

1. How will the role of directory services evolve?
2. How will Microsoft's Active Directory affect the market for directory services?
3. How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Source: GartnerGroup

A directory service is nothing more than a database of useful information. Ideally, the database is distributed and replicated for ubiquitous access, high performance and fault tolerance. Directory services in and of themselves are not worth much. The true value of a directory service is derived from the applications and intra- and inter-enterprise business processes that leverage the information contained within the directory.

Directories are not simply intended for seeking people's e-mail addresses. Directories may be used to store information about any network object (e.g., a mailbox, printer or World Wide Web page URL). In the future, directories will be used to manage the allocation of network resources (e.g., to provide network policy management). The directory can also be used to store items such as a set of user preferences (e.g., natural-language usage or a preferred application set) or locations of key resources, so that wherever the user logs on, the preferred environment can be created to make the user feel "at home." With a directory service, a user should be able to log on once to a set of interconnected resources in such a way that his or her environment appears normal, the location of the data is transparent and the user achieves a single sign-on. Directories help link people together — to facilitate the completion of communications between humans and humans, humans and applications, and applications and applications.

How will the role of directory services evolve?

Directory Services Myths and Realities

Myth	Reality
Directory services solve single sign-on	OS and application vendors retain authentication; no single vendor has a critical mass of support
Directory services provide a single enterprise directory service	Multiple directories will continue to exist
Directory services provide a single point of administration	No single vendor has a critical mass of support; integration must come from the directory vendor or value-added, third-party software
Directory services are different from databases	A directory service is a database and several database vendors (IBM and Oracle) are selling directory service products based on their databases
The NOS vendor should provide the organization's primary directory	Directory services are provided by a variety of non-NOS vendors; network services are only one demand driver for directories
LDAP solves the multiple-directory problem	LDAP standardizes a directory access protocol, not a directory service

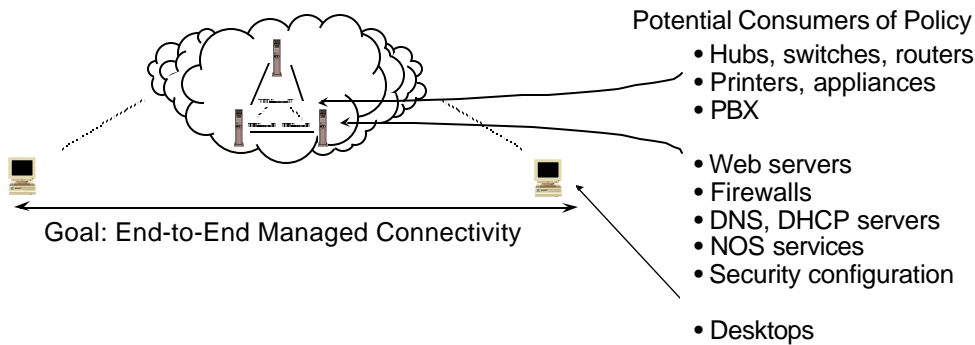
Source: GartnerGroup

There are many misconceptions about what a directory service will and will not provide. The most common misconception is that a directory service will somehow magically solve the single-sign-on (SSO) problem. This is not the case. Application and operating system (OS) vendors (e.g., Oracle, Novell, Microsoft and others) continue to require their own native authentication architectures. No single directory has gathered enough market momentum for independent software vendors (ISVs) to risk their future by linking their applications directly to a single vendor's directory. Another misconception is that a single enterprisewide directory is achievable (or even desirable). No single directory has a critical mass of support. Furthermore, some aspects of a network directory (fast network response time and convergence) are not critical to application directories. More important is the elusive goal of a single point of administration to add and delete information one time for the entire enterprise. While standards for directory synchronization and replication are forming, no solution exists today to solve this problem. Furthermore, simply installing a directory service on a platform (e.g., Netscape on Solaris or NDS on AIX) does not guarantee integration of the directory service with the local OS. *Action Item: Enterprises pursuing a directory service strategy should: 1) set expectations — there is no “silver bullet” to solve the multiple-directory problem; and 2) not overpromise and underdeliver — no single directory technology solves SSO or provides a single point of administration for the enterprise. Multiple directories will continue to exist.*

Sixty percent of organizations will have deployed policy-based networking for specific areas of congestion by year-end 2003; however, fewer than half of these will have policy-enabled their entire networks end to end (0.7 probability).

The difficulties in device instrumentation, end-to-end integration, lack of interoperability and configuration will all conspire to keep policy implementations minimal in all but data centers, “Web farms” and service provider networks through 2000 (0.7 probability).

Policy-Based Networking



Application	Phase III: Applications (e.g., SAP, Lotus Notes), routines within application time-sensitive traffic (voice, video and audio) vs. plain old data, user id, group, role, business unit (via directory integration)
Logical	Phase II: IP source/destination, port source/destination, IP TOS, user id (determined by DHCP, Dynamic DNS integration)
Physical	Phase I: MAC address

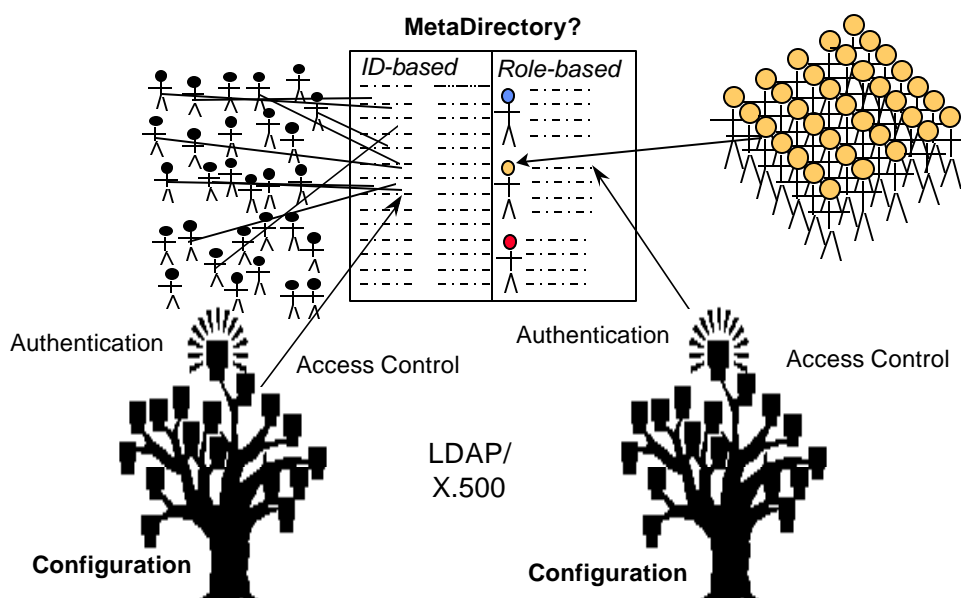
Source: GartnerGroup

Key Issue: How will the role of directory services evolve?

