Red Hat Directory Server 12

Red Hat Directory Server 설치

Directory Server 설치, 업데이트 및 제거를 관리하는 방법 인스턴스 작업을 시작하는 데 필요한 기본 작업

Last Updated: 2024-08-25

Red Hat Directory Server 12 Red Hat Directory Server 설치

Directory Server 설치, 업데이트 및 제거를 관리하는 방법 인스턴스 작업을 시작하는 데 필요한 기본 작업

법적 공지

초록

명령줄 또는 웹 콘솔을 사용하여 Directory Server 12 및 관련 서비스를 설치, 업데이트 및 제거합니다. FIPS 모드에서 인스턴스를 실행하고, 테스트 항목을 생성하고, 웹 콘솔에 로그인하고, Directory Server 인스턴스를 시작 및 중지하며 LDAP 및 LDAPS 포트 번호를 변경하는 방법을 알아봅니다.

차례

RED HAT DIRECTORY SERVER에 대한 피드백 제공

Red Hat의 문서 및 제품에 대한 의견을 제공해 주셔서 감사합니다. Red Hat이 어떻게 이를 개선할 수 있는지 알려 주십시오. 이렇게 하려면 다음을 수행합니다.

- Jira (계정 필요)를 통해 Red Hat Directory Server 설명서에 피드백을 제출하려면 다음을 수행합니다.
  1. Red Hat 문제 추적기 로 이동하십시오.
  2. **요약** 필드에 설명 제목을 입력합니다.
  3. **설명** 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
  4. 대화 상자 하단에서 **생성** 을 클릭합니다.
- Jira를 통해 Red Hat Directory Server 제품에 대한 피드백을 제출하기 위해 필요한 경우:
  1. Red Hat 문제 추적기 로 이동하십시오.
  2. **문제 생성** 페이지에서 **다음을** 클릭합니다.
  3. **Summary** 필드를 입력합니다.
  4. **Component** 필드에서 구성 요소를 선택합니다.
  5. 다음을 포함하여 **Description** 필드를 작성합니다.
     a. 선택한 구성 요소의 버전 번호입니다.
     b. 문제 또는 개선을 위한 제안을 재현하는 단계입니다.
  6. **생성**을 클릭합니다.

1장. .INF 파일을 사용하여 명령줄에서 새 인스턴스 설정

명령줄에 **.inf** 파일을 사용하여 Directory Server를 설정하면 고급 설정을 사용자 지정할 수 있습니다. 예를 들어 **.inf** 파일에서 다음 설정을 사용자 지정할 수 있습니다.

- 서비스를 시작한 후 **ns-slapd** Directory Server 프로세스에서 사용하는 사용자 및 그룹입니다. 다른 사용자 및 그룹을 사용하는 경우 설치를 시작하기 전에 사용자와 그룹을 수동으로 생성해야 합니다.
- 구성, 백업 및 데이터 디렉터리와 같은 경로.
- 인증서 유효성.

1.1. 사전 요구 사항

- 이 서버는 Red Hat Directory Server 12 릴리스 노트에 설명된 대로 최신 Red Hat Directory Server 버전의 요구 사항을 충족합니다.

1.2. DIRECTORY SERVER 패키지 설치

다음 절차에 따라 Directory Server 패키지를 설치합니다.

사전 요구 사항

- 시스템을 Red Hat 서브스크립션 관리 서비스에 등록했습니다.
- Red Hat 계정에 유효한 Red Hat Directory Server 서브스크립션이 있어야 합니다.
- RHEL 기본 리포지토리(**BaseOS** 및 **AppStream**)가 활성화되어 있습니다.

절차

1. 계정에 SCA(Simple Content Access)를 비활성화한 경우:
   a. Red Hat Directory Server 서브스크립션을 제공하는 Red Hat 계정의 사용 가능한 서브스크립션을 나열하고 풀 ID를 기록해 둡니다.

```
# subscription-manager list --all --available --matches 'Red Hat Directory Server'
...
Subscription Name:   Example Subscription
Provides:            ...
                     Red Hat Directory Server
                     ...
Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
Available:           1
...
```

   b. 풀 ID를 사용하여 Red Hat Directory Server 서브스크립션을 시스템에 연결합니다.

```
# subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
Successfully attached a subscription for: Example Subscription
```

2. Directory Server 리포지토리를 활성화합니다. 예를 들어 Directory Server 12.4 리포지토리를 활성화하려면 다음을 실행합니다.

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. **redhat-ds:12** 모듈을 설치합니다.

```
# dnf module install redhat-ds:12
```

이 명령은 필요한 모든 종속 항목을 자동으로 설치합니다.

추가 리소스

- Red Hat Subscription Manager 사용
- 간단한 컨텐츠 액세스
- 활성화해야 하는 Red Hat 리포지토리의 이름은 무엇입니까?

1.3. DIRECTORY SERVER 인스턴스 설치를 위한 .INF 파일 생성

dscreate 유틸리티의 **.inf** 파일을 만들고 환경에 맞게 파일을 조정합니다. 이후 단계에서는 이 파일을 사용하여 새 Directory Server 인스턴스를 만듭니다.

사전 요구 사항

- **redhat-ds:12** 모듈을 설치했습니다.

절차

1. **dscreate create-template** 명령을 사용하여 템플릿 **.inf** 파일을 생성합니다. 예를 들어 템플릿을 **/root/instance_name.inf** 파일에 저장하려면 다음을 입력합니다.

```
# dscreate create-template /root/instance_name.inf
```

생성된 파일에는 설명을 포함하여 사용 가능한 모든 매개변수가 포함되어 있습니다.

2. 이전 단계에서 생성한 파일을 편집합니다.

   a. 설치를 사용자 지정하도록 설정할 매개변수의 주석을 제거합니다.
   모든 매개변수에는 기본값이 있습니다. 그러나 Red Hat은 프로덕션 환경에 대한 특정 매개변수를 사용자 지정하는 것이 좋습니다. 예를 들어 **[slapd]** 섹션에서 다음 매개변수를 설정합니다.

```
instance_name = instance_name
root_password = password
```

   b. 인스턴스 생성 중에 접미사를 자동으로 생성하려면 **[backend-userroot]** 섹션에서 다음 매개변수를 설정합니다.

```
create_suffix_entry = True
suffix = dc=example,dc=com
```

중요

인스턴스 생성 중에 접미사를 생성하지 않는 경우 이 인스턴스에 데이터를 저장하기 전에 나중에 수동으로 생성해야 합니다.

c. 선택 사항: 다른 매개변수의 주석을 제거하고 환경에 적절한 값으로 설정합니다. 예를 들어 이러한 매개변수를 사용하여 인증 자격 증명 및 changelog 트리밍과 같은 복제 옵션을 지정하거나 LDAP 및 LDAPS 프로토콜에 대해 다른 포트를 설정합니다.

참고

기본적으로 생성한 새 인스턴스에는 자체 서명된 인증서 및 TLS가 활성화된 TLS가 포함됩니다. 보안을 강화하기 위해 이 기능을 사용하지 않는 것이 좋습니다. 자체 서명된 인증서를 나중에 CA(인증 기관)에서 발급한 인증서로 교체할 수 있습니다.

추가 리소스

- Directory Server에 대한 TLS 암호화 연결 활성화

1.4. .INF 파일을 사용하여 새 DIRECTORY SERVER 인스턴스 설정

이 섹션에서는 **.inf** 파일을 사용하여 명령줄을 사용하여 새 Directory Server 인스턴스를 설정하는 방법을 설명합니다.

사전 요구 사항

- Directory Server 인스턴스에 대한 **.inf** 파일을 생성하셨습니다.

절차

1. **.inf** 파일을 **dscreate from-file** 명령에 전달하여 새 인스턴스를 생성합니다.

```
# dscreate from-file /root/instance_name.inf
Starting installation ...
Validate installation settings ...
Create file system structures ...
Create self-signed certificate database ...
Perform SELinux labeling ...
Perform post-installation tasks ...
Completed installation for instance: slapd-instance_name
```

dscreate 유틸리티는 인스턴스를 자동으로 시작하고 시스템이 부팅될 때 서비스를 시작하도록 RHEL을 구성합니다.

2. 방화벽에서 필요한 포트를 엽니다.

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

3. 방화벽 구성을 다시 로드합니다.

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

2장. 대화형 설치 프로그램을 사용하여 명령줄에서 새 인스턴스 설정

관리자는 Directory Server 대화형 설치 관리자를 사용하여 새 인스턴스의 구성에 대한 질문에 대답하여 새 인스턴스를 설정할 수 있습니다.

설치 중에 추가 설정을 사용자 지정하려면 대화형 설치 프로그램 대신 **.inf** 파일을 사용합니다. 자세한 내용은 *1장..inf 파일을 사용하여 명령줄에서 새 인스턴스 설정* 의 내용을 참조하십시오.

2.1. 사전 요구 사항

- 이 서버는 Red Hat Directory Server 12 릴리스 노트에 설명된 대로 최신 Red Hat Directory Server 버전의 요구 사항을 충족합니다.

2.2. DIRECTORY SERVER 패키지 설치

다음 절차에 따라 Directory Server 패키지를 설치합니다.

사전 요구 사항

- 시스템을 Red Hat 서브스크립션 관리 서비스에 등록했습니다.
- Red Hat 계정에 유효한 Red Hat Directory Server 서브스크립션이 있어야 합니다.
- RHEL 기본 리포지토리(**BaseOS** 및 **AppStream**)가 활성화되어 있습니다.

절차

1. 계정에 SCA(Simple Content Access)를 비활성화한 경우:

   a. Red Hat Directory Server 서브스크립션을 제공하는 Red Hat 계정의 사용 가능한 서브스크립션을 나열하고 풀 ID를 기록해 둡니다.

   ```
   # subscription-manager list --all --available --matches 'Red Hat Directory Server'
   ...
   Subscription Name:   Example Subscription
   Provides:            ...
                        Red Hat Directory Server
                        ...
   Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
   Available:           1
   ...
   ```

   b. 풀 ID를 사용하여 Red Hat Directory Server 서브스크립션을 시스템에 연결합니다.

   ```
   # subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
   Successfully attached a subscription for: Example Subscription
   ```

2. Directory Server 리포지토리를 활성화합니다. 예를 들어 Directory Server 12.4 리포지토리를 활성화하려면 다음을 실행합니다.

   ```
   # subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
   Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
   ```

3. **redhat-ds:12** 모듈을 설치합니다.

```
# dnf module install redhat-ds:12
```

이 명령은 필요한 모든 종속 항목을 자동으로 설치합니다.

추가 리소스

- Red Hat Subscription Manager 사용
- 간단한 컨텐츠 액세스
- 활성화해야 하는 Red Hat 리포지토리의 이름은 무엇입니까?

2.3. 대화식 설치 프로그램을 사용하여 인스턴스 생성

이 섹션에서는 대화형 설치 관리자를 사용하여 새 Directory Server 인스턴스를 만드는 방법을 설명합니다.

절차

1. 대화형 설치 프로그램을 시작합니다.

```
# dscreate interactive
```

2. 대화형 설치 프로그램의 질문에 대답합니다.
설치 프로그램에서 대부분의 질문 뒤에 대괄호로 표시된 기본값을 사용하려면 값을 입력하지 않고 **Enter** 를 누릅니다.

```
Install Directory Server (interactive mode)
===========================================

Enter system's hostname [server.example.com]:

Enter the instance name [server]: instance_name

Enter port number [389]:

Create self-signed certificate database [yes]:

Enter secure port number [636]:

Enter Directory Manager DN [cn=Directory Manager]:

Enter the Directory Manager password: password
Confirm the Directory Manager Password: password

Enter the database suffix (or enter "none" to skip) [dc=server,dc=example,dc=com]:
dc=example,dc=com

Create sample entries in the suffix [no]:

Create just the top suffix entry [no]: yes
```

```
Do you want to start the instance after the installation? [yes]:

Are you ready to install? [no]: yes
```

참고

일반 텍스트로 암호를 설정하는 대신 **pwd *hash*유틸리티로 생성된 {*algorithm*} 해시** 문자열을 설정할 수 있습니다.

3. 방화벽에서 필요한 포트를 엽니다.

