Red Hat Directory Server 12

Red Hat Directory Server のインストール

Directory Server のインストール、更新、およびアンインストールを管理する手順と、インスタンスの操作を開始するために必要となる基本的なタスク

Last Updated: 2024-09-19

Red Hat Directory Server 12 Red Hat Directory Server のインストール

Directory Server のインストール、更新、およびアンインストールを管理する手順と、インスタンスの操作を開始するために必要となる基本的なタスク

法律上の通知

概要

コマンドラインまたは Web コンソールを使用して、Directory Server 12 と関連サービスをインストール、更新、およびアンインストールします。FIPS モードでインスタンスを実行する方法、テストエントリーを作成する方法、Web コンソールにログインする方法、Directory Server インスタンスを起動および停止する方法、LDAP および LDAPS ポート番号を変更する方法について説明します。

目次

RED HAT DIRECTORY SERVER に関するフィードバックの提供

Red Hat のドキュメントおよび製品に関するご意見をお待ちしております。ドキュメントの改善点があればお知らせください。以下の方法で送信してください。

- Jira を通じて Red Hat Directory Server ドキュメントに関するフィードバックを送信する場合 (アカウントが必要):
  1. Red Hat Issue Tracker にアクセスしてください。
  2. **Summary** フィールドにわかりやすいタイトルを入力します。
  3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
  4. ダイアログの下部にある **Create** をクリックします。
- Jira を通じて Red Hat Directory Server 製品に関するフィードバックを送信する場合 (アカウントが必要):
  1. Red Hat Issue Tracker にアクセスしてください。
  2. **Create Issue** ページで、**Next** をクリックします。
  3. **Summary** フィールドに入力します。
  4. **Component** フィールドでコンポーネントを選択します。
  5. **Description** フィールドに以下の内容を入力します。
     a. 選択したコンポーネントのバージョン番号。
     b. 問題を再現するための手順、または改善のための提案。
  6. **Create** をクリックします。

第1章 .INF ファイルを使用したコマンドラインで新規インスタンスの設定

コマンドラインで **.inf** ファイルを使用して Directory Server を設定すると、高度な設定をカスタマイズできます。たとえば、**.inf** ファイルで以下の設定をカスタマイズできます。

- サービスの開始後に **ns-slapd** Directory Server プロセスが使用しているユーザーおよびグループ。別のユーザーおよびグループを使用する場合、ユーザーおよびグループは、インストールを開始する前に手動で作成する必要があります。
- 設定、バックアップ、データディレクトリーなどのパス。
- 証明書の有効性

1.1. 前提条件

- Red Hat Directory Server 12 リリースノート で説明されているように、サーバーが、最新の Red Hat Directory Server バージョンの要件を満たしている。

1.2. DIRECTORY SERVER パッケージのインストール

以下の手順に従って、Directory Server パッケージをインストールします。

前提条件

- システムを Red Hat サブスクリプション管理サービスに登録する。
- Red Hat アカウントに有効な Red Hat Directory Server サブスクリプションがある。
- RHEL のデフォルトのリポジトリー **BaseOS** および **AppStream** が有効になっている。

手順

1. アカウントで Simple Content Access (SCA) が無効になっている場合、以下を実行します。
   a. Red Hat Directory Server サブスクリプションを提供する Red Hat アカウントで利用可能なサブスクリプションをリスト表示し、プール ID をメモします。

```
# 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. プール ID を使用して、Red Hat Directory Server サブスクリプションをシステムに割り当てます。

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

2. Directory Server リポジトリーを有効にします。たとえば、Directory Server 12.4 リポジトリーを有効にするには、次のコマンドを実行します。

```
# 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** モジュールをインストールします。

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

このコマンドにより、必要な依存関係がすべて自動的にインストールされます。

関連情報

- Red Hat Subscription Manager の使用
- Simple Content Access
- What are the names of the Red Hat repositories that have to be enabled

1.3. DIRECTORY SERVER インスタンスインストール用の .INF ファイルの作成

dscreate ユーティリティー用の **.inf** ファイルを作成し、お使いの環境にファイルを調整します。後のステップで、このファイルを使用して新しい Directory Server インスタンスを作成します。

前提条件

- **redhat-ds:12** モジュールがインストールされている。

手順

1. **dscreate create-template** コマンドを使用して、**.inf** テンプレートを作成します。たとえば、テンプレートを **/root/instance_name.inf** ファイルに保存するには、次のコマンドを実行します。

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

作成したファイルには、説明を含む利用可能なすべてのパラメーターが含まれます。

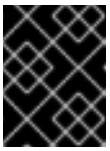
2. 前の手順で作成したファイルを編集します。

   a. インストールをカスタマイズするように設定するパラメーターのコメントを解除します。すべてのパラメーターにデフォルト値があります。ただし、Red Hat は、実稼働環境用に特定のパラメーターをカスタマイズすることを推奨します。たとえば、**[slapd]** セクションに少なくとも以下のパラメーターを設定します。

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

   b. インスタンスの作成時に接尾辞を自動的に作成するには、**[backend-userroot]** セクションに次のパラメーターを設定します。

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



重要

インスタンスの作成時に接尾辞を作成しない場合は、後で、このインスタンスにデータを保存する前に手動で作成する必要があります。

c. 必要に応じて、他のパラメーターのコメントを解除し、お使いの環境に適切な値に設定します。たとえば、これらのパラメーターを使用して、認証認証情報や変更ログのトリミングなどのレプリケーションオプションを指定したり、LDAP および LDAPS プロトコルに異なるポートを設定したりします。

注記

デフォルトでは、作成する新規インスタンスには自己署名証明書と TLS 有効化が含まれます。Red Hat では、セキュリティーを強化するために、この機能を無効にしないことを推奨します。自己署名証明書は、後で認証局 (CA) が発行する証明書に置き換えることができること注意してください。

関連情報

- Directory Server への TLS 暗号化接続の有効化

1.4. .INF ファイルを使用した新しい DIRECTORY SERVER インスタンスの設定

本セクションでは、**.inf** ファイルを使用して、コマンドラインを使用して新しい Directory Server インスタンスを設定する方法を説明します。

前提条件

- Directory Server インスタンスの **.inf** ファイルが作成されている。

手順

1. **.inf** ファイルを **dscreate from-file** コマンドに渡して、新しいインスタンスを作成します。

```
# 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 ユーティリティーはインスタンスを自動的に起動し、システムの起動時に RHEL がサービスを開始するように設定します。

2. ファイアウォールで必要なポートを開きます。

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

3. ファイアウォール設定を再読み込みします。

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

第2章 インタラクティブインストーラーを使用してコマンドラインで新規インスタンスの設定

管理者は、新規インスタンスの設定に関する質問に回答して、Directory Server インタラクティブインストーラーが新規インスタンスを設定できます。

インストール時に追加設定をカスタマイズする場合は、インタラクティブインストーラーの代わりに **.inf** ファイルを使用します。詳細は、*1章.inf ファイルを使用したコマンドラインで新規インスタンスの設定* を参照してください。

2.1. 前提条件

- Red Hat Directory Server 12 リリースノート で説明されているように、サーバーが、最新の Red Hat Directory Server バージョンの要件を満たしている。

2.2. DIRECTORY SERVER パッケージのインストール

以下の手順に従って、Directory Server パッケージをインストールします。

前提条件

- システムを Red Hat サブスクリプション管理サービスに登録する。
- Red Hat アカウントに有効な Red Hat Directory Server サブスクリプションがある。
- RHEL のデフォルトのリポジトリー **BaseOS** および **AppStream** が有効になっている。

手順

1. アカウントで Simple Content Access (SCA) が無効になっている場合、以下を実行します。
   a. Red Hat Directory Server サブスクリプションを提供する Red Hat アカウントで利用可能なサブスクリプションをリスト表示し、プール ID をメモします。

```
# 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. プール ID を使用して、Red Hat Directory Server サブスクリプションをシステムに割り当てます。

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

2. Directory Server リポジトリーを有効にします。たとえば、Directory Server 12.4 リポジトリーを有効にするには、次のコマンドを実行します。

```
# 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** モジュールをインストールします。

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

このコマンドにより、必要な依存関係がすべて自動的にインストールされます。

関連情報

- Red Hat Subscription Manager の使用
- Simple Content Access
- What are the names of the Red Hat repositories that have to be enabled

2.3. インタラクティブインストーラーを使用したインスタンスの作成

本セクションでは、対話型インストーラーを使用して、新しい Directory Server インスタンスを作成する方法を説明します。

手順

1. 対話型インストーラーを起動します。

```
# dscreate interactive
```

2. 対話型インストーラーの質問に答えます。
インストーラーのほとんどの質問の後ろにある角括弧内に表示されるデフォルト値を使用するには、値を入力せずに **Enter** キーを押します。

