Red Hat Directory Server 9.0 9.1 Release Notes

Highlighted features and updates related to Red Hat Directory Server 9.1 (9.1.0 - 9.1.2)

Marc Muehlfeld Petr Bokoč Ella Deon Ballard

Red Hat Directory Server 9.0 9.1 Release Notes

Highlighted features and updates related to Red Hat Directory Server 9.1 (9.1.0 - 9.1.2)

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

Petr Bokoč
Red Hat Customer Content Services

Ella Deon Ballard
Red Hat Customer Content Services

Legal Notice

Abstract

These release notes contain information about fixed bugs, known issues, and new features in this release of Red Hat Directory Server. This documentation is no longer maintained. For details, see .

Table of Contents

These release notes contain important information available at the release of Red Hat Directory Server version 9.1. 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 9.1.

Important

Note that this document only contains release notes for features which are not available in the base Red Hat Enterprise Linux release.

Many of the new features and bug fixes in Red Hat Directory Server are in the *389-ds-base* package. These updates are documented in:

Directory Server 9.1.2

- Red Enterprise Linux 6.9 Release Notes

Directory Server 9.1.1

- Red Enterprise Linux 6.8 Release Notes

Directory Server 9.1.0

- Red Enterprise Linux 6.7 Release Notes
- Red Enterprise Linux 6.6 Release Notes
- Red Enterprise Linux 6.5 Release Notes
- Updates Available in Red Enterprise Linux 6.4

1. Deprecated Documentation

Important

Note that as of June 10, 2017, the support for Red Hat Directory Server 9 has ended. For details, see *"Red Hat Directory Server Life Cycle policy"*. Red Hat recommends users of Directory Server 9 to update to the latest version.

Due to the end of the maintenance phase of this product, this documentation is no longer updated. Use it only as a reference!

2. New in Red Hat Directory Server 9.1

Directory Server 9.1 has introduced many features to make managing the directory service and its data easier.

2.1. New: Auto Membership Plug-in

Being able to assign new entries to groups, automatically, at the time that an account is created ensures that the appropriate policies and functionality are immediately applied to those entries — without requiring administrator intervention.

The Auto Membership Plug-in uses an LDAP search to identify new members for a given static group, and then automatically adds those new entries as members as soon as they are created.

Automembership essentially allows a static group to act similar a dynamic group, at least for adding new members. This can allow administrators to add users to specific user groups, to create special groups for Windows users as part of Windows integration, or to create host groups.

The Auto Membership Plug-in allows sub-filters on results. So, for example, host entries within one IP range could be added to a web servers group while host entries within another IP range could be added to a desktop group, and servers outside either range could be added to a fallback group.

Three tasks allow the Auto Membership Plug-in to run against existing users and update their group memberships:

- *rebuild membership*, which re-runs the Auto Membership Plug-in on existing entries to update the group membership; this is essentially a fix-up task
- *automember export updates*, which does a test-run of what the membership changes would be and writes them to a specified LDIF file
- *map updates*, which inputs the entries from an LDIF file, performs a test-run, and then writes what the results of the fix-up task would be to a given LDIF file

This can ease group administration as desired membership policies are created or modified.

2.2. New: Security Strength Factor Setting for the Root DSE

A new server configuration attribute, ***nsslapd-minssf-exclude-rootdse***, allows security strength factor (SSF) settings to be ignored for queries against the root DSE. This allows clients to access root DSE information which may be required for operations without having to use a secure connection.

2.3. Enhanced: logconv.pl Script Options

The **logconv.pl** script parses the access log for a Directory Server instance and provides a summary of connections, binds, operations (by type), and error or return codes.

The **logconv.pl** could return summaries for the entire log or only within a specified time range. New options have been added that show per-minute (**-M**) or per-second (**-m**) statistics, in addition to the summary, for the entire log or for the given time range. These per-minute or per-second statistics are exported to a CSV file, which can be imported into other programs for further analysis.

Additionally, summary statistics have been added for three more operation types:

- Compares
- Mod DN
- Proxy authenticated operations

2.4. Enhanced: Access Logging Information

The access log information for some operations types has been enhanced:

- Compare operations now log the DN of the user which initiated the operation.
- Proxy operations in the access log now include the proxy ID as whom the operation was run (**authzid**) as well as the real use which ran the operation (**dn**).

2.5. Enhanced: Deleting Managed Entries Plug-in Configuration

The Managed Entries Plug-in uses child configuration entries to define instance-specific managed entries rules. Previously, these configuration entries could not be deleted, which meant that the only way that a managed entries configuration could be disabled was to set the scope to a null setting.

Now, Managed Entries Plug-in configuration entries can be deleted.

2.6. Enhanced: PAM Pass-Through Authentication Rules per Directory Suffix

PAM pass-through authentication allows a user authenticating to the Directory Server to be authenticated against the system credentials defined in a PAM module. (The authentication request is *passed-through* to the other identity provider.)

Previously, PAM pass-through authentication was enabled for and defined for the entire directory. Starting in Red Hat Directory Server 9.1, PAM pass-through authentication can be defined for entries within a suffix of the directory, rather than the entire directory.

The entries to which PAM pass-through applies are identified with the ***`pamFilter`*** plug-in attribute in the PAM Pass-Through Authentication Plug-in configuration entry. This allos a search filter which can target a specific user, specific attribute and value, or a suffix in the tree.

Because of the new flexibility in where to apply PAM pass-through authentication rules, the PAM Pass-Through Authentication Plug-in has been enhanced to allow multiple configuration entries. This allows there to be multiple directory filters, mapping methods, and other settings, depending on specific needs within the directory.

2.7. New: Setting an ACI for the Directory Manager

Access control instructions are set at different points in the directory tree, at the root suffix, subsuffixes, or even user (leaf) levels. ACIs can also be set on configuration suffixes, such as **`cn=config`**. However, with that structure for ACI targets, it was not possible to set any ACI on the Directory Manager user because that is a special user which exists outside the directory tree.

Beginning with this update, there is a new plug-in, RootDN Access Control Plug-in, which defines some access control rules for the root user (Directory Manager) account. This allows restrictions based on time of day and host or IP address of the source machine, for enhanced security.

2.8. New: Disabling Replication Agreements

In previous versions of Directory Server there was no explicit way to disable a replication agreement. The only methods to suspend replication were to change the schedule or to delete the agreement entirely.

The ***`nsds5ReplicaEnabled`*** attribute is introduced in this update, which works as a switch to enable or disable a replication agreement. This allows a master server to be removed from the topology for maintenance or updates without having to completely dismantle the replication configuration for that server.

2.9. New: CLEANRUV Clean-up Task

When a server is removed from the replication topology, the metadata for that server and its update operations (the RUV) still remain on the other servers. Retaining that server and RUV information can create unstable behavior with other master servers in certain situations.

Two new tasks have been introduced for cleaning out lingering RUVs:

- CLEANRUV, which removes the RUVs for the specified replica on a single master

- CLEANALLRUV, which removes the RUVs for the specified replica on a master **and then replicates that operation to all other masters and hubs in the replication topology**

These tasks can be initiated by creating a task entry in **cn=tasks**. Alternatively, the task to remove a dead replica from the RUV of another replica can be initiated by adding an attribute for the task to the second replica entry:

```
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsds5task: CLEANALLRUVreplicaID
```

2.10. New: Account Usability Control for LDAP Searches

This update to Directory Server introduced a new **ldapsearch** control which allows credential-less bind attempts to return authentication information about an account.

Most of the time, for the Directory Server to return authentication information about a user account, a client actually binds (or attempts to bind) as that user. And a bind attempt requires some sort of user credentials, usually a password or a certificate. While the Directory Server allows unauthenticated binds and anonymous binds, neither of those binds returns any user account information.

There are some situations where a client requires information about a user account — specifically whether an account should be allowed to authenticate — in order to perform some other operation, but the client either does not have or does use any credentials for the user account in Directory Server. Essentially, the client needs to perform a credential-less yet authenticated bind operation to retrieve the user account information (including password expiration information, if the account has a password).

