 도메인에 추가합니다. 예를 들어 IdM DNS 도메인이 *idm.example.com* 인 경우 example.com 상위 도메인에 이름 서버(NS) 레코드를 추가합니다.

중요

IdM DNS 서버가 설치되면 이 단계를 반복합니다.

b. 시간 서버의 _ntp._udp 서비스(SRV) 레코드를 IdM DNS에 추가합니다. IdM DNS에 새로 설치된 IdM 서버의 시간 서버에 SRV 레코드가 있으면 이 기본 IdM 서버에서 사용하는 시간 서버와 동기화되도록 향후 복제본 및 클라이언트 설치가 자동으로 구성됩니다.

추가 리소스

- ipa-server-install 에서 허용하는 전체 옵션 목록은 ipa-server-install --help 명령을 실행하십시오.

4장. IDM 서버 설치: 통합 DNS를 사용, 루트 CA로 외부 CA를 사용

통합된 DNS를 사용하여 새로운 IdM(Identity Management) 서버를 설치하는 경우 다음과 같은 이점이 있습니다.

- 네이티브 IdM 툴을 사용하여 많은 유지 관리 및 DNS 레코드 관리를 자동화할 수 있습니다. 예를 들어 설정 중에 DNS SRV 레코드가 자동으로 생성되고 나중에 이 레코드가 자동으로 업데이트됩니다.
- IdM 서버를 설치하는 동안 글로벌 전달자를 설정하여 나머지 인터넷과 안정적으로 연결할 수 있습니다. 글로벌 전달자는 Active Directory와의 신뢰에도 유용합니다.
- 도메인의 이메일이 IdM 도메인 외부의 이메일 서버에서 스팸으로 간주되지 않도록 DNS 역방향 영역을 설정할 수 있습니다.

통합 DNS로 IdM을 설치하면 다음과 같은 몇 가지 제한 사항이 있습니다.

- IdM DNS는 범용 DNS 서버로 사용할 수 없습니다. 일부 고급 DNS 기능은 지원되지 않습니다.

이 장에서는 루트 CA로 외부 CA(인증 기관)를 사용하여 새 IdM 서버를 설치하는 방법을 설명합니다.

4.1. 대화형 설치

ipa-server-install 유틸리티를 사용한 대화형 설치 중에 시스템의 기본 구성(예: 영역, 관리자의 암호, Directory Manager의 암호)을 제공해야 합니다.

ipa-server-install 설치 스크립트는 /var/log/ipaserver-install.log에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

다음 절차에서는 서버 설치 방법을 설명합니다.

- 통합 DNS

- 루트 CA로 외부 CA(인증 기관) 사용

사전 요구 사항

- 사용하는 외부 CA의 유형을 결정합니다 (--external-ca-type 옵션). 자세한 내용은 ipa-server-install(1) 매뉴얼 페이지를 참조하십시오.

- 또는 대체 AD CS(Active Directory 인증서 서비스) 템플릿을 지정할 수 있는 --external-ca-profile 옵션을 결정합니다. 예를 들어 AD CS 설치 관련 개체 식별자를 지정하려면 다음을 수행합니다.

```
[root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-
profile=1.3.6.1.4.1.311.21.8.8950086.10656446.2706058.12775672.480128.147.7130143.4405632:1
```

절차

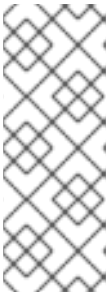
1. --external-ca 옵션을 사용하여 ipa-server-install 유틸리티를 실행합니다.

```
# ipa-server-install --external-ca
```

Microsoft Certificate Services CA를 사용하는 경우 --external-ca-type 옵션도 사용합니다. 자세한 내용은 ipa-server-install(1) 매뉴얼 페이지를 참조하십시오.

2. 스크립트에서 통합 DNS 서비스를 구성하라는 메시지가 표시됩니다. yes 또는 no를 입력합니다. 이 절차에서는 통합 DNS가 있는 서버를 설치하고 있습니다.

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```



참고

통합 DNS 없이 서버를 설치하려는 경우 아래 단계에 설명된 대로 설치 스크립트에서 DNS 구성을 요청하는 메시지를 표시하지 않습니다. DNS 없이 서버를 설치하는 단계에 대한 자세한 내용은 *6장. IdM 서버 설치: 통합 DNS 없이, 루트 CA로 통합된 CA를 포함* 을 참조하십시오.

3. 이 스크립트는 몇 가지 필수 설정을 입력하라는 메시지를 표시하고 대괄호에 권장되는 기본 값을 제공합니다.

- 기본값을 허용하려면 **Enter** 를 누릅니다.

- 사용자 지정 값을 제공하려면 필요한 값을 입력합니다.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

주의

이러한 이름을 신중하게 계획하십시오. 설치가 완료된 후에는 변경할 수 없습니다.

4. **Directory Server** 슈퍼 유저(**cn=Directory Manager**)의 암호와 **IdM**(**Identity Management**) 관리 시스템 사용자 계정(**admin**)에 대해 암호를 입력합니다.

```
Directory Manager password:
IPA admin password:
```

5. 스크립트에서 서버별 **DNS** 전달자를 입력하라는 메시지를 표시합니다.

```
Do you want to configure DNS forwarders? [yes]:
```

- 서버별 **DNS** 전달자를 구성하려면 **yes** 를 입력한 다음 명령줄의 지침을 따릅니다. 설치 프로세스에서 **IdM LDAP**에 전달자 **IP** 주소를 추가합니다.

  - 전달 정책 기본 설정의 경우 **ipa-dns-install(1)** 도움말 페이지의 **--forward-policy** 설명을 참조하십시오.

- **DNS** 전달을 사용하지 않으려면 **no** 를 입력합니다.

DNS 전달자가 없으면 **IdM** 도메인의 호스트에서 인프라의 다른 내부 **DNS** 도메인의 이

름을 확인할 수 없습니다. 호스트는 **DNS** 쿼리를 확인하기 위해 공용 **DNS** 서버에서만 유지됩니다.

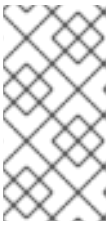
6.

스크립트에서 서버와 연결된 **IP** 주소에 대한 **DNS** 역방향**(PTR)** 레코드가 구성되어 있는지 확인하라는 메시지가 표시됩니다.

```
Do you want to search for missing reverse zones? [yes]:
```

검색 및 누락된 역방향 영역을 실행하는 경우 스크립트는 **PTR** 레코드와 함께 역방향 영역을 생성할지 여부를 요청합니다.

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```



참고

IdM을 사용하여 역방향 영역을 관리하는 것은 선택 사항입니다. 대신 외부 **DNS** 서비스를 사용할 수 있습니다.

7.

yes 를 입력하여 서버 구성을 확인합니다.

```
Continue to configure the system with these values? [no]: yes
```

8.

인증서 시스템 인스턴스를 구성하는 동안 유틸리티는 인증서 서명 요청**(CSR): /root/ipa.csr:**

```
...

Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
  [1/8]: creating certificate server user
  [2/8]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-install as:
/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
```

이 경우**:**

a.

/root/ipa.csr에 있는 **CSR**을 외부 **CA**에 제출합니다. 이 프로세스는 외부 **CA**로 사용할 서비스에 따라 다릅니다.

b.

기본 64로 인코딩된 Blob(Windows CA의 PEM 파일 또는 Base_64 인증서)에서 발급한 인증서와 CA의 CA 인증서 체인을 검색합니다. 다시 말하지만, 프로세스는 모든 인증서 서비스에 따라 다릅니다. 일반적으로 웹 페이지 또는 알림 이메일의 다운로드 링크를 사용하면 관리자가 필요한 모든 인증서를 다운로드할 수 있습니다.

중요

CA 인증서뿐만 아니라 CA의 전체 인증서 체인을 가져옵니다.

c.

ipa-server-install을 다시 실행합니다. 이번에는 새로 발급한 CA 인증서와 CA 체인 파일의 위치 및 이름을 지정합니다. 예를 들어 다음과 같습니다.

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-file=/tmp/cacert.pem
```

9.

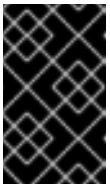
이제 설치 스크립트가 서버를 구성합니다. 작업이 완료될 때까지 기다립니다.

10.

설치 스크립트가 완료되면 다음과 같은 방식으로 DNS 레코드를 업데이트합니다.

a.

상위 도메인의 DNS 위임을 IdM DNS 도메인에 추가합니다. 예를 들어 IdM DNS 도메인이 *idm.example.com* 인 경우 example.com 상위 도메인에 이름 서버(NS) 레코드를 추가합니다.

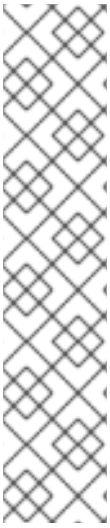


중요

IdM DNS 서버가 설치되면 이 단계를 반복합니다.

b.

시간 서버의 _ntp._udp 서비스(SRV) 레코드를 IdM DNS에 추가합니다. IdM DNS에 새로 설치된 IdM 서버의 시간 서버에 SRV 레코드가 있으면 이 기본 IdM 서버에서 사용하는 시간 서버와 동기화되도록 향후 복제본 및 클라이언트 설치가 자동으로 구성됩니다.



참고

ipa-server-install --external-ca 명령은 다음 오류로 인해 실패하는 경우가 있습니다.

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s
CA -f /tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

이 오류는 ***_proxy** 환경 변수가 설정될 때 발생합니다. 이 문제의 해결 방법은 **Troubleshooting: 외부 CA 설치에 실패**에서 참조하십시오.

4.2. 문제 해결: 외부 CA 설치에 실패

ipa-server-install --external-ca 명령은 다음 오류와 함께 실패합니다.

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f
/tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

env|grep proxy 명령은 다음과 같은 변수를 표시합니다.

```
# env|grep proxy
http_proxy=http://example.com:8080
ftp_proxy=http://example.com:8080
https_proxy=http://example.com:8080
```

이는 다음을 의미합니다.

***_proxy** 환경 변수를 사용하면 서버가 설치되지 않습니다.

문제를 해결하려면 다음을 수행합니다.

1. 다음 쉘 스크립트를 사용하여 ***_proxy** 환경 변수를 설정 해제합니다.

```
# for i in ftp http https; do unset ${i}_proxy; done
```

2. **pkidestroy** 유틸리티를 실행하여 실패한 **CA**(인증 기관) 하위 시스템 설치를 제거합니다.

```
# pkidestroy -s CA -i pki-tomcat; rm -rf /var/log/pki/pki-tomcat /etc/sysconfig/pki-
tomcat /etc/sysconfig/pki/tomcat/pki-tomcat /var/lib/pki/pki-tomcat /etc/pki/pki-tomcat
/root/ipa.csr
```

3. 실패한 **IdM(Identity Management)** 서버 설치를 제거합니다.

```
# ipa-server-install --uninstall
```

4. **ipa-server-install --external-ca** 를 실행합니다.

5장. IDM 서버 설치: CA 없이 통합된 DNS 사용

통합된 DNS를 사용하여 새로운 IdM(Identity Management) 서버를 설치하는 경우 다음과 같은 이점이 있습니다.

- 네이티브 IdM 툴을 사용하여 많은 유지 관리 및 DNS 레코드 관리를 자동화할 수 있습니다. 예를 들어 설정 중에 DNS SRV 레코드가 자동으로 생성되고 나중에 이 레코드가 자동으로 업데이트됩니다.
- IdM 서버를 설치하는 동안 글로벌 전달자를 설정하여 나머지 인터넷과 안정적으로 연결할 수 있습니다. 글로벌 전달자는 Active Directory와의 신뢰에도 유용합니다.
- 도메인의 이메일이 IdM 도메인 외부의 이메일 서버에서 스팸으로 간주되지 않도록 DNS 역방향 영역을 설정할 수 있습니다.

통합 DNS로 IdM을 설치하면 다음과 같은 몇 가지 제한 사항이 있습니다.

- IdM DNS는 범용 DNS 서버로 사용할 수 없습니다. 일부 고급 DNS 기능은 지원되지 않습니다.

이 장에서는 CA(인증 기관) 없이 새 IdM 서버를 설치하는 방법을 설명합니다.

5.1. CA 없이 IDM 서버를 설치하는 데 필요한 인증서

이 섹션에는 CA(인증 기관) 없이 IdM(Identity Management) 서버를 설치하는 데 필요한 인증서 및 이러한 인증서를 ipa-server-install 유틸리티에 제공하는 데 사용되는 명령줄 옵션이 나열되어 있습니다.

중요

가져온 인증서 파일에는 LDAP 및 Apache 서버 인증서를 발급한 CA의 전체 CA 인증서 체인이 포함되어야 하므로 자체 서명된 타사 서버 인증서를 사용하여 서버 또는 복제본을 설치할 수 없습니다.

LDAP 서버 인증서 및 개인 키

- 인증서의 --dirsrv-cert-file 및 LDAP 서버 인증서에 대한 개인 키 파일

- --dirsrv-cert-file에 지정된 파일의 개인 키에 액세스하기 위한 암호의 --dirsrv-pin

Apache 서버 인증서 및 개인 키

- 인증서 및 개인 키 파일의 --HTTP-cert-file - Apache 서버 인증서

- --http-cert-file 에 지정된 파일에서 개인 키에 액세스하기 위한 --HTTP-pin

LDAP 및 Apache 서버 인증서를 발급한 CA의 전체 CA 인증서 체인

- 전체 CA 인증서 체인 또는 그 일부의 인증서 파일의 --dirsrv-cert-file 및 --http-cert-file

다음 형식으로 --dirsrv-cert-file 및 --http-cert-file 옵션에 지정된 파일을 제공할 수 있습니다.

- 개인 정보 보호 메일 (PEM) 인코딩 인증서 (RFC 7468). Identity Management 설치 프로그램에서는 연결된 PEM 인코딩 오브젝트를 허용합니다.

- 구분 인코딩 규칙(DER)

- PKCS #7 인증서 체인 오브젝트

- PKCS #8 개인 키 오브젝트

- PKCS #12 아카이브

--dirsrv-cert-file 및 --http-cert-file 옵션을 여러 번 지정하여 여러 파일을 지정할 수 있습니다.

전체 CA 인증서 체인을 완료하는 인증서 파일 (일부 환경에서는 필요하지 않음)

- --CA-cert-file: LDAP, Apache Server 및 Kerberos NetNamespace 인증서를 발급한 CA의 CA 인증서가 포함된 파일 또는 파일에 대한 --CA-cert-file 다른 옵션에서 제공하는 인

증서 파일에 CA 인증서가 없는 경우 이 옵션을 사용합니다.

--dirsrv-cert-file 및 --http-cert-file 을 사용하여 제공하는 파일과 함께 제공되는 파일에 는 LDAP 및 Apache 서버 인증서를 발급한 CA의 전체 CA 인증서 체인이 포함되어야 합니다.

Kerberos 키 배포 센터 (KDC) PKINIT 인증서 및 개인 키 (선택 사항)

- --PKINIT-cert-file for the Kerberos자리 SSL 인증서 및 개인 키
- --pkinit-cert-file 에 지정된 파일에서 Kerberos자리 개인 키에 액세스하기 위한 비밀번호 --PKINIT-pin
- pkinit 설정 단계를 비활성화하는 --no-pkinit

PKINIT 인증서를 제공하지 않으면 ipa-server-install 은 자체 서명된 인증서를 사용하여 로컬 NetNamespace로 IdM 서버를 구성합니다.

추가 리소스

- 이러한 옵션을 지정하는 인증서 파일이 적용되는 방법에 대한 자세한 내용은 ipa-server-install(1) 매뉴얼 페이지를 참조하십시오.
- RHEL IdM PKINIT 인증서를 생성하는 데 필요한 PKINIT 확장 기능에 대한 자세한 내용은 이 문서 를 참조하십시오.

5.2. 대화형 설치

ipa-server-install 유틸리티를 사용한 대화형 설치 중에 시스템의 기본 구성(예: 영역, 관리자의 암호, Directory Manager의 암호)을 제공해야 합니다.

ipa-server-install 설치 스크립트는 /var/log/ipaserver-install.log에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

절차

1. **ipa-server-install** 유틸리티를 실행하고 필요한 모든 인증서를 제공합니다. 예를 들어 다음과 같습니다.

```
[root@server ~]# ipa-server-install \
   --http-cert-file /tmp/server.crt \
   --http-cert-file /tmp/server.key \
   --http-pin secret \
   --dirsrv-cert-file /tmp/server.crt \
   --dirsrv-cert-file /tmp/server.key \
   --dirsrv-pin secret \
   --ca-cert-file ca.crt
```

제공된 인증서에 대한 자세한 내용은 **CA 없이 IdM 서버를 설치하는 데 필요한 인증서** 를 참조하십시오.

2. 스크립트에서 통합 **DNS** 서비스를 구성하라는 메시지가 표시됩니다. **yes** 또는 **no**를 입력합니다. 이 절차에서는 통합 **DNS**가 있는 서버를 설치하고 있습니다.

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

참고

통합 **DNS** 없이 서버를 설치하려는 경우 아래 단계에 설명된 대로 설치 스크립트에서 **DNS** 구성을 요청하는 메시지를 표시하지 않습니다. **IdM 서버 설치를 참조하십시오. DNS를 통합하지 않고 루트 CA로 통합 CA가 있는 경우 DNS** 없이 서버를 설치하는 단계에 대한 세부 사항.

3. 이 스크립트는 몇 가지 필수 설정을 입력하라는 메시지를 표시하고 대괄호에 권장되는 기본값을 제공합니다.

- 기본값을 허용하려면 **Enter** 를 누릅니다.
- 사용자 지정 값을 제공하려면 필요한 값을 입력합니다.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

주의

이러한 이름을 신중하게 계획하십시오. 설치가 완료된 후에는 변경할 수 없습니다.

4. **Directory Server** 슈퍼 유저**(cn=Directory Manager)**의 암호와 **IdM(Identity Management)** 관리 시스템 사용자 계정**(admin)**에 대해 암호를 입력합니다.

```
Directory Manager password:
IPA admin password:
```

5. 스크립트에서 서버별 **DNS** 전달자를 입력하라는 메시지를 표시합니다.

```
Do you want to configure DNS forwarders? [yes]:
```

- 서버별 **DNS** 전달자를 구성하려면 **yes** 를 입력한 다음 명령줄의 지침을 따릅니다. 설치 프로세스에서 **IdM LDAP**에 전달자 **IP** 주소를 추가합니다.
  - 전달 정책 기본 설정의 경우 **ipa-dns-install(1)** 도움말 페이지의 **--forward-policy** 설명을 참조하십시오.
- **DNS** 전달을 사용하지 않으려면 **no** 를 입력합니다.

DNS 전달자가 없으면 **IdM** 도메인의 호스트에서 인프라의 다른 내부 **DNS** 도메인의 이름을 확인할 수 없습니다. 호스트는 **DNS** 쿼리를 확인하기 위해 공용 **DNS** 서버에서만 유지됩니다.

6. 스크립트에서 서버와 연결된 **IP** 주소에 대한 **DNS** 역방향**(PTR)** 레코드가 구성되어 있는지 확인하라는 메시지가 표시됩니다.

```
Do you want to search for missing reverse zones? [yes]:
```

검색 및 누락된 역방향 영역을 실행하는 경우 스크립트는 **PTR** 레코드와 함께 역방향 영역을 생성할지 여부를 요청합니다.

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

참고

IdM을 사용하여 역방향 영역을 관리하는 것은 선택 사항입니다. 대신 외부 **DNS** 서비스를 사용할 수 있습니다.

7. **yes** 를 입력하여 서버 구성을 확인합니다.

```
Continue to configure the system with these values? [no]: yes
```

8. 이제 설치 스크립트가 서버를 구성합니다. 작업이 완료될 때까지 기다립니다.

9. 설치 스크립트가 완료되면 다음과 같은 방식으로 **DNS** 레코드를 업데이트합니다.

a. 상위 도메인의 **DNS** 위임을 **IdM DNS** 도메인에 추가합니다. 예를 들어 **IdM DNS** 도메인이 ***idm.example.com*** 인 경우 **example.com** 상위 도메인에 이름 서버(**NS**) 레코드를 추가합니다.

중요

IdM DNS 서버가 설치되면 이 단계를 반복합니다.

b. 시간 서버의 **_ntp._udp** 서비스(**SRV**) 레코드를 **IdM DNS**에 추가합니다. **IdM DNS**에 새로 설치된 **IdM** 서버의 시간 서버에 **SRV** 레코드가 있으면 이 기본 **IdM** 서버에서 사용하는 시간 서버와 동기화되도록 향후 복제본 및 클라이언트 설치가 자동으로 구성됩니다.

6장. IDM 서버 설치: 통합 DNS 없이, 루트 CA로 통합된 CA를 포함

이 장에서는 통합 DNS 없이 새로운 IdM(Identity Management) 서버를 설치하는 방법을 설명합니다.

참고

Red Hat은 IdM 배포 내의 기본 사용을 위해 IdM 통합 DNS를 설치하는 것이 좋습니다. IdM 서버는 DNS도 관리하는 경우 일부 DNS 레코드 관리를 자동화할 수 있는 DNS와 네이티브 IdM 툴 간에 긴밀하게 통합됩니다.

자세한 내용은 DNS 서비스 및 호스트 이름 계획을 참조하십시오.

6.1. 대화형 설치

ipa-server-install 유틸리티를 사용한 대화형 설치 중에 시스템의 기본 구성(예: 영역, 관리자의 암호, Directory Manager의 암호)을 제공해야 합니다.

ipa-server-install 설치 스크립트는 /var/log/ipaserver-install.log에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

다음 절차에서는 서버를 설치합니다.

- 통합 DNS 없음
- 기본 CA인 루트 CA(Integrated Identity Management) 인증 기관(CA)을 사용하는 경우

절차

1. ipa-server-install 유틸리티를 실행합니다.

```
# ipa-server-install
```

2. 스크립트에서 통합 DNS 서비스를 구성하라는 메시지가 표시됩니다. Enter 를 눌러 기본 no 옵션을 선택합니다.

```
Do you want to configure integrated DNS (BIND)? [no]:
```

3. 이 스크립트는 몇 가지 필수 설정을 입력하라는 메시지를 표시하고 대괄호에 권장되는 기본 값을 제공합니다.

- 기본값을 허용하려면 **Enter** 를 누릅니다.
- 사용자 지정 값을 제공하려면 필요한 값을 입력합니다.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

주의

이러한 이름을 신중하게 계획하십시오. 설치가 완료된 후에는 변경할 수 없습니다.

4. **Directory Server superuser(cn=Directory Manager)**의 암호와 **IdM** 관리 시스템 사용자 계정(관리자)을 입력합니다.

```
Directory Manager password:
IPA admin password:
```

5. **yes** 를 입력하여 서버 구성을 확인합니다.

```
Continue to configure the system with these values? [no]: yes
```

6. 이제 설치 스크립트가 서버를 구성합니다. 작업이 완료될 때까지 기다립니다.

7. 설치 스크립트는 **DNS** 리소스 레코드가 있는 파일을 생성합니다. **/tmp/ipa.system.records.UFRPto.db** 파일은 아래 예제 출력에 있습니다. 이러한 레코드를 기존

외부 DNS 서버에 추가합니다. DNS 레코드를 업데이트하는 프로세스는 특정 DNS 솔루션에 따라 다릅니다.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

중요

기존 DNS 서버에 DNS 레코드를 추가할 때까지 서버 설치가 완료되지 않습니다.

추가 리소스

- DNS 시스템에 추가해야 하는 DNS 리소스 레코드에 대한 자세한 내용은 외부 DNS 시스템의 IdM DNS 레코드를 참조하십시오.

6.2. 비대화형 설치

이 절차에서는 통합 DNS 또는 통합 IdM(Identity Management) 인증 기관(CA)을 기본 CA인 루트 CA로 설치하지 않은 서버를 설치합니다.

참고

ipa-server-install 설치 스크립트는 /var/log/ipaserver-install.log에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

절차

1. 옵션을 사용하여 ipa-server-install 유틸리티를 실행하여 필요한 모든 정보를 제공합니다. 비대화형 설치에 필요한 최소 옵션은 다음과 같습니다.

   - --realm: Kerberos 영역 이름을 제공합니다.
   - --ds-password: 디렉터리 서버 슈퍼 사용자 디렉터리 관리자(DM)의 암호를 제공합니다.

- **--admin-password:** IdM 관리자인 **admin**의 암호를 제공합니다.

- **--unattended:** 설치 프로세스에서 호스트 이름 및 도메인 이름에 대한 기본 옵션을 선택하도록 합니다.

예를 들어 다음과 같습니다.

```
# ipa-server-install --realm IDM.EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended
```

2. 설치 스크립트는 **DNS** 리소스 레코드가 있는 파일을 생성합니다. **/tmp/ipa.system.records.UFRPto.db** 파일은 아래 예제 출력에 있습니다. 이러한 레코드를 기존 외부 **DNS** 서버에 추가합니다. **DNS** 레코드를 업데이트하는 프로세스는 특정 **DNS** 솔루션에 따라 다릅니다.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

중요

기존 **DNS** 서버에 **DNS** 레코드를 추가할 때까지 서버 설치가 완료되지 않습니다.

추가 리소스

- **DNS** 시스템에 추가해야 하는 **DNS** 리소스 레코드에 대한 자세한 내용은 외부 **DNS** 시스템의 **IdM DNS** 레코드를 참조하십시오.

- **ipa-server-install** 에서 허용하는 전체 옵션 목록은 **ipa-server-install --help** 명령을 실행하십시오.

6.3. 외부 DNS 시스템의 IDM DNS 레코드

통합 **DNS** 없이 **IdM** 서버를 설치한 후 **IdM** 서버의 **LDAP** 및 **Kerberos DNS** 리소스 레코드를 외부 **DNS** 시스템에 추가해야 합니다.

ipa-server-install 설치 스크립트는 **/tmp/ipa.system. historys. <*random_characters*> .db** 형식의 파일 이름을 사용하여 **DNS** 리소스 레코드 목록을 포함하는 파일을 생성하고 해당 레코드를 추가하는 명령을 출력합니다.

```
Please add records in this file to your DNS system: /tmp/ipa.system.records.6zdjqxh3.db
```

다음은 파일의 내용입니다.

```
_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.
```

참고

IdM 서버의 **LDAP** 및 **Kerberos DNS** 리소스 레코드를 **DNS** 시스템에 추가한 후 **ipa-ca** 용으로 **DNS** 관리 도구가 **PTR** 레코드를 추가하지 않았는지 확인합니다. **DNS**에 **ipa-ca**에 대한 **PTR** 레코드가 있으면 후속 **IdM** 복제본 설치가 실패할 수 있습니다.

7장. IDM 서버 설치: 루트 CA로 외부 CA가 있는 통합 DNS 없음

이 장에서는 외부 CA(인증 기관)를 루트 CA로 사용하는 통합 DNS 없이 새로운 IdM(Identity Management) 서버를 설치하는 방법을 설명합니다.

참고

Red Hat은 IdM 배포 내의 기본 사용을 위해 IdM 통합 DNS를 설치하는 것이 좋습니다. IdM 서버는 DNS도 관리하는 경우 일부 DNS 레코드 관리를 자동화할 수 있는 DNS와 네이티브 IdM 툴 간에 긴밀하게 통합됩니다.

자세한 내용은 DNS 서비스 및 호스트 이름 계획을 참조하십시오.

7.1. 외부 CA가 있는 IDM CA를 루트 CA로 설치할 때 사용되는 옵션

다음 조건 중 하나가 적용되는 경우 외부 CA가 있는 IdM 인증 기관(CA)을 루트 CA로 설치할 수 있습니다.

- ipa-server-install 명령을 사용하여 새 IdM 서버 또는 복제본을 설치하고 있습니다.
- ipa-ca-install 명령을 사용하여 기존 IdM 서버에 CA 구성 요소를 설치하고 있습니다.

이 섹션에서는 루트 CA를 루트 CA와 함께 IdM CA를 설치하는 동안 CSR(인증서 서명 요청)을 생성하는 데 사용할 수 있는 두 명령의 옵션에 대해 설명합니다.

--external-ca-type=*TYPE*

외부 CA의 유형입니다. 가능한 값은 *generic* 및 *ms-cs* 입니다. 기본값은 *generic* 입니다. 생성된 CSR에 MS CS(Microsoft Certificate Services)에 필요한 템플릿 이름을 포함하려면 *ms-cs* 를 사용합니다. 기본이 아닌 프로필을 사용하려면 **--external-ca-type=ms-cs** 와 함께 **--external-ca-profile** 옵션을 사용합니다.

--external-ca-profile=*PROFILE_SPEC*

IdM CA의 인증서를 발행할 때 MS CS를 적용할 인증서 프로필 또는 템플릿을 지정합니다.

--external-ca-profile 옵션은 **--external-ca-type** 이 **ms-cs**인 경우에만 사용할 수 있습니다.

다음 방법 중 하나로 **MS CS** 템플릿을 식별할 수 있습니다.

- ***<oid>:<majorVersion>[:<minorVersion>]***. 인증서 템플릿을 **OID**(오브젝트 **ID**) 및 주요 버전으로 지정할 수 있습니다. 선택적으로 마이너 버전을 지정할 수도 있습니다.

- ***<name>***. 인증서 템플릿을 이름으로 지정할 수 있습니다. **name**은 **:** 문자를 포함할 수 없으며 **OID**가 될 수 없으며, 그렇지 않으면 **OID** 기반 템플릿 설치자 구문이 우선합니다.

- ***default***. 이 지정자를 사용하는 경우 템플릿 이름 ***SubCA*** 가 사용됩니다.

특정 시나리오에서 **AD(Active Directory)** 관리자는 **AD CS**의 내장 템플릿인 **Subordinate Certification Authority (SCA)** 템플릿을 사용하여 조직의 요구 사항에 맞게 고유한 템플릿을 만들 수 있습니다. 예를 들어 새 템플릿에는 사용자 지정된 유효 기간이 있고 사용자 지정된 확장 기능이 있을 수 있습니다. 연결된 **OID**(오브젝트 식별자)는 **AD** 인증서 템플릿 콘솔에서 확인할 수 있습니다.

AD 관리자가 원래의 기본 제공 템플릿을 비활성화한 경우 **IdM CA**의 인증서를 요청할 때 **OID** 또는 새 템플릿의 이름을 지정해야 합니다. **AD** 관리자에게 새 템플릿의 이름 또는 **OID**를 제공하도록 요청합니다.

원래 **SCA AD CS** 템플릿이 여전히 활성화되어 있는 경우 **--external-ca-type=ms-cs** 옵션을 추가로 사용하지 않고 **--external-ca-type=ms - cs** 를 지정하여 사용할 수 있습니다. 이 경우 **subCA** 외부 **CA** 프로필이 사용됩니다. 이 프로필은 **SCA AD CS** 템플릿에 해당하는 기본 **IdM** 템플릿입니다.

7.2. 대화형 설치

ipa-server-install 유틸리티를 사용한 대화형 설치 중에 시스템의 기본 구성(예: 영역, 관리자의 암호, **Directory Manager**의 암호)을 제공해야 합니다.

ipa-server-install 설치 스크립트는 **/var/log/ipaserver-install.log**에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

다음 절차에서는 서버 설치 방법을 설명합니다.

- 통합 **DNS** 없음

- 루트 CA로 외부 CA(인증 기관) 사용

절차

1. --external-ca 옵션을 사용하여 ipa-server-install 유틸리티를 실행합니다.

   - MS CS(Microsoft 인증서 서비스) CA를 사용하는 경우 --external-ca-type 및 --external-ca-profile 옵션도 사용합니다. 예를 들어 1.3.6.1.4.1.311.21.8.8950086.10656446.2706058.12775672.480128.147.7130143.4405632:1 Object Identifier(OID) 템플릿을 사용하여 서명 인증서를 발급된 CA와 함께 IdM 서버를 설치하려면 다음을 실행합니다.

     ```
     [root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-profile=1.3.6.1.4.1.311.21.8.8950086.10656446.2706058.12775672.480128.147.7130143.4405632:1
     ```

     --external-ca-type 및 --external-ca-profile 옵션에 대한 자세한 내용은 외부 CA를 루트 CA로 사용하여 IdM CA를 설치할 때 사용되는 옵션을 참조하십시오.

   - IdM CA의 서명 인증서를 생성하는 데 MS CS를 사용하지 않는 경우 다른 옵션이 필요하지 않을 수 있습니다.

     ```
     # ipa-server-install --external-ca
     ```

2. 스크립트에서 통합 DNS 서비스를 구성하라는 메시지가 표시됩니다. Enter 를 눌러 기본 no 옵션을 선택합니다.

   ```
   Do you want to configure integrated DNS (BIND)? [no]:
   ```

3. 이 스크립트는 몇 가지 필수 설정을 입력하라는 메시지를 표시하고 대괄호에 권장되는 기본 값을 제공합니다.

   - 기본값을 허용하려면 Enter 를 누릅니다.
   - 사용자 지정 값을 제공하려면 필요한 값을 입력합니다.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

주의

이러한 이름을 신중하게 계획하십시오. 설치가 완료된 후에는 변경할 수 없습니다.

4. Directory Server superuser(cn=Directory Manager)의 암호와 IdM 관리 시스템 사용자 계정(관리자)을 입력합니다.

```
Directory Manager password:
IPA admin password:
```

5. yes 를 입력하여 서버 구성을 확인합니다.

```
Continue to configure the system with these values? [no]: yes
```

6. 인증서 시스템 인스턴스를 구성하는 동안 유틸리티는 인증서 서명 요청(CSR): /root/ipa.csr:

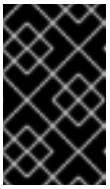
```
...

Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
  [1/8]: creating certificate server user
  [2/8]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-
install as:
/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
```

이 경우:

a. /root/ipa.csr에 있는 CSR을 외부 CA에 제출합니다. 이 프로세스는 외부 CA로 사용할 서비스에 따라 다릅니다.

b.

기본 64로 인코딩된 Blob(Windows CA의 PEM 파일 또는 Base_64 인증서)에서 발급한 인증서와 CA의 CA 인증서 체인을 검색합니다. 다시 말하지만, 프로세스는 모든 인증서 서비스에 따라 다릅니다. 일반적으로 웹 페이지 또는 알림 이메일의 다운로드 링크를 사용하면 관리자가 필요한 모든 인증서를 다운로드할 수 있습니다.



중요

CA 인증서뿐만 아니라 CA의 전체 인증서 체인을 가져옵니다.

c. ipa-server-install을 다시 실행합니다. 이번에는 새로 발급한 CA 인증서와 CA 체인 파일의 위치 및 이름을 지정합니다. 예를 들어 다음과 같습니다.

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-
cert-file=/tmp/cacert.pem
```

7. 이제 설치 스크립트가 서버를 구성합니다. 작업이 완료될 때까지 기다립니다.

8. 설치 스크립트는 DNS 리소스 레코드가 있는 파일을 생성합니다. /tmp/ipa.system.records.UFRPto.db 파일은 아래 예제 출력에 있습니다. 이러한 레코드를 기존 외부 DNS 서버에 추가합니다. DNS 레코드를 업데이트하는 프로세스는 특정 DNS 솔루션에 따라 다릅니다.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

중요

기존 DNS 서버에 DNS 레코드를 추가할 때까지 서버 설치가 완료되지 않습니다.

추가 리소스

- DNS 시스템에 추가해야 하는 DNS 리소스 레코드에 대한 자세한 내용은 외부 DNS 시스템의 IdM DNS 레코드를 참조하십시오.

- **ipa-server-install --external-ca** 명령은 다음 오류로 인해 실패하는 경우가 있습니다.

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s
CA -f /tmp/pass:quotes[configuration_file]' returned non-zero exit status 1
Configuration of CA failed
```

이 오류는 ***_proxy** 환경 변수가 설정될 때 발생합니다. 이 문제의 해결 방법은 Troubleshooting: 외부 CA 설치에 실패에서 참조하십시오.

7.3. 비대화형 설치

다음 절차에서는 서버를 설치합니다.

- 통합 DNS 없음
- 루트 CA로 외부 CA(인증 기관) 사용

참고

ipa-server-install 설치 스크립트는 **/var/log/ipaserver-install.log**에 로그 파일을 생성합니다. 설치에 실패하면 로그를 통해 문제를 식별하는 데 도움이 될 수 있습니다.

사전 요구 사항

- 사용하는 외부 CA의 유형을 결정합니다 (**--external-ca-type** 옵션). 자세한 내용은 **ipa-server-install(1)** 매뉴얼 페이지를 참조하십시오.
- 또는 대체 AD CS(Active Directory 인증서 서비스) 템플릿을 지정할 수 있는 **--external-ca-profile** 옵션을 결정합니다. 예를 들어 AD CS 설치 관련 개체 식별자를 지정하려면 다음을 수행합니다.

```
[root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-
ca-
profile=1.3.6.1.4.1.311.21.8.8950086.10656446.2706058.12775672.480128.147.7130143.44
05632:1
```

절차

1. 옵션을 사용하여 **ipa-server-install** 유틸리티를 실행하여 필요한 모든 정보를 제공합니다. 루트 **CA**로 외부 **CA**를 사용하여 **IdM** 서버를 비대화형 설치에 필요한 최소 옵션은 다음과 같습니다.

   - 외부 **CA**를 지정하는 **--external-ca** 는 루트 **CA**입니다.
   - **--realm: Kerberos** 영역 이름을 제공합니다.
   - **--ds-password:** 디렉터리 서버 슈퍼 사용자 디렉터리 관리자**(DM)**의 암호를 제공합니다.
   - **--admin-password: IdM** 관리자인 **admin**의 암호를 제공합니다.
   - **--unattended:** 설치 프로세스에서 호스트 이름 및 도메인 이름에 대한 기본 옵션을 선택하도록 합니다.

   예를 들어 다음과 같습니다.

   ```
   # ipa-server-install --external-ca --realm IDM.EXAMPLE.COM --ds-password
   DM_password --admin-password admin_password --unattended
   ```

   Microsoft Certificate Services CA를 사용하는 경우 **--external-ca-type** 옵션도 사용합니다. 자세한 내용은 **ipa-server-install(1)** 매뉴얼 페이지를 참조하십시오.

2. 인증서 시스템 인스턴스를 구성하는 동안 유틸리티는 인증서 서명 요청**(CSR): /root/ipa.csr:**

   ```
   ...

   Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes
     [1/11]: configuring certificate server instance
   The next step is to get /root/ipa.csr signed by your CA and re-run /usr/sbin/ipa-server-
   install as:
   /usr/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-
   cert-file=/path/to/external_ca_certificate
   The ipa-server-install command was successful
   ```

   이 경우:

a.

/root/ipa.csr에 있는 CSR을 외부 CA에 제출합니다. 이 프로세스는 외부 CA로 사용할 서비스에 따라 다릅니다.

b.

기본 64로 인코딩된 Blob(Windows CA의 PEM 파일 또는 Base_64 인증서)에서 발급한 인증서와 CA의 CA 인증서 체인을 검색합니다. 다시 말하지만, 프로세스는 모든 인증서 서비스에 따라 다릅니다. 일반적으로 웹 페이지 또는 알림 이메일의 다운로드 링크를 사용하면 관리자가 필요한 모든 인증서를 다운로드할 수 있습니다.

중요

CA 인증서뿐만 아니라 CA의 전체 인증서 체인을 가져옵니다.

c.

ipa-server-install을 다시 실행합니다. 이번에는 새로 발급한 CA 인증서와 CA 체인 파일의 위치 및 이름을 지정합니다. 예를 들어 다음과 같습니다.

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-
cert-file=/tmp/cacert.pem --realm IDM.EXAMPLE.COM --ds-password
DM_password --admin-password admin_password --unattended
```

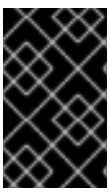
3.

이제 설치 스크립트가 서버를 구성합니다. 작업이 완료될 때까지 기다립니다.

4.

설치 스크립트는 DNS 리소스 레코드가 있는 파일을 생성합니다. /tmp/ipa.system.records.UFRPto.db 파일은 아래 예제 출력에 있습니다. 이러한 레코드를 기존 외부 DNS 서버에 추가합니다. DNS 레코드를 업데이트하는 프로세스는 특정 DNS 솔루션에 따라 다릅니다.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



중요

기존 DNS 서버에 DNS 레코드를 추가할 때까지 서버 설치가 완료되지 않습니다.

추가 리소스

-

DNS 시스템에 추가해야 하는 DNS 리소스 레코드에 대한 자세한 내용은 외부 DNS 시스템의 IdM DNS 레코드를 참조하십시오.

7.4. 외부 DNS 시스템의 IDM DNS 레코드

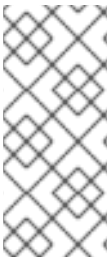
통합 DNS 없이 IdM 서버를 설치한 후 IdM 서버의 LDAP 및 Kerberos DNS 리소스 레코드를 외부 DNS 시스템에 추가해야 합니다.

ipa-server-install 설치 스크립트는 /tmp/ipa.system. historys. *<random_characters>* .db 형식의 파일 이름을 사용하여 DNS 리소스 레코드 목록을 포함하는 파일을 생성하고 해당 레코드를 추가하는 명령을 출력합니다.

```
Please add records in this file to your DNS system: /tmp/ipa.system.records.6zdjqxh3.db
```

다음은 파일의 내용입니다.

```
_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.
```



참고

IdM 서버의 LDAP 및 Kerberos DNS 리소스 레코드를 DNS 시스템에 추가한 후 ipa-ca 용으로 DNS 관리 도구가 PTR 레코드를 추가하지 않았는지 확인합니다. DNS에 ipa-ca에 대한 PTR 레코드가 있으면 후속 IdM 복제본 설치가 실패할 수 있습니다.

8장. LDIF 파일에서 사용자 지정 데이터베이스 설정을 사용하여 IDM 서버 또는 복제본 설치

Directory Server 데이터베이스의 사용자 지정 설정을 사용하여 IdM 서버 및 IdM 복제본을 설치할 수 있습니다. 다음 절차에서는 데이터베이스 설정을 사용하여 LDAP Data Interchange Format(LDIF) 파일을 생성하는 방법과 이러한 설정을 IdM 서버 및 복제본 설치 명령에 전달하는 방법을 보여줍니다.

사전 요구 사항

- IdM 환경의 성능을 향상시키는 사용자 정의 Directory Server 설정을 확인했습니다. IdM 디렉터리 서버 성능 조정을 참조하십시오.

절차

1. 사용자 지정 데이터베이스 설정으로 LDIF 형식으로 텍스트 파일을 만듭니다. 대시(-)를 사용하여 LDAP 특성을 별도로 수정합니다. 이 예에서는 유휴 시간 제한 및 최대 파일 설명자에 기본값이 아닌 값을 설정합니다.

```
dn: cn=config
changetype: modify
replace: nsslapd-idletimeout
nsslapd-idletimeout=1800
-
replace: nsslapd-maxdescriptors
nsslapd-maxdescriptors=8192
```

2. --dirsrv-config-file 매개변수를 사용하여 LDIF 파일을 설치 스크립트에 전달합니다.

   a. IdM 서버를 설치하려면 다음을 수행합니다.

   ```
   # ipa-server-install --dirsrv-config-file filename.ldif
   ```

   b. IdM 복제본을 설치하려면 다음을 수행합니다.

   ```
   # ipa-replica-install --dirsrv-config-file filename.ldif
   ```

추가 리소스

- ipa-server-install 및 ipa-replica-install 명령에 대한 옵션

9장. IPA-SERVER-INSTALL 및 IPA-REPLICA-INSTALL 명령에 대한 옵션

ipa-server-install 및 ipa-replica-install 명령에는 대화형 설치 중에 요청되지 않은 추가 정보를 제공하는 데 사용할 수 있는 다양한 인수가 있습니다. 이러한 옵션을 사용하여 자동 설치를 스크립팅할 수도 있습니다. 다음 표에는 가장 일반적인 몇 가지 옵션이 표시되어 있습니다. 전체 옵션 목록은 ipa-server-install(1) 및 ipa-replica-install(1) 매뉴얼 페이지를 참조하십시오.

표 9.1. ipa-server-install 및 ipa-replica-install 명령에 대한 옵션

인수	설명
-a *<ipa_admin_password>*	Kerberos 영역에 인증하기 위한 **admin** IdM 관리자 계정의 암호입니다.
-d, --debug	보다 자세한 출력을 위해 디버그 로깅을 활성화합니다.
--dirsrv-config-file *<LDIF_file_name>*	디렉터리 서버 인스턴스의 구성을 수정하는 데 사용되는 LDIF 파일의 경로입니다.
--hostname=*server.idm.example.com*	IdM 서버 시스템의 정규화된 도메인 이름입니다. 숫자, 소문자 영문자, 하이픈(-)만 허용됩니다.
--idmax=*<number>*	IdM 서버에서 할당할 수 있는 ID의 상한을 설정합니다. 기본값은 ID 시작 값과 199999입니다.
--idstart=*<number>*	IdM 서버에서 할당할 수 있는 ID의 하한 또는 시작 값을 설정합니다. 기본값은 임의로 선택됩니다.
--ip-address *127.0.0.1*	서버의 IP 주소를 지정합니다. 이 옵션은 로컬 인터페이스와 연결된 IP 주소만 허용합니다.
-n *example.com*	IdM 도메인에 사용할 LDAP 서버 도메인의 이름입니다. 일반적으로 IdM 서버의 호스트 이름을 기반으로 합니다.
-p *<directory_manager_password>*	LDAP 서비스의 사용자 **cn=Directory Manager** 의 암호입니다.
-P *<kerberos_main_password>*	NetNamespace 관리자의 암호입니다. 값을 지정하지 않으면 임의로 생성됩니다.
-r *<KERBEROS_REALM_NAME>*	**EXAMPLE.COM** 과 같이 대문자로 IdM 도메인에 대해 생성할 Kerberos 영역의 이름입니다.
--setup-ca	이 복제본에 CA를 설치하고 구성합니다. CA가 구성되지 않은 경우 인증서 작업이 CA가 설치된 다른 복제본으로 전달됩니다.

인수	설명
--forwarder=*192.0.2.1*	DNS 서비스에 사용할 DNS 전달자를 제공합니다. 둘 이상의 전달자를 지정하려면 이 옵션을 여러 번 사용합니다.
--no-forwarders	전달자 대신 DNS 서비스와 함께 루트 서버를 사용합니다.
--no-reverse	DNS 도메인이 설정될 때 역방향 DNS 영역을 생성하지 않습니다. (역방향 DNS 영역이 이미 구성된 경우 기존 역방향 DNS 영역이 사용됩니다.) 이 옵션을 사용하지 않으면 기본값은 true이며 이는 역방향 DNS를 설치 스크립트에서 구성해야 한다고 가정합니다.
--setup-dns	설치 스크립트에 IdM 도메인 내에 DNS 서비스를 설정하도록 지시합니다. 통합 DNS 서비스를 사용하는 것은 선택 사항이므로 이 옵션이 설치 스크립트로 전달되지 않으면 DNS가 구성되지 않습니다.
-U, **--unattended**	사용자 입력을 요청하지 않는 자동 설치 세션을 활성화합니다.

추가 리소스

- **ipa-server-install(1) 매뉴얼 페이지**
- **ipa-replica-install(1) 매뉴얼 페이지**

10장. IDM 서버 설치 문제 해결

다음 섹션에서는 실패한 IdM 서버 설치에 대한 정보와 일반적인 설치 문제를 해결하는 방법을 설명합니다.

10.1. IDM 서버 설치 오류 로그 검토

IdM(Identity Management) 서버를 설치할 때 디버깅 정보가 다음 로그 파일에 추가됩니다.

- /var/log/ipaserver-install.log
- /var/log/httpd/error_log
- /var/log/dirsrv/slapd-*INSTANCE-NAME*/access
- /var/log/dirsrv/slapd-*INSTANCE-NAME*/errors

로그 파일의 마지막 줄에서 성공 또는 실패를 보고하고 ERROR 및 DEBUG 항목은 추가 컨텍스트를 제공합니다.

실패한 IdM 서버 설치 문제를 해결하려면 로그 파일 끝에 있는 오류를 검토하고 이 정보를 사용하여 해당 문제를 해결합니다.

