



Red Hat Directory Server 11

Release Notes

Noteworthy features and updates related to Red Hat Directory Server 11 (11.9)

Red Hat Directory Server 11 Release Notes

Noteworthy features and updates related to Red Hat Directory Server 11 (11.9)

Legal Notice

Copyright © 2024 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

The release notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Directory Server 11 and document known issues in this release, as well as notable bug fixes, technology previews, deprecated functionalities, and other details.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	5
CHAPTER 1. GENERAL INFORMATION	6
1.1. DIRECTORY SERVER SUPPORT POLICY AND LIFE CYCLE	6
1.2. SYSTEM REQUIREMENTS	6
1.2.1. General hardware requirements	6
1.2.1.1. Disk space	6
1.2.1.2. Required RAM	6
1.2.2. Software requirements	7
1.2.2.1. Supported platforms for Directory Server	7
1.2.2.2. Supported platforms for the Directory Server user interface in the web console	7
1.2.2.3. Supported platforms for the Windows Synchronization utility	8
1.3. SOFTWARE CONFLICTS	8
1.4. NOTES ABOUT MIGRATING TO DIRECTORY SERVER 11	8
New command-line utilities in Directory Server 11	8
The Directory Server 11 default password storage scheme was changed to PBKDF2-SHA512	9
Migration procedure	9
CHAPTER 2. RED HAT DIRECTORY SERVER 11.9	10
2.1. IMPORTANT UPDATES AND NEW FEATURES	10
Directory Server rebased to version 1.4.3.39	10
Important updates and new features in the 389-ds-base package	10
2.2. BUG FIXES	10
The Directory Server web console no longer shows an exception while trying to display an entry with binary attribute in the LDAP Browser	10
The Directory Server web console no longer changes attribute names to lowercase characters when attributeTypes are added	10
The ns-slapd binary is now linked with the thread-safe libldap_r library, no longer causing segmentation fault	10
Directory Server now flushes the entry cache less frequently	10
Bug fixes in the 389-ds-base package	11
2.3. KNOWN ISSUES	11
Access log displays an error message during Directory Server installation in FIPS mode	11
Directory Server web console does not automatically update settings that are changed outside the web console	11
The dsconf utility does not compact the changelog	11
Configuring a referral for a suffix fails in Directory Server	12
CHAPTER 3. RED HAT DIRECTORY SERVER 11.8	13
3.1. IMPORTANT UPDATES AND NEW FEATURES	13
Directory Server rebased to version 1.4.3.37	13
Important updates and new features in the 389-ds-base packages	13
3.2. BUG FIXES	13
Directory Server now uses a backend suffix only if the suffix is defined	13
Directory Server no longer fails after the OS upgrade	13
RHDS healthcheck no longer reports misleading messages when the suffix is correctly defined	13
The cockpit-389-ds package upgrade now updates the 389-ds-base and python3-lib389 packages	13
The ds-replcheck now retrieves RUV data	14
The ns-slapd process no longer fails when you run the upgradednformat command	14
You can now select suffixes for export in the RHDS web console	14
A password change for the Directory Server replication manager account now works correctly	14
Bug fixes in the 389-ds-base package	14

3.3. KNOWN ISSUES	14
Access log displays an error message during Directory Server installation in FIPS mode	14
Directory Server web console does not automatically update settings that are changed outside the web console	15
The dsconf utility does not compact the changelog	15
Configuring a referral for a suffix fails in Directory Server	15
CHAPTER 4. RED HAT DIRECTORY SERVER 11.7	17
4.1. IMPORTANT UPDATES AND NEW FEATURES	17
Directory Server rebased to version 1.4.3.34	17
Important updates and new features in the 389-ds-base packages	17
4.2. BUG FIXES	17
The ns-slapd binary is now linked with the thread-safe libldap_r library, no longer causing segmentation fault	17
Directory Server now flushes the entry cache less frequently	17
Bug fixes in the 389-ds-base packages	17
4.3. KNOWN ISSUES	17
Access log displays an error message during Directory Server installation in FIPS mode	17
Directory Server settings that are changed outside the web console's window are not automatically visible	18
Configuring a referral for a suffix fails in Directory Server	18
Directory Server replication fails after changing password of the replication manager account	18
Known issues in the 389-ds-base package	19
CHAPTER 5. RED HAT DIRECTORY SERVER 11.6	20
5.1. HIGHLIGHTED UPDATES AND NEW FEATURES	20
Directory Server rebased to version 1.4.3.31	20
LDAP browser is now fully supported	20
Highlighted updates and new features in the 389-ds-base packages	20
5.2. KNOWN ISSUES	20
Directory Server settings that are changed outside the web console's window are not automatically visible	20
Configuring a referral for a suffix fails in Directory Server	20
Directory Server replication fails after changing password of the replication manager account	21
Known issues in the 389-ds-base packages	21
CHAPTER 6. RED HAT DIRECTORY SERVER 11.5	22
6.1. HIGHLIGHTED UPDATES AND NEW FEATURES	22
Directory Server rebased to version 1.4.3.28	22
Highlighted updates and new features in the 389-ds-base packages	22
6.2. TECHNOLOGY PREVIEWS	22
The Directory Server web console provides an LDAP browser as Technology Preview	22
Bug fixes in the 389-ds-base packages	22
6.3. KNOWN ISSUES	22
Directory Server settings that are changed outside the web console's window are not automatically visible	22
Configuring a referral for a suffix fails in Directory Server	23
Directory Server replication fails after changing password of the replication manager account	23
Known issues in the 389-ds-base packages	23
CHAPTER 7. RED HAT DIRECTORY SERVER 11.4	24
7.1. HIGHLIGHTED UPDATES AND NEW FEATURES	24
Directory Server rebased to version 1.4.3.27	24
Highlighted updates and new features in the 389-ds-base packages	24
7.2. BUG FIXES	24
The dsconf utility no longer fails when using LDAPS URLs	24
Bug fixes in the 389-ds-base packages	24

