Red Hat Directory Server 12

Installing Red Hat Directory Server

Instructions for installing Red Hat Directory Server

Last Updated: 2022-05-18

Red Hat Directory Server 12 Installing Red Hat Directory Server

Instructions for installing Red Hat Directory Server

Legal Notice

Abstract

This guide contains information about installing, updating, and uninstalling Red Hat Directory Server 12 and associated services.

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. SETTING UP A NEW INSTANCE ON THE COMMAND LINE USING A .INF FILE

When you set up Directory Server using a **.inf** file on the command line you can customize advanced settings. For example, you can customize in the **.inf** file the following settings:

- The user and group the **ns-slapd** Directory Server process uses after the service has started. Note that, if you use a different user and group, you must manually create the user and group before you start the installation.
- Paths, such as the configuration, backup, and data directory.
- Certificate validity.

1.1. PREREQUISITES

- The server meets the requirements of the latest Red Hat Directory Server version as described in the Red Hat Directory Server 12 Release Notes .

1.2. INSTALLING THE DIRECTORY SERVER PACKAGES

Use the following procedure to install the Directory Server packages.

Prerequisites

- You registered the system to the Red Hat subscription management service.
- You have a valid Red Hat Directory Server subscription in your Red Hat account.
- The RHEL default repositories, **BaseOS** and **AppStream**, are enabled.

Procedure

1. List the available subscriptions in your Red Hat account that provide a Red Hat Directory Server subscription, and note the pool ID:

```
# 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. Attach the Red Hat Directory Server subscription to the system using the its pool ID:

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

3. Enable the **dirsrv-12-for-rhel-9-x86_64-rpms** repository:

```
# subscription-manager repos --enable=dirsrv-12-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12-for-rhel-9-x86_64-rpms' is enabled for this system.
```

4. Install the **redhat-ds:12** module:

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

This command automatically installs all required dependencies.

Additional resources

- Using and Configuring Subscription Manager

1.3. CREATING A .INF FILE FOR A DIRECTORY SERVER INSTANCE INSTALLATION

Create a **.inf** file for the **dscreate** utility, and adjust the file to your environment. In a later step, you will use this file to create the new Directory Server instance.

Prerequisites

- You installed the **redhat-ds:12** module.

Procedure

1. Use the **dscreate create-template** command to create a template **.inf** file. For example, to store the template in the **/root/instance_name.inf** file, enter:

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

The created file contains all available parameters including descriptions.

2. Edit the file that you created in the previous step:

   a. Uncomment the parameters that you want to set to customize the installation.
   All parameters have defaults. However, Red Hat recommends that you customize certain parameters for a production environment. For example, set at least the following parameters in the **[slapd]** section:

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

   b. To automatically create a suffix during instance creation, set the following parameters in the **[backend-userroot]** section:

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

IMPORTANT

If you do not create a suffix during instance creation, you must create it later manually before you can store data in this instance.

c. Optional: Uncomment other parameters and set them to appropriate values for your environment. For example, use these parameters to specify different ports for the LDAP and LDAPS protocol.

NOTE

By default, new instances that you create include a self-signed certificate and TLS enabled. For increased security, Red Hat recommends that you do not disable this feature. Note that you can replace the self-signed certificate with a certificate issued by a Certificate Authority (CA) at a later date.

Additional resources

- Enabling TLS-encrypted connections to Directory Server

1.4. USING A .INF FILE TO SET UP A NEW DIRECTORY SERVER INSTANCE

This section describes how to use a **.inf** file to set up a new Directory Server instance using the command line.

Prerequisites

- You created a **.inf** file for the Directory Server instance.

Procedure

1. Pass the **.inf** file to the **dscreate from-file** command to create the new instance:

```
# 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
```

The **dscreate** utility automatically starts the instance and configures RHEL to start the service when the system boots.

2. Open the required ports in the firewall:

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

3. Reload the firewall configuration:

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

CHAPTER 2. SETTING UP A NEW INSTANCE ON THE COMMAND LINE USING THE INTERACTIVE INSTALLER

Administrators can use the Directory Server interactive installer to set up a new instance by answering questions about the configuration for the new instance.

If you want to customize additional settings during the installation, use a **.inf** file instead of the interactive installer. For details, see Chapter 1, *Setting up a new instance on the command line using a .inf file*.

2.1. PREREQUISITES

- The server meets the requirements of the latest Red Hat Directory Server version as described in the Red Hat Directory Server 12 Release Notes .

2.2. INSTALLING THE DIRECTORY SERVER PACKAGES

Use the following procedure to install the Directory Server packages.

Prerequisites

- You registered the system to the Red Hat subscription management service.
- You have a valid Red Hat Directory Server subscription in your Red Hat account.
- The RHEL default repositories, **BaseOS** and **AppStream**, are enabled.

Procedure

1. List the available subscriptions in your Red Hat account that provide a Red Hat Directory Server subscription, and note the pool ID:

```
# 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. Attach the Red Hat Directory Server subscription to the system using the its pool ID:

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

3. Enable the **dirsrv-12-for-rhel-9-x86_64-rpms** repository:

```
# subscription-manager repos --enable=dirsrv-12-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12-for-rhel-9-x86_64-rpms' is enabled for this system.
```

4. Install the **redhat-ds:12** module:

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

This command automatically installs all required dependencies.

