
Red Hat Directory Server 7.1 SP7 Release Notes

Copyright © 2008 Red Hat

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

August 27, 2008

1. System Requirements	2
2. Installing Directory Server 7.1 SP7	4
2.1. Obtaining Packages	4
2.2. Installing Directory Server 7.1 SP7 on Red Hat Enterprise Linux	5
2.3. Installing Directory Server 7.1 SP7 on HP-UX and Sun Solaris	6
2.4. Installing Synchronization Services	7
3. Bugs Fixed in Directory Server 7.1 SP7	8
4. Known Issues	11

This is a service pack release for bug fixes and patches for the 7.1 version of Red Hat Directory Server. These Release Notes contain important information available at the time of the release of Red Hat Directory Server 7.1 SP7. System requirements, installation notes, known problems, resources, and other current issues are addressed here. Read this document before beginning to use Directory Server 7.1 SP7.

There are no new features in Directory Server 7.1 SP7.

1. System Requirements

This section contains information related to installing and upgrading Red Hat Directory Server 7.1 SP7, including prerequisites and hardware or platform requirements.

Directory Server Supported Platforms

Directory Server 7.1 SP7 is supported on the following platforms:

- HP-UX 11i (PA-RISC, 64-bit)
- Red Hat Enterprise Linux 3 Update 4 (i386, 32-bit)
- Red Hat Enterprise Linux 4 (i386, 32-bit)
- Sun Solaris 9 (SPARC, 32-bit)
- Sun Solaris 9 (SPARC, 64-bit)

Directory Server Console Supported Platforms

The Directory Server Console is supported on the following platforms:

- HP-UX 11i (PA-RISC, 64-bit)
- Red Hat Enterprise Linux 3 Update 4 (i386, 32-bit)
- Red Hat Enterprise Linux 4 (i386, 32-bit)
- Sun Solaris 9 (SPARC, 32-bit)
- Sun Solaris 9 (SPARC, 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.

Windows Sync Service Platforms

The Windows Sync tool runs on these Windows platforms:

- Windows 2003 Active Directory
- Windows 2000 Active Directory
- Windows NT SAM Registry

Web Application Browser Support

Directory Server 7.1 SP7 supports the following browsers to access web-based interfaces, such as **Admin Express** (for administrators), **Org Chart**, and **Phonebook** (for all users):

- Firefox 1.0 (Red Hat Enterprise Linux 3 and 4 and Solaris 9)
- Mozilla 1.4 (HP-UX)
- Mozilla 1.4.3 (Red Hat Enterprise Linux 3 and Solaris 9)
- Mozilla 1.7.3 (Red Hat Enterprise Linux 4)
- Microsoft Internet Explorer 6.0 (Windows; supported only for Org Chart and Phonebook)



NOTE

Red Hat Directory Server web tools like Admin Express and Org Chart are not support-

ted on Netscape browsers or any browser running on Mac.

2. Installing Directory Server 7.1 SP7

To install Directory Server 7.1 SP7 on Red Hat Enterprise Linux, simply download the RPM and either upgrade the existing installation with the `rpm -U` flag, as described in [Section 2.2, “Installing Directory Server 7.1 SP7 on Red Hat Enterprise Linux”](#), or install a new Directory Server using the RPM package with the `rpm -i` flag and configure the server.

To install Directory Server 7.1 SP7 on HP-UX and Sun Solaris, download the packages from Red Hat Network, extract the binaries, then run the setup command.

For instructions on installing and configuring Directory Server 7.1 SP7, see the *Directory Server Installation Guide*, available at <http://www.redhat.com/1docs/1manuals/1dir-server/1install/17.1/1index.html>.

2.1. Obtaining Packages

Red Hat Network (RHN) (<http://1rhn.redhat.com>) is the software distribution mechanism for Red Hat customers. When purchasing the entitlements for Red Hat Directory Server 7.1 SP7, you will also have received account login information for Red Hat Network.

1. Log into Red Hat Network.
2. Go to the **Channels** tab, and select the Red Hat Directory Server 7.1 channel. Browse through the complete channel list if needed.
3. Go to the **Downloads** tab in the Red Hat Directory Server 7.1 channel, and download the Red Hat Directory Server packages.



NOTE

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

ISO images containing both RPM and SRPM package files are available as downloads through the Red Hat Directory Server 7.1 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.

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.

2.2. Installing Directory Server 7.1 SP7 on Red Hat Enterprise Linux

On Red Hat Enterprise Linux, it is possible to upgrade an existing installation with the `rpm -U` flag or install a new Directory Server using the RPM package with the `rpm -i` flag.



