



Red Hat Directory Server 12

Red Hat Directory Server のバックアップおよび 復元

バックアップおよび復元に関する留意事項および手順

Red Hat Directory Server 12 Red Hat Directory Server のバックアップおよび復元

バックアップおよび復元に関する留意事項および手順

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 © 2023 | You need to change the HOLDER entity in the en-US/Backing_up_and_restoring_Red_Hat_Directory_Server.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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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

実稼動環境では、機能するテスト済みのバックアップおよび復元ストラテジーが重要です。このドキュメントでは、ユーティリティーと、Red Hat Directory Server が提供する Web コンソールを使って Directory Server インスタンスをバックアップして復元する方法を説明します。

目次

RED HAT ドキュメントへのフィードバック (英語のみ)	3
第1章 DIRECTORY SERVER のバックアップ	4
1.1. インスタンスの実行中コマンドラインを使用した全データベースのバックアップ	4
1.2. インスタンスのオフライン時コマンドラインを使用した全データベースのバックアップ	5
1.3. WEB コンソールを使用した全データベースのバックアップ	6
1.4. 設定ファイル、証明書データベース、およびカスタムスキーマファイルのバックアップ	6
第2章 グループのメンバーが DIRECTORY SERVER をバックアップすることの許可、およびグループメンバーの1つとしてのバックアップの実行	8
2.1. グループが DIRECTORY SERVER をバックアップすることの許可	8
2.2. 通常ユーザーとしてのバックアップの実行	9
第3章 DIRECTORY SERVER の復元	11
3.1. インスタンスの実行中コマンドラインを使用した全データベースの復元	11
3.2. インスタンスのオフライン時コマンドラインを使用した全データベースの復元	11
3.3. WEB コンソールを使用した全データベースの復元	12
3.4. 複製されたエントリーが含まれるデータベースの復元	13

RED HAT ドキュメントへのフィードバック (英語のみ)

弊社ドキュメントに対するご意見をお聞かせください。ドキュメントの改善点はございませんか。改善点を報告する場合は、以下のように行います。

- 特定の文章に簡単なコメントを記入する場合は、以下の手順を行います。
 1. ドキュメントの表示が **Multi-page HTML** 形式になっていることを確認してください。ドキュメントの右上隅に **Feedback** ボタンがあることを確認してください。
 2. マウスカーソルを使用して、コメントを追加するテキストの部分を強調表示します。
 3. 強調表示されたテキストの下に表示される **Add Feedback** ポップアップをクリックします。
 4. 表示される指示に従ってください。
- より詳細なフィードバックをお寄せいただく場合は、Bugzilla のチケットを作成してください。
 1. [Bugzilla](#) の Web サイトに移動します。
 2. Component (コンポーネント) として **Documentation** を使用します。
 3. **Description** フィールドに、ドキュメントの改善に向けたご提案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. **Submit Bug** をクリックします。

第1章 DIRECTORY SERVER のバックアップ

Directory Server のバックアップには以下が含まれます。

- データベースのインデックス化された属性が含まれる LDIF ファイル **dse_index.ldif**
- インスタンスの設定属性が含まれる LDIF ファイル **dse_instance.ldif**
- データベースで定義されたインデックスの **.db** ファイルが含まれる、各バックエンドのディレクトリー (**userRoot** など)
- トランザクションログファイル **log.***
- データベースのバージョンファイル **DBVERSION**

Directory Server は個別のデータベースのバックアップをサポートしない点に注意してください。

設定などの他の重要なファイルのバックアップに関する詳細は、[設定ファイル](#)、[証明書データベース](#)、および[カスタムスキーマファイルのバックアップ](#)を参照してください。

バックアップとは対照的に、[Directory Server からのデータのエクスポート](#)で説明されているようにデータをエクスポートできます。エクスポート機能を使用して、サブツリーなどの特定のデータをサーバーから LDIF 形式でエクスポートします。

1.1. インスタンスの実行中コマンドラインを使用した全データベースのバックアップ

実行中の Directory Server インスタンスのデータベースをすべてバックアップするには、**dsconf backup create** コマンドを使用します。

