Red Hat Directory Server 11

Installation Guide

Instructions for installing Red Hat Directory Server 11.0

Last Updated: 2020-03-02

Red Hat Directory Server 11 Installation Guide

Instructions for installing Red Hat Directory Server 11.0

Marc Muehlfeld
Red Hat Customer Content Services
mmuehlfeld@redhat.com

Legal Notice

Copyright © 2020 Red Hat, Inc.

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.

Abstract

This guide contains information about installing, updating, and uninstalling Red Hat Directory Server 11.0 and associated services.

Table of Contents

PREFACE

This guide contains information about installing, updating, and uninstalling Red Hat Directory Server and the Password Synchronization service. Additionally, this guide includes information about migrating Directory Server 10 to Directory Server 11.

To familiarize yourself with the concepts of a directory service and planning a Directory Server installation, see the Red Hat Directory Server Deployment Guide.

For details about managing and configuring a Directory Server instance after the installation, see the Red Hat Directory Server Administration Guide.

CHAPTER 1. INSTALLING THE DIRECTORY SERVER PACKAGES

This chapter contains information about installing the Red Hat Directory Server packages.

Prerequisites

- Red Hat Enterprise Linux (RHEL) is installed on the server.
  For details about the RHEL version required by the Red Hat Directory Server version you want to install, see the Red Hat Directory Server 11 Release Notes .
- The system Directory Server is registered to the Red Hat subscription management service.
  For details about using **Subscription Manager**,see the corresponding section in the Using and Configuring Subscription Manager guide.
- A valid Red Hat Directory Server subscription is available in your Red Hat account.

1.1. INSTALLING THE DIRECTORY SERVER PACKAGES

Use the following procedure to install the Directory Server packages.

Procedure

1. List the available subscriptions in your Red Hat account and identify the pool ID that provides Red Hat Directory Server. For example:

```
# subscription-manager list --available --all
...
Subscription Name:   Red Hat Enterprise Linux Developer Suite
Provides:            ...
                     Red Hat Directory Server
                     ...
Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
Available:           1
...
```

2. Attach the Red Hat Directory Server subscription to the system using the pool ID from the previous step:

```
# subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
Successfully attached a subscription for: Red Hat Enterprise Linux Developer Suite
```

3. Enable the **dirsrv-11-for-rhel-8-x86_64-rpms** repository:

```
# 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. Install the **redhat-ds:11** module:

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

   This command automatically installs all required dependencies.

Additional resources

- For details about installing Red Hat Enterprise Linux and registering the system to the subscription management service, see Red Hat Enterprise Linux Installation Guide.
- For further details about using the **subscription-manager** utility, see the Using and Configuring Subscription Manager guide.
- For details about enabling repositories, see the Managing Basic Software-Installation Tasks with Subscription Manager and Yum section in the Red Hat Enterprise Linux System Administrator's Guide.

CHAPTER 2. SETTING UP A NEW DIRECTORY SERVER INSTANCE

Directory Server supports creating a new instance:

- Using a **.inf** file on the command line
- Using the interactive command line installer
- Using the Web Console

Prerequisites

- The server meets the hardware and software requirements for the latest Red Hat Directory Server version as described in the Red Hat Directory Server Release Notes .
- The Directory Server server packages are installed as described in Chapter 1, *Installing the Directory Server packages*.
- The server's fully-qualified domain name (FQDN) can be resolved using DNS.

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

Using the command line to set up a new instance enables administrators to customize additional settings during the instance creation.

This section describes:

- Creating and customizing the **.inf** file
- Using the **.inf** file with the **dscreate** utility to set up the new instance
- Opening the required ports in the firewall

If you want to set only the frequently used configuration parameters during the installation, you can use the interactive installer. For details, see Section 2.2, "Setting up a new instance on the command line using the interactive installer".

2.1.1. Creating a .inf file for a Directory Server instance installation

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

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:

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

   The created file contains all available parameters with descriptions

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

a. Uncomment the parameters that you want to set to customize the installation.

NOTE

All parameters have defaults. However, Red Hat recommends to customize certain parameters for a production environment.

For example, set at least the following parameters:

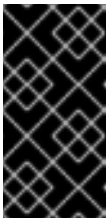
```
[slapd]
# instance_name (str)
# Description: ...
# Default value: localhost
instance_name = instance_name

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

The template file that you create with the **dscreate create-template** command contains the comprehensive list of parameters you can configure in these sections.

b. To automatically create a suffix during instance creation, uncomment the **suffix** parameter in the **[backend-userroot]** section. For example:

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



IMPORTANT

Instead of creating the suffix during instance creation, you can create it later as described in Creating Databases in the Red Hat Directory Server Administration Guide. However, without creating a suffix, you cannot store data in this instance.

c. Optionally, 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

- For a full list of parameters that you can set in the **.inf** file and descriptions of each parameter, see the template file that the **dscreate create-template** command creates.