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

4. 방화벽 구성을 다시 로드합니다.

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

3장. 웹 콘솔을 사용하여 새 인스턴스 설정

브라우저 기반 인터페이스를 사용하여 Directory Server를 설정하는 경우 Directory Server 웹 콘솔을 사용할 수 있습니다.

3.1. 사전 요구 사항

- 서버는 Red Hat Directory Server 12 릴리스 노트에 설명된 대로 최신 Red Hat Directory Server 버전의 요구 사항을 충족합니다.
- Directory Server 패키지 설치에 설명된 대로 Directory Server 패키지를 설치했습니다.

3.2. 웹 콘솔을 사용하여 새 DIRECTORY SERVER 인스턴스 설정

이 섹션에서는 웹 콘솔을 사용하여 새 Directory Server 인스턴스를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

- **cockpit** 웹 콘솔 패키지가 설치되어 있습니다.
- **cockpit.socket** systemd 장치가 활성화되어 시작됩니다.
- 웹 콘솔 액세스를 허용하기 위해 로컬 방화벽에서 포트 **9090** 을 열었습니다.

절차

1. 브라우저를 사용하여 Directory Server 호스트의 포트 9090에서 실행 중인 웹 콘솔에 연결합니다.

   > **https://*server.example.com*:9090**

2. **root** 사용자로 로그인하거나 sudo 권한이 있는 사용자로 로그인합니다.
3. **Red Hat Directory Server** 항목을 선택합니다.
4. 새 인스턴스를 생성합니다.
   - 서버에 인스턴스가 없는 경우 **Create New Instance** (새 인스턴스 생성) 버튼을 클릭합니다.
   - 서버가 이미 기존 인스턴스를 실행하는 경우 **작업을** 선택하고 **Create New Instance** 를 클릭합니다.
5. **Create New Server Instance** (새 서버 인스턴스 생성) 양식의 필드를 작성합니다.
   - **Instance Name**: 인스턴스의 이름을 설정합니다. 인스턴스 이름을 생성한 후에는 변경할 수 없습니다.
   - port : LDAP 프로토콜의 포트 번호를 설정합니다. **포트는 다른 인스턴스 또는 서비스에서 사용해서는 안 됩니다. 기본 포트는 389입니다.**
   - **Secure Port: LDAPS 프로토콜의 포트 번호를 설정합니다. 포트는 다른 인스턴스 또는 서비스에서 사용해서는 안 됩니다. 기본 포트는 636입니다.**

- **자체 서명된 TLS 인증서 만들기:** 인스턴스에서 **TLS** 암호화를 활성화하고 자체 서명된 인증서를 생성합니다.

  보안을 강화하기 위해 자체 서명 인증서 및 **TLS**가 활성화된 새 인스턴스를 생성하는 것이 좋습니다. 자체 서명된 인증서를 나중에 **CA**(인증 기관)에서 발급한 인증서로 교체할 수 있습니다.

- **Directory Manager DN:** 인스턴스 관리자의 고유 이름(**DN**)을 설정합니다. 기본값은 **cn=Directory Manager** 입니다.

- **Directory Manager Password:** 인스턴스의 관리자 암호를 설정합니다.

- **확인 암호: Directory Manager** 암호 필드에 있는 것과 동일한 값으로 설정해야 합니다.

- **Create Database:** 인스턴스 생성 중에 접미사를 자동으로 생성하려면 이 필드를 선택합니다.

  중요

  인스턴스 생성 중에 접미사를 생성하지 않는 경우 이 인스턴스에 데이터를 저장하기 전에 나중에 수동으로 생성해야 합니다.

  이 옵션을 활성화하면 추가 필드를 작성합니다.

  - **Database Suffix:** 백엔드의 접미사를 설정합니다.
  - **Database Name:** 백엔드 데이터베이스의 이름을 설정합니다.
  - **데이터베이스 초기화:** 이 필드를 **Suffix Entry** 만들기로 설정합니다.

6. 인스턴스 생성을 클릭합니다.

새 인스턴스가 시작되고 시스템이 부팅될 때 자동으로 시작하도록 구성됩니다.

7. 방화벽에서 필요한 포트를 엽니다.

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

8. 방화벽 구성을 다시 로드합니다.

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

추가 리소스

- Directory Server에 대한 TLS 암호화 연결 활성화

4장. 루트가 아닌 사용자로 새 인스턴스 설정

루트 권한이 없는 경우 사용자로 Directory Server 설치를 수행할 수 있습니다. 이 방법을 사용하여 Directory Server를 테스트하고 LDAP 애플리케이션을 개발할 수 있습니다. 그러나 루트가 아닌 사용자가 실행하는 인스턴스에는 다음과 같은 제한 사항이 있습니다.

- SNMP(Simple Network Management Protocol)는 지원하지 않습니다.
- 1024 포트만 사용할 수 있습니다.

4.1. DIRECTORY SERVER를 사용자로 설치하기 위한 환경 준비

루트 권한이 없으면 Directory Server 인스턴스를 만들고 관리하려면 dscreate ds-root 명령을 사용하여 적절한 환경을 준비해야 합니다.

사전 요구 사항

- 디렉터리 서버 패키지를 root 사용자로 설치했습니다.

절차

1. PATH 변수에 $HOME/bin 이 있는지 확인합니다. 그렇지 않은 경우:
   a. ~/.bash_profile 파일에 다음을 추가합니다.

```
PATH="$HOME/bin:$PATH"
```

   b. ~/bash_profile 파일을 다시 읽습니다.

```
$ source ~/.bash_profile
```

2. 사용자 지정 위치를 사용하도록 인스턴스 생성 환경을 구성합니다.

```
$ dscreate ds-root $HOME/dsroot $HOME/bin
```

이 명령은 표준 설치 경로를 **$HOME/dsroot/** 로 교체하고 **$HOME/bin/** 디렉터리에 표준 **Directory Server** 관리 유틸리티 사본을 생성합니다.

3. 쉘에서 새 경로를 사용하도록 하려면 다음을 수행합니다.

   a. 캐시를 지웁니다.

   ```
   $ hash -r dscreate
   ```

   b. 쉘이 명령의 올바른 경로를 사용하는지 확인합니다.

   ```
   $ which dscreate
   ~/bin/dscreate
   ```

dscreate 명령의 경우 쉘은 이제 **/usr/bin/dscreate** 대신 **$HOME/bin/dscreate** 를 사용합니다.

4.2. 루트가 아닌 사용자로 새 인스턴스 설치

루트 권한 없이 **Directory Server**를 설치하려면 대화형 설치 프로그램을 사용할 수 있습니다. 설치 후 **Directory Server**는 사용자 지정 위치에 인스턴스를 생성하고 사용자가 정상적으로**dsctl, ds conf** 유틸리티를 실행할 수 있습니다.

사전 요구 사항

- 루트가 아닌 설치를 위한 환경을 준비하셨습니다.
- **firewall-cmd** 유틸리티를 사용할 수 있는 **sudo** 권한이 있는 경우 외부에서 **Directory Server** 인스턴스를 사용할 수 있도록 해야 합니다.

절차

1. 대화식 설치 프로그램을 사용하여 인스턴스 생성

   a. 대화형 설치 프로그램을 시작합니다.

   ```
   $ dscreate interactive
   ```

b. 대화형 설치 프로그램의 질문에 대답합니다.

설치 프로그램에서 대부분의 질문 뒤에 대괄호로 표시된 기본값을 사용하려면 값을 입력하지 않고 **Enter** 를 누릅니다.

참고

설치하는 동안 인스턴스 포트 및 보안 포트 번호 **1024**(예: **1389** 및 **1636**)를 선택해야 합니다. 그렇지 않으면 사용자에게 권한 있는 포트(**1-1023**)에 바인딩할 수 있는 권한이 없습니다.

```
Install Directory Server (interactive mode)
===========================================
Non privileged user cannot use semanage, will not relabel ports or files.

Selinux support will be disabled, continue? [yes]: yes

Enter system's hostname [server.example.com]:

Enter the instance name [server]: instance_name

Enter port number [389]: 1389

Create self-signed certificate database [yes]:

Enter secure port number [636]: 1636

Enter Directory Manager DN [cn=Directory Manager]:

Enter the Directory Manager password: password
Confirm the Directory Manager Password: password

Enter the database suffix (or enter "none" to skip)
[dc=server,dc=example,dc=com]: dc=example,dc=com

Create sample entries in the suffix [no]:

Create just the top suffix entry [no]: yes

Do you want to start the instance after the installation? [yes]:

Are you ready to install? [no]: yes
```

참고

일반 텍스트로 암호를 설정하는 대신 **pwd *hash***유틸리티로 생성된 **{*algorithm*}** 해시 문자열을 설정할 수 있습니다.

2. 선택 사항: 외부에서 **Directory Server** 인스턴스를 사용할 수 있도록 하려면 다음을 수행합니다.

   a. 방화벽에서 포트를 엽니다.

```
# sudo firewall-cmd --permanent --add-port={1389/tcp,1636/tcp}
```

   b. 방화벽 구성을 다시 로드합니다.

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

검증

- **ldapsearch** 명령을 실행하여 사용자가 인스턴스에 연결할 수 있는지 테스트합니다.

```
$ ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com:1389 -b
"dc=example,dc=com" -s sub -x "(objectclass=*)"
```

추가 리소스

- root가 아닌 사용자 설치를 위한 환경 준비
- 루트가 아닌 권한으로 1024 미만의 포트를 바인딩하는 방법

5장. 로드 밸런서 뒤에서 KERBEROS 인증을 사용하여 DIRECTORY SERVER 설치

로드 밸런서를 사용하고 Kerberos 인증을 지원하는 Directory Server 인스턴스를 설치하려면 설치 중에 비해 추가 단계가 필요합니다.

사용자가 GSSAPI(Generic Security Services API)를 사용하여 서비스에 액세스하는 경우 Kerberos 주체에는 서비스 호스트의 DNS 이름이 포함됩니다. 사용자가 로드 밸런서에 연결하는 경우 주체에는 로드 밸런서의 DNS 이름이 포함됩니다(예: ldap/loadbalancer.example.com@EXAMPLE.COM, Directory Server 인스턴스의 DNS 이름이 아님).

연결에 성공하려면 로드 밸런서 DNS 이름이 다른 경우에도 요청을 수신하는 Directory Server 인스턴스에서 로드 밸런서와 동일한 이름을 사용해야 합니다.

이 섹션에서는 로드 밸런서 뒤에서 Kerberos 인증을 통해 Directory Server 인스턴스를 설정하는 방법에 대해 설명합니다.

5.1. 사전 요구 사항

- 이 서버는 Red Hat Directory Server 12 릴리스 노트에 설명된 대로 최신 Red Hat Directory Server 버전의 요구 사항을 충족합니다.

5.2. DIRECTORY SERVER 패키지 설치

다음 절차에 따라 Directory Server 패키지를 설치합니다.

사전 요구 사항

- 시스템을 Red Hat 서브스크립션 관리 서비스에 등록했습니다.
- Red Hat 계정에 유효한 Red Hat Directory Server 서브스크립션이 있어야 합니다.
- RHEL 기본 리포지토리(BaseOS 및 AppStream)가 활성화되어 있습니다.

절차

1. 계정에 SCA(Simple Content Access)를 비활성화한 경우:

   a. Red Hat Directory Server 서브스크립션을 제공하는 Red Hat 계정의 사용 가능한 서브스크립션을 나열하고 풀 ID를 기록해 둡니다.

```
# subscription-manager list --all --available --matches 'Red Hat Directory Server'
...
Subscription Name:   Example Subscription
Provides:            ...
                     Red Hat Directory Server
                     ...
Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
Available:           1
...
```

   b. 풀 ID를 사용하여 Red Hat Directory Server 서브스크립션을 시스템에 연결합니다.

```
# subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
Successfully attached a subscription for: Example Subscription
```

2. Directory Server 리포지토리를 활성화합니다. 예를 들어 Directory Server 12.4 리포지토리를 활성화하려면 다음을 실행합니다.

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. redhat-ds:12 모듈을 설치합니다.

```
# dnf module install redhat-ds:12
```

   이 명령은 필요한 모든 종속 항목을 자동으로 설치합니다.