This can be done through an **ldapsearch** by passing the *Account Usability Extension Control*. This control acts as if it performs an authenticated bind operation for a given user and returns the account status for that user, but without actually binding to the server. This allows a client to determine whether that account can be used to log in and then to pass that account information to another application, like PAM.

Important

The OpenLDAP tools used by Directory Server do not support the Account Usability Extension Control. Other LDAP utilities, like OpenDS, or other clients which do support the control can be used.

2.11. New: Operational Attribute for the Last Password Change Time

Previously, any change to an entry updated the ***modifyTimeStamp*** operational attribute.

Starting with this update, a new operational attribute, ***pwdUpdateTime***, is used specifically for the last modify time of passwords, separate from the overall entry modify time. This gives password and lockout policies another attribute to evaluate for account inactivity or password expiration.

Tracking the last password change time is enabled in the ***passwordTrackUpdateTime*** configuration attribute.

2.12. Enhanced: simple paged results

Simple paged results break search results into smaller chunks, with a certain number of results per page, to make it easier to read and browse search results.

This update allows simple paged results (an **ldapsearch** control) to be combined with server-side sorting on results (another **ldapsearch** control).

2.13. Enhanced: Tracking Changes by Bind DN

In previous versions of Directory Server, whenever an entry was created or modified, there was an operational attribute added to the entry with the modifying entry's name. However, the ***creatorsName*** and ***modifiersName*** attributes only showed whatever entry directly edited the entry. If an entry was edited through a plug-in — such as the MemberOf Plug-in updating a user entry when a group entry is edited — ther the ***modifiersName*** attribute showed the plug-in name — but not the identity of whatever user triggered the plug-in operation.

The new ***internalModifiersName*** operational attribute shows the name of whatever Directory Server plug-in performed an operation, while the ***modifiersName*** attribute now reflects whatever *bound user* initiated the operation.

```
dn: uid=bjensen,ou=people,dc=example,dc=com
...
modifiersname: uid=jsmith,ou=people,dc=example,dc=com
internalModifiersname: cn=memberof plugin,cn=plugins,cn=config
```

Tracking the bind DN is enabled by setting the ***nsslapd-plugin-binddn-tracking*** configuration attribute.

2.14. Enhanced: Synchronization of Posix Attributes

On Linux systems, system users and groups are identified as Posix entries, and LDAP Posix attributes contain that required information. When Windows users are synced over, they have ***ntUser*** and ***ntGroup*** attributes automatically added which identify them as Windows accounts. However, by default, no Posix attributes are synced over (even if they exist on the Active Directory entry) and no Posix attributes are added on the Directory Server side.

The new Posix Winsync API Plug-in synchronizes Posix attributes set on Active Directory over to the corresponding Directory Server entry.

Note

Syncing Posix attributes is uni-directional. **It syncs Posix attributes from Active Directory entries to Directory Server entries.** An Posix attributes added or modified on a Directory Server entry are not synced over to the corresponding Active Directory entry.

2.15. Enhanced: Support for IPv6 for Additional Directory Operations

Initial support for IPv6 addresses was added in Red Hat Directory Server 9.0, but not all directory operations could be performed over IPv6. This update extends IPv6 support to the remaining directory tasks, including replication, installation, chaining databases, and access control instructions.

Note

Note that the Windows Console provided as part of Red Hat Directory Server does not support IPv6-only networks.

2.16. New: Configuration for Disk Monitoring

If the disk space on the system where the Directory Server is running reaches a critical point, the **slapd** process can crash and, potentially, corrupt the directory database and lose information.

These updates to Directory Server introduce the ability to monitor disk space in the partition or mount point where the **slapd** process is running. If the disk space reaches an administrator-defined threshold, then the **slapd** process shuts down gracefully — preserving the database and directory data.

A new set of configuration options, ***nsslapd-disk-monitoring****, set whether disk monitoring is enabled for the **slapd** process and the disk space thresholds, grace periods for disk space warnings, and whether to lower logging levels and disable logging before shutting down the server.

2.17. Enhanced: Disabling Legacy-Style Password Lockouts

There are different ways of interpreting when the maximum password failure (***passwordMaxFailure***) has been reached. It depends on how the server counts the last failed attempt in the overall failure count.

The traditional behavior for LDAP clients is to assume that the failure occurs after the limit has been reached. So, if the failure limit is set to three, then the lockout happens at the fourth failed attempt. This also means that if the fourth attempt is successful, then the user can authenticate successfully, even though the user technically hit the failure limit. This is basically *n+1* on the count.

LDAP clients increasingly expect the maximum failure limit to look at the last failed attempt in the count as the final attempt. So, if the failure limit is set to three, then at the third failure, the account is locked. A fourth attempt, even with the correct credentials, fails. This is *n* on the count.

A new attribute, ***passwordLegacyPolicy***, is available in Red Hat Directory Server to disable the legacy password policy behavior and allow newer LDAP clients to interact properly with password policies in Directory Server.

2.18. Enhanced: Support for PLAIN Mechanism with SASL Authentication

Support has been added for the PLAIN mechanism with SASL authentication. While not recommended for most situations, SASL/PLAIN can be useful for anonymous connections or for times when a UID, rather than a DN, is used for authentication.

2.19. Enhanced: Changed DNA Plug-in Configuration

Previously, the Distributed Number Assignment (DNA) Plug-in was configured in a plug-in entry with the **extensibleObject** object class. The schema has been enhanced so that there is a new, plug-in specific object class called **dnaPluginConfig**.

2.20. Enhanced: Rejecting Modifications to Specified Attributes for Replication

Changes to some attributes may not represent real changes to an entry — such as an automatic change to the modify timestamp attribute from a plug-in, when no other attributes were modified.

To reduce replication load and to improve the performance of some applications, it is beneficial to ignore changes to those attributes when replicating entries. A list of attributes can be configured which can be ignored when the server evaluates entries to enter into the changelog and trigger replication. This list is defined in the ***nsds5ReplicaStripAttrs*** attribute on the replication agreement entry.

2.21. Enhanced: Setting TLSv1 for Secure Connections

Previously, both SSL encryption and TLS encryption were set together and defined with the same (SSL-specific) attributes. A new attribute, ***nsTLS1***, has been introduced which enables TLS connections, independently of SSL connections. This allows the stronger TLS protocol to be used and SSL to be disabled.

2.22. Enhanced: Performing MemberOf Evaluations Across Backends

Previously, the MemberOf Plug-in evaluated group membership based solely on groups and users defined within the local backend. For distributed deployments, this meant that group membership was incompletely evaluated because there could well be identities in a different subsuffix than a group it belongs to.

A new plug-in attribute has been added, ***memberOfAllBackends***, which sets whether the MemberOf Plug-in should evaluate the local suffix only or all subsuffixes for membership information. When set to **on**, the plug-in evaluates every suffix and backend.

2.23. Enhanced: Added nsslapd-readonly to External Schema

Previously, the ***nsldap-readonly*** configuration attribute was not part of the external schema. The read-only setting is used by replication to signal whether the given server can accept modify operations from users (supplier) or whether it can only receive updates from a master server (consumer).

Because the ***nsslapd-readonly*** attribute was not public, it could not be used in access control configuration, which meant that it was not possible to grant certain users the appropriate rights to manage replication without making them server administrators.

The ***nsslapd-readonly*** attribute has been added to the external schema, so it can now be used to create ACIs.

3. System Requirements

This section contains information related to installing and upgrading Red Hat Directory Server 9.1, including prerequisites and hardware or platform requirements.

3.1. Required JRE

Red Hat Directory Server 9.1 requires Oracle Java Runtime Environment (JRE) 1.8.0 or OpenJDK 1.8.0 for Red Hat Enterprise Linux 6.

Important

When the new JRE is installed for Directory Server 9.1, it is no longer possible to manage older instances of Directory Server using the Directory Server Console because the required JREs for the different Directory Server versions are different. You must migrate any older instance to Directory Server 9.1 if you need to manage that instance with the Directory Server Console.

