# OpenDJ 2.6.0 Release Notes

**Mark Craig**

**Software release date: July 04, 2013**

**Publication date: July 03, 2013**

## Abstract

Notes covering OpenDJ hardware & software requirements, fixes, known issues. The OpenDJ project offers open source LDAP directory services in Java.

# Table of Contents

# About OpenDJ

OpenDJ is an LDAPv3 compliant directory service, developed for the Java platform, providing a high performance, highly available, and secure store for the identities managed by your organization. Its easy installation process, combined with the power of the Java platform makes OpenDJ the simplest, fastest directory to deploy and manage. OpenDJ directory server comes with plenty of tools and a full-featured LDAP SDK for Java. OpenDJ directory server also offers REST access to directory data over HTTP.

OpenDJ is free to download, evaluate, and use in developing your applications and solutions. You can also check out and modify the source code to build your own version if you prefer. ForgeRock offers training and support subscriptions to help you get the most out of your deployment.

These release notes are written for everyone working with the OpenDJ 2.6.0 release. Read these notes before you install or upgrade OpenDJ software. These notes cover hardware and software prerequisites for installing and upgrading OpenDJ software. These notes list key features added and changed in this release. They also cover compatibility with previous releases and alert you to potential changes coming up that could affect your scripts and applications. Finally, these notes list both issues fixed since the previous release and known issues open at the time of release.

See the *Installation Guide* for more after you read these release notes. The installation guide covers installation and upgrade for OpenDJ directory server, OpenDJ REST LDAP gateway, and OpenDJ DSML gateway.

# Chapter 1. What's New in OpenDJ 2.6.0

Compared to the OpenDJ 2.4.6 release, OpenDJ 2.6.0 provides the following new features.

- OpenDJ now provides native RESTful access over HTTP to directory data (OPENDJ-808). See the procedure, *To Set Up REST Access to OpenDJ Directory Server*, to activate this feature.

  OpenDJ REST LDAP gateway lets clients access directory data in remote LDAP servers over HTTP (OPENDJ-757). See the procedure, *To Install OpenDJ REST LDAP Gateway*, to get started.

- OpenDJ now lets you delegate authentication to another LDAP directory service, such as Active Directory. The feature is called *pass through authentication* (PTA) (OPENDJ-262). With PTA, OpenDJ replays a user's simple bind operation against the remote directory service. If the bind is successful, OpenDJ considers the user authenticated to perform subsequent operations like searches and updates in OpenDJ.

  For PTA to work, OpenDJ must be able to match its OpenDJ entry for the user with the user's entry on the remote directory service. The two entries must correspond in one of the following ways.

  - Both the OpenDJ entry and the remote entry have the same DN.
  - The OpenDJ entry has an attribute that holds the DN of the entry on the remote directory service.
  - The OpenDJ entry and the remote entry share an attribute that has exactly the same value.

  If user entries do not match originally, you can no doubt add an attribute to users' OpenDJ entries when configuring them to use pass through authentication.

  To configure PTA, you set up an LDAP pass through authentication policy in OpenDJ's configuration, and then assign the policy to users in the same way you would assign a password policy. See the *Administration Guide* for details.

- OpenDJ now provides Debian and RPM packages (OPENDJ-408).

- The OpenDJ upgrade process and **upgrade** command have changed to facilitate native packaging on more platforms and to make upgrade easier to handle over time (OPENDJ-455).

Also, you can now force OpenDJ upgrade to complete if errors occur in non-interactive mode (OPENDJ-522).

See *Upgrading to OpenDJ 2.6.0* for instructions.

