Release Notes

OpenDJ 3

Mark Craig

ForgeRock AS
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

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

Table of Contents

About OpenDJ Software

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 and fastest directory to deploy and manage. OpenDJ directory server comes with plenty of tools and also offers REST access to directory data over HTTP.

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

These release notes are written for everyone using the OpenDJ 3 release. Read these notes before you install or upgrade OpenDJ software.

These release notes cover the following topics:

- Hardware and software prerequisites for installing and upgrading OpenDJ software
- Compatibility with previous releases
- Potential upcoming deprecation and removals that affect scripts and applications
- Issues fixed since the previous release
- Known issues open at the time of release

See the Installation Guide after you read these *Release Notes*. The *Installation Guide* covers installation and upgrade for OpenDJ directory server, OpenDJ REST to LDAP gateway, and OpenDJ DSML gateway.

Chapter 1
What's New In OpenDJ

OpenDJ 3 provides many new capabilities compared to OpenDJ 2.6.

1.1. New Features

This release of OpenDJ software includes the following new features:

New Database Backend

OpenDJ directory server now provides a PDB backend type for backends that use embedded databases for storage (OPENDJ-1602).

PDB backends provide the same full LDAPv3 compliance and the same ease of use as previous choices.

If you do choose to move directory data to a PDB backend, note that you must import the data again into the new backend. This is necessary due to the change in underlying storage implementations. You can make the move, for example, by exporting LDIF from the old backend and then importing the LDIF into the new backend, or simply through OpenDJ replication by initializing a server using the new backend from an existing replica.

The PDB database backend is based on a key-value store that is under an Apache license.

New JE Backend Implementation

The Local DB backend (default data store) implementation has changed to benefit from the same improvements as the new PDB backend.

The Local DB backend type has been replaced by a JE backend type. The **upgrade** command can migrate the OpenDJ backend configuration and directory data. For details, see Chapter 2, "*Upgrading to OpenDJ 3*" in the *Installation Guide*.

The JE backend benefits from improvements that result in a more compact database, optimized indexes, faster data imports, and better overall performance.

New Replication Log

OpenDJ directory server has an improved replication changelog implementation based on log files (OPENDJ-1215).

This feature decouples the replication log from the key-value database, and optimizes replication log space and performance characteristics. The new replication log consumes less space and less CPU. In addition, the new implementation makes it possible to guarantee total ordering for changes across replicated servers and consistent change numbers. Applications polling for changes and using change numbers rather than cookies can now fail over to another replica without risk of missing a change or getting inconsistent search results.

For details on making change numbers consistent across replicas, see Procedure 8.17, "To Align Draft Change Numbers" in the *Administration Guide*.

Certificate Matching Rules

OpenDJ directory server now implements the certificate-matching rule, `certificateExactMatch` (OPENDJ-883).

The attributes `userCertificate` and `cACertificate` now use the `certificateExactMatch` matching rule as indicated by RFC 4523.

You can now run queries against the directory to retrieve entries with a specific certificate or specific content of a certificate. Combined with the Matched Values control, this allows you to retrieve one specific certificate anywhere in the directory data in a single request. This feature makes OpenDJ highly suitable as the central repository of public certificates, useful in certificate management systems.

PKCS5S2 Password Storage Scheme

OpenDJ directory server now supports the PKCS5S2 password storage scheme (OPENDJ-1510).

This feature allows encoding of user passwords using the Atlassian PBKDF2-based message digest algorithm.

ForgeRock Common Audit

OpenDJ directory server now includes ForgeRock's common audit framework, with support for logging to files, databases, and the UNIX system log (Syslog) (OPENDJ-2270).

ForgeRock common audit allows you to handle audit events in a common way across the ForgeRock platform, to centralize audit logs, and to trace transactions through the platform. Log files can be signed to make tampering evident.

For more information, see Section 17.5.2, "Common ForgeRock Access Logs" in the *Administration Guide*.

New Changelog Privilege

OpenDJ directory server now requires a privilege, `changelog-read` to read and search entries under `cn=changelog` (OPENDJ-1351).

This feature eases administration of access control to `cn=changelog` entries, which are used by administrative and synchronization tools to retrieve changes applied through data replication.

Disk Space Monitoring

Disk space monitoring supports new backend types as a server-wide facility (OPENDJ-1809, OPENDJ-1790).

This feature makes it easier to monitor and control total disk space use.

SOAP 1.2 Support in DSML Gateway

OpenDJ DSML gateway now supports SOAP 1.2 (OPENDJ-1187).

