

Benefits of Novell® eDirectory™ 8.8 SP5 over 8.7.3x

Table of Contents:	2 Novell eDirectory 8.8 SP5 Features and Benefits
	2 Features
	7 Performance
	8 Interoperability
	8 Compatibility
	8 Scalability
	9 Appendix



Novell® eDirectory™ 8.8 SP5

Features and Benefits

Novell eDirectory is the most widely used identity foundation for managing internal and Web-based relationships between user identities, corporate assets and security policies. Novell eDirectory 8.8 SP5 is a standards-compliant, cross-platform, highly scalable, fault-tolerant and high-performance directory service solution.

This white paper lists eDirectory 8.8 SP5 features and performance results that demonstrate the advantages of deploying eDirectory 8.8 SP5. This white paper is not intended to be a comprehensive guide that addresses deployment patterns, but serves as an executive summary of the benefits of eDirectory 8.8 SP5 over eDirectory 8.7.3x.

Following are the objectives of this white paper:

- *An executive summary of the new features in the eDirectory 8.8 SP5 product line*
- *Performance results indicating the advantages of using eDirectory 8.8 SP5*
- *Interoperability of eDirectory 8.8 SP5 with other Novell products*
- *Compatibility of eDirectory 8.8 SP5 with other existing versions of eDirectory*

Features

Installing eDirectory in a Custom Location

Novell eDirectory 8.8 SP5 offers you the flexibility to install the application, data and configuration files in a location of your choice. Installing eDirectory in a custom location provides the advantage of having multiple versions of eDirectory without disturbing the existing setup. You can test the new eDirectory

version without actually upgrading your current eDirectory, while the test results help you decide whether you should retain your existing version or upgrade it.

Non-root Install

On supported Linux* and UNIX* versions, eDirectory supports non-root installation and configuration of eDirectory servers. Novell eDirectory 8.7.3x and previous versions could be installed and configured only by a root user with only a single instance of eDirectory running on a host. With eDirectory 8.8 or later, any non-root user can use a tarball build to install eDirectory.

After the installation, a non-root user can configure eDirectory server instances by using his or her individual tarball installation, or opt for a binary installation performed by the root user.

Multiple Instances

Traditionally, only one instance of eDirectory could be configured on a server. With the introduction of the Multiple Instances feature, you can configure the following:

- *Multiple instances of eDirectory on a single server*
- *Multiple replicas of the same tree or partition on a single server*

With Multiple Instances, you can configure a pilot setup on a single host before investing in the required hardware. Also, the high-end hardware can be leveraged by configuring more than one instance.

Unattended Install or Upgrade

Novell eDirectory 8.8 SP5 supports automated installations and upgrades so that it can be silently installed or upgraded without human intervention.

- *On Linux and UNIX, the unattended install or upgrade is facilitated by a script and a configuration utility.*
- *On Windows*, the predefined text files facilitate the unattended install or upgrade.*
- *On NetWare®, the system protection kit for the eDirectory 8.8 SP5 upgrade facilitates the unattended upgrade.*

Automatic Deployment through Novell ZENworks®

On Linux, eDirectory leverages Novell ZENworks Linux Management to provide an easy upgrade, distribution and deployment of eDirectory. If an eDirectory feature is updated (upgraded or patched) on the Novell site, you are automatically notified to install eDirectory on a host that has the ZENworks Linux Management server installed, and then roll it out to the other servers that have ZENworks Linux Management clients. Also, you can subscribe to specific eDirectory features through ZENworks Linux Management.

Standards Compliance

- **FHS compliance.** *On Linux and UNIX, to avoid file conflicts with the other product application files, eDirectory adheres to the Filesystem Hierarchy Standard (FHS). Novell eDirectory follows FHS if you have chosen to install eDirectory in the default location. For a custom location, custom_location/default_path is the directory structure.*
- **LSB compliance.** *Novell eDirectory 8.8 SP5 is compliant with Linux Standard Base (LSB). LSB also recommends FHS compliance. All eDirectory packages in Linux are prefixed with "novell."*

Server Health Checks

Novell eDirectory introduces server health checks that determine the health of the eDirectory server before an upgrade begins. By default, server health checks are performed before every eDirectory upgrade. A server health check can be performed by using the ndscheck (dscheck on NetWare) diagnostic tool.

In earlier versions of eDirectory 8.7.3x, the eDirectory upgrade could not perform the health check for the eDirectory server before starting the upgrade. The upgrade operation failed if the server health was not as stable as expected, which could leave eDirectory in an inconsistent state. In some cases, the server could not automatically roll back to the pre-upgrade setting. The ndscheck tool resolves these issues by ensuring that the server is ready for the upgrade.