- OpenDJ now lets you filter access and audit logs to focus on messages that interest you. OpenDJ supports many criteria for flexible log filtering (OPENDJ-308).
- OpenDJ now includes an ETag attribute for optimistic concurrency control (OPENDJ-409).
- OpenDJ now supports the PBKDF2 password storage scheme (OPENDJ-510).
- OpenDJ now lets you use more TLS cipher suites in SSFs, including those provided by Bouncy Castle and IBM (OPENDJ-826).
- OpenDJ can now synchronize Samba password attribute values with the `userPassword` attribute value, ensuring that when users change their LDAP passwords in OpenDJ or change their LanMan or NT passwords in Samba, their password attribute values all stay in sync (OPENDJ-233, OPENDJ-511). To activate this feature, configure the OpenDJ Samba Password plugin by using the **dsconfig** command.
- The OpenDJ dictionary password validator can now check whether a password value contains dictionary words as substrings (OPENDJ-295).
- The character set password validator now supports optional character sets (OPENDJ-168). Also, The character set password validator now understands classes like "All non-Latin characters" (OPENDJ-620)
- OpenDJ now provides a read-only, non-searchable operational attribute, `ds-pwd-password-expiration-time`, to make it easier to read the password expiration time for an account (OPENDJ-441).
- OpenDJ now computes last login time as UTC time when the value is expressed in GeneralizedTime syntax (OPENDJ-418).
- OpenDJ now lets you escape characters in **make-ldif** templates (OPENDJ-800).
- Country String syntax now validates ISO 3166 codes (OPENDJ-562).
- OpenDJ now sets `isMemberOf` on groups as well as user entries (OPENDJ-513).
- Performance has been significantly improved for searches with a virtual attribute in the filter (OPENDJ-508).

- OpenDJ now better supports more, and larger static groups (OPENDJ-197).
- OpenDJ now supports checking that entries of new group members exist (OPENDJ-221). OpenDJ can now ensure both that members' entries exist when they are added to groups, and also that members are removed from groups when their entries are deleted.
- OpenDJ now includes attribute syntax validation for X.509 certificate values (OPENDJ-482).
- OpenDJ now runs more reliably as a Windows Service (OPENDJ-617).
- OpenDJ now provides the **rebuild-index --rebuildDegraded** command for rebuilding degraded indexes (OPENDJ-406).
- The OpenDJ **rebuild-index** command now provides an option, `--clearDegradedState`, to forcefully clear the state of an unused index for a newly created attribute (OPENDJ-473).
- Import now performs better when handling LDIF entries with attributes that have many values, such as large static group entries (OPENDJ-469).
- Persistent connections can now be identified when querying `cn=monitor` for the LDAP client connection handler. (OPENDJ-677).
- OpenDJ now lets you configure the access log to display LDAP controls (OPENDJ-60).
- OpenDJ now adds `Unindexed` to access log response messages for unindexed searches, making it easier to identify searches rejected by default (OPENDJ-246).
- OpenDJ now logs use of the proxied authorization V1 control with `obsoleteProxiedAuthzV1Control` (OPENDJ-283).
- OpenDJ now logs only fatal errors, severe errors, warnings, and notices at startup time (OPENDJ-438).
- The mechanism to determine during setup whether the configuration has been modified runs a more effective check (OPENDJ-446).
- OpenDJ now lets you setup the server in command-line mode without creating a default backend (OPENDJ-435).
- OpenDJ schema for configuration attributes has been cleaned up (OPENDJ-393).
- OpenDJ now uses Berkeley JE 5, which brings many performance improvements (OPENDJ-371, OPENDJ-662).

With the new version, explicitly use the Java setting `-XX:+UseCompressedOops` to improve performance, even if the setting is enabled by default in recent versions of the Java runtime environment. To apply JVM settings for your server, edit `config/java.properties`, and apply the changes with the **dsjavaproperties** command.

