



# Red Hat Directory Server 11

## インストールガイド

Red Hat Directory Server のインストール手順



# Red Hat Directory Server 11 インストールガイド

---

## Red Hat Directory Server のインストール手順

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

## 法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Installation\_Guide.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

本ガイドでは、Red Hat Directory Server 11 と関連サービスのインストール、更新、アンインストールを説明します。

## 目次

はじめに .....	4
多様性を受け入れるオープンソースの強化 .....	5
<b>第1章 DIRECTORY SERVER パッケージのインストール .....</b>	<b>6</b>
前提条件 .....	6
1.1. DIRECTORY SERVER パッケージのインストール .....	6
手順 .....	6
関連情報 .....	7
<b>第2章 新しい DIRECTORY SERVER インスタンスの設定 .....</b>	<b>8</b>
前提条件 .....	8
2.1. .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 .....	8
2.1.1. Directory Server インスタンスインストール用の .inf ファイルの作成 .....	8
手順 .....	8
関連情報 .....	10
2.1.2. .inf ファイルを使用した新しい Directory Server インスタンスの設定 .....	10
前提条件 .....	10
手順 .....	10
2.1.3. ファイアウォールで必要なポートを開く .....	10
前提条件 .....	11
手順 .....	11
関連情報 .....	11
2.2. 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 .....	11
2.2.1. インタラクティブインストーラーでサポートされている設定 .....	12
2.2.2. 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 .....	12
2.2.3. ファイアウォールで必要なポートを開く .....	13
前提条件 .....	13
手順 .....	13
関連情報 .....	14
2.3. WEB コンソールを使用した新規インスタンスの設定 .....	14
2.3.1. Web コンソールで新しい Directory Server インスタンスの設定 .....	14
前提条件 .....	14
手順 .....	14
関連情報 .....	16
2.3.2. ファイアウォールで必要なポートを開く .....	16
前提条件 .....	17
手順 .....	17
関連情報 .....	17
<b>第3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 .....</b>	<b>18</b>
前提条件 .....	18
3.1. ロードバランサーの背後で KERBEROS でインスタンスを設定する際の相違点について .....	18
3.2. DIRECTORY SERVER インスタンスインストール用の .INF ファイルの作成 .....	18
手順 .....	18
関連情報 .....	20
3.3. .INF ファイルを使用した新しい DIRECTORY SERVER インスタンスの設定 .....	20
前提条件 .....	20
手順 .....	20
3.4. ファイアウォールで必要なポートを開く .....	21
前提条件 .....	21
手順 .....	21

関連情報	21
3.5. 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	22
前提条件	22
手順	22
<b>第4章 DIRECTORY SERVER の更新</b>	<b>23</b>
前提条件	23
4.1. DIRECTORY SERVER パッケージの更新	23
<b>第5章 DIRECTORY SERVER 10 から DIRECTORY SERVER 11 への移行</b>	<b>24</b>
前提条件	24
5.1. レプリケーション方法を使用した DIRECTORY SERVER 11 への移行	24
手順	24
5.2. エクスポートおよびインポートの方法を使用した DIRECTORY SERVER 11 への移行	24
手順	25
<b>第6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</b>	<b>27</b>
6.1. パスワード同期サービスの仕組みの理解	27
6.2. 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	27
前提条件	27
手順	27
6.3. パスワード同期サービスのインストール	28
前提条件	28
手順	28
6.4. パスワード同期サービスの更新	29
前提条件	29
手順	29
6.5. パスワード同期サービスのアンインストール	30
前提条件	30
手順	30
<b>第7章 DIRECTORY SERVER のアンインストール</b>	<b>31</b>
7.1. DIRECTORY SERVER のアンインストール	31
前提条件	31
手順	31
関連情報	32
<b>付録A RED HAT DIRECTORY SERVER 11 でコマンドラインユーティリティーが置き換え</b>	<b>33</b>
<b>付録B 改訂履歴</b>	<b>36</b>



## はじめに

本ガイドでは、Red Hat Directory Server および Password Synchronization サービスのインストール、更新、およびアンインストールを説明します。また、本ガイドでは、Directory Server 10 から Directory Server 11 への移行を説明します。

ディレクトリーサービスの概念や Directory Server のインストール計画について理解しておく場合は、[Red Hat Directory Server デプロイメントガイド](#) を参照してください。

インストール後の Directory Server インスタンスの管理および設定に関する詳細は、[Red Hat Directory Server 管理ガイド](#) を参照してください。



