Release Notes

/ OpenDJ 3.5

Latest update: 3.5.3

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 iv
1. What's New In OpenDJ 3 1
    1.1. What's New In OpenDJ 3.5.3 1
    1.2. What's New In OpenDJ 3.5.2 1
    1.3. What's New In OpenDJ 3.5.1 2
    1.4. What's New In OpenDJ 3.5.0 3
    1.5. What's New In OpenDJ 3.0.0 5
    1.6. Security Advisories 10
2. Before You Install OpenDJ Software 11
    2.1. Java Environment 11
    2.2. Maximum Open Files 11
    2.3. Operating System 12
    2.4. Application Servers 12
    2.5. FQDNs For Replication 12
    2.6. Hardware 13
3. OpenDJ Compatibility 15
    3.1. Important Changes to Existing Functionality 15
    3.2. Deprecated Functionality 19
    3.3. Removed Functionality 19
4. OpenDJ Fixes, Limitations, and Known Issues 20
    4.1. Key Fixes 20
    4.2. Limitations 25
    4.3. Known Issues 26
5. Documentation Updates 30
6. How to Report Problems and Provide Feedback 33
7. Support 34

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.

Note

The OEM distribution of OpenDJ directory server does not include Berkeley DB Java Edition, and so does not support JE backends.

These release notes are written for everyone using the OpenDJ 3.5 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 3

Before you install OpenDJ or update your existing OpenDJ installation, read these release notes.

1.1. What's New In OpenDJ 3.5.3

OpenDJ directory server 3.5.3 is a maintenance release that resolves a number of issues. It is strongly recommended that you update to this release to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

In addition to bug fixes, this release includes the following improvement.

Replication server configurations now include these advanced properties for monitoring disk space use and stopping operations when the disk is full:

`disk-low-threshold`

When this threshold is reached, the server logs warnings and sends warnings to the disk space monitoring subsystem.

The directory administrator must take action to provide more disk space.

`disk-full-threshold`

When this threshold is reached, the server stops operations and lets connected directory servers fail over to another replication server. The replication server can resume operations once free disk space rises above the `disk-low-threshold` setting.

1.2. What's New In OpenDJ 3.5.2

OpenDJ directory server 3.5.2 is a maintenance release that resolves a number of issues, and brings the new capabilities described in this section. It is strongly recommended that you update to this release to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

Backend Database Storage Upgrade

OpenDJ server software now uses a more recent JE Backend implementation, one that is distributed under the Apache License, Version 2.0.

Important

The PDB Backend implementation was deprecated in the next major release, ForgeRock Directory Services 5 (internal version: 4.0.x). That release first shipped on March 29, 2017.

For all new installations, choose JE Backends instead of PDB Backends.

This license is suitable for OEM deployments. The separate OEM deliverables are therefore no longer provided.

Support for TLSv1.2-Only Deployments

All tools now fully support TLSv1.2-only deployments.

OpenDJ server software already supported TLSv1.2-only deployments.

Whitelisting/Blocking for Administrative Connections

The server administration connector has new properties, `allowed-client` and `denied-client`.

These properties let you specify a set of host names or address masks to determine which clients can and cannot establish administrative connections.

1.3. What's New In OpenDJ 3.5.1

OpenDJ directory server 3.5.1 is a maintenance release that resolves a number of issues, and brings the new capabilities described in this section. It is strongly recommended that you update to this release to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

Return Subordinate Naming Contexts

By default, OpenDJ directory server lists only top-level suffixes as naming contexts in the root DSE. For example, suppose the server is configured with two backends, `userRoot` for `dc=example,dc=com`, `subRoot` for `dc=subdomain,dc=example,dc=com`. By default, the root DSE shows only the top-level domain as a naming context:

```
namingContexts: dc=example,dc=com
```

The server now has a boolean root DSE backend configuration property, `show-subordinate-naming-contexts`, that you can set to `true` to cause the root DSE to show subordinate naming contexts (OPENDJ-3305).