- For details about installing a certificate after the installation, see the Managing the NSS Database Used by Directory Server section in the Red Hat Directory Server Administration Guide.

2.1.2. 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

- A **.inf** file for the Directory Server instance created as described in Section 2.1.1, "Creating a **.inf** file for a Directory Server instance installation".

Procedure

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

```
# dscreate from-file /root/instance_name.inf
Starting installation...
Created symlink /etc/systemd/system/multi-user.target.wants/dirsrv@instance_name.service
→ /usr/lib/systemd/system/dirsrv@.service.
Completed installation for instance_name
```

   The created instance is automatically started and configured to start when the system boots.

2. Open the required ports in the firewall. See Section 2.1.3, "Opening required ports in the firewall"

2.1.3. Opening required ports in the firewall

To allow other machines to connect to Directory Server over the network, open the required ports in the local firewall.

If no ports were specified during the instance creation, the instance uses port **389** for the LDAP and port **636** for the LDAPS protocol.

Prerequisites

- The port numbers for the LDAP and LDAPS protocols set during the instance creation.

Procedure

1. Ensure that the **firewalld** service is running.
   - To find out if **firewalld** is currently running:

```
# 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
   ...
```

   - To start **firewalld** and configure the service to start automatically when the system boots:

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

2. Open the required ports using the **firewall-cmd** utility. For example, to open the LDAP and LDAPS default ports in the default firewall zone:

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

3. Reload the firewall configuration to ensure that the change occurs immediately:

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

Additional resources

- For details on using **firewall-cmd** to open ports on a system, see the Red Hat Enterprise Linux Security Guide or the **firewall-cmd(1)** man page.

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

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

For a list of settings supported by the interactive installer, see Section 2.2.1, "Settings supported in the interactive installer"

This section describes:

- The list of settings supported by the interactive installer
- Staring the interactive installer
- Opening the required ports in the firewall

If you want to customize additional settings during the installation, use a **.inf** file instead of the interactive installer. For details, see Section 2.1, "Setting up a new instance on the command line using a **.inf** file".

2.2.1. Settings supported in the interactive installer

If you use the interactive installer, you can set the following settings:

- Host name of the system
- Enabling or disabling strict host name validation
- Name of the instance
- LDAP port number
- LDAPS port number
- Auto-creation of a self-signed certificate
- DN of the directory manager account

- Password of the directory manager account
- Optional creation of a database suffix

2.2.2. Creating an instance using the interactive installer

To start the interactive installer to set up a new instance, enter:

```
# dscreate interactive
```

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

Example 2.1. Using the interactive installer

```
# dscreate interactive

Install Directory Server (interactive mode)
===========================================

Enter system's hostname [server.example.com]:

Use strict hostname verification (set to "no" if using GSSAPI behind a load balancer) [yes]:

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 Directory Manager password: password
Confirm 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]: yes

Are you ready to install? [no]: yes

Starting installation...
Created symlink /etc/systemd/system/multi-user.target.wants/dirsrv@server-rhel8.service →
/usr/lib/systemd/system/dirsrv@.service.
Completed installation for instance_name
```

NOTE

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

2.2.3. Opening required ports in the firewall

To allow other machines to connect to Directory Server over the network, open the required ports in the local firewall.

If no ports were specified during the instance creation, the instance uses port **389** for the LDAP and port **636** for the LDAPS protocol.

Prerequisites

- The port numbers for the LDAP and LDAPS protocols set during the instance creation.

Procedure

1. Ensure that the **firewalld** service is running.
   - To find out if **firewalld** is currently running:

```
# 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
   ...
```

   - To start **firewalld** and configure the service to start automatically when the system boots:

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

2. Open the required ports using the **firewall-cmd** utility. For example, to open the LDAP and LDAPS default ports in the default firewall zone:

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

3. Reload the firewall configuration to ensure that the change occurs immediately:

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

Additional resources

- For details on using **firewall-cmd** to open ports on a system, see the Red Hat Enterprise Linux Security Guide or the **firewall-cmd(1)** man page.

2.3. SETTING UP A NEW INSTANCE USING THE WEB CONSOLE

Administrators can use the web console to create a new instance using a browser-based interface.

