
Red Hat Directory Server 8.0

Release Notes

8.0 and Errata

Copyright © 2008 Red Hat, Inc.

Copyright © 2008 Red Hat, Inc.. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later with the restrictions noted below (the latest version of the OPL is presently available at <http://www.opencontent.org/openpub/>).

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

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

Updated: October 29, 2008

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	2
1.1. Adaptation to Filesystem Hierarchy Standards	2
1.2. New Password Hashing Algorithms Support	3
1.3. Improved SASL Support for Kerberos Authentication	3
1.4. Enhanced Password Syntax Checking	3
1.5. Support for IPv6	4
1.6. Changed Platform Support	4
2. System Requirements	4
2.1. Perl Prerequisites	4
2.2. Directory Server Supported Platforms	5
2.3. Directory Server Console Supported Platforms	5
2.4. Windows Sync Service Platforms	6
2.5. Web Application Browser Support	6
3. Installing Directory Server 8.0	7
3.1. Obtaining Packages	7
3.2. Running setup-ds-admin.pl	8
4. Bugs Fixed in Directory Server 8.0	8
5. Known Issues	10
6. Errata Updates	14
7. Document History	19

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 Enterprise Linux 5 i386 (32-bit)
- Red Hat Enterprise Linux 5 x86_64 (64-bit)



NOTE

Red Hat Directory Server 8.0 is supported running on a virtual guest on Red Hat Enterprise Linux 5 Virtualization Server.

- 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 Enterprise Linux 5 i386 (32-bit)
- Red Hat Enterprise Linux Server 5 x86_64 (64-bit)



NOTE

Red Hat Directory Server 8.0 is supported running on a virtual guest on Red Hat Enterprise Linux 5 Virtualization Server.

- 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 Enterprise Linux 5 i386 (32-bit)
- Red Hat Enterprise Linux 5 x86_64 (64-bit)



NOTE

Red Hat Directory Server 8.0 is supported running on a virtual guest on Red Hat Enterprise Linux 5 Virtualization Server.

- 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 more detailed instructions on installing Directory Server 8.0, see the *Directory Server Installation Guide* at <http://1www.redhat.com/1docs/1manuals/1dir-server/>.

3.1. Obtaining Packages

Red Hat Network (RHN) (<http://1rhn.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 <i>street</i> in Directory Server is multi-valued, while the corresponding <i>streetAddress</i> on Active Directory is single-valued. Synchronization for a Directory Server entry with multiple <i>street</i> values would fail on Active Directory. In Directory Server 8.0, only the first Directory Server <i>streetAddress</i> value is synchronized.
231221	The default equality index for the <i>nsds5ReplConflict</i> 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 <i>cn</i> and then <i>givenName</i> , and one of the entries had a <i>cn</i> attribute but no <i>givenName</i> 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 <i>initials</i> 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 <i>initials</i> attribute for Directory Server entries is truncated to six characters when it is synchronized.
243227	<p>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 back with its original <i>ntUniqueID</i> value, but Active Directory uses a DN-based GUID, so re-adding the entry failed with a naming violation.</p> <p>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</p>

Bug Number	Description
	resurrected with the original GUID. In both cases, the resurrected entry retains all of its original attributes and values.
243820	<p>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.</p> <p>Directory Server 8.0 shuts down the active browsing index, it closes cleanly, and if an error occurs, it removes the index file successfully.</p>
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	<p>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.</p> <p>Directory Server 8.0 disallows range searches on indexed integer-valued attributes by default. There are two ways this can be enabled:</p> <ul style="list-style-type: none"> • 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 <i>nsMatchingRule</i> attribute, specifying one of the supported ordering matching rules, to the index configuration for the attribute. This is recommended for existing schema. <div data-bbox="438 1467 1417 1668" style="background-color: #800000; color: white; padding: 10px;">  <p>WARNING Red Hat strongly recommends that you do <i>not</i> change the default or standard schema used by Directory Server.</p> </div> <p>For example, to perform range searches on an attribute with INTEGER syntax, such as <i>uidNumber</i>, add a matching rule to the attribute configuration, such as adding nsMatchingRule: integerOrderingMatch to the <i>uidNumber</i> index configuration, and then re-index that attribute.</p> <p>See the <i>Directory Server Administrator's Guide</i> for more information about configuring database indexes and re-generating indexes.</p>
268101	If a password was changed, the <i>modifiersname</i> setting was always set to