- OpenDJ now exposes the `je.log.fileCacheSize` property through the `ds-cfg-db-log-filecache-size` configuration attribute (OPENDJ-383).
- OpenDJ verify and rebuild index commands now use JE 5 disk ordered cursoring (OPENDJ-372).
- More OpenDJ tools now prompt for a bind password when none is provided (OPENDJ-358).
- OpenDJ DSML gateway now allows authentication using an ID rather than a DN (OPENDJ-352).
- OpenDJ DSML gateway can now connect over SSL to the LDAP server (OPENDJ-269).
- OpenDJ now lets you configure attributes to be removed or renamed on update (OPENDJ-258).
- Subordinate indexes `id2children` and `id2subtree` can now be disabled on OpenDJ JE backends to improve performance when repeated adds and deletes are performed beneath the same entry (OPENDJ-250).
- OpenDJ now calls Account Status Notification Handlers when an account in enabled or disabled by the **manage-account** (OPENDJ-248).
- Change log content and configuration has been improved in this release (OPENDJ-194).
- Default database cache size, request handler counts, and replication purge delay are now set more sensibly for default installations (OPENDJ-116, OPENDJ-186).
- Collective attributes can now be applied based on the values of virtual attributes (OPENDJ-76).
- OpenDJ now lets you execute control-panel as any user, not only the user who installed OpenDJ (OPENDJ-19).

# Chapter 2. Before You Install OpenDJ Software

This chapter covers requirements to consider before you run OpenDJ, especially before you run OpenDJ in your production environment.

If you have a special request to support a combination not listed here, contact ForgeRock at info@forgerock.com.

## 2.1. Java Environment

OpenDJ software consists of pure Java applications. OpenDJ servers and clients therefore should run on any system with full Java support. OpenDJ is tested on a variety of operating systems, including Solaris SPARC and x86, various Linux distributions, Microsoft Windows, and Apple Mac OS X.

OpenDJ software requires Java 6 or 7, specifically at least the Java Standard Edition runtime environment. ForgeRock has tested most with Oracle Java Platform, Standard Edition.

ForgeRock recommends that you keep your Java installation up to date with the latest security fixes.

To build applications with the OpenDJ LDAP SDK, you need the corresponding Java SDK.

## 2.2. Maximum Open Files

OpenDJ needs to be able to open many files, especially when handling many client connections. Linux systems in particular often set a limit of 1024 per user, which is too low for OpenDJ.

When setting up OpenDJ for production use, make sure OpenDJ can use at least use at least 64K (65536) file descriptors. For example when running OpenDJ as user `opendj` on a Linux system that uses `/etc/security/limits.conf` to set user level limits, you can set soft and hard limits by adding these lines to the file.

```
opendj soft nofile 65536
opendj hard nofile 131072
```

The example above assumes the system has enough file descriptors available overall. You can check the Linux system overall maximum as follows.

```
$ cat /proc/sys/fs/file-max
204252
```

## 2.3. Operating System

OpenDJ software depends on the Java environment more than it depends on the underlying operating system. That said, OpenDJ 2.6.0 has been validated on the following operating systems.

- Apple Mac OS X 10.7, 10.8
- Linux 2.6 and later
- Microsoft Windows Server 2008 R2 and Windows Server 2012
- Oracle Solaris 11 x86

In order to avoid directory database file corruption after crashes or power failures on Linux systems, enable file system write barriers and make sure that the file system journaling mode is ordered. For details on how to enable write barriers and how to set the journaling mode for data, see the options for your file system in the **mount** command manual page.

## 2.4. Virtualization

ForgeRock has tested OpenDJ software on systems running atop VMware vSphere Hypervisor (ESXi) 5.1.

## 2.5. Application Servers

OpenDJ directory server runs as a standalone Java service, and does not depend on an application server.

OpenDJ DSML gateway has been validated on Apache Tomcat 6 and 7.

OpenDJ REST LDAP gateway has been validated on Apache Tomcat 6 and Jetty 8.

## 2.6. FQDNs For Replication

OpenDJ replication requires that you use fully qualified domain names, such as `opendj.example.com`.

Although you can use host names like `my-laptop.local` for evaluation, in production and even in your lab, you must either ensure DNS is set up correctly to provide fully qualified domain names, or set up `/etc/hosts` (or `C:\Windows\System32\drivers\etc\hosts`) to provide fully qualified domain names.

