Red Hat Enterprise Linux 9

Identity Management 서비스 액세스

IdM에 로그인하고 서비스를 관리하는 가이드

Last Updated: 2022-08-29

Red Hat Enterprise Linux 9 Identity Management 서비스 액세스

IdM에 로그인하고 서비스를 관리하는 가이드

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 콘솔 및 WebUI에서 IdM(Identity Management) 사용자로 로그인하는 방법과 RHEL 9 IdM 서비스를 시작하고 중지하는 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

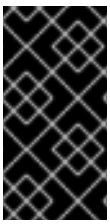
RED HAT 문서에 관한 피드백 제공

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. 명령줄에서 ID 관리에 로그인

IdM(Identity Management)은 Kerberos 프로토콜을 사용하여 SSO(Single Sign-On)를 지원합니다. SSO(Single Sign-On)는 사용자가 올바른 사용자 이름과 암호를 한 번만 입력한 다음 시스템이 자격 증명을 요청하는 메시지를 표시하지 않고 IdM 서비스에 액세스합니다.



중요

IdM에서 SSSD(System Security Services Daemon)는 사용자가 Kerberos 주체 이름을 사용하여 IdM 클라이언트 시스템의 데스크탑 환경에 성공적으로 로그인한 후 사용자에게 티켓 통합 티켓(TGT)을 자동으로 가져옵니다. 즉, 로그인 후 사용자는 **kinit** 유틸리티를 사용하여 IdM 리소스에 액세스할 필요가 없습니다.

Kerberos 인증 정보 캐시 또는 Kerberos TGT가 만료된 경우 IdM 리소스에 액세스하려면 Kerberos 티켓을 수동으로 요청해야 합니다. 다음 섹션에서는 IdM에서 Kerberos를 사용할 때 기본 사용자 작업을 보여줍니다.

1.1. KINIT 를 사용하여 IDM에 수동으로 로그인

이 절차에서는 **kinit** 유틸리티를 사용하여 IdM(Identity Management) 환경에 수동으로 인증하는 방법을 설명합니다. **kinit** 유틸리티는 IdM 사용자를 대신하여 Kerberos 티켓(TGT)을 가져오고 캐시합니다.

참고

초기 Kerberos TGT를 제거했거나 만료된 경우에만 이 절차를 사용하십시오. IdM 사용자는 로컬 시스템에 로그인할 때 IdM에 자동으로 로그인됩니다. 즉, 로그인 후 **kinit** 유틸리티를 사용하여 IdM 리소스에 액세스할 필요가 없습니다.

절차

1. IdM에 로그인

   - 로컬 시스템에 현재 로그인한 사용자의 사용자 이름에서 사용자 이름을 지정하지 않고 **kinit** 를 사용합니다. 예를 들어 로컬 시스템에서 **example_user** 로 로그인한 경우:

     ```
     [example_user@server ~]$ kinit
     Password for example_user@EXAMPLE.COM:
     [example_user@server ~]$
     ```

     로컬 사용자의 사용자 이름이 IdM의 사용자 항목과 일치하지 않으면 인증 시도에 실패합니다.

     ```
     [example_user@server ~]$ kinit
     kinit: Client 'example_user@EXAMPLE.COM' not found in Kerberos database while
     getting initial credentials
     ```

   - 로컬 사용자 이름에 일치하지 않는 Kerberos 사용자 이름을 사용하여 필요한 사용자 이름을 **kinit** 유틸리티에 전달합니다. 예를 들어 **admin** 사용자로 로그인하려면 다음을 수행합니다.

     ```
     [example_user@server ~]$ kinit admin
     Password for admin@EXAMPLE.COM:
     [example_user@server ~]$
     ```

2. 선택적으로 로그인에 성공했는지 확인하려면 **klist** 유틸리티를 사용하여 캐시된 TGT를 표시합니다. 다음 예에서 캐시에는 **example_user** 주체의 티켓이 포함되어 있습니다. 즉, 이 특정 호스트에서만 **example_user** 만 IdM 서비스에 액세스할 수 있습니다.

```
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: example_user@EXAMPLE.COM

Valid starting     Expires            Service principal
11/10/2019 08:35:45  11/10/2019 18:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

1.2. 사용자의 활성 KERBEROS 티켓 삭제

이 섹션에서는 사용자의 활성 Kerberos 티켓이 포함된 인증 정보 캐시를 지우는 방법에 대해 설명합니다.

절차

1. Kerberos 티켓을 삭제하려면 다음을 수행합니다.

```
[example_user@server ~]$ kdestroy
```

2. 필요한 경우 Kerberos 티켓이 삭제되었는지 확인하려면 다음을 수행하십시오.

```
[example_user@server ~]$ klist
klist: Credentials cache keyring 'persistent:0:0' not found
```

1.3. KERBEROS 인증을 위한 외부 시스템 구성

이 섹션에서는 IdM(Identity Management) 사용자가 Kerberos 자격 증명을 사용하여 외부 시스템에서 IdM에 로그인할 수 있도록 외부 시스템을 구성하는 방법을 설명합니다.

외부 시스템에서 Kerberos 인증을 활성화하면 인프라에 여러 영역 또는 겹치는 도메인이 포함된 경우 특히 유용합니다. **ipa-client-install** 을 통해 시스템이 IdM 도메인에 등록되지 않은 경우에도 유용합니다.

IdM 도메인의 멤버가 아닌 시스템에서 IdM에 Kerberos 인증을 활성화하려면 외부 시스템에 IdM 관련 Kerberos 구성 파일을 정의합니다.

사전 요구 사항

- **jenkinsfile5-tekton** 패키지가 외부 시스템에 설치되어 있습니다.
  패키지가 설치되었는지 확인하려면 다음 CLI 명령을 사용하십시오.

```
# dnf list installed krb5-workstation
Installed Packages
krb5-workstation.x86_64    1.16.1-19.el8    @BaseOS
```

절차

1. IdM 서버의 **/etc/krb5.conf** 파일을 외부 시스템으로 복사합니다. 예를 들어 다음과 같습니다.

```
# scp /etc/krb5.conf root@externalsystem.example.com:/etc/krb5_ipa.conf
```

주의

외부 시스템의 기존 jenkinsfile **5.conf** 파일을 덮어쓰지 마십시오.

2. 외부 시스템에서 복사된 IdM Kerberos 구성 파일을 사용하도록 터미널 세션을 설정합니다.

```
$ export KRB5_CONFIG=/etc/krb5_ipa.conf
```

KRB5_CONFIG 변수는 로그아웃할 때까지 일시적으로 존재합니다. 이러한 손실을 방지하려면 다른 파일 이름으로 변수를 내보냅니다.

3. **/etc/krb5.conf.d/** 디렉터리에서 외부 시스템으로 Kerberos 구성 스니펫을 복사합니다.

외부 시스템의 사용자는 **kinit** 유틸리티를 사용하여 IdM 서버에 인증할 수 있습니다.

1.4. 추가 리소스

- jenkinsfile **5.conf(5)** 매뉴얼 페이지.
- **kinit(1)** 도움말 페이지.
- **klist(1)** 도움말 페이지.
- **kdestroy(1)** 도움말 페이지.

2장. IDENTITY MANAGEMENT 서비스 보기, 시작 및 중지

IdM(Identity Management) 서버는 도메인 컨트롤러(DC)로 작동하는 Red Hat Enterprise Linux 시스템입니다. IdM 서버, 특히 디렉터리 서버, CA(인증 기관), DNS 및 Kerberos를 통해 다양한 서비스가 실행되고 있습니다.

2.1. IDM 서비스

이 섹션에서는 IdM 서버 및 클라이언트에서 설치 및 실행할 수 있는 서비스에 대해 설명합니다.

IdM 서버에서 호스팅하는 서비스 목록

다음 서비스 대부분은 IdM 서버에 설치할 필요가 없습니다. 예를 들어 인증 기관(CA) 또는 IdM 도메인 외부의 외부 서버에 DNS 서버와 같은 서비스를 설치할 수 있습니다.

Kerberos

jenkinsfile **5kdc** 및 **kadmin** 서비스

IdM은 **Kerberos** 프로토콜을 사용하여 SSO(Single Sign-On)를 지원합니다. Kerberos를 사용하면 사용자는 올바른 사용자 이름과 암호를 한 번만 제공해야 하며 시스템이 자격 증명을 다시 요청하지 않고 IdM 서비스에 액세스할 수 있습니다.

Kerberos는 다음 두 부분으로 나뉩니다.

- Net **Namespace5kdc** 서비스는 Kerberos 인증 서비스 및 KDC(Key Distribution Center) 데몬입니다.
- **kadmin** 서비스는 Kerberos 데이터베이스 관리 프로그램입니다.

IdM에서 Kerberos를 사용하여 인증하는 방법에 대한 자세한 내용은 명령줄에서 ID 관리에 로그인하고 웹 UI에서 IdM에 로그인하십시오. Kerberos 티켓 사용.

LDAP 디렉터리 서버

dirsrv 서비스

IdM **LDAP 디렉터리 서버** 인스턴스는 Kerberos, 사용자 계정, 호스트 항목, 서비스, 정책, DNS 등과 관련된 모든 IdM 정보를 저장합니다. LDAP 디렉터리 서버 인스턴스는 Red Hat Directory Server 와 동일한 기술을 기반으로 합니다. 그러나 IdM 특정 작업으로 조정됩니다.

인증 기관

pki-tomcatd 서비스

통합 **인증 기관(CA)** 은 Red Hat Certificate System 과 동일한 기술을 기반으로 합니다. **PKI** 는 인증서 시스템 서비스에 액세스하기 위한 명령줄 인터페이스입니다.

필요한 모든 인증서를 독립적으로 생성하고 제공하는 경우 통합 CA 없이 서버를 설치할 수도 있습니다.

자세한 내용은 CA 서비스 플래닝을 참조하십시오.

DNS(Domain Name System)

named 서비스

IdM은 동적 서비스 검색에 **DNS** 를 사용합니다. IdM 클라이언트 설치 유틸리티는 DNS의 정보를 사용하여 클라이언트 시스템을 자동으로 구성할 수 있습니다. 클라이언트가 IdM 도메인에 등록된 후 DNS를 사용하여 도메인 내에서 IdM 서버 및 서비스를 찾습니다. Red Hat Enterprise Linux의 DNS(Domain Name

System) 프로토콜의 **BIND** (Berkeley Internet Name Domain) 구현에는 **이름이** 지정된 DNS 서버가 포함되어 있습니다. **named-pkcs11** 은 PKCS#11 암호화 표준에 대한 기본 지원으로 구축된 BIND DNS 서버의 버전입니다.

자세한 내용은 DNS 서비스 및 호스트 이름 계획을 참조하십시오.

Apache HTTP Server

httpd 서비스

Apache HTTP 웹 서버는 IdM 웹 UI를 제공하고 인증 기관과 기타 IdM 서비스 간의 통신을 관리합니다.

Samba / Winbind

SMB 및 **winbind** 서비스

Samba는 Red Hat Enterprise Linux에서 CIFS(Common Internet File System) 프로토콜이라고도 하는 SMB(Server Message Block) 프로토콜을 구현합니다. NetNamespace 서비스를 통해 SMB 프로토콜을 사용하면 파일 공유 및 공유 프린터와 같은 서버의 리소스에 액세스할 수 있습니다. AD(Active Directory) 환경으로 트러스트를 구성한 경우 'Winbind' 서비스는 IdM 서버와 AD 서버 간의 통신을 관리합니다.

일회성 암호(OTP) 인증

ipa-otpd 서비스

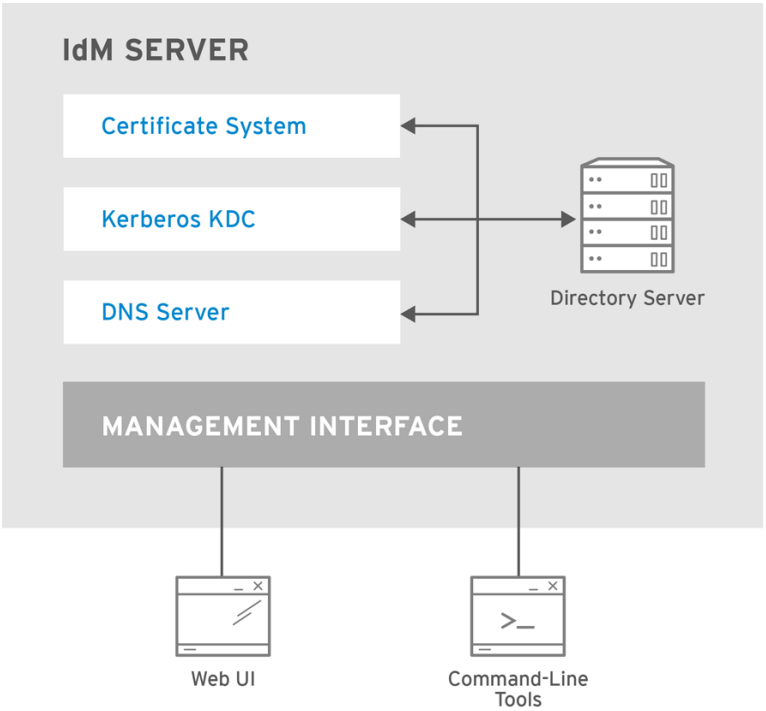
일회용 암호(OTP)는 이중 인증의 일부로 하나의 세션에 대해서만 인증 토큰에 의해 생성되는 암호입니다. OTP 인증은 **ipa-otpd** 서비스를 통해 Red Hat Enterprise Linux에서 구현됩니다.

자세한 내용은 한 번 암호를 사용하여 ID 관리 웹 UI에 로그인합니다 .

OpenDNSSEC

ipa-dnskeysyncd 서비스

OpenDNSSEC 는 DNSSEC(DNS Security extensions) 키 및 영역 서명 프로세스를 자동화하는 DNS 관리자입니다. **ipa-dnskeysyncd** 서비스는 IdM Directory Server와 OpenDNSSEC 간의 동기화를 관리합니다.



IdM 클라이언트에서 호스팅하는 서비스 목록

- System Security Services Daemon: **sssd** 서비스

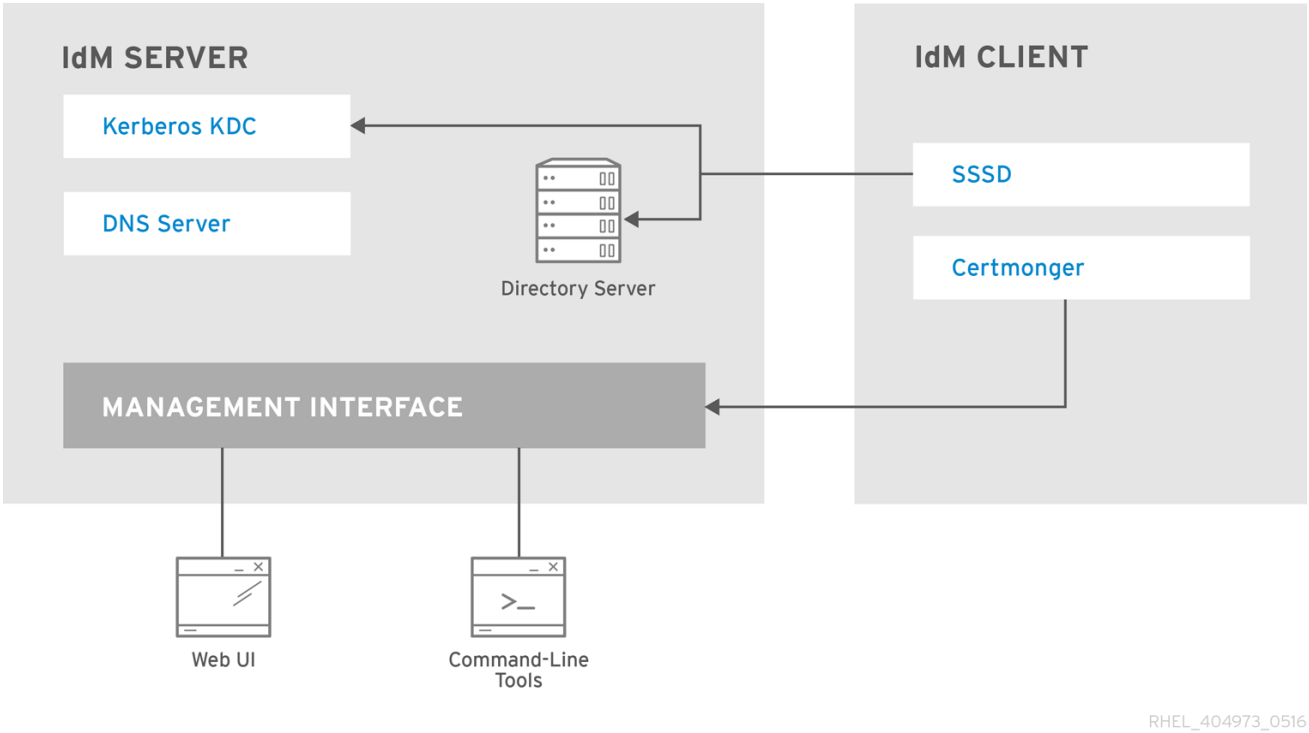
SSSD(**System Security Services Daemon**)는 사용자 인증 및 캐싱 자격 증명을 관리하는 클라이언트 측 애플리케이션입니다. 캐싱을 사용하면 IdM 서버를 사용할 수 없거나 클라이언트가 오프라인인 경우 로컬 시스템에서 정상적인 인증 작업을 계속할 수 있습니다.

자세한 내용은 SSSD 이해 및 이점을 참조하십시오.

- certmonger: **certmonger** 서비스

certmonger 서비스는 클라이언트의 인증서를 모니터링하고 갱신합니다. 시스템의 서비스에 대한 새 인증서를 요청할 수 있습니다.

자세한 내용은 certmonger를 사용하여 서비스에 대한 IdM 인증서 가져오기를 참조하십시오.

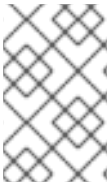


2.2. IDM 서비스의 상태 보기

IdM 서버에 구성된 IdM 서비스의 상태를 보려면 **ipactl status** 명령을 실행합니다.