The following example sets the option to `true`, and shows the result:

```
$ dsconfig \
 set-root-dse-backend-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --set show-subordinate-naming-contexts:true \
 --trustAll \
 --no-prompt

$ ldapsearch \
 --port 1389 \
 --baseDN "" \
 --searchScope base \
 "(&)" namingContexts
dn:
namingContexts: dc=example,dc=com
namingContexts: dc=subdomain,dc=example,dc=com
```

1.4. What's New In OpenDJ 3.5.0

OpenDJ directory server 3.5.0 is a maintenance release that resolves a number of issues, and brings the new capabilities described in this section. It is strongly recommended that you update to this release to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

1.4.1. New Features and Improvements

The following enhancements are compatible with the previous release of OpenDJ directory server 3:

REST/HTTP Data Access

REST to LDAP now supports multiple APIs each with multiple versions, resource type inheritance, subresource definitions, and protection with OAuth 2.0. In addition, OpenDJ directory server now allows you to expose administrative information over REST:

- REST to LDAP views are now configured separately from HTTP connection handlers (OPENDJ-2755). This means you can configure multiple HTTP views for the same LDAP directory data. Furthermore, OpenDJ directory server can offer additional functionality on the same HTTP handler.

  HTTP endpoints, which provide HTTP views of LDAP directory data, are defined using the **dsconfig** command, and configured using separate JSON files.

  The upgrade process does not migrate your existing configuration. Instead, the HTTP connection handler is disabled, You must migrate the configuration manually after upgrading OpenDJ directory server. For details concerning configuration changes, see "Important

Changes to Existing Functionality". For an introduction to accessing directory data over HTTP, see "*Performing RESTful Operations*" in the *Directory Server Developer's Guide*.

- This version introduces REST to LDAP authorization mechanisms, which map the user identity in an HTTP request to an LDAP user account. HTTP authorization mechanisms allow more fine-grained configuration than the previous `authentication-required` boolean setting. For example, REST to LDAP can act as an OAuth 2.0 resource server (OPENDJ-2774, OPENDJ-2880). You can choose to resolve OAuth 2.0 access tokens by making requests to OpenAM, by accessing tokens stored in OpenDJ directory server itself when the server is acting as a CTS store, or by making requests to an RFC 7662-compliant authorization server.

  HTTP authorization mechanisms can be fully managed in OpenDJ directory server using the **dsconfig** command.

  HTTP authorization mechanisms also allow you map anonymous HTTP requests to a specified LDAP authorization identity (OPENDJ-2926).

  For details, see "To Set Up HTTP Authorization" in the *Administration Guide* and "*REST to LDAP Configuration*" in the *Reference*.

- OpenDJ directory server administrative information can now be exposed over REST (OPENDJ-3130). By default, the API to OpenDJ directory server configuration serves read-write resources under `/admin/config`. The API to monitoring information serves read-only resources under `/admin/monitor`.

  For details, see "To Set Up REST Access to Administrative Data" in the *Administration Guide*.

- REST to LDAP configuration now supports multiple API versions, as well as resource type inheritance and support for subresources (OPENDJ-2871).

  For details, see "*REST to LDAP Configuration*" in the *Reference*.

- OpenDJ REST to LDAP gateway now supports logging as described in "To Install OpenDJ REST to LDAP Gateway" in the *Installation Guide*.

- HTTP access logs now include `cs-uri` and `cs-uri-stem` fields, supplying information about the URI and path requested (OPENDJ-2950).

Data Confidentiality

This version of OpenDJ directory server introduces data confidentiality and integrity for directory backends, indexes, and replication change logs (OPENDJ-2616, OPENDJ-2617, OPENDJ-3007). This feature uses encryption to ensure that data on disk remains confidential and that data is accurate and consistent when read from a backend. It helps protect data on disk when OpenDJ directory server is deployed in the cloud or on a shared infrastructure.

For details, see "Encrypting Directory Data" in the *Administration Guide* and "To Encrypt External Change Log Data" in the *Administration Guide*.

Audit Event Handling

OpenDJ directory server now includes an Elasticsearch audit event handler (OPENDJ-3082).

For configuration instructions, see "Elasticsearch Audit Event Handler Configuration" in the *Administration Guide*.

Password Storage

OpenDJ directory server now implements a Bcrypt password storage scheme that uses the bcrypt message digest algorithm (OPENDJ-2435).

For more about password storage schemes, see "Configuring Password Storage" in the *Administration Guide*.

Native Packaging

RPM packages no longer include a dependency on a Java runtime environment (OPENDJ-2191). This makes it easier to choose which Java implementation to use.

Pass-Through Authentication

OpenDJ directory server now provides an additional property for mapping LDAP attributes in pass-through authentication (OPENDJ-1626).

The `mapped-search-filter-template` property overrides the filter used when searching for the user, substituting `%s` with the value of the local entry's `mapped-attribute`.