## 多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[Red Hat CTO である Chris Wright のメッセージ](#) をご覧ください。

## 第1章 DIRECTORY SERVER パッケージのインストール

本章では、Red Hat Directory Server パッケージをインストールする方法を説明します。

### 前提条件

- Red Hat Enterprise Linux (RHEL) がサーバーにインストールされている。  
インストールする Red Hat Directory Server バージョンに必要な RHEL バージョンの詳細は、[Red Hat Directory Server 11 リリースノート](#) を参照してください。
- システムの Directory Server が Red Hat サブスクリプション管理サービスに登録されている。  
**Subscription Manager** の使用に関する詳細は、[Configuring Subscription Manager の使用および設定](#) の該当するセクションを参照してください。
- Red Hat Directory Server の有効なサブスクリプションは、お使いの Red Hat アカウントで利用できます。
- RHEL のデフォルトのリポジトリ **BaseOS** および **AppStream** が有効になっています。

### 1.1. 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。

#### 手順

1. Red Hat アカウントで利用可能なサブスクリプションを一覧表示し、Red Hat Directory Server を提供するプール ID を特定します。以下に例を示します。

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

2. 前の手順でプール 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
```

3. **dirsrv-11-for-rhel-8-x86\_64-rpms** リポジトリを有効にします。

```
# subscription-manager repos --enable=dirsrv-11-for-rhel-8-x86_64-rpms  
Repository 'dirsrv-11-for-rhel-8-x86_64-rpms' is enabled for this system.
```

4. **redhat-ds:11** モジュールをインストールします。

```
# yum module install redhat-ds:11
```

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 Enterprise Linux のインストールおよびシステムをサブスクリプション管理サービスに登録する方法は、[Red Hat Enterprise Linux インストールガイド](#) を参照してください。
- **subscription-manager** ユーティリティーの使用方法は、[Subscription Manager の使用および設定](#) ガイドを参照してください。
- リポジトリの有効化に関する詳細は、Red Hat Enterprise Linux システム管理者のガイドの [Subscription Manager および Yum を使用した基本的なソフトウェアインストールタスクの管理](#) を参照してください。

## 第2章 新しい DIRECTORY SERVER インスタンスの設定

Directory Server は、新規インスタンスの作成をサポートします。

- [コマンドラインで .inf ファイルの使用](#)
- [対話式コマンドラインインストーラーの使用](#)
- [Web コンソールの使用](#)

### 前提条件

- [Red Hat Directory Server 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 バージョンのハードウェアおよびソフトウェアの要件を満たしている。
- Directory Server サーバーパッケージは、[1章 Directory Server パッケージのインストール](#) の説明に従ってインストールされます。
- サーバーの完全修飾ドメイン名 (FQDN) は DNS を使用して解決できます。

### 2.1. .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

.inf を使用して Directory Server をインストールすると、高度な設定をカスタマイズできます。たとえば、対話式インストーラーおよび Web コンソールの設定の他に、.inf で以下の設定をカスタマイズできます。

- サービスの起動後に **ns-slaped** Directory Server プロセスが使用するユーザーおよびグループ。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
- ロードバランサーの背後で GSSAPI を使用してインスタンスをインストールする場合は、厳密なホストチェックを無効にします。

このセクションでは、以下について説明します。

- [.inf ファイルの作成およびカスタマイズ](#)
- [dscreate ユーティリティーで .inf ファイルを使用して新しいインスタンスをセットアップ](#)
- [ファイアウォールで必要なポートを開く](#)

インストール時に頻繁に使用される設定パラメーターのみを設定する場合は、インタラクティブインストーラーを使用できます。詳細は、「[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](#)」を参照してください。

#### 2.1.1. Directory Server インスタンスインストール用の .inf ファイルの作成

本セクションでは、**dscreate** ユーティリティー用に .inf 設定ファイルを作成する方法と、お使いの環境に .inf ファイルを調整する方法を説明します。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。

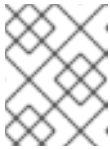
手順

1. **dscreate create-template** コマンドを使用して、**.inf** テンプレートファイルを作成します。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ています。

2. 直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。



### 注記

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、少なくとも以下のパラメーターを設定します。

```
[slapd]
# instance_name (str)
# Description: ...
# Default value: localhost
instance_name = instance_name

# root_password (str)
# Description: ...
# Default value: directory manager password
root_password = password
```

**dscreate create-template** コマンドで作成するテンプレートファイルには、これらのセクションで設定できるパラメーターの総合的な一覧が含まれます。

- 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、以下を実行します。
  - i. **create\_suffix\_entry** パラメーターのコメントを解除し、**true** に設定します。

```
# create_suffix_entry (bool)
# Description: ...
# Default value: False
create_suffix_entry = True
```

- ii. **suffix** パラメーターのコメントを解除し、接尾辞を設定します。