By 2003, for directory-enabled network services, policy-based networking will be a significant demand driver. A policy is a rule. Policy-based networking is the use of rules to govern network operation. Policies can apply to any object on the network — a user, a group of users, a role, a device or an application (e.g., Bob’s packets get higher priority, members of the finance department can access www.stockmaster.com while others cannot, the SAP application gets guaranteed response time, the printer gets a fixed IP address). Despite industry hype, few standards exist for policy management. There is no standard way to describe a policy object and, thus, no vendor interoperability of policies in a heterogeneous environment. Furthermore, there is no standard way of storing and accessing these policies, although, in the longer term, directory services will play this role. Therefore, policy management will evolve in three phases: static, dynamic and directory-enabled configuration with proprietary implementations being the norm for at least the next five years. *Action Item: Organizations should clearly distinguish network hardware vendors’ motivations for pushing policy management from the organization’s own business needs. Until quantifiable costs/benefits can be derived, upgrades should be driven by the need to overcome specific areas of congestion, not by the illusory benefits of policy enablement. Initial candidates for policy management are constrained WAN links, data center and “Web farm” backbones, and ISPs providing “business class” network access.*

Complex directory issues will not be resolved during the five-year planning period. Enterprises should work to minimize directory project impact on public key infrastructure (PKI) developments by opting for lowest-common-denominator approaches and migrating to new architectures as necessary.

Directories and PKI



Source: GartnerGroup

Key Issue: How will the role of directory services evolve?

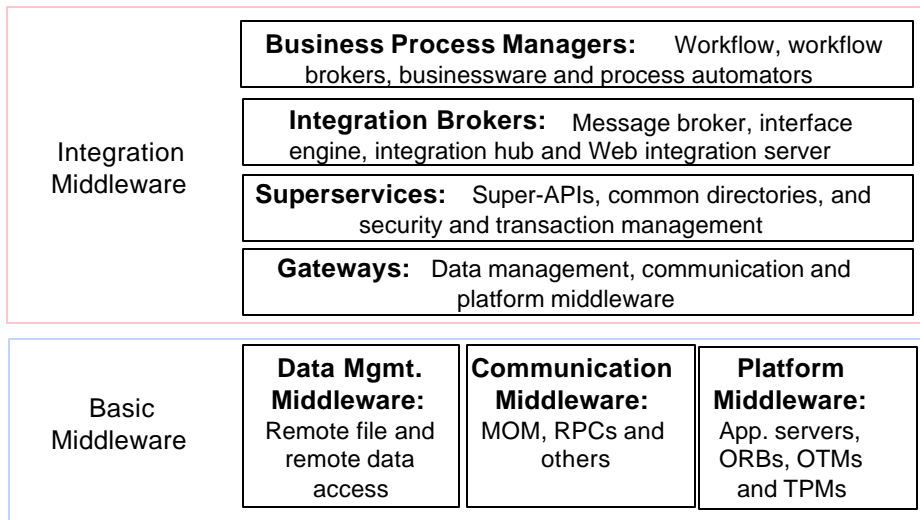
Directory services will evolve to become a critical component of a distributed-security architecture. X.509 certificates were originally intended for secure access to an X.500 directory. Now, with X.509 v.3, directories (or databases) of any type can be used to store and allow access to certificates and the public keys they contain. Most new implementations support LDAP-enabled directories for this purpose.

In addition to providing access to certificates, directories can be used to store permissions, access levels, role-based rules and other attributes.

Enterprises have faced some difficulty trying to synchronize directory projects with certificate projects. Different divisions of an enterprise and application owners may have their own priorities for the directory project. For example, networking may use NetWare Directory Services (NDS) for its purposes; office systems maintain e-mail-specific directories. Privacy issues arise when a directory is used for human resources information, such as salary or home address information. Directory products are often optimized for specific applications. The multiplicity of directories leads to consideration of directory synchronization and metadirectories containing all enterprise directory information, often conceptually without consideration of business value.

By 2002, the major middleware vendors will support directory services as part of their integration middleware platforms (0.8 probability).

Middleware: Another Role for Directories



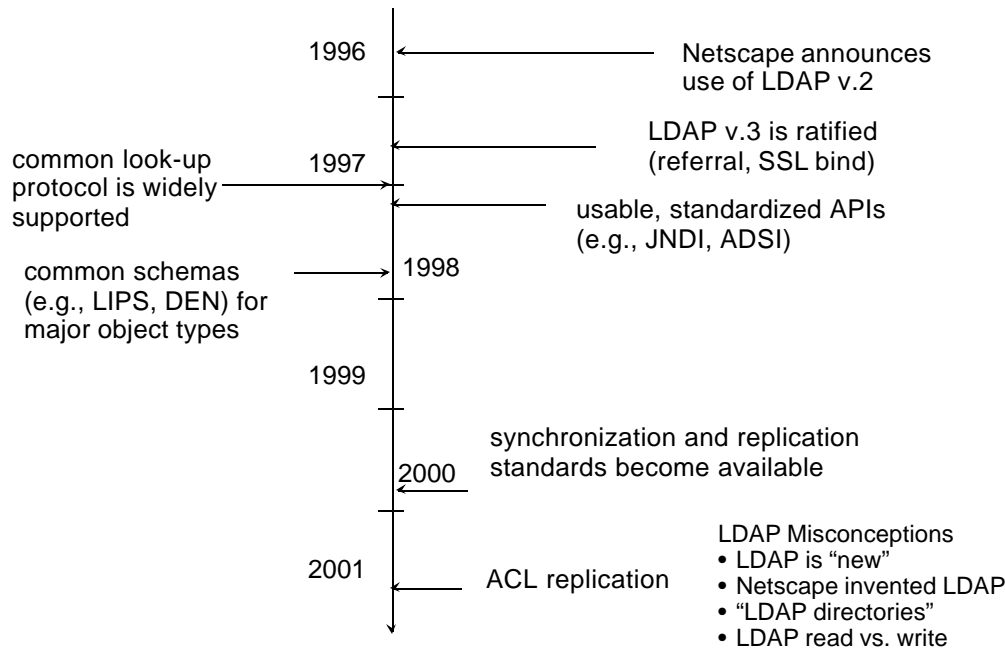
Source: GartnerGroup

Key Issue: How will the role of directory services evolve?

Middleware is the software “glue” that helps programs and databases that run on different computers work together. We define middleware as “runtime system software that directly enables application-level interactions among programs in a distributed computing environment.” In this taxonomy, *integration middleware* is high-level, interapplication middleware that provides some function or set of functions that is specifically related to connecting application programs or middleware products that differ from each other. Integration middleware complements or is a superset of basic communication middleware, platform middleware or data management middleware. One of the important parts of integration middleware is the *superservice*. A superservice presents to the application program its own superAPI, effectively masking or superseding the API(s) exposed by other software layers. A superservice provides services, such as metadirectory, security and/or transaction management, across two or more OSs, ORBs, TP monitors, DBMSs, application servers and/or networking layers. Middleware vendors that offer directory services include Gradient (Gradient’s PC-DCE product family includes the distributed security, directory and time services of DCE. Gradient’s NetCrusader product family includes security technologies for authentication, encryption and authorization) and Candle (Candle’s Roma Business Services Platform offers an LDAP-based directory, which facilitates application program reuse and makes it easier for programmers to address messages using high-level business service names rather than by using hard-wired queue names). Another example is PeerLogic, which acquired ICL’s i500 in 1998.

