Red Hat Directory Server 12

Backing up and restoring Red Hat Directory Server

Considerations and procedures about backup and restore

Last Updated: 2022-05-18

Red Hat Directory Server 12 Backing up and restoring Red Hat Directory Server

Considerations and procedures about backup and restore

Legal Notice

Abstract

A working and tested backup and restore strategy is vital in a production environment. This documentation describes how to back up and restore a Directory Server instance using utilities and the web console provided by Red Hat Directory Server.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
  1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
  2. Use your mouse cursor to highlight the part of text that you want to comment on.
  3. Click the **Add Feedback** pop-up that appears below the highlighted text.
  4. Follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
  1. Go to the Bugzilla website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.

CHAPTER 1. BACKING UP DIRECTORY SERVER

A backup in Directory Server contains:

- An LDIF file **dse_index.ldif** containing database indexed attributes
- An LDIF file **dse_instance.ldif** containing instance configuration attributes
- A directory for each backend, for example **userRoot**, which contains **.db** files for indexes defined in the database
- A transaction log file **log.***
- A database version file **DBVERSION**

Note that Directory Server does not support backing up individual databases.

For details about backing up other important files, such as the configuration, see Backing up configuration files, the certificate database, and custom schema files.

In contrast to a backup, you can export data as described in Exporting data from Directory Server . Use the export feature to export specific data from a server, such as a subtree, in LDIF format.

1.1. BACKING UP ALL DATABASES USING THE COMMAND LINE WHILE THE INSTANCE IS RUNNING

To back up all databases of the Directory Server instance that is running, use the **dsconf backup create** command.

Prerequisites

- The **dirsrv** user has write permissions in the destination directory.
- The Directory Server instance is running.

Procedure

1. Back up all databases:

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

   By default, **dsconf** stores the backup in a subdirectory called ***instance_name-YYYY_MM_DD_hh_mm_ss*** in the **/var/lib/dirsrv/slapd-*instance_name*/bak/** directory. To specify a different location, append a directory name to the command.

2. Search the **/var/log/dirsrv/slapd-*instance_name*/errors** log for problems during the backup.

Additional resources

- To display all additional settings that you can use to back up data, see the output of the **dsconf *ldap://server.example.com* backup create --help** command.
- Backing up configuration files, the certificate database, and custom schema files

- Restoring all databases using the command line while the instance is running
- Exporting data from Directory Server

1.2. BACKING UP ALL DATABASES USING THE COMMAND LINE WHILE THE INSTANCE IS OFFLINE

To back up databases when the Directory Server instance is offline, use the **dsctl db2bak** command.

Prerequisites

- The **dirsrv** user has write permissions in the destination directory.
- The Directory Server instance is not running.

Procedure

1. Back up all databases:

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

   By default, **dsctl db2bak** stores the backup in a subdirectory called ***instance_name-YYYY_MM_DD_hh_mm_ss*** in the **/var/lib/dirsrv/slapd-*instance_name*/bak/** directory. To specify a different location, append a directory name to the command.

   Optionally, pass the **-v** option to the command to display verbose output:

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

2. Search the **/var/log/dirsrv/slapd-*instance_name*/errors** log for problems during the backup.
3. Optional: Start the instance:

```
# dsctl instance_name start
```

Additional resources

- Backing up configuration files, the certificate database, and custom schema files
- Restoring all databases using the command line while the instance is offline
- Exporting data from Directory Server

1.3. BACKING UP ALL DATABASES USING THE WEB CONSOLE

Directory Server supports data backup using the web console.

Prerequisites

- The **dirsrv** user has write permissions in the destination directory.
- You are logged in to the instance in the web console.

Procedure

1. Click the **Actions** button, and select **Manage Backups**.
2. Click **Create Backup**.
3. Enter a name for the backup, such as a time stamp to indicate the creation date and time of the backup.
4. Click **Create Backup**.
5. To check the log for problems during the backup, open the **Monitoring → Logging → Errors Log** menu.