7.3. KNOWN ISSUES	25
Directory Server settings that are changed outside the web console's window are not automatically visible	25
The Directory Server Web Console does not provide an LDAP browser	25
Known issues in the 389-ds-base packages	25
CHAPTER 8. RED HAT DIRECTORY SERVER 11.3	26
8.1. HIGHLIGHTED UPDATES AND NEW FEATURES	26
Directory Server rebased to version 1.4.3.16	26
Highlighted updates and new features in the 389-ds-base packages	26
8.2. BUG FIXES	26
The lib389 library no longer fails to delete entries discovered by the Account object	26
Bug fixes in the 389-ds-base packages	26
8.3. KNOWN ISSUES	27
Directory Server settings that are changed outside the web console's window are not automatically visible	27
The Directory Server Web Console does not provide an LDAP browser	27
CHAPTER 9. RED HAT DIRECTORY SERVER 11.2	28
9.1. HIGHLIGHTED UPDATES AND NEW FEATURES	28
Directory Server rebased to version 1.4.3.8	28
Highlighted updates and new features in the 389-ds-base packages	28
9.2. BUG FIXES	28
Bug fixes in the 389-ds-base packages	28
9.3. KNOWN ISSUES	28
Directory Server settings that are changed outside the web console's window are not automatically visible	29
The Directory Server Web Console does not provide an LDAP browser	29
CHAPTER 10. RED HAT DIRECTORY SERVER 11.1	30
10.1. HIGHLIGHTED UPDATES AND NEW FEATURES	30
Directory Server rebased to version 1.4.2.4	30
A health check feature has been added to Directory Server	30
Highlighted updates and new features in the 389-ds-base packages	30
10.2. BUG FIXES	30
Bug fixes in the 389-ds-base packages	30
10.3. KNOWN ISSUES	30
Directory Server settings that are changed outside the web console's window are not automatically visible	30
The Directory Server Web Console does not provide an LDAP browser	31
Known issues in the 389-ds-base packages	31
10.4. REMOVED FUNCTIONALITY	31
The nunc-stans framework has been removed	31
CHAPTER 11. RED HAT DIRECTORY SERVER 11.0	32
11.1. HIGHLIGHTED UPDATES AND NEW FEATURES	32
Directory Server introduces new command-line utilities to manage instances	32
Directory Server now provides a browser-based user interface	32
The default value of the nsslapd-unhashed-pw-switch parameter is now off	32
Highlighted updates and new features in the 389-ds-base packages	33
11.2. KNOWN ISSUES	33
Directory Server settings that are changed outside the web console's window are not automatically visible	33
The Directory Server Web Console does not provide an LDAP browser	33

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

CHAPTER 1. GENERAL INFORMATION

This chapter contains general information about Red Hat Directory Server 11, independent of the minor version.

1.1. DIRECTORY SERVER SUPPORT POLICY AND LIFE CYCLE

For details, see the [Red Hat Directory Server Errata Support Policy](#) document.

1.2. SYSTEM REQUIREMENTS

1.2.1. 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.

1.2.1.1. Disk space

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

Table 1.1. 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.

1.2.1.2. 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 1.2. 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.

1.2.2. Software requirements

Learn about required platforms for Directory Server packages, the web console, and windows synchronization.

1.2.2.1. Supported platforms for Directory Server

Red Hat supports Directory Server {DSVERSTRING} if it runs on the following platforms:

- A Red Hat Enterprise Linux {RHELVER} built for AMD and Intel 64-bit 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.