Additional resources

- Using and Configuring Subscription Manager

2.3. CREATING AN INSTANCE USING THE INTERACTIVE INSTALLER

This section explains how to use the interactive installer to create a new Directory Server instance.

Procedure

1. Start the interactive installer:

```
# dscreate interactive
```

2. Answer the questions of the interactive installer.
   To use the default values displayed in square brackets behind most questions in the installer, press **Enter** without entering a value.

```
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]:

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

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

NOTE

Instead of setting a password in clear text you can set a **{*algorithm*}*hash*** string generated by the **pwdhash** utility.

3. Open the required ports in the firewall:

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

4. Reload the firewall configuration:

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

CHAPTER 3. SETTING UP A NEW INSTANCE USING THE WEB CONSOLE

If you prefer a browser-based interface to set up Directory Server, you can use the Directory Server web console.

3.1. PREREQUISITES

- The server meets the requirements of the latest Red Hat Directory Server version as described in the Red Hat Directory Server 12 Release Notes .

3.2. INSTALLING THE DIRECTORY SERVER PACKAGES

Use the following procedure to install the Directory Server packages.

Prerequisites

- You registered the system to the Red Hat subscription management service.
- You have a valid Red Hat Directory Server subscription in your Red Hat account.
- The RHEL default repositories, **BaseOS** and **AppStream**, are enabled.

Procedure

1. List the available subscriptions in your Red Hat account that provide a Red Hat Directory Server subscription, and note the pool ID:

```
# 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. Attach the Red Hat Directory Server subscription to the system using the its pool ID:

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

3. Enable the **dirsrv-12-for-rhel-9-x86_64-rpms** repository:

```
# subscription-manager repos --enable=dirsrv-12-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12-for-rhel-9-x86_64-rpms' is enabled for this system.
```

4. Install the **redhat-ds:12** module:

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

This command automatically installs all required dependencies.

Additional resources

- Using and Configuring Subscription Manager

3.3. USING THE WEB CONSOLE TO SET UP A NEW DIRECTORY SERVER INSTANCE

This section describes how to use the web console to set up a new Directory Server instance.

Prerequisites

- The **cockpit** web console package is installed.
- The **cockpit.socket** systemd unit is enabled and started.
- You opened port **9090** in the local firewall to allow accessing the web console.

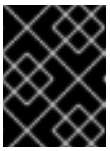
Procedure

1. Use a browser to connect to the web console running on port 9090 on the Directory Server host:

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

2. Log in as the **root** user or as a user with sudo privileges.
3. Select the **Red Hat Directory Server** entry.
4. Create a new instance:
   - If no instance exists on the server, click the **Create New Instance** button.
   - If the server already runs existing instances, select **Actions** and click **Create New Instance**.
5. Complete the fields of the **Create New Server Instance** form:
   - **Instance Name**: Sets the name of the instance. Note that you cannot change the name of an instance after it has been created.
   - **Port**: Sets the port number of the LDAP protocol. The port must not be in use by another instance or service. The default port is 389.
   - **Secure Port**: Sets the port number of the LDAPS protocol. The port must not be in use by another instance or service. The default port is 636.
   - **Create Self-Signed TLS Certificate DB**: Enables TLS encryption in the instance, and creates a self-signed certificate.
     For increased security, Red Hat recommends that you create the new instance with the self-signed certificate and TLS enabled. Note that you can replace the self-signed certificate with a certificate issued by a Certificate Authority (CA) at a later date.
   - **Directory Manager DN**: Sets the distinguished name (DN) of the administrative user of the instance. The default value is **cn=Directory Manager**.

- **Directory Manager Password**: Sets the password of the administrative user of the instance.
- **Confirm Password**: Must be set to the same value as in the **Directory Manager Password** field.
- **Create Database**: Select this field to automatically create a suffix during instance creation.



IMPORTANT

If you do not create a suffix during instance creation, you must create it later manually before you can store data in this instance.

If you enabled this option, fill the addition fields:

  - **Database Suffix**: Sets the suffix for the back end.
  - **Database Name**: Sets the name of the back end database.
  - **Database Initialization**: Set this field to **Create Suffix Entry**.

6. Click **Create Instance**.
   The new instance starts and is configured to start automatically when the system boots.
7. Open the required ports in the firewall:

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

8. Reload the firewall configuration:

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

Additional resources

- Enabling TLS-encrypted connections to Directory Server

CHAPTER 4. INSTALLING DIRECTORY SERVER WITH KERBEROS AUTHENTICATION BEHIND A LOAD BALANCER

Installing Directory Server instances that work behind a load balancer and support Kerberos authentication require additional steps compared during the installation.