Proxied Authorization

OpenDJ directory server now returns clearer messages about account status and password expiration when a proxied operation fails (OPENDJ-2036).

Performance

This version of OpenDJ directory server reduces lock contention for some types of modify and delete requests (OPENDJ-2709).

This version of OpenDJ directory server better manages the number of threads on multi-core systems to improve online import and index rebuild operations (OPENDJ-3123).

1.5. What's New In OpenDJ 3.0.0

OpenDJ 3 provides many new capabilities compared to OpenDJ 2.6.

1.5.1. 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.

Upgrading to the OpenDJ 3 OEM release from OpenDJ 2.6 changes the configuration to create an empty backend with identical configuration. After upgrade old data is no longer accessible. To make the change to the new backend type, you must import the data again into the new backend because the underlying storage implementation is different.

To keep your data during upgrade, either export LDIF from the old backend before upgrading and then import the LDIF you exported into the new backend after upgrading, or get existing data through OpenDJ replication by initializing a new server using the new backend from an existing replica. For details, see "*Upgrading to OpenDJ 3.5*" in the *Installation Guide*.

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 "*Upgrading to OpenDJ 3.5*" 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-1034).

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 "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-2260).

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 "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).

1.5.2. 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 "Using the Modify Password and Reset Password Actions" 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 "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).

1.6. 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.

Note

ForgeRock validates OpenDJ software with OpenJDK and Oracle JDK, and does occasionally run sanity tests with other JDKs such as the IBM JDK and Azul's Zulu. Support for very specific Java and hardware combinations is best-effort. This means that if you encounter an issue when using a particular JVM/hardware combination, you must also demonstrate the problem on a system that is widespread and easily tested by any member of the community.

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 3.5 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

The changes in this section are listed by version.

3.1.1. Important Changes in 3.5.1

The **import-ldif** `--skipDNValidation` option now displays a warning message, but otherwise has no effect.

If you suspect that some entries in the LDIF might be invalid, use the `--rejectFile` option to capture entries rejected by the server during import.

3.1.2. Important Changes in 3.5

Take the following changes into account when upgrading to OpenDJ 3.5:

- When creating a resource with HTTP POST, the `_action=create` query string parameter is now optional.
- REST to LDAP configuration has changed significantly in ways that are not compatible with earlier versions. The changes let you configure multiple endpoints each with multiple versions, resource type inheritance, subresource definitions, and protection with OAuth 2.0. This version of REST to LDAP also brings many minor improvements.

  For the REST to LDAP interface which is still of Evolving stability (defined in "ForgeRock Product Interface Stability" in the *Reference*), the upgrade process does not migrate your existing configuration. Instead, you must migrate the configuration manually after upgrading OpenDJ software.

  If you use the HTTP connection handler to allow direct HTTP access to OpenDJ directory server, how you set up REST access to directory data has changed. The HTTP connection handler configuration has been separated from the HTTP endpoint configuration so that a single handler can expose multiple endpoints.

There are two types of HTTP endpoints. For REST access to user directory data, use a Rest2ldap endpoint. For REST access to administrative data, use an Admin endpoint.

Rest2ldap endpoints can expose multiple versions of the same API. For details, see "Mapping Configuration File" in the *Reference*.

HTTP connection handler properties have moved to HTTP endpoint properties as described in the following table:

HTTP Configuration Properties

Previous HTTP Connector Property	Current HTTP Endpoint Property
`authentication-required`	Use the `authorization-mechanism` property instead to define how to extract the identity from an HTTP request and resolve it to an LDAP user identity.
N/a	`base-path` (new, on all HTTP endpoints) The default `base-path` for the default Rest2ldap endpoint is `/api`. The default `base-path` for the default Admin endpoint is `/admin`. The base path is the same as the name of the endpoint, and it can only be written when you create an HTTP endpoint.
`config-file`	`config-directory` (on Rest2ldap endpoints) The specified file system directory can contain multiple files. Each file defines a version of a REST API.

The configuration files for Rest2ldap endpoints configure only the mappings from JSON resources to LDAP entries. Authentication and authorization settings are configured using the **dsconfig** command.

In addition, the `authenticationFilter` settings in the configuration file for the REST to LDAP gateway are no longer present. Use the `authorization` settings instead to achieve the same ends.

In the configuration file for the REST to LDAP gateway, connection security settings have been consolidated in a top-level `security` field.

