Red Hat Directory Server 10

Release Notes

Highlighted features and updates related to Red Hat Directory Server 10 (10.0 - 10.4)

Last Updated: 2019-08-07

Red Hat Directory Server 10 Release Notes

Highlighted features and updates related to Red Hat Directory Server 10 (10.0 - 10.4)

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

Petr Bokoč
Red Hat Customer Content Services

Tomáš Čapek
Red Hat Customer Content Services

Legal Notice

Abstract

This document describes all highlighted features, bug fixes, and known issues in Red Hat Directory Server 10.

Table of Contents

CHAPTER 1. SOFTWARE CONFLICTS

Directory Server cannot be installed on any system that has a Red Hat Enterprise Linux Identity Management server (also called *IPA server*) installed. Likewise, no Red Hat Enterprise Linux Identity Management server can be installed on a system with a Directory Server instance.

CHAPTER 2. DIRECTORY SERVER 10.4

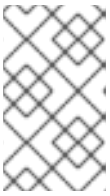
2.1. SYSTEM REQUIREMENTS

This section contains information related to installing and upgrading to Directory Server 10.4, including prerequisites and platform requirements.

2.1.1. Supported Platforms for Directory Server

Red Hat supports Directory Server 10.4 on the following platforms:

- Red Hat Enterprise Linux 7.7 or later



NOTE

Directory Server 10.4 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.

2.1.2. Supported Platforms for Directory Server Console

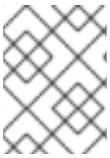
Red Hat supports running the Directory Server Console on the following platforms:

- Red Hat Enterprise Linux 7.7 or later
- Microsoft Windows Server 2016
- Microsoft Windows 10 (64-bit)

2.1.2.1. Required Java Runtime Environment

The Directory Server Console requires one of the following Java Runtime Environments:

- OpenJDK 1.8.0 for Red Hat Enterprise Linux
- Oracle Java Runtime Environment (JRE) 8
- Oracle Java Runtime Environment (JRE) 9



NOTE

To run Red Hat Directory Server Console on Microsoft Windows, you must install a 64-bit JRE.

2.1.3. Supported Platforms for Windows Synchronization Utility

The Windows Synchronization utility for Directory Server 10.4 is supported for:

- Active Directory on Microsoft Windows Server 2016

2.1.4. Web Application Browser Support

Directory Server 10.4 supports for web-based interfaces, such as Admin Express and online help tools:

- Mozilla Firefox ESR 60 and later

2.2. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 10.4:

Directory Server rebased to version 1.3.9.1

The 389-ds-base packages have been upgraded to upstream version 1.3.9.1, 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-1-3-9-0.html

Highlighted Updates and New Features in the 389-ds-base Package

Features in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.7 Release Notes:

- The ***replicaLastUpdateStatusJSON*** status attribute has been added to replication agreements
- The Auto Membership plug-in can now be additionally invoked by modify operations

2.3. BUG FIXES

This section describes bugs fixed in Directory Server 10.4 that have a significant impact on users:

Bug Fixes in the 389-ds-base Package

Bug fixes in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.7 Release Notes:

- Directory Server now updates the ***pwdLastSet*** field of a user on password changes
- Searches with scope **one** no longer return incomplete results
- Directory Server no longer truncates ***nsSSL3Ciphers*** values longer than 1023 characters
- Directory Server now correctly rejects the current password if ***passwordInHistory*** is set to **0**
- Directory Server no longer uses the CoS attribute with a higher priority than the real attribute
- Directory Server no longer crashes when shutting down the service while a **cleanAllRUV** task is running
- Directory Server flushes the entry cache after a back end transaction plug-in failed
- The **ds-replcheck** utility no longer incorrectly reports non-matching tombstone entries on replicas
- Directory Server did not return the ***shadowWarning*** attribute if ***passwordWarning*** was set lower than **86400**
- The time after which Directory Server deletes tasks has been changed
- Directory Server no longer ignores IPv6 addresses in an ACI if both IPv6 and IPv4 addresses are used
- Replicating **modrdn** operations to read-only instances now succeeds

2.4. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 10.4:

Admin Server does not support TLS 1.3

Directory Server uses the Apache web server with the **mod_nss** module to provide the Admin Server service. In Red Hat Enterprise Linux 7.7, this module does not support the TLS 1.3 protocol. As a consequence, you cannot configure the Directory Server Admin Server to use this protocol version. The latest TLS version **mod_nss** supports is 1.2.

Previously Unresolved Known Issues in Red Hat Directory Server 10.4

- The Directory Server Console is not able to connect to all instances in multi-homed environments
- Directory Server Console logins fail using the **uid** value
- Stopping and starting a remote Admin Server fails when SELinux is enabled

2.5. DEPRECATED FUNCTIONALITY

This section describes deprecated functionality in Directory Server 10.4:

The Perl and shell scripts for Directory Server have been deprecated

The Perl and shell scripts, which are provided by the 389-ds-base package, have been deprecated. The scripts will be replaced by new utilities in the next major release of Red Hat Directory Server.

The *Shell Scripts* and *Perl Scripts* sections in the *Red Hat Directory Server Command, Configuration, and File Reference* have been updated. The descriptions of affected scripts contain now a note that they are deprecated.

The Directory Server Console has been deprecated

The Java-based Directory Server Console has been deprecated and will be replaced in the next major release of Red Hat Directory Server.