1.2. Product Improvements

This release of OpenDJ software includes the following enhancements:

Ease of Use

The following improvements make working with OpenDJ easier for users and for administrators:

- OpenDJ directory server now orders attributes according to search request attribute list order (OPENDJ-1082).
- OpenDJ directory server logs information to help you more effectively determine why a directory server replica switches its connection to a different replication server (OPENDJ-1053).
- OpenDJ directory server now allows ordering matching rules to reuse equality indexes where possible (OPENDJ-1864).
- OpenDJ directory server can now bind to a local address when making outgoing connections (OPENDJ-1565).

  This improvement introduces a new configuration attribute, `source-address`, that you can set for Replication Domains, Replication Servers, and LDAP Pass-Through Authentication Policies. If the `source-address` property is set to an IP address, OpenDJ binds to the address before connecting to the remote server. The address must be one assigned to an existing network interface.
- The **dsconfig** command now supports a `--batch` option for reading subcommands from standard input (OPENDJ-1840).
- The SMTP account status notification handler can now send HTML email (OPENDJ-1985).

  To send HTML format notifications, use HTML templates and set the advanced boolean property for the notification handler, `send-email-as-html`, to `true`.
- OpenDJ directory server now allows you to set the RMI port number for the JMX connection handler (OPENDJ-1161), and to set the listen address for the JMX connection handler (OPENDJ-821).

Use the property `rmi-port` to set the port number. Restart the connection handler for the change to take effect.

Use the property `listen-address` to set the listen address. Restart the server for the change to take effect.

- OpenDJ directory server now logs appropriate information about memory use when running in an IBM Java virtual machine (OPENDJ-1616).
- The **create-rc-script** command now supports FreeBSD (OPENDJ-2238).
- Several OpenDJ directory server commands now remove temporary log files after successful completion (OPENDJ-2436).

Password Management

The following enhancements concern how passwords are managed:

- OpenDJ directory server now provides a mechanism to reference password validators from subentry password policies (OPENDJ-1295).

  To configure password validators for a subentry password policy, add the auxiliary object class, `pwdValidatorPolicy`, and set the multi-valued attribute, `ds-cfg-password-validator`, to the DNs of the password validator configuration entries.
- OpenDJ directory server now matches non-default salt sizes in SMD5 passwords (OPENDJ-1451).
- OpenDJ directory server now more effectively cleans memory of password values after using them (OPENDJ-1036).

REST to LDAP

The following improvements concern HTTP access to directory data:

- OpenDJ REST to LDAP gateway now supports SSL and StartTLS connections to directory servers (OPENDJ-1033).
- OpenDJ REST to LDAP gateway and HTTP connection handler now support a password modify action that corresponds to the LDAP Password Modify extended operation (OPENDJ-2383).

  This action requires HTTPS to protect passwords.

  For details and examples, see Section 1.8.2, "Using the Password Modify Action" in the *Directory Server Developer's Guide*.
- OpenDJ REST to LDAP gateway and HTTP connection handler now support paged results for queries (OPENDJ-701).

For details and examples, see Section 1.9, "Querying Resource Collections" in the *Directory Server Developer's Guide*.

Native Packaging

The following improvements have been made to native packaging:

- Debian and RPM packages now provide service management scripts to manage the server with the **service** command (OPENDJ-1114, OPENDJ-1068).
- RPM packages now set the correct package group for SuSE Linux (OPENDJ-1070).
- Debian and RPM packages now include man pages for command-line tools, and the **man** command path is set during package installation (OPENDJ-2177).

1.3. Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For details of all the security advisories across ForgeRock products, see Security Advisories in the *Knowledge Base library*.

Chapter 2

Before You Install OpenDJ Software

This chapter covers requirements to consider before you run OpenDJ directory server, 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 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 Mac OS X.

OpenDJ software requires Java 7 or 8, specifically at least the Java Standard Edition runtime environment.

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

2.2. Maximum Open Files

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

When setting up OpenDJ for production use, make sure OpenDJ can 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 server software 3 is supported on the following operating systems:

- Linux 2.6 and later
- Microsoft Windows Server 2008, 2008 R2, 2012, and 2012 R2
- Oracle Solaris 10, 11

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. Application Servers

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

OpenDJ REST to LDAP gateway, and OpenDJ DSML gateway run on Apache Tomcat and Jetty.

ForgeRock supports only stable container releases. See the Tomcat and Jetty documentation for details on which container version supports the Java version used in your deployment.

