

Novell

NDS eDirectory 8.5

Reviewers Guide

Quick Profile.....	2
Installation Requirements.....	3
Overview.....	4
NDS Market Facts.....	4
Directory Concepts.....	5
Who Uses NDS eDirectory?.....	7
What can I do With NDS eDirectory?.....	8
Benefits	9
What's New?.....	10
NDS eDirectory Features.....	12
How NDS eDirectory Works.....	14
Installation Hints.....	15
Using NDS eDirectory.....	17
Comparative Information.....	18
About Novell – Contact Information.....	19
Glossary.....	20

Quick Profile

Product: NDS eDIRECTORY 8.5

Summary: NDS® eDirectory™ is a stand-alone, cross-platform directory service that serves as the foundation for the many directory-enabled services that power e-businesses. The number of directory-based applications is rapidly increasing, many of which provide crucial e-business functionality such as automated business-relationship management, supply-chain management, and electronic store fronts. Other services that directory-enabled products can facilitate include automated provisioning, enhanced security, customer profiling, electronic wallets, automated notification systems, customized Web interfaces, and virtual private networks (VPNs).

Announce date: September 28, 2000

Availability: October 16, 2000

Key New Benefits: Stronger LDAP application support, filtered replication, federation, support for DirXML, ICE (Import/Convert/Export) Utility, iMonitor, better performance, automatic tuning for caching and indexing.

Pricing: There is no charge for NDS eDirectory if purchased with NetWare 5.x. Sun Solaris, Microsoft Windows NT and Windows 2000, Linux and Compaq Tru64 Unix versions are \$2 per user.

Licensing: NetWare - matches user count.

Windows NT/2000, Linux, Solaris, Tru64 - per user

Corporate or open-ended user count pricing available

Special pricing schemes for ISV/OEMs and ISP/ASPs

Availability

- Novell Authorized Resellers
- Through Novell Direct Sales
- Novell Web Site - <http://www.novell.com/products/nds>

For Additional Information: www.novell.com/products/nds

Installation Requirements

Administration Workstation Requirements

- Using ConsoleOne
- For any Windows workstation (NT, 98, 2000)--Novell Client

Server System Requirements: NetWare, Windows NT, Linux

Objects	Processor	Memory	Hard Disk
100K	Pentium III 450-700 MHz (Single)	384 MB	144 MB
1 Million	Pentium III 450-700 MHz (Dual)	2 GB	1.5 GB
10 Million	Pentium III 450-700 MHz (2-4)	2 GB+	15 GB

Server System Requirements: Solaris

Objects	Processor	Memory	Hard Disk (min)
100K	Sun Enterprise 4500	384 MB	144 MB
1 Million	Sun Enterprise 5500	2 GB	1.5 GB
10 Million	Sun Enterprise 6500 with multiple processors	2 GB+	15 GB

Overview

As the Internet connects more and more businesses, the need for better management intensifies. eBusinesses need the ability to manage shared information, distributed relationships, connections and the resources and infrastructure that support them. The ability to manage diverse and geographically disparate resources is key to the success of any eBusiness or e-commerce partner. Managing identities and 'who has access to what', monitoring behavior, controlling quality of service--all through a simple, easy to use interface is critical to the evolution of business-to-business (B2B) and business-to-consumer (B2C) markets.

But the complexity of today's network environments is preventing organizations from realizing this goal. Multiple platforms, legacy systems, internal and external networks, and an endless stream of new technology make managing networks more difficult than ever. At the same time, the network is evolving from a medium that provides connectivity and information sharing to one that will serve as the new strategic platform for eBusiness.

At Novell, we envision a world in which all types of networks work together as one Net to provide the power and flexibility organizations need to succeed in the Net economy. NDS eDirectory is the solution to this Inter-networking management need. As the next generation of Novell's leading directory, NDS eDirectory allows organizations to easily manage Internet relationships and resources. The result is an extremely powerful and versatile management solution that allows e-businesses to manage all aspects of customer, partner, supplier, and employee identities and relationships. eDirectory allows you to easily manage who has access to what, when and how--anywhere on the Internet.

NDS Market Facts

Since NDS was introduced in 1993, it has become the world's most popular directory service, with over 66 million users. NDS 8, first released on NetWare 5, introduced a greater level of functionality than any previous version, with support for billions of objects, industry leading search performance, scalability and open Internet standards.

With the release of NDS 8, Novell committed to make NDS available on leading OS platforms in order to fulfill its vision of one Net – where applications and services run seamlessly across all networks regardless of operating system. NDS eDirectory fulfills that commitment running natively on multiple platforms, bringing the power of NDS to e-businesses with heterogeneous networks.

Novell's eDirectory significantly simplifies the complexities of managing users and resources in a mixed Win2000, NT, NetWare, Unix and Linux environment. It is the industry's only secure, scalable, cross-platform directory service, allowing organizations to centrally store and manage information across all networks and operating systems, and leverages existing IT investments. It supports many existing and emerging standards in the directory space such as LDAP (Lightweight Directory Access Protocol), SSL (Secure Socket Layer), DNS (Domain Name System), LDIF (Light-weight Data Interchange Format), XML (Extensible Markup Language), XSL (eXtensible Stylesheet Language), XSLT (eXtensible Stylesheet Language Transformations), HTTP (HyperText Transport Protocol), ADSI (Active Directory Service Interface), ODBC (Open Database Connectivity), JDBC (Java Database Connectivity) and many others. It is also designed to be extensible for accommodating legacy and proprietary solutions.

Directory Concepts

Directory services are one of the most powerful yet least understood networking technologies. The evolution of the Internet and e-business has intensified the need for a viable identity management service that allows individuals and systems to securely interact across all types of networks — the Internet, intranets, and extranets; wired to wireless; corporate and public — across leading operating systems. Identities of associates, customers, partners and suppliers are validated and access to specific applications and resource is easily managed through a secure, full-service directory service. This allows companies to build highly customized e-business relationships.

Novell's eDirectory is the industry's premier and most prevalent directory service technology. Several characteristics differentiate a true directory service from a common database or user identification list with user IDs and passwords. These characteristics are hierarchy, inheritance, standards support and distributed systems.

Hierarchy - In 1988, the X.500 standard was established for managing online directories of users and resources. The X.500 standard is hierarchical meaning that it appears like an inverted tree with a single trunk at the top and branches that extend below. This hierarchical structure fits the world's classification system: countries, states, cities, streets, houses, families, etc. The objective is to have a directory organization structure that can classify any resource globally. Every resource or user can be classified by the company it belongs to (tree), the division it is in (organizational unit), the department that it is part of (group), and it's unique characteristics. Using a hierarchical organization structure, it is possible to classify and map relationships between any two users or resources--no matter where they may physically reside.

[insert image_1.jpg]

Inheritance - Hierarchy is crucially important to the second distinguishing characteristic of a directory service, inheritance. Objects in a tree (organizational units, groups, users, services, etc.) are defined by attributes--characteristics such as access rights, descriptive properties, etc. Inheritance makes it possible for many objects lower in the tree to be assigned or 'inherit' properties from other objects higher in the tree. For example, a 'group' object might have a URL attribute that provides 15 people in the group with access to a specific Internet data feed. By changing the URL attribute once at the group level, all 15 users will automatically inherit access through the new address. Inheritance is a powerful characteristic that makes it possible to manage large quantities of users and resources with a few simple steps.

Standards Support - The number of disparate and single purpose user management solutions for verifying identity and granting access is staggering. Many applications have their own proprietary user database; each of the leading operating systems have their own methods; and thousands of others have been kludged together to accommodate existing IT environments. Integrating, synchronizing and managing these disparate systems is a daunting, if not impossible, task. The evolution of an open standard that provides true directory characteristics that are extensible or modifiable is extremely important. Lightweight Directory Access Protocol (LDAP) is that standard. It provides the capability to import or export directory objects and their attributes as well as extend a directory schema (add new object types or properties). The ability to pull disparate directories together for central management based on open standards support is a primary requirement for an exceptional directory service. Open standards becomes increasingly important as disparate resources are connected across the Internet

Distributed Systems - Conceptually, a directory service appears as a single central repository of all resource information. In reality, an enterprise level directory service must have the ability to be distributed both physically and virtually. To avoid a single point of failure (if all directory information were in one physical place at the time of a disaster), copies of a directory must be placed in different locations and linked in such a way that if one location goes down, all information is still accessible from other locations. A directory must also have the ability to be distributed or divided virtually so that pieces of it are available for different applications. For example, some user object attributes like 'phone number' and 'address' may be valuable throughout a directory network; other attributes such as 'directory rights' only need to be available from where the user regularly logs in. NDS eDirectory is distributed using replicas, partitions and indexes.

A true directory service then becomes the nerve center for a distributed system of resources. It holds attribute or characteristic information about the resources; it monitors status; it prevents or grants access; and it includes mechanisms to protect or heal itself in the event of outages. A directory can vastly simplify administration by consolidating all management functions to a single service. All applications, users, peripherals, devices, connections, processes, groups, etc. can be managed through a single interface using a directory service such as NDS eDirectory.

Who Uses NDS eDirectory?

NDS eDirectory was created for ISPs, ASPs and IT departments of organizations who need an industry-strength directory service as a strong foundation for building their e-business solutions. The current release has been carefully built for interoperability with other directories and databases. As a result, it has use across many different applications--both on a closed network and across the Internet. It is especially applicable in mixed environments for managing heterogeneous networks. Here are a few examples of how organizations are implementing eDirectory to solve identity management problems and create leading edge applications.

Organization Type	What they do	NDS eDirectory implementation
Software Developer	Software maintenance service	Delivers upgrades and patches over the Internet to subscribers--NDS eDirectory manages subscribers.
Equipment Manufacturer	Sell equipment through network of distributors and dealerships	NDS eDirectory provides distributors and resellers with personalized view of account information.
Application Service Provider (ASP)	Provides small business and HR applications through the Internet	NDS eDirectory controls who has access to which applications based on user or group identity along with billing statistics.
Internet Service Provider (ISP)	Provides Internet access, e-mail, Web-hosting, etc.	NDS eDirectory manage user accounts and coordinates accounting information.
E-commerce site	Sells retail goods through the Internet	eDirectory manages customer accounts. Application tracks customer activity and grants privileges based on buying behavior and serves up customized Web content based on a user's profile or identity.
Information Publisher	Provides specialized, quality information to specific customers	NDS eDirectory used for customer profiles and controlling who has access to what information.
Trade Exchange	Aggregates news, messages, auctions, e-commerce sites, etc. for exchange members	NDS eDirectory manages relationships between exchange members. Monitors behavior and controls access to databases.
Small, Medium and Large Corporations	Business of all types	NDS eDirectory provides graded levels of directory services access (e.g. applications, databases, systems, etc.) internally and externally with customers, partners, suppliers, employees and other businesses.

What can I do with NDS eDirectory?

Potential directory-based applications for NDS eDirectory fall into several broad categories. Some of the more common uses include the following:

Activity	Example
Automated provisioning	NDS eDirectory can be used to 'auto-provision' new objects in the directory. An example is setting up a new employee as a user. By pre-establishing rights to resources such as e-mail, Internet connections, specific applications, etc. by groups or organizations, once a new user is added to the directory, all of these resources are automatically available on first login. With one simple 'add new user' operation, access to all group resources are instantly available.
Customized Web sites	Web sites can use NDS eDirectory to control what Web pages or what Web icons will appear based on a user's identity. NDS eDirectory can be used to create 'personal portals' that display applications, Web links, icons, or customized applets depending on user or group identity.
Supply-Chain Management	NDS eDirectory can be used to collect and store information and attributes about suppliers, partners and customers. These attributes can then be used to control or monitor what information is available to whom. Preferred customers can see custom price lists; suppliers can monitor inventory; customers can check account status, etc.
E-Commerce	There is no limit to the number of type of e-commerce applications that can be created using NDS eDirectory. Directory information can be used to monitor and administer e-commerce components such as Web servers, transaction servers, databases, firewalls, routers, caching appliances, etc. NDS eDirectory can be used as both a monitoring tool for processes as well as an authentication tool. NDS eDirectory's certificate authority capability enables the management of digital certificates for authentication.
Dynamic Document Publication	A directory management system allows publishers to grant or limit access to documents or portions of documents based on identity. Report publishers for example, can limit access to document abstracts for 'guests' or grant full access plus extended search and document management services to established clients.
User Management Systems	Again, NDS eDirectory can be used for any user management solution. Applications, networks, phone books, listings, etc. Users can be organized by function, group, geographical location, company, and many other classifications.
Customer self-service	Implementation of NDS eDirectory enables companies (especially Web-based) to provide higher levels of customer self-service. The directory controls access to specific applications, limits views to specified accounts, and enables the implementation of tools that help customers help themselves.
Network Management Systems	Novell's strong point - management of all users and resources on the network with a reliable, robust, secure and distributed solution.
Virtual Private Networks	Used in conjunction with network infrastructure equipment, NDS eDirectory can be used to establish VPN relationships and links and provide quality of service to VPN users based on identity.
Sharable Address Books	When NDS eDirectory is used as the basis for a 'white pages' directory, object information and attributes can be used for many types of different address books. Simple or complete listings, various formats, indexes or sort orders can be created for shared use among many groups or applications.
Quality of Service	With today's ability for technology to provide varying levels of performance and service, NDS eDirectory is a natural fit for managing quality of service. Preferred customers, company executives or premium partners, based on identity verification, can get more bandwidth, preferred routing, premium levels of fault tolerance.
Enterprise Network Management	NDS eDirectory enables efficient management of corporate resources (e.g., proxy, firewall, e-mail, file, print, NT shares, NT domains, NT users, applications, desktops, DHCP, Solaris user accounts, network bandwidth, help desk, etc.)

Benefits

NDS eDirectory benefits extend to ASPs, ISPs, ISVs, enterprise companies and organizations of all types and sizes. The major advantages of eDirectory can be categorized as follows:

Foundation for Directory-enabled Applications	A directory foundation enables administrators to manage all applications, users and resources from a single point using a single interface. User and group identities and relationships are established once and available for use by any application on the network or across the Internet.
Access Resources with Single Login	NDS eDirectory eliminates the need for multiple logins or multiple user ID/password combinations. A user's identity is established once and then available for all authentication needs. Any application can verify identity with the directory, thus eliminating the need for application user databases.
Securely Protect Online Resources	NDS eDirectory controls access to any network or online resource. Access control can be established for applications, files, devices, connections, Web sites, e-mail, news/discussion groups, databases, information repositories, etc. This access can be controlled over local networks, through VPNs, over the Internet or across wireless connections.
Personalization	NDS eDirectory provides personalization through identity management. Identities include attribute information that specifies what users have access to and what level of service they are entitled to. On verified login, personalization can provide better bandwidth, preferred pricing, access to more information, extended application functionality, etc. Personalization also includes relationship management--which groups a user is a member of and what rights and privileges flow from those relationships.
Quality of Service	Once identity is established, quality of service levels can be granted. Being part of the 'executive staff' group could entitle members to more bandwidth, higher level income reports, or priority status with travel requests.
Simplified Management	An obvious and direct benefit of NDS eDirectory is the ability to 'manage much more with much less effort'. Entire organizations can be granted or denied access with one simple step. One user can be granted or denied access to many resources with a single process. NDS eDirectory can manage all types of resources from any point on the Internet.
Reduced Cost of Network Computing	NDS eDirectory reduces the total cost of ownership in multiple ways. Administration costs are reduced as fewer people can easily manage more resources. Integration and development costs are reduced or eliminated as all applications and resources can use a single directory. Users can more efficiently access more resources with less effort. NDS eDirectory builds a repository of identity intelligence that is valuable to new Web applications and inter-company relationships.

What's New?

NDS eDirectory 8.5 has been enhanced over previous versions for performance and with a list of new and updated features that include:

Feature	Description
New Access Agent	Novell's directory user agent has been consolidated into a single package (NDSBase) simplifying the process of directory-enabling an application. This and its dependent package (NDSSlp) are the only ones required to support directory-enabled applications to access NDS eDirectory server.
Command Line Configuration	New command line utilities, ndsconfig and ldapconfig, have been introduced to augment the screen-based ndscfg utility. These utilities make it quick and easy to create new trees, add a new replica server into an existing tree, query or modify parameters for the replica server and its LDAP service.
Filtered Replication	Incoming or outgoing filters can now be applied on objects (or attributes of an object) when synchronizing data with another replica server. It is now possible, for instance, to place a replica server in a branch office that only contains address book information. By using filters to throttle synchronization traffic, a partition can now be replicated to over 100 servers.
Custom Indexes	Custom indexes on arbitrary attributes are now supported. Indexes can be configured and managed through ConsoleOne snap-ins for the server object or through LDIF files. This enables different geographical sites to have their own custom indexes for personal or unique use that are not replicated to other locations.
Schema Upgrades	POSIX Schema (RFC 2307) is now available in the default installation. A command line utility, ndssch, is provided to add any custom schema updates to NDS eDirectory. This is in addition to the ability to upgrade schema through LDIF imports and through Schema Manager tool in ConsoleOne.
DNS Federation	Trees can now be created under DNS domains. When a server in such a tree encounters an object from another such tree, it will automatically lookup DNS to locate the server for the remote object and establish communications. Essentially, this means a tree no longer limits the namespace for NDS objects. They can be merged into a single large namespace through DNS.
Flexible Cache Management	Linux system administrators will have more flexibility in specifying cache memory. Cache allocation can be specified in terms of percent of free memory or available memory, with free memory computed dynamically at intervals, if necessary. Administrators can also tune caches for bulk updates (typical during initial population) or for fast searches (regular operations).

<p>Full-service LDAP v3</p>	<p>Novell has added many extensions and controls such as VLV (virtual list view) that makes it easy to browse through containers containing millions of objects and server-side sort (reduces computational load on the client by pre-sorting results at the server side). DSE (Directory Server specific Entry) response has been expanded to return much more information about the replica server.</p> <p>Traditional LDAP-based utilities like ldapsearch, ldapmodify, ldapdelete are now included. In addition, a separate toolkit allows developers to create utilities for managing partitions and replicas through LDAP extensions and controls.</p> <p>A powerful command line utility, ICE (for Import, Convert, Export), allows LDIF files to be imported into NDS or NDS data exported into LDIF files is now included.</p>
<p>LDIF (LDAP Data Interchange Format)</p>	<p>NDS eDirectory accepts an expanded set of LDIF codes including the ability to describe Schema, Access Rights, LDAP mappings and Attribute Indexes.</p>
<p>Internet Ready Security</p>	<p>NICI (Novell International Cryptographic Infrastructure) is now fully implemented in user space and will run on all commercial distributions of Linux. SSL support for LDAP is now available on all supported platforms.</p>
<p>ConsoleOne – unified graphical management console</p>	<p>The much anticipated ConsoleOne graphical shell now runs natively on Linux along with all the required management snap-ins.</p>
<p>NDS iMonitor – HTTP Portal</p>	<p>A HTTP portal that allows directory administrators to monitor NDS server agent operations such as synchronization, server uptime and availability all the way down to packet level throughout the network through a Web browser. Works even across a firewall.</p> <p>The portal service can be loaded on any replica server in the tree, to monitor any NDS operation on the entire tree.</p>
<p>ICE Utility (Import/Convert/Export)</p>	<p>ICE is a powerful directory management and administration tool providing customers with the ability to efficiently import large amounts of data in LDIF format into NDS (and other LDAP directories), export data from LDAP directories (including NDS) to LDIF format, and migrate data between LDAP directories. In addition to its ability to import and export data, the Novell Import Convert Export utility can also utilize XML rules to process data. The XML rules used by ICE are the same rules that DirXML uses. The utility supports schema, placement and creation rules. Examples of the tasks that can be accomplished with these rules include mapping schema elements, changing the placement of objects, and providing default values for required attributes.</p>

NDS eDirectory Features

The following is a summary list of features and functions that are available to administrators, users and developers using NDS eDirectory:

Feature	Benefit
Scalability	
Billions of objects per tree	Unlimited capacity for managing the largest collections of network resources.
Millions of objects per container	Unlimited capability for storing user profiles, policies, rules, etc.
High performance	Independent third-party Key Labs benchmarking study found NDS eDirectory performed LDAP searches up to 35% faster than Netscape Directory Server.
Fast search, auxiliary classes, referrals, controls	Enhances high performance use of the directory by any application.
Indexed objects and attributes	Flexible attribute-level indexes allow performance to be optimized based on usage profiles.
NDS Partitions - segments directory into smaller pieces	Enhances speed of authentication for distributed and remote users.
Interoperability	
Full LDAP Compliance	Provides an open standard for access by any application designed to take advantage of LDAP.
Multiple Platform Hosting	Designed to run on multiple operating systems including NetWare, Windows NT/2000, Linux, Solaris and Tru64.
Interoperable Cross Platform	NDS eDirectory running on any platform can interoperate with NDS eDirectory running on any other platform.
Programmability	SDK enables developers and ISVs to create specialized directory applications or directory-enabled applications using indexes, auxiliary classes, referrals and controls.
Standards Support	
Native LDAP	Interoperability with all LDAP-enabled directories and applications.
LDIF	Lightweight Data Interchange Format enables import of directory information from other sources.
Network Protocol Support Security	Works across TCP/IP networks as well as IPX. Secure Socket Layer (SSL) support ensures secure session connections.
Other Internet Standards	Supports Hyper-Text Markup Language (HTML), Domain Name System (DNS), XML (eXtensible Markup Language), XSL (eXtensible Stylesheet Language), XSLT (eXtensible Stylesheet Language Transformations), and many others.
Interface	eDirectory management interface options include Java (ConsoleOne), HTML (Web) or Windows.
Identity Management	
Unique Identity	Individually specify rights and access to resources for any individual or unique user.
Group Membership	Grant multiple rights or access to objects through

Organization Membership	group membership. Establish rights and access for partners, customers, suppliers (outside stakeholders) to internal or shared information. Manage online relationships.
Containment	Hierarchy allows child objects (those lower in the tree) to inherit attributes of parents. Characteristics of containers such as organizational units (OUs) apply to objects in container.
Utilities	
ICE (Import/Convert/Export)	Easy import of millions/billions of objects into the directory.
Management Utilities	Monitor, repair, manage partitions and replicas, etc.
Management	
Multiple interface options - Windows, Web, ConsoleOne	Administrators can select their interface of choice depending on workstation and location.
Central management	All resources are managed from a single management console.
Fault Tolerance	
Replication	NDS eDirectory contents can be replicated to multiple servers in different locations creating an automatic fail-over solution in the event of a downed server.
Multi-master	NDS eDirectory master replicas may be available at alternate locations in case of failure for automatic fail-over.
Security	
PKI, cryptography and authentication services	Provides administrators with easy, flexible control over their site's security policies.
Multiple authentication options including encrypted passwords over SSL, X.509 v3 certificates, and smart cards	Enables secure environment with the Internet, extranet and electronic commerce.
Novell Modular Authentication Service (NMAS)	Security implementations are extensible via Novell Modular Authentication Service (NMAS) that provide multiple login methods based on password, physical device or token and biometric authentication.
Stores access control list (ACL) information	Allows single sign-on for any application or service using the directory.

How NDS eDirectory Works

NDS eDirectory runs natively on multiple operating systems. Novell NDS eDirectory works along the same principles of previous versions of NDS except that it now extends to include the management of resources through the Internet.

There are excellent resources available on Novell's Web site that provide a baseline for understanding what NDS eDirectory is and how it works. Check out the following links for more information:

- **A primer on NDS Objects -** <http://developer.novell.com/research/sections/netmanage/dirprimer/2000/november/p001101.htm>
- **A description of Replicas and how they work -** <http://developer.novell.com/research/sections/netmanage/dirprimer/2000/septembe/p000901.htm>
- **Novell's AppNotes on the Web -** <http://developer.novell.com/research/index.htm>

[insert image_2.jpg]

Installation Hints

Included with NDS eDirectory 8.5 is a comprehensive 'quick start' guide that details installation for each of the supported operating systems (NetWare, Windows NT/2000, Solaris, Linux, and Tru64). Using this guide should answer most questions for general installation.

Since eDirectory implementations can range from simple to very complex and can be used for a multitude of different applications, a complete, step-by-step guide would be difficult. The following sequence is generally followed when setting up NDS eDirectory for the first time.

- Install or prepare the appropriate operating system with adequate memory and disk space.
- Depending on the intended configuration, your entire NDS eDirectory can be set up to run a single dedicated server, to run on one server in conjunction with other applications such as Web server or database, or it can be distributed across several shared or dedicated servers. Install NDS eDirectory.
- Connect this instance of NDS eDirectory with other instances of NDS depending on configuration.
- Configure resources in the directory. This includes creating trees, organizational units, organizations, groups and users as well as servers and applications. Configuring organizations, groups and users is usually done manually through one of the NDS eDirectory interfaces. Many NDS eDirectory applications will configure themselves automatically on install.
- Establish replicas and partitions for redundancy, fault tolerance and distributed access. Several tools are available from third-party vendors to assist in this process.
- Establish parameters for working with LDAP-enabled applications or tying to other LDAP directories.

Sample eDirectory LDAP configuration screens.

[insert image_3.jpg]

[insert image_4.jpg]

Using NDS eDirectory

Due to its flexibility, eDirectory can be applied to many, many different solutions. A complete description of designing an eDirectory application is beyond the scope of this guide and more detailed information can be found in Novell's NDS eDirectory™ Design 2000 document located at <http://www.novell.com/products/nds/nds-design-2000.html>.

Some general directory design guidelines from this document include:

- Novell recommends a single tree for most organizations. The benefits of one tree include single user identity, simple administration and security, and a single point of management.
- Disk and memory needed depends on the size of your tree. To calculate disk requirements, a typical NDS object is 3 to 5 KB in size. Other approximations are 75 MB of disk space for every 50,000 users.
- If your organization is geographically distributed, let Organization Units (OU) represent different geographical areas. This decreases replication traffic across WAN links.
- Note the following limits:

Partition size	Unlimited objects
Total number of partitions in tree	Unlimited
Number of child partitions per parent	150 partitions
Number of replicas per partition	50 replicas
Number of replicas per server	250 replicas

- Design the top of the tree based on the WAN infrastructure
- Design the bottom of the tree based on the organization of network resources
- Partition the top of the tree based on the WAN infrastructure
- Do not create a partition that spans your WAN infrastructure
- Partition around the local servers in each geographic area
- Keep master replicas in central locations

Comparative Information

Other products in the Internet directory space are available. In all cases however, these products are relatively immature in functionality, scalability and performance when compared to NDS eDirectory and its proven track record. NDS has been used for years by the world's leading enterprise companies in environments that demand scalability, fault tolerance, performance, cross platform support and extensive integration capability.

Product	Company	Advantages	Disadvantages compared to NDS eDirectory
Microsoft Active Directory	Microsoft, Corp. www.microsoft.com	Broad application support	Limited scalability, limited cross platform support (Windows 2000 centric), no event system, weak distributed replica model, limited administration client support
SecureWay Directory	IBM www.ibm.com	Builds on established DB/2 customer base	Limited to DB2 database, performance sub NDS standard
iPlanet Directory Server (Netscape)	iPlanet www.iplanet.com	Good performance on single server, open standards based, broad client support	LDAP based protocol is more gateway than directory service, limited fault tolerance (no multiple server replication), scalability limited to single server
Oracle Internet Directory (OID)	Oracle www.oracle.com	Based on Oracle 8i, large installed customer base	Lack of ISV support, product maturity, scalability compared to NDS eDirectory
X.500 Directories	Peer Logic, Nexor, Siemens, Syntegra, DCL, etc.	Open standards based	Minimal market acceptance, established product support, ongoing enhancements and development

In some instances, databases containing user IDs and passwords are considered in lieu of a directory service. The advantages of using a database for access control are usually only apparent if the applications being controlled are also written using the same database (i.e. access to accounting and finance applications written in Oracle are controlled using UIDs and passwords contained in Oracle). The disadvantages of using a common database for access control are many. Databases typically are centrally located and not distributed limiting failover and fault tolerance abilities. They require extensive programming to interface with other applications not built on the same database. And, they do not have the benefits of hierarchy and inheritance that are included with NDS eDirectory.

About Novell

Novell, Inc. (NASDAQ:NOVL), is the leading provider of Net services software that delivers services to secure and power all types of networks — the Internet, intranets, and extranets; wired to wireless; corporate and public — across leading operating systems. Novell's Net services software provides the foundation for one Net — a single global network that supports new applications and forms of business. Net Services software gives IT organizations a way to adapt and accelerate their transformation to e-business, simplify the management and control of all networks, create a secure foundation for doing business on the Net, and help deliver a consistent and high-quality experience to end users in all locations. Worldwide channel, consulting, education and technical support programs, along with strategic alliances, combine Novell Net services software with third-party products and services to form complete Net solutions.

For information on Novell's complete range of products and services, contact Novell's Customer Response Center at (888) 321-4CRC (4272), or visit Novell's Web site at <http://www.novell.com>. Press may access Novell announcements and company information on the World Wide Web at <http://www.novell.com/pressroom>. In addition, detailed comparisons between Novell products and competitive offerings from other vendors are available on the Web at <http://www.novell.com/advantage>.

Press Contacts:

Dawn Harris
Novell, Inc.
Phone: (408) 967-7712
E-mail: daharris@novell.com

Alan Dunton
Porter Novelli Convergence Group
Phone: (415) 538-7547
E-mail: alan.dunton@pnicg.com

Glossary

ConsoleOne - Java-based console management interface for all of Novell's products. ZFS can only be managed through ConsoleOne.

DirXML - Novell product that gives NDS the ability to replicate data to external application data stores and to NDS itself in a filtered fashion. DirXML servers can expose the filtered set of NDS data through LDAP, XML, or any application data format.

DNS - Domain Name Service, name resolution software that lets users or applications locate computers in an IP network or across the Internet.

eDirectory - Novell's latest generation directory service designed to accommodate eBusinesses and the Internet.

Hierarchy - A structure that has a predetermined ordering from high to low with lower objects being identified in relation to higher objects.

HTML - HyperText Markup Language, the document format used on the World Wide Web.

Identity - Identities include all of the information that define an individual's profile. This information at a minimum includes user ID and password. It can be extended to include address and contact information as well as a comprehensive collection of access rights and authorities.

Indexes - In NDS/eDirectory, indexes are lists of all or portions of a directory that are available for high speed lookup or quick access by applications.

Inheritance - Characteristics or relationships passed on by virtue of relationship.

Partition - In NDS/eDirectory, a partition is a segment or portion of the directory that is usually separated and placed on another server. Partitioning enables eDirectory to scale indefinitely.

LDAP - Lightweight Directory Access Protocol, a standards based protocol used to access directory information. LDAP is a simplified version of the DAP protocol, which is used to gain access to X.500 directories. It is easier to code the query in LDAP than in DAP, but LDAP is less comprehensive.

LDIF - Lightweight Data Interchange Format, a standards based format for exchanging information with LDAP based directories.

NDS - Novell Directory Service, the industry's first true directory service introduced in 1993.

Policies - the enforcement of rules and regulations associated with activities, events, and processes. In ZFS, the rules and regulations governing installation, monitoring, and managing of network resources.

Policy Engine - The NDS enabled mechanism that enforces established rules and regulations.

Replica - Replicas are 'copies' of a directory or portions of a directory. Replicas are strategically distributed reduce latency in directory access and lookup.

SSL - Secure Socket Layer is the leading security protocol on the Internet. It enables the establishment of a secure connection between the browser and a Web server through the use of public and secret keys.

XML - Extensible Markup Language, an open standard for describing data and defining data elements on a Web page and business-to-business documents.

XSL - XML Stylesheet Language is a style sheet format for XML documents.