CHAPTER 3. DIRECTORY SERVER 10.3

3.1. SYSTEM REQUIREMENTS

This section contains information related to installing and upgrading to Directory Server 10.3, including prerequisites and platform requirements.

3.1.1. Supported Platforms for Directory Server

Red Hat supports Directory Server 10.3 on the following platforms:

- Red Hat Enterprise Linux 7.6 or later

NOTE

Directory Server 10.3 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.

3.1.2. Supported Platforms for Directory Server Console

Red Hat supports running the Directory Server Console on the following platforms:

- Red Hat Enterprise Linux 7.6 or later
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 (64-bit)
- Microsoft Windows 8.1 (64-bit)

3.1.2.1. Required Java Runtime Environment

The Directory Server Console requires one of the following Java Runtime Environments:

- OpenJDK 1.8.0 for Red Hat Enterprise Linux
- Oracle Java Runtime Environment (JRE) 8
- Oracle Java Runtime Environment (JRE) 9

NOTE

To run Red Hat Directory Server Console on Microsoft Windows, you must install a 64-bit JRE.

3.1.3. Supported Platforms for Windows Synchronization Utility

The Windows Synchronization utility for Directory Server 10.3 is supported for:

- Active Directory on Microsoft Windows Server 2016

- Active Directory on Microsoft Windows Server 2012 R2

3.1.4. Web Application Browser Support

Directory Server 10.3 supports for web-based interfaces, such as Admin Express and online help tools:

- Mozilla Firefox ESR 60 and later

3.2. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 10.3:

Directory Server rebased to version 1.3.8.4
The 389-ds-base packages have been upgraded to upstream version 1.3.8.4, 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:

- http://directory.fedoraproject.org/docs/389ds/releases/release-1-3-8-4.html

3.3. BUG FIXES

This section describes bugs fixed in Directory Server 10.3 that have a significant impact on users:

Bug Fixes in the 389-ds-base Package
Bug fixes in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.6 Release Notes:

- Directory Server correctly generates the CSN
- Directory Server now supports certificates with all ciphers supported by NSS
- Directory Server clients are no longer randomly restricted by anonymous resource limits
- Thread processing in Directory Server has been serialized
- Deleting the ***memberOf*** attribute in Directory Server works correctly
- The **PBKDF2_SHA256** password storage scheme can now be used in Directory Server
- Creating a Directory Server back end with the name **default** is now supported
- The Directory Server **Pass-through** plug-in now supports encrypted connections using the **STARTTLS** command
- Updated Directory Server SNMP MIB definitions
- Using the password policy feature works correctly if **chain on update** is enabled
- Directory Server now retrieves members of the replica bind DN group when the first session is started
- The Disk Monitoring feature shuts down Directory Server on low disk space
- Directory Server no longer logs a warning when searching a non-existent DN in ***entrydn*** attributes

- The **pwdhash** utility no longer crashes when using the ***CRYPT*** password storage scheme
- Directory Server no longer crashes when removing connections from an active list
- Improved performance when the fine-grained password policy is enabled in Directory Server
- The default of the ***nsslapd-enable-nunc-stans*** parameter has been changed to **off**

3.4. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 10.3:

Previously Unresolved Known Issues in Red Hat Directory Server 10.3

- The Directory Server Console is not able to connect to all instances in multi-homed environments
- Directory Server Console logins fail using the **uid** value
- Stopping and starting a remote Admin Server fails when SELinux is enabled

3.5. DEPRECATED FUNCTIONALITY

This section describes deprecated functionality in Directory Server 10.3:

The Perl and shell scripts for Directory Server have been deprecated

The Perl and shell scripts, which are provided by the 389-ds-base package, have been deprecated. The scripts will be replaced by new utilities in the next major release of Red Hat Directory Server.

The *Shell Scripts* and *Perl Scripts* sections in the *Red Hat Directory Server Command, Configuration, and File Reference* have been updated. The descriptions of affected scripts contain now a note that they are deprecated.

The Directory Server Console has been deprecated

The Java-based Directory Server Console has been deprecated and will be replaced in the next major release of Red Hat Directory Server.

CHAPTER 4. DIRECTORY SERVER 10.2

4.1. SYSTEM REQUIREMENTS

This section contains information related to installing and upgrading to Directory Server 10.2, including prerequisites and platform requirements.

4.1.1. Supported Platforms for Directory Server

Red Hat supports Directory Server 10.2 on the following platforms:

- Red Hat Enterprise Linux 7.5 or later

NOTE

Directory Server 10.2 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.

4.1.2. Supported Platforms for Directory Server Console

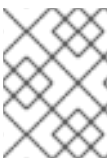
Red Hat supports running the Directory Server Console on the following platforms:

- Red Hat Enterprise Linux 7.5 or later
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 (64-bit)
- Microsoft Windows 8.1 (64-bit)

4.1.2.1. Required Java Runtime Environment

The Directory Server Console requires one of the following Java Runtime Environments:

- OpenJDK 1.8.0 for Red Hat Enterprise Linux
- Oracle Java Runtime Environment (JRE) 8
- Oracle Java Runtime Environment (JRE) 9



NOTE

To run Red Hat Directory Server Console on Microsoft Windows, you must install a 64-bit JRE.