```
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
```

注記

クリアテキストでパスワードを設定する代わりに、**pwdhash** ユーティリティーで生成された **{algorithm}hash** 文字列を設定できます。

3. ファイアウォールで必要なポートを開きます。

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

4. ファイアウォール設定を再読み込みします。

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

第3章 WEB コンソールを使用した新規インスタンスの設定

Directory Server のセットアップにブラウザーベースのインターフェイスを使用する場合は、Directory Server Web コンソールを使用できます。

3.1. 前提条件

- Red Hat Directory Server 12 リリースノート で説明されているように、サーバーが、最新の Red Hat Directory Server バージョンの要件を満たしている。
- Directory Server パッケージのインストール の説明に従って Directory Server パッケージをインストールしている。

3.2. WEB コンソールで新しい DIRECTORY SERVER インスタンスの設定

本セクションでは、Web コンソールを使用して、新しい Directory Server インスタンスを設定する方法を説明します。

前提条件

- Web コンソールパッケージ **cockpit** がインストールされます。
- **cockpit.socket** systemd ユニットが有効化されて起動しています。
- ローカルファイアウォールでポート **9090** を開いて、Web コンソールへのアクセスを許可しました。

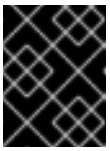
手順

1. ブラウザーを使用して、Directory Server ホストのポート 9090 で実行している Web コンソールに接続します。

   https://server.example.com:9090

2. **root** ユーザー、または sudo 権限を持つユーザーとしてログインします。
3. **Red Hat Directory Server** エントリーを選択します。
4. 新規インスタンスを作成します。
   - サーバーにインスタンスが存在しない場合は、**Create New Instance** ボタンをクリックします。
   - サーバーが既存のインスタンスを実行している場合は、**Actions** を選択し、**Create New Instance** をクリックします。
5. **Create New Server Instance** フォームのフィールドに入力します。
   - **Instance Name**: インスタンスの名前を設定します。インスタンスの作成後にインスタンス名を変更することはできません。
   - **Port**: LDAP プロトコルのポート番号を設定します。ポートは、別のインスタンスまたはサービスが使用中にすることはできません。デフォルトのポートは 389 です。

- **Secure Port**: LDAPS プロトコルのポート番号を設定します。ポートは、別のインスタンスまたはサービスが使用中にすることはできません。デフォルトのポートは 636 です。
- **Create Self-Signed TLS Certificate DB**: インスタンスで TLS 暗号化を有効にし、自己署名証明書を作成します。
  セキュリティーを強化するために、Red Hat は、自己署名証明書と TLS を有効にして新規インスタンスを作成することを推奨します。自己署名証明書は、後で認証局 (CA) が発行する証明書に置き換えることができること注意してください。
- **Directory Manager DN**: インスタンスの管理ユーザーの識別名 (DN) を設定します。デフォルト値は **cn=Directory Manager** です。
- **Directory Manager Password**: インスタンスの管理ユーザーのパスワードを設定します。
- **Confirm Password**: **Directory Manager Password** フィールドと同じ値に設定されていることを確認します。
- **Create Database**: このフィールドを選択すると、インスタンスの作成中に接尾辞が自動的に作成されます。



重要

インスタンスの作成時に接尾辞を作成しない場合は、後で、このインスタンスにデータを保存する前に手動で作成する必要があります。

このオプションを有効にした場合は、追加フィールドに入力します。

  - **Database Suffix**: バックエンドの接尾辞を設定します。
  - **Database Name**: バックエンドデータベースの名前を設定します。
  - **Database Initialization**: このフィールドを **Create Suffix Entry** に設定します。

6. **Create Instance** をクリックします。
   新しいインスタンスが起動し、システムの起動時に自動的に起動するように設定されています。
7. ファイアウォールで必要なポートを開きます。

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

8. ファイアウォール設定を再読み込みします。

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

関連情報

- Directory Server への TLS 暗号化接続の有効化

第4章 NON-ROOT ユーザーとして新しいインスタンスを設定

root 権限がない場合は、Directory Server のインストールをユーザーとして実行できます。この方法を使用して、Directory Server をテストし、LDAP アプリケーションを開発します。ただし、**non-root** ユーザーが実行するインスタンスには、次のような制限があることに注意してください。

- Simple Network Management Protocol (SNMP) はサポートしていません。
- 1024 以上のポートのみを使用できます。

4.1. ユーザーとして DIRECTORY SERVER をインストールするための環境の準備

root 権限がない場合、Directory Server インスタンスを作成および管理する前に、**dscreate ds-root** コマンドを使用して適切な環境を準備する必要があります。

前提条件

- **root** ユーザーとして Directory Server パッケージをインストールしている。

手順

1. PATH 変数に **$HOME/bin** があることを確認します。そうでない場合は、以下を行います。
   a. ~/**.bash_profile** ファイルに以下を追加します。

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

   b. ~/**bash_profile** ファイルを再読み込みします。

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

2. カスタムの場所を使用するようにインスタンス作成環境を設定します。

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

   このコマンドは、標準のインストールパスを **$HOME/dsroot/** に置き換え、標準の Directory Server 管理ユーティリティーのコピーを **$HOME/bin/** ディレクトリーに作成します。

3. シェルが新しいパスを使用するようにするには、以下を行います。
   a. キャッシュをクリアします。

   ```
   $ hash -r dscreate
   ```

   b. シェルがコマンドへの正しいパスを使用していることを確認します。

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

dscreate コマンドで、シェルが /**usr/bin/dscreate** の代わりに **$HOME/bin/dscreate** を使用するようになりました。

4.2. NON-ROOT ユーザーとして新しいインスタンスをインストール

root 権限なしで Directory Server をインストールする場合、対話型インストーラを使用できます。インストール後、Directory Server はカスタムの場所にインスタンスを作成し、ユーザーは通常どおり **dscreate**、**dsctl**、**dsconf** ユーティリティーを実行できます。

前提条件

- non-root インストール用の環境を準備している。
- **firewall-cmd** ユーティリティーを使用するための **sudo** 権限がある (外部から Directory Server インスタンスを使用できるようにする場合)。

手順

1. 対話型インストーラーを使用したインスタンスの作成
   a. 対話型インストーラーを起動します。

```
$ dscreate interactive
```

   b. 対話型インストーラーの質問に答えます。
   インストーラーのほとんどの質問の後ろにある角括弧内に表示されるデフォルト値を使用するには、値を入力せずに **Enter** キーを押します。

注記

インストール中に、**1024 より大きい** インスタンスポートとセキュアポートの番号 (たとえば 1389 と 1636) を選択する必要があります。選択しない場合、ユーザーは特権ポート (1-1023) にバインドする権限を持ちません。

```
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
```

注記

クリアテキストでパスワードを設定する代わりに、**pwdhash** ユーティリティーで生成された **{algorithm}hash** 文字列を設定できます。

2. オプション: 外部から Directory Server インスタンスを使用できるようにする場合、以下を行います。

   a. ファイアウォールでポートを開きます。

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

   b. ファイアウォール設定を再読み込みします。

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

検証

- **ldapsearch** コマンドを実行して、ユーザーがインスタンスに接続できることをテストします。

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

関連情報

- non-root ユーザーによるインストールのための環境の準備
- non-root 権限で 1024 未満のポートをバインドする方法

第5章 ロードバランサーの背後で KERBEROS 認証を使用した DIRECTORY SERVER のインストール

ロードバランサーの背後で動作し、Kerberos 認証をサポートする Directory Server インスタンスをインストールするには、インストール中に比較する追加の手順が必要です。

Generic Security Services API (GSSAPI) を使用してサービスにアクセスする場合、Kerberos プリンシパルにはサービスのホストの DNS 名が含まれます。ユーザーがロードバランサーに接続する場合、プリンシパルにはロードバランサーの DNS 名 (例: **ldap/loadbalancer.example.com@EXAMPLE.COM**) が含まれ、Directory Server インスタンスの DNS 名ではありません。

正常に接続するには、リクエストを受け取る Directory Server インスタンスは、ロードバランサーの DNS 名が異なる場合でもロードバランサーと同じ名前を使用する必要があります。

このセクションでは、ロードバランサーの背後で Kerberos 認証をサポートする Directory Server インスタンスを設定する方法について説明します。

5.1. 前提条件

- Red Hat Directory Server 12 リリースノート で説明されているように、サーバーが、最新の Red Hat Directory Server バージョンの要件を満たしている。

5.2. DIRECTORY SERVER パッケージのインストール

以下の手順に従って、Directory Server パッケージをインストールします。

前提条件

- システムを Red Hat サブスクリプション管理サービスに登録する。
- Red Hat アカウントに有効な Red Hat Directory Server サブスクリプションがある。
- RHEL のデフォルトのリポジトリー **BaseOS** および **AppStream** が有効になっている。

手順

1. アカウントで Simple Content Access (SCA) が無効になっている場合、以下を実行します。
   a. Red Hat Directory Server サブスクリプションを提供する Red Hat アカウントで利用可能なサブスクリプションをリスト表示し、プール ID をメモします。

```
# 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. プール ID を使用して、Red Hat Directory Server サブスクリプションをシステムに割り当てます。

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

2. Directory Server リポジトリーを有効にします。たとえば、Directory Server 12.4 リポジトリーを有効にするには、次のコマンドを実行します。

```
# 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** モジュールをインストールします。

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

このコマンドにより、必要な依存関係がすべて自動的にインストールされます。

関連情報

- Red Hat Subscription Manager の使用
- Simple Content Access
- What are the names of the Red Hat repositories that have to be enabled

5.3. DIRECTORY SERVER インスタンスインストール用の .INF ファイルの作成

dscreate ユーティリティー用の **.inf** ファイルを作成し、お使いの環境にファイルを調整します。後のステップで、このファイルを使用して新しい Directory Server インスタンスを作成します。

前提条件

- **redhat-ds:12** モジュールがインストールされている。

手順

1. **dscreate create-template** コマンドを使用して、**.inf** テンプレートを作成します。たとえば、テンプレートを **/root/instance_name.inf** ファイルに保存するには、次のコマンドを実行します。

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

作成したファイルには、説明を含む利用可能なすべてのパラメーターが含まれます。

2. 前の手順で作成したファイルを編集します。

   a. インストールをカスタマイズするように設定するパラメーターのコメントを解除します。すべてのパラメーターにデフォルト値があります。ただし、Red Hat は、実稼働環境用に特定のパラメーターをカスタマイズすることを推奨します。たとえば、**[slapd]** セクションに少なくとも以下のパラメーターを設定します。

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

b. GSSAPI 認証でロードバランサーの背後でインスタンスを使用するには、**[general]** セクションの **full_machine_name** パラメーターを、Directory Server ホストの FQDN ではなく、ロードバランサーの完全修飾ドメイン名 (FQDN) に設定します。

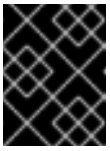
```
full_machine_name = loadbalancer.example.com
```

c. **[general]** セクションの **strict_host_checking** パラメーターのコメントを解除して、**False** に設定します。