```
# suffix (str)
# Description: ...
# Default value:
suffix = dc=example,dc=com
```



## 重要

インスタンスの作成時に接尾辞を作成する代わりに、Red Hat Directory Server 管理ガイドの [データベースの作成](#) で説明されているように、後で作成することができます。ただし、接尾辞を作成せずに、このインスタンスにデータを保存することはできません。

- 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、LDAP プロトコルおよび LDAPS プロトコルに異なるポートを指定するには、これらのパラメーターを使用します。



## 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 は、セキュリティを強化するために、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に注意してください。

### 関連情報

- **.inf** ファイルに設定できるパラメーターの完全一覧と各パラメーターの説明は、**dscreate create-template** コマンドが作成するテンプレートファイルを参照してください。
- インストール後に証明書をインストールする方法は、Red Hat Directory Server 管理ガイドの [Directory Server が使用する NSS データベースの管理](#) を参照してください。

## 2.1.2. .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、[「Directory Server インスタンスインストール用の .inf ファイルの作成」](#) の説明に従って作成されている。

### 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。以下に例を示します。

```
# dscreate from-file /root/instance_name.inf
Starting installation...
Completed installation for instance_name
```

作成されたインスタンスは自動的に起動され、システムの起動時に起動するように設定されています。

2. ファイアウォールで必要なポートを開きます。[「ファイアウォールで必要なポートを開く」](#) を参照

## 2.1.3. ファイアウォールで必要なポートを開く

他のマシンがネットワーク経由で Directory Server に接続できるようにするには、ローカルのファイアウォールで必要なポートを開きます。

インスタンスの作成時にポートが指定されていないと、そのインスタンスは LDAP にポート **389** を使用し、LDAPS プロトコルにはポート **636** を使用します。

#### 前提条件

- インスタンスの作成時に設定される LDAP プロトコルおよび LDAPS プロトコルのポート番号。

#### 手順

1. **firewalld** サービスが実行していることを確認します。

- **firewalld** が実行中であることを確認するには、次のコマンドを実行します。

```
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
   enabled)
   Active: active (running) since Fri 2018-06-15 14:06:33 CEST; 1h 17min ago
   ...
```

- **firewalld** を起動し、システムの起動時にサービスが自動的に起動するように設定するには、次のコマンドを実行します。

```
# systemctl start firewalld
# systemctl enable firewalld
```

2. **firewall-cmd** ユーティリティーを使用して必要なポートを開きます。たとえば、デフォルトのファイアウォールゾーンで LDAP および LDAPS のデフォルトポートを開くには、次を実行します。

```
# 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、変更が即座に行われることを確認します。

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

#### 関連情報

- **firewall-cmd** を使用してシステムでポートを開く方法は、Red Hat Enterprise Linux の [セキュリティーガイド](#) または man ページ **firewall-cmd(1)** を参照してください。

## 2.2. 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。

インタラクティブインストーラーで対応している設定の一覧は、「[インタラクティブインストーラーでサポートされている設定](#)」を参照してください。

このセクションでは、以下について説明します。

- [インタラクティブインストーラーで対応している設定の一覧](#)

- [対話式インストーラーの起動](#)
- [ファイアウォールで必要なポートを開く](#)

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、[「.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。

### 2.2.1. インタラクティブインストーラーでサポートされている設定

インタラクティブインストーラーを使用する場合は、以下の設定を設定できます。

- システムのホスト名
- 厳密なホスト名検証の有効化または無効化
- インスタンスの名前
- LDAP ポート番号
- LDAPS ポート番号
- 自己署名証明書の自動作成
- ディレクトリーマネージャーアカウントの DN
- ディレクトリーマネージャーアカウントのパスワード
- データベースの接尾辞の任意の作成

### 2.2.2. 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

インタラクティブインストーラーを起動して新規インスタンスを設定するには、以下を入力します。

#### # dscreate interactive

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。

#### 例2.1 対話式インストーラーの使用

```
# dscreate interactive
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**

Starting installation...

Completed installation for **instance\_name**



### 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。

### 2.2.3. ファイアウォールで必要なポートを開く

他のマシンがネットワーク経由で Directory Server に接続できるようにするには、ローカルのファイアウォールで必要なポートを開きます。

インスタンスの作成時にポートが指定されていないと、そのインスタンスは LDAP にポート **389** を使用し、LDAPS プロトコルにはポート **636** を使用します。

#### 前提条件

- インスタンスの作成時に設定される LDAP プロトコルおよび LDAPS プロトコルのポート番号。

#### 手順

1. **firewalld** サービスが実行していることを確認します。

- **firewalld** が実行中であることを確認するには、次のコマンドを実行します。

```
# systemctl status firewalld
```

```
● firewalld.service - firewalld - dynamic firewall daemon
```

```
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
```

```
Active: active (running) since Fri 2018-06-15 14:06:33 CEST; 1h 17min ago
```

```
...
```

- **firewalld** を起動し、システムの起動時にサービスが自動的に起動するように設定するには、次のコマンドを実行します。

```
# systemctl start firewalld
```

```
# systemctl enable firewalld
```

2. **firewall-cmd** ユーティリティーを使用して必要なポートを開きます。たとえば、デフォルトのファイアウォールゾーンで LDAP および LDAPS のデフォルトポートを開くには、次を実行します。

