



AberdeenGroup

**Kick-Starting a
Directory-Enabled IT
Infrastructure:
Delegation Rights
Management in Active
Directory**

An Executive White Paper

December 2000

Aberdeen Group, Inc.
*One Boston Place
Boston, Massachusetts 02108 USA
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeem.com*

Kick-Starting a Directory-Enabled IT Infrastructure: Delegation Rights Management in Active Directory

Preface

Even though Windows 2000 was only recently released (March 2000), Aberdeen research indicates that it is more scalable, stable, and secure than Windows NT. In its research report *Proving the Point: Interviews with Next-Generation Windows 2000 dot.coms*, (March 2000) Aberdeen concluded that, under certain conditions, “Windows 2000 looks like a real winner in terms of enterprise readiness based upon significant improvements in reliability, performance, and manageability.” These benefits have spurred enterprises to begin planning and implementing pilots of migration from NT to 2000. Some cutting edge IT departments have already completed worldwide Windows 2000 rollouts, while most firms are evaluating, budgeting, and planning migrations at a cautious — but steady — pace over the next 18 months to 24 months.

Microsoft’s latest server platform is both more complex and more comprehensive than its predecessor, Windows NT. A key network service of Windows 2000 is Active Directory, which expands and enhances the services previously available in Windows NT. Although initial implementations use Active Directory for traditional network operating system (NOS) functions such as user authorization and authentication and resource management, Active Directory’s design is complex and flexible enough to be used as a general enterprise-scale directory and as a platform for directory-enabled applications. In fact, Microsoft is counting on Active Directory as a central integration point for its .NET services initiative.

In this *Executive White Paper*, Aberdeen evaluates the business benefits of a directory-guided IT infrastructure and reviews the business implications of an Active Directory-based environment. This *Paper* strongly advocates including Active Directory administration and management strategy in the NT-to-2000 design and migration process. As an example of a solution for managing the delegated administration capabilities of Active Directory, this *Executive White Paper* discusses DM/ActiveRoles from FastLane Technologies, Inc.

This *Executive White Paper* is intended for organizations considering, planning, or migrating to Windows 2000 and Active Directory. It is most relevant to two audiences:

- Firms with 1,000 seats or greater of Windows 2000 products and
- Firms with a desire to create a tightly controlled Active Directory environment with predictable service level agreements.

Executive Summary

The benefits of a directory-enabled IT infrastructure are well known. These benefits include centralized management of data common to many applications, delegated administration capabilities, automated network provisioning of employees and partners, and improved security. The introduction of Windows 2000, and its

Active Directory component, has forced enterprises to adopt a directory-enabled infrastructure, whether they are ready for it or not. Aberdeen's evaluation of the new platform indicates that the increased reliability and performance qualities of Windows 2000 are compelling enough to drive adoption for a wide number of uses by a broad range of industries.

The challenge for organizations adopting Windows 2000 and Active Directory is to manage its complexity while leveraging the network services it provides for the highest return on investment. Given the dependence of the NOS environment and other applications on Active Directory, directory administration and the management of the directory objects are absolutely critical to successful Windows 2000 deployments. Aberdeen research indicates that several early adopters are now paying a high price for not including administration and management planning in the directory design process.

While Microsoft provides basic tools that are sufficient for small or out-of-the-box Active Directory deployments, third-party solutions are required to access the full range of Active Directory's capabilities. Firms undertaking Windows 2000 migration have two choices:

1. Purchase tools from suppliers who have extended their Windows NT toolset. These products require little retraining and closely match existing tools. However, they may also transfer some of NT's design limitations or create external points-of-failure in the new fault tolerant Active Directory environment.
2. Purchase tools from suppliers that have redesigned their products from the ground up for Active Directory. These tools focus on administration and management, leaving authentication, data replication, and inter-network communications to Active Directory. However, they may require new technical skills and management techniques.

The second option provides a strong example of efficiencies gained from directory-enabled applications. Aberdeen research indicates that a large number of software and hardware suppliers are quickly integrating a directory-enabled architecture in their product roadmaps. Enterprises can also receive a competitive advantage — in terms of faster time-to-market, lower administration costs, better partner and customer communications, and higher cross-application interoperability — by embracing a directory-enabled IT infrastructure. The relative newness of this approach, though, means there is a shortage of experts in the field. Therefore, enterprises should leverage the expertise and experience available by starting with directory-enabled products from directory-focused suppliers.

A prime example of both a directory-enabled application and a product designed specifically to manage and administer Active Directory is DM/ActiveRoles from FastLane Technologies, Inc., a division of Quest Software. Aberdeen finds this

product to be blazing the trail of directory-enabled applications with decreased development time and increased cross-enterprise flexibility. The three key benefits of DM/ActiveRoles for Active Directory administration and management are that it:

1. Simplifies Active Directory management and administration through customized templates that allow easy delegation of rights and tasks;
2. Provides an intuitive, graphical map of Active Directory's delegated administration rights in the Microsoft Management Control console; and
3. Enables complete auditing of all Active Directory access controls.

Benefits of a Directory-Enabled IT Infrastructure

With almost all Windows 2000 rollouts, enterprises will also implement Active Directory. Aberdeen research shows that most initial Active Directory deployments are primarily to support the NOS environment. At the same time, these enterprises recognize an enterprise directory's future use will extend far beyond simple operating system and network services. They understand that the Active Directory deployment is the first step towards a full-blown, directory-enabled IT infrastructure that will provide:

- *Centralized Content Management:* Objects stored in a central directory can be tracked and managed across the entire organization as opposed to a long, involved hunt-and-gather mission to find perhaps conflicting information about object relationships inside different applications.
- *Delegated Administration:* Even though the data is consolidated, enterprise directories allow for granular delegated control of data administration and management. For example, enterprises can delegate management to human resources for control over the hiring, firing, and salary data; to network administrators for control of access rights and firewalls; and to accounting for control of purchasing information.
- *Mass e-Provisioning:* A directory-enabled infrastructure can automatically create or disable employee or client accounts, triggered by a provisioning program that grants rights by category or group. This function eliminates the need to enable every new hire or disable every departing employee in each and every application. Some firms are extending the use of e-Provisioning to include issuing telephone access codes and wireless device access, assigning office space, and configuring PCs based on an individual's business function as described by the directory.
- *Increased Security:* Directories can store public key infrastructure (PKI) certificates and use these certificates to authenticate users across the enterprise. Also, several independent software vendors (ISVs) are designing directory-enabled applications such as intelligently permeable firewalls and single sign-on applications.

- *Cross-Application User Administration:* Directories consolidate user information from many directory-enabled applications for a unified view of each employee, customer, or partner for more coherent and informed monitoring and management.
- *Customer and Partner Relationship Management:* Directory-based user management increases the speed and reliability of creating, monitoring, and analyzing e-Commerce relationships beyond the customer's firewall. For business-to-business (B-to-B) environments, a firm can specify which resources will be exposed to which partners and when, while monitoring how these resources are used — all at a granular and verifiable level.

Microsoft recognizes the exponential benefits of an integrated directory infrastructure. Microsoft itself is leveraging Active Directory's availability, redundancy, and security features for Microsoft's .NET initiative, which includes Windows 2000, Exchange 2000, and SQL Server 2000. In addition, Microsoft promotes the development and usage of Active Directory-enabled applications.

One Plus One Equals Three with Directory-Enabled Infrastructure

Active Directory is "an essential and inseparable part of the Windows 2000 network architecture, ... a directory service designed for distributed networking environments" ("Active Directory Overview," Microsoft Corporation, June 1999). As this quote indicates — in Windows NT/2000 environments — Active Directory is the nexus of networkwide manageability, security, and interoperability.

As a core component of Windows 2000, Active Directory not only provides the benefits listed previously, it delivers an effect greater than the sum of the individual parts. As an enterprise directory like Active Directory stores more objects, integrates more applications, and coordinates more interactions between users, applications, and devices, the information stored in the directory increases in value. The directory quickly becomes a business-critical application, where the enterprise's operation is dependent on the directory's efficient and effective operation. Figure 1 depicts the network services that Active Directory supplies for various applications and devices.

Business-Critical Qualities of Active Directory

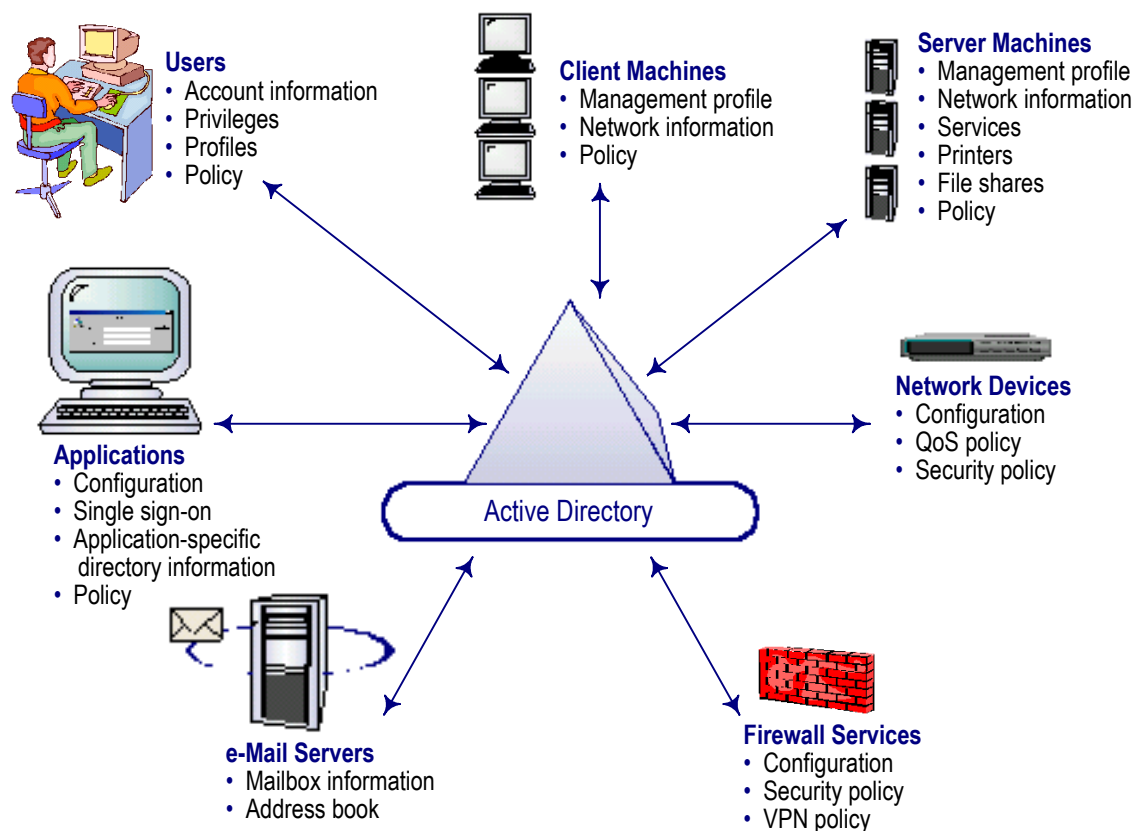
Given its expanded responsibility, Active Directory possesses three benefits required by any enterprise-scale directory:

1. *Reliability:* Because Windows 2000 and multiple other applications will depend on Active Directory for operation, it must have rock solid, 24x7x365 reliability. Active Directory's distributed, hierarchical domain structure and multimaster replication model ensure it will be accessible both locally and remotely. Barring a networkwide shutdown, as long as the application is connected to the network, it will be able to access Ac-

tive Directory's services. The multimaster model, where each instance of the directory can be the "master" or the "slave" on a directory-object level, allows local changes to be transmitted to other instances of the directory and also allows distributed management capabilities.

2. *Flexibility*: Active Directory can adapt to changing network infrastructures and still maintain manageability as it scales from very small to very large. Its architecture allows schema extensions to integrate with existing applications and to facilitate intra- and inter-company communication. The flexibility allows Active Directory to support business models in various industries, from financial services and e-Businesses to traditional manufacturing and academic institutions, all of which have different constituents, infrastructure designs, and directory dependencies.
3. *Interoperability*: To be as open as possible to other applications and resources, Active Directory is based on Internet-standard technologies, such as the lightweight directory access protocol (LDAP), Kerberos, and hypertext transfer protocol (HTTP). Using open standards allows ISVs to hook into Active Directory for user authentication, device configuration, and other functions not core to their applications.

Figure 1: Active Directory in an Enterprise Network



Source: Microsoft Corp., May 2000

Delegated Rights Administration Causes Distinct Management Challenges

Even though Active Directory consolidates network objects into a single consolidated store, it is unreasonable — and unscalable — to expect one group of administrators to manage the entire directory. One department at a U.S. headquarters cannot be responsible for administering an entire multinational corporation. With Active Directory, network administrators can delegate administration to individuals or departments within the separate domains. Local department administrators can be authorized to create and change passwords for that department's personnel.

Management delegation is possible because Active Directory uses a hierarchical domain structure. Unlike Window NT domains — where each domain has a Primary Domain Controller (PDC) with multiple Backup Domain Controllers (BDCs) and administrators in each domain had either all or nothing access — Active Directory design follows a tree-like structure, much like the Windows Explorer model for organizing files. Domains still exist in Active Directory; however, they can be linked together much more easily. This architecture allows an enterprise to build a directory topology that matches its organizational chart or business topology. Figure 2 depicts a typical hierarchical topology.

This design allows for a more scalable distributed management model. Instead of all or nothing access, as in NT domains, Active Directory administrators can delegate responsibility to the individuals most appropriate for the job from a business-level perspective. This capability is essential for providing the flexibility, availability, and interoperability previously discussed.

Organizational Units Increase Flexibility and Complexity

An important design component of Active Directory is Organizational Units (OUs). OUs allow directory objects to be grouped together and then managed as a single unit. For example, users can be placed into a single OU that reflects their administrative boundary. A help desk group can be given the rights to add new accounts, reset passwords, and manage group memberships for this OU. As users and groups are added to this OU, the help desk group automatically acquires the appropriate rights over the new objects.

OUs increase the scalability of Active Directory in that administrators do not need to manage each individual directory object. Group policies can also be applied to the OU and are automatically applied to any object within the OU. Also, individual objects can be added to a specific OU and automatically have the group policy applied to them.

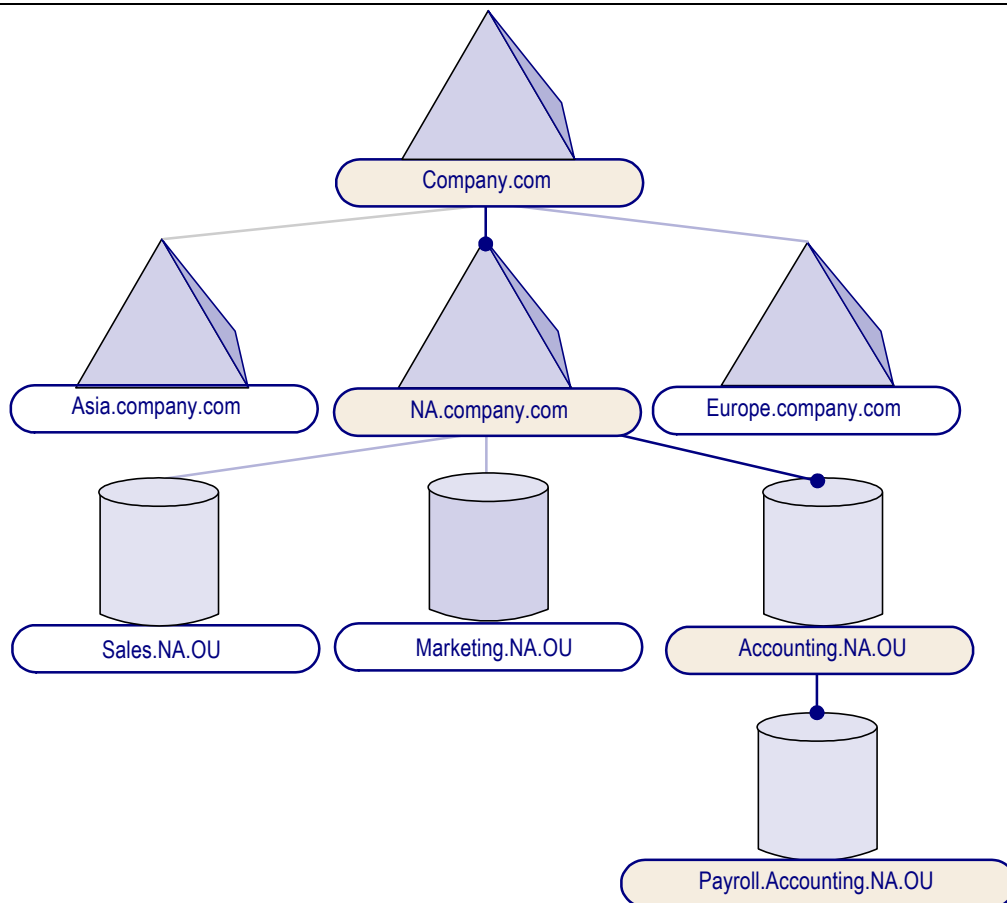
The use of OUs for delegation of administration is a key feature that is being used pervasively among the recent adopters of Active Directory. Administration responsibility can be delegated to give specific individuals control over specific OUs. The