2.5. 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 the hosts file (`/etc/hosts` or `C:\Windows\System32\drivers\etc\hosts`) to supply fully qualified domain names.

2.6. 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.

2.6.1. Memory Requirements

For a server evaluation installation, you need 256 MB memory (32-bit) or 1 GB memory (64-bit) available, 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 directory server and four times the disk space needed to house initial production data in LDIF format. OpenDJ directory server stores data, indexes for the data, operational attribute data, and historical information for replication. The server configuration trades disk space for performance and resilience, compacting and purging data for good performance and for protection against temporary outages. In addition, it makes sense to leave space for growth in database size as client applications modify and add entries over time.

For a more accurate estimate of the disk space needed, import a known fraction of the initial LDIF with OpenDJ directory server configured in the same way as expected in 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 generally 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.

2.6.2. Processor Alternatives

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 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.

Chip multi-threading (CMT) processors can do very well on directory servers providing pure search throughput, though response times are higher. However, CMT processors are 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 deployments with high write throughput requirements.

2.6.3. Network 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. Consider using separate interfaces for administrative traffic and for application traffic.

To estimate what network hardware you need, calculate the size of the data returned 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 require 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.

2.6.4. Storage Requirements

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.

Storage hardware must house not only directory data including historical data for replication, but also directory server logs. On a heavily used directory, access logs call for dedicated storage.

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 the directory service also writes changelog data and historical information in order to resolve potential replication conflicts. As for network throughput, base your storage throughput on peak loads.

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

Take the following changes into account when upgrading to OpenDJ 3:

- Improvements to the LDIF import feature have resulted in the following changes:
  - The **import-ldif** command always removes all the data for the target suffix before importing from LDIF.

    This is the case even when using the `--excludeBranch` and `--includeBranch` options. These options now only cause the **import-ldif** command to filter the LDIF content.
  - The **import-ldif** command no longer supports the `-a, --append` and `-r, --replaceExisting` options.

    To append to an existing database, either export the existing data to LDIF, concatenate the data to append, and then import, or add the data to append, rather than importing it.

    To replace existing entries when appending data, either delete the entries to be replaced and then add them, or export the existing data to LDIF, remove the entries to replace, concatenate the data to append, and then import.
  - As previously, a single backend can hold data for more than one suffix, as long as no suffix is a child of another suffix in the same backend.

    To separate suffixes where one suffix is the parent and another the child, put the parent in one backend and the child in the other.
- Improvements that allow OpenDJ directory server to use pluggable backends have resulted in incompatible updates to some backup archives:
  - Configuration, schema, and task backend backup archives now all have backup archives named `backup-`*`backend-id-backup-id`*.
  - The backup archive content for schema backends has changed.

Rather than using a backup archive with the **backup** command, use a file system backup if you must revert an upgrade to 3. After successful upgrade, do not restore backup archives generated with older versions of the **backup** command.

- RESTful access to directory data has changed in the following ways:
  - RESTful access now supports *upsert*, which means HTTP PUT creates the resource if it does not exist, and updates the resource if it does exist. To prevent a create if the resource does not exist, use an `If-Match: *` header. Continue to prevent an update of the wrong revision of a resource by using an `If-Match: revision` header.
  - Query results now include `totalPagedResults` and `totalPagedResultsPolicy` fields. In addition query parameters `_pagedResultsCookie` and `_pagedResultsOffset` are now mutually exclusive. For details see Section 1.1.11, "Query" in the *Directory Server Developer's Guide*.
  - Individual resources returned now always include `_id` and `_rev` fields, even when those fields are not requested.
- LDAP SDK 3 `makeldif.template` files are not backwards-compatible with the OpenDJ directory server **make-ldif** command.

  When specifying a branch in LDAP SDK **makeldif** templates, you must now also specify the object classes for the branch. Server **make-ldif** templates require branch specifications that do not specify the object classes for the branch.
- The following commands now delete their temporary log files on successful completion:
  - **control-panel**
  - **dsreplication**
  - **setup**
  - **status**

  The GUI tools do not delete their temporary log files.
- The following global ACI settings have changed:
  - The `debugsearchindex` attribute has been added to the list of attributes that are not allowed according to the `Anonymous read access` global ACI.
  - The OID for the ForgeRock Transaction ID request control, `1.3.6.1.4.1.36733.2.1.5.1`, has been added to the list of OIDs that are allowed by the `Anonymous control access` global ACI.