```
# 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、変更が即座に行われることを確認します。

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

#### 関連情報

- **firewall-cmd** を使用してシステムでポートを開く方法は、Red Hat Enterprise Linux の [セキュリティガイド](#) または man ページ **firewall-cmd(1)** を参照してください。

## 2.3. WEB コンソールを使用した新規インスタンスの設定

管理者は、Web コンソールを使用して、ブラウザベースのインターフェイスを使用して新規インスタンスを作成することができます。

このセクションでは、以下について説明します。

- [Web コンソールで新規インスタンスの作成](#)
- [ファイアウォールで必要なポートを開く](#)

### 2.3.1. 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 コンソールがサーバーにインストールされ、ローカルのファイアウォールで 9090 ポートが開いている。  
詳細は、**RHEL 8** で **Web** コンソールを使用したシステムの管理の [Web コンソールのインストール](#) セクションを参照してください。

#### 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。以下に例を示します。

```
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 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。

### Create New Server Instance ✕

Instance Name

Port

Secure Port

Create Self-Signed TLS Certificate DB

Directory Manager DN

Directory Manager Password

Confirm Password

---

**Optional Database Settings**

Database Suffix

Database Name

Do Not Initialize Database

Create Suffix Entry

Create Suffix Entry And Add Sample Entries

- **Instance Name:** インスタンスの名前を設定します。



#### 重要

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。



## 重要

セキュリティを強化するために、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に注意してください。

- **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。
  - **Database Suffix:** バックエンドの接尾辞を設定します。デフォルト値は **dc=example,dc=com** です。
  - **Database Name:** バックエンドデータベースの名前を設定します。バックエンドの接尾辞を指定した場合は、このフィールドに入力する必要があります。
6. 以下のいずれかのオプションを選択します。
- **Do Not Initialize Database:** インストーラーはデータベースと接尾辞を作成しません。
  - **Create Suffix Entry:** インストーラーは、**Database Suffix** フィールドおよび **Database Name** フィールドに入力した値に基づいて、データベースと接尾辞を作成します。
  - **Create Suffix Entry And Add Sample Entries:** インストーラーは、**Database Suffix** フィールドおよび **Database Name** フィールドに入力されている値に基づいてデータベースと接尾辞を作成します。さらに、インストーラーはディレクトリーにサンプルエントリーを作成します。



## 注記

インストール時に接尾辞を作成しない場合は、ディレクトリーにエントリーを追加する前に手動で作成する必要があります。

7. **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。
8. ファイアウォールで必要なポートを開きます。 [「ファイアウォールで必要なポートを開く」](#) を参照

### 関連情報

- Web コンソールの詳細は、[RHEL 8 Web コンソールを使用したシステムの管理](#) を参照してください。
- インストール後に証明書をインストールする方法は、Red Hat Directory Server 管理ガイドの [Directory Server が使用する NSS データベースの管理](#) を参照してください。

### 2.3.2. ファイアウォールで必要なポートを開く

他のマシンがネットワーク経由で Directory Server に接続できるようにするには、ローカルのファイアウォールで必要なポートを開きます。

インスタンスの作成時にポートが指定されていないと、そのインスタンスは LDAP にポート **389** を使用し、LDAPS プロトコルにはポート **636** を使用します。

#### 前提条件

- インスタンスの作成時に設定される LDAP プロトコルおよび LDAPS プロトコルのポート番号。

#### 手順

1. **firewalld** サービスが実行していることを確認します。

- **firewalld** が実行中であることを確認するには、次のコマンドを実行します。

```
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
  enabled)
  Active: active (running) since Fri 2018-06-15 14:06:33 CEST; 1h 17min ago
  ...
```

- **firewalld** を起動し、システムの起動時にサービスが自動的に起動するように設定するには、次のコマンドを実行します。

```
# systemctl start firewalld
# systemctl enable firewalld
```

2. **firewall-cmd** ユーティリティを使用して必要なポートを開きます。たとえば、デフォルトのファイアウォールゾーンで LDAP および LDAPS のデフォルトポートを開くには、次を実行します。

```
# 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、変更が即座に行われることを確認します。

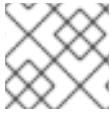
```
# firewall-cmd --reload
```

#### 関連情報

- **firewall-cmd** を使用してシステムでポートを開く方法は、Red Hat Enterprise Linux の [セキュリティガイド](#) または man ページ **firewall-cmd(1)** を参照してください。

## 第3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

高可用性を提供するには、ロードバランサーの背後で2つの Directory Server インスタンスをインストールします。ユーザーは Kerberos で認証できるようにする必要があります。



### 注記

このシナリオの設定は、コマンドラインでのみサポートされます。

このシナリオの設定には、以下の手順が含まれます。

- [インスタンス作成用の .inf ファイルを作成](#)
- [dscreate ユーティリティーで .inf ファイルを使用して、新しいインスタンスをセットアップ](#)
- [ファイアウォールで必要なポートを開く](#)
- [ロードバランサーのキータブを作成し、Directory Server がキータブを使用するように設定](#)