추가 리소스

- Red Hat Subscription Manager 사용
- 간단한 컨텐츠 액세스

- 활성화해야 하는 **Red Hat** 리포지토리의 이름은 무엇입니까?

5.3. DIRECTORY SERVER 인스턴스 설치를 위한 .INF 파일 생성

dscreate 유틸리티의 **.inf** 파일을 만들고 환경에 맞게 파일을 조정합니다. 이후 단계에서는 이 파일을 사용하여 새 **Directory Server** 인스턴스를 만듭니다.

사전 요구 사항

- **redhat-ds:12** 모듈을 설치했습니다.

절차

1. **dscreate create-template** 명령을 사용하여 템플릿 **.inf** 파일을 생성합니다. 예를 들어 템플릿을 **/root/instance_name.inf** 파일에 저장하려면 다음을 입력합니다.

```
# dscreate create-template /root/instance_name.inf
```

생성된 파일에는 설명을 포함하여 사용 가능한 모든 매개변수가 포함되어 있습니다.

2. 이전 단계에서 생성한 파일을 편집합니다.

   a. 설치를 사용자 지정하도록 설정할 매개변수의 주석을 제거합니다.

   모든 매개변수에는 기본값이 있습니다. 그러나 **Red Hat**은 프로덕션 환경에 대한 특정 매개변수를 사용자 지정하는 것이 좋습니다. 예를 들어 **[slapd]** 섹션에서 다음 매개변수를 설정합니다.

```
instance_name = instance_name
root_password = password
```

   b. **GSSAPI** 인증이 있는 로드 밸런서의 인스턴스를 사용하려면 **[general]** 섹션에서 **full_machine_name** 매개변수를 디렉터리 서버 호스트의 **FQDN** 대신 로드 밸런서의 **FQDN**(정규화된 도메인 이름)으로 설정합니다.

```
full_machine_name = loadbalancer.example.com
```

c. **[general]** 섹션에서 **strict_host_checking** 매개변수의 주석을 제거하고 **False** 로 설정합니다.

```
strict_host_checking = False
```

d. 인스턴스 생성 중에 접미사를 자동으로 생성하려면 **[backend-userroot]** 섹션에서 다음 매개변수를 설정합니다.

```
create_suffix_entry = True
suffix = dc=example,dc=com
```

중요

인스턴스 생성 중에 접미사를 생성하지 않는 경우 이 인스턴스에 데이터를 저장하기 전에 나중에 수동으로 생성해야 합니다.

e. 선택 사항: 다른 매개변수의 주석을 제거하고 환경에 적절한 값으로 설정합니다. 예를 들어 이러한 매개변수를 사용하여 인증 자격 증명 및 **changelog** 트리밍과 같은 복제 옵션을 지정하거나 **LDAP** 및 **LDAPS** 프로토콜에 대해 다른 포트를 설정합니다.

참고

기본적으로 생성한 새 인스턴스에는 자체 서명된 인증서 및 **TLS**가 활성화된 **TLS**가 포함됩니다. 보안을 강화하기 위해 이 기능을 사용하지 않는 것이 좋습니다. 자체 서명된 인증서를 나중에 **CA**(인증 기관)에서 발급한 인증서로 교체할 수 있습니다.

추가 리소스

- Directory Server에 대한 TLS 암호화 연결 활성화

5.4. .INF 파일을 사용하여 새 DIRECTORY SERVER 인스턴스 설정

이 섹션에서는 **.inf** 파일을 사용하여 명령줄을 사용하여 새 **Directory Server** 인스턴스를 설정하는 방법을 설명합니다.

사전 요구 사항

- Directory Server 인스턴스에 대한 .inf 파일을 생성하셨습니다.

절차

1. .inf 파일을 dscreate from-file 명령에 전달하여 새 인스턴스를 생성합니다.

```
# dscreate from-file /root/instance_name.inf
Starting installation ...
Validate installation settings ...
Create file system structures ...
Create self-signed certificate database ...
Perform SELinux labeling ...
Perform post-installation tasks ...
Completed installation for instance: slapd-instance_name
```

dscreate 유틸리티는 인스턴스를 자동으로 시작하고 시스템이 부팅될 때 서비스를 시작하도록 RHEL을 구성합니다.

2. 방화벽에서 필요한 포트를 엽니다.

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

3. 방화벽 구성을 다시 로드합니다.

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

5.5. 로드 밸런서의 키탭 생성 및 키 탭을 사용하도록 DIRECTORY SERVER 구성

사용자가 GSSAPI를 사용하여 로드 밸런서 뒤에서 Directory Server로 인증하려면 먼저 로드 밸런서에 대한 Kerberos 사용자를 만들고 Kerberos 주체를 사용하도록 Directory Server를 구성해야 합니다. 이 섹션에서는 이 프로세스에 대해 설명합니다.

사전 요구 사항

- 다음 .inf 파일 구성이 포함된 인스턴스입니다.
  - full_machine_name 매개변수는 로드 밸런서의 DNS 이름으로 설정됩니다.

- **strict_host_checking** 매개변수는 **False** 로 설정됩니다.

절차

1. 로드 밸런서의 **Kerberos** 사용자(예: **ldap/*loadbalancer.example.com_@_EXAMPLE.COM***)를 만듭니다. 서비스 주체를 생성하는 절차는 **Kerberos** 설치에 따라 다릅니다. 자세한 내용은 **Kerberos** 서버 설명서를 참조하십시오.

2. 선택 사항: **keytab** 파일에 추가 주체를 추가할 수 있습니다. 예를 들어 사용자가 **Kerberos** 인증을 사용하여 직접 로드 밸런서 뒤의 **Directory Server** 인스턴스에 연결할 수 있도록 하려면 **Directory Server** 호스트에 대한 추가 주체를 추가합니다. 예: **ldap/*server1.example.com@EXAMPLE.COM*.**

3. 서비스 키탭 파일을 **Directory Server** 호스트에 복사하고 이를 **/etc/dirsrv/slapd-*instance_name*/ldap.keytab** 파일에 저장합니다.

4. 서비스 **keytab**의 경로를 **/etc/sysconfig/slapd-*instance_name*** 파일에 추가합니다.

```
KRB5_KTNAME=/etc/dirsrv/slapd-instance_name/ldap.keytab
```

5. **Directory Server** 인스턴스를 다시 시작합니다.

```
# dsctl instance_name restart
```

검증

- **GSSAPI** 프로토콜을 사용하여 로드 밸런서에 연결할 수 있는지 확인합니다.

```
# ldapsearch -H ldap://loadbalancer.example.com -Y GSSAPI
```

Directory Server 호스트 자체와 같이 **keytab** 파일에 **Kerberos** 사용자를 추가하는 경우 다음 연결도 확인합니다.

```
# ldapsearch -H ldap://server1.example.com -Y GSSAPI
```

6장. FIPS 모드에서 DIRECTORY SERVER 실행

Directory Server는 연방 정보 처리 표준 (FIPS)을 완전히 지원합니다. Directory Server를 실행하는 경우 FIPS 모드에서 실행하면 보안 관련 설정이 변경됩니다. 예를 들어 SSL은 자동으로 비활성화되어 TLS 1.2 및 1.3 암호화만 사용됩니다.

6.1. FIPS 모드 활성화

FIPS(Federal Information Processing Standard) 모드에서 Directory Server를 사용하려면 RHEL 및 Directory Server에서 모드를 활성화합니다.

사전 요구 사항

- RHEL에서 FIPS 모드를 활성화했습니다.

절차

1. NSS(네트워크 보안 서비스) 데이터베이스에 FIPS 모드를 활성화합니다.

```
# modutil -dbdir /etc/dirsrv/slapd-instance_name/ -fips true
```

2. 인스턴스를 다시 시작합니다.

```
# dsctl instance_name restart
```

검증

- NSS 데이터베이스에 FIPS 모드가 활성화되어 있는지 확인합니다.

```
# modutil -dbdir /etc/dirsrv/slapd-instance_name/ -chkfips true
FIPS mode enabled.
```

이 명령은 모듈이 FIPS 모드 인 경우 FIPS 모드를 활성화합니다.

6.2. 추가 리소스

- 연방 정보 처리 표준 (FIPS)
- 시스템을 FIPS 모드로 전환

7장. DIRECTORY SERVER를 새 마이너 버전으로 업데이트

Red Hat은 Red Hat Directory Server 12의 업데이트된 버전을 자주 릴리스합니다. 이 섹션에서는 Directory Server 패키지를 업데이트하는 방법에 대해 설명합니다.

Red Hat Directory Server 11을 버전 12로 마이그레이션하려면 Directory Server 11을 Directory Server 12로 마이그레이션하십시오.

7.1. DIRECTORY SERVER 패키지 업데이트

dnf 유틸리티를 사용하여 관련 패키지도 자동으로 업데이트하는 모듈을 업데이트합니다. 다음 절차에서는 버전 12.3에서 12.4로 Directory Server를 업데이트합니다.

사전 요구 사항

- Red Hat Directory Server 12.3이 서버에 설치되어 있습니다.
- Red Hat 계정에 유효한 Red Hat Directory Server 서브스크립션이 있어야 합니다.

절차

1. Directory Server 12.3 리포지토리를 비활성화합니다.

```
# subscription-manager repos --disable dirsrv-12.3-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.3-for-rhel-9-x86_64-rpms' is disabled for this system.
```

2. Directory Server 12.4 리포지토리를 활성화합니다.

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. Directory Server 패키지를 업데이트합니다.

```
# dnf module update redhat-ds
```

dnf 모듈은 redhat-ds 명령을 사용하여 Directory Server 패키지 및 해당 종속 항목을 버전

12.4로 업데이트합니다.

업데이트 프로세스는 서버의 모든 인스턴스에 대해 **dirsrv** 서비스를 자동으로 다시 시작합니다.

추가 리소스

- 활성화해야 하는 **Red Hat** 리포지토리의 이름은 무엇입니까**?**

8장. DIRECTORY SERVER 11에서 DIRECTORY SERVER 12로 마이그레이션

마이그레이션을 시작하기 전에 수행해야 하는 작업을 포함하여 Red Hat Directory Server 11에서 12로 마이그레이션하는 방법을 알아보십시오.

중요

Red Hat은 Red Hat Directory Server 10 또는 11에서 버전 12로만 마이그레이션을 지원합니다. 이전 버전에서 Directory Server를 마이그레이션하려면 Directory Server 10 또는 11로 증분 마이그레이션을 수행해야 합니다.

Red Hat 은 leapp 업그레이드 툴을 사용하여 Directory Server 10 또는 11 서버를 버전 12로 업그레이드할 수 없습니다.

8.1. 사전 요구 사항

- 기존 Directory Server 설치는 버전 11에서 실행되며 사용 가능한 모든 업데이트가 설치되어 있습니다.

8.2. 복제 방법을 사용하여 DIRECTORY SERVER 12로 마이그레이션

복제 토폴로지에서 복제 방법을 사용하여 Directory Server 12로 마이그레이션합니다.

절차

1. Directory Server 12를 설치합니다.

2. Directory Server 12 호스트에서 복제를 활성화하지만 복제 계약을 생성하지는 않습니다. 복제 활성화에 대한 자세한 내용은 *Red Hat Directory Server 12* 의 복제 설명서 구성 및 관리를 참조하십시오.

3. Directory Server 11 호스트에서 복제를 활성화하고 Directory Server 12 호스트를 가리키는 복제 계약을 만듭니다. 자세한 내용은 *Red Hat Directory Server 11 관리자 가이드의 Multi-Supplier Replication 섹션을 참조하십시오.*

중요

Directory Server 11 호스트에서 사용자 지정 구성을 사용한 경우 **dse.ldif** 레이아웃이 버전 간에 변경되므로 **Directory Server 12** 호스트의 **dse.ldif** 구성 파일을 **Directory Server 11** 호스트의 파일로 교체 하지 마십시오. 대신 **dsconf** 유틸리티 또는 웹 콘솔을 사용하여 필요한 각 매개변수 및 플러그인에 대한 사용자 지정 구성을 추가합니다.

4. 선택 사항: **Directory Server 12** 호스트 간에 복제 계약을 통해 추가 **Directory Server 12** 호스트를 설정합니다.