This section describes:

- Using the web console to create the new instance
- Opening the required ports in the firewall

2.3.1. 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

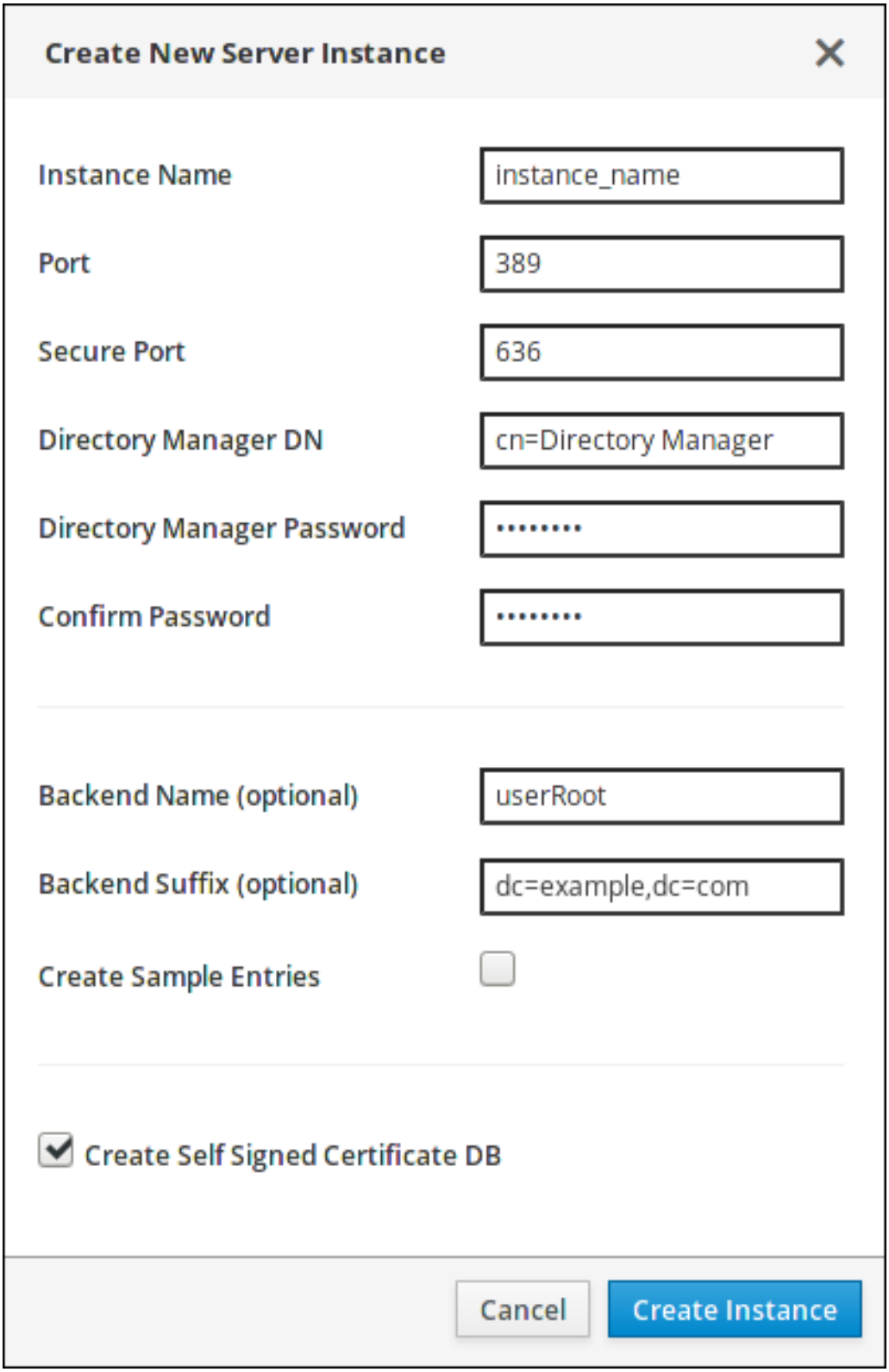
- The web console is installed on the server, and port 9090 is opened in the local firewall. For details, see the Installing the web console section in the **Managing systems using the RHEL 8 web console** guide.

Procedure

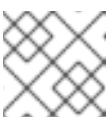
1. Use a browser to connect to the web console running on port 9090 on the Directory Server host. For example:

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

2. Log in as the **root** user or as a user with sudo privileges.
3. Select the **389 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 Instance**.
5. Complete the fields of the **Create New Server Instance** form:



- **Instance Name**: Sets the name of the instance.