By year-end 2002, 80 percent of all enterprises will have a ubiquitous LDAP-enabled directory infrastructure in place; however, 90 percent of these will be serviced by Microsoft, Novell or Netscape (0.7 probability).

LDAP: Helpful, but Not a Panacea



Source: GartnerGroup

Key Issue: How will the role of directory services evolve?

LDAP is a lightweight version of the X.500 Directory Access Protocol. LDAP is not a directory service, but rather a protocol for standardized client access to different vendors' directories, allowing directory vendors to compete based on functionality. In 2000, all leading directory products support LDAP as the least common denominator for looking up information. LDAP v.2 did not solve the more difficult problems of directory referral, and synchronization and replication. LDAP v.3 (ratified in mid-1997) addressed referrals but did not provide a robust synchronization and replication mechanism. LDAP-enabled products have been delivered by all of the leading network operating system (NOS) and directory vendors, but the longer-term (and more difficult) problems of cross-authentication (single sign-on) and directory synchronization (single point of administration) will not be addressed by LDAP in heterogeneous environments until 2H00 for synchronization and replication, and 2H01 for cross-authentication (0.6 probability). *Action Item: Enterprises must understand LDAP's role in leveraging directories. For internally developed applications, enterprises should immediately begin to use LDAP. We recommend design and initial deployment of an LDAP-enabled directory infrastructure to begin to support these applications.*

By year-end 2002, Novell will switch to a “universal NDS license” (0.8 probability), effectively giving away NetWare, instead of charging per user for its directory-enabled management capabilities (0.7 probability).

By year-end 2002, Novell will ship at least two mainstream directory-enabled products that do not require NDS as the directory service (0.7 probability).

File/Print/Directory Is a Commodity

What is a commodity? “undifferentiated”

What a commodity is not: unimportant or free



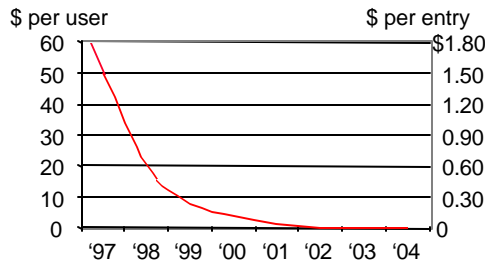
Downward pressure from:

- Microsoft bundles Active Directory with Win2000
- Microsoft will require Active Directory for the back office
- Threat of Linux, open source
- Database vendors are directory vendors
- Remaining directory vendors will become cutthroat



Key to directory longevity:

- It is not about technology
- Value is in directory-enabled software, directory integration and management
- Complexity kills
- Build the installed base quickly and increase switching costs



Source: GartnerGroup

Key Issue: How will the role of directory services evolve?

A commodity is undifferentiated, and thus any supplier can fulfill a commodity requirement as well as any other. File-and-print sharing is a commodity in 2000. We expect directory services to become commoditized in the next three years. Several factors will contribute to the commoditization of the directory services market: the collapse of the X.500 directory market; the entry of database vendors into the directory market; and market consolidation. The most significant impact will come from Microsoft, with its bundling of Active Directory with Windows 2000 and the increasing interdependencies created between Active Directory and Microsoft’s Back Office and Office products. Linux and the open-source movement will have some impact on commoditization as well. As directories become commoditized, decisions come down to price and manageability. We have long stated that enterprises that purchased directories like Novell’s NDS and Banyan’s StreetTalk did not purchase a directory service; they purchased a powerful directory-enabled administrative tool for managing users, groups and access control across a number of distributed servers. Likewise, value to vendors will not be in revenue generated by directory sales but rather in that generated through the sale of directory-enabled software and services that leverage the directory.

Action Item: When choosing a platform for file, print and directory services, enterprises should focus on total cost of ownership (TCO) through the ease of administration and management, and the ability to leverage the directory with other directory-enabled software products.

How will Microsoft's Active Directory affect the market for directory services?

To address the network service provider market, Cisco will deliver Active Directory on Solaris within six months of the ship date of Microsoft's Active Directory on NT, and on HP-UX within one year (0.7 probability).

Cisco's protection of its relationship with Microsoft will prevail and, by 2002, enterprises choosing Cisco's directory-enabled policy-based networking (PBN) products will have no choice but to install Active Directory (0.9 probability).

Cisco and Active Directory

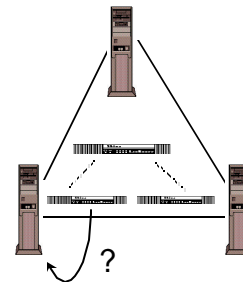
Why Cisco needs a directory strategy:

- There are limits to what Cisco can do within IOS
- Phase III (2000 to 2004) of policy-based networking requires linkage to a directory service
 - Phase I, static policies
 - Phase II, linkage to user ID via DDNS
 - Phase III, linkage to organizational role via DS
 - Phase IV, policy unification
- Drives added value into software
- Increases vendor lock-in and switching cost of Cisco's products

Why Cisco chose Active Directory:

- Why reinvent the wheel building a directory itself?
- Looked at Banyan and Novell; Microsoft appeared to have market momentum
- Cisco has a poor track record of server-based software development
- Cisco's Active Directory on Unix targets NSP market where Microsoft has no "mind share"
- Cisco plans to support other directories through "interoperability," not natively

Application-Aware Network



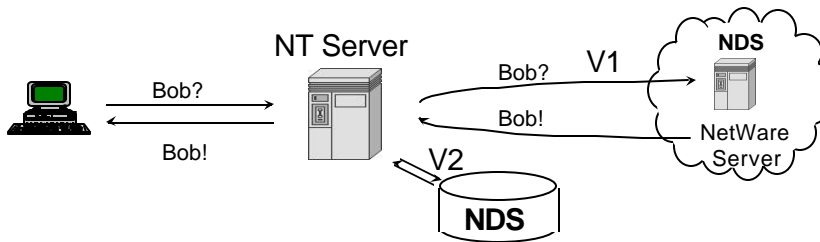
- Directory look-up
- Policy look-up
- Authentication
- Configuration

Source: GartnerGroup

Cisco and Microsoft have received a great deal of industry attention as a result of their agreement concerning Microsoft's Active Directory. On 7 May 1997, Cisco announced that it was adopting Active Directory as its directory service for integration with its products. In addition, Cisco will port Active Directory to Unix. We believe Cisco's porting of Active Directory to Unix is targeted at the carrier and Internet service provider (ISP) market, not at the typical organization. Cisco is facing pressure as switching and routing are commoditized and moved into silicon. Cisco must drive its value "up the food chain" into software and intelligent network services. One significant area in which Cisco will require directory enablement is in providing policy-based networking. Phase II of CiscoAssure's policy implementation will provide directory enablement. Rather than build its own directory, Cisco looked first to Banyan and Novell before turning to Microsoft as a provider of its de facto directory service. Since Active Directory is not capable of storing dynamic information, Cisco has developed specific value-added software directly on top of Active Directory. At this point Cisco will directly support only Active Directory, although it has pledged "interoperability" with other vendors' products, such as Novell's NDS. *Action Item: Organizations using Cisco products in conjunction with another vendor's directory service should request in writing Cisco's official support for those directory configurations. Organizations waiting on Cisco's Active Directory-enabled policy-based networking products should not consider deployment until the first major service pack for Windows 2000 is delivered and proved stable, at least until late 2000 or early 2001.*

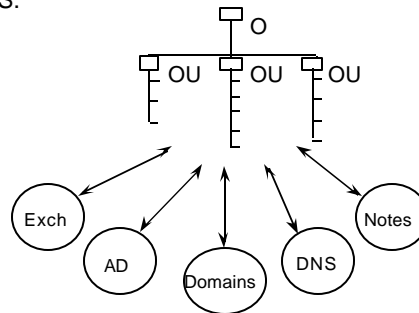
Novell will provide two-way NDS-to-AD synchronization capabilities within nine months of commercial availability of Windows 2000 (by year-end 2000; 0.8 probability).