前提条件

- **dirsrv** ユーザーに、バックアップ先ディレクトリーの書き込みパーミッションがある。
- Directory Server インスタンスが実行している。

手順

1. すべてのデータベースをバックアップします。

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backup create
The backup create task has finished successfully
```

デフォルトでは、**dsconf** は、バックアップを `/var/lib/dirsrv/slapd-instance_name/bak/` ディレクトリーの `instance_name-YYYY_MM_DD_hh_mm_ss` というサブディレクトリーに保存します。別の場所を指定するには、コマンドにディレクトリー名を追加します。

2. バックアップ中の問題について、`/var/log/dirsrv/slapd-instance_name/errors` ログを検索します。

関連情報

- データのバックアップに使用できる追加の設定をすべて表示するには、**dsconf ldap://server.example.com backup create --help** コマンドの出力を参照してください。

- [設定ファイル、証明書データベース、およびカスタムスキーマファイルのバックアップ](#)
- [インスタンスの実行中コマンドラインを使用した全データベースの復元](#)
- [ディレクトリーサーバーからのデータのエクスポート](#)

1.2. インスタンスのオフライン時コマンドラインを使用した全データベースのバックアップ

Directory Server インスタンスがオフライン時にデータベースのバックアップを作成するには、**dsctl db2bak** コマンドを使用します。

前提条件

- **dirsrv** ユーザーに、バックアップ先ディレクトリーの書き込みパーミッションがある。
- Directory Server インスタンスが実行していない。

手順

1. すべてのデータベースをバックアップします。

```
# dsctl instance_name db2bak
db2bak successful
```

デフォルトでは、**dsctl db2bak** は、バックアップを `/var/lib/dirsrv/slaped-instance_name/bak/` ディレクトリーの `instance_name-YYYY_MM_DD_hh_mm_ss` というサブディレクトリーに保存します。別の場所を指定するには、コマンドにディレクトリー名を追加します。

必要に応じて、コマンドに **-v** オプションを指定して詳細な出力を表示します。

```
# dsctl -v instance_name db2bak
...
DEBUG: Instance allocated
DEBUG: systemd status -> True
...
INFO: db2bak successful
```

2. バックアップ中の問題について、`/var/log/dirsrv/slaped-instance_name/errors` ログを検索します。
3. オプション: インスタンスを起動します。

```
# dsctl instance_name start
```

関連情報

- [設定ファイル、証明書データベース、およびカスタムスキーマファイルのバックアップ](#)
- [インスタンスのオフライン時コマンドラインを使用した全データベースの復元](#)
- [ディレクトリーサーバーからのデータのエクスポート](#)

1.3. WEB コンソールを使用した全データベースのバックアップ

Directory Server は、Web コンソールを使用したデータのバックアップをサポートします。

前提条件

- **dirsrv** ユーザーに、バックアップ先ディレクトリーの書き込みパーミッションがある。
- 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. **Actions** ボタンをクリックして、**Manage Backups** を選択します。
2. **Create Backup** をクリックします。
3. バックアップの作成日時を示すタイムスタンプなど、バックアップの名前を入力します。
4. **Create Backup** をクリックします。
5. バックアップ中の問題についてログを確認するには、**Monitoring** → **Logging** → **Errors Log** メニューを開きます。

サーバーは、バックアップを `/var/lib/dirsrv/slapped-instance_name/bak/` ディレクトリー内の指定した名前のサブディレクトリーに保存します。

関連情報

- [設定ファイル、証明書データベース、およびカスタムスキーマファイルのバックアップ](#)
- [Web コンソールを使用した全データベースの復元](#)
- [ディレクトリーサーバーからのデータのエクスポート](#)

1.4. 設定ファイル、証明書データベース、およびカスタムスキーマファイルのバックアップ

Directory Server に統合されているバックアップメカニズムは、データベースのみのバックアップを作成します。ただし、`/etc/dirsrv/slapped-instance_name/` ディレクトリーには追加のファイルが保存されています。これらのファイルは、たとえば、ハードウェア障害後に別のサーバー上でインスタンスを復元するのに必要になります。

Web コンソールで設定ディレクトリーのバックアップはできないことに注意してください。



重要

バックアップ時に、証明書データベースを更新しないでください。そうでない場合は、このデータベースがバックアップで一貫性がない可能性があります。

手順

- `/etc/dirsrv/slapped-instance_name/` ディレクトリーの内容をアーカイブファイルに保存します。