NOTE

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.
- **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**: Set's 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.
- **Backend Name**: Sets the name of the back end database. Filling this field is required if you specify a back end suffix.
- **Backend Suffix**: Sets the suffix for the back end. The default value is **cn=example,dc=com**.
- Optionally, select **Create Sample Entries** to create some example organizational units, users, and groups in the suffix.

6. Optionally, select **Create Self Signed Certificate DB** to automatically enable TLS encryption in the new instance with a self-signed certificate.

IMPORTANT

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.

7. Click **Create Instance**.
   The new instance starts and is configured to start automatically when the system boots.
8. Open the required ports in the firewall. See Section 2.3.2, "Opening required ports in the firewall"

Additional resources

- For further details about the web console, see the Managing systems using the RHEL 8 web console guide.
- For details about installing a certificate after the installation, see the Managing the NSS Database Used by Directory Server section in the Red Hat Directory Server Administration Guide.

2.3.2. Opening required ports in the firewall

To allow other machines to connect to Directory Server over the network, open the required ports in the local firewall.

If no ports were specified during the instance creation, the instance uses port **389** for the LDAP and port **636** for the LDAPS protocol.

Prerequisites

- The port numbers for the LDAP and LDAPS protocols set during the instance creation.

Procedure

1. Ensure that the **firewalld** service is running.
   - To find out if **firewalld** is currently running:

     ```
     # 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
       ...
     ```

   - To start **firewalld** and configure the service to start automatically when the system boots:

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

2. Open the required ports using the **firewall-cmd** utility. For example, to open the LDAP and LDAPS default ports in the default firewall zone:

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

3. Reload the firewall configuration to ensure that the change occurs immediately:

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

Additional resources

- For details on using **firewall-cmd** to open ports on a system, see the Red Hat Enterprise Linux Security Guide or the **firewall-cmd(1)** man page.

CHAPTER 3. INSTALLING DIRECTORY SERVER WITH KERBEROS AUTHENTICATION BEHIND A LOAD BALANCER

To provide high availability, install two Directory Server instances behind a load balancer. Users must be able to authenticate with Kerberos.

NOTE

Setting up this scenario is supporting only using the command line.

Setting up this scenario contains the following steps:

- Create a **.inf** file for the instance creation
- Use the **.inf** file with the **dscreate** utility to set up the new instance
- Open the required ports in the firewall
- Create a keytab for the load balancer and configure Directory Server to use the keytab

Prerequisites

- The server meets the hardware and software requirements for the latest Red Hat Directory Server version as described in the Red Hat Directory Server Release Notes .
- The Directory Server server packages are installed as described in Chapter 1, *Installing the Directory Server packages*.

3.1. UNDERSTANDING THE DIFFERENCES WHEN SETTING UP AN INSTANCE WITH KERBEROS BEHIND A LOAD BALANCER

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 and not the DNS name from Directory Server. For example: **ldap/loadbalancer.example.com@EXAMPLE.COM**.

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.

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

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

Procedure

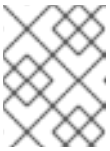
1. Use the **dscreate create-template** command to create a template **.inf** file. For example, to store the template in the **/root/instance_name.inf** file:

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

The created file contains all available parameters with descriptions

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

   a. Uncomment the parameters that you want to set to customize the installation.

   NOTE

   All parameters have defaults. However, Red Hat recommends to customize certain parameters for a production environment.

   For example, set at least the following parameters:

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

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

   The template file that you create with the **dscreate create-template** command contains the comprehensive list of parameters you can configure in these sections.

   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:

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

   For details, see Section 3.1, “Understanding the differences when setting up an instance with Kerberos behind a load balancer”.

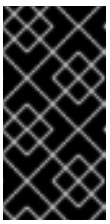
   c. Uncomment the **strict_host_checking** parameter in the **[general]** section and set it to **False**:

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

   d. To automatically create a suffix during instance creation, uncomment the **suffix** parameter in the **[backend-userroot]** section. For example:

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

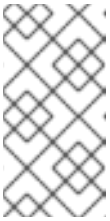
```
suffix = dc=example,dc=com
```



IMPORTANT

Instead of creating the suffix during instance creation, you can create it later as described in Creating Databases in the Red Hat Directory Server Administration Guide. However, without creating a suffix, you cannot store data in this instance.

e. Optionally, 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

- For a full list of parameters that you can set in the **.inf** file and descriptions of each parameter, see the template file that the **dscreate create-template** command creates.
- For details about installing a certificate after the installation, see the Managing the NSS Database Used by Directory Server section in the Red Hat Directory Server Administration Guide.