3.2. Perl Prerequisites

Directory Server 9.1 does not package **nsperl** with the product. **perldap** should work with the version of **perl** pre-installed on the system.

Use the Perl version that is installed with the Red Hat Enterprise Linux operating system in **`/usr/bin/perl`** for both 32-bit and 64-bit versions of Red Hat Directory Server.

3.3. Fonts

A font package must be installed before the Directory Server Console can be launched. Any font package is acceptable.

3.4. Software Conflicts

Directory Server cannot be installed on any system that has a Red Hat Enterprise Linux Identity Management server installed. (The Identity Management server is also called an *IPA server*.)

Likewise, no Red Hat Enterprise Linux Identity Management server can be installed on a system with a Directory Server instance.

3.5. Directory Server Supported Platforms

Directory Server 9.1 is supported on the following platforms:

- Red Hat Enterprise Linux 6 x86 (32-bit)
- Red Hat Enterprise Linux 6 x86_64 (64-bit)

Note

Red Hat Directory Server 9.1 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.

3.6. Directory Server Console Supported Platforms

The Directory Server Console is supported on the following platforms:

- Red Hat Enterprise Linux 6 i386 (32-bit)
- Red Hat Enterprise Linux 6 x86_64 (64-bit)
- Microsoft Windows Server 2008 R2 (64-bit)

Note

The Directory Server Console can be installed on additional Windows platforms at an additional cost.

3.7. Windows Sync Service Platforms

The Windows Sync tool runs on these Windows platforms:

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

3.8. Web Application Browser Support

Directory Server 9.1 supports the following browsers to access web-based interfaces, such as **Admin Express** and online help tools:

- Firefox 17 and higher
- Microsoft Internet Explorer 8 and higher

4. Installing Directory Server 9.1

For more detailed instructions on installing Directory Server 9.1, see the *Directory Server Installation Guide*.

4.1. Installing the JRE

Directory Server 9.1 requires either Oracle Java Runtime Environment (JRE) 1.8.0 or OpenJDK 1.8.0.

For example:

```
[root@server ~]# yum install java-1.8.0-openjdk
```

OpenJDK is also available for download from http://openjdk.java.net/install/.

Important

When the new JRE is installed for Directory Server 9.1, it is no longer possible to manage older instances of Directory Server using the Directory Server Console because the required JREs for the different Directory Server versions are different. You must migrate any older instance to Directory Server 9.1 if you need to manage that instance with the Directory Server Console.

4.2. Installing Packages

1. Register your system using **`subscription-manager`** and attach the appropriate subscriptions to your system. For example:

```
[root@server ~]# subscription-manager register --auto-attach
[root@server1 ~]# subscription-manager list --available

+-------------------------------------------+
    Available Subscriptions
+-------------------------------------------+
....
ProductName:            Red Hat Directory Server
ProductId:              MKT-rhds
```

```
PoolId:                 abcd1234
Quantity:               10
Expires:                2017-09-21
[root@server1 ~]# subscription-manager attach --pool=abcd1234
```

2. If necessary, enable the appropriate **yum** repo. For example, for a 64-bit system:

```
[root@server ~]# subscription-manager repos --enable rhel-x86_64-
server-6-rhdirserv-9
```

3. Use the **yum** command to install all of the Red Hat server and console packages:

```
[root@server ~]# yum install redhat-ds* redhat-idm-console
```

The **PassSync.msi** installer is available in the WinSync package in the Directory Server channel, through the **Downloads** tab. Download this file to the Windows machine, and then double-click the icon and go through the installer.

There are two PassSync packages available, one for 32-bit Windows servers and one for 64-bit. Make sure to select the appropriate packages for your Windows platform.

Note

PassSync is supported on Microsoft Windows Server 2008 R2 only.

4.3. Running setup-ds-admin.pl to Create a Server Instance

After installing the packages, run the **setup-ds-admin.pl** script to configure the new Directory Server and Admin Server instances. For example:

```
setup-ds-admin.pl
```

At least one Admin Server instance is required, but after that first Admin Server is created, then additional Directory Server instances can be created using **setup-ds.pl**. The Directory Server instances then point to the Configuration Directory Server and Admin Server.

See the *Directory Server Installation Guide* for more information about **setup-ds-admin.pl** script options and the Directory Server configuration interface.

4.4. Upgrading from Directory Server 8.2 to Directory Server 9.1

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

Note

Upgrade is only supported from 8.2 to 9.1. Other versions of Red Hat Directory Server should be migrated to 8.2 and then upgraded to 9.1.

5. Basic Information about Red Hat Directory Server

This is some basic information for using and managing Directory Server. The Directory Server information is explained in much more detail in the *Administrator's Guide*.

Starting and Stopping the Directory Server and Admin Server

The Directory Server and Admin Server instances are started and stopped using basic service command line tools. For example, on Red Hat Enterprise Linux:

```
service dirsrv-admin start
service dirsrv start
```

Running just **`service dirsrv start`** starts all instances of the Directory Server on the host machine. To start a single instance, use the name of the instance in the command:

```
service dirsrv start example
```

Starting the Directory Server Console

To start the Directory Server Console, run the **`redhat-idm-console`** command.

```
redhat-idm-console
```

It is also possible to specify the user to log into the Console as using the **`-u`** and **`-w`** options and to give the URL to the Admin Server using the **`-a`** option.

```
redhat-idm-console -u "cn=Directory Manager" -w secret -a
http://ldap.example.com:9830
```

Default Port Numbers

These are the default port numbers for the Directory Server and Admin Server:

- The standard LDAP port is **`389`**.
- The secure (SSL) LDAPS port is **`636`**.
- The Admin Server port is **`9830`**.

Directory Server File Locations

Red Hat Directory Server 9.1 conforms to the Filesystem Hierarchy Standards. For more information on FHS, see the FHS homepage, http://www.pathname.com/fhs/. The files and directories installed with Directory Server are listed in the tables below for each supported platform.

Table 1. Basic Directory Locations

File or Directory	Location
Log files	/var/log/dirsrv/slapd-*instance*
Configuration files	/etc/dirsrv/slapd-*instance* /var/lib/dirsrv/slapd-*instance*

File or Directory	Location
Instance directory	/usr/lib/dirsrv/slapd-*instance* on 32-bit systems /usr/lib64/dirsrv/slapd-*instance* on 64-bit systems
Database files	/var/lib/dirsrv/slapd-*instance*/db
Certificate and key databases	/etc/dirsrv/slapd-*instance*
Schema files	/etc/dirsrv/slapd-*instance*/schema
Runtime files	/var/lock/dirsrv/slapd-*instance* /var/run/dirsrv/
Tools	/usr/bin/ /usr/sbin/

UTF-8 and Language Support

Directory Server supports all international charactersets by default because directory data is stored in UTF-8. UTF-8 characters are fully supported for all DNs and DN components. Web services can be customized to display charactersets other than UTF-8, though UTF-8 and Latin-1 are the default for Directory Server web applications.

Directory Server can also use specified matching rules and collation orders based on language preferences in search operations.

The locales and charactersets supported by Directory Server are listed in more detail in Appendix D, "Internationalization," in the *Administrator's Guide*.

6. Bugs Fixed in 9.1

Directory Server 9.1 contains bug fixes for components in the directory service and associated tools. The list of bugs fixed in Directory Server 9.1 are listed in the erratum for this release, RHBA-2013:0960. The list of issues that are addressed in the Directory Server 9.1 update is in Table 2, “Bugs Fixed in This Release”.

Additionally, this release rolls in fixes that have been fixed incrementally in errata for Red Hat Enterprise Linux 6.3, Red Hat Enterprise Linux 6.4, and Z-stream (minor update) releases of the **`389-ds-base`** package. These different errata and important fixed issues are listed in the subsequent tables.

