Red Hat Directory Server 12

Red Hat Directory Server 12 release notes

Noteworthy features and updates related to Red Hat Directory Server 12 (12.3)

Last Updated: 2024-03-20

Red Hat Directory Server 12 Red Hat Directory Server 12 release notes

Noteworthy features and updates related to Red Hat Directory Server 12 (12.3)

Legal Notice

Abstract

Learn about improvements and additions that have been implemented in Red Hat Directory Server 12. These include notable bug fixes, known problems, technology previews, deprecated functionality, and other details about this release.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION 3

CHAPTER 1. GENERAL INFORMATION 4
1.1. DIRECTORY SERVER SUPPORT POLICY AND LIFE CYCLE 4
1.2. SOFTWARE CONFLICTS 4
1.3. MIGRATING TO DIRECTORY SERVER 12 4
1.4. NOTES ABOUT MIGRATING TO DIRECTORY SERVER 12 4

CHAPTER 2. RED HAT DIRECTORY SERVER 12.3 5
2.1. GENERAL HARDWARE REQUIREMENTS 5
2.2. SOFTWARE REQUIREMENTS 6
2.3. IMPORTANT UPDATES AND NEW FEATURES 7
2.4. BUG FIXES 8
2.5. KNOWN ISSUES 10
2.6. DEPRECATED FUNCTIONALITY 10
2.7. REMOVED FUNCTIONALITY 11

CHAPTER 3. RED HAT DIRECTORY SERVER 12.2 12
3.1. GENERAL HARDWARE REQUIREMENTS 12
3.2. SOFTWARE REQUIREMENTS 13
3.3. IMPORTANT UPDATES AND NEW FEATURES 14
3.4. BUG FIXES 15
3.5. KNOWN ISSUES 15
3.6. DEPRECATED FUNCTIONALITY 16

CHAPTER 4. RED HAT DIRECTORY SERVER 12.1 17
4.1. GENERAL HARDWARE REQUIREMENTS 17
4.2. SOFTWARE REQUIREMENTS 18
4.3. HIGHLIGHTED UPDATES AND NEW FEATURES 19
4.4. KNOWN ISSUES 20

CHAPTER 5. RED HAT DIRECTORY SERVER 12.0 22
5.1. SYSTEM REQUIREMENTS 22
5.2. HIGHLIGHTED UPDATES AND NEW FEATURES 22
5.3. BUG FIXES 23
5.4. TECHNOLOGY PREVIEWS 25
5.5. KNOWN ISSUES 25
5.6. REMOVED FUNCTIONALITY 26

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 submitting feedback through Jira (account required):
  1. Log in to the Jira website.
  2. Click **Create** in the top navigation bar
  3. Enter a descriptive title in the **Summary** field.
  4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
  5. Click **Create** at the bottom of the dialogue.
- For submitting feedback through Bugzilla (account required):
  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. GENERAL INFORMATION

Lean about Red Hat Directory Server 12 general information that is independent of the minor versions.

1.1. DIRECTORY SERVER SUPPORT POLICY AND LIFE CYCLE

For details, see the Red Hat Directory Server Errata Support Policy document.

1.2. SOFTWARE CONFLICTS

You cannot install Directory Server on a system that has a Red Hat Enterprise Linux Identity Management (IdM) server installed. Likewise, no Red Hat Enterprise Linux IdM server can be installed on a system with a Directory Server instance.

1.3. MIGRATING TO DIRECTORY SERVER 12

- For a procedure about migrating Directory Server 11 to Directory Server 12, see the Migrating Directory Server 11 to Directory Server 12 chapter.
- For a procedure about migrating Directory Server 10 to Directory Server 12, see Migrating Directory Server 10 to Directory Server 12 chapter.

1.4. NOTES ABOUT MIGRATING TO DIRECTORY SERVER 12

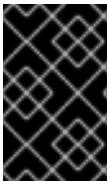
The Directory Server 12 default password storage scheme is PBKDF2-SHA512

Directory Server 12 uses the **PBKDF2-SHA512** scheme as a default password storage scheme, which is more secure than **SSHA**, **SSHA512**, and other schemes. Therefore, if some of your applications, such as **freeradius**, do not support the **PBKDF2-SHA512** scheme, and you must set a weaker password storage scheme back, note that Directory Server updates user passwords not only when an application adds or modifies the user entry, but also during a successful bind operation. However, you can disable an update on bind operations by setting the **nsslapd-enable-upgrade-hash** parameter in the **cn=config** entry to **off**.

New command-line utilities starting Directory Server 11

Since version 11, Directory Server provides new command line utilities to manage server instances and users. These utilities replace the Perl scripts used for management tasks in Directory Server 10 and earlier versions.

For a list of commands in previous versions and their replacements in Directory Server 12, see the Command-line utilities replaced in Red Hat Directory Server 11 appendix in the *Red Hat Directory Server Installation Guide*.