```
[root@server ~]# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
pki-tomcatd Service: RUNNING
smb Service: RUNNING
winbind Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

서버의 **ipactl status** 명령의 출력은 IdM 구성에 따라 다릅니다. 예를 들어 IdM 배포에 DNS 서버가 포함되지 않으면 **named** 서비스가 목록에 없습니다.



참고

IdM 웹 UI를 사용하여 특정 IdM 서버에서 실행되는 모든 IdM 서비스의 상태를 볼 수 없습니다. 다른 서버에서 실행되는 Kerberized 서비스는 IdM 웹 UI의 **ID → 서비스** 탭에서 볼 수 있습니다.

전체 서버 또는 개별 서비스만 시작하거나 중지할 수 있습니다.

전체 IdM 서버를 시작, 중지 또는 다시 시작하려면 다음을 참조하십시오.

- 전체 ID 관리 서버 시작 및 중지: ipactl 유틸리티

개별 IdM 서비스를 시작, 중지 또는 다시 시작하려면 다음을 참조하십시오.

- 개별 Identity Management 서비스 시작 및 중지: systemctl 유틸리티

IdM 소프트웨어 버전을 표시하려면 다음을 참조하십시오.

- IdM 소프트웨어 버전을 표시하는 방법

2.3. 전체 ID 관리 서버 시작 및 중지:IPACTL 유틸리티

ipactl 유틸리티를 사용하여 설치된 모든 서비스와 함께 전체 IdM 서버를 중지, 시작 또는 다시 시작합니다. **ipactl** 유틸리티를 사용하면 모든 서비스가 적절한 순서로 중지, 시작 또는 다시 시작됩니다. **ipactl** 명령을 실행하기 위해 유효한 Kerberos 티켓이 필요하지 않습니다.

ipactl 명령

전체 IdM 서버를 시작하려면 다음을 수행합니다.

```
# ipactl start
```

전체 IdM 서버를 중지하려면 다음을 수행합니다.

```
# ipactl stop
```

전체 IdM 서버를 다시 시작하려면 다음을 수행합니다.

```
# ipactl restart
```

IdM을 구성하는 모든 서비스의 상태를 표시하려면 다음을 수행합니다.

```
# ipactl status
```

중요

IdM 웹 UI를 사용하여 **ipactl** 명령을 수행할 수 없습니다.

2.4. 개별 IDENTITY MANAGEMENT 서비스 시작 및 중지:SYSTEMCTL 유틸리티

IdM 구성 파일을 수동으로 변경하는 것은 권장되지 않습니다. 그러나 특정 상황에서는 관리자가 특정 서비스의 수동 구성을 수행해야 합니다. 이러한 경우 **systemctl** 유틸리티를 사용하여 개별 IdM 서비스를 중지, 시작 또는 다시 시작합니다.

예를 들어 다른 IdM 서비스를 수정하지 않고 Directory Server 동작을 사용자 지정한 후 **systemctl** 을 사용합니다.

```
# systemctl restart dirsrv@REALM-NAME.service
```

또한 Active Directory와 함께 IdM 신뢰를 처음 배포할 때 **/etc/sssd/sssd.conf** 파일을 수정하여 다음을 추가합니다.

- 원격 서버에 대기 시간이 높은 환경에서 시간 초과 구성 옵션을 조정하는 특정 매개변수
- Active Directory 사이트 선호도를 조정하는 특정 매개변수
- 글로벌 IdM 설정에서 제공하지 않는 특정 구성 옵션에 대한 덮어쓰기

/etc/sssd/sssd.conf 파일에서 변경한 사항을 적용하려면 다음을 수행합니다.

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

SSSD(System Security Services Daemon)가 자동으로 다시 읽히거나 구성을 다시 적용하지 않으므로 **systemctl restart sssd.service** 를 실행해야 합니다.

IdM ID 범위에 영향을 미치는 변경 사항에 대해서는 전체 서버 재부팅이 권장됩니다.

중요

여러 IdM 도메인 서비스를 다시 시작하려면 항상 **ipactl** 을 사용합니다. IdM 서버와 함께 설치된 서비스 간의 종속성으로 인해 해당 서비스가 시작되고 중지된 순서가 중요합니다. **ipactl** 유틸리티를 사용하면 서비스가 적절한 순서로 시작되고 중지됩니다.

유용한 systemctl 명령

특정 IdM 서비스를 시작하려면 다음을 수행합니다.

```
# systemctl start name.service
```

특정 IdM 서비스를 중지하려면 다음을 수행합니다.

```
# systemctl stop name.service
```

특정 IdM 서비스를 다시 시작하려면 다음을 수행합니다.

```
# systemctl restart name.service
```

특정 IdM 서비스의 상태를 보려면 다음을 수행합니다.

```
# systemctl status name.service
```

중요

IdM 웹 UI를 사용하여 IdM 서버에서 실행되는 개별 서비스를 시작하거나 중지할 수 없습니다. **ID** → 서비스로 이동하고 서비스를 선택하여 웹 UI를 사용하여 Kerberized 서비스의 설정을 수정할 수 있습니다.

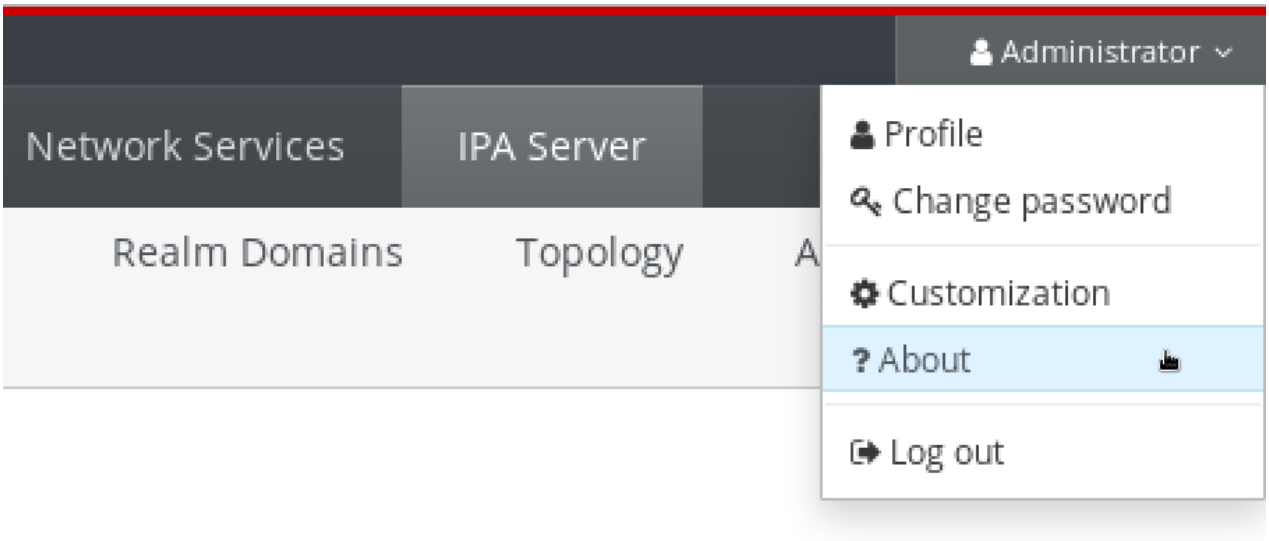
2.5. IDM 소프트웨어 버전을 표시하는 방법

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
```

3장. IDM 명령줄 유틸리티 소개

다음 섹션에서는 IdM(Identity Management) 명령줄 유틸리티를 사용하는 기본 사항에 대해 설명합니다.

사전 요구 사항

- IdM 서버 설치 및 액세스 가능.

  자세한 내용은 Identity Management 설치를 참조하십시오.

- IPA 명령줄 인터페이스를 사용하려면 유효한 Kerberos 티켓으로 IdM을 인증합니다.

3.1. IPA 명령줄 인터페이스란 무엇입니까?

IPA 명령줄 인터페이스(CLI)는 IdM(Identity Management) 관리를 위한 기본 명령줄 인터페이스입니다.

IdM을 관리하는 다양한 하위 명령(예: ipa user-add 명령)을 지원하여 새 사용자를 추가합니다.

IPA CLI를 사용하면 다음을 수행할 수 있습니다.

- 네트워크에서 사용자, 그룹, 호스트 및 기타 오브젝트를 추가, 관리 또는 제거합니다.
- 인증서를 관리합니다.
- 검색 항목.
- 오브젝트를 표시하고 나열합니다.
- 액세스 권한을 설정합니다.

- 올바른 명령 구문에 대한 도움말을 가져옵니다.

3.2. IPA 도움말이란 무엇입니까?

IPA 도움말은 IdM 서버에 대한 내장 문서 시스템입니다.

IPA 명령줄 인터페이스(CLI)는 로드된 IdM 플러그인 모듈의 사용 가능한 도움말 주제를 생성합니다. IPA 도움말 유틸리티를 사용하려면 다음이 필요합니다.

- IdM 서버가 설치되어 실행되고 있어야 합니다.
- 유효한 Kerberos 티켓을 사용하여 인증됩니다.

옵션 없이 ipa help 명령을 입력하면 기본 도움말 사용과 가장 일반적인 명령 예제에 대한 정보가 표시됩니다.

다음 옵션을 다양한 ipa 도움말 사용 사례에 사용할 수 있습니다.