- Table 3, “Bugs Fixed in Red Hat Enterprise Linux 6.3 Errata”
- Table 4, “Bugs Fixed in Red Hat Enterprise Linux 6.4 Errata”

Table 2. Bugs Fixed in This Release

Bug Number	Description
182509	The changelog used for replication stored passwords in clear text in order to replicate them. In some contexts, this could be a security risk.
510182	If the DNA Plug-in was triggered during an account creation or update operation but that operation failed, the DNA counter was still incremented. This resulted in a gap in the range, where the number was used up but not assigned to an entry attribute.

Bug Number	Description
830350	An issue in the htmladmin CGI caused a segmentation fault when restarting an Admin Server instance which used an IP address instead of a hostname.
887394	A problem in a CGI for the Admin Server Console caused a segmentation fault when attempting to restart the server.
889575	The **`remove-ds-admin.pl`** script, by default, leaves the security databases (**`cert8.db`**, **`key3.db`**, and **`secmod.db`**) intact after removing an instance. This prevents a new instance from being created later. A new option, **`-a`**, has been added to the **`remove-ds-admin.pl`** script to remove all generated data for an instance, allowing Admin Server to be re-installed later.
905266	Internally, the Admin Server only checked for the results of a bind operation if an LDAP control was also sent with the connection. If there were no LDAP controls sent, then the operation reported a successful bind even if the bind, in fact, failed. Now, the Admin Server and admin utilities always check the bind result, regardless of whether LDAP controls are sent with the request.
928560	Removing the Admin Server using the **`remove-ds-admin.pl`** script did not also stop the Admin Server process. This left the process running indefinitely and kept port 9830 tied up.
953600	An improperly configred SELinux policy caused AVCs when an administrator attempted to shut down the Admin Server from the Console. This prevented the Admin Server from restarting.

Table 3. Bugs Fixed in Red Hat Enterprise Linux 6.3 Errata

RHBA-2012:1067	
Bugzilla	**Description**
834096	Simultaneous updates that included deleting an attribute in an entry could cause the domain directory server to abort with a segmentation fault. This update checks whether a modified attribute entry has a NULL value. Now, the server handles simultaneous updates as expected.
836251	The get_entry function did not accept a NULL pblock. As a consequence, the Account Usability feature did not return the correct information about user account expiration and locked status.
RHSA-2012:0997	
Bugzilla	**Description**
CVE-2012-2678	A flaw was found in the way Directory Server handled password changes. If an LDAP user has changed their password, and the Directory Server has not been restarted since that change, an attacker able to bind to the Directory Server could obtain the plain text version of that user's password via the "unhashed#user#password" attribute.
CVE-2012-2746	When the password for an LDAP user was changed, and audit logging was enabled (it is disabled by default), the new password was written to the audit log in plain text form. This update introduces a new configuration parameter, "nsslapd-auditlog-logging-hide-unhashed-pw", which when set to "on" (the default option), prevents Directory Server from writing plain text passwords to the audit log. This option can be configured in /etc/dirsrv/slapd-ID/dse.ldif.

RHSA-2012:0813	
Bugzilla	**Description**
CVE-2012-0833	A flaw was found in the way the Directory Server daemon (ns-slapd) handled access control instructions (ACIs) using certificate groups. If an LDAP user that had a certificate group defined attempted to bind to the Directory Server, it would cause ns-slapd to enter an infinite loop and consume an excessive amount of CPU time.
743979	Previously, Directory Server used the Netscape Portable Runtime (NSPR) implementation of the read/write locking mechanism. This implementation allowed deadlocks to occur if Directory Server was under a heavy load, which caused the server to become unresponsive. With this update, Directory Server now uses the POSIX implementation of the locking mechanism, and deadlocks no longer occur under a heavy load.
745201	Previously, Distinguished Names (DNs) were not included in access log records of LDAP compare operations. Consequently, this information was missing in the access logs. Now, DNs are logged and can be found in the access logs.
752577	When Directory Server was under heavy load and operating in a congested network, problems with client connections sometimes occurred. When there was a connection problem while the server was sending simple paged result search results to the client, the LDAP server called a cleanup routine incorrectly. Consequently, a memory leak occurred and the server terminated unexpectedly. Now, cleanup tasks are run correctly and no memory leaks occur.
757897	Previously, certain operations with the change sequence number were not performed efficiently by the server. Consequently, the ns-slapd daemon consumed up to 100% of CPU time when performing a large number of CSN operations during content replication. With this update, the underlying source code has been modified to perform the CSN operations efficiently. As a result, large numbers of CSN operations can be performed during content replications without any performance issues.
757898	Allocated memory was not correctly released in the underlying code for the SASL GSSAPI authentication method when checking Simple Authentication and Security Layer (SASL) identity mappings. This problem could cause memory leaks when processing SASL bind requests, which eventually caused the LDAP server to terminate unexpectedly with a segmentation fault. This update adds function calls that are needed to free allocated memory correctly.
759301	Directory Server did not handle the entry update sequence number (USN) index correctly. Consequently, the index sometimes became out of sync with the main database and search operations on USN entries returned incorrect results. This update modifies the underlying source code of the Entry USN plug-in. As a result, the Entry USN index is now handled by the server correctly.
772777	Previously, search filter attributes were normalized and substring regular expressions were compiled repeatedly for every entry in the search result set. Consequently, using search filters with many attributes and substring subfilters resulted in poor search performance. This update ensures that search filters are pre-compiled and pre-normalized before being applied. These changes result in better search performance when applying search filters with many attributes and substring subfilters.

RHSA-2012:0813	
Bugzilla	**Description**
772778	Previously, the number of access control instructions to be cached was limited to 200. Consequently, evaluating a Directory Server entry against more than 200 ACIs failed with the following error message: *acl_TestRights - cache overflown* The default ACI cache limit has been increased to 2000 and allows it to be configurable by means of the new parameter ***nsslapd-aclpb-max-selected-acls*** in the ACL Plug-in configuration.
772779	Previously, the restore command contained a code path leading to an infinite loop. Consequently, Directory Server sometimes became unresponsive when performing a restore from a database backup.
781485	Previously, performing the ldapmodify operation to modify replica update vector (RUV) entries was allowed. Consequently, Directory Server became unresponsive when performing such operations.
781495	Previously, to identify restart events of Directory Server, the logconv.pl script searched server logs for the "conn=0 fd=" string. Consequently, the script reported a wrong number of server restarts. This update modifies the script to search for the "conn=1 fd=" string instead. As a result, the correct number of server restarts is now returned.
781500	When reloading a database from an LDIF file that contained an RUV element with an obsolete or decommissioned replication master, the changelog was invalidated. As a consequence, Directory Server emitted error messages and required re-initialization. This update ensures that the user is properly informed about obsolete or decommissioned replication masters, and that such masters are deleted from the RUV entries.
781516	Previously, when a non-leaf node became a tombstone entry, its child entries lost the parent-child relationships. Consequently, non-leaf tombstone entries could have been reaped prior to their child tombstone entries. This update fixes the underlying source code so that parent-child relationships are maintained even when a non-leaf entry is deleted. As a result, tombstones are now reaped correctly in the bottom-up order.
781529	Previously, no validation of managed entry attributes against the managed entry template was performed before updating Directory Server's managed entries. Consequently, managed entries could have been updated after updating an original entry attribute that was not contained in the managed entry template.
81533	Previously, Directory Server did not shut down before all running tasks had been completed. Consequently, it sometimes took a long time for the Directory Server to shut down when a long-running task was being carried out.
781537	Directory Server expected the value of the authzid attribute to be fully BER-encoded. Consequently, the following error was returned when performing the ldapsearch command with proxy authorization: *unable to parse proxied authorization control (2 (protocol error))*
781538	Previously, the buffer for matching rule OIDs had a fixed size of 1024 characters. Consequently, matching rule OIDs got truncated when their total length exceeded 1024 characters.
781539	Executing the ldapsearch command on the "cn=config" object returned all attributes of the object, including attributes with empty values. This update ensures that attributes with empty values are not saved into "cn=config" and enhances the ldapsearch command with a check for empty attributes.
781541	Log records of proxy operations displayed the bound user as the one who performed the operation, rather than the proxy user. This behavior has been changed.

RHSA-2012:0813	
Bugzilla	**Description**
784343	The database upgrade scripts checked if the server was offline by checking for the presence of .pid files. In some cases, however, the files remain present even if the associated processes have already been terminated. Consequently, the upgrade scripts sometimes assumed that the Directory Server was online and did not proceed with the database upgrade even if the server was actually offline.
784344	Previously, the repl-monitor command used only the subdomain part of hostnames for host identification. Consequently, hostnames with the identical subdomain part (for example: "ldap.domain1", "ldap.domain2") were identified as a single host, and inaccurate output was produced.
788140	The server used unnormalized DN strings to perform internal search and modify operations while the code for modify operations expected normalized DN strings. Consequently, error messages like the following one were logged when performing replication with domain names specified in unnormalized format: *NSMMReplicationPlugin - repl_set_mtn_referrals: could not set referrals for replica dc=example,dc=com: 32*
788724	The code for extensible search filters used strcmp routines for value comparison. Consequently, using extensible search filters with binary data returned incorrect results.
788725	Value normalization of the search filter did not respect the used filter type and matching rules. When using different values than the default comparison type for the searched attribute syntax, search attempts returned incorrect results.
788729	Tombstones of child entries in a database were handled incorrectly. Therefore, if the database contained deleted entries that were converted to tombstones, an attempt to reindex the entryrdn index failed with the following error message: *_entryrdn_insert_key: Getting "nsuniqueid=ca681083-69f011e0-8115a0d5-f42e0a24,ou=People,dc=example,dc=com" failed*
788731	RUV tombstone entries were indexed incorrectly by the entryrdn index. Consequently, attempts to search for such entries were not successful.
788741	The Distributed Numeric Assignment Plug-in used too short timeout for requests to replicate a range of UIDs. Consequently, using replication with DNA to add users sometimes failed on networks with high latency, returning the following error message: *Operations error: Allocation of a new value for range cn=posix ids,cn=distributed numeric assignment plugin,cn=plugins,cn=config failed* With this update, the default timeout for such replication requests has been set to 10 minutes.
788745	Change sequence numbers in the RUV were not refreshed when a replication role was changed, leading to inconsistent data.
788749	Errors in schema files were not reported clearly in log files. Consequently, the messages could be incorrectly interpreted as reporting an error in the dse.ldif file.
788750	The server used an outdated version of the nisDomain schema after an upgrade. Consequently, restarting Directory Server after an upgrade produced the following error message: *attr_syntax_create - Error: the EQUALITY matching rule [caseIgnoreMatch] is not compatible with the syntax [1.3.6.1.4.1.1466.115.121.1.26] for the attribute [nisDomain]*
788751	Directory Server previously did not properly release allocated memory after finishing normalization operations. This caused memory leaks to occur during server's runtime.

RHSA-2012:0813	
Bugzilla	**Description**
788753	The "connection" attribute was not included in the cn=monitor schema, which caused the access control information (ACI) handling code to ignore the ACI. Consequently, requesting the connection attribute when performing anonymous search on cn=monitor returned the connection attribute, even though it was denied by the default ACI. This update ensures that the ACI is processed even if the attribute is not in the schema.
788755	Previously, IPv4-mapped IPv6 addresses were treated as independent addresses by Directory Server. Consequently, errors were reported during server startup when such addresses conflicted with standard IPv4 addresses.
790491	A NULL pointer dereference sometimes occurred when initializing a Directory Server replica. Consequently, the server terminated unexpectedly with a segmentation fault.
796770	A double free error sometimes occurred during operations with orphaned tombstone entries. Consequently, when an orphaned tombstone entry was passed to the tombstone_to_glue function, the Directory Server terminated unexpectedly.
800215	An internal loop was incorrectly handled in the ldapcompare command. Consequently, performing concurrent comparison operations on virtual attributes caused the Directory Server to become unresponsive.
803930	When upgrading Directory Server, server startup had been initiated before the actual upgrade procedure finished. Consequently, the startup failed with the following error message: *ldif2dbm - _get_and_add_parent_rdns: Failed to convert DN cn=TESTRELM.COM to RDN*
811291	The range read operation did not correctly handle situations when an entry was deleted while a ranged search operation was being performed. Consequently, performing delete and ranged search operations concurrently under heavy loads caused the Directory Server to terminate unexpectedly.
813964	When performing delete and search operations against Directory Server under high load, the DB_MULTIPLE_NEXT pointer to the stack buffer could have been set to an invalid value. As a consequence, pointer's dereference lead to an attempt to access memory that was not allocated for the stack buffer. This caused the server to terminate unexpectedly with a segmentation fault. Now, if the pointer's value is invalid, the page or value is considered deleted and the stack buffer is reloaded.
815991	The ldap_initialize() function is not thread-safe. Consequently, Directory Server terminated unexpectedly during startup when using replication with many replication agreements. This update ensures that calls of the ldap_initialize() function are protected by a mutual exclusion.
819643 821542	An attempt to rename an RDN failed if the new string sequence was the same except of using the different lower/upper case of some letters. This update fixes the code so that it is possible to rename RDNs to the same string sequence with case difference.
822700	ACI handling did not reject incorrectly specified DNs. Consequently, incorrectly specified DNs in an ACI caused Directory Server to terminate unexpectedly during startup or after an online import.
824014	Previously, the code handling the entryusn attribute modified cache entries directly. Consequently under heavy loads, the server terminated unexpectedly when performing delete and search operations using the entryusn and memberof attributes with referential integrity enabled.

Table 4. Bugs Fixed in Red Hat Enterprise Linux 6.4 Errata

RHSA-2013:0503	
Bugzilla	**Description**
CVE-2012-4450	A flaw was found in the way Directory Server enforced ACLs after performing an LDAP modify relative distinguished name (modrdn) operation. After modrdn was used to move part of a tree, the ACLs defined on the moved DN were not properly enforced until the server was restarted. This could allow LDAP users to access information that should be restricted by the defined ACLs.
742381	Due to certain changes under the cn=config suffix, when an attribute value was deleted and then added back in the same modify operation, error 53 was returned. Consequently, the configuration could not be reset. This update allows delete operations to succeed if the attribute is added back in the same modify operation and reset the configuration file as expected.
757836	Previously, the logconv.pl script used a connection number equal to 0 (conn=0) as a restart point, which caused the script to return incorrect restart statistics. Directory Server is now configured to use connection number equal to 1 (conn=1) as the restart point.
803873	The Windows Sync feature uses the name in a search filter to perform an internal search to find an entry. Parentheses, (and), are special characters in the LDAP protocol and therefore must be escaped. However, an attempt to synchronize an entry containing parentheses in the name from an Active Directory erver failed with an error. With this update, Directory Server properly escapes the parentheses.
818762	When having an entry in a Directory Server with the same user name, group name, or both as an entry in Active Directory and simultaneously the entry in Active Directory was out of scope of the Windows Sync feature, the Directory Server entry was deleted. This update adds the new winSyncMoveAction Directory Server attribute for the Windows Sync agreement entry, which allows the user to specify the behavior of out-of-scope Active Directory entries. The value could be set to: - none, which means that an out-of-scope Active Directory entry does nothing to the corresponding Directory Server entry - delete, which means that an out-of-scope Active Directory entry deletes the corresponding Directory Server entry - unsync, which means that an out-of-scope Active Directory entry is unsynchronized with the corresponding Directory Server entry and changes made to either entry are not synchronized By default, the value is set to none.
830334	Due to an incorrect interpretation of an error code, Directory Server considered an invalid chaining configuration setting as the disk full error and shut down unexpectedly.
830335	Previously, restoring an LDIF file from a replica which had older changes that other servers did not see yet, could lead to these updates not being replicated to other replicas. With this update, Directory Server checks the change sequence numbers (CSNs) and allows the older updates to be replicated.
830336	When a Directory Server was under a heavy read and write load, and an update request was processed, a DB_LOCK_DEADLOCK error message appeared in the error log, such as: *entryrdn-index - _entryrdn_put_data: Adding the parent link (XXX) failed: DB_LOCK_DEADLOCK: Locker killed to resolve a deadlock (-30994)* These errors are common under these circumstances and there should not have been recorded in the error log.