For details concerning the current configuration files, see "*REST to LDAP Configuration*" in the *Reference*.

- The RESTful `passwordModify` action has been split into `modifyPassword` and `resetPassword` actions. The `modifyPassword` action lets the user change their password, taking the old and new password as input. The `resetPassword` lets the user or administrator reset a password to a generated value.

For details on the new actions, see "Using the Modify Password and Reset Password Actions" in the *Directory Server Developer's Guide*.

- OpenDJ RPM packages no longer express a dependency on a Java runtime environment. You must make sure you install a Java runtime environment in order to use OpenDJ software.
- Upgrade your deployment to at least OpenDJ directory server 2.6.0 before upgrading to this version. For details on upgrading to that version, see *Upgrading to OpenDJ 2.6.0*.

3.1.3. Important Changes in 3.0

The following changes were introduced in OpenDJ 3.0.0:

- 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 3.5. 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 "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 3.5 `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 "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 "ACI: Disable Anonymous Access" in the *Administration Guide*.

3.2. Deprecated Functionality

This section lists deprecated functionality, as defined in "ForgeRock Product Interface Stability" in the *Reference*:

- The following OpenDJ directory server commands are deprecated:

  setup

  This command is likely to change extensively in a future release.

  uninstall

  This command is likely to be removed in a future release.

- 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

This section covers key bug fixes in OpenDJ 3 software.

4.1.1. Key Fixes in 3.5.3

The following important bugs were fixed in this release:

- OPENDJ-4316: HTTP Connector leaks Session objects
- OPENDJ-3825: Spring daylight savings change can break recurring tasks
- OPENDJ-3931: Replication fails to propagate all changes added after a backup/restore to a newly created instance
- OPENDJ-4148: Disk Monitoring Service notifies of passed over thresholds too often
- OPENDJ-4349: NPE logging MODIFYDN to CSV logs
- OPENDJ-334: PermissiveModifyRequestControl not replicated which may cause divergence
- OPENDJ-4007: Referential Integrity plugin checks all modifications when run as preModifyOperation
- OPENDJ-4087: Persistent search result for cn=changelog does not have EntryChangeNotification control
- OPENDJ-4027: Contention in compressed schema
- OPENDJ-4234: Poor changelog search performance using changenumber ranges
- OPENDJ-4317: Replication: search on cn=changelog with cookie does not retrieve changes
- OPENDJ-4275: Changelog searches cursor through inappropriate replica DBs
- OPENDJ-4392: NPE in JE deadlock detection logic during add/del stress test

- OPENDJ-4328: Specifying ciphers on the Administration Connector causes tool connection failures
- OPENDJ-4212: Replication server thread blocked on ServerHandler.acquirePermitInSendWindow()
- OPENDJ-4115: build and publish missing changes gets confused with non-local changes
- OPENDJ-3507: After upgrading a 2.6.2 server to 3.5.1 server is spinning at 93% CPU

4.1.2. Key Fixes in 3.5.2

The following important bugs were fixed in this release:

- OPENDJ-3793: ThreadInterruptedException when stopping OpenDJ with PwdSyncPlugin installed
- OPENDJ-3791: Upgrade needs to remove old je.jar
- OPENDJ-3767: Offline modifications made to 'schema/99-user.ldif' are no longer replicated
- OPENDJ-3650: Modify-increment values are rejected as not being integers
- OPENDJ-3609: ldif-diff/ldifdiff fails to properly differentiate schema files.
- OPENDJ-3488: Removing an Auxiliary Objectclass from a user in a replicated topology not applied on the remote server
- OPENDJ-3446: ZipException during backup results in a failed backup when a duplicate log entry is found
- OPENDJ-3380: Creating a backend with null base DN can render the instance unusable
- OPENDJ-3237: Disk full scenario can result in empty offline.state files and lead to changelogDb read failure
- OPENDJ-3221: dsconfig cannot connect when the Administration Connector is configured for TLSv1.2 only
- OPENDJ-3045: DNs with backslashes (\) don't display in Control Panel Manage Entries
- OPENDJ-1135: DS sometimes fail to connect to RS after server restart

4.1.3. Key Fixes in 3.5.1

The following important bugs were fixed in this release:

- OPENDJ-3337: dsreplication status on a DS, shows a DS+RS missing after the DS+RS is disabled/enabled.
- OPENDJ-3309: Replication server connection listener thread exits silently
- OPENDJ-3288: Upgrading backends with compressed entries results in unusable JE backends

- OPENDJ-3281: Modify operations may not be replayed if case is mixed on attribute values
- OPENDJ-3231: dsreplication status uses wrong bind DN
- OPENDJ-3230: upgrade: running verify-index on objectclass index incorrectly reports errors
- OPENDJ-3223: upgrade to 3.5.0 should rebuild indexes using DN syntax
- OPENDJ-3147: Regressions on Virtual Static Group membership checks
- OPENDJ-3133: dsreplication status reports M.C. (Missing Changes) when none exist.