Novell and Active Directory



Redirection Model: Novell installs software on host platform that intercepts and redirects authentication and directory look-up requests to NDS.

Synchronization Model: All user information stored and managed using NDS. Administration is through NDS or native tools. Information is synchronized to and from NDS with bidirectional synchronization connectors to other directory services.



Source: GartnerGroup

Key Issue: How will Microsoft's Active Directory affect the market for directory services?

With NT v.4, Novell has used a redirection model with its NDS for NT product to provide a solution for managing heterogeneous NDS and NT domain environments. We believe this approach will be difficult, if not impossible, for Novell to implement with Active Directory in Windows 2000 for Microsoft's own applications. While Novell's redirection may work for non-Microsoft applications that do not make extensive use of Active Directory's capabilities, we believe Microsoft's own applications will exploit specific capabilities of Active Directory that cannot be redirected into Active Directory (e.g., Microsoft implementation of catalog services differs substantially from Novell's). We believe the more pragmatic and achievable solution for Novell will be to have NDS manage Active Directory using a bidirectional synchronization model. Novell implements such a solution today to support the Exchange directory with NDS for NT v.2 using unidirectional synchronization. The argument of redirection vs. synchronization misses the point: Novell must and will have a solution for NDS to manage Active Directory either as an evolution of NDS for NT or as a part of its metadirectory strategy. In addition, we expect third-party companies such as NetVision and FastLane to also provide tools to manage the coexistence of NDS and Active Directory (and other directories like Lotus Notes and Netscape). *Action Item: Organizations using NDS and NDS for NT should consider the use of NDS to manage Active Directory deployments as a way to reduce cost and minimize redundant administrative tasks beginning in the late 2000 into 2001 time frame.*

Enterprises evaluating directory service technologies must look beyond the technical “speeds and feeds” of a directory service to the selection criteria that directly affect the long-term ability to maintain and integrate the directory in the enterprise.

Enterprise Directory Selection Criteria

Criteria	Weight	Score	Total
Support for LDAP v.2 read/write v.3 read/write future commitment to LDUP and ACL replication	10		
Application developer support	9		
Size of installed base	9		
Delegation of authority	8		
Ease of installation/migration	8		
Availability and cost of service and support	8		
Management interface ease of use	7		
PKI support	7		
Bundled synchronization tools	7		
Scalability/performance/throughput	7		
Multiplatform support	6		
Integration with native OS security and directory	6		
Multimaster change control	5		
Built-in reporting/auditing capabilities	5		
Third-party tool support	5		
Developer's toolkit and APIs	4		
Availability and cost of consulting and systems integration	4		
Native support for LDAP (not gateway)	3		
Cost	3		
Licensing model	2		

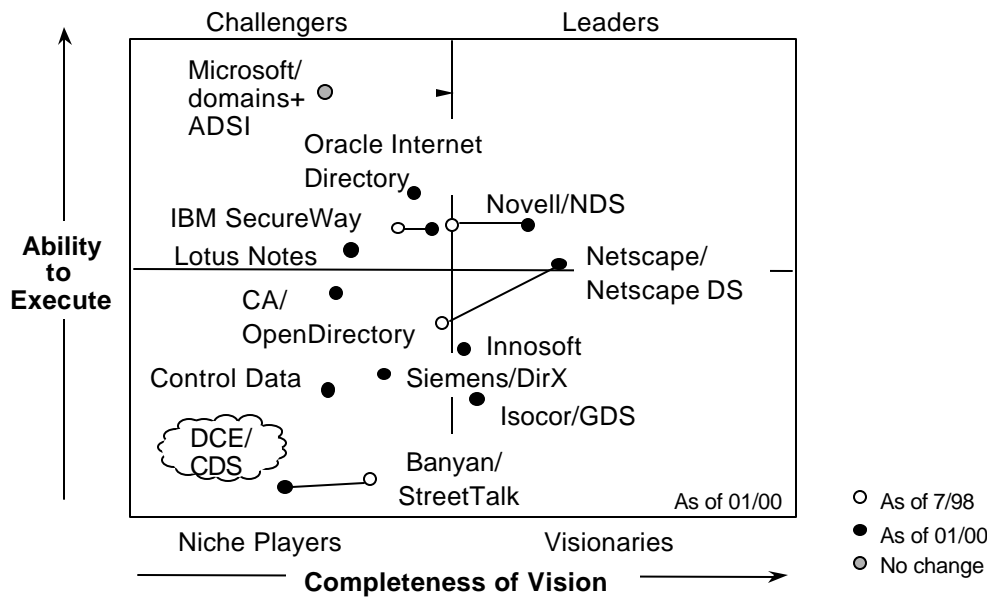
Source: GartnerGroup

Key Issue: How will Microsoft's Active Directory affect the market for directory services?

We use the term “enterprise directory service” to describe a directory service that can serve emerging directory requirements, such as LDAP-enabled application support and PKI support, and become a focal point for directory consolidation as well as integration with legacy e-mail and NOS directories. Rather than focusing primarily on the technical aspects of a directory service by asking questions like “How many queries per second can this directory handle?” we believe the more important questions enterprises should ask are: “How complex is this directory to get up and running?” “Where can we find service and support?” and “What applications are available to leverage this directory?” These “soft” limitations are what ultimately caused the decline of X.500. The weightings of the selection criteria are our recommended weightings for a general-purpose directory capable of supporting internally developed or externally purchased LDAP-enabled applications. If a directory was selected to only support a specific function (e.g., only PKI), then the enterprise's criteria would need to be re-weighted to reflect the single-purpose nature of the directory, e.g., the importance of ISV support could be reduced and the importance of PKI support would become the highest-weighted item. To use the model, an enterprise should construct a spreadsheet similar to the one above, including any additional criteria the enterprise feels is important and adjusting the weightings according to its needs, using our weightings as a suggested guideline. The weighting, multiplied by the scoring, should be totaled and the highest-scoring vendor selected.

No single vendor-specific directory will dominate the industry through 2001 (0.8 probability).