4.1.3. Supported Platforms for Windows Synchronization Utility

The Windows Synchronization utility for Directory Server 10.2 is supported for:

- Active Directory on Microsoft Windows Server 2016

- Active Directory on Microsoft Windows Server 2012 R2

4.1.4. Web Application Browser Support

Directory Server 10.2 supports for web-based interfaces, such as Admin Express and online help tools:

- Mozilla Firefox ESR 52 and later

4.2. HIGHLIGHTED UPDATES AND NEW FEATURES

This section documents new features and important updates in Directory Server 10.2:

Directory Server rebased to version 1.3.7.5
The 389-ds-base packages have been upgraded to upstream version 1.3.7.5, 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:

- http://directory.fedoraproject.org/docs/389ds/releases/release-1-3-7-2.html
- http://directory.fedoraproject.org/docs/389ds/releases/release-1-3-7-3.html
- http://directory.fedoraproject.org/docs/389ds/releases/release-1-3-7-4.html
- http://directory.fedoraproject.org/docs/389ds/releases/release-1-3-7-5.html

Highlighted Updates and New Features in the 389-ds-base Package
Features in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.5 Release Notes:

- Directory Server no longer displays replication conflict entries in search results
- New utility to compare two Directory Server instances
- Directory Server now supports enabling the **memberOf** plug-in on read-only replicas
- The **pwdhash** utility can now retrieve the storage scheme from the configuration directory
- Directory Server supports additional password storage scheme
- Directory Server now uses separate normalized DN caches for each worker thread

4.3. BUG FIXES

This section describes bugs fixed in Directory Server 10.2 that have a significant impact on users:

Bug Fixes in the 389-ds-base Package
Bug fixes in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.5 Release Notes:

- The Directory Server trivial word check password policy now works as expected
- Backup now succeeds if replication was enabled and a changelog file existed
- Using a large number of CoS templates no longer slow down the virtual attribute processing time

- Directory Server no longer logs an error if not running the **cleanallruv** task
- The Directory Server password policies now work correctly
- A buffer overflow has been fixed in Directory Server
- Directory Server now sends the password expired control during grace logins
- An unnecessary global lock has been removed from Directory Server
- Directory Server now correctly sets whether virtual attributes are operational
- Replication now works correctly with TLS client authentication and FIPS mode enabled
- Directory Server searches with a scope set to ***one*** have been fixed
- The **memberOf** plug-in now logs all update attempts of the ***memberOf*** attribute
- ACIs with the ***targetfilter*** keyword work correctly
- Directory Server now handles binds during an online initialization correctly
- Clear error message when sending TLS data to a non-LDAPS port
- The **dirsrv@.service** meta target is now linked to **multi-user.target**

4.4. KNOWN ISSUES

This section documents known problems and, if applicable, workarounds in Directory Server 10.2:

Known Issues in the 389-ds-base Package

Known Issues in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.5 Release Notes:

- Directory Server can terminate unexpectedly during shutdown

Previously Unresolved Known Issues in Red Hat Directory Server 10.2

- The Directory Server Console is not able to connect to all instances in multi-homed environments
- Directory Server Console logins fail using the **uid** value
- Stopping and starting a remote Admin Server fails when SELinux is enabled

CHAPTER 5. DIRECTORY SERVER 10.1.1

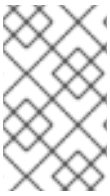
5.1. SYSTEM REQUIREMENTS

This section contains information related to installing and upgrading to Directory Server 10.1.1, including prerequisites and platform requirements.

5.1.1. Supported Platforms for Directory Server

Red Hat supports Directory Server 10.1.1 on the following platforms:

- Red Hat Enterprise Linux 7.4 or later



NOTE

Directory Server 10.1.1 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.

5.1.2. Supported Platforms for Directory Server Console

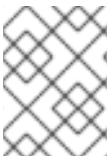
Red Hat supports running the Directory Server Console on the following platforms:

- Red Hat Enterprise Linux 7.4 or later
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 10 (64-bit)
- Microsoft Windows 8.1 (64-bit)

5.1.2.1. Required Java Runtime Environment

The Directory Server Console requires:

- OpenJDK 1.8.0 for Red Hat Enterprise Linux
- Oracle Java Runtime Environment (JRE) 8



NOTE

To run Red Hat Directory Server Console on Microsoft Windows, you must install a 64-bit JRE.

5.1.3. Supported Platforms for Windows Synchronization Utility

The Windows Synchronization utility for Directory Server 10.1.1 is supported for:

- Active Directory on Microsoft Windows Server 2016

- Active Directory on Microsoft Windows Server 2012 R2

5.1.4. Web Application Browser Support

For web-based interfaces, such as Admin Express and online help tools, Directory Server 10.1.1 supports:

- Mozilla Firefox ESR 52 and later

5.2. HIGHLIGHTED UPDATES AND NEW FEATURES

This part documents new features and important updates in Directory Server 10.1.1:

Highlighted Updates and New Features in the 389-ds-base Package
Features in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.4 Release Notes:

- The **dbmon.sh** script now uses instance names to connect to Directory Server instances
- Improved auto-tuning support in Directory Server
- Directory Server now uses the **SSHA_512** password storage scheme as default
- Directory Server now uses the **tcmalloc** memory allocator
- Directory Server now uses the **nunc-stans** framework
- Improved performance of the Directory Server **memberOf** plug-in
- Directory Server now logs severity levels in the error log file
- Directory Server now supports the **PBKDF2_SHA256 password** storage scheme