    This change makes it easier for ForgeRock components that act as LDAP clients of OpenDJ directory server to transmit ForgeRock transaction IDs used by the Common Audit framework. Only LDAP clients with access to use the transaction ID request control can effectively transmit transaction IDs to OpenDJ directory server.

The ForgeRock TransactionID request control has Internal/Undocumented interface stability as defined in Section I.2, "ForgeRock Product Interface Stability" in the *Reference*.

When you upgrade from earlier versions of OpenDJ directory server, the previous `global-aci` settings are not updated. To apply the changes manually, change the relevant `global-aci` settings by using the **dsconfig** command. For an example of how to change a `global-aci` property, see Example 6.2, "ACI: Disable Anonymous Access" in the *Administration Guide*.

3.2. Deprecated Functionality

This section lists deprecated functionality. Deprecation is defined in Section I.2, "ForgeRock Product Interface Stability" in the *Reference*.

OpenDJ makes use of environment variables aligned with the project name to use `OPENDJ`. Use of the old variables is Deprecated. Support for older variables is likely to be removed in a future release.

3.3. Removed Functionality

- Support for Java 6 has been removed.
- The **dsframework** command has been removed.
- The `local-db` backend database type has been removed, and replaced with pluggable backend database types.

  Some commands have changed as a result. The **dbtest** utility has been removed, and replaced by the **backendstat** command.

  The **dsconfig** subcommands pertaining to `local-db` backends have been removed, and replaced with subcommands for pluggable backends.

  The OpenDJ directory server **upgrade** command migrates directory data to pluggable backends, updating the directory configuration in the process.
- The OpenDJ LDAP SDK version used in this release is not compatible with the 2.x SDK.

Chapter 4

OpenDJ Fixes, Limitations, and Known Issues

This chapter covers the status of key issues and limitations for OpenDJ 3. For details and information on other issues, see the OpenDJ issue tracker.

4.1. Key Fixes

Note

OpenDJ 2.6.0 and later versions include important improvements to replication. Replication remains fully compatible with earlier versions. However, some operations that work fine with OpenDJ 2.6.0 and later, 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 or later 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-2362: Setting CLEANER_MIN_FILE_UTILIZATION instead of CLEANER_MIN_UTILIZATION
- OPENDJ-2339: RDNs with single space values cause problems
- OPENDJ-2274: OpenDJ: World-readable permissions are set on the config.ldif.startok and archived-config files.
- OPENDJ-2196: OpenDJ does not return the isMemberOf attribute via REST
- OPENDJ-2159: PDB Storage is read-only when using the verify-index tool on Windows
- OPENDJ-2152: ldapsearch ignores ldapsearch.useSSL=true in a tools.properties
- OPENDJ-2046: HTTP Connection Handler doesn't return anything and spins on connection closure
- OPENDJ-2027: Command-line tools requiring arguments should display usage if none are given
- OPENDJ-1969: IdleTimeLimitThread fails with null ConnectionHandlers or null ClientConnections
- OPENDJ-1968: NPE in GoverningStructureRuleVirtualAttributeProvider if entry has no structural object classes
- OPENDJ-1882: currentConnections from cn=monitor is not decremented when JMX connections close

- OPENDJ-1829: JMX connector listens on a random port number
- OPENDJ-1764: admin-backend.ldif can end up empty
- OPENDJ-1610: Original password is not put in password history when password is reset without specifying the new password
- OPENDJ-1586: Nested groups fail to return indirect members with DBs larger than 10 entries
- OPENDJ-1443: OpenDJ returns an "invalid credential:expired" when password has expired even if the provided password is wrong
- OPENDJ-1431: Trimming of draftcndb gets stuck, changelog keeps growing in size
- OPENDJ-1427: Control panel reports duplicate ds-sync-hist values for pwdHistory
- OPENDJ-1375: Subtree delete control can wait forever for an id2subtree lock
- OPENDJ-1366: Arguments logged in wrong order for ERROR_REPLAYING_OPERATION
- OPENDJ-1359: Control panel requires incremental backups specify the parent
- OPENDJ-1358: Backup task logs path in ID field, and ID in path field
- OPENDJ-1354: replication threads BLOCKED in pendingChanges queue
- OPENDJ-1322: Control-Panel.bat can not start and stop the OpenDJ server when running as a windows service
- OPENDJ-1294: ldappasswordmodify -D <DN> -w - fails without prompting password from stdin
- OPENDJ-1283: Replayed Modify operations are rejected if the backend writability mode is internal-only
- OPENDJ-1275: Connections stop getting closed due to idle time outs
- OPENDJ-1269: JMX connection counter not being decremented when connections are closed.
- OPENDJ-1266: State index is not updated when an index is deleted
- OPENDJ-1239: dsreplication logs warnings for each replication server under cn=monitor
- OPENDJ-1228: Concatenated schema may contain more than valid schema, possibly leading to further issues
- OPENDJ-1226: Upgrade should only consider .ldif files under config/schema
- OPENDJ-1204: Access Log timestamp doesn't have milliseconds for Connect and Disconnect entries
- OPENDJ-1196: updateSchemaFile "succeeds" if it can't find schema in the templates
- OPENDJ-1190: Under rare circumstances, the DS replication recovery thread (RSUpdater) can spin