RHSA-2013:0503	
Bugzilla	**Description**
830337	When a Directory Server was configured to use multi-master replication and the entry USN plug-in, a delete operation was not replicated to the other masters. This update prevents the USN plug-in from changing the delete operation into a delete tombstone operation and from removing the operation before it logs into the change log to replay to other servers. As a result, the delete operation is replicated to all servers as expected.
830338	Previously, Directory Server did not refresh its Kerberos cache. Consequently, if a new Kerberos ticket was issued for a host that had already authenticated against a Directory Server, it would be rejected by this server until it was restarted. With this update, the Kerberos cache is flushed after an authentication failure.
830343	Using the Managed Entry plug-in in conjunction with other plug-ins, such as Distributed Numeric Assignment (DNA), MemberOf, and Auto Member, led to problems with delete operations on entries that managed the Managed Entry plug-in. The manager entry was deleted, but the managed entry was not. The deadlock retry handling has been improved so that both entries are deleted during the same database operation.
830344	Previously, replication errors logged in the error log could contain incorrect information. With this update, the replication errors have been modified to be more useful in diagnosing and fixing problems.
830346	When audit logging in a Directory Server was enabled, LDAP add operations were ignored and were not logged. This update removes a regression in the audit log code that caused the add operation to be ignored, and LDAP add operations are now logged to the audit log as expected.
830348	Directory Servers with a large number of replication agreements took a considerable amount of time to shut down due to a long sleep interval coded in the replication stop code. This sleep interval has been reduced to speed up the system termination.
830349	Previously, in a SASL map definition, using a compound search filter that included the ampersand (&) character failed because the ampersand was escaped.
832560	When replication was configured and a conflict occurred, under certain circumstances, an error check did not reveal this conflict, because a to-be-deleted attribute was already deleted by another master. Consequently, the conflict terminated the server. This update improves error checks to prevent replication conflicts from crashing the server.
833202	Previously, internal entries that were in the cache were freed when retrying failed transactions due to a deadlock. This behavior caused problems in a Directory Server and this server could terminate under a heavy update load. With this update, the cached internal entries are no longer freed and directory servers do not crash in the described scenario.
833218	Due to improper deadlock handling, the database reported an error instead of retrying the transaction. Consequently, under a heavy load, the Directory Server got deadlock errors when attempting to write to the database. The deadlock handling has been fixed and Directory Server works as expected in such a case.
834047	Internal access control prohibited deleting newly added or modified passwords. This update allows the user to delete any password if they have the modify rights.

RHSA-2013:0503	
Bugzilla	**Description**
834054	Certain operations, other than ldapmodify operations, can cause the Directory Server to modify internal attributes. For example, a bind operation can cause updates to password failure counters. In these cases, Directory Server was updating attributes that could only be updated during an explicit ldapmodify operation, such as the modifyTimestamp attribute. This update adds a new internal flag to skip the update of these attributes on other than modify operations.
834056	Due to an invalid configuration setup in the Auto Memmber plug-in, the Directory Server became unresponsive under certain circumstances. With this update, the configuration file is validated, invalid configurations are not allowed, and the server no longer hangs.
834057	When using SNMP monitoring, Directory Server terminated at startup if there were multiple LDAP servers listed in the ldap-agent.conf file. With this update, the buffer between LDAP servers no longer resets and Directory Server starts up regardless of the number of LDAP servers listed in the configuration file.
834064	Previously, the dnaNextValue counter was incremented in the pre-operation stage. Consequently, if the operation failed, the counter was still incremented. Now, the dnaNextValue counter is not incremented if the operation fails.
834065	When a replication agreement was added without the LDAP bind credentials, the replication process failed with a number of errors. With this update, Directory Server validates the replication configuration and ensures that all needed credentials are supplied. As a result, Directory Server rejects invalid replication configuration before attempting to replicate with invalid credentials.
834075	Previously, the logconv.pl script did not grab the correct search base, and as a consequence, the searching statistics were invalid. A new hash has been created to store connections and operation numbers from search operations. As a result, logconv.pl now grabs the correct search base and no longer produces incorrect statistics.
838706	When using the Referential Integrity plug-in, renaming a user DN did not rename the user's DN in the user's groups, unless that case matched exactly. With this update, case-insensitive comparisons or DN normalizations are performed, so that the member attributes are updated when the user is renamed.
840153	Previously, the Attribute Uniqueness plug-in did comparisons of un-normalized values. Consequently, using this plug-in and performing the LDAP rename operation on an entry containing one of the attributes which were tested for uniqueness by this plug-in caused the LDAP rename operation to fail with the following error: *Constraint Violation - Another entry with the same attribute value already exists.* With this update, Attribute Uniqueness ensures that comparisons are performed between values which were normalized the same way, and LDAP rename works as expected.
841600	When the Referential Integrity plug-in was used with a delay time greater than 0, and the LDAP rename operation was performed on a user entry with DN specified by one or more group entries under the scope of the Referential Integrity plug-in, the user entry DN in the group entries did not change.
842438	To improve the performance, the entry cache size is supposed to be larger then the primary database size if possible. Previously, Directory Server did not alert the user that the size of the entry cache was too small. Consequently, the user could not notice that the size of the entry cache was too small and that they should enlarge it. With this update, the configured entry cache size and the primary database size are examined, and if the entry cache is too small, a warning is logged in the error log.

RHSA-2013:0503	
Bugzilla	**Description**
842440	Previously, the Memberof plug-in code executed redundant DN normalizations and therefore slowed down the system.
842441	Previously, the Directory Server could disallow changes that were made to the nsds5ReplicaStripAttrs attribute using the ldapmodify operation. Consequently, the attribute could only be set manually in the dse.ldif file when the server was shut down. With this update, the user is now able to set the nsds5ReplicaStripAttrs attribute using the ldapmodify operation.
850683	Previously, Directory Server did not check attribute values for the nsds5ReplicaEnabled feature which caused this feature to be disabled. With this update, Directory Server checks if the attribute value for nsds5ReplicaEnabled is valid and reports an error if it is not.
852088	When multi-master replication or database chaining was used with the TLS/SSL protocol, a server using client certificate-based authentication was unable to connect and connection errors appeared in the error log. With this update, the internal TLS/SSL and certificate setup is performed correctly and communication between servers works as expected.
852202	Previously, there was a race condition in the replication code. When two or more suppliers were attempting to update a heavily loaded consumer at the same time, the consumer could, under certain circumstances, switch to total update mode, erase the database, and abort replication with an error. The underlying source code has been modified to prevent the race condition. As a result, the connection is now protected against access from multiple threads and multiple suppliers.
852839	Due to the use of an uninitialized variable, a heavily loaded server processing multiple simultaneous delete operations could terminate unexpectedly under certain circumstances. This update provides a patch that initializes the variable properly.
855438	Due to an incorrect attempt to send the cleanallruv task to the Windows WinSync replication agreements, the task became unresponsive. With this update, the WinSync replication agreements are ignored and the cleanallruv task no longer hangs in the described scenario.
856657	Previously, the dirsrv init script always returned 0, even when one or all the defined instances failed to start. This update applies a patch that improves the underlying source code and dirsrv no longer returns 0 if any of the defined instances failed.
858580	The schema reload task reloads schema files in the schema directory. Simultaneously, Directory Server has several internal schemas which are not stored in the schema directory. These schemas were lost after the schema reload task was executed. Consequently, adding a posixAccount class failed. With this update, the internal schemas are stashed in a hash table and reloaded with external schemas. As result, adding a posixAccount is successful.
863576	When abandoning a simple paged result request, Directory Server tried to acquire a connection lock twice, and because the connection lock is not self reentrant, Directory Server was waiting for the lock forever and stopped the server. This update provides a patch that eliminates the second lock.
864594	Previously, anonymous resource limits applied to the Directory Manager. However, the Directory Manager should never have any limits. With this update, anonymous resource limits no longer apply to Directory Manager.