5. **Directory Server 12** 호스트만 사용하도록 클라이언트를 구성합니다.

6. **Directory Server 11** 호스트에서 **Directory Server 12** 호스트를 가리키는 복제 계약을 제거합니다. ***Red Hat Directory Server 11** 관리 가이드의 복제 토폴로지에서 **Directory Server** 인스턴스 제거*를 참조하십시오.

7. **Directory Server 11** 호스트를 제거합니다. ***Red Hat Directory Server 11** 설치 가이드에서 디렉터리 서버 제거*를 참조하십시오.

8.3. 내보내기 및 가져오기 방법을 사용하여 DIRECTORY SERVER 12로 마이그레이션

내보내기 및 가져오기 방법을 사용하여 복제가 없는 인스턴스와 같은 소규모 **Directory Server** 환경을 마이그레이션합니다.

절차

1. 기존 **Directory Server 11** 호스트에서 다음 단계를 수행합니다.

   a. **dirsrv** 서비스를 중지하고 비활성화합니다.

   ```
   # dsctl instance_name stop
   # systemctl disable dirsrv@instance_name
   ```

   b. 백엔드를 내보냅니다. 예를 들어 사용자**Root** 백엔드를 내보내 **/var/lib/dirsrv/slapd-*instance_name*/userRoot.ldif** 파일에 저장하려면 다음을 실행합니다.

```
# dsctl instance_name db2ldif userroot
/var/lib/dirsrv/slapd-instance_name/userRoot.ldif
```

c. 다음 파일을 **Directory Server 12**를 설치하려는 새 호스트에 복사합니다.

- 이전 단계에서 내보낸 **/var/lib/dirsrv/slapd-*instance_name*/userRoot.ldif** 파일입니다.
- **/etc/dirsrv/slapd-*instance_name*/dse.ldif** 구성 파일입니다.

  중요

  dse.ldif 레이아웃이 다른 버전이 변경되므로 **Directory Server 12** 호스트의 **dse.ldif** 구성 파일을 **Directory Server 11** 호스트의 파일로 교체하지 마십시오. 참조용으로 **dse.ldif** 파일을 저장합니다.

- **/etc/dirsrv/slapd-*instance_name*/schema/99user.ldif,** 사용자 지정 스키마를 사용하는 경우
- **TLS**가 활성화된 인스턴스를 마이그레이션하고 **Directory Server 12** 설치에 대해 동일한 호스트 이름을 재사용하려면 다음 파일을 새 호스트에 복사하십시오.
  - **/etc/dirsrv/slapd-*instance_name*/cert9.db**
  - **/etc/dirsrv/slapd-*instance_name*/key4.db**
  - **/etc/dirsrv/slapd-*instance_name*/pin.txt**

d. **Directory Server 12** 호스트에서 동일한 호스트 이름과 **IP**를 사용하려면 이전 서버의 연결을 끊습니다.

2. 새 호스트에서 다음 단계를 수행합니다.

a. **Directory Server 12를 설치합니다.**

b. **선택 사항: TLS 암호화를 구성합니다.**

- 새 설치에서 **Directory Server 11** 인스턴스와 다른 호스트 이름을 사용하는 경우 ***Red Hat Directory Server** 보안* 설명서의 **Directory Server에 TLS 암호화 연결 활성화 섹션을** 참조하십시오.

- 이전 **Directory Server 11** 설치와 동일한 호스트 이름을 사용하려면 다음을 수행합니다.

  i. 인스턴스를 중지합니다.

  ```
  # dsctl instance_name stop
  ```

  ii. 이미 존재하는 경우 **NSS(Network Security Services)** 데이터베이스와 **Directory Server**의 암호 파일을 제거합니다.

  ```
  # rm /etc/dirsrv/slapd-instance_name/cert*.db
  /etc/dirsrv/slapd-instance_name/key*.db
  /etc/dirsrv/slapd-instance_name/pin.txt
  ```

  iii. **Directory Server 11** 호스트에서 복사한 **cert9.db,key4.db, pin.txt** 파일을 **/etc/dirsrv/slapd-*instance_name*/** 디렉터리에 배치합니다.

  iv. **NSS** 데이터베이스 및 암호 파일에 대한 올바른 권한을 설정합니다.

  ```
  # chown dirsrv:root /etc/dirsrv/slapd-instance_name/cert9.db
  /etc/dirsrv/slapd-instance_name/key4.db
  /etc/dirsrv/slapd-instance_name/pin.txt

  # chmod 600 /etc/dirsrv/slapd-instance_name/cert9.db
  /etc/dirsrv/slapd-instance_name/key4.db
  /etc/dirsrv/slapd-instance_name/pin.txt
  ```

  v. 인스턴스를 시작합니다.

  ```
  # dsctl instance_name start
  ```

c. 사용자 지정 스키마를 사용한 경우 **99user.ldif** 파일을 **/etc/dirsrv/slapd-*instance_name*/schema/** 디렉터리에 배치하고 적절한 권한을 설정하고 인스턴스를 다시 시작합니다.

```
# cp /tmp/99user.ldif /etc/dirsrv/slapd-instance_name/schema/

# chmod 644 /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# chown root:root /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# dsctl instance_name restart
```

d. **LDIF** 파일을 가져옵니다. 예를 들어 ***/var/lib/dirsrv/slapd-*instance_name*/ldif/migration.ldif*** 파일을 **userRoot** 데이터베이스로 가져오려면 다음을 실행합니다.

```
# dsconf -D 'cn=Directory Manager' ldap://server.example.com backend import
userRoot /var/lib/dirsrv/slapd-instance_name/ldif/migration.ldif
```

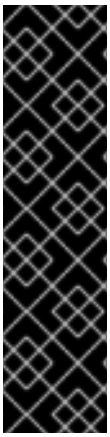
Directory Server에는 **/var/lib/dirsrv/slapd-*instance_name*/** 디렉터리에 가져오려는 **LDIF** 파일이 필요합니다.

중요

Directory Server 11 호스트에서 사용자 지정 구성을 사용한 경우 **Directory Server 12** 호스트의 **dse.ldif** 구성 파일을 **Directory Server 11** 호스트의 파일로 교체 하지 마십시오. 대신 **dsconf** 유틸리티 또는 웹 콘솔을 사용하여 필요한 각 매개변수 및 플러그인에 대해 사용자 지정 구성을 수동으로 추가합니다.

9장. DIRECTORY SERVER 10을 DIRECTORY SERVER 12로 마이그레이션

마이그레이션을 시작하기 전에 수행해야 하는 작업을 포함하여 **Red Hat Directory Server 10**에서 **12**로 마이그레이션하는 방법을 알아봅니다.



중요

Red Hat은 **Red Hat Directory Server 10** 또는 **11**에서 버전 **12**로만 마이그레이션을 지원합니다. 이전 버전에서 **Directory Server**를 마이그레이션하려면 **Directory Server 10** 또는 **11**로 증분 마이그레이션을 수행해야 합니다.

Red Hat 은 **leapp** 업그레이드 툴을 사용하여 **Directory Server 10** 또는 **11** 서버를 버전 **12**로 업그레이드할 수 없습니다.

9.1. 사전 요구 사항

- 기존 **Directory Server** 설치는 버전 **10**에서 실행되며 사용 가능한 모든 업데이트가 설치되어 있습니다.

9.2. 복제 방법을 사용하여 DIRECTORY SERVER 10을 버전 12로 마이그레이션

복제 토폴로지에서 복제 방법을 사용하여 **Directory Server 12**로 마이그레이션합니다.

절차

1. 새 호스트에 **Directory Server 12**를 설치합니다.

2. **Directory Server 12** 호스트에서 복제를 활성화하지만 복제 계약을 생성하지는 않습니다. 복제 활성화에 대한 자세한 내용은 ***Red Hat Directory Server 12*** 설명서의 복제 구성 및 관리를 참조하십시오.

3. **Directory Server 10** 호스트에서 복제를 활성화하고 **Directory Server 12** 호스트를 가리키는 복제 계약을 만듭니다. 복제 활성화에 대한 자세한 내용은 **Red Hat Directory Server 10** 관리 가이드의 **15**장 "복제 관리"를 참조하십시오.

중요

Directory Server 10 호스트에서 사용자 지정 구성을 사용한 경우 **dse.ldif** 레이아웃이 버전 간에 변경되므로 **Directory Server 12** 호스트의 **dse.ldif** 구성 파일을 이전 버전의 파일로 교체 하지 마십시오. 대신 **dsconf** 유틸리티 또는 웹 콘솔을 사용하여 필요한 각 매개변수 및 플러그인에 대한 사용자 지정 구성을 추가합니다.

4. 선택 사항: **Directory Server 12** 호스트 간에 복제 계약을 통해 추가 **Directory Server 12** 호스트를 설정합니다.

5. **Directory Server 12** 호스트만 사용하도록 클라이언트를 구성합니다.

6. **Directory Server 10** 호스트에서 **Directory Server 12** 호스트를 가리키는 복제 계약을 제거합니다.

```
# ldapmodify -D "cn=Directory Manager" -W -x -p 389 -h server_ds_10.example.com
dn: cn=agreement-to-DS-12-
server,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
changetype: delete
```

7. **Directory Server 10** 호스트를 설치 제거합니다. Red Hat Directory Server 10 설치 가이드의 4.8 장 "시스템 디렉터리 서버 제거" 장을 참조하십시오.

9.3. 내보내기 및 가져오기 방법을 사용하여 DIRECTORY SERVER 10을 버전 12로 마이그레이션

내보내기 및 가져오기 방법을 사용하여 대규모 **Directory Server** 환경을 마이그레이션합니다.

절차

1. 기존 **Directory Server 10** 호스트에서 다음 단계를 수행합니다.

   a. **dirsrv** 서비스를 중지하고 비활성화합니다.

```
# dsctl instance_name stop
# systemctl disable dirsrv@instance_name
```

   b.

백엔드를 내보냅니다. 예를 들어 사용자Root 백엔드를 내보내고 /tmp/userRoot.ldif 파일에 저장하려면 다음을 수행합니다.

```
# db2ldif -Z instance_name -n userRoot -a /tmp/userRoot.ldif
```

c. 다음 파일을 Directory Server 12를 설치하려는 새 호스트에 복사합니다.

- 이전 단계에서 내보낸 LDIF 파일 userRoot.ldif 입니다.
- 사용자 지정 스키마를 사용하는 경우 /etc/dirsrv/slapd-*instance_name*/schema/99user.ldif 파일입니다.
- /etc/dirsrv/slapd-*instance_name*/dse.ldif 구성 파일입니다.

  중요

  dse.ldif 레이아웃이 버전 간에 변경되므로 Directory Server 12 호스트의 dse.ldif 구성 파일을 Directory Server 10 호스트의 파일로 교체하지 마십시오. 참조용으로 dse.ldif 파일을 저장합니다.

- TLS가 활성화된 인스턴스를 마이그레이션하고 Directory Server 12 설치에 동일한 호스트 이름을 재사용하려면 복사하십시오.
  - /etc/dirsrv/slapd-*instance_name*/cert8.db
  - /etc/dirsrv/slapd-*instance_name*/key3.db
  - /etc/dirsrv/slapd-*instance_name*/pin.txt

d. Directory Server 12 호스트에서 동일한 호스트 이름과 IP를 사용하려면 이전 서버의 연결을 끊습니다.

2. 새 Directory Server 12 호스트에서 다음 단계를 수행합니다.

a. **Directory Server 12를 설치합니다.**

b. **선택 사항: TLS 암호화를 구성합니다.**

- 새 설치에서 **Directory Server 10** 인스턴스와 다른 호스트 이름을 사용하는 경우 ***Red Hat Directory Server** 보안* 설명서의 **Directory Server에 대한 TLS 암호화 연결 활성화** 섹션을 참조하십시오.