If a user accesses a service using Generic Security Services API (GSSAPI), the Kerberos principal includes the DNS name of the service's host. In case the user connects to a load balancer, the principal contains the DNS name of the load balancer, for example: **ldap/loadbalancer.example.com@EXAMPLE.COM**, and not the DNS name of the Directory Server instance.

To facilitate successful connection, the Directory Server instance that receives the request must use the same name as the load balancer, even if the load balancer DNS name is different.

This section describes how to set up an Directory Server instance with Kerberos authentication support behind a load balancer.

4.1. PREREQUISITES

- The server meets the requirements of the latest Red Hat Directory Server version as described in the Red Hat Directory Server 12 Release Notes .

4.2. INSTALLING THE DIRECTORY SERVER PACKAGES

Use the following procedure to install the Directory Server packages.

Prerequisites

- You registered the system to the Red Hat subscription management service.
- You have a valid Red Hat Directory Server subscription in your Red Hat account.
- The RHEL default repositories, **BaseOS** and **AppStream**, are enabled.

Procedure

1. List the available subscriptions in your Red Hat account that provide a Red Hat Directory Server subscription, and note the pool ID:

```
# 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. Attach the Red Hat Directory Server subscription to the system using the its pool ID:

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

3. Enable the **dirsrv-12-for-rhel-9-x86_64-rpms** repository:

```
# subscription-manager repos --enable=dirsrv-12-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12-for-rhel-9-x86_64-rpms' is enabled for this system.
```

4. Install the **redhat-ds:12** module:

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

This command automatically installs all required dependencies.

Additional resources

- Using and Configuring Subscription Manager

4.3. CREATING A .INF FILE FOR A DIRECTORY SERVER INSTANCE INSTALLATION

Create a **.inf** file for the **dscreate** utility, and adjust the file to your environment. In a later step, you will use this file to create the new Directory Server instance.

Prerequisites

- You installed the **redhat-ds:12** module.

Procedure

1. Use the **dscreate create-template** command to create a template **.inf** file. For example, to store the template in the **/root/instance_name.inf** file, enter:

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

The created file contains all available parameters including descriptions.

2. Edit the file that you created in the previous step:

   a. Uncomment the parameters that you want to set to customize the installation.
   All parameters have defaults. However, Red Hat recommends that you customize certain parameters for a production environment. For example, set at least the following parameters in the **[slapd]** section:

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

   b. To use the instance behind a load balancer with GSSAPI authentication, set the **full_machine_name** parameter in the **[general]** section to the fully-qualified domain name (FQDN) of the load balancer instead of the FQDN of the Directory Server host:

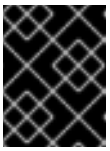
```
full_machine_name = loadbalancer.example.com
```

c. Uncomment the **strict_host_checking** parameter in the **[general]** section and set it to **False**:

```
strict_host_checking = False
```

d. To automatically create a suffix during instance creation, set the following parameters in the **[backend-userroot]** section:

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



IMPORTANT

If you do not create a suffix during instance creation, you must create it later manually before you can store data in this instance.

e. Optional: Uncomment other parameters and set them to appropriate values for your environment. For example, use these parameters to specify different ports for the LDAP and LDAPS protocol.

NOTE

By default, new instances that you create include a self-signed certificate and TLS enabled. For increased security, Red Hat recommends that you do not disable this feature. Note that you can replace the self-signed certificate with a certificate issued by a Certificate Authority (CA) at a later date.

Additional resources

- Enabling TLS-encrypted connections to Directory Server

4.4. USING A .INF FILE TO SET UP A NEW DIRECTORY SERVER INSTANCE

This section describes how to use a **.inf** file to set up a new Directory Server instance using the command line.

Prerequisites

- You created a **.inf** file for the Directory Server instance.

Procedure

1. Pass the **.inf** file to the **dscreate from-file** command to create the new instance:

```
# 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
```

The **dscreate** utility automatically starts the instance and configures RHEL to start the service when the system boots.

2. Open the required ports in the firewall:

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

3. Reload the firewall configuration:

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

4.5. CREATING A KEYTAB FOR THE LOAD BALANCER AND CONFIGURING DIRECTORY SERVER TO USE THE KEYTAB

Before user can authenticate to Directory Server behind a load balancer using GSSAPI, you must create a Kerberos principal for the load balancer and configure Directory Server to use the Kerberos principal. This section describes this procedure.

Prerequisites

- An instance that contains the following **.inf** file configuration:
  - The **full_machine_name** parameter set to the DNS name of the load balancer.
  - The **strict_host_checking** parameter set to **False**.

Procedure

1. Create the Kerberos principal for the load balancer, for example **ldap/*loadbalancer.example.com*_@_*EXAMPLE.COM***. The procedure to create the service principal depends on your Kerberos installation. For details, see your Kerberos server's documentation.

2. Optional: You can add further principals to the keytab file. For example, to enable users to connect to the Directory Server instance behind the load balancer directly using Kerberos authentication, add additional principals for the Directory Server host. For example, **ldap/*server1.example.com*@*EXAMPLE.COM***.

3. Copy the service keytab file to the Directory Server host, and store it, for example, in the **/etc/dirsrv/slapd-*instance_name*/ldap.keytab** file.

4. Add the path to the service keytab to the **/etc/sysconfig/slapd-*instance_name*** file:

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

5. Restart the Directory Server instance:

```
# dsctl instance_name restart
```

Verification

Verification

- Verify that you can connect to the load balancer using the GSSAPI protocol:

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

  If you added additional Kerberos principals to the keytab file, such as for the Directory Server host itself, also verify these connections:

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

CHAPTER 5. RUNNING DIRECTORY SERVER IN FIPS MODE

Directory Server fully supports the Federal Information Processing Standard (FIPS) 140-2. When you run Directory Server run in FIPS mode, security-related settings change. For example, SSL is automatically disabled and only TLS 1.2 and 1.3 encryption is used.

5.1. ENABLING THE FIPS MODE

To use Directory Server in Federal Information Processing Standard (FIPS) mode, enable the mode in RHEL and Directory Server.

Prerequisites

- You enabled the FIPS mode in RHEL.

Procedure

1. Enable the FIPS mode for the network security services (NSS) database:

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

2. Restart the instance:

```
# dsctl instance_name restart
```

Verification

- Verify that FIPS mode is enabled for the NSS database:

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

  The command returns **FIPS mode enabled**, if the module is in FIPS mode.

5.2. ADDITIONAL RESOURCES

- Federal Information Processing Standard (FIPS)
- Switching the system to FIPS mode

CHAPTER 6. UPDATING DIRECTORY SERVER TO A NEW MINOR VERSION

Red Hat frequently releases updated versions of Red Hat Directory Server 12. This section describes how to update the Directory Server packages.

If you instead want to migrate Red Hat Directory Server 11 to version 12, see Migrating Directory Server 11 to Directory Server 12.

6.1. UPDATING THE DIRECTORY SERVER PACKAGES

You can use the **dnf** utility to update the module, which also automatically updates the related packages.

Prerequisites

- Red Hat Directory Server 12 is installed on the server.
- The system to update is registered to the Red Hat subscription management service.
- A valid Red Hat Directory Server subscription is attached to the server.

Procedure

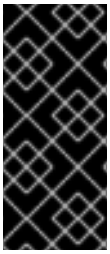
- Use the **dnf module update redhat-ds** command to check for new updates of Directory Server packages and their dependencies, and to install them:

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

  The update process automatically restarts the **dirsrv** services for all instances on the server.

CHAPTER 7. MIGRATING DIRECTORY SERVER 11 TO DIRECTORY SERVER 12

This chapter contains information about migrating from Red Hat Directory Server 11 to 12, including tasks that you must perform before the migration begins.



IMPORTANT

Red Hat supports only migrations from Red Hat Directory Server 11 to 12.

To migrate Directory Server 7, 8, 9, and 10 to version 12, you must first migrate the installation to Directory Server 11. For details, see the Migrating Directory Server 10 to Directory Server 11 chapter in the **Red Hat Directory Server 11 Installation Guide**.

7.1. PREREQUISITES

- The existing Directory Server installation runs on version 11 and has all available updates installed.

7.2. MIGRATING TO DIRECTORY SERVER 12 USING THE REPLICATION METHOD

In a replication topology, use the replication method to migrate to Directory Server 12.

Procedure

1. Install Directory Server 12.
2. On the Directory Server 12 host, enable replication, but do not create a replication agreement. For details about enabling replication, see the Configuring and managing replication documentation for Red Hat Directory Server 12.
3. On the Directory Server 11 host, enable replication and create a replication agreement that points to the Directory Server 12 host. For more information, see the Multi-Supplier Replication section in the **Red Hat Directory Server 11 Administrator Guide**.
4. Optional: Set up further Directory Server 12 hosts with replication agreements between the Directory Server 12 hosts.
5. Configure your clients to use only the Directory Server 12 hosts.
6. Remove the replication agreements with Directory Server 11 hosts. See Removing a Directory Server Instance from the Replication Topology in the **Red Hat Directory Server 11 Administrator Guide**.
7. Uninstall the Directory Server 11 hosts. See Uninstalling Directory Server in the **Red Hat Directory Server 11 Installation Guide**.

7.3. MIGRATING TO DIRECTORY SERVER 12 USING THE EXPORT AND IMPORT METHOD

Use the export and import method to migrate small Directory Server environments, such as instances without replication.

Procedure

1. Perform the following steps on the existing Directory Server 11 host:
   a. Stop and disable the **dirsrv** service:

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

   b. Export the back end. For example, to export the **userRoot** back end and store it in the **/tmp/userRoot.ldif** file:

```
# dsctl instance_name db2ldif userroot /tmp/userRoot.ldif
```

   c. Copy the following files to the new host where you want to install Directory Server 12:
      - The LDIF file that you exported in the previous step.
      - **/etc/dirsrv/slapd-instance_name/schema/99user.ldif**, if you use a custom schema
      - If you want to migrate an instance with TLS enabled and reuse the same host name for the Directory Server 12 installation, copy the following files to the new host:
        - **/etc/dirsrv/slapd-instance_name/cert9.db**
        - **/etc/dirsrv/slapd-instance_name/key4.db**
        - **/etc/dirsrv/slapd-instance_name/pin.txt**

   d. If you want to reuse the same host name and IP on the Directory Server 12 host, disconnect the old server from the network.

2. Perform the following steps on the new host:
   a. Install Directory Server 12.
   b. Optional: Configure TLS encryption:
      - If the new installation uses a different host name than the Directory Server 11 instance, see the Enabling TLS-encrypted connections to Directory Server section in the **Securing Red Hat Directory Server** documentation.
      - To use the same host name as the previous Directory Server 11 installation:
        i. Stop the instance:

```
# dsctl instance_name stop
```

        ii. Remove the Network Security Services (NSS) databases and the password file for Directory Server, if they already exist:

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

        iii. Store the **cert9.db**, **key4.db**, and **pin.txt** files that you copied from the Directory Server 11 host in the **/etc/dirsrv/slapd-*instance_name*/** directory.

iv. Set the correct permissions for the NSS databases and the password file:

```
# 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. Start the instance:

```
# dsctl instance_name start
```