```
# cd /etc/dirsrv/  
# tar -zcvf /root/config_slapd-instance_name-$(date +%Y-%m-%d_%H-%M-%S).tar.gz  
slapd-instance_name/
```

これにより、`/etc/dirsrv/slapd-instance_name/` ディレクトリーの内容で
`/root/config_slapd-instance_name-time_stamp.tar.gz` アーカイブが作成されます。

第2章 グループのメンバーが DIRECTORY SERVER をバックアップすることの許可、およびグループメンバーの1つとしてのバックアップの実行

グループのメンバーに、インスタンスをバックアップしバックアップを実施するパーミッションを設定できます。バックアップスクリプトまたは cron ジョブに **cn=Directory Manager** の認証情報を設定する必要がなくなるため、セキュリティが向上します。また、グループを変更して、バックアップのパーミッションを簡単に許可し、取り消すことができます。

2.1. グループが DIRECTORY SERVER をバックアップすることの許可

この手順を使用して、**cn=backup_users,ou=groups,dc=example,dc=com** グループを追加し、このグループのメンバーがバックアップタスクを作成するのを許可します。

前提条件

- **ou=groups,dc=example,dc=com** エントリーがデータベースに存在する。

手順

1. **cn=backup_users,ou=groups,dc=example,dc=com** グループを作成します。

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" group create --cn backup_users
```

2. **cn=backup_users,ou=groups,dc=example,dc=com** グループのメンバーがバックアップタスクを作成するのを許可するアクセス制御手順 (ACI) を追加します。

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com

dn: cn=config
changetype: modify
add: aci
aci: (target = "ldap:///cn=backup,cn=tasks,cn=config")(targetattr="*")
(version 3.0 ; acl "permission: Allow backup_users
group to create backup tasks" ; allow (add, read, search) groupdn
= "ldap:///cn=backup_users,ou=groups,dc=example,dc=com");)
-
add: aci
aci: (target = "ldap:///cn=config")(targetattr = "nsslapd-bakdir ||
objectClass") (version 3.0 ; acl "permission: Allow backup_users
group to access bakdir attribute" ; allow (read,search)
groupdn = "ldap:///cn=backup_users,ou=groups,dc=example,dc=com");)
```

3. ユーザーを作成します。
 - a. ユーザーアカウントを作成します。

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" user create --uid="example" --cn="example" --
uidNumber="1000" --gidNumber="1000" --homeDirectory="/home/example/" --
displayName="Example User"
```

- b. ユーザーアカウントのパスワードを設定します。

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" account reset_password
"uid=example,ou=People,dc=example,dc=com" "password"
```

4. `uid=example,ou=People,dc=example,dc=com` ユーザーを
`cn=backup_users,ou=groups,dc=example,dc=com` グループに追加します。

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" group add_member backup_users
uid=example,ou=People,dc=example,dc=com
```

検証

- `cn=config` エントリーに設定された ACI を表示します。

```
# ldapsearch -o ldif-wrap=no -LLLx -D "cn=directory manager" -W -H
ldap://server.example.com -b cn=config aci=* aci -s base
dn: cn=config
aci: (target = "ldap:///cn=backup,cn=tasks,cn=config")(targetattr="*)(version 3.0 ; aci
"permission: Allow backup_users group to create backup tasks" ; allow (add, read, search)
groupdn = "ldap:///cn=backup_users,ou=groups,dc=example,dc=com";)
aci: (target = "ldap:///cn=config")(targetattr = "nsslapd-bakdir || objectClass")(version 3.0 ; aci
"permission: Allow backup_users group to access bakdir attribute" ; allow (read,search)
groupdn = "ldap:///cn=backup_users,ou=groups,dc=example,dc=com";)
...
```