## 2.7. Hardware

Thanks to the underlying Java platform, OpenDJ software runs well on a variety of processor architectures. Many directory service deployments meet their service-level agreements without the very latest or very fastest hardware.

For a server evaluation installation, you need 256 MB memory (32-bit) or 1 GB memory (64-bit) available to OpenDJ, with 100 MB free disk space for the software and a small set of sample data. For installation in production, read the rest of this section. You need at least 2 GB memory for OpenDJ and 4 times the disk space needed to house initial production data in LDIF format.[1] To get a more accurate estimate of the disk space needed, import a known fraction of the initial LDIF with OpenDJ configured as for production, run tests based on the estimated rates of change and growth in directory data, and then use the actual space used in the test environment to estimate how much disk space you need in production.

OpenDJ directory servers almost always benefit from having enough system memory to cache all directory database files used. The reason is that reading from and writing to memory is typically much faster than reading from and writing to disk storage. For small data sets, you might not need extra memory. For large directories with millions of user directory entries, the system might not have enough slots to house sufficient memory to cache everything. To improve performance in such cases, one approach is to add solid state drives as an intermediate cache between memory and disk storage.

Processor architectures that provide fast single thread execution tend to help OpenDJ software deliver the lowest response times. For top end performance in terms both of sub-millisecond response times and also of throughput ranging from tens of thousands to hundreds of thousands of operations per second, the latest x86/x64 architecture chips tend to perform better than others tested. Chip multi-threading (CMT) processors can do very well on

[1] OpenDJ stores data in Berkeley DB Java Edition, which is implemented as a rolling log. Berkeley DB appends updates to the end of the last log file, and marks old pages as deleted. Berkeley DB cleaner threads monitor the log file occupancy ratio, moving the data to get rid of old log files. Yet, with the default occupancy ratio of 50%, log files are cleaned only when they have less than 50% valid pages. As a result, the database can reach twice its initial size in the worst case.

Furthermore, when you import data from LDIF, OpenDJ stores not only the data, but also builds indexes for many of the attributes, resulting in some growth. Replication historical data and other operational attributes can also take up space.

Finally, it makes sense to leave space for growth in the database size as you modify and add entries over time.

directory servers providing pure search throughput, even though response times can be higher. Yet, CMT processors can be slow to absorb hundreds or thousands of write operations per second. Their slower threads get blocked waiting on resources, and thus are not optimal for topologies with high write throughput requirements.

On systems with fast processors and enough memory to cache directory data completely, the network can become a bottleneck. Even if a single 1 Gbit Ethernet interface offers plenty of bandwidth to handle your average traffic load, it can be too small for peak traffic loads. Furthermore, you might choose to use separate interfaces for administrative traffic and application traffic. To estimate what network hardware you need, calculate the size of the data you return to applications during peak load. For example, if you expect to have a peak load of 100,000 searches per second, each returning a full 8 KB entry, you need a network that can handle 800 MB/sec (3.2 Gbit/sec) throughput, not counting any other operations such as writes that result in replication traffic.

The storage hardware you choose must allow you to house not only directory data including historical data for replication, but also logs. If you choose to retain access logs for auditing purposes on a heavily used directory, dedicate storage for the log archives as well. Furthermore, your storage must also keep pace with the write throughput. Write throughput can arise from modify, modify DN, add, and delete operations, but it can also result from bind operations. Such is the case when the last successful bind is recorded, and when account lockout is configured, for example. In a replicated topology, not only does a directory service write entries to disk when they are changed, but a directory service also writes changelog data and historical information in order to resolve potential replication conflicts. You base your network throughput needs on peak loads. Also base your storage throughput needs on peak loads.

## Note

OpenDJ servers do not currently support network file systems such as NFS for database storage. Provide sufficient disk space on local storage such as internal disk or an attached disk array.

# Chapter 3. OpenDJ Compatibility

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

## 3.1. Important Changes to Existing Functionality

OpenDJ 2.6.0 improves on earlier releases introducing many new features. Also take the following into account.