1.2.2.2. 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
------------------	---------

Operating system	Browser
Red Hat Enterprise Linux {RHELVER}	<ul style="list-style-type: none"> ● Mozilla Firefox 115 and later ● Chrome 88 and later
Windows Server 2016 and 2019	<ul style="list-style-type: none"> ● Mozilla Firefox 115 and later ● Chrome 88 and later
Windows 10 and 11	<ul style="list-style-type: none"> ● Mozilla Firefox 115 and later ● Microsoft Edge 88 and later ● Chrome 88 and later

1.2.2.3. 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

1.3. SOFTWARE CONFLICTS

Directory Server cannot be installed on any 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.

1.4. NOTES ABOUT MIGRATING TO DIRECTORY SERVER 11

Consider the following information if you want to migrate an existing Directory Server 10 environment to Directory Server 11.

New command-line utilities in Directory Server 11

Directory Server 11 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 11, 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.

The Directory Server 11 default password storage scheme was changed to PBKDF2-SHA512

Directory Server 11 now 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**.

Migration procedure

For a procedure about migrating Directory Server 10 to Directory Server 11, see the corresponding chapter in the [Red Hat Directory Server Installation Guide](#).

CHAPTER 2. RED HAT DIRECTORY SERVER 11.9

Learn about new updates and new features, bug fixes, and known issues implemented in Directory Server 11.9.

2.1. IMPORTANT UPDATES AND NEW FEATURES

Learn about new features and important updates in Directory Server 11.9.

Directory Server rebased to version 1.4.3.39

The **389-ds-base** package has been upgraded to upstream version 1.4.3.39.

Important updates and new features in the **389-ds-base** package

The Red Hat Directory Server features that are included in the **389-ds-base** package are documented in the Red Hat Enterprise Linux 8.10 Release Notes:

- [The HAProxy protocol is now supported for the **389-ds-base** package](#)

2.2. BUG FIXES

Learn about bugs fixed in Directory Server 11.9 that have a significant impact on users.

The Directory Server web console no longer shows an exception while trying to display an entry with binary attribute in the LDAP Browser

Previously, when an LDAP entry contained a binary attribute, such as **jpegPhoto**, **userCertificate**, the web console displayed an exception when you wanted to see the entry details in the **LDAP Browser**. With this update, the web console handles entries with binary attributes correctly and the exception no longer appears.

(BZ#2239787)

The Directory Server web console no longer changes attribute names to lowercase characters when attributeTypes are added

Previously, when you added an attribute to an object class by using the web console, the uppercase characters in the attribute name were changed to lowercase characters. With this update, the attribute name case is no longer changed.

(BZ#2257790)

The **ns-slapd** binary is now linked with the thread-safe **libldap_r** library, no longer causing segmentation fault

An upstream change in the build system introduced a regression by linking the **ns-slapd** binary with the non thread-safe **libldap** library instead of the thread-safe **libldap_r**. Consequently, the **ns-slapd** process could fail with a segmentation fault. This update fixes the problem with the build system code and the **ns-slapd** binary is now linked back with the thread-safe **libldap_r** library. As a result, the segmentation fault no longer occurs.

(BZ#2264534)

Directory Server now flushes the entry cache less frequently

Previously, Directory Server flushed its entry cache even when it was not necessary. As a result, in certain situations, Directory Server was unresponsive and had bad performance. With this update, Directory Server flushes the entry cache only when it is necessary.

(2268177)

Bug fixes in the 389-ds-base package

The Red Hat Directory Server bug fixes that are included in the **389-ds-base** package are documented in the Red Hat Enterprise Linux 8.10 Release Notes:

- SELinux labeling for **dirsrv** files was moved to DEBUG log level
- Directory Server no longer causes a segmentation fault when a backend is configured without a related suffix
- Directory Server no longer fails after abandoning the paged result search
- Directory Server now starts correctly after an upgrade if you configured a custom value for the connection table size
- Directory Server no longer fails when Content Synchronization plug-in is enabled dynamically

2.3. KNOWN ISSUES

Learn about known problems and, if applicable, workarounds in Directory Server 11.9.

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)

Directory Server web console does not automatically update settings that are changed outside the web console

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if you change the configuration outside of the console window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console window.

(BZ#1654281)

The **dsconf** utility does not compact the changelog

Currently, the **dsconf** utility does not compact the replication changelog when you run the **dsconf backend compact-db --only-changelog** command.