```
$ ipa help [TOPIC | COMMAND | topics | commands]
```

- [2] 모든 매개변수는 선택 사항이며 ipa 도움말 만 작성할 수 있으며 명령이 실행됩니다.
- | 파이프 문자 수단 또는 습니다. 따라서 기본 ipa help 명령을 사용하여 topIC , COMMAND 또는 주제 또는 명령을 지정할 수 있습니다.
  - 주제: ipa 도움말 주제를 실행하여 IPA 도움말 (예: 사용자, 인증서,서버 등)의 항목 목록을 표시할 수 있습니다.
  - top /Enical letters 가 있는 I/E는 변수입니다. 따라서 특정 주제(예: ipa help 사용자)를 지정할 수 있습니다.
  - ipa help 명령을 입력하여 IPA 도움말(예: user-add,ca-enable,server-show 등)의 명령 목록을 표시할 수 있습니다.

- 대 /도: 대문자로 된 **Command MAND**는 변수입니다. 따라서 **ipa help user-add** 와 같은 특정 명령을 지정할 수 있습니다.

3.3. IPA 도움말 주제 사용

다음 절차에서는 명령줄 인터페이스에서 **IPA** 도움말을 사용하는 방법을 설명합니다.

절차

1. 터미널을 열고 **IdM** 서버에 연결합니다.

2. **ipa help** 주제 를 입력하여 도움말에서 다루는 주제 목록을 표시합니다.

```
$ ipa help topics
```

3. 주제 중 하나를 선택하고 다음 패턴에 따라 명령을 만듭니다. **ipa help** ***[topic_name]***. **topic_name** 문자열 대신 이전 단계에서 나열한 주제 중 하나를 추가합니다.

   예에서는 다음 항목을 사용합니다 .

```
$ ipa help user
```

4. **IPA** 도움말 출력이 너무 길어 전체 텍스트를 볼 수 없는 경우 다음 구문을 사용하십시오.

```
$ ipa help user | less
```

   그런 다음 아래로 스크롤하여 전체 도움말을 읽을 수 있습니다.

IPA CLI에는 사용자 항목에 대한 도움말 페이지가 표시됩니다. 개요를 읽은 후에는 주제 명령으로 작업하는 패턴을 사용하여 많은 예를 확인할 수 있습니다.

3.4. IPA 도움말 명령 사용

다음 절차에서는 명령줄 인터페이스에서 **IPA** 도움말 명령을 만드는 방법을 설명합니다.

절차

1. 터미널을 열고 **IdM** 서버에 연결합니다.

2. **ipa help** 명령을 입력하여 도움말에서 다루는 명령 목록을 표시합니다.

```
$ ipa help commands
```

3. 명령 중 하나를 선택하고 다음 패턴에 따라 **help** 명령을 생성합니다. **ipa help <** ***COMMAND*****>. &lt ;COMMAND& gt;** 문자열 대신 이전 단계에서 나열한 명령 중 하나를 추가합니다.

```
$ ipa help user-add
```

추가 리소스

- **ipa man** 페이지.

3.5. IPA 명령 구조

IPA CLI는 다음 유형의 명령을 구분합니다.

- **IdM** 서버에서 기본 제공 명령 **tekton-databind built-in** 명령을 모두 사용할 수 있습니다.

- 플러그인 제공 명령

IPA 명령의 구조를 사용하면 다양한 유형의 오브젝트를 관리할 수 있습니다. 예를 들어 다음과 같습니다.

- 사용자,

- 호스트,
- DNS 레코드
- 인증서,

그리고 많은 다른.

이러한 오브젝트 대부분의 경우 IPA CLI에는 다음을 위한 명령이 포함됩니다.

- add(추가)
- 수정 (mod)
- 삭제 (del)
- 검색 (Find)
- 표시(표시)

명령에는 다음과 같은 구조가 있습니다.

ipa user-add, ipa user-mod, ipa user-del, ipa user-find, ipa user-show

ipa host-add, ipa host-mod, ipa host-del, ipa host-find, ipa host-show

ipa dnsrecord-add,ipa dnsrecord-mod,ipa dnsrecord-del,ipa dnsrecord-find,ipa dn history-show

ipa user-add [options] 를 사용하여 사용자를 생성할 수 있습니다. 여기서 **[options]** 는 선택 사항입니다. **ipa user-add** 명령만 사용하는 경우 스크립트에서 세부 정보를 하나씩 요청합니다.

기존 오브젝트를 변경하려면 오브젝트를 정의해야 합니다. 따라서 명령에는 오브젝트 **ipa user-mod USER_NAME [options]** 도 포함됩니다.

3.6. IPA 명령을 사용하여 IDM에 사용자 계정 추가

다음 절차에서는 명령줄을 사용하여 **IdM(Identity Management)** 데이터베이스에 새 사용자를 추가하는 방법을 설명합니다.

사전 요구 사항

- **IdM** 서버에 사용자 계정을 추가하려면 관리자 권한이 있어야 합니다.

절차

1. 터미널을 열고 **IdM** 서버에 연결합니다.
2. 새 사용자를 추가하려면 명령을 입력합니다.

```
$ ipa user-add
```

이 명령은 사용자 계정을 생성하는 데 필요한 기본 데이터를 제공하도록 요청하는 스크립트를 실행합니다.

3. **이름:** 필드에 새 사용자의 첫 번째 이름을 입력하고 **Enter** 키를 누릅니다.
4. **성 :** 필드에 새 사용자의 마지막 이름을 입력하고 **Enter** 키를 누릅니다.
5. **User login [suggested user name]:** 사용자 이름을 입력하거나 **Enter** 키를 눌러 제안된 사용자 이름을 수락합니다.

사용자 이름은 전체 **IdM** 데이터베이스에 대해 고유해야 합니다. 해당 사용자 이름이 이미 존재하기 때문에 오류가 발생하면 **ipa user-add** 명령을 사용하여 프로세스를 반복하고 다른 고유

한 사용자 이름을 사용합니다.

사용자 이름을 추가한 후 사용자 계정이 IdM 데이터베이스에 추가되고 IPA 명령줄 인터페이스(CLI)는 다음 출력을 출력합니다.

```
---------------------
Added user "euser"
---------------------
User login: euser
First name: Example
Last name: User
Full name: Example User
Display name: Example User
Initials: EU
Home directory: /home/euser
GECOS: Example User
Login shell: /bin/sh
Principal name: euser@IDM.EXAMPLE.COM
Principal alias: euser@IDM.EXAMPLE.COM
Email address: euser@idm.example.com
UID: 427200006
GID: 427200006
Password: False
Member of groups: ipausers
Kerberos keys available: False
```

참고

기본적으로 사용자 암호는 사용자 계정에 설정되어 있지 않습니다. 사용자 계정을 생성하는 동안 암호를 추가하려면 다음 구문과 함께 **ipa user-add** 명령을 사용합니다.

```
$ ipa user-add --first=Example --last=User --password
```

IPA CLI에서 사용자 이름과 암호를 추가하거나 확인하라는 메시지가 표시됩니다.

사용자가 이미 생성된 경우 **ipa user-mod** 명령을 사용하여 암호를 추가할 수 있습니다.

추가 리소스

- 매개변수에 대한 자세한 내용은 **ipa help user-add** 명령을 실행합니다.

3.7. IPA 명령을 사용하여 IDM에서 사용자 계정 수정

각 사용자 계정에 대해 여러 매개 변수를 변경할 수 있습니다. 예를 들어 사용자에게 새 암호를 추가할 수 있습니다.

기본 명령 구문은 변경 사항을 수행하려는 기존 사용자 계정을 정의해야 하므로 **user-add** 구문과 다릅니다. 예를 들어 암호를 추가합니다.

사전 요구 사항

- 사용자 계정을 수정하려면 관리자 권한이 있어야 합니다.

절차

1. 터미널을 열고 **IdM** 서버에 연결합니다.

2. **ipa user-mod** 명령을 입력하고 수정할 사용자를 지정하고, 암호를 추가하기 위해 **--password** 와 같은 옵션을 지정합니다.

```
$ ipa user-mod euser --password
```

이 명령은 새 암호를 추가할 수 있는 스크립트를 실행합니다.

3. 새 암호를 입력하고 **Enter** 키를 누릅니다.

IPA CLI는 다음 출력을 출력합니다.

```
---------------------
Modified user "euser"
---------------------
User login: euser
First name: Example
Last name: User
Home directory: /home/euser
Principal name: euser@IDM.EXAMPLE.COM
Principal alias: euser@IDM.EXAMPLE.COM
Email address: euser@idm.example.com
UID: 427200006
GID: 427200006
```

```
Password: True
Member of groups: ipausers
Kerberos keys available: True
```

이제 사용자 암호가 계정에 설정되어 사용자가 IdM에 로그인할 수 있습니다.

추가 리소스

- 매개변수에 대한 자세한 내용은 ipa help user-mod 명령을 실행합니다.

3.8. IDM 유틸리티에 값 목록을 제공하는 방법

IdM(Identity Management)은 다중 값 속성에 대한 값을 목록에 저장합니다.

IdM은 멀티값 목록을 제공하는 다음 방법을 지원합니다.

- 동일한 명령 호출 내에서 동일한 명령줄 인수를 여러 번 사용합니다.

```
$ ipa permission-add --right=read --permissions=write --permissions=delete ...
```

- 또는 쉘이 확장을 수행하는 경우 목록을 curly braces로 묶을 수 있습니다.

```
$ ipa permission-add --right={read,write,delete} ...
```

위의 예제에서는 오브젝트에 권한을 추가하는 permission-add 명령을 보여줍니다. 이 오브젝트는 예제에 언급되어 있지 않습니다. … 대신 권한을 추가하려는 개체를 추가해야 합니다.

명령줄에서 이러한 다중값 속성을 업데이트하면 IdM에서 이전 값 목록을 새 목록으로 완전히 덮어씁니다. 따라서 다중 값 특성을 업데이트할 때 추가하려는 단일 값이 아닌 완전히 새 목록을 지정해야 합니다.

예를 들어 위의 명령에서 권한 목록에 읽기, 쓰기 및 삭제가 포함됩니다. permission-mod 명령으로 목록을 업데이트하려면 모든 값을 추가해야 합니다. 그렇지 않으면 언급되지 않은 값이 삭제됩니다.

예 1: ipa permission-mod 명령은 이전에 추가한 모든 권한을 업데이트합니다.

-

```
$ ipa permission-mod --right=read --right=write --right=delete ...
```

또는

```
$ ipa permission-mod --right={read,write,delete} ...
```

예: 명령에 포함되지 않기 때문에 **ipa permission-mod** 명령은 **--right=delete** 인수를 삭제합니다.

```
$ ipa permission-mod --right=read --right=write ...
```

또는

```
$ ipa permission-mod --right={read,write} ...
```

3.9. IDM 유틸리티와 함께 특수 문자를 사용하는 방법

ipa 명령에 특수 문자가 포함된 명령줄 인수를 전달할 때 백슬래시(\)를 사용하여 이러한 문자를 이스케이프합니다. 예를 들어 일반적인 특수 문자에는 각도 대괄호(< 및 >), 앰퍼샌드(&), 별표（*） 또는 세로 막대(|)가 포함됩니다.

예를 들어 별표（*）를 이스케이프하려면 다음을 수행합니다.

```
$ ipa certprofile-show certificate_profile --out=exported\*profile.cfg
```

이스케이프되지 않은 특수 문자가 포함된 명령은 쉘이 이러한 문자를 올바르게 구문 분석할 수 없기 때문에 예상대로 작동하지 않습니다.

4장. 명령줄에서 IDENTITY MANAGEMENT 항목 검색

다음 섹션에서는 오브젝트를 검색하거나 표시하는 데 도움이 되는 IPA 명령을 사용하는 방법을 설명합니다.

4.1. IDM 항목 나열 개요

이 섹션에서는 특정 유형의 IdM 항목을 검색하는 데 도움이 되는 ipa *-find 명령을 설명합니다.

모든 find 명령을 나열하려면 다음 ipa help 명령을 사용하십시오.

```
$ ipa help commands | grep find
```

특정 사용자가 IdM 데이터베이스에 포함되어 있는지 확인해야 합니다. 그런 다음 다음 명령을 사용하여 모든 사용자를 나열할 수 있습니다.

```
$ ipa user-find
```

지정된 속성에 키워드가 포함된 사용자 그룹을 나열하려면 다음을 실행합니다.

```
$ ipa group-find keyword
```

예를 들어 ipa group-find *admin* 명령은 이름 또는 설명이 문자열 admin 이 포함된 모든 그룹을 나열합니다.

```
---------------
3 groups matched
---------------
  Group name: admins
  Description: Account administrators group
  GID: 427200002

  Group name: editors
  Description: Limited admins who can edit other users
  GID: 427200002

  Group name: trust admins
  Description: Trusts administrators group
```

사용자 그룹을 검색할 때 특정 사용자가 포함된 그룹으로 검색 결과를 제한할 수도 있습니다.

```
$ ipa group-find --user=user_name
```

특정 사용자가 포함되지 않은 그룹을 검색하려면 다음을 수행합니다.

```
$ ipa group-find --no-user=user_name
```

4.2. 특정 항목에 대한 세부 정보 표시

ipa *-show 명령을 사용하여 특정 IdM 항목에 대한 세부 정보를 표시합니다.

절차

- *server.example.com* 이라는 호스트에 대한 세부 정보를 표시하려면 다음을 수행하십시오.