- OPENDJ-1189: Integer overflow while sizing scratch files building indexes
- OPENDJ-1183: Cannot reset userPassword through REST interface due to lack of privileges
- OPENDJ-1172: Deadlock between replication threads during shutdown.
- OPENDJ-1160: Write operations to non-groups force groups to be reloaded
- OPENDJ-1148: VLV rebuildTask needs improvement
- OPENDJ-1146: Memory leak in OpenDJ 2.6.0
- OPENDJ-1142: OpenDJ setup does not work in Java8 EA - A security class cannot be found in this JVM
- OPENDJ-1138: searchrate throws java.lang.IndexOutOfBoundsException
- OPENDJ-1131: Rest2LDAP fails to start with GlassFish3.1
- OPENDJ-1115: Internal errors from ModifyOperation - change number was not found in pending list
- OPENDJ-1094: ECL virtual lastChangeNumber attribute can decrement
- OPENDJ-1090: ECL changenumbers get reset after a purge and server restart
- OPENDJ-1056: Secure listener should not be created if proper keying material is not 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-1016: Control panel does not follow static group recommendation from documentation
- OPENDJ-948: Unauthorized disclosure of directory contents
- OPENDJ-737: OpenDJ Administration Connector KeyStore Pin File must be defined and non empty
- OPENDJ-452: Manual add of new schema objectclass in 99-user.ldif are not replicated
- OPENDJ-365: Potential deadlock in JE backend while performing a mix of update operations
- OPENDJ-49: Replication replay does not take into consideration the server/backend's writability mode.

4.2. Limitations

OpenDJ 3 has the following limitations:

- 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.
- When creating additional database backends, adjust the database cache settings to avoid allocating all memory available to the JVM to database cache. Over-allocating memory to database cache leads to out of memory errors.

  By default, a new database backend has `db-cache-percent` set to `50`. When creating a new database backend, you can raise or lower this value by using the `--set db-cache-percent:`*value* option, where *value* is the percentage of JVM memory to allocate to the new backend.
- PDB backend databases limit key size to two KB. In practice, this means, for example, that DN size is limited to roughly two KB.

  Attempts to create an entry with a DN (or other key) larger than the limit cause a `KeyTooLongException` in the underlying backend.
- OpenDJ replication is designed to permit an unlimited number of replication servers in your topology. Project testing has focused on topologies of up to eight replication servers.
- Antivirus and intrusion detection systems that do a deep inspection of database files are not compatible with OpenDJ directory server. Disable antivirus and intrusion detection systems, or at least prevent them from operating on OpenDJ directory server files.
- OpenDJ plugin extensions must follow these guidelines:
  - 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.
  - 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 after upgrade (OPENDJ-991). See that issue for notes on how make that version of the extension work with OpenDJ after upgrade.

4.3. Known Issues

Tip

When deploying OpenDJ servers in production, make sure that you follow the installation instructions. Allow OpenDJ directory server to use at least 64K (65536) file descriptors. Also tune the JVM appropriately.