The server stores the backup in a subdirectory with the name you entered in the **/var/lib/dirsrv/slapd-*instance_name*/bak/** directory.

Additional resources

- Backing up configuration files, the certificate database, and custom schema files
- Restoring all databases using the web console
- Exporting data from Directory Server

1.4. BACKING UP CONFIGURATION FILES, THE CERTIFICATE DATABASE, AND CUSTOM SCHEMA FILES

The backup mechanism integrated into Directory Server backs up only the databases. However, there are additional files stored in the **/etc/dirsrv/slapd-*instance_name*/** directory which are required to, for example, restore an instance on a different server after a hardware failure.

Note that you cannot back up the configuration directory in the web console.

IMPORTANT

During the backup, do not update the certificate database. Otherwise, this database might not be consistent in the backup.

Procedure

- Store the content of the **/etc/dirsrv/slapd-*instance_name*/** directory into an archive file:

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

This creates the **/root/config_slapd-*instance_name-time_stamp*.tar.gz** archive with the content of the **/etc/dirsrv/slapd-*instance_name*/** directory.

CHAPTER 2. ENABLING MEMBERS OF A GROUP TO BACK UP DIRECTORY SERVER AND PERFORMING THE BACKUP AS ONE OF THE GROUP MEMBERS

You can configure that members of a group have permissions to back up an instance and perform the backup. This increases the security because you no longer need to set the credentials of **cn=Directory Manager** in your backup script or cron jobs. Additionally, you can easily grant and revoke the backup permissions by modifying the group.

2.1. ENABLING A GROUP TO BACK UP DIRECTORY SERVER

Use this procedure to add the **cn=backup_users,ou=groups,dc=example,dc=com** group and enable members of this group to create backup tasks.

Procedure

1. Create the **cn=backup_users,ou=groups,dc=example,dc=com** group:

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

2. Add an access control instruction (ACI) that allows members of the **cn=backup_users,ou=groups,dc=example,dc=com** group to create backup tasks:

```
# 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. Create a user:

   a. Create a user account:

```
# 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. Set a password on the user account:

```
# 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. Add the **uid=example,ou=People,dc=example,dc=com** user to the **cn=backup_users,ou=groups,dc=example,dc=com** group:

```
# 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
```

Verification

- Display the ACIs set on the **cn=config** entry:

```
# 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 ; 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";)
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";)
...
```

2.2. PERFORMING A BACKUP AS A REGULAR USER

You can perform backups as a regular user instead of **cn=Directory Manager**.

Prerequisites

- You enabled members of the **cn=backup_users,ou=groups,dc=example,dc=com** group to perform backups.
- The user you use to perform the backup is a member of the **cn=backup_users,ou=groups,dc=example,dc=com** group.

Procedure

- Create a backup task using one of the following methods:
  - Using the **dsconf backup create** command:

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

  - By manually creating the task:

```
# 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
```

Verification

- Verify that the backup was created:

```
# 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
...
```

Additional resources

- Enabling a group to back up Directory Server

CHAPTER 3. RESTORING DIRECTORY SERVER

In certain situations, for example after a hardware failure, you need to restore Directory Server. You can do that using the command line or the web console. Note that Directory Server does not support restoration of individual databases.

When you want to populate the database with custom data, use the import feature. You can import specific data from a server in LDIF format. For details, see Importing data to Directory Server .

3.1. RESTORING ALL DATABASES USING THE COMMAND LINE WHILE THE INSTANCE IS RUNNING

To restore all databases on the Directory Server instance that is running, use the **dsconf backup restore** command.

Prerequisites

- You have a Directory Server backup.
- The **dirsrv** user has read permissions in the backup directory.
- The Directory Server instance is running.

Procedure

1. Restore all databases from the backup stored in the **/var/lib/dirsrv/slapd-*instance_name*/bak/*instance_name-YYYY_MM_DD_hh_mm_ss*** directory:

```
# 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. Search the **/var/log/dirsrv/slapd-*instance_name*/errors** log for problems during the restore.