Enterprise Directory — Follow No Leader



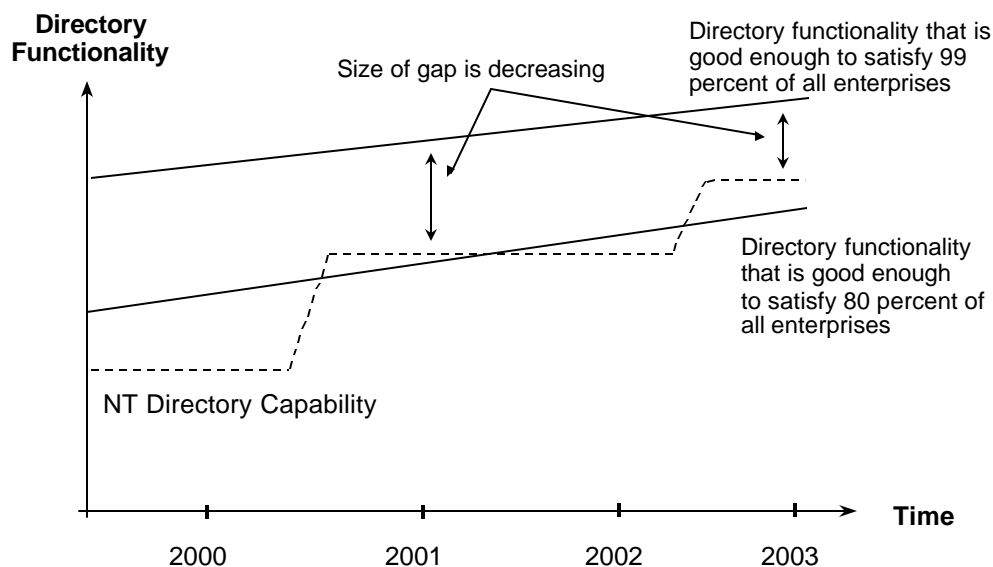
Source: GartnerGroup

Key Issue: How will Microsoft's Active Directory affect the market for directory services?

Directories are undergoing maturation of the current technology and rapid evolution. There has also been major consolidation recently: Zoomit acquired by Microsoft, OpenDirectory by Platinum and then CA, ICL's i500 by PeerLogic, Isocor by Critical Path, CDS by Syntegra, Siemens partnering with Oracle, and the creation of the Sun-Netscape Alliance following AOL's acquisition of Netscape. The convergence of application directories and network service directories is being driven by Microsoft, Sun-Netscape and Novell. IBM's strategy remains fragmented between Domino, SecureWay and Tivoli product lines, but we expect to see this addressed with a more coherent product strategy in 2000 (0.7 probability). All significant players recognize the importance of metadirectories and synchronization (Microsoft bought Zoomit, Netscape licensed Isocor code, Novell invested in NetVision). The result of this market evolution is that directory services will increasingly be delivered as part of a broad-capability Internet platform from Microsoft, Sun-Netscape, IBM or Oracle. Novell is trying to remain in this game with multiple partnerships, most recently bundling IBM's WebSphere with NetWare v.5.1. Products like those from Isocor and Siemens will retain a role where enterprises wish to retain independent directory services. However, integration with legacy systems and business applications will remain a challenge: achieving enterprise directory services remains an integration project rather than a package selection exercise. *Action Item: In the next five years, the goal of a single unified enterprise directory will remain elusive. Enterprises should focus on directory consolidation and synchronization projects with an immediate return on investment.*

How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Active Directory: Not the Best, but “Good Enough”



Source: GartnerGroup

The most common mistake enterprises make concerning Active Directory is somehow assuming that Microsoft intends to build the world's best directory service. Questions like "Is Active Directory as good as NDS?" or "Is Active Directory as good as X.500?" are misguided.

The answer to these questions is "no," — at least not in the first release. However, these organizations are asking the wrong question. The correct question is: "Is Active Directory good enough for what I need it to do?" We believe that, for most organizations, the answer to this questions will be "yes."

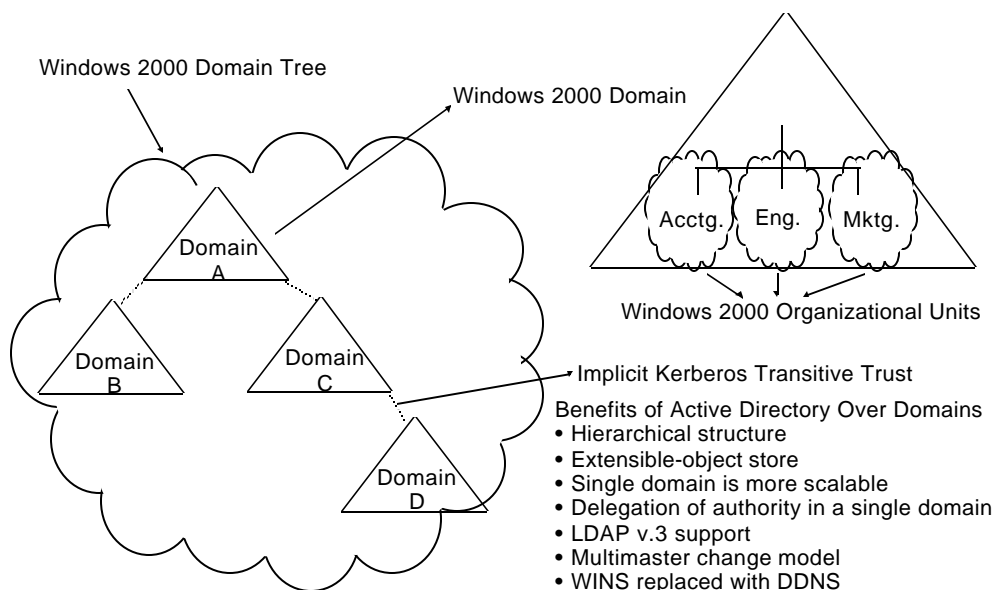
Rarely are any of Microsoft's products "best-of-breed." Microsoft's design point is not to be the most scalable/reliable/secure/ _____ (fill in the blank with your favorite server attribute) product in the world. Microsoft designs products that provide "good enough" functionality for 80 percent to 90 percent of all usage scenarios and then slowly improves the product over time.

This philosophy holds true with Microsoft's Active Directory, which will fall short in several areas on its first release but is far superior to the legacy domain architecture it replaced. Is Active Directory the "best" directory technology available? No. Will Active Directory be "good enough" to manage large numbers of users, groups and access control in a distributed Windows 2000 environment? Yes. That is Microsoft's design goal.

Windows 2000 Server will not be available in a reasonably stable, feature-complete release until at least 1H00, and it will not be suitable for widespread production deployments until at least late 2000 (0.7 probability).

Active Directory will not be as technically capable as Novell's NDS when shipped, or within the following three years, at least through year-end 2003 (0.8 probability).