To work around this problem, run the **COMPACT_CL5** task manually:

```
$ ldapmodify -x -D "cn=Directory Manager" -W -H ldap://server.example.com
```

```
dn: cn=replica,cn=suffix_name,cn=mapping tree,cn=config
changetype: modify
replace: nsds5task
nsds5task: COMPACT_CL5
```

```
modifying entry "cn=replica,cn=suffix_name,cn=mapping tree,cn=config"
```

(BZ#2245042)

Configuring a referral for a suffix fails in Directory Server

If you set a back-end referral in Directory Server, setting the state of the backend using the **dsconf** **<instance_name> backend suffix set --state referral** command fails with the following error:

```
Error: 103 - 9 - 53 - Server is unwilling to perform - [] - need to set nsslapd-referral before moving to referral state
```

As a consequence, configuring a referral for suffixes fails. To work around the problem:

1. Set the **nsslapd-referral** parameter manually:

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

```
dn: cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
changetype: modify
add: nsslapd-referral
nsslapd-referral: ldap://remote_server:389/dc=example,dc=com
```

2. Set the back-end state:

```
# dsconf <instance_name> backend suffix set --state referral
```

As a result, with the workaround, you can configure a referral for a suffix.

(BZ#2063033)

CHAPTER 3. RED HAT DIRECTORY SERVER 11.8

Learn about new updates and new features, known issues, and deprecated functionality implemented in Directory Server 11.8.

3.1. IMPORTANT UPDATES AND NEW FEATURES

Learn about new features and important updates in Directory Server 11.8.

Directory Server rebased to version 1.4.3.37

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.37.

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

The Red Hat Directory Server features that are included in the **389-ds-base** packages are documented in the Red Hat Enterprise Linux 8.9 Release Notes:

- New **passwordAdminSkipInfoUpdate: on/off** configuration option is now available

3.2. BUG FIXES

Learn about bugs fixed in Directory Server 11.8 that have a significant impact on users.

Directory Server now uses a backend suffix only if the suffix is defined

Previously, if a backend configuration entry was not associated with a suffix, the server failed at startup. With this update, Directory Server uses a suffix of a backend only if the suffix is defined. As a result, the server no longer fails at startup.

(BZ#2246307)

Directory Server no longer fails after the OS upgrade

Previously, when the **nsslapd-conntablesizes** was present in the **/etc/dirsrv/slapped-*instance_name*/dse.ldif** file, Directory Server failed to start after the operating system (OS) upgrade. As a result, you had to remove the **nsslapd-conntablesizes** setting from the **dse.ldif** file before starting the server. With this update, the custom configuration of the connection table size works as expected and Directory Server no longer fails at start.

(BZ#2245946)

RHDS healthcheck no longer reports misleading messages when the suffix is correctly defined

Previously, when you defined a suffix using mixed case or upper case for the **nsslapd-backend** and **nsslapd-directory** attributes, the **dsctl healthcheck** command could report misleading error messages, despite the suffix being correctly defined. With this update, the **dsctl healthcheck** command no longer reports error messages about the suffix defined using mixed case or upper case.

(BZ#2215296)

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. 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 upgrades **389-ds-base** and **python3-lib389** packages.

(BZ#22245690)

The **ds-replcheck** now retrieves RUV data

Previously, the **ds-replcheck** tool reported an error that a supplier had no Replica Update Vector (RUV) entry, even though a direct search on the replica configuration entry showed the RUV data. With this update, the **ds-replcheck** tool now provides the replication state that indicates if the replication is not fully initialized.

(BZ#2211690)

The **ns-slapd** process no longer fails when you run the **upgradednformat** command

Previously, when you upgraded the DN format with the **upgradednformat** command, the **upgradednformat** command failed, leading to a problem with disk space. With this update, **upgradednformat** works as expected.

(BZ#2172258)

You can now select suffixes for export in the RHDS web console

Previously, when you attempted to select a suffix to export in the **Database → Backups & LDIFs → LDIFs → Create LDIF**, only the first suffix in the drop-down list was available. With this update, you can select the suffix to export.

(BZ#2219559)

A password change for the Directory Server replication manager account now works correctly

Previously, after a password change, Directory Server did not properly update the password cache for the replication agreement. As a consequence, when you changed the password for the replication manager account, the replication failed. With this update, Directory Server updates the cache properly and, as a result, the replication works as expected.

(BZ#2101473)

Bug fixes in the **389-ds-base** package

The Red Hat Directory Server bug fixes that are included in the **389-ds-base** package are documented in the Red Hat Enterprise Linux 8.9 Release Notes:

- [Changing a security parameter now works correctly in Directory Server](#)
- [Directory Server now calculates the **dtablesiz**e based on the maximum number of opened descriptors](#)
- [The **dsctl healthcheck** command now uses the password storage scheme **PBKDF2-SHA512** by default](#)
- [Paged searches from a regular user now do not impact performance](#)
- [You can now enable and disable ciphers in Directory Server as expected](#)

3.3. KNOWN ISSUES

Learn about known problems and, if applicable, workarounds in Directory Server 11.8.