사전 요구 사항

- IdM 로그 파일의 내용을 표시하려면 root 권한이 있어야 합니다.

절차

1. tail 명령을 사용하여 로그 파일의 마지막 행을 표시합니다. 다음 예제는 /var/log/ipaserver-install.log 의 마지막 10행을 표시합니다.

```
[user@server ~]$ sudo tail -n 10 /var/log/ipaserver-install.log
[sudo] password for user:
value = gen.send(prev_value)
```

```
File "/usr/lib/python3.6/site-packages/ipapython/install/common.py", line 65, in _install
for unused in self._installer(self.parent):
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/init.py", line 564, in main
master_install(self)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/install.py", line 291, in
decorated
raise ScriptError()

2020-05-27T22:59:41Z DEBUG The ipa-server-install command failed, exception:
ScriptError:
2020-05-27T22:59:41Z ERROR The ipa-server-install command failed. See
/var/log/ipaserver-install.log for more information
```

2. 로그 파일을 대화형으로 검토하려면 **less** 유틸리티를 사용하여 로그 파일의 끝을 열고 ↑ 및 ↓ 화살표 키를 사용하여 이동합니다. 다음 예제에서는 **/var/log/ipaserver-install.log** 파일을 대화식으로 엽니다.

```
[user@server ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

3. 이 검토 프로세스를 나머지 로그 파일과 함께 반복하여 추가 문제 해결 정보를 수집합니다.

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

추가 리소스

- 실패한 **IdM** 서버 설치를 확인할 수 없고 **Red Hat** 기술 지원 서브스크립션이 있는 경우 **Red Hat** 고객 포털에서 기술 지원 케이스를 열고 **sosreport**의 서버를 제공합니다.

- **sosreport** 유틸리티는 **RHEL** 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. **sosreport** 유틸리티에 대한 자세한 내용은 **What is an sosreport and how to create one in Red Hat Enterprise Linux?** 를 참조하십시오.

10.2. IDM CA 설치 오류 검토

IdM(Identity Management) 서버에 **CA(**인증 기관**)** 서비스를 설치하면 디버깅 정보가 다음 위치(권장 우선 순위 순서로)에 추가됩니다.

위치	설명
/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log	**pkispawn** 설치 프로세스의 상위 수준 문제 및 Python 추적
journalctl -u pki-tomcatd@pki-tomcat output	**pki-tomcatd@pki-tomcat** 서비스의 오류
/var/log/pki/pki-tomcat/ca/debug.*$DATE*.log	PKI(Public Key Infrastructure) 제품의 핵심에 있는 대규모 JAVA 스택 추적
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit log file	PKI 제품의 감사 로그
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.*$DATE*.log**	인증서를 사용하는 서비스 주체, 호스트 및 기타 엔티티에 대한 인증서 작업의 낮은 수준의 디버그 데이터

참고

선택적 CA 구성 요소를 설치하는 동안 전체 IdM 서버 설치에 실패하면 CA에 대한 세부 정보가 기록되지 않습니다. /var/log/ipaserver-install.log 파일에 로그인되어 전체 설치 프로세스가 실패했음을 나타냅니다. CA 설치 실패와 관련된 자세한 내용은 위에 나열된 로그 파일을 검토하는 것이 좋습니다.

이 동작에 대한 유일한 예외는 CA 서비스를 설치하고 루트 CA가 외부 CA인 경우입니다. 외부 CA에서 인증서에 문제가 있는 경우 /var/log/ipaserver-install.log 에 오류가 기록됩니다.

실패한 IdM CA 설치 문제를 해결하려면 이러한 로그 파일 끝에 있는 오류를 검토하고 이 정보를 사용하여 해당 문제를 해결합니다.

사전 요구 사항

- **IdM 로그 파일의 내용을 표시하려면 root 권한이 있어야 합니다.**

절차

1.

로그 파일을 대화형으로 검토하려면 **less** 유틸리티를 사용하여 로그 파일의 끝을 열고 **ScriptError** 항목을 검색하는 동안 ↑ 및 ↓ 화살표 키를 사용하여 이동합니다. 다음 예제에서는 **/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log**를 엽니다.

```
[user@server ~]$ sudo less -N +G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. 위에 나열된 모든 로그 파일과 함께 이 검토 프로세스를 반복하여 추가 문제 해결 정보를 수집합니다.

추가 리소스

- 실패한 **IdM** 서버 설치를 확인할 수 없고 **Red Hat** 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 **sosreport**의 서버를 제공합니다.
- **sosreport** 유틸리티는 **RHEL** 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. **sosreport** 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

10.3. 부분적인 IDM 서버 설치 제거

IdM 서버 설치에 실패하면 일부 구성 파일을 그대로 유지할 수 있습니다. **IdM** 서버 설치 시도에 대한 추가 시도가 실패하고 설치 스크립트에서 **IPA**가 이미 구성되어 있다고 보고합니다.

기존 부분 **IdM** 구성이 있는 시스템 예

```
[root@server ~]# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-server-install command failed. See /var/log/ipaserver-install.log for more information
```

이 문제를 해결하려면 부분적인 **IdM** 서버 구성을 제거하고 설치 프로세스를 다시 시도합니다.

사전 요구 사항

- root 권한이 있어야 합니다.

절차

1. IdM 서버로 구성하려는 호스트에서 IdM 서버 소프트웨어를 설치 제거합니다.

```
[root@server ~]# ipa-server-install --uninstall
```

2. 반복적으로 실패한 설치로 인해 IdM 서버를 설치하는 데 어려움이 있는 경우 운영 체제를 다시 설치하십시오.

IdM 서버를 설치하기 위한 요구 사항 중 하나는 사용자 지정이 없는 클린 시스템입니다. 실패한 설치로 인해 시스템 파일을 예기치 않게 수정하여 호스트의 무결성이 손상될 수 있습니다.

추가 리소스

- IdM 서버 설치 제거에 대한 자세한 내용은 IdM 서버 제거를 참조하십시오.
- 반복된 제거 시도 후 설치가 실패하고 Red Hat 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 sosreport 의 서버를 제공합니다.
- sosreport 유틸리티는 RHEL 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. sosreport 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

추가 리소스

- IdM 서버 설치 제거에 대한 자세한 내용은 IdM 서버 제거를 참조하십시오.
- 반복된 제거 시도 후 설치가 실패하고 Red Hat 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 sosreport 의 서버를 제공합니다.
- sosreport 유틸리티는 RHEL 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. sosreport 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

10.4. 추가 리소스

- IdM 복제본 설치 문제를 해결하려면 IdM 복제본 설치 문제 해결을 참조하십시오.
- IdM 클라이언트 설치 문제를 해결하려면 IdM 클라이언트 설치 문제 해결을 참조하십시오.

11장. IDM 서버 설치 제거

이 절차에서는 server123.idm.example.com 이라는 IdM(Identity Management) 서버를 제거하는 방법을 설명합니다.

사전 요구 사항

- root 가 server123.idm.example.com에 액세스할 수 있습니다.
- IdM 관리자의 인증 정보가 있습니다.

절차

1. IdM 환경에서 통합 DNS를 사용하는 경우 server123.idm.example.com이 활성화된 유일한 DNS 서버가 아닌지 확인합니다.

```
[root@server123 ~]# ipa server-role-find --role 'DNS server'
----------------------
2 server roles matched
----------------------
  Server name: server456.idm.example.com
  Role name: DNS server
  Role status: enabled
[...]
----------------------------
Number of entries returned 2
----------------------------
```

server123이 토폴로지의 나머지 DNS 서버인 경우 다른 IdM 서버에 DNS 서버 역할을 추가합니다. 자세한 내용은 ipa-dns-install(1) 매뉴얼 페이지를 참조하십시오.

2. IdM 환경에서 통합 CA(인증 기관)를 사용하는 경우:

   a. server123.idm.example.com이 유일하게 활성화된 CA 서버가 아닌지 확인합니다.

```
[root@server123 ~]# ipa server-role-find --role 'CA server'
----------------------
2 server roles matched
----------------------
  Server name: server123.idm.example.com
  Role name: CA server
```

```
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: CA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

server123이 토폴로지의 유일한 나머지 CA 서버인 경우 다른 IdM 서버에 CA 서버 역할을 추가합니다. 자세한 내용은 ipa-ca-install(1) 매뉴얼 페이지를 참조하십시오.

b.

IdM 환경에서 자격 증명 모음을 활성화한 경우, server123.idm.example.com이 유일하게 활성화된 KMS 복구 기관(KRA) 서버가 아닌지 확인합니다.

```
[root@server123 ~]# ipa server-role-find --role 'KRA server'
--------------------
2 server roles matched
--------------------
  Server name: server123.idm.example.com
  Role name: KRA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: KRA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

server123이 토폴로지에 있는 유일한 KRA 서버인 경우 다른 IdM 서버에 KRA 서버 역할을 추가합니다. 자세한 내용은 man ipa-kra-install(1) 에서 참조하십시오.

c.

server123.idm.example.com이 CA 갱신 서버가 아닌지 확인합니다.

```
[root@server123 ~]# ipa config-show | grep 'CA renewal'
  IPA CA renewal master: r8server.idm.example.com
```

server123이 CA 갱신 서버인 경우 CA 갱신 서버 역할을 다른 서버로 이동하는 방법에 대한 자세한 내용은 IdM CA 갱신 서버 변경 및 재설정 을 참조하십시오.

d.

server123.idm.example.com이 현재 인증서 해지 목록(CRL) 게시자가 아닌지 확인합니다.

```
[root@server123 ~]# ipa-crlgen-manage status
CRL generation: disabled
```

출력에 server123에서 CRL 생성이 활성화되었음을 표시하는 경우 CRL 게시자 역할을 다른 서버로 이동하는 방법에 대한 자세한 내용은 IdM CA 서버에서 CRL 생성을 참조하십시오.

3. 토폴로지의 다른 IdM 서버에 연결합니다.

```
$ ssh idm_user@server456
```

4. 서버에서 IdM 관리자의 자격 증명을 가져옵니다.

```
[idm_user@server456 ~]$ kinit admin
```

5. 토폴로지의 서버에 할당된 DNA ID 범위를 확인합니다.

```
[idm_user@server456 ~]$ ipa-replica-manage dnarange-show
server123.idm.example.com: 1001-1500
server456.idm.example.com: 1501-2000
[...]
```

출력에서는 DNA ID 범위가 server123과 server456 모두에 할당되었음을 보여줍니다.

6. server123이 DNA ID 범위가 할당된 토폴로지의 유일한 IdM 서버인 경우 server456에 테스트 IdM 사용자를 생성하여 서버에 DNA ID 범위가 할당되어 있는지 확인합니다.

```
[idm_user@server456 ~]$ ipa user-add test_idm_user
```

7. 토폴로지에서 server123.idm.example.com을 삭제합니다.

```
[idm_user@server456 ~]$ ipa server-del server123.idm.example.com
```

참고

ipa server-del 명령을 실행하면 도메인 및 **ca** 접미사 모두 **server123**과 관련된 모든 복제 데이터 및 계약이 제거됩니다. 이는 처음에는 **ipa-replica-manage del *server123*** 명령을 사용하여 이러한 데이터를 제거해야 하는 도메인 수준 **0 IdM** 토폴로지와 다릅니다. 도메인 수준 **0 IdM** 토폴로지는 **RHEL 7.2** 이하에서 실행되는 **IdM** 토폴로지입니다. **ipa domainlevel-get** 명령을 사용하여 현재 도메인 수준을 확인합니다.

8. **server123.idm.example.com**으로 돌아가 기존 **IdM** 설치를 제거합니다.

```
[root@server123 ~]# ipa-server-install --uninstall
...
Are you sure you want to continue with the uninstall procedure? [no]: yes
```

9. **server123.idm.example.com**을 가리키는 모든 이름 서버(NS) **DNS** 레코드가 **DNS** 영역에서 삭제되었는지 확인합니다. 이는 **IdM** 또는 외부 **DNS**에서 관리하는 통합 **DNS**를 사용하는지 여부에 관계없이 적용됩니다. **IdM**에서 **DNS** 레코드를 삭제하는 방법에 대한 자세한 내용은 **IdM CLI**의 **DNS** 레코드 삭제를 참조하십시오.

추가 리소스

- **RHEL 7** 설명서에서 도메인 수준 표시 및 향상
- 복제본 토폴로지 계획
- **IdM CA** 갱신 서버에 대한 설명
- **IdM CA** 서버에서 **CRL** 생성

12장. IDM 서버 이름 변경

기존 IdM(Identity Management) 서버의 호스트 이름은 변경할 수 없습니다. 그러나 서버를 다른 이름의 복제본으로 교체할 수 있습니다.

절차

1. 기존 서버를 대체할 새 복제본을 설치하여 복제본에 필요한 호스트 이름과 IP 주소가 있는지 확인합니다. 자세한 내용은 IdM 복제본 설치를 참조하십시오.

중요

설치 제거 중인 서버가 CRL(인증서 해지 목록) 게시자 서버인 경우 계속하기 전에 다른 서버를 CRL 게시자 서버로 만듭니다.

마이그레이션 절차의 컨텍스트에서 이 작업을 수행하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- RHEL 7 IdM CA 서버에서 CRL 생성 중지
- 새로운 RHEL 8 IdM CA 서버에서 CRL 생성 시작

2. 기존 IdM 서버 인스턴스를 중지합니다.

```
[root@old_server ~]# ipactl stop
```

3. IdM 서버 설치 제거에 설명된 대로 기존 서버를 설치 제거합니다.

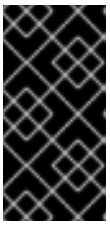
13장. IDM 업데이트 및 다운그레이드

13.1. IDM 패키지 업데이트

yum 유틸리티를 사용하여 시스템의 IdM(Identity Management) 패키지를 업데이트할 수 있습니다.

- 프로필과 관련된 모든 IdM 패키지를 업데이트하고 사용 가능한 업데이트가 있는 경우 다음을 수행합니다.

```
# yum upgrade ipa-*
```



중요

업데이트를 설치하기 전에 RHEL 시스템과 관련된 이전에 릴리스된 모든 에라타를 적용했는지 확인하십시오.

- 또는 활성화된 리포지토리에서 프로필에 사용 가능한 최신 버전과 일치하도록 패키지를 설치하거나 업데이트하려면 다음을 수행합니다.

```
# yum distro-sync ipa-*
```

하나 이상의 서버에서 IdM 패키지를 업데이트한 후 토폴로지의 다른 모든 서버는 패키지를 업데이트하지 않은 경우에도 업데이트된 스키마를 수신합니다. 이렇게 하면 새 스키마를 사용하는 새 항목을 다른 서버에 복제할 수 있습니다.

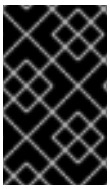
주의

여러 IdM 서버를 업데이트할 때 다른 서버를 업데이트하기 전에 한 서버를 업데이트한 후 10분 이상 기다립니다. 그러나 서버의 성공적인 업데이트에 필요한 실제 시간은 배포된 토폴로지, 연결 대기 시간, 업데이트로 생성된 변경 사항 수에 따라 달라집니다.

두 개 이상의 서버가 동시에 업데이트되거나 업그레이드 간에 짧은 간격으로 업데이트되는 경우 토폴로지 전체에서 업그레이드 후 데이터 변경 사항을 복제할 수 있는 충분한 시간이 없으므로 복제 이벤트가 충돌할 수 있습니다.

13.2. IDM 패키지 DOWNGRADING

IdM 패키지를 수동으로 다운그레이드하는 것은 지원되지 않습니다. yum distro-sync 를 사용하여 모듈에서 패키지를 업데이트하고 다운그레이드합니다.



중요

ipa-* 패키지에서 yum downgrade 명령을 실행하지 마십시오.

추가 리소스

- yum(8) man page

14장. IDM 클라이언트 설치를 위한 시스템 준비

이 장에서는 IdM(Identity Management) 클라이언트를 설치하기 위해 시스템이 충족해야 하는 조건에 대해 설명합니다.

14.1. IDM 클라이언트의 DNS 요구 사항

기본적으로 클라이언트 설치 프로그램은 _ldap._tcp.DOMAIN DNS SRV 레코드를 검색합니다. 호스트 이름의 상위 도메인에 대한 DNS SRV 레코드입니다. 예를 들어 클라이언트 시스템에 호스트 이름 client1.idm.example.com 이 있는 경우 설치 관리자는 각각 _ldap._tcp.idm.example.com,_ldap._tcp.example.com 및 _ldap._tcp.com DNS SRV 레코드에서 IdM 서버 호스트 이름을 검색하려고 합니다. 그런 다음 검색된 도메인을 사용하여 시스템에서 클라이언트 구성 요소(예: SSSD 및 Kerberos 5 구성)를 구성합니다.

그러나 IdM 클라이언트의 호스트 이름이 기본 DNS 도메인의 일부일 필요는 없습니다. 클라이언트 시스템 호스트 이름이 IdM 서버의 하위 도메인에 없는 경우 ipa-client-install 명령의 --domain 옵션으로 IdM 도메인을 전달합니다. 이 경우 클라이언트를 설치한 후 SSSD 및 Kerberos 구성 요소 모두 구성 파일에 도메인이 설정되어 IdM 서버를 자동으로 검색하는 데 사용합니다.

추가 리소스

- IdM의 DNS 요구 사항에 대한 자세한 내용은 IdM에 대한 호스트 이름 및 DNS 요구 사항을 참조하십시오.

14.2. IDM 클라이언트의 포트 요구 사항

IdM(Identity Management) 클라이언트는 서비스와 통신하기 위해 IdM 서버의 여러 포트에 연결합니다.

IdM 클라이언트에서 이러한 포트가 *발신 방향으로* 열려 있어야 합니다. firewalld 와 같이 발신 패킷을 필터링하지 않는 방화벽을 사용하는 경우 해당 포트는 발신 방향으로 이미 사용 가능합니다.

추가 리소스

- 사용되는 특정 포트에 대한 자세한 내용은 IdM에 대한 포트 요구 사항을 참조하십시오.

14.3. IDM 클라이언트의 IPV6 요구 사항

IdM(Identity Management)에서는 IdM에 등록하려는 호스트의 커널에서 IPv6 프로토콜을 활성화할 필요가 없습니다. 예를 들어 내부 네트워크가 IPv4 프로토콜만 사용하는 경우 IPv4 를 사용하여 IdM 서버와 통신하도록 SSSD(System Security Services Daemon)를 구성할 수 있습니다. /etc/sssd/sssd.conf 파일의 [domain/*NAME*] 섹션에 다음 행을 삽입하면 됩니다.

```
lookup_family_order = ipv4_only
```

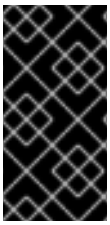
추가 리소스

- lookup_family_order 옵션에 대한 자세한 내용은 sssd.conf(5) 매뉴얼 페이지를 참조하십시오.

14.4. IDM:CLIENT 스트림에서 IDM 클라이언트 패키지 설치

RHEL8에서는 IdM(Identity Management) 클라이언트를 설치하는 데 필요한 패키지가 모듈로 제공됩니다.

idm:client 스트림은 idm 모듈의 기본 스트림입니다. 시스템에 서버 구성 요소를 설치할 필요가 없는 경우 이 스트림을 사용하여 IdM 클라이언트 패키지를 다운로드합니다. 서버 구성 요소가 필요하지 않은 경우 특히 장기간 지원되는 IdM 클라이언트 소프트웨어를 지속적으로 사용해야 하는 경우 idm:client 스트림을 사용하는 것이 좋습니다.



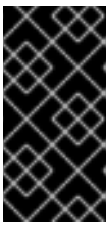
중요

호스트에 IdM 복제본을 설치하려는 경우 idm:client 스트림을 사용하지 마십시오. 이 경우에는 idm:DL1 스트림을 대신 사용합니다.

사전 요구 사항

- 이전에 idm:DL1 스트림을 활성화하여 패키지에서 다운로드한 후 idm:client 스트림으로 전환할 때 먼저 모든 관련 콘텐츠를 명시적으로 제거하고 idm:DL1 스트림을 활성화하기 전에 idm:DL1 스트림을 비활성화해야 합니다.

  진행 방법에 대한 자세한 내용은 이후 스트림으로 전환을 참조하십시오.



중요

현재 스트림을 비활성화하지 않고 새 스트림을 활성화하면 오류가 발생합니다.

절차

- IdM 클라이언트 설치에 필요한 패키지를 다운로드하려면 다음을 수행합니다.

```
# yum module install idm
```

14.5. IDM:DL1 스트림에서 IDM 클라이언트 패키지 설치

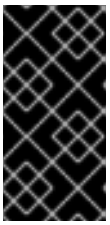
RHEL8에서는 IdM(Identity Management) 클라이언트를 설치하는 데 필요한 패키지가 모듈로 제공됩니다.

idm:DL1 스트림을 사용하도록 설정해야 패키지를 다운로드할 수 있습니다. IdM 서버 구성 요소를 시스템에 설치해야 하는 경우 이 스트림을 사용하여 IdM 클라이언트 패키지를 다운로드합니다.

사전 요구 사항

- 이전에 idm:DL1 스트림을 활성화하여 해당 스트림에서 패키지를 다운로드한 후 idm:DL1 스트림을 활성화하기 전에 먼저 모든 관련 콘텐츠를 명시적으로 제거하고 idm:client 스트림을 비활성화해야 합니다.

  진행 방법에 대한 자세한 내용은 이후 스트림으로 전환을 참조하십시오.



중요

현재 스트림을 비활성화하지 않고 새 스트림을 활성화하면 오류가 발생합니다.

절차

1. idm:DL1 스트림을 통해 제공되는 RPM으로 전환하려면 다음을 수행합니다.

```
# yum module enable idm:DL1
# yum distro-sync
```

2. IdM 클라이언트 설치에 필요한 패키지를 다운로드하려면 다음을 수행합니다.

```
# yum module install idm:DL1/client
```

15장. IDM 클라이언트 설치

다음 섹션에서는 ipa-client-install 유틸리티를 사용하여 시스템을 IdM(Identity Management) 클라이언트로 구성하는 방법을 설명합니다. 시스템을 IdM 클라이언트로 구성하여 IdM 도메인에 등록하고, 시스템이 도메인의 IdM 서버에서 IdM 서비스를 사용할 수 있도록 합니다.

IdM(Identity Management) 클라이언트를 성공적으로 설치하려면 클라이언트를 등록하는 데 사용할 수 있는 인증 정보를 제공해야 합니다.

15.1. 사전 요구 사항

- IdM 클라이언트 설치를 위한 시스템을 준비했습니다. 자세한 내용은 IdM 클라이언트 설치 시스템 준비를 참조하십시오.

15.2. 사용자 자격 증명을 사용하여 클라이언트 설치: 대화형 설치

이 절차에서는 권한 있는 사용자의 자격 증명을 사용하여 도메인에 시스템을 등록하여 IdM(Identity Management) 클라이언트를 대화형으로 설치하는 방법을 설명합니다.

사전 요구 사항

- 클라이언트를 IdM 도메인에 등록할 수 있는 사용자의 인증 정보가 있는지 확인합니다. 예를 들어 Enrollment Administrator 역할이 있는 hostadmin 사용자일 수 있습니다.

절차

1. IdM 클라이언트로 구성하려는 시스템에서 ipa-client-install 유틸리티를 실행합니다.

```
# ipa-client-install --mkhomedir
```

다음 조건 중 하나가 적용되는 경우 --enable-dns-updates 옵션을 추가하여 클라이언트 시스템의 IP 주소로 DNS 레코드를 업데이트합니다.

- 클라이언트가 등록된 IdM 서버는 통합된 DNS를 사용하여 설치됨
- 네트워크의 DNS 서버는 GSS-TSIG 프로토콜을 사용하여 DNS 항목 업데이트를 허용합니다.

```
# ipa-client-install --enable-dns-updates --mkhomedir
```

클라이언트가 **DNS** 업데이트를 활성화하는 경우 유용합니다.

- 동적 호스트 구성 프로토콜을 사용하여 발행된 동적 **IP** 주소 보유
- 고정 **IP** 주소가 있지만 할당되었지만 **IdM** 서버는 이에 대해 알 수 없습니다.

2. 설치 스크립트는 **DNS** 레코드와 같은 모든 필요한 설정을 자동으로 가져옵니다.

- **IdM DNS** 영역에 **SRV** 레코드가 올바르게 설정된 경우 스크립트에서 다른 모든 필수 값을 자동으로 검색하고 표시합니다. 확인하려면 **yes** 를 입력합니다.

```
Client hostname: client.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: server.example.com
BaseDN: dc=example,dc=com

Continue to configure the system with these values? [no]: yes
```

- 다른 값으로 시스템을 설치하려면 **no** 를 입력합니다. 그런 다음 **ipa-client-install** 을 다시 실행하고 **ipa-client-install** 에 명령줄 옵션을 추가하여 필요한 값을 지정합니다. 예를 들면 다음과 같습니다.
  - **--hostname**
  - **--realm**
  - **--domain**
  - **--server**

- **--mkhomedir**

중요

정규화된 도메인 이름은 유효한 **DNS** 이름이어야 합니다.

- 숫자, 영문자 및 하이픈(**-**)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 **DNS** 오류가 발생할 수 있습니다.
- 호스트 이름은 모두 소문자여야 합니다. 대문자는 사용할 수 없습니다.

- 스크립트에서 일부 설정을 자동으로 가져오지 못하면 값을 입력하라는 메시지를 표시합니다.

3. 이 스크립트는 **ID**가 클라이언트를 등록하는 데 사용할 사용자의 메시지를 표시합니다. 예를 들어 **Enrollment Administrator** 역할이 있는 **hostadmin** 사용자일 수 있습니다.

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

4. 이제 설치 스크립트가 클라이언트를 구성합니다. 작업이 완료될 때까지 기다립니다.

```
Client configuration complete.
```

추가 리소스

- 클라이언트 설치 스크립트가 **DNS** 레코드를 검색하는 방법에 대한 자세한 내용은 **ipa-client-install(1)** 매뉴얼 페이지의 **DNS** 자동 검색 섹션을 참조하십시오.

15.3. 일회성 암호를 사용하여 클라이언트 설치: 대화형 설치

이 절차에서는 일회성 암호를 사용하여 대화형으로 **IdM(Identity Management)** 클라이언트를 설치하는 방법을 설명합니다.

사전 요구 사항

- 도메인의 서버에서 향후 클라이언트 시스템을 IdM 호스트로 추가합니다. ipa host-add 명령과 함께 --random 옵션을 사용하여 등록에 사용할 일회성 임의 암호를 생성합니다.

참고

ipa host-add <client_fqdn > 명령을 사용하려면 DNS를 통해 클라이언트 FQDN을 확인할 수 있어야 합니다. 확인할 수 없는 경우 --ip address 옵션을 사용하여 IdM 클라이언트 시스템의 IP 주소를 제공하거나 --force 옵션을 사용합니다.

```
$ ipa host-add client.example.com --random
 --------------------------------------------
Added host "client.example.com"
 --------------------------------------------
 Host name: client.example.com
 Random password: W5YpARl=7M.n
 Password: True
 Keytab: False
 Managed by: server.example.com
```

참고

시스템을 IdM 도메인에 등록한 후 생성된 암호가 무효화됩니다. 등록 완료 후 적절한 호스트 키탭으로 교체됩니다.

절차

1. IdM 클라이언트로 구성하려는 시스템에서 ipa-client-install 유틸리티를 실행합니다.

일회성 임의 암호를 제공하려면 --password 옵션을 사용합니다. 암호에는 종종 특수 문자가 포함되어 있으므로 작은따옴표(')로 묶습니다.

```
# ipa-client-install --mkhomedir --password=password
```

다음 조건 중 하나가 적용되는 경우 --enable-dns-updates 옵션을 추가하여 클라이언트 시스템의 IP 주소로 DNS 레코드를 업데이트합니다.

- 클라이언트가 등록된 IdM 서버는 통합된 DNS를 사용하여 설치됨
-

네트워크의 **DNS** 서버는 **GSS-TSIG** 프로토콜을 사용하여 **DNS** 항목 업데이트를 허용합니다.

```
# ipa-client-install --password 'W5YpARl=7M.n' --enable-dns-updates --mkhomedir
```

클라이언트가 **DNS** 업데이트를 활성화하는 경우 유용합니다.

- 동적 호스트 구성 프로토콜을 사용하여 발행된 동적 **IP** 주소 보유
- 고정 **IP** 주소가 있지만 할당되었지만 **IdM** 서버는 이에 대해 알 수 없습니다.

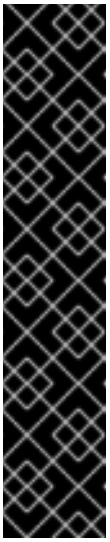
2. 설치 스크립트는 **DNS** 레코드와 같은 모든 필요한 설정을 자동으로 가져옵니다.

- **IdM DNS** 영역에 **SRV** 레코드가 올바르게 설정된 경우 스크립트에서 다른 모든 필수 값을 자동으로 검색하고 표시합니다. 확인하려면 **yes** 를 입력합니다.

```
Client hostname: client.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: server.example.com
BaseDN: dc=example,dc=com

Continue to configure the system with these values? [no]: yes
```

- 다른 값으로 시스템을 설치하려면 **no** 를 입력합니다. 그런 다음 **ipa-client-install** 을 다시 실행하고 **ipa-client-install** 에 명령줄 옵션을 추가하여 필요한 값을 지정합니다. 예를 들면 다음과 같습니다.
  - **--hostname**
  - **--realm**
  - **--domain**
  - **--server**

- **--mkhomedir**



중요

정규화된 도메인 이름은 유효한 **DNS** 이름이어야 합니다.

- 숫자, 영문자 및 하이픈(**-**)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 **DNS** 오류가 발생할 수 있습니다.
- 호스트 이름은 모두 소문자여야 합니다. 대문자는 사용할 수 없습니다.

- 스크립트에서 일부 설정을 자동으로 가져오지 못하면 값을 입력하라는 메시지를 표시합니다.

3. 이제 설치 스크립트가 클라이언트를 구성합니다. 작업이 완료될 때까지 기다립니다.

```
Client configuration complete.
```

추가 리소스

- 클라이언트 설치 스크립트가 **DNS** 레코드를 검색하는 방법에 대한 자세한 내용은 **ipa-client-install(1)** 매뉴얼 페이지의 **DNS** 자동 검색 섹션을 참조하십시오.

15.4. 클라이언트 설치: 비대화형 설치

비대화식 설치의 경우 명령줄 옵션을 사용하여 **ipa-client-install** 유틸리티에 필요한 모든 정보를 제공해야 합니다. 다음 섹션에서는 비대화형 설치에 필요한 최소 옵션에 대해 설명합니다.

클라이언트 등록을 위한 인증 방법 옵션

사용 가능한 옵션은 다음과 같습니다.

- **--principal** 및 **--password**: 클라이언트를 등록할 권한이 있는 사용자의 인증 정보를 지정합니다.

- **--random:** 클라이언트에 대해 생성된 일회성 임의 암호를 지정합니다.

- **--keytab** 을 사용하여 이전 등록의 키탭을 지정합니다.

자동 설치 옵션

--unattended 옵션을 사용하면 사용자 확인 없이도 설치를 실행할 수 있습니다.

IdM DNS 영역에 **SRV** 레코드가 올바르게 설정된 경우 스크립트에서 다른 모든 필수 값을 자동으로 검색합니다. 스크립트가 값을 자동으로 검색할 수 없는 경우 다음과 같은 명령줄 옵션을 사용하여 값을 제공하십시오.

- **--hostname:** 클라이언트 시스템에 대해 정적 정규화된 도메인 이름(**FQDN**)을 지정합니다.

중요

FQDN은 유효한 **DNS** 이름이어야 합니다.

  - 숫자, 영문자 및 하이픈(**-**)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 **DNS** 오류가 발생할 수 있습니다.

  - 호스트 이름은 모두 소문자여야 합니다. 대문자는 사용할 수 없습니다.

- **--domain: example.com**과 같이 기존 **IdM** 배포의 기본 **DNS** 도메인을 지정합니다. 이름은 **IdM Kerberos** 영역 이름의 소문자 버전입니다.

- 연결할 **IdM** 서버의 **FQDN**을 지정하는 **--server** 입니다. 이 옵션을 사용하면 **Kerberos**의 **DNS** 자동 검색이 비활성화되고 고정 **list of NetNamespace** 및 **Admin servers**가 구성됩니다. 정상적인 상황에서는 서버 목록이 기본 **IdM DNS** 도메인에서 검색되므로 이 옵션이 필요하지 않습니다.

- **--realm:** 기존 **IdM** 배포의 **Kerberos** 영역을 지정합니다. 일반적으로 **IdM** 설치에서 사용하는 기본 **DNS** 도메인의 대문자 버전입니다. 정상적인 상황에서는 영역 이름이 **IdM** 서버에

서 검색되므로 이 옵션이 필요하지 않습니다.

비대화형 설치를 위한 기본 **ipa-client-install** 명령의 예:

```
# ipa-client-install --password 'W5YpARl=7M.n' --mkhomedir --unattended
```

추가 옵션을 지정하여 비대화식 설치를 위한 **ipa-client-install** 명령의 예입니다.

```
# ipa-client-install --password 'W5YpARl=7M.n' --domain idm.example.com --server
server.idm.example.com --realm IDM.EXAMPLE.COM --mkhomedir --unattended
```

추가 리소스

- **ipa-client-install** 에서 허용하는 전체 옵션 목록은 **ipa-client-install(1)** 매뉴얼 페이지를 참조하십시오.

15.5. 클라이언트를 설치한 후 사전-IDM 구성 제거

ipa-client-install 스크립트는 **/etc/openldap/ldap.conf** 및 **/etc/sssd/sssd.conf** 파일에서 이전 **LDAP** 및 **SSSD(System Security Services Daemon)** 구성을 제거하지 않습니다. 클라이언트를 설치하기 전에 이러한 파일에서 구성을 수정한 경우 스크립트에서 새 클라이언트 값을 추가하지만 주석 처리합니다. 예를 들어 다음과 같습니다.

```
BASE   dc=example,dc=com
URI    ldap://ldap.example.com

#URI ldaps://server.example.com # modified by IPA
#BASE dc=ipa,dc=example,dc=com # modified by IPA
```

새 **IdM(Identity Management)}** 구성 값을 적용하려면 다음을 수행합니다.

1. **/etc/openldap/ldap.conf** 및 **/etc/sssd/sssd.conf** 를 엽니다.

2. 이전 구성을 삭제합니다.

3. 새 IdM 구성의 주석을 제거합니다.

4. 시스템 전체 LDAP 구성에 의존하는 서버 프로세스에 변경 사항을 적용하려면 다시 시작해야 할 수 있습니다. openldap 라이브러리를 사용하는 애플리케이션은 일반적으로 시작 시 구성을 가져옵니다.

15.6. IDM 클라이언트 테스트

명령줄 인터페이스는 ipa-client-install에 성공했지만 자체 테스트를 수행할 수도 있음을 알려줍니다.

IdM(Identity Management) 클라이언트가 서버에 정의된 사용자에 대한 정보를 가져올 수 있는지 테스트하려면 서버에 정의된 사용자를 확인할 수 있는지 확인합니다. 예를 들어 기본 admin 사용자를 확인하려면 다음을 실행합니다.

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

인증이 올바르게 작동하는지 테스트하려면 루트 가 아닌 사용자의 root 사용자로 이동합니다.

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

15.7. IDM 클라이언트 설치 중 수행되는 연결

IdM 클라이언트 설치 중에 수행된 요청에는 ipa-client -install, IdM(Identity Management) 클라이언트 설치 툴에서 수행하는 작업이 나열됩니다.

표 15.1. IdM 클라이언트 설치 중 수행되는 요청

작업	사용된 프로토콜	목적
클라이언트 시스템에 구성된 DNS 해석기에 대한 DNS 확인	DNS	IdM 서버의 IP 주소를 검색하려면 (선택 사항) A/AAAA 및 SSHFP 레코드 추가
IdM 복제본에서 포트 88(TCP/TCP6 및 UDP/UDP6) 요청	Kerberos	Kerberos 티켓을 얻으려면

작업	사용된 프로토콜	목적
검색된 또는 구성된 IdM 서버의 IdM Apache 기반 웹 서비스에 대한 JSON-RPC 호출	HTTPS	IdM 클라이언트 등록, LDAP 방법 실패 시 CA 인증서 체인 검색, 필요한 경우 인증서 발행 요청
SASL GSSAPI 인증, 일반 LDAP 또는 둘 다를 사용하여 IdM 서버의 포트 389에 TCP/TCP6을 통한 요청	LDAP	IdM 클라이언트 등록, SSSD 프로세스의 ID 검색, 호스트 주체의 Kerberos 키 검색
NTP(Network Time Protocol) 검색 및 해결 (선택 사항)	NTP	클라이언트 시스템과 NTP 서버 간 시간 동기화

15.8. 설치 후 배포 중 IDM 클라이언트와의 통신

IdM(Identity Management) 프레임워크의 클라이언트 측은 다음 두 가지 애플리케이션을 사용하여 구현됩니다.

- **ipa 명령행 인터페이스 (CLI)**
- ***(선택 사항)* 브라우저 기반 웹 UI**

CLI 설치 후 작업은 IdM 클라이언트 설치 후 배포 중에 CLI에서 수행하는 작업을 보여줍니다. 웹 UI 설치 후 작업은 IdM 클라이언트 설치 후 배포 중에 웹 UI에서 수행하는 작업을 보여줍니다.

표 15.2. CLI 설치 후 작업

작업	사용된 프로토콜	목적
클라이언트 시스템에 구성된 DNS 해석기에 대한 DNS 확인	DNS	IdM 서버의 IP 주소 검색
IdM 복제본에서 포트 88(TCP/TCP6 및 UDP/UDP6) 및 464(TCP/TCP6 및 UDP/UDP6)에 대한 요청	Kerberos	Kerberos 티켓을 얻으려면 Kerberos 암호를 변경하고 IdM 웹 UI에 인증
검색된 또는 구성된 IdM 서버의 IdM Apache 기반 웹 서비스에 대한 JSON-RPC 호출	HTTPS	**ipa** 유틸리티 사용

표 15.3. 웹 UI 설치 후 작업

작업	사용된 프로토콜	목적
검색된 또는 구성된 IdM 서버의 IdM Apache 기반 웹 서비스에 대한 JSON-RPC 호출	HTTPS	IdM 웹 UI 페이지 검색

추가 리소스

- SSSD 데몬이 IdM 및 Active Directory 서버에서 사용 가능한 서비스와 통신하는 방법에 대한 자세한 내용은 SSSD 통신 패턴입니다.
- certmonger 데몬이 IdM 및 Active Directory 서버에서 사용 가능한 서비스와 통신하는 방법에 대한 자세한 내용은 certmonger 통신 패턴을 참조하십시오.

15.9. SSSD 통신 패턴

SSSD(System Security Services Daemon)는 원격 디렉터리 및 인증 메커니즘에 액세스하기 위한 시스템 서비스입니다. ID 관리 IdM 클라이언트에 구성된 경우 인증, 권한 부여 및 기타 ID 및 정책 정보를 제공하는 IdM 서버에 연결됩니다. IdM 서버가 AD(Active Directory)와의 신뢰 관계에 있는 경우 SSSD는 Kerberos 프로토콜을 사용하여 AD 사용자에 대한 인증을 수행합니다. 기본적으로 SSSD는 Kerberos를 사용하여 로컬이 아닌 사용자를 인증합니다. 특히 SSSD는 LDAP 프로토콜을 대신 사용하도록 구성할 수 있습니다.

SSSD는 여러 서버와 통신하도록 구성할 수 있습니다. 아래 표에는 IdM의 SSSD에 대한 일반적인 통신 패턴이 표시되어 있습니다.

표 15.4. IdM 서버와 통신할 때 IdM 클라이언트의 SSSD 통신 패턴

작업	사용된 프로토콜	목적
클라이언트 시스템에 구성된 DNS 해석기에 대한 DNS 확인	DNS	IdM 서버의 IP 주소 검색
ID 관리 복제본 및 Active Directory 도메인 컨트롤러의 포트 88(TCP/TCP6 및 UDP/UDP6), 464(TCP/TCP6 및 UDP/UDP6)에 대한 요청	Kerberos	Kerberos 티켓을 얻으려면 Kerberos 암호를 변경하십시오.

작업	사용된 프로토콜	목적
SASL GSSAPI 인증, 일반 LDAP 또는 둘 다를 사용하여 IdM 서버의 포트 389에 TCP/TCP6을 통한 요청	LDAP	IdM 사용자 및 호스트에 대한 정보를 얻으려면 HBAC 및 sudo 규칙, 자동 마운트 맵, SELinux 사용자 컨텍스트, 공용 SSH 키 및 IdM LDAP에 저장된 기타 정보를 다운로드합니다.
(선택 사항) 스마트 카드 인증의 경우 OCSP(Online Certificate Status Protocol) 응답자를 구성합니다. 이는 종종 포트 80을 통해 수행되지만 클라이언트 인증서의 OCSP 응답자 URL의 실제 값에 따라 달라집니다.	HTTP	스마트 카드에 설치된 인증서의 상태에 대한 정보를 얻으려면

표 15.5. Active Directory 도메인 컨트롤러에 연결할 때 신뢰 에이전트 역할을 하는 IdM 서버의 SSSD의 통신 패턴

작업	사용된 프로토콜	목적
클라이언트 시스템에 구성된 DNS 해석기에 대한 DNS 확인	DNS	IdM 서버의 IP 주소 검색
ID 관리 복제본 및 Active Directory 도메인 컨트롤러의 포트 88(TCP/TCP6 및 UDP/UDP6), 464(TCP/TCP6 및 UDP/UDP6)에 대한 요청	Kerberos	Kerberos 티켓을 얻으려면 Kerberos 암호를 변경하고 원격으로 Kerberos를 관리합니다.
포트 389(TCP/TCP6 및 UDP/UDP6) 및 3268(TCP/TCP6)에 대한 요청	LDAP	Active Directory 사용자 및 그룹 정보를 쿼리하려면 Active Directory 도메인 컨트롤러를 검색합니다.
(선택 사항) 스마트 카드 인증의 경우 OCSP(Online Certificate Status Protocol) 응답자를 구성합니다. 이는 종종 포트 80을 통해 수행되지만 클라이언트 인증서의 OCSP 응답자 URL의 실제 값에 따라 달라집니다.	HTTP	스마트 카드에 설치된 인증서의 상태에 대한 정보를 얻으려면

추가 리소스

- 설치 후 배포 중 IdM 클라이언트와의 통신

15.10. CERTMONGER 통신 패턴

certmonger 는 IdM(Identity Management) 서버 및 IdM 클라이언트에서 실행 중인 데몬으로 호스트의 서비스와 관련된 SSL 인증서를 적절하게 갱신할 수 있습니다. 표 15.6. “certmonger 통신 패턴” 은

IdM 서버에서 IdM 클라이언트의 certmonger 유틸리티에서 수행하는 작업을 보여줍니다.

표 15.6. certmonger 통신 패턴

작업	사용된 프로토콜	목적
클라이언트 시스템에 구성된 DNS 해석기에 대한 DNS 확인	DNS	IdM 서버의 IP 주소 검색
IdM 복제본에서 포트 88(TCP/TCP6 및 UDP/UDP6) 및 464(TCP/TCP6 및 UDP/UDP6)에 대한 요청	Kerberos	Kerberos 티켓을 얻으려면
검색된 또는 구성된 IdM 서버의 IdM Apache 기반 웹 서비스에 대한 JSON-RPC 호출	HTTPS	새 인증서 요청
IdM 서버의 포트 8080(TCP/TCP6)을 통해 액세스	HTTP	OCSP(Online Certificate Status Protocol) 응답자 및 인증서 상태를 얻으려면
(보통 설치된 서버 또는 인증서 추적이 전송된 서버에 있음) IdM 서버의 포트 8443(TCP/TCP6)을 통해 액세스	HTTPS	IdM 서버에서 인증 기관을 관리하려면 (IdM 서버 및 복제본 설치 중에만 해당)

추가 리소스

- 설치 후 배포 중 IdM 클라이언트와의 통신

16장. KICKSTART로 IDM 클라이언트 설치

Kickstart 등록은 Red Hat Enterprise Linux를 설치할 때 IdM(Identity Management) 도메인에 새 시스템을 자동으로 추가합니다.

16.1. KICKSTART로 클라이언트 설치

이 절차에서는 Kickstart 파일을 사용하여 IdM(Identity Management) 클라이언트를 설치하는 방법을 설명합니다.

사전 요구 사항

- Kickstart 등록 전에 sshd 서비스를 시작하지 마십시오. 클라이언트를 등록하기 전에 sshd를 시작하면 SSH 키가 자동으로 생성되지만 16.2절. "클라이언트 설치를 위한 Kickstart 파일"의 Kickstart 파일은 기본 솔루션인 동일한 용도로 스크립트를 사용합니다.

절차

1. IdM 서버에서 호스트 항목을 미리 만들고 항목의 임시 암호를 설정합니다.

```
$ ipa host-add client.example.com --password=secret
```

Kickstart에서 암호를 사용하여 클라이언트 설치 중에 인증하고 첫 번째 인증 시도 후에 만료됩니다. 클라이언트가 성공적으로 설치되면 keytab을 사용하여 인증합니다.

2. 16.2절. "클라이언트 설치를 위한 Kickstart 파일"에 설명된 콘텐츠로 Kickstart 파일을 만듭니다. network 명령을 사용하여 Kickstart 파일에 네트워크가 올바르게 구성되었는지 확인합니다.

3. Kickstart 파일을 사용하여 IdM 클라이언트를 설치합니다.

16.2. 클라이언트 설치를 위한 KICKSTART 파일

이 섹션에서는 IdM(Identity Management) 클라이언트를 설치하는 데 사용할 수 있는 Kickstart 파일의 내용을 설명합니다.

설치할 패키지 목록의 ipa-client 패키지

ipa-client 패키지를 kickstart 파일의 %packages 섹션에 추가합니다. 예를 들어 다음과 같습니다.

```
%packages
...
ipa-client
...
```

IdM 클라이언트의 설치 후 지침

설치 후 지침에는 다음이 포함되어야 합니다.

- 등록하기 전에 SSH 키가 생성되었는지 확인하는 명령
- 다음을 지정하는 동안 ipa-client-install 유틸리티를 실행하는 명령입니다.
  - IdM 도메인 서비스에 액세스하고 구성하는 데 필요한 모든 정보
  - IdM 서버에서 클라이언트 호스트를 사전 생성할 때 설정하는 암호입니다. 16.1절. “Kickstart로 클라이언트 설치”

예를 들어, 일회성 암호를 사용하고 DNS를 통한 대신 명령줄에서 필요한 옵션을 검색하는 Kickstart 설치에 대한 설치 후 지침은 다음과 같습니다.

```
%post --log=/root/ks-post.log

# Generate SSH keys; ipa-client-install uploads them to the IdM server by default
/usr/libexec/openssh/sshd-keygen rsa

# Run the client install script
/usr/sbin/ipa-client-install --hostname=client.example.com --domain=EXAMPLE.COM --
enable-dns-updates --mkhomedir -w secret --realm=EXAMPLE.COM --
server=server.example.com
```

선택적으로 다음과 같은 다른 옵션을 킥스타트 파일에 포함할 수도 있습니다.

- 비대화식 설치의 경우 ipa-client-install에 --unattended 옵션을 추가합니다.

- 클라이언트 설치 스크립트에서 시스템에 대한 인증서를 요청하도록 하려면 다음을 수행합니다.

  - **ipa-client-install**에 **--request-cert** 옵션을 추가합니다.

  - **Kickstart chroot** 환경에서 **getcert** 및 **ipa-client-install** 유틸리티 모두에 대해 시스템 버스 주소를 **/dev/null**로 설정합니다. 이렇게 하려면 **ipa-client-install** 명령 앞에 **Kickstart** 파일의 설치 후 지침에 다음 행을 추가하십시오.

```
# env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null getcert list
# env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null ipa-client-install
```

16.3. IDM 클라이언트 테스트

명령줄 인터페이스는 **ipa-client-install**에 성공했지만 자체 테스트를 수행할 수도 있음을 알려줍니다.