- 이전 **Directory Server 10** 설치와 동일한 호스트 이름을 사용하려는 경우:

  i. 인스턴스를 중지합니다.

  ```
  # dsctl instance_name stop
  ```

  ii. 이미 존재하는 경우 **NSS(Network Security Services)** 데이터베이스와 **Directory Server**의 암호 파일을 제거합니다.

  ```
  # rm /etc/dirsrv/slapd-instance_name/cert*.db
  /etc/dirsrv/slapd-instance_name/key*.db
  /etc/dirsrv/slapd-instance_name/pin.txt
  ```

  iii. **Directory Server 10** 호스트에서 복사한 **cert8.db,key3.db, pin.txt** 파일을 **/etc/dirsrv/slapd-*instance_name*/** 디렉터리로 이동합니다.

  iv. **NSS** 데이터베이스 및 암호 파일에 대한 올바른 권한을 설정합니다.

  ```
  # chown dirsrv:root /etc/dirsrv/slapd-instance_name/cert8.db
  /etc/dirsrv/slapd-instance_name/key3.db
  /etc/dirsrv/slapd-instance_name/pin.txt

  # chmod 600 /etc/dirsrv/slapd-instance_name/cert8.db
  /etc/dirsrv/slapd-instance_name/key3.db
  /etc/dirsrv/slapd-instance_name/pin.txt
  ```

  v. 인스턴스를 시작합니다.

  ```
  # dsctl instance_name start
  ```

c.
사용자 지정 스키마를 사용한 경우 **99user.ldif** 파일을 **/etc/dirsrv/slapd-*instance_name*/schema/** 디렉터리에 복원한 후 적절한 권한을 설정한 다음 인스턴스를 다시 시작합니다.

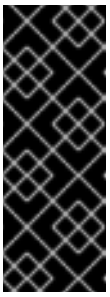
```
# cp /tmp/99user.ldif /etc/dirsrv/slapd-instance_name/schema/

# chmod 644 /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# chown root:root /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# dsctl instance_name restart
```

d.
준비한 **/tmp/userRoot.ldif** 파일을 **Directory Server 10** 호스트에서 **/var/lib/dirsrv/slapd-*instance_name*/ldif/** 디렉터리에 배치합니다.

e.
userRoot.ldif 파일을 가져와서 모든 항목이 있는 **userRoot** 백엔드를 복원합니다.

```
# dsconf -D 'cn=Directory Manager' ldap://server.example.com backend import
userRoot /var/lib/dirsrv/slapd-instance_name/ldif/userRoot.ldif
```

Directory Server 12는 **/var/lib/dirsrv/slapd-*instance_name*/** 디렉토리에서만 **LDIF** 파일을 가져올 수 있습니다.



중요

Directory Server 10 호스트에서 사용자 지정 구성을 사용한 경우 **Directory Server 12** 호스트의 **dse.ldif** 구성 파일을 이전 버전의 파일로 교체하지 마십시오. 대신 **dsconf** 유틸리티 또는 웹 콘솔을 사용하여 필요한 각 매개변수 및 플러그인에 대해 사용자 지정 구성을 수동으로 추가합니다.

10장. 암호 동기화 서비스 설치, 업데이트 및 설치 제거

Active Directory와 Red Hat Directory Server 간의 암호를 동기화하려면 암호 암호 동기화 서비스를 사용합니다. 암호 동기화 서비스를 설치, 업데이트 및 제거할 수 있습니다.

10.1. 암호 동기화 서비스

Active Directory를 사용하여 암호 동기화를 설정하면 Directory Server에서 암호를 제외한 사용자 개체의 모든 특성을 검색합니다. Active Directory는 암호화된 암호만 저장하지만 Directory Server는 다른 암호화를 사용합니다. 따라서 Active Directory 사용자 암호는 Directory Server에 의해 암호화되어야 합니다.

Active Directory와 Directory Server 간에 암호 동기화를 활성화하기 위해 Red Hat Directory 암호 동기화 서비스는 DC(Domain Controller)의 루틴을 변경하는 Windows 암호를 변경합니다. 사용자 또는 관리자가 암호를 설정하거나 업데이트하는 경우 서비스는 Active Directory에 암호화되어 저장되기 전에 일반 텍스트로 암호를 검색합니다. 이 프로세스를 통해 Red Hat Directory Password Sync 를 사용하여 일반 텍스트 암호를 Directory Server로 보낼 수 있습니다. 암호를 보호하기 위해 서비스는 Directory Server에 대한 LDAPS 연결만 지원합니다. Directory Server가 사용자 항목에 암호를 저장하면 암호는 Directory Server에 구성된 암호 저장 스키마로 자동 암호화됩니다.

중요

Active Directory에서 모든 쓰기 가능 DC는 암호 작업을 처리할 수 있습니다. 따라서 Active Directory 도메인의 모든 쓰기 가능 DC에 Red Hat Directory Password Sync 를 설치해야 합니다.

10.2. 암호 동기화 서비스 설치 관리자 다운로드

Red Hat Directory Password Sync 서비스를 설치하려면 고객 포털에서 설치 프로그램을 다운로드합니다.

사전 요구 사항

- 유효한 Red Hat Directory Server 서브스크립션이 있어야 합니다.
- Red Hat 고객 포털에 계정이 있습니다.

절차

1. Red Hat 고객 포털에 로그인합니다.

2. 페이지 상단에서 다운로드를 클릭합니다.

3. 제품 목록에서 **Red Hat Directory Server** 를 선택합니다.

4. **Version** 필드에서 **12** 를 선택합니다.

5. **PassSync** 설치 관리자 다운로드 .

6. 설치 프로그램을 모든 쓰기 가능 **Active Directory** 도메인 컨트롤러 **(DC)**에 복사합니다.

10.3. 암호 동기화 서비스 설치

이 섹션에서는 **Windows** 도메인 컨트롤러(**DC**)에 **Red Hat Directory Password Sync** 를 설치하는 방법을 설명합니다. 쓰기 가능한 모든 **Windows DC**에서 이 절차를 수행하십시오.

사전 요구 사항

- 최신 버전의 **PassSync** 설치 관리자를 **Windows Active Directory** 도메인 컨트롤러 **(DC)**에 다운로드했습니다.
- **Directory Server**에서 **TLS** 암호화를 활성화했습니다.
- **Active Directory** 도메인을 준비하셨습니다.
- **Directory Server**에서 동기화하기 위한 계정을 생성하셨습니다.

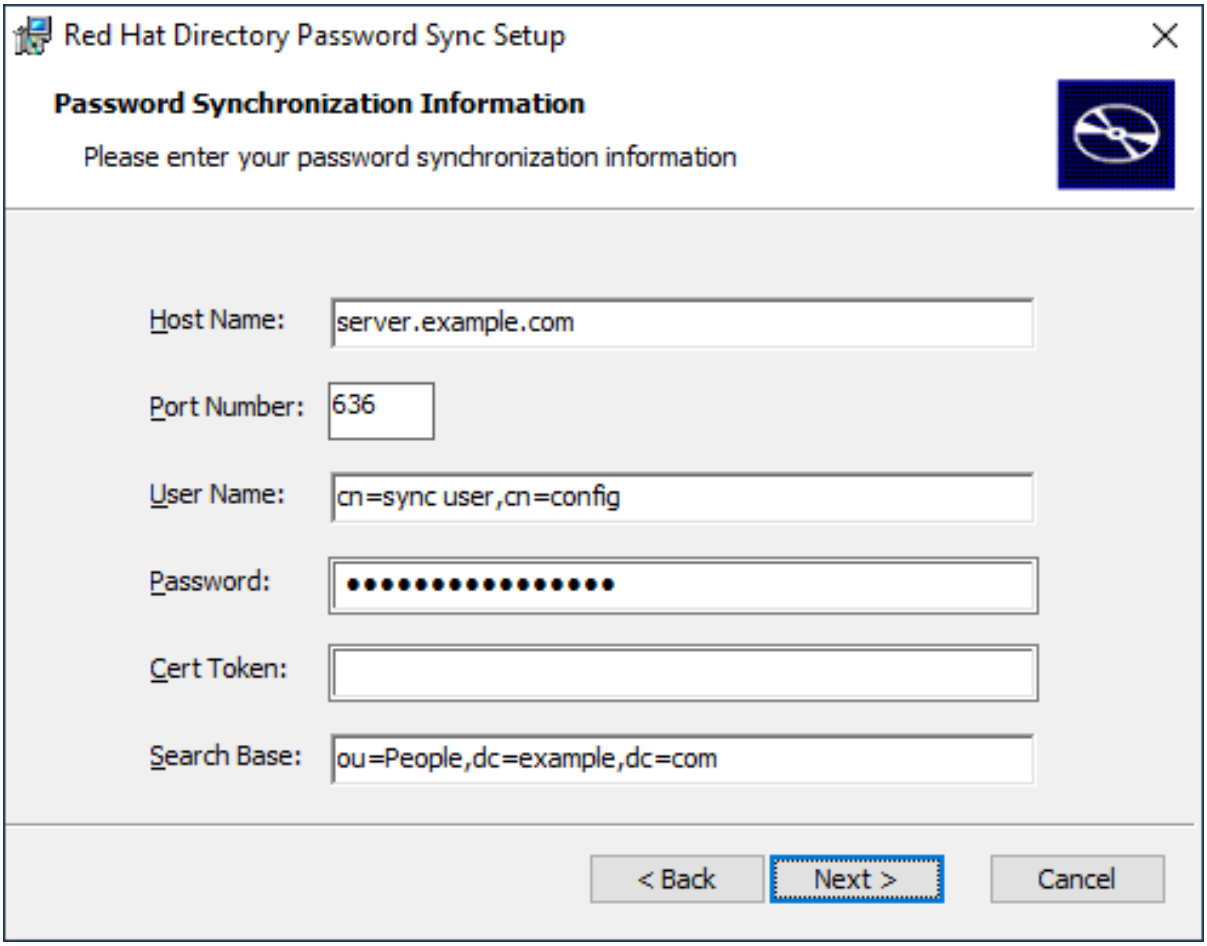
절차

1. **DC**에 소프트웨어를 설치할 수 있는 권한이 있는 사용자로 **Active Directory DC**에 로그인합니다.

2. **RedHat-PassSync-ds12.*-x86_64.msi** 파일을 두 번 클릭하여 설치합니다.

3. **Red Hat Directory Password Sync** 설정이 표시됩니다. 다음을 클릭합니다.

4. **Directory Server** 환경에 따라 필드를 작성합니다. 예를 들면 다음과 같습니다.



Directory Server 호스트의 다음 정보를 필드에 입력합니다.

- **Host Name: Directory Server** 호스트의 이름을 설정합니다. 또는 필드를 **Directory Server** 호스트의 **IPv4** 또는 **IPv6** 주소로 설정할 수 있습니다.

- 포트 번호: **LDAPS** 포트 번호를 설정합니다.

- **User Name:** 동기화 사용자 계정의 고유 이름(**DN**)을 설정합니다.

- **password:** 동기화 사용자의 암호를 설정합니다.
- 인증서 토큰**: Directory Server** 호스트에서 복사한 서버 인증서의 암호를 설정합니다.
- **search base:** 동기화된 사용자 계정이 포함된 **Directory Server** 항목의 **DN**을 설정합니다.

5. 다음을 클릭하여 설치를 시작합니다.
6. 완료 를 클릭합니다.
7. **Windows DC**를 재부팅합니다.

중요

DC를 재부팅하지 않으면 **PasswordHook.Subnet** 라이브러리 가 활성화되어 있지 않으며 암호 동기화가 실패합니다.

8. **Directory Server**에서 복제를 활성화하고 **WinSync** 계약을 만듭니다.

추가 리소스

- **Directory Server**에 대한 **TLS** 암호화 연결 활성화

10.4. 암호 동기화 서비스 업데이트

이 섹션에서는 **Windows** 도메인 컨트롤러(**DC**)에서 기존 **Red Hat Directory Password Sync** 설치를 업데이트하는 방법을 설명합니다.

쓰기 가능한 모든 **Windows DC**에서 이 절차를 수행하십시오.

사전 요구 사항

- **Red Hat Directory Password Sync** 가 **Windows DC**에서 실행되고 있습니다.

- 최신 버전의 **PassSync** 설치 관리자를 **Windows Active Directory DC**에 다운로드했습니다.

절차

1. **DC**에 소프트웨어를 설치할 수 있는 권한이 있는 사용자로 **Active Directory** 도메인 컨트롤러에 로그인합니다.

2. **RedHat-PassSync-ds12.*-x86_64.msi** 파일을 두 번 클릭합니다.

3. 다음을 클릭하여 설치를 시작합니다.