RHSA-2013:0503	
Bugzilla	**Description**
868841	Even if an entry in Active Directory did not contain all the required attributes for the POSIX account entry, the entry was synchronized to the Directory Server as a POSIX entry. Consequently, the synchronization failed due to a missing attribute error. With this update, if an entry does not have all the required attributes, the POSIX account related attributes are dropped and the entry is synchronized as an ordinary entry. As a result, the synchronization is successful.
870158	When a Directory Server was under a heavy load, deleting entries using the Entry USN feature caused tombstone entry indexes to be processed incorrectly. Consequently, the server could become unresponsive. This update fixes Directory Server to process tombstone indexes correctly, so that the server no longer hangs in this situation.
870162	Previously, the abandon request checked if the operation to abandon existed. When a search operation was already finished and an operation object had been released, a Simple Page Results request could fail due to this check. This update modifies Directory Server to skip operation existence checking, so that simple paged results requests are always successfully aborted.
875862	Previously, the DNA plug-in attempted to dereference a NULL pointer value for the dnaMagicRegen attribute. Consequently, if DNA was enabled with no dnamagicregen value specified in its configuration and an entry with an attribute that triggered the DNA value generation was added, the server could terminate unexpectedly. This update improves the Directory Server to check for an empty dnamagicregen value before it attempts to dereference this value.
876694	Previously, the code to check if a new superior entry existed, returned the *No such object error* only when the operation was requested by the Directory Manager. Consequently, if an ordinary non-root user attempted to use the modrdn operation to move an entry to a non-existing parent, the server terminated unexpectedly. This update provides a patch that removes the operator condition so that the check returns the *No such object* error even if the requester is an ordinary user, and the modrdn operation performed to the non-existing parent successfully fails for any user.
876727	If a filter contained a range search, the search retrieved one ID per one idl_fetch attribute and merged it to the ID list using the idl_union() function. This process is slow, especially when the range search result size is large. With this update, Directory Server switches to ALLID mode by using the nsslapd-rangelookthroughlimit switch instead of creating a complete ID list. As a result, the range search takes less time.
891930	An attempt to add a new entry to the DNA plug-in when the range of values was depleted returned a vague error about failing to allocate a new value for the range. The error message has been improved with more details about the failure.
896256	Previously, an upgrade of the 389-ds-base packages affected configuration files. Consequently, custom configuration files were reverted to by default. This update provides a patch to ensure that custom changes in configuration files are preserved during the upgrade process.
834061	Previously, Directory Server did not include the SO_KEEPALIVE settings and connections could not be closed properly. This enhancement implements the SO_KEEPALIVE settings to the Directory Server connections.
RHBA-2012:1345-1	

RHBA-2012:1345-1	
757773	Prior to this update, the Red Hat Directory Server Console showed the same SSL port for two simultaneous Directory Server instances, which could lead to LDAP operation conflicts. As a consequence, SSL configuration, certificate management and other operations could fail. This update fixes the Console so that it will use different SSL ports.
806566	Prior to this update, the Red Hat Directory Server Console did not support the class of service (CoS) merge-schemes qualifier. As a consequence, a CoS configured through the CLI to use the merge-schemes qualifier would strip the cosAttribute attribute when the CoS was viewed or modified in the Console.
RHSA-2013:0503-3	
CVE-2012-4450	A flaw was found in the way Directory Server enforced ACLs after performing an LDAP modify relative distinguished name (modrdn) operation. After modrdn was used to move part of a tree, the ACLs defined on the moved (Distinguished Name) were not properly enforced until the server was restarted. This could allow LDAP users to access information that should be restricted by the defined ACLs.
RHSA-2013:0742-2	
CVE-2013-1897	It was found that the Directory Server did not properly restrict access to entries when the nsslapd-allow-anonymous-access configuration setting was set to rootdse. An anonymous user could connect to the LDAP database and, if the search scope is set to base, obtain access to information outside of the root DSE.
929107	Previously, the schema-reload plug-in was not thread-safe. Consequently, executing the schema-reload.pl script under heavy load could cause the ns-slapd process to terminate unexpectedly with a segmentation fault.
929111	An out of scope problem for a local variable, in some cases, caused the modrdn operation to terminate unexpectedly with a segmentation fault. This update declares the local variable at the proper place of the function so it does not go out of scope, and the modrdn operation no longer crashes.
929114	A task manually constructed an exact value to be removed from the configuration if the replica-force-cleaning option was used. Consequently, the task configuration was not cleaned up, and every time the server was restarted, the task attempted to rebuild the value to remove again. This update searches the configuration for the exact value to delete, instead of manually building the value, and the task does not restart when the server is restarted.
929115	Previously, a NULL pointer dereference could have occurred when attempting to get effective rights on an entry that did not exist, leading to an unexpected termination due to a segmentation fault. This update checks for NULL entry pointers and returns the appropriate error.
929196	A problem in the lock timing in the DNA plug-in caused a deadlock if the DNA operation was executed with other plug-ins. This update moves the release timing of the problematic lock, and the DNA plug-in does not cause the deadlock.
RHSA-2013:0628-1	
CVE-2013-0312	A flaw was found in the way LDAPv3 control data was handled by Directory Server. If a malicious user were able to bind to the directory (even anonymously) and send an LDAP request containing crafted LDAPv3 control data, they could cause the server to crash, denying service to the directory.

RHSA-2013:0628-1	
910994	After an upgrade from Red Hat Enterprise Linux 6.3 to version 6.4, the upgrade script did not update the schema file for the pamConfig object class. Consequently, new features for PAM such as configuration of multiple instances and the pamFilter attribute could not be used because of the schema violation. With this update, the upgrade script updates the schema file for the pamConfig object class.
910996	The Directory Server failed when multi-valued attributes were replaced. The problem occurred when replication was enabled, while the server executing the modification was configured as a single master and there was at least one replication agreement. Consequently, the modification requests were refused by the master server, which returned a code 20 *Type or value exists* error message. These requests were replacements of multi-valued attributes, and the error only occurred when one of the new values matched one of the current values of the attribute, but had a different letter case.
911467	The DNA Plug-in, under certain conditions, could log error messages with the "DB_LOCK_DEADLOCK" error code when attempting to create an entry with a uidNumber attribute.
911468	Posix Winsync plugin was calling an intefilenamernal modify function which was not necessary. The internal modify call failed and logged an error message *slapi_modify_internal_set_pb: NULL parameter*, which was not clear. This patch stops calling the internal modify function if it is not necessary.
911469	Under certain conditions, the dse.ldif file had 0 bytes after a server termination or when the machine was powered off. Consequently, after the system was brought up, a Directory Server or IdM system could be unable to restart, leading to production server outages. Now, the server mechanism by which the dse.ldif is written is more robust, and tries all available backup dse.ldif files, and outages no longer occur.
911474	Due to an incorrect interpretation of an error code, a Directory Server considered an invalid chaining configuration setting as the disk full error and shut down unexpectedly. Now, a more appropriate error code is in use and the server no longer shuts down from invalid chaining configuration settings.
914305	While trying to remove a tombstone entry, the ns-slapd daemon terminated unexpectedly with a segmentation fault. With this update, removal of tombstone entries no longer causes crashes.

7. Known Issues

The following are some of the relevant known issues in Directory Server 9.1. If applicable, supported workarounds are also described.

Table 5. Known Issues in Directory Server 9.1

Bug Number	Description	Workaround
158369	The sync attribute mapping for groups includes a number of attributes that are not actually legal on group objects, such as l, ou, and o. If someone creates an ntGroup entry with any of these attributes that is not an ou, the synced entry add will fail on Active Directory because of a schema violation.	