Bug Number	Description
	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)(status=ACTIVE)(role=DSAdmin)" 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: <ul style="list-style-type: none"> Viewing logs in the Directory Server Console or in Admin Express Removing the Directory Server instance <p>In Directory Server 8.0, it is no longer possible to create a Directory Server instance with a period (.) in the server ID.</p>
383141	Directory Server crashed if the <i>nsslapd-listenhost</i> 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.	<i>Never</i> edit the Administration Server ciphers through the Console. Instead, edit the console.conf file directly. This file is located in /etc/dirsrv/admin-srv/directory .
159025	Installing a certificate with the same name as an existing certificate fails in the Directory Server Console with the error <i>Internal error: Fail to install certificate -8169</i> .	If it is necessary to have two certificates with the same name, install the second certificate through the command line using certutil . <pre>certutil -importcert -v / path/ to/certificate_file</pre>

Bug Number	Description	Workaround
171140	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>By default, not all attributes are automatically replicated to consumers in multi-master replication, including several password-associated attributes such as <i>passwordRetryCount</i>, <i>retryCountResetTime</i>, and <i>accountUnlockTime</i>.</p>	<p>To replicate these attributes, set the <i>passwordIsGlobalPolicy</i> configuration attribute to 1 in the cn=config entry using ldapmodify. For example:</p> <pre data-bbox="1018 1081 1372 1283">dn: cn=config changetype: modify replace: passwordIs\ GlobalPolicy passwordIsGlobal\ Policy: 1</pre>
230808	<p>In Directory Server 8.0, the 00core.ldif file has been 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.</p> <p>However, on startup, the Directory Server may record schema-related errors. For example:</p> <pre data-bbox="443 1664 994 1821">[02/Jan/2008:11:20:33 -0800] - Entry "cn=config" has unknown object class "nsslapdConfig"</pre>	
250535	<p>On HP-UX and Solaris, the repl-monitor.pl script returns an error that it cannot find the appropriate Mozilla/LDAP/Conn.pm PerlLDAP modules.</p>	<ul style="list-style-type: none"> • On Solaris, edit the repl-monitor.pl script directly so that it uses the proper Perl binary (/

Bug Number	Description	Workaround
		<p><code>opt/perl5x/bin/perl</code> instead of the one in your path.</p> <ul style="list-style-type: none"> On HP-UX, edit the <code>repl-monitor.pl</code> script directly so that it uses the proper Perl binary (<code>opt/perl_64/bin/perl</code>) instead of the one in your path. Then, add the following line after the comment block describing the usage in <code>repl-monitor.pl</code>: <pre data-bbox="927 891 1326 1128">"use lib qw(/opt/dirsrv/lib/p erl / opt/ dirsrv/ lib/perl/arch)"</pre>
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 <i>Cannot write to file...</i> if a relative path is given for the file.	<p>Import and export operations through a remote Console are successful in two scenarios:</p> <ul style="list-style-type: none"> Using a relative path to import or export an LDIF file on the local machine (through both the Configuration and the Import 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). <p>However, importing or export-</p>