The following important issues remained open at the time of this release:

- OPENDJ-2631: OOME error while importing 100M entries (online-import) causes the server to crash
- OPENDJ-2624: start-ds in split mode on Windows randomly times out
- OPENDJ-2609: NoSuchElementException on ldapsearch --sortorder when using corresponding vlv index
- OPENDJ-2605: Debian packages should be idempotent
- OPENDJ-2573: Steady high modification load can cause PDB database to grow indefinitely
- OPENDJ-2515: CommonAudit throughput regression
- OPENDJ-2506: Create-backend on Windows: problem with db-cache-percent management
- OPENDJ-2496: Replication on Windows: Failure when stopping a server
- OPENDJ-2446: dsreplication purge-historical uses an inappropriate amount of server memory if many entries match search criteria
- OPENDJ-2415: OpenDJ : ldapmodify fails to add like values with differing case, when caseExactIA5Match is used
- OPENDJ-2408: Setup fails on windows if the opendj instance path contains spaces
- OPENDJ-2357: OpenDJ: debugsearchindex incorrectly returns UNINDEXED when the values exceed the index entry limit.
- OPENDJ-2356: verify-index: not supported against online JE backend
- OPENDJ-2223: Administration Connector hang while deleting backend
- OPENDJ-2222: OpenDJ: Server should not allow creation of a new backend with a sub-suffix when the entry exists in the parent suffix and backend
- OPENDJ-2190: Replicas cannot always keep up with sustained high write throughput
- OPENDJ-2074: excessive emails on out of space condition
- OPENDJ-2048: Setup.bat fails to launch GUI mode, whereas setup.bat --verbose succeeds
- OPENDJ-2007: tools.properties in instance config folder no longer used
- OPENDJ-1998: yum remove depends on running server
- OPENDJ-1906: Improve static group refresh performance
- OPENDJ-1880: KeyTooLongException when creating entries whose dn is longer that 2Kb
- OPENDJ-1783: Unfair write lock policy may cause unpredictable response times

- OPENDJ-1776: Pure RSes cannot detect disk low/full
- OPENDJ-1667: dsconfig batch file processing removes double and single-quotes from attribute values
- OPENDJ-1633: Unable to run tools in offline mode when tools.properties is set up
- OPENDJ-1583: Update procedure of opendj rpm does not consider ownership of processes and files
- OPENDJ-1555: Unresponsive persistent searches on cn=changelog can block the whole server
- OPENDJ-1363: JMXMBean does not handle local connections correctly
- OPENDJ-1325: An error occurred while attempting to perform index rebuild: The database environment could not be opened: (JE 5.0.73)
- OPENDJ-1309: First dsreplication enable could warn before replicating schema
- OPENDJ-1290: Nested backends handles hasSubordinates attribute incorrectly
- OPENDJ-1279: HTTP Connection Handler sometimes returns Internal Server Error when under stress
- OPENDJ-1213: LDIFReader should reject LDIF that contains trailing space
- OPENDJ-1192: Modify request replay failures
- OPENDJ-1169: Exception/error lost when logging ERR_LOOP_REPLAYING_OPERATION
- OPENDJ-1158: rebuild-index leaves backend offline if a backup is running
- OPENDJ-1151: OpenDJ unable to initialize the SSL context an doesn't start
- OPENDJ-1087: OpenDJ Console: Validation checks missing
- OPENDJ-1071: Tasks sometimes fail with error message "There are no tasks defined with ID ..."
- OPENDJ-1052: Exception is logged during dsreplication enable when cn=admin user doesn't exist
- OPENDJ-1007: InstallHelper: endless loop, and other issues
- OPENDJ-990: dsreplication ignores parameter --propertiesFilePath
- OPENDJ-954: Restarted DS fails to detect if it is out of sync
- OPENDJ-934: Changes to RS window-size property require a server restart
- OPENDJ-862: Strange ds-privilege-name behavior
- OPENDJ-810: Non-atomic password state updates
- OPENDJ-640: Text Query Against indexed telephoneNumber Attribute Very Slow

- OPENDJ-573: mustChangePassword function makes-up password change state
- OPENDJ-561: Add operation doesn't get password policy from ds-pwp-password-policy-dn;collective
- OPENDJ-560: Add operation doesn't use subentry-based password policy
- 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 in to the administrative control panel with FIPS-140 enabled in certain cases
- OPENDJ-505: dsreplication enable fails when hostname contains an underscore
- OPENDJ-454: Naming conflict of 2 adds with same DN leaves DIT inconsistent
- OPENDJ-431: Server-side sort control only works on result sets of less than 100000 entries
- OPENDJ-412: Blocked persistent searches may block all worker threads
- OPENDJ-390: ConcurrentModificationException during backup all
- OPENDJ-270: dsreplication disable takes a long time

Chapter 5

How to Report Problems and Provide Feedback

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

If you have found issues or reproducible bugs within OpenDJ 3, report them using the OpenDJ issue tracker.

When requesting help with a problem, 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 and version
  - Storage type and version
  - Java version
  - Web container and 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, use the ForgeRock website.