c. If you used a custom schema, restore the **99user.ldif** file into the **/etc/dirsrv/slapd-*instance_name*/schema/** directory, set appropriate permissions, and restart the instance:

```
# 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. Import the LDIF file. For example, to import the ***/var/lib/dirsrv/slapd-*instance_name*/ldif/migration.ldif*** file into the **userRoot** database:

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

Note that Directory Server requires the LDIF file you want to import in the **/var/lib/dirsrv/slapd-*instance_name*/** directory.

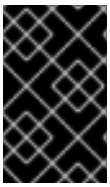
CHAPTER 8. INSTALLING, UPDATING, AND UNINSTALLING THE PASSWORD SYNCHRONIZATION SERVICE

To synchronize passwords between Active Directory and Red Hat Directory Server, you use the password password synchronization service. You can install, update, and remove the password synchronization service.

8.1. THE PASSWORD SYNCHRONIZATION SERVICE

When you set up password synchronization with Active Directory, Directory Server retrieves all attributes of user objects except the password. Active Directory stores only encrypted passwords, but Directory Server uses different encryption. As a result, Active Directory users passwords must be encrypted by Directory Server.

To enable password synchronization between Active Directory and Directory Server, the **Red Hat Directory Password Sync** service hooks up into the Windows password changing routine of a domain controller (DC). If a user or administrator sets or updates a password, the service retrieves the password in plain text before it is encrypted and stored in Active Directory. This process enables **Red Hat Directory Password Sync** to send the plain text password to Directory Server. To protect the password, the service supports only LDAPS connections to Directory Server. When Directory Server stores the password in the user's entry, the password is automatically encrypted with the password storage scheme configured in Directory Server.



IMPORTANT

In an Active Directory, all writable DCs can process password actions. Therefore, you must install **Red Hat Directory Password Sync** on every writable DC in the Active Directory domain.

8.2. DOWNLOADING THE PASSWORD SYNCHRONIZATION SERVICE INSTALLER

To install **Red Hat Directory Password Sync** service, download the installer from the Customer Portal.

Prerequisites

- You have a valid Red Hat Directory Server subscription.
- You have an account on the Red Hat Customer Portal.

Procedure

1. Log into the Red Hat Customer Portal.
2. Click **Downloads** at the top of the page.
3. Select **Red Hat Directory Server** from the product list.
4. Select **12** in the **Version** field.
5. Download **PassSync Installer**.
6. Copy the installer to every writable Active Directory domain controller (DC).

8.3. INSTALLING THE PASSWORD SYNCHRONIZATION SERVICE

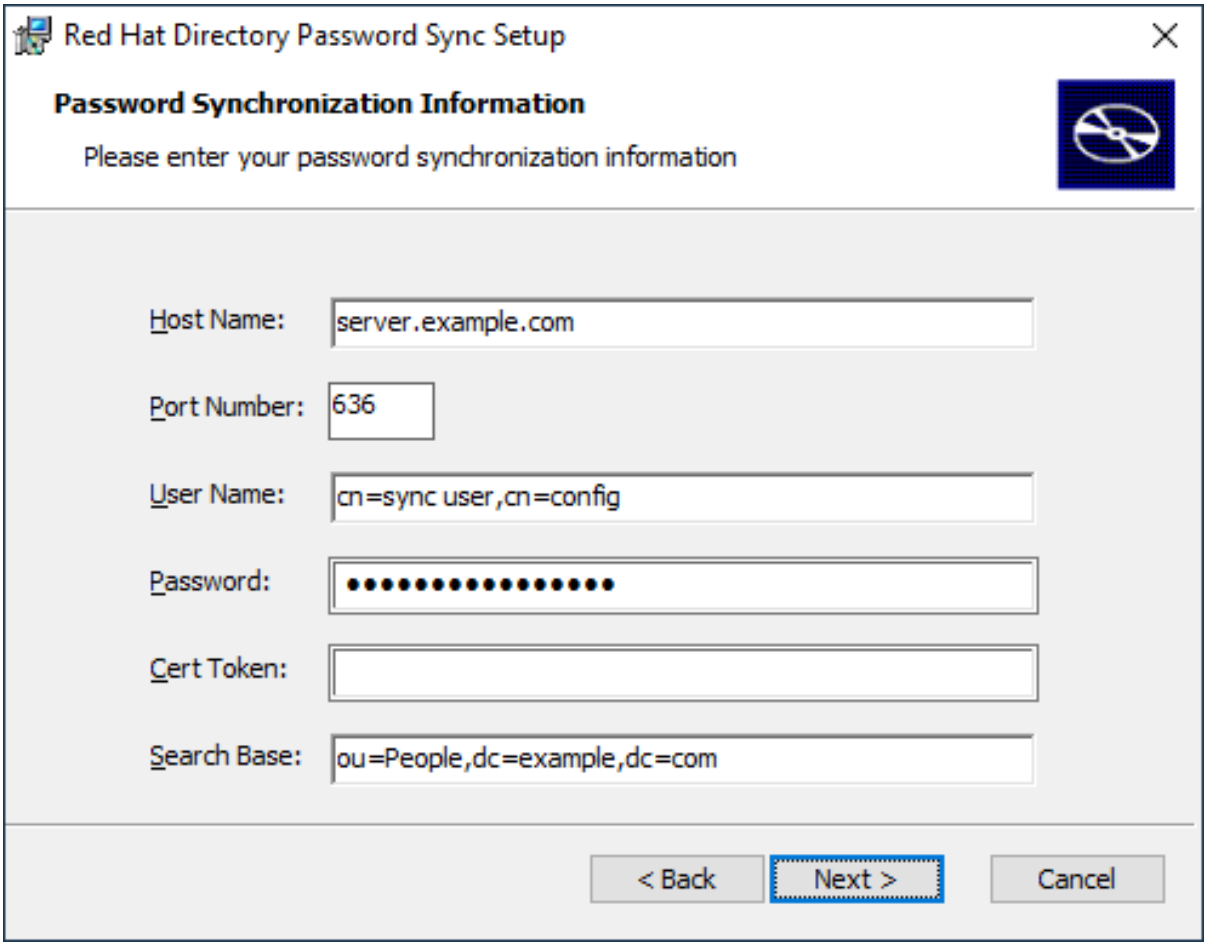
This section describes how to install the **Red Hat Directory Password Sync** on Windows domain controllers (DC). Perform this procedure on every writable Windows DC.

Prerequisites

- You downloaded the latest version of the **PassSync Installer** to the Windows Active Directory domain controller (DC).
- You enabled TLS encryption in Directory Server.
- You prepared the Active Directory domain.
- You created an account for synchronization in Directory Server.

Procedure

1. Log in to the Active Directory DC with a user that has permissions to install software on the DC.
2. Double-click the **RedHat-PassSync-ds12.*-x86_64.msi** file to install it.
3. The **Red Hat Directory Password Sync Setup** appears. Click **Next**.
4. Fill the fields according to your Directory Server environment. For example:



Fill the following information of the Directory Server host into the fields:

- **Host Name**: Sets the name of the Directory Server host. Alternatively, you can set the field to the IPv4 or IPv6 address of the Directory Server host.

- **Port Number**: Sets the LDAPS port number.
- **User Name**: Sets the distinguished name (DN) of the synchronization user account.
- **Password**: Sets the password of the synchronization user.
- **Cert Token**: Sets the password of the server certificate copied from the Directory Server host.
- **Search Base**: Sets the DN of the Directory Server entry that contains the synchronized user accounts.

5. Click **Next** to start the installation.
6. Click **Finish**.
7. Reboot the Windows DC.

IMPORTANT

Without rebooting the DC, the **PasswordHook.dll** library is not enabled and password synchronization fails.

8. Enable replication in Directory Server and create a WinSync agreement.

Additional resources

- Enabling TLS-encrypted connections to Directory Server

8.4. UPDATING THE PASSWORD SYNCHRONIZATION SERVICE

This section describes how to update an existing **Red Hat Directory Password Sync** installation on a Windows domain controller (DC).

Perform this procedure on every writable Windows DC.

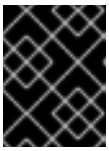
Prerequisites

- **Red Hat Directory Password Sync** is running on your Windows DC.
- You downloaded the latest version of the **PassSync Installer** to the Windows Active Directory DC.

Procedure

1. Log in to the Active Directory domain controller with a user that has permissions to install software on the DC.
2. Double-click the **RedHat-PassSync-ds12.*-x86_64.msi** file.
3. Click **Next** to begin installing.
4. Click the **Modify** button.

5. The setup displays the configuration set during the previous installation. Click **Next** to keep the existing settings.
6. Click **Next** to start the installation.
7. Click **Finish**.
8. Reboot the Windows DC.



IMPORTANT

Without rebooting the DC, the **PasswordHook.dll** library is not enabled and password synchronization will fail.

8.5. UNINSTALLING THE PASSWORD SYNCHRONIZATION SERVICE

If you no longer require the **Red Hat Directory Password Sync** service, remove it from the Active Directory domain controller (DC).

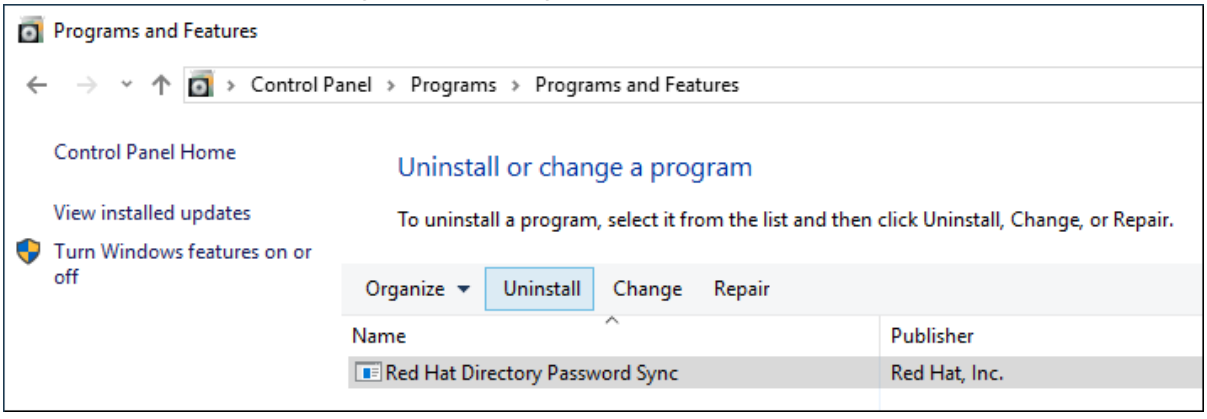
Prerequisites

- **Red Hat Directory Password Sync** is installed on the Windows DC.

Procedure

Log in to the Active Directory domain controller with a user that has permissions to remove software from the DC.

1. Open the **Control Panel**
2. Click **Programs** and then **Programs and Features**
3. Select the **Red Hat Directory Password Sync** entry, and click the **Uninstall** button.



4. Click **Yes** to confirm.

CHAPTER 9. REMOVING A DIRECTORY SERVER INSTANCE

If you no longer require a Directory Server instance, you can remove it to regain disk space. If you run multiple instances on one server, removing a specific instance does not affect the other instances.

9.1. REMOVING AN INSTANCE USING THE COMMAND LINE

You can remove a Directory Server instance using the command line.

Prerequisites

- The instance has been removed from a replication topology, if it was part of one.

Procedure

1. Optional: Create a backup of the Directory Server directories:
   a. Stop the instance:

   ```
   # dsctl instance_name stop
   ```

   b. Copy the **/var/lib/dirsrv/slapd-*instance_name*/** directory:

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

   This directory contains the database, as well as the backup and export directory.

   c. Copy the **/etc/dirsrv/slapd-*instance_name*/** directory:

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

2. Remove the instance:

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

Verification

- Verify that the **/var/lib/dirsrv/slapd-*instance_name*/** and **/etc/dirsrv/slapd-*instance_name*/** directories have been removed:

  ```
  # 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
  ```

Additional resources

- Removing an instance from a replication topology

9.2. REMOVING AN INSTANCE USING THE WEB CONSOLE

You can remove a Directory Server instance using the web console. However, if you want to create a backup of the Directory Server directories which contain, for example, the databases and configuration files, you must copy these directories on the command line.

Prerequisites

- The instance has been removed from a replication topology, if it was part of one.
- You are logged in to the instance in the web console.

Procedure

1. Optional: Create a backup of the Directory Server directories.
   a. Click the **Actions** button, and select **Stop instance**.
   b. Copy the **/var/lib/dirsrv/slapd-*instance_name*/** directory:

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

      This directory contains the database, as well as the backup and export directory.
   c. Copy the **/etc/dirsrv/slapd-*instance_name*/** directory:

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

2. Click the **Actions** button, and select **Remove this instance**.
3. Select **Yes, I am sure**, and click **Remove Instance** to confirm.

Verification

- Verify that the **/var/lib/dirsrv/slapd-*instance_name*/** and **/etc/dirsrv/slapd-*instance_name*/** directories have been removed:

  ```
  # 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
  ```

Additional resources

- Removing an instance from a replication topology

CHAPTER 10. UNINSTALLING DIRECTORY SERVER

If you no longer need a Directory Server instance, you can uninstall it to reclaim space.

10.1. UNINSTALLING DIRECTORY SERVER

If you no longer require Directory Server running on a server, uninstall the packages as described in this section.

Procedure

1. Remove all instances from the replication topology. If your instance is not a member of a replication topology skip this step.
2. Remove all instances from the server. For each instance, enter:

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

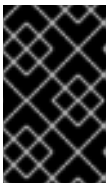
3. Remove the Directory Server packages:

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

4. Optional: Disable the **dirsrv-12-for-rhel-8-x86_64-rpms** repository:

```
# 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. Optional: Remove the Red Hat Directory Server subscription from the system:



IMPORTANT

If you remove a subscription that provides additional products than Directory Server, you will not be able to install or update packages for these products.