4.1.4. Key Fixes in 3.5.0

The following important bugs were fixed in this release:

- OPENDJ-3034: Equality filter with an invalid attribute value evaluates as unindexed rather than an empty result set
- OPENDJ-3032: throwIfIA5IllegalCharacter does not check the first character
- OPENDJ-2969: changelogDb could not be read on OpenDJ instance startup
- OPENDJ-2814: Invalid attribute syntax behavior fails to reject non-boolean syntax values
- OPENDJ-2761: Import does not work when using heap buffers.
- OPENDJ-2731: Middle and final substring indexes fail to return candidates, resulting in an unindexed search.
- OPENDJ-2727: Low performance during import with large index-entry-limit
- OPENDJ-2721: JE is using all the available heap memory during import.
- OPENDJ-2719: PDB entries cannot be larger than 4MB
- OPENDJ-2697: Upgrading JE backend with mixed case loses data
- OPENDJ-2692: Setting up localization with -Duser.language=... doesn't work anymore
- OPENDJ-2659: Privileges can be lost after the BIND
- OPENDJ-2609: NoSuchElementException on ldapsearch --sortorder when using corresponding vlv index
- OPENDJ-1906: Improve static group refresh performance

4.1.5. Key Fixes in 3.0.0

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 3.5 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.

- REST to LDAP query filters do not work with properties of subtypes.

  For example, the default example configuration describes a user type, and a POSIX user type that inherits from the user type. If your query filter is based on a POSIX user type property that is not a property of the user type, such as `loginShell` or `gidNumber`, the filter always evaluates to false, and the query returns nothing.

- When the global server property `invalid-attribute-syntax-behavior` is set to `accept` or `warn`, a search on group membership using a value with invalid syntax returns nothing.

- Due to a Java issue on Windows systems (JDK-8057894), when configuring OpenDJ directory server with data confidentiality enabled you might see an error message containing the following text:

  ```
  Unexpected CryptoAPI failure generating seed
  ```

  If this happens, try running the command again.

- On Windows 8 systems, spurious exceptions from the Grizzly subsystem are displayed when enabling replication with the GUI.

  These exceptions can safely be ignored.

- 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 issues are known to exist in OpenDJ 3.5.3:

- OPENDJ-4598: Replication Server cursoring through obsolete replica IDs causing high CPU spin
- OPENDJ-4295: Syslog data is not fully RFC compliant

- OPENDJ-4210: Cannot import/export LDIF in offline mode after configuring OpenDJ Password Synchronization Plugin
- OPENDJ-4185: Changelog not populated with new changes if an RS+DS goes down and replication fails to catch up when it's restarted
- OPENDJ-3868: Proxied persistent searches are not cancelled/abandoned when the client abandons them or disconnects
- OPENDJ-4178: Performance drop with complex subtree searches between 2.x and 3.5.1/4.0.0
- OPENDJ-3697: OPENDJ service using net start returns early with START_PENDING if OpenDJ starts slowly
- OPENDJ-3877: Proxy authentication configuration not working in rest2ldap servlet
- OPENDJ-3438: Online rebuild-index memory calculation is inappropriate when multiple PDB backends are involved
- OPENDJ-3494: PDB backend spins and runs out of memory if system clock is set backwards
- OPENDJ-3435: Paging controls ignored for certain query filters.
- OPENDJ-3399: DirectoryException while rebuilding index on JE instance during upgrade
- OPENDJ-3153: REST to LDAP gateway: changing password fails when using proxied authorization
- OPENDJ-3212: java.lang.OutOfMemoryError occurred during upgrade
- OPENDJ-3070: JE backends corrupt when low on disk space
- OPENDJ-3057: Replication Server starts listener although ChangeLog DB is unusable
- OPENDJ-2784: Modify RDN does not work if there ACIs with targetattrfilters deny(write) on ldap:/// anyone
- OPENDJ-4058: IDM Account Status notification handler doesn't look for certificates correctly
- OPENDJ-3614: Fully disabling replication using --hostname <IP> only disables the local instance
- OPENDJ-3555: Syslog audit handler does not publish HTTP events if "topics" parameter contains multiple values
- OPENDJ-3341: REST to LDAP gateway: HTTP response for API description is empty
- OPENDJ-3926: On Windows, 'logs/errors' file permissions are not correct when running in production mode
- OPENDJ-3410: Control-Panel: manage schema -> modifying a custom entry does not work
- OPENDJ-3029: dsreplication disable --disableAll does not remove all replication data from other instances' cn=admin data backend.