5.3. BUG FIXES

This part describes bugs fixed in Directory Server 10.1.1 that have a significant impact on users:

Bug Fixes in the 389-ds-base Package
Bug fixes in Red Hat Directory Server, that are included in the 389-ds-base package, are documented in Red Hat Enterprise Linux 7.4 Release Notes:

- In FIPS mode, the **slapd_pk11_getInternalKeySlot()** function is now used to retrieve the key slot for a token

5.4. KNOWN ISSUES

This part documents known problems and, if applicable, workarounds in Directory Server 10.1.1:

Plug-in-specific Configuration Parameters Take Precedence over Old-style *nsslapd-pluginarg Parameters**
In Red Hat Directory Server 10, you can configure certain plug-ins, such as **Attribute Uniqueness** and **Referential Integrity**, using either the new plug-in configuration parameters or the old-style ***nsslapd-pluginarg**** parameters. If both parameters types are present in the plug-in configuration, the new configuration parameters take precedence and the old plug-in argument style parameters are ignored.

To avoid problems, Red Hat recommends using the **Advanced Editor** in the Directory Server Console to configure a plug-in's arguments. For further details, see the corresponding section in the *Red Hat Directory Server Administration Guide*.

Previously Unresolved Known Issues in Red Hat Directory Server 10.1.1

- The Directory Server Console is not able to connect to all instances in multi-homed environments
- Directory Server Console logins fail using the **uid** value
- Stopping and starting a remote Admin Server fails when SELinux is enabled

CHAPTER 6. RED HAT DIRECTORY SERVER 10.1

6.1. SYSTEM REQUIREMENTS

This section contains information related to installing and upgrading Red Hat Directory Server 10.1, including prerequisites and hardware or platform requirements.

6.1.1. Required JRE

Red Hat Directory Server 10.1 requires Oracle Java Runtime Environment (JRE) 1.8.0 or OpenJDK 1.8.0 for Red Hat Enterprise Linux. Note that you only need the JRE for the Directory Server Console.

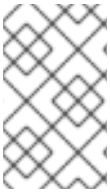
IMPORTANT

It is not possible to manage instances of Directory Server older than 8.1 (which used JDK 1.5) with the 10.1 Directory Server Console because they are using different JRE versions. You must migrate any older instance to Directory Server 10.1 if you need to manage that instance with the Directory Server Console.

6.1.2. Supported Platforms for Directory Server

Directory Server 10.1 is supported on the following platforms:

- Red Hat Enterprise Linux 7.3 or later



NOTE

Red Hat Directory Server 10.1 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.

6.1.3. Supported Platforms for Directory Server Console

The Directory Server Console is supported on the following platforms:

- Red Hat Enterprise Linux 7.3 or later
- Red Hat Enterprise Linux 6.8 or later
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 10 (64-bit)
- Microsoft Windows 8.1 (64-bit)

NOTE

Note that on Microsoft Windows, 64-bit JRE is required for the Windows Console as Red Hat Directory Server 10.1 only provides 64-bit version of it.

6.1.4. Supported Platforms for Windows Synchronization Tool

The Windows Sync utility runs on these Windows platforms:

- Active Directory on Microsoft Windows Server 2012 R2
- Active Directory on Microsoft Windows Server 2012
- Active Directory on Microsoft Windows Server 2008 R2

6.1.5. Web Application Browser Support

Directory Server 10.1 supports the following browsers to access web-based interfaces, such as Admin Express and online help tools:

- Mozilla Firefox 31.x or later

6.2. HIGHLIGHTED UPDATES AND NEW FEATURES

IMPORTANT

Note that this document only contains release notes for features which are not available in the base Red Hat Enterprise Linux 7.3 release. Many of the new features and bug fixes in Red Hat Directory Server are in the 389-ds-base package, and those are documented in Red Hat Enterprise Linux 7.3 Release Notes .

Directory Server 10.1 has introduced the following new features and important updates to make managing the directory service and its data easier and more secure:

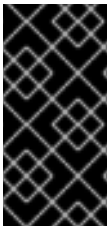
Setup can now complete even if the FQDN cannot be strictly resolved
Previously, when creating a server instance, the setup script checked that the fully qualified domain name (FQDN) can be strictly resolved, and did not continue if that was not the case. This prevented the setup from completing on certain configurations, such as cases where **ns-slapd** was located behind a load balancing server.

This update adds a way to circumvent this requirement by setting the **General.StrictHostCheck=false** option by using it on the command line when running the **setup-ds-admin.pl** script, or in the configuration **.inf** file during a silent setup. If you use this option, the setup script will accept the FQDN specified by **General.FullMachineName** without checking it against the DNS server.

Directory Console now supports additional operating systems
The **Directory Console** now supports additional operating systems. For details, see Section 6.1.4, "Supported Platforms for Windows Synchronization Tool".

Log files are now displayed separately in the Administration Server Console
Previously, the log files displayed in the **Administration Server Console** under the **Configuration** tab were named **Accesses and Errors**. With this update, each log file (Access log, Error log, Audit log and Audit fail log) is displayed separately with an appropriate title, which is clearer and more precise.