4. 수정 버튼을 클릭합니다.

5. 설정에는 이전 설치 중에 설정된 구성이 표시됩니다. 다음을 클릭하여 기존 설정을 유지합니다.

6. 다음을 클릭하여 설치를 시작합니다.

7. 완료 를 클릭합니다.

8. **Windows DC**를 재부팅합니다.

중요

DC를 재부팅하지 않으면 **PasswordHook.Subnet** 라이브러리 가 활성화되어 있지 않으며 암호 동기화가 실패합니다.

10.5. 암호 동기화 서비스 설치 제거

Red Hat Directory Password Sync 서비스가 더 이상 필요하지 않은 경우 **Active Directory** 도메인 컨

트롤러 (DC)에서 제거하십시오.

사전 요구 사항

- **Red Hat Directory Password Sync** 가 **Windows DC**에 설치되어 있습니다.

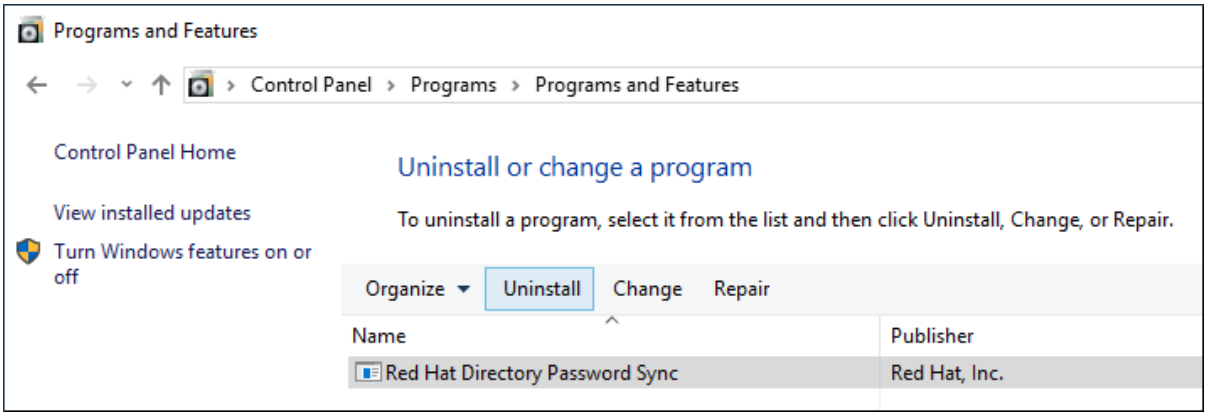
절차

DC에서 소프트웨어를 제거할 수 있는 권한이 있는 사용자로 **Active Directory** 도메인 컨트롤러에 로그인합니다.

1. 컨트롤 패널을엽니다.

2. 프로그램 및 프로그램 및 기능을클릭합니다.

3. **Red Hat Directory Password Sync** 항목을 선택하고 **Uninstall** 버튼을 클릭합니다.



4. **Yes** 를 클릭하여 확인합니다.

11장. DIRECTORY SERVER 인스턴스 제거

더 이상 **Directory Server** 인스턴스가 필요하지 않은 경우 이를 제거하여 디스크 공간을 복구할 수 있습니다. 한 서버에서 여러 인스턴스를 실행하는 경우 특정 인스턴스를 제거해도 다른 인스턴스에는 영향을 미치지 않습니다.

11.1. 명령줄을 사용하여 인스턴스 제거

명령줄을 사용하여 **Directory Server** 인스턴스를 제거할 수 있습니다.

사전 요구 사항

- 인스턴스가 복제 토폴로지에 포함된 경우 해당 인스턴스가 제거되었습니다.

절차

1. 선택 사항: **Directory Server** 디렉터리의 백업을 생성합니다.

   a. 인스턴스를 중지합니다.

   ```
   # dsctl instance_name stop
   ```

   b. **/var/lib/dirsrv/slapd-*instance_name*/** 디렉터리를 복사합니다.

   ```
   # cp -rp /var/lib/dirsrv/slapd-instance_name/ /root/var-lib-
   dirsrv-instance_name.bak/
   ```

   이 디렉터리에는 데이터베이스뿐만 아니라 백업 및 내보내기 디렉터리가 포함되어 있습니다.

   c. **/etc/dirsrv/slapd-*instance_name*/** 디렉터리를 복사합니다.

   ```
   # cp -rp /etc/dirsrv/slapd-instance_name/ /root/etc-dirsrv-instance_name.bak/
   ```

2. 인스턴스를 제거합니다.

   -

```
# dsctl instance_name remove --do-it
Removing instance ...
Completed instance removal
```

검증

- /var/lib/dirsrv/slapd-*instance_name*/ 및 /etc/dirsrv/slapd-*instance_name*/ 디렉터리가 제거되었는지 확인합니다.

```
# ls /var/lib/dirsrv/slapd-instance_name /etc/dirsrv/slapd-instance_name/
ls: cannot access '/var/lib/dirsrv/slapd-instance_name': No such file or directory
ls: cannot access '/etc/dirsrv/slapd-instance_name': No such file or directory
```

추가 리소스

- 복제 토폴로지에서 인스턴스 제거

11.2. 웹 콘솔을 사용하여 인스턴스 제거

웹 콘솔을 사용하여 Directory Server 인스턴스를 제거할 수 있습니다. 그러나 데이터베이스 및 구성 파일과 같이 포함된 Directory Server 디렉터리의 백업을 생성하려면 이러한 디렉터리를 명령줄에 복사해야 합니다.

사전 요구 사항

- 인스턴스가 복제 토폴로지에 포함된 경우 해당 인스턴스가 제거되었습니다.
- 웹 콘솔에서 인스턴스에 로그인되어 있습니다.

절차

1. 선택 사항: Directory Server 디렉터리의 백업을 생성합니다.
   a. Actions 버튼을 클릭하고 Stop instance 를 선택합니다.
   b. /var/lib/dirsrv/slapd-*instance_name*/ 디렉터리를 복사합니다.

```
# cp -rp /var/lib/dirsrv/slapd-instance_name/ /root/var-lib-dirsrv-instance_name.bak/
```

이 디렉터리에는 데이터베이스뿐만 아니라 백업 및 내보내기 디렉터리가 포함되어 있습니다.

c. /etc/dirsrv/slapd-*instance_name*/ 디렉터리를 복사합니다.

```
# cp -rp /var/lib/dirsrv/slapd-instance_name/ /root/etc-dirsrv-instance_name.bak/
```

2. **Actions** 버튼을 클릭하고 이 인스턴스 제거를 선택합니다.

3. **Yes, I am sure** 를 선택하고 **Remove Instance** 를 클릭하여 확인합니다.

검증

- /var/lib/dirsrv/slapd-*instance_name*/ 및 /etc/dirsrv/slapd-*instance_name*/ 디렉터리가 제거되었는지 확인합니다.

```
# ls /var/lib/dirsrv/slapd-instance_name /etc/dirsrv/slapd-instance_name/
ls: cannot access '/var/lib/dirsrv/slapd-instance_name': No such file or directory
ls: cannot access '/etc/dirsrv/slapd-instance_name': No such file or directory
```

추가 리소스

- 복제 토폴로지에서 인스턴스 제거

12장. DIRECTORY SERVER 설치 제거

더 이상 Directory Server 인스턴스가 필요하지 않은 경우 이를 제거하여 공간을 확보할 수 있습니다.

12.1. DIRECTORY SERVER 설치 제거

더 이상 서버에서 실행 중인 Directory Server가 필요하지 않은 경우 이 섹션에 설명된 대로 패키지를 제거합니다.

절차

1. 복제 토폴로지에서 모든 인스턴스를 제거합니다. 인스턴스가 복제 토폴로지의 멤버가 아닌 경우 이 단계를 건너뜁니다.

2. 서버에서 모든 인스턴스를 제거합니다. 각 인스턴스에 대해 다음을 입력합니다.

```
# dsctl instance_name remove --do-it
```

3. Directory Server 패키지를 제거합니다.

```
# dnf module remove redhat-ds
```

4. 선택 사항: dirsrv-12-for-rhel-8-x86_64-rpms 리포지토리를 비활성화합니다.

```
# subscription-manager repos --disable=dirsrv-12-for-rhel-8-x86_64-rpms
Repository 'dirsrv-12-for-rhel-8-x86_64-rpms' is disabled for this system.
```

5. 선택 사항: 시스템에서 Red Hat Directory Server 서브스크립션을 제거합니다.

중요

Directory Server보다 추가 제품을 제공하는 서브스크립션을 제거하면 이러한 제품의 패키지를 설치하거나 업데이트할 수 없습니다.

- 호스트에 연결된 서브스크립션을 나열합니다.

```
# subscription-manager list --consumed
Subscription Name:   Example Subscription
...
Pool-ID:             5ab6a8df96b03fd30aba9a9c58da57a1
...
```

- 이전 단계의 풀 ID를 사용하여 서브스크립션을 제거합니다.

```
# subscription-manager remove --pool=5ab6a8df96b03fd30aba9a9c58da57a1
2 local certificates have been deleted.
The entitlement server successfully removed these pools:
  5ab6a8df96b03fd30aba9a9c58da57a1
The entitlement server successfully removed these serial numbers:
  1658239469356282126
```

추가 리소스

- 복제 토폴로지에서 인스턴스 제거

13장. 웹 콘솔을 사용하여 DIRECTORY SERVER에 로그인

웹 콘솔은 관리 작업을 수행하는 데 사용할 수 있는 브라우저 기반 GUI(그래픽 사용자 인터페이스)입니다. Directory Server 패키지는 웹 콘솔의 Directory Server 사용자 인터페이스를 자동으로 설치합니다.

사전 요구 사항

- 웹 콘솔에 액세스할 수 있는 권한이 있습니다.

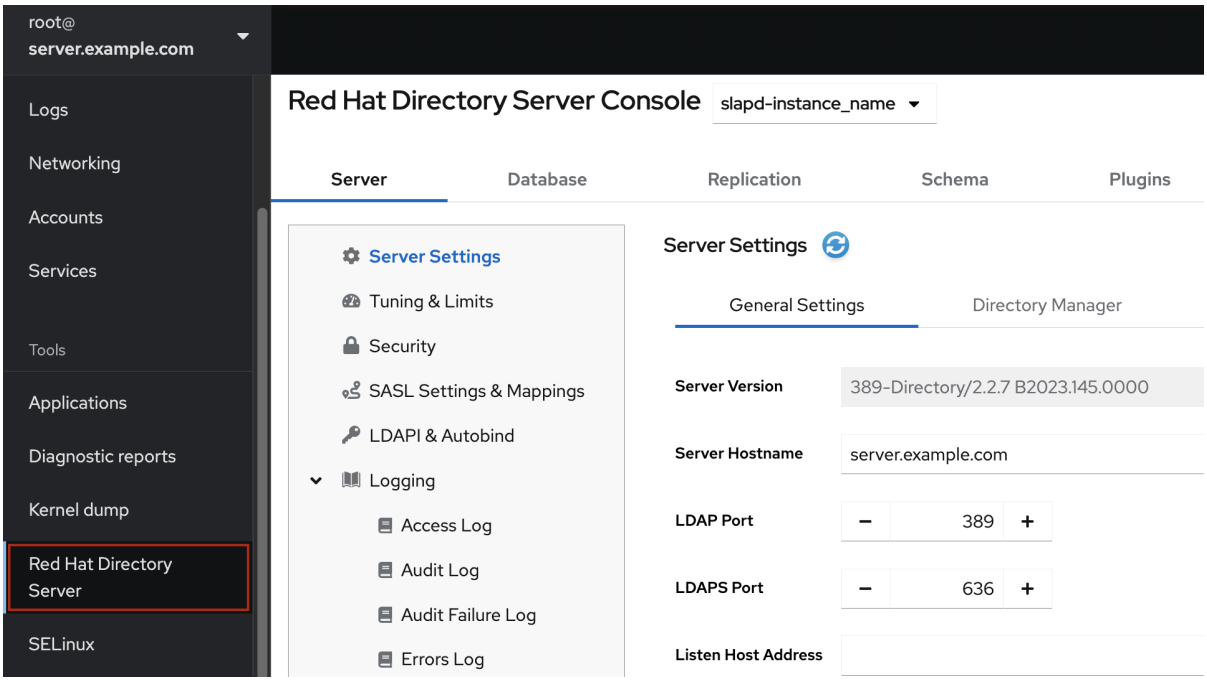
절차

1. 브라우저에서 다음 URL을 사용하여 웹 콘솔에 액세스합니다.

```
https://<directory_server_host>:9090
```

2. sudo 권한이 있는 사용자로 로그인합니다.

3. Red Hat Directory Server 항목을 선택합니다.



추가 리소스

- RHEL 웹 콘솔에 로그인.

14장. DIRECTORY SERVER 인스턴스 시작 및 중지

명령줄 또는 웹 콘솔을 사용하여 Directory Server 인스턴스를 시작, 중지 및 다시 시작할 수 있습니다.

14.1. 명령줄을 사용하여 DIRECTORY SERVER 인스턴스 시작 및 중지

dsctl 유틸리티를 사용하여 Directory Server 인스턴스를 시작, 중지 또는 다시 시작합니다.

중요

dsctl 유틸리티는 Directory Server 인스턴스를 중지하는 유일한 올바른 방법입니다. 데이터 손실 및 손상을 방지하기 위해 kill 명령을 사용하여 ns-slapd 프로세스를 종료하지 마십시오.

절차

- 인스턴스를 시작하려면 다음을 실행합니다.

```
# dsctl instance_name start
```

- 인스턴스를 중지하려면 다음을 실행합니다.

```
# dsctl instance_name stop
```

- 인스턴스를 다시 시작하려면 다음을 실행합니다.

```
# dsctl instance_name restart
```

선택적으로 시스템이 부팅될 때 Directory Server 인스턴스가 자동으로 시작되도록 활성화할 수 있습니다.

- 단일 인스턴스의 경우 다음을 실행합니다.

```
# systemctl enable dirsrv@instance_name
```

- 서버의 모든 인스턴스에 대해 다음을 실행합니다.

```
# systemctl enable dirsrv.target
```

검증

dsctl 또는 systemctl 유틸리티를 사용하여 인스턴스 상태를 확인할 수 있습니다.

- dsctl 유틸리티를 사용하여 인스턴스 상태를 보려면 다음을 실행합니다.

```
# dsctl instance_name status
```

- systemctl 유틸리티를 사용하여 인스턴스 상태를 보려면 다음을 실행합니다.

```
# systemctl status dirsrv@instance_name
```

추가 리소스

- systemctl을 사용하여 시스템 서비스 관리

14.2. 웹 콘솔을 사용하여 DIRECTORY SERVER 인스턴스 시작 및 중지

웹 콘솔을 사용하여 Directory Server 인스턴스를 시작, 중지 또는 다시 시작할 수 있습니다.

사전 요구 사항

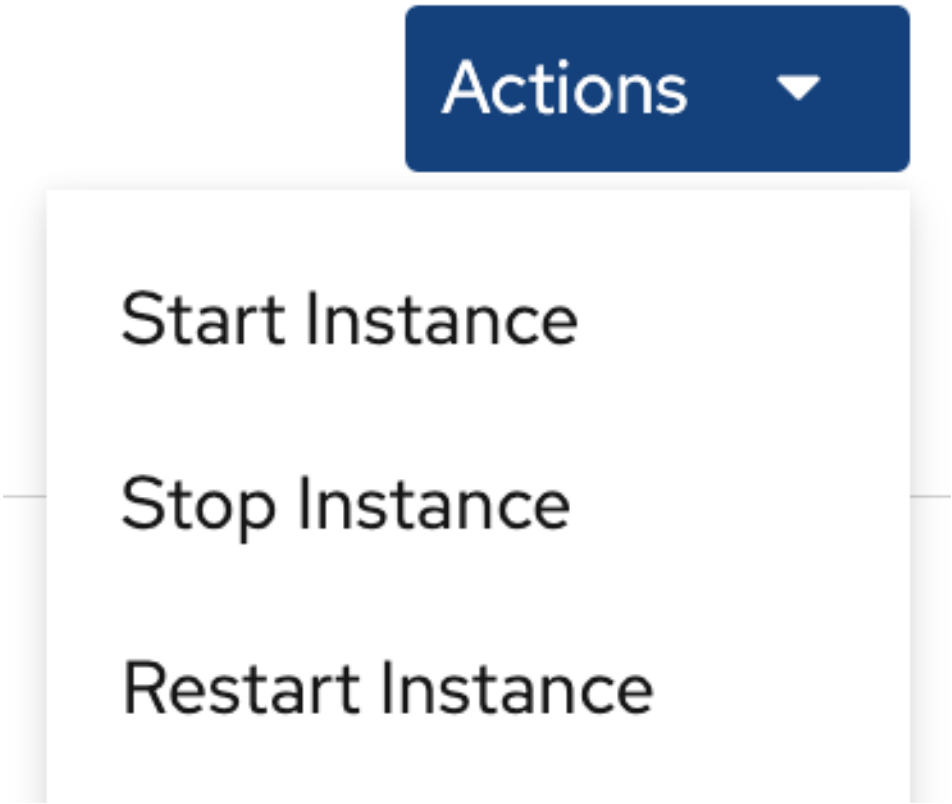
- 웹 콘솔에 로그인되어 있습니다. 자세한 내용은 다음을 참조하십시오.
- 웹 콘솔을 사용하여 Directory Server에 로그인

절차

1. Directory Server 인스턴스를 선택합니다.

2. 작업 버튼을 클릭하고 실행할 작업을 선택합니다.

- 인스턴스 시작
- 인스턴스 중지
- 인스턴스 재시작



검증

- **Directory Server** 인스턴스가 실행 중인지 확인합니다. 인스턴스가 실행되고 있지 않으면 웹 콘솔에 다음 메시지가 표시됩니다.

> **This server instance is not running, either start it from the Actions dropdown menu, or choose a different instance.**

15장. LDAP 및 LDAPS 포트 번호 변경

기본적으로 Directory Server는 LDAP에 포트 389 를 사용하고, 활성화하면 포트 636 을 LDAPS 프로토콜로 사용합니다. 예를 들어 포트 번호를 변경하여 한 호스트에서 여러 Directory Server 인스턴스를 실행할 수 있습니다.

중요

다른 서비스에서는 인스턴스에 대해 프로토콜에 할당한 새 포트를 사용해서는 안 됩니다.

15.1. 명령줄을 사용하여 포트 번호 변경

명령줄을 사용하여 LDAP 및 LDAPS 프로토콜의 포트 번호를 변경할 수 있습니다. LDAP 및 LDAPs 포트를 변경하려면 nsslapd-port 및 nsslapd-securePort 매개변수를 업데이트해야 합니다.

절차

1. 선택 사항: 인스턴스의 현재 포트 번호를 표시합니다.

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-port nsslapd-securePort
```

2. LDAP 포트 변경:

   a. LDAP 프로토콜의 새 포트를 설정합니다. 예를 들어 1389 로 설정하려면 다음을 실행합니다.

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-port=1389
```

   b. 이전 단계에서 할당한 LDAP 포트의 ldap_port_t 유형을 설정합니다.

```
# semanage port -a -t ldap_port_t -p tcp 1389
```

3. LDAPS 포트를 변경합니다.

a. LDAPS 프로토콜의 새 포트를 설정합니다. 예를 들어 1636 으로 설정하려면 다음을 실행합니다.

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
nsslapd-securePort=1636
```

b. 이전 단계에서 할당한 LDAPS 포트의 ldap_port_t 유형을 설정합니다.

```
# semanage port -a -t ldap_port_t -p tcp 1636
```

4. 인스턴스를 다시 시작합니다.

```
# dsctl instance_name restart
```

검증

1. Directory Server가 명령으로 새 LDAP 포트를 사용하는지 확인합니다.

```
# dsconf instance_name config get nsslapd-port
```

2. 이제 Directory Server가 명령으로 새 LDAPS 포트 번호를 사용하는지 확인합니다.

```
# dsconf instance_name config get nsslapd-securePort
```

추가 리소스

- nsslapd-securePort 매개변수에 대한 자세한 내용은 nsslapd-securePort 매개변수 설명을참조하십시오.
- nsslapd-port 매개변수에 대한 자세한 내용은 nsslapd-port 매개변수 설명을참조하십시오.

15.2. 웹 콘솔을 사용하여 포트 번호 변경

웹 콘솔을 사용하여 LDAP 및 LDAPS 프로토콜의 포트 번호를 변경할 수 있습니다.

사전 요구 사항

- 웹 콘솔에서 인스턴스에 로그인되어 있습니다.

절차

1. **LDAP** 포트 변경:
   a. **Server Setting** 메뉴를 엽니다.
   b. **Server Setting** 탭에서 새 포트 번호를 **LDAP Port** 필드에 입력합니다.
2. 저장을 클릭합니다.
3. **LDAPS** 포트를 변경합니다.
   a. **Server Setting** 메뉴를 엽니다.
   b. 일반 설정 탭에서 새 포트 번호를 **LDAPS** 포트 필드에 입력합니다.
   c. 저장을 클릭합니다.
4. 작업을 클릭하고 인스턴스 재시작 을 선택하여 인스턴스를 다시 시작합니다.

검증

1. 서버 설정에서 변경된 포트가 반영되는지 확인합니다.

추가 리소스

- 인스턴스를 다시 시작하는 방법에 대한 자세한 내용은 웹 콘솔을 사용하여 **Directory Server** 인스턴스 시작 및 중지를참조하십시오.
-

웹 콘솔을 사용하여 **Directory Server**에 로그인하는 방법에 대한 자세한 내용은 웹 콘솔 을 사용하여 **Directory Server** 로그인을참조하십시오.

16장. .DSRC 파일을 사용하여 DIRECTORY SERVER 명령줄 유틸리티의 기본 옵션 관리

~/.dsrc 파일은 Directory Server 명령줄 유틸리티를 사용하는 명령을 간소화합니다. 기본적으로 LDAP URL 또는 바인딩 고유 이름(DN)과 같은 정보를 이러한 유틸리티의 명령에 전달할 수 있습니다. 매번 이러한 설정을 지정하지 않고 명령줄 유틸리티를 사용하도록 ~/dsrc 파일에 설정을 저장할 수 있습니다.

16.1. .DSRC 파일이 명령을 간소화하는 방법

인스턴스의 LDAP URL과 ~/.dsrc 파일에 바인딩 DN을 지정할 수 있습니다.

```
# server1
uri = ldap://server1.example.com
binddn = cn=Directory Manager
basedn = dc=example,dc=com
```

이러한 설정으로 더 짧은 Directory Server 명령을 사용할 수 있습니다. 예를 들어 사용자 계정을 생성하려면 다음을 수행합니다.

```
# dsidm server1 user create
```

~/.dsrc 파일이 없으면 명령에 bind DN, LDAP URL, 기본 DN을 지정해야 합니다.

```
# dsidm -D cn=Directory Manager ldap://server1.example.com -b "dc=example,dc=com" user
create
```

16.2. DSCTL 유틸리티를 사용하여 .DSRC 파일 생성

dsctl 유틸리티를 사용하여 수동으로 생성하는 대신 ~/.dsrc 파일을 생성할 수 있습니다.

절차

- 다음을 실행합니다.

```
# dsctl instance_name dsrc create ...
```

다음 옵션을 명령에 추가할 수 있습니다.

- **--uri**

--uri 옵션을 사용하는 경우 **protocol://host_name_or_IP_address_or_socket**형식의 **URL**을 인스턴스로 설정합니다.

예를 들면 다음과 같습니다.

a. **--uri ldap://server.example.com**

b. **--uri = ldaps://server.example.com**

c. **--uri = ldapi://%%2fvar%%2frun%%2fslapd-instance_name.socket**

Directory Server 소켓의 경로를 설정하면 경로에 슬래시 (/) 대신 **%%02** 를 사용합니다.

중요

서버는 **ldapi URL**을 사용할 때 **Directory Server** 명령줄 유틸리티를 실행하는 사용자의 사용자 **ID(UID)** 및 그룹 **ID(GID)**를 식별합니다. **root** 사용자로 명령을 실행하면 **UID**와 **GID**가 모두 **0** 이고 **Directory Server**는 해당 암호를 입력하지 않고 **cn=Directory Manager** 로 자동으로 인증합니다.

- **--starttls**

--starttls 옵션을 사용하는 경우 **LDAP** 포트에 연결할 유틸리티를 구성한 다음 **STARTTLS** 명령을 전송하여 암호화된 연결로 전환합니다.

- **--basedn**

-basedn 옵션을 사용하는 경우 기본 고유 이름(**DN**)을 설정합니다.

예: --basedn dc=example,dc=com

- --binddn

-basedn 옵션을 사용하는 경우 바인딩 DN을 설정합니다.

예: --binddn cn=Directory Manager

- --pwdfile

--pwdfile 을 사용하는 경우 바인딩 DN의 암호가 포함된 파일의 경로를 설정합니다.

예: --pwdfile /root/rhds.pwd

- --tls-cacertdir

--tls-cacertdir 옵션을 사용하는 경우 LDAPS 연결을 사용하는 경우 서버의 인증서를 확인하는 데 필요한 CA(인증 기관) 인증서가 있는 디렉터리를 정의하는 이 매개변수의 경로를 설정합니다.

예: --tls-cacertdir /etc/pki/CA/certs/

참고

CA 인증서를 지정된 디렉터리에 복사하는 경우에만 c_rehash /etc/pki/CA/certs/ 명령을 사용할 수 있습니다.

- --tls-cert

--tls-certl 옵션을 사용하는 경우 서버 인증서의 절대 경로를 설정합니다.

예: **--tls-cert /etc/dirsrv/slapd-instance_name/Server-Cert.crt**

- **--tls-key**

--tls-key 옵션을 사용하는 경우 서버의 개인 키에 대한 절대 경로를 설정합니다.

예: **--tls-key /etc/dirsrv/slapd-instance_name/Server-Cert.key**

- **--tls-reqcert**

--tls-reqcert 옵션을 사용하는 경우 **TLS** 세션의 서버 인증서에 클라이언트 유틸리티가 수행하는 검사를 설정합니다.

예: **--tls-reqcert hard**

이러한 매개변수를 사용할 수 있습니다.

a. **Never:** 유틸리티는 서버 인증서를 요청하거나 확인하지 않습니다.

b. **allow:** 유틸리티는 인증서 오류를 무시하고 연결이 어쨌든 설정됩니다.

c. **hard:** 유틸리티는 인증서 오류에 대한 연결을 종료합니다.

- **--saslmech**

--saslmech 옵션을 사용하는 경우 **SASL** 메커니즘을 **PLAIN** 또는 **EXTERNAL** 로 설정합니다.

예: **--saslmech PLAIN**

16.3. 디렉터리 서버 유틸리티를 사용할 때 원격 및 로컬 연결 확인

Directory Server 연결을 보호 할 때 **Directory Server** 명령을 원격으로 및 로컬로 호출할 수 있습니다. **LDAP URL**을 지정하여 **Directory Server** 명령을 실행하면 서버에서 원격 연결로 간주하고 시스템 전체 설정과 함께 **/etc/openldap/ldap.conf** 구성 파일을 확인하여 명령을 진행합니다.

지정된 인스턴스 이름을 사용하여 **Directory Server** 명령을 실행하면 서버에서 **~/.dsrc** 파일이 있는지 확인하고 다음 논리를 적용하여 계속 진행합니다.

1. **Directory Server**는 **~/.dsrc** 파일을 원격 연결로 간주하고 **/etc/openldap/ldap.conf** 구성 파일과 시스템 전체 설정에 인스턴스 이름과 **LDAP URL**이 모두 포함되어 있는지 확인합니다.

2. 디렉터리 서버는 **~/.dsrc** 파일을 로컬 연결로 간주하고 로컬 **dse.ldif** 파일의 **nsslapd-certdir** 설정을 사용하여 **~/.dsrc** 파일에 지정된 인스턴스 이름만 포함하거나 **~/.dsrc** 파일이 없는 경우 연결을 보호합니다. **nsslapd-certdir** 이 없는 경우 서버는 기본 경로 **/etc/dirsrv/slapd-instance_name/** 을 사용하여 인스턴스의 **NSS(Network Security Services)** 데이터베이스를 저장합니다.

추가 리소스

- **nsslapd-certdir** 매개변수

17장. 테스트 항목 생성

dsctl ldifgen 명령은 다양한 유형의 테스트 항목이 있는 **LDIF** 파일을 생성합니다. 예를 들어 이 **LDIF** 파일을 사용하여 테스트 인스턴스 또는 하위 트리를 채워 **Directory Server**의 성능을 예제 항목으로 테스트할 수 있습니다.

17.1. 생성할 수 있는 테스트 항목 개요

다음 엔트리 유형 인수 중 하나를 **dsctl ldifgen** 에 전달할 수 있습니다.

- **users:** 사용자 항목이 포함된 **LDIF** 파일을 생성합니다.
- **groups:** 정적 그룹 및 멤버 항목이 포함된 **LDIF** 파일을 만듭니다.
- **Cos-def:** 고전적인 포인터 또는 간접 서비스 클래스(**CoS**) 정의를 포함하는 **LDIF** 파일을 만듭니다.
- **cos-template: CoS** 템플릿이 포함된 **LDIF** 파일을 만듭니다.
- **roles:** 관리, 필터링된 또는 간접 역할 항목이 포함된 **LDIF** 파일을 만듭니다.
- **MOD-load:** 수정 작업이 포함된 **LDIF** 파일을 만듭니다. **ldapmodify** 유틸리티를 사용하여 파일을 디렉터리에 로드합니다.
- 중첩된: 계단식 또는 골절 트리 설계에 크게 중첩된 항목이 포함된 **LDIF** 파일을 만듭니다.

참고

dsctl ldifgen 명령은 LDIF 파일만 생성합니다. 파일을 Directory Server 인스턴스에 로드하려면 다음을 사용합니다.

- mod-load 옵션을 사용하여 LDIF 파일을 생성한 후 ldapmodify 유틸리티
- 기타 모든 옵션에 대한 ldapadd 유틸리티

중첩된 항목 유형을 제외하고 명령줄 옵션을 제공하지 않으면 dsctl ldifgen 명령에서 대화형 모드를 사용합니다.

```
# dsctl instance_name ldifgen entry_type
```

17.2. 예제 사용자 항목을 사용하여 LDIF 파일 생성

dsctl ldifgen users 명령을 사용하여 예제 사용자 항목이 있는 LDIF 파일을 만듭니다.

절차

1. 예를 들어, /tmp/users.ldif 라는 LDIF 파일을 생성하고, dc=example,dc=com 접미사에 CloudEvent 일반 사용자를 추가하려면 다음을 입력합니다.

```
# dsctl instance_name ldifgen users --suffix "dc=example,dc=com" --number 100000 --
generic --ldif-file=/tmp/users.ldif
```

이 명령은 다음 OU(조직 단위)를 생성하고 이러한 OU에 사용자를 무작위로 할당합니다.

- ou=accounting
- ou=product development
- ou=product testing

- **ou=human** 리소스
- **ou=payroll**
- **ou=people**
- **ou=groups**

자세한 내용 및 기타 옵션을 사용하여 **LDIF** 파일을 만들려면 다음을 입력합니다.

```
# dsctl instance_name ldifgen users --help
```

2. 선택 사항: 디렉터리에 테스트 항목을 추가합니다.

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/users.ldif
```

17.3. 예제 그룹 항목을 사용하여 LDIF 파일 생성

dsctl ldifgen groups 명령을 사용하여 예제 사용자 항목이 있는 **LDIF** 파일을 생성합니다.

절차

1. 예를 들어 **ou=groups,dc=example,dc=com** 항목에 **500** 그룹을 추가하고 각 그룹에 **100**개의 멤버가 있는 **LDIF** 파일을 생성하려면 **/tmp/groups.ldif** 라는 **LDIF** 파일을 생성합니다.

```
# dsctl instance_name ldifgen groups --number 500 --suffix "dc=example,dc=com" --
parent "ou=groups,dc=example,dc=com" --num-members 100 --create-members --
member-parent "ou=People,dc=example,dc=com" --ldif-file /tmp/groups.ldif
example_group__
```

이 명령은 또한 **LDIF** 문을 생성하여 **ou=People,dc=example,dc=com** 의 사용자 항목을 추가합니다.

자세한 내용 및 기타 옵션을 사용하여 **LDIF** 파일을 만들려면 다음을 입력합니다.

```
# dsctl instance_name ldifgen groups --help
```

2. 선택 사항: 디렉터리에 테스트 항목을 추가합니다.

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/groups.ldif
```

17.4. 예제 COS 정의를 사용하여 LDIF 파일 생성

dsctl ldifgen cos-def 명령을 사용하여 **CoS(Class of Service)** 정의를 사용하여 **LDIF** 파일을 생성합니다.

절차

1. 예를 들어 **ou=cos-definitions,dc=example,dc=com** 항목에 클래식 **CoS** 정의를 추가하는 **LDIF** 파일 **/tmp/cos-definition.ldif** 를 생성하려면 다음을 입력합니다.

```
# dsctl instance_name ldifgen cos-def Postal_Def --type classic --parent "ou=cos
definitions,dc=example,dc=com" --cos-specifier businessCatagory --cos-template
"cn=sales,cn=classicCoS,dc=example,dc=com" --cos-attr postalcode
telephonenumber --ldif-file /tmp/cos-definition.ldif
```

자세한 내용 및 기타 옵션을 사용하여 **LDIF** 파일을 만들려면 다음을 입력합니다.

```
# dsctl instance_name ldifgen cos-def --help
```

2. 선택 사항: 디렉터리에 테스트 항목을 추가합니다.

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/cos-definition.ldif
```

17.5. 예제 수정 문을 사용하여 LDIF 파일 생성

dsctl ldifgen mod-load 명령을 사용하여 업데이트 작업이 포함된 **LDIF** 파일을 생성합니다.

절차

1. 예를 들어 **/tmp/modifications.ldif** 라는 **LDIF** 파일을 생성하려면 다음을 수행합니다.

```
# dsctl instance_name ldifgen mod-load --num-users 1000 --create-users --
parent="ou=People,dc=example,dc=com" --mod-attrs="sn" --add-users 10 --modrdn-
users 100 --del-users 100 --delete-users --ldif-file=/tmp/modifications.ldif
```

이 명령은 다음을 수행하는 문을 사용하여 /tmp/modifications.ldif 파일이라는 파일을 생성합니다.

- 1000개의 ADD 작업이 포함된 LDIF 파일을 생성하여 ou=People,dc=example,dc=com 에 사용자 항목을 생성합니다.
- sn 속성을 변경하여 모든 항목을 수정합니다.
- 10개의 사용자 항목을 추가합니다.
- 100개의 MODRDN 작업을 수행합니다.
- 100개 항목 삭제
- 끝에 남아 있는 모든 항목을 삭제

  자세한 내용 및 기타 옵션을 사용하여 LDIF 파일을 만들려면 다음을 입력합니다.

  ```
  # dsctl instance_name ldifgen mod-load --help
  ```

2. 선택 사항: 디렉터리에 테스트 항목을 추가합니다.

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/modifications.ldif
```

17.6. 중첩된 예제 항목을 사용하여 LDIF 파일 생성

dsctl ldifgen nested 명령을 사용하여 고도로 중첩된 cascading fractal 구조를 포함하는 LDIF 파일을 생성합니다.

절차

1. 예를 들어, /tmp/nested.ldif 라는 LDIF 파일을 생성하려면 dc=example,dc=com 항목 아래의 OU(전체 조직 단위)에 600명의 사용자를 추가하고, 각 OU는 최대 100명의 사용자 수를 포함하는 100명의 사용자를 입력합니다.

```
# dsctl instance_name ldifgen nested --num-users 600 --node-limit 100 --suffix
"dc=example,dc=com" --ldif-file /tmp/nested.ldif
```

자세한 내용 및 기타 옵션을 사용하여 LDIF 파일을 만들려면 다음을 입력합니다.

```
# dsctl instance_name ldifgen nested --help
```

2. 선택 사항: 디렉터리에 테스트 항목을 추가합니다.

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/nested.ldif
```