IMPORTANT

The Perl scripts used for management tasks in Directory Server 10 and earlier versions are still available in the **389-ds-base-legacy-tools** package. However, Red Hat only supports the new **dsconf**, **dsctl**, **dscreate**, and **dsidm** command-line utilities.

CHAPTER 2. RED HAT DIRECTORY SERVER 12.3

Learn about new system requirements, important updates and new features, known issues, and deprecated functionality implemented in Directory Server 12.3.

2.1. GENERAL HARDWARE REQUIREMENTS

The hardware requirements are based on tests run with the following prerequisites:

- The server uses default indexes.
- Each LDAP entry has a size of 1.5 KB and 30 or more attributes.

Disk space

The following table provides guidelines for the recommended disk space for Directory Server based on the number of entries.

Table 2.1. Required disk space

Number of entries	Database size	Database cache	Server and logs	Total disk space
10,000 - 500,000	2 GB	2 GB	4 GB	**8 GB**
500,000 - 1,000,000	5 GB	2 GB	4 GB	**11 GB**
1,000,000 - 5,000,000	21 GB	2 GB	4 GB	**27 GB**
5,000,000 - 10,000,000	42 GB	2 GB	4 GB	**48 GB**

The total disk space does not include space for backups and replication metadata. With enabled replication, its metadata can require up to 10% more of the total disk space.

A replication changelog with 1 million changes can add at least 315 MB to the total disk space requirement.

The temporary file system (tmpfs) mounted in **/dev/shm/** should have at least 4 GB of available space to store RHDS temporary files.

Required RAM

Make sure your system has enough RAM available to keep the entire database in cache. The required RAM size can be higher than the recommended one depending on server configuration and usage patterns.

Table 2.2. Required RAM size

Number of entries	Entry cache	Entry cache with replication [a]	Database cache	DN cache	NDN cache	Total RAM size [b]
10,000 - 500,000	4 GB	5 GB	1.5 GB	45 MB	160 MB	**7 GB**
500,000 - 1,000,000	8 GB	10 GB	1.5 GB	90 MB	320 MB	**12 GB**
1,000,000 - 5,000,000	40 GB	50 GB	1.5 GB	450 MB	1.6 GB	**54 GB**
5,000,000 - 10,000,000	80 GB	100 GB	1.5 GB	900 MB	3.2 GB	**106 GB**

[a] Entry cache with replication includes the entry's replication state and metadata.

[b] Total RAM size assumes you enabled replication.

2.2. SOFTWARE REQUIREMENTS

Supported platforms for Directory Server

Red Hat supports Red Hat Directory Server 12.3 if it runs on the following platforms:

- A Red Hat Enterprise Linux 9.3 built for **AMD64** and **Intel 64** architectures.
- A Red Hat Enterprise Linux virtual guest on a certified hypervisor. For details, see the Which hypervisors are certified to run Red Hat Enterprise Linux? solution article.

Supported platforms for the Directory Server user interface in the web console

Red Hat supports the browser-based Directory Server user interface in the web console in the following environments:

Operating system	Browser
Red Hat Enterprise Linux 9.3	• Mozilla Firefox 115.4.0 and later • Chrome 88 and later
Windows Server 2016 and 2019:	• Mozilla Firefox 115.4.0 and later • Chrome 88 and later

Operating system	Browser
Windows 10	• Mozilla Firefox 115.4.0 and later • Microsoft Edge 88 and later • Chrome 88 and later

Supported platforms for the Windows Synchronization utility

Red Hat supports the Windows Synchronization utility for Active Directory running on:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

2.3. IMPORTANT UPDATES AND NEW FEATURES

Learn about new features and important updates in Red Hat Directory Server 12.3.

Directory Server now backs up configuration files, the certificate database, and custom schema files

Previously, Directory Server backed up only databases. With this update, when you run **dsconf backup create** or **dsctl db2bak** command, Directory Server also backs up configuration files, the certificate database, and custom schema files that are stored in the **/etc/dirsrv/slapd-*instance_name*/** directory to the backup default directory **/var/lib/dirsrv/slapd-*instance_name*/bak/config_files/**.

Directory Server also backs up these files when you perform the backup by using the web console.

(BZ#2147446)

The Alias Entries plug-in is now available in Directory Server

When you enable the **Alias Entries** plug-in, a search for an entry returns the entry that you set as an aliased entry. For example, Barbara Jensen, an employee in the Example company, got married and her surname changed. Her old entry **uid=bjensen,ou=people,dc=example,dc=com** contains the alias to her new entry **uid=bsmith,ou=people,dc=example,dc=com**. When the plug-in is enabled, the search for the **uid=bjensen,ou=people,dc=example,dc=com** entry returns the **uid=bsmith,ou=people,dc=example,dc=com** entry information.

Use the **-a find** parameter for the **ldapsearch** command to retrieve entries with aliases.

Currently, the **Alias Entries** plug-in supports only *base* level searches.

For more information, see the Alias Entries plug-in description.

(BZ#2203173)

The checkAllStateAttrs configuration option is now available

You can apply both account inactivity and password expiration when a user authenticates by using the **checkAllStateAttrs** setting. When you enable this parameter, it checks the main state attribute and, if the account information is correct, it then checks the alternate state attribute.

(BZ#2174161)

You can now save credentials and aliases for a replication report using the Directory Server web console

Previously, when you used the web console to set credentials and aliases for a replication monitoring report, these settings were no longer present after the web console reload. With this enhancement, when you set the credentials and aliases for the replication report, Directory Server saves new settings in the **.dsrc** file and the web console uploads saved settings after the reload.

(BZ#2030884)

Important updates and new features in the 389-ds-base packages

Directory Server 12.3 features that are included in the **389-ds-base** packages are documented in Red Hat Enterprise Linux 9.3 Release Notes:

- RHEL 9.3 provides 389-ds-base 2.3.4
- Directory Server can now close a client connection if a **bind** operation fails
- Automembership plug-in improvements. It no longer cleans up groups by default
- New **passwordAdminSkipInfoUpdate**: on/off configuration option is now available
- New **slapi_memberof()** plug-in function is now available for Directory Server plug-ins and client applications
- Directory Server now replaces the virtual attribute **nsRole** with an indexed attribute for managed and filtered roles
- New **nsslapd-numlisteners** configuration option is now available

2.4. BUG FIXES

Learn about bugs fixed in Red Hat Directory Server 12.3 that have a significant impact on users.

The cockpit-389-ds package upgrade now updates the 389-ds-base and python3-lib389 packages

Previously, the **cockpit-389-ds** package did not specify the version of the **389-ds-base** package it depends on. As a result, the upgrade of the **cockpit-389-ds** package alone did not update the **389-ds-base** and **python3-lib389** packages which could lead to misalignment and compatibility issues between packages. With this update, the **cockpit-389-ds** package depends on the **389-ds-base** exact version and the update of the **cockpit-389-ds** package also upgrades **389-ds-base** and **python3-lib389** packages.

(BZ#2240021)

Disabling replication on a consumer no longer crashes the server

Previously, when you disabled replication on a consumer server, Directory Server tried to remove the changelog on the consumer where it did not exist. As a consequence, the server terminated unexpectedly with the following error:

```
Error: -1 - Can't contact LDAP server - []
```

With this update, disabling replication on a consumer works as expected.

(BZ#2184599)

A non-root instance no longer fails to start after creation

Previously, Rust plug-ins were incorrectly disabled in the non-root instance template and the default password scheme was moved to Rust-based hasher. As a result, the non-root instance could not be created. With this update, a non-root instance supports Rust plug-ins and you can create the instance with the PBKDF2-SHA512 default password scheme.

(BZ#2151864)

The dsconf utility now accepts only value 65535 as the replica-id when setting a hub or a consumer role

Previously, when you configured a hub or a consumer role, the **dsconf** utility also accepted the **replica-id** option with a value other than **65535**. With this update, the **dsconf** utility accepts only **65535** as the **replica-id** value for a hub or a consumer role. If you do not specify this value in a **dsconf** command, then Directory Server assigns the **replica-id** value **65535** automatically.

(BZ#1987373)

The dscreate ds-root command now normalizes paths

Previously, when you created an instance under a non-root user and provided a **bin_dir** argument value that contained a trailing slash, **dscreate ds-root** failed to find the **bin_dir** value in the **$PATH** variable. As a result, the instance under a non-root user was not created. With this update, **dscreate ds-root** command normalizes paths, and the instance is created as expected.

(BZ#2151868)

The dsconf utility now has the fixup option to create fix-up tasks for the entryUUID plug-in

Previously, the **dsconf** utility did not provide an option to create fix-up tasks for the **entryUUID** plug-in. As a consequence, administrators could not use **dsconf** to create a task to automatically add **entryUUID** attributes to existing entries. With this update, you can use the **dsconf** utility with the **fixup** option to create fix-up tasks for the **entryUUID** plug-in. For example, to fix all entries under the **dn=example,dc=com** entry that contain a **uid** attribute, enter:

```
# dsconf instance_name plugin entryuuid fixup -f “(uid=*)” “dn=example,dc=com"
```

(BZ#2047175)

Access log no longer displays an error message during Directory Server installation in FIPS mode

Previously, when you installed Directory Server in FIPS mode, the access log file displayed the following error message:

```
[time_stamp]
- WARN - slapd_do_all_nss_ssl_init - ERROR: TLS is not enabled, and the
machine is in FIPS mode. Some functionality won’t work correctly (for
example, users with PBKDF2_SHA256 password scheme won’t be able to log
in). It’s highly advisable to enable TLS on this instance.
```

With this update, the issue has been fixed, and the error message is no longer present in the access log.

(BZ#2153668)

Directory Server 12.3 bug fixes that are included in the389-ds-base packages are documented in Red Hat Enterprise Linux 9.3 Release Notes:

- Paged searches from a regular user now do not impact performance
- The LMDB import now works faster
- Schema replication now works correctly in Directory Server
- Referral mode is now working correctly in Directory Server
- The **dirsrv** service now starts correctly after reboot
- Changing a security parameter now works correctly

2.5. KNOWN ISSUES

Learn about known problems and, if applicable, workarounds in Directory Server 12.3.

Directory Server can import LDIF files only from /var/lib/dirsrv/slapd-*instance_name*/ldif/

Since RHEL 8.3, Red Hat Directory Server (RHDS) uses its own private directories and the **PrivateTmp** systemd directive is enabled by default for the LDAP services. As a result, RHDS can only import LDIF files from the **/var/lib/dirsrv/slapd-*instance_name*/ldif/** directory. If the LDIF file is stored in a different directory, such as **/var/tmp**, **/tmp**, or **/root**, the import fails with an error similar to the following:

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

To work around this problem, complete the following steps:

1. Move the LDIF file to the **/var/lib/dirsrv/slapd-*instance_name*/ldif/** directory:

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
   ```

2. Set permissions that allow the **dirsrv** user to read the file:

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. Restore the SELinux context:

   ```
   # restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

For more information, see the solution article LDAP Service cannot access files under the host's /tmp and /var/tmp directories.

(BZ#2075525)

Known issues in the 389-ds-base packages

Red Hat Directory Server 12.3 known issues that affect **389-ds-base packages** are documented in Red Hat Enterprise Linux 9.3 Release Notes:

- When the **nsslapd-numlisteners** attribute value is more than 2, Directory Server fails

2.6. DEPRECATED FUNCTIONALITY

Learn about functionality that has been deprecated in Red Hat Directory Server 12.3.

Deprecated functionality in the 389-ds-base packages

Directory Server 12.3 functionality that has been deprecated in the **389-ds-base** packages is documented in the Red Hat Enterprise Linux 9.3 Release Notes:

- The **nsslapd-ldapimaprootdn** parameter is deprecated

2.7. REMOVED FUNCTIONALITY

Learn about functionality that has been removed in Red Hat Directory Server 12.3.

Removed functionality in the 389-ds-base packages

Removed functionality in Red Hat Directory Server, that are included in the **389-ds-base** packages, are documented in the Red Hat Enterprise Linux 9.3 Release Notes:

- The **nsslapd-conntablesize** configuration parameter has been removed from **389-ds-base**

CHAPTER 3. RED HAT DIRECTORY SERVER 12.2

Learn about new system requirements, important updates and new features, known issues, and deprecated functionality implemented in Directory Server 12.2.

3.1. GENERAL HARDWARE REQUIREMENTS

The hardware requirements are based on tests run with the following prerequisites:

- The server uses default indexes.
- Each LDAP entry has a size of 1.5 KB and 30 or more attributes.

Disk space

The following table provides guidelines for the recommended disk space for Directory Server based on the number of entries.

Table 3.1. Required disk space

Number of entries	Database size	Database cache	Server and logs	Total disk space
10,000 - 500,000	2 GB	2 GB	4 GB	**8 GB**
500,000 - 1,000,000	5 GB	2 GB	4 GB	**11 GB**
1,000,000 - 5,000,000	21 GB	2 GB	4 GB	**27 GB**
5,000,000 - 10,000,000	42 GB	2 GB	4 GB	**48 GB**

The total disk space does not include space for backups and replication metadata. With enabled replication, its metadata can require up to 10% more of the total disk space.

A replication changelog with 1 million changes can add at least 315 MB to the total disk space requirement.

The temporary file system (tmpfs) mounted in **/dev/shm/** should have at least 4 GB of available space to store RHDS temporary files.

Required RAM

Make sure your system has enough RAM available to keep the entire database in cache. The required RAM size can be higher than the recommended one depending on server configuration and usage patterns.

Table 3.2. Required RAM size

Number of entries	Entry cache	Entry cache with replication [a]	Database cache	DN cache	NDN cache	Total RAM size [b]
10,000 - 500,000	4 GB	5 GB	1.5 GB	45 MB	160 MB	**7 GB**
500,000 - 1,000,000	8 GB	10 GB	1.5 GB	90 MB	320 MB	**12 GB**
1,000,000 - 5,000,000	40 GB	50 GB	1.5 GB	450 MB	1.6 GB	**54 GB**
5,000,000 - 10,000,000	80 GB	100 GB	1.5 GB	900 MB	3.2 GB	**106 GB**

[a] Entry cache with replication includes the entry's replication state and metadata.

[b] Total RAM size assumes you enabled replication.

3.2. SOFTWARE REQUIREMENTS

Supported platforms for Directory Server

Red Hat supports Red Hat Directory Server 12.2 if it runs on the following platforms:

- A Red Hat Enterprise Linux 9.2 built for **AMD64** and **Intel 64** architectures.
- A Red Hat Enterprise Linux virtual guest on a certified hypervisor. For details, see the Which hypervisors are certified to run Red Hat Enterprise Linux? solution article.