```
$ ipa host-show server.example.com

Host name: server.example.com
Principal name: host/server.example.com@EXAMPLE.COM
...
```

4.3. 검색 크기 및 시간 제한 조정

IdM 사용자 목록을 요청하는 등의 일부 쿼리는 매우 많은 항목을 반환할 수 있습니다. 이러한 검색 작업을 튜닝하면 **ipa *-find** 명령(예: **ipa user-find**) 및 해당 목록을 웹 UI에 표시할 때 전체 서버 성능을 향상시킬 수 있습니다.

검색 크기 제한

클라이언트 CLI 또는 IdM 웹 UI에 액세스하는 브라우저에서 서버로 전송되는 요청에 대해 반환되는 최대 항목 수를 정의합니다.

기본값: 100개 항목.

검색 시간 제한

서버가 검색을 실행할 때까지 대기하는 최대 시간(초)을 정의합니다. 검색이 이 제한에 도달하면 서버는 검색을 중지하고 해당 시간에 검색된 항목을 반환합니다.

기본값: 2초.

값을 -1 로 설정하면 검색할 때 IdM에서 제한을 적용하지 않습니다.

중요

검색 크기 또는 시간 제한을 너무 높게 설정하면 서버 성능에 부정적인 영향을 미칠 수 있습니다.

4.3.1. 명령줄에서 검색 크기 및 시간 제한 조정

다음 절차에서는 명령줄에서 검색 크기 및 시간 제한을 조정하는 방법을 설명합니다.

- 전역
- 특정 항목의 경우

절차

1. CLI에서 현재 검색 시간 및 크기 제한을 표시하려면 ipa config-show 명령을 사용합니다.

```
$ ipa config-show

Search time limit: 2
Search size limit: 100
```

2. 모든 쿼리에 대해 전역적으로 제한을 조정하려면 ipa config-mod 명령을 사용하고 --searchrecordslimit 및 --searchtimelimit 옵션을 추가합니다. 예를 들어 다음과 같습니다.

```
$ ipa config-mod --searchrecordslimit=500 --searchtimelimit=5
```

3. 특정 쿼리에 대해서만 제한을 일시적으로 조정하려면 명령에 --sizelimit 또는 --timelimit 옵션을 추가합니다. 예를 들어 다음과 같습니다.

```
$ ipa user-find --sizelimit=200 --timelimit=120
```

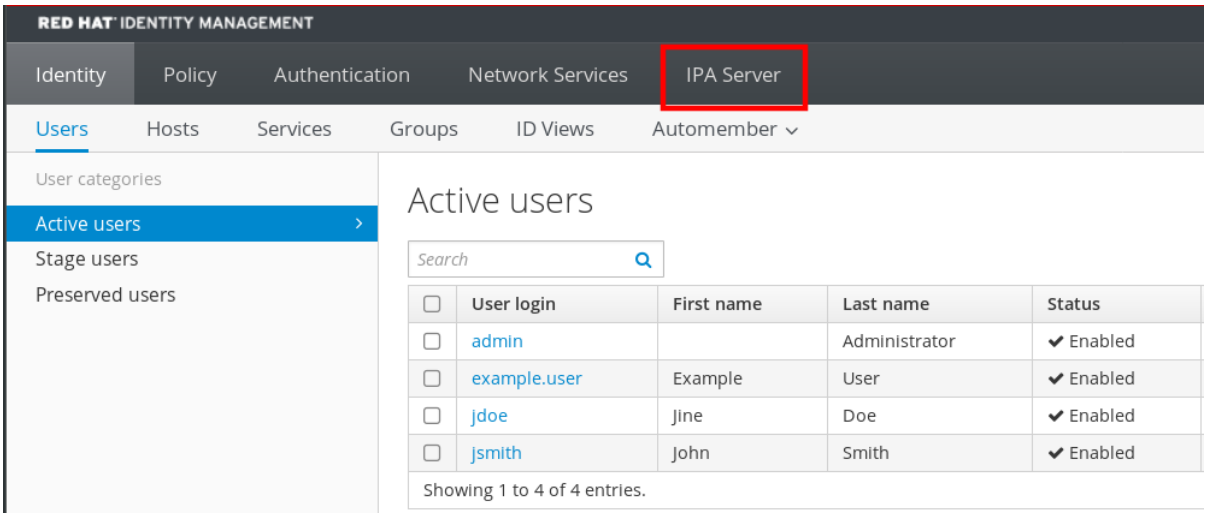
4.3.2. 웹 UI에서 검색 크기 및 시간 제한 조정

다음 절차에서는 IdM 웹 UI에서 글로벌 검색 크기 및 시간 제한을 조정하는 방법을 설명합니다.

절차

1. IdM 웹 UI에 로그인합니다.

2. IPA Server 를 클릭합니다.



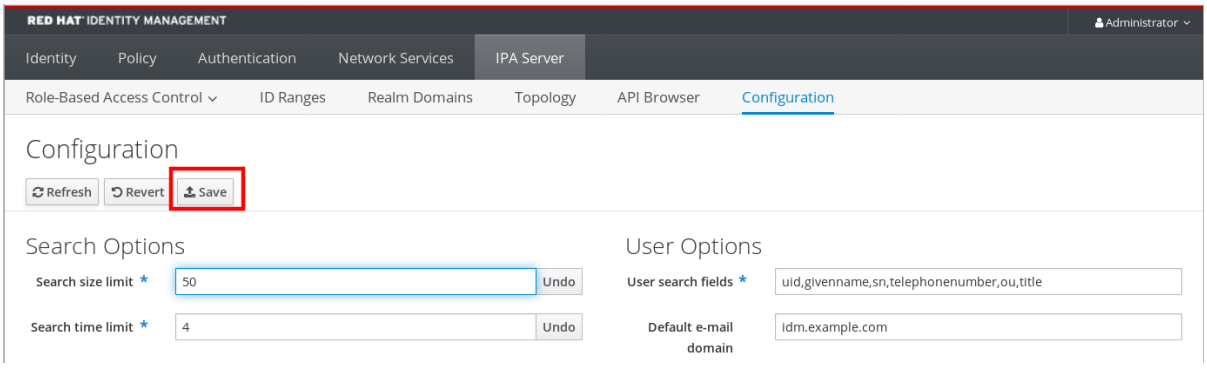
3. IPA 서버 탭에서 구성을 클릭합니다.

4. 검색 옵션 영역에서 필요한 값을 설정합니다.

   기본값은 다음과 같습니다.

   - 검색 크기 제한: 100개 항목
   - 검색 시간 제한: 2 초

5. 페이지 상단에서 저장을 클릭합니다.


RED HAT IDENTITY MANAGEMENT
Administrator
Identity
Policy
Authentication
Network Services
IPA Server
Role-Based Access Control
ID Ranges
Realm Domains
Topology
API Browser
Configuration
Configuration
Refresh
Revert
Save
Search Options
Search size limit *
50
Undo
Search time limit *
4
Undo
User Options
User search fields *
uid,givenname,sn,telephonenumber,ou,title
Default e-mail domain
idm.example.com

5장. 웹 브라우저에서 IDM 웹 UI에 액세스

다음 섹션에서는 IdM(Identity Management) 웹 UI에 대한 개요를 제공하고 여기에 액세스하는 방법을 설명합니다.

5.1. IDM 웹 UI란?

IdM(Identity Management) 웹 UI는 IdM 명령줄 툴에 대한 그래픽 대안인 IdM 관리를 위한 웹 애플리케이션입니다.

IdM 웹 UI에 다음과 같이 액세스할 수 있습니다.

- IdM 사용자: IdM 서버의 사용자에게 부여된 권한에 따라 제한된 작업 세트입니다. 기본적으로 활성 IdM 사용자는 IdM 서버에 로그인하고 자체 계정을 설정할 수 있습니다. 다른 사용자 또는 IdM 서버 설정은 변경할 수 없습니다.
- 관리자: IdM 서버에 대한 모든 액세스 권한
- Active Directory 사용자: 사용자에게 부여된 권한에 따라 작업 세트입니다. Active Directory 사용자는 이제 ID 관리를 위한 관리자가 될 수 있습니다. 자세한 내용은 AD 사용자 활성화에서 IdM 관리를 참조하십시오.

5.2. 웹 UI 액세스에 지원되는 웹 브라우저

IdM(Identity Management)은 웹 UI에 연결하기 위해 다음 브라우저를 지원합니다.

- Mozilla Firefox 38 이상
- Google Chrome 46 이상

참고

브라우저가 **TLS v1.3**을 사용하려고 시도하는 경우 스마트 카드로 **IdM** 웹 **UI**에 액세스하는 데 문제가 있을 수 있습니다.

```
[ssl:error] [pid 125757:tid 140436077168384] [client 999.999.999.999:99999] AH:
verify client post handshake
[ssl:error] [pid 125757:tid 140436077168384] [client 999.999.999.999:99999]
AH10158: cannot perform post-handshake authentication
[ssl:error] [pid 125757:tid 140436077168384] SSL Library Error:
error:14268117:SSL routines:SSL_verify_client_post_handshake:extension not
received
```

이는 최신 버전의 브라우저에 **TLS Post-Handshake Authentication(PHA)**이 기본적으로 활성화되어 있지 않거나 **PHA**를 지원하지 않기 때문입니다. 스마트 카드 인증을 사용하여 **IdM** 웹 **UI**에 액세스하는 경우와 같이 웹 사이트의 일부에만 **TLS** 클라이언트 인증서가 필요한 경우 **PHA**가 필요합니다.

이 문제를 해결하려면 **/etc/httpd/conf.d/ssl.conf** 구성 파일의 **SSLProtocol** 옵션에 **-TLSv1.3** 을 추가하여 **TLS v1.3**을 비활성화합니다.