```
strict_host_checking = False
```

d. インスタンスの作成時に接尾辞を自動的に作成するには、**[backend-userroot]** セクションに次のパラメーターを設定します。

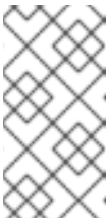
```
create_suffix_entry = True
suffix = dc=example,dc=com
```



重要

インスタンスの作成時に接尾辞を作成しない場合は、後で、このインスタンスにデータを保存する前に手動で作成する必要があります。

e. 必要に応じて、他のパラメーターのコメントを解除し、お使いの環境に適切な値に設定します。たとえば、これらのパラメーターを使用して、認証認証情報や変更ログのトリミングなどのレプリケーションオプションを指定したり、LDAP および LDAPS プロトコルに異なるポートを設定したりします。



注記

デフォルトでは、作成する新規インスタンスには自己署名証明書と TLS 有効化が含まれます。Red Hat では、セキュリティーを強化するために、この機能を無効にしないことを推奨します。自己署名証明書は、後で認証局 (CA) が発行する証明書に置き換えることができること注意してください。

関連情報

- Directory Server への TLS 暗号化接続の有効化

5.4. .INF ファイルを使用した新しい DIRECTORY SERVER インスタンスの設定

本セクションでは、**.inf** ファイルを使用して、コマンドラインを使用して新しい Directory Server インスタンスを設定する方法を説明します。

前提条件

- Directory Server インスタンスの **.inf** ファイルが作成されている。

手順

1. **.inf** ファイルを **dscreate from-file** コマンドに渡して、新しいインスタンスを作成します。

```
# 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 ユーティリティーはインスタンスを自動的に起動し、システムの起動時に RHEL がサービスを開始するように設定します。

2. ファイアウォールで必要なポートを開きます。

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

3. ファイアウォール設定を再読み込みします。

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

5.5. ロードバランサーのキータブの作成、およびキータブを使用するように DIRECTORY SERVER の設定

ユーザーが GSSAPI を使用してロードバランサーの背後にある Directory Server に対して認証できるようにするには、ロードバランサー用に Kerberos プリンシパルを作成し、Directory Server が Kerberos プリンシパルを使用するように設定します。本セクションでは、この手順を説明します。

前提条件

- 以下の **.inf** ファイル設定を含むインスタンス:
  - **full_machine_name** パラメーターがロードバランサーの DNS 名に設定された。
  - **strict_host_checking** パラメーターが **False** に設定されています。

手順

1. ロードバランサーの Kerberos プリンシパルを作成します (例: **ldap/loadbalancer.example.com_@_EXAMPLE.COM**)。サービスプリンシパルを作成する手順は、Kerberos インストールによって異なります。詳細は、Kerberos サーバーのドキュメントを参照してください。

2. 必要に応じて、キータブファイルにさらにプリンシパルを追加できます。たとえば、ユーザーが Kerberos 認証を使用してロードバランサーの背後にある Directory Server インスタンスに直接接続できるようにするには、Directory Server ホスト用に追加のプリンシパルを追加します。たとえば、**ldap/server1.example.com@EXAMPLE.COM** です。

3. サービスのキータブファイルを Directory Server ホストにコピーし、たとえば **/etc/dirsrv/slapd-instance_name/ldap.keytab** ファイルに保存します。

4. サービスキータブへのパスを **/etc/sysconfig/slapd-instance_name** ファイルに追加します。

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

5. Directory Server インスタンスを再起動します。

```
# dsctl instance_name restart
```

検証

- GSSAPI プロトコルを使用してロードバランサーに接続できることを確認します。

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

Directory Server ホスト自体など、キータブファイルに Kerberos プリンシパルを追加した場合は、この接続を確認します。

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

第6章 DIRECTORY SERVER を FIPS モードで実行する

Directory Server は、連邦情報処理標準 (FIPS) 140-2 を完全にサポートします。Directory Server を FIPS モードで実行すると、セキュリティー関連の設定が変更されます。たとえば、SSL は自動的に無効になり、TLS 1.2 および 1.3 暗号化のみが使用されます。

6.1. FIPS モードの有効化

Directory Server を Federal Information Processing Standard (FIPS) モードで使用するには、RHEL および Directory Server でモードを有効にします。

前提条件

- RHEL で FIPS モードを有効にしました。

手順

1. ネットワークセキュリティーサービス (NSS) データベースの FIPS モードを有効にします。

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

2. インスタンスを再起動します。

```
# dsctl instance_name restart
```

検証

- NSS データベースで FIPS モードが有効になっていることを確認します。

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

モジュールが FIPS モードの場合、このコマンドは **FIPS mode enabled** を返します。

6.2. 関連情報

- FIPS (Federal Information Processing Standard)
- FIPS モードへのシステムの切り替え

第7章 DIRECTORY SERVER を新しいマイナーバージョンに更新

Red Hat は Red Hat Directory Server 12 の更新バージョンを頻繁にリリースします。本セクションでは、Directory Server パッケージを更新する方法を説明します。

代わりに、Red Hat Directory Server 11 をバージョン 12 に移行する場合は、Migrating Directory Server 11 to Directory Server 12 を参照してください。

7.1. DIRECTORY SERVER パッケージの更新

dnf ユーティリティーを使用してモジュールを更新します。これにより、関連するパッケージも自動的に更新されます。次の手順では、Directory Server をバージョン 12.3 から 12.4 に更新します。

前提条件

- サーバーに Red Hat Directory Server 12.3 がインストールされている。
- Red Hat アカウントに有効な Red Hat Directory Server サブスクリプションがある。

手順

1. Directory Server 12.3 リポジトリーを無効にします。

```
# 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 リポジトリーを有効にします。

```
# 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 パッケージを更新します。

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

dnf module update redhat-ds コマンドは、Directory Server パッケージとその依存関係をバージョン 12.4 に更新します。

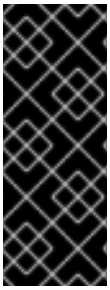
更新プロセスは、サーバー上のすべてのインスタンスの **dirsrv** サービスを自動的に再起動します。

関連情報

- What are the names of the Red Hat repositories that have to be enabled

第8章 DIRECTORY SERVER 11 から DIRECTORY SERVER 12 への移行

移行を開始する前に実行する必要があるタスクなど、Red Hat Directory Server 11 から 12 への移行を説明します。



重要

Red Hat は、Red Hat Directory Server 10 または 11 からバージョン 12 への移行のみをサポートしています。Directory Server を以前のバージョンから移行するには、Directory Server 10 または 11 への増分移行を実行する必要があります。

Red Hat は、**leapp** アップグレードツールを使用した Directory Server 10 または 11 サーバーのバージョン 12 へのインプレースアップグレードをサポート **しません**。

8.1. 前提条件

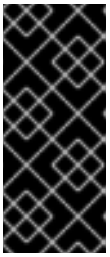
- 既存の Directory Server インストールはバージョン 11 で実行し、利用可能な更新がすべてインストールされています。

8.2. レプリケーション方法を使用した DIRECTORY SERVER 12 への移行

レプリケーショントポロジーでは、レプリケーション方法を使用して Directory Server 12 に移行します。

手順

1. Directory Server 12 をインストールします。
2. Directory Server 12 ホストでレプリケーションを有効にしますが、レプリカ合意は作成しないでください。レプリケーションの有効化の詳細は、**Red Hat Directory Server 12**の レプリケーションの設定および管理 に関するドキュメントを参照してください。
3. Directory Server 11 ホストでレプリケーションを有効にし、Directory Server 12 ホストを参照するレプリカ合意を作成します。詳細は、**Red Hat Directory Server 11 管理者ガイド** の マルチサプライヤーのレプリケーション セクションを参照してください。



重要

dse.ldif のレイアウトがバージョン間で異なるため、Directory Server 11 ホストでカスタム設定を使用した場合は、Directory Server 12 ホストの **dse.ldif** 設定ファイルを Directory Server 11 ホストのファイルで **置き換えない** でください。代わりに、**dsconf** ユーティリティーまたは Web コンソールを使用して、必要なパラメーターおよびプラグインごとにカスタム設定を追加してください。

4. 必要に応じて、Directory Server 12 ホスト間で、レプリカ合意のある追加の Directory Server 12 ホストを設定します。
5. Directory Server 12 ホストのみを使用するようにクライアントを設定します。
6. Directory Server 11 ホストで、Directory Server 12 ホストを参照するレプリカ合意を削除します。**Red Hat Directory Server 11 管理者ガイド** の レプリケーショントポロジーからの Directory Server インスタンスの削除 を参照してください。