IdM(Identity Management) 클라이언트가 서버에 정의된 사용자에 대한 정보를 가져올 수 있는지 테스트하려면 서버에 정의된 사용자를 확인할 수 있는지 확인합니다. 예를 들어 기본 **admin** 사용자를 확인하려면 다음을 실행합니다.

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

인증이 올바르게 작동하는지 테스트하려면 루트 가 아닌 사용자의 **root** 사용자로 이동합니다.

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

17장. IDM 클라이언트 설치 문제 해결

다음 섹션에서는 실패한 IdM 클라이언트 설치에 대한 정보와 일반적인 설치 문제를 해결하는 방법을 설명합니다.

17.1. IDM 클라이언트 설치 오류 검토

IdM(Identity Management) 클라이언트를 설치할 때 디버깅 정보가 /var/log/ipaclient-install.log에 추가됩니다. 클라이언트 설치에 실패하면 설치 관리자는 오류를 기록하고 변경 사항을 롤백하여 호스트에 대한 수정 사항을 취소합니다. 설치 관리자도 롤백 프로시저를 기록하므로 설치 프로그램이 로그 파일의 끝에는 설치 실패가 없을 수 있습니다.

실패한 IdM 클라이언트 설치 문제를 해결하려면 /var/log/ipaclient-install.log 파일에서 ScriptError라는 행을 검토하고 이 정보를 사용하여 해당 문제를 해결합니다.

사전 요구 사항

- IdM 로그 파일의 내용을 표시하려면 root 권한이 있어야 합니다.

절차

1. grep 유틸리티를 사용하여 /var/log/ipaserver-install.log 파일에서 ScriptError 키워드를 모두 검색합니다.

```
[user@server ~]$ sudo grep ScriptError /var/log/ipaclient-install.log
[sudo] password for user:
2020-05-28T18:24:50Z DEBUG The ipa-client-install command failed, exception:
ScriptError: One of password / principal / keytab is required.
```

2. 로그 파일을 대화형으로 검토하려면 less 유틸리티를 사용하여 로그 파일의 끝을 열고 ↑ 및 ↓ 화살표 키를 사용하여 이동합니다.

```
[user@server ~]$ sudo less -N +G /var/log/ipaclient-install.log
```

추가 리소스

- 실패한 IdM 클라이언트 설치를 해결할 수 없고 Red Hat 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 sosreport 의 클라이언트를 제공합니다.

- sosreport 유틸리티는 RHEL 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. sosreport 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

17.2. 클라이언트 설치에서 DNS 레코드를 업데이트하지 못하는 경우 문제 해결

IdM 클라이언트 설치 프로그램은 nsupdate 명령을 실행하여 PTR, SSHFP 및 추가 DNS 레코드를 생성합니다. 그러나 클라이언트 소프트웨어를 설치 및 구성한 후 클라이언트가 DNS 레코드를 업데이트할 수 없는 경우 설치 프로세스가 실패합니다.

이 문제를 해결하려면 구성을 확인하고 /var/log/client-install.log 에서 DNS 오류를 검토합니다.

사전 요구 사항

- IdM 환경의 DNS 솔루션으로 IdM DNS를 사용하고 있습니다.

절차

1. 클라이언트가 있는 DNS 영역의 동적 업데이트가 활성화되어 있는지 확인합니다.

```
[user@server ~]$ ipa dnszone-mod idm.example.com. --dynamic-update=TRUE
```

2. DNS 서비스를 실행하는 IdM 서버에 TCP 및 UDP 프로토콜 모두에 대해 포트 53이 열려 있는지 확인합니다.

```
[user@server ~]$ sudo firewall-cmd --permanent --add-port=53/tcp --add-port=53/udp
[sudo] password for user:
success
[user@server ~]$ firewall-cmd --runtime-to-permanent
success
```

3. grep 유틸리티를 사용하여 /var/log/client-install.log에서 nsupdate 명령의 내용을 검색하여 실패하는 DNS 레코드 업데이트를 확인합니다.

```
[user@server ~]$ sudo grep nsupdate /var/log/ipaclient-install.log
```

추가 리소스

-

실패한 설치를 해결할 수 없고 **Red Hat** 기술 지원 서브스크립션이 있는 경우 **Red Hat** 고객 포털에서 기술 지원 케이스를 열고 **sosreport** 의 클라이언트를 제공합니다.

- **sosreport** 유틸리티는 **RHEL** 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. **sosreport** 유틸리티에 대한 자세한 내용은 **What is an sosreport and how to create one in Red Hat Enterprise Linux?** 를 참조하십시오.

17.3. 클라이언트 설치가 IDM KERBEROS 영역에 참여하지 못하는 경우 문제 해결

클라이언트가 **IdM Kerberos** 영역에 참여할 수 없는 경우 **IdM** 클라이언트 설치 프로세스가 실패합니다.

```
Joining realm failed: Failed to add key to the keytab
child exited with 11

Installation failed. Rolling back changes.
```

이 오류는 빈 **Kerberos keytab**으로 인해 발생할 수 있습니다.

사전 요구 사항

- 시스템 파일을 제거하려면 **root** 권한이 필요합니다.

절차

1. **/etc/krb5.keytab**을 제거합니다.

```
[user@client ~]$ sudo rm /etc/krb5.keytab
[sudo] password for user:
[user@client ~]$ ls /etc/krb5.keytab
ls: cannot access '/etc/krb5.keytab': No such file or directory
```

2. **IdM** 클라이언트 설치를 다시 시도합니다.

추가 리소스

- 실패한 설치를 해결할 수 없고 **Red Hat** 기술 지원 서브스크립션이 있는 경우 **Red Hat** 고객 포털에서 기술 지원 케이스를 열고 **sosreport** 의 클라이언트를 제공합니다.

- **sosreport** 유틸리티는 **RHEL** 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. **sosreport** 유틸리티에 대한 자세한 내용은 **What is an sosreport and how to create one in Red Hat Enterprise Linux?** 를 참조하십시오.

17.4. 추가 리소스

- 첫 번째 **IdM** 서버 설치 문제를 해결하려면 **IdM** 서버 설치 문제 해결을 참조하십시오.

- **IdM** 복제본 설치 문제를 해결하려면 **IdM** 복제본 설치 문제 해결을 참조하십시오.

18장. IDM 클라이언트 다시 등록

18.1. IDM의 클라이언트 다시 등록

이 섹션에서는 IdM(Identity Management) 클라이언트를 다시 등록하는 방법을 설명합니다.

클라이언트 시스템이 삭제되고 IdM 서버와의 연결이 끊어진 경우(예: 클라이언트의 하드웨어 장애로 인해) 키탭이 있고 키를 다시 등록할 수 있습니다. 이 시나리오에서는 동일한 호스트 이름을 가진 IdM 환경에서 클라이언트를 다시 가져옵니다.

다시 등록할 때 클라이언트는 새 Kerberos 키 및 SSH 키를 생성하지만 LDAP 데이터베이스의 클라이언트 ID는 변경되지 않고 유지됩니다. 다시 등록한 후, 호스트에는 IdM 서버와 연결이 끊기기 전에 이전에와 동일한 FQDN 이 있는 동일한 LDAP 오브젝트에 키와 기타 정보가 있습니다.

중요

도메인 항목이 아직 활성 상태인 클라이언트만 다시 등록할 수 있습니다. 클라이언트(ipa-client-install --uninstall를 사용하여)를 설치 제거했거나 호스트 항목을 비활성화한 경우(ipa host-disable를 사용하여) 다시 등록할 수 없습니다.

이름을 바꾼 후에는 클라이언트를 다시 등록할 수 없습니다. 이는 IdM에서 LDAP의 클라이언트 항목의 키 속성이 클라이언트의 호스트 이름인 FQDN 이기 때문입니다. 클라이언트의 LDAP 오브젝트를 다시 등록하면 클라이언트의 이름 변경은 클라이언트의 키 및 기타 정보가 새 FQDN 이 있는 다른 LDAP 오브젝트의 키 및 기타 정보가 있음을 의미합니다. 따라서 클라이언트 이름을 바꾸는 유일한 방법은 IdM에서 호스트를 제거하고 호스트의 호스트 이름을 변경한 후 새 이름으로 IdM 클라이언트로 설치하는 것입니다. 클라이언트 이름 변경에 대한 자세한 내용은 IdM 클라이언트 시스템 복원 을 참조하십시오.

클라이언트 다시 등록 시 발생하는 사항

IdM을 다시 설치하는 동안 다음과 같습니다.

- 원래 호스트 인증서 취소
- 새 SSH 키 생성
- 새 키탭 생성

18.2. 사용자 자격 증명을 사용하여 클라이언트를 다시 시작하십시오. 대화형 재롤

이 절차에서는 권한 있는 사용자의 인증 정보를 사용하여 IdM(Identity Management) 클라이언트를 대화형으로 다시 할당하는 방법을 설명합니다.

1. 클라이언트 시스템을 동일한 호스트 이름으로 다시 생성합니다.

2. 클라이언트 시스템에서 ipa-client-install --force-join 명령을 실행합니다.

```
# ipa-client-install --force-join
```

3. 스크립트에서 클라이언트를 다시 할당하는 데 사용할 ID를 사용자에게 묻는 메시지를 표시합니다. 예를 들어 Enrollment Administrator 역할이 있는 hostadmin 사용자일 수 있습니다.

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

추가 리소스

- 인증된 사용자의 자격 증명을 사용하여 클라이언트를 등록하는 방법에 대한 자세한 내용은 사용자 인증 정보를 사용하여 클라이언트 설치를 참조하십시오. 대화형 설치.

18.3. 클라이언트 KEYTAB을 사용하여 클라이언트 다시 등록: 비대화형 재롤

사전 요구 사항

- 원래 클라이언트 키탭 파일(예: /tmp 또는 /root 디렉토리)을 백업합니다.

절차

이 절차에서는 클라이언트 시스템의 keytab을 사용하여 IdM(Identity Management) 클라이언트를 비대화형으로 다시 할당하는 방법을 설명합니다. 예를 들어 클라이언트 키 탭을 사용하여 다시 등록하면 자동화된 설치에 적합합니다.

1. 클라이언트 시스템을 동일한 호스트 이름으로 다시 생성합니다.

2. 백업 위치의 키탭 파일을 다시 생성한 클라이언트 시스템의 **/etc/** 디렉터리에 복사합니다.

3. **ipa-client-install** 유틸리티를 사용하여 클라이언트를 다시 등록하고 **--keytab** 옵션으로 키탭 위치를 지정합니다.

```
# ipa-client-install --keytab /etc/krb5.keytab
```

참고

--keytab 옵션에 지정된 키탭은 등록을 시작하도록 인증하는 경우에만 사용됩니다. 다시 등록할 때 **IdM**은 클라이언트에 대한 새 키탭을 생성합니다.

18.4. IDM 클라이언트 테스트

명령줄 인터페이스는 **ipa-client-install**에 성공했지만 자체 테스트를 수행할 수도 있음을 알려줍니다.

IdM(Identity Management) 클라이언트가 서버에 정의된 사용자에 대한 정보를 가져올 수 있는지 테스트하려면 서버에 정의된 사용자를 확인할 수 있는지 확인합니다. 예를 들어 기본 **admin** 사용자를 확인하려면 다음을 실행합니다.

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

인증이 올바르게 작동하는지 테스트하려면 루트 가 아닌 사용자의 **root** 사용자로 이동합니다.

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

19장. IDM 클라이언트 설치 제거

관리자는 환경에서 IdM(Identity Management) 클라이언트를 제거할 수 있습니다.

19.1. IDM 클라이언트 설치 제거

클라이언트를 제거하면 SSSD(System Security Services Daemon)와 같은 시스템 서비스의 모든 특정 IdM 구성과 함께 IdM(Identity Management) 도메인에서 클라이언트를 제거합니다. 그러면 클라이언트 시스템의 이전 구성이 복원됩니다.

절차

1. ipa-client-install --uninstall 명령을 입력합니다.

```
[root@client ~]# ipa-client-install --uninstall
```

2. 선택 사항: IdM 사용자에 대해 Kerberos 티켓(TGT)을 받을 수 없는지 확인합니다.

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting
initial credentials
[root@client ~]#
```

Kerberos TGT 티켓이 성공적으로 반환되면 IdM 클라이언트 설치 제거의 추가 제거 단계를 따르십시오. 이전의 여러 설치 후 추가 단계는 다음과 같습니다.

3. 클라이언트에서 /etc/krb5.keytab이 아닌 다른 각 키탭에서 이전 Kerberos 보안 주체를 제거합니다.

```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. IdM 서버에서 IdM에서 클라이언트 호스트의 모든 DNS 항목을 제거합니다.

```
[root@server ~]# ipa dnsrecord-del
Record name: old-client-name
Zone name: idm.example.com
No option to delete specific record provided.
```

```
Delete all? Yes/No (default No): yes
----------------------
Deleted record "old-client-name"
```

5. IdM 서버에서 IdM LDAP 서버에서 클라이언트 호스트 항목을 제거합니다. 이렇게 하면 모든 서비스가 제거되고 해당 호스트에 대해 발행된 모든 인증서가 취소됩니다.

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

중요

IdM LDAP 서버에서 클라이언트 호스트 항목을 제거하는 것은 다른 IP 주소 또는 다른 호스트 이름으로 나중에 클라이언트를 다시 등록할 때 중요합니다.

19.2. IDM 클라이언트 설치 제거: 이전 여러 설치 후 추가 단계

IdM(Identity Management) 클라이언트로 호스트를 여러 번 설치 및 제거하는 경우 제거 프로시저가 사전 IdM Kerberos 구성을 복원하지 않을 수 있습니다.

이 경우 IdM Kerberos 구성을 수동으로 제거해야 합니다. 극단적인 경우 운영 체제를 다시 설치해야 합니다.

사전 요구 사항

- ipa-client-install --uninstall 명령을 사용하여 호스트에서 IdM 클라이언트 구성을 설치 제거합니다. 그러나 IdM 서버에서 IdM 사용자에 대한 Kerberos 티켓(TGT)을 계속 받을 수 있습니다.
- /var/lib/ipa-client/sysrestore 디렉터리가 비어 있으므로 디렉터리의 파일을 사용하여 시스템의 사전-IdM-client 구성을 복원할 수 없습니다.

절차

1. /etc/krb5.conf.ipa 파일을 확인합니다.
   - /etc/ krb5.conf.ipa 파일의 내용이 IdM 클라이언트를 설치하기 전에 jenkinsfile5.conf 파일의 내용과 동일한 경우 다음을 수행할 수 있습니다.

i. **/etc/krb5.conf** 파일을 삭제합니다.

```
# rm /etc/krb5.conf
```

ii. **/etc/krb5.conf.ipa** 파일의 이름을 **/etc/krb5.conf**로 바꿉니다.

```
# mv /etc/krb5.conf.ipa /etc/krb5.conf
```

- **IdM** 클라이언트 설치 전에 **/etc/ krb5.conf.ipa** 파일의 내용과 동일하지 않은 경우 운영 체제 설치 후 **Kerberos** 구성을 상태로 직접 복원할 수 있습니다.

i. **krb5-libs** 패키지를 다시 설치합니다.

```
# yum reinstall krb5-libs
```

종속성으로 이 명령은 또한 **jenkinsfile krb5-workstation** 패키지 및**/etc/krb5.conf** 파일의 원래 버전을 다시 설치합니다.

2. 존재하는 경우 **var/log/ipaclient-install.log** 파일을 제거하십시오.

검증 단계

- **IdM** 사용자 인증 정보를 가져옵니다. 이 실패는 다음과 같습니다.

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting
initial credentials
[root@r8server ~]#
```

이제 **/etc/krb5.conf** 파일이 팩토리 상태로 복원되었습니다. 따라서 호스트에서 **IdM** 사용자를 위한 **Kerberos TGT**를 가져올 수 없습니다.

20장. IDM 클라이언트 시스템 이름 변경

다음 섹션에서는 IdM(Identity Management) 클라이언트 시스템의 호스트 이름을 변경하는 방법을 설명합니다.

주의

클라이언트 이름 변경은 수동 절차입니다. 호스트 이름을 변경해야 하는 경우가 아니면 이 작업을 수행하지 마십시오.

IdM 클라이언트의 이름을 변경하려면 다음이 포함됩니다.

1. 호스트 준비 자세한 내용은 이름 변경을 위해 IdM 클라이언트 준비를 참조하십시오.
2. 호스트에서 IdM 클라이언트 설치 제거. 자세한 내용은 클라이언트 설치 제거를 참조하십시오.
3. 호스트 이름 변경 자세한 내용은 클라이언트 종료를 참조하십시오.
4. 새 이름으로 호스트에 IdM 클라이언트 설치. 자세한 내용은 클라이언트 재설치를 참조하십시오.
5. IdM 클라이언트 설치 후 호스트 구성. 자세한 내용은 서비스 다시 추가, 인증서 다시 생성 및 호스트 그룹 다시 추가를 참조하십시오.

20.1. 이름 변경을 위해 IDM 클라이언트 준비

현재 클라이언트를 제거하기 전에 클라이언트의 특정 설정을 기록해 둡니다. 시스템을 새 호스트 이름으로 다시 등록한 후 이 설정을 적용합니다.

- 시스템에서 실행 중인 서비스를 확인합니다.

- **ipa service-find** 명령을 사용하고 출력의 인증서로 서비스를 식별합니다.

```
$ ipa service-find old-client-name.example.com
```

- 또한 각 호스트에는 **ipa *service-find*** 출력에 표시되지 않는 기본 호스트 서비스가 있습니다. 호스트 주체라고도 하는 호스트 서비스에 대한 서비스 *주체*는 ***host /old-client-name.example.com*** 입니다.

- **ipa service-find *old-client-name.example.com*** 에서 표시되는 모든 서비스 주체의 경우 ***old-client-name.example.com*** 시스템에서 해당 키 탭의 위치를 확인합니다.

```
# find / -name "*.keytab"
```

클라이언트 시스템의 각 서비스에는 ***service_name/host_name@REALM*** 형식의 **Kerberos** 주체(예: **ldap/ old-client-name.example.com@EXAMPLE.COM**)가*있습니다*.

- 시스템이 속한 모든 호스트 그룹을 식별합니다.

```
# ipa hostgroup-find old-client-name.example.com
```

20.2. IDM 클라이언트 설치 제거

클라이언트를 제거하면 **SSSD(System Security Services Daemon)**와 같은 시스템 서비스의 모든 특정 **IdM** 구성과 함께 **IdM(Identity Management)** 도메인에서 클라이언트를 제거합니다. 그러면 클라이언트 시스템의 이전 구성이 복원됩니다.

절차

1. **ipa-client-install --uninstall** 명령을 입력합니다.

```
[root@client ~]# ipa-client-install --uninstall
```

2. 선택 사항: **IdM** 사용자에 대해 **Kerberos** 티켓(**TGT**)을 받을 수 없는지 확인합니다.

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting
initial credentials
[root@client ~]#
```

- Kerberos TGT 티켓이 성공적으로 반환되면 IdM 클라이언트 설치 제거의 추가 제거 단계를 따르십시오. 이전의 여러 설치 후 추가 단계는 다음과 같습니다.

3. 클라이언트에서 /etc/krb5.keytab이 아닌 다른 각 키탭에서 이전 Kerberos 보안 주체를 제거합니다.

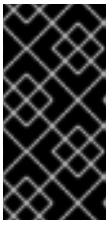
```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. IdM 서버에서 IdM에서 클라이언트 호스트의 모든 DNS 항목을 제거합니다.

```
[root@server ~]# ipa dnsrecord-del
Record name: old-client-name
Zone name: idm.example.com
No option to delete specific record provided.
Delete all? Yes/No (default No): yes
----------------------
Deleted record "old-client-name"
```

5. IdM 서버에서 IdM LDAP 서버에서 클라이언트 호스트 항목을 제거합니다. 이렇게 하면 모든 서비스가 제거되고 해당 호스트에 대해 발행된 모든 인증서가 취소됩니다.

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



중요

IdM LDAP 서버에서 클라이언트 호스트 항목을 제거하는 것은 다른 IP 주소 또는 다른 호스트 이름으로 나중에 클라이언트를 다시 등록할 때 중요합니다.

20.3. IDM 클라이언트 설치 제거: 이전 여러 설치 후 추가 단계

IdM(Identity Management) 클라이언트로 호스트를 여러 번 설치 및 제거하는 경우 제거 프로시저가 사전 IdM Kerberos 구성을 복원하지 않을 수 있습니다.

이 경우 IdM Kerberos 구성을 수동으로 제거해야 합니다. 극단적인 경우 운영 체제를 다시 설치해야 합니다.

사전 요구 사항

- **ipa-client-install --uninstall** 명령을 사용하여 호스트에서 **IdM** 클라이언트 구성을 설치 제거합니다. 그러나 **IdM** 서버에서 **IdM** 사용자에 대한 **Kerberos** 티켓**(TGT)**을 계속 받을 수 있습니다.

- **/var/lib/ipa-client/sysrestore** 디렉터리가 비어 있으므로 디렉터리의 파일을 사용하여 시스템의 사전**-IdM-client** 구성을 복원할 수 없습니다.

절차

1. **/etc/krb5.conf.ipa** 파일을 확인합니다.

   - **/etc/ krb5.conf.ipa** 파일의 내용이 **IdM** 클라이언트를 설치하기 전에 **jenkinsfile5.conf** 파일의 내용과 동일한 경우 다음을 수행할 수 있습니다.

     i. **/etc/krb5.conf** 파일을 삭제합니다.

     ```
     # rm /etc/krb5.conf
     ```

     ii. **/etc/krb5.conf.ipa** 파일의 이름을 **/etc/krb5.conf**로 바꿉니다.

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - **IdM** 클라이언트 설치 전에 **/etc/ krb5.conf.ipa** 파일의 내용과 동일하지 않은 경우 운영 체제 설치 후 **Kerberos** 구성을 상태로 직접 복원할 수 있습니다.

     i. **krb5-libs** 패키지를 다시 설치합니다.

     ```
     # yum reinstall krb5-libs
     ```

     종속성으로 이 명령은 또한 **jenkinsfile krb5-workstation** 패키지 및**/etc/krb5.conf** 파일의 원래 버전을 다시 설치합니다.

2. 존재하는 경우 **var/log/ipaclient-install.log** 파일을 제거하십시오.

검증 단계

- IdM 사용자 인증 정보를 가져옵니다. 이 실패는 다음과 같습니다.

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting
initial credentials
[root@r8server ~]#
```

이제 /etc/krb5.conf 파일이 팩토리 상태로 복원되었습니다. 따라서 호스트에서 IdM 사용자를 위한 Kerberos TGT를 가져올 수 없습니다.

20.4. 호스트 시스템 이름 변경

필요에 따라 머신의 이름을 바꿉니다. 예를 들어 다음과 같습니다.

```
# hostnamectl set-hostname new-client-name.example.com
```

새 호스트 이름을 사용하여 IdM(Identity Management) 클라이언트를 IdM 도메인에 다시 설치할 수 있습니다.

20.5. IDM 클라이언트 다시 설치

클라이언트 설치에 설명된 절차에 따라 이름이 지정된 호스트에 클라이언트를 설치합니다.

20.6. 서비스 다시 추가, 인증서 다시 생성, 호스트 그룹 다시 추가

IdM(Identity Management) 서버에서 이름 변경을 위해 IdM 클라이언트 준비에서 확인된 모든 서비스에 대해 새 키탭을 추가합니다.

+

```
[root@server ~]# ipa service-add service_name/new-client-name
```

1. 이름 변경을 위해 IdM 클라이언트 준비에 할당된 인증서가 할당된 서비스에 대한 인증서를 생성합니다. 이 작업을 수행할 수 있습니다.

- IdM 관리 툴 사용
- certmonger 유틸리티 사용

2. 이름 변경을 위해 IdM 클라이언트 준비에 확인된 호스트 그룹에 클라이언트를 다시 추가합니다.

21장. IDM 복제본 설치를 위한 시스템 준비

다음 링크에는 IdM(Identity Management) 복제본을 설치하는 요구 사항이 나열되어 있습니다. 설치하기 전에 시스템이 이러한 요구 사항을 충족하는지 확인하십시오.

1. 대상 시스템이 IdM 서버 설치에 대한 일반적인 요구 사항을 충족하는지 확인합니다.
2. 대상 시스템이 IdM 복제본 설치에 대한 추가 요구 사항을 충족하는지 확인합니다.
3. IdM 도메인에 등록할 대상 시스템에 권한을 부여합니다. 자세한 내용은 요구 사항에 가장 적합한 다음 섹션 중 하나를 참조하십시오.
   - IdM 클라이언트에 복제본 설치 승인
   - IdM에 등록되지 않은 시스템에 복제본 설치 승인

21.1. 복제본 버전 요구 사항

RHEL (Red Hat Enterprise Linux) 8 복제본은 RHEL 7.4 이상에서 실행되는 IdM(Identity Management) 서버에서만 작동합니다. RHEL 8에서 실행되는 IdM 복제본을 기존 배포에 도입하기 전에 모든 IdM 서버를 RHEL 7.4 이상으로 업그레이드하고 도메인 수준을 1로 변경합니다.

또한 복제본은 동일한 버전 또는 이후 버전의 IdM을 실행해야 합니다. 예를 들어 다음과 같습니다.

- Red Hat Enterprise Linux 8에 IdM 서버가 설치되어 있으며 IdM 4.x 패키지를 사용합니다.
- Red Hat Enterprise Linux 8 이상에도 복제본을 설치하고 IdM 버전 4.x 이상을 사용해야 합니다.

이렇게 하면 구성에서 서버에서 복제본으로 올바르게 복사할 수 있습니다.

IdM 소프트웨어 버전을 표시하는 방법에 대한 자세한 내용은 IdM 소프트웨어 버전을 표시하는 방법을 참조하십시오.

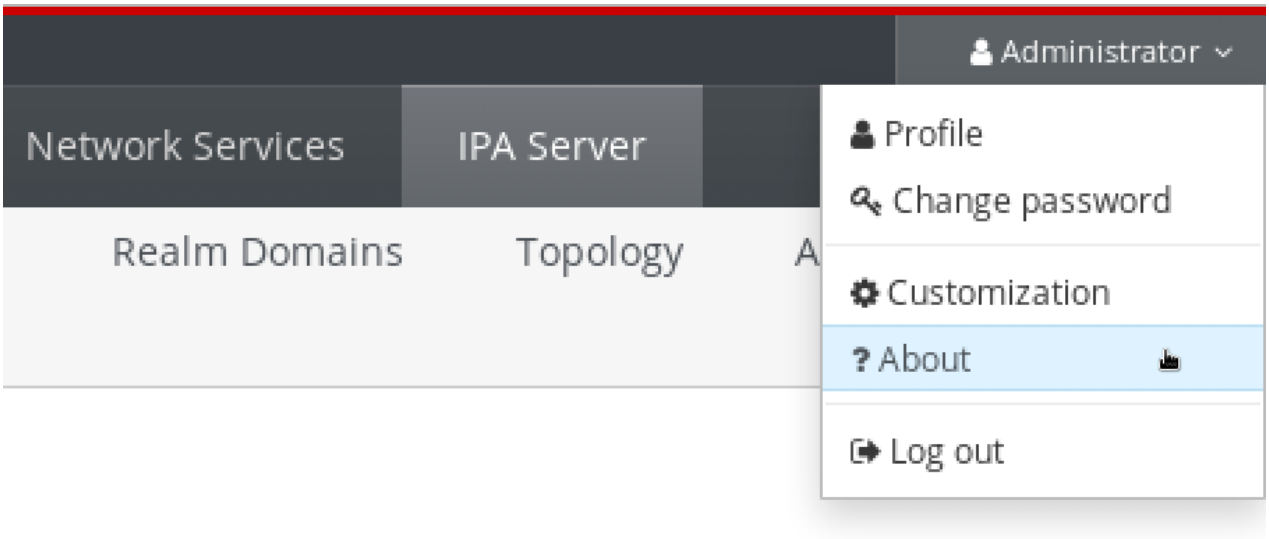
21.2. IDM 소프트웨어 버전을 표시하는 방법

다음과 같이 IdM 버전 번호를 표시할 수 있습니다.

- IdM WebUI
- ipa 명령
- rpm 명령

웹 UI를 통해 버전 표시

IdM WebUI의 오른쪽 상단에 있는 사용자 이름 메뉴에서 About을 선택하여 소프트웨어 버전을 표시할 수 있습니다.



ipa 명령으로 버전 표시

명령줄에서 ipa --version 명령을 사용합니다.

```
[root@server ~]# ipa --version
VERSION: 4.8.0, API_VERSION: 2.233
```

rpm 명령으로 버전 표시

IdM 서비스가 제대로 작동하지 않는 경우 rpm 유틸리티를 사용하여 현재 설치된 ipa-server 패키지의 버전 번호를 확인할 수 있습니다.

```
[root@server ~]# rpm -q ipa-server
ipa-server-4.8.0-11.module+el8.1.0+4247+9f3fd721.x86_64
```

21.3. IDM 클라이언트에 복제본 설치 승인

ipa- replica-install 유틸리티를 실행하여 기존 IdM(Identity Management) 클라이언트에 복제본을 설치할 때 아래의 방법 1 또는 방법 2 를 선택하여 복제본 설치를 승인합니다. 다음 중 하나가 적용되는 경우 Method 1을 선택합니다.

- 고급 시스템 관리자가 절차의 초기 부분을 수행하고 나머지를 수행하기 위해 하위 관리자가 필요합니다.
- 복제본 설치를 자동화하려고 합니다.

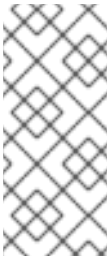
방법 1: ipaservers 호스트 그룹

1. IdM 관리자로 IdM 호스트에 로그인합니다.

```
$ kinit admin
```

2. ipaservers 호스트 그룹에 클라이언트 시스템을 추가합니다.

```
$ ipa hostgroup-add-member ipaservers --hosts client.idm.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.idm.example.com, client.idm.example.com
-------------------------
Number of members added 1
-------------------------
```



참고

ipaservers 그룹의 멤버십은 관리자의 자격 증명과 유사한 시스템 상승 권한을 부여합니다. 따라서 다음 단계에서 ipa-replica-install 유틸리티는 주니어 시스템 관리자가 성공적으로 호스트에서 실행할 수 있습니다.

방법 2: 권한 있는 사용자의 자격 증명

권한 있는 사용자의 자격 증명을 제공하여 복제본 설치를 승인하려면 다음 방법 중 하나를 선택합니다.

- ipa-replica-install 유틸리티를 시작한 후 IdM(Identity Management)에서 인증 정보를 대화식으로 표시하도록 합니다. 이는 기본 동작입니다.
- ipa-replica-install 유틸리티를 실행하기 전에 권한 있는 사용자로 클라이언트에 로그인합니다. 기본 권한 있는 사용자는 admin:

```
$ kinit admin
```

추가 리소스

- 설치 절차를 시작하려면 IdM 복제본 설치 를 참조하십시오.
- Ansible 플레이북을 사용하여 IdM 복제본을 설치할 수 있습니다. 자세한 내용은 Ansible 플레이북을 사용하여 Identity Management 복제본 설치를 참조하십시오.

21.4. IDM에 등록되지 않은 시스템에 복제본 설치 승인

IdM(Identity Management) 도메인에 등록되지 않은 시스템에 복제본을 설치할 때 ipa-replica-install 유틸리티는 먼저 시스템을 클라이언트로 등록한 다음 복제본 구성 요소를 설치합니다. 이 시나리오에서는 아래의 Method 1 또는 Method 2 를 선택하여 복제본 설치를 인증합니다. 다음 중 하나가 적용되는 경우 Method 1을 선택합니다.

- 고급 시스템 관리자가 절차의 초기 부분을 수행하고 나머지를 수행하기 위해 하위 관리자가 필요합니다.
- 복제본 설치를 자동화하려고 합니다.

방법 1: IdM 서버에서 생성된 임의의 암호

도메인의 모든 서버에서 다음 명령을 입력합니다.

1. 관리자로 로그인합니다.

```
$ kinit admin
```

2. 외부 시스템을 IdM 호스트로 추가합니다. ipa host-add 명령과 함께 --random 옵션을 사용하여 후속 복제본 설치에 사용할 임의의 일회성 암호를 생성합니다.

```
$ ipa host-add replica.example.com --random
--------------------------------------------------
Added host "replica.example.com"
--------------------------------------------------
  Host name: replica.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```

시스템을 IdM 도메인에 등록한 후 생성된 암호가 무효화됩니다. 등록 완료 후 적절한 호스트 키탭으로 교체됩니다.

3. 시스템을 ipaservers 호스트 그룹에 추가합니다.

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.example.com, replica.example.com
-------------------------
Number of members added 1
-------------------------
```

참고

ipaservers 그룹의 멤버십은 관리자의 자격 증명과 유사한 시스템 상승 권한을 부여합니다. 따라서 다음 단계에서 ipa-replica-install 유틸리티는 생성된 임의의 암호를 제공하는 주니어 시스템 관리자가 호스트에서 성공적으로 실행할 수 있습니다.

방법 2: 권한 있는 사용자의 자격 증명

이 방법을 사용하면 권한 있는 사용자의 인증 정보를 제공하여 복제본 설치를 인증합니다. 기본 권한 있는 사용자는 admin 입니다.

IdM 복제본 설치 유틸리티를 실행하기 전에 작업이 필요하지 않습니다. 설치 중에 직접 ipa-replica-install명령에 보안 주체 이름 및 암호 옵션(--principal *admin* --admin- *password*password)을 추가합니다.

추가 리소스

- 설치 절차를 시작하려면 IdM 복제본 설치 를 참조하십시오.

- Ansible 플레이북을 사용하여 IdM 복제본을 설치할 수 있습니다. 자세한 내용은 Ansible 플레이북을 사용하여 Identity Management 복제본 설치를 참조하십시오.

22장. IDM 복제본 설치

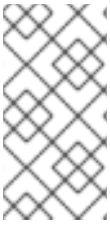
다음 섹션에서는 IdM(Identity Management) 복제본을 설치하는 방법을 설명합니다. 복제본 설치 프로세스는 기존 서버의 구성을 복사하고 해당 구성을 기반으로 복제본을 설치합니다.

사전 요구 사항

- 시스템이 IdM 복제본 설치를 준비 했는지 확인합니다.

중요

이 준비 작업이 수행되지 않으면 IdM 복제본을 설치하면 실패합니다.



참고

한 번에 하나의 IdM 복제본을 설치합니다. 동시에 여러 복제본을 설치하는 것은 지원되지 않습니다.

절차

개별 유형의 복제본 설치 프로시저는 다음을 참조하십시오.

- 22.1절. “통합된 DNS 및 CA를 사용하여 IdM 복제본 설치”
- 22.2절. “CA가 없는 통합 DNS를 사용하여 IdM 복제본 설치”
- 22.3절. “통합된 DNS 및 CA를 사용하지 않고 IdM 복제본 설치”
- 22.4절. “통합 DNS 없이 IdM 복제본 설치 및 CA 없음”
- 22.5절. “IdM 숨겨진 복제본 설치”

복제본 설치 절차의 문제를 해결하려면 다음을 참조하십시오.

- 23장. *IdM 복제본 설치 문제 해결*

설치 후 다음을 참조하십시오.

- 22.6절. “IdM 복제본 테스트”

22.1. 통합된 DNS 및 CA를 사용하여 IDM 복제본 설치

이 절차에서는 IdM(Identity Management) 복제본 설치를 설명합니다.

- 통합 DNS 사용
- 인증 기관(CA) 사용

예를 들어 통합 CA를 사용하여 IdM 서버를 설치한 후 복원력을 위해 CA 서비스를 복제할 수 있습니다.

중요

CA를 사용하여 복제본을 구성할 때 복제본의 CA 구성은 다른 서버의 CA 구성을 미러링해야 합니다.

예를 들어 서버에 통합 IdM CA가 루트 CA로 포함된 경우 새 복제본도 루트 CA로 통합 CA를 사용하여 설치해야 합니다. 이 경우 다른 CA 구성은 사용할 수 없습니다.

ipa-replica-install 명령에 --setup-ca 옵션을 포함하면 초기 서버의 CA 구성이 복사됩니다.

사전 요구 사항

- 시스템이 IdM 복제본 설치를 준비 했는지 확인합니다.

절차

1. 다음 옵션을 사용하여 **ipa-replica-install** 을 입력합니다.

- **--setup-dns:** 복제본을 **DNS** 서버로 구성

- **--forwarder:** 서버별 전달자를 사용하지 않으려면 **--forwarder** 또는 **--no-forwarder** 를 지정합니다. 페일오버 이유로 여러 서버별 전달자를 지정하려면 **--forwarder** 를 여러 번 사용합니다.

참고

ipa-replica-install 유틸리티는 **DNS** 설정과 관련된 다른 여러 옵션(예: **--no-reverse** 또는 **--no-host-dns**)을 허용합니다. 이에 대한 자세한 내용은 **ipa-replica-install(1)** 매뉴얼 페이지를 참조하십시오.

- **--setup-ca -** 복제본에 **CA**를 포함

예를 들어 통합 **DNS** 서버와 **IdM** 서버에서 관리하지 않는 모든 **DNS** 요청을 **IP 192.0.2.1**에서 실행되는 **DNS** 서버로 전달하는 **CA**를 설정하려면 다음을 실행합니다.

```
# ipa-replica-install --setup-dns --forwarder 192.0.2.1 --setup-ca
```

2. 설치가 완료되면 상위 도메인의 **DNS** 위임을 **IdM DNS** 도메인에 추가합니다. 예를 들어 **IdM DNS** 도메인이 **idm.example.com** 인 경우 **example.com** 상위 도메인에 이름 서버(**NS**) 레코드를 추가합니다.

중요

IdM DNS 서버를 설치한 후 매번 이 단계를 반복합니다.

22.2. CA가 없는 통합 DNS를 사용하여 IDM 복제본 설치

이 절차에서는 **IdM(Identity Management)** 복제본 설치를 설명합니다.

- 통합 **DNS** 사용

- CA가 이미 설치되어 있는 IdM 환경의 CA(인증 기관)가 없으면. 복제본이 CA가 설치된 IdM 서버에 모든 인증서 작업을 전달합니다.

사전 요구 사항

- 시스템이 IdM 복제본 설치를 준비 했는지 확인합니다.

절차

1. 다음 옵션을 사용하여 ipa-replica-install 을 입력합니다.

   - --setup-dns: 복제본을 DNS 서버로 구성

   - --forwarder: 서버별 전달자를 사용하지 않으려면 --forwarder 또는 --no-forwarder 를 지정합니다. 페일오버 이유로 여러 서버별 전달자를 지정하려면 --forwarder 를 여러 번 사용합니다.

   예를 들어 IdM 서버에서 관리하지 않는 모든 DNS 요청을 IP 192.0.2.1에서 실행되는 DNS 서버로 전달하는 통합 DNS 서버로 복제본을 설정하려면 다음을 실행합니다.

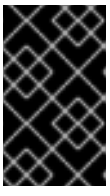
   ```
   # ipa-replica-install --setup-dns --forwarder 192.0.2.1
   ```

   참고

   ipa-replica-install 유틸리티는 DNS 설정과 관련된 다른 여러 옵션(예: --no-reverse 또는 --no-host-dns)을 허용합니다. 이에 대한 자세한 내용은 ipa-replica-install(1) 매뉴얼 페이지를 참조하십시오.

2. 설치가 완료되면 상위 도메인의 DNS 위임을 IdM DNS 도메인에 추가합니다. 예를 들어 IdM DNS 도메인이 idm.example.com 인 경우 example.com 상위 도메인에 이름 서버(NS) 레코드를 추가합니다.

   중요

   IdM DNS 서버를 설치한 후 매번 이 단계를 반복합니다.

22.3. 통합된 DNS 및 CA를 사용하지 않고 IDM 복제본 설치

이 절차에서는 IdM(Identity Management) 복제본 설치를 설명합니다.

- 통합 DNS 없음
- 인증 기관(CA) 사용

중요

CA를 사용하여 복제본을 구성할 때 복제본의 CA 구성은 다른 서버의 CA 구성을 미러링해야 합니다.

예를 들어 서버에 통합 IdM CA가 루트 CA로 포함된 경우 새 복제본도 루트 CA로 통합 CA를 사용하여 설치해야 합니다. 이 경우 다른 CA 구성은 사용할 수 없습니다.

ipa-replica-install 명령에 --setup-ca 옵션을 포함하면 초기 서버의 CA 구성이 복사됩니다.

사전 요구 사항

- 시스템이 IdM 복제본 설치를 준비 했는지 확인합니다.

절차

1. --setup-ca 옵션을 사용하여 ipa-replica-install 을 입력합니다.

```
# ipa-replica-install --setup-ca
```

2. 새로 생성된 IdM DNS 서비스 레코드를 DNS 서버에 추가합니다.

   a. IdM DNS 서비스 레코드를 nsupdate 형식의 파일로 내보냅니다.

```
$ ipa dns-update-system-records --dry-run --out dns_records_file.nsupdate
```

b.

nsupdate 유틸리티 및 **dns_ historys_file.nsupdate** 파일을 사용하여 **DNS** 서버에 **DNS** 업데이트 요청을 제출합니다. 자세한 내용은 **RHEL 7** 설명서에서 **nsupdate**를 사용하여 외부 **DNS** 레코드 업데이트에서 참조하십시오. 또는 **DNS** 레코드 추가에는 **DNS** 서버 설명서를 참조하십시오.

22.4. 통합 DNS 없이 IDM 복제본 설치 및 CA 없음

이 절차에서는 **IdM(Identity Management)** 복제본 설치를 설명합니다.

- 통합 **DNS** 없음
- 필요한 인증서를 수동으로 제공하여 **CA**(인증 기관)가 없는 경우. 여기서 가정은 첫 번째 서버가 **CA** 없이 설치되었다는 것입니다.

중요

가져온 인증서 파일에는 **LDAP** 및 **Apache** 서버 인증서를 발급한 **CA**의 전체 **CA** 인증서 체인이 포함되어야 하므로 자체 서명된 타사 서버 인증서를 사용하여 서버 또는 복제본을 설치할 수 없습니다.

사전 요구 사항

- 시스템이 **IdM** 복제본 설치를 준비 했는지 확인합니다.

절차

- **ipa-replica-install** 을 입력하고 다음 옵션을 추가하여 필요한 인증서 파일을 제공합니다.
  - **--dirsrv-cert-file**
  - **--dirsrv-pin**
  - **--http-cert-file**

- **--http-pin**

이러한 옵션을 사용하여 제공되는 파일에 대한 자세한 내용은 5.1절. “CA 없이 IdM 서버를 설치하는 데 필요한 인증서” 을 참조하십시오.

예를 들어 다음과 같습니다.

```
# ipa-replica-install \
   --dirsrv-cert-file /tmp/server.crt \
   --dirsrv-cert-file /tmp/server.key \
   --dirsrv-pin secret \
   --http-cert-file /tmp/server.crt \
   --http-cert-file /tmp/server.key \
   --http-pin secret
```

참고

--ca-cert-file 옵션을 추가하지 마십시오. **ipa-replica-install** 유틸리티는 설치한 첫 번째 서버에서 자동으로 인증서 정보의 이 부분을 사용합니다.

22.5. IDM 숨겨진 복제본 설치

숨겨진(연결할 수 없음) 복제본은 모든 서비스가 실행 중이고 사용 가능한 **IdM(Identity Management)** 서버입니다. 그러나 **DNS**에 **SRV** 레코드가 없으며 **LDAP** 서버 역할은 활성화되지 않습니다. 따라서 클라이언트는 서비스 검색을 사용하여 이러한 숨겨진 복제본을 감지할 수 없습니다.

숨겨진 복제본에 대한 자세한 내용은 숨겨진 복제본 모드 를 참조하십시오.

사전 요구 사항

- 시스템이 IdM 복제본 설치를 준비 했는지 확인합니다.

절차

- 숨겨진 복제본을 설치하려면 다음 명령을 사용하십시오.

```
ipa-replica-install --hidden-replica
```

이 명령은 **DNS SRV** 레코드가 없고 **LDAP** 서버 역할이 비활성화된 복제본을 설치합니다.

기존 복제본의 모드를 **hidden**으로 변경할 수도 있습니다. 자세한 내용은 숨겨진 복제본의 데모 및 승격 을 참조하십시오.

22.6. IDM 복제본 테스트

복제본을 생성한 후 복제본이 데이터를 예상대로 복제하는지 확인합니다. 다음 절차를 사용할 수 있습니다.

절차

1. 새 복제본에 사용자를 생성합니다.

```
[admin@new_replica ~]$ ipa user-add test_user
```

2. 사용자가 다른 복제본에 표시되는지 확인합니다.

```
[admin@another_replica ~]$ ipa user-show test_user
```

22.7. IDM 복제본 설치 중 수행되는 연결

IdM 복제본 설치 중 수행된 요청에는 **ipa-replica-install, IdM(Identity Management)** 복제본 설치 도구에서 수행하는 작업이 나열됩니다.

표 22.1. IdM 복제본 설치 중 수행되는 요청

작업	사용된 프로토콜	목적
클라이언트 시스템에 구성된 DNS 해석기에 대한 DNS 확인	DNS	IdM 서버의 IP 주소 검색
검색된 IdM 서버의 포트 88(TCP/TCP6 및 UDP/UDP6)에 대한 요청	Kerberos	Kerberos 티켓을 얻으려면
검색된 또는 구성된 IdM 서버의 IdM Apache 기반 웹 서비스에 대한 JSON-RPC 호출	HTTPS	IdM 클라이언트 등록, 필요한 경우 복제본 키 검색 및 인증서 발행

작업	사용된 프로토콜	목적
SASL GSSAPI 인증, 일반 LDAP 또는 둘 다를 사용하여 IdM 서버의 포트 389에 TCP/TCP6을 통한 요청	LDAP	IdM 클라이언트 등록, CA 인증서 체인 검색, LDAP 데이터 복제
IdM 서버의 포트 22에 TCP/TCP6을 통한 요청	SSH	연결이 작동하는지 확인하려면 다음을 수행하십시오.
(선택 사항) IdM 서버의 포트 8443(TCP/TCP6)을 통한 액세스	HTTPS	IdM 서버에서 인증 기관을 관리하려면 (IdM 서버 및 복제본 설치 중에만 해당)

23장. IDM 복제본 설치 문제 해결

다음 섹션에서는 실패한 IdM 복제본 설치에 대한 정보와 몇 가지 일반적인 설치 문제를 해결하는 방법을 설명합니다.

23.1. IDM 복제본 설치 오류 검토

이 절차에서는 IdM 복제본 실패 문제를 해결하는 방법을 설명합니다.

IdM(Identity Management) 복제본을 설치할 때 복제본의 다음 로그 파일에 디버깅 정보가 추가됩니다.

- /var/log/ipareplica-install.log
- /var/log/ipareplica-conncheck.log
- /var/log/ipaclient-install.log
- /var/log/httpd/error_log
- /var/log/dirsrv/slapd-*INSTANCE-NAME*/access
- /var/log/dirsrv/slapd-*INSTANCE-NAME*/errors
- /var/log/ipaserver-install.log

또한 복제본 설치 프로세스에서는 복제본에 연결할 IdM 서버의 다음 로그 파일에 디버깅 정보를 추가합니다.

- /var/log/httpd/error_log

- /var/log/dirsrv/slapd-*INSTANCE-NAME*/access

- /var/log/dirsrv/slapd-*INSTANCE-NAME*/errors

각 로그 파일의 마지막 줄은 성공 또는 실패를 보고하고 **ERROR** 및 **DEBUG** 항목은 추가 컨텍스트를 제공합니다.

실패한 IdM 복제본 설치 문제를 해결하려면 두 호스트(복제본 및 서버)에서 이러한 로그 파일 끝에 있는 오류를 검토하고 이 정보를 사용하여 해당 문제를 해결합니다.

사전 요구 사항

- IdM 로그 파일의 내용을 표시하려면 root 권한이 있어야 합니다.