```
SSLProtocol all -TLSv1 -TLSv1.1 -TLSv1.3
```

IdM은 **ssl.conf** 파일을 관리하며 패키지 업데이트 중에 해당 내용을 덮어쓸 수 있습니다. **IdM** 패키지를 업데이트한 후 사용자 정의 설정을 확인합니다.

5.3. 웹 UI 액세스

다음 절차에서는 **IdM(Identity Management)** 웹 **UI**에 암호를 사용하여 처음 로그인하는 방법을 설명합니다.

첫 번째 로그인 후 다음을 사용하여 인증하도록 **IdM** 서버를 구성할 수 있습니다.

- **Kerberos** 티켓

  자세한 내용은 Identity Management의 Kerberos 인증을 참조하십시오.

- 스마트 카드

자세한 내용은 스마트 카드 인증을 위한 IdM 서버 구성을 참조하십시오.

- 일회성 암호(OTP)는 암호 및 Kerberos 인증과 결합할 수 있습니다.

  자세한 내용은 ID 관리에서 하나의 OTP(암호) 인증을 참조하십시오.

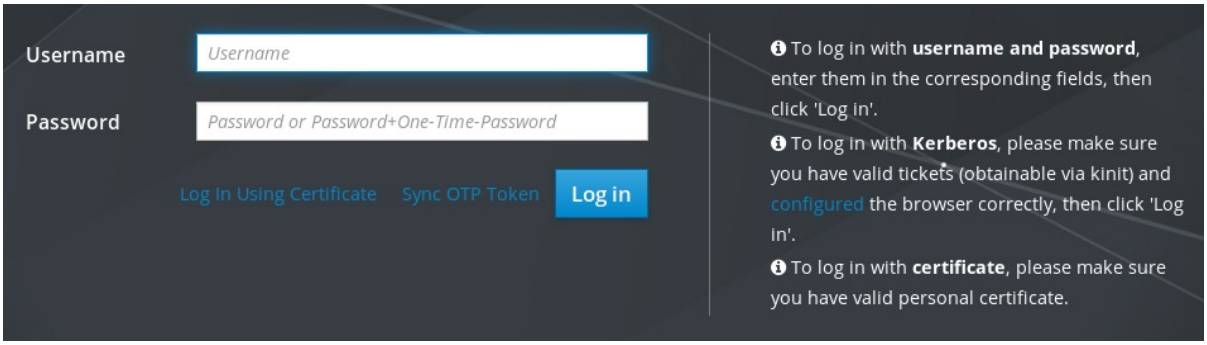
절차

1. IdM 서버 URL을 브라우저 주소 표시줄에 입력합니다. 이름은 다음 예와 유사합니다.

   ```
   https://server.example.com
   ```

   IdM 서버의 DNS 이름을 사용하여 server.example.com 을 변경해야 합니다.

   브라우저에서 IdM 웹 UI 로그인 화면이 열립니다.



- 서버가 응답하지 않거나 로그인 화면이 열려 있지 않으면 연결하는 IdM 서버의 DNS 설정을 확인합니다.

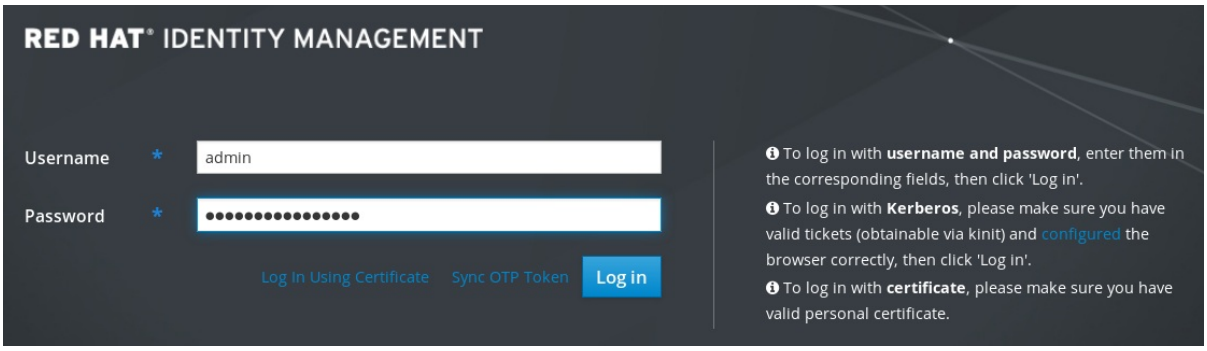
- 자체 서명된 인증서를 사용하는 경우 브라우저에 경고가 발행됩니다. 인증서를 확인하고 로그인을 계속하려면 보안 예외를 수락합니다.

  보안 예외를 방지하려면 인증 기관에서 서명한 인증서를 설치합니다.

2. 웹 UI 로그인 화면에서 IdM 서버 설치 중에 추가한 관리자 계정 자격 증명을 입력합니다.

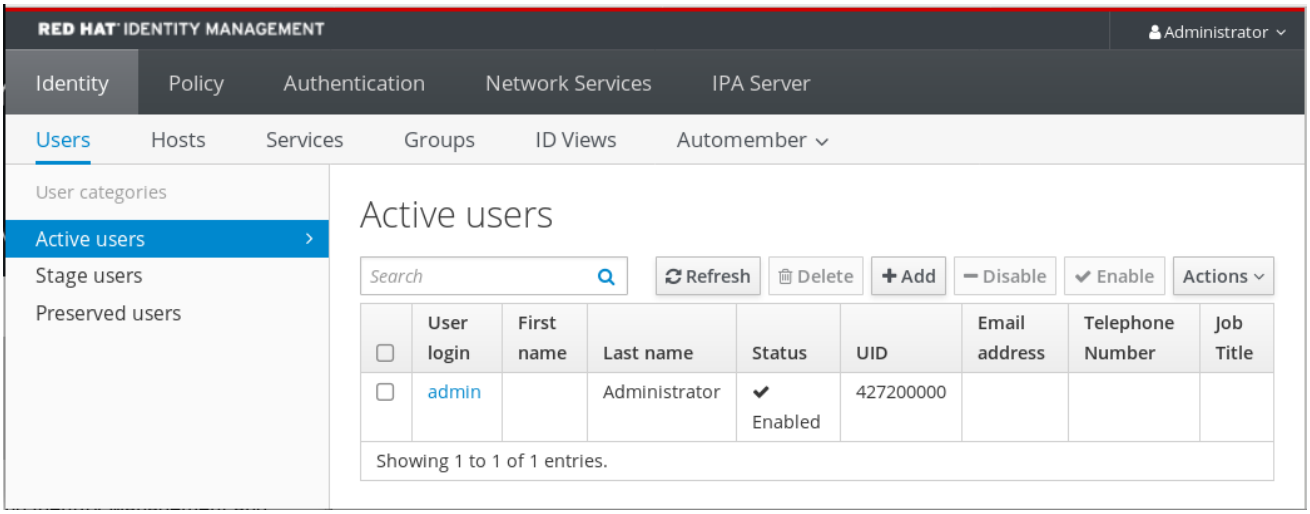
   자세한 내용은 통합 CA가 있는 통합 DNS를 사용하여 ID 관리 서버 설치를 참조하십시오.

   개인 계정 자격 증명을 입력하고 IdM 서버에 이미 입력한 경우에도 입력할 수 있습니다.



3. Log in (로그인)을 클릭합니다.

로그인에 성공하면 IdM 서버 구성을 시작할 수 있습니다.



6장. 웹 UI에서 IDM 로그인: KERBEROS 티켓 사용

다음 섹션에서는 IdM 웹 UI에 Kerberos 로그인을 활성화하고 Kerberos 인증을 사용하여 IdM에 액세스할 수 있는 환경의 초기 구성에 대해 설명합니다.

사전 요구 사항

- 네트워크 환경에 IdM 서버 설치

  자세한 내용은 Red Hat Enterprise Linux 9에 Identity Management설치를 참조하십시오.

6.1. IDENTITY MANAGEMENT의 KERBEROS 인증

IdM(Identity Management)은 Kerberos 프로토콜을 사용하여 SSO(Single Sign-On)를 지원합니다. SSO(Single Sign-On) 인증을 사용하면 올바른 사용자 이름과 암호를 한 번만 제공할 수 있으며, 자격 증명을 다시 입력하지 않고 Identity Management 서비스에 액세스할 수 있습니다.

IdM 서버는 DNS 및 인증서 설정이 올바르게 구성된 경우 설치 직후 Kerberos 인증을 제공합니다. 자세한 내용은 Identity Management 설치를 참조하십시오.

호스트에서 Kerberos 인증을 사용하려면 다음을 설치합니다.

- IdM 클라이언트

  자세한 내용은 시스템 준비에서 ID 관리 클라이언트 설치를 참조하십시오.

- jenkinsfile5conf 패키지

6.2. KINIT 를 사용하여 IDM에 수동으로 로그인

이 절차에서는 kinit 유틸리티를 사용하여 IdM(Identity Management) 환경에 수동으로 인증하는 방법을 설명합니다. kinit 유틸리티는 IdM 사용자를 대신하여 Kerberos 티켓(TGT)을 가져오고 캐시합니다.

참고

초기 **Kerberos TGT**를 제거했거나 만료된 경우에만 이 절차를 사용하십시오. **IdM** 사용자는 로컬 시스템에 로그인할 때 **IdM**에 자동으로 로그인됩니다. 즉, 로그인 후 **kinit** 유틸리티를 사용하여 **IdM** 리소스에 액세스할 필요가 없습니다.

절차

1. **IdM**에 로그인

- 로컬 시스템에 현재 로그인한 사용자의 사용자 이름에서 사용자 이름을 지정하지 않고 **kinit** 를 사용합니다. 예를 들어 로컬 시스템에서 **example_user** 로 로그인한 경우:

```
[example_user@server ~]$ kinit
Password for example_user@EXAMPLE.COM:
[example_user@server ~]$
```

로컬 사용자의 사용자 이름이 **IdM**의 사용자 항목과 일치하지 않으면 인증 시도에 실패합니다.

```
[example_user@server ~]$ kinit
kinit: Client 'example_user@EXAMPLE.COM' not found in Kerberos database
while getting initial credentials
```

- 로컬 사용자 이름에 일치하지 않는 **Kerberos** 사용자 이름을 사용하여 필요한 사용자 이름을 **kinit** 유틸리티에 전달합니다. 예를 들어 **admin** 사용자로 로그인하려면 다음을 수행합니다.

```
[example_user@server ~]$ kinit admin
Password for admin@EXAMPLE.COM:
[example_user@server ~]$
```

2. 선택적으로 로그인에 성공했는지 확인하려면 **klist** 유틸리티를 사용하여 캐시된 **TGT**를 표시합니다. 다음 예에서 캐시에는 **example_user** 주체의 티켓이 포함되어 있습니다. 즉, 이 특정 호스트에서만 **example_user** 만 **IdM** 서비스에 액세스할 수 있습니다.

```
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: example_user@EXAMPLE.COM

Valid starting     Expires            Service principal
11/10/2019 08:35:45  11/10/2019 18:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

6.3. KERBEROS 인증을 위한 브라우저 구성

Kerberos 티켓으로 인증을 활성화하려면 브라우저 구성이 필요할 수 있습니다.

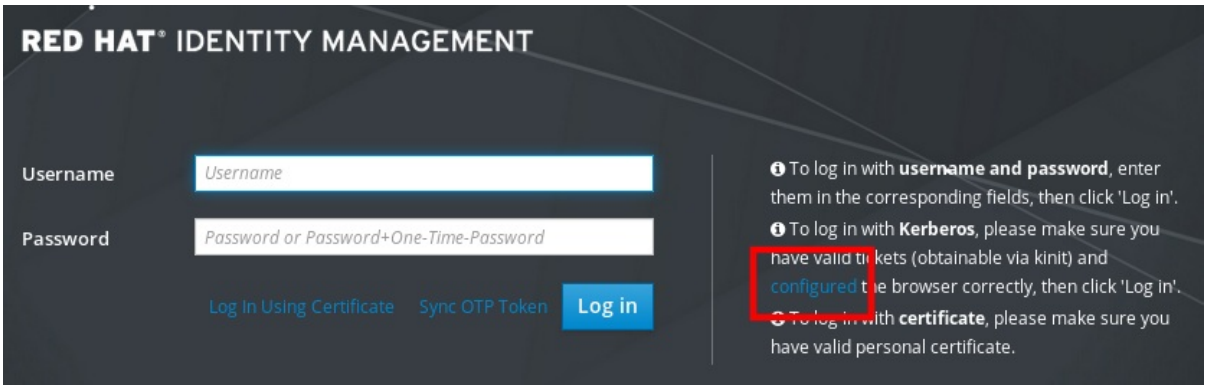
다음 단계에서는 **IdM** 도메인 액세스에 대한 **Kerberos** 협상을 지원하는 데 도움이 됩니다.

각 브라우저는 **Kerberos**를 다른 방식으로 지원하며 다른 설정이 필요합니다. **IdM** 웹 **UI**에는 다음 브라우저에 대한 지침이 포함되어 있습니다.

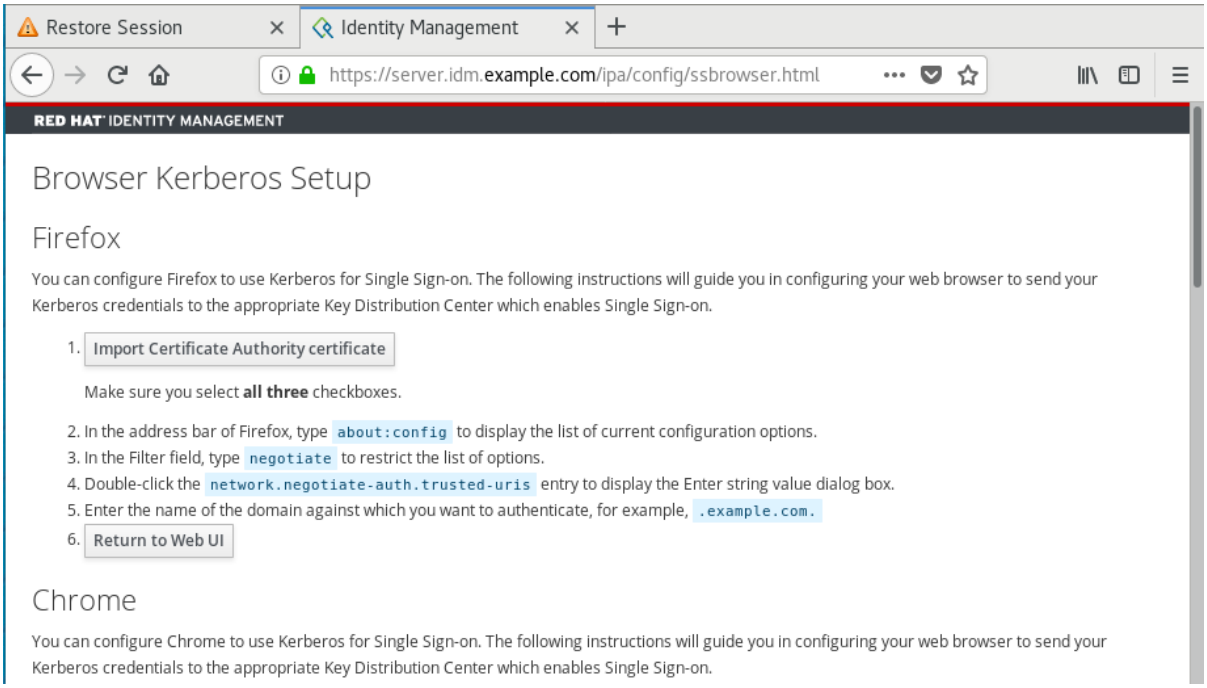
- **Firefox**
- **Chrome**

절차

1. 웹 브라우저에서 **IdM** 웹 **UI** 로그인 대화 상자를 엽니다.
2. 웹 **UI** 로그인 화면에서 브라우저 구성 링크를 클릭합니다.



3. 구성 페이지의 단계를 따릅니다.



설정 후 **IdM** 웹 **UI**로 돌아가서 로그인 을 클릭합니다.

6.4. KERBEROS 티켓을 사용하여 웹 UI에 로그인

이 절차에서는 **Kerberos ticket-granting** 티켓(**TGT**)을 사용하여 **IdM** 웹 **UI**에 로그인하는 방법을 설명합니다.

TGT는 사전 정의된 시간에 만료됩니다. 기본 시간 간격은 **24**시간이며 **IdM** 웹 **UI**에서 변경할 수 있습니다.

시간 간격이 만료된 후 티켓을 갱신해야 합니다.

- **kinit** 명령 사용.
- 웹 **UI** 로그인 대화 상자에서 **IdM** 로그인 자격 증명 사용.

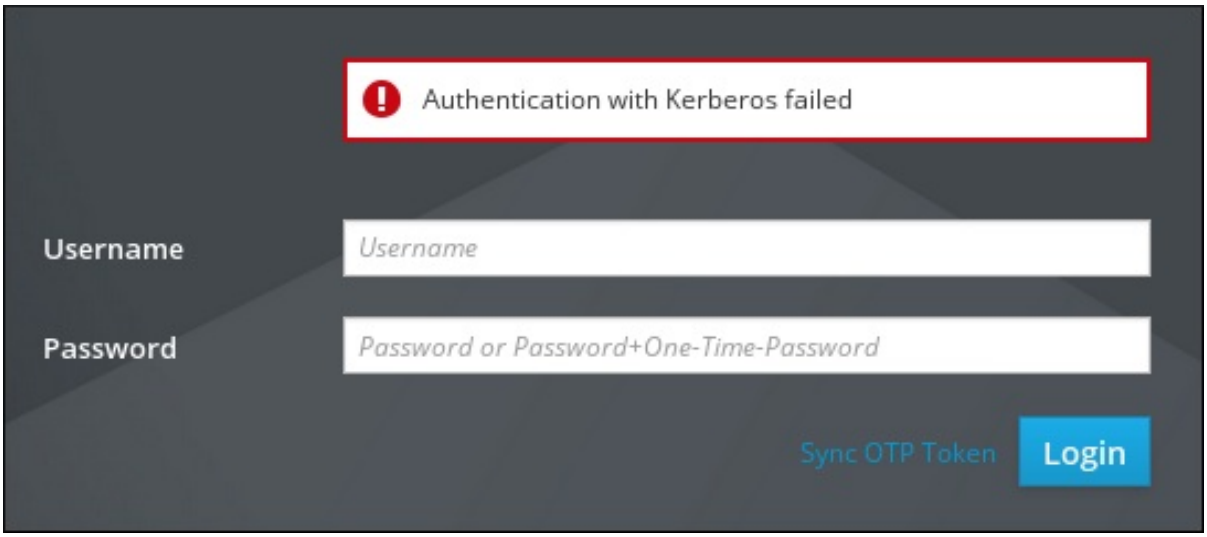
절차

- **IdM** 웹 **UI**를 엽니다.