7. Directory Server 11 ホストをアンインストールします。**Red Hat Directory Server 11 インストールガイド** の Directory Server のアンインストール を参照してください。

8.3. エクスポートおよびインポートの方法を使用した DIRECTORY SERVER 12 への移行

エクスポートおよびインポートの方法を使用して、小規模な Directory Server 環境 (レプリケーションのないインスタンスなど) を移行します。

手順

1. 既存の Directory Server 11 ホストで以下の手順を実行します。

   a. **dirsrv** サービスを停止し、無効にします。

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

   b. バックエンドをエクスポートします。たとえば、**userRoot** バックエンドをエクスポートして **/var/lib/dirsrv/slapd-instance_name/userRoot.ldif** ファイルに保存するには、次を実行します。

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

   c. Directory Server 12 をインストールする新しいホストに以下のファイルをコピーします。

   - 前の手順でエクスポートした **/var/lib/dirsrv/slapd-instance_name/userRoot.ldif** ファイル
   - **/etc/dirsrv/slapd-instance_name/dse.ldif** 設定ファイル

   重要

   dse.ldif のレイアウトがバージョン間で異なるため、Directory Server 12 ホストの **dse.ldif** 設定ファイルを Directory Server 11 ホストのファイルで **置き換えない** でください。参照用に **dse.ldif** ファイルを保存してください。

   - カスタムムスキーマを使用する場合、**/etc/dirsrv/slapd-instance_name/schema/99user.ldif**
   - TLS が有効なインスタンスを移行し、Directory Server 12 のインストールに同じホスト名を再利用するには、以下のファイルを新しいホストにコピーします。
     - **/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 ホストの同じホスト名および IP を再利用するには、ネットワークから古いサーバーを切断します。

2. 新規ホストで以下の手順を実行します。

   a. Directory Server 12 をインストールします。

   b. 必要に応じて、TLS 暗号化を設定します。

      - 新規インストールで Directory Server 11 インスタンスとは異なるホスト名を使用する場合は、**Red Hat Directory Server のセキュリティー保護** ドキュメントの Directory Server への TLS 暗号化接続の有効化 セクションを参照してください。

      - 以前の Directory Server 11 インストールと同じホスト名を使用するには、以下を実行します。

        i. インスタンスを停止します。

        ```
        # dsctl instance_name stop
        ```

        ii. Network Security Services (NSS) データベース、および Directory Server のパスワードファイルが存在する場合は削除します。

        ```
        # 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 ホストからコピーした **cert9.db** ファイル、**key4.db** ファイル、および **pin.txt** ファイルを **/etc/dirsrv/slapd-instance_name/** ディレクトリーに配置します。

        iv. NSS データベースおよびパスワードファイルに適切なパーミッションを設定します。

        ```
        # 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. インスタンスを起動します。

        ```
        # dsctl instance_name start
        ```

   c. カスタムスキーマを使用している場合は、**99user.ldif** ファイルを **/etc/dirsrv/slapd-instance_name/schema/** ディレクトリーに配置し、適切なパーミッションを設定してインスタンスを再起動します。

   ```
   # 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 ファイルをインポートします。たとえば、**/var/lib/dirsrv/slapd- instance_name /ldif/migration.ldif** ファイルを **userRoot** データベースにインポートするには:

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

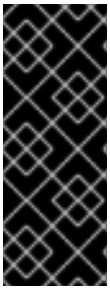
Directory Server では、インポートする LDIF ファイルが **/var/lib/dirsrv/slapd-instance_name/** ディレクトリーに必要であることに注意してください。

重要

Directory Server 11 ホストでカスタム設定を使用した場合は、Directory Server 12 ホストの **dse.ldif** 設定ファイルを Directory Server 11 ホストのファイルで **置き換えない** でください。代わりに、**dsconf** ユーティリティーまたは Web コンソールを使用して、必要なパラメーターおよびプラグインごとにカスタム設定を手動で追加してください。

第9章 DIRECTORY SERVER 10 から DIRECTORY SERVER 12 への移行

移行を開始する前に実行する必要があるタスクなど、Red Hat Directory Server 10 から 12 への移行について説明します。



重要

Red Hat は、Red Hat Directory Server 10 または 11 からバージョン 12 への移行のみをサポートしています。Directory Server を以前のバージョンから移行するには、Directory Server 10 または 11 への増分移行を実行する必要があります。

Red Hat は、**leapp** アップグレードツールを使用した Directory Server 10 または 11 サーバーのバージョン 12 へのインプレースアップグレードをサポート **しません**。

9.1. 前提条件

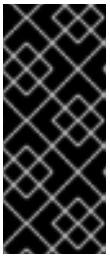
- 既存の Directory Server インストールはバージョン 10 で実行し、利用可能な更新がすべてインストールされています。

9.2. レプリケーション方法を使用した DIRECTORY SERVER 10 からバージョン 12 への移行

レプリケーショントポロジーでは、レプリケーション方法を使用して Directory Server 12 に移行します。

手順

1. 新しいホストに Directory Server 12 をインストールします。
2. Directory Server 12 ホストでレプリケーションを有効にしますが、レプリカ合意は作成しないでください。レプリケーションの有効化の詳細は、**Red Hat Directory Server 12** ドキュメントの レプリケーションの設定および管理 を参照してください。
3. Directory Server 10 ホストでレプリケーションを有効にし、Directory Server 12 ホストを参照するレプリカ合意を作成します。レプリケーションの有効化の詳細は、Red Hat Directory Server 10 管理ガイド の第 15 章「レプリケーションの管理」を参照してください。



重要

dse.ldif のレイアウトがバージョン間で異なるため、Directory Server 10 ホストでカスタム設定を使用した場合は、Directory Server 12 ホストの **dse.ldif** 設定ファイルを以前のバージョンのファイルで **置き換えない** でください。代わりに、**dsconf** ユーティリティーまたは Web コンソールを使用して、必要なパラメーターおよびプラグインごとにカスタム設定を追加してください。

4. 必要に応じて、Directory Server 12 ホスト間で、レプリカ合意のある追加の Directory Server 12 ホストを設定します。
5. Directory Server 12 ホストのみを使用するようにクライアントを設定します。
6. Directory Server 10 ホストで、Directory Server 12 ホストを参照するレプリカ合意を削除します。

```
# 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 ホストをアンインストールします。Red Hat Directory Server 10 Installation Guide の第 4.8 章「Directory Server のアンインストール」を参照してください。

9.3. エクスポートおよびインポート方法を使用した DIRECTORY SERVER 10 からバージョン 12 への移行

エクスポートおよびインポート方法を使用して、大規模な Directory Server 環境を移行します。

手順

1. 既存の Directory Server 10 ホストで以下の手順を実行します。
   a. **dirsrv** サービスを停止し、無効にします。

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

   b. バックエンドをエクスポートします。たとえば、**userRoot** バックエンドをエクスポートし、これを **/tmp/userRoot.ldif** ファイルに保存するには、以下を行います。

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

   c. Directory Server 12 をインストールする新しいホストに以下のファイルをコピーします。
      - 前のステップでエクスポートした LDIF ファイル **userRoot.ldif**
      - カスタムスキーマを使用する場合、**/etc/dirsrv/slapd-instance_name/schema/99user.ldif** ファイル
      - **/etc/dirsrv/slapd-instance_name/dse.ldif** 設定ファイル

      重要

      dse.ldif のレイアウトがバージョン間で異なるため、Directory Server 12 ホストの **dse.ldif** 設定ファイルを Directory Server 10 ホストのファイルで **置き換えない** でください。参照用に **dse.ldif** ファイルを保存してください。

      - TLS が有効なインスタンスを移行し、Directory Server 12 のインストールに同じホスト名を再利用するには、以下をコピーします。
        - **/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 ホストの同じホスト名および IP を再利用するには、ネットワークから古いサーバーを切断します。

2. 新しい Directory Server 12 ホストで以下の手順を実行します。

   a. Directory Server 12 をインストールします。

   b. 必要に応じて、TLS 暗号化を設定します。

      - 新規インストールで Directory Server 10 インスタンスとは異なるホスト名を使用する場合は、**Red Hat Directory Server のセキュリティー保護** ドキュメントの Directory Server への TLS 暗号化接続の有効化 セクションを参照してください。

      - 以前の Directory Server 10 インストールと同じホスト名を使用するには、以下を実行します。

        i. インスタンスを停止します。

        ```
        # dsctl instance_name stop
        ```

        ii. Network Security Services (NSS) データベース、および Directory Server のパスワードファイルが存在する場合は削除します。

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

        iii. **/etc/dirsrv/slapd-instance_name/** ディレクトリーの Directory Server 10 ホストからコピーした **cert8.db** ファイル、**key3.db** ファイル、および **pin.txt** ファイルを移動します。

        iv. NSS データベースおよびパスワードファイルに適切なパーミッションを設定します。

        ```
        # 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. インスタンスを起動します。

        ```
        # dsctl instance_name start
        ```

   c. カスタムスキーマを使用している場合は、**99user.ldif** ファイルを **/etc/dirsrv/slapd-instance_name/schema/** ディレクトリーに復元し、適切なパーミッションを設定してインスタンスを再起動します。