2.2. 通常ユーザーとしてのバックアップの実行

`cn=Directory Manager` ではなく、通常のユーザーとしてバックアップを実行できます。

前提条件

- `cn=backup_users,ou=groups,dc=example,dc=com` グループのメンバーがデータをバックアップするのを許可している。
- バックアップの実行に使用するユーザーが
`cn=backup_users,ou=groups,dc=example,dc=com` グループのメンバーである。

手順

- 以下の方法のいずれかを使用してバックアップタスクを作成します。

- `dsconf backup create` コマンドの使用:

```
# dsconf -D "uid=example,ou=People,dc=example,dc=com"
ldap://server.example.com backup create
```

- タスクの手動での作成:

```
# ldapadd -D "uid=example,ou=People,dc=example,dc=com" -W -H
ldap://server.example.com
```

```
dn: cn=backup-2021_07_23_12:55_00,cn=backup,cn=tasks,cn=config
changetype: add
objectClass: extensibleObject
nsarchivedir: /var/lib/dirsrv/slapd-instance_name/bak/backup-2021_07_23_12:55_00
nsdatabasetype: ldbm database
cn: backup-2021_07_23_12:55_00
```

検証

- バックアップが作成されたことを確認します。

```
# ls -l /var/lib/dirsrv/slapd-instance_name/bak/
total 0
drwx-----. 3 dirsrv dirsrv 108 Jul 23 12:55 backup-2021_07_23_12_55_00
...
```

関連情報

- [グループが Directory Server をバックアップすることの許可](#)

第3章 DIRECTORY SERVER の復元

ハードウェア障害の後などの特定の状況では、Directory Server を復元する必要があります。これは、コマンドラインまたは Web コンソールを使用して実行できます。Directory Server は個別のデータベースの復元をサポートしない点に注意してください。

データベースにカスタムデータを入力する場合は、インポート機能を使用します。サーバーから特定のデータを LDIF 形式でインポートできます。詳細は [Directory Server へのデータのインポート](#) を参照してください。

3.1. インスタンスの実行中コマンドラインを使用した全データベースの復元

実行中の Directory Server インスタンスにすべてのデータベースを復元するには、**dsconf backup restore** コマンドを使用します。

前提条件

- Directory Server のバックアップがある。
- **dirsrv** ユーザーに、バックアップディレクトリーの読み取りパーミッションがある。
- Directory Server インスタンスが実行している。

手順

1. `/var/lib/dirsrv/slapd-instance_name/bak/instance_name-YYYY_MM_DD_hh_mm_ss` ディレクトリーに保存されているバックアップから、すべてのデータベースを復元します。

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backup restore
/var/lib/dirsrv/slapd-instance_name/bak/instance_name-YYYY_MM_DD_hh_mm_ss
The backup restore task has finished successfully
```

2. 復元中の問題について、`/var/log/dirsrv/slapd-instance_name/errors` ログを検索します。

関連情報

- データの復元に使用できる追加の設定をすべて表示するには、**dsconf ldap://server.example.com backup restore --help** コマンドの出力を参照してください。
- [インスタンスの実行中コマンドラインを使用した全データベースのバックアップ](#)
- [ディレクトリーサーバーへのデータのインポート](#)

3.2. インスタンスのオフライン時コマンドラインを使用した全データベースの復元

インスタンスがオフライン時にすべてのデータベースを復元するには、**dsctl bak2db** コマンドを使用します。

前提条件

- Directory Server のバックアップがある。

- **dirsrv** ユーザーに、バックアップディレクトリーの読み取りパーミッションがある。
- Directory Server インスタンスが実行していない。

手順

1. `/var/lib/dirsrv/slapd-instance_name/bak/instance_name-YYYY_MM_DD_hh_mm_ss` ディレクトリーに保存されているバックアップから、すべてのデータベースを復元します。

```
# dsctl instance_name bak2db /var/lib/dirsrv/slapd-instance_name/bak/instance_name-
YYYY_MM_DD_hh_mm_ss/
bak2db successful
```

必要に応じて、コマンドに `-v` オプションを指定して詳細な出力を表示します。