SecretStore Integration with eDirectory

Novell eDirectory 8.8 SP5 provides an option to configure Novell SecretStore® 3.4x during eDirectory configuration. Before eDirectory 8.8, SecretStore required manual installation.

Novell SecretStore is a simple and secure password management solution that enables you to use a single authentication to eDirectory to access most UNIX, Windows, Web and mainframe applications. For more information, refer to the SecretStore documentation at: www.novell.com/documentation/secretstore34/

Novell eDirectory 64-bit Support

64-bit eDirectory is supported on Linux, Solaris* and Windows 64-bit platforms. 32-bit eDirectory can be upgraded to 64-bit eDirectory.

NICI Backup and Restore

Novell International Cryptographic Infrastructure (NICI) stores keys and user data in the user-specific directories.

Previously, NICI backup and restore operations were manually performed. With eDirectory 8.8 SP5, NICI backup and restore solutions have been automated. A switch has been added to the eDirectory backup solution (DSBK and eMBox backup) to enable:

- *Backing up the NICI keys when an eDirectory backup is run*
- *Restoring the NICI keys when an eDirectory restore is run*

eDirectory Backup with SMS

SMS is an API framework consumed by the backup applications to provide a complete backup solution. SMS helps in backing up applications directly to tape. Target service agent (TSA) for eDirectory (tsands), services the eDirectory targets and provides an implementation of the Novell SMS API for the directory trees. TSA for eDirectory is now extended for Novell Open Enterprise Server for Linux. For more information, refer to the SMS documentation at: www.novell.com/documentation/oes/smsadmin/?page=/documentation/oes/smsadmin/data/hhc3nq5m.html#hhc3nq5m

ICE Utility on Windows

The ICE utility is now available on Windows as well as the Linux/UNIX/NetWare platforms.

The ndspasstore Utility

ndspasstore is a utility that stores encrypted passwords for the SAdmin user and the eDirectory users. It securely stores the eDirectory user password to automate the execution of the ndsbackup utility without providing the passwords in clear text scripts.

Priority Synchronization

Priority Sync is complementary to the current synchronization process of eDirectory. Through Priority Sync, modified critical data such as passwords can be synchronized with greater speed. Priority Sync is supported between two or more eDirectory 8.8 or later servers hosting the same partition.

Priority Sync is typically useful for large deployments, when critical data of an object is modified and changes need to be synchronized immediately on the other servers.

Data Encryption

All versions of eDirectory 8.8 allow specific data to be encrypted on the disk. The same data can be transmitted between two or more eDirectory servers in an encrypted form. Data encryption provides greater security for the confidential information.

Encrypted Attributes

Before eDirectory 8.8, data was stored in clear text on the disk in an internal format. Information such as Social Security numbers and credit card numbers needs to be protected. For example, when a server is hosted in a public domain or when eDirectory is configured on a shared server, the Encrypted Attributes feature can be used to protect the critical information.

Policies can be written to only allow access to the encrypted data over secure channels such as an LDAP SSL port or the HTTP secure port.

Encrypted Replication

Encrypted Replication means encrypting data that is transferred between two or more eDirectory servers.

Data was transmitted in clear text during replication in eDirectory versions before eDirectory 8.8. It might be necessary to

protect confidential data over the wire by encrypting it. This feature is useful when the directory servers are spread across geographical locations through a WAN or hostile environment and there is a need to encrypt sensitive data on the wire.

Encrypted Replication policies are flexible. They can be configured in several ways, including:

- *If only partitions holding the sensitive data in an eDirectory tree need protection, these partitions can be selected for encrypted replication.*
- *Encrypted Replication can also be enabled on specific replicas.*

Nested Groups

Management of identities via grouping is a commonly used feature in eDirectory and identity management deployments. Groups allow easier management of access control administration and are often used by other directory enabled applications. One common use of groups is found in e-mail applications that use groups for mail aliases.

Previous versions of eDirectory supported grouping of user objects but did not allow a group to be nested within another group. Nested groups now help make organizing and maintaining groups more efficient.

LDAP-based Backup

LDAP-based Backup backs up the attributes and attribute values, one object at a time. It allows you to perform an incremental backup where the object is backed up only if there are changes to the object. It also provides a consistent interface that any third-party backup application or developer can use to back up eDirectory on all the supported platforms. The LDAP-based Backup feature

is designed to provide more flexibility in backup and restore operations.