3.3. 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

- A **.inf** file for the Directory Server instance created as described in Section 3.2, "Creating a **.inf** file for a Directory Server instance installation".

Procedure

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

```
# dscreate from-file /root/instance_name.inf
Starting installation...
Created symlink /etc/systemd/system/multi-user.target.wants/dirsrv@instance_name.service
→ /usr/lib/systemd/system/dirsrv@.service.
Completed installation for instance_name
```

   The created instance is automatically started and configured to start when the system boots.

2. Open the required ports in the firewall. See Section 3.4, "Opening required ports in the firewall"

3.4. OPENING REQUIRED PORTS IN THE FIREWALL

To allow other machines to connect to Directory Server over the network, open the required ports in the local firewall.

If no ports were specified during the instance creation, the instance uses port **389** for the LDAP and port **636** for the LDAPS protocol.

Prerequisites

- The port numbers for the LDAP and LDAPS protocols set during the instance creation.

Procedure

1. Ensure that the **firewalld** service is running.
   - To find out if **firewalld** is currently running:

     ```
     # 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
       ...
     ```

   - To start **firewalld** and configure the service to start automatically when the system boots:

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

2. Open the required ports using the **firewall-cmd** utility. For example, to open the LDAP and LDAPS default ports in the default firewall zone:

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

3. Reload the firewall configuration to ensure that the change occurs immediately:

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

Additional resources

- For details on using **firewall-cmd** to open ports on a system, see the Red Hat Enterprise Linux Security Guide or the **firewall-cmd(1)** man page.

3.5. 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***
2. Optionally, 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***.
   The procedure to create the service principal depends on your Kerberos installation. For details, see your Kerberos server's documentation.
3. Copy the service keytab file to the Directory Server. For example, store it 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:

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

6. Verify that you can connect to the load balancer using the GSSAPI protocol. For example:

   ```
   # 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, you must also verify these connections. For example:

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

CHAPTER 4. UPDATING DIRECTORY SERVER

Red Hat frequently releases updated versions of Red Hat Directory Server 11. This section describes how to update the Directory Server packages.

If you instead want to migrate Red Hat Directory Server 10 to version 11, see Chapter 5, *Migrating Directory Server 10 to Directory Server 11*.

Prerequisites

- Red Hat Directory Server 11 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.

4.1. UPDATING THE DIRECTORY SERVER PACKAGES

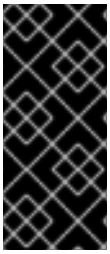
Use the **yum module update redhat-ds** command to check for new updates of Directory Server packages and their dependencies, and to install them:

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

During the update, the **dirsrv** service restartes automatically for all instances on the server.

CHAPTER 5. MIGRATING DIRECTORY SERVER 10 TO DIRECTORY SERVER 11

This chapter contains information about migrating from Red Hat Directory Server 10 to 11, including tasks that you must perform before the migration begins.



IMPORTANT

Red Hat supports only migrations from Red Hat Directory Server 10 to 11.

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

Prerequisites

- The existing Directory Server installation runs on version 10 and has all available updates installed.

5.1. MIGRATING TO DIRECTORY SERVER 11 USING THE REPLICATION METHOD

In a replication topology, use the replication method to migrate to Directory Server 11.

Procedure

1. Install Directory Server 11. See Chapter 2, *Setting up a new Directory Server instance* .
2. Optionally, configure TLS. See the Enabling TLS chapter in the *Red Hat Directory Server 11 Administrator Guide*.
3. Enable replication on a Directory Server 10 host. For more information, see the Configuring the Read-Write Replicas on the Supplier Servers section in the *Red Hat Directory Server 10 Administrator Guide*.
4. Set up the replication agreement on the Directory Server 11 host. See the Multi-Master Replication section in the *Red Hat Directory Server 11 Administrator Guide* .
5. Optionally, set up further Directory Server 11 hosts with replication agreements between the Directory Server 11 hosts.
6. Configure your clients to use only the Directory Server 11 hosts.
7. Remove the replication agreements with Directory Server 10 hosts. See Removing a Directory Server Instance from the Replication Topology in the *Red Hat Directory Server 11 Administrator Guide*.
8. Uninstall the Directory Server 10 hosts. See Uninstalling Directory Server in the *Red Hat Directory Server 10 Installation Guide*.

5.2. MIGRATING TO DIRECTORY SERVER 11 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. On the existing Directory Server 10 host:
   a. Stop and disable the **dirsrv** service:

```
# systemctl stop dirsrv@instance_name
# 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:

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

   c. Copy the following files to the new host where you want to install Directory Server 11:
      - 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 11 installation, copy the following files to the new host:
        - **/etc/dirsrv/slapd-instance_name/cert8.db**
        - **/etc/dirsrv/slapd-instance_name/key3.db**
        - **/etc/dirsrv/slapd-instance_name/pin.txt**

   d. If you want to reuse the same host name and IP on the Directory Server 11 host, disconnect the old server from the network.

2. On the new host:
   a. Install Directory Server 11. For details, see Chapter 2, *Setting up a new Directory Server instance*.
   b. Optionally, configure TLS encryption:
      - If the new installation uses a different host name than the Directory Server 10 instance:
        i. See the Enabling TLS chapter in the *Red Hat Directory Server Administrator Guide*.
      - To use the same host name as the previous Directory Server 10 installation:
        i. Stop the instance:

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

        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 **cert8.db**, **key3.db**, and **pin.txt** files that you copied from the Directory Server 10 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/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. Start the instance:

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

Directory Server automatically converts the NSS databases to the SQLite format. The converted databases are stored in the **cert9.db** and **key4.db** files in the **/etc/dirsrv/slapd-*instance_name*/** directory.

vi. Optionally, remove the old NSS databases, to avoid confusion:

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

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. For example:

```
# 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. Import the LDIF file. For example, to import the **/tmp/migration.ldif** file into the **userRoot** database:

```
# dsconf -D 'cn=Directory Manager' ldap://server.example.com backend import
userRoot /tmp/migration.ldif
```

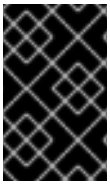
CHAPTER 6. INSTALLING, UPDATING, AND UNINSTALLING THE PASSWORD SYNCHRONIZATION SERVICE

To synchronize passwords between Active Directory and Red Hat Directory Server, you must use the password password synchronization service. This chapter contains information about how the password synchronization service functions, as well as how to install, update, and remove it.

6.1. UNDERSTANDING THE PASSWORD SYNCHRONIZATION SERVICE WORKS

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 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.

6.2. DOWNLOADING THE PASSWORD SYNCHRONIZATION SERVICE INSTALLER

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

Prerequisites

- A valid Red Hat Directory Server subscription
- 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 **11** in the **Version** field.
5. Download the **PassSync Installer**.

6. Copy the installer to every writeable Active Directory domain controller (DC).

6.3. INSTALLING THE PASSWORD SYNCHRONIZATION SERVICE

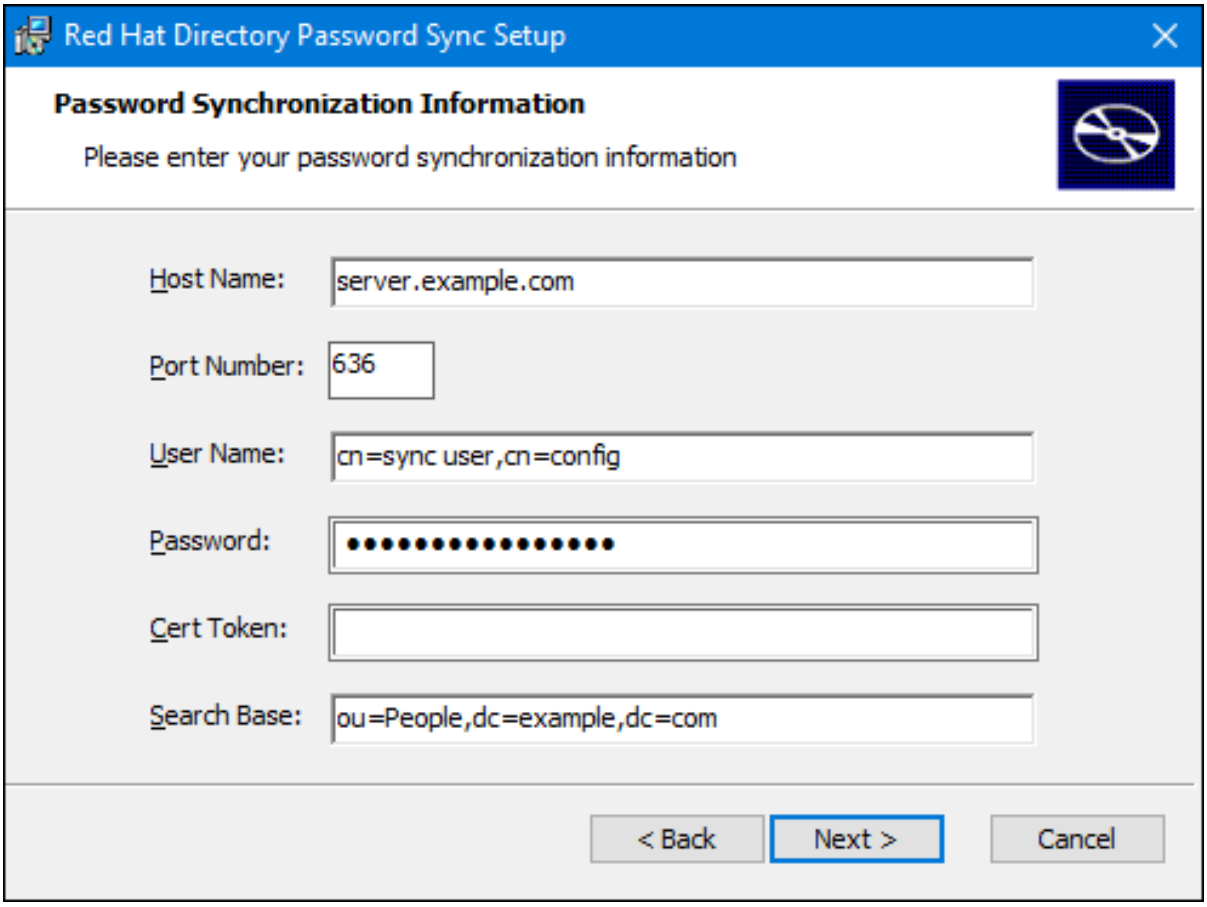
This section describes how to install the **Red Hat Directory Password Sync** on Windows domain controllers (DC). For further detail, see Section 6.1, "Understanding the password synchronization service works".

Prerequisites

- The latest version of the **PassSync Installer** downloaded to the Windows Active Directory domain controller (DC). For details, see Section 6.2, "Downloading the password synchronization service installer".
- A prepared Directory Server host as described in the following sections in the Red Hat Directory Server Administration Guide:
  - Configure TLS on Directory Server
  - Configure the Active Directory Domain
  - Select or Create the Synchronization Identity

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-ds11.*-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.

NOTE

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

8. Configure the password synchronization service as described in the Configure the Password Sync Service section in the Red Hat Directory Server Administration Guide. Until the service is fully configured, password synchronization will fail.

Repeat this procedure on every writable Windows DC.

6.4. UPDATING THE PASSWORD SYNCHRONIZATION SERVICE

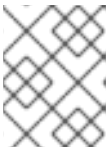
This section describes how to update an existing **Red Hat Directory Password Sync** installation on a Windows domain controller (DC).

Prerequisites

- **Red Hat Directory Password Sync** is running on your Windows DCs.
- The latest version of the **PassSync Installer** downloaded to the Windows Active Directory domain controller (DC). For details, see Section 6.2, "Downloading the password synchronization service installer".

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-ds11.*-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.



NOTE

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

Repeat this procedure on every writable Windows DC.

6.5. UNINSTALLING THE PASSWORD SYNCHRONIZATION SERVICE

This section contains information about uninstalling the **Red Hat Directory Password Sync** service from a Windows domain controller (DC).

Prerequisites

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

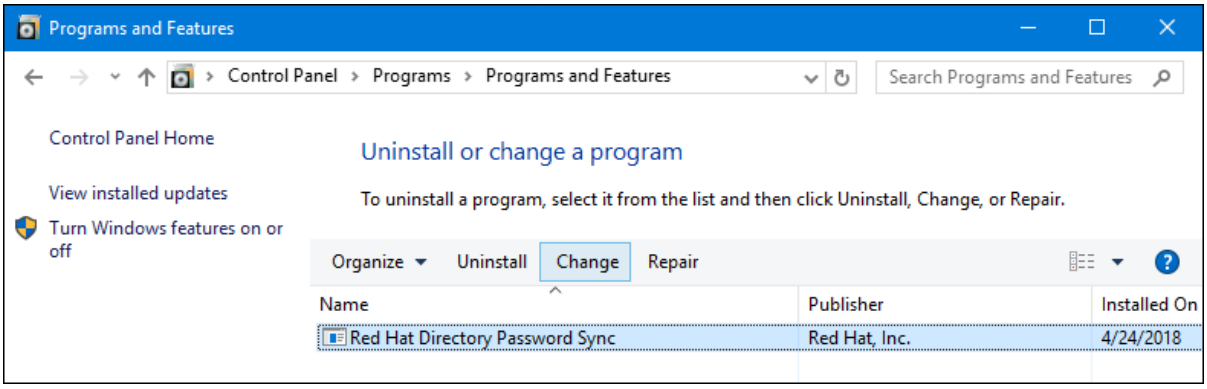
Procedure

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

2. Open the **Control Panel**

3. Click **Programs** and then **Programs and Features**

4. Select the **Red Hat Directory Password Sync** entry, and click the **Uninstall** button.



5. Click **Yes** to confirm.

CHAPTER 7. UNINSTALLING DIRECTORY SERVER

In certain situations, administrators what to uninstall Directory Server from a host. This chapter describes this procedure.

7.1. UNINSTALLING DIRECTORY SERVER

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

Prerequisites

- Directory Server installed on the host

Procedure

1. Remove all instances from the replication topology. If you instance is not a member of a replication topology skip this step.
   For details about removing an instance from the topology, see Removing a Supplier from the Replication Topology in the Red Hat Directory Server Administration Guide.

2. Remove all instances from the server.
   For details, see Removing a Directory Server Instance in the Red Hat Directory Server Administration Guide.

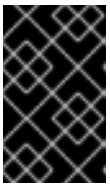
3. Remove the Directory Server packages:

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

4. Optionally, disable the **dirsrv-11-for-rhel-8-x86_64-rpms** repository:

   ```
   # 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. Optionally, 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:   Red Hat Enterprise Linux Developer Suite
     ...
     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