### 前提条件

- [Red Hat Directory Server 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 バージョンのハードウェアおよびソフトウェアの要件を満たしている。
- Directory Server サーバーパッケージは、[1章 Directory Server パッケージのインストール](#) の説明に従ってインストールされます。

### 3.1. ロードバランサーの背後で KERBEROS でインスタンスを設定する際の相違点について

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、Directory Server からの DNS 名ではなく、ロードバランサーの DNS 名が含まれます。たとえば、`ldap/loadbalancer.example.com@EXAMPLE.COM` になります。

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。

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

本セクションでは、`dscreate` ユーティリティー用に `.inf` 設定ファイルを作成する方法と、お使いの環境に `.inf` ファイルを調整する方法を説明します。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。

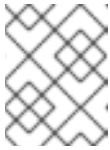
#### 手順

1. `dscreate create-template` コマンドを使用して、`.inf` テンプレートファイルを作成します。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ています。

2. 直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。



### 注記

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、少なくとも以下のパラメーターを設定します。

```
[slapd]
# instance_name (str)
# Description: ...
# Default value: localhost
instance_name = instance_name

# root_password (str)
# Description: ...
# Default value: directory manager password
root_password = password
```

**dscreate create-template** コマンドで作成するテンプレートファイルには、これらのセクションで設定できるパラメーターの総合的な一覧が含まれます。

- 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。

```
[general]
# full_machine_name (str)
# Description: ...
# Default value: loadbalancer.example.com
full_machine_name = loadbalancer.example.com
```

詳細は、「[ロードバランサーの背後で Kerberos でインスタンスを設定する際の相違点について](#)」を参照してください。

- 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 (bool)
# Description: ...
# Default value: True
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、以下を実行します。
  - i. **create\_suffix\_entry** パラメーターのコメントを解除し、**true** に設定します。

```
# create_suffix_entry (bool)
# Description: ...
# Default value: False
```

```
create_suffix_entry = True
```

- ii. **suffix** パラメーターのコメントを解除し、接尾辞を設定します。

```
# suffix (str)
# Description: ...
# Default value:
suffix = dc=example,dc=com
```



### 重要

インスタンスの作成時に接尾辞を作成する代わりに、Red Hat Directory Server 管理ガイドの [データベースの作成](#) で説明されているように、後で作成することができます。ただし、接尾辞を作成せずに、このインスタンスにデータを保存することはできません。

- 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、LDAP プロトコルおよび LDAPS プロトコルに異なるポートを指定するには、これらのパラメーターを使用します。



### 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 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に注意してください。

## 関連情報

- **.inf** ファイルに設定できるパラメーターの完全一覧と各パラメーターの説明は、**dscreate create-template** コマンドが作成するテンプレートファイルを参照してください。
- インストール後に証明書をインストールする方法は、Red Hat Directory Server 管理ガイドの [Directory Server が使用する NSS データベースの管理](#) を参照してください。

## 3.3. .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、[「Directory Server インスタンスインストール用の .inf ファイルの作成」](#) の説明に従って作成されている。

### 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。以下に例を示します。



```
# dscreate from-file /root/instance_name.inf
Starting installation...
Completed installation for instance_name
```

作成されたインスタンスは自動的に起動され、システムの起動時に起動するように設定されています。

2. ファイアウォールで必要なポートを開きます。「[ファイアウォールで必要なポートを開く](#)」を参照

### 3.4. ファイアウォールで必要なポートを開く

他のマシンがネットワーク経由で Directory Server に接続できるようにするには、ローカルのファイアウォールで必要なポートを開きます。

インスタンスの作成時にポートが指定されていないと、そのインスタンスは LDAP にポート **389** を使用し、LDAPS プロトコルにはポート **636** を使用します。

#### 前提条件

- インスタンスの作成時に設定される LDAP プロトコルおよび LDAPS プロトコルのポート番号。

#### 手順

1. **firewalld** サービスが実行していることを確認します。

- **firewalld** が実行中であることを確認するには、次のコマンドを実行します。

```
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
  enabled)
  Active: active (running) since Fri 2018-06-15 14:06:33 CEST; 1h 17min ago
  ...
```

- **firewalld** を起動し、システムの起動時にサービスが自動的に起動するように設定するには、次のコマンドを実行します。

```
# systemctl start firewalld
# systemctl enable firewalld
```

2. **firewall-cmd** ユーティリティを使用して必要なポートを開きます。たとえば、デフォルトのファイアウォールゾーンで LDAP および LDAPS のデフォルトポートを開くには、次を実行します。

```
# 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、変更が即座に行われることを確認します。

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

#### 関連情報

- **firewall-cmd** を使用してシステムでポートを開く方法は、Red Hat Enterprise Linux の [セキユ](#)

[リティーガイド](#) または man ページ `firewall-cmd(1)` を参照してください。

### 3.5. 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。たとえば、`ldap/loadbalancer.example.com@EXAMPLE.COM` です。
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。  
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。
3. サービスキータブファイルを Directory Server にコピーします。たとえば、これを `/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。