   ```
   # 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. Directory Server 10 ホストで準備した **/tmp/userRoot.ldif** ファイルを **/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーに配置します。

e. **userRoot.ldif** ファイルをインポートして、すべてのエントリーで **userRoot** バックエンドを復元します。

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

Directory Server 12 は、**/var/lib/dirsrv/slapd-instance_name/** ディレクトリーからのみ LDIF ファイルをインポートできます。

重要

Directory Server 10 ホストでカスタム設定を使用した場合は、Directory Server 12 ホストの **dse.ldif** 設定ファイルを以前のバージョンのファイルで **置き換えない** でください。代わりに、**dsconf** ユーティリティーまたは Web コンソールを使用して、必要なパラメーターおよびプラグインごとにカスタム設定を手動で追加してください。

第10章 パスワード同期サービスのインストール、更新、およびアンインストール

Active Directory と Red Hat Directory Server との間でパスワードを同期するには、パスワードの同期サービスを使用します。パスワード同期サービスをインストール、更新、および削除できます。

10.1. パスワードの同期サービス

Active Directory とパスワードの同期を設定すると、Directory Server は、パスワード以外のユーザーオブジェクトの属性をすべて取得します。Active Directory は暗号化されたパスワードのみを保存しますが、Directory Server が異なる暗号化を使用します。したがって、Active Directory ユーザーのパスワードを Directory Server で暗号化する必要があります。

Active Directory と Directory Server 間のパスワード同期を有効にするために、**Red Hat Directory Password Sync** サービスは、ドメインコントローラー (DC) の Windows パスワード変更ルーチンにフックアップします。ユーザーまたは管理者がパスワードを設定または更新すると、サービスは、暗号化して Active Directory に保存する前に、プレーンテキストでパスワードを取得します。このプロセスにより、**Red Hat Directory パスワード同期** によりプレーンテキストのパスワードが Directory Server に送信できるようになります。このパスワードを保護するため、サービスは Directory Server への LDAPS 接続のみをサポートします。Directory Server がパスワードをユーザーのエントリーに保存すると、Directory Server に設定したパスワードストレージスキームでパスワードが自動的に暗号化されます。

重要

Active Directory では、書き込み可能なすべての DC がパスワードアクションを処理できます。したがって、Active Directory ドメインのすべての書き込み可能な DC に **Red Hat Directory パスワード同期** をインストールする必要があります。

10.2. パスワード同期サービスインストーラーのダウンロード

Red Hat Directory パスワード同期 サービスをインストールするには、カスタマーポータルからインストーラーをダウンロードします。

前提条件

- 有効な Red Hat Directory Server サブスクリプションがあります。
- Red Hat カスタマーポータル にアカウントがあります。

手順

1. Red Hat カスタマーポータル にログインします。
2. ページ上部の **ダウンロード** をクリックします。
3. 製品リストから **Red Hat Directory Server** を選択します。
4. **Version** フィールドで **12** を選択します。
5. **PassSync Installer** をダウンロードします。
6. インストーラーを、書き込み可能なすべての Active Directory ドメインコントローラー (DC) にコピーします。

10.3. パスワード同期サービスのインストール

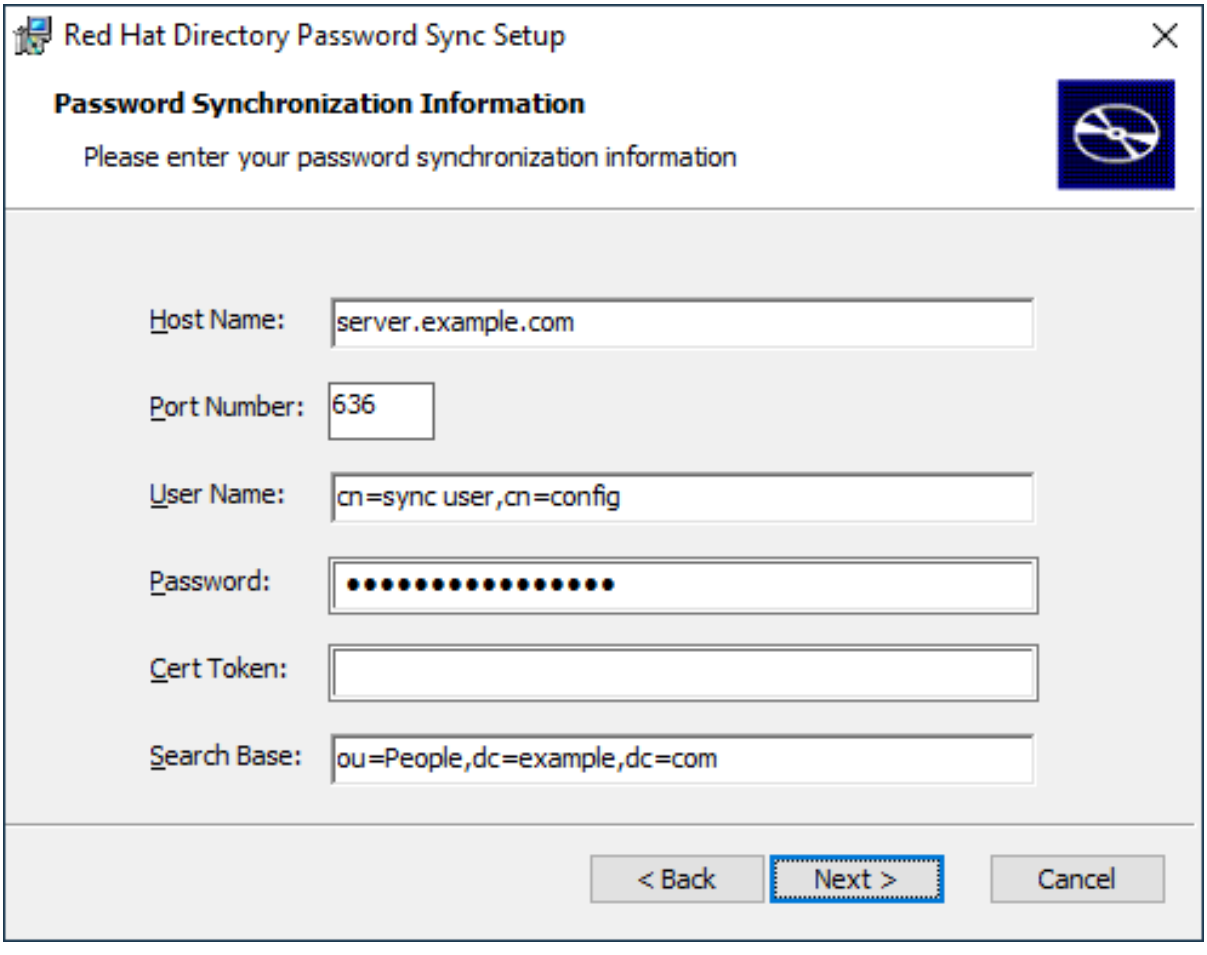
本セクションでは、Windows ドメインコントローラー (DC) に **Red Hat Directory パスワード同期** をインストールする方法を説明します。書き込み可能なすべての Windows DC でこの手順を実行します。

前提条件

- Windows Active Directory ドメインコントローラー (DC) に最新バージョンの **PassSync Installer** をダウンロードしています。
- Directory Server で TLS 暗号化を有効にしています。
- Active Directory ドメインを準備しています。
- Directory Server で同期用のアカウントを作成しています。

手順

1. DC にソフトウェアをインストールする権限を持つユーザーで Active Directory DC にログインします。
2. **RedHat-PassSync-ds12.*-x86_64.msi** ファイルをダブルクリックしてインストールします。
3. **Red Hat Directory パスワード同期セットアップ** が表示されます。**次へ** をクリックします。
4. Directory Server 環境に応じてフィールドに入力します。以下に例を示します。



Directory Server ホストの以下の情報をフィールドに入力します。

- **Host Name**: Directory Server ホストの名前を設定します。または、このフィールドを Directory Server ホストの IPv4 アドレスまたは IPv6 アドレスに設定できます。
- **Port Number**: LDAPS ポート番号を設定します。
- **User Name**: 同期ユーザーアカウントの識別名 (DN) を設定します。
- **Password**: 同期ユーザーのパスワードを設定します。
- **Cert Token**: Directory Server ホストからコピーされたサーバー証明書のパスワードを設定します。
- **Search Base**: 同期されたユーザーアカウントが含まれる Directory Server エントリーの DN を設定します。

5. **Next** をクリックしてインストールを開始します。
6. **Finish** をクリックします。
7. Windows DC を再起動します。

重要

DC を再起動すると、**PasswordHook.dll** ライブラリーが有効ではなく、パスワードの同期に失敗します。

8. Directory Server でレプリケーションを有効にし、WinSync 同意を作成します。

関連情報

- Directory Server への TLS 暗号化接続の有効化

10.4. パスワード同期サービスの更新

本セクションでは、Windows ドメインコントローラー (DC) での既存の **Red Hat Directory パスワード同期** インストールを更新する方法を説明します。

書き込み可能なすべての Windows DC でこの手順を実行します。

前提条件

- **Red Hat Directory Password Sync** が Windows DC で実行している。
- **PassSync Installer** の最新バージョンを Windows Active Directory DC にダウンロードしています。

手順

1. DC にソフトウェアをインストールする権限を持つユーザーで Active Directory ドメインコントローラーにログインします。
2. **RedHat-PassSync-ds12.*-x86_64.msi** ファイルをダブルクリックします。
3. **Next** をクリックしてインストールを開始します。

4. **Modify** ボタンをクリックします。
5. この設定は、以前のインストール時に行った設定を表示します。**Next** をクリックして既存の設定を保持します。
6. **Next** をクリックしてインストールを開始します。
7. **Finish** をクリックします。
8. Windows DC を再起動します。

重要

DC を再起動すると、**PasswordHook.dll** ライブラリーが有効ではなく、パスワードの同期に失敗します。

10.5. パスワード同期サービスのアンインストール

Red Hat Directory Password Sync サービスが不要になった場合は、Active Directory ドメインコントローラー (DC) から削除します。

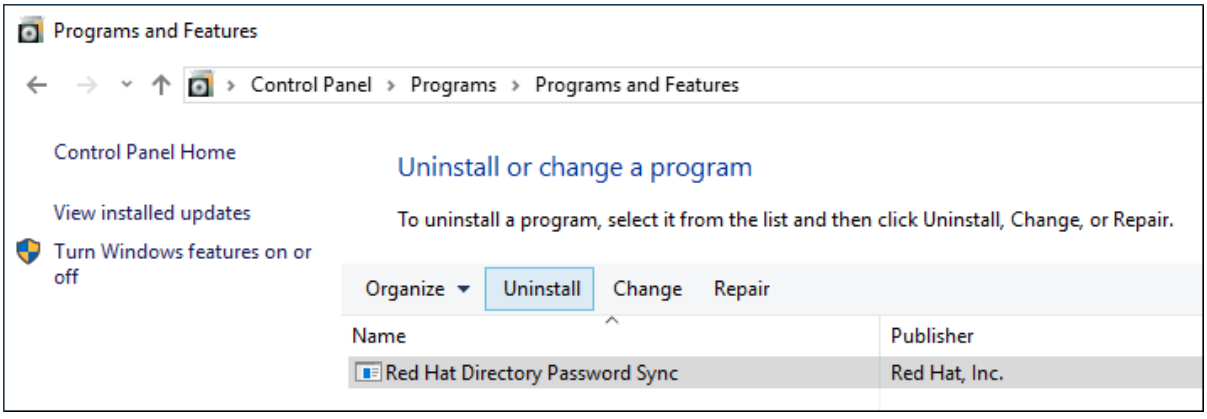
前提条件

- **Red Hat Directory Password Sync** は Windows DC にインストールされています。

手順

DC からソフトウェアを削除するパーミッションを持つユーザーで Active Directory ドメインコントローラーにログインします。

1. **Control Panel** を開きます。
2. **Programs** をクリックしてから、**Programs and Features** をクリックします。
3. **Red Hat Directory Password Sync** エントリーを選択し、**Uninstall** ボタンをクリックします。



4. **Yes** をクリックして確定します。

第11章 DIRECTORY SERVER インスタンスの削除

Directory Server インスタンスが不要になった場合は、それを削除してディスク容量を取り戻すことができます。1 つのサーバーで複数のインスタンスを実行している場合、特定のインスタンスを削除しても他のインスタンスには影響しません。

11.1. コマンドラインを使用したインスタンスの削除

コマンド行を使用して、Directory Server インスタンスを削除できます。

前提条件

- インスタンスがレプリケーショントポロジーの一部であった場合、インスタンスがレプリケーショントポロジーから削除されました。

手順

1. オプション: Directory Server ディレクトリーのバックアップを作成します。
   a. インスタンスを停止します。

   ```
   # dsctl instance_name stop
   ```

   b. **/var/lib/dirsrv/slapd-instance_name/** ディレクトリーをコピーします。

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

   ディレクトリーには、データベースと、バックアップおよびエクスポートのディレクトリーが含まれます。

   c. **/etc/dirsrv/slapd-instance_name/** ディレクトリーをコピーします。

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

2. インスタンスを削除します。

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

検証

- **/var/lib/dirsrv/slapd-instance_name/** および **/etc/dirsrv/slapd-instance_name/** ディレクトリーが削除されていることを確認します。