6.3. BUG FIXES



IMPORTANT

Note that this document only contains release notes for features which are not available in the base Red Hat Enterprise Linux 7.3 release. Many of the new features and bug fixes in Red Hat Directory Server are in the 389-ds-base package, and those are documented in Red Hat Enterprise Linux 7.3 Release Notes .

Directory Server 10.1 fixes the following bugs:

Ownership and file mode of certificate files is now correctly reset during upgrade

Previously, the backup process for certificate files during an upgrade did not honor file ownership and file modes. This bug has been fixed and the upgrade process now correctly preserves both.

The Administration Console no longer uses outdated ciphers

Previously, the default cipher suite selected when enabling **SSL** using the **Administration Console** was the outdated **fortezza** cipher suite. Consequently, the Directory Server logged the following error messages when starting:

```
SSL alert: Cipher suite fortezza_null is not available in NSS 3.19.  Ignoring fortezza_null
SSL alert: Cipher suite fortezza is not available in NSS 3.19.  Ignoring fortezza
SSL alert: Cipher suite fortezza_rc4_128_sha is not available in NSS 3.19.  Ignoring
fortezza_rc4_128_sha
```

With this update, the Console does not enable the **fortezza** cipher suite by default. As a result, Directory Server does not use outdated ciphers by default in this situation.

An obsolete description for was removed from the help

The **Help** page on the **Server Info** screen in the **Administration Console** previously showed the **Security level** field, which indicated whether the server used "domestic" (US-based, 128-bit) or "export" (non-US based, 40-bit) ciphers. This field was previously removed from the actual **Server Info** screen as it was no longer relevant, but was left in the help page by mistake. This update removes all mentions of this field from the help page as well.

Directory Server Console window can no longer be located off-screen at startup

Red Hat Directory Server Console window coordinates are stored in user preferences in the **o=netscaperoot** suffix. Previously, if the console was used by the same user on two different systems with different monitor setups, it was possible for the coordinates to be off screen on one of them, and consequently the console window could be hidden after logging in. This update adds a check which compares saved window coordinates with the current screen size, and resets the window location if currently outside the screen, which ensures the window is always visible.

setup-ds-admin.pl no longer fails after running **remove-ds-admin.pl** due to missing configuration files

Previously, executing the **remove-ds-admin.pl** script removed files in the **Administration Server** configuration directory if no backup was available for them. Consequently, if the user executed the **setup-ds-admin.pl** script after running **remove-ds-admin.pl**, the setup script failed. The problem occurred in the following situations:

- when **remove-ds-admin.pl** was executed repeatedly
- when **remove-ds-admin.pl** was executed without executing the **setup-ds-admin.pl** first

Instead of removing the files, **remove-ds-admin.pl** now overrides them from backup if one is available. As a result, the script no longer removes files that do not have a backup, and **setup-ds-admin.pl** no longer fails in this situation.

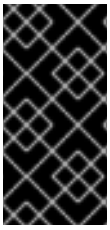
URLs for git repositories in 389-admin.spec now use HTTPS

Previously, several URLs for the **git.fedorahosted.org** repositories in the **389-admin.spec** file used the insecure **HTTP** protocol. The URLs have been updated to use the **HTTPS** protocol instead. As a result, content from the git repositories is now downloaded securely over **HTTPS**.

An architecture mismatch between the 64-bit DS Console and the 32-bit JRE no longer causes the Console to become unresponsive

When using the 64-bit version of the **Directory Server Console** with the 32-bit version of the **Java Runtime Environment** (JRE), the Console became unresponsive when the user tried to connect to an **Administration Server** over HTTPS using the Console. This update ensures that the exception causing this bug is handled properly. As a result, the Console logs a meaningful message and exits in the described situation.

6.4. KNOWN ISSUES



IMPORTANT

Note that this document only contains release notes for features which are not available in the base Red Hat Enterprise Linux 7.3 release. Many of the new features and bug fixes in Red Hat Directory Server are in the 389-ds-base package, and those are documented in Red Hat Enterprise Linux 7.3 Release Notes .

The following are some of the most important known issues in Directory Server 10.1. If applicable, supported workarounds are also described.

The Directory Server Console is not able to connect to all instances in multi-homed environments

The **Directory Server Console** is only able to connect to the first instance, if all of the following conditions are met:

- Multiple Directory Server instances are installed on one host.
- Each instance is bound to a different local network interface.
- All instances use the same port number, such as 389.

To work around the problem, run the Directory Server instances on different ports.

For further details, see the corresponding section in the *Red Hat Directory Server 10 Installation Guide*.

Directory Server Console logins fail using the uid value

The **Directory Server Console** enables users to log in using the full distinguished name (DN) or the value of the **uid** attribute of an account. When using the **uid** value to log in, the **Directory Server Console** performs an anonymous bind to locate the entry matching the value. As a consequence, if anonymous binds are disabled, the **Directory Server Console** is unable to locate the entry, and logging in using the **uid** value fails. To work around this problem, enter the full DN in the user name field and as a result, logins work like expected.

Stopping and starting a remote Admin Server fails when SELinux is enabled

Due to a limitation of **systemd**, **Admin Express** and the **Directory Server Console** fails to start or stop the **Admin Server** on remote hosts running **SELinux** in ***enforcing*** mode. To work around the problem, start and stop the **Admin Server** on the host that is running the service.

CHAPTER 7. RED HAT DIRECTORY SERVER 10.0

7.1. SYSTEM REQUIREMENTS

This section contains information related to installing and upgrading Red Hat Directory Server 10.0, including prerequisites and hardware or platform requirements.