- For further details about using the **subscription-manager** utility, see the Using and Configuring Subscription Manager guide.

APPENDIX A. COMMAND-LINE UTILITIES REPLACED IN RED HAT DIRECTORY SERVER 11

The following table lists utilities in Directory Server 10 and earlier versions together with their replacements in Directory Server 11:

Directory Server 10 and earlier	Directory Server 11
bak2db **bak2db.pl**	**dsctl bak2db**
cl-dump **cl-dump.pl**	**dsconf replication dump-changelog**
cleanallruv.pl	**dsconf repl-tasks cleanallruv**
db2bak **db2bak.pl**	**dsctl db2bak**
db2index **db2index.pl**	**dsctl db2index**
db2ldif **db2ldif.pl**	**dsctl db2ldif**
dbgen	No replacement
dbmon.sh	No replacement
dbverify	No replacement
dn2rdn	No replacement.
fixup-linkedattrs.pl	**dsconf plugin linked-attr fixup**
fixup-memberof.pl	**dsconf plugin memberof fixup**
fixup-memberuid.pl	No replacement
infadd	No replacement
ldif	No replacement
ldif2db **ldif2db.pl**	**dsctl ldif2db**
ldif2ldap	No replacement

Directory Server 10 and earlier	Directory Server 11
migrate-ds.pl	No replacement
migratecred	No replacement
mmldif	No replacement
monitor	**dsconf backend monitor** **dsconf backend monitor-suffix**
ns-accountstatus.pl	**dsidm user status**
ns-activate.pl	**dsidm user unlock**
ns-inactivate.pl	**dsidm user lock**
ns-newpwpolicy.pl	**dsconf localpwp adduser** **dsconf localpwp addsubtree**
remove-ds.pl	**dsctl remove**
repl-monitor **repl-monitor.pl**	**dsconf repl-agmt status**
restart-slapd	**dsctl restart**
restoreconfig	No replacement
rsearch	No replacement
saveconfig	No replacement
schema-reload.pl	**dsconf schema reload**
setup-ds.pl	**dscreate**
start-slapd	**dsctl start**
stop-slapd	**dsctl stop**
suffix2instance	No replacement
syntax-validate.pl	No replacement
upgradednformat	No replacement

Directory Server 10 and earlier	Directory Server 11
usn-tombstone-cleanup.pl	**dsconf usn cleanup**
verify-db.pl	No replacement
vlvindex	**dsconf backend vlv-index**

APPENDIX B. REVISION HISTORY

Note that revision numbers relate to the edition of this manual, not to version numbers of Red Hat Directory Server.

Version	Date and change	Author
11.0-1	Nov 05 2019: Red Hat Directory Server 11.0 release of this guide	Marc Muehlfeld