- The upgrade process and **upgrade** command have changed to facilitate native packaging on more platforms. See *Upgrading to OpenDJ 2.6.0* for instructions.
- The default DB cache size is now 50%, rather than 10%.

  If you have multiple backends, configure cache sizes accordingly.
- The number of LDAP request handlers now defaults to half the CPU count.
- The replication purge delay default has increased from one day to three days.
- Syntax checking has been added for certificate and country attribute values. This affects applications updating those attribute values. Applications updating country attribute values must now use Country String syntax for example, which uses two-character codes from ISO 3166 such as `US` instead of full names such as `United States`.
- The following global ACI settings have changed.
  - OpenDJ directory server now allows any client to use the LDAP Permissive Modify Request control, `1.2.840.113556.1.4.1413`, by default for newly installed servers.
  - The "Anonymous read access" global ACI has changed. The list of attributes that are not allowed has been changed to add `includedAttributes` and to remove `targetUniqueID`.

  When you upgrade from earlier versions of OpenDJ, however, the previous `global-aci` settings are not updated. To apply the changes manually, change the relevant `global-aci` settings by using the **dsconfig** command. An example of how to change a `global-aci` property can be found in the *Administration Guide*, *ACI: Disable Anonymous Access*.

- For the SNMP Connection Handler, the default `security-agent-file` has changed to `opendj-snmp.security` (OPENDJ-982), and the upgrade process changes the file name. The `community` has also changed to `OpenDJ`. If the SNMP Connection Handler fails to start after upgrade, use the **dsconfig** command to make sure that the `security-agent-file` property is correctly set for your installation.

## 3.2. Deprecated Functionality

OpenDJ 2.6.0 makes use of new environment variables aligned with the project name to use `OPENDJ`. Use of the old variables is Deprecated. The old variables are likely to be removed in a future release.

The **dsframework** command is Deprecated and likely to be removed in a future release.

The following OpenDJ LDAP SDK methods are Deprecated and likely to be removed in a future release.

- `org.forgerock.opendj.ldap.LDAPListenerOptions#getTCPNIOTransport`
- `org.forgerock.opendj.ldap.LDAPListenerOptions#setTCPNIOTransport`
- `org.forgerock.opendj.ldap.LDAPOptions#getTCPNIOTransport`
- `org.forgerock.opendj.ldap.LDAPOptions#setTCPNIOTransport`

## 3.3. Removed Functionality

Native packages in SVR4 format for Solaris are not provided at this time.

# Chapter 4. OpenDJ Fixes, Limitations, & Known Issues

This chapter covers the status of key issues and limitations for OpenDJ 2.6.0 and OpenDJ SDK 2.6.0. For details and information on other issues, see the OpenDJ issue tracker.

## 4.1. Key Fixes

### Note

This release contains fixes that resolve security issues within OpenDJ. Older versions of OpenDJ contain these security issues. It is recommended that you upgrade to this release to resolve these security issues. ForgeRock customers can contact support for detials on the security issues.

OpenDJ 2.6.0 also includes important improvements to replication. Replication remains fully compatible with earlier versions. However, some operations that work fine with OpenDJ 2.6.0, such as replicating large groups and replicating high volumes of adds and deletes, can cause issues for earlier versions. Make sure you upgrade all servers to 2.6.0 before allowing clients to take advantage of write operations that could cause trouble for older servers.

The following important bugs were fixed in this release.