절차

1. **tail** 명령을 사용하여 기본 로그 파일 /var/log/ipareplica-install.log의 최신 오류를 표시합니다. 다음 예제에서는 마지막 10행을 표시합니다.

```
[user@replica ~]$ sudo tail -n 10 /var/log/ipareplica-install.log
[sudo] password for user:
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line
424, in decorated
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line
785, in promote_check
  ensure_enrolled(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line
740, in ensure_enrolled
  raise ScriptError("Configuration of client side components failed!")

2020-05-28T18:24:51Z DEBUG The ipa-replica-install command failed, exception:
ScriptError: Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR The ipa-replica-install command failed. See
/var/log/ipareplica-install.log for more information
```

2. 로그 파일을 대화형으로 검토하려면 **less** 유틸리티를 사용하여 로그 파일의 끝을 열고 ↑ 및 ↓ 화살표 키를 사용하여 이동합니다.

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-install.log
```

3. (선택 사항) /var/log/ipareplica-install.log는 복제본 설치의 기본 로그 파일이지만, 복제본 및 서버의 추가 파일과 함께 이 검토 프로세스를 반복하여 추가 문제 해결 정보를 수집할 수 있습니다.

복제본에서 다음을 수행합니다.

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-conncheck.log
[user@replica ~]$ sudo less -N +G /var/log/ipaclient-install.log
[user@replica ~]$ sudo less -N +G /var/log/httpd/error_log
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
[user@replica ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

서버에서 다음을 수행합니다.

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

추가 리소스

- 실패한 복제본 설치를 확인할 수 없고 Red Hat 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 sosreport를 복제본 및 서버의 sosreport를 제공합니다.
- sosreport 유틸리티는 RHEL 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. sosreport 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

23.2. IDM CA 설치 오류 검토

IdM(Identity Management) 복제본에 CA(인증 기관) 서비스를 설치하면 복제본과 통신하는 IdM 서버의 여러 위치에 디버깅 정보가 추가됩니다.

표 23.1. 복제본(권장된 우선 순위대로)에서 다음을 수행합니다.

위치	설명
/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log	**pkispawn** 설치 프로세스의 상위 수준 문제 및 Python 추적
journalctl -u pki-tomcatd@pki-tomcat output	**pki-tomcatd@pki-tomcat** 서비스의 오류
/var/log/pki/pki-tomcat/ca/debug.*$DATE*.log	PKI(Public Key Infrastructure) 제품의 핵심에 있는 대규모 JAVA 스택 추적
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit	PKI 제품의 감사 로그
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.*$DATE*.log**	인증서를 사용하는 서비스 주체, 호스트 및 기타 엔티티에 대한 인증서 작업의 낮은 수준의 디버그 데이터

복제본에서 연결하는 서버에서 다음을 수행합니다.

- **/var/log/httpd/error_log** 로그 파일

기존 IdM 복제본에 CA 서비스를 설치하면 디버깅 정보도 다음 로그 파일에 기록됩니다.

- **/var/log/ipareplica-ca-install.log** 로그 파일

참고

선택적 CA 구성 요소를 설치하는 동안 전체 IdM 복제본 설치에 실패하면 CA에 대한 세부 정보가 기록되지 않습니다. /var/log/ipareplica-install.log 파일에 로그인되어 전체 설치 프로세스가 실패했음을 나타냅니다. CA 설치 실패와 관련된 자세한 내용은 위에 나열된 로그 파일을 검토하는 것이 좋습니다.

이 동작에 대한 유일한 예외는 CA 서비스를 설치하고 루트 CA가 외부 CA인 경우입니다. 외부 CA에서 인증서에 문제가 있는 경우 /var/log/ipareplica-install.log에 오류가 기록됩니다.

실패한 IdM CA 설치 문제를 해결하려면 이러한 로그 파일 끝에 있는 오류를 검토하고 이 정보를 사용하여 해당 문제를 해결합니다.

사전 요구 사항

- IdM 로그 파일의 내용을 표시하려면 root 권한이 있어야 합니다.

절차

1. 로그 파일을 대화형으로 검토하려면 less 유틸리티를 사용하여 로그 파일의 끝을 열고 ScriptError 항목을 검색하는 동안 ↑ 및 ↓ 화살표 키를 사용하여 이동합니다. 다음 예제에서는 /var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log를 엽니다.

```
[user@server ~]$ sudo less -N +G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. 위에 나열된 모든 로그 파일과 함께 이 검토 프로세스를 반복하여 추가 문제 해결 정보를 수집합니다.

추가 리소스

- 실패한 IdM 서버 설치를 확인할 수 없고 Red Hat 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 sosreport의 서버를 제공합니다.

- sosreport 유틸리티는 RHEL 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. sosreport 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

23.3. 부분적인 IDM 복제본 설치 제거

IdM 복제본 설치에 실패하면 일부 구성 파일이 나중에 남아 있을 수 있습니다. IdM 복제본을 추가로 설치하려고 하면 실패할 수 있으며 설치 스크립트에서 IPA가 이미 구성되어 있다고 보고합니다.

기존 부분 IdM 구성이 있는 시스템 예

```
[root@server ~]# ipa-replica-install
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --
uninstall'.
The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

이 문제를 해결하려면 복제본에서 IdM 소프트웨어를 제거하고, IdM 토폴로지에서 복제본을 제거한 다음 설치 프로세스를 다시 시도합니다.

사전 요구 사항

- root 권한이 있어야 합니다.

절차

1. IdM 복제본으로 구성하려는 호스트에서 IdM 서버 소프트웨어를 설치 제거합니다.

```
[root@replica ~]# ipa-server-install --uninstall
```

2. 토폴로지의 다른 모든 서버에서 ipa server-del 명령을 사용하여 제대로 설치하지 않은 복제본에 대한 참조를 삭제합니다.

```
[root@other-replica ~]# ipa server-del replica.idm.example.com
```

3. 복제본 설치를 시도합니다.

4. 반복적으로 실패한 설치로 인해 IdM 복제본을 설치하는 데 어려움이 있는 경우 운영 체제를 다시 설치하십시오.

IdM 복제본을 설치하기 위한 요구 사항 중 하나는 사용자 지정이 없는 클린 시스템입니다. 실패한 설치로 인해 시스템 파일을 예기치 않게 수정하여 호스트의 무결성이 손상될 수 있습니다.

추가 리소스

- IdM 복제본 설치 제거에 대한 자세한 내용은 IdM 복제본 설치 제거를 참조하십시오.
- 반복된 제거 시도 후 설치가 실패하고 Red Hat 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 sosreport를 복제본 및 서버의 sosreport를 제공합니다.
- sosreport 유틸리티는 RHEL 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. sosreport 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

23.4. 잘못된 인증 정보 오류 해결

Invalid credentials 오류로 인해 IdM 복제본 설치에 실패하면 호스트의 시스템 클럭이 서로 동기화되지 않을 수 있습니다.

```
[27/40]: setting up initial replication
Starting replication, please wait until this has completed.
Update in progress, 15 seconds elapsed
[ldap://server.example.com:389] reports: Update failed! Status: [49 - LDAP error: Invalid
credentials]

[error] RuntimeError: Failed to start replication
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    Failed to start
replication
ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    The ipa-replica-
install command failed. See /var/log/ipareplica-install.log for more information
```

클럭이 동기화되지 않는 동안 --no-ntp 또는 -N 옵션을 사용하여 복제본 설치를 시도하면 서비스가 Kerberos로 인증할 수 없기 때문에 설치에 실패합니다.

이 문제를 해결하려면 두 호스트의 클럭을 동기화하고 설치 프로세스를 다시 시도합니다.

사전 요구 사항

- 시스템 시간을 변경하려면 **root** 권한이 있어야 합니다.

절차

1. 시스템 클럭을 수동으로 또는 **chronyd**와 동기화합니다.

   수동으로 동기화

   서버에 시스템 시간을 표시하고 일치하도록 복제본의 시간을 설정합니다.

   ```
   [user@server ~]$ date
   Thu May 28 21:03:57 EDT 2020

   [user@replica ~]$ sudo timedatectl set-time '2020-05-28 21:04:00'
   ```

   - **chronyd**와 동기화:

     chrony 툴을 사용하여 시스템 시간을 구성 및 설정하도록 Chrony 제품군을 사용하여 NTP 구성을 참조하십시오.

2. **IdM** 복제본 설치를 다시 시도합니다.

추가 리소스

- 실패한 복제본 설치를 확인할 수 없고 **Red Hat** 기술 지원 서브스크립션이 있는 경우 Red Hat 고객 포털에서 기술 지원 케이스를 열고 **sosreport**를 복제본 및 서버의 **sosreport**를 제공합니다.

- **sosreport** 유틸리티는 **RHEL** 시스템에서 구성 세부 정보, 로그 및 시스템 정보를 수집합니다. **sosreport** 유틸리티에 대한 자세한 내용은 What is an sosreport and how to create one in Red Hat Enterprise Linux? 를 참조하십시오.

23.5. 추가 리소스

- 첫 번째 IdM 서버 설치 문제를 해결하려면 IdM 서버 설치 문제 해결을 참조하십시오.

- IdM 클라이언트 설치 문제를 해결하려면 IdM 클라이언트 설치 문제 해결을 참조하십시오.

24장. IDM 복제본 설치 제거

IdM 관리자는 토폴로지에서 IdM(Identity Management) 복제본을 제거할 수 있습니다. 자세한 내용은 IdM 서버 설치 제거를 참조하십시오.

25장. 기존 IDM 서버에 DNS 설치

이 섹션에서는 원래 설치된 IdM(Identity Management) 서버에 DNS 서비스를 설치하는 방법을 설명합니다.

사전 요구 사항

- 다음과 같이 IdM 서버 설치에 설명된 대로 통합 DNS와 함께 IdM을 사용할 때의 이점과 제한 사항을 이해할 수 있습니다. 통합 DNS를 사용하여 루트 CA로 통합 CA.
- IdM 서버에 대한 루트 액세스 권한이 있습니다.

절차

1. [선택 사항] DNS가 IdM 서버에 설치되어 있지 않은지 확인합니다.

```
[root@r8server ~]# ipa server-role-show r8server.idm.example.com
Role name: DNS server
  Server name: r8server.idm.example.com
  Role name: DNS server
  Role status: absent
```

출력은 IdM DNS를 서버에서 사용할 수 없음을 확인합니다.

2. idm:DL1 스트림을 활성화합니다.

```
[root@r8server ~]# yum module enable idm:DL1
```

3. ipa-dns-server 패키지 및 해당 종속 항목을 다운로드합니다.

```
[root@r8server ~]# yum module install idm:DL1/dns
```

4. 스크립트를 시작하여 서버에 DNS를 설치합니다.

```
[root@r8server ~]# ipa-dns-install
```

a.

스크립트에서 서버별 **DNS** 전달자를 입력하라는 메시지를 표시합니다.

```
Do you want to configure DNS forwarders? [yes]:
```

- 서버별 **DNS** 전달자를 구성하려면 **yes** 를 입력한 다음 명령줄의 지침을 따릅니다. 설치 프로세스에서 **IdM LDAP**에 전달자 **IP** 주소를 추가합니다.
  - 전달 정책 기본 설정의 경우 **ipa-dns-install(1)** 도움말 페이지의 **--forward-policy** 설명을 참조하십시오.
- **DNS** 전달을 사용하지 않으려면 **no** 를 입력합니다.

DNS 전달자가 없으면 **IdM** 도메인의 호스트에서 인프라의 다른 내부 **DNS** 도메인의 이름을 확인할 수 없습니다. 호스트는 **DNS** 쿼리를 확인하기 위해 공용 **DNS** 서버에서만 유지됩니다.

b.

스크립트에서 서버와 연결된 **IP** 주소에 대한 **DNS** 역방향(**PTR**) 레코드가 구성되어 있는지 확인하라는 메시지가 표시됩니다.

```
Do you want to search for missing reverse zones? [yes]:
```

검색 및 누락된 역방향 영역을 실행하는 경우 스크립트는 **PTR** 레코드와 함께 역방향 영역을 생성할지 여부를 요청합니다.

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

참고

IdM을 사용하여 역방향 영역을 관리하는 것은 선택 사항입니다. 대신 외부 **DNS** 서비스를 사용할 수 있습니다.

추가 리소스

- **man ipa-dns-install(1)**

26장. CA 없이 배포에서 IDM 서버에 IDM CA 서비스 추가

CA(인증 기관) 구성 요소 없이 IdM(Identity Management) 도메인을 이전에 설치한 경우 ipa-ca-install 명령을 사용하여 도메인에 IdM CA 서비스를 추가할 수 있습니다. 요구 사항에 따라 다음 옵션 중 하나를 선택할 수 있습니다.

- IdM 인증서 서버 CA를 루트 CA로 추가합니다.
- 외부 CA를 루트 CA로 사용하여 IdM 인증서 서버 CA를 하위 CA로 추가합니다.

참고

지원되는 CA 구성에 대한 자세한 내용은 CA 서비스 플래닝을 참조하십시오.

26.1. 첫 번째 IDM CA를 기존 IDM 도메인에 루트 CA로 설치

이전에 CA(인증 기관) 구성 요소 없이 IdM(Identity Management)을 설치한 경우 나중에 IdM 서버에 CA를 설치할 수 있습니다. 이 절차에서는 외부 루트 CA에 종속적이지 않은 IdM CA인 *idmserver* 서버에 설치하는 방법을 설명합니다.

사전 요구 사항

- *idmserver* 에 대한 루트 권한이 있습니다.
- IdM 서버는 *idmserver* 에 설치되어 있습니다.
- IdM 배포에 CA가 설치되지 않았습니다.
- IdM 디렉터리 관리자 암호를 알고 있습니다.

절차

1. *idmserver* 에서 IdM 인증서 서버 CA를 설치합니다.

```
[root@idmserver ~] ipa-ca-install
```

2. 토폴로지의 각 IdM 호스트에서 ipa-certupdate 유틸리티를 실행하여 IdM LDAP의 새 인증서에 대한 정보로 호스트를 업데이트합니다.

중요

IdM CA 인증서를 생성한 후 ipa-certupdate 를 실행하지 않으면 인증서가 다른 IdM 시스템에 배포되지 않습니다.

26.2. 기존 IDM 도메인에 외부 CA를 루트 CA로 포함하는 첫 번째 IDM CA 설치

이전에 CA(인증 기관) 구성 요소 없이 IdM(Identity Management)을 설치한 경우 나중에 IdM 서버에 CA를 설치할 수 있습니다. 이 절차에서는 *idmserver* 서버에서 0개 또는 여러 중간 CA가 있는 외부 루트 CA에 해당하는 IdM CA를 설치하는 방법을 설명합니다.

사전 요구 사항

- *idmserver* 에 대한 루트 권한이 있습니다.
- IdM 서버는 *idmserver* 에 설치되어 있습니다.
- IdM 배포에 CA가 설치되지 않았습니다.
- IdM 디렉터리 관리자 암호를 알고 있습니다.

절차

1. 설치를 시작합니다.

```
[root@idmserver ~] ipa-ca-install --external-ca
```

2. 명령줄 인터페이스에서 CSR(인증서 서명 요청)이 저장되었음을 알립니다.

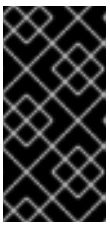
3. **CSR**을 외부 **CA**에 제출합니다.

4. 발급한 인증서를 **IdM** 서버에 복사합니다.

5. **ipa-ca-install:**에 외부 **CA** 파일에 인증서 및 전체 경로를 추가하여 설치를 계속합니다.

```
[root@idmserver ~]# ipa-ca-install --external-cert-file=/root/master.crt --external-cert-file=/root/ca.crt
```

6. 토폴로지의 각 **IdM** 호스트에서 **ipa-certupdate** 유틸리티를 실행하여 **IdM LDAP**의 새 인증서에 대한 정보로 호스트를 업데이트합니다.



중요

IdM CA 인증서를 생성한 후 **ipa-certupdate** 를 실행하지 않으면 인증서가 다른 **IdM** 시스템에 배포되지 않습니다.

27장. CA가 포함된 배포에서 IDM 서버에 IDM CA 서비스 추가

IdM(Identity Management) 환경에 IdM 인증 기관(CA) 서비스가 이미 설치되어 있지만 특정 IdM 서버인 *idmserver* 가 설치된 경우, ipa-ca-install 명령을 사용하여 *idmserver* 에 CA 서비스를 추가할 수 있습니다.

참고

이 절차는 다음 두 시나리오 모두에서 동일합니다.

- IdM CA는 루트 CA입니다.
- IdM CA는 외부 루트 CA와 관련이 있습니다.

사전 요구 사항

- *idmserver* 에 대한 루트 권한이 있습니다.
- IdM 서버는 *idmserver* 에 설치되어 있습니다.
- IdM 배포에 다른 IdM 서버에 CA가 설치되어 있습니다.
- IdM 디렉터리 관리자 암호를 알고 있습니다.

절차

- *idmserver* 에서 IdM 인증서 서버 CA를 설치합니다.

```
[root@idmserver ~] ipa-ca-install
```

28장. 복제 토폴로지 관리

이 장에서는 IdM(Identity Management) 도메인에서 서버 간 복제를 관리하는 방법을 설명합니다.

28.1. 복제 계약, 토폴로지 접미사 및 토폴로지 세그먼트 설명

복제본을 생성할 때 IdM(Identity Management)은 초기 서버와 복제본 간의 복제 계약을 생성합니다. 그런 다음 복제된 데이터는 토폴로지 접미사에 저장되고 두 개의 복제본이 접미사 사이에 복제 계약이 있는 경우 접미사는 토폴로지 세그먼트를 형성합니다. 이러한 개념은 다음 섹션에서 자세히 설명합니다.

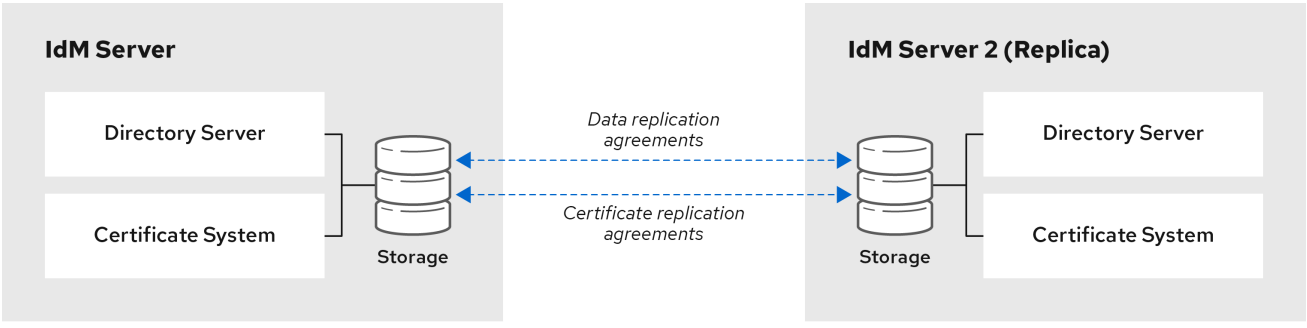
- 복제 계약
- 토폴로지 접미사
- 토폴로지 세그먼트

28.1.1. 복제 계약

관리자가 기존 서버를 기반으로 복제본을 생성하면 IdM(Identity Management)은 초기 서버와 복제본 간의 *복제 계약*을 생성합니다. 복제 계약을 사용하면 두 서버 간에 데이터와 구성이 지속적으로 복제됩니다.

IdM은 *여러 읽기/쓰기 복제본 복제*를 사용합니다. 이 구성에서 복제 계약에 연결된 모든 복제본은 업데이트를 수신 및 제공하므로 공급업체 및 소비자로 간주됩니다. 복제 계약서는 항상 양방향입니다.

그림 28.1. 서버 및 복제본 계약



IdM은 다음 두 가지 유형의 복제 계약을 사용합니다.

도메인 복제 계약

이러한 계약에서는 ID 정보를 복제합니다.

인증서 복제 계약

이러한 계약에서는 인증서 정보를 복제합니다.

두 복제 채널은 모두 독립적입니다. 두 서버에는 두 가지 유형의 복제 계약이 구성되어 있을 수 있습니다. 예를 들어 서버 A와 서버 B에 도메인 복제 계약만 구성되어 있는 경우 인증서 정보가 아닌 ID 정보만 복제됩니다.

28.1.2. 토폴로지 접미사

*토폴로지 접미사*는 복제된 데이터를 저장합니다. IdM은 domain 및 ca의 두 가지 유형의 토폴로지 접미사를 지원합니다. 각 접미사는 별도의 서버인 별도의 복제 토폴로지를 나타냅니다.

복제 계약이 구성되면 두 개의 다른 서버에 동일한 유형의 토폴로지 접미사가 사용됩니다.

domain suffix: dc=*example*,dc=*com*

domain suffix에는 모든 도메인 관련 데이터가 포함되어 있습니다.

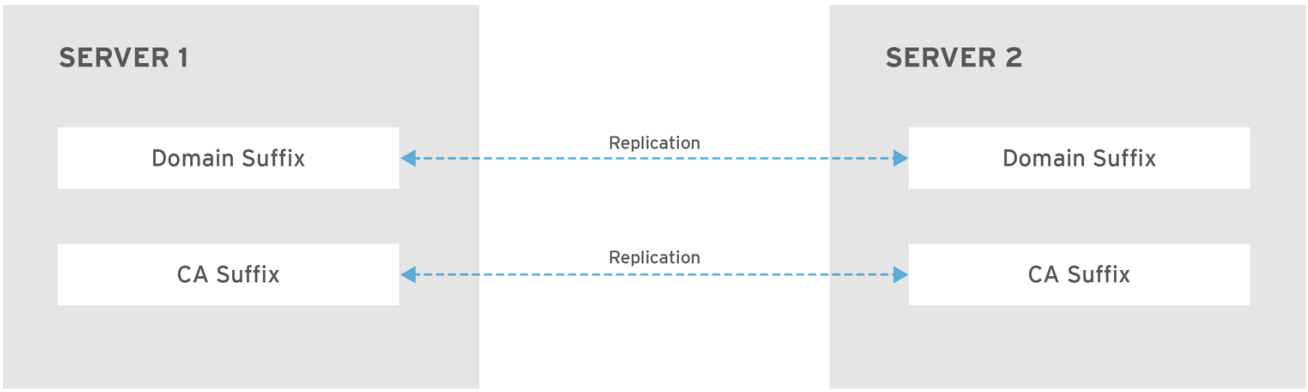
두 복제본의 domain 접미사 간 복제 계약이 있는 경우 사용자, 그룹 및 정책과 같은 디렉터리 데이터를 공유합니다.

ca suffix: o=ipaca

ca 접미사에는 인증서 시스템 구성 요소에 대한 데이터가 포함되어 있습니다. CA(인증 기관)가 설치된 서버에만 존재합니다.

두 복제본의 ca 접미사 간에 복제 계약이 있는 경우 인증서 데이터를 공유합니다.

그림 28.2. 토폴로지 접미사



초기 토폴로지 복제 연결은 새 복제본을 설치할 때 **ipa-replica-install** 스크립트에서 두 서버 간에 설정됩니다.

예 28.1. 토폴로지 접미사 보기

ipa topologysuffix-find 명령은 토폴로지 접미사 목록을 표시합니다.

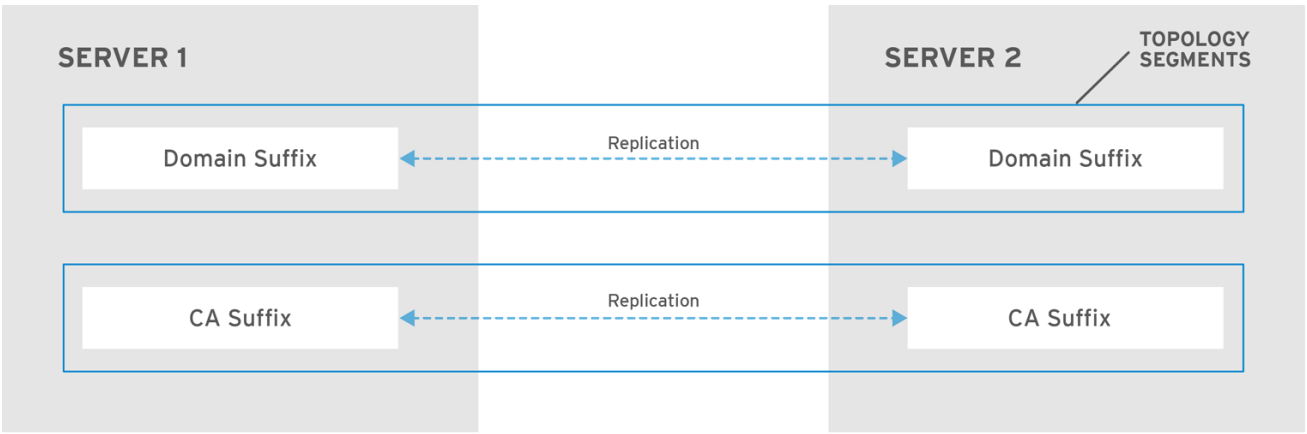
```
$ ipa topologysuffix-find
---------------------------
2 topology suffixes matched
---------------------------
  Suffix name: ca
  Managed LDAP suffix DN: o=ipaca

  Suffix name: domain
  Managed LDAP suffix DN: dc=example,dc=com
----------------------------
Number of entries returned 2
----------------------------
```

28.1.3. 토폴로지 세그먼트

두 복제본의 접미사 간에 복제 계약이 있는 경우 접미사는 *토폴로지 세그먼트*를 형성합니다. 각 토폴로지 세그먼트는 *왼쪽* 노드 와 *오른쪽* 노드로 구성됩니다. 노드는 복제 계약에 조인된 서버를 나타냅니다.

IdM의 토폴로지 세그먼트는 항상 양방향입니다. 각 세그먼트는 서버 A에서 서버 B에, 서버 B에서 서버 A까지의 두 개의 복제 계약을 나타냅니다. 따라서 데이터는 두 가지 방향으로 복제됩니다.

그림 28.3. 토폴로지 세그먼트



예 28.2. 토폴로지 세그먼트 보기

ipa topologysegment-find 명령은 도메인 또는 **CA** 접미사에 대해 구성된 현재 토폴로지 세그먼트를 표시합니다. 예를 들어 도메인 접미사의 경우:

```
$ ipa topologysegment-find
Suffix name: domain
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

이 예제에서 도메인 관련 데이터는 **server1.example.com** 과 **server2.example.com**의 두 서버 간에만 복제됩니다.

특정 세그먼트에 대한 세부 정보만 표시하려면 **ipa topologysegment-show** 명령을 사용합니다.

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: server1.example.com-to-server2.example.com
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

28.2. 토폴로지 그래프를 사용하여 복제 토폴로지 관리

웹 UI의 토폴로지 그래프는 도메인의 서버 간 관계를 보여줍니다. 웹 UI를 사용하면 토폴로지의 표현을 조작하고 변환할 수 있습니다.

토폴로지 그래프 액세스

토폴로지 그래프에 액세스하려면 다음을 수행합니다.

1. IPA 서버 → 토폴로지 → 토폴로지 그래프를 선택합니다.
2. 그래프에 즉시 반영되지 않는 토폴로지를 변경하는 경우 새로 고침을 클릭합니다.

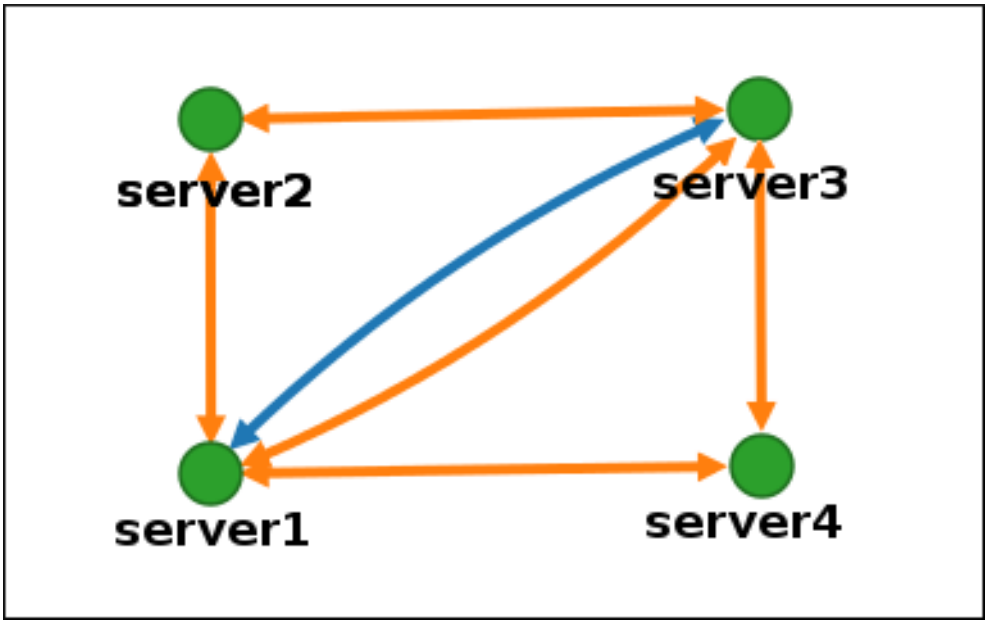
토폴로지 그래프 해석

도메인 복제 계약에 조인된 서버는 주황색 화살표로 연결됩니다. CA 복제 계약에 가입된 서버는 파란색 화살표로 연결됩니다.

토폴로지 그래프 예: 권장 토폴로지

아래 권장 토폴로지 예제에서는 4개의 서버에 대해 사용 가능한 권장 토폴로지 중 하나를 보여줍니다. 각 서버는 최소 두 개의 다른 서버에 연결되어 있고 두 개 이상의 서버는 CA 마스터입니다.

그림 28.4. 권장되는 토폴로지 예

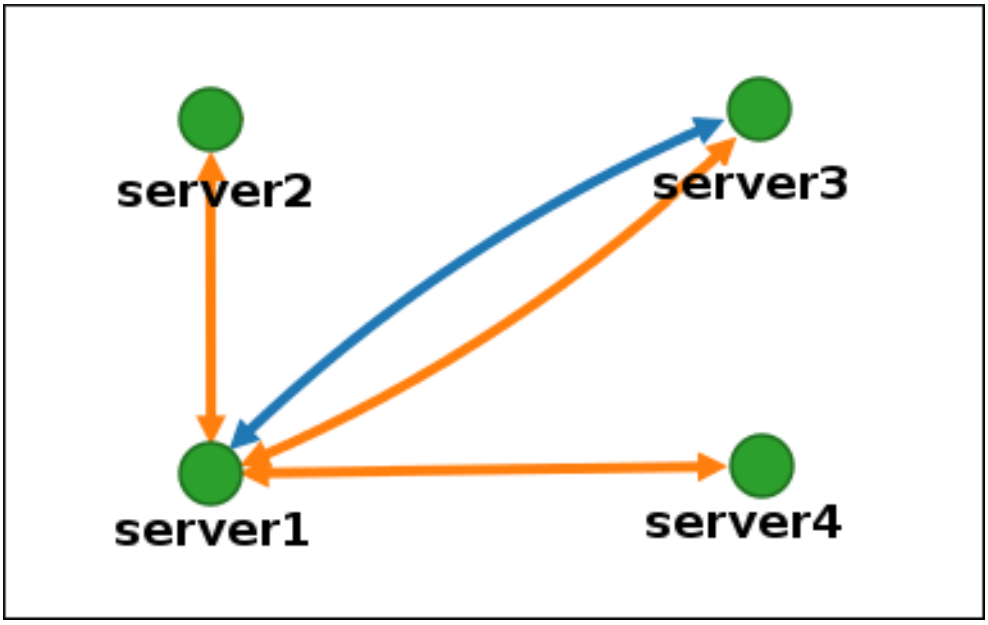


토폴로지 그래프 예: 디스크 토폴로지

아래 권장되지 않는 토폴로지 예에서 **server1** 은 단일 장애 지점입니다. 다른 모든 서버는 이 서버와 복제 계약을 맺고 있지만 다른 서버와는 계약하지 않습니다. 따라서 **server1** 이 실패하면 다른 모든 서버가 격리됩니다.

이와 같은 토폴로지를 생성하지 마십시오.

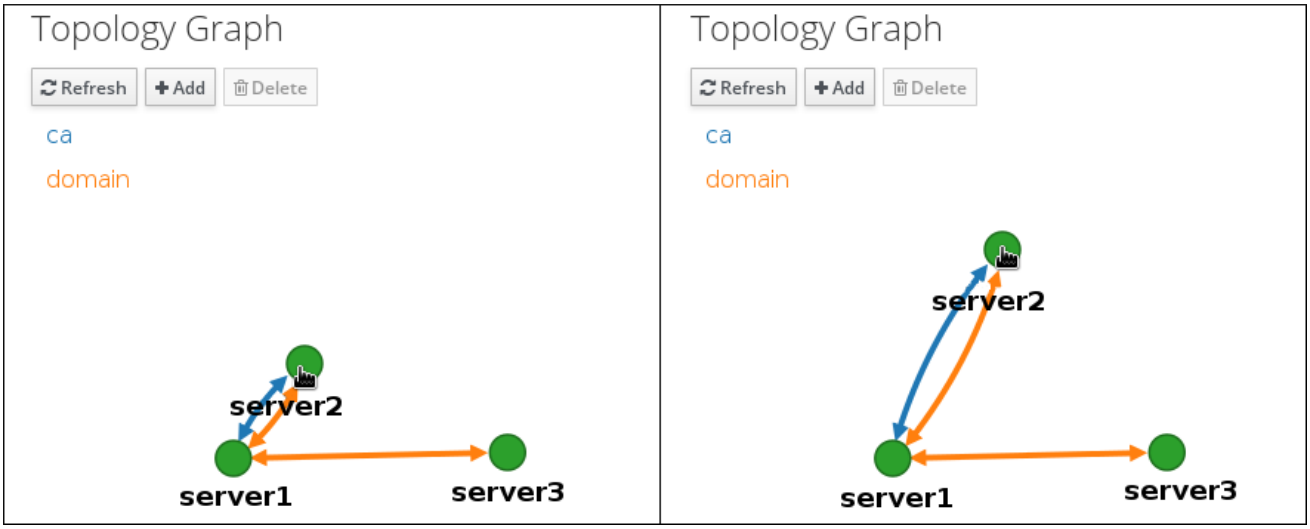
그림 **28.5.** 권장되지 않는 토폴로지 예: 단일 오류 지점



토폴로지 뷰 사용자 지정

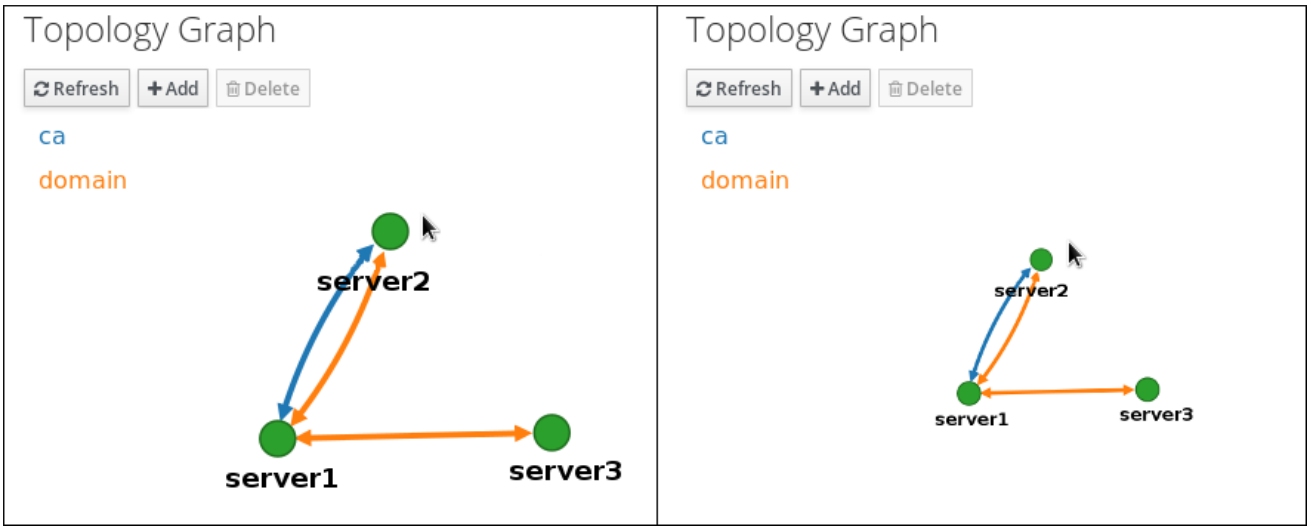
마우스를 드래그하여 개별 토폴로지 노드를 이동할 수 있습니다.

그림 **28.6.** 토폴로지 그래프 노드 이동



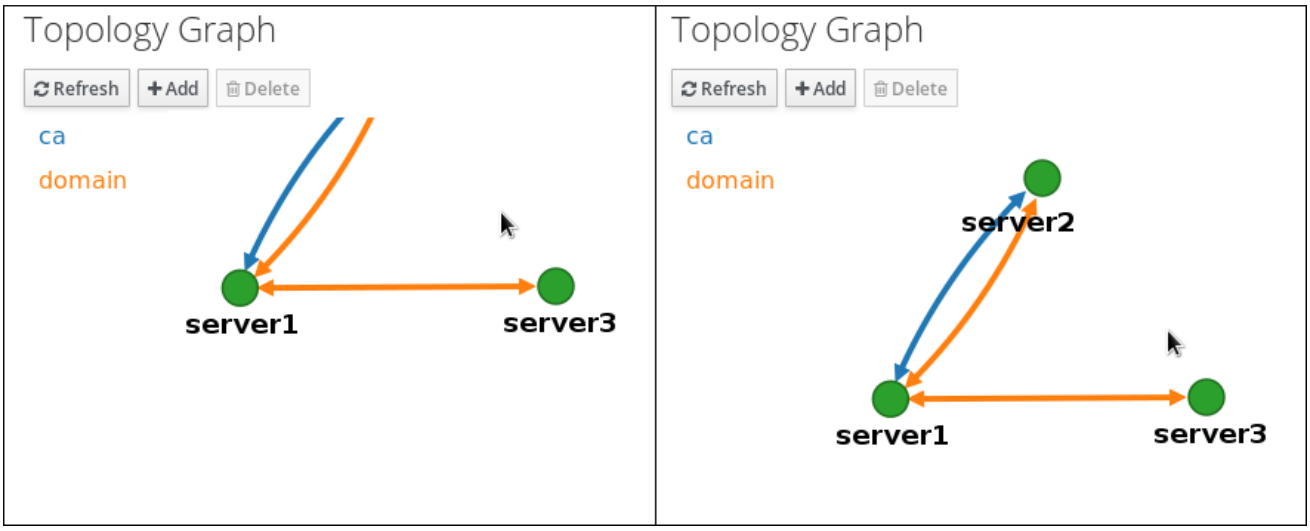
마우스 샤드를 사용하여 토폴로지 그래프를 확대하고 축소할 수 있습니다.

그림 28.7. 토폴로지 그래프 확대



왼쪽 마우스 버튼을 유지하여 토폴로지 그래프의 캔버스를 이동할 수 있습니다.

그림 28.8. 토폴로지 그래프 캔버스 이동



28.3. 웹 UI를 사용하여 두 서버 간 복제 설정

IdM(Identity Management)의 웹 인터페이스를 사용하여 두 서버를 선택하고 간에 새 복제 계약을 생성할 수 있습니다.

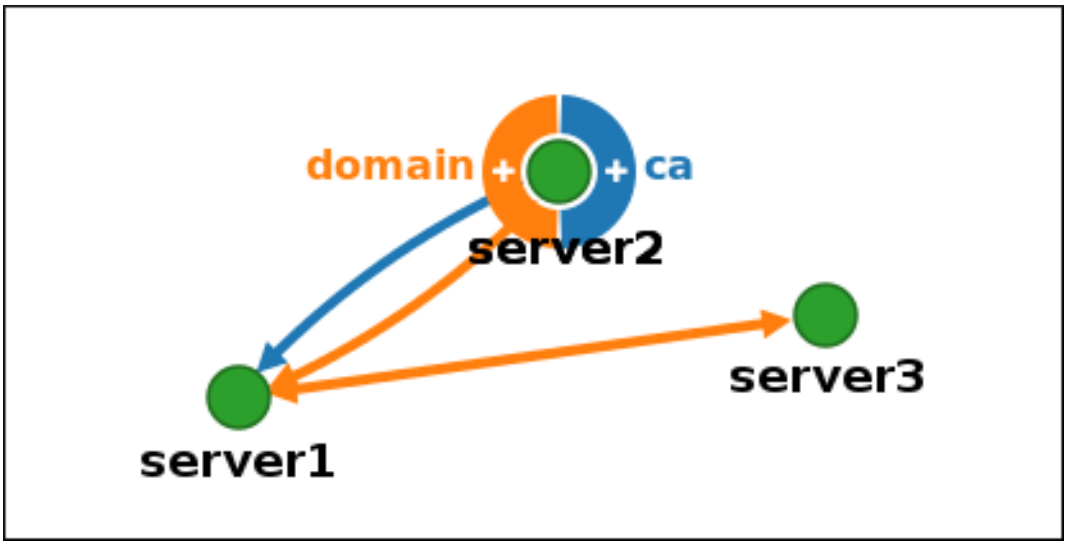
사전 요구 사항

- **IdM** 관리자 인증 정보가 있습니다.

절차

1. 토폴로지 그래프에서 서버 노드 중 하나에 마우스를 올려 놓습니다.

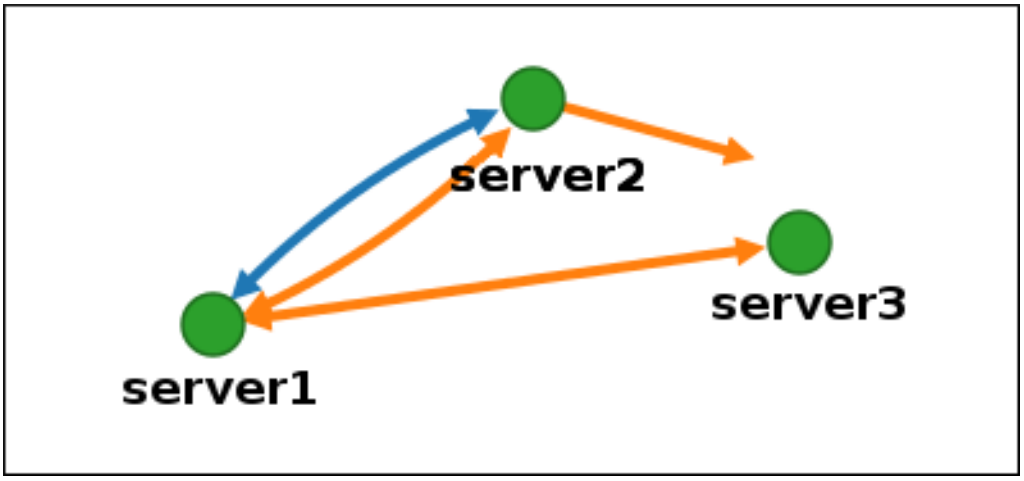
그림 28.9. 도메인 또는 CA 옵션



2. 생성할 토폴로지 세그먼트 유형에 따라 도메인 또는 원의 ca 부분을 클릭합니다.

3. 새 복제 계약을 나타내는 새 화살표가 마우스 포인터 아래에 표시됩니다. 마우스를 다른 서버 노드로 이동하여 클릭합니다.

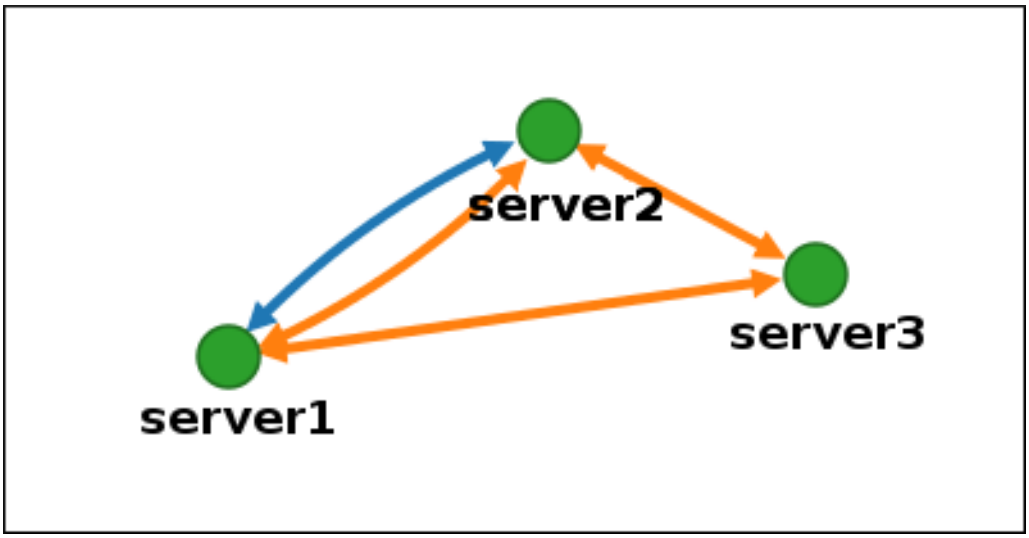
그림 28.10. 새 세그먼트 생성



4. 토폴로지 세그먼트 추가 창에서 추가를 클릭하여 새 세그먼트의 속성을 확인합니다.

두 서버 간의 새 토폴로지 세그먼트는 복제 계약에 조인합니다. 이제 토폴로지 그래프에서 업데이트된 복제 토폴로지를 표시합니다.

그림 28.11. 새 세그먼트 생성



28.4. 웹 UI를 사용하여 두 서버 간 복제 중지

IdM(Identity Management)의 웹 인터페이스를 사용하면 서버에서 복제 계약을 제거할 수 있습니다.

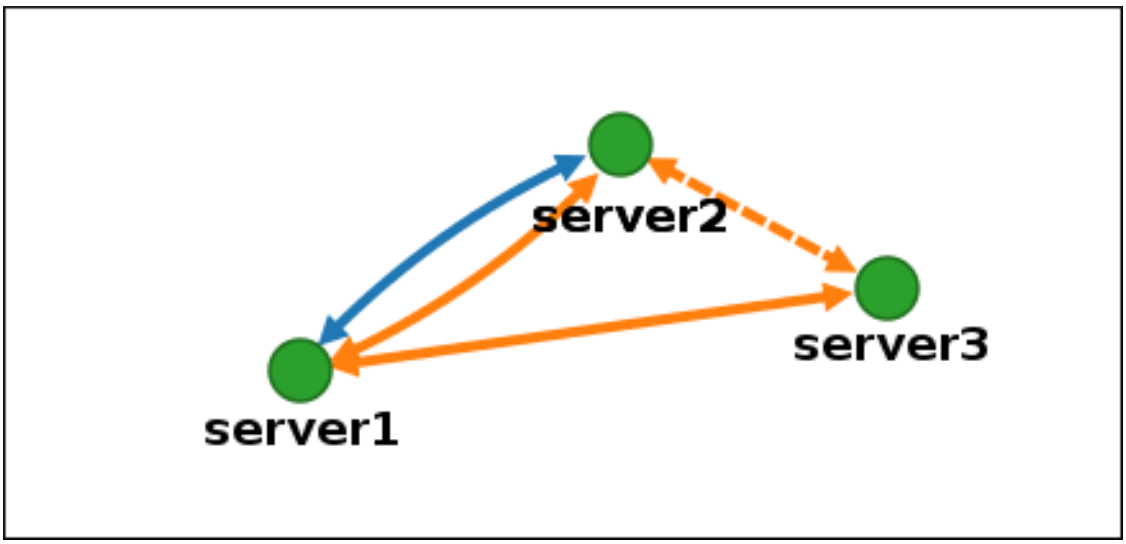
사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

1. 제거할 복제 계약을 나타내는 화살표를 클릭합니다. 이것은 화살표를 강조합니다.