LDAP Auditing

Auditing operations is becoming more and more important to administrators. eDirectory 8.8 SP5 now includes the ability to provide an extensive auditing of the LDAP operations through the LDAP event subsystem. This subsystem generates LDAP-specific events with all the relevant information required by an application to audit the LDAP traffic.

LDAP Network Address Login Restrictions

LDAP now enforces network address login restrictions. This allows control over whether LDAP logins can be performed based on eDirectory station restriction policies.

Case-sensitive Universal Passwords

An administrator can now enable the Universal Password feature and enforce case-sensitive password policies. The following clients and utilities are enabled to use this new functionality:

- *Novell Client™ 4.9 and later*
- *Administration utilities upgraded to eDirectory 8.8*
- *Novell iManager 2.6 and later, except when it is running on Windows*

Making the passwords case-sensitive adds to the security of the directory logins. In eDirectory 8.7.3x, the Universal Password feature enabled the passwords to be case-sensitive only when you logged in through the Novell Client32™. In eDirectory 8.8 SP5, you can make your passwords case-sensitive for all the clients that are upgraded to eDirectory 8.8 SP5 by enforcing the use of case-sensitive passwords.

Authentication to eDirectory through SASL-GSSAPI

The SASL-GSSAPI mechanism for eDirectory enables users to authenticate to eDirectory through LDAP by using a Kerberos ticket and without entering the eDirectory password. The Kerberos ticket is obtained by authenticating to a Kerberos server.

This feature is primarily useful for LDAP application users in environments that already have a Kerberos infrastructure in place.

Security Object Caching

The security container is created off the root partition when the first server is installed in the tree. After Universal Password was introduced, if a user logged into eDirectory through Novell Modular Authentication Service (NMAS™), the NMAS server accessed the

information in the security container to authenticate the login.

When the partition having the security container was not locally present, the NMAS server contacted the server that had this partition. This had an adverse impact on the performance of NMAS authentication, especially when the server containing the partition with the security container was accessed over WAN links. Adding the partition containing the security container on all servers might not be practical in several setups.

With eDirectory 8.8 SP5, the security container data is cached on the local server, which eliminates the need for NMAS to access a security container located on a different machine. When a user logs in, NMAS can easily access the information locally, which increases the performance.

Features and Supported Platforms

Features	Linux	UNIX†	NetWare	Windows
Installing eDirectory 8.8 in a Custom Location	Yes	Yes	No	Yes
Non-root Install	Yes	Yes	No	No
Unattended Install/Upgrade	Yes	Yes	Yes	Yes
Automatic Deployments through Novell ZENworks	Yes	No	No	No
Standards Compliance (FHS,LSB)	Yes	Yes	No	No
Server Health Checks	Yes	Yes	Yes	Yes
SecretStore Integration with eDirectory	Yes	Yes	Yes	Yes
Novell eDirectory 64-bit Support	Yes	Yes (Solaris only)	No	Yes
Multiple Instances	Yes	Yes	No	No
NICI Backup and Restore	Yes	Yes	Yes	Yes
Novell eDirectory Backup with SMS	Yes	No	Yes	No
ICE Utility	Yes	Yes	Yes	Yes
The ndspassstore Utility	Yes	Yes	No	Yes
Priority Synchronization	Yes	Yes	Yes	Yes
Data Encryption—Encrypted Attributes	Yes	Yes	Yes	Yes
Data Encryption—Encrypted Replication	Yes	Yes	No	Yes
Nested Groups	Yes	Yes	Yes	Yes
LDAP-based Backup	Yes	Yes	Yes	Yes
LDAP Auditing	Yes	Yes	Yes	Yes
LDAP Network Address Login Restrictions	Yes	Yes	Yes	Yes
Case-sensitive Universal Passwords	Yes	Yes	Yes	Yes
Authentication to eDirectory through SASL-GSSAPI	Yes	Yes	Yes	Yes
Security Object Caching	Yes	Yes	Yes	Yes
ldif2dib	Yes	Yes	No	Yes

† UNIX = Solaris and AIX

Novell eDirectory 8.8 SP5 supports more platforms with 32-bit and 64-bit operating systems compared to eDirectory 8.7.3x. For more information on the platform and feature support, refer to the eDirectory documentation at: www.novell.com/documentation/edir88/

Performance

Performance Results

A significant improvement in performance has been observed in eDirectory 8.8 SP5 for most of the LDAP operations. The following table shows the performance data of eDirectory 8.8 SP5 32-bit vs. eDirectory 8.7.3 SP10b on SUSE® Linux Enterprise Server 10 SP2 64-bit in a sample environment with similar loads.