- OPENDJ-988: Filtering access logs by userdn doesn't work
- OPENDJ-982: Upgrade: SNMP Connection Handler does not start after the upgrade
- OPENDJ-962: Subject Attr To User Attr Cert Mapper has wrong default configuration
- OPENDJ-940: Import-ldif NPE if base entry contains invalid attribute values and skipDNValidation is set
- OPENDJ-926: SchemaBackend ignores instance dir
- OPENDJ-925: SchemaConfigManager tries to load files twice
- OPENDJ-922: Replication window size is too small on high latency networks
- OPENDJ-900: Cannot use backups to initialize a replica

- OPENDJ-899: ModDN with the same value ignored by ACIs
- OPENDJ-895: Document ACIs and privileges required for basic LDAP operations
- OPENDJ-888: Maintaining ds-sync-hist for a large group is inefficient
- OPENDJ-886: connected-to attributes under cn=monitor are wrong when all RSes are down
- OPENDJ-885: Replication replay may lose changes if it can't acquire a writeLock
- OPENDJ-882: NullPointerException in access log filtering code
- OPENDJ-875: Use of hostnames in replication protocol causes failover problems
- OPENDJ-868: cannot add attributes to referential integrity plugin
- OPENDJ-846: Intermittent Replication Failure
- OPENDJ-818: dsreplication status shows disabled servers as enabled
- OPENDJ-798: Cannot be part of 2 replication topologies if a third topology shares a common suffix
- OPENDJ-797: dsconfig cannot edit custom password policy after upgrade to 2.5.0-Xpress1
- OPENDJ-765: Modify with replace attr=value and delete attr gets misrecorded in ds-sync-hist
- OPENDJ-761: Migration from deprecated password storage schemes doesn't work during a simple bind
- OPENDJ-680: Upgrade may change ds-cfg-base-dn to dc=example,dc=com on userRoot configuration
- OPENDJ-668: Cannot configure ssl-cipher-suites on admin connector
- OPENDJ-664: Password validator: default of check-substrings = false breaks rule of least surprise
- OPENDJ-652: Connections from Solaris 10 ldapclient can cause LDAPS request handler to spin
- OPENDJ-649: Add supportedTLSCiphers and supportedTLSProtocols to RootDSE and system monitor

- OPENDJ-627: ConnectionPool internal state becomes invalid when stale connections are discarded
- OPENDJ-625: ModifyDN does not allow the same (normalized) DN
- OPENDJ-622: DSML ExtendedRequest text requestValues don't work
- OPENDJ-621: No documentation for schema definition extensions
- OPENDJ-618: DSML gateway should send an AuthResponse for the initial bind
- OPENDJ-615: Replication silently skips entries referring to non-existent global password policies
- OPENDJ-608: DSML gateway NPE in response to extended requests without request values
- OPENDJ-602: Referrals returned when not in scope.
- OPENDJ-601: Syntax for offline backup is incorrect
- OPENDJ-590: ConnectionPool may return already closed/disconnected connections
- OPENDJ-587: Control-panel rebuild-index shouldn't disable the backend and use offline command
- OPENDJ-578: Documentation should reflect that --type is now required for `dsconfig create-password-policy`
- OPENDJ-568: ldiffdiff and ldifmodify documentation is incorrect
- OPENDJ-565: Attribute Value password validator finds password in the userPassword attribute
- OPENDJ-564: SSF based access controls don't seem to be working
- OPENDJ-561: Add operation doesn't get password policy from ds-pwp-password-policy-dn;collective
- OPENDJ-556: Strange ACI results
- OPENDJ-548: Unable to run ldap commands as any user other than root after updating java.properties
- OPENDJ-532: When replication is enabled cn=changelog appears in namingcontexts output
- OPENDJ-528: rebuild-index doesn't rebuild properly DN2ID after an upgrade from OpenDS 2.2.