- OPENDJ-3886: Modifying Json File-Based Access Logger configuration can cause a corrupt log record
- OPENDJ-3299: Editing an existing custom objectClass throws a ConflictingSchemaElementException exception
- OPENDJ-4006: forgerock-je included in releases does not work with Azul Zulu
- OPENDJ-3504: LDAP bytesRead/Written and SNMP counters (dsApplIfInBytes and dsApplIfOutBytes) are not incremented
- OPENDJ-3234: Unhelpful error messages when server cannot read/write tasks backend
- OPENDJ-4243: Replication status's Age of Oldest Missing Change (AOMC) is not reset even if Missing Changes (MC) is 0
- OPENDJ-3343: Invalid Conflict resolution on Add sequence when Parent & Child are added on different replica
- OPENDJ-4296: Rebuilding index on two backends at the same time causes NPE
- OPENDJ-3380: Creating a backend with null base DN can render the instance unusable
- OPENDJ-3963: JMXClientConnections are leaked
- OPENDJ-3437: Cannot delete access log publisher when it is disabled
- OPENDJ-4011: Setup requires TLS to be enabled when using --productionMode
- OPENDJ-3471: ldifsearch command fails to consume @objectclass notation in attribute list
- OPENDJ-3645: SASL DIGEST-MD5: "digest-uri" parameter is not taken into account
- OPENDJ-3643: On Windows "java.properties" does not support values containing "=" character
- OPENDJ-3896: Change number indexer exits due to uncaught IllegalStateException
- OPENDJ-3878: Example plugin POM has wrong parent and is missing repositories
- OPENDJ-3579: Setting Logfile permissions with dsconfig has no effect on Windows
- OPENDJ-4059: dsconfig --bindDN should default to "cn=Directory Manager"
- OPENDJ-3469: Clicking Runtime Options - Java Settings results in an InvocationTargetException exception
- OPENDJ-3406: dsreplication status hangs when client uses TLSv1.2 and server uses TLSv1.1
- OPENDJ-3480: Updating schema backend properties while it's enabled leaves the backend in broken state

- OPENDJ-3054: ldapmodify silently discards duplicate values
- OPENDJ-3224: Infinite loop reading replication changelog if a CSN appears more than once
- OPENDJ-4226: Online list backups command throws error
- OPENDJ-4228: status command with keystore options throws ArrayIndexOutOfBoundsException
- OPENDJ-3966: The Bcrypt storage scheme displays the wrong syntax Range and default for the bcrypt-cost
- OPENDJ-3904: Delivery includes QuickSetup.app and Uninstall.app files for commands that were removed

Chapter 5
Documentation Updates

Warning

Many examples in the documentation trust server certificates with the `--trustAll` option.

Examples using the `--trustAll` option are insecure except within a trusted network segment.

In production deployments, use appropriate trust options. For details, see the Tools Reference in the *Reference*.

The following table tracks changes to the documentation from the release of OpenDJ 3.0.0:

Documentation Change Log

Date	Description
2020-11-06	Added OPENDJ-4598 to the list of known issues.
2018-11-28	• Corrected "*OpenDJ Fixes, Limitations, and Known Issues*" to indicate that the following issue was fixed in version 3.5.3, OPENDJ-4316: HTTP Connector leaks Session objects.
2018-10-09	• Added a procedure "To Move Data from a PDB Backend to a JE Backend" in the *Installation Guide*.
2018-03-05	• Documented that each backend needs its own backup directory in "Backing Up Directory Data" in the *Administration Guide*. • Updated "SNMP-Based Monitoring" in the *Administration Guide* to describe how to find the OpenDMK installer .jar file.
2018-01-24	Release of OpenDJ 3.5.3. • Updated the release notes. • Updated examples using **dsreplication disable --disableAll**. In order to remove the replica's settings from remote replica servers' configurations, authenticate as the global admin using the `--adminUID` option, and not as the local Directory Manager using the `--bindDN` option. • Updated Javadoc, which now describes all ForgeRock classes and interfaces required to write server plugins and LDAP client applications.
2017-07-31	• Refreshed formatting. • Mentioned deprecation of the PDB Backend type. Choose JE Backends instead for all new installations.