Supported platforms for the Directory Server user interface in the web console

Red Hat supports the browser-based Directory Server user interface in the web console in the following environments:

Operating system	Browser
Red Hat Enterprise Linux 9.2	• Mozilla Firefox 102.11.0 and later • Chrome 88 and later
Windows Server 2016 and 2019:	• Mozilla Firefox 102.11.0 and later • Chrome 88 and later

Operating system	Browser
Windows 10	• Mozilla Firefox 102.11.0 and later • Microsoft Edge 88 and later • Chrome 88 and later

Supported platforms for the Windows Synchronization utility

Red Hat supports the Windows Synchronization utility for Active Directory running on:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

3.3. IMPORTANT UPDATES AND NEW FEATURES

Learn about new features and important updates in Red Hat Directory Server 12.2.

Directory Server 12.2 rebased to upstream version 2.2.7

Directory Server 12.2 is based on upstream version 2.2.7 which provides a number of bug fixes and enhancements over the previous version. For a complete list of notable changes, read the upstream release notes before updating: https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-1.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-2.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-3.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-4.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-5.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-6.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-7.html

The dsconf utility can now set timeout for tasks

Previously, if a task took longer than four minutes, **dsconf** returned the following message:

```
DEBUG: The backup create task has failed with the error code: (None)
...
```

With this enhancement, you can set the required timeout for the task by using the **--timeout** option. The timeout does not stop the task, however it stops the **dsconf** utility from waiting for the task result.

(BZ#1993124)

You can now import and export certificates using the web console

Previously, you could only import a certificate from a file on the server filesystem using the web console. With this release, you can also import a file by copy-pasting a **base64**-encoded certificate. Additionally, you can export certificate authority and server certificates.

(BZ#1751264)

Important updates and new features in the 389-ds-base packages

Directory Server 12.2 features that are included in the **389-ds-base** packages are documented in Red Hat Enterprise Linux 9.2 Release Notes:

- Directory server now supports ECDSA private keys for TLS
- Directory Server now supports extended logging of search operations
- The NUNC_STANS error logging level was replaced by the new **1048576** logging level
- Directory Server introduces the security log
- Directory Server now can compress archived log files
- Default behavior change: Directory Server now returns a DN in exactly the same spelling as it was added to the database
- New **nsslapd-auditlog-display-attrs** configuration parameter for the Directory Server audit log
- New **pamModuleIsThreadSafe** configuration option is now available
- Directory Server can now import a certificate bundle

3.4. BUG FIXES

Learn about bugs fixed in Red Hat Directory Server 12.2 that have a significant impact on users.

Directory Server 12.2 bug fixes that are included in the **389-ds-base** packages are documented in Red Hat Enterprise Linux 9.2 Release Notes:

- A password change for the Directory Server replication manager account now works correctly
- The **dscreate** utility works now correctly when uses a custom path with the **db_dir** parameter

3.5. KNOWN ISSUES

Learn about known problems and, if applicable, workarounds in Directory Server 12.2.

Directory Server can import LDIF files only from /var/lib/dirsrv/slapd-*instance_name*/ldif/

Since RHEL 8.3, Red Hat Directory Server (RHDS) uses its own private directories and the **PrivateTmp** systemd directive is enabled by default for the LDAP services. As a result, RHDS can only import LDIF files from the **/var/lib/dirsrv/slapd-*instance_name*/ldif/** directory. If the LDIF file is stored in a different directory, such as **/var/tmp**, **/tmp**, or **/root**, the import fails with an error similar to the following:

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

To work around this problem, complete the following steps:

1. Move the LDIF file to the **/var/lib/dirsrv/slapd-*instance_name*/ldif/** directory:

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
   ```

2. Set permissions that allow the **dirsrv** user to read the file:

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. Restore the SELinux context:

```
# restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
```

For more information, see the solution article LDAP Service cannot access files under the host's /tmp and /var/tmp directories.

(BZ#2075525)

Access log displays an error message during Directory Server installation in FIPS mode

When you install Directory Server in the FIPS mode, the access log file displays the following error message:

```
[time_stamp]
- WARN - slapd_do_all_nss_ssl_init - ERROR: TLS is not enabled, and the
machine is in FIPS mode. Some functionality won't work correctly (for
example, users with PBKDF2_SHA256 password scheme won't be able to log
in). It's highly advisable to enable TLS on this instance.
```

Such behavior happens because at first, Directory Server finds that TLS is not initialized and logs the error message. However, later when the **dscreate** utility completes TLS initialization and enables security, the error message is no longer present.

(BZ#2153668)

Known issues in the 389-ds-base packages

Red Hat Directory Server 12.2 known issues that affect **389-ds-base packages** are documented in Red Hat Enterprise Linux 9.2 Release Notes:

- The **dsconf** utility has no option to create fix-up tasks for the **entryUUID** plug-in
- Configuring a referral for a suffix fails in Directory Server
- Directory Server terminates unexpectedly when started in referral mode

3.6. DEPRECATED FUNCTIONALITY

Learn about functionality that has been deprecated in Red Hat Directory Server 12.2.

Deprecated functionality in the 389-ds-base packages

Directory Server 12.2 functionality that has been deprecated in the **389-ds-base** packages is documented in the Red Hat Enterprise Linux 9.2 Release Notes:

- The **nsslapd-idlistscanlimit** parameter is deprecated and its default value has been changed

CHAPTER 4. RED HAT DIRECTORY SERVER 12.1

Learn about new system requirements, highlighted updates and new features, known issues, and deprecated functionality implemented in Directory Server 12.1.

4.1. GENERAL HARDWARE REQUIREMENTS

The hardware requirements are based on tests run with the following prerequisites:

- The server uses default indexes.
- Each LDAP entry has a size of 1.5 KB and 30 or more attributes.

Disk space

The following table provides guidelines for the recommended disk space for Directory Server based on the number of entries.

Table 4.1. Required disk space

Number of entries	Database size	Database cache	Server and logs	Total disk space
10,000 - 500,000	2 GB	2 GB	4 GB	**8 GB**
500,000 - 1,000,000	5 GB	2 GB	4 GB	**11 GB**
1,000,000 - 5,000,000	21 GB	2 GB	4 GB	**27 GB**
5,000,000 - 10,000,000	42 GB	2 GB	4 GB	**48 GB**

The total disk space does not include space for backups and replication metadata. With enabled replication, its metadata can require up to 10% more of the total disk space.

A replication changelog with 1 million changes can add at least 315 MB to the total disk space requirement.

The temporary file system (tmpfs) mounted in **/dev/shm/** should have at least 4 GB of available space to store RHDS temporary files.

Required RAM

Make sure your system has enough RAM available to keep the entire database in cache. The required RAM size can be higher than the recommended one depending on server configuration and usage patterns.

Table 4.2. Required RAM size

Number of entries	Entry cache	Entry cache with replication [a]	Database cache	DN cache	NDN cache	Total RAM size [b]
10,000 - 500,000	4 GB	5 GB	1.5 GB	45 MB	160 MB	**7 GB**
500,000 - 1,000,000	8 GB	10 GB	1.5 GB	90 MB	320 MB	**12 GB**
1,000,000 - 5,000,000	40 GB	50 GB	1.5 GB	450 MB	1.6 GB	**54 GB**
5,000,000 - 10,000,000	80 GB	100 GB	1.5 GB	900 MB	3.2 GB	**106 GB**

[a] Entry cache with replication includes the entry's replication state and metadata.

[b] Total RAM size assumes you enabled replication.

4.2. SOFTWARE REQUIREMENTS

Supported platforms for Directory Server

Red Hat supports Directory Server 12.1 if it runs on the following platforms:

- A Red Hat Enterprise Linux 9.1 built for **AMD64** and **Intel 64** architectures.
- A Red Hat Enterprise Linux virtual guest on a certified hypervisor. For details, see the Which hypervisors are certified to run Red Hat Enterprise Linux? solution article.

Supported platforms for the Directory Server user interface in the web console

Red Hat supports the browser-based Directory Server user interface in the web console in the following environments:

Operating system	Browser
Red Hat Enterprise Linux 9.2	• Mozilla Firefox 102.3.0 and later • Chrome 88 and later
Windows Server 2016 and 2019:	• Mozilla Firefox 102.3.0 and later • Chrome 88 and later

Operating system	Browser
Windows 10	• Mozilla Firefox 102.3.0 and later • Microsoft Edge 88 and later • Chrome 88 and later

Supported platforms for the Windows Synchronization utility

Red Hat supports the Windows Synchronization utility for Active Directory running on:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

4.3. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 12.1.

Directory Server 12.1 rebased to upstream version 2.1.3

Directory Server 12.1 is based on upstream version 2.1.3 which provides a number of bug fixes and enhancements over the previous version. For a complete list of notable changes, read the upstream release notes before updating:

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-0.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-1.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-3.html

The LDAP browser is now fully supported

With this enhancement, you can manage LDAP entries from the **LDAP Browser** tab in the web console. For example, you can:

- Browse the directory using **Tree** or **Table** view.
- Manage entries, such as users, groups, roles, organizational units (OUs), and custom entries.
- Manage Access Control Instructions (ACIs).
- Manage classes of service definition (CoS).
- Search for entries.

Highlighted updates and new features in the 389-ds-base packages

Features in Red Hat Directory Server, that are included in the **389-ds-base** packages, are documented in the Red Hat Enterprise Linux 9.1 Release Notes:

- Directory Server now supports recursive delete operations when using **ldapdelete**
- You can now set basic replication options during the Directory Server installation

- Directory Server now supports canceling the Auto Membership plug-in task
- Directory Server now supports instance creation by a non-root user
- Replication changelog trimming is now enabled by default in Directory Server

4.4. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 12.1.

Directory Server can import LDIF files only from /var/lib/dirsrv/slapd-*instance_name*/ldif/

The **dsconf backend import** command requires that you specify the path to the LDIF file you want to import. However, due to file system and SELinux permissions, as well as other operating system restrictions, Directory Server can only import LDIF files from the **/var/lib/dirsrv/slapd-*instance_name*/ldif/** directory. If the LDIF file is stored in a different directory, the import fails with an error similar to the following:

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

To work around this problem:

1. Move the file to the /var/lib/dirsrv/slapd-*instance_name*/ldif/ directory:

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

2. Set permissions that allow the **dirsrv** user to read the file:

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. Restore the SELinux context:

   ```
   # restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

(BZ#2081352)

Directory Server replication fails after changing password of the replication manager account

After a password change, Directory Server does not properly update the password cache for the replication agreement. As a consequence, when you change the password for the replication manager account, the replication breaks. To work around this problem, restart the Directory Server instance. As a result, the cache is rebuilt at start-up, and the replication connection binds with the new password instead of the old one.

(BZ#1956987)

Known issues in the 389-ds-base packages

Known issues in Red Hat Directory Server, that are included in the **389-ds-base** packages, are documented in the Red Hat Enterprise Linux 9.1 Release Notes:

- The **dsconf** utility has no option to create fix-up tasks for the **entryUUID** plug-in
- Configuring a referral for a suffix fails in Directory Server

- Directory Server terminates unexpectedly when started in referral mode

Deprecated functionality in the 389-ds-base packages

Red Hat Directory Server deprecated functionality that has been removed from the **389-ds-base** packages is documented in the Red Hat Enterprise Linux 9.1 Release Notes:

- **-h** and **-p** options were deprecated in OpenLDAP client utilities

CHAPTER 5. RED HAT DIRECTORY SERVER 12.0

This section contains information related to installing Directory Server 12.0, including prerequisites and platform requirements.

5.1. SYSTEM REQUIREMENTS

This section contains information related to installing Directory Server 12.0, including prerequisites and platform requirements.

Supported platforms for Directory Server

Red Hat supports Directory Server 12.0 only on Red Hat Enterprise Linux 9.0 built for **AMD64** and **Intel 64** architectures.

Directory Server 12.0 is supported running on a Red Hat Enterprise Linux virtual guest on a certified hypervisor. For details, see the Which hypervisors are certified to run Red Hat Enterprise Linux? solution article.

Supported platforms for the Directory Server user interface in the web console

Red Hat supports the browser-based Directory Server user interface in the web console in the following environments:

Operating system	Browser
Red Hat Enterprise Linux 9.0	• Mozilla Firefox 91.8.0 and later • Chrome 88 and later
Windows Server 2016 and 2019:	• Mozilla Firefox 91.8.0 and later • Chrome 88 and later
Windows 10	• Mozilla Firefox 91.8.0 and later • Microsoft Edge 88 and later • Chrome 88 and later

Supported platforms for the Windows Synchronization utility

Red Hat supports the Windows Synchronization utility for Active Directory running on:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

5.2. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 12.0.

Directory Server 12.0 is based on upstream version 2.0.14

Directory Server 12.0 is based on upstream version 2.0.14 which provides a number of bug fixes and enhancements over the previous version. For a complete list of notable changes, read the upstream release notes before updating:

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-14.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-13.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-12.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-11.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-10.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-9.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-8.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-7.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-6.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-5.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-4.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-3.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-2.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-1.html

Highlighted updates and new features in the **389-ds-base** packages

Features in Red Hat Directory Server, that are included in the **389-ds-base** packages, are documented in the Red Hat Enterprise Linux 9.0 Release Notes:

- Directory Server no longer uses a global changelog
- Directory Server now stores memory-mapped files of databases on a **tmpfs** file system

5.3. BUG FIXES

This section describes bugs fixed in Directory Server 12.0 that have a significant impact on users.

Manually changing the entry cache configuration now works correctly in the web console.

By default, Directory Server uses automatic cache tuning. However, previously you could not disable the automatic cache tuning setting in the web console and set manually the desired entry cache configuration. This update fixes the problem and, as a result, you can now manually configure the entry cache in the web console.

Fixed typos in different parts of the web console

Previously, different parts of the web console contained mistakes in the text fields. As a consequence, incorrect information messages were displayed to a user. This update fixes the issue and the web console now shows the correct text messages.

Changing the configuration of several plug-ins now works correctly in the web console

Previously, when you tried to change the configuration of a plug-in using the web console, an incorrect error message was displayed, or a loading loop did not disappear. Consequently, you could not save a new configuration or did not know if the configuration was saved successfully. The following plug-in were affected:

- Posix Winsync plug-in
- Referential Integrity plug-in
- RootDN Access Control plug-in
- Retro Changelog plug-in

This update fixes the issue. As a result, you can now configure these plug-ins using the web console as expected.

Changelog export now works as expected in the web console

Previously in the web console, when exporting the changelog for debugging purposes, you could select both options: **Decode Base64 changes** and **Only Export CSNs**. However, only the **Export CSNs** option was taken into account. In this release, it is possible to check only one of the options, and the changelog is exported according to the selected one as expected.