- OPENDJ-520: Worker threads are too greedy when caching memory used for encoding/decoding entries and protocol messages
- OPENDJ-504: Performing Query on telephoneNumber attribute thats not a number returns all entries
- OPENDJ-500: Upgrade trunk (2.5.0) to JE 5.0.48
- OPENDJ-494: dsreplication initialize reports negative percentage of completion
- OPENDJ-488: Cancel request succeeds with result code 118 (CANCELED) when it should receive result code 0 (SUCCESS)
- OPENDJ-487: Normal acis under cn=config are not loaded at startup
- OPENDJ-475: Incorrect behaviour/result code regarding non-critical controls
- OPENDJ-472: offline import LDIF reject entries, doesn't report the correct count of them, and store them in both rejected and skipped files.
- OPENDJ-464: NPE in PasswordPolicyStateExtendedResult results in eternal waiting
- OPENDJ-462: Spinning threads in JE backend importer
- OPENDJ-459: User's privileges not working with SASL EXTERNAL auth
- OPENDJ-456: OpenDJ schema replication fails for 3rd server of topology
- OPENDJ-433: Every other permissions-subjects pair in ACI is ignored
- OPENDJ-432: LDAPURL doesn't always url-decode baseDN
- OPENDJ-427: AuthenticatedConnectionFactory hides exception with NPE
- OPENDJ-420: Rare SSLExceptions while handling LDAPS connections and big LDAP searches
- OPENDJ-410: Frequent corruption in ds-sync-hist ordering index.
- OPENDJ-400: ControlPanel issue with values containing \n (such as sunxmlkeyvalue)
- OPENDJ-398: Misleading replication messages: "Replication server XXXX was attempting to connect to replication server YYYY but has disconnected in handshake phase"
- OPENDJ-387: dsreplication initialize-all reports negative percentage of completion

- OPENDJ-380: index-entry-limit=0 not working as expected
- OPENDJ-377: Kerberos authentication with AD KDC fails with LoginException(Client not found in Kerberos database (6))
- OPENDJ-349: manage-account returns Seconds Until Idle Account Lockout: 0 (zero) if the last log on date is more than 24 days before the idle lock out interval.
- OPENDJ-344: Upgrade fails when there's an extension with additional JAR dependency.
- OPENDJ-333: Missing entryUUID attributes in "cn=admin data" backend prevent updates from being replicated.
- OPENDJ-323: If you attempt to rebuild an index that doesn't exist while OpenDJ is running then the backend is left offline
- OPENDJ-322: Binary encoding option causing problems in replace operations
- OPENDJ-320: log-file-permissions ignores group permissions
- OPENDJ-315: OpenDJ not restart when enable as automatic windows service after reboot
- OPENDJ-310: Replicated changes to referral entries are not applied on replicas
- OPENDJ-293: InternalClientConnection memory leak when performing password modify/state extended operations or SASL binds
- OPENDJ-282: dsreplication enable fails with duplicate server ID, while it's about the same server being referenced.
- OPENDJ-274: Replication mishandles a Modify operation with multiple modifications on the same attribute.
- OPENDJ-271: ExternalSASLBindRequestImpl throws java.lang.IllegalStateException
- OPENDJ-254: The show-all-attributes flag breaks schema modification, when enabled.
- OPENDJ-242: Password Policy State Extended Operation anomalities...
- OPENDJ-223: Modify operation isn't replayed on replica exactly as on original server.

- OPENDJ-219: Replication server and draft changelog DB code may attempt to reference closed DB
- OPENDJ-184: Transient errors when accessing cn=changelog DraftCN DB result in complete shutdown of the replication service.
- OPENDJ-173: External ChangeLog cookies content is altered by Change purging and prevents from continuing search with a previous returned cookie.
- OPENDJ-169: Modifying an existing object class definition requires server restart
- OPENDJ-159: LDAP connections use stale default schema if it is changed after factory creation.
- OPENDJ-156: Errors when parsing collective attribute definitions
- OPENDJ-150: ChangeLogEntry schema is not compliant with internet-draft
- OPENDJ-146: java.lang.OutOfMemoryError: Java heap space
- OPENDJ-136: On Windows, upgrade fails with NPE during Verify phase
- OPENDJ-135: upgrade -r fails on Windows
- OPENDJ-134: upgrade fails when server registered as Windows service
- OPENDJ-130: External change log, used in compliance with Internet-draft, shows a divergence between replicas under load.
- OPENDJ-98: Searches on cn=monitor take a long time
- OPENDJ-65: Host domain name lost from FQDN while enabling replication for a new replica using disreplication enable
- OPENDJ-57: ECL: lastChangeNumber and firstChangeNumber reset to zero when the changelog is purged to empty
- OPENDJ-55: Failing modify operations causing memory leak
- OPENDJ-21: Account Status Notifications (password changed/reset) are not sent for the Password Modify Extended Operation

## 4.2. Limitations

Release 2.6.0 has the following limitations, none of which are new since 2.4.6.