Windows 2000: Active Directory: Better Than Domains



Source: GartnerGroup

Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Microsoft uses the term "domain" to describe its logical grouping of users and resources in NT v.4 and in Windows 2000. With NT v.4, the domain information is stored on each domain controller in the registry. With Windows 2000, Microsoft has chosen a variant of its Jet database (similar to Exchange) to store the information. By breaking the information out of the registry, Microsoft has increased the scalability of what a single domain can hold from approximately 15,000 objects with NT v.4 to 1 million with Windows 2000. Windows 2000 domains add a hierarchical structure based on organizational units to better organize network resources for users and administrators. With NT v.4, there is no way for Microsoft's software to enable delegation of authority within a single domain without the use of third-party software. Windows 2000 provides the ability to delegate administration on any object or attribute. NT v.4 domains are static, whereas the information in Windows 2000 may be extended. All major limitations with NT v.4 domains have been addressed with Active Directory. *Action Item: Enterprises should: 1) understand that despite being called a "domain," NT v.4 domains are quite different from Windows 2000 domains and that major retraining of administrators, help desk and users will be necessary; 2) begin planning their Active Directory domain structure in mid-2000 after Windows 2000 has shipped and stabilized; and 3) not plan on Windows 2000 production deployments until at least early to mid-2001 at the earliest target date for widespread deployments of Active Directory.*

Fifty percent of Microsoft's NOS installed base of NT servers will have migrated to Windows 2000 and Active Directory within three years of commercial availability of Windows 2000 — half as long it took 50 percent of Novell's installed base to migrate from NetWare v.3 to NetWare v.4 (0.8 probability).

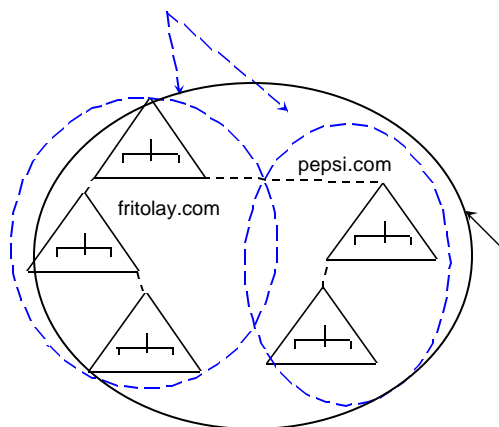
Active Directory: Advantages

Tree:

Contiguous name space
Transitive trust between domains
Common schema
Common catalog

Advantages

- Minimized dependence on time
- Knowledge Consistency Checker
- Sites replicate through bridgehead servers with scheduling, cost assignment and compression
- Attribute-level replication
- Supports nonreplicated attributes
- Arbitrary nesting of groups
- Certificates are standard user attribute
- Global catalog of common attributes



Forest:

Two or more trees
Noncontiguous name space
Transitive trust between trees
Common schema
Common catalog

Source: GartnerGroup

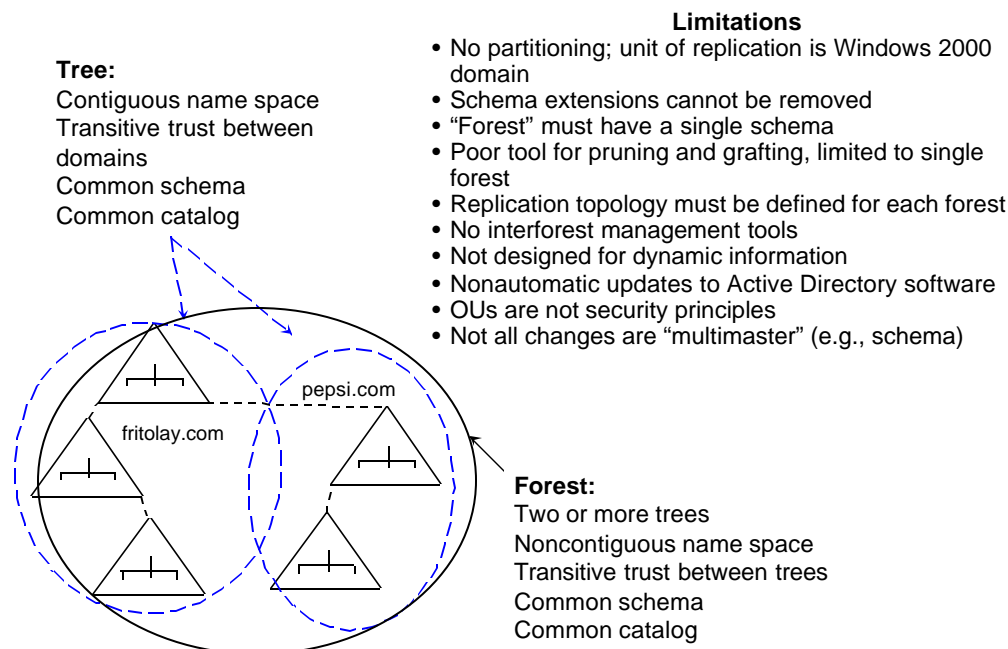
Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Microsoft's biggest advantage over competitors like Novell and Netscape is not technology. In several areas, Microsoft favored simplicity over capability. The result is a directory that will be easier to get up and running out-of-the-box but not as powerful as other directories. For example, Microsoft includes a technology called the "Knowledge Consistency Checker" that automatically configures connections for replication among servers. Active Directory has minimal dependence on time — an area where Novell's NDS requires significant planning. As compared to NT domains and the Exchange directory, Active Directory will support attribute-level (as opposed to object-level) replication. Replication among sites can be configured so that only one copy of changes is sent across slower network segments, and this replication may be scheduled for off hours and compressed to reduce bandwidth requirements. Finally, Microsoft is an aggressive supporter of PKI using X.509 certificates, and Active Directory is designed to support certificates as a standard user attribute. *Action Item: Enterprises coming from a NetWare v.4 environment will find Active Directory more simple to understand and implement than NDS. Enterprises coming from an NT v.4 environment should bring in outside expertise for the design of the Windows 2000 domain architecture, as the concepts of a hierarchical, replicated directory service will be new. In any case, enterprises should minimize the number of domains used in Windows 2000 — the best domain design in Windows 2000 (and in NT v.4) will remain a single domain.*

Because Active Directory domains lack partitioning, 70 percent of organizations with more than 1,000 users will be forced to implement multiple Active Directory domains to overcome bandwidth constraints (0.8 probability).

User inexperience with directory services and the nuances of Active Directory will cause 60 percent of Active Directory installations to be redesigned within 18 months of deployment (0.8 probability).