그림 28.12. 토폴로지 세그먼트가 강조 표시됨

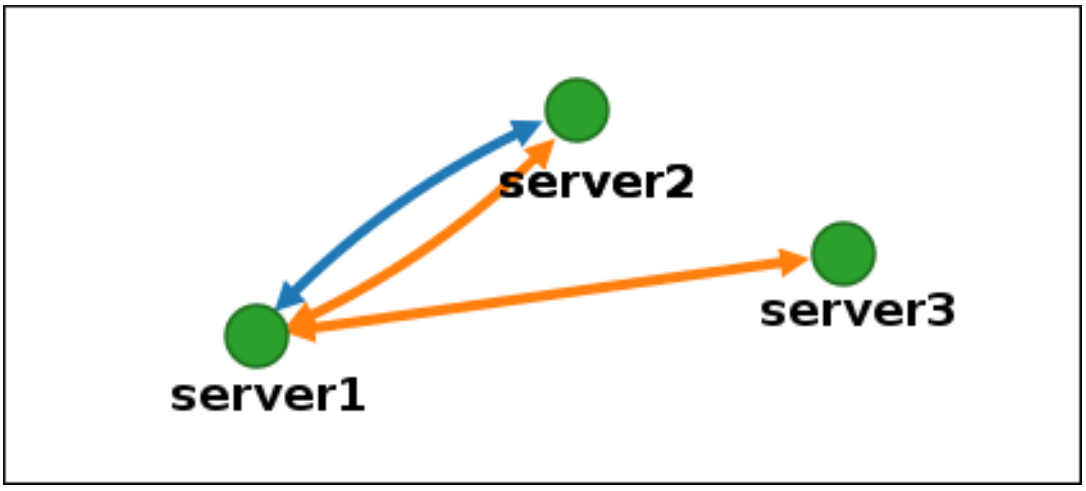


2. 삭제를 클릭합니다.

3. 확인 창에서 확인을 클릭합니다.

IdM은 두 서버 간의 토폴로지 세그먼트를 제거하여 복제 계약을 삭제합니다. 이제 토폴로지 그래프에서 업데이트된 복제 토폴로지를 표시합니다.

그림 28.13. 토폴로지 세그먼트 삭제



28.5. CLI를 사용하여 두 서버 간 복제 설정

ipa topologysegment-add 명령을 사용하여 두 서버 간 복제 계약을 구성할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

1. ipa topologysegment-add 명령을 사용하여 두 서버의 토폴로지 세그먼트를 생성합니다. 메시지가 표시되면 다음을 제공합니다.
   - 필수 토폴로지 접미사: domain 또는 ca
   - 두 서버를 나타내는 왼쪽 노드와 올바른 노드

- 필요에 따라 세그먼트에 대한 사용자 정의 이름

  예를 들어 다음과 같습니다.

```
$ ipa topologysegment-add
Suffix name: domain
Left node: server1.example.com
Right node: server2.example.com
Segment name [server1.example.com-to-server2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

  새 세그먼트를 추가하면 복제 계약의 서버에 연결됩니다.

2. *선택 사항:* **ipa topologysegment-show** 명령을 사용하여 새 세그먼트가 구성되었는지 확인합니다.

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: new_segment
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

28.6. CLI를 사용하여 두 서버 간 복제 중지

ipa topology_segment-del 명령을 사용하여 명령줄에서 복제 계약을 종료할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

1. 복제를 중지하려면 서버 간 해당 복제 세그먼트를 삭제해야 합니다. 이를 위해서는 세그먼트 이름을 알아야 합니다.

이름을 모르는 경우 **ipa topologysegment-find** 명령을 사용하여 모든 세그먼트를 표시하고 출력에서 필요한 세그먼트를 찾습니다. 메시지가 표시되면 필요한 토폴로지 접미사: **domain** 또는 **ca** 를 입력합니다. 예를 들어 다음과 같습니다.

```
$ ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 8
----------------------------
```

2. **ipa topologysegment-del** 명령을 사용하여 두 서버에 연결된 토폴로지 세그먼트를 제거합니다.

```
$ ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
-----------------------------
Deleted segment "new_segment"
-----------------------------
```

세그먼트를 삭제하면 복제 계약이 제거됩니다.

3. *선택 사항:* **ipa topologysegment-find** 명령을 사용하여 세그먼트가 더 이상 나열되지 않는지 확인합니다.

```
$ ipa topologysegment-find
Suffix name: domain
------------------
7 segments matched
------------------
  Segment name: server2.example.com-to-server3.example.com
  Left node: server2.example.com
  Right node: server3.example.com
  Connectivity: both

...
```

```
----------------------------
Number of entries returned 7
----------------------------
```

28.7. 웹 UI를 사용하여 토폴로지에서 서버 제거

IdM(Identity Management) 웹 인터페이스를 사용하여 토폴로지에서 서버를 제거할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.
- 제거하려는 서버는 나머지 토폴로지를 사용하여 다른 서버를 연결하는 유일한 서버가 아닙니다. 이로 인해 다른 서버가 분리될 수 없습니다.
- 제거하려는 서버는 마지막 CA 또는 DNS 서버가 아닙니다.

주의

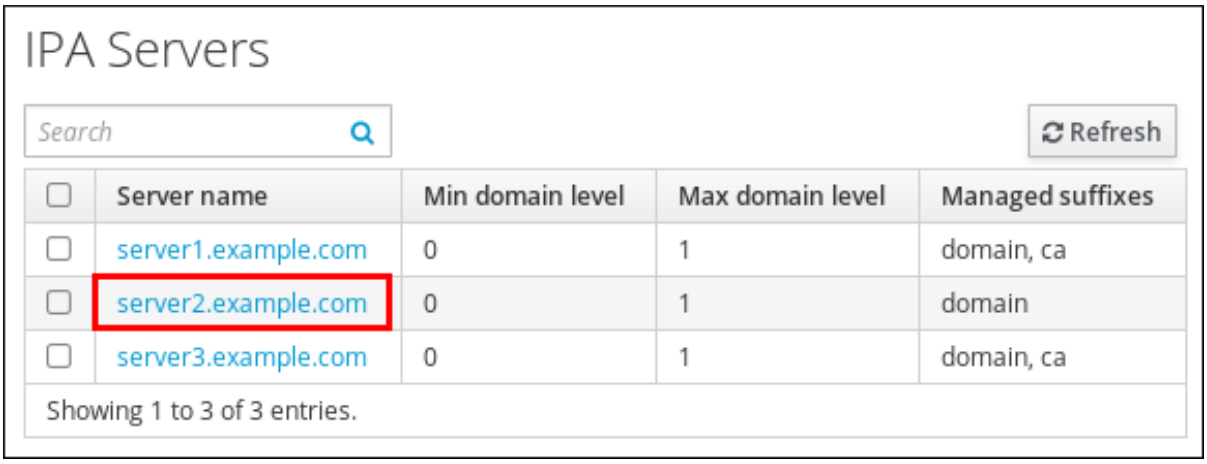
서버를 제거하는 것은 되돌릴 수 없는 작업입니다. 서버를 제거하면 토폴로지에 다시 도입할 수 있는 유일한 방법은 시스템에 새 복제본을 설치하는 것입니다.

절차

시스템에서 서버 구성 요소를 제거하지 않고 토폴로지에서 서버를 제거하려면 다음을 수행합니다.

1. IPA 서버 → 토폴로지 → IPA 서버를 선택합니다.
2. 삭제할 서버 이름을 클릭합니다.

그림 28.14. 서버 선택



3. **Delete Server** (서버 삭제)를 클릭합니다.

28.8. CLI를 사용하여 토폴로지에서 서버 제거

명령줄 인터페이스를 사용하여 토폴로지에서 서버를 제거할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.
- 제거하려는 서버는 나머지 토폴로지를 사용하여 다른 서버를 연결하는 유일한 서버가 아닙니다. 이로 인해 다른 서버가 분리되지 않습니다.
- 제거하려는 서버는 마지막 CA 또는 DNS 서버가 아닙니다.

중요

서버를 제거하는 것은 되돌릴 수 없는 작업입니다. 서버를 제거하면 토폴로지에 다시 도입할 수 있는 유일한 방법은 시스템에 새 복제본을 설치하는 것입니다.

절차

server1.example.com 을 제거하려면 다음을 수행합니다.

1. 다른 서버에서 **ipa server-del** 명령을 실행하여 **server1.example.com** 을 제거합니다. 이 명

령은 서버를 가리키는 모든 토폴로지 세그먼트를 제거합니다.

```
[user@server2 ~]$ ipa server-del
Server name: server1.example.com
Removing server1.example.com from replication topology, please wait...
----------------------------------------------------
Deleted IPA server "server1.example.com"
----------------------------------------------------
```

2. *선택 사항*: server1.example.com 에서 ipa server-install --uninstall 명령을 실행하여 시스템에서 서버 구성 요소를 제거합니다.

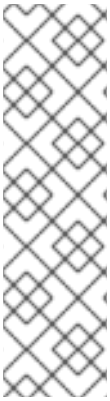
```
[root@server1 ~]# ipa server-install --uninstall
```

28.9. 웹 UI를 사용하여 IDM 서버에서 서버 역할 보기

IdM 서버에 설치된 서비스를 기반으로 다양한 *서버 역할을* 수행할 수 있습니다. 예를 들어 다음과 같습니다.

- CA 서버
- DNS 서버
- KRA(Key recovery authority) 서버.

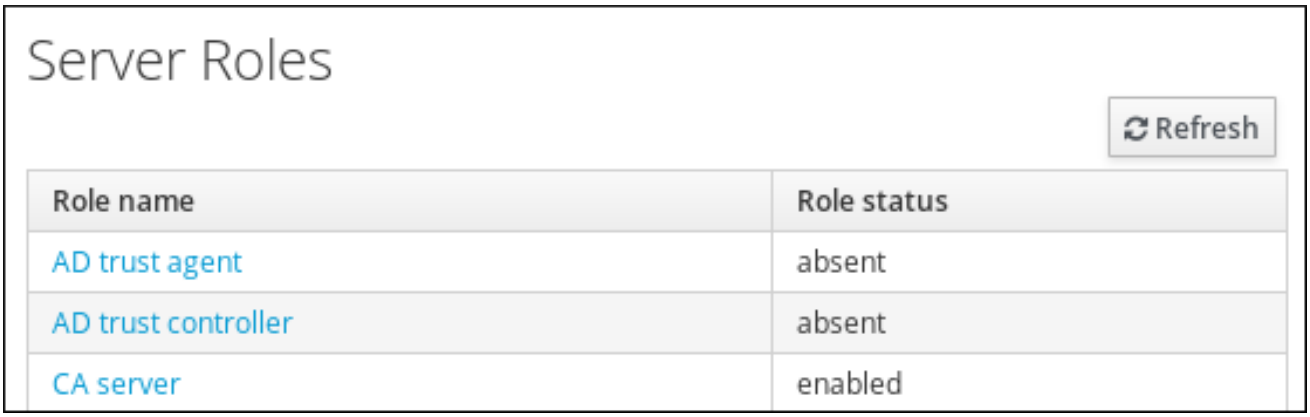
지원되는 서버 역할의 전체 목록은 IPA 서버 토폴로지 서버 역할을 참조하십시오.



참고

- 역할 status absent 는 토폴로지의 서버가 역할을 수행하지 않음을 의미합니다.
- 역할 상태가 활성화되어 있으면 토폴로지에서 하나 이상의 서버에서 역할을 수행하고 있습니다.

그림 28.15. 웹 UI에서 서버 역할



28.10. CLI를 사용하여 IDM 서버의 서버 역할 보기

IdM 서버에 설치된 서비스를 기반으로 다양한 *서버 역할을* 수행할 수 있습니다. 예를 들어 다음과 같습니다.

- CA 서버
- DNS 서버
- KRA(Key recovery authority) 서버.

다음 명령을 사용하여 토폴로지에서 어떤 역할을 수행하는 서버를 볼 수 있습니다.

- ipa config-show 명령은 모든 CA 서버와 현재 CA 갱신 서버를 표시합니다.

```
$ ipa config-show
  ...
  IPA masters: server1.example.com, server2.example.com, server3.example.com
  IPA CA servers: server1.example.com, server2.example.com
  IPA CA renewal master: server1.example.com
```

- ipa server-show 명령은 특정 서버에서 활성화된 역할 목록을 표시합니다. 예를 들어 *server.example.com* 에서 활성화된 역할 목록은 다음과 같습니다.

```
$ ipa server-show
Server name: server.example.com
  ...
```

```
Enabled server roles: CA server, DNS server, KRA server
```

- **ipa server-find --servrole** 은 특정 서버 역할이 활성화된 모든 서버를 검색합니다. 예를 들어 모든 **CA** 서버를 검색하려면 다음을 수행합니다.

```
$ ipa server-find --servrole "CA server"
--------------------
2 IPA servers matched
--------------------
  Server name: server1.example.com
  ...

  Server name: server2.example.com
  ...
----------------------------
Number of entries returned 2
----------------------------
```

28.11. 복제본을 CA 갱신 서버 및 CRL 게시자 서버로 승격

IdM 배포에서 포함된 **CA**(인증 기관)를 사용하는 경우 **IdM CA** 서버 중 하나가 **CA** 갱신 서버인 **CA** 하위 시스템 인증서 갱신을 관리하는 서버입니다. **IdM CA** 서버 중 하나는 인증서 해지 목록을 생성하는 서버인 **IdM CRL** 게시자 서버 역할을 합니다. 기본적으로 **CA** 갱신 서버 및 **CRL** 게시자 서버 역할은 시스템 관리자가 **ipa-server-install** 또는 **ipa-ca-install** 명령을 사용하여 **CA** 역할을 설치한 첫 번째 서버에 설치됩니다.

사전 요구 사항

- **IdM** 관리자 인증 정보가 있습니다.

절차

- 현재 **CA** 갱신 마스터를 변경합니다.
- **CRL**을 생성하도록 복제본을 구성합니다.

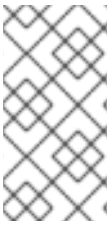
28.12. 숨겨진 복제본 검증 또는 승격

복제본이 설치되면 복제본이 숨겨지거나 표시되는지 여부를 구성할 수 있습니다.

숨겨진 복제본에 대한 자세한 내용은 숨겨진 복제본 모드 를 참조하십시오.

복제본이 CA 갱신 서버인 경우 이 복제본이 숨겨지기 전에 서비스를 다른 복제본으로 이동합니다.

자세한 내용은 IdM CA 갱신 서버 변경 및 재설정 을 참조하십시오.



참고

RHEL 8.1에 기술 프리뷰로 도입된 숨겨진 복제본 기능은 RHEL 8.2부터 완전히 지원됩니다.

절차

- 복제본을 숨기려면 다음을 입력합니다.

```
# ipa server-state replica.idm.example.com --state=hidden
```

또는 다음 명령을 사용하여 복제본을 볼 수도 있습니다.

```
# ipa server-state replica.idm.example.com --state=enabled
```

29장. IDM 상태 점검 툴 설치 및 실행

이 장에서는 IdM 상태 점검 툴과 이를 설치 및 실행하는 방법에 대해 설명합니다.

사전 요구 사항

- Healthcheck 툴은 RHEL 8.1 이상에서만 사용할 수 있습니다.

29.1. IDM에서 상태 점검

IdM(Identity Management)의 Healthcheck 툴은 IdM 환경의 상태에 영향을 줄 수 있는 문제를 찾는 데 도움이 됩니다.

참고

Healthcheck 도구는 Kerberos 인증 없이 사용할 수 있는 명령줄 도구입니다.

모듈은 서로 독립적입니다.

Healthcheck는 테스트를 위한 독립적인 모듈로 구성되어 있습니다.

- 복제 문제
- 인증서 유효성
- 인증 기관 인프라 문제
- IdM 및 Active Directory 신뢰 문제
- 올바른 파일 권한 및 소유권 설정

두 개의 출력 형식

Healthcheck는 출력 유형 옵션을 사용하여 설정할 수 있는 다음 출력을 생성합니다.

- json: JSON 형식의 machine-readable output (기본값)
- human: 사람이 읽을 수 있는 출력

--output-file 옵션을 사용하여 다른 파일 대상을 지정할 수 있습니다.

결과

각 Healthcheck 모듈은 다음 결과 중 하나를 반환합니다.

SUCCESS

예상한 대로 구성

WARNING

실수는 아니지만 또는 평가할 가치가 있습니다.

ERROR

예상대로 구성되지 않았습니다.

심각

상당한 영향을 미칠 수 있으므로 예상대로 구성되지 않았습니다.

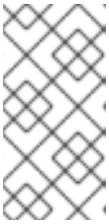
29.2. IDM 상태 점검 설치

이 섹션에서는 IdM 상태 점검 툴을 설치하는 방법을 설명합니다.

절차

- ipa-healthcheck 패키지를 설치합니다.

```
[root@server ~]# yum install ipa-healthcheck
```



참고

RHEL 8.1 및 8.2 시스템에서 **yum install /usr/bin/ipa-healthcheck** 명령을 대신 사용합니다.

검증 단계

- **--failures-only** 옵션을 사용하여 **ipa-healthcheck** 만 보고 오류를 보고합니다. 완전히 작동하는 IdM 설치는 **[]** 의 빈 결과를 반환합니다.

```
[root@server ~]# ipa-healthcheck --failures-only
[]
```

추가 리소스

- **ipa-healthcheck --help** 를 사용하여 지원되는 모든 인수를 확인합니다.

29.3. IDM 상태 점검 실행

상태 점검은 로그 회전을 사용하여 수동으로 또는 자동으로 실행할 수 있습니다.

사전 요구 사항

- **Healthcheck** 툴이 설치되어 있어야 합니다. IdM 상태 점검 설치를 참조하십시오.

절차

- 수동으로 **healthcheck**을 실행하려면 **ipa-healthcheck** 명령을 입력합니다.

```
[root@server ~]# ipa-healthcheck
```

추가 리소스

모든 옵션에 대한 자세한 내용은 **man page: man ipa-healthcheck** 를 참조하십시오.

29.4. 추가 리소스

- IdM 상태 점검 사용에 대한 예는 Configuring and managing Identity Management 가이드

의 다음 섹션을 참조하십시오.

- 서비스 확인
- IdM 및 AD 신뢰 구성 확인
- 인증서 확인
- 시스템 인증서 확인
- 디스크 공간 확인
- IdM 구성 파일에 대한 권한 확인
- 복제 확인

- 이러한 장은 단일 가이드로 구성되어 있습니다. IdM 상태 점검을 사용하여 IdM 환경 모니터링

30장. ANSIBLE 플레이북을 사용하여 IDENTITY MANAGEMENT 서버 설치

다음 섹션에서는 Ansible 을 사용하여 시스템을 IdM 서버로 구성하는 방법을 설명합니다. 시스템을 IdM 서버로 구성하면 IdM 도메인이 설정되고 시스템에서 IdM 서비스를 IdM 클라이언트에 제공할 수 있습니다. ipaserver Ansible 역할을 사용하여 배포를 관리할 수 있습니다.

사전 요구 사항

- Ansible 및 IdM 개념을 이해할 수 있습니다.
  - Ansible 역할
  - Ansible 노드
  - Ansible 인벤토리
  - Ansible 작업
  - Ansible 모듈
  - Ansible 플레이 및 플레이북

30.1. ANSIBLE 및 IDM 설치를 위한 이점

Ansible은 시스템 구성, 소프트웨어 배포 및 롤링 업데이트를 수행하는 데 사용되는 자동화 툴입니다. Ansible에는 IdM(Identity Management) 지원이 포함되며, Ansible 모듈을 사용하여 IdM 서버, 복제본, 클라이언트 또는 전체 IdM 토폴로지 설정과 같은 설치 작업을 자동화할 수 있습니다.

IdM을 설치하기 위해 Ansible을 사용할 때의 이점

다음 목록은 수동 설치와 달리 Ansible을 사용하여 Identity Management를 설치하는 이점이 있습니다.

- 관리 노드에 로그인할 필요가 없습니다.

- 개별적으로 배포할 각 호스트의 설정을 구성할 필요가 없습니다. 대신 전체 클러스터를 배포하는 데 하나의 인벤토리 파일이 있을 수 있습니다.

- 나중에 관리 작업을 위해 인벤토리 파일을 재사용할 수 있습니다(예: 사용자 및 호스트 추가). IdM과 관련이 없는 것과 같은 작업에도 인벤토리 파일을 재사용할 수 있습니다.

30.2. ANSIBLE-FREEIPA 패키지 설치

이 섹션에서는 IdM(Identity Management)을 설치 및 관리하기 위해 Ansible 역할 및 모듈을 제공하는 ansible-freeipa 패키지를 설치하는 방법을 설명합니다.

사전 요구 사항

- 관리형 노드에서 다음을 수행합니다.
  - 관리형 노드가 고정 IP 주소 및 작동 중인 패키지 관리자가 있는 Red Hat Enterprise Linux 8 시스템인지 확인합니다.
- 컨트롤러 의 경우:
  - 컨트롤러가 유효한 서브스크립션이 있는 Red Hat Enterprise Linux 시스템인지 확인합니다. 그렇지 않은 경우 대체 설치 지침은 공식 Ansible 설명서 설치 가이드 를 참조하십시오.
  - 컨트롤러에서 SSH 프로토콜을 통해 관리형 노드에 연결할 수 있는지 확인합니다. 관리형 노드가 컨트롤러의 /root/.ssh/known_hosts 파일에 나열되어 있는지 확인합니다.

절차

Ansible 컨트롤러에서 다음 절차를 사용합니다.

1. 시스템이 RHEL 8.5 및 이전 버전에서 실행중인 경우 필요한 리포지토리를 활성화합니다.

```
# subscription-manager repos --enable ansible-2.8-for-rhel-8-x86_64-rpms
```

2. 시스템이 RHEL 8.5 이하에서 실행 중인 경우 ansible 패키지를 설치합니다.

```
# yum install ansible
```

3. ansible-freeipa 패키지를 설치합니다.

```
# yum install ansible-freeipa
```

역할 및 모듈은 /usr/share/ansible/roles/ 및 /usr/share/ansible/plugins/modules 디렉터리에 설치됩니다.

30.3. 파일 시스템의 ANSIBLE 역할 위치

기본적으로 ansible-freeipa 역할은 /usr/share/ansible/roles/ 디렉터리에 설치됩니다. ansible-freeipa 패키지의 구조는 다음과 같습니다.

- /usr/share/ansible/roles/ 디렉터리는 Ansible 컨트롤러에 ipaserver,ipareplica 및 ipaclient 역할을 저장합니다. 각 역할 디렉터리는 README.md 마크다운 파일에서 역할에 대한 예제, 기본 개요, 라이센스 및 문서를 저장합니다.

```
[root@server]# ls -1 /usr/share/ansible/roles/
ipaclient
ipareplica
ipaserver
```

- /usr/share/doc/ansible-freeipa/ 디렉터리는 README.md 마크다운 파일에 개별 역할 및 토폴로지에 대한 문서를 저장합니다. 또한 playbooks/ 하위 디렉터리를 저장합니다.

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/
playbooks
README-client.md
README.md
README-replica.md
README-server.md
README-topology.md
```

- /usr/share/doc/ansible-freeipa/playbooks/ 디렉터리는 예제 플레이북을 저장합니다.

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/playbooks/
install-client.yml
```

```
install-cluster.yml
install-replica.yml
install-server.yml
uninstall-client.yml
uninstall-cluster.yml
uninstall-replica.yml
uninstall-server.yml
```

30.4. 통합 DNS 및 통합 CA를 루트 CA로 사용한 배포에 대한 매개변수 설정

IdM 통합 DNS 솔루션을 사용하는 환경에서 통합 CA를 루트 CA로 설치하기 위해 IdM 서버를 설치하기 위한 인벤토리 파일을 구성하려면 이 절차를 완료합니다.

참고

이 절차의 인벤토리에는 INI 형식을 사용합니다. 또는 YAML 또는 JSON 형식을 사용할 수 있습니다.

절차

1. 편집할 인벤토리 파일을 엽니다. IdM 서버로 사용하려는 호스트의 정규화된 도메인 이름(FQDN)을 지정합니다. FQDN 이 다음 기준을 충족하는지 확인합니다.

   - 영숫자 및 하이픈(-)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 DNS 오류가 발생할 수 있습니다.
   - 호스트 이름은 모두 소문자여야 합니다.

2. IdM 도메인 및 영역 정보를 지정합니다.

3. 다음 옵션을 추가하여 통합 DNS를 사용할 것을 지정합니다.

   ```
   ipaserver_setup_dns=yes
   ```

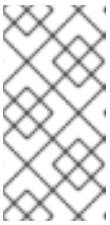
4. DNS 전달 설정을 지정합니다. 다음 옵션 중 하나를 선택합니다.

   - 설치 프로그램이 /etc/resolv.conf 파일에서 forwarders를 사용하도록 하려면 ipaserver_auto_forwarders=yes 옵션을 사용합니다. /etc/resolv.conf 파일에 지정된 이름

서버가 **localhost 127.0.0.1** 주소이거나 가상 프라이빗 네트워크에 있고 사용 중인 **DNS** 서버는 일반적으로 공용 인터넷에서 연결할 수 없는 경우 이 옵션을 사용하지 마십시오.

- **ipaserver_forwarders** 옵션을 사용하여 전달자를 수동으로 지정합니다. 설치 프로세스에서는 설치된 **IdM** 서버의 **/etc/named.conf** 파일에 전달자 **IP** 주소를 추가합니다.

- **ipaserver_no_forwarders=yes** 옵션을 사용하여 대신 사용할 루트 **DNS** 서버를 구성합니다.



참고

DNS 전달자가 없으면 환경이 분리되어 있으며 인프라의 다른 **DNS** 도메인의 이름은 확인되지 않습니다.

5. **DNS** 역방향 레코드 및 영역 설정을 지정합니다. 다음 옵션 중에서 선택합니다.

- **ipaserver_allow_zone_overlap=yes** 옵션을 사용하여 영역이 이미 확인 가능한 경우에도 **(reverse)** 영역을 생성할 수 있습니다.

- **ipaserver_reverse_zones** 옵션을 사용하여 역방향 영역을 수동으로 지정합니다.

- 설치 프로그램이 역방향 **DNS** 영역을 생성하지 않도록 하려면 **ipaserver_no_reverse=yes** 옵션을 사용합니다.

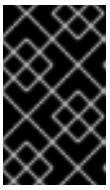
참고

IdM을 사용하여 역방향 영역을 관리하는 것은 선택 사항입니다. 대신 외부 **DNS** 서비스를 사용할 수 있습니다.

6. **admin** 및 **Directory Manager** 의 암호를 지정합니다. **Ansible Vault**를 사용하여 암호를 저장하고 플레이북 파일에서 **Vault** 파일을 참조합니다. 또는 덜 안전한 경우 인벤토리 파일에서 직접 암호를 지정합니다.

7. (선택 사항) **IdM** 서버에서 사용할 사용자 지정 **firewalld** 영역을 지정합니다. 사용자 지정 영역을 설정하지 않으면 **IdM**에서 서비스를 기본 **firewalld** 영역에 추가합니다. 사전 정의된 기본 영

역은 **public** 입니다.



중요

지정된 **firewalld** 영역이 있어야 하며 영구적으로 있어야 합니다.

필수 서버 정보가 있는 인벤토리 파일의 예(암호 제외)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
[...]
```

필수 서버 정보가 있는 인벤토리 파일의 예(암호 포함)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

사용자 지정 **firewalld** 영역이 있는 인벤토리 파일의 예

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

Ansible Vault 파일에 저장된 **admin** 및 **Directory Manager** 암호를 사용하여 **IdM** 서버를 설정하는 플레이북의 예

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

인벤토리 파일에서 **admin** 및 **Directory Manager** 암호를 사용하여 **IdM** 서버를 설정하는 플레이북의 예

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    state: present
```

추가 리소스

- 전달 정책 기본 설정은 **ipa-dns-install(1)** 매뉴얼 페이지의 **--forward-policy** 설명을 참조하십시오.

- **ipaserver** 역할에서 사용하는 **DNS** 변수에 대한 자세한 내용은 **/usr/share/doc/ansible-freeipa** 디렉터리의 **README-server.md** 파일의 **DNS** 변수 섹션을 참조하십시오.

30.5. 외부 DNS 및 통합 CA를 루트 CA로 사용한 배포에 대한 매개변수 설정

외부 **DNS** 솔루션을 사용하는 환경에서 통합 **CA**를 루트 **CA**로 설치하기 위해 **IdM** 서버를 설치하기 위한 인벤토리 파일을 구성하려면 이 절차를 완료합니다.

참고

이 절차의 인벤토리 파일은 **INI** 형식을 사용합니다. 또는 **YAML** 또는 **JSON** 형식을 사용할 수 있습니다.

절차

1. 편집할 인벤토리 파일을 엽니다. **IdM** 서버로 사용하려는 호스트의 정규화된 도메인 이름 **(FQDN)**을 지정합니다. **FQDN** 이 다음 기준을 충족하는지 확인합니다.

   - 영숫자 및 하이픈(**-**)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 **DNS** 오류가 발생할 수 있습니다.

   - 호스트 이름은 모두 소문자여야 합니다.

2. **IdM** 도메인 및 영역 정보를 지정합니다.

3. **ipaserver_setup_dns** 옵션이 **no** 로 설정되었거나 존재하지 않는지 확인합니다.

4. **admin** 및 **Directory Manager** 의 암호를 지정합니다. **Ansible Vault**를 사용하여 암호를 저장하고 플레이북 파일에서 **Vault** 파일을 참조합니다. 또는 덜 안전한 경우 인벤토리 파일에서 직접 암호를 지정합니다.

5.

(선택 사항) IdM 서버에서 사용할 사용자 지정 firewalld 영역을 지정합니다. 사용자 지정 영역을 설정하지 않으면 IdM에서 서비스를 기본 firewalld 영역에 추가합니다. 사전 정의된 기본 영역은 public 입니다.

중요

지정된 **firewalld** 영역이 있어야 하며 영구적으로 있어야 합니다.

필수 서버 정보가 있는 인벤토리 파일의 예(암호 제외)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

필수 서버 정보가 있는 인벤토리 파일의 예(암호 포함)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

사용자 지정 firewalld 영역이 있는 인벤토리 파일의 예

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

Ansible Vault 파일에 저장된 **admin** 및 **Directory Manager** 암호를 사용하여 **IdM** 서버를 설정하는 플레이북의 예

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

인벤토리 파일에서 **admin** 및 **Directory Manager** 암호를 사용하여 **IdM** 서버를 설정하는 플레이북의 예

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    state: present
```

30.6. ANSIBLE 플레이북을 사용하여 통합 CA를 루트 CA로 IDM 서버 배포

Ansible 플레이북을 사용하여 통합 인증 기관(CA)을 루트 CA로 사용하여 IdM 서버를 배포하려면 이 절차를 완료합니다.

참고

이 절차의 인벤토리에는 INI 형식을 사용합니다. 또는 YAML 또는 JSON 형식을 사용할 수 있습니다.

사전 요구 사항

- 다음 절차 중 하나를 선택하여 시나리오에 해당하는 매개변수를 설정했습니다.
  - 통합 DNS 절차
  - 외부 DNS가 있는 프로세스

절차

1. 플레이북 파일 이름(예: install-server.yml)을 사용하여 ansible-playbook 명령을 실행합니다. -i 옵션으로 인벤토리 파일을 지정합니다.

```
$ ansible-playbook -v -i <path_to_inventory_directory>/hosts
<path_to_playbooks_directory>/install-server.yml
```

v , -vv 또는 - vv v 옵션을 사용하여 상세 정보 표시 수준을 지정합니다.

CLI(명령줄 인터페이스)에서 Ansible 플레이북 스크립트의 출력을 볼 수 있습니다. 다음 출력은 스크립트가 0개 작업으로 성공적으로 실행된 것을 보여줍니다.

```
PLAY RECAP
server.idm.example.com : ok=18   changed=10   unreachable=0    failed=0
skipped=21   rescued=0    ignored=0
```

2. 다음 옵션 중 하나를 선택합니다.

- IdM 배포에서 외부 DNS를 사용하는 경우: /tmp/ipa.system. recordss.UFRPto.db 파일에 포함된 DNS 리소스 레코드 를 기존 외부 DNS 서버에 추가합니다. DNS 레코드를 업데이트하는 프로세스는 특정 DNS 솔루션에 따라 다릅니다.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

중요

기존 DNS 서버에 DNS 레코드를 추가할 때까지 서버 설치가 완료되지 않습니다.

- IdM 배포에서 통합 DNS를 사용하는 경우:
  - 상위 도메인의 DNS 위임을 IdM DNS 도메인에 추가합니다. 예를 들어 IdM DNS 도메인이 *idm.example.com* 인 경우 example.com 상위 도메인에 이름 서버(NS) 레코드를 추가합니다.

중요

IdM DNS 서버가 설치되면 이 단계를 반복합니다.

  - 시간 서버의 _ntp._udp 서비스(SRV) 레코드를 IdM DNS에 추가합니다. IdM DNS에 새로 설치된 IdM 서버의 시간 서버에 SRV 레코드가 있으면 이 기본 IdM 서버에서 사용하는 시간 서버와 동기화되도록 향후 복제본 및 클라이언트 설치가 자동으로 구성됩니다.

추가 리소스

- 외부 CA를 사용하여 IdM 서버를 루트 CA로 배포하는 방법에 대한 자세한 내용은 Ansible 플레이북을 사용하여 외부 CA를 루트 CA로 IdM 서버배포를 참조하십시오.

30.7. 통합 DNS 및 외부 CA를 루트 CA로 사용하여 배포에 대한 매개변수 설정

IdM 통합 DNS 솔루션을 사용하는 환경에서 외부 CA를 루트 CA로 설치하기 위한 인벤토리 파일을 구성하려면 이 절차를 완료합니다.

참고

이 절차의 인벤토리 파일은 INI 형식을 사용합니다. 또는 YAML 또는 JSON 형식을 사용할 수 있습니다.

절차

1. 편집할 인벤토리 파일을 엽니다. IdM 서버로 사용하려는 호스트의 정규화된 도메인 이름(FQDN)을 지정합니다. FQDN 이 다음 기준을 충족하는지 확인합니다.

- 영숫자 및 하이픈(-)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 DNS 오류가 발생할 수 있습니다.
- 호스트 이름은 모두 소문자여야 합니다.

2. IdM 도메인 및 영역 정보를 지정합니다.

3. 다음 옵션을 추가하여 통합 DNS를 사용할 것을 지정합니다.

```
ipaserver_setup_dns=yes
```

4. DNS 전달 설정을 지정합니다. 다음 옵션 중 하나를 선택합니다.

- 설치 프로세스에서 /etc/resolv.conf 파일의 forwarders를 사용하도록 하려면 ipaserver_auto_forwarders=yes 옵션을 사용합니다. /etc/resolv.conf 파일에 지정된 이름 서버가 localhost 127.0.0.1 주소이거나 가상 프라이빗 네트워크에 있고 사용 중인 DNS 서버는 일반적으로 공용 인터넷에서 연결할 수 없는 경우 이 옵션을 사용하지 않는 것이 좋습니다.
- ipaserver_forwarders 옵션을 사용하여 전달자를 수동으로 지정합니다. 설치 프로세스에서는 설치된 IdM 서버의 /etc/named.conf 파일에 전달자 IP 주소를 추가합니다.
- ipaserver_no_forwarders=yes 옵션을 사용하여 대신 사용할 루트 DNS 서버를 구성합니다.

참고

DNS 전달자가 없으면 환경이 분리되어 있으며 인프라의 다른 DNS 도메인의 이름은 확인되지 않습니다.

5. DNS 역방향 레코드 및 영역 설정을 지정합니다. 다음 옵션 중에서 선택합니다.

- ipaserver_allow_zone_overlap=yes 옵션을 사용하여 영역이 이미 확인 가능한 경우에도 (reverse) 영역을 생성할 수 있습니다.
- ipaserver_reverse_zones 옵션을 사용하여 역방향 영역을 수동으로 지정합니다.
- 설치 프로세스에서 역방향 DNS 영역을 생성하지 않으려면 ipaserver_no_reverse=yes 옵션을 사용합니다.

참고

IdM을 사용하여 역방향 영역을 관리하는 것은 선택 사항입니다. 대신 외부 DNS 서비스를 사용할 수 있습니다.

6. admin 및 Directory Manager 의 암호를 지정합니다. Ansible Vault를 사용하여 암호를 저장하고 플레이북 파일에서 Vault 파일을 참조합니다. 또는 덜 안전한 경우 인벤토리 파일에서 직접 암호를 지정합니다.

7. (선택 사항) IdM 서버에서 사용할 사용자 지정 firewalld 영역을 지정합니다. 사용자 지정 영역을 설정하지 않으면 IdM에서 서비스를 기본 firewalld 영역에 추가합니다. 사전 정의된 기본 영역은 public 입니다.

중요

지정된 firewalld 영역이 있어야 하며 영구적으로 있어야 합니다.

필수 서버 정보가 있는 인벤토리 파일의 예(암호 제외)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
[...]
```

필수 서버 정보가 있는 인벤토리 파일의 예(암호 포함)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

사용자 지정 **firewalld** 영역이 있는 인벤토리 파일의 예

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
```

```
ipaserver_firewalld_zone=custom zone

[...]
```

8. 설치의 첫 번째 단계에 대한 플레이북을 생성합니다. **CSR**(인증서 서명 요청)을 생성하고 컨트롤러에서 관리 노드로 복사하는 지침을 입력합니다.

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: yes

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: yes
```

9. 설치의 마지막 단계에 대해 다른 플레이북을 생성합니다.

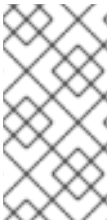
```
---
- name: Playbook to configure IPA server Step -1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files: "/root/chain.crt"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] + '-chain.crt' }}" to /root/chain.crt on node
    copy:
      src: "{{ groups.ipaserver[0] + '-chain.crt' }}"
      dest: "/root/chain.crt"
      force: yes

  roles:
  - role: ipaserver
    state: present
```

추가 리소스

- 전달 정책 기본 설정은 **ipa-dns-install(1)** 매뉴얼 페이지의 **--forward-policy** 설명을 참조하십시오.
- **ipaserver** 역할에서 사용하는 **DNS** 변수에 대한 자세한 내용은 **/usr/share/doc/ansible-freeipa** 디렉터리의 **README-server.md** 파일의 **DNS** 변수 섹션을 참조하십시오.

30.8. 외부 DNS 및 외부 CA를 사용하여 배포에 대한 매개변수 설정

외부 **DNS** 솔루션을 사용하는 환경의 루트 **CA**로 외부 **CA**를 사용하여 **IdM** 서버를 설치하기 위한 인벤토리 파일을 구성하려면 다음 절차를 완료합니다.



참고

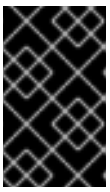
이 절차의 인벤토리 파일은 **INI** 형식을 사용합니다. 또는 **YAML** 또는 **JSON** 형식을 사용할 수 있습니다.

절차

1. 편집할 인벤토리 파일을 엽니다. **IdM** 서버로 사용하려는 호스트의 정규화된 도메인 이름 **(FQDN)**을 지정합니다. **FQDN** 이 다음 기준을 충족하는지 확인합니다.
   - 영숫자 및 하이픈(**-**)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 **DNS** 오류가 발생할 수 있습니다.
   - 호스트 이름은 모두 소문자여야 합니다.
2. **IdM** 도메인 및 영역 정보를 지정합니다.
3. **ipaserver_setup_dns** 옵션이 **no** 로 설정되었거나 존재하지 않는지 확인합니다.
4. **admin** 및 **Directory Manager** 의 암호를 지정합니다. **Ansible Vault**를 사용하여 암호를 저장하고 플레이북 파일에서 **Vault** 파일을 참조합니다. 또는 덜 안전한 경우 인벤토리 파일에서 직접

암호를 지정합니다.

5. (선택 사항) IdM 서버에서 사용할 사용자 지정 firewalld 영역을 지정합니다. 사용자 지정 영역을 설정하지 않으면 IdM에서 서비스를 기본 firewalld 영역에 추가합니다. 사전 정의된 기본 영역은 public 입니다.



중요

지정된 firewalld 영역이 있어야 하며 영구적으로 있어야 합니다.

필수 서버 정보가 있는 인벤토리 파일의 예(암호 제외)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

필수 서버 정보가 있는 인벤토리 파일의 예(암호 포함)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

사용자 지정 firewalld 영역이 있는 인벤토리 파일의 예

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

6. 설치의 첫 번째 단계에 대한 플레이북을 생성합니다. **CSR**(인증서 서명 요청)을 생성하고 컨트롤러에서 관리 노드로 복사하는 지침을 입력합니다.

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: yes

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: yes
```

7. 설치의 마지막 단계에 대해 다른 플레이북을 생성합니다.

```
---
- name: Playbook to configure IPA server Step -1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
```

```
vars:
  ipaserver_external_cert_files: "/root/chain.crt"

pre_tasks:
- name: Copy "{{ groups.ipaserver[0] + '-chain.crt' }}" to /root/chain.crt on node
  copy:
    src: "{{ groups.ipaserver[0] + '-chain.crt' }}"
    dest: "/root/chain.crt"
    force: yes

roles:
- role: ipaserver
  state: present
```

추가 리소스

- 외부 DNS 및 외부 서명된 CA를 사용하여 IdM 서버를 설치할 때 사용할 수 있는 옵션에 대한 자세한 내용은 Installing an IdM server를 참조하십시오. 통합 DNS가 없으면 루트 CA로 외부 CA가 있는 입니다.

30.9. ANSIBLE 플레이북을 사용하여 외부 CA를 루트 CA로 IDM 서버 배포

Ansible 플레이북을 사용하여 외부 CA(인증 기관)를 루트 CA로 사용하여 IdM 서버를 배포하려면 이 절차를 완료합니다.

참고

이 절차의 인벤토리 파일은 INI 형식을 사용합니다. 또는 YAML 또는 JSON 형식을 사용할 수 있습니다.

사전 요구 사항

- 다음 절차 중 하나를 선택하여 시나리오에 해당하는 매개변수를 설정했습니다.
  - 통합 DNS 절차
  - 외부 DNS가 있는 프로세스

절차

1. 설치의 첫 번째 단계에 대한 지침이 포함된 플레이북 파일의 이름으로 ansible-playbook 명

령을 실행합니다(예: install-server-step1.yml). -i 옵션으로 인벤토리 파일을 지정합니다.

```
$ ansible-playbook -v -i <path_to_inventory_directory>/host.server
<path_to_playbooks_directory>/install-server-step1.yml
```

v , -vv 또는 - vv v 옵션을 사용하여 상세 정보 표시 수준을 지정합니다.

CLI(명령줄 인터페이스)에서 Ansible 플레이북 스크립트의 출력을 볼 수 있습니다. 다음 출력은 스크립트가 0개 작업으로 성공적으로 실행된 것을 보여줍니다.

```
PLAY RECAP
server.idm.example.com : ok=18   changed=10   unreachable=0    failed=0
skipped=21   rescued=0    ignored=0
```

2. 컨트롤러에서 ipa.csr 인증서 서명 요청 파일을 찾아 외부 CA에 제출합니다.

3. 다음 단계의 플레이북에서 찾을 수 있도록 외부 CA가 컨트롤러 파일 시스템에 서명한 IdM CA 인증서를 배치합니다.

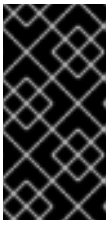
4. 설치의 최종 단계(예: install-server-step2.yml)에 대한 지침이 포함된 플레이북 파일의 이름으로 ansible-playbook 명령을 실행합니다. -i 옵션으로 인벤토리 파일을 지정합니다.

```
$ ansible-playbook -v -i <path_to_inventory_directory>/host.server
<path_to_playbooks_directory>/install-server-step2.yml
```

5. 다음 옵션 중 하나를 선택합니다.

- IdM 배포에서 외부 DNS를 사용하는 경우: /tmp/ipa.system. recordss.UFRPto.db 파일에 포함된 DNS 리소스 레코드 를 기존 외부 DNS 서버에 추가합니다. DNS 레코드를 업데이트하는 프로세스는 특정 DNS 솔루션에 따라 다릅니다.