7.1.1. Required JRE

Red Hat Directory Server 10.0 requires Oracle Java Runtime Environment (JRE) 1.6.0 or OpenJDK 1.6.0 for Red Hat Enterprise Linux. Note that you only need JRE for Directory Server Console.

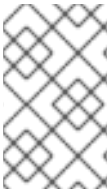
IMPORTANT

It is not possible to manage instances of Directory Server older than 8.1 (which used JRE 1.5) with the 10.0 Directory Server Console because they are using different JRE versions. You must migrate any older instance to Directory Server 10.0 if you need to manage that instance with the Directory Server Console.

7.1.2. Supported Platforms for Directory Server

Directory Server 10.0 is supported on the following platforms:

- Red Hat Enterprise Linux 7.1 (64-bit) or later



NOTE

Red Hat Directory Server 10.0 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.

7.1.3. Supported Platforms for Directory Server Console

The Directory Server Console is supported on the following platforms:

- Red Hat Enterprise Linux 7.1 (64-bit) or later

7.1.4. Supported Platforms for Windows Synchronization Tool

The Windows Sync utility runs on these Windows platforms:

- Active Directory on Microsoft Windows Server 2008 R2
- Active Directory on Microsoft Windows Server 2012
- Active Directory on Microsoft Windows Server 2012 R2

7.1.5. Web Application Browser Support

Directory Server 10.0 supports the following browsers to access web-based interfaces, such as Admin Express and online help tools:

- Mozilla Firefox 31.x or later

7.2. HIGHLIGHTED UPDATES AND NEW FEATURES

IMPORTANT

Note that this document only contains release notes for features which are not available in the base Red Hat Enterprise Linux 7.1 release. Many of the new features and bug fixes in Red Hat Directory Server are in the 389-ds-base package, and those are documented in Red Hat Enterprise Linux 7.1 Release Notes .

Directory Server 10.0 has introduced the following new features and important updates to make managing the directory service and its data easier and more secure.

TLS 1.0 or newer is enabled by default

Due to CVE-2014-3566, SSLv3 and older protocol versions are disabled by default. The Admin Server now accepts more secure SSL protocols like **TLSv1.1** and **TLSv1.2**. You can also define the SSL range that the console will use when communicating with Directory Server instances.

Password administrators

The Directory Manager can now add the Password Administrator role to a user or a group of users (not to be confused with general password maintenance). A password administrator can perform any user password operations which includes adding pre-hashed passwords, using different storage schemes, or setting passwords of any length or value.

For more information, see the related documentation in the Administration Guide.

The **nsds5ReplicaProtocolTimeout** attribute

When stopping the server, disabling replication, or removing a replication agreement, there is a timeout on how long to wait before stopping replication when the server is under load. The **nsds5ReplicaProtocolTimeout** attribute can be used to configure this timeout and its default value is 120 seconds.

For more information, see the related documentation in the Configuration, Command, and File Reference Guide.

The **nsds5ReplicaBackoffMin** and **nsds5ReplicaBackoffMax** attributes

The new **nsds5ReplicaBackoffMin** and **nsds5ReplicaBackoffMax** attributes are used in environments with heavy replication traffic, where updates need to be sent as fast as possible. By default, if a remote replica is busy, the replication protocol will go into a "back off" state, and it will retry to send it updates at the next interval of the back-off timer. The default settings maybe not be sufficient under certain circumstances and you can use these attributes to configure the minimum and maximum wait times.

For more information, see the related documentation in the Configuration, Command, and File Reference Guide.

Perl scripts support more secure connections

The new **-P** command-line parameter is now available for Perl scripts and takes a protocol name as a parameter. The supported protocols are StartTLS, LDAPS, LDAPI, and LDAP; this sequence also defines the order the script uses if fallback is needed.

For more information, see the related documentation in the Configuration, Command, and File Reference Guide.

Instance-specific scripts centralized

The new **-Z** command-line parameter takes one parameter, the server instance identifier. The script uses the identifier to get information such as the server location, or necessary configuration settings including port number, root DN, and security settings.

For more information, see the related documentation in the Configuration, Command, and File Reference Guide.

The memberOf plug-in shared configuration

Replicating plug-in configuration helps maintain consistent configuration on the network, which is especially useful in large deployments. The **memberOf** plug-in configuration can be stored in a shared configuration entry in any back end or suffix, outside of the **cn=config** suffix. In the plug-in entry, the **nsslapd-pluginConfigArea** attribute is used to specify the location of the shared configuration.

For more information, see the related documentation in the Administration Guide.

Plug-in back end transaction support

There are two new plug-in types available in Red Hat Directory Server 10: **betxnpreoperation** and **betxnpostoperation**. These types signify that if the plug-in fails to perform its operation, or some error occurs, the entire operation is rolled back and undone, and an error message is returned to the client.

Change in behavior of thememberOf plug-in

In Red Hat Directory Server 10, the **memberOf** plug-in, as well as most other plug-ins, is a back-end transaction plug-in and its default behavior now prevents unexpected failures if a schema is not in place.

