Red Hat Directory Server 8.0 Release Notes

Red Hat Documentation Team

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive
Raleigh, NC 27606-2072
USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park, NC 27709
USA

Abstract

These Release Notes contain important information available at the time of the release of Red Hat Directory Server 8.0. New features, system requirements,

installation notes, known problems, resources, and other current issues are addressed here. Read this document before beginning to use Directory Server 8.0.

1. New in Red Hat Directory Server 8.0

Directory Server 8.0 includes several new features for enhanced authentication and password security, changed platform support, and support for IPv6 clients. Directory Server 8.0 also introduces a new, standards-based filesystem architecture.

- *Section 1.1, “Adaptation to Filesystem Hierarchy Standards”*
- *Section 1.2, “New Password Hashing Algorithms Support”*
- *Section 1.3, “Improved SASL Support for Kerberos Authentication”*
- *Section 1.4, “Enhanced Password Syntax Checking”*
- *Section 1.6, “Changed Platform Support”*
- *Section 1.5, “Support for IPv6”*

1.1. Adaptation to Filesystem Hierarchy Standards

Directory Server 8.0 components have been split into multiple, separate components. Rather than being installed into a single installation directory, Directory Server follows the Filesystem Hierarchy Standard (FHS), which distributes the libraries and files. This new FHS layout more closely integrates Directory Server with its base operating system and leverages existing platform components, such as the Apache web server. The FHS layout will also minimize the overhead of creating and deploying patches and updates.

1.2. New Password Hashing Algorithms Support

The existing SHA support in Directory Server has been extended to support for `SHA-256`, `SHA-384`, `SHA-512`, and `MD5` algorithms. These algorithms are used for hashed password storage to offset any potential insecurities in the existing SHA-1 hashing algorithm.

1.3. Improved SASL Support for Kerberos Authentication

Directory Server 8.0 extends and strengthens its support for SASL authentication using the

`GSS-API` to a Kerberos domain. Additional SASL tools have been added to the Mozilla LDAP C SDK.

1.4. Enhanced Password Syntax Checking

Password syntax checking enforces rules for password strings, so that any password has to meet or exceed certain criteria. Directory Server 8.0 adds password syntax checking to better enforce its password policies. All password syntax checking can be applied globally, per subtree, or per user.

In changes to the default password policies, the default minimum password length in Directory Server 8.0 has been set to eight characters, and checks for trivial words has been improved. A trivial word is any value stored in the `uid`, `cn`, `sn`, `givenName`, `ou`, or `mail` attributes of the user's entry. Additionally, Directory Server 8.0 includes more password enforcement options, providing different optional categories for the password syntax:

- Minimum number of digit characters (0-9)
- Minimum number of ASCII alphabetic characters, both upper- and lower-case
- Minimum number of uppercase ASCII alphabetic characters
- Minimum number of lowercase ASCII alphabetic characters
- Minimum number of special ASCII characters, such as `!@#$`
- Minimum number of 8-bit characters
- Maximum number of times that the same character can be immediately repeated, such as `aaabbb`
- Minimum number of character categories required per password; a category can be upper- or lower-case letters, special characters, digits, or 8-bit characters

1.5. Support for IPv6

Directory Server 8.0 accepts incoming connections from IPv6 clients. Additionally, IPv6 support has been added to the LDAP SDK, so many command-line tools and scripts included with Directory Server 8.0 can understand and use IPv6 addresses.

NOTE

Directory Server will not interpret IPv6 addresses in access control instructions or use IPv6 connections for operations such as replication and chaining.

1.6. Changed Platform Support

Directory Server 8.0 is supported on the following platforms:

- HP-UX 11i Itanium/IPF
- Red Hat Enterprise Linux 4 i386 (32-bit)
- Red Hat Enterprise Linux 4 x86_64 (64-bit)
- Red Hat Virtualization Server 5 i386 (32-bit)
- Red Hat Virtualization Server 5 x86_64 (64-bit)

> **NOTE**
>
> Red Hat Directory Server 8.0 is supported running on a virtual guest on Red Hat Virtualization Server 5.

- Sun Solaris 9 (SPARC v9, 64-bit)

2. System Requirements

This section contains information related to installing and upgrading Red Hat Directory Server 8.0, including prerequisites and hardware or platform requirements.

2.1. Perl Prerequisites

Directory Server 8.0 does not package **nsperl** with the product. **perldap** should work with the version of **perl** pre-installed on the system.

There are some prerequisites for **perl** to run **perldap** with the pre-installed version.