```
# 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
```

関連情報

- レプリケーショントポロジーからのインスタンスの削除

11.2. WEB コンソールを使用したインスタンスの削除

Web コンソールを使用して、Directory Server インスタンスを削除できます。ただし、データベースや設定ファイルなどを含む Directory Server ディレクトリーのバックアップを作成する場合は、コマンド行でこれらのディレクトリーをコピーする必要があります。

前提条件

- インスタンスがレプリケーショントポロジーの一部であった場合、インスタンスがレプリケーショントポロジーから削除されました。
- Web コンソールでインスタンスにログインしている。

手順

1. オプション: Directory Server ディレクトリーのバックアップを作成します。
   a. **Actions** ボタンをクリックし、**Stop instance** を選択します。
   b. **/var/lib/dirsrv/slapd-instance_name/** ディレクトリーをコピーします。

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

      ディレクトリーには、データベースと、バックアップおよびエクスポートのディレクトリーが含まれます。
   c. **/etc/dirsrv/slapd-instance_name/** ディレクトリーをコピーします。

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

2. **Actions** ボタンをクリックし、**Remove this instance** を選択します。
3. **Yes, I am sure** を選択し、**Remove Instance** をクリックして確認します。

検証

- **/var/lib/dirsrv/slapd-instance_name/** および **/etc/dirsrv/slapd-instance_name/** ディレクトリーが削除されていることを確認します。

```
# 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
```

関連情報

- レプリケーショントポロジーからのインスタンスの削除

第12章 DIRECTORY SERVER のアンインストール

Directory Server インスタンスが必要なくなった場合は、これをアンインストールして領域を解放できます。

12.1. DIRECTORY SERVER のアンインストール

サーバーで Directory Server を実行する必要がなくなった場合は、本セクションの説明に従ってパッケージをアンインストールします。

手順

1. レプリケーショントポロジーからすべてのインスタンスを削除します。インスタンスがレプリケーショントポロジーのメンバーではない場合は、この手順を省略します。
2. サーバーからすべてのインスタンスを削除します。インスタンスごとに、次のように入力します。

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

3. Directory Server パッケージを削除します。

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

4. 必要に応じて、**dirsrv-12-for-rhel-8-x86_64-rpms** リポジトリーを無効にします。

```
# 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. 必要に応じて、システムから Red Hat Directory Server サブスクリプションを削除します。

重要

Directory Server 以外の製品を提供するサブスクリプションを削除すると、これらの製品のパッケージをインストールしたり更新したりできなくなります。

- ホストに割り当てられているサブスクリプションをリスト表示します。

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

- 前の手順でプール ID を使用してサブスクリプションを削除します。

```
# 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
```

関連情報

- レプリケーショントポロジーからのインスタンスの削除

第13章 WEB コンソールを使用した DIRECTORY SERVER へのログイン

Web コンソールは、管理タスクの実行に使用できるブラウザーベースのグラフィカルユーザーインターフェイス (GUI) です。Directory Server パッケージは、Web コンソールの Directory Server ユーザーインターフェイスを自動的にインストールします。

前提条件

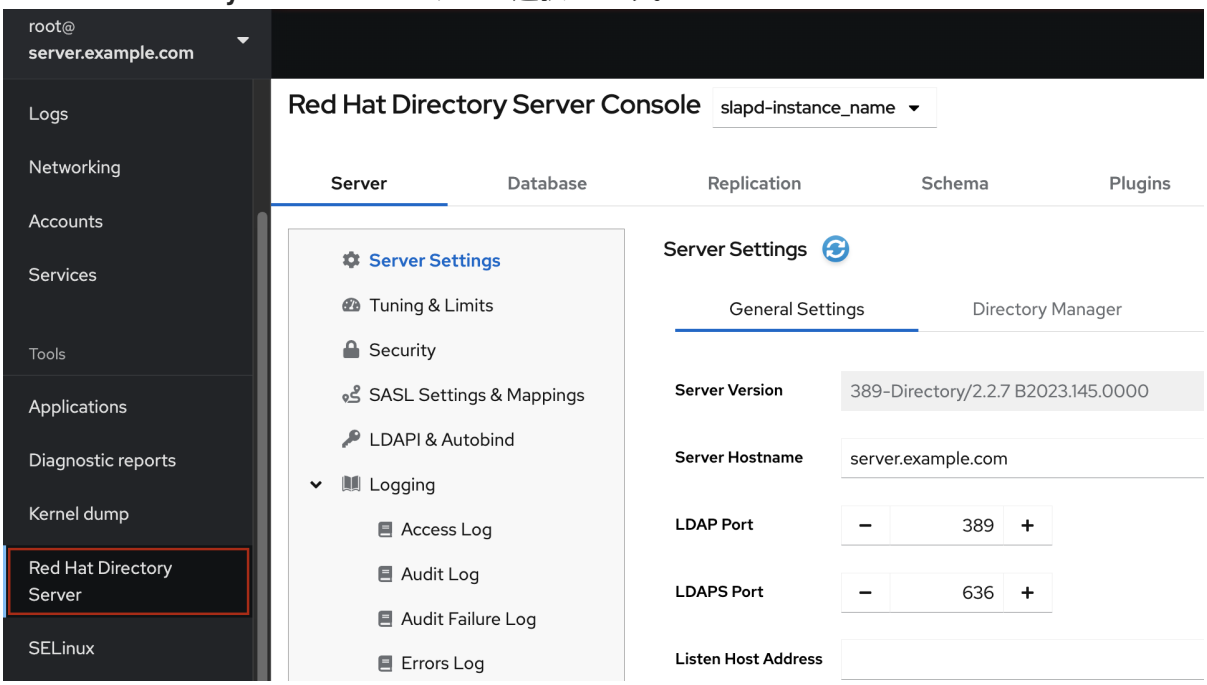
- Web コンソールにアクセスする権限がある。

手順

1. ブラウザーで次の URL を使用して Web コンソールにアクセスします。

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

2. **sudo** 権限を持つユーザーとしてログインします。
3. **Red Hat Directory Server** エントリーを選択します。



関連情報

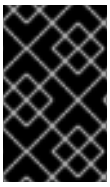
- RHEL Web コンソールへのログイン

第14章 DIRECTORY SERVER インスタンスの起動および停止

コマンドラインまたは Web コンソールを使用して、Directory Server インスタンスを起動、停止、再起動できます。

14.1. コマンドラインを使用した DIRECTORY SERVER インスタンスの起動および停止

dsctl ユーティリティーを使用して、Directory Server インスタンスを起動、停止、または再起動します。



重要

dsctl ユーティリティーは、Directory Server インスタンスを停止する唯一の正しい方法です。データの損失や破損を避けるために、**kill** コマンドを使用して **ns-slapd** プロセスを終了しないでください。