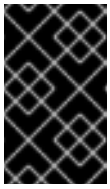
```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



중요

기존 **DNS** 서버에 **DNS** 레코드를 추가할 때까지 서버 설치가 완료되지 않습니다.

- **IdM** 배포에서 통합 **DNS**를 사용하는 경우:
  - 상위 도메인의 **DNS** 위임을 **IdM DNS** 도메인에 추가합니다. 예를 들어 **IdM DNS** 도메인이 ***idm.example.com*** 인 경우 **example.com** 상위 도메인에 이름 서버(**NS**) 레코드를 추가합니다.



중요

IdM DNS 서버가 설치되면 이 단계를 반복합니다.

  - 시간 서버의 **_ntp._udp** 서비스(**SRV**) 레코드를 **IdM DNS**에 추가합니다. **IdM DNS**에 새로 설치된 **IdM** 서버의 시간 서버에 **SRV** 레코드가 있으면 이 기본 **IdM** 서버에서 사용하는 시간 서버와 동기화되도록 향후 복제본 및 클라이언트 설치가 자동으로 구성됩니다.

추가 리소스

통합 **CA**를 사용하여 **IdM** 서버를 루트 **CA**로 배포하는 방법에 대한 자세한 내용은 **Ansible** 플레이북을 사용하여 통합 **CA**가 있는 **IdM** 서버배포를 참조하십시오.

30.10. 추가 리소스

- 인벤토리 기본 사항: 형식, 호스트 및 그룹
- **IdM** 서버 설치에 필요한 샘플 **Ansible** 플레이북 및 **ansible-freeipa** 업스트림 설명서에서 사용 가능한 변수 목록을 확인할 수 있습니다.

31장. ANSIBLE 플레이북을 사용하여 IDENTITY MANAGEMENT 복제본 설치

Ansible 을 사용하여 시스템을 IdM 복제본으로 구성하여 IdM 도메인에 등록하고, 시스템이 도메인의 IdM 서버에서 IdM 서비스를 사용할 수 있도록 합니다.

배포는 ipareplica Ansible 역할에 의해 관리됩니다. 이 역할은 자동 검색 모드를 사용하여 IdM 서버, 도메인 및 기타 설정을 식별할 수 있습니다. 그러나 다양한 복제본 그룹이 서로 다른 시간에 배포되는 경우 계층형 모델에 여러 복제본을 배포하는 경우 각 그룹의 특정 서버 또는 복제본을 정의해야 합니다.

사전 요구 사항

- Ansible 제어 노드에 ansible-freeipa 패키지를 설치했습니다.
- Ansible 및 IdM 개념을 이해할 수 있습니다.
  - Ansible 역할
  - Ansible 노드
  - Ansible 인벤토리
  - Ansible 작업
  - Ansible 모듈
  - Ansible 플레이 및 플레이북

31.1. IDM 복제본 설치를 위한 기본, 서버 및 클라이언트 변수 지정

IdM 복제본을 설치하기 위한 인벤토리 파일을 구성하려면 이 절차를 완료합니다.

사전 요구 사항

- Ansible 컨트롤러에 ansible-freeipa 패키지를 설치했습니다.

절차

1. 편집할 인벤토리 파일을 엽니다. IdM 복제본이 될 호스트의 FQDN(정규화된 도메인 이름)을 지정합니다. FQDN은 유효한 DNS 이름이어야 합니다.

   - 숫자, 영문자 및 하이픈(-)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 DNS 오류가 발생할 수 있습니다.
   - 호스트 이름은 모두 소문자여야 합니다.

   정의된 복제본의 FQDN만 있는 간단한 인벤토리 호스트 파일의 예

   ```
   [ipareplicas]
   replica1.idm.example.com
   replica2.idm.example.com
   replica3.idm.example.com
   [...]
   ```

   IdM 서버가 이미 배포되어 있고 IdM DNS 영역에 SRV 레코드가 올바르게 설정된 경우 스크립트에서 다른 모든 필수 값을 자동으로 검색합니다.

2. 필요한 경우 다음 시나리오 중 가장 가까운 인벤토리 파일에 추가 정보를 제공하십시오.

   시나리오 1

   자동 검색을 방지하고 [ipareplicas] 섹션에 나열된 모든 복제본이 있는 경우 인벤토리 파일의 [ipaservers] 섹션에 서버를 설정합니다.

   정의된 IdM 서버 및 복제본의 FQDN이 있는 인벤토리 호스트 파일의 예

   ```
   [ipaservers]
   ```

```
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]
```

시나리오 **2**

또는 자동 검색을 방지하되 특정 서버로 특정 복제본을 배포하려는 경우 인벤토리 파일의 **[ipareplicas]** 섹션에서 특정 복제본의 서버를 개별적으로 설정합니다.

특정 복제본에 대해 정의된 특정 **IdM** 서버가 있는 인벤토리 파일의 예

```
[ipaservers]
server.idm.example.com
replica1.idm.example.com

[ipareplicas]
replica2.idm.example.com
replica3.idm.example.com ipareplica_servers=replica1.idm.example.com
```

위의 예에서 **replica3.idm.example.com** 은 이미 배포된 **replica1.idm.example.com** 을 해당 복제 소스로 사용합니다.

시나리오 **3**

하나의 배치에 여러 복제본을 배포하고 시간이 우려되는 경우 다중 계층 복제본 배포가 유용할 수 있습니다. 인벤토리 파일에 특정 복제본 그룹(예: **[ipareplicas_tier1]** 및 **[ipareplicas_tier2]**)을 정의하고 **install-replica.yml** 플레이북의 각 그룹에 대해 별도의 플레이를 설계합니다.

복제본 계층이 정의된 인벤토리 파일 예

```
[ipaservers]
server.idm.example.com
```

```
[ipareplicas_tier1]
replica1.idm.example.com

[ipareplicas_tier2]
replica2.idm.example.com \
ipareplica_servers=replica1.idm.example.com,server.idm.example.com
```

ipareplica_servers 의 첫 번째 항목이 사용됩니다. 두 번째 항목은 대체 옵션으로 사용됩니다. **IdM** 복제본을 배포하기 위해 여러 계층을 사용하는 경우 플레이북에서 별도의 작업을 통해 먼저 **tier1**에서 복제본을 배포한 다음 **tier2**에서 복제본을 복제해야 합니다.

다른 복제본 그룹에 대해 다른 플레이가 있는 플레이북 파일의 예

```
---
- name: Playbook to configure IPA replicas (tier1)
  hosts: ipareplicas_tier1
  become: true

  roles:
  - role: ipareplica
    state: present

- name: Playbook to configure IPA replicas (tier2)
  hosts: ipareplicas_tier2
  become: true

  roles:
  - role: ipareplica
    state: present
```

시나리오 **4**

복제본이 기본 영역 대신 지정된 **firewalld** 영역을 사용하도록 하려면 인벤토리 파일에 지정할 수 있습니다. 예를 들어, 기본적으로 설정된 퍼블릭 영역 대신 **IdM** 설치에 내부 **firewalld** 영역을 사용하려는 경우 유용할 수 있습니다.

사용자 지정 영역을 설정하지 않으면 **IdM**에서 서비스를 기본 **firewalld** 영역에 추가합니다. 사전 정의된 기본 영역은 **public** 입니다.

중요

지정된 **firewalld** 영역이 있어야 하며 영구적으로 있어야 합니다.

사용자 지정 **firewalld** 영역이 있는 간단한 인벤토리 호스트 파일의 예

```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_firewalld_zone=custom zone
```

시나리오 **5**

복제본이 **IdM DNS** 서비스를 호스팅하도록 하려면 **ipareplica_setup_dns=yes** 행을 **[ipareplicas:vars]** 섹션에 추가합니다. 또한 서버당 **DNS** 전달자를 사용할지 여부를 지정합니다.

- 서버별 전달자를 구성하려면 **ipareplica_forwarders** 변수와 **[ipareplicas:vars]** 섹션에 문자열 목록을 추가합니다(예: **ipareplica_forwarders=192.0.2.1,192.0.2.2**).
- **per-server forwarders**를 구성하지 않으려면 **[ipareplicas:vars]** 섹션에 다음 행을 추가합니다. **ipareplica_no_forwarders=yes**.
- 복제본의 **/etc/resolv.conf** 파일에 나열된 **forwarders**에 따라 서버별 전달자를 구성하려면 **ipareplica_auto_forwarders** 변수를 **[ipareplicas:vars]** 섹션에 추가합니다.

복제본에서 **DNS** 및 서버별 전달자를 설정하는 지침이 있는 인벤토리 파일의 예

```
[ipaservers]
```

```
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_setup_dns=yes
ipareplica_forwarders=192.0.2.1,192.0.2.2
```

추가 리소스

- **ipareplica** 변수에 대한 자세한 내용은 **/usr/share/ansible/roles/ipareplica/README.md Markdown** 파일을 참조하십시오.

31.2. ANSIBLE 플레이북을 사용하여 IDM 복제본을 설치하기 위한 자격 증명 지정

IdM 복제본 설치에 대한 권한 부여를 구성하려면 이 절차를 완료합니다.

사전 요구 사항

- **Ansible** 컨트롤러에 **ansible-freeipa** 패키지를 설치했습니다.

절차

1. 복제본을 배포할 권한이 있는 사용자의 암호를 지정합니다(예: **IdM** 관리자).

   - **Red Hat**은 **Ansible Vault**를 사용하여 암호를 저장하고 플레이북 파일에서 **Vault** 파일을 참조하는 것이 좋습니다(예: **install-replica.yml**).

   Ansible Vault 파일의 인벤토리 파일 및 암호의 주체를 사용하는 플레이북 파일의 예

```
- name: Playbook to configure IPA replicas
  hosts: ipareplicas
  become: true
```

```
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipareplica
    state: present
```

Ansible Vault를 사용하는 방법에 대한 자세한 내용은 공식 Ansible Vault 설명서를 참조하십시오.

- 덜 안전한 경우, 인벤토리 파일에서 직접 **admin** 의 자격 증명을 제공하십시오. 인벤토리 파일의 **[ipareplicas:vars]** 섹션에서 **ipaadmin_password** 옵션을 사용합니다. 인벤토리 파일과 **install-replica.yml** 플레이북 파일은 다음과 같습니다.

hosts.replica 파일의 예

```
[...]
[ipareplicas:vars]
ipaadmin_password=Secret123
```

인벤토리 파일의 **principal** 및 **password**를 사용하는 플레이북의 예

```
- name: Playbook to configure IPA replicas
  hosts: ipareplicas
  become: true

  roles:
  - role: ipareplica
    state: present
```

- 또는 덜 안전하지 않은 경우 인벤토리 파일에 직접 복제본을 배포할 권한이 있는 다른 사용자의 자격 증명을 제공합니다. 다른 권한 있는 사용자를 지정하려면 사용자 이름에

ipaadmin_principal 옵션을 사용하고 암호에 **ipaadmin_password** 옵션을 사용합니다. 인벤토리 파일과 **install-replica.yml** 플레이북 파일은 다음과 같습니다.

hosts.replica 파일의 예

```
[...]
[ipareplicas:vars]
ipaadmin_principal=my_admin
ipaadmin_password=my_admin_secret123
```

인벤토리 파일의 **principal** 및 **password**를 사용하는 플레이북의 예

```
- name: Playbook to configure IPA replicas
  hosts: ipareplicas
  become: true

  roles:
  - role: ipareplica
    state: present
```

추가 리소스

- **ipareplica Ansible** 역할에서 허용하는 옵션에 대한 자세한 내용은 **/usr/share/ansible/roles/ipareplica/README.md** 마크다운 파일을 참조하십시오.

31.3. ANSIBLE 플레이북을 사용하여 IDM 복제본 배포

Ansible 플레이북을 사용하여 **IdM** 복제본을 배포하려면 이 절차를 완료합니다.

사전 요구 사항

- **IdM** 복제본을 설치하기 위해 인벤토리 파일을 구성했습니다.

- IdM 복제본 설치를 위한 권한 부여를 구성했습니다.

절차

- Ansible 플레이북을 사용하여 IdM 복제본을 설치하려면 플레이북 파일의 이름과 함께 ansible-playbook 명령을 사용합니다(예: install-replica.yml). -i 옵션으로 인벤토리 파일을 지정합니다.

```
$ ansible-playbook -v -i <path_to_inventory_directory>/hosts.replica
<path_to_playbooks_directory>/install-replica.yml
```

v , -vv 또는 - vv v 옵션을 사용하여 상세 정보 표시 수준을 지정합니다.

Ansible은 Ansible 플레이북 스크립트 실행에 대해 알려줍니다. 다음 출력은 스크립트가 0 개 작업으로 성공적으로 실행된 것을 보여줍니다.

```
PLAY RECAP
replica.idm.example.com : ok=18   changed=10   unreachable=0    failed=0
skipped=21   rescued=0    ignored=0
```

이제 IdM 복제본이 설치되어 있습니다.

32장. ANSIBLE 플레이북을 사용하여 IDENTITY MANAGEMENT 클라이언트 설치

다음 섹션에서는 Ansible 을 사용하여 시스템을 IdM(Identity Management) 클라이언트로 구성하는 방법을 설명합니다. 시스템을 IdM 클라이언트로 구성하여 IdM 도메인에 등록하고, 시스템이 도메인의 IdM 서버에서 IdM 서비스를 사용할 수 있도록 합니다.

배포는 ipaclient Ansible 역할에 의해 관리됩니다. 기본적으로 이 역할은 자동 검색 모드를 사용하여 IdM 서버, 도메인 및 기타 설정을 식별합니다. Ansible 플레이북이 인벤토리 파일에서 지정된 설정을 사용하도록 역할을 수정할 수 있습니다.

사전 요구 사항

- Ansible 제어 노드에 ansible-freeipa 패키지를 설치했습니다.
- Ansible 및 IdM 개념을 이해할 수 있습니다.
  - Ansible 역할
  - Ansible 노드
  - Ansible 인벤토리
  - Ansible 작업
  - Ansible 모듈
  - Ansible 플레이 및 플레이북

32.1. 자동 검색 클라이언트 설치 모드에 대한 인벤토리 파일의 매개변수 설정

Ansible 플레이북을 사용하여 Identity Management 클라이언트를 설치하려면 인벤토리 파일에서 대상 호스트 매개 변수를 구성합니다(예: inventory/hosts).

- 호스트에 대한 정보
- 작업에 대한 권한 부여

인벤토리 파일은 보유한 인벤토리 플러그인에 따라 여러 형식 중 하나일 수 있습니다. **INI**와 유사한 형식은 **Ansible**의 기본값 중 하나이며 아래 예제에서 사용됩니다.

참고

RHEL의 그래픽 사용자 인터페이스와 함께 스마트 카드를 사용하려면 **Ansible** 플레이북에 **ipaclient_mkhomedir** 변수를 포함해야 합니다.

사전 요구 사항

- 제어 노드에서 배포 지침을 확인하고 **install-client.yml** 파일의 매개변수 확인을 참조하십시오.

절차

1. **IdM** 클라이언트가 될 호스트의 정규화된 호스트 이름(**FQDN**)을 지정합니다. 정규화된 도메인 이름은 유효한 **DNS** 이름이어야 합니다.
   - 숫자, 영문자 및 하이픈(**-**)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 **DNS** 오류가 발생할 수 있습니다.
   - 호스트 이름은 모두 소문자여야 합니다. 대문자는 사용할 수 없습니다.

   IdM DNS 영역에 **SRV** 레코드가 올바르게 설정된 경우 스크립트에서 다른 모든 필수 값을 자동으로 검색합니다.

   클라이언트 **FQDN**이 정의된 간단한 인벤토리 호스트 파일의 예

```
[ipaclients]
client.idm.example.com
[...]
```

2. 클라이언트 등록 자격 증명을 지정합니다. 다음 인증 방법을 사용할 수 있습니다.

- 클라이언트를 등록할 권한이 있는 사용자의 암호 입니다. 이는 기본 옵션입니다.

  - **Ansible Vault**를 사용하여 암호를 저장하고 플레이북 파일에서 **Vault** 파일을 참조하는 것이 좋습니다(예: **install-client.yml**).

    Ansible Vault 파일의 인벤토리 파일 및 암호의 주체를 사용하는 플레이북 파일의 예

```
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaclient
    state: present
```

  - 더 안전하게 **inventory/hosts** 파일의 **[ipaclients:vars]** 섹션에서 **ipa admin _password** 옵션을 사용하여 **admin**의 자격 증명을 제공하십시오. 또는 권한이 있는 다른 사용자를 지정하려면 사용자 이름에 **ipaadmin_principal** 옵션을 사용하고 암호에 **ipaadmin_password** 옵션을 사용합니다. **inventory/hosts** 인벤토리 파일 및 **install-client.yml** 플레이북 파일은 다음과 같습니다.

    인벤토리 호스트 파일 예

```
[...]
[ipaclients:vars]
ipaadmin_principal=my_admin
ipaadmin_password=Secret123
```

인벤토리 파일에서 보안 주체 및 암호를 사용하는 플레이북의 예

```
- name: Playbook to unconfigure IPA clients
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: true
```

- 이전 등록의 클라이언트 키탭 이 계속 사용 가능한 경우.

  이 옵션은 시스템이 이전에 **ID** 관리 클라이언트로 등록된 경우 사용할 수 있습니다. 이 인증 방법을 사용하려면 **#ipaclient_keytab** 옵션의 주석을 제거하여 **keytab**을 저장하는 파일의 경로를 지정합니다(예: **inventory/hosts** 의 **[ipaclient:vars]** 섹션).

- 등록 중에 생성할 임의의 일회용 암호 **(OTP)**입니다. 이 인증 방법을 사용하려면 인벤토리 파일에서 **ipaclient_use_otp=yes** 옵션을 사용합니다. 예를 들어 **inventory/hosts** 파일의 **[ipaclients:vars]** 섹션에서 **ipaclient_use_otp=yes** 옵션의 주석을 달 수 있습니다. **OTP**를 사용하면 다음 옵션 중 하나를 지정해야 합니다.

  - 예를 들어 **inventory/hosts** 파일 의 **[ipaclients:vars]** 섹션에 **ipaadmin_password** 값을 제공하여 클라이언트 등록 권한이 있는 사용자의 암호입니다.

  - 예를 들어 **inventory/hosts** 의 **[ipaclients:vars]** 섹션에 **ipaadmin_keytab** 의 값을 제공하여 **admin keytab.**

추가 리소스

- **ipaclient Ansible** 역할에서 허용하는 옵션에 대한 자세한 내용은 **/usr/share/ansible/roles/ipaclient/README.md README** 파일을 참조하십시오.

32.2. 클라이언트 설치 중 자동 검색을 수행할 수 없는 경우 인벤토리 파일의 매개변수 설정

Ansible 플레이북을 사용하여 **Identity Management** 클라이언트를 설치하려면 인벤토리 파일에서 대

상 호스트 매개 변수를 구성합니다(예: inventory/hosts).

- 호스트, IdM 서버, IdM 도메인 또는 IdM 영역에 대한 정보
- 작업에 대한 권한 부여

인벤토리 파일은 보유한 인벤토리 플러그인에 따라 여러 형식 중 하나일 수 있습니다. INI와 유사한 형식은 Ansible의 기본값 중 하나이며 아래 예제에서 사용됩니다.

참고

RHEL의 그래픽 사용자 인터페이스와 함께 스마트 카드를 사용하려면 Ansible 플레이북에 ipaclient_mkhomedir 변수를 포함해야 합니다.

사전 요구 사항

- 제어 노드에서 배포 지침을 확인하고 install-client.yml 파일의 매개변수 확인을 참조하십시오.

절차

1. IdM 클라이언트가 될 호스트의 정규화된 호스트 이름(FQDN)을 지정합니다. 정규화된 도메인 이름은 유효한 DNS 이름이어야 합니다.
   - 숫자, 영문자 및 하이픈(-)만 허용됩니다. 예를 들어 밑줄은 허용되지 않으며 DNS 오류가 발생할 수 있습니다.
   - 호스트 이름은 모두 소문자여야 합니다. 대문자는 사용할 수 없습니다.
2. inventory/hosts 파일의 관련 섹션에 다른 옵션을 지정합니다.
   - 클라이언트가 등록할 IdM 서버를 나타내는 [ipaservers] 섹션에 있는 서버의 FQDN

- 다음 두 가지 옵션 중 하나입니다.

  - 클라이언트가 등록할 **IdM** 서버의 **DNS** 도메인 이름을 나타내는 **[ipaclients:vars]** 섹션의 **ipaclient_domain** 옵션

  - **[ipaclients:vars]** 섹션의 **ipaclient_realm** 옵션으로 **IdM** 서버에서 제어하는 **Kerberos** 영역의 이름을 나타냅니다.

클라이언트 **FQDN,** 서버 **FQDN** 및 정의된 도메인을 사용하는 인벤토리 호스트 파일의 예

```
[ipaclients]
client.idm.example.com

[ipaservers]
server.idm.example.com

[ipaclients:vars]
ipaclient_domain=idm.example.com
[...]
```

3. 클라이언트 등록 자격 증명을 지정합니다. 다음 인증 방법을 사용할 수 있습니다.

- 클라이언트를 등록할 권한이 있는 사용자의 암호 입니다. 이는 기본 옵션입니다.

  - **Red Hat**은 **Ansible Vault**를 사용하여 암호를 저장하고 플레이북 파일에서 **Vault** 파일을 참조하는 것이 좋습니다(예**: install-client.yml).** 직접**: Ansible Vault** 파일의 보안 주체 및 암호의 보안 주체를 사용하는 **. examples** 플레이북 파일입니다.

```
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true
  vars_files:
  - *playbook_sensitive_data.yml*

  roles:
  - role: ipaclient
    state: present
```

- 더 안전하게 **inventory/hosts** 파일의 **[ipaclients:vars]** 섹션에서 **ipa admin _password** 옵션을 사용하여 **admin**의 자격 증명을 제공하십시오. 또는 권한이 있는 다른 사용자를 지정하려면 사용자 이름에 **ipaadmin_principal** 옵션을 사용하고 암호에 **ipaadmin_password** 옵션을 사용합니다. **install-client.yml Playbook** 파일은 다음과 같이 표시될 수 있습니다.

인벤토리 호스트 파일 예

```
[...]
[ipaclients:vars]
ipaadmin_principal=my_admin
ipaadmin_password=Secret123
```

인벤토리 파일에서 보안 주체 및 암호를 사용하는 플레이북의 예

```
- name: Playbook to unconfigure IPA clients
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: true
```

- 이전 등록의 클라이언트 키탭 이 계속 사용 가능한 경우:

이 옵션은 시스템이 이전에 **ID** 관리 클라이언트로 등록된 경우 사용할 수 있습니다. 이 인증 방법을 사용하려면 **ipaclient_keytab** 옵션의 주석을 제거하여 **keytab**을 저장하는 파일의 경로를 지정합니다(예: **inventory/hosts** 의 **[ipaclient:vars]** 섹션).

- 등록 중에 생성할 임의의 일회용 암호 (**OTP**)입니다. 이 인증 방법을 사용하려면 인벤토리 파일에서 **ipaclient_use_otp=yes** 옵션을 사용합니다. 예를 들어 **inventory/hosts** 파일의 **[ipaclients:vars]** 섹션에서 **#ipaclient_use_otp=yes** 옵션의 주석을 달 수 있습니다. **OTP**를 사용하면 다음 옵션 중 하나를 지정해야 합니다.

  - 예를 들어 **inventory/hosts** 파일 의 **[ipaclients:vars]** 섹션에 **ipaadmin_password** 값

을 제공하여 클라이언트 등록 권한이 있는 사용자의 암호입니다.

- 예를 들어 **inventory/hosts** 의 **[ipaclients:vars]** 섹션에 **ipaadmin_keytab** 의 값을 제공하여 **admin keytab.**

추가 리소스

- **ipaclient Ansible** 역할에서 허용하는 옵션에 대한 자세한 내용은 **/usr/share/ansible/roles/ipaclient/README.md README** 파일을 참조하십시오.

32.3. INSTALL-CLIENT.YML 파일에서 매개변수 확인

install-client.yml 플레이북 파일에는 **IdM** 클라이언트 배포에 대한 지침이 포함되어 있습니다.

절차

- 파일을 열고 플레이북의 지침이 배포 계획과 일치하는지 확인합니다. 일반적으로 내용은 다음과 같습니다.

```
---
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: present
```

개별 항목이 나타내는 것은 다음과 같습니다.

- **hosts** 항목은 **ansible** 스크립트가 **ipa-client-install** 스크립트를 실행할 호스트의 **FQDN** 을 검색하는 **inventory/hosts** 파일의 섹션을 지정합니다.
- **become: true** 항목은 **ipa-client-install** 스크립트를 실행하는 동안 **root**의 자격 증명이 호출되도록 지정합니다.
- **role: ipaclient** 항목은 호스트에 설치할 역할을 지정합니다. 이 경우 **ipa** 클라이언트 역할입니다.

- **state: present** 항목은 클라이언트를 설치 제거하는 대신 설치하도록 지정합니다(없음없음).

32.4. ANSIBLE PLAYBOOK을 사용하여 IDM 클라이언트 등록에 대한 권한 부여 옵션

이 참조 섹션에서는 IdM 클라이언트 등록에 대한 개별 권한 부여 옵션에 인벤토리 및 플레이북 파일 예제를 제공합니다.

표 32.1. Ansible을 사용하여 IdM 클라이언트 등록에 대한 권한 부여 옵션

권한 부여 옵션	참고	인벤토리 파일 예	install-client.yml 플레이북 파일 예
클라이언트를 등록할 권한이 있는 사용자의 암호: 옵션 1	Ansible 자격 증명 모음에 저장된 암호	[ipaclients:vars] [...]	- name: Playbook to configure IPA clients with username/password hosts: ipaclients become: true vars_files: - playbook_sensitive_data.yml roles: - role: ipaclient state: present
클라이언트를 등록할 권한이 있는 사용자의 암호: 옵션 2	인벤토리 파일에 저장된 암호	[ipaclients:vars] ipaadmin_password=Secret123	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true
임의의 일회성 암호(one-time password)입니다. 옵션 1	OTP + 관리자 암호	[ipaclients:vars] ipaadmin_password=Secret123 ipaclient_use_otp=yes	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true

권한 부여 옵션	참고	인벤토리 파일 예	install-client.yml 플레이북 파일 예
임의의 일회성 암호(one-time password)입니다. 옵션 2	OTP + 관리자 키 탭	[ipaclients:vars] ipaadmin_keytab=/tmp/admin.keytab ipaclient_use_otp=yes	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true
이전 등록의 클라이언트 키탭		[ipaclients:vars] ipaclient_keytab=/tmp/krb5.keytab	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true

32.5. ANSIBLE 플레이북을 사용하여 IDM 클라이언트 배포

IdM 환경에 IdM 클라이언트를 배포하는 Ansible 플레이북을 사용하려면 이 절차를 완료합니다.

사전 요구 사항

- **IdM 클라이언트 배포의 매개변수가 배포 시나리오에 일치하도록 설정되어 있습니다.**
  - 자동 검색 클라이언트 설치 모드에 대한 인벤토리 파일의 매개변수 설정
  - 클라이언트 설치 중 자동 검색을 수행할 수 없는 경우 인벤토리 파일의 매개변수 설정
- **install-client.yml에서 매개변수를 확인했습니다.**

절차

-

Ansible 플레이북을 사용하여 IdM 클라이언트를 설치하려면 플레이북 파일의 이름과 함께 ansible-playbook 명령을 사용합니다(예: install-client.yml). -i 옵션으로 인벤토리 파일을 지정합니다.

```
$ ansible-playbook -v -i inventory/hosts install-client.yml
```

v , -vv 또는 - vv v 옵션을 사용하여 상세 정보 표시 수준을 지정합니다.

Ansible은 Ansible 플레이북 스크립트 실행에 대해 알려줍니다. 다음 출력은 작업이 실패하지 않았기 때문에 스크립트가 성공적으로 실행되었음을 보여줍니다.

```
PLAY RECAP
client1.idm.example.com : ok=18 changed=10 unreachable=0 failed=0 skipped=21
rescued=0 ignored=0
```

참고

Ansible은 다양한 색상을 사용하여 실행 중인 프로세스에 대한 다양한 유형의 정보를 제공합니다. /etc/ansible/ansible.cfg 파일의 [colors] 섹션에서 기본 색상을 수정할 수 있습니다.

```
[colors]
[...]
#error = red
#debug = dark gray
#deprecate = purple
#skip = cyan
#unreachable = red
#ok = green
#changed = yellow
[...]
```

이제 Ansible 플레이북을 사용하여 호스트에 IdM 클라이언트를 설치했습니다.

32.6. ANSIBLE 설치 후 IDENTITY MANAGEMENT 클라이언트 테스트

CLI(명령줄 인터페이스)는 ansible-playbook 명령이 성공했지만 자체 테스트를 수행할 수도 있음을 알려줍니다.

ID 관리 클라이언트가 서버에 정의된 사용자에 대한 정보를 가져올 수 있는지 테스트하려면 서버에 정의된 사용자를 확인할 수 있는지 확인합니다. 예를 들어 기본 admin 사용자를 확인하려면 다음을 실행합

니다.

```
[user@client1 ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

인증이 올바르게 작동하는지 테스트하려면 **su -** 가 이미 존재하는 다른 **IdM** 사용자로 작동합니다.

```
[user@client1 ~]$ su - idm_user
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[idm_user@client1 ~]$
```

32.7. ANSIBLE 플레이북을 사용하여 IDM 클라이언트 설치 제거

Ansible 플레이북을 사용하여 **IdM** 클라이언트로 호스트를 제거하려면 이 절차를 완료합니다.

사전 요구 사항

- **IdM** 관리자 자격 증명.

절차

- **IdM** 클라이언트를 설치 제거하려면 플레이북 파일의 이름과 함께 **ansible-playbook** 명령을 사용합니다(예: **uninstall-client.yml**). **-i** 옵션으로 인벤토리 파일을 지정하고 선택적으로 **-v, -vv** 또는 **- vv v** 옵션을 사용하여 세부 정보 표시 수준을 지정합니다.

```
$ ansible-playbook -v -i inventory/hosts uninstall-client.yml
```

중요

클라이언트를 다시 설치하기로 결정하는 경우 클라이언트의 기본 IdM 구성만 호스트에서 제거하지만 호스트의 구성 파일은 그대로 둡니다. 또한 설치 제거에는 다음과 같은 제한 사항이 있습니다.

- IdM LDAP 서버에서 클라이언트 호스트 항목을 제거하지 않습니다. 설치 제거는 호스트 등록을 취소만 합니다.
- IdM에서 클라이언트에 있는 서비스는 제거되지 않습니다.
- IdM 서버에서 클라이언트의 DNS 항목을 제거하지 않습니다.
- /etc/krb5.keytab 이 아닌 키탭의 이전 주체는 제거되지 않습니다.

제거 제거는 IdM CA에서 호스트에 대해 실행된 모든 인증서를 제거합니다.

추가 리소스

- IdM 클라이언트 제거를 참조하십시오.

II 부. IDM 및 AD 통합

33장. IDM과 AD 간 신뢰 설치

이 장은 ID 관리 IdM 서버와 AD(Active Directory) 간에 트러스트를 만드는 것을 목표로 하며, 두 서버가 동일한 서쪽에 있습니다.

사전 요구 사항

- 먼저 Identity Management와 Active Directory 문서 간의 가장 큰 신뢰를 계획 해야 합니다.
- AD는 도메인 컨트롤러와 함께 설치됩니다.
- IdM 서버가 설치되어 실행 중입니다.
  - 자세한 내용은 Identity Management 설치를 참조하십시오.
- Kerberos는 통신에서 최대 5분 지연이 필요하기 때문에 AD 서버와 IdM 서버 모두 시계가 동기화되어야 합니다.
- unique#150 names는 Active Directory 도메인을 식별하는 데 매우 중요하기 때문에 신뢰에 배치된 각 서버에 대한 complete names.
  - Active Directory 또는 IdM 도메인의 complete name은 일반적으로 해당 DNS 도메인의 첫 번째 부분입니다. DNS 도메인이 ad.example.com 인 경우 complete 이름은 일반적으로 AD 입니다. 그러나 필요하지 않습니다. important is that the rfc name is just one word without periods. rootfs 이름의 최대 길이는 15자입니다.
- IdM 시스템에는 커널에 IPv6 프로토콜이 활성화되어 있어야 합니다.
  - IPv6를 비활성화하면 IdM 서비스에서 사용하는 CLDAP 플러그인이 초기화되지 않습니다.

33.1. 지원되는 WINDOWS SERVER 버전

RHEL 8.4에서 IdM(Identity Management)은 Windows Server 2008 R2 또는 이전 버전을 실행하는 Active Directory 도메인 컨트롤러를 사용하여 Active Directory에 대한 신뢰 설정을 지원하지 않습니다.

RHEL IdM에는 이제 Windows Server 2012 이상에서만 지원되는 신뢰 관계를 설정할 때 SMB 암호화가 필요합니다.

다음과 같은 하위 도메인 및 도메인 기능 수준을 사용하는 AD(Active Directory) 장애 조치와의 트러스트 관계를 설정할 수 있습니다.

- Velero 기능 수준 범위: Windows Server 2012 — Windows Server 2016
- 도메인 기능 수준 범위: Windows Server 2012 — Windows Server 2016

IdM(Identity Management)은 다음 운영 체제를 실행하는 Active Directory 도메인 컨트롤러를 사용한 신뢰 설정을 지원합니다.

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

33.2. 신뢰의 작동 방식

Identity Management IdM과 AD(Active Directory) 간의 신뢰는 Cross-realm Kerberos 신뢰에 설정됩니다. 이 솔루션은 Kerberos 기능을 사용하여 서로 다른 ID 소스 간의 신뢰를 설정합니다. 따라서 모든 AD 사용자는 다음을 수행할 수 있습니다.

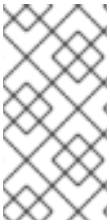
- Linux 시스템 및 리소스에 액세스하려면 로그인합니다.
- SSO(Single Sign-On) 사용.

모든 IdM 오브젝트는 신뢰의 IdM에서 관리됩니다.

모든 AD 오브젝트는 신뢰의 AD에서 관리됩니다.

복잡한 환경에서는 단일 IdM 창은 여러 AD forests에 연결할 수 있습니다. 이러한 설정을 사용하면 조직의 다양한 기능에 대한 업무를 보다 효과적으로 분리할 수 있습니다. AD 관리자는 사용자와 관련된 사용자 및 정책에 중점을 둘 수 있으며 Linux 관리자는 Linux 인프라를 완전히 제어할 수 있습니다. 이러한 경우 IdM에 의해 제어되는 Linux 영역은 AD 리소스 도메인 또는 영역과 유사하지만 Linux 시스템과 유사합니다.

AD의 관점에서 Identity Management는 단일 AD 도메인이 있는 별도의 AD 재정의를 나타냅니다. AD forest 루트 도메인과 IdM 도메인 간의 교차 트러스트가 설정된 경우 AD domain의 사용자는 IdM 도메인의 Linux 시스템 및 서비스와 상호 작용할 수 있습니다.



참고

신뢰 환경에서 IdM을 사용하면 ID 뷰를 사용하여 IdM 서버에서 AD 사용자의 POSIX 속성을 구성할 수 있습니다.

33.3. AD 관리 권한

AD (Active Directory)와 IdM (Identity Management) 간에 신뢰를 구축하려는 경우 적절한 AD 권한으로 AD 관리자 계정을 사용해야합니다.

이러한 AD 관리자는 다음 그룹 중 하나의 멤버여야 합니다.

- AD forest의 Enterprise Admin 그룹
- Active Directory 도메인의 도메인 관리 루트 도메인 도메인 도메인 도메인 도메인 도메인 (Domain Admins) group for your AD domains

추가 리소스

- 엔터프라이즈 관리자에 대한 자세한 내용은 Enterprise 관리자를 참조하십시오.

- 도메인 관리자에 대한 자세한 내용은 도메인 관리자를 참조하십시오.

- AD 신뢰에 대한 자세한 내용은 How Domain and Forest Trusts Work 을 참조하십시오.

33.4. AD 및 RHEL에서 공통 암호화 유형 지원

기본적으로 Identity Management는 RC4, AES-128 및 AES-256 Kerberos 암호화 유형을 지원하여 교차 영역의 신뢰를 설정합니다.

RC4 암호화는 최신 AES-128 및 AES-256 암호화 유형보다 덜 안전한 것으로 간주되므로 기본적으로 더 이상 사용되지 않으며 비활성화되어 있습니다. 반대로 AD(Active Directory) 사용자 자격 증명과 AD 도메인 간의 신뢰는 RC4 암호화를 지원하며 AES 암호화 유형을 지원하지 않을 수 있습니다.

일반적인 암호화 유형이 없으면 IdM과 AD 하위 도메인 간의 통신이 작동하지 않거나 일부 AD 계정이 인증할 수 없습니다. 이 문제를 해결하려면 다음 설정 중 하나를 수정하십시오.

Active Directory에서 AES 암호화 지원 활성화 (권장 옵션)

Active Directory의 AD 도메인 간 신뢰가 강력한 AES 암호화 유형을 지원하도록 하려면 다음 Microsoft 문서를 참조하십시오. AD DS: 보안: 신뢰할 수 있는 도메인의 리소스에 액세스할 때 Kerberos "Unsupported etype" 오류

RHEL에서 RC4 지원 활성화

모든 IdM 신뢰 컨트롤러, 신뢰 에이전트 및 AD 도메인 컨트롤러에 대한 인증이 수행됩니다.

a. update-crypto-policies 명령을 사용하여 DEFAULT 암호화 정책 외에 AD-SUPPORT 암호화 하위 정책을 활성화합니다.

```
[root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT
Setting system policy to DEFAULT:AD-SUPPORT
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

b. 호스트를 다시 시작합니다.

중요

AD-SUPPORT 암호화 하위 정책은 **RHEL 8.3** 이상에서만 사용할 수 있습니다.

- **RHEL 8.2**에서 **RC4**에 대한 지원을 활성화하려면 암호 **= RC4-128+** 를 사용하여 사용자 정의 암호화 모듈 정책을 생성 및 활성화합니다. 자세한 내용은 정책 한정자를 사용하여 시스템 전체 암호화 정책 사용자 지정을 참조하십시오.

- **RHEL 8.0** 및 **RHEL 8.1**에서 **RC4**에 대한 지원을 활성화하려면 **/etc/crypto-policies/back-ends/krb5.config** 파일의 **permitted_enctypes** 옵션에 **+rc4** 를 추가합니다.

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
```

추가 리소스

- 전체 시스템 암호화 정책 사용을 참조하십시오.

- 신뢰 컨트롤러 및 신뢰 에이전트 를 참조하십시오.

33.5. IDM과 AD 간 통신에 필요한 포트

AD(Active Directory) 및 **IdM(Identity Management)** 환경 간의 통신을 활성화하려면 **AD** 도메인 컨트롤러 및 **IdM** 서버의 방화벽에서 다음 포트를 엽니다.

표 **33.1. AD** 신뢰에 필요한 포트

서비스	포트	프로토콜
끝점 확인 portmapper	135	TCP
NetBIOS-DGM	138	TCP 및 UDP
NetBIOS-SSN	139	TCP 및 UDP
Microsoft-DS	445	TCP 및 UDP

서비스	포트	프로토콜
Dynamic RPC	49152-65535	TCP
AD 글로벌 카탈로그	3268	TCP
LDAP	389	TCP 및 UDP

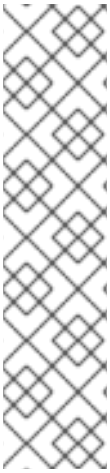
참고

TCP 포트 **389**는 신뢰를 얻기 위해 **IdM** 서버에서 열 필요는 없지만 **IdM** 서버와 통신하는 클라이언트가 필요합니다.

포트를 열기 위해 다음 방법을 사용할 수 있습니다.

- **firewalld** 서비스는 특정 포트를 활성화하거나 포트를 포함하는 다음 서비스를 활성화할 수 있습니다.
  - **FreeIPA** 신뢰 설정
  - **LDAP**를 사용하는 **FreeIPA**
  - **Kerberos**
  - **DNS**

자세한 내용은 **CLI**를 사용하여 포트 제어를 참조하십시오.

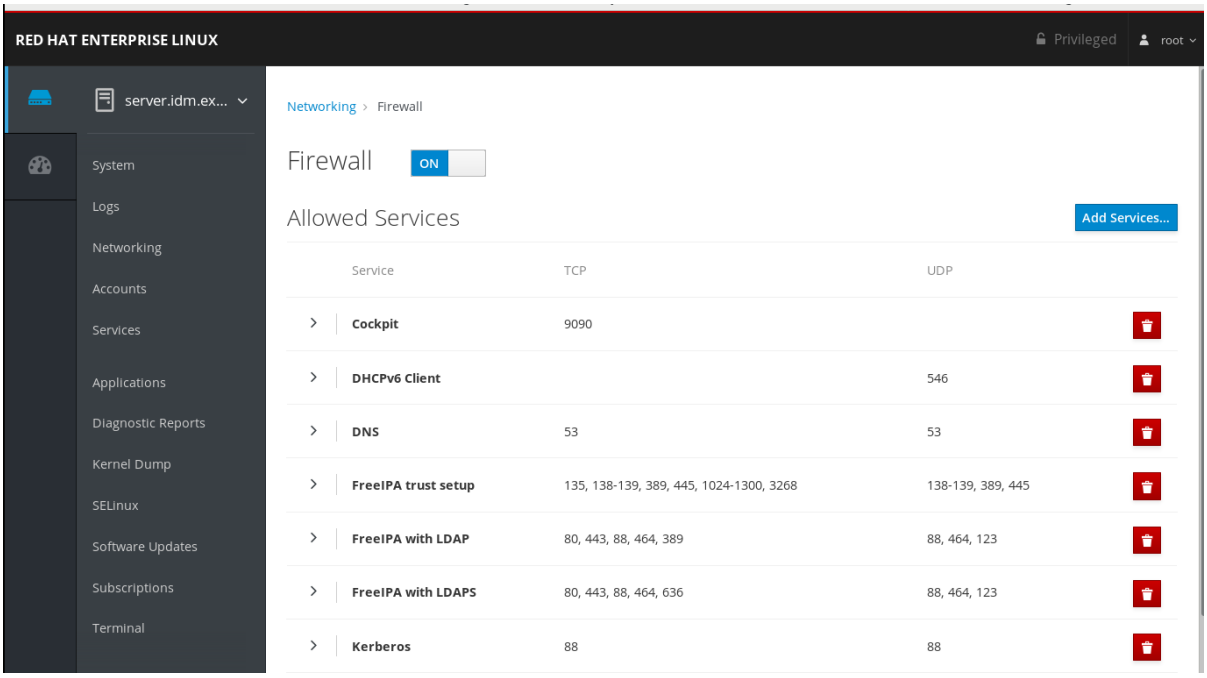


참고

RHEL 8.2 및 이전 버전을 사용하는 경우 freeipa-trust Firewalld 서비스에는 1024-1300 의 RPC 포트 범위가 포함되어 있으며 이는 잘못된 것입니다. RHEL 8.2 및 이전 버전에서는 freeipa-trust Firewalld 서비스를 활성화하는 것 외에도 TCP 포트 범위 49152-65535 를 수동으로 열어야 합니다.

이 문제는 버그 1850418에서 RHEL 8.3 이상에 수정되어 올바른 동적 RPC 범위를 포함하도록 freeipa-trust.xml 정의를 업데이트합니다.

- **firewalld 서비스를 기반으로 방화벽 설정이 있는 UI인 RHEL 웹 콘솔.**



웹 콘솔을 통한 방화벽 구성에 대한 자세한 내용은 웹 콘솔 을 사용하여 방화벽에서 서비스활성화를 참조하십시오.

참고

RHEL 8.2 및 이전 버전을 사용하는 경우 FreeIPA 트러스트 설정 서비스에는 1024-1300 의 RPC 포트 범위가 포함되어 있으며 이는 올바르지 않습니다. RHEL 8.2 및 이전 버전에서는 RHEL 웹 콘솔에서 FreeIPA 신뢰 설정 서비스를 활성화하는 것 외에도 TCP 포트 범위 49152-65535 를 수동으로 열어야 합니다.

이 문제는 버그 1850418에서 RHEL 8.3 이상에 수정되어 올바른 동적 RPC 범위를 포함하도록 freeipa-trust.xml 정의를 업데이트합니다.

표 33.2. 신뢰의 IdM 서버에 필요한 포트

서비스	포트	프로토콜
Kerberos	88, 464	TCP 및 UDP
LDAP	389	TCP
DNS	53	TCP 및 UDP

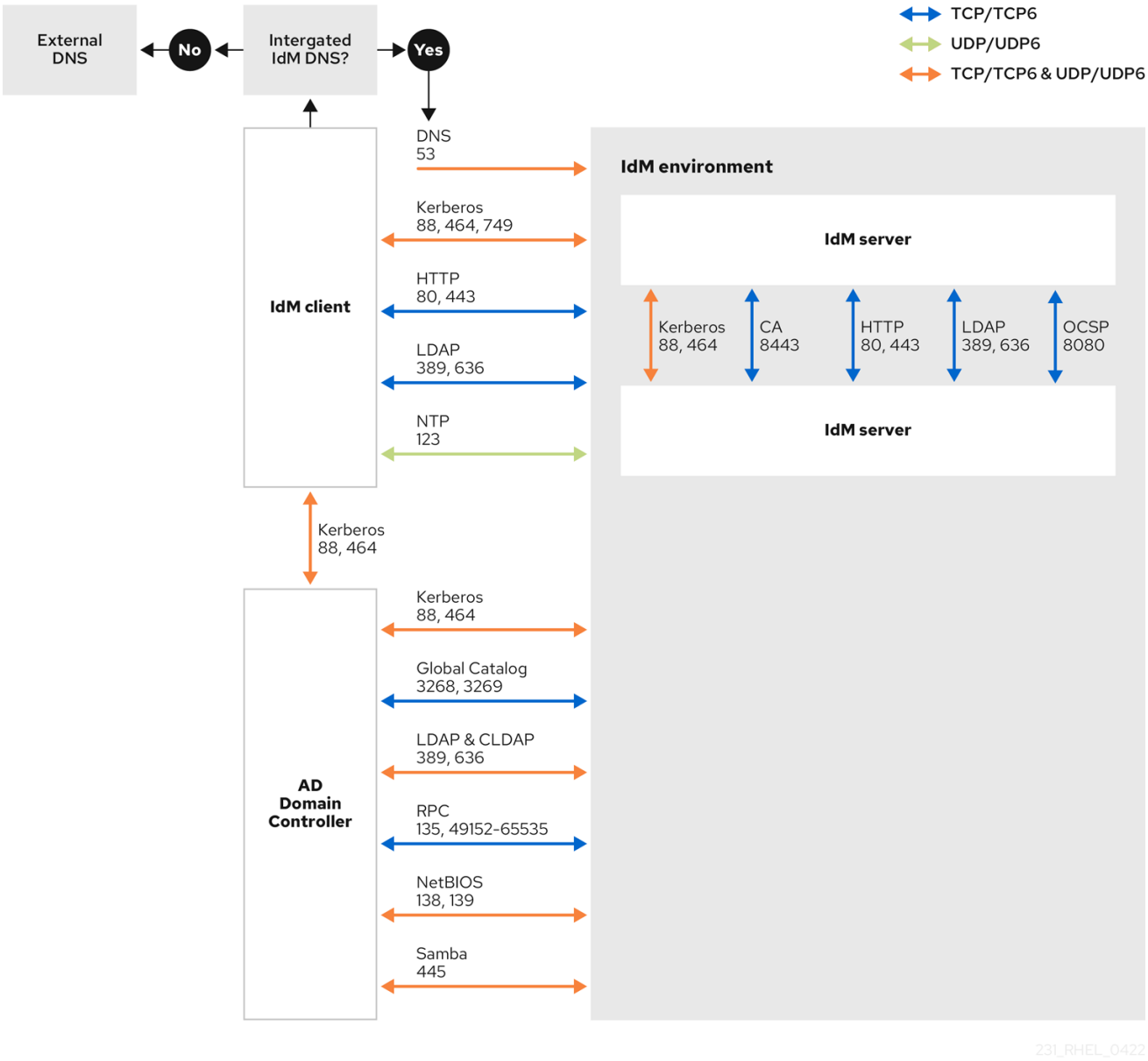
표 33.3. AD 신뢰의 IdM 클라이언트에 필요한 포트

서비스	포트	프로토콜
Kerberos	88	UDP 및 TCP

참고

libkrb5 라이브러리는 UDP를 사용하며 KDC(Key Distribution Center)에서 전송된 데이터가 너무 크면 TCP 프로토콜로 돌아갑니다. Active Directory는 KC(Privilege Attribute Certificate)를 Kerberos 티켓에 연결하여 크기를 증가시키고 TCP 프로토콜을 사용해야 합니다. 기본적으로 Red Hat Enterprise Linux 7.4의 SSSD에서 문제가 발생하지 않고 나중에 사용자 인증에 TCP를 사용합니다. libkrb5가 TCP를 사용하기 전에 크기를 구성하려면 /etc/krb.5.conf 파일에서 udp_preference_limit 를 설정합니다. 자세한 내용은 jenkinsfile 5.conf(5) 매뉴얼 페이지를 참조하십시오.

다음 다이어그램은 IdM 클라이언트, IdM 서버 및 AD 도메인 컨트롤러가 서로 통신할 때 사용하는 포트 및 프로토콜을 보여줍니다.



추가 리소스

- Windows Server 2008 이상의 동적 RPC 포트 범위에 대한 자세한 내용은 Windows Vista 및 Windows Server 2008 이후 TCP/IP의 기본 동적 포트 범위를 참조하십시오.

33.6. 신뢰에 대한 DNS 및 영역 설정 구성

신뢰에서 IdM(Identity Management) 및 AD(Active Directory)를 연결하기 전에 서버가 서로를 보고 도메인 이름을 올바르게 확인해야 합니다. 이 시나리오에서는 다음과 같은 도메인 이름을 사용하도록 DNS 구성에 대해 설명합니다.

- 통합된 DNS 서버 및 인증 기관을 사용하는 하나의 기본 IdM 서버입니다.
- AD 도메인 컨트롤러 1개.

DNS 설정에는 다음이 필요합니다.

- IdM 서버의 DNS 영역 구성
- AD에서 조건부 DNS 전달 구성
- DNS 구성의 정확성 확인

33.6.1. 고유한 기본 DNS 도메인

Windows에서 모든 도메인은 Kerberos 영역과 동시에 DNS 도메인입니다. 도메인 컨트롤러에서 관리하는 모든 도메인에는 고유한 전용 DNS 영역이 있어야 합니다. IdM(Identity Management)이 Active Directory(AD)에서 재정의할 때에도 적용됩니다. AD는 IdM에 자체 DNS 도메인이 있을 것으로 예상합니다. 신뢰 설정이 작동하려면 DNS 도메인을 Linux 환경 전용으로 사용해야 합니다.

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

- AD의 경우 *ad.example.com* 및 IdM용 *idm.example.com*
- *example.com* for AD 및 *idm.example.com* for IdM
- AD의 경우 *ad.example.com* 및 IdM용 *example.com*

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

Kerberos 영역 이름을 기본 DNS 도메인 이름의 대문자로 표시

Kerberos 영역 이름은 모든 문자 대문자가 있는 기본 DNS 도메인 이름과 동일해야 합니다. 예를 들어 도메인 이름이 AD의 경우 *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 확인할 수 있는 DNS 레코드

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

IdM 및 AD DNS 도메인

IdM에 결합된 시스템을 여러 DNS 도메인에 배포할 수 있습니다. Red Hat은 Active Directory가 소유한 것과 다른 DNS 영역에 IdM 클라이언트를 배포하는 것이 좋습니다. 기본 IdM DNS 도메인에는 AD 트러스트를 지원하기 위한 적절한 SRV 레코드가 있어야 합니다.

참고

IdM과 Active Directory 간에 신뢰가 있는 일부 환경에서는 Active Directory DNS 도메인에 포함된 호스트에 IdM 클라이언트를 설치할 수 있습니다. 그러면 호스트는 IdM의 Linux 중심 기능을 활용할 수 있습니다. 이는 권장되지 않으며 몇 가지 제한 사항이 있습니다. 자세한 내용은 Active Directory DNS 도메인에 IdM 클라이언트 구성을 참조하십시오.

