Which directory offers the best LDAP server?

Directory Services

www.novell.com

WHITE PAPER

Novell®

table of contents

Which directory offers
the best LDAP server?

an eBusiNess-ready LDAP directory service

You need an LDAP directory, you really need one, but not just any LDAP directory. You need an enterprise-class, eBusiness-ready LDAP directory service with a rich feature set and superior developer support—and it'd be nice if it ran on your existing platforms…all of your existing platforms.

Novell® NDS® eDirectory™ is that directory.

Featuring a native implementation of LDAP, eDirectory runs on virtually every major commercial platform. It is scalable and secure. You can develop to it with Java™, ActiveX*, C/C++ or scripting interfaces with confidence that your code will conform to the latest standards. And you don't have to write separate applications for all those platforms you currently support.

WHICH DIRECTORY OFFERS THE BEST LDAP SERVER?

NDS eDirectory has been awarded the directory service "Product of the Year" honor by Network Magazine, a leading networking focused publication, marking the third year in a row that an NDS product has taken this prize, but this award is just the latest in the list of industry honors received by NDS products in the last several years from Network Computing, Information Week, Network World and other internationally recognized organizations.

So, if you need a flexible and scalable LDAP directory—and you know you do—when you compare the other directory products, we're sure you'll decide that there is nothing that really competes with NDS eDirectory. But don't take our word for it, look at the competition and compare the features. Actually, we've saved you the trouble and done the comparison for you—all you have to do is read on.

THE LDAP LINEUP

LDAP Rocks! The Lightweight Directory Access Protocol (LDAP) was created by a group of protocol engineers at the University of Michigan as an easy to implement method of accessing X.500 directories over TCP/IP. LDAP has quickly become the de facto directory access standard for Internet-ready user management and e-commerce solutions. LDAP is widely implemented; every major directory supports LDAP, while LDAP clients are ubiquitous (Web browsers, for example). There are even LDAP-only directory servers. Unfortunately, each vendor's LDAP directory provides differing functionality using varying methods.

The X.500 specifications—the industry standard for directories—describe a massively scalable directory service designed to serve in highly distributed environments. These standards define distributed operations, methods of inter-server communication, data management methods, and describe a mechanism for providing secure access to the directory. X.500 was originally developed as a means of creating an international "White Pages" with many independent entities owning their own data, and yet having the totality of the information appear as a unified tree to users. X.500 defines a general-purpose directory design and is easily extensible to allow for ongoing enhancements.

Then there were the network operating system directories; Novell Directory Services®, Banyan* StreetTalk*, NT domains, and, more recently, Active Directory*. Because they have had an easily available user base, many developers have written applications using them and vendors have developed many tools to simplify usage. Consider the number of available products leveraging NDS, or Windows NT* Domains, both of which have been around long enough to build up market share.

We're going to look at a number of directory products; LDAP-only, network operating system, and X.500-based directory services. You will be able to see how the architectural foundation and primary intended function of the directory has influenced the resulting directory service.

iPlanet

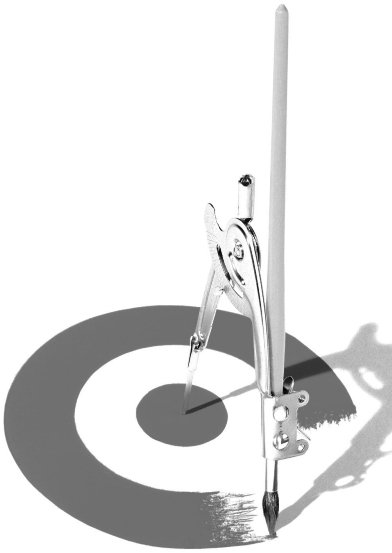
iPlanet* Directory Server is an LDAP-only server designed for user authentication and management in e-commerce, extranet and intranet implementations. iPlanet is the foundation for a suite of e-commerce products delivered by the Sun-Netscape alliance. Sun has recently acquired Innosoft and is incorporating their directory products, including an LDAP proxy server, into the iPlanet line.

Functional aspects

iPlanet was created at Netscape by core members of the team that built the University of Michigan *Standalone LDAP Server* (SLAPD). It is a fully LDAP-compliant directory capable of using its own datastore or plugging into a relational database. The just released version 5 has supposedly undergone a complete re-design to improve scalability, performance and availability.

Scalability—iPlanet v5 claims "virtually unlimited scalability" in press releases, but claims only "over 50 million entries per server" (version 4 supported 50 million objects per server) in its specifications. This version introduces finer-grained partitioning so that the tree may be spread among more servers, hopefully improving scalability as well as performance. iPlanet also provides APIs that enable plugging in a relational database, such as Oracle*, as the data storage system, extending scalability and reliability, but most likely reducing performance.

Replication—iPlanet v5 introduces a multi-master model (actually a dual-master) which is, essentially a primary master and a backup master. Should the primary be unavailable, the secondary takes over. Once the primary is back on line,



its updated by the former secondary then reasserts its primacy. Replication is done via LDAP, and is not automatic—replication agreement must be manually created for each pair of servers that will be involved in replication.

Replication granularity—iPlanet v5 introduces flexible partitioning of the directory tree, allowing sub-trees to be distributed among multiple directory servers. No finer replication filtering capabilities (such as object or attribute replication filters) exist.

Synchronization—Updates are done via changelog files resulting in possible unneeded data being sent during the replication process. For example, if several changes are made to the same object, rather than sending only the net changes, directories using changelog style synchronization will send all of the interim changes as well.

Directory Tools—iPlanet includes limited tools, including a Java administration console that allows delegation of administration only at the host, server, or task level, although v5 does introduce the concept of nested roles to improve delegation. The NT Domain Synchronization tool which was a part of version 4 is no longer available in v5. Netscape Communicator* is not only the primary client for iPlanet, it is also used for LDIF import operations.

Technical aspects

The iPlanet directory server is an LDAP-only directory server that provides a high level of overall performance and manageability. iPlanet support for LDAP v.3 is comprehensive.

X.500 compliance—iPlanet does not support any significant portions of the X.500 standards beyond those mandated by LDAP. iPlanet does not provide automatic server discovery or knowledge reference creation, relying upon manual construction of knowledge references between directory servers.

LDAP support—As iPlanet is an LDAP-only directory server, it provides comprehensive support for LDAP v. 3 including extensions such as virtual list views, persistent search, and server-side sorting.

LDIF—LDIF support for importing and exporting directory information is provided. Version 5 introduces LDIF support for schema modifications.

Security—iPlanet supports LDAP over SSL, X.509 certificates, the FPS-140 cipher suite, and user-defined mechanisms such as Kerberos via the Simple Authentication and Security Layer (SASL). PKCS#11 is supported for hardware accelerated SSL. While there is a certificate management product available as part of the iPlanet product line, it is not free. User authentication is provided through user ID/password, X.509v3 public-key certificates, or administrator-defined method. Version 5 also introduces support for digest MD5 authentication.

DNS Integration/Federation—Support for DNS naming via DC objects (RFC 2247) is introduced in iPlanet version 5. DNS SRV records are not used for directory server location.

Developer Outlook

The iPlanet Developer site includes SDKs and substantial programming resources in the form of documentation, newsgroups, tools, code samples, TechNotes, whitepapers, and iPlanet server downloads.

Interfaces—iPlanet programmatic interfaces include C, Java, JavaScript*, Perl, and HTML via an HTML Gateway. Custom connectors to external data sources can be developed with PerlLDAP.

Software Developer Kit—There are free downloadable Netscape* Directory SDKs for C and Java, as well as Perl LDAP for Solaris* and Windows NT only. Sun has recently announced the availability of a iPlanet Developer Pack and Java 2 Enterprise Edition (J2EE) Component Library (which costs $1295 per developer).

Developer Support—The iPlanet developer community offers support via newsgroups, FAQs, and a newsletter. Although there is no free support, fee-based support is available at a reduced price ($150 v. $300) for community members.

3rd Party—iPlanet is being integrated into an wide variety of business solutions including online wireless, billing, selling, procurement, trading, communication services, and open digital marketplaces.

Business perspective

iPlanet is designed for use outside the corporate firewall as an Internet-based server. With its lack of back-end features, it is most appropriate for Internet directory deployments, but not designed for enterprise network management, or large-scale distributed directory applications.

Market Acceptance—Sun claims 70% of the LDAP-only directory market with 330 million licenses worldwide.

Supported Platforms—Sun* Solaris 2.6 for SPARC, Sun Solaris 8 for SPARC, Hewlett Packard* HP-UX* 11.0, IBM* AIX* 4.3.3 (PowerPC), Microsoft* Windows* NT 4 Server (x86 only), and Microsoft Windows 2000 Server. HP has bundled iPlanet with HP-UX.

Consulting—The Sun/Netscape Alliance provides (for a fee) iPlanet Professional Services to work with your business on all phases of directory-enabling your internet and e-commerce operations, including planning, integration, deployment, and maintenance.

Cost—The list price for iPlanet server is $995 (with 100 client licenses), additional licenses are 10 for $100 ($10 per CAL). You should also consider the cost of ancillary products like the certificate server, and relatively expensive development tools like the J2EE components.

SecureWay

IBM's SecureWay* Directory is an LDAP-only product designed for Internet user management and e-commerce operations. SecureWay directory is a component of many IBM products including WebSphere*, SecureWay On-Demand Server, OS/390*, OS/400*, and AIX.

Functional aspects

SecureWay is an SLAPD-based directory service using IBM's DB/2 database as the data store. It requires the presence of an SSL-enabled Web server on the network. Some basic functionality, such as referrals between directory servers, requires manual configuration.

Scalability—SecureWay is capable of managing up to 4 billion entries in a single tree.

Replication—SecureWay uses a single-master replication model and replication relationships must be manually configured. Only direct replication operations are supported—not cascaded replication (where a replica serves as the source for another replica).

Replication granularity—Selective replication by attribute or subtree is not supported.

Synchronization—SecureWay uses changelog files for synchronization processes.

Directory Tools—SecureWay provides multiple administrative tools, each with a limited scope of functionality. DSA configuration is done via WebAdmin, a Web-based interface, while management of directory information uses a Java-based Directory Management Tool (DMT). SecureWay has multiple LDIF tools that create LDIF files from standard input, translate data to and from relational databases, and perform bulkloading tasks, although bulkload operations require downing the server. Directory administration can be delegated down to the attribute level.

Technical aspects

The SecureWay directory server is an LDAP-only directory server based on SLAPD. While its support for LDAP, LDIF, and the security protocols is comprehensive, it doesn’t provide full X.500 functionality.

X.500 compliance—SecureWay doesn’t implement the X.500 standards beyond those used by LDAP.

LDAP support—LDAP v. 3 is fully supported, as is directory browsing via HTTP.

LDIF—Basic LDIF support for LDIF-based data import, export and bulkload operations is provided.

Security—SASL, Kerberos, CRAM MD-5, GSSAPI, and SSL are supported, although SSL requires installing GSKIT on the SecureWay server. Password authentication can also use SHA, crypt, or imask. Audit logging is supported.

DNS Integration/Federation—IBM provides comprehensive information on configuring DNS service (SRV) records for locating SecureWay servers.

Developer Outlook

SecureWay developer resources are provided in client SDKs and references documenting directory access using popular programming languages.

Interfaces—SecureWay allows programmatic access via C, Java 1.2, JNDI, ODBC, SQL, and browsing via HTTP.

Software Developer Kit—Client and server SDKs in C and JNDI for Windows NT, AIX, Solaris, and HP-UX are available from IBM. Plug-in developer kits allow extension of directory functionality for database-related, auditing, and LDAP operations.

Developer Support—In addition to an online technical database, SecureWay developer support is provided via newsgroups, newsletters, online documentation, as well as support downloads.

3rd Party—IBM has formed partnerships with companies such as Bowstreet, Lucent, Aventail, and RadiantLogic to develop applications that leverage the SecureWay directory.

Business perspective

SecureWay leverages the wide acceptance of LDAP, plus their installed DB/2 customer base, to provide an LDAP directory server on traditional IBM platforms (currently free) as well as most leading competitors.

Market acceptance—While holding no significant market percentage yet, SecureWay partnerships are establishing the foundations leading to an increasing market share.

Supported Platforms—AIX, OS/390, OS/400, Solaris, Windows NT 4 Server, and Windows 2000 Server. A Linux* version is in beta.

Consulting—Consulting support for implementing IBM directory solutions is provided by the IBM Software Services teams, offering comprehensive assistance in planning, design, and deployment.

Cost—IBM provides SecureWay as a no-charge download.

OpenLDAP

OpenLDAP is a collection of open source LDAP components developed as a project of the OpenLDAP Foundation, and based on the University of Michigan's stand-alone LDAP server (SLAPD). OpenLDAP also includes a **SLURPD** stand-alone LDAP replication server, the **LDAPD** LDAP-to-X.500 gateway, utilities, tools, clients, and developer-contributed packages. As a directory product, OpenLDAP has a very high geek factor—if you recompile your operating system kernel for fun, you will probably find it rather amusing.

Functional aspects

OpenLDAP server is provided as source code and must be compiled for the specific installation environment before it is usable. OpenLDAP links to other SLAPD servers via manually configured *referral* entries (akin to X.500 knowledge references). OpenLDAP's no cost software and low hardware requirements make it a good selection if you are forced to deploy a directory service with nominal expenditures.

Replication—OpenLDAP uses single master replication. Replication services for OpenLDAP are provided by the SLURPD stand-alone LDAP replication server which provides replication services via the LDAP protocol to update replicas. SLAPD supports replication to X.500 directories via *LDAPD*, which functions as a gateway to the X.500 DSA. Initial database population can be accomplished via LDAP or via the LDIF2LDBM directory loading tool.

Replication granularity—SLAPD and SLURPD don't allow selective replication.

Synchronization—OpenLDAP can generate replication logfiles, writing the file in a variant of the LDIF format. SLURPD uses these replication logs as a changelog file for synchronization operations.

Directory Tools—OpenLDAP comes with command line tools for viewing the directory database, converting data to LDIF format, importing LDIF, and creating indexes.

Technical aspects

OpenLDAP support for the LDAP standards is version dependent, in that OpenLDAP 1.x doesn't support LDAP v.3 (provided in version 2.0). Likewise, the support for industry standard security protocols is nominal in OpenLDAP 1.x, and only supports all three (SASL, Kerberos, SSL) in version 2.0.

X.500 compliance—Supports only the portions of X.500 that LDAP incorporates, such as the X.500 naming conventions.

LDAP support—OpenLDAP 1.x supports LDAPv2+ (adhering to RFC 1777 with U-Mich extensions). OpenLDAP 2.0 will provide LDAPv3 support. OpenLDAP 1.x doesn't allow changes to the schema via LDAP. Adding new object class definitions or changing existing ones in the slapd.conf or local schema file is how schema changes are accomplished with OpenLDAP.

LDIF—Supports LDIF only for import of directory content.

Security—SLAPD supports MIT's Kerberos 4 for authentication, though it may not be supported by default in the distribution build code and may thus require specific configuration prior to build. In OpenLDAP 2.0, strong authentication is provided via SASL. Linux OpenLDAP packages for RedHat* and TurboLinux* with Kerberos, SSL, SASL support enabled are available. There is a degree of support for TLS/SSL in OpenLDAP 2.0, yet you have to rebuild OpenLDAP specifying TLS support.

DNS Integration/Federation—There is no explicit support for using the DNS namespace in conjunction with OpenLDAP.

Developer Outlook

If you want to help develop a directory server, rather than applications for a directory server, OpenLDAP is a likely playground for you. Developers working on the OpenLDAP project contribute functionality beyond that provided in the base set. If, however, you need to develop enterprise-class applications that use a directory service, it may not be the best choice.

Interfaces—SLAPD communicates between its frontend LDAP services and backend database management via a well-defined C API, allowing for flexible SLAPD extensions. Members of the OpenLDAP developers community have contributed other interfaces such as TCL scripting.

Software Developer Kit—OpenLDAP includes an LDAP Software Development Kit(SDK). A number of programmable database modules are provided, allowing developers to integrate external data sources via common programming languages such as PERL, Shell, SQL, and TCL.

Developer Support—There is a community of developers who work on the OpenLDAP project, developing a range of functionality within the OpenLDAP product.

3rd Party—While there is an ever-growing group of applications which can talk to any LDAP server, there are no known applications built specifically for the OpenLDAP directory server product.

Business perspective

The free OpenLDAP directory server is advantageous to universities, students, researchers, and users needing an LDAP server to develop to, yet for most companies it doesn't present a viable off-the-shelf directory solution.

Market acceptance—Nominal—used at the University of Michigan, but there is no visible commercial market penetration.

Supported Platforms—Source code is available for the BeOS, Compaq* (Digital) UNIX* (OSF/1), Data General DGuX, FreeBSD, Hewlett Packard HP-UX, IBM AIX, Linux, Microsoft Windows (NT/98/95), OpenBSD, Silicon Graphics IRIX, Sun Microsystems Solaris, and Sun Microsystems SunOS. Packaged versions of OpenLDAP are available for Debian GNU/Linux, FreeBSD, NetBSD, and Red Hat Linux.

Consulting—The OpenLDAP site has a job board for people who have worked with OpenLDAP to advertise their consulting and technical services.

Cost—OpenLDAP is available for free.

Active Directory

Active Directory (AD), Microsoft's initial foray into the directory service market is still in its first revision. Active Directory is a hybrid of the NT 4 domain model, DNS, and LDAP with multiple proprietary aspects. If you are familiar with eDirectory (or other X.500-based directory services), you will note substantial differences in the AD design and operations.

Functional aspects

The complexity of Active Directory deserves special mention, and requires just a bit of explanation. Microsoft chose to maintain the older NT domain model directly in AD, and integrated it with the DNS location service functionality. An NT domain maps to a DNS domain, meaning the top level of the AD tree must be congruent with the DNS domain hierarchy. To allow for more than one DNS domain hierarchy, Microsoft created a top level container called the *forest* that provides multi-tree functionality, but also presents operational constrictions, contingencies, and issues.

The choice to support the old NT domain architecture creates some interesting limitations—the domain boundary is the only point of partitioning the DIB and is a security boundary for administrative rights. This lack of flexibility can make it difficult to design and administer AD the way that you want to.

In addition, Active Directory has two operating modes which supply different levels of functionality:

- **Mixed-mode**—AD *must* operate in mixed-mode while there are *any* down-level Domain Controllers (DC) on the network. AD has limitations in mixed-mode, some groups are not available limiting security functionality and complicating administration. Microsoft has created new groups to facilitate network management, but they are not available while AD is operating in mixed-mode. Nested groups, another feature designed to streamline security administration are also prohibited in mixed-mode.
- **Native-mode**—When only Windows 2000 domain controllers (DC) are present on the network, native-mode can be employed providing access to all AD functionality. This state, however, is not likely to be attained by most enterprises soon after AD deployment, as there will be many NT 4 DCs on the

network. Once AD has been switched to native-mode, there is no going back to mixed-mode and no backward compatibility for NT 4 DCs.

Scalability—Active Directory is capable of supporting multiple trees each containing millions of objects.

Replication—While Active Directory does provide multi-master replication, partitioning and replica assignment in AD is inflexible. Partitions are created automatically on domain boundaries and cannot be created anywhere else. A DC *must* hold a replica and can only hold *one* replica: a replica of the domain of which it is a member.

Replication granularity—AD has no filtered replication capabilities.

Synchronization—AD doesn't employ X.500 replication, but rather uses proprietary synchronization routines based on sites (a technology derived from their Exchange mail application) requiring site configuration and management. Certain synchronization issues arise with Microsoft's use of multi-valued attributes to identify group membership, resulting in possible update conflicts and loss of group update information.

Directory Tools—Most AD management is done via the Microsoft Management Console (MMC), which uses snap-in modules to provide administrative access in Windows 2000. The MMC, however, does not supply integrated AD management, as many snap-ins are needed just to manage the directory itself. Some additional Active Directory tools are provided, such as the Active Directory Migration Tool. There are also tools available via secondary products such as the Microsoft Windows 2000 Server Resource Kit.

Technical aspects

Active Directory's support for LDAP v.2 and v.3 supplies an industry standard access methodology to the directory service repository and operations. Active Directory supports a range of programming interfaces and developer tools, and much of the programming information and some tools are provided for free.

X.500 compliance—Active Directory doesn't adhere to X.500 standard beyond that which is required for LDAP support, deviating from the standards for things like naming, security, and DIB management. Object names must be unique within the entire domain, not just the OU, complicating user management. OUs are not security principals in AD, preventing administration and security by OU and requiring that access control be managed via groups thus complicating administration, especially with large and dynamic directories. Additionally, locking partition boundaries to domains hinders DIB management.

LDAP support—AD fully supports LDAP v.3 but AD design presents some limitations for LDAP functionality. LDAP is unaware of the AD concept of forests and thus, for example, searches can't traverse the forest and are limited to a single AD tree.

LDIF support—AD can use LDIF for importing and exporting directory data as well as performing schema updates.

Security—Active Directory does provide support for SSL/PCT, SASL, and X.509 PK certificate management, and uses Kerberos for authentication, yet lack of interoperability between different vendor's Kerberos and PKI implementations are ongoing issues. Microsoft implements Kerberos using a proprietary Privilege Access Certificate in its Kerberos tickets, preventing interoperability with other vendors adhering to the Kerberos 5 standard. In addition, in Active Directory there is a lack of tree-wide delegation of administrative rights, and no dynamic rights inheritance.

DNS Integration/Federation—AD relies on DNS as its location service and uses DNS SRV records to support this functionality. AD requires that the top of the AD tree be congruent with a DNS domain. While the DNS support is nice, the dependency on DNS can also be problematic:

- Even small businesses must set up DNS services in order to use Active Directory, and if DNS is not configured perfectly, AD will not install or function correctly.
- The DNS servers on the network must support Dynamic DNS (DDNS), and AD has complicated DNS records beyond readability, making DNS support labrythine and problematic.

Additionally, Active Directory servers configured with more than 51 IP address will fail, preventing management of users and access to resources.

Developer Outlook

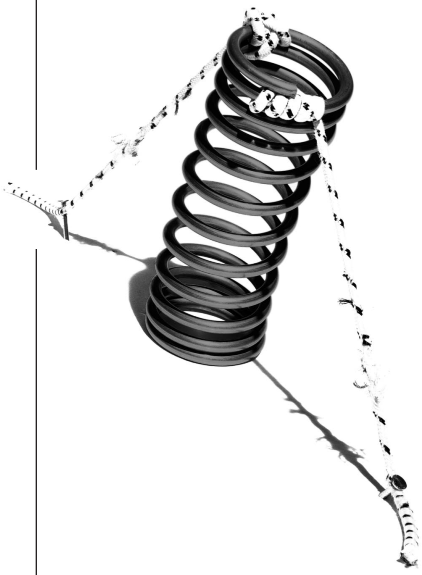
Microsoft provides a robust development environment, supplying lots of developer tools for the Windows environment, yet Microsoft's development environment is shifting to their new .NET paradigm, changing the development languages and tools, and focusing on the development of all Windows applications as Web services. This fundamental shift from their traditional Win32 environment leaves developers uncertain about the future of application development for the Windows platform.

Technical issues also add complexity to application development. For example, the AD restrictions on security principals mean that, since applications can not be granted access rights directly, a User account must be created for the application. This creates an additional layer of administration and complicates the process of directory-enabling applications.

Interfaces—Active Directory Service Interfaces (ADSI) is a set of COM interfaces which use an LDAP provider to talk to Active Directory. The MAPI interface is also supported for application compatibility, as is the Security Account Manager (SAM) API for down-level NT DCs and clients. Additionally, support is provided for Visual Basic, Perl, JavaScript, WSH environment, and the LDAP C API.

Software Developer Kit—Microsoft recommends developing for Active Directory using the ADSI SDK, and also provides directory access in their development language products.

Developer Support—Microsoft provides detailed information resources via the Microsoft Developer Network, TechNet, as well as extensive online access to development information and tools.



3rd Party—Products designed to take advantage of Active Directory are just starting to ship and this will probably help boost the overall adoption rate. While thousands of applications will probably run on Windows 2000 eventually, at this point fewer than 70 applications have been certified for Windows 2000 from a total of 45 vendors.

Business perspective

Microsoft's Active Directory is specifically designed as to enhance and extend the management and functionality of existing NT networks in an enterprise environment. For enterprises vested in Windows NT networks and clients, Active Directory allows corporate IT to enhance network functionality, ease NT domain management, and improve user access to network resources. Active Directory is not a generic LDAP directory server, nor is it optimized to provide LDAP services in an e-commerce environment. Its focus is on inside-the-firewall Windows network service provisioning, user management, and corporate network resource control.

Market acceptance—Due to the inherent complexity of migrating existing NT networks to Active Directory, market acceptance of Active Directory has been somewhat slow. In the year after release of Windows 2000, research from IDC reflects that only about one-third of the shipped copies of Windows NT and 2000 combined were Windows 2000 (and most of those were Windows 2000 Professional), indicating a slow adoption rate of Windows 2000 Server and Active Directory. According to Gartner Group "only about 3% of the NT server installed base was converted to Win 2000 last year", and a Giga survey found that for companies who have installed Windows 2000 Server "…only 10 percent to 15 percent of those have used Active Directory".

Supported Platforms—Active Directory runs only on the Windows 2000 Server platform, and client platforms are limited to Windows-based clients. This single-platform approach to a directory service limits it applicability to heterogeneous enterprise networks, and restricts the flexibility of networks centered on Active Directory.

Consulting—Microsoft Consulting Services does provide extensive Active Directory support, and while there are many 3rd Party consultants familiar with Windows NT and 2000, fewer have extensive experience with planning, designing, and implementing Active Directory.

Cost—Active Directory is only available as part of Windows 2000 Server, thus every AD server requires a copy of Windows 2000 Server costing $1199 ($3999 for Advance Server) with 10 user licenses and $40 per additional CAL. Yet because an AD server can only hold a single replica, every replica requires its own standalone server (as opposed to, say, eDirectory which allows 250 replicas per server).

Critical Path InJoin and LiveContent DIRECTORY

LiveContent DIRECTORY was created by PeerLogic, which was recently acquired by Critical Path who also makes the InJoin* (formerly called *Global Directory Server*) directory service product. Critical Path is incorporating LiveContent into its InJoin directory product line.

Note: Because these products are so similar, and from the same vendor, we are evaluating them together. In the few instances where they are not functionally identical, the differences are noted.

Functional aspects

Both InJoin and LiveContent supply scalable X.500 distributed directory operations, and while they use different replication and synchronization methods, they provide equivalent degrees of directory functionality. While they are both powerful directory service implementations, complexity is a factor.

Scalability—InJoin and LiveContent are both highly scalable directory products capable of maintaining 20 million directory entries per DSA with sustained access rates of 100 reads per second for read and search operations.

Replication—Both directories support X.500-based single-master replication via primary and secondary shadowing mechanisms, but do not support multi-master replication. Shadow relationships are manually established via administration tools.

Replication granularity—The replication mechanisms support filtering down to the attribute level.

Synchronization—These products differ in their approach to synchronization of directory content.

- **LiveContent Synchronization**—Automatic synchronization is supplied via modification log (i.e. change logs), and synchronization APIs are also supported.
- **InJoin Synchronization**—Synchronization is performed in a transactional two-phase commit process that allows roll-back/ roll-forward of directory changes.

Directory Tools—Each of these directory services provide their own set of tools for administration and interoperability.

- **LiveContent Tools**—Administration tools include Directory Administration Center (DAC), essentially a Windows NT only DUA that uses a standard Winsock interface. DAC allows administration of local and remote DSAs. The DAC environment also supports X/Open's XDS & XOM APIs. Platform-neutral, single point of administration is supported via iCon, a Web browser based administration tool. LiveContent DIRECTORY includes a command-line scripting language for import of schema and content.
- **InJoin Tools**—Directory Navigator is InJoin's management console providing centralized administration of the directory. Single point of administration capability is also supported via browser client.

Technical aspects

These directories are fully X.500-compliant directory services, supporting standards and operations as delineated in the 1993 X.500 specifications, as well as the LDAP v.3 standards.

X.500 compliance—InJoin and LiveContent fully adhere to the 1993 X.500 standards supporting all the administrative, information, functional, security, and DSA models as well as X.500

protocols including DAP, DSP, and DISP.

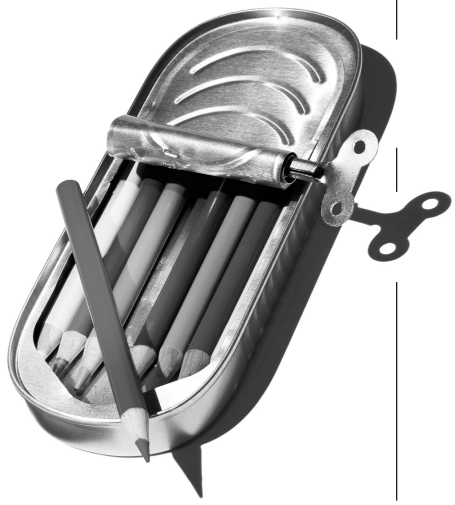
All X.500 functionality is provided, including such useful features as chaining and referral mechanisms for query resolution, dynamic schema configuration, subtree pruning and grafting, and collective attributes.

LDAP support—Both InJoin and LiveContent fully support LDAP v.3 including all standard LDAP operations, and they provide support for LDAP v3 process handling including paged results for LDAP queries, debugging, tracing, logging, alerts, and statistics.

LDIF—InJoin and LiveContent support the import and export of directory schema and content information via LDIF.

Security—Security in both of these directory services is implemented in adherence with the X.500 standards, supplying hierarchical delegation of security administration, access control, and configurable strong authentication. SASL and X.509 security mechanisms are provided.

- **LiveContent Security**—TLS and SSL security are supported via the LiveContent DIRECTORY TLS Adaptor API. LiveContent DIRECTORY also supports a proprietary Crypto Adaptor API (via proprietary LiveContent DIRECTORY API) which operates as a security module handler.
- **InJoin Security**—InJoin Directory provides comprehensive directory-wide user access controls, and native support for SSL/TLS and data encryption. Note: SSL is supported only on Windows NT 4 and Sun Solaris 2.6.



DNS Integration/Federation—The DNS namespace and functions are not included nor integrated into either InJoin directory, nor the LiveContent DIRECTORY product or operations.

Developer Outlook

Administration tools for these products supply the needed ability to manage the distributed set of directory servers, and support the import and export of directory content.

Interfaces

Both LiveContent and InJoin natively support DAP and LDAP user agents (with full v.2 and v.3 APIs), and directory client access via HTTP to Netscape Navigator and Microsoft Internet Explorer browsers.

- **LiveContent Interfaces**—Supported API's include the LDAP C API, X/Open Directory Services (XDS), and a LiveContent DIRECTORY Proprietary API. The XDS implementation includes support for the X/Open OSI-Abstract-Data Manipulation (XOM) API, as well as X/Open specified packages Basic Directory Contents Package and MHS Directory User Package. iGateway, an integrated gateway product exposes a backend ODBC interface for integration of SQL-based datasets.
- **InJoin Interfaces**—Provides support for X.500 standard protocols, as well as LDAP and HTTP.

Software Developer Kit—Only limited development tools are directly provided, with Critical Path pointing to LDAP interface kits by other vendors to supply language-specific development support.

- **LiveContent**—The iGateway add-on has a developer toolkit, the LiveContent Directory Db Adapter (ODBC) API, for creating other ODBC interfaces. LiveContent documentation notes the availability of LDAP interface toolkits for a number of development environments including LDAP for ActiveX, LDAP via PERL, and LDAP Java class libraries.
- **InJoin**—InJoin has a range of application tools available—TRANS supports hosting CICS, COBOL, PL/1, VSAM , and DB2 applications on Unix or NT, Path3270 allows a developer to use any Java IDE to connect with, and integrate legacy mainframe applications, BROKER which integrates information across multiple platforms, and BATCH which provides batch management on Unix or NT.

Developer Support—Online developer resources aren't available for either LiveContent or InJoin directory products.

3rd Party—Online Critical Path references don't describe any 3rd party applications developed specifically for LiveContent or InJoin.

Business perspective

Both InJoin and LiveContent have the flexibility and scalability of true X.500-based directory services, and as such can well support a wide range of business and IT operations.

Market Acceptance—Both of there products are deployed in large-scale messaging environments, including a wide range of businesses, as well as the European postal, financial, and government environments. Critical Path customers encompass a broad spectrum of industry and technology leaders, including IBM, Cisco, Intel, Lucent, AOL, AT&T, HP, EDS, and many others.

Supported Platforms—the range of supported platforms is one of the more striking differences between these two directory service implementations.

- **LiveContent** —Sun Solaris 2.6, 2.7, HP UX 10.20, 11, Windows NT 4. According to PeerLogic/Critical Path, LiveContent is available on other UNIX platforms on request.
- **InJoin**—InJoin Directory Server is available for Windows NT 4/2000 (Intel*), Sun Solaris 2.6, HP/UX 11, AIX 4.3, SGI IRIX 6.5.

Consulting services—As part of the array of integrated directory solutions, Critical Path offers its InTouch services providing consultants to assist in requirements analysis, integration planning, as well as designing and deploying directory infrastructures with ongoing support.

Cost—Pricing information per server and per client for each of these directory services is not readily available from Critical Path's product information, yet a recent networking magazine review cited the client access license cost at $100,000 per 100,000 users (or $1 per CAL).

eTrust/OpenDirectory

The eTrust Directory from Computer Associates (CA) is an X.500-based distributed directory service providing a robust, extensible, and scalable solution supporting high levels of concurrent users. The eTrust Directory is a component of the eTrust suite, an integrated collection of infrastructure security and management products.

Functional aspects

ETrust is fully X.500 compliant. It uses CA's Ingres RDBMS as the backend data store providing flexible and reliable directory storage and retrieval. eTrust supports load balancing, query streaming, and can also serve as a router for proxies and firewall applications. eTrust can run multiple DSAs on the same server—essentially multiple instances of the directory server—increasing the number of concurrent users supported per server.

Scalability—eTrust Directory employs a fully distributed directory information base, supporting tens of millions of directory entries with millisecond response times. eTrust employs a fully-indexed directory database to provide extremely high performance and achieves linear scalability via increase in disk storage and processor expansion.

Replication—Uses single-master replication based on the X.525 primary and secondary shadowing mechanisms. Shadow relationships are manually established.

Replication Granularity—Attribute level replication filtering is supported.

Synchronization—The DXreplicator mechanism uses a transactional two-phase commit process with checkpoints and rollback functionality. The DXserver DSA supports 'multiwrite' operations which allows all DSAs in a naming context to be dynamically synchronized while maintaining real-time directory operations.

Directory Tools—eTrust supplies a lightweight DUA called DXplorer that supports import/export of schema, as well as database content loading, dumping, replication, and archiving. Any external LDAP server can be integrated into eTrust Directory via DXlink. Tools for scripting of directory operations, and synchronizing of external data are included in DXtools. eTrust Directory integrates with the Unicenter TNG for enterprise network administration, and PKI certificate validation is supported by eTrust OCSPro.

Technical aspects

eTrust provides a fully distributed X.500 directory service, allowing dynamic schema updates and extensions, modifications to access controls, knowledge references, and tracing configurations. eTrust also supports dynamic directory configuration and control, allowing online backups and hot swapping of databases.

X.500 compliance—eTrust has full X.500 compliance, supporting all functional, DSA, authority, and information models, as well as the X.500 protocols including DAP, DSP, and DISP. It also supports query chaining and referral. DXserver stores comprehensive knowledge references to all DSAs in the directory allowing shortest path routing of directory queries.

LDAP support—eTrust fully supports LDAP v.3 including extensions such as virtual list views, persistent search, and server-side sorting. eTrust uses DXLink to incorporate LDAP servers into the directory.

LDIF—eTrust Directory does support import/export of schema, as well as database content loading, dumping, replication, and archiving via Java-based DXplorer tool.

Security—eTrust enforces access controls on all directory entries, and fully supports rule-based access controls and rights inheritance. X.509 PKI certificates from VeriSign, Entrust, and Baltimore Tech can be used for strong authentication. Kerberos, SASL, and SSL are supported, as well as X.700 and SNMP monitoring for logging, tracing, and alarms.

DNS Integration/Federation—Support for DNS integration and namespace federation is not specified.

Developer Outlook

CA supplies useful eTrust directory management and LDAP synchronization tools, yet offers limited developer information for the eTrust directory product.

Interfaces—eTrust documentation lacks specified development interface information.

Developer Support—eTrust provides schema and communications support for a range of directory-enabled applications (via LDAP), including DEN, CTI/IVR, HR, Security, Postal, as well as support for document management, catalog, government, and financial services. While CA supplies a set of integrated eTrust applications, little data is available for external developer information and APIs.

Software Developer Kit—CA does not appear to provide any SDK for the eTrust Directory.

3rd Party—While CA has an impressive array of development partners, they don't reference any 3rd party applications specifically for eTrust.

Business perspective

eTrust is a suite of services integrated with the eTrust Directory, providing a robust, extensible, and massively scalable enterprise identity management or e-commerce solution. eTrust Directory can integrate LDAP services from multiple vendors (Active Directory, iPlanet, NDS, any LDAP-compliant directory) into a unified directory service without gateways or metadirectory components.

Market acceptance—eTrust Directory has limited but significant market presence, mostly in large-scale government or enterprise environments.

Supported Platforms—eTrust runs only on Microsoft Windows NT and Windows 2000, as well as Sun Solaris 2.6, 2.7, and 2.8.

Consulting—CA provides consulting services supporting all aspects of business solution implementation with CA products, supplying value-added planning, integration, deployment, and ongoing support.

Cost—While the server price is not available, a recent networking magazine review placed the client access license cost at $20,000 for 100,000 users (or $.20 per CAL).

THE eDIRECTORY ADVANTAGE

We have looked at three styles of directories, three sets of strengths and weaknesses. Time for a quick recap.

LDAP is great for clients and directories to talk to each other. However, LDAP specifies only a *directory access method*, and a directory service is a lot more than an access method.

LDAP, being an access protocol, doesn't define the X.500 distributed directory mechanisms. That makes sense, as LDAP was designed to access *X.500* directories and it relied on the underlying directory for that functionality.

X.500 is the foundation for high performance, massively scalable, and highly distributed directory services. Due to the focus of X.500, these directories have typically been associated with the same sorts of companies you think of when you think of mainframes. Until LDAP came along, X.500-ready clients weren't everywhere, and since they lacked the relatively captive user base of network-focused directories, development for them wasn't *quite* as impressive.

Network-focused directories are easier to use and have more application support. What most network directory services have lacked, however, is the massive scalability of X.500 and the universal clients of LDAP. Again, this makes sense; they weren't designed to be distributed across the world like X.500 and, as they were tied to a specific network operating system, the client architecture could be limited to a relevant subset.

So where does NDS eDirectory fit? It's the best of all of these.

eDirectory is a time-tested, cross platform, enterprise-ready directory service grounded in X.500 with native LDAP support, providing you with a secure foundation for your internet, intranet, and e-commerce applications. Moreover, because it has been around as an enterprise network directory service since 1993, NDS has had time to mature and build a base of products that leverage it. There are over 1800 applications and 139 million users who rely on NDS eDirectory every day. In fact, according to the International Data Corporation (IDC), eighty percent of Fortune 1000 companies using a directory service are using NDS!

eDirectory technology is the foundation for enterprise management, security, e-commerce, collaboration and Internet solutions from Novell.

Technology mileposts

NDS eDirectory has undergone numerous changes since Novell introduced it in 1992. Let's take a quick look at some of the significant LDAP-related mileposts on the way to eDirectory 8.5.

NetWare 4—LDAP Services for NDS released as a free add-on product for NDS in 1997.

NetWare 5—LDAP Services for NDS integrated into base NDS product.

NDS eDirectory 8.0—Improvements in LDAP search performance, DNS namespace support, and caching and indexing enhancements.

NDS eDirectory 8.5—Released as stand-alone product for Windows NT/2000, Linux, Solaris, and Tru64 UNIX with DirXML™ support on all platforms. Substantial LDAP enhancements—full version 3 support for auxiliary classes, schema updates via LDAP and LDIF, ICE (Import/Convert/Export) LDIF utility, and support for LDAP over SSL. Filtered replication also introduced.

Functional advantages

eDirectory is rooted in the X.500 design for massively scalable directory services, giving it powerful, yet manageable, distributed capabilities. Native LDAP support is also provided along with other critical Internet standards like XML, making it easy to access with ubiquitous clients. eDirectory's time in the network field shows too; with easily managed operations, automatic configuration of many inter-server processes, and mature integrated tools. As you will see, eDirectory leverages this best-of-breed design and operations to its advantage, and yours.

Scalability—Novell has publicly demonstrated that eDirectory can manage more than a billion objects in a single tree. This capability far exceeds what most enterprise networks or eBusinesses will require.

LDAP Performance—eDirectory 8.5 has substantially improved LDAP performance, with automatic optimization of caching and indexing; its improved so much that LDAP catalogs are no longer needed. LDAP searches perform with consistent speed, even with millions of objects in the directory. The LDAP search capabilities of competing directories generally decrease in direct proportion to the number of users added to the directory. Key Labs, an independent consulting firm, tested eDirectory against iPlanet and found that LDAP searches were up to 50% faster on eDirectory.

Replication—eDirectory provides powerful and easy to administer multi-master replication. Replica placement and management is highly flexible—eDirectory allows 50 replicas of a partition and 250 replicas per server. Automatic replication processes ensure performance and fault tolerance, while robust customization abilities allow you to place replicas where you need them. While eDirectory uses multi-master replication by default, it also allows single-master style replication with read-only replicas. Read-only replicas operate as a shadow in a master-shadow relationship and provide a means of distributing copies of the directory for look-ups.

Replication granularity—Many times, you only need a sub-set of directory information for your application. If, for example, you only need the business-related address book portion of a User object, why replicate the entire object? By filtering directory replication, you can create a replica that just contains the address book information. You can create replication filters at the object or attribute level for either inbound or outbound replication, facilitating the creation of custom views of the directory. Because they create very small replicas and keep synchronized data to a minimum, filters allow much larger replication rings (over 100 servers) supporting large-scale Internet or e-commerce deployments. You enjoy greater flexibility in directory deployment along with improved network and directory performance.

Synchronization—eDirectory uses *transitive synchronization*, a powerful method of updating replicas that reduces network traffic and server load while maintaining data integrity. eDirectory servers act as intermediaries to other eDirectory servers in a sort of cascaded replication to perform synchronization operations more efficiently, and across disparate network protocols—IPX to TCP/IP, for example. Prioritized synchronization ensures that critical updates, like security and password

changes, are replicated quickly (in 10 seconds), while most directory changes are scheduled to occur on a regular, but much less frequent basis.

Referential integrity—Referential integrity ensures that when you attempt to change data, all related and dependent objects are confirmed in those changes which are not propagated out to other datastores until ythe references are checked.

Partitioning—No limits on partition size means you can design your directory based solely on what works best in your environment. A single container can hold millions of objects, giving you plenty of space to easily manage those massive trees. There's also no need to manually tell one directory server where another is, as there is with many other directory products—eDirectory creates the references needed for inter-server operation automatically as you partition the directory. Directory information is stored efficiently as well; an eDirectory partition holding a million objects will only take about one GB of disk space.

Directory Tools—eDirectory has a broad range of tools that provide powerful means of simplify directory management.

- *ConsoleOne*™ provides a platform independent unified interface for administering eDirectory, including directory information, servers, and LDAP components.
- *iMonitor* is a browser based monitoring and diagnostics tool lets you keep an eye on all of your eDirectory servers from anywhere on the network.
- The *Import/Convert/Export* (ICE) utility provides a mechanism for moving large amounts of directory information between NDS and LDAP, or between LDAP directories, via LDIF files. ICE uses the same XML rules as DirXML for creation, and placement of objects as well as schema mapping. You can use XML rules to perform tasks such as providing default values when creating objects or mapping schema elements.
- Traditional LDAP utilities like ldapsearch, ldapmodify, ldapdelete are included.

Technical advantages

eDirectory blends the architecture of X.500 and the ubiquitous nature of LDAP with robust security services to provide the technical foundation for a global directory service ready for any mission-critical task.

Best Combination of X.500 and LDAP—NDS eDirectory is grounded in X.500, the industry standard for a high-performance, scalable, and secure directory service. It incorporates the X.500 architecture for distributed operations and administration with a powerful data storage system to provide a world-class directory service. Soon, eDirectory will be able to communicate with X.500 directories via the standard X.500 protocols as Novell and Nexor are partnering to build DirXML connectors to X.500 directory services.

eDirectory fully implements LDAP version 3 as well as popular extensions and controls allowing advanced query handling such as virtual list view (VLV) and server-side sorting of search results that makes browsing containers containing millions of objects easier. LDAP extensions and controls can also be used to create utilities for managing partitions and replicas. A DirXML connector for iPlanet is available, providing changelog style synchronization—unfortunately since changelogs aren't standardized, this connector is limited to iPlanet at this time.

LDIF—eDirectory uses an extended set of LDIF codes, providing a way to update access rights, define attributes to index, change schema definitions, and configure NDS-LDAP mappings using LDIF files. eDirectory's LDIF utility provides a mechanism for importing and exporting directory information and performing migrations from server-to-server.

Security—eDirectory supports flexible user authentication methods ranging from passwords encrypted over SSL to X.509v3 certificates or security tokens, such as smart cards. eDirectory supports LDAP over SSL for secure connections (especially important if clients are using clear-text passwords) to the directory on all platforms. Novell Certificate Server™, available free from Novell, integrates with eDirectory to provide and manage PKI certificates. SASL is supported, allowing authentication mechanisms such as Kerberos for LDAP. eDirectory provides access control and delegated administrative rights down to the attribute level.

Novell Modular Authentication Service (NMAS™) 2.0 supports extensions to security mechanisms to support authentication using biometric devices, tokens such as smartcards, and passwords. NMAS can provide differential access based on how a user authenticated to the network. Someone with just a password can be allowed to get to their e-mail, for example, while the directory requires a security token to get to financial records.

DNS Integration/Federation—eDirectory now integrates DNS functionality to provide support for world-wide NDS referrals via DNS. eDirectory trees can be created within the corporate DNS domain structure and DNS used as the location service for these trees, facilitating distributed business across the Internet. When a directory server receives a request for an object within another DNS domain, it uses DNS to locate the other eDirectory server and continues directory operations transparently.

Developer advantages

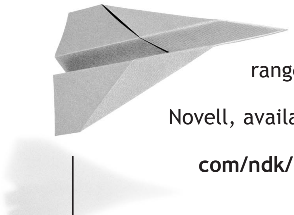
Novell believes that eDirectory can provide critical functionality to your application, and they'd like to help you access it. That's why they provide comprehensive tools and support to developers including an array of offerings supporting core internet technologies like LDAP, Java, and XML, as well as the old standards like C/C++.

Interfaces—In addition to the LDAP C API, eDirectory supports a variety of programmatic and administrative access methods. You can choose between the traditional DSAPI (Novell's port of the X.500 XDS APIs), ADSI (Active Directory Services Interface), and LDAP interfaces. You can write eDirectory applications using C/C++, Java, ActiveX controls, JavaBeans components, JNDI/JNCL, as well as ODBC and JDBC queries. Supported scripting languages include JavaScript, Perl, and Net Basic.

XML-based access to eDirectory information is provided via Directory XML (DirXML), which also supports XSL and XSLT. In the interest of helping set a standard for XML-based access to directories, Novell has offered the DirXML specification to

OASIS for adoption as the open standard for the Directory Services Markup Language (DSML) 2.0.

Novell Developer Kit—Novell provides a wide range of no-charge downloadable software development kits and libraries. Here's just a sampling; NDS libraries for C and Java, NDS Authentication services, LDAP Libraries for C and Java, and eCommerce LDAP Beans. JNDI support, including class libraries, providers, extensions, and controls are available, as are a DirXML driver kit, and Single Sign-on for C and Java. There is even a toolkit for creating utilities that managing partitions and replicas through LDAP extensions and controls. You can check out the full range of developer downloads from Novell, available at **http://developer.novell.com/ndk/downloadaz.htm**.



Bundled eDirectory for ISVs—Novell has created a version of eDirectory that can be bundled with your application providing customers without an installed directory service the benefit of a directory-enabled solution. If multiple applications, each with their own copy of eDirectory, exist on the same network, they can even share a single installation of eDirectory eliminating the need to support multiple stand-alone application-specific directory services.

DeveloperNet®—DeveloperNet includes comprehensive development tools, technical information, developer support, advanced training, and co-marketing programs. DeveloperNet makes it easier for you to deliver secure, scalable directory-ready solutions in areas like e-commerce or customer relationship management. Industry-leading companies like IBM, Sun Microsystems, Lucent, and Oracle have signed on as DeveloperNet partners and the program has over 100,000 members world-wide. There are multiple levels of DeveloperNet membership available:

- The **Net** membership is free and provides free online access to the Novell Developer Kit, Developer Support Forums, AppNotes, Novell Support Connection, and the DeveloperNet University.
- At the **NetPlus** level, you get all of the above, plus the latest release of NDS eDirectory, a one-year subscription to the Novell Developer Kit, and two 25-user copies of NetWare 5.1
- **NetProfessional** level membership offers Novell Software Evaluation Library™ (SEL), with 100-user versions of many Novell products, annual NDK and AppNotes subscriptions, two developer support incidents, four shipments of the Novell Support Connection, and Metrowerks CodeWarrior for Windows, Professional Edition.
- **Executive** and **Strategic** memberships are available for strategic development partners and large enterprises that require unlimited compatibility testing and a high level of support.

Developer Support—Novell's Worldwide Developer Support offers services for hardware and software developers as well as compatibility testing services.

- **Software and International Developer Support**: Provides support on the NDK and application compatibility for the US, hardware and software developers in Europe, as well as DeveloperNet, software, partnerships, and 3rd party support for the Asia Pacific region.

- **Developer Solutions Team**: This team works on NDS integration for both hardware and software, including in lab testing support in Provo, San Jose, Boston, and Taiwan This team provides on-site developer support and liaison services for selected partners.
- **Hardware Developer Support Team**: Systems support group works with major hardware vendors such as Intel, Dell, Compaq, and Hewlett-Packard to provide developer support and deal with compatibility issues. The Device Drivers and Printing (DDAP) group supports Novell partners working with a variety of infrastructure hardware. This team also handles hardware testing, including the creation of testing tools for developer and Yes certification testing.
- **Developer Labs**: Novell has four developer labs, located in Provo, San Jose, Boston and Taiwan, available for use in development and testing of your eDirectory-enabled solutions. Novell's Developer Lab can speed your development process to get products to market faster. These labs offer access to the complete array of Novell software deployed on a network that includes both LAN and WAN topology. You'll also benefit from the expertise of top Novell engineering talent available to help you—each lab has two senior engineers to assist you as you test the deployment, migration, and operations of your products. Novell staff will even negotiate non-disclosure agreements for the engineers you will be working with, so you can rest assured that your work at Novell Labs stays secret until *you* want to talk about it.
- **Certification**: Once you are done at the Developer Lab, your product should be ready to submit to the certification lab. Here, your application will be evaluated to see if it gets the Novell Yes Tested and Approved mark that certifies application compatibility with Novell Net Services software.

Novell Solutions Search—Once you have developed your product, you need to tell the world about it. Well, Novell has a way to help with that part of the product development process too: Novell Solutions Search(NSS), a free service available to Novell Partners and DeveloperNet subscribers. NSS provides a searchable database of the myriad of software, hardware, and professional services available for Novell products. The information in NSS is refreshed periodically to maintain high quality listings.

By registering your product with NSS you gain access to the tens of thousands of people a day who visit Novell's site looking for technology solutions. Registration is simple, you can do it quickly via a convenient online form. If Novell has certified the product, the Yes Tested and Approved mark appears next to your NSS listing, letting potential customers know that your solution is compatible with Novell products. (Hardware products *must* be certified by Novell to be included in the NSS database.)

All the information you need about NSS is available at **http://developer.novell.com/nss/**.

3rd Party Business Solution Offerings—Hundreds of independent vendors have developed a wide range of NDS eDirectory-based solutions for business operations, and e-commerce applications—

too many to list here! But if you browse to **http://www.novell.com/partners/corporate/current.html**, you can see the company you'll be keeping when you develop to NDS eDirectory.

Tools—eDirectory has a broad range of tools that provide powerful means of simplify directory management.

- *iMonitor* is a browser based monitoring and diagnostics tool lets you keep an eye on all of your eDirectory servers from anywhere on the network.
- *ConsoleOne* provides a platform independent unified interface for administering both eDirectory and its LDAP components.
- The *Import/Convert/Export* (ICE) utility provides a mechanism for moving large amounts of directory information between NDS and LDAP, or between LDAP directories, via LDIF files. ICE uses the same XML rules as DirXML for creation, and placement of objects as well as schema mapping. You can use XML rules to perform tasks such as providing default values when creating objects or mapping schema elements.

Time to market advantages—As a developer, using eDirectory means you don't have to build another application directory, speeding application deployment and leveraging what the informed customer is buying right now and in the future. The broad range of access methods means you don't have to rewrite existing applications that use any of these interfaces—just plug them in and you're ready to go.

Business advantages

NDS eDirectory can help you manage identity information for people (employees, customers, etc.) across disparate networks; NetWare, Windows, Linux, and UNIX. It can also facilitate relationship management between companies (partners, vendors, etc), something that is increasingly important as more business is conducted on-line. Using eDirectory you can provide secure access to the resources your employees and business partners need while protecting those they don't.

Increasing market acceptance—When you are selecting something as critical as your directory infrastructure product, you want to be sure it'll be around (and working) in a few years. After all, directory deployments aren't undertaken lightly, you can't afford to re-engineer your business because your directory vendor decides to change things, or worse yet, goes out of business!

When you choose Novell's NDS eDirectory, you get a mature and widely adopted product backed by a company that has been in the directory business for a long time. That's why companies like British Telecom, Red Hat, CNN and Yahoo! depend on eDirectory to support mission-critical operations from user management to e-commerce.

Largest installed base—With an installed user base of over 139 million, NDS is a mature proven product. Many other directory products are in their earliest implementations, or only deployed in a highly limited fashion, depriving the vendors of the experience Novell has used to improve NDS over the years. In addition to supporting all LDAP applications, more than 1800 directory-enabled applications have been built using eDirectory as the information repository.

Cross-platform availability—eDirectory 8.5 is a truly stand-alone directory running on Novell NetWare, Windows NT, Windows 2000, Sun Solaris, Linux, and Compaq Tru64 UNIX (with IBM AIX in beta). eDirectory is fully interoperable cross-platform—any eDirectory 8.5 server can communicate with any other eDirectory 8.5 server, as well as any LDAP 3 compliant application or directory. Client libraries and LDAP tools are available for Linux, Solaris, and Tru64 UNIX, as well as Windows.

NDS eDirectory is the first, and so far *only*, directory to pass the rigorous testing required for SunTone Program Certification, demonstrating superior performance and reliability. eDirectory has, in passing Sun's tests, met requirements for scalability, security, and availability as well as optimization for SunTone architecture.

When you deploy eDirectory you can choose the platform based on your current environment and business needs. When you compare this to the proprietary single-platform "my way or the highway" approach from many other directory vendors, the advantage is clear.

Novell Consulting—Novell consultants have extensive experience designing and deploying solutions for Novell customers worldwide. Whether it's directory integration or migration, management tools or a new application, Novell Consulting can help provide a greater Return On Investment (ROI) for eDirectory customers. Consultants can provide comprehensive project management including needs assessment, planning, technology selection, deployment, optimization and customization. Novell Consulting also releases products that enhance security, ease directory management, and extend Novell product functionality.

Cost—eDirectory costs $2 per user.

NOVELL DEVELOPMENT PARTNER COOL SOLUTIONS

Now that you know a little more about eDirectory's capabilities and how Novell can help you develop world-class applications, perhaps a bit of inspiration would be useful. Many independent vendors have come up with what we like to call "Cool Solutions"—particularly useful, innovative, or just plain *cool* ways to leverage eDirectory. Here's a couple of examples of business solutions vendors are developing with NDS eDirectory.

Business Layers eProvision DayOne

eProvision DayOne*, named 'Directory Products Best of Show 2000' by the Electronic Messaging Association, demonstrates the power of eDirectory as the foundation for next-generation business applications. DayOne leverages eDirectory to provide a policy-based business provisioning and procurement solution that uses LDAP to streamline the process of bringing new employees online and making them production from "day one."

DayOne uses employee profiles stored in the directory and XML connectors to automatically register people with HR and IT, providing immediate registration with network resources, services, devices, applications, and PBX. This ensures that new employees, business partners and others who need access to company resources get everything they need quickly, and with a minimum of hassle. eProvision DayOne supplies a Web-based GUI for management of the process and automatically notifies HR, IT, and appropriate managers of unfinished tasks to insure timely completion of the provisioning process.

Connectotel Ltd *Mobile Phone Policy Manager*

Mobile Phone Policy Manager (MPPM) delivers policy-based management of mobile device including cellphones. User and policy information is stored in eDirectory and all management tasks are performed via NWAdmin snap-ins. MPPM services fall into four categories:

- Asset Registration which maintains a registry of people and their wireless devices,
- Zero Day Start which (like DayOne) addresses the need to get new employees up and running quickly
- Support for text-to-cellphone messaging for devices that are not Wireless Access Protocol (WAP) enabled
- Policy-Based Management which provides a centralized point of administration for Short Message Service (SMS) features

eDIRECTORY: THE RIGHT CHOICE FOR LDAP

Novell provides more than just great directory services.

We help CTOs, architects, and project leads design comprehensive directory solutions to address the world's most pressing information technology problems, and provide consulting and support services to ensure that your directory project successfully accomplishes your business goals.

We support our developer community with a rich set of tools and comprehensive documentation, to help software developers understand, access (and profit by using) our products to deliver complete directory-enabled applications.

We stand behind our directory services with many years of practical experience deploying directory solutions in the enterprise networks and eBusiness environments. We continue to enhance, extend, and refine our directory service capabilities to support the evolving set of industry standards and technologies required by business.

What's that worth to you? Let us help you deliver your directory-enabled business solutions with our time-tested, award winning NDS eDirectory product.

Novell Product Training and Support Services

For more information about Novell's worldwide product training, certification programs, consulting and technical support services, please visit: **www.novell.com/services**

For More Information

Contact your local
Novell Authorized Reseller,
or visit the Novell Web site at:
www.novell.com

You may also call Novell at:

1 888 321 4272	US/Canada
1 801 861 4272	Worldwide
1 801 861 8473	Facsimile

Novell, Inc.
1800 South Novell Place
Provo, Utah 84606 USA

www.novell.com

Novell.