Kerberos 인증이 올바르게 작동하고 유효한 티켓이 있으면 자동으로 인증되고 웹 UI가 열립니다.

티켓이 만료된 경우 먼저 자격 증명으로 인증해야 합니다. 그러나 다음에 IdM 웹 UI가 로그인 대화 상자를 열지 않고 자동으로 열립니다.

Kerberos 인증을 사용한 오류 메시지가 표시되면 브라우저가 Kerberos 인증을 위해 구성되었는지 확인합니다. Kerberos 인증을 위한 브라우저 구성을 참조하십시오.



6.5. KERBEROS 인증을 위한 외부 시스템 구성

이 섹션에서는 IdM(Identity Management) 사용자가 Kerberos 자격 증명을 사용하여 외부 시스템에서 IdM에 로그인할 수 있도록 외부 시스템을 구성하는 방법을 설명합니다.

외부 시스템에서 Kerberos 인증을 활성화하면 인프라에 여러 영역 또는 겹치는 도메인이 포함된 경우 특히 유용합니다. ipa-client-install 을 통해 시스템이 IdM 도메인에 등록되지 않은 경우에도 유용합니다.

IdM 도메인의 멤버가 아닌 시스템에서 IdM에 Kerberos 인증을 활성화하려면 외부 시스템에 IdM 관련 Kerberos 구성 파일을 정의합니다.

사전 요구 사항

- jenkinsfile5-tekton 패키지가 외부 시스템에 설치되어 있습니다.

  패키지가 설치되었는지 확인하려면 다음 CLI 명령을 사용하십시오.

```
# dnf list installed krb5-workstation
Installed Packages
krb5-workstation.x86_64    1.16.1-19.el8    @BaseOS
```

절차

1. IdM 서버의 /etc/krb5.conf 파일을 외부 시스템으로 복사합니다. 예를 들어 다음과 같습니다.

```
# scp /etc/krb5.conf root@externalsystem.example.com:/etc/krb5_ipa.conf
```

> 주의
>
> 외부 시스템의 기존 jenkinsfile 5.conf 파일을 덮어쓰지 마십시오.

2. 외부 시스템에서 복사된 IdM Kerberos 구성 파일을 사용하도록 터미널 세션을 설정합니다.

```
$ export KRB5_CONFIG=/etc/krb5_ipa.conf
```

KRB5_CONFIG 변수는 로그아웃할 때까지 일시적으로 존재합니다. 이러한 손실을 방지하려면 다른 파일 이름으로 변수를 내보냅니다.

3. /etc/krb5.conf.d/ 디렉터리에서 외부 시스템으로 Kerberos 구성 스니펫을 복사합니다.

4. Kerberos 인증에 대한 브라우저 구성에 설명된 대로 외부 시스템에서 브라우저를 구성합니다.

외부 시스템의 사용자는 kinit 유틸리티를 사용하여 IdM 서버에 인증할 수 있습니다.

6.6. ACTIVE DIRECTORY 사용자를 위한 웹 UI 로그인

Active Directory 사용자에 대해 웹 UI 로그인을 사용하도록 설정하려면 Default Trust View 에서 각 Active Directory 사용자에 대한 ID 재정의를 정의합니다. 예를 들어 다음과 같습니다.

-

```
[admin@server ~]$ ipa idoverrideuser-add 'Default Trust View' ad_user@ad.example.com
```

추가 리소스

- Active Directory 사용자에 ID 보기 사용

7장. 한 번 암호를 사용하여 ID 관리 웹 UI에 로그인

IdM 웹 UI에 대한 액세스는 여러 방법을 사용하여 보호할 수 있습니다. 기본 인증은 암호 인증입니다.

암호 인증의 보안을 높이기 위해 두 번째 단계를 추가하고 자동으로 생성된 일회용 암호(OTP)가 필요할 수 있습니다. 가장 일반적인 사용은 사용자 계정과 연결된 암호를 결합하고 하드웨어 또는 소프트웨어 토큰에 의해 생성된 시간 제한 암호를 결합하는 것입니다.

다음 섹션은 다음을 수행하는 데 도움이 됩니다.

- IdM에서 OTP 인증이 작동하는 방식을 알아보십시오.
- IdM 서버에서 OTP 인증을 구성합니다.
- OTP 토큰을 만들고 휴대폰의 FreeOTP 앱과 동기화합니다.
- 사용자 암호와 일회성 암호 조합을 사용하여 IdM 웹 UI에 인증합니다.
- 웹 UI에서 토큰을 다시 동기화합니다.

7.1. 사전 요구 사항

- 웹 브라우저에서 IdM 웹 UI에 액세스

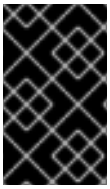
7.2. ID 관리에서 한 번만 암호(OTP) 인증

일회성 암호는 인증 보안에 대한 추가 단계를 제공합니다. 인증은 비밀번호 + 자동으로 생성된 암호를 사용합니다.

한 번에 암호를 생성하려면 하드웨어 또는 소프트웨어 토큰을 사용할 수 있습니다. IdM은 소프트웨어 및 하드웨어 토큰을 모두 지원합니다.

Identity Management는 다음과 같은 두 가지 표준 OTP 메커니즘을 지원합니다.

- HMAC-Based One-Time Password (HOTP) 알고리즘은 카운터를 기반으로 합니다. HMAC는 해시된 메시지 인증 코드입니다.
- TOTP(Time-Based One-Time Password) 알고리즘은 시간 기반 이동 요소를 지원하기 위한 octetsP의 확장입니다.



중요

IdM은 Active Directory 트러스트 사용자를 위한 OTP 로그인을 지원하지 않습니다.

7.3. 웹 UI에서 한 번만 암호 활성화

IdM 웹 UI를 사용하면 하드웨어 또는 소프트웨어 장치를 구성하여 일회성 암호를 생성할 수 있습니다.

로그인 대화 상자의 전용 필드의 일반적인 암호 바로 뒤에 한 번 암호를 입력합니다.

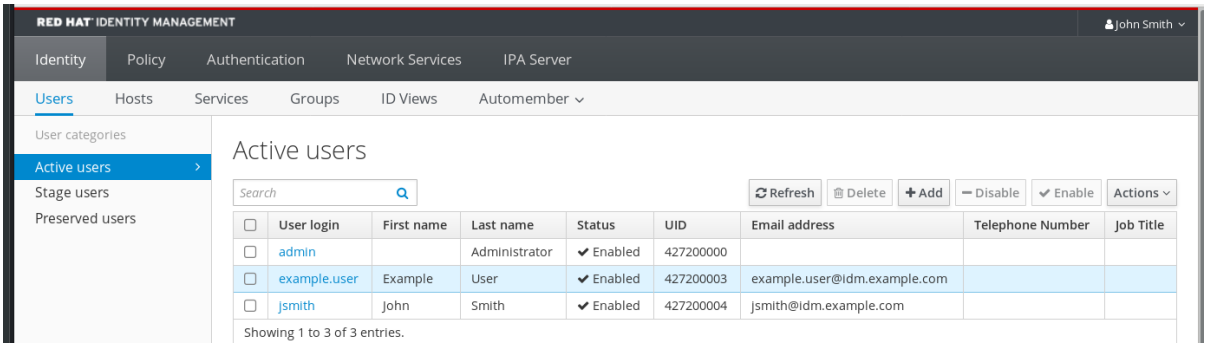
관리자만 사용자 설정에서 OTP 인증을 활성화할 수 있습니다.

사전 요구 사항

- 관리 권한

절차

1. 사용자 이름과 암호를 사용하여 IdM 웹 UI에 로그인합니다.
2. Identity → 사용자 → 활성 사용자 탭을 엽니다.



3. 사용자 이름을 클릭하여 사용자 설정을 엽니다.

4. 사용자 인증 유형에서 두 가지 인증 (암호 + OTP) 을 선택합니다.

5. 저장을 클릭합니다.

이 시점에서 OTP 인증이 IdM 서버에서 활성화됩니다.

이제 사용자 또는 사용자가 새 토큰 ID를 사용자 계정에 할당해야 합니다.

7.4. 웹 UI에 OTP 토큰 추가

다음 섹션에서는 IdM 웹 UI 및 소프트웨어 토큰 생성기에 토큰을 추가하는 데 도움이 됩니다.

사전 요구 사항

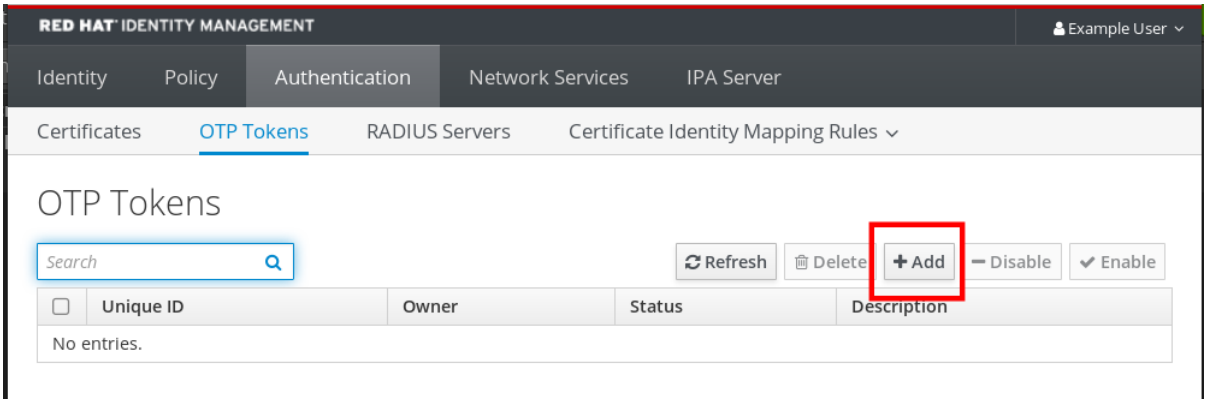
- IdM 서버의 활성 사용자 계정.
- 관리자가 IdM 웹 UI의 특정 사용자 계정에 대해 OTP를 활성화했습니다.
- OTP 토큰을 생성하는 소프트웨어 장치(예: FreeOTP).

절차

1. 사용자 이름 및 암호를 사용하여 **IdM** 웹 **UI**에 로그인합니다.

2. 휴대폰에서 토큰을 만들려면 인증 → **OTP** 토큰 탭을 엽니다.

3. 추가를 클릭합니다.



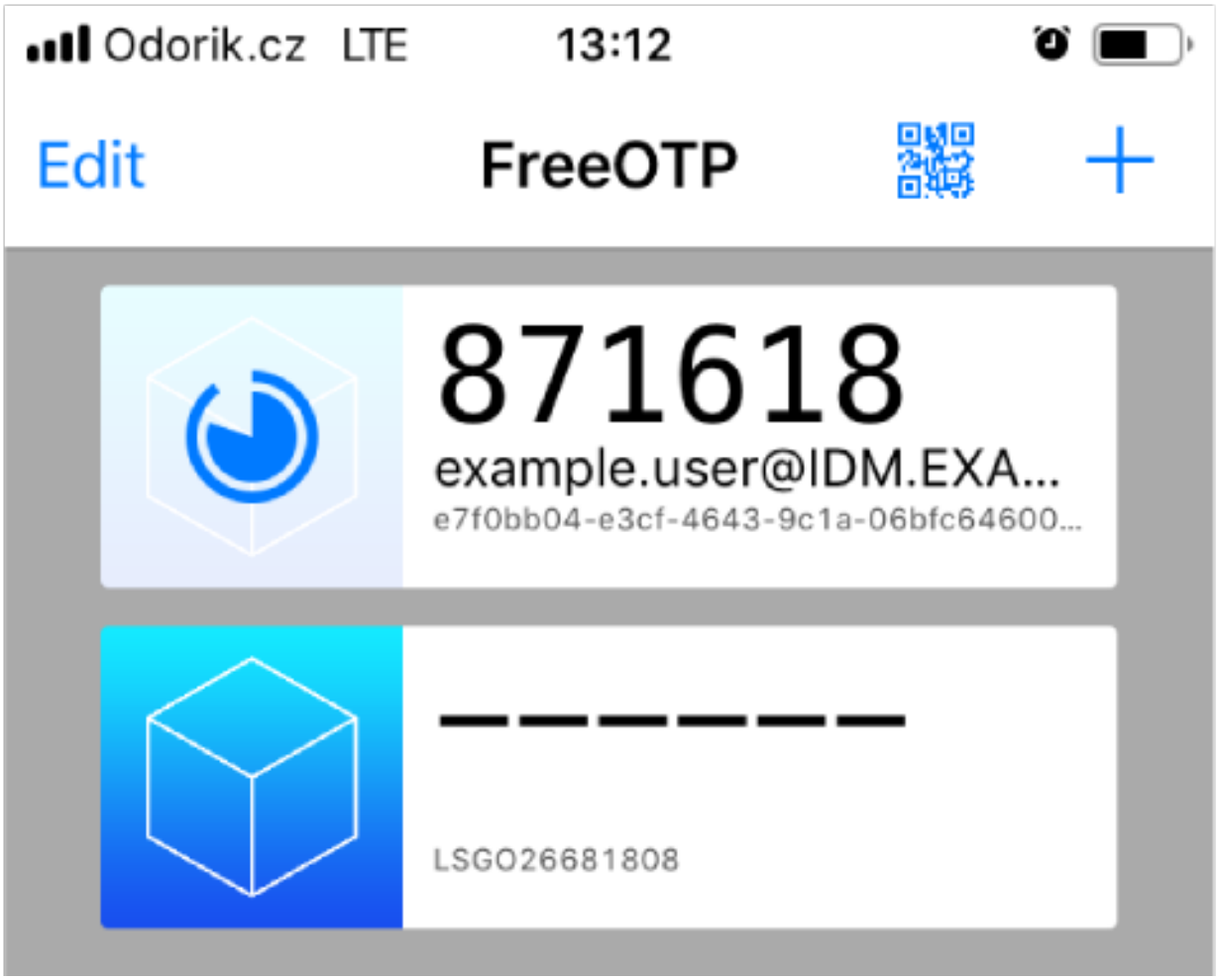
4. **OTP** 토큰 추가 대화 상자에서 모든 항목을 채우지 않고 추가를 클릭합니다.