다음 명령을 실행하여 시스템 설정과 관련된 필수 SRV 레코드 목록을 가져올 수 있습니다.

```
$ ipa dns-update-system-records --dry-run
```

생성된 목록은 예를 다음과 같이 찾을 수 있습니다.

```
IPA DNS records:
_kerberos-master._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos-master._udp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos.idm.example.com. 86400 IN TXT "IDM.EXAMPLE.COM"
_kpasswd._tcp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_kpasswd._udp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_ldap._tcp.idm.example.com. 86400 IN SRV 0 100 389 server.idm.example.com.
_ipa-ca.idm.example.com. 86400 IN A 192.168.122.2
```

동일한 IdM 영역에 속하는 다른 DNS 도메인의 경우 AD에 대한 신뢰가 구성되면 SRV 레코드를 구성할 필요가 없습니다. 그 이유는 AD 도메인 컨트롤러에서 SRV 레코드를 사용하지 않고 trust에 대한 이름 접미사 라우팅 정보를 기반으로 합니다.

33.6.2. IdM 웹 UI에서 DNS 전달 영역 구성

이 섹션에서는 IdM 웹 UI를 사용하여 IdM(Identity Management) 서버에 새 DNS 전달 영역을 추가하는 방법을 설명합니다.

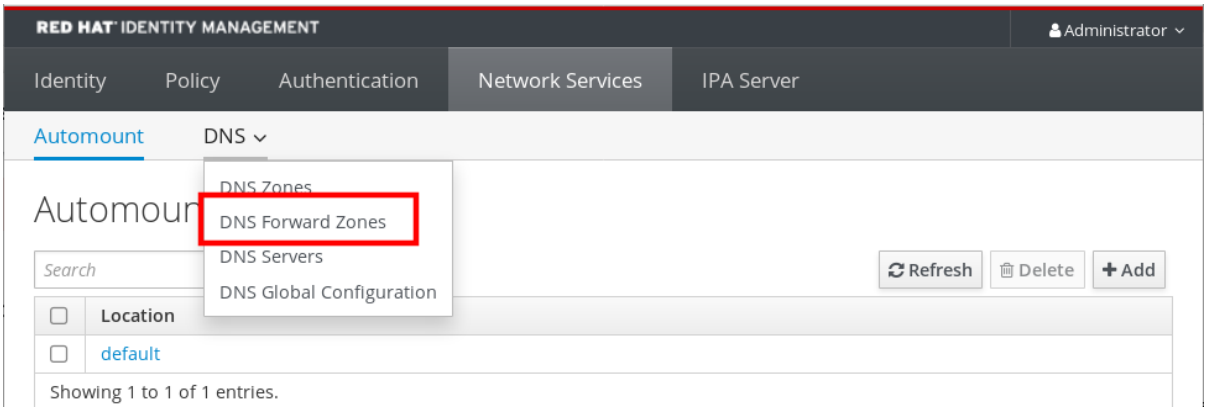
DNS 전달 영역을 사용하면 특정 영역에 대한 DNS 쿼리를 다른 DNS 서버로 전달할 수 있습니다. 예를 들어 AD(Active Directory) 도메인에 대한 DNS 쿼리를 AD DNS 서버로 전달할 수 있습니다.

사전 요구 사항

- 관리자 권한이 있는 사용자 계정을 사용하여 IdM 웹 UI에 액세스할 수 있습니다.
- DNS 서버가 올바르게 구성되어 있습니다.

절차

1. 관리자 권한으로 IdM 웹 UI에 로그인합니다. 자세한 내용은 웹 브라우저에서 IdM 웹 UI 액세스를 참조하십시오.
2. Network Services 탭을 클릭합니다.
3. DNS 탭을 클릭합니다.
4. 드롭다운 메뉴에서 DNS Forward Zones 항목을 클릭합니다.



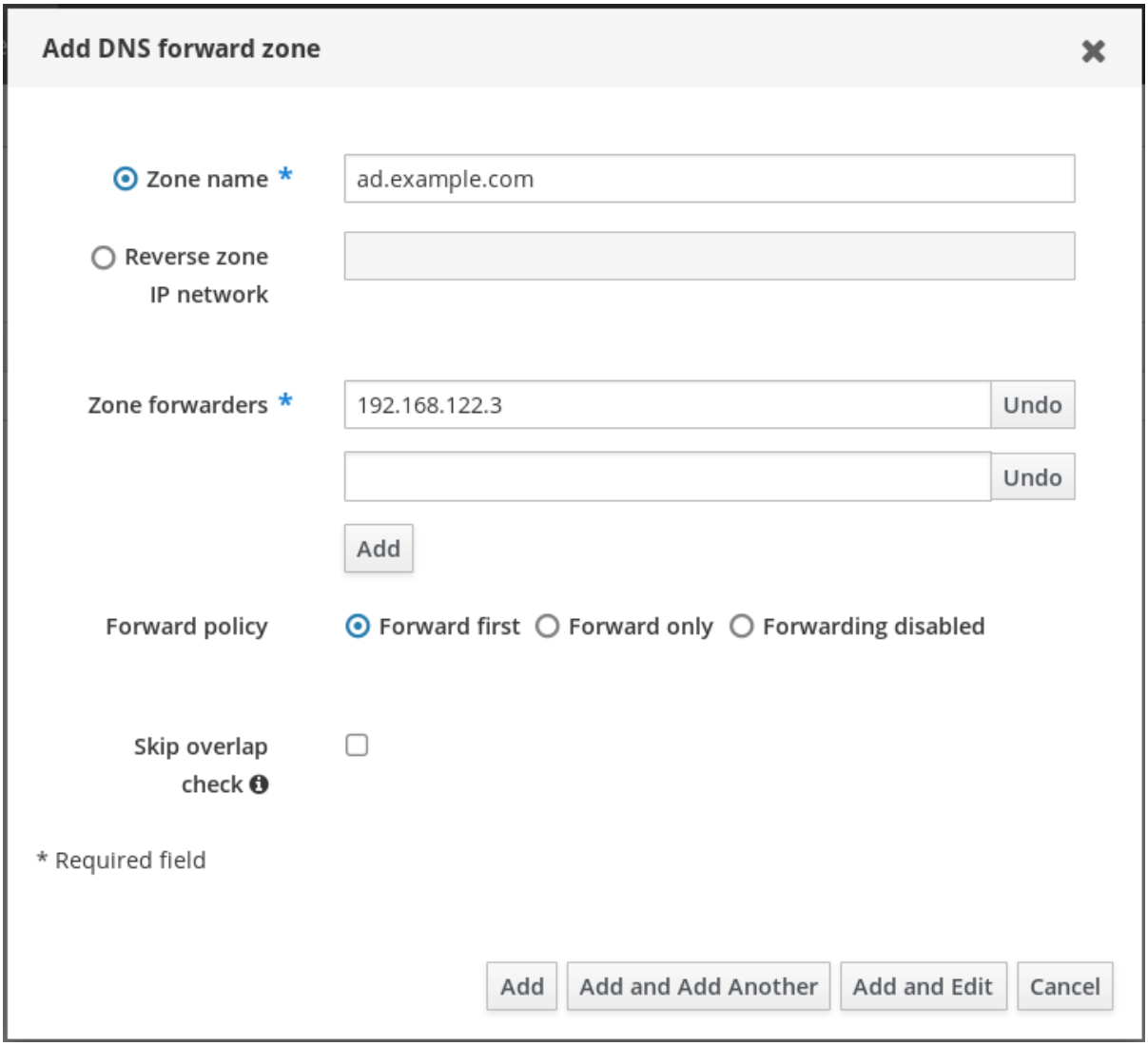
5. **Add** 버튼을 클릭합니다.

6. **DNS** 전달 영역 추가 대화 상자에서 영역 이름을 추가합니다.

7. **Zone forwarders** 항목에서 추가 버튼을 클릭합니다.

8. **Zone forwarders** 필드에서 새 전달 영역을 만들 서버의 **IP** 주소를 추가합니다.

9. **Add** 버튼을 클릭합니다.

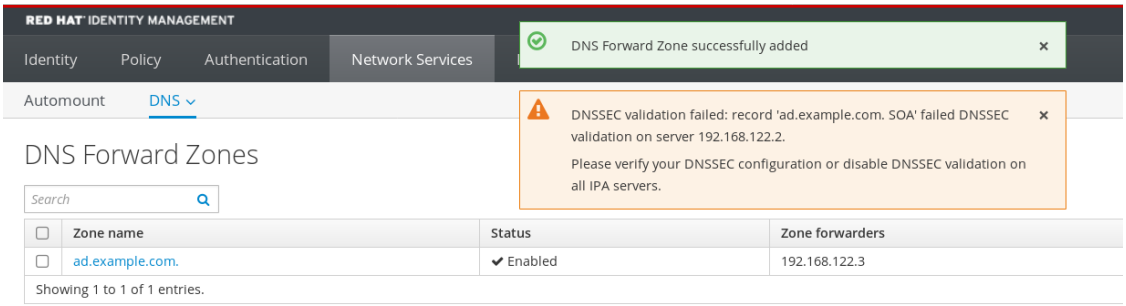


전달된 영역이 **DNS** 설정에 추가되어 **DNS Forward Zones** 설정에서 확인할 수 있습니다. 웹 **UI**는 다

음과 같은 팝업 메시지를 사용하여 성공을 알립니다. **DNS Forward Zone**이 성공적으로 추가되었습니다.

참고

구성에 새 전달 영역을 추가한 후 **Web UI**에 **DNSSEC** 검증 실패에 대한 경고가 표시될 수 있습니다.



DNSSEC (Domain Name System Security Extensions)는 공격으로부터 **DNS**를 보호하기 위해 디지털 서명으로 **DNS** 데이터를 보호합니다. 이 서비스는 **IdM** 서버에서 기본적으로 활성화됩니다. 원격 **DNS** 서버에서 **DNSSEC**를 사용하지 않기 때문에 경고가 표시됩니다. 원격 **DNS** 서버에서 **DNSSEC**를 활성화하는 것이 좋습니다.

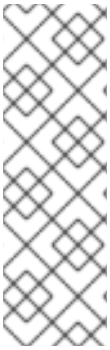
원격 서버에서 **DNSSEC** 검증을 활성화할 수 없는 경우 **IdM** 서버에서 **DNSSEC**를 비활성화할 수 있습니다.

1. 편집할 적절한 구성 파일을 선택합니다.

   - **IdM** 서버에서 **RHEL 8.0** 또는 **RHEL 8.1**을 사용하는 경우 **/etc/named.conf** 파일을 엽니다.
   - **IdM** 서버가 **RHEL 8.2** 이상을 사용하는 경우 **/etc/named/ipa-options-ext.conf** 파일을 엽니다.

2. 다음 **DNSSEC** 매개변수를 추가합니다.

```
dnssec-enable no;
dnssec-validation no;
```



3. 구성 파일을 저장하고 닫습니다.

4. DNS 서비스를 다시 시작하십시오.

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

검증 단계

- 원격 DNS 서버의 이름과 함께 nslookup 명령을 사용합니다.

```
$ nslookup ad.example.com
Server:        192.168.122.2
Address:       192.168.122.2#53

No-authoritative answer:
Name:          ad.example.com
Address:       192.168.122.3
```

도메인 전달이 올바르게 구성된 경우 nslookup 요청에 원격 DNS 서버의 IP 주소가 표시됩니다.

33.6.3. CLI에서 DNS 전달 영역 구성

이 섹션에서는 CLI(명령줄 인터페이스)를 사용하여 IdM(Identity Management) 서버에 새 DNS 전달 영역을 추가하는 방법을 설명합니다.

DNS 전달 영역을 사용하면 특정 영역에 대한 DNS 쿼리를 다른 DNS 서버로 전달할 수 있습니다. 예를 들어 AD(Active Directory) 도메인에 대한 DNS 쿼리를 AD DNS 서버로 전달할 수 있습니다.

사전 요구 사항

- 관리자 권한이 있는 사용자 계정으로 CLI에 액세스할 수 있습니다.
- DNS 서버가 올바르게 구성되어 있습니다.

절차

-

AD 도메인에 대한 DNS 전달 영역을 생성하고 --forwarder 옵션을 사용하여 원격 DNS 서버의 IP 주소를 지정합니다.

```
# ipa dnsforwardzone-add ad.example.com --forwarder=192.168.122.3 --forward-policy=first
```

참고

구성에 새 전달 영역을 추가한 후 /var/log/ message 시스템 로그에 DNSSEC 검증 실패에 대한 경고가 표시될 수 있습니다.

```
named-pkcs11[2572]: no valid DS resolving 'host.ad.example.com/A/IN':
192.168.100.25#53
```

DNSSEC (Domain Name System Security Extensions)는 공격으로부터 DNS를 보호하기 위해 디지털 서명으로 DNS 데이터를 보호합니다. 이 서비스는 IdM 서버에서 기본적으로 활성화됩니다. 원격 DNS 서버에서 DNSSEC를 사용하지 않기 때문에 경고가 표시됩니다. 원격 DNS 서버에서 DNSSEC를 활성화하는 것이 좋습니다.

원격 서버에서 DNSSEC 검증을 활성화할 수 없는 경우 IdM 서버에서 DNSSEC를 비활성화할 수 있습니다.

1. 편집할 적절한 구성 파일을 선택합니다.
   - IdM 서버에서 RHEL 8.0 또는 RHEL 8.1을 사용하는 경우 /etc/named.conf 파일을 엽니다.
   - IdM 서버가 RHEL 8.2 이상을 사용하는 경우 /etc/named/ipa-options-ext.conf 파일을 엽니다.
2. 다음 DNSSEC 매개변수를 추가합니다.

```
dnssec-enable no;
dnssec-validation no;
```

3. 구성 파일을 저장하고 닫습니다.
4. DNS 서비스를 다시 시작하십시오.

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

검증 단계

- 원격 DNS 서버의 이름과 함께 nslookup 명령을 사용합니다.

```
$ nslookup ad.example.com
Server:        192.168.122.2
Address:       192.168.122.2#53

No-authoritative answer:
Name:          ad.example.com
Address:       192.168.122.3
```

도메인 전달이 올바르게 구성된 경우 nslookup 요청에 원격 DNS 서버의 IP 주소가 표시됩니다.

33.6.4. AD에서 DNS 전달 구성

이 섹션에서는 IdM(Identity Management) 서버에 대한 AD(Active Directory)에서 DNS 전달을 설정하는 방법을 설명합니다.

사전 요구 사항

- AD가 설치된 Windows Server
- 두 서버에서 DNS 포트가 열려 있습니다.

절차

1. Windows Server에 로그인합니다.
2. 서버 관리자 열기 .
3. Open DNS Manager.
4. Conditional Forwarders 에서 다음을 사용하여 새 조건부 전달자를 추가합니다.
   - IdM 서버 IP 주소

- 정규화된 도메인 이름(예: *server.idm.example.com*)

5. 설정을 저장합니다.

33.6.5. DNS 구성 확인

신뢰를 구성하기 전에 IdM(Identity Management) 및 AD(Active Directory) 서버가 서로 해결할 수 있는지 확인합니다.

사전 요구 사항

- sudo 권한으로 로그인해야 합니다.

절차

1. TCP 서비스 레코드를 통해 UDP 및 LDAP를 통해 Kerberos에 대한 DNS 쿼리를 실행합니다.

```
[admin@server ~]# dig +short -t SRV _kerberos._udp.idm.example.com.
0 100 88 server.idm.example.com.

[admin@server ~]# dig +short -t SRV _ldap._tcp.idm.example.com.
0 100 389 server.idm.example.com.
```

명령에서 모든 IdM 서버를 나열해야 합니다.

2. IdM Kerberos 영역 이름을 사용하여 TXT 레코드에 대한 DNS 쿼리를 실행합니다. 가져온 값은 IdM을 설치할 때 지정한 Kerberos 영역과 일치해야 합니다.

```
[admin@server ~]# dig +short -t TXT _kerberos.idm.example.com.
"IDM.EXAMPLE.COM"
```

이전 단계에서 예상 레코드를 모두 반환하지 않은 경우 누락된 레코드로 DNS 구성을 업데이트합니다.

- IdM 환경에서 통합 DNS 서버를 사용하는 경우 시스템 레코드를 업데이트할 옵션 없이 ipa dns-update-system-records 명령을 입력합니다.

```
[admin@server ~]$ ipa dns-update-system-records
```

- IdM 환경에서 통합 DNS 서버를 사용하지 않는 경우:

1. IdM 서버에서 IdM DNS 레코드를 파일로 내보냅니다.

```
[admin@server ~]$ ipa dns-update-system-records --dry-run --out
dns_records_file.nsupdate
```

이 명령은 관련 IdM DNS 레코드를 사용하여 dns_ historys_file.nsupdate 라는 파일을 생성합니다.

2. nsupdate 유틸리티 및 dns_ historys_file.nsupdate 파일을 사용하여 DNS 서버에 DNS 업데이트 요청을 제출합니다. 자세한 내용은 RHEL 7 설명서에서 nsupdate를 사용하여 외부 DNS 레코드 업데이트에서 참조하십시오. 또는 DNS 레코드 추가에는 DNS 서버 설명서를 참조하십시오.

3. TCP 서비스 레코드를 통해 Kerberos 및 LDAP에 대한 DNS 쿼리를 실행하는 명령을 사용하여 AD의 서비스 레코드를 확인할 수 있는지 확인합니다.

```
[admin@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

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

33.7. ACTIVE DIRECTORY DNS 도메인에 IDM 클라이언트 구성

Active Directory에서 제어하는 DNS 도메인에 클라이언트 시스템이 있고 해당 클라이언트가 RHEL 기능을 활용하기 위해 IdM 서버에 가입해야 하는 경우 Active Directory DNS 도메인의 호스트 이름을 사용하여 클라이언트에 액세스하도록 사용자를 구성할 수 있습니다.

중요

이는 권장되지 않으며 몇 가지 제한 사항이 있습니다. Red Hat은 항상 Active Directory가 소유한 것과 다른 DNS 영역에 IdM 클라이언트를 배포하고 IdM 호스트 이름을 통해 IdM 클라이언트에 액세스하는 것이 좋습니다.

IdM 클라이언트 구성은 Kerberos를 통한 SSO(Single Sign-On) 필요 여부에 따라 달라집니다.

33.7.1. Kerberos SSO(Single Sign-On) 없이 IdM 클라이언트 구성

암호 인증은 IdM 클라이언트가 Active Directory DNS 도메인에 있는 경우 사용자가 IdM 클라이언트의 리소스에 액세스할 수 있는 유일한 인증 방법입니다. 다음 절차에서는 Kerberos Single Sign-On 없이 클라이언트를 구성하는 방법을 설명합니다.

절차

1. SSSD(System Security Services Daemon)가 IdM 서버와 통신할 수 있도록 --domain=IPA_DNS_Domain 옵션과 함께 IdM 클라이언트를 설치합니다.

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

이 옵션은 Active Directory DNS 도메인에 대한 SRV 레코드 자동 감지 기능을 비활성화합니다.

2. /etc/krb5.conf 구성 파일을 열고 [domain_realm] 섹션에서 Active Directory 도메인의 기존 매핑을 찾습니다.

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

3. 두 행을 Active Directory DNS 영역에 있는 Linux 클라이언트의 정규화된 도메인 이름(FQDN)을 IdM 영역에 매핑하는 항목으로 바꿉니다.

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

기본 매핑을 대체하면 Kerberos에서 Active Directory 도메인에 대한 요청을 IdM Kerberos 배포 센터(KDC)로 보내는 것을 방지할 수 있습니다. 대신 Kerberos는 SRV DNS 레코드를 통해 자동 검색을 사용하여 NetNamespace를 찾습니다.

33.7.2. SSO(Single Sign-On) 없이 SSL 인증서 요청

SSL 기반 서비스에는 원래(A/AAAA) 및 CNAME 레코드가 모두 인증서에 있어야 하므로 모든 시스템 호스트 이름을 다루는 dNSName 확장자 레코드가 있는 인증서가 필요합니다. 현재 IdM 데이터베이스는 IdM 데이터베이스의 오브젝트를 호스트하는 데만 인증서를 발행합니다.

사용 가능한 SSO(Single Sign-On)가 없는 IdM에는 이미 데이터베이스의 FQDN에 대한 호스트 오브젝트가 있으며 certmonger 는 이 이름을 사용하여 인증서를 요청할 수 있습니다.

사전 요구 사항

- Kerberos SSO(Single Sign-On) 없이 IdM 클라이언트 구성 절차에 따라 IdM 클라이언트를 설치하고 구성합니다.

절차

- FQDN을 사용하여 인증서를 요청하려면 certmonger 를 사용합니다.

```
[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 인증 기관(CA)에 인증합니다.

33.7.3. Kerberos SSO(Single Sign-On)로 IdM 클라이언트 구성

IdM 클라이언트의 리소스에 액세스하려면 Kerberos SSO(Single Sign-on)가 필요한 경우 클라이언트는 IdM DNS 도메인(예: idm-client.idm.example.com) 내에 있어야 합니다. IdM 클라이언트의 A/AAAA 레코드를 가리키는 Active Directory DNS 도메인에 idm-client.ad.example.com 을 생성해야 합니다.

Kerberos 기반 애플리케이션 서버의 경우 MIT Kerberos는 애플리케이션의 키 탭에서 사용 가능한 호스트 기반 보안 주체를 수락할 수 있는 방법을 지원합니다.

절차

- IdM 클라이언트에서 /etc/krb5.conf 구성 파일의 [libdefaults] 섹션에서 다음 옵션을 설정하여 Kerberos 서버를 대상으로 하는 데 사용되는 Kerberos 주체의 엄격한 검사를 비활성화합니다.

```
ignore_acceptor_hostname = true
```

33.7.4. SSO(Single Sign-On)를 사용하여 SSL 인증서 요청

SSL 기반 서비스에는 원래(A/AAAA) 및 CNAME 레코드가 모두 인증서에 있어야 하므로 모든 시스템 호스트 이름을 다루는 dNSName 확장자 레코드가 있는 인증서가 필요합니다. 현재 IdM 데이터베이스는 IdM 데이터베이스의 오브젝트를 호스트하는 데만 인증서를 발행합니다.

이 절차에서는 IdM에서 ipa-client.example.com 의 호스트 오브젝트를 생성하고 실제 IdM 시스템의 호스트 오브젝트가 이 호스트를 관리하는 방법을 설명합니다.

사전 요구 사항

- Kerberos Single Sign-On으로 IdM 클라이언트 구성에 설명된 대로 Kerberos 서버를 대상으로 하는 데 사용되는 Kerberos 주체에 대한 엄격한 검사를 비활성화했습니다.

절차

1. IdM 서버에 새 호스트 오브젝트를 생성합니다.

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

호스트 이름이 CNAME 레코드가 아닌 A/AAAA 레코드이므로 --force 옵션을 사용합니다.

2. IdM 서버에서 IdM DNS 호스트 이름을 허용하여 IdM 데이터베이스의 Active 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
```

3. Active Directory DNS 도메인 내의 호스트 이름에 대한 dNSName 확장 레코드와 함께 IdM 클라이언트의 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
```

33.8. 신뢰 설정

이 섹션에서는 명령줄을 사용하여 IdM 측에 대해 IdM(Identity Management)/AD(Identity Management)/Active Directory를 구성하는 방법을 설명합니다.

사전 요구 사항

- DNS가 올바르게 구성되어 있습니다. IdM 및 AD 서버 모두 서로 다른 이름을 확인할 수 있어야 합니다. 자세한 내용은 신뢰에 대한 DNS 및 영역 설정 구성을 참조하십시오.
- 지원되는 AD 및 IdM 버전이 배포됩니다. 자세한 내용은 지원되는 Windows Server 버전을 참조하십시오.
- Kerberos 티켓을 받을 수 있습니다. 자세한 내용은 kinit를 사용하여 IdM에 수동으로 로그인하는 방법을 참조하십시오.

33.8.1. 신뢰를 위한 IdM 서버 준비

AD를 사용한 신뢰를 구축하기 전에 IdM 서버에서 ipa-adtrust-install 유틸리티를 사용하여 IdM 도메인을 준비해야 합니다.

참고

ipa-adtrust-install 명령을 실행하는 시스템은 자동으로 AD 신뢰 컨트롤러가 됩니다. 그러나 IdM 서버에서 ipa-adtrust-install 을 한 번만 실행해야 합니다.

사전 요구 사항

- IdM 서버가 설치되어 있어야 합니다.
- 패키지를 설치하고 IdM 서비스를 다시 시작하려면 루트 권한이 필요합니다.

절차

1. 필수 패키지를 설치합니다.

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

2. IdM 관리자로 인증합니다.

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

3. ipa-adtrust-install 유틸리티를 실행합니다.

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

IdM이 통합된 DNS 서버와 함께 설치된 경우 DNS 서비스 레코드가 자동으로 생성됩니다.

통합된 DNS 서버 없이 IdM을 설치한 경우, ipa-adtrust-install 은 DNS에 수동으로 추가해야 하는 서비스 레코드 목록을 인쇄합니다.

4. 스크립트에서 /etc/samba/smb.conf가 이미 존재하고 다시 작성됨을 묻는 메시지를 표시합니다.

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your
existing Samba configuration.

Do you wish to continue? [no]: yes
```

5. 스크립트에서 이전 Linux 클라이언트가 신뢰할 수 있는 사용자로 작업할 수 있는 호환성 플러그인인 slapi-nis 플러그인을 구성하도록 프롬프트를 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]: yes
```

6. 메시지가 표시되면 IdM 도메인의 NetBIOS 이름을 입력하거나 Enter 를 눌러 제안된 이름을 수락합니다.

```
Trust is configured but no NetBIOS domain name found, setting it now.
Enter the NetBIOS name for the IPA domain.
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
```

```
Example: EXAMPLE.

NetBIOS domain name [IDM]:
```

7. SID 생성 작업을 실행하여 기존 사용자의 SID를 생성하라는 메시지가 표시됩니다.

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

이는 리소스 집약적인 작업이므로 사용자가 많은 경우 한 번에 이 작업을 실행할 수 있습니다.

8. (선택 사항) 기본적으로 Dynamic RPC 포트 범위는 Windows Server 2008 이상에서는 49152-65535 로 정의됩니다. 환경에 대해 다른 Dynamic RPC 포트 범위를 정의해야 하는 경우 다른 포트를 사용하도록 Samba를 구성하고 방화벽 설정에서 해당 포트를 엽니다. 다음 예제에서는 포트 범위를 55000-65000으로 설정합니다.

```
[root@ipaserver ~]# net conf setparm global 'rpc server dynamic port range' 55000-65000
[root@ipaserver ~]# firewall-cmd --add-port=55000-65000/tcp
[root@ipaserver ~]# firewall-cmd --runtime-to-permanent
```

9. 트러스트의 DNS 구성 확인에 설명된 대로 DNS가 올바르게 구성되었는지 확인합니다.

중요

ipa-ad trust-install 을 실행한 후 언제든지 DNS 구성 확인에 설명된 대로 DNS 구성을 확인할 것을 강력히 권장합니다. 특히 IdM 또는 AD에서 통합 DNS 서버를 사용하지 않는 경우.

10. ipa 서비스를 다시 시작하십시오.

```
[root@ipaserver ~]# ipactl restart
```

11. smbclient 유틸리티를 사용하여 Samba가 IdM 측에서 Kerberos 인증에 응답하는지 확인합니다.

```
[root@ipaserver ~]# smbclient -L server.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
    Sharename       Type      Comment
```

```
---------      ----     -------
IPC$           IPC      IPC Service (Samba 4.15.2)
...
```

33.8.2. 명령줄을 사용하여 신뢰 계약 설정

이 섹션에서는 명령줄을 사용하여 신뢰 계약을 설정하는 방법을 설명합니다. IdM(Identity Management) 서버를 사용하면 세 가지 유형의 신뢰 계약을 구성할 수 있습니다.

- 단방향 신뢰 data bind-default 옵션. 단방향 트러스트를 사용하면 AD(Active Directory) 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있지만 다른 방법은 액세스할 수 없습니다. IdM 도메인은 AD forest을 신뢰하지만 AD forest에서 IdM 도메인을 신뢰하지 않습니다.

- AD 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있도록 2방향 신뢰 tektonTwo-way 트러스트를 사용할 수 있습니다.

  신뢰 경계를 통해 작동하도록 S4U2Self 및 S4U2Proxy Microsoft 확장이 예상되는 Microsoft SQL Server와 같은 솔루션에 대해 양방향 신뢰를 구성해야 합니다. RHEL IdM 호스트의 애플리케이션은 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 로그인하는 것을 허용하지 않으며, IdM의 양방향 신뢰 솔루션은 사용자에게 AD의 단방향 신뢰 솔루션에 비해 추가 권한을 부여하지 않습니다.

  - 양방향 신뢰를 만들려면 명령에 다음 옵션을 추가하십시오. --two-way=true

- 외부 신뢰 - IdM과 다른 extra의 AD 도메인 간의 신뢰 관계입니다. tree 신뢰는 항상 Active Directory domain의 IdM과 루트 도메인 간의 신뢰를 설정하는 반면, 외부 신뢰는 IdM에서 domain 내 도메인으로 설정할 수 있습니다. 관리 또는 조직의 이유로 dejoration 루트 도메인 간에 Failed 트러스트를 설정할 수 없는 경우에만 이 방법을 사용하는 것이 좋습니다.

  - 외부 신뢰를 생성하려면 명령에 다음 옵션을 추가합니다. --external=true

이 섹션에서는 단방향 신뢰 계약을 만드는 방법을 보여줍니다.

사전 요구 사항

- Windows 관리자의 사용자 이름 및 암호입니다.
- IdM 서버가 신뢰에 사용할 준비가 되어 있습니다.

절차

- ipa trust-add 명령을 사용하여 AD 도메인 및 IdM 도메인에 대한 신뢰 계약을 생성합니다.
  - SSSD를 사용하여 STS를 기반으로 AD 사용자의 UID 및 GID를 자동으로 생성할 수 있도록 하려면 Active Directory 도메인 ID 범위 유형과의 신뢰 계약을 생성합니다. 가장 일반적인 구성입니다.

```
[root@server ~]# ipa trust-add --type=ad ad.example.com --admin
<ad_admin_username> --password --range-type=ipa-ad-trust
```

  - Active Directory에서 사용자에 대한 POSIX 특성(예: uidNumber 및 gidNumber)을 구성하고 SSSD가 이 정보를 처리하려는 경우 POSIX 속성 ID 범위 유형으로 Active Directory 도메인과 의 신뢰 계약을 생성합니다.

```
[root@server ~]# ipa trust-add --type=ad ad.example.com --admin
<ad_admin_username> --password --range-type=ipa-ad-trust-posix
```

주의

신뢰를 생성할 때 ID 범위 유형을 지정하지 않으면 IdM은 tree 루트 도메인의 AD 도메인 컨트롤러에서 세부 정보를 요청하여 적절한 범위 유형을 자동으로 선택합니다. IdM에서 POSIX 속성을 감지하지 않으면 신뢰 설치 스크립트에서 Active Directory 도메인 ID 범위를 선택합니다.

IdM이 forest 루트 도메인의 POSIX 속성을 감지하면 신뢰 설치 스크립트에서 POSIX 속성 ID 범위를 사용하여 Active Directory 도메인 을 선택하고 UID 및 GID가 AD에 올바르게 정의되었다고 가정합니다. POSIX 속성이 AD에서 올바르게 설정되지 않은 경우 AD 사용자를 확인할 수 없습니다.

예를 들어, IdM 시스템에 액세스해야 하는 사용자와 그룹이 Lake 루트 도메인의 일부가 아닌 경우 설치 스크립트가 하위 AD 도메인에 정의된 POSIX 특성을 탐지하지 못할 수 있습니다. 이 경우 신뢰를 설정할 때 POSIX ID 범위 유형을 명시적으로 선택하는 것이 좋습니다.

33.8.3. IdM 웹 UI에서 신뢰 계약 설정

이 섹션에서는 IdM 웹 UI를 사용하여 IdM 측에 IdM(Identity Management)/AD(Active Directory) 신뢰 계약을 구성하는 방법을 설명합니다.

사전 요구 사항

- DNS가 올바르게 구성되어 있습니다. IdM 및 AD 서버 모두 서로 다른 이름을 확인할 수 있어야 합니다.
- 지원되는 AD 및 IdM 버전이 배포됩니다.
- Kerberos 티켓을 받을 수 있습니다.
- 웹 UI에 신뢰를 생성하기 전에 다음과 같이 트러스트를 위해 IdM 서버를 준비합니다. 신뢰를 위해 IdM 서버 준비.

- **IdM 관리자로 로그인해야 합니다.**

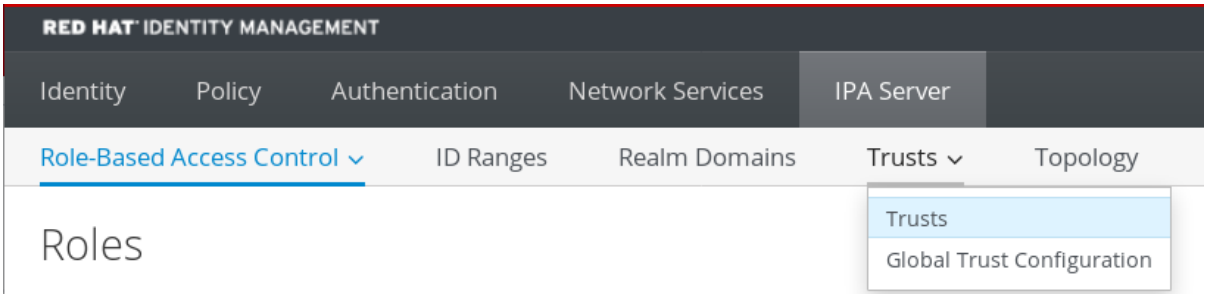
절차

1. **관리자 권한으로 IdM 웹 UI에 로그인합니다. 자세한 내용은 웹 브라우저에서 IdM 웹 UI 액세스를 참조하십시오.**

2. **IdM 웹 UI에서 IPA 서버 탭을 클릭합니다.**

3. **IPA 서버 탭에서 신뢰 탭을 클릭합니다.**

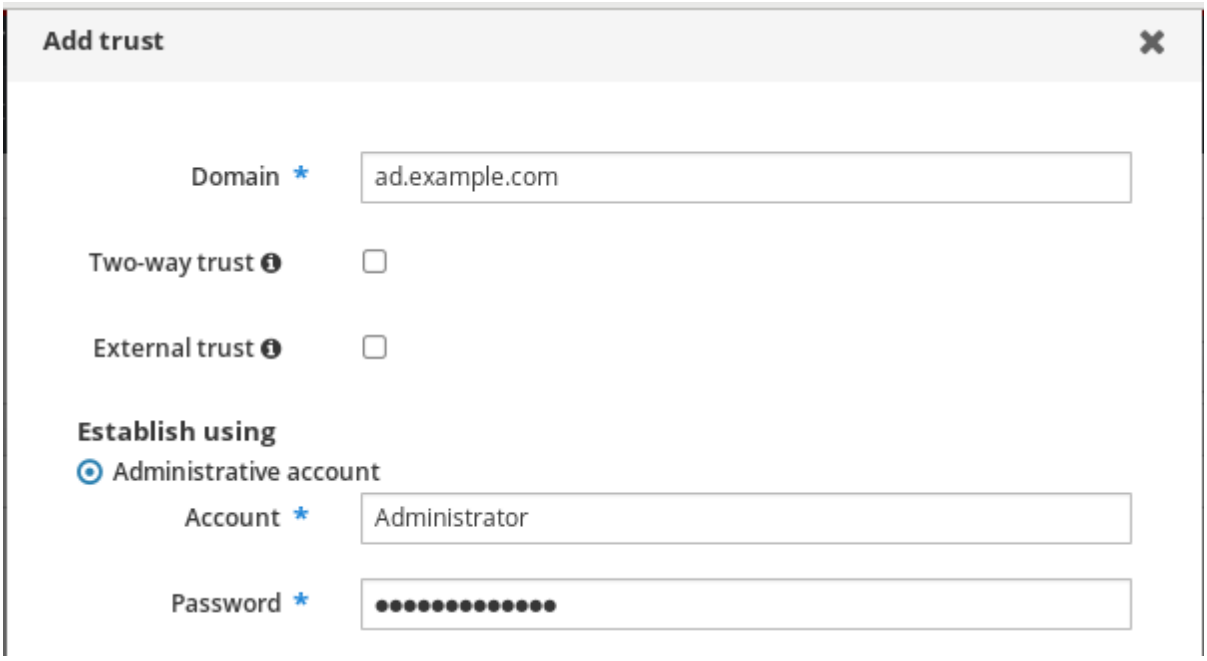
4. **드롭다운 메뉴에서 신뢰 옵션을 선택합니다.**



5. **Add (추가) 버튼을 클릭합니다.**

6. **신뢰 추가 대화 상자에서 Active Directory 도메인의 이름을 입력합니다.**

7. **계정 및 암호 필드에서 Active Directory 관리자의 관리자 자격 증명을 추가합니다.**



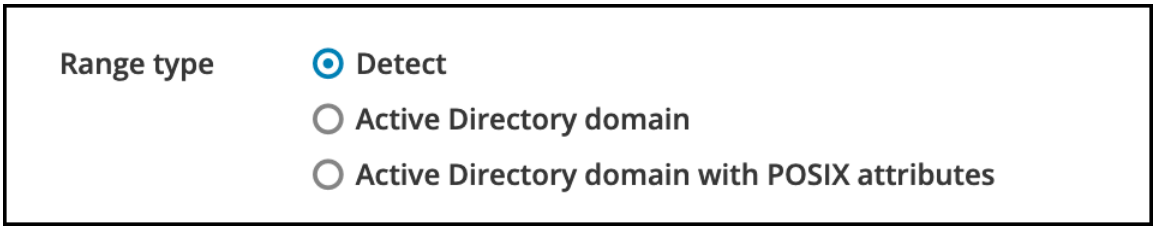
8. *(선택 사항)* **AD** 사용자와 그룹이 **IdM**의 리소스에 액세스할 수 있도록 하려면 양방향 트러스트 를 선택합니다. 그러나 **IdM**의 양방향 신뢰는 사용자에게 **AD**의 단방향 신뢰 솔루션과 비교하여 추가 권한을 제공하지 않습니다. 두 솔루션 모두 기본 **cross-forest trust traces** 필터링 설정으로 인해 동일하게 안전한 것으로 간주됩니다.

9. *(선택 사항)* **Active Directory**의 루트 도메인이 아닌 **AD** 도메인을 사용하여 트러스트를 구성하는 경우 외부 신뢰를 선택합니다. **tree** 신뢰는 항상 **Active Directory forest**의 **IdM**과 루트 도메인 간의 신뢰를 설정해야 하지만, **IdM**에서 **AD domain** 내의 모든 도메인으로 외부 신뢰를 구축할 수 있습니다.

10. *(선택 사항)* 기본적으로 신뢰 설치 스크립트는 적절한 **ID** 범위 유형을 탐지합니다. 다음 옵션 중 하나를 선택하여 **ID** 범위 유형을 명시적으로 설정할 수도 있습니다.

    a. **SSSD**를 사용하여 **STS**를 기반으로 **AD** 사용자의 **UID** 및 **GID**를 자동으로 생성할 수 있도록 하려면 **Active Directory** 도메인 **ID** 범위 유형을 선택합니다. 가장 일반적인 구성입니다.

    b. **Active Directory**에서 사용자에 대한 **POSIX** 속성(예: **uidNumber** 및 **gidNumber**)을 구성하고 **SSSD**가 이 정보를 처리하려는 경우 **POSIX** 속성 **ID** 범위 유형으로 **Active Directory** 도메인 을 선택합니다.



주의

기본 검색 옵션에서 **Range** 유형 설정을 그대로 두면 IdM은 tree 루트 도메인의 AD 도메인 컨트롤러에서 세부 정보를 요청하여 적절한 범위 유형을 자동으로 선택합니다. IdM에서 POSIX 속성을 감지하지 않으면 신뢰 설치 스크립트에서 Active Directory 도메인 ID 범위를 선택합니다.

IdM이 forest 루트 도메인의 POSIX 속성을 감지하면 신뢰 설치 스크립트에서 POSIX 속성 ID 범위를 사용하여 Active Directory 도메인을 선택하고 UID 및 GID가 AD에 올바르게 정의되었다고 가정합니다. POSIX 속성이 AD에서 올바르게 설정되지 않은 경우 AD 사용자를 확인할 수 없습니다.

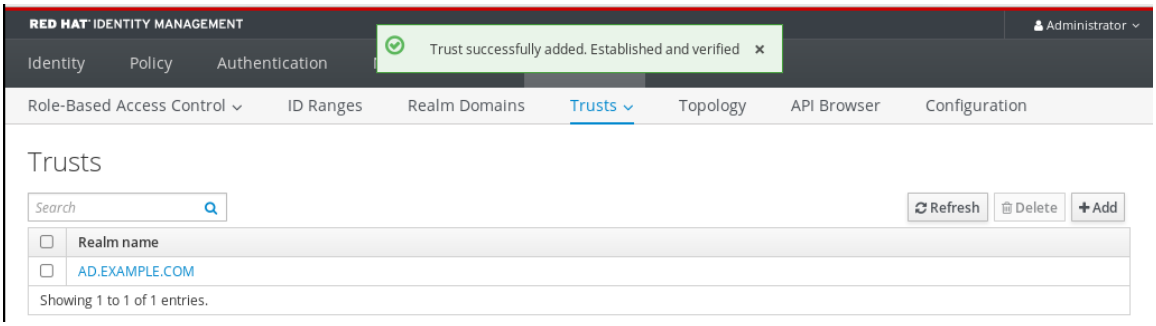
예를 들어, IdM 시스템에 액세스해야 하는 사용자와 그룹이 Lake 루트 도메인의 일부가 아닌 경우 설치 스크립트가 하위 AD 도메인에 정의된 POSIX 특성을 탐지하지 못할 수 있습니다. 이 경우 신뢰를 설정할 때 POSIX ID 범위 유형을 명시적으로 선택하는 것이 좋습니다.

11. 추가를 클릭합니다.

검증 단계

- IdM 서버에 신뢰가 성공적으로 추가되면 IdM 웹 UI에 녹색 팝업 창을 볼 수 있습니다. 이는 다음을 의미합니다.
  - 도메인 이름

- Windows Server의 사용자 이름 및 암호가 올바르게 추가되었습니다.



이제 신뢰 연결 및 Kerberos 인증을 계속 테스트할 수 있습니다.

33.8.4. Ansible을 사용하여 신뢰 계약 설정

이 섹션에서는 Ansible 플레이북을 사용하여 IdM(Identity Management)과 AD(Active Directory) 간에 단방향 신뢰 계약을 설정하는 방법을 설명합니다. 다음과 같은 세 가지 유형의 트러스트 계약을 구성할 수 있습니다.

- 단방향 신뢰 data bind-default 옵션. 단방향 트러스트를 사용하면 AD(Active Directory) 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있지만 다른 방법은 액세스할 수 없습니다. IdM 도메인은 AD forest을 신뢰하지만 AD forest에서 IdM 도메인을 신뢰하지 않습니다.

- AD 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있도록 2방향 신뢰 tektonTwo-way 트러스트를 사용할 수 있습니다.

  신뢰 경계를 통해 작동하도록 S4U2Self 및 S4U2Proxy Microsoft 확장이 예상되는 Microsoft SQL Server와 같은 솔루션에 대해 양방향 신뢰를 구성해야 합니다. RHEL IdM 호스트의 애플리케이션은 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 로그인하는 것을 허용하지 않으며, IdM의 양방향 신뢰 솔루션은 사용자에게 AD의 단방향 신뢰 솔루션에 비해 추가 권한을 부여하지 않습니다.

  - 양방향 신뢰를 생성하려면 아래 플레이북 작업에 다음 변수를 추가합니다. two_way: true

- 외부 신뢰 - IdM과 다른 extra의 AD 도메인 간의 신뢰 관계입니다. tree 신뢰는 항상 Active Directory domain의 IdM과 루트 도메인 간의 신뢰를 설정하는 반면, 외부 신뢰는 IdM에서 domain 내 도메인으로 설정할 수 있습니다. 관리 또는 조직의 이유로 dejoration 루트 도메인 간에 Failed 트러스트를 설정할 수 없는 경우에만 이 방법을 사용하는 것이 좋습니다.

  - 외부 신뢰를 생성하려면 아래 플레이북 작업에 다음 변수를 추가합니다. external: true

사전 요구 사항

- Windows 관리자의 사용자 이름 및 암호입니다.
- IdM 관리자 암호입니다.
- IdM 서버가 신뢰에 사용할 준비가 되어 있습니다.
- 4.8.7 버전의 IdM을 사용하고 있습니다. 서버에 설치한 IdM 버전을 보려면 ipa --version 를 실행합니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.8 이상을 사용하고 있습니다.
  - ansible-freeipa 패키지가 설치되어 있습니다.
  - ~/*MyPlaybooks*/ 디렉터리에 신뢰를 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 Ansible 인벤토리 파일을 생성했습니다.

절차

1. ~/*MyPlaybooks*/ 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. 사용 사례에 따라 다음 시나리오 중 하나를 선택합니다.

- ID 매핑 신뢰 계약을 생성하려면 SSSD에서 libc를 기반으로 AD 사용자 및 그룹의 UID 및 GID를 자동으로 생성하는 경우 다음 콘텐츠를 사용하여 add-trust.yml 플레이북을 생성합니다.

```
---
- name: Playbook to create a trust
  hosts: ipaserver
  become: true

  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: SomeADMINpassword
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        range_type: ipa-ad-trust
        state: present
```

  예에서는 다음을 수행합니다.

  - realm 은 AD 영역 이름 문자열을 정의합니다.
  - admin 은 AD 도메인 관리자 문자열을 정의합니다.
  - password 는 AD 도메인 관리자의 암호 문자열을 정의합니다.

- POSIX 신뢰 계약을 만들려면 SSSD에서 AD에 저장된 POSIX 속성(예: uidNumber 및 gidNumber)을 처리하는 경우 다음 콘텐츠를 사용하여 add-trust.yml 플레이북을 만듭니다.

```
---
- name: Playbook to create a trust
  hosts: ipaserver
  become: true

  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: SomeADMINpassword
        realm: ad.example.com
```

```
    admin: Administrator
    password: secret_password
    range_type: ipa-ad-trust-posix
    state: present
```

- VirtIO 루트 도메인의 AD 도메인 컨트롤러에서 다음 콘텐츠를 사용하여 세부 정보를 요청하여 IdM에서 적절한 범위 유형, ipa-ad-trust 또는 ipa-ad-trust-posix 를 자동으로 선택하려는 신뢰 계약을 생성하려면 다음 콘텐츠를 사용하여 add-trust.yml 플레이북을 생성합니다.

```
---
- name: Playbook to create a trust
  hosts: ipaserver
  become: true

  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: SomeADMINpassword
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        state: present
```

주의

신뢰를 생성할 때 ID 범위 유형을 지정하지 않고 IdM에서 AD forest 루트 도메인의 POSIX 속성을 검색하지 않으면 신뢰 설치 스크립트에서 Active Directory 도메인 ID 범위를 선택합니다.

IdM이 forest 루트 도메인의 POSIX 속성을 감지하면 신뢰 설치 스크립트에서 POSIX 속성 ID 범위를 사용하여 Active Directory 도메인 을 선택하고 UID 및 GID가 AD에 올바르게 정의되었다고 가정합니다.

그러나 POSIX 속성이 AD에서 올바르게 설정되지 않으면 AD 사용자를 확인할 수 없습니다. 예를 들어, IdM 시스템에 액세스해야 하는 사용자와 그룹이 Lake 루트 도메인의 일부가 아닌 경우 설치 스크립트가 하위 AD 도메인에 정의된 POSIX 특성을 탐지하지 못할 수 있습니다. 이 경우 신뢰를 설정할 때 POSIX ID 범위 유형을 명시적으로 선택하는 것이 좋습니다.

3. 파일을 저장합니다.

4. 플레이북 파일 및 인벤토리 파일을 지정하여 **Ansible** 플레이북을 실행합니다.

```
$ ansible-playbook -v -i inventory add-trust.yml
```

추가 리소스

- /usr/share/doc/ansible-freeipa/README-trust.md
- /usr/share/doc/ansible-freeipa/playbooks/trust

33.8.5. Kerberos 구성 확인

Kerberos 구성을 확인하려면 **IdM(Identity Management)** 사용자의 티켓을 받을 수 있고 **IdM** 사용자가 서비스 티켓을 요청할 수 있는지 테스트합니다.