```
# systemctl restart dirsrv@instance_name
```

6. 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。以下に例を示します。

```
# 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、この接続を確認する必要もあります。以下に例を示します。

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

## 第4章 DIRECTORY SERVER の更新

Red Hat は Red Hat Directory Server 11 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 10 をバージョン 11 に移行する場合は、[5章 Directory Server 10 から Directory Server 11 への移行](#)を参照してください。

### 前提条件

- サーバーに Red Hat Directory Server 11 がインストールされている。
- 更新するシステムは、Red Hat サブスクリプション管理サービスに登録されています。
- 有効な Red Hat Directory Server サブスクリプションがサーバーに割り当てられている。

### 4.1. DIRECTORY SERVER パッケージの更新

**yum module update redhat-ds** コマンドを実行して、Directory Server パッケージとその依存関係の新規更新を確認し、これらをインストールします。

```
# yum module update redhat-ds
```

更新時に、**dirsrv** サービスはサーバー上のすべてのインスタンスに対して自動的に再起動します。

## 第5章 DIRECTORY SERVER 10 から DIRECTORY SERVER 11 への移行

本章では、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 11 への移行を説明します。



### 重要

Red Hat は、Red Hat Directory Server 10 から 11 への移行のみをサポートします。

Directory Server 7、8、9 をバージョン 11 に移行するには、最初にインストールを Directory Server 10 に移行する必要があります。詳細は、Red Hat Directory Server 10 インストールガイドの [前のバージョンからの移行](#) を参照してください。

### 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。

### 5.1. レプリケーション方法を使用した DIRECTORY SERVER 11 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 11 に移行します。

#### 手順

1. Directory Server 11 をインストールします。[2章新しい Directory Server インスタンスの設定](#) を参照してください。
2. オプションで TLS を設定します。[Red Hat Directory Server 11 管理ガイドの TLS の有効化](#) の章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 11 管理ガイドの マルチサプライヤーレプリケーションの設定](#) セクションを参照してください。
4. Directory Server 10 ホストでレプリケーションを有効にし、Directory Server 11 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 10 管理者ガイドの Supplier Server で読み書きレプリカの設定](#) セクションを参照してください。
5. 必要に応じて、Directory Server 11 ホスト間でレプリカ合意を持つ Directory Server 11 ホストを設定します。
6. Directory Server 11 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。
7. Directory Server 10 ホストとのレプリカ合意を削除します。[Red Hat Directory Server 11 管理者ガイドの Replication Topology から Directory Server インスタンスを削除](#) を参照してください。
8. Directory Server 10 ホストをアンインストールします。[Red Hat Directory Server 10 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。

### 5.2. エクスポートおよびインポートの方法を使用した DIRECTORY SERVER 11 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 10 ホスト上で以下を行います。

a. **dirsrv** サービスを停止し、無効にします。

```
# systemctl stop dirsrv@instance_name
# 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 11 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 LDIF ファイル。
- カスタムスキーマの場合は **/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 11 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/cert8.db**
  - **/etc/dirsrv/slapd-instance\_name/key3.db**
  - **/etc/dirsrv/slapd-instance\_name/pin.txt**

d. Directory Server 11 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. 新しいホストで以下を行います。

a. Directory Server 11 をインストールします。詳細は、[2章新しいDirectory Server インスタンスの設定](#)を参照してください。

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、以下を行います。
  - i. **Red Hat Directory Server** 管理ガイドの [TLSの有効化](#) の章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。

```
# systemctl stop dirsrv@instance_name
```

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` ファイルを保存します。
- 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。

```
# systemctl start dirsrv@instance_name
```

Directory Server は NSS データベースを自動的に SQLite 形式に変換します。変換されたデータベースは、`/etc/dirsrv/slapd-instance_name/` ディレクトリーの `cert9.db` ファイルおよび `key4.db` ファイルに保存されます。

- vi. 必要に応じて、混乱を避けるために、古い NSS データベースを削除します。

```
# rm /etc/dirsrv/slapd-instance_name/cert8.db /etc/dirsrv/slapd-
instance_name/key3.db
```

- 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。以下に例を示します。