If the **memberOf** plug-in fails to update a member entry with the **memberOf** attribute, the entire operation is aborted. This typically occurs because the entry does not have an object class that allows **memberOf**. Currently, there are two standard object classes that allow **memberOf**: **inetUser** and **inetAdmin**. Alternatively, a custom object class needs to be created that has **memberOf** among its allowed attributes. These object class(es) need to be present in any entry that has the potential of being a member of a group, including groups.

An additional change concerns scenarios when nested groups are created. Previously, creating nested groups always worked even if **memberOf** was not added to the bottom group. Now, creating a nested group fails unless the group has an object class that allows **memberOf**.

Improved referential integrity plug-in configuration

The new-style configuration for the Referential Integrity plug-in uses the more descriptive and convenient **referint*** attributes. The configuration using the **pluginarg*** attributes still works but is deprecated.

The second improvement allows you to define scope for handling references to deleted entries. The correctly defined scope prevents performance impacts and provides flexibility of restricting the referential integrity to selected subtrees.

For more information, see the related documentation in the *Administration Guide*.

Dynamic plug-ins

Directory Server 10.0 supports dynamic plug-ins that can be enabled without restarting the Directory Server. Allowing for dynamically enabled plug-ins makes server administration significantly easier. By using dynamic plug-ins, you can avoid restarting the server multiple times to install and configure the plug-ins.

For more information, see the related documentation in the Administration Guide.

Fine grained ID list size

The ID scan limit (**nsslapd-idlistscanlimit**) can be set per attribute, instead of for the entire database. The limit can be used to pseudo-index attributes that normally could not be indexed without impacting the entire database. This feature is very useful for addressing unavoidable unindexed searches.

Content **SyncRepl** contant synchronization plug-in

The new **SyncRepl** plug-in provides a mechanism for a client to synchronize its copy of a database with the changing content of a Directory Server, according to RFC 4533. In contrast to replication, **SyncRepl** is not oriented on changes or updates but on entries. Complete entries, after being updated, are sent to the client.

Database and changelog compaction

Previously, when an entry was deleted, a gap remained on the database page, thus growing the database files in size over time. In Red Hat Directory Server 10, the databases, including the changelog, are compacted every 30 days. This interval can also be customized by configuring the **nsslapd-db-compactdb-interval** and **nsslapd-changelogcompactdb-interval** attributes.

Read entry controls

When performing a modify operation, you can specify **pre-read** and **post_read** controls. The **pre-read** control returns a copy of the entry before it was modified and the **post-read** control returns the entry after the modify. Both controls can be used on the same operation.

The benefit of the **post-read** control is that you can see the entry after any changes a plug-in applied to it, after the initial update was performed.

Normalized DN cache

DN normalization is an expensive and unavoidable task that the server needs to do for most operations. Red Hat Directory Server 10 provides normalized DN cache that improves performance.

Schema replication improvements

Previously, it was possible that schema definitions could get incorrectly overwritten depending on where new schema definitions were added in the replication deployment. Now, during a replication session, a supplier checks that the consumer schema is a subset of the supplier schema before sending its schema. Then, the consumer checks that the consumer schema is a subset of the supplier schema before accepting the supplier's schema.

The **Read Entry Controls** LDAP extension

Directory Server now supports an extension to LDAP to allow clients to read the target entry of an update operation, such as **Add**, **Delete**, **Modify**, or **ModifyDN**. The extension utilizes controls attached to update requests to request and return copies of the target entry.

The LDAP content synchronization operation

Directory Server now supports the LDAP Content Synchronization Operation, or Sync Operation for short, which allows a client to maintain a synchronized copy of a fragment of a Directory Information Tree (DIT). The Sync Operation is defined as a set of controls and other protocol elements that extend the Search Operation.

SASL mapping fallback and prioritization

Previously, in deployments using many SASL mappings or overlapping matching criteria by design, only the first matching SASL mapping was checked. If that mapping failed, the bind operation also failed even if there were other matching mappings that could work. In Red Hat Directory Server 10, the **nsslapd-sasl-mapping-fallback** configuration option has been implemented to keep checking all the matching mappings. The **nsSaslMapPriority** prioritization option has also been added to be available for each mapping.

SASL mechanism control for authentication

In some environments, many SASL mechanisms are available but only certain ones are preferred. The **nsslapd-allowed-sasl-mechanisms** attribute allows you to define a specific mechanism on a server allowed for authentication.

Command-line replication monitoring

Red Hat Directory Server 10.0 has the ability to produce a CLI-based report for monitoring replication. The **repl-monitor.pl** script accepts both command-line parameters and a configuration file to report easily parsable information, including **Replica Root**, **Max CSN**, **Time Lag**, or **Update Status**.

Improvements to the logconv.pl script

When using the **LDAP_DEBUG_TIMING** access log level to collect microsecond etime timing, **logconv.pl** is now able to read this data and calculate statistics with microsecond resolution.

Instead of previously used flat files for temporary storage when analyzing large access logs, **logconv.pl** now uses Berkeley DB files using the perl **DB_File** module and tied hashes and arrays, which considerably improves the script's performance on large logs.

WinSync plug-in improvements for an easier way to configure data to be synchronized

With the new **winSyncSubtreePair** parameter, it is now possible to configure synchronization between multiple subtree pairs. To do this, specify **winSyncSubtreePair** multiple times to define the required Directory Server (DS) and Active Directory (AD) subtrees.

Two new parameters offer an easier way to configure which users or groups are synchronized with WinSync: the **winSyncDirectoryFilter** parameter sets a filter on DS, and the **winSyncWindowsFilter** parameter sets a filter on the AD server. These filters then select the data to be synchronized.