Configuring credentials and naming aliases for the replication topology report now works correctly in the web console

Previously, you could not set the credentials or naming aliases for the replication topology report using the web console because fields in the pop-up windows **Add Report Credentials** and **Add Report Alias**, where you needed to enter the required information, were not writable. In this release, the fields in the pop-up windows are writable, and you can set the report credentials, or configure the naming aliases as expected.

The Directory Server web console now validates logging configuration values

Previously, the Directory Server web console accepted invalid values for different types of logs on the **Logging** page. As a consequence, an error occurred when the user tried to save the settings. This update adds the validation for the logging configuration values. As a result, the web console does not accept invalid input.

Attributes on the **Schema** page are no longer editable after using the search feature

Previously, after searching for an attribute in the **Schema** page of the Directory Server web console, a Cascading Style Sheet (CSS) misconfiguration caused the attribute to be editable. With this update, the edit function is now disabled.

Enabling DNA plug-in no longer fails

Previously, an attempt to enable Distributed Numeric Assignment (DNA) plug-in in the Directory Server web console failed and resulted in a browser error. With this update, enabling DNA plug-in works as expected.

Adding a configuration entry in Account Policy plug-in no longer fails

Previously, an attempt to add a configuration entry in Account Policy plug-in sometimes failed with an error. To fix the problem, this update disables the **Create Config** button if the **Shared Config DN** value is not specified.

Import from an LDIF file with replication metadata now works correctly

Previously, importing an LDIF file with replication metadata could cause the replication to fail in certain cases:

In the first case, a replication update vector (RUV) entry placed before the suffix entry in an imported LDIF file was ignored. As a consequence, the replication with the imported replica failed, because of a generation ID mismatch. This update ensures that Directory Server writes the skipped RUV entry at the end of the import.

In the second case, a changelog reinitialized after an RUV mismatch did not contain the starting change sequence numbers (CSNs). As a consequence, the replication with the imported replica failed, because of a missing CSN in the changelog. This update ensures that Directory Server creates the RUV **maxcsn** entries, when reinitializing the changelog.

As a result, with this update, administrators do not have to reinitialize the replication after importing from an LDIF file that contains replication metadata.

Bug fixes in the 389-ds-base packages

Bug fixes in Red Hat Directory Server, that are included in the **389-ds-base** packages, are documented in the Red Hat Enterprise Linux 9.0 Release Notes:

- Authenticating to Directory Server in FIPS mode with passwords hashed with the PBKDF2 algorithm now works as expected

5.4. TECHNOLOGY PREVIEWS

This section documents unsupported Technology Previews in Directory Server 12.0.

The Directory Server web console provides an LDAP browser as a Technology Preview

An LDAP browser has been added to the Directory Server web console. Using the **LDAP Browser** tab in the web console, you can:

- Browse the directory
- Manage entries, such as users, groups, organizational units (OUs), and custom entries
- Manage ACI

Note that Red Hat provides this feature as an unsupported Technology Preview.

5.5. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 12.0.

Directory Server can import LDIF files only from /var/lib/dirsrv/slapd-*instance_name*/ldif/

The **dsconf backend import** command requires that you specify the path to the LDIF file you want to import. However, due to file system and SELinux permissions, as well as other operating system restrictions, Directory Server can only import LDIF files from the

/var/lib/dirsrv/slapd-*instance_name*/ldif/ directory. If the LDIF file is stored in a different directory, the import fails with an error similar to the following:

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

To work around this problem:

1. Move the file to the /var/lib/dirsrv/slapd-*instance_name*/ldif/ directory:

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

2. Set permissions that allow the **dirsrv** user to read the file:

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. Restore the SELinux context:

   ```
   # restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

Directory Server replication fails after changing password of the replication manager account

After a password change, Directory Server does not properly update the password cache for the replication agreement. As a consequence, when you change the password for the replication manager account, the replication breaks. To work around this problem, restart the Directory Server instance. As a result, the cache is rebuilt at start-up, and the replication connection binds with the new password instead of the old one.

Known issues in the 389-ds-base packages

Known issues in Red Hat Directory Server, that are included in the **389-ds-base** packages, are documented in the Red Hat Enterprise Linux 9.0 Release Notes:

- The **dsconf** utility has no option to create fix-up tasks for the **entryUUID** plug-in
- Configuring a referral for a suffix fails in Directory Server
- Directory Server terminates unexpectedly when started in referral mode

5.6. REMOVED FUNCTIONALITY

This section documents functionality that has been removed in Directory Server 12.0.

The nsslapd-subtree-rename-switch parameter has been removed

Previously, administrators could configure Directory Server to prevent moving entries between sub-trees in a database. Due to stability issues, this feature has been removed and, consequently, the **nsslapd-subtree-rename-switch** parameter no longer exists. As a result, moving entries between sub-trees can no longer be deactivated. As an alternative, if you require this feature, create an access control instruction (ACI).