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)

Directory Server web console does not automatically update settings that are changed outside the web console

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console window.

(BZ#1654281)

The **dsconf** utility does not compact the changelog

Currently, the **dsconf** utility does not compact the replication changelog when you run the **dsconf backend compact-db --only-changelog** command.

To work around this problem, run the **COMPACT_CL5** task manually:

```
$ ldapmodify -x -D "cn=Directory Manager" -W -H ldap://server.example.com

dn: cn=replica,cn=suffix_name,cn=mapping tree,cn=config
changetype: modify
replace: nsds5task
nsds5task: COMPACT_CL5

modifying entry "cn=replica,cn=suffix_name,cn=mapping tree,cn=config"
```

(BZ#2245042)

Configuring a referral for a suffix fails in Directory Server

If you set a back-end referral in Directory Server, setting the state of the backend using the **dsconf <instance_name> backend suffix set --state referral** command fails with the following error:

```
Error: 103 - 9 - 53 - Server is unwilling to perform - [] - need to set nsslapd-referral before moving to
referral state
```

As a consequence, configuring a referral for suffixes fail. To work around the problem:

1. Set the **nsslapd-referral** parameter manually:

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

dn: cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
```

```
changetype: modify
add: nsslapd-referral
nsslapd-referral: ldap://remote_server:389/dc=example,dc=com
```

2. Set the back-end state:

```
# dsconf <instance_name> backend suffix set --state referral
```

As a result, with the workaround, you can configure a referral for a suffix.

(BZ#2063033)

CHAPTER 4. RED HAT DIRECTORY SERVER 11.7

Learn about new system requirements, updates and new features, known issues, and deprecated functionality implemented in Directory Server 11.7.

4.1. IMPORTANT UPDATES AND NEW FEATURES

Learn about new features and important updates in Directory Server 11.7.

Directory Server rebased to version 1.4.3.34

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.34.

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

The Red Hat Directory Server features that are included in the **389-ds-base** packages are documented in the Red Hat Enterprise Linux 8.8 Release Notes:

- New [nsslapd-auditlog-display-attrs](#) configuration parameter for the Directory Server audit log
- Directory server now supports ECDSA private keys for TLS
- New [pamModuleIsThreadSafe](#) configuration option is now available

4.2. BUG FIXES

Learn about bugs fixed in Directory Server 11.7 that have a significant impact on users.

The **ns-slapd** binary is now linked with the thread-safe **libldap_r** library, no longer causing segmentation fault

An upstream change in the build system introduced a regression by linking the **ns-slapd** binary with the non thread-safe **libldap** library instead of the thread-safe **libldap_r**. Consequently, the **ns-slapd** process could fail with a segmentation fault. This update fixes the problem with the build system code and the **ns-slapd** binary is now linked back with the thread-safe **libldap_r** library. As a result, the segmentation fault no longer occurs.

(BZ#2268138)

Directory Server now flushes the entry cache less frequently

Previously, Directory Server flushed its entry cache even when it was not necessary. As a result, in certain situations, Directory Server was unresponsive and had bad performance. With this update, Directory Server flushes the entry cache only when it is necessary.

(BZ#2268136)

Bug fixes in the **389-ds-base** packages

The Red Hat Directory Server bug fixes that are included in the **389-ds-base** packages are documented in the Red Hat Enterprise Linux 8.8 Release Notes:

- [The scheduled time of the changelog compaction now works correctly](#)

4.3. KNOWN ISSUES

Learn about known problems and, if applicable, workarounds in Directory Server 11.7.

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)

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

(BZ#1654281)

Configuring a referral for a suffix fails in Directory Server

If you set a back-end referral in Directory Server, setting the state of the backend using the **dsconf <instance_name> backend suffix set --state referral** command fails with the following error:

```
Error: 103 - 9 - 53 - Server is unwilling to perform - [] - need to set nsslapd-referral before moving to
referral state
```

As a consequence, configuring a referral for suffixes fail. To work around the problem:

1. Set the **nsslapd-referral** parameter manually:

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

dn: cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
changetype: modify
add: nsslapd-referral
nsslapd-referral: ldap://remote_server:389/dc=example,dc=com
```

2. Set the back-end state:

```
# dsconf <instance_name> backend suffix set --state referral
```

As a result, with the workaround, you can configure a referral for a suffix.