```
# 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

# systemctl restart dirsrv@instance_name
```

- 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を注意してください。

## 第6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する必要があります。本章では、パスワードの同期サービスがどのように機能するか、またそのインストール、更新、および削除の方法を説明します。

### 6.1. パスワード同期サービスの仕組みの理解

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 との間でパスワード同期を有効にするには、**Red Hat Directory** パスワード同期 サービスフックが DC のルーチンを変更する Windows パスワードに切り替わります。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せん。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。

### 6.2. 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前に、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
- [Red Hat カスタマーポータル](#) のアカウント

#### 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. バージョン フィールドで **11** を選択します。
5. **PassSync** インストーラー 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。

## 6.3. 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。詳細は「[パスワード同期サービスの仕組みの理解](#)」を参照してください。

### 前提条件

- Windows Active Directory ドメインコントローラー (DC) にダウンロードした最新バージョンの **PassSync Installer**。詳細は、「[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](#)」を参照してください。
- Red Hat Directory Server 管理ガイドの [Active Directory と Directory Server 間の Synchronization の設定](#) で説明されているように、準備された Directory Server ホスト。

### 手順

1. DC にソフトウェアをインストール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。
2. **RedHat-PassSync-ds11.\*-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。

**Red Hat Directory Password Sync Setup**

**Password Synchronization Information**

Please enter your password synchronization information

Host Name:

Port Number:

User Name:

Password:

Cert Token:

Search Base:

< Back    Next >    Cancel

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。



### 注記

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. Red Hat Directory Server 管理ガイドの [パスワード同期サービスの設定](#) で説明されているように、パスワード同期サービスを設定します。サービスが完全に設定されるまで、パスワード同期は失敗します。

書き込み可能なすべての Windows DC でこの手順を繰り返します。

## 6.4. 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。

### 前提条件

- **Red Hat Directory Password Sync** が Windows DC で実行されている。
- Windows Active Directory ドメインコントローラー (DC) にダウンロードした最新バージョンの **PassSync Installer**。詳細は、[「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」](#) を参照してください。

### 手順

1. DC にソフトウェアをインストール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。
2. **RedHat-PassSync-ds11.\*-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。



### 注記

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。

書き込み可能なすべての Windows DC でこの手順を繰り返します。

## 6.5. パスワード同期サービスのアンインストール

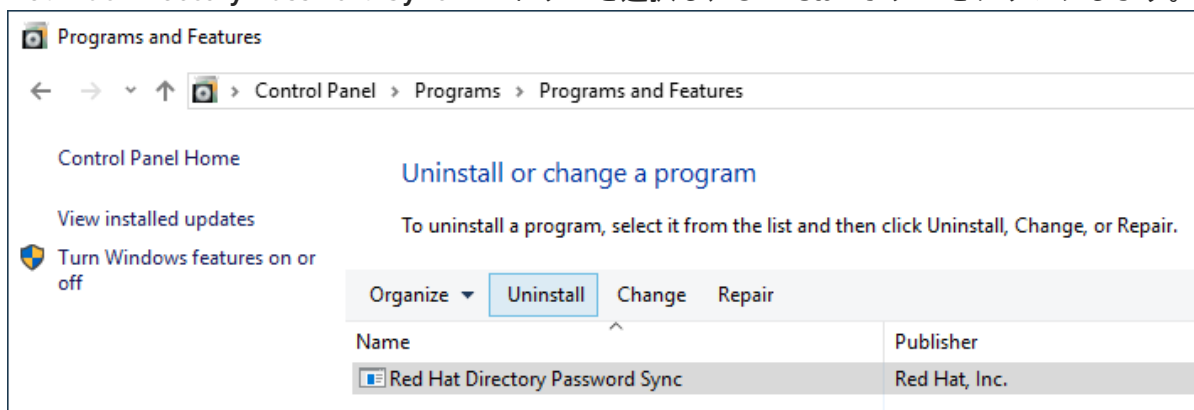
本セクションでは、Windows ドメインコントローラー (DC) から **Red Hat Directory** パスワード同期サービスをアンインストールする方法を説明します。

### 前提条件

- Windows DC で実行している **Red Hat Directory** パスワード同期。

### 手順

1. 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。
2. コントロールパネルを開きます。
3. **Programs** をクリックしてから、**Programs and Features** をクリックします。
4. **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。



5. **Yes** をクリックして確定します。

## 第7章 DIRECTORY SERVER のアンインストール

特定の状況では、管理者がホストから Directory Server をアンインストールする方法を説明します。本章では、この手順を説明します。

### 7.1. 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。

#### 前提条件

- ホストにインストールされている Directory Server

#### 手順

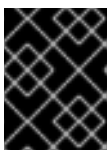
1. レプリケーショントポロジーからすべてのインスタンスを削除します。インスタンスがレプリケーショントポロジーのメンバーではない場合は、この手順を省略します。  
トポロジーからインスタンスを削除する方法は、Red Hat Directory Server 管理ガイドの [Replication Topology からサプライヤーの削除](#) を参照してください。
2. サーバーからすべてのインスタンスを削除します。  
詳細は、Red Hat Directory Server 管理ガイドの [Directory Server インスタンスの削除](#) を参照してください。
3. Directory Server パッケージを削除します。