- For Red Hat Enterprise Linux systems, use the Perl version that is installed with the operating system in `/usr/bin/perl` for both 32-bit and 64-bit versions of Red Hat Directory Server.
- On Solaris systems, Red Hat Directory Server is installed with a Perl package, `RHATperlx`, that must be used. This package contains a 64-bit version of Perl 5.8. It is not possible to use the Perl version installed in `/usr/bin/perl` on Solaris because it is 32 bit and will not work with Directory Server's 64-bit components.
- On HP-UX, Red Hat Directory Server uses the Perl version installed with the operating system in `/opt/perl_64/bin/perl`. Contact Hewlett-Packard support if this Perl version is not installed.

2.2. Directory Server Supported Platforms

Directory Server 8.0 is supported on the following platforms:

- HP-UX 11i Itanium/IPF
- Red Hat Enterprise Linux 4 i386 (32-bit)
- Red Hat Enterprise Linux 4 x86_64 (64-bit)
- Red Hat Virtualization Server 5 i386 (32-bit)
- Red Hat Virtualization Server 5 x86_64 (64-bit)

> **NOTE**
>
> Red Hat Directory Server 8.0 is supported running on a virtual guest on Red Hat Virtualization Server 5.

- Sun Solaris 9 (SPARC v9, 64-bit)

2.3. Directory Server Console Supported Platforms

The Directory Server Console is supported on the following platforms:

- HP-UX 11i Itanium/IPF
- Red Hat Enterprise Linux 4 i386 (32-bit)
- Red Hat Enterprise Linux 4 x86_64 (64-bit)
- Red Hat Virtualization Server 5 i386 (32-bit)
- Red Hat Virtualization Server 5 x86_64 (64-bit)
- Sun Solaris 9 (SPARC v9, 64-bit)
- Windows XP
- Windows 2000 Server
- Windows 2003 Server

> **NOTE**
>
> The Directory Server Console can be installed on additional Windows platforms

at an additional cost.

2.4. Windows Sync Service Platforms

The Windows Sync tool runs on these Windows platforms:

- Windows 2003 Active Directory
- Windows 2000 Active Directory

2.5. Web Application Browser Support

Directory Server 8.0 supports the following browsers to access web-based interfaces, such as **Admin Express** and online help tools:

- Firefox 1.0 (Red Hat Enterprise Linux 4 and Solaris 9)
- Mozilla 1.4 (HP-UX)
- Mozilla 1.4.3 (Solaris 9)
- Mozilla 1.7.3 (Red Hat Enterprise Linux 4)
- Microsoft Internet Explorer 6.0 (Windows)

NOTE

Red Hat Directory Server web tools like Admin Express and Org Chart are not supported on Netscape browsers or any browser running on Mac.

3. Installing Directory Server 8.0

For instructions on installation of Directory Server 8.0, see the *Directory Server Installation Guide*, available at *http://www.redhat.com/docs/manuals/dir-server/*.

3.1. Obtaining Packages

Red Hat Network (RHN) (*http://rhn.redhat.com*) is the software distribution mechanism for Red Hat customers. You may have received account login information for RHN, including entitlements the Red Hat Directory Server 8.0 release. If so, you need to use the RHN website to obtain your software. Once are logged into RHN, go to **Channels** (view complete list if needed) and in Red Hat Directory Server 8.0 channel, go to the **Downloads** tab. The Solaris 9 64-bit packages can be found there under the ISOs list, as well as the tarball (`.tar.gz` file) archive for the source code.

> **NOTE**
>
> The files are tarball (`.tar.gz`) archive files, not ISO images.

Customers looking for RPMs for Directory Server 8.0 can access these files from the RHN website or through `yum` or `up2date`, using an account with entitlements for the Red Hat Directory Server 8.0 release. There are also ISO images containing both RPM and SRPM package files, available as downloads for the Red Hat Directory Server 8.0 channel. The RPM packages can be downloaded and installed in the usual manner. The ISO images can be downloaded and burned on to a CD-recordable media using the appropriate software.

3.2. Running setup-ds-admin.pl

After installing the packages, run the `setup-ds-admin.pl` script to configure the new Directory Server and Administration Server instances. See the *Directory Server Installation Guide* for more information about `setup-ds-admin.pl` script options and the Directory Server configuration interface.

4. Bugs Fixed in Directory Server 8.0

The following are some of the most important bugs fixed for Directory Server 8.0.