手順

- インスタンスを起動するには、次のコマンドを実行します。

```
# dsctl instance_name start
```

- インスタンスを停止するには、次のコマンドを実行します。

```
# dsctl instance_name stop
```

- インスタンスを再起動するには、次のコマンドを実行します。

```
# dsctl instance_name restart
```

必要に応じて、システムの起動時に Directory Server インスタンスが自動的に起動するようにすることができます。

- 単一インスタンスの場合は、次のコマンドを実行します。

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

- サーバー上のすべてのインスタンスの場合は、次のコマンドを実行します。

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

検証

dsctl ユーティリティーまたは **systemctl** ユーティリティーを使用して、インスタンスのステータスを確認できます。

- **dsctl** ユーティリティーを使用してインスタンスのステータスを表示するには、次のコマンドを実行します。

```
# dsctl instance_name status
```

- **systemctl** ユーティリティーを使用してインスタンスのステータスを表示するには、次のコマンドを実行します。

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

関連情報

- systemctl によるシステムサービス管理

14.2. WEB コンソールを使用した DIRECTORY SERVER インスタンスの起動および停止

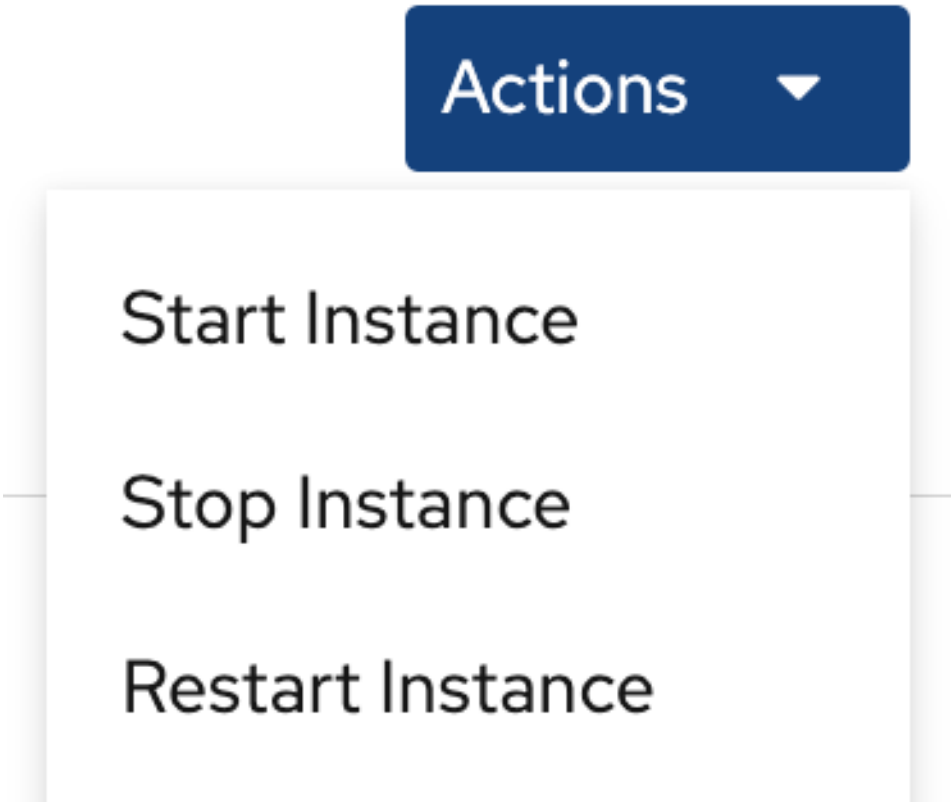
Web コンソールを使用して、Directory Server インスタンスを起動、停止、または再起動できます。

前提条件

- Web コンソールにログインしている。詳細は、以下を参照してください。
- Web コンソールを使用した Directory Server へのログイン

手順

1. Directory Server インスタンスを選択します。
2. **Actions** ボタンをクリックし、実行するアクションを選択します。
   - **Start Instance**
   - **Stop Instance**
   - **Restart Instance**



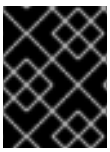
検証

- Directory Server インスタンスが実行していることを確認します。インスタンスが実行されていない場合、Web コンソールに次のメッセージが表示されます。

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

第15章 LDAP および LDAPS ポート番号の変更

デフォルトでは、Directory Server は LDAP にポート **389** を使用し、有効な場合は LDAPS プロトコルにポート **636** を使用します。たとえば、1 台のホストで複数の Directory Server インスタンスを実行するなど、これらのポート番号を変更できます。



重要

他のサービスは、インスタンスのプロトコルに割り当てた新しいポートを使用しないでください。

15.1. コマンドラインを使用したポート番号の変更

コマンドラインを使用して LDAP プロトコルおよび LDAPS プロトコルのポート番号を変更するには、次を実行します。LDAP および LDAP のポート変更には、**nsslapd-port** および **nsslapd-securePort** パラメーターを更新する必要があります。

手順

1. 必要に応じて、インスタンスの現在のポート番号を表示します。

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

2. LDAP ポートを変更するには、以下を行います。
   a. LDAP プロトコルの新しいポートを設定します。たとえば、**1389** に設定するには、以下を実行します。

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

   b. 前の手順で割り当てた LDAP ポートの **ldap_port_t** タイプを設定します。

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

3. LDAPS ポートを変更するには、以下を実行します。
   a. LDAPS プロトコルの新しいポートを設定します。たとえば、**1636** に設定するには、以下を実行します。

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

   b. 前の手順で割り当てた LDAPS ポートの **ldap_port_t** タイプを設定します。

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

4. インスタンスを再起動します。

```
# dsctl instance_name restart
```

検証

1. コマンドを使用して、Directory Server が新しい LDAP ポートを使用していることを確認します。

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

2. コマンドで、Directory Server が新しい LDAPS ポート番号を使用していることを確認します。

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

関連情報

- **nsslapd-securePort** パラメーターの詳細は、nsslapd-securePort パラメーターの説明 を参照してください。
- **nsslapd-port** パラメーターの詳細は、nsslapd-port パラメーターの説明 を参照してください。

15.2. WEB コンソールを使用したポート番号の変更

Web コンソールを使用して LDAP プロトコルおよび LDAPS プロトコルのポート番号を変更するには、以下を行います。

前提条件

- Web コンソールでインスタンスにログインしている。

手順

1. LDAP ポートを変更するには、以下を行います。
   a. **Server Setting** メニューを開きます。
   b. **Server Setting** タブで、**LDAP Port** フィールドに新しいポート番号を入力します。
2. **Save** をクリックします。
3. LDAPS ポートを変更するには、以下を実行します。
   a. **Server Setting** メニューを開きます。
   b. **General Settings** タブで、**LDAPS Port** フィールドに新しいポート番号を入力します。
   c. **Save** をクリックします。
4. **Action** をクリックし、**Restart Instance** を選択してインスタンスを再起動します。

検証

1. サーバー設定で、変更したポートが反映されていることを確認します。

関連情報

- インスタンスの再起動に関する詳細は、Web コンソールを使用した Directory Server インスタンスの起動と停止 を参照してください。

- Web コンソールを使用した Directory Server へのログインの詳細は、Web コンソールを使用した Directory Server へのログイン を参照してください。

第16章 .DSRC ファイルを使用した DIRECTORY SERVER コマンドラインユーティリティーのデフォルトオプションの管理

~/**.dsrc** ファイルは、Directory Server コマンドラインユーティリティーを使用するコマンドを簡素化します。デフォルトでは、**LDAP URL** やバインド識別名 (DN) などの情報をこのユーティリティーのコマンドに渡すことができます。設定を ~/**dsrc** ファイルに保存すると、毎回設定を指定しなくてもコマンドラインユーティリティーを使用できます。

16.1. .DSRC ファイルによってコマンドが簡素化される仕組み

~/**.dsrc** ファイルでは、インスタンスの LDAP URL とバインド DN を指定できます。

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

これらの設定により、より短い Directory Server コマンドを使用できます。たとえば、ユーザーアカウントを作成するには、次のようにします。

```
# dsidm server1 user create
```

~/**.dsrc** ファイルがない場合は、コマンドでバインド DN、LDAP URL、およびベース DN を指定する必要があります。

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

16.2. DSCTL ユーティリティーを使用した .DSRC ファイルの作成

~/**.dsrc** ファイルを手動で作成する代わりに、**dsctl** ユーティリティーを使用して作成できます。

手順

- 以下を実行します。

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

このコマンドには次のオプションを追加できます。

- **--uri**

--uri オプションを使用する場合は、**protocol://host_name_or_IP_address_or_socket** の形式で URL をインスタンスに設定します。

以下に例を示します。

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

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

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

Directory Server ソケットへのパスを設定する場合は、パスにスラッシュ **(/)** ではなく **%%02** を使用します。

重要

ldapi URL を使用すると、サーバーは、Directory Server コマンドラインユーティリティーを実行するユーザーのユーザー ID (UID) とグループ ID (GID) を識別します。**root** ユーザーとしてコマンドを実行すると、UID と GID の両方が **0** になり、Directory Server は、対応するパスワードを入力しなくても、**cn=Directory Manager** としてユーザーを自動的に認証します。