```
# yum module remove redhat-ds
```

4. 必要に応じて、`dirsrv-11-for-rhel-8-x86_64-rpms` リポジトリを無効にします。

```
# subscription-manager repos --disable=dirsrv-11-for-rhel-8-x86_64-rpms
Repository 'dirsrv-11-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 の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一覧表示します。

```
# 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

- **subscription-manager** ユーティリティーの使用方法は、[Subscription Manager の使用および設定](#) ガイドを参照してください。

## 付録A RED HAT DIRECTORY SERVER 11 でコマンドラインユーティリティーが置き換え

以下の表は、Directory Server 10 以前のバージョンにおけるユーティリティーと、Directory Server 11 における代替ユーティリティーの一覧です。

Directory Server 10 以前	Directory Server 11
<b>bak2db</b> <b>bak2db.pl</b>	<b>dsctl bak2db</b>
<b>cl-dump</b> <b>cl-dump.pl</b>	<b>dsconf replication dump-changelog</b>
<b>cleanallruv.pl</b>	<b>dsconf repl-tasks cleanallruv</b>
<b>db2bak</b> <b>db2bak.pl</b>	<b>dsctl db2bak</b>
<b>db2index</b> <b>db2index.pl</b>	<b>dsctl db2index</b>
<b>db2ldif</b> <b>db2ldif.pl</b>	<b>dsctl db2ldif</b>
<b>dbgen</b>	<b>dsctl ldifgen</b>
<b>dbmon.sh</b>	<b>dsconf monitor dbmon</b>
<b>dbverify</b>	<b>dsctl dbverify</b>
<b>dn2rdn</b>	代替はありません。
<b>fixup-linkedattrs.pl</b>	<b>dsconf plugin linked-attr fixup</b>
<b>fixup-memberof.pl</b>	<b>dsconf plugin memberof fixup</b>
<b>fixup-memberuid.pl</b>	<b>dsconf plugin posix-winsync fixup</b>
<b>infadd</b>	代替はありません。
<b>ldif</b>	代替はありません。
<b>ldif2db</b> <b>ldif2db.pl</b>	<b>dsctl ldif2db</b>
<b>ldif2ldap</b>	代替はありません。

Directory Server 10 以前	Directory Server 11
<b>migrate-ds.pl</b>	代替はありません。
<b>migratecred</b>	代替はありません。
<b>mmldif</b>	代替はありません。
<b>monitor</b>	<b>dsconf backend monitor</b> <b>dsconf backend monitor-suffix</b>
<b>ns-accountstatus.pl</b>	<b>dsidm user status</b>
<b>ns-activate.pl</b>	<b>dsidm user unlock</b>
<b>ns-inactivate.pl</b>	<b>dsidm user lock</b>
<b>ns-newpwpolicy.pl</b>	<b>dsconf localpwp adduser</b> <b>dsconf localpwp addsubtree</b>
<b>remove-ds.pl</b>	<b>dsctl remove</b>
<b>repl-monitor</b> <b>repl-monitor.pl</b>	<b>dsconf replication monitor</b>
<b>restart-slapd</b>	<b>dsctl restart</b>
<b>restoreconfig</b>	代替はありません。
<b>rsearch</b>	代替はありません。
<b>saveconfig</b>	代替はありません。
<b>schema-reload.pl</b>	<b>dsconf schema reload</b>
<b>setup-ds.pl</b>	<b>dscreate</b>
<b>start-slapd</b>	<b>dsctl start</b>
<b>stop-slapd</b>	<b>dsctl stop</b>
<b>suffix2instance</b>	代替はありません。
<b>validate-syntax.pl</b>	<b>dsconf schema validate-syntax</b>
<b>upgradednformat</b>	代替はありません。

Directory Server 10 以前	Directory Server 11
<b>usn-tombstone-cleanup.pl</b>	<b>dsconf usn cleanup</b>
<b>verify-db.pl</b>	代替はありません。
<b>vlvindex</b>	<b>dsconf backend vlv-index</b>

## 付録B 改訂履歴

改訂番号は本ガイドに関するものであり、Red Hat Directory Server のバージョン番号ではありません。

バージョン	日付と変更	変更点
11.5-1	2022年3月10日: Red Hat Directory Server 11.5 版のガイドをリリース	Marc Muehlfeld
11.4-1	2021年11月9日: Red Hat Directory Server 11.4 版のガイドをリリース	Marc Muehlfeld
11.3-1	2021年5月3日: Red Hat Directory Server 11.3 版のガイドをリリース	Marc Muehlfeld
11.2-1	2020年11月3日: Red Hat Directory Server 11.2 版のガイドをリリース	Marc Muehlfeld
11.1-1	2020年4月28日: Red Hat Directory Server 11.1 版のガイドをリリース	Marc Muehlfeld
11.0-1	2019年11月5日: Red Hat Directory Server 11.0 版のガイドをリリース	Marc Muehlfeld