Bug Number	Description
207567	When Windows Sync was initiated, existing entries in subfolders were not synchronized, only the immediate children of the specified subtree. The synchronization has been fixed so that the scope is for the entire subtree, not one-level.
207893	Windows Sync inappropriately synchronized existing hashed passwords in Directory Server with Active Directory, which assumed that the hash was the plain text password, which reset the user's password. This has been fixed.
212671	The *street* in Directory Server is multi-valued, while the corresponding *streetAddress* on Active Directory is single-valued. Synchronization for a Directory

Bug Number	Description
	Server entry with multiple *street* values would fail on Active Directory. In Directory Server 8.0, only the first Directory Server *streetAddress* value is synchronized.
231221	The default equality index for the *nsds5ReplConflict* attribute did not return information about the attribute in a search. A default presence index has been added in Directory Server 8.0.
231507	If an entry had a null attribute indexed in a VLV index, then Directory Server would crash when that entry was modified. For example, a browsing index was created which sorted entries by `cn` and then `givenName`, and one of the entries had a `cn` attribute but no `givenName` attribute. The Directory Server would crash when that entry was modified. This has been fixed.
242551	If there was a large backlog of tombstone (deleted) entries on Directory Server, synchronization performance between Directory Server and Active Directory was severely degraded because of how long Directory Server took scanning tombstone entries for potential changes. This has been fixed.
243221	Synchronization would fail if an *initials* attribute for a Directory Server entry had too many characters. Directory Server allows an unlimited number of characters, while Active Directory has a limit of six characters. This has been fixed so that the *initials* attribute for Directory Server entries is truncated to six characters when it is synchronized.
243227	If a synchronized entry was deleted from Directory Server, then added back to a different part of the directory tree, the resurrected entry was deleted from both Directory Server and Active Directory. This is because of the way Active Directory handles tombstone entries. When the entry was added back to the Directory Server, it was added

Bug Number	Description
	back with its original ntUniqueId value, but Active Directory uses a DN-based GUID, so re-adding the entry failed with a naming violation. In Directory Server 8.0, Windows Sync has been enhanced to better deal with resurrecting tombstone entries in Active Directory. On Active Directory 2000, the entry is resurrected with a new GUID; on Active Directory 2003, the entry is resurrected with the original GUID. In both cases, the resurrected entry retains all of its original attributes and values.
243820	When Directory Server was shut down, the active browsing index was interrupted; rather than closing cleanly, the file was corrupted. Trying to delete the index failed because the Directory Server did not recognize the corrupt file, but trying to recreate the index also failed because the corrupt file caused the process to hang. Directory Server 8.0 shuts down the active browsing index, it closes cleanly, and if an error occurs, it removes the index file successfully.
247725	If the RDN of an entry ended in a double backslash (\\), then Directory Server would crash when an LDIF containing that entry was imported. This has been fixed.
249366	If an attribute with INTEGER syntax was longer than the 32-bit limit, ldapsearch filters could return entries which did not match the search criteria. because Directory Server versions 7.1 and earlier allowed search filters on all INTEGER syntax attributes by default. However, this violated the LDAPv3 definition for INTEGER syntax attributes. Directory Server 8.0 disallows range searches on indexed integer-valued attributes by default. There are two ways this can be

Bug Number	Description
	enabled: • Specify `ORDERING` and a supported ordering matching rule in the schema definition for the attribute. This is recommended for new or user-defined schema. • Add the *`nsMatchingRule`* attribute, specifying one of the supported ordering matching rules, to the index configuration for the attribute. This is recommended for existing schema. **WARNING** Red Hat strongly recommends that you do *not* change the default or standard schema used by Directory Server. For example, to perform range searches on an attribute with `INTEGER` syntax, such as *`uidNumber`*, add a matching rule to the attribute configuration, such as adding `nsMatchingRule: integerOrderingMatch` to the *`uidNumber`* index configuration, and then re-index that attribute. See the *Directory Server Administration Guide* for more information about configuring database indexes and re-generating indexes.
268101	If a password was changed, the *`modifiersname`* setting was always set to `cn=server,cn=plugins,cn=config`, regardless of which user changed the password. This has been fixed.
297221	A malformed member URL for dynamic groups, such as leaving off a closing parenthesis, made Directory Server crash. For example, the entry "ldap:///o=example.com??sub?(&(objectclass=inetorgperson)(statu

Bug Number	Description
	would make Directory Server crash because it is missing the terminal parenthesis. This has been fixed.
371771	In previous releases of Directory Server, it was possible to create a Directory Server instance with a period (`.`) in the server ID, such as `slapd-ldap.example`. However, two important functions failed if a server ID has that format: • Viewing logs in the Directory Server Console or in **Admin Express** • Removing the Directory Server instance In Directory Server 8.0, it is no longer possible to create a Directory Server instance with a period (`.`) in the server ID.
383141	Directory Server crashed if the *`nsslapd-listenhost`* attribute, which gave the Directory Server hostname, had a value associated with multiple addresses. This has been fixed.

Table 1. Bugs Fixed in Directory Server 8.0

5. Known Issues

The following are some of the most important known issues in Directory Server 8.0. If applicable, supported workarounds are also described.