- OpenDJ directory server provides full LDAP v3 support, except for alias dereferencing, and limited support for LDAPv2.

- When you configure account lockout as part of password policy, OpenDJ locks an account after the specified number of consecutive authentication failures. Account lockout is not transactional across a replication topology, however. Global account lockout occurs as soon as the authentication failure times have been replicated.
- OpenDJ is not fully integrated with Microsoft Windows, yet OpenDJ directory server can be run as a service, and thus displayed in the Windows Services Control Panel.
- OpenDJ replication is designed to permit an unlimited number of replication servers in your topology. Project testing has, however, focused only on topologies of up to eight replication servers.
- OpenDJ plugin extensions must follow the guidelines set forth in the `README` file delivered in `opendj/example-plugin.zip`. When developing your extension, aim to remain loosely coupled with any particular version of OpenDJ. Libraries used must be installed in `opendj/lib/extensions/` (or bundle them in your .jar). Keep your configuration separate from the server configuration. Also, unless you are reusing standard schema definitions, keep your schema definitions separate as well.

  This can affect how your extension works after upgrade. In particular `opendj-accountchange-handler-1.0.0` does not work with OpenDJ 2.6.0 after upgrade (OPENDJ-991). See that issue for notes on how make that version of the extension work with OpenDJ 2.6.0.

## 4.3. Known Issues

### Tip

When deploying for production, make sure that you follow the installation instructions on allowing OpenDJ to use at least 64K (65536) file descriptors, and on tuning the JVM appropriately.

The following important issues remained open at the time this release became available.

- OPENDJ-1048: OpenDJ QuickSetup creates the "licenseAccepted" file in the wrong place
- OPENDJ-1043: Worker Thread was interrupted while waiting for new work while shutting down
- OPENDJ-1033: The Rest2LDAP servlet does not support SSL
- OPENDJ-934: Changes to RS window-size property require a server restart

- OPENDJ-810: Non-atomic password state updates
- OPENDJ-631: Modifications made by ldif-diff causes bad replication data
- OPENDJ-557: Identical changes recorded in duplicate changelog records
- OPENDJ-527: rebuild-index --rebuildAll corrupts the indexes for certain data sets
- OPENDJ-518: Cannot log into the administrative control panel with FIPS-140 enabled in certain cases
- OPENDJ-514: OpenDJ SDK SASL integrity/confidentiality violates protocol
- OPENDJ-452: Manual add of new schema objectclass in 99-user.ldif are not replicated
- OPENDJ-412: Blocked persistent searches may block all worker threads
- OPENDJ-365: Potential deadlock in JE backend while performing a mix of update operations
- OPENDJ-270: dsreplication disable takes a long time
- OPENDJ-49: Replication replay does not take into consideration the server/backend's writability mode.

# Chapter 5. How to Report Problems & Provide Feedback

If you have questions regarding OpenDJ which are not answered by the documentation, there is a mailing list which can be found at https://lists.forgerock.org/mailman/listinfo/opendj where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenDJ 2.6.0, report them in the OpenDJ issue tracker.

When requesting help with a problem, please include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Description of the environment, including the following information:
  - Machine type
  - Operating system & version
  - Storage type & version
  - Java version
  - Web container & version (if applicable)
  - OpenDJ release version
  - Any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any relevant access and error logs, stack traces, or core dumps

# Chapter 6. Support

You can purchase OpenDJ support subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see http://forgerock.com/partners/find-a-partner/.