For more information, see the related documentation in the Administration Guide.

POSIX WinSync SID enhancements

The **WinSync** plug-in can now be enhanced to allow more control over which users and groups are synchronized, as well as automatically converting non-POSIX users from Active Directory into POSIX users in Directory Server.

Better control over the MODDN and MODRDN operations

With the enhanced Access Control Instructions (ACIs), it is possible to define a source tree and a destination tree, allow or deny the MODDN and MODRDN operations, and also specify the source

and destination targets in the same ACI. You can, for example, enable users to move an entry from one part of the tree to another, but at the same time forbid them to move an entry from or to other parts of the tree. You can also forbid users to delete or add entries.

Root DSE searches no longer display operational attributes by default

Running the **ldapsearch** utility with the **-s base -b ""** options now displays only the user attributes and not the operational attributes. Previously, a root DSE search displayed all attributes by default. To ensure compatibility with earlier versions, you can use the **nsslapd-return-default-opattr** attribute in the root DSE.

Improved behavior of the**remove-ds-admin.pl** script

When **remove-ds-admin.pl** is used to remove all Directory Servers and Admin Server, the script now replaces the following configuration files with their defaults saved in a backup directory: **httpd.conf**, **console.conf**, **admserv.conf**, and **nss.conf**. This way, a subsequent installation picks these files up seamlessly.

Additionally, when the **-a** (all) parameter is not used, the following files containing security information are preserved: **cert8.db**, **key3.db**, **secmod.db**, and **password.conf**.

The uniqueness plug-in now supports enforcing unique values across sets of attributes

Previously, Directory Server only supported configuring unique values for a single attribute. As a consequence, administrators were not able to enforce unique values across different attributes. The ***uniqueness-attribute-name*** is now multi-valued. As a result, you are now able to enforce unique values across sets of attributes. For further details, see the corresponding section in the *Directory Server Administration Guide*.

7.3. KNOWN ISSUES

IMPORTANT

Note that this document only contains release notes for features which are not available in the base Red Hat Enterprise Linux 7.1 release. Many of the new features and bug fixes in Red Hat Directory Server are in the 389-ds-base package, and those are documented in Red Hat Enterprise Linux 7.1 Release Notes .

The following are some of the most important known issues in Directory Server 10.0. If applicable, supported workarounds are also described.

- The Windows Console provided as part of Red Hat Directory Server does not yet support IPv6-only networks.
- Due to a bug in the SELinux policy, Admin server fails to restart remotely from console in Enforcing mode. To work around this problem, you can restart the server in Permissive mode or define a custom SELinux policy to allow access for the Admin server. Instructions on how to create the custom policy are included in details of AVC denial messages in the **sealert** utility.
- If the **remove-ds-admin.pl** script is executed without an installed Admin server, it removes configuration files that were installed from the RPM package. As a consequence, subsequently run **setup-ds-admin.pl** script terminates without creating the configuration file backups. To work around this problem, run the **yum reinstall 389-admin** command to recover the missing files.

- If a pipe file is present but the **ds-logpipe.py** script is not running, an attempt to restart the Directory Server fails and the system becomes unresponsive.

- Global syntax checking attributes should be enforced if the settings are not configured in the local password policy. However, if both global and local password policies are configured, the global policies are not being enforced as the default. To work around this issue, follow these steps:

  1. Enable global syntax checking.

  2. Enable fine-grained password checking.

  3. Edit the local password policy to contain all password syntax attributes. Set the values to something other than the default setting, as listed in the *Configuration, Command, and File Reference*.

  4. Edit the local password policy with the required values, even if they are the defaults.

APPENDIX A. REVISION HISTORY

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

Revision 10.4-1 **Tue Aug 06 2019** **Marc Muehlfeld**
Red Hat Directory Server 10.4 release of the guide.

Revision 10.3-1 **Wed Oct 24 2018** **Marc Muehlfeld**
Red Hat Directory Server 10.3 release of the guide.

Revision 10.2-1 **Tue Apr 10 2018** **Marc Muehlfeld**
Red Hat Directory Server 10.2 release of the guide.

Revision 10.1-5 **Tue Aug 01 2017** **Marc Muehlfeld**
Red Hat Directory Server 10.1.1 release of the guide.

Revision 10.1-4 **Fri Feb 24 2017** **Marc Muehlfeld**
Added 10.1 feature: The uniqueness plug-in now supports enforcing unique values across certain attributes.

Revision 10.1-3 **Wed Jan 11 2017** **Marc Muehlfeld**
Merged the 10.0 and 10.1 Release Notes into one document.

Revision 10.1-2 **Mon Dec 12 2016** **Marc Muehlfeld**
Added two 10.1 known issues.

Revision 10.1-1 **Thu Nov 10 2016** **Marc Muehlfeld**
Updated required JRE version and supported platforms for Directory Server Console.

Revision 10.1-0 **Wed Nov 02 2016** **Marc Muehlfeld**
Red Hat Directory Server 10.1 release of the guide.

Revision 10.0-2 **Fri Jun 12 2015** **Tomáš Čapek**
Updated the Known Issues section.

Revision 10.0-1 **Tue Jun 09 2015** **Tomáš Čapek**
Red Hat Directory Server 10 release of the guide.