(BZ#2063033)

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#2101473)

Known issues in the **389-ds-base** package

Red Hat Directory Server known issues that affect **389-ds-base** package are documented in Red Hat Enterprise Linux 8.8 8.8 Release Notes:

- The **default** keyword for enabled ciphers in the NSS does not work in conjunction with other ciphers (BZ#1817505)

CHAPTER 5. RED HAT DIRECTORY SERVER 11.6

Learn about new system requirements, highlighted updates and new features, known issues, and deprecated functionality implemented in Directory Server 11.6.

5.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.6.

Directory Server rebased to version 1.4.3.31

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.31.

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 8.7 Release Notes:

- [Directory Server now supports canceling the Auto Membership plug-in task](#)
- [Directory Server now supports recursive delete operations when using `ldapdelete`](#)
- [You can now set basic replication options during the Directory Server installation](#)
- [Replication changelog trimming is now enabled by default in Directory Server](#)

5.2. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.6.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

(BZ#1654281)

Configuring a referral for a suffix fails in Directory Server

If you set a back-end referral in Directory Server, setting the state of the backend using the **dsconf** `<instance_name> backend suffix set --state referral` command fails with the following error:

```
Error: 103 - 9 - 53 - Server is unwilling to perform - [] - need to set nsslapd-referral before moving to referral state
```

As a consequence, configuring a referral for suffixes fail. To work around the problem:

1. Set the **nsslapd-referral** parameter manually:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com
dn: cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
changetype: modify
add: nsslapd-referral
nsslapd-referral: ldap://remote_server:389/dc=example,dc=com
```

2. Set the back-end state:

```
# dsconf <instance_name> backend suffix set --state referral
```

As a result, with the workaround, you can configure a referral for a suffix.

(BZ#2063140)

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#2101473)

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 8.7 Release Notes:

- [The **default** keyword for enabled ciphers in the NSS does not work in conjunction with other ciphers \(BZ#1817505\)](#)

CHAPTER 6. RED HAT DIRECTORY SERVER 11.5

6.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.5.

Directory Server rebased to version 1.4.3.28

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.28 which provides a number of bug fixes and enhancements over the previous version:

- A potential deadlock in replicas has been fixed.
- The server no longer terminates unexpectedly when the **dnalInterval** is set to **0**.
- The performance of connection handling has been improved.
- Improved performance of **targetfilter** in access control instructions (ACI).

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 8.6 Release Notes:

- [Directory Server now stores memory-mapped files of databases on a tmpfs file system](#)

6.2. TECHNOLOGY PREVIEWS

This section documents unsupported Technology Previews in Directory Server 11.5.

The Directory Server web console provides an LDAP browser as 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.

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 8.6 Release Notes:

- [Authenticating to Directory Server in FIPS mode with PBKDF2-hashed passwords now works as expected](#)

6.3. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.5.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console,

the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

Configuring a referral for a suffix fails in Directory Server

If you set a back-end referral in Directory Server, setting the state of the backend using the **dsconf <instance_name> backend suffix set --state referral** command fails with the following error:

```
Error: 103 - 9 - 53 - Server is unwilling to perform - [] - need to set nsslapd-referral before moving to referral state
```

As a consequence, configuring a referral for suffixes fail. To work around the problem:

1. Set the **nsslapd-referral** parameter manually:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com
dn: cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
changetype: modify
add: nsslapd-referral
nsslapd-referral: ldap://remote_server:389/dc=example,dc=com
```

2. Set the back-end state:

```
# dsconf <instance_name> backend suffix set --state referral
```

As a result, with the workaround, you can configure a referral for a suffix.

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 8.6 Release Notes:

- [The **default** keyword for enabled ciphers in the NSS does not work in conjunction with other ciphers](#)

CHAPTER 7. RED HAT DIRECTORY SERVER 11.4

7.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.4.

Directory Server rebased to version 1.4.3.27

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.27, 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-1-4-3-24.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-23.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-22.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-21.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-20.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-19.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-18.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-3-17.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 8.5 Release Notes:

- Directory Server now supports temporary passwords
- Directory Server supports the **entryUUID** attribute
- The **dnalInterval** configuration attribute is now supported
- Directory Server can exclude attributes and suffixes from the retro changelog database
- Directory Server provides monitoring settings that can prevent database corruption caused by lock exhaustion
- Added a new message to help set up **nsSSLPersonalitySSL**

7.2. BUG FIXES

This section describes bugs fixed in Directory Server 11.4 that have a significant impact on users.

The **dsconf** utility no longer fails when using LDAPS URLs

Previously, the **dsconf** utility did not correctly resolve TLS settings for remote connections. As a consequence, even if the certificate configuration was correct, using **dsconf** with a remote LDAPS URL failed with an **certificate verify failed** error. The **dsconf** connection code has been fixed. As a result, using remote LDAPS URLs with **dsconf** now works as expected.