Bug Number	Description	Workaround
		<p>ing the database to the remote machine will fail if you supply a relative path.</p> <p>When importing or exporting databases on a remote machine, do <i>not</i> use relative paths for the LDIF. Always supply the absolute path or use the Browse button to select a file.</p>
426421	<p>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.</p>	<p>Do not install Password Sync and the Windows version of the Directory Server Console on the same machine.</p>
426439	<p>When using the Console to install a CRL, if the CRL is placed in the proper directory, <code>/etc/dirsrv/slaped-instance_name</code>, the Console returns an error that it cannot locate the file.</p>	<p>Put the CRL in the Administration Server directory, <code>/etc/dirsrv/admin-serv</code>, and the Console can locate the CRL file automatically.</p>
427321	<p>If a Directory Server instance is migrated from a previous version to Directory Server 8.0, the <code>nsslapd-saslpath</code> is not migrated with the <code>dse.ldif</code> 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.</p>	<p>Use <code>ldapmodify</code> to edit the 8.0 <code>dse.ldif</code> file and add the <code>nsslapd-saslpath</code> set in the previous version.</p>
430993	<p>The log deletion policies set for the access, audit, and error logs can be ignored if the two parameters defining the time amount (integer) and time unit (day, week, month, or year) are not in the proper order. In <code>dse.ldif</code>, the time amount must be listed first, then the time unit must be listed next. For example:</p> <pre data-bbox="435 1576 1002 1715">nsslapd-access\ log-logexpirationtime: 2 nsslapd-access\ log-logexpirationtimeunit: week</pre> <p>Additionally, setting the deletion time in the Directory Server Console may be ignored in some circumstances. Changing only one of the defaults for the deletion policy in the Directory Server Console will add only that one parameter to the <code>dse.ldif</code> file. If only one of the parameters is in the file, than the <code>nsslapd-TYPElog-logexpirationtime</code> defaults to not ex-</p>	<p>Edit the 8.0 <code>dse.ldif</code> file and add both the <code>nsslapd-typelog-logexpirationtime</code> and <code>nsslapd-typelog-logexpirationtimeunit</code> parameters in the proper order, so that both the expiration time amount and unit are explicitly defined.</p>


Bug Number	Description	Workaround
	piring (PR_INT32_MAX) and <code>nsslapd-TYPElog-logexpirationtimeunit</code> defaults to <code>-1*unit_in_second</code> .	
468474	<p>Changes to the <code>10dsdata.ldif.tmpl</code> template file in the 8.0.4 version of Red Hat Directory Server introduced changes to the migration process from Red Hat Directory Server 7.1 to Red Hat Directory Server 8.0.4. Migration removes the <code>cn=FQDN, ou=domain, o=NetscapeRoot</code> entry and all of its children, but in migrating to 8.0.4, the migration script is unable to add back that entry or its children. The children of <code>cn=FQDN, ou=domain, o=NetscapeRoot</code> include the Administration Server SIE registration entry, leaving only the <code>slapd</code> (Directory Server) registration in the SIE.</p> <div style="background-color: #c8863f; color: white; padding: 10px; border: 1px solid #c8863f;">  <p>IMPORTANT This only affects a migration from Red Hat Directory Server 7.1 to Red Hat Directory Server 8.0.4.</p> </div>	<p>Run the <code>setup-ds-admin.pl</code> script with the <code>-u</code> option to restore the original SIE Administration Server configuration entry and its children. For example:</p> <pre style="background-color: #f0f0f0; padding: 5px;">setup-ds-admin.pl -u</pre>

Table 2. Known Issues in Directory Server 8.0

6. Errata Updates

The following erratas have been issued for Red Hat Directory Server, fixing important security and performance issues. The complete list of erratas issued for Red Hat Directory Server 8.0 is available through Red Hat Network:

- [Red Hat Enterprise Linux 5₁](#)
- [Red Hat Enterprise Linux 4₂](#)

Release Date	Errata Release	Bug Number	Description
August 27, 2008	RHSA 2008:0602	233642	The change sequence numbers in multi-master replication had a built-in skew to accommodate differences in the clocks on master servers. However, this skew could grow un-

¹ <https://rhn.redhat.com/errata/rhel5-dirserv-8-errata.html>
² <https://rhn.redhat.com/errata/rhel4-dirserv-8-errata.html>


Release Date	Errata Release	Bug Number	Description
			der some circumstances to the point that it falsely hit the maximum allowed skew (one day, by default) and stopped replication entirely. Because the problem was in the timestamps of the CSNs for the masters, replication could not be easily restarted. The severity of the problem increased with the number of updates made to the Directory Server.
		428163	A problem in the SASL IO handling meant that memory was not reallocated after SASL binds. For example, a simple bind coming immediately after a SASL bind may fail.
		431103	<p>Attempting to create a new Directory Server instance using a remote Configuration Directory would fail.</p> <p>Along with fixing the bug, a new options was added to the <code>setup-ds-admin.pl</code> script, <code>-u</code>, which will check the host server for existing Directory Server instances and then re-register them with the specified Configuration Directory. This option is mentioned in "Updating and Re-registering Directory Server Instances"³ in the <i>Red Hat Directory Server Installation Guide</i>.</p>
		440333	Uninitialized variables in plug-ins for logging and access controls caused errors when running the <code>ns-slaped</code> process.
		442103	If the Directory Server Console was set to use SSL, then clicking the Manage Certificates button in the Directory Server Console Tasks tab threw Java exceptions and the window would not open.
		442170	If an entry with a large attribute value, such as over 32KB, was replicated, the replication could fail because the buffer size was too small. However, an incorrect error code was returned, so the cause of the failure was not apparent.
		448831 454065 (CVE 2008-2930)	A flaw in the way the Directory Server handled LDAP search requests using patterns could allow a remote attacker to cause the Directory Server to use large amounts of CPU time. Pat-

³ http://redhat.com/docs/manuals/dir-server/install/8.0/Installation_Guide-Advanced_Configuration-Making-DS.html#Installation_Guide-Advanced_Configuration-Reregistering-with-Config-DS

Release Date	Errata Release	Bug Number	Description
			<p>tern searches were not restricted by normal directory search time limits. If the attacker had access to LDAP service, he could create a search request with a search pattern that matched specially-crafted data records, running searches without time limits and consuming CPU time.</p> <p>The Directory Server has been updated to apply the <i>nsslapd-timelimit</i> attribute to the pattern search query run time. This attribute has a default limit of 3600 seconds (one hour). To shorten the time limit, modify the <i>nsslapd-timelimit</i> parameter in cn=config. For example:</p> <pre>ldapmodify -D "cn=Directory Manager" -w password dn: cn=config changetype: modify replace: nsslapd-timelimit nsslapd-timelimit: 30</pre>
		450973	<p>Password policy attributes are not replicated by default. However, if a password attribute such as <i>accountunlocktime</i> was added to an entry, the server would attempt to replicate that attribute, which would cause an error. Rather than correctly processing the error, replication would fail.</p>
		452169	<p>In replication scenarios, if an attribute value was scheduled to be deleted and also was indexed or had an attribute subtype which was indexed, the Directory Server would crash during the index operation.</p>
		452323	<p>If the Administration Server was restarted, trying to create a new instance of the <i>Directory Server</i> through the Directory Server Console would fail.</p>
		454328	<p>The Directory Server crashed when groups were added to each other as members, such as Group 2 being added as a member to Group 1, Group 3 being added to Group 2, and so on. This is because the stack size for the <i>memberOf</i> plug-in on 64-bit systems was hard-coded to 256KB, which meant that relatively small loops could still overflow the stack.</p>
		458506 458693 (CVE	<p>There was a memory leak error in the SASL bind code. This error was difficult to trigger in</p>

Release Date	Errata Release	Bug Number	Description
		2008-3283) 458977 (CVE 2008-3283)	real-world scenarios because it required sending a 0-valued password for a SASL bind, but it could be triggered by an anonymous user.
		458507 458693 (CVE 2008-3283) 458977 (CVE 2008-3283)	There was a memory leak error when changing the password storage scheme. This error could only be triggered by an admin user, not an anonymous user.
		458510 458693 (CVE 2008-3283) 458977 (CVE 2008-3283)	There was a memory leak error when a user attempted to change a password; if the given DN for the password change was null, the operation defaulted to changing the password for the bind DN, and there was a small memory leak at that transition. This could be triggered by an anonymous user.
		458666 458693 (CVE 2008-3283) 458977 (CVE 2008-3283)	There were two memory leak errors with password policy settings: <ul style="list-style-type: none"> • When trivial word checking was enabled in the password policy, there was a small leak with running trivial word checking when a user changed his password. • When the password policy settings were changed, there was a small memory leak.
		458668 458693 (CVE 2008-3283) 458977 (CVE 2008-3283)	There was a memory leak error in the SASL mapping code with the regular expressions which are used with the identity mapping to look up a user's bind DN based on the user and user realm.
		458675 458693 (CVE 2008-3283) 458977 (CVE 2008-3283)	There was a memory leak error in how Directory Server handled value sets where there were several duplicate, non-sequential values added to an attribute, such as adding foo, bar, bat, foo. This leak could only be triggered by an authenticated user to the Directory Server who had the rights to modify attributes in an entry, including self-write access, and if replication was being used.
		458677 458693 (CVE 2008-3283) 458977 (CVE 2008-3283)	There was a memory leak error in the index code for searches which were run against the index with a range or with a matching rule.

Release Date	Errata Release	Bug Number	Description
August 27, 2008	RHSA 2008:0601	245248 454621 (CVE 2008-2929) 454660 (CVE 2008-2929)	Admin Express, the web interface for basic server management hosted by the Administration Server, used non-escaped URLs to access some of its services. This meant that browsers would attempt to execute the scripts passed in the URL rather than opening the URL.
		413531 454621 (CVE 2008-2929) 454660 (CVE 2008-2929)	The Directory Server web services, such as Admin Express, could be configured to accept language configurations which would cause the web services to quit functioning and make the server fail with segfault errors.
		454060 454621 (CVE 2008-2929) 454660 (CVE 2008-2929)	The Directory Server Gateway and Administration Server Express interfaces had scripting issues caused by improperly parsing a percent (%) -escaped value provided by a user. A remote attacker could exploit this flaw to execute cross-site attacks against Directory Server users or administrators who used those web services.
May 9, 2008	RHSA 2008:0269	444712 (CVE-2008-1677)	A buffer overflow flaw was found in Red Hat Directory Server's regular expression handler. An unauthenticated attacker could construct a malicious LDAP query that could execute arbitrary code or cause the Directory Server to crash.
May 1, 2008	RHBA 2008:0265	428764	Directory Server had a memory leak when a search request was sent with an extensible matching search filter, a search filter with a specified matching rule. A linked list was created but only the memory allocated for the first item in the list was freed when the list was no longer required.
April 15, 2008	RHSA 2008:0201	437301 (CVE-2008-0892)	The Administration Server replication monitor CGI scripts had a shell command injection flaw which could allow an attacker with access to the replication monitor page to execute arbitrary shell commands with the privileges of the Administration Server.



NOTE
By default, the Administration Server runs as `nobody`, an unprivileged user.

Release Date	Errata Release	Bug Number	Description
		437320 (CVE-2008-0893)	The Administration Server did not properly restrict access to CGI scripts. An anonymous user could access the Administration Server's TCP port to access restricted Directory Server information or perform administrative tasks. By default, the Administration Server uses port 9830.
April 1, 2008	RHBA 2008:0203	435730	<i>Fractional replication</i> is replication which synchronizes user-selected attributes rather than full entries. Initially, fractional replication could be configured only from a supplier to dedicated consumers. The fractional replication plug-in has been enhanced to allow fractional replication between suppliers. This also improves the performance of other Directory Server plug-ins which depend on fractional replication and required supplier to supplier fractional replication.
March 19, 2008	RHBA 2008:0191	436107 (CVE-2008-0889)	The Directory Server Console, <code>redhat-idm-console</code> , is a Java-based interface which managed the Directory Server and Administration Server. On Red Hat Enterprise Linux, Directory Server used insecure permissions for the <code>redhat-idm-console</code> start script. This could allow local users to modify the Console start script to run arbitrary code with the full privileges of the Directory Server Console user.

Table 3. Bugs Fixed in Errata Updates for Directory Server 8.0

7. Document History

Revision History

Revision 8.0.3	October 29, 2008	dlackey@redhat.com Deon Lackey
Adding known issue on additional required step when migrating from Directory Server 7.1 to Directory Server 8.0.4. Adding full list of errata releases.		
Revision 8.0.2	September 2, 2008	dlackey@redhat.com Deon Lackey
Clarifying supported platforms list for Red Hat Enterprise Linux systems and virtualization.		
Revision 8.0.1	August 27, 2008	dlackey@redhat.com Deon Lackey
Adding new errata updates and fixes for Errata RHSA-2008:0601 and RHSA-2008:0602.		
Revision 8.0.0	January 15, 2008	dlackey@redhat.com

com

Official release draft.