- List the subscriptions attached to the host:

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

- Remove the subscription using the pool id from the previous step:

```
# 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
```

Additional resources

- Removing an instance from a replication topology

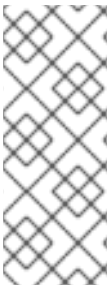
CHAPTER 11. CREATING TEST ENTRIES

The **dsctl ldifgen** command creates LDIF files with different types of test entries. For example, you can use this LDIF file to populate a test instance or a sub-tree to test the performance of Directory Server with the example entries.

11.1. OVERVIEW OF TESTING ENTRIES YOU CAN CREATE

You can pass one of the following entry type arguments to **dsctl ldifgen**:

- **users**: Creates an LDIF file that contains user entries.
- **groups**: Creates an LDIF file that contains static group and member entries.
- **cos-def**: Creates an LDIF file that either contains a classic pointer or an indirect Class of Service (CoS) definition.
- **cos-template**: Creates an LDIF file that contains a CoS template.
- **roles**: Creates an LDIF file that contains managed, filtered, or indirect role entries.
- **mod-load**: Creates an LDIF file that contains modify operations. Use the **ldapmodify** utility to load the file into the directory.
- **nested**: Creates an LDIF file that contains heavily nested entries in a cascading or fractal tree design.



NOTE

The **dsctl ldifgen** command creates only the LDIF file. To load the file into your Directory Server instance, use the:

- **ldapmodify** utility after you created an LDIF file using the **mod-load** option
- **ldapadd** utility for all other options

Except for the nested entry type, if you do not provide any command line options, the **dsctl ldifgen** command uses an interactive mode:

```
# dsctl instance_name ldifgen entry_type
```

11.2. CREATING AN LDIF FILE WITH EXAMPLE USER ENTRIES

Use the **dsctl ldifgen users** command to create an LDIF file with example user entries.

Procedure

1. For example, to create an LDIF file named **/tmp/users.ldif** that adds 100,000 generic users to the **dc=example,dc=com** suffix, enter:

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

Note that the command creates the following organizational units (OU) and randomly assigns the users to these OUs:

- **ou=accounting**
- **ou=product development**
- **ou=product testing**
- **ou=human resources**
- **ou=payroll**
- **ou=people**
- **ou=groups**
  For further details and other options you can use to create the LDIF file, enter:

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

2. Optional: Add the test entries to the directory:

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

11.3. CREATING AN LDIF FILE WITH EXAMPLE GROUP ENTRIES

Use the **dsctl ldifgen groups** command to create an LDIF file with example user entries.

Procedure

1. For example, to create an LDIF file named **/tmp/groups.ldif** that adds 500 groups to the **ou=groups,dc=example,dc=com** entry, and each group has 100 members, enter:

   ```
   # 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__
   ```

   Note that the command also creates LDIF statements to add the user entries in **ou=People,dc=example,dc=com**.

   For further details and other options you can use to create the LDIF file, enter:

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

2. Optional: Add the test entries to the directory:

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

11.4. CREATING AN LDIF FILE WITH AN EXAMPLE COS DEFINITION

Use the **dsctl ldifgen cos-def** command to create an LDIF file with a Class of Service (CoS) definition.

Procedure

1. For example, to create an LDIF file named **/tmp/cos-definition.ldif** that adds a classic CoS definition to the **ou=cos-definitions,dc=example,dc=com** entry, enter:

```
# 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
```

   For further details and other options you can use to create the LDIF file, enter:

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

2. Optional: Add the test entries to the directory:

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

11.5. CREATING AN LDIF FILE WITH EXAMPLE MODIFICATION STATEMENTS

Use the **dsctl ldifgen mod-load** command to create an LDIF file that contains update operations.

Procedure

1. For example, to create an LDIF file named **/tmp/modifications.ldif**:

```
# 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
```

   This command creates a file named **/tmp/modifications.ldif** file with the statements that do the following:

   - Create an LDIF file with 1000 **ADD** operations to create user entries in **ou=People,dc=example,dc=com**.
   - Modify all entries by changing their **sn** attributes.
   - Add additional 10 user entries.
   - Perform 100 **MODRDN** operations.
   - Delete 100 entries
   - Delete all remaining entries at the end
     For further details and other options you can use to create the LDIF file, enter:

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

2. Optional: Add the test entries to the directory:

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

11.6. CREATING AN LDIF FILE WITH NESTED EXAMPLE ENTRIES

Use the **dsctl ldifgen nested** command to create an LDIF file that contains a heavily nested cascading fractal structure.

Procedure

1. For example, to create an LDIF file named **/tmp/nested.ldif** that adds 600 users in total in different organizational units (OU) under the **dc=example,dc=com** entry, with each OU containing a maximum number of 100 users, enter:

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

   For further details and other options you can use to create the LDIF file, enter:

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

2. Optional: Add the test entries to the directory:

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