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 8.5 Release Notes:

- [The database indexes created by plug-ins are now enabled](#)
- [The replication session update speed is now enhanced](#)

7.3. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.4.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

The Directory Server Web Console does not provide an LDAP browser

The web console enables administrators to manage and configure Directory Server 11 instances. However, it does not provide an integrated LDAP browser. To manage users and groups in Directory Server, use the **dsidm** utility. To display and modify directory entries, use a third-party LDAP browser or the OpenLDAP client utilities provided by the **openldap-clients** package.

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 8.5 Release Notes:

- [The **default** keyword for enabled ciphers in the NSS does not work in conjunction with other ciphers](#)

CHAPTER 8. RED HAT DIRECTORY SERVER 11.3

8.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.3.

Directory Server rebased to version 1.4.3.16

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.16, 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://www.port389.org/docs/389ds/releases/release-1-4-3-16.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-15.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-14.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-13.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-12.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-11.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-10.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-9.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 8.4 Release Notes:

- Directory Server can now reject internal unindexed searches
- Directory Server supports setting replication agreement bootstrap credentials
- The `dsidm` utility supports renaming and moving entries
- Directory Server now logs the work and operation time in **RESULT** entries
- The default value of **nsslapd-nagle** has been turned off to increase the throughput

8.2. BUG FIXES

This section describes bugs fixed in Directory Server 11.3 that have a significant impact on users.

The **lib389** library no longer fails to delete entries discovered by the **Account** object

Previously, the **_protected** flag of the **Account** object in the **lib389** Directory Server library was enabled. As a consequence, **delete** operations failed. This update sets the flag to **False**. As a result, the library no longer fails if you delete or rename entries discovered by the **Account** object.

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 8.4 Release Notes:

- Creating replication agreements with certificate-based authentication now works as expected

8.3. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.3.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

The Directory Server Web Console does not provide an LDAP browser

The web console enables administrators to manage and configure Directory Server 11 instances. However, it does not provide an integrated LDAP browser. To manage users and groups in Directory Server, use the **dsidm** utility. To display and modify directory entries, use a third-party LDAP browser or the OpenLDAP client utilities provided by the **openldap-clients** package.

CHAPTER 9. RED HAT DIRECTORY SERVER 11.2

9.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.2.

Directory Server rebased to version 1.4.3.8

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.8, 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://www.port389.org/docs/389ds/releases/release-1-4-3-8.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-7.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-6.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-5.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-4.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-3.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-2.html>
- <https://www.port389.org/docs/389ds/releases/release-1-4-3-1.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 8.3 Release Notes:

- Directory Server exports the private key and certificate to a private name space when the service starts
- Directory Server now supports the `pwdReset` operation attribute
- Directory Server can now turn an instance to read-only mode if the disk monitoring threshold is reached
- Directory Server now logs the work and operation time in `RESULT` entries

9.2. BUG FIXES

This section describes bugs fixed in Directory Server 11.2 that have a significant impact on users.

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 8.3 Release Notes:

- Directory Server no longer leaks memory when using indirect COS definitions

9.3. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.2.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

The Directory Server Web Console does not provide an LDAP browser

The web console enables administrators to manage and configure Directory Server 11 instances. However, it does not provide an integrated LDAP browser. To manage users and groups in Directory Server, use the **dsidm** utility. To display and modify directory entries, use a third-party LDAP browser or the OpenLDAP client utilities provided by the **openldap-clients** package.

CHAPTER 10. RED HAT DIRECTORY SERVER 11.1

10.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.1.

Directory Server rebased to version 1.4.2.4

The **389-ds-base** packages have been upgraded to upstream version 1.4.2.4, 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-1-4-2-4.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-3.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-2.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-1.html>

A health check feature has been added to Directory Server

This enhancement adds a health check feature to Directory Server. The **dsctl healthcheck** command performs read-only operations on a Directory Server instance and reports, for example, if the instance is configured properly or if replication agreements are working correctly.

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 8.2 Release Notes:

- [Certain legacy scripts have been replaced in Directory Server](#)
- [Directory Server sets the sslVersionMin parameter based on the system-wide crypto policy](#)

10.2. BUG FIXES

This section describes bugs fixed in Directory Server 11.1 that have a significant impact on users.

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 8.2 Release Notes:

- [Directory Server instance names can now have up to 103 characters](#)
- [The dsctl utility no longer fails to manage instances with a hyphen in their name](#)

10.3. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.1.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This

applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

The Directory Server Web Console does not provide an LDAP browser

The web console enables administrators to manage and configure Directory Server 11 instances. However, it does not provide an integrated LDAP browser. To manage users and groups in Directory Server, use the **dsidm** utility. To display and modify directory entries, use a third-party LDAP browser or the OpenLDAP client utilities provided by the **openldap-clients** package.