Active Directory: Limitations



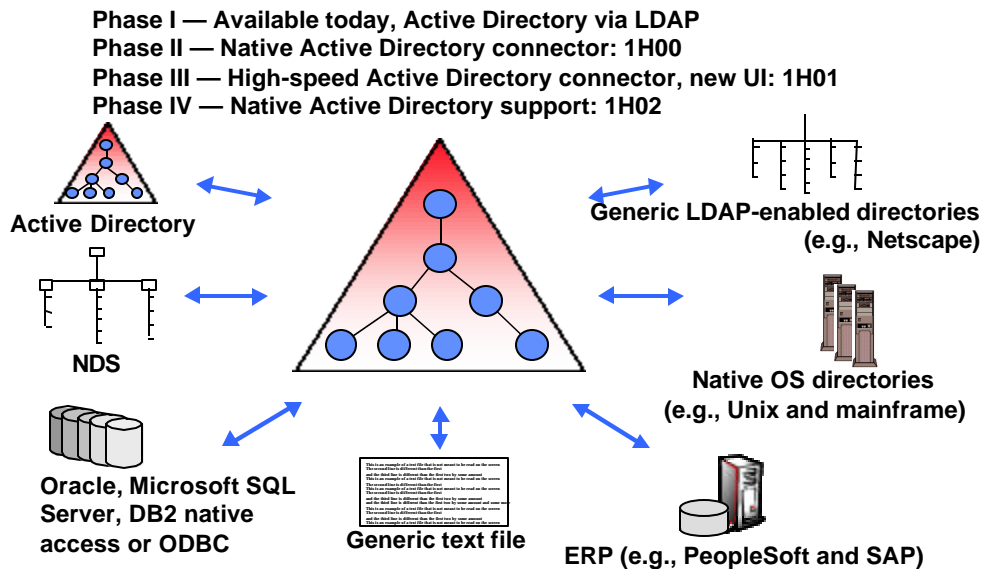
Source: GartnerGroup

Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Like any Microsoft 1.0 release, Active Directory will lack key features found in other products on the market. Most notably, Active Directory supports no partitioning (breaking up) of the directory database within a single NT domain. For domains that span geographic boundaries, the bandwidth requirements to keep all information synchronized are likely to force organizations with multiple geographic locations to implement multiple Active Directory domains. Microsoft marketing will claim that creating domains is Active Directory's method of partitioning. This is misleading. While an Active Directory domain is Microsoft's smallest unit of replication like a partition, it is not a partition. A directory partition is purely an administrative construct, transparent to end users. An Active Directory domain is a naming boundary, a Kerberos security boundary and an administrative boundary. Furthermore, group policies cannot span multiple domains. Extensions to the schema cannot be removed in the first release. Organizational units (OUs) cannot function as security principles, meaning that it is not possible to assign directory rights to an OU for any object in the OU. Finally, Microsoft provides no tools for organizations that must manage multiple "forests." *Action Item: Enterprises should understand and design within the limitations of the first release of Active Directory. Schema extensions should be avoided and larger organizations (greater than 5,000 desktops) should expect multiple Active Directory domains to be required simply to overcome bandwidth requirements on constrained network links. Enterprises migrating from NetWare v.4 will find Active Directory easier, but less capable.*

Microsoft will not deliver metadirectory capabilities using Active Directory as the core repository until at least 1H02 (0.7 probability).

Microsoft's Metadirectory Services



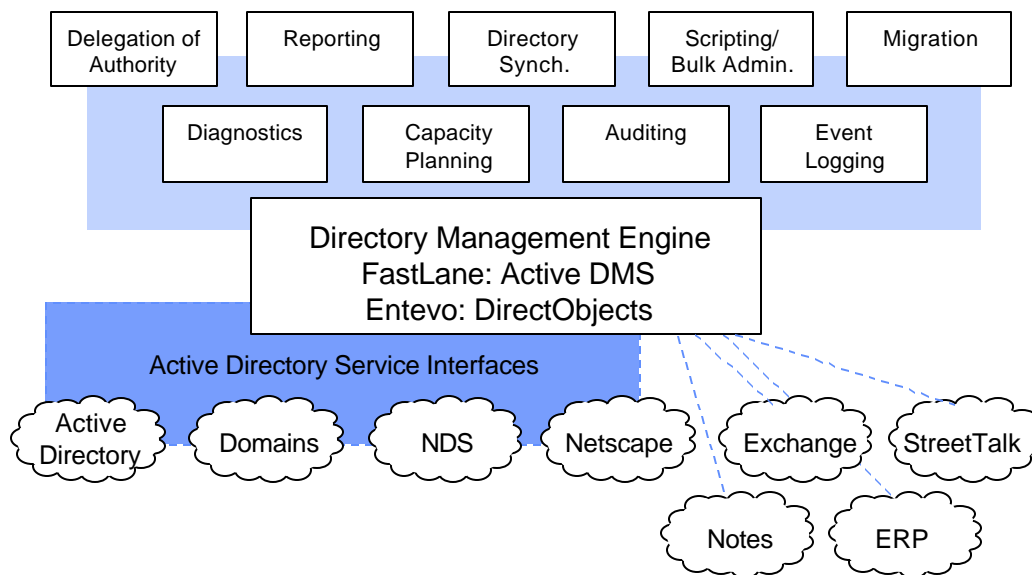
Source: GartnerGroup

Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

The classic definition of a metadirectory is a directory that acts as a superset of all other directories — a “mother of all directories.” Metadirectories have evolved from stand-alone products to services that enable a given directory to synchronize and exchange information with other data repositories. We believe this capability is critical if a directory is to function in a broader role as an enterprise directory service. All of the major enterprise directory vendors, including IBM, Microsoft, Netscape, Novell and Oracle, plan to add metadirectory functionality to their products. Microsoft’s acquisition of Zoomit in July 1999 signaled its intention to provide metadirectory capabilities — initially using the Zoomit directory and in the longer term using Active Directory. This announcement was a change in strategy for Microsoft, since it previously positioned Active Directory as the only directory an enterprise will need. Microsoft’s acquisition indicates that it understands Active Directory will not be the only directory used in most enterprises and that Active Directory falls short in several areas. *Action Item: For enterprises seeking a solution in 2000, we recommend MMS only to those with more than 10,000 desktops and a commitment to a Microsoft and Active Directory-centric architecture. Others should consider Netscape, Isocor, Siemens and Novell as alternatives.*

Through 2001, for 80 percent of large and midsize enterprises, deploying a single Windows NT v.4 domain and using a third-party tool for delegation of authority can reduce NT Server cost of ownership by 10 percent to 20 percent compared with a multimaster domain implementation and can ease the migration to Active Directory (0.7 probability).

The Larger Problem of Directory Management: FastLane, Entevo and Mission-Critical Software