Date	Description
2017-04-27	Refreshed the list of known issues.
2017-04-26	Release of OpenDJ 3.5.2. • Updated the release notes. • Updated "Encrypting Directory Data" in the *Administration Guide* to correct the explanation of how shared symmetric keys are encrypted.
2017-02-22	Added a section explaining how JE and PDB backends use disk storage, "About Database Backends" in the *Administration Guide*.
2016-10-27	Release of OpenDJ 3.5.1. • Updated the release notes. • Improved explanations in "*Indexing Attribute Values*" in the *Administration Guide*. • Updated "To Upgrade Replicated Servers" in the *Installation Guide* to clarify that replicas must be upgraded sequentially, not all at once.
2016-07-26	Refreshed the list in "Known Issues". Fixed problems in the installation guide concerning file names in "To Prepare For Installation" in the *Installation Guide*, and concerning configuration instructions in "To Install OpenDJ REST to LDAP Gateway" in the *Installation Guide*.
2016-07-07	Release of OpenDJ 3.5.0. Updates to release notes. Additional documentation changes: • Described configuration for new data confidentiality capabilities. For details, read "Encrypting Directory Data" in the *Administration Guide* and "To Encrypt External Change Log Data" in the *Administration Guide*. • Described updated configuration for REST to LDAP. For details concerning configuration changes, see "Important Changes to Existing Functionality", and "RESTful Client Access Over HTTP" in the *Administration Guide*. For an introduction to accessing directory data over HTTP, see "*Performing RESTful Operations*" in the *Directory Server Developer's Guide*. If you are using OpenDJ 3.0, HTTP connection handler configuration is described in "RESTful Client Access (3.0)" in the *Administration Guide*. REST operations are described in see "*Performing RESTful Operations (3.0)*" in the *Directory Server Developer's Guide*. The 3.0 REST to LDAP configuration is described in "*REST to LDAP Configuration (3.0)*" in the *Reference*. • Clarified requirements for disaster recovery when restoring from encrypted backup files. For details, read "*Backing Up and Restoring Data*" in the *Administration Guide*.

Date	Description
	• Described how to configure and use the new Elasticsearch audit event handler in "Elasticsearch Audit Event Handler Configuration" in the *Administration Guide*. • Described how to allow a regular user to read the external change log in "To Allow a User to Read the Change Log" in the *Administration Guide*. • Described basic OpenDJ directory server plugin development in "*Writing an OpenDJ Server Plugin*" in the *Directory Server Developer's Guide*. • Updated "*Standards, RFCs, & Internet-Drafts*" in the *Reference* to include LDAP schema-related RFCs that were supported but not mentioned in that part of the documentation. • Updated tuning advice for backend databases in "*Tuning Servers For Performance*" in the *Administration Guide*. • Updated "Managing Account Status Notification" in the *Administration Guide* to describe how to send HTML mail messages. • Clarified use of exclusions in fractional replication in "Fractional Replication" in the *Administration Guide*. • Mentioned the new fields in HTTP access logs, `cs-uri` and `cs-uri-stem`, in "HTTP Access Logs" in the *Administration Guide*. • Described new logging configuration in "To Install OpenDJ REST to LDAP Gateway" in the *Installation Guide*. • Fully described the server shutdown process in "Stopping a Server" in the *Administration Guide*. • Documented supported extensible matching rules in "Configure an Extensible Match Index" in the *Administration Guide*. • Demonstrated use of persistent search in "Search: Performing a Persistent Search" in the *Directory Server Developer's Guide*. • Corrected "To Assign Password Policy for an Entire Branch" in the *Administration Guide*.
2016-01-16	Initial release of OpenDJ 3.0.0.

Chapter 6

How to Report Problems and Provide Feedback

If you have questions regarding OpenDJ that are not answered by the documentation, you can ask questions on the OpenDJ forum at https://forgerock.org/forum/fr-projects/opendj/. There is also 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 3.5, 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 7
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.