```
# dsctl -v instance_name bak2db
/var/lib/dirsrv/slapd-instance_name/bak/instance_name-YYYY_MM_DD_hh_mm_ss/
...
DEBUG: Instance allocated
DEBUG: OK group dirsrv exists
DEBUG: OK user dirsrv exists
DEBUG: systemd status -> True
...
INFO: bak2db successful
```

2. 復元中の問題について、`/var/log/dirsrv/slapd-instance_name/errors` ログを検索します。
3. オプション: インスタンスを起動します。

```
# dsctl instance_name start
```

関連情報

- [インスタンスのオフライン時コマンドラインを使用した全データベースのバックアップ](#)
- [ディレクトリーサーバーへのデータのインポート](#)

3.3. WEB コンソールを使用した全データベースの復元

Directory Server は、Web コンソールを使用したデータの復元をサポートします。

前提条件

- バックアップが、`/var/lib/dirsrv/slapd-instance_name/bak/` ディレクトリーに保存されている。
- **dirsrv** ユーザーに、バックアップディレクトリーの読み取りパーミッションがある。
- 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. **Actions** メニューをクリックして、**Manage Backups** を選択します。表示されるウィンドウには、`/var/lib/dirsrv/slaped-instance_name/bak/` ディレクトリーで利用可能なバックアップが表示されます。
2. 復元するバックアップの横にある **Actions** メニューを開き、**Restore Backup** を選択します。
3. **Yes** をクリックして確定します。
4. 復元中の問題についてログを確認するには、**Monitoring** → **Logging** → **Errors Log** メニューを開きます。

関連情報

- [Web コンソールを使用した全データベースのバックアップ](#)
- [ディレクトリーサーバーへのデータのインポート](#)

3.4. 複製されたエントリーが含まれるデータベースの復元

サプライヤーサーバーを復元すると、いくつかの状況が発生する可能性があります。

- コンシューマーサーバーも復元します。
非常にまれな状況では、すべてのデータベースで、(データが同期されるため)、コンシューマーはサプライヤーと同期したままとなり、他に何もする必要はありません。レプリケーションは中断せずに再開します。
- サプライヤーだけが復元します。
サプライヤーのみが復元された場合や、コンシューマーが別のバックアップから復元された場合は、サプライヤーがコンシューマーを再初期化して、データベースのデータを更新します。
- サプライヤーサーバーでチェンジログエントリーの有効期限が切れていません。
データベースのバックアップの取得後にサプライヤーの変更ログが期限切れになっていない場合は、ローカルコンシューマーを復元し、通常のコピーを続けます。この状態は、**cn=changelog5,cn=config** エントリーで、最大 changelog age 属性 **nsslapd-changelogmaxage** に設定された値よりも短い期間内にバックアップを取得した場合に限り発生します。

Directory Server は、レプリカとその changelog 間の互換性を自動的に検出します。不一致が検出されると、サーバーは古い changelog ファイルを削除し、空のファイルを新たに作成します。

- changelog エントリーは、ローカルバックアップの時間以降、サプライヤーサーバーで期限切れです。
changelog エントリーの有効期限が切れている場合は、コンシューマーを再初期化します。

例3.1 Directory Server のレプリケーショントポロジーの復元

2つのサプライヤーと2つのコンシューマーサーバーで設定されるレプリケーション環境のサーバーをすべて復元するには、以下を実行します。

1. `restore` または `import` のいずれかを使用して、最初のサプライヤーを再初期化します。
2. レプリケーションを使用して残りのサーバーをオンラインに初期化します。
 - a. 最初のサプライヤーから2番目のサプライヤーを初期化します。

- b. サプライヤーからコンシューマーを初期化します。
3. 各サーバーでレプリケーションのステータスを表示し、レプリケーションが正しく機能していることを確認します。

復元操作中に、復元されたデータベースに関連する changelog が削除されます。再初期化が必要であることを示すメッセージが、サプライヤーサーバーのログファイルに記録されます。

関連情報

- [nsslapd-changelogmaxage](#)
- [インスタンスの実行中コマンドラインを使用した全データベースの復元](#)
- [ディレクトリーサーバーへのデータのインポート](#)
- [レプリケーションの設定および管理](#)