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 8.2 Release Notes:

- [Directory Server warns about missing attributes in the schema if those attributes are used in a search filter](#)

10.4. REMOVED FUNCTIONALITY

This section documents features that have been removed from Directory Server 11.1.

The nunc-stans framework has been removed

The **nunc-stans** framework has been removed from Directory Server, and the server now uses the improved core connection handling mechanism in Directory Server.

If you previously enabled the framework manually, Directory Server logs the following warning:

```
WARN - slapd_daemon - cn=config: nsslapd-enable-nunc-stans is on. nunc-stans has been
depreciated and this flag is now ignored.
WARN - slapd_daemon - cn=config: nsslapd-enable-nunc-stans should be set to off or deleted from
cn=config.
```

To prevent Directory Server from logging this warning, remove the **nsslapd-enable-nunc-stans** from the **cn=config** entry:

```
$ ldapmodify -D "cn=Directory Manager" -W -p 389 -h server.example.com -x
dn: cn=config
changetype: modify
delete: nsslapd-enable-nunc-stans
```

CHAPTER 11. RED HAT DIRECTORY SERVER 11.0

11.1. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 11.0.

Directory Server introduces new command-line utilities to manage instances

Red Hat Directory Server 11.0 introduces the **dscreate**, **dsconf**, and **dsctl** utilities. These utilities simplify managing Directory Server using the command line. For example, you can now use a command with parameters to configure a feature instead of sending complex LDIF statements to the server.

The following is an overview of the purpose of each utility:

- Use the **dscreate** utility to create new Directory Server instances using the interactive mode or an INF file. Note that the INF file format is different from the one the installer used in previous Directory Server versions.
- Use the **dsconf** utility to manage Directory Server instances during run time. For example, use **dsconf** to:
 - Configure settings in the **cn=config** entry
 - Configure plug-ins
 - Configure replication
 - Back up and restore an instance
- Use the **dsctl** utility to manage Directory Server instances while they are offline. For example, use **dsctl** to:
 - Start and stop an instance
 - Re-index the server database
 - Back up and restore an instance

These utilities replace the Perl and shell scripts marked as deprecated in Directory Server 10. The scripts are still available in the unsupported **389-ds-base-legacy-tools** package, however Red Hat only supports managing Directory Server using the new utilities.

Note that configuring Directory Server using LDIF statements is still supported, but Red Hat recommends using the utilities.

For further details about using the utilities, see the [Red Hat Directory Server 11 Documentation](#) .

Directory Server now provides a browser-based user interface

This enhancement adds a browser-based interface to Red Hat Directory Server that replaces the Java-based Console used in previous versions. As a result, administrators can now use the Red Hat Enterprise Linux web console to manage Directory Server instances using a browser.

For further details, see the [Red Hat Directory Server 11 Documentation](#) .

Note that the browser-based user interface does not contain an LDAP browser.

The default value of the `nsslapd-unhashed-pw-switch` parameter is now `off`

In certain situations, for example when synchronizing passwords with Active Directory (AD), a Directory Server plug-in must store the unencrypted password on the hard disk. The **nsslapd-unhashed-pw-switch** configuration parameter determines whether and how Directory Server stores unencrypted passwords. To improve the security in scenarios that do not require plug-ins to store unencrypted passwords, the default value of the **nsslapd-unhashed-pw-switch** parameter has been changed in Directory Server 11.0 from **on** to **off**.

If you want to configure password synchronization with AD, manually enable **nsslapd-unhashed-pw-switch** on the Directory Server instance that has the Windows synchronization agreement configured:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-unhashed-pw-switch=on
```

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 8.1 Release Notes:

- [New password syntax checks in Directory Server](#)
- [Directory Server now provides improved internal operations logging support](#)

11.2. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 11.0.

Directory Server settings that are changed outside the web console's window are not automatically visible

Because of the design of the Directory Server module in the Red Hat Enterprise Linux 8 web console, the web console does not automatically display the latest settings if a user changes the configuration outside of the console's window. For example, if you change the configuration using the command line while the web console is open, the new settings are not automatically updated in the web console. This applies also if you change the configuration using the web console on a different computer. To work around the problem, manually refresh the web console in the browser if the configuration has been changed outside the console's window.

The Directory Server Web Console does not provide an LDAP browser

The web console enables administrators to manage and configure Directory Server 11 instances. However, it does not provide an integrated LDAP browser. To manage users and groups in Directory Server, use the **dsidm** utility. To display and modify directory entries, use a third-party LDAP browser or the OpenLDAP client utilities provided by the **openldap-clients** package.