	Performance Improvements in 8.8.5 32-bit Vs 8.7.3.10b in %
ICE Upload Test	
Regular Objects	29.39
With Passwords	26.76
Large Size	19.54
Many Values	28.06
Non-standard Naming	37.54
References	47.79
LDAP Test	
Add Basic Users	33.7
Add Bind Users	90.8
Compare Basic Users	4.33
Compare Bind Users	1.9
Modify Basic Users	88.56
Modify Bind Users	58.01
Delete Basic Users	77
Delete Bind Users	56.79
DIRMARK	
Dirmark Search Test	240.73
Bind Test with Login Updates Enabled	
Single-user Bind	712.23
Bind with NDS® Password	691.91
Bind with SSHA Password	279.6
Bind Test with Login Updates Disabled	
Single-user Bind	498.23
Bind with NDS Password	462.18
Bind with SSHA Password	346.58

Build Used	
eDir 8.7.3.10b + ssp205	FCS
eDir 8.8.5	FCS
Hardware	
Server	
Make	HP
Model	ProLiant* DL580 G4
CPU	4 X 3 GHz Intel* Xeon*
RAM	10 GB
Client	
Make/Model	Unbranded
CPU	2 X 2.6 GHz
RAM	8 GB
OS	openSUSE® 10.3

Subtree Search Performance Improvement

AncestorID Indexing. Before eDirectory 8.8, subtree search performance for a large tree with a significantly nested structure remained flat irrespective of the base DN search. In eDirectory 8.8, subtree search performance has been improved by storing additional hierarchical information on each entry. The hierarchical information is used for quick subtree scope evaluation, leading to faster subtree searches.

ACL Optimization. For every attribute on the object returned during a subtree search, all ACLs on the user objects are evaluated. The search operation can be slow if the number of ACLs increases. This is overcome by accessing ACLs only once for the container during the subtree search. After computing RightsBuffer up to the container level, they are serialized and stored in the cache. The cache is reused for all the entries being returned as part of the subtree search. This leads to better subtree and one-level search performance.

Bulk Load Performance

The Idif2dib utility allows bulk loading of data from LDIF files to the Novell eDirectory database (DIB), when the eDirectory server is offline. This offline utility achieves a faster bulk load compared to the other online tools. The Idif2dib utility is quite useful for populating large user databases with entries from an LDIF file. Online tools such as ICE and Idapmodify might be slower than Idif2dib because of the overheads associated with the online bulk load. For example, schema checking, protocol translation and access control checks.

Other Performance Factors

References are maintained by using a new FLAIM index. This increases the performance of add and modify operations. In addition, as the size of an entry in the cache is reduced, more entries can be cached with the same memory.

Interoperability

Novell eDirectory interoperability enhances collaboration capabilities of the applications that make use of directory services and helps reduce IT expenditure. For more information on eDirectory 8.8.SP5 interoperability with other Novell products, refer to the eDirectory 8.8 SP5 and Supported Novell Products Web site at: www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7003446&sliceId=1&docTypeID=DT_TID_1_1&dialogID=60214438&statId=0%20%2060216276

Compatibility

Similar to eDirectory 8.7.3x, eDirectory 8.8 SP5 is also compatible with the older versions of eDirectory in the same tree. For example, eDirectory 8.8 SP5 running on SUSE Linux Enterprise Server 10 SP2 64-bit can coexist with eDirectory 8.7.3 SP9 running on NetWare 6.5 SP6/Red Hat* 4.0. If you have a large number of servers, you can easily upgrade them individually to eDirectory 8.8 SP5 without disturbing the existing environment of mixed versions of eDirectory.

Scalability

In eDirectory 8.8 SP5 64-bit, the FLAIM cache can be scaled beyond the 32-bit eDirectory limit, leading to improved performance. Enhancements in the schema cache and event system lead to greater search scalability.

Appendix

Definitions and Terminology

UNIX—Refers to Solaris and AIX

NICI—Novell International Cryptographic Infrastructure

NMAS—Novell Modular Authentication Service

SASL—Simple Authentication and Security Layer

GSSAPI—Generic Security Services Application Program Interface

SMS—Storage Management Services

TSA—Target Service Agent

ICE—Import Convert Export

Priority Sync—Priority Synchronization

www.novell.com



Contact your local Novell
Solutions Provider, or call
Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA