

NetIQ eDirectory 9.0 SP2 Release Notes

November 2016



NetIQ eDirectory 9.0 SP2 includes new features and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the eDirectory Community Support Forums, our community Web site that also includes product notifications, blogs, and product user groups.

For a full list of all issues resolved in NetIQ eDirectory 9.x, including all patches and service packs, refer to [TID 7016794, "History of Issues Resolved in NetIQ eDirectory 9.x"](#).

For more information about this release and for the latest release notes, see the [Documentation](#) Web site. To download this product, see the [Product Upgrade](#) Web site.

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "System Requirements," on page 5](#)
- ♦ [Section 3, "Installing or Upgrading," on page 5](#)
- ♦ [Section 4, "Known Issues," on page 5](#)
- ♦ [Section 5, "Additional Documentation," on page 7](#)
- ♦ [Section 6, "Legal Notices," on page 8](#)

1 What's New?

eDirectory 9.0 SP2 provides the following enhancements, and fixes in this release:

- ♦ [Section 1.1, "Enhancements," on page 1](#)
- ♦ [Section 1.2, "Updates for Dependent Components," on page 3](#)
- ♦ [Section 1.3, "Operating System Support," on page 3](#)
- ♦ [Section 1.4, "Fixed Issues," on page 3](#)
- ♦ [Section 1.5, "Supported Upgrade Paths," on page 5](#)

1.1 Enhancements

This release introduces the following enhancements:

- ♦ [Section 1.1.1, "Flexible Options to Define Security Configuration," on page 2](#)
- ♦ [Section 1.1.2, "New eDirectory Events to Monitor Login and Authenticate Session," on page 2](#)
- ♦ [Section 1.1.3, "Automatic Containerization of FLAIM Attributes," on page 3](#)
- ♦ [Section 1.1.4, "Creating and Managing Compound Indexes," on page 3](#)

1.1.1 Flexible Options to Define Security Configuration

This release introduces configurable Transport Layer Security (TLS) parameters that allows you to define the following parameters during the TLS communication of LDAP server:

- ♦ **Ciphers**
- ♦ **Protocol**

This release introduces `ldapSSLConfig` attribute which allows you to define protocols and ciphers both in the LDAP server and group object. This release supports the ciphers in the OpenSSL Cipher list format. For more information, see [Configuring Protocols and Ciphers Using ldapSSLConfig Attribute](#) in the *NetIQ eDirectory Administration Guide*.

You can define the following protocols for use with LDAP server:

- ♦ SSLv3
- ♦ TLSv1.0
- ♦ TLSv1.1
- ♦ TLSv1.2

NOTE

- ♦ SSLv3 is disabled by default.
 - ♦ Few cipher configurations allow NULL ciphers. NULL ciphers are not secure and NetIQ recommends to explicitly disable them.
-

For more information, see [Configuring Protocols and Ciphers Using ldapSSLConfig Attribute](#) in the *NetIQ eDirectory Administration Guide*.

1.1.2 New eDirectory Events to Monitor Login and Authenticate Session

This release introduces the following two events to monitor the login and authenticate session events:

- ♦ DSE_LOGIN_EX
- ♦ DSE_AUTHENTICATE

NOTE: To monitor these two events, you need to enable both the XDAS and NMAS Auditing.

DSE_LOGIN_EX event is mapped to the Create Session event in XDAS which is used to monitor the login to the eDirectory tree. For more information, see [Mapping eDirectory Events with XDAS Events](#) in the *NetIQ eDirectory Administration Guide*.

NOTE: eDirectory 9.0 SP2 onwards, DSE_LDAP_CONNECTION event will not be available to monitor Create Session event anymore.

DSE_AUTHENTICATE event is mapped to the Authenticate Session event in XDAS which is used to monitor the background authentication in the eDirectory tree. For more information, see [Mapping eDirectory Events with XDAS Events](#) in the *NetIQ eDirectory Administration Guide*.

NOTE: eDirectory 9.0 SP2 onwards, DSE_LDAP_BIND, DSE_LDAP_BINDRESPONSE and DSE_LOGIN events will not be available to monitor Authenticate Session event anymore.

1.1.3 Automatic Containerization of FLAIM Attributes

This release introduces the option to containerize the FLAIM attributes automatically if the attribute has more than 25 values and a value larger than 2048 bytes. Administrator can disable the automatic containerization if needed. For more information, see [FLAIM Attribute Containerization](#) in the [NetIQ eDirectory Tuning Guide](#).

1.1.4 Creating and Managing Compound Indexes

In previous releases, eDirectory allowed you to create indexes only on one attribute based on a value, presence, or a substring index. This release introduces a new option to create and manage value indexes on multiple attributes. This feature helps to perform search operations on multiple attributes much faster. For more information, see [Index Manager](#) in the [NetIQ eDirectory Administration Guide](#).

1.2 Updates for Dependent Components

In this release, the Java and OpenSSL versions have been upgraded.

Upgrading the Java Version

In this release, the Java version has been updated to 1.8.0_112. The service pack installer automatically upgrade the Java version. No manual steps are required for this.

Upgrading the OpenSSL Version

In this release, the OpenSSL version has been updated to 1.0.2. The service pack installer automatically upgrade the OpenSSL version. No manual steps are required for this.

1.3 Operating System Support

In addition to the platforms introduced in previous releases of eDirectory, this release adds support for the following operating system:

- ♦ RHEL 7.3 (Red Hat Enterprise Linux)

1.4 Fixed Issues

This release includes the following software fixes that resolve several previous issues:

1.4.1 Resolved Security Vulnerabilities

This release resolves the following security vulnerabilities:

- ♦ **CVE-2016-9168:** Resolves the Clickjacking web application vulnerability.
- ♦ **CVE-2016-9166:** Downgrade of communication security.

1.4.2 eDirectory Throws Multiple Login Events to the SLM Server

Issue: Each login attempt to the eDirectory server triggers two events; one event from NMAS and another event from the DS.

Fix: The XDAS event mechanism has been updated to trigger only one event for the login either by NMAS or by DS. The Create Session event is mapped to `DSE_LOGIN_EX` which is used to monitor the login events now. (Bug 613609)

1.4.3 An LDAP Search Using Paged Results and Sort Controls Causes eDirectory Crash

Issue: eDirectory crashes when an LDAP search is performed using both the paged result control and the server-side sort.

Fix: The LDAP server has been enhanced to handle both the paged results control and the server-side sort control in the same search request. Capability to determine the order in which the two controls are performed has also been added. (Bug 834316)

1.4.4 PKI Certificates Do Not Comply With RFC 5280

Issue: Certificates created by the PKI CA contain serial numbers longer than 20 bytes, these do not comply with the RFC 5280.

Fix: PKI CA now generates certificates with serial numbers smaller than 20 bytes. (Bug 934091)

1.4.5 eDirectory Displays Error Message While Restoring a Backed Up Object

Issue: eDirectory displays the `0xFFFFDFF0B` error while backing up a restored object.

Fix: This issue is fixed. (Bug 964463)

1.4.6 eDirectory Crashes in FSGetDomain While Performing Heavy LDAP Operations

Issue: eDirectory crashes while performing heavy LDAP operations. This occurs while getting the next reference from a cursor if the block is not read properly while accessing it.

Fix: eDirectory has been upgraded to read the block properly and position the cursor to it before accessing. (Bug 965402)

1.4.7 eDirectory Crashes While Searching on an Object with Multiple Naming Attribute

Issue: eDirectory crashes while searching on an object with multiple naming attribute and the operational attribute name.

Fix: eDirectory has been upgraded to allocate sufficient buffer while reading the RDN from the object. (Bug 969168)

1.4.8 Intermittent Long Delays While Performing LDAP Searches

Issue: LDAP searches get delayed because of intermittent long delays.

Fix: eDirectory has been upgraded to handle the LDAP searches without causing any delay. (Bug 981856)

1.4.9 CIFS Users Cannot Access DFS Junctions Because of Socket Leak in eDirectory

Issue: Socket leaks in eDirectory is noticed when an interface name is used instead of an IP address.

Fix: This service pack updates eDirectory not to leak sockets any more. (Bug 987581)

1.5 Supported Upgrade Paths

To upgrade to eDirectory 9.0 SP2, you need to be on eDirectory 8.8.8.x or above. For more information on upgrading eDirectory, see the [NetIQ eDirectory Installation Guide](#).

2 System Requirements

For information about prerequisites, hardware requirements, and supported operating systems, see the [NetIQ eDirectory Installation Guide](#).

NOTE: This version of eDirectory supports Identity Manager 4.5 SP4. For more information, see [NetIQ Identity Manager 4.5 Service Pack 4 Release Notes](#).

3 Installing or Upgrading

To upgrade to eDirectory 9.0 SP2, you need to be on eDirectory 8.8.8.x or 9.0. For more information on upgrading eDirectory, see the [NetIQ eDirectory Installation Guide](#).

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact [Technical Support](#).

For the list of the known issues in eDirectory 9.0, refer to the [Known Issues](#) section in the respective release notes.

4.1 ntls.log File Allows Read/Write Permission for All Users

Issue: In case of a fresh installation of eDirectory 9.0 SP2 on any server, only the root users and administrators have the permission to read or write the `ntls.log` file. However, on servers where eDirectory has been upgraded to 9.0 SP2 from 9.0 or 9.0 SP1, the `ntls.log` file has the read/write permission set for all users.

Workaround: Change the file permission after upgrading to eDirectory 9.0 SP2 to allow read/write permission only for root users or administrators.

4.2 eDirectory Continues to Use Existing Non-Secure Connection after Upgrading With EBA

Issue: If a non-EBA eDirectory server is upgraded with EBA or added to a tree which is EBA enabled, eDirectory continues to use existing non-secure connections.

Workaround: You must restart the eDirectory server after upgrading or adding to an EBA enabled tree.

4.3 LDAP Operation Fails when LOW Strength Cipher Is Defined

Issue: LDAP operation fails on secure port when LOW strength Cipher is defined in the `ldapSSLConfig` attribute.

Workaround: We do not have any work around for this issue at the moment.

4.4 Enabling EBA on an eDirectory Server Fails when EBACA Is Missing in the Replica Ring

Issue: Enabling EBA on an eDirectory server fails when the EBACA is not present in the replica ring of the partition containing the server object.

Workaround: Grant inheritable read access over the ACL attribute to the EBACA server object at the eDirectory tree root level.

4.5 Unable to Define ldapSSLConfig Attribute Using the ldapConfig get/set Command

Issue: As per the current behavior, all LDAP attributes except `ldapSSLConfig` can be defined using the `ldapConfig set/get` command.

Workaround: The administrator needs to set the value of `ldapsslconfig` using the **Modify Object** plugin in iManager. You can also use `LDIF` to set the value for this particular attribute.

4.6 eDirectory Server is Not Enabled with EBA After Upgrading

Issue: When upgrading from eDirectory 8.8.8.x to eDirectory 9.0.x, if master replica of the partition is eDirectory 8.8.8.x and there is no EBACA in the tree, enabling EBA on the eDirectory server fails. EBA can be enabled on the master server.

Workaround: You must not enable EBA when upgrading from eDirectory 8.8.8.x to 9.0.x. After upgrading eDirectory, run the `ndsconfig upgrade` utility to enable EBA on the server.

4.7 eDirectory Generates Multiple Tree Keys After Dibcloning

Issue: Dibcloning an eDirectory servers generates multiple inconsistent tree keys.

Workaround: You must update the ACL of the cloned server to use the tree key from the master server before running. For more information, see [TID 7018175](#).

4.8 eDirectory Fails to Upgrade to version 9.0 SP2

Issue: eDirectory fails to upgrade to version 9.0 SP2 after upgrading the OS from SLES 11 to SLES 12.

Workaround: Perform the following actions:

- 1 Remove `gperftools`
- 2 Install the `google-perftools rpm` (`google-perftools-2.4-2.x86_64.rpm`)
- 3 Run the installer with `-b` option

4.9 Unable to select Bind Restrictions for Ciphers

Issue: Bind Restrictions for Ciphers option is deactivated in iManager 3.0 SP2. You can not select this option while using the Identity Manager 4.6 with eDirectory 9.0 SP2 when Suite B is enabled on IDV.

Workaround: Clear browser cache and restart the Tomcat server.

4.10 Uninstallation of eDirectory Fails on Windows

Issue: Uninstallation of eDirectory fails on Windows 2012 R2 with the error code -641 when you browse for users in the eDirectory login wizard.

Workaround: Enter the admin login credentials in the eDirectory login wizard to finish the uninstallation successfully.

5 Additional Documentation

- ♦ [Section 5.1, “Revamped Documentation,” on page 7](#)
- ♦ [Section 5.2, “iManager,” on page 7](#)
- ♦ [Section 5.3, “Novell International Cryptographic Infrastructure \(NICI\),” on page 7](#)
- ♦ [Section 5.4, “eDirectory Issues on Open Enterprise Server \(UNIX only\),” on page 7](#)

5.1 Revamped Documentation

The eDirectory documentation has been revamped. Content from NMAS Administration Guide, Password Management Guide, and Certificate Server Guide is now part of the [eDirectory Administration Guide](#). Use the following links to access these chapters in the eDirectory Administration Guide:

- ♦ [NMAS](#)
- ♦ [Password Management](#)
- ♦ [Certificate Server](#)

5.2 iManager

For iManager information, refer to the [iManager online documentation](#).

5.3 Novell International Cryptographic Infrastructure (NICI)

The NICI Administration Guide is included in the [eDirectory documentation page](#).

5.4 eDirectory Issues on Open Enterprise Server (UNIX only)

For more information on eDirectory issues on Open Enterprise Server (OES), see [OES Readme \(http://www.novell.com/documentation/oes2/\)](#).

6 Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.