   이 단계에서 **IdM** 서버는 서버에 기본 매개변수가 포함된 토큰을 생성하고 **QR** 코드가 있는 페이지를 엽니다.

5. **QR** 코드를 휴대폰에 복사합니다.

6. 확인 을 클릭하여 **QR** 코드를 닫습니다.

이제 한 번 암호를 생성하고 **IdM** 웹 **UI**에 로그인할 수 있습니다.



7.5. 한 번에 웹 UI에 로그인

이 절차에서는 한 번 OTP(암호)를 사용하여 IdM 웹 UI에 처음 로그인하는 방법을 설명합니다.

사전 요구 사항

- OTP 인증에 사용 중인 사용자 계정의 ID 관리 서버에서 OTP 구성이 활성화됩니다. 관리자는 또한 사용자가 OTP를 활성화할 수 있습니다.

  OTP 구성을 활성화하려면 웹 UI에서 한 번 암호 활성화를 참조하십시오.

- OTP 토큰을 생성하는 하드웨어 또는 소프트웨어 장치.

절차

1. ID 관리 로그인 화면에서 사용자 이름 또는 IdM 서버 관리자 계정의 사용자 이름을 입력합니

다.

2. 위에 입력한 사용자 이름의 암호를 추가합니다.

3. 장치에서 한 번 암호를 생성합니다.

4. 암호 바로 뒤에 공백 없이 암호를 입력합니다.

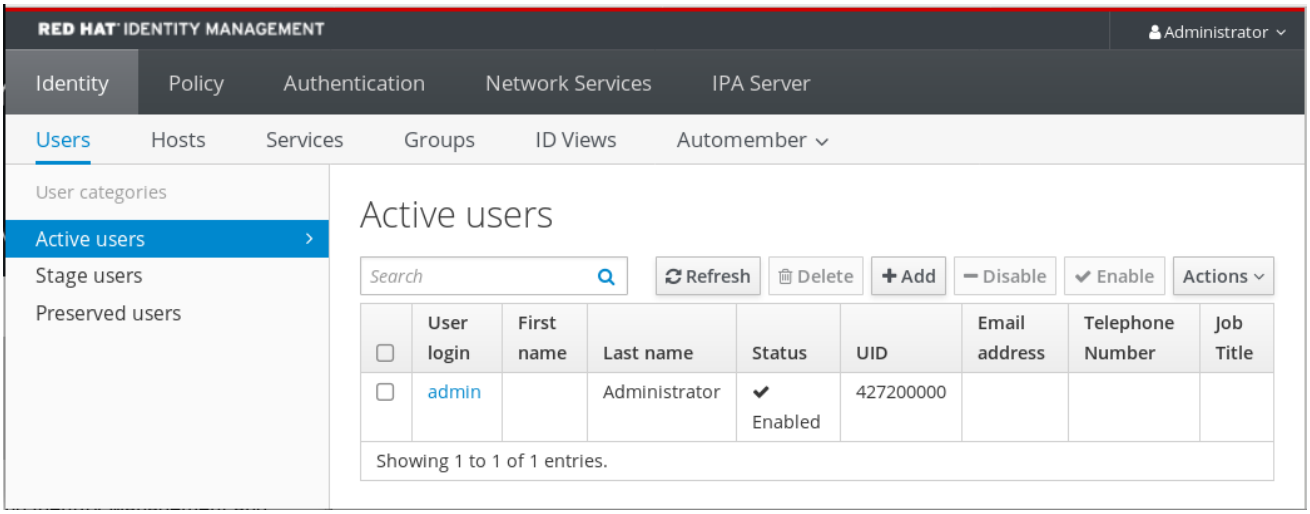
5. **Log in** (로그인)을 클릭합니다.

인증에 실패하면 **OTP** 토큰을 동기화합니다.

CA에서 자체 서명된 인증서를 사용하는 경우 브라우저에 경고를 발행합니다. 인증서를 확인하고 로그인을 계속하려면 보안 예외를 수락합니다.

IdM 웹 **UI**가 열려 있지 않으면 **ID** 관리 서버의 **DNS** 구성을 확인합니다.

로그인에 성공하면 **IdM** 웹 **UI**가 표시됩니다.



7.6. 웹 UI를 사용하여 OTP 토큰 동기화

OTP(One Time Password)로 로그인에 실패하면 **OTP** 토큰이 올바르게 동기화되지 않습니다.

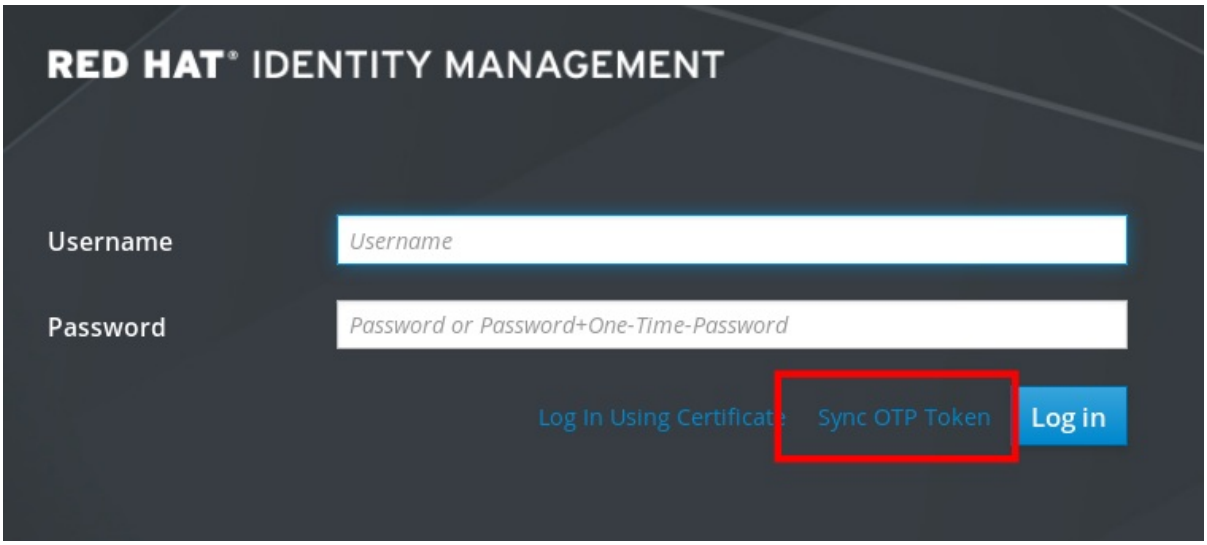
다음 텍스트에서는 토큰 재동기화에 대해 설명합니다.

사전 요구 사항

- 로그인 화면이 열립니다.
- **OTP** 토큰을 생성하는 장치는 구성되어 있습니다.

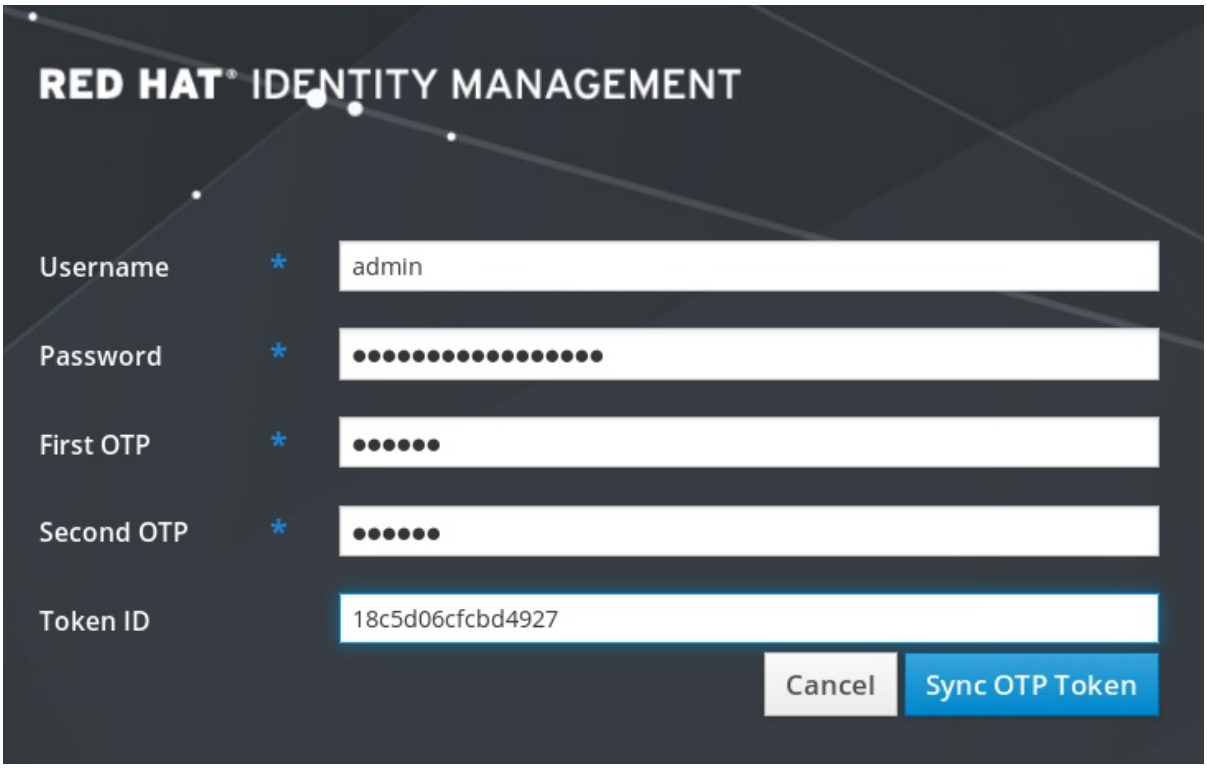
절차

1. **IdM** 웹 **UI** 로그인 화면에서 **OTP** 토큰 동기화 를 클릭합니다.



2. 로그인 화면에서 사용자 이름과 **ID** 관리 암호를 입력합니다.
3. 한 번 암호를 생성하고 **First OTP** 필드에 입력합니다.
4. 한 번 다른 비밀번호를 생성하고 **Second OTP** 필드에 입력합니다.

5. 필요한 경우 토큰 **ID**를 입력합니다.



6. **Sync OTP Token (OTP** 토큰 동기화)을 클릭합니다.

동기화에 성공하면 **IdM** 서버에 로그인할 수 있습니다.

7.7. 만료된 암호 변경

Identity Management 관리자는 다음 로그인 시 암호를 변경해야 할 수 있습니다. 암호를 변경할 때까지 **IdM** 웹 **UI**에 성공적으로 로그인할 수 없음을 의미합니다.

비밀번호 만료는 웹 **UI**에 처음 로그인하는 동안 발생할 수 있습니다.

만료 암호 대화 상자가 나타나면 절차의 지침을 따르십시오.