절차

1. **AD(Active Directory)** 사용자를 위한 티켓을 요청하십시오.

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

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

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

AD 서비스 티켓이 성공적으로 부여되면 요청된 다른 모든 티켓과 함께 **cross-realm** 티켓-granting 티켓 **(TGT)**이 기재되어 있습니다. **TGT**의 이름은 **jenkinsfiletgt/IPA.DOMAIN@AD.DOMAIN**입니다.

```
[root@server ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/server.idm.example.com@IDM.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
```

```
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IDM.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
```

localauth 플러그인은 **Kerberos** 주체를 로컬 **SSSD(System Security Services Daemon)** 사용자 이름에 매핑합니다. 이를 통해 **AD** 사용자는 **Kerberos** 인증을 사용하고 **GSSAPI** 인증을 직접 지원하는 **Linux** 서비스에 액세스할 수 있습니다.

33.8.6. IdM의 신뢰 구성 확인

신뢰를 구성하기 전에 **IdM(Identity Management)** 및 **AD(Active Directory)** 서버가 서로 해결할 수 있는지 확인합니다.

사전 요구 사항

- 관리자 권한으로 로그인해야 합니다.

절차

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

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

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

이 명령을 실행하면 **ipa-adtrust-install** 이 실행된 모든 **IdM** 서버가 나열됩니다. 첫 번째 신뢰 관계를 설정하기 전에 일반적으로 **IdM** 서버에서 **ipa-adtrust-install** 을 실행하지 않은 경우 출력이 비어 있습니다.

2. **TCP** 서비스 레코드를 통해 **Kerberos** 및 **LDAP**에 대한 **DNS** 쿼리를 실행하여 **IdM**에서 **AD**의 서비스 레코드를 확인할 수 있는지 확인합니다.

```
[root@server ~]# dig +short -t SRV _kerberos._tcp.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.
```

.

33.8.7. AD에서 신뢰 구성 확인

신뢰를 구성한 후 다음을 확인합니다.

- IdM(Identity Management) 호스트 서비스는 AD(Active Directory) 서버에서 확인할 수 있습니다.
- AD 서비스는 AD 서버에서 확인할 수 있습니다.

사전 요구 사항

- 관리자 권한으로 로그인해야 합니다.

절차

1. AD 서버에서 nslookup.exe 유틸리티를 설정하여 서비스 레코드를 조회합니다.

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

2. TCP 서비스 레코드를 통해 UDP 및 LDAP를 통해 Kerberos의 도메인 이름을 입력합니다.

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

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

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

   "IDM.EXAMPLE.COM"
```

4. TCP 서비스 레코드를 통해 UDP 및 LDAP를 통해 MS DC Kerberos에 대한 DNS 쿼리를 실행합니다.

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

Active Directory는 다른 AD 도메인 컨트롤러 및 IdM 신뢰 컨트롤러와 같은 AD 특정 프로토콜 요청에 응답할 수 있는 도메인 컨트롤러만 검색합니다. ipa-adtrust-install 툴을 사용하여 IdM 서버를 신뢰 컨트롤러로 승격하고 ipa server-role-find --role 'AD trust controller' 명령을 사용하여 어떤 서버가 신뢰 컨트롤러인지 확인할 수 있습니다.

5. AD 서버에서 AD 서비스를 확인할 수 있는지 확인합니다.

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

6. TCP 서비스 레코드를 통해 UDP 및 LDAP를 통해 Kerberos의 도메인 이름을 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
```

33.8.8. 신뢰 에이전트 생성

신뢰 에이전트는 AD 도메인 컨트롤러에 대해 ID 조회를 수행할 수 있는 IdM 서버입니다.

예를 들어 Active Directory와의 신뢰가 있는 IdM 서버의 복제본을 생성하는 경우 복제본을 신뢰 에이전트로 설정할 수 있습니다. 복제본에는 AD 신뢰 에이전트 역할이 자동으로 설치되지 않습니다.

사전 요구 사항

- IdM은 Active Directory 트러스트와 함께 설치됩니다.
- sssd-tools 패키지가 설치되어 있습니다.

절차

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

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

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

2. 신뢰 에이전트에서 IdM 서비스를 다시 시작합니다.

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

3. 신뢰 에이전트의 SSSD 캐시에서 모든 항목을 제거합니다.

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

4. 복제본에 AD 신뢰 에이전트 역할이 설치되어 있는지 확인합니다.

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

추가 리소스

- --add-agents 옵션에 대한 자세한 내용은 ipa-adtrust-install(1) 매뉴얼 페이지를 참조하십시오.
- 신뢰 에이전트에 대한 자세한 내용은 계획 ID 관리 가이드의 신뢰 컨트롤러 및 신뢰 에이전트 를 참조하십시오.

33.8.9. CLI에서 POSIX ID 범위에 대한 자동 개인 그룹 매핑 활성화

기본적으로 SSSD는 AD에 저장된 POSIX 데이터에 의존하는 POSIX 신뢰를 설정한 경우 AD(Active Directory) 사용자를 위해 개인 그룹을 매핑하지 않습니다. AD 사용자에게 기본 그룹이 구성되어 있지 않은 경우 IdM을 확인할 수 없습니다.

다음 절차에서는 명령줄에서 auto_private_groups SSSD 매개변수에 대한 하이브리드 옵션을 설정하여 ID 범위에 대한 자동 개인 그룹 매핑을 활성화하는 방법을 설명합니다. 결과적으로 IdM은 AD에 기본 그룹이 구성되지 않은 AD 사용자를 확인할 수 있습니다.

사전 요구 사항

- IdM과 AD 환경 간에 POSIX 교차 검색을 성공적으로 설정했습니다.

절차

1. 모든 ID 범위를 표시하고 수정하려는 AD ID 범위를 기록합니다.

```
[root@server ~]# ipa idrange-find
----------------
2 ranges matched
----------------
  Range name: IDM.EXAMPLE.COM_id_range
  First Posix ID of the range: 882200000
  Number of IDs in the range: 200000
  Range type: local domain range

  Range name: AD.EXAMPLE.COM_id_range
  First Posix ID of the range: 1337000000
  Number of IDs in the range: 200000
```

```
  Domain SID of the trusted domain: S-1-5-21-4123312420-990666102-3578675309
  Range type: Active Directory trust range with POSIX attributes
---------------------------
Number of entries returned 2
---------------------------
```

2. ipa idrange-mod 명령을 사용하여 AD ID 범위의 자동 개인 그룹 동작을 조정합니다.

```
[root@server ~]# ipa idrange-mod --auto-private-groups=hybrid
AD.EXAMPLE.COM_id_range
```

3. 새 설정을 사용하도록 SSSD 캐시를 재설정합니다.

```
[root@server ~]# sss_cache -E
```

추가 리소스

- AD 사용자를 위해 개인 그룹을 자동으로 매핑하는 옵션

33.8.10. IdM WebUI에서 POSIX ID 범위에 대한 자동 개인 그룹 매핑 활성화

기본적으로 SSSD는 AD에 저장된 POSIX 데이터에 의존하는 POSIX 신뢰를 설정한 경우 AD(Active Directory) 사용자를 위해 개인 그룹을 매핑하지 않습니다. AD 사용자에게 기본 그룹이 구성되어 있지 않은 경우 IdM을 확인할 수 없습니다.

이 절차에서는 IdM(Identity Management) WebUI에서 auto_private_groups SSSD 매개변수에 대한 하이브리드 옵션을 설정하여 ID 범위에 대한 자동 개인 그룹 매핑을 활성화하는 방법을 설명합니다. 결과적으로 IdM은 AD에 기본 그룹이 구성되지 않은 AD 사용자를 확인할 수 있습니다.

사전 요구 사항

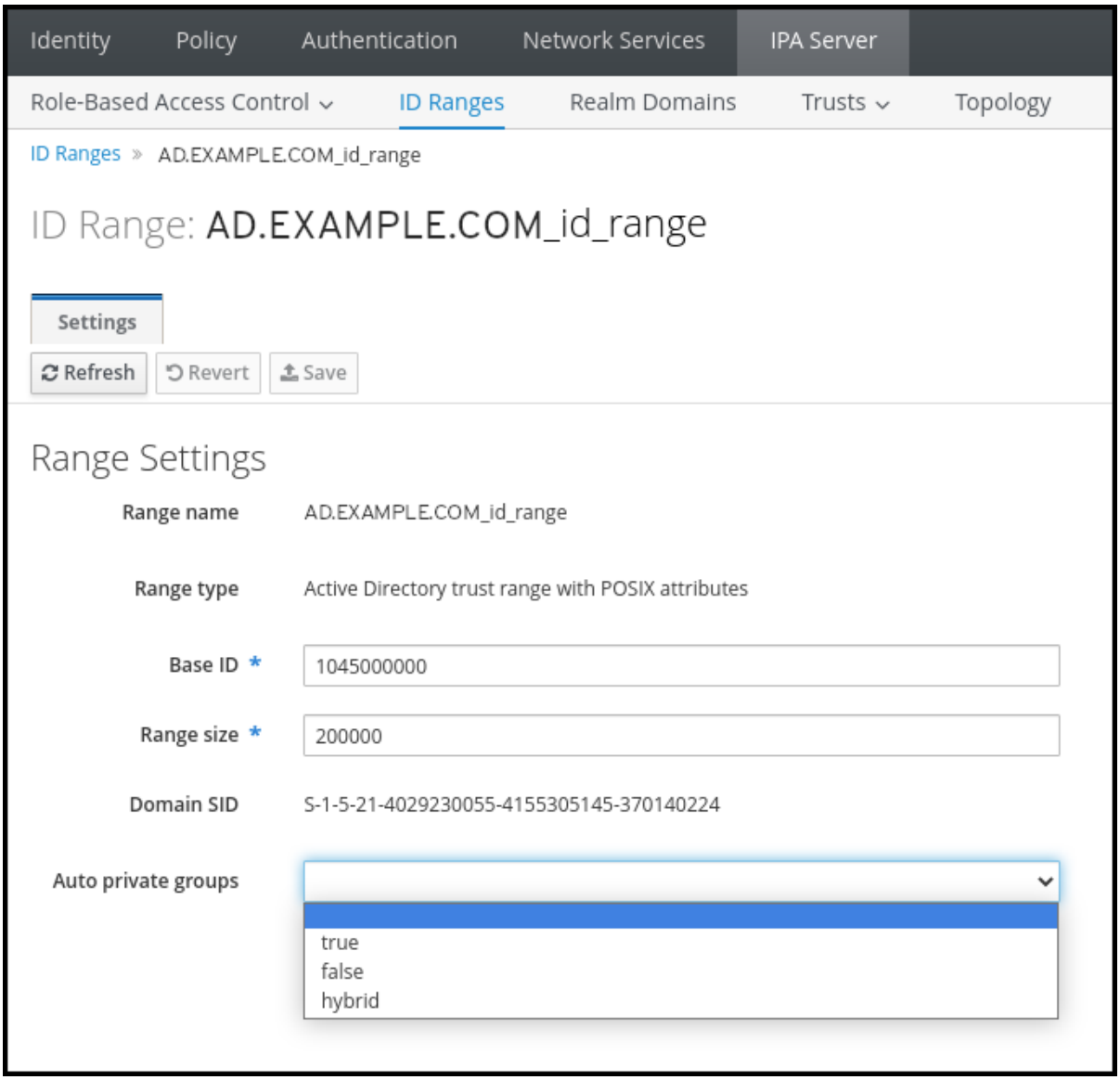
- IdM과 AD 환경 간에 POSIX 교차 검색을 성공적으로 설정했습니다.

절차

1. 사용자 이름 및 암호를 사용하여 IdM 웹 UI에 로그인합니다.
2. IPA 서버 → ID 범위 탭을 엽니다.

3. **AD.EXAMPLE.COM_id_range** 와 같이 수정할 **ID** 범위를 선택합니다.

4. 자동 개인 그룹 드롭다운 메뉴에서 하이브리드 옵션을 선택합니다.



5. 저장 버튼을 클릭하여 변경 사항을 저장합니다.

추가 리소스

- AD 사용자를 위해 개인 그룹을 자동으로 매핑하는 옵션

33.9. 가장 광범위한 트러스트 설정 문제 해결

이 장에서는 IdM(Identity Management) 환경과 AD(Active Directory) 도메인 간 트러스트를 구성하는 프로세스 문제 해결에 대해 설명합니다.

33.9.1. AD를 사용하여 가장 간 트러스트를 설정할 때 이벤트 시퀀스

ipa trust-add 명령을 사용하여 AD(Active Directory) 도메인 컨트롤러(DC) 도메인 컨트롤러(DC)와의 교차 트러스트를 설정하는 경우 명령은 명령을 실행한 사용자를 대신하여 작동하며 IdM 서버에서 다음 작업을 수행합니다. If you have trouble establishing a cross-forest trust, you can use this list to help narrow down and troubleshoot your issue.

제품 1: 명령은 설정 및 입력 확인

1. IdM 서버에 Trust Controller 역할이 있는지 확인합니다.

2. ipa trust-add 명령에 전달된 옵션을 확인합니다.

3. 신뢰할 수 있는 tree 루트 도메인과 연결된 ID 범위를 확인합니다. ID 범위 유형 및 속성을 ipa trust-add 명령에 대한 옵션으로 지정하지 않은 경우 Active Directory에서 검색됩니다.

제품 2 이 명령은 Active Directory 도메인에 대한 트러스트를 설정하려고 시도합니다.

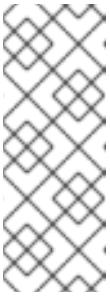
4. 각 신뢰 방향에 대해 별도의 신뢰 오브젝트를 생성합니다. 각 오브젝트는 양변(IdM 및 AD) 모두에서 생성됩니다. 단방향 신뢰를 설정하는 경우 각 측에서 하나의 개체만 생성됩니다.

5. IdM 서버는 Samba 제품군을 사용하여 Active Directory의 도메인 컨트롤러 기능을 처리하고 대상 AD PDC에 신뢰 오브젝트를 생성합니다.

    a. IdM 서버는 대상 DC의 IPC$ 공유에 대한 보안 연결을 설정합니다. RHEL 8.4 이후 연결은 세션에 사용되는 AES 기반 암호화를 사용하여 연결이 충분히 안전한지 확인하기 위해 Windows Server 2012 이상을 사용하는 SMB3 프로토콜 이상이 필요합니다.

    b. IdM 서버는 LSA QueryTrustedDomainInfoByName 호출을 사용하여 신뢰할 수 있는 도메인 오브젝트(TDO)를 쿼리합니다.

    c. TDO가 이미 존재하는 경우 LSA DeleteTrustedDomain 호출을 사용하여 제거합니다.



참고

이 호출은 **Incoming Forest Trust Builder** 그룹의 구성원과 같이 **domain Admin (EA)** 또는 **Domain Admin (DA)** 권한이 없는 경우 이 호출이 실패합니다. 이전 **TDO**가 자동으로 제거되지 않으면 **AD** 관리자가 **AD**에서 수동으로 제거해야 합니다.

d. **IdM** 서버는 **LSA CreateTrustedDomainEx2** 호출을 사용하여 새 **TDO**를 생성합니다. **TDO** 자격 증명은 **128**개의 임의의 문자가 있는 **Samba** 제공 암호 생성기를 사용하여 임의로 생성됩니다.

e. 그런 다음 새로운 **TDO**가 **LSA Set informationTrustedDomain** 호출을 사용하여 수정되어 신뢰에서 지원하는 암호화 유형이 올바르게 설정되어 있는지 확인합니다.

i. **Active Directory**의 디자인 방식 때문에 **RC4_HMAC_MD5** 암호화 유형이 활성화된 경우 **RC4** 키가 사용되지 않습니다.

ii. **AES128_CTS_HMAC_SHA1_96** 및 **AES256_CTS_HMAC_SHA1_96** 암호화 유형이 활성화됩니다.

6. **Lake** 트러스트의 경우 **LSA SetDataTrustedDomain** 호출을 사용하여 내 도메인의 전송에 도달할 수 있는지 확인합니다.

7. **LSA RSetForestTrust Information** 호출을 사용하여 **AD, AD**와 통신할 경우 **AD**와 통신할 경우 다른 **forest(IdM)**에 대한 신뢰 토폴로지 정보를 추가합니다.

참고

이 단계는 다음 세 가지 이유 중 하나로 인해 충돌이 발생할 수 있습니다.

1. **LSA_SID_DISABLED_ECDHELICT** 오류로 보고되는 **STS** 네임스페이스가 충돌합니다. 이 충돌은 해결할 수 없습니다.

2. **tekton** 네임스페이스 충돌은 **LSA_NB_DISABLED_octetsLICT** 오류로 보고되었습니다. 이 충돌은 해결할 수 없습니다.

3. **DNS** 네임스페이스는 **LSA_TLN_DISABLED_octetsLICT** 오류로 보고한 최상위 이름(**TLN**)과 충돌합니다. **IdM** 서버는 다른 **tree**로 인해 발생하는 경우 **TLN** 충돌을 자동으로 해결할 수 있습니다.

TLN 충돌을 해결하기 위해 **IdM** 서버는 다음 단계를 수행합니다.

1. 충돌하는 섬김에 대한 트러스트 정보를 검색합니다.**Retrieving the trust information for the conflicting forest.**

2. **IdM DNS** 네임스페이스의 제외 항목을 **AD forest**에 추가합니다.

3. 충돌 하는 오버라이드에 대 한 트러스트 정보를 설정 합니다.

4. 원래 트리에 대한 신뢰를 설정합니다.**Retry establishing the trust to the original forest.**

IdM 서버는 **forest** 트러스트를 변경할 수 있는 **AD** 관리자의 권한으로 **ipa trust-add** 명령을 인증한 경우에만 이러한 충돌을 해결할 수 있습니다. 이러한 권한에 대한 액세스 권한이 없는 경우 원래 **delator**의 관리자는 **Windows UI UI**의 **Active Directory Domains** 및 **Trusts** 섹션에서 위의 단계를 수동으로 수행해야 합니다.

8. 존재하지 않는 경우 신뢰할 수 있는 도메인의 **ID** 범위를 생성합니다.

9. **For a forest trust, query Active Directory domain controllers from the forest root for details about the forest topology. IdM 서버는 이 정보를 사용하여 신뢰할 수 있는 섬에서 추가 도메인에 대한 추가 ID 범위를 생성합니다.**

추가 리소스

- 신뢰 컨트롤러 및 신뢰 에이전트
- 개요 문서 **(Microsoft)**
- 기술 문서 **(Microsoft)**
- **Active Directory(Microsoft)**의 권한 있는 계정 및 그룹

33.9.2. AD 신뢰를 설정하기 위한 사전 요구 사항 체크리스트

다음 체크리스트를 사용하여 AD 도메인과의 신뢰를 생성하기 위한 사전 요구 사항을 검토할 수 있습니다.

표 33.4. 테이블

구성 요소	설정	추가 세부 정보
제품 버전	Active Directory 도메인은 지원되는 Windows Server 버전을 사용하고 있습니다.	지원되는 Windows Server 버전
AD 관리자 권한	Active Directory 관리 계정은 다음 그룹 중 하나의 멤버여야 합니다. • Active Directory의 **Enterprise Admin (EA)** 그룹 • **도메인 관리자(DA)** 그룹 AD forest 루트 도메인의 도메인 관리자 (DA) 그룹	
네트워킹	모든 IdM 서버에 대해 Linux 커널에서 IPv6 지원이 활성화됩니다.	IdM의 IPv6 요구 사항

구성 요소	설정	추가 세부 정보
날짜 및 시간	두 서버의 날짜 및 시간 설정이 일치하는지 확인합니다.	IdM의 시간 서비스 요구 사항
암호화 유형	다음 AD 계정에는 AES 암호화 키가 있습니다. • AD Administrator • AD 사용자 계정 • AD 서비스 AD에서 최근에 AES 암호화를 활성화한 경우 다음 단계를 사용하여 새 AES 키를 생성합니다. 1. 섬에 있는 모든 AD 도메인 간의 신뢰 관계를 다시 설정합니다. 2. AD 관리자, 사용자 계정 및 서비스의 암호를 변경합니다.	• IdM의 암호화 유형 지원 • GPO를 사용하여 Active Directory의 AES 암호화 유형 활성화
방화벽	양방향 통신을 위해 IdM 서버 및 AD 도메인 컨트롤러에서 필요한 모든 포트를 열었습니다.	IdM과 AD 간 통신에 필요한 포트
DNS	• IdM 및 AD 각각 고유한 기본 DNS 도메인이 있습니다. • IdM 및 AD DNS 도메인이 겹치지 않습니다. • LDAP 및 Kerberos 서비스에 대한 적절한 DNS 서비스(SRV) 레코드 • 신뢰의 모든 DNS 도메인에서 DNS 레코드를 확인할 수 있습니다. • Kerberos 영역 이름은 기본 DNS 도메인 이름의 대문자 버전입니다. 예를 들어 DNS 도메인 **example.com** 에는 해당 Kerberos 영역 **EXAMPLE.COM**이 있습니다.	신뢰에 대한 DNS 및 영역 설정 구성

구성 요소	설정	추가 세부 정보
토폴로지	신뢰 컨트롤러로 구성한 IdM 서버를 사용하여 신뢰를 구축하고 있는지 확인합니다.	신뢰 컨트롤러 및 신뢰 에이전트

33.9.3. AD 트러스트를 설정하기 위한 시도의 디버그 로그 수집

IdM 환경과 AD 도메인 간에 신뢰를 설정하는 데 문제가 발생하는 경우 다음 단계를 사용하여 자세한 오류 로깅을 활성화하여 신뢰를 구축하기 위한 시도의 로그를 수집할 수 있습니다. 이러한 로그를 검토하여 문제 해결에 도움이되거나 Red Hat 기술 지원 케이스에 제공할 수 있습니다.

사전 요구 사항

- **IdM 서비스를 다시 시작하려면 root 권한이 필요합니다.**

절차

1. **IdM 서버에 대한 디버깅을 활성화하려면 다음 콘텐츠를 사용하여 /etc/ipa/server.conf 파일을 생성하십시오.**

```
[global]
debug=True
```

2. **httpd 서비스를 다시 시작하여 디버깅 구성을 로드합니다.**

```
[root@trust_controller ~]# systemctl restart httpd
```

3. **qcow 및 win bind 서비스를 중지합니다.**

```
[root@trust_controller ~]# systemctl stop smb winbind
```

4. **rootfs 및 winbind 서비스의 디버깅 로그 수준을 설정합니다.**

```
[root@trust_controller ~]# net conf setparm global 'log level' 100
```

5. **IdM 프레임워크에서 사용하는 Samba 클라이언트 코드에 대한 디버그 로깅을 활성화하려면 /usr/share/ipa/dpdk.conf.empty 구성 파일을 편집하여 다음 콘텐츠를 적용합니다.**

```
[global]
log level = 100
```

6. 이전 **Samba** 로그를 제거합니다.

```
[root@trust_controller ~]# rm /var/log/samba/log.*
```

7. **qcow** 및 **win bind** 서비스를 시작합니다.

```
[root@trust_controller ~]# systemctl start smb winbind
```

8. 자세한 정보 표시 모드가 활성화된 트러스트를 설정하려고 하면 타임스탬프를 출력합니다.

```
[root@trust_controller ~]# date; ipa -vvv trust-add --type=ad ad.example.com
```

9. 실패한 요청에 대한 정보는 다음 오류 로그 파일을 검토하십시오.

   a. **/var/log/httpd/error_log**

   b. **/var/log/samba/log.***

10. 디버깅을 비활성화합니다.

```
[root@trust_controller ~]# mv /etc/ipa/server.conf /etc/ipa/server.conf.backup
[root@trust_controller ~]# systemctl restart httpd
[root@trust_controller ~]# systemctl stop smb winbind
[root@trust_controller ~]# net conf setparm global 'log level' 0
[root@trust_controller ~]# mv /usr/share/ipa/smb.conf.empty
/usr/share/ipa/smb.conf.empty.backup
[root@trust_controller ~]# systemctl start smb winbind
```

11. *(선택 사항)* 인증 문제의 원인을 확인할 수 없는 경우

   a. 최근에 생성한 로그 파일을 수집 및 보관합니다.

```
[root@trust_controller ~]# tar -xcvf debugging-trust.tar /var/log/httpd/error_log
/var/log/samba/log.*
```

b. **Red Hat** 기술 지원 케이스를 열고 시도에서 타임 스탬프 및 디버그 로그를 제공합니다.

추가 리소스

- IPA - AD Trust Troubleshooting

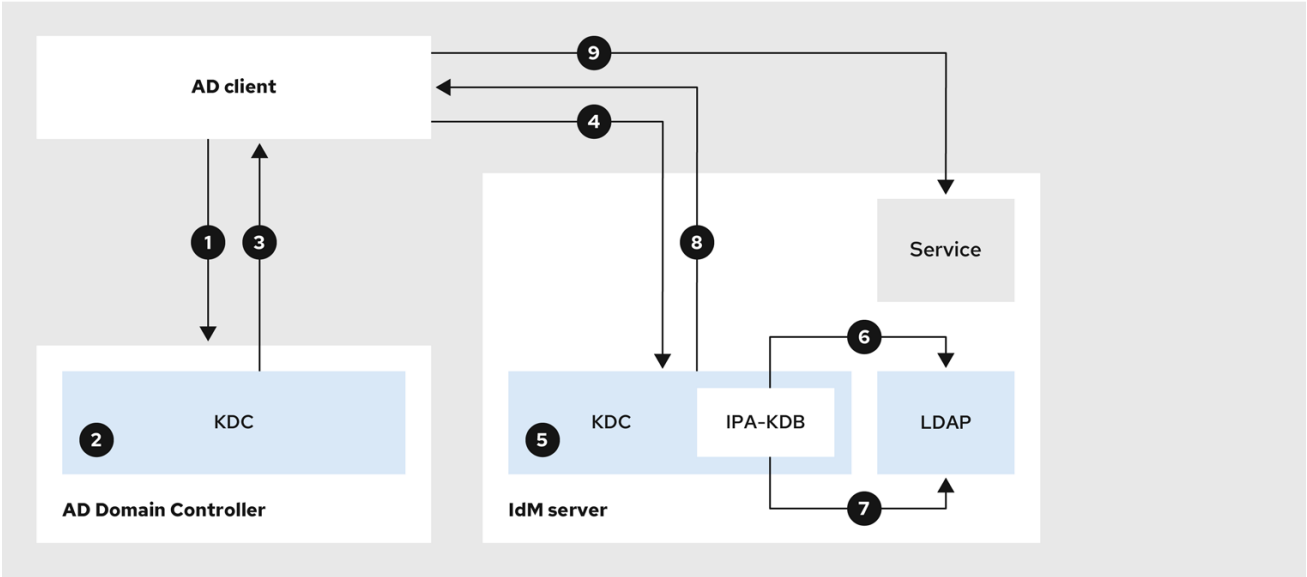
33.10. 다른 대리점의 서비스에 대한 클라이언트 액세스 문제 해결

IdM(Identity Management) 및 **AD(Active Directory)** 환경 간의 신뢰를 구성한 후 한 도메인의 클라이언트가 다른 도메인의 서비스에 액세스할 수 없는 문제가 발생할 수 있습니다. 다음 다이어그램을 사용하여 문제를 해결합니다.

33.10.1. AD forest 루트 도메인의 호스트가 IdM 서버에서 서비스를 요청할 때 정보 흐름

다음 다이어그램에서는 **AD(Active Directory)** 클라이언트가 **IdM(Identity Management)** 도메인에서 서비스를 요청할 때 정보 흐름을 설명합니다.

AD 클라이언트에서 **IdM** 서비스에 액세스하는 데 문제가 있는 경우 이 정보를 사용하여 문제 해결 노력을 좁히고 문제의 원인을 확인할 수 있습니다.



231_RHEL_0422

1. AD 클라이언트는 AD Kerberos Distribution Center(KDC)에 연결하여 IdM 도메인에서 서비스에 대한 TGS 요청을 수행합니다.

2. AD NetNamespace는 서비스가 신뢰할 수 있는 IdM 도메인에 속함을 인식합니다.

3. AD NetNamespace는 클라이언트에 신뢰할 수 있는 IdM NetNamespace에 추천과 함께 TGT(Cross-realm ticket-granting ticket)를 보냅니다.

4. AD 클라이언트는 교차 실시간 TGT를 사용하여 IdM NetNamespace에 티켓을 요청합니다.

5. IdM UUID는 교차 실m TGT로 전송되는 Privileged Privileged Attribute Certificate (MS-PAC)의 유효성을 검증합니다.

6. IPA-KDB 플러그인은 LDAP 디렉토리를 확인하여 외부 주체가 요청된 서비스에 대한 티켓을 받을 수 있는지 확인할 수 있습니다.

7. IPA-KDB 플러그인은 MS-PAC를 디코딩하고 데이터를 검증 및 필터링합니다. 로컬 그룹과 같은 추가 정보로 MS-PAC를 보강해야 하는지 확인하기 위해 LDAP 서버에서 조회를 수행합니다.

8. IPA-KDB 플러그인은 PAC를 인코딩하고 서명하여 서비스 티켓에 연결한 후 AD 클라이언트에 전송합니다.

9. 이제 AD 클라이언트에서 IdM NetNamespace에서 발행한 서비스 티켓을 사용하여 IdM 서비스에 문의할 수 있습니다.

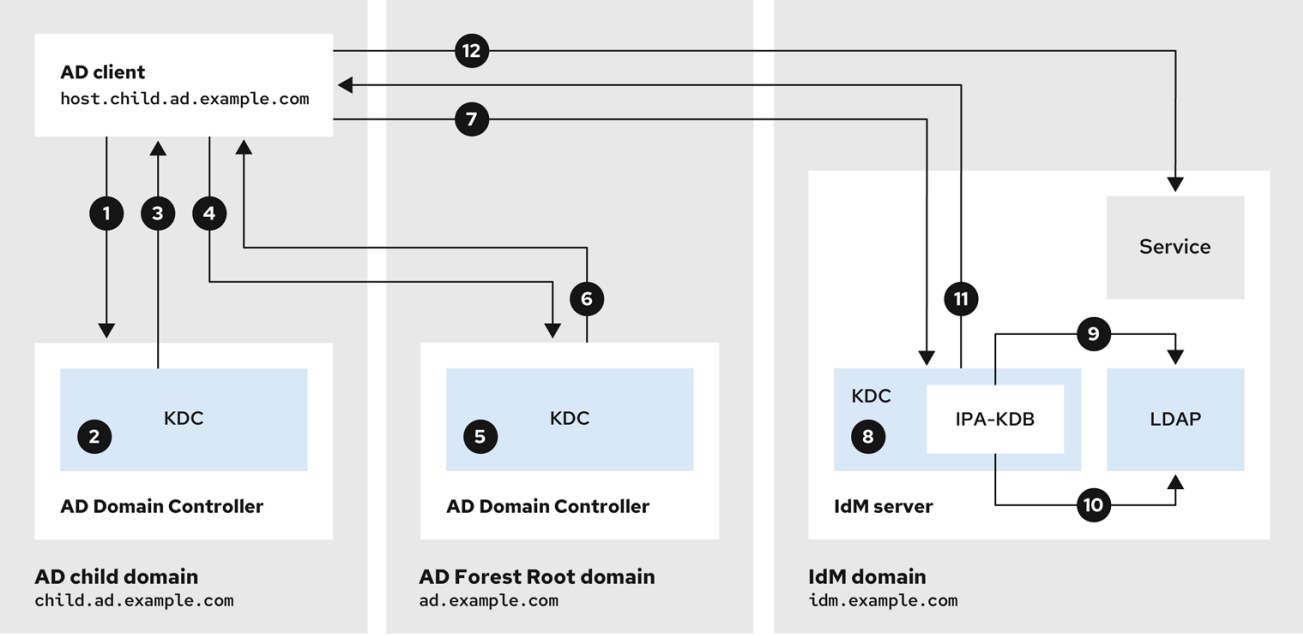
추가 리소스

- AD 하위 도메인의 호스트가 IdM 서버에서 서비스를 요청할 때 정보 흐름

33.10.2. AD 하위 도메인의 호스트가 IdM 서버에서 서비스를 요청할 때 정보 흐름

다음 다이어그램에서는 하위 도메인의 **AD(Active Directory)** 호스트가 **IdM(Identity Management)** 도메인에서 서비스를 요청할 때 정보 흐름을 설명합니다. 이 시나리오에서는 **AD** 클라이언트는 하위 도메인의 **KDC(Kerberos Distribution Center)**에 접속한 다음 **AD forest** 루트의 **NetNamespace**에 연결하고, 마지막으로 **IdM service**에 대한 액세스를 요청하도록 **IdM**에 연결합니다.

AD 클라이언트에서 **IdM** 서비스에 액세스하는 데 문제가 있고 **AD** 클라이언트가 **AD forest** 루트의 하위 도메인인 도메인에 속하는 경우 이 정보를 사용하여 문제 해결 노력을 좁히고 문제의 원인을 확인할 수 있습니다.



1. **AD** 클라이언트는 자체 도메인의 **AD Kerberos Distribution Center(KDC)**에 연결하여 **IdM** 도메인에서 서비스에 대한 **TGS** 요청을 수행합니다.

2. 하위 도메인인 **child.ad.example.com** 의 **AD NetNamespace**는 서비스가 신뢰할 수 있는 **IdM** 도메인에 속함을 인식합니다.

3. 하위 도메인의 **AD NetNamespace**는 클라이언트에 **AD forest** 루트 도메인 **ad.example.com** 에 대한 조회 티켓을 보냅니다.

4. **AD** 클라이언트는 **IdM** 도메인에 있는 서비스의 **AD forest** 루트 도메인의 **NetNamespace**에 연결합니다.

5. forest 루트 도메인의 NetNamespace는 서비스가 신뢰할 수 있는 IdM 도메인에 속함을 인식합니다.

6. AD NetNamespace는 클라이언트에 신뢰할 수 있는 IdM NetNamespace에 추천과 함께 TGT(Cross-realm ticket-granting ticket)를 보냅니다.

7. AD 클라이언트는 교차 실시간 TGT를 사용하여 IdM NetNamespace에 티켓을 요청합니다.

8. IdM UUID는 교차 실m TGT로 전송되는 Privileged Privileged Attribute Certificate (MS-PAC)의 유효성을 검증합니다.

9. IPA-KDB 플러그인은 LDAP 디렉토리를 확인하여 외부 주체가 요청된 서비스에 대한 티켓을 받을 수 있는지 확인할 수 있습니다.

10. IPA-KDB 플러그인은 MS-PAC를 디코딩하고 데이터를 검증 및 필터링합니다. 로컬 그룹과 같은 추가 정보로 MS-PAC를 보강해야 하는지 확인하기 위해 LDAP 서버에서 조회를 수행합니다.

11. IPA-KDB 플러그인은 PAC를 인코딩하고 서명하여 서비스 티켓에 연결한 후 AD 클라이언트에 전송합니다.

12. 이제 AD 클라이언트에서 IdM NetNamespace에서 발행한 서비스 티켓을 사용하여 IdM 서비스에 문의할 수 있습니다.

추가 리소스

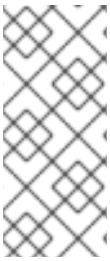
- AD forest 루트 도메인의 호스트가 IdM 서버에서 서비스를 요청할 때 정보 흐름

33.10.3. IdM 클라이언트가 AD 서버에서 서비스를 요청할 때 정보 흐름

다음 다이어그램에서는 IdM과 AD 사이에 양방향 트러스트를 구성한 경우 IdM(Identity Management) 클라이언트가 AD(Active Directory) 도메인에서 서비스를 요청할 때 정보 흐름을 설명합니다.

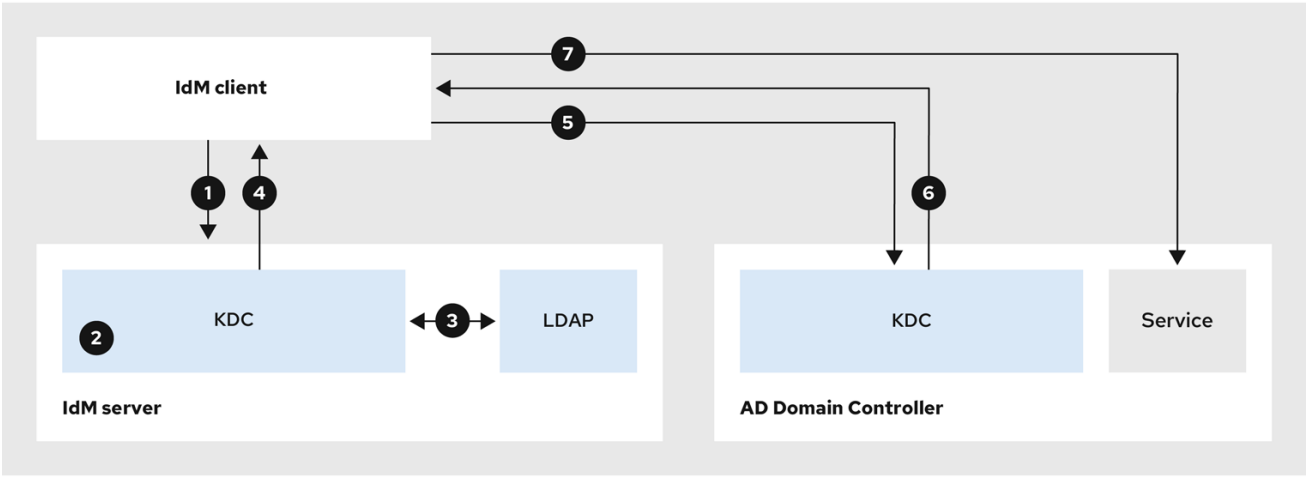
IdM 클라이언트에서 AD 서비스에 액세스하는 데 문제가 있는 경우 이 정보를 사용하여 문제 해결 노

력을 좁히고 문제의 원인을 확인할 수 있습니다.



참고

기본적으로 IdM은 AD에 일방향 트러스트를 설정합니다. 즉, AD charts의 리소스에 대해 cross-realm ticket-granting 티켓(TGT)을 발행할 수 없습니다. 신뢰할 수 있는 AD 도메인에서 서비스에 대한 티켓을 요청하려면 양방향 신뢰를 구성합니다.



1. IdM 클라이언트는 연결하려는 AD 서비스의 IdM Kerberos Distribution Center(KDC)에서 TGT(ticket-granting ticket)를 요청합니다.

2. IdM NetNamespace는 서비스가 AD 영역에 속하고, 영역이 알려진 신뢰할 수 있고 신뢰할 수 있는지 확인하며, 클라이언트가 해당 영역에서 서비스를 요청할 수 있는지 확인합니다.

3. IdM directory Server의 사용자 주체에 대한 정보를 사용하여 IdM NetNamespace는 사용자 주체에 대한 권한 있는 속성 인증서(MS-PAC) 레코드와 함께 cross-realm TGT를 생성합니다.

4. IdM NetNamespace가 IdM 클라이언트에 cross-realm TGT를 보냅니다.

5. IdM 클라이언트는 AD NetNamespace에 연결하여 AD 서비스에 대한 티켓을 요청하여 IdM NetNamespace에서 제공하는 MS-PAC가 포함된 교차 실명 TGT를 표시합니다.

6. AD 서버는 PAC의 유효성을 확인 및 필터링하고 AD 서비스에 대한 티켓을 반환합니다.

7. 이제 IPA 클라이언트가 AD 서비스에 연결할 수 있습니다.

추가 리소스

- 단방향 신뢰 및 양방향 신뢰

33.11. 명령줄을 사용하여 신뢰 제거

이 섹션에서는 명령줄 인터페이스를 사용하여 IdM 측에 대한 IdM(Identity Management)/Active Directory(AD) 트러스트를 제거하는 방법을 설명합니다.

사전 요구 사항

- IdM 관리자로서 Kerberos 티켓을 받을 수 있습니다. 자세한 내용은 웹 UI의 Logging to IdM 을 참조하십시오. Kerberos 티켓 사용.

절차

1. ipa trust-del 명령을 사용하여 IdM에서 신뢰 구성을 제거합니다.

```
[root@server ~]# ipa trust-del ad_domain_name
-----------------------------
Deleted trust "ad_domain_name"
-----------------------------
```

2. Active Directory 구성에서 trust 오브젝트를 제거합니다.

검증 단계

- ipa trust-show 명령을 사용하여 신뢰가 제거되었는지 확인합니다.

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

33.12. IDM 웹 UI를 사용하여 신뢰 제거

이 섹션에서는 IdM 웹 UI를 사용하여 IdM(Identity Management)/Active Directory(AD) 신뢰를 제거하는 방법을 설명합니다.

사전 요구 사항

- Kerberos 티켓을 받을 수 있습니다. 자세한 내용은 웹 UI의 Logging to IdM을 참조하십시오. Kerberos 티켓 사용.

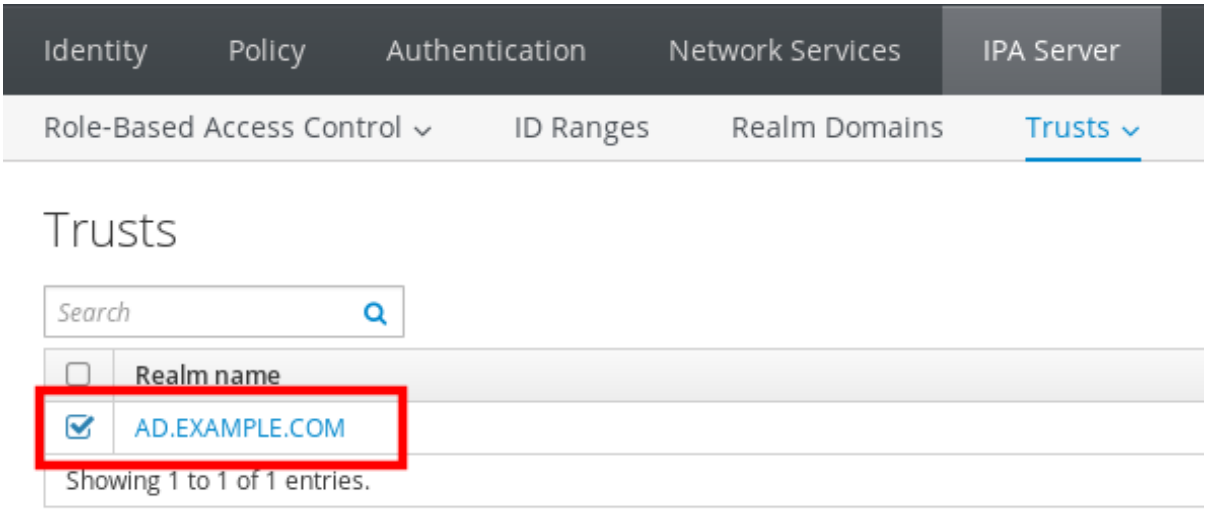
절차

1. 관리자 권한으로 IdM 웹 UI에 로그인합니다. 자세한 내용은 웹 브라우저에서 IdM 웹 UI 액세스를 참조하십시오.

2. IdM 웹 UI에서 IPA 서버 탭을 클릭합니다.

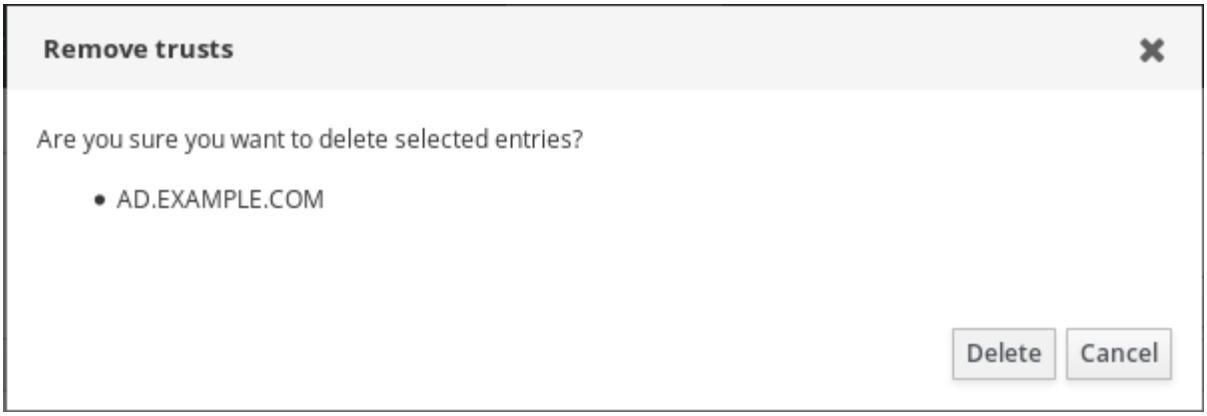
3. IPA 서버 탭에서 신뢰 탭을 클릭합니다.

4. 제거할 신뢰를 선택합니다.



5. 삭제 버튼을 클릭합니다.

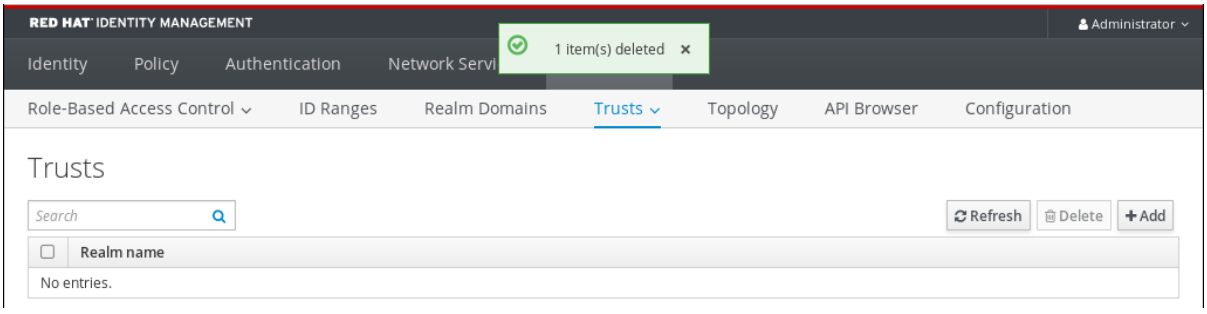
6. 신뢰 제거 대화 상자에서 삭제 를 클릭합니다.



7. Active Directory 구성에서 trust 오브젝트를 제거합니다.

검증 단계

- 신뢰가 성공적으로 삭제되면 웹 UI에 텍스트와 함께 녹색 팝업이 표시됩니다.



33.13. ANSIBLE을 사용하여 신뢰 제거

이 섹션에서는 Ansible 플레이북을 사용하여 IdM 측에 대한 IdM(Identity Management)/Active Directory(AD) 트러스트를 제거하는 방법을 설명합니다.

사전 요구 사항

- IdM 관리자로서 Kerberos 티켓을 받을 수 있습니다. 자세한 내용은 웹 UI의 Logging to IdM 을 참조하십시오. Kerberos 티켓 사용.

- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.8 이상을 사용하고 있습니다.
  - ansible-freeipa 패키지가 설치되어 있습니다.
  - ~/*MyPlaybooks*/ 디렉터리에서 신뢰를 제거하는 IdM 서버의 정규화된 도메인 이름(FQDN)을 사용하여 Ansible 인벤토리 파일을 생성했습니다.

절차

1. ~/*MyPlaybooks*/ 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. 다음 콘텐츠를 사용하여 del-trust.yml 플레이북을 생성합니다.

```
---
- name: Playbook to delete trust
  hosts: ipaserver
  become: true

  tasks:
    - name: ensure the trust is absent
      ipatrust:
        ipaadmin_password: SomeADMINpassword
        realm: ad.example.com
        state: absent
```

예제에서 realm 은 AD 영역 이름 문자열을 정의합니다.

3. 파일을 저장합니다.

4. 플레이북 파일 및 인벤토리 파일을 지정하여 Ansible 플레이북을 실행합니다.

```
$ ansible-playbook -v -i inventory del-trust.yml
```

검증 단계

- **ipa trust-show** 명령을 사용하여 신뢰가 제거되었는지 확인합니다.

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

추가 리소스

- **/usr/share/doc/ansible-freeipa/README-trust.md**

- **/usr/share/doc/ansible-freeipa/playbooks/trust**