Additional resources

- To display all additional settings that you can use to restore data, see the output of the **dsconf *ldap://server.example.com* backup restore --help** command.
- Backing up all databases using the command line while the instance is running
- Importing data to Directory Server

3.2. RESTORING ALL DATABASES USING THE COMMAND LINE WHILE THE INSTANCE IS OFFLINE

To restore all databases when the instance is offline, use the **dsctl bak2db** command.

Prerequisites

- You have a Directory Server backup.

- The **dirsrv** user has read permissions in the backup directory.
- The Directory Server instance is not running.

Procedure

1. Restore all databases from the backup stored in the **/var/lib/dirsrv/slapd-*instance_name*/bak/*instance_name-YYYY_MM_DD_hh_mm_ss*** directory:

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

   Optionally, pass the **-v** option to the command to display verbose output:

```
# 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. Search the **/var/log/dirsrv/slapd-*instance_name*/errors** log for problems during the restore.
3. Optional: Start the instance:

```
# dsctl instance_name start
```

Additional resources

- Backing up all databases using the command line while the instance is offline
- Importing data to Directory Server

3.3. RESTORING ALL DATABASES USING THE WEB CONSOLE

Directory Server supports restoring data using the web console.

Prerequisites

- A backup is stored in the **/var/lib/dirsrv/slapd-*instance_name*/bak/** directory.
- The **dirsrv** user has read permissions in the backup directory.
- You are logged in to the instance in the web console.

Procedure

1. Click the **Actions** menu, and select **Manage Backups**. The displayed window lists the available backups in the **/var/lib/dirsrv/slapd-*instance_name*/bak/** directory.

2. Open the **Actions** menu next to the backup you want to restore, and select **Restore Backup**.
3. Click **Yes** to confirm.
4. To check the log for problems during the restore, open the **Monitoring → Logging → Errors Log** menu.

Additional resources

- Backing up all databases using the web console
- Importing data to Directory Server

3.4. RESTORING DATABASES THAT INCLUDE REPLICATED ENTRIES

Several situations can occur when a supplier server is restored:

- The consumer servers are also restored.
  For the very unlikely situation, that all databases are restored from backups taken at exactly the same time (so that the data are in sync), the consumers remain synchronized with the supplier, and it is not necessary to do anything else. Replication resumes without interruption.
- Only the supplier is restored.
  If only the supplier is restored or if the consumers are restored from backups taken at different times, reinitialize the consumers for the supplier to update the data in the database.
- Changelog entries have not yet expired on the supplier server.
  If the supplier's changelog has not expired since the database backup was taken, then restore the local consumer and continue with normal operations. This situation occurs only if the backup was taken within a period of time that is shorter than the value set for the maximum changelog age attribute, **nsslapd-changelogmaxage**, in the **cn=changelog5,cn=config** entry.

  Directory Server automatically detects the compatibility between the replica and its changelog. If a mismatch is detected, the server removes the old changelog file and creates a new, empty one.
- Changelog entries have expired on the supplier server since the time of the local backup.
  If changelog entries have expired, reinitialize the consumer.

> **Example 3.1. Restoring a Directory Server replication topology**
>
> To restore all servers in a replication environment, consisting of two suppliers and two consumer servers:
>
> 1. Reinitialize the first supplier using either restore or import.
> 2. Online-initialize the remaining servers by using replication:
>   a. Initialize the second supplier from the first one.
>   b. Initialize the consumers from the supplier.
> 3. On each server, display the replication status to verify that replication works correctly.

The changelog associated with the restored database will be erased during the restore operation. A message will be logged to the supplier server's log files indicating that reinitialization is required.

Additional resources

- nsslapd-changelogmaxage
- Restoring all databases using the command line while the instace is running
- Importing data to Directory Server
- Configuring and managing replication