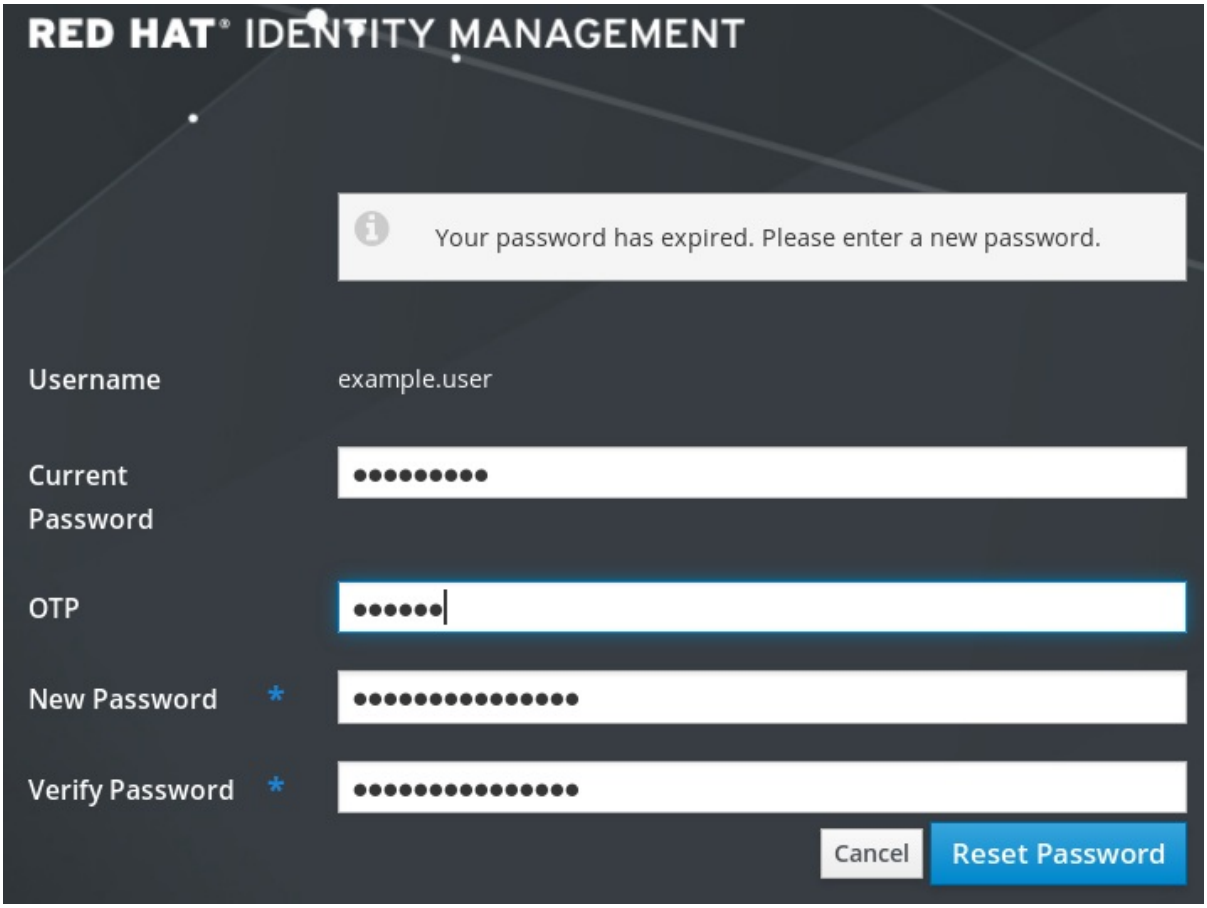
사전 요구 사항

- 로그인 화면이 열립니다.
- IdM 서버에 대한 활성 계정입니다.

절차

1. 암호 만료 로그인 화면에서 사용자 이름을 입력합니다.
2. 위에 입력한 사용자 이름의 암호를 추가합니다.
3. OTP 필드에서 암호 인증을 한 번 사용하는 경우 한 번 암호를 생성합니다.

   OTP 인증을 활성화하지 않은 경우 필드를 비워 둡니다.
4. 확인을 위해 새 암호를 두 번 입력합니다.
5. 암호 재설정 을 클릭합니다.



암호가 성공적으로 변경되면 일반적인 로그인 대화 상자가 표시됩니다. 새 암호로 로그인합니다.

8장. IDM 로그 파일 및 디렉터리

다음 섹션을 사용하여 IdM(Identity Management)의 개별 구성 요소를 모니터링, 분석 및 문제를 해결합니다.

- LDAP
- Apache 웹 서버
- 인증서 시스템
- Kerberos
- DNS
- custodia

또한 IdM 서버와 클라이언트를 모니터링, 분석 및 해결하고 IdM 서버에서 감사 로깅을 활성화할 수 있습니다.

8.1. IDM 서버 및 클라이언트 로그 파일 및 디렉터리

다음 표에서는 IdM(Identity Management) 서버 및 클라이언트가 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다. 파일과 디렉터리를 사용하여 설치 오류 문제를 해결할 수 있습니다.

디렉토리 또는 파일	설명
/var/log/ipaserver-install.log	IdM 서버의 설치 로그입니다.
/var/log/ipareplica-install.log	IdM 복제본의 설치 로그입니다.
/var/log/ipaclient-install.log	IdM 클라이언트의 설치 로그입니다.
/var/log/sssd/	SSSD의 로그 파일입니다. sssd.conf 파일 또는 sssctl 명령을 사용하여 SSSD에 대한 세부 로깅을 활성화할 수 있습니다.

디렉토리 또는 파일	설명
~/.ipa/log/cli.log	원격 프로시저 호출(RPC)에서 반환된 오류에 대한 로그 파일이며 **ipa** 유틸리티에서 응답합니다. 도구를 실행하는**유효한 사용자를** 위해 홈 디렉터리에 생성됩니다. 이 사용자는 실패한 **ipa** 명령을 수행하기 전에 TGT(티켓 부여 티켓)의 IdM 사용자 이름과 다른 사용자 이름이 있을 수 있습니다. 예를 들어 시스템에 **root** 로 로그인하고 IdM **관리자** TGT를 가져온 경우**/root/.ipa/log/cli.log** 파일에 오류가 기록됩니다.
/etc/logrotate.d/	DNS, SSSD, Apache, Tomcat 및 Kerberos에 대한 로그 회전 정책입니다.
/etc/pki/pki-tomcat/logging.properties	이 링크는 **/usr/share/pki/server/conf/logging.properties** 에서 기본 인증 기관 로깅 구성을 가리킵니다.

추가 리소스

- IdM 서버 설치 문제 해결
- IdM 클라이언트 설치 문제 해결
- IdM 복제본 설치 문제 해결
- IdM에서 SSSD를 사용한 인증 문제 해결

8.2. DIRECTORY SERVER 로그 파일

다음 표에서는 IdM(Identity Management) 디렉터리 서버(DS) 인스턴스에서 로그 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다. 파일과 디렉터리를 사용하여 DS 관련 문제를 해결할 수 있습니다.

표 8.1. Directory Server 로그 파일

디렉터리 또는 파일	설명
/var/log/dirsrv/slapd-*REALM_NAME*/	IdM 서버에서 사용하는 DS 인스턴스와 관련된 파일을 기록합니다. 여기에 기록된 대부분의 작동 데이터는 server-replica 상호 작용과 관련이 있습니다.
/var/log/dirsrv/slapd-*REALM_NAME*/audit	DS 구성에서 감사가 활성화된 경우 모든 DS 작업에 대한 감사 추적을 포함합니다.

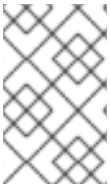
디렉터리 또는 파일	설명
/var/log/dirsrv/slapd-*REALM_NAME*/access	도메인 DS 인스턴스에 대해 시도된 액세스 및 실패한 작업에 대한 자세한 정보를 포함합니다.
/var/log/dirsrv/slapd-*REALM_NAME*/errors	

추가 리소스

- 서버 및 데이터베이스 활동 모니터링
- 로그 파일 참조

8.3. IDM 서버에서 감사 로깅 활성화

다음 절차에서는 감사 목적으로 IdM(Identity Management) 서버에서 로깅을 활성화하는 방법을 설명합니다. 자세한 로그를 사용하여 데이터를 모니터링하고 문제를 해결하며 네트워크에서 의심 스러운 활동을 검사할 수 있습니다.



참고

LDAP 서비스가 로깅된 경우 특히 값이 큰 경우 LDAP 서비스가 느려질 수 있습니다.

사전 요구 사항

- 디렉터리 관리자 암호

절차

1. LDAP 서버에 바인딩합니다.

```
$ ldapmodify -D "cn=Directory Manager" -W << EOF
```

2. [Enter]를 누릅니다.

3. 다음과 같이 수행할 모든 수정 사항을 지정합니다.

```
dn: cn=config
changetype: modify
replace: nsslapd-auditlog-logging-enabled
nsslapd-auditlog-logging-enabled: on
-
replace:nsslapd-auditlog
nsslapd-auditlog: /var/log/dirsrv/slapd-REALM_NAME/audit
-
replace:nsslapd-auditlog-mode
nsslapd-auditlog-mode: 600
-
replace:nsslapd-auditlog-maxlogsize
nsslapd-auditlog-maxlogsize: 100
-
replace:nsslapd-auditlog-logrotationtime
nsslapd-auditlog-logrotationtime: 1
-
replace:nsslapd-auditlog-logrotationtimeunit
nsslapd-auditlog-logrotationtimeunit: day
```

4. 새 줄에 **EOF** 를 입력하여 **ldapmodify** 명령의 끝을 나타냅니다.

5. **[추가]**를 두 번 누릅니다.

6. 감사 로깅을 활성화하려는 다른 모든 **IdM** 서버에서 이전 단계를 반복합니다.

검증

- **/var/log/dirsrv/slapd-REALM_NAME/audit** 파일을 엽니다.

```
389-Directory/1.4.3.231 B2021.322.1803
server.idm.example.com:636 (/etc/dirsrv/slapd-IDM-EXAMPLE-COM)

time: 20220607102705
dn: cn=config
result: 0
changetype: modify
replace: nsslapd-auditlog-logging-enabled
nsslapd-auditlog-logging-enabled: on
[...]
```

파일이 더 이상 비어 있지 않기 때문에 감사가 활성화되었는지 확인합니다.

중요

시스템은 변경을 수행하는 항목의 바인딩된 LDAP 고유 이름(DN)을 기록합니다. 따라서 로그를 사후 처리해야 할 수 있습니다. 예를 들어 IdM Directory Server에서는 레코드를 수정한 AD 사용자의 ID를 나타내는 ID 덮어쓰기 DN입니다.

```
$ modifiersName: ipaanchoruuid=:sid:s-1-5-21-19610888-1443184010-
1631745340-279100,cn=default trust
view,cn=views,cn=accounts,dc=idma,dc=idm,dc=example,dc=com
```

pysss_nss_idmap.getnamebysid Python 명령을 사용하여 사용자 SID가 있는 경우 AD 사용자를 조회합니다.

```
>>> import pysss_nss_idmap
>>> pysss_nss_idmap.getnamebysid('S-1-5-21-1273159419-3736181166-
4190138427-500'))
{'S-1-5-21-1273159419-3736181166-4190138427-500': {'name':
'administrator@ad.vm', 'type': 3}}
```

추가 리소스

- Directory Server 로그 파일
- IPA/IDM Server 및 Replica Servers KCS 솔루션에 감사 로깅을 활성화하는 방법

8.4. IDM APACHE 서버 로그 파일

다음 표에서는 IdM(Identity Management) Apache 서버가 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다.

표 8.2. Apache Server 로그 파일

디렉토리 또는 파일	설명
/var/log/httpd/	Apache 웹 서버의 로그 파일입니다.

디렉토리 또는 파일	설명
/var/log/httpd/access_log	Apache 서버의 표준 액세스 및 오류 로그. IdM 웹 UI 및 RPC 명령줄 인터페이스에서 Apache를 사용하므로 IdM 관련 메시지는 Apache 메시지와 함께 기록됩니다. 액세스 로그는 주로 사용자 보안 주체 및 사용되는 URI만 로그이며 종종 RPC 끝점입니다. 오류 로그에는 IdM 서버 로그가 포함되어 있습니다.
/var/log/httpd/error_log	

추가 리소스

- **Apache 문서의** 파일 로그

8.5. IDM의 인증서 시스템 로그 파일

다음 표에서는 IdM(Identity Management) 인증서 시스템이 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다.

표 8.3. 인증서 시스템 로그 파일

디렉토리 또는 파일	설명
/var/log/pki/pki-ca-spawn.*time_of_installation*.log	IdM CA(인증 기관)의 설치 로그입니다.
/var/log/pki/pki-kra-spawn.*time_of_installation*.log	IdM KMS(Key recovery Authority)에 대한 설치 로그입니다.
/var/log/pki/pki-tomcat/	PKI 작업 로그의 최상위 디렉터리입니다. CA 및 KRA 로그를 포함합니다.
/var/log/pki/pki-tomcat/ca/	인증서 작업과 관련된 로그가 있는 디렉터리입니다. IdM에서 이러한 로그는 인증서를 사용하는 서비스 주체, 호스트 및 기타 엔터티에 사용됩니다.
/var/log/pki/pki-tomcat/kra	KRA와 관련된 로그가 있는 디렉터리입니다.
/var/log/messages	다른 시스템 메시지 사이에 인증서 오류 메시지가 포함됩니다.

추가 리소스

- **Red Hat Certificate System** *관리 가이드에서* 하위 시스템 로그 구성

8.6. IDM의 KERBEROS 로그 파일

다음 표에서는 Kerberos가 IdM(Identity Management)에서 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다.

표 8.4. Kerberos 로그 파일

디렉토리 또는 파일	설명
/var/log/krb5kdc.log	Kerberos NetNamespace 서버의 기본 로그 파일입니다.
/var/log/kadmind.log	Kerberos 관리 서버의 기본 로그 파일입니다.
이러한 파일의 위치는 jenkinsfile **5.conf** 파일에서 구성됩니다. 일부 시스템에서는 다를 수 있습니다.	

8.7. IDM의 DNS 로그 파일

다음 표에서는 DNS가 IdM(Identity Management)에서 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다.

표 8.5. DNS 로그 파일

디렉토리 또는 파일	설명
/var/log/messages	DNS 오류 메시지 및 기타 시스템 메시지가 포함됩니다. 이 파일의 DNS 로깅은 기본적으로 활성화되어 있지 않습니다. 이를 활성화하려면 **# /usr/sbin/rndc querylog** 명령을 입력합니다. 이 명령을 실행하면 다음 행이**var/log/data** bind에 추가됩니다. **6월 26 17:37:33 r8server named-pkcs11[1445]: 컨트롤 채널 명령 'querylog'** **6월 26 17:37:33 r8server named-pkcs11[1445]: 쿼리 로깅이 이제 시작되었습니다.** 로깅을 비활성화하려면 명령을 다시 실행합니다.

8.8. IDM의 CUSTODIA 로그 파일

다음 표에서는 Custodia가 IdM(Identity Management)에서 정보를 기록하는 데 사용하는 디렉터리 및 파일을 제공합니다.

표 8.6. custodia 로그 파일

디렉토리 또는 파일	설명
/var/log/custodia/	Custodia 서비스의 로그 파일 디렉터리입니다.

8.9. 추가 리소스

- 로그 파일 보기. **journalctl** 을 사용하여 **systemd** 장치 파일의 로깅 출력을 볼 수 있습니다.