Bug Number	Description	Workaround
151705	The Administration Server Console is hard-coded to set all TLS ciphers to enabled. Disabling the TLS ciphers through the Console is not saved, and the ciphers are re-enabled when the Administration Server is restarted.	*Never* edit the Administration Server ciphers through the Console. Instead, edit the `console.conf` file directly. This file is located in `/etc/dirsrv/admin-serv/` directory.
159025	Installing a certificate with the same name as an existing certificate fails in the Directory	If it is necessary to have two certificates with the same name,

Bug Number	Description	Workaround
	Server Console with the error *Internal error: Fail to install certificate -8169*.	install the second certificate through the command line using `certutil`. `certutil -importcert -v /path/to/certificate_file`
171140	Upgrading the **Windows Sync** service on the Windows server from version 7.1 to version 7.1 SP1 or higher (including 8.0) requires two things: • Rebooting the Windows machine. • Performing a full manual resynchronization. To manually synchronize Active Directory and Directory Server, open the Directory Server Console, and, in the **Configuration** tab, click the **Replication** folder, select the database, and the right-click on the synchronization agreement.	

190824	By default, not all attributes are automatically replicated to consumers in multi-master replication, including several password-associated attributes such as *`passwordRetryCount`*, *`retryCountResetTime`*, and *`accountUnlockTime`*.	To replicate these attributes, set the *`passwordIsglobalPolicy`* configuration attribute to `1` in the `cn=config` entry using `ldapmodify`. For example:
		`dn: cn=config`
		`changetype: modify`
		`replace: passwordIsGlobalPolicy`
		`passwordIsGlobalPolicy: 1`

230808	In Directory Server 8.0, the `00core.ldif` file has be split so that `00core.ldif`, correctly, only contains the schema directly required for starting the server. The other schema previously in that file have been moved to a new standard schema file, `01common.ldif`. However, on startup, the Directory Server may record schema-related errors. For example:	

Bug Number	Description	Workaround

	`[02/Jan/2008:11:20:33 -0800] - Entry "cn=config" has`
	`      unknown object class "nsslapdConfig"`	

250535	On HP-UX and Solaris, the `repl-monitor.pl` script returns an error that it cannot find the appropriate `Mozilla/LDAP/Conn.pm` PerLDAP modules.	- On Solaris, edit the `repl-monitor.pl` script directly so that it uses the proper Perl binary (`/opt/perl5x/bin/perl`) instead of the one in your path. - On HP-UX, edit the `repl-monitor.pl` script directly so that it uses the proper Perl binary (`/opt/perl_64/bin/perl`) instead of the one in your path. Then, add the following line after the comment block describing the usage in `repl-monitor.pl`: `"use lib qw(/opt/dirsrv/lib/perl /opt/dirsrv/lib/perl/arch)"`
426139	When a non-privileged user logs into the Directory Server Console and selects the **Configuration** tab, the Console throws Java exception errors to standard output.	
426145	When performing any import or export database operation through a remote Console will fail with the error *Cannot write to file...* if a relative path is given for the file.	Import and export operations through a remote Console are successful in two scenarios: - Using a relative path to import or export an LDIF file on the local machine (through both the **Configuration** and the **Import**

Bug Number	Description	Workaround
		and **Export** tasks in the **Tasks**). - Using an absolute path to import or export an LDIF file to the remote machine (through both the **Configuration** and the **Import** and **Export** tasks in the **Tasks**). However, importing or exporting the database to the remote machine will fail if you supply a relative path. When importing or exporting databases on a remote machine, do *not* use relative paths for the LDIF. Always supply the absolute path or use the **Browse** button to select a file.
426421	If both **Password Sync** and the Directory Server Console are installed on the same Windows machine, then the Directory Server Console will load the **Password Sync**`nss3.dll`, and will fail when it attempts to open.	Do not install **Password Sync** and the Windows version of the Directory Server Console on the same machine.
426439	When using the Console to install a CRL, if the CRL is placed in the proper directory, `/etc/dirsrv/slapd-`*`instance_name`*, the Console returns an error that it cannot locate the file.	Put the CRL in the Administration Server directory, `/etc/dirsrv/admin-serv`, and the Console can locate the CRL file automatically.
427321	If a Directory Server instance is migrated from a previous version to Directory Server 8.0, the *`nsslapd-saslpath`* is not migrated with the `dse.ldif` on the new 8.0 instance, so that the SASL libraries cannot be loaded. This configuration attribute is properly created in fresh Directory Server installations.	Use `ldapmodify` to edit the 8.0 `dse.ldif` file and add the *`nsslapd-saslpath`* set in the previous version.

Table 2. Known Issues in Directory Server 8.0