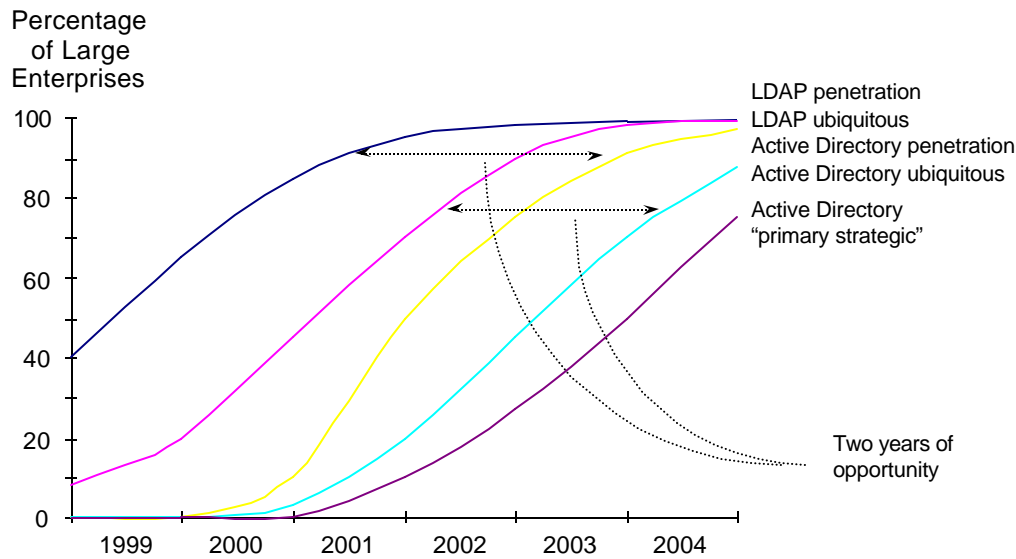
Source: GartnerGroup

Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Several NT tool vendors are evolving their product platforms to enable a “virtual active directory” today — enabling the creation of a hierarchical directory structure on NT v.4 today as a way of better managing NT v.4 today and planning for Windows 2000 in the future. FastLane Technologies and Entevo (and, more recently, Mission Critical Software) have very similar visions for delivering directory management tools within a larger architectural framework across multiple directory services including Active Directory, NT v.4 domains and NDS. This is accomplished through the use of Microsoft’s Active Directory Services Interfaces (ADSI) API, which can support domains, Active Directory, NDS and LDAP directories within a single application. These tools provide an excellent way of better managing the multiple-directory problem today while providing a migration path to Active Directory in the future. We expect that these tool vendors will evolve into directory management vendors using Active Directory as the focal point for directory management, synchronization, reporting and administration after Windows 2000 and Active Directory are delivered. As further evidence of the importance of multidirectory interoperability, on 7 July 1999, Microsoft announced the acquisition of Zoomit — a vendor of metadirectory technology. The announcement indicates that even Microsoft understands multiple directories will exist for many more years.

Although Active Directory will have been deployed in 90 percent of large organizations by year-end 2003, LDAP directories will have achieved the same level of penetration at least two years earlier (0.7 probability).

LDAP vs. Active Directory?



Source: GartnerGroup

Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Active Directory will be delivered with Windows 2000, but Windows 2000 delays have created an opportunity for other vendors, notably Novell and SNA — e.g., Cisco chose Active Directory as its focal point for directory integration and its suffering from Windows 2000/Active Directory delays. In contrast, Nortel/Bay Networks has taken a decidedly “directory neutral” stance. In terms of market penetration and ubiquity within large enterprises, LDAP-enabled directories hold approximately a two-year lead over Active Directory. Much of Active Directory’s promise is untested. Active Directory was created without the benefit of leveraging proven directory technology on the market (e.g., X.500 or NDS). Thus, Active Directory has unknown performance, scalability, stability and bandwidth requirements. Furthermore, given the pressure on the Windows 2000 program, we expect that Microsoft will not initially deliver the robust set of migration, pruning, grafting, reporting, auditing, troubleshooting and diagnostic tools necessary to support large Active Directory deployments.

Planning for Active Directory will constitute at least 40 percent of the overall Windows 2000 migration planning effort. Planning for Active Directory will be more complex than the planning for any other Microsoft product previously installed.

Directory Planning and Migration Team

Representation Phase I

Network-operating-system support team
 Electronic-mail support team
 DNS/DHCP (Unix?)
 Physical network support
 Data security
 Desktop support group
 Database administrators



Issues

- Naming standards
- Domain/tree/forest design
- DNS integration
- Delegation of authority
- Replication requirements
- NT v.4 domain integration
- Contents of catalog
- Directory vs. database

Representation Phase II

Help desk
 Training
 Business units
 Application developers

Issues

- Support
- Administrator training
- End-user training
- System backup and recovery

<20 servers 3-month planning effort 3–6-month implementation	<100 servers 6–9-month planning effort 6–18-month implementation	>200 servers 9–15-month planning effort 1–2-year implementation
--------------------------------------------------------------------	------------------------------------------------------------------------	-----------------------------------------------------------------------

Source: GartnerGroup

Key Issue: How will the strengths and weaknesses of Active Directory affect the organizations that deploy it?

Installation of a directory service architecture is a long and politically charged process. Multiple areas from within the IT organization must be represented in the initial planning and design phase. Active Directory's dependence on dynamic DNS requires coordination with the DNS/DHCP support group (typically on Unix). The convergence of the Exchange directory and the NOS directory within Active Directory will require coordination with the electronic-mail support team and the NOS support team. The physical-network support team (e.g., hubs, firewalls and wide-area network) must be represented to assess the impact of Active Directory's replication characteristics on the enterprise network. Data security must be involved to help define standard access control and administration policies. If NT desktops, Zero Administration Windows or roaming profiles are to be supported within Active Directory, the desktop support group must be involved. Many organizations that deployed hundreds of domains using NT v.4 will find that basic issues such as naming conventions have never been addressed. Directory design is a long process that will take up to a year and a half for larger organizations before the rollout begins. The actual rollout itself must be phased in, requiring coexistence with an NT v.4 domain architecture in a typical enterprise for more than a year. We do not recommend the formation of this team until the first generally available release of Windows 2000 has shipped in 1H00. This requires that this team's activities begin in 2000, and that the actual rollout beginning in 2001 be budgeted for in 2000.

Enterprises should:

- Understand that multiple directories will continue to exist within the enterprise. We believe the real issue to tackle with immediate impact is not trying to implement a single directory, but rather coexistence with other directory services and Active Directory, including directory synchronization, consolidated user administration and single (reduced) sign-on.
- When using NT v.4 and seriously considering a migration to Windows 2000 and Active Directory, consider domain consolidation today, use LDAP wherever possible, register for their OID, budget for Windows 2000 and Active Directory pilots in 2Q00, begin lab testing Windows 2000 in 2Q00, begin Active Directory planning in 2Q00, and budget for widespread production deployments in 1H01.
- Look beyond the technical capabilities of the directory (e.g., how many transactions per second). Many of the important issues, such as ease of installation and management, have nothing to do with technology, but have everything to do with the long-term maintainability of the directory service.
- Understand and design within the limitations of the first release of Active Directory. Schema extensions should be avoided, and organizations should plan on multiple Active Directory domains simply to overcome bandwidth requirements on constrained network links.
- Keep their domain designs simple. Domain design largely comes down to two issues: scalability and politics. In all cases, the simpler the domain design is, the more manageable and easily audited the environment is. A simpler domain design today will position the enterprise for an easier migration to Windows 2000 and Active Directory in the future.
- When using Cisco equipment with no plans to move to Active Directory, require Cisco to commit in writing to supporting other vendors' directory services and clarify what "interoperability" with these directories will provide.
- When using NDS, pressure Novell to clarify how and when it will provide tools to manage Active Directory in a heterogeneous NDS and Active Directory environment.
- Expect the design phase of an Active Directory deployment to last at least six months and, for most large organizations, at least one year. Rollout of Active Directory will be a protracted multiyear process; designing for coexistence with NT v.4 domains should be considered mandatory.
- When designing the Active Directory structure: involve the appropriate planning groups; minimize the total number of domains; arrange multiple domains geographically to reduce bandwidth requirements; use a single forest wherever possible; and avoid schema extensions until Microsoft provides a way to remove them.
- Not plan on widespread production deployments of Active Directory until early to mid-2001 at the earliest, allowing time for Active Directory to mature, application vendors to certify their applications, third-party tools to appear and the Active Directory design to be laid out and piloted, and therefore planning on living within the limitations of NT domains for at least the next year.
- Understand and design within the limitations of the first release of Active Directory. Schema extensions should be avoided and organizations should plan on multiple Active Directory domains simply to overcome bandwidth requirements on constrained network links.
- Expect to supplement any enterprise networked NT Server deployment with third-party tools for at least the next five years in the areas of directory, security and management from vendors such as FastLane Technologies, Mission Critical Software, Entevo, Novell, Aleita Systems and NetPro.