- **--starttls**

--starttls オプションを使用する場合は、LDAP ポートに接続し、**STARTTLS** コマンドを送信して暗号化された接続に切り替えるようにするようにユーティリティーを設定します。

- **--basedn**

--basedn オプションを使用する場合は、ベース識別名 (DN) を設定します。

例: **--basedn dc=example,dc=com**

- **--binddn**

--basedn オプションを使用する場合は、バインド DN を設定します。

例: **--binddn cn=Directory Manager**

- **--pwdfile**

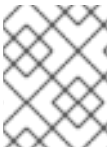
--pwdfile を使用する場合は、バインド DN のパスワードを含むファイルへのパスを設定します。

例: **--pwdfile /root/rhds.pwd**

- **--tls-cacertdir**

--tls-cacertdir オプションを使用する場合は、このパラメーターに、LDAPS 接続を使用する場合にサーバーの証明書を検証するために必要な認証局 (CA) 証明書を含むディレクトリーを定義するパスを設定します。

例: **--tls-cacertdir /etc/pki/CA/certs/**



注記

c_rehash /etc/pki/CA/certs/ コマンドは、CA 証明書を指定したディレクトリーにコピーする場合にのみ使用できます。

- **--tls-cert**

--tls-certl オプションを使用する場合は、サーバーの証明書への絶対パスを設定します。

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

- **--tls-key**

--tls-key オプションを使用する場合は、サーバーの秘密鍵への絶対パスを設定します。

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

- **--tls-reqcert**

--tls-reqcert オプションを使用する場合は、クライアントユーティリティーが TLS セッションのサーバー証明書に対して実行するチェック内容を設定します。

例: **--tls-reqcert hard**

次のパラメーターが利用可能です。

a. **never**: ユーティリティーはサーバー証明書を要求または確認しません。

b. **allow**: ユーティリティーは証明書エラーを無視します。その場合も、接続は確立されます。

c. **Hard**: ユーティリティーは、証明書エラーが発生した場合に接続を終了します。

- **--saslmech**

--saslmech オプションを使用する場合は、使用する SASL メカニズムを **PLAIN** または **EXTERNAL** に設定します。

例: **--saslmech PLAIN**

16.3. DIRECTORY SERVER ユーティリティー使用時のリモートおよびローカル接続の解決

Directory Server 接続を保護するときに、Directory Server コマンドをリモートまたはローカルで呼び出すことができます。LDAP URL を指定して Directory Server コマンドを実行すると、サーバーは、それをリモート接続と見なし、コマンドを続行するために、システム全体の設定とともに **/etc/openldap/ldap.conf** 設定ファイルをチェックします。

インスタンス名を指定して Directory Server コマンドを実行すると、サーバーは、~/**.dsrc** ファイルが存在するかどうかを確認し、次のロジックを適用して続行します。

1. Directory Server は、~/**.dsrc** ファイルをリモート接続と見なし、**/etc/openldap/ldap.conf** 設定ファイルとシステム全体の設定にインスタンス名と LDAP URL の両方が含まれているかどうかを確認します。

2. ~/**.dsrc** ファイルに特定のインスタンス名のみが含まれている場合、または ~/**.dsrc** ファイルが存在しない場合、Directory Server は ~/**.dsrc** ファイルをローカル接続と見なし、ローカルの **dse.ldif** ファイルの **nsslapd-certdir** 設定を使用して接続を保護します。**nsslapd-certdir** が存在しない場合、サーバーはデフォルトのパス **/etc/dirsrv/slapd-instance_name/** を使用してインスタンスのネットワークセキュリティーサービス (NSS) データベースを保存します。

関連情報

- nsslapd-certdir パラメーター

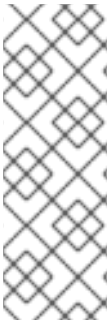
第17章 テストエントリーの作成

dsctl ldifgen コマンドは、異なるタイプのテストエントリーを持つ LDIF ファイルを作成します。たとえば、この LDIF ファイルを使用して、テストインスタンスまたはサブツリーを設定すると、サンプルエントリーで Directory Server のパフォーマンスをテストできます。

17.1. 作成できるテストエントリーの概要

以下のエントリータイプの引数のいずれかを **dsctl ldifgen** に渡すことができます。

- **users**: ユーザーエントリーが含まれる LDIF ファイルを作成します。
- **groups**: 静的グループおよびメンバーエントリーが含まれる LDIF ファイルを作成します。
- **cos-def**: 従来のポインターまたは間接的な Class of Service (CoS) 定義が含まれる LDIF ファイルを作成します。
- **cos-template**: CoS テンプレートが含まれる LDIF ファイルを作成します。
- **roles**: 管理されたロールエントリー、フィルターが設定されたロールエントリー、または間接ロールエントリーが含まれる LDIF ファイルを作成します。
- **mod-load**: 変更操作が含まれる LDIF ファイルを作成します。**ldapmodify** ユーティリティーを使用して、ファイルをディレクトリーにロードします。
- **nested**: カスケードツリーやフラクタルツリーのように重く入れ子になったエントリーを含む LDIF ファイルを作成します。



注記

dsctl ldifgen コマンドは LDIF ファイルのみを作成します。ファイルを Directory Server インスタンスに読み込むには、以下を使用します。

- **mod-load** オプションを使用して LDIF ファイルを作成した後の **ldapmodify** ユーティリティー
- その他のすべてのオプションの **ldapadd** ユーティリティー

ネストされたエントリータイプを除き、コマンドラインオプションを指定しないと、**dsctl ldifgen** コマンドはインタラクティブモードを使用します。

```
# dsctl instance_name ldifgen entry_type
```

17.2. サンプルユーザーエントリーを使用した LDIF ファイルの作成

dsctl ldifgen users コマンドを使用して、サンプルユーザーエントリーのある LDIF ファイルを作成します。

手順

1. 例えば、**dc=example,dc=com** 接尾辞に 100,000 人の一般ユーザーを追加する **/tmp/users.ldif** という名前の LDIF ファイルを作成するには、次のように入力します。

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

このコマンドは、以下の組織単位 (OU) を作成し、ユーザーをこれらの OU にランダムに割り当てることに注意してください。

- **ou=accounting**
- **ou=product development**
- **ou=product testing**
- **ou=human resources**
- **ou=payroll**
- **ou=people**
- **ou=groups**
  詳細と、LDIF ファイルの作成に使用できるその他のオプションについては、以下を入力します。

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

2. オプション: テスト項目をディレクトリーに追加します。

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

17.3. グループエントリーの例を使用した LDIF ファイルの作成

dsctl ldifgen groups コマンドを使用して、サンプルユーザーエントリーのある LDIF ファイルを作成します。

手順

1. たとえば、500 グループを **ou=groups,dc=example,dc=com** エントリーに追加し、各グループに 100 メンバーが含まれる **/tmp/groups.ldif** という名前の LDIF ファイルを作成するには、次のコマンドを実行します。

```
# 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__
```

このコマンドは、LDIF 文を作成して、**ou=People,dc=example,dc=com** にユーザーエントリーを追加することに注意してください。

詳細と、LDIF ファイルの作成に使用できるその他のオプションについては、以下を入力します。

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

2. オプション: テスト項目をディレクトリーに追加します。

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

17.4. COS 定義の例を使用した LDIF ファイルの作成

dsctl ldifgen cos-def コマンドを使用して、Class of Service (CoS) 定義を持つ LDIF ファイルを作成します。

手順

1. たとえば、従来の CoS 定義を **ou=cos-definitions,dc=example,dc=com** エントリーに追加する **/tmp/cos-definition.ldif** という名前の LDIF ファイルを作成するには、次のように入力します。

```
# 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
```

詳細と、LDIF ファイルの作成に使用できるその他のオプションについては、以下を入力します。

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

2. オプション: テスト項目をディレクトリーに追加します。

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

17.5. EXAMPLE MODIFICATION STATEMENTS を使用した LDIF ファイルの作成

dsctl ldifgen mod-load コマンドを使用して、更新操作が含まれる LDIF ファイルを作成します。

手順

1. たとえば、**/tmp/modifications.ldif** という名前の LDIF ファイルを作成するには:

```
# 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
```

このコマンドは、以下を実行するステートメントを **含む/tmp/modifications.ldif** ファイルという名前のファイルを作成します。

- 1000 の **ADD** 操作を含む LDIF ファイルを作成して、 **ou=People,dc=example,dc=com** にユーザーエントリーを作成します。
- **sn** 属性を変更して、すべてのエントリーを変更します。

- 10 ユーザーエントリーを追加します。
- 100 個の **MODRDN** 操作を実行します。
- 100 エントリーの削除
- 末尾の残りのエントリーをすべて削除します。
  詳細と、LDIF ファイルの作成に使用できるその他のオプションについては、以下を入力します。

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

2. オプション: テスト項目をディレクトリーに追加します。

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

17.6. ネストされたサンプルエントリーを持つ LDIF ファイルの作成

dsctl ldifgen nested コマンドを使用して、大きく入れ子になったカスケードフラクタル構造を含む LDIF ファイルを作成します。

手順

1. たとえば、**/tmp/nested.ldif** という名前の LDIF ファイルを作成するには、**dc=example,dc=com** エントリー配下の異なる組織単位 (OU) に合計 600 ユーザーの追加し、各 OU には最大 100 ユーザーを含めます。次のように入力します。

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

   詳細と、LDIF ファイルの作成に使用できるその他のオプションについては、以下を入力します。

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

2. オプション: テスト項目をディレクトリーに追加します。

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