NOTE

RPMs for Directory Server 7.1 SP7 are also available to Red Hat Enterprise Linux users by running `update` using an account with entitlements for the Red Hat Directory Server 7.1 SP7 release.

To upgrade Red Hat Directory Server 7.1 (or any previous 7.1 service pack) on a Red Hat Enterprise Linux 3 or 4 system:

1. Log in as `root`.
2. Run `rpm` to upgrade the Directory Server using the package appropriate for your version of Red Hat Enterprise Linux.
 - For Red Hat Enterprise Linux 3:

```
rpm -U redhat-ds-7.1SP7-11.RHEL3.i386.rpm
```

- For Red Hat Enterprise Linux 4:

```
rpm -U redhat-ds-7.1SP7-11.RHEL4.i386.rpm
```

3. *For upgrading from SP4 or earlier.* Run the setup script again.

```
# cd /opt/redhat-ds  
# ./setup/setup -r
```



NOTE

When upgrading from an Directory Server instance version 7.1SP4 or older, you must run the setup script to resolve security issues addressed in 7.1SP5. If you are upgrading from version 7.1SP5, then this is not necessary.

To install a new installation of Red Hat Directory Server 7.1 SP7:

1. Log in as `root`.
2. Run `rpm` to install the Directory Server using the package appropriate for your version of Red Hat Enterprise Linux.

- For Red Hat Enterprise Linux 3:

```
rpm -i redhat-ds-7.1SP7-11.RHEL3.i386.rpm
```

- For Red Hat Enterprise Linux 4:

```
rpm -i redhat-ds-7.1SP7-11.RHEL4.i386.rpm
```

3. Go through the configuration process as described in the *Directory Server Installation Guide*.

2.3. Installing Directory Server 7.1 SP7 on HP-UX and Sun Solaris

1. Log in as `root`.
2. Create a new directory for the new Directory Server service pack version.

```
mkdir ds71sp7
```

3. Open the new directory.

```
cd ds71sp7
```

4. Download the Directory Server product binaries file to this directory.
5. Unpack the product binaries.

```
gzip -dc filename.tar.gz | tar -xvof -
```

filename is the product binaries file; the exact name depends on your platform.

6. Make sure that the Configuration Directory Server instance on the machine is running and that the Administration Server instance is stopped.

```
# cd serverRoot./stop-admin  
# cd serverRoot/slapd-instance./restart-slapd
```

7. Open the new **ds71sp7** directory, and extract the binary files for the new service pack setup program by running the **setup** command with the **-b** option.

```
# cd /path/to/ds71sp7  
# ./setup -b serverRoot
```

8. Run the **setup** program again to install the service pack.



NOTE

When upgrading from an Directory Server instance version 7.1SP4 or older, you must run the setup script to resolve security issues addressed in 7.1SP5. If you are upgrading from version 7.1SP5, then this is not necessary.

9. Supply the configuration information as prompted by the installer. An upgrade usually requires this information:
 - Agreeing to the setup and licensing terms.
 - The full path to the server root directory (the installation directory) where Directory Server 7.1 is located; by default, this is **/opt/redhat-ds/servers**.
 - The Configuration Administrator's password for the Directory Server 7.1 instance.

The upgrade process begins after all of the 7.1 instance information is given.

2.4. Installing Synchronization Services

If Windows synchronization will be used on a Windows server in conjunction with a Red Hat Directory Server 7.1 server, then install the 7.1 SP7 Windows Sync services on the Windows machine:

1. Uninstall the **Password Sync** services. If the Windows sync peer is an NT server, then also uninstall the **User Sync** service. This is described in the *Directory Server 7.1 Administrator's Guide*, available at <http://1www.redhat.com/1docs/1manuals/1dir-server/1ag/17.1/1sync.html#2878810>.



NOTE

The SSL databases or keystore are preserved and can be re-used after upgrade is complete.

2. Copy the the updated **msi** files from `/opt/redhat-ds/winsync/` to the Windows system.
3. Double-click the new **msi** files to install them.
4. Reboot the Windows system after re-installing the **Password Sync** and, on NT, **User Sync** services.
5. Perform a full resynchronization between the Directory Server and Windows sync servers.
 - a. In the Directory Server Console, click the **Configuration** tab.
 - b. Expand the **Replication** folder in the left navigation window.
 - c. Click the name of the Directory Server database which is synchronized with the Windows directory, and select the sync agreement.
 - d. Select **manual synchronization** from the drop-down menu.

3. Bugs Fixed in Directory Server 7.1 SP7

The following are some of the most important bugs fixed for Directory Server 7.1 SP7. Along with this service pack, some 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 7.1 SP7 for Red Hat Enterprise Linux is available through Red Hat Network at <https://1rhnl.redhat.com/1errata/1rhel-dirserv-71-errata.html>.

Red Hat Directory Server 7.1 SP7 is released as an update as Erratum RHSA 2008:0596, which is associated with Bugzilla #453229.

Bug Number	Alternate ID	Description
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 under 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

Bug Number	Alternate ID	Description
		<p>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.</p> <p>This has been fixed.</p>
440333		<p>There were uninitialized variables in plug-ins for logging and access controls. These have been fixed.</p>
448831	CVE-2008-2930 454065	<p>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. Pattern 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>accountunlock-time</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> <p>This has been fixed.</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> <p>This has been fixed.</p>
453916	413531 453921 CVE-2008-2928	<p>Several Directory Server CGI applications were affected by a buffer overflow flaw in the routine which parses Accept Language HTTP headers. The web services could be configured to allow acceptable language configurations which caused the</p>

Bug Number	Alternate ID	Description
		<p>web services to quit functioning and crash the server. A remote attacker with access to the Administration Server web interface could exploit the flaw to crash those CGIs or, possibly, to execute arbitrary code with the privileges of the Administration Server, which typically runs as the <code>root</code> user on the host machine.</p> <p>This has been fixed.</p>
454328		<p>The Directory Server crashed on some looping operations, such as recursively adding groups as members to other groups (Group A becomes a member of Group B, which becomes a member of Group C, and so on). Because the stack size for 64-bit systems was hard-coded to 256KB, relatively small loops could still overflow the stack.</p> <p>This has been fixed.</p>
454621	245248 454658 CVE- 2008-2929	<p>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.</p> <p>These errors have been fixed.</p>
458171		<p>On HP-UX, when running an approximate search, the search code could return an error code 3, which corresponds to the LDAP error code for exceeding the search time limit. This meant that an approximate search could end prematurely with a timeout error, even though the time limit had not been reached.</p> <p>This error has been fixed.</p>
458506	CVE- 2008-3283 458692 458977	<p>There was a memory leak error in the SASL bind code. This error was difficult to trigger in real-world scenarios because it required sending a 0-valued password for a SASL bind, but it could be triggered by an anonymous user.</p> <p>This error has been fixed.</p>
458507	CVE- 2008-3283 458692 458977	<p>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.</p> <p>This error has been fixed.</p>
458510	CVE- 2008-3283	<p>There was a memory leak error when a user attempted to change a password; if the given DN for the password change</p>

Bug Number	Alternate ID	Description
	458692 458977	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. This error has been fixed.
458666	CVE-2008-3283 458692 458977	When trivial word checking was enabled in the password policy, there was a small memory leak when trivial word checking was run when a user changed his password. This error has been fixed.
458668	CVE-2008-3283 458692 458977	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. This error has been fixed.
458675	CVE-2008-3283 458692 458977	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. This error has been fixed.
458677	CVE-2008-3283 458692 458977	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. This error has been fixed.

Table 1. Bugs Fixed in Directory Server 7.1 SP7

4. Known Issues

The following are some of the most important known issues in Directory Server 7.1 SP7. When possible, supported workarounds are also described.

Bug Number	Description	Workaround
171140	Upgrading the Windows Sync service on the Windows server from version 7.1 to version 7.1 SP1 or higher (including 7.1 SP7) requires two things: <ul style="list-style-type: none"> • Rebooting the Windows machine. 	

Bug Number	Description	Workaround
	<ul style="list-style-type: none">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.	
311851	SASL mapping entries are dynamically created and stored in the configuration file at the instance generation. The mapping entries are associated with the primary suffix. If a second root suffix is added and entries under the second suffix need to be mapped by SASL mapping, there are no mapping entries created for them. The original SASL mapping entries point to the first suffix.	Manually create SASL mapping entries that are associated with the second suffix.
400341	If a user other than the admin user logs into the Console and attempts to change the admin user's password, the password is not properly updated.	Only change the admin user password through the Console when logged in as the admin user.
429631	If a Windows directory is synchronized with a virtual directory tree in Red Hat Directory Server, then the Red Hat Directory Server crashes when synchronization is initiated.	Do not use virtual branch entries as the synchronization database.

Table 2. Known Issues in Directory Server 7.1 SP7