Bug Number	Description	Workaround
190862	Global syntax checking attributes should be enforced if the settings aren't configured in the local password policy. However, if both global and local password policies are configured, the global policies aren't being enforced as the default.	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 settings, as listed in the *Configuration, Command, and File Reference*. 4. Re-edit the local password policy with the desired values, even if they are the defaults.
191772	If the configuration Directory Server is unavailable, Admin Express shows an internal server error. The task to access the Admin Express web page cannot be authenticated, so the attempt to open the page fails.	
667943	Restarting the Directory Server hangs if a pipe file is present but the **`ds-logpipe.py`** script is not running.	
712202	If a replication agreement is configured with an unresolvable hostname, it returns a generic error rather than an indication that the hostname cannot be resolved: `[09/Jun/2011:14:21:21 -0400] slapi_ldap_bind - Error: could not send bind request for id [(anon)] mech [EXTERNAL]: error -1 (Can't contact LDAP server) 0 (unknown) 0 (Success)`	Change the password policy attributes from the command line.
712845	The Directory Server Console does not allow you to set password policy-related time (such as expiration time or user change time) in hours, minutes, or seconds.	Change the password policy attributes from the command line.
622957 723029 724829	There are a lot of problems associated with trying to load certificates on hardware security modules (HSMs) using the Directory Server Console. Some of these are related to SELinux policies which restrict access to HSMs, and some are due to problems in the Directory Server Console or the Admin Server, which can throw exceptions or fail to generate requests or certificates.	Use NSS tools such as **`certutil`** to install certificates on HSMs rather than the Directory Server Console.

Bug Number	Description	Workaround
732079	Upgrading the server fails if the Directory Server user is **root**.	The Directory Server should run as the system user **nobody**.

743702	The ***nsslapd-counters*** attribute cannot be set to **off** or the server fails to restart with the error that the counters cannot be found:
	`[05/Oct/2011:10:07:28 -0400] - slapd stopped.`
	`[05/Oct/2011:10:07:42 -0400] - 389-Directory/1.2.9.12 B2011.276.2240 starting up`
	`[05/Oct/2011:10:07:42 -0400] - cache_init: slapi counter is not available.`
	`[05/Oct/2011:10:07:42 -0400] - ldbm_instance_create: cache_init failed`
		The ***nsslapd-counters*** attribute must be set to **on**.

743703	The Directory Server cannot run on the same machine as an NFS share. The Directory Server will stop servicing client requests.	Remove any NFS mount points on the server.

824048	When attempting to register a new Directory Server instance using **register.pl**, the operation fails because it cannot map the instance to an Admin Server ID.
	`[12/05/22:17:46:33] - [Setup] Info Registering new Config DS: dhcp201-194`
	`[12/05/22:17:46:43] - [Setup] Info Registering Sub DSes:`
	`[12/05/22:17:47:05] - [Setup] Fatal The map value 'ServerAdminID' for key 'as_uid' did not map to a value in any of the given information files.`
	`[12/05/22:17:47:05] - [Setup] Fatal Exiting . . .`	

893178	Encrypted attributes are decrypted when replicated to another master server. However, the attributes are not re-encrypted after being replicated, so they are in plaintext on the receiving server.	

Bug Number	Description	Workaround
905621	All POSIX attributes (such as ***uidNumber***, ***gidNumber***, and ***homeDirectory***) are synchronized between Active Directory and Directory Server entries. However, if a new POSIX entry or POSIX attributes are added to an existing entry in the Directory Server, *only the POSIX attributes are synchronized over to the Active Directory corresponding entry*. The POSIX object class (**posixAccount** for users and **posixGroup** for groups) is not added to the Active Directory entry.	This issue does not affect entries or synchronization and can be ignored.
908170	Some changes were made to enhance the DNA plug-in performance. One effect of these changes is that there must be an interval between dynamic DNA configuration changes of 35 seconds. This includes both DNA configuration changes and any directory entry changes which would trigger a DNA plug-in operation.	

908307	Attempting to stop the Admin Server through the Admin Express UI fails because it cannot resolve the IP address. There are errors in the log that read *ap_get_remote_host could not resolve 255.255.255.255*.
	
	`[Tue Feb 05 15:47:39 2013] [notice] [client 255.255.255.255] admserv_host_ip_check: ap_get_remote_host could not resolve 255.255.255.255, referer: http://admin-server.example.com:9830/admin-serv/tasks/configuration/HTMLAdmin?op=status`
	`[Tue Feb 05 15:47:39 2013] [notice] [client 255.255.255.255] admserv_host_ip_check: ap_get_remote_host could not resolve 255.255.255.255`
	`[Tue Feb 05 15:47:39 2013] [crit] [client 255.255.255.255] configuration error: couldn't check access.  No groups file?: /tasks/operation/Stop`
		Disable SELinux so that the Admin Express process can properly access the stop scripts and host information.

Bug Number	Description	Workaround
920597	The ACI validation only works if a parenthesis is present in the ACI statement. If an invalid ACI is created without a parenthesis in it, then the invalid ACI is successuflly added to the Directory Server configuration.	
927915	The Windows version of the Directory Server Console can only manage a single instance of Directory Server. If additional instances are added to the Console, then the Console fails to open with this error: `Failed to install local copy of redhat-ds-9.1.0.jar or one of its supporting files. Please ensure that the appropriate console package is installed on the Administration Server.`	
947298	The **Save** button is not always enabled on the fine-grained password policy windows in the Directory Server Console. If the policy is *disabled* for a user, there is a wanring box that pops up to confirm that the administrator wants to disable the policy. Acknowledging the box also saves the modification, which disables the **Save** button. No other edits are possible on that page because the button is disabled and, therefore, the changes cannot be saved.	Close and then re-open the user password policy window to refresh the window and re-enable the **Save** button.
951708	If FIPS mode is enabled for the Admin Server, then the Admin Server instance cannot be accessed using the Admin Server Console and the **Configuration** tab does not work.	Run the Directory Server in FIPS mode, but make sure that FIPS mode is disabled for the Admin Server. `modutil -dbdir /location/of/admin-srv/instance -fips false`
952517	Argument number 4 in the 7-bit Check Plug-in configuration is required. (The argument value is a comma.) If this argument is deleted, then the server fails to restart and core dumps.	Do not remove the argument specifying the comma (,), or re-add it if it has been deleted.
952682	The ***nsslapd-db-transaction-batch-val*** attribute has a default value of zero (0). If this attribute is changed *and then* there is a modify operation to change it back to zero, the attribute value is actually set to -1 and can no longer be modified by **ldapmodify**.	1. Stop the server. 2. Open the **dse.ldif** file. 3. Edit the ***nsslapd-db-transaction-batch-val*** attribute value directly. 4. Restart the server.

Bug Number	Description	Workaround
971332	When attempting to disable a user account through the Directory Server Console, the ***nsAccountLockout*** attribute is not set on the entry. This means that the account is not actually disabled.	Set the ***nsAccountLockout*** attribute using the **ldapmodify** utility.
974214	The Admin Express UI shows a different instance creation time for the server than the Directory Server Console displays. The Admin Express time is two hours earlier than the Console time.	

8. Revision History

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

Revision 9.1-12 **Mon Jun 26 2017** **Marc Muehlfeld**

Added a statement that this documentation is deprecated and no longer maintained.

Revision 9.1-11 **Fri Feb 24 2017** **Marc Muehlfeld**

Replaced "Upgrading from Directory Server 8.2 to Directory Server 9.1" section with a link to the corresponding section in the "Installation Guide".

Revision 9.1-10 **Thu Dec 15 2016** **Marc Muehlfeld**

Updated required JRE version.

Revision 9.1-4 **Thu Sep 10 2015** **Tomáš Čapek**

Added note that Windows Console does no support IPv6-only networks.

Revision 9.1-3 **June 30, 2013** **Ella Deon Lackey**

Initial release for Red Hat Directory Server 9.1.