hierarchical model also allows for delegation to be inherited down the tree so that control can be granted for entire domains, specific parts of domains, or OUs within a domain. Active Directory's capabilities are robust enough that management can be delegated all the way down to the individual object or attribute level. The native Active Directory delegation model also provides robust self-service functionality, so that each employee can be responsible for entering and updating his or her own contact information.

Make Delegated Administration Work *for* You, Not Against

A potential downside to this delegation model is that, as more rights are delegated to a wider group of administrators, it becomes increasingly challenging to manage and maintain those delegated rights. Distributed management means distributed control and distributed responsibility. Active Directory provides a large number of objects and each object has a large number of associated attributes. The sheer volume of Active Directory objects and attribute rights poses unique challenges for Active Directory customers.

Figure 2: Typical Active Directory Hierarchical Topology



Source: Aberdeen Group, December 2000

For large, distributed firms with complicated organizational topologies, managing rights delegation is a critical concern not to be taken lightly. Without strong, reliable management tools, enterprises increase their security risk as more individuals are involved in overall management. A department administrator forgets to rescind access rights for a disgruntled former salesperson who, post-pink slip, purposefully alters sales records. A busy IT technician grants temporary rights to her assistant to manage a specific OU, but that assistant does not have the requisite security level to access the information.

Basic Management Tools from Microsoft = Sufficient for Some, Not for Others

Microsoft does provide some basic management tools for delegating responsibilities, managing user and group permissions, discovering management hierarchies of the various OUs, and monitoring security settings. However, these tools are limited in their scope with somewhat nonintuitive user interfaces. None of them provide a graphical representation of the rights hierarchy, and significant manual effort is required to use these tools.

Microsoft's tools are well suited for basic Active Directory deployments where a small group of administrators can use the tools to enhance their institutional knowledge of the business relationships and rights access. When searching for specific relationships or delegation paths, these organizations do not have a large number of potential combinations to sift through. With the combination of the administrator's expertise and the Microsoft tools, security rights delegation paths can be divined and actions can be taken.

However, Microsoft's tools are not sufficient in more complex or very large environments. The complexity of the Active Directory access control model requires simplification to enable an administrator to relate the business requirements of the enterprise to the technical settings within Active Directory. Without such a tool, administrators may spend hours or even days after a security breach tracing the delegation paths of particular access hierarchies in order to determine which specific administrative capabilities a user has over the directory.

New Administration Tools Needed for a New Architecture

Given the relatively recent release of Windows 2000 and Active Directory, it is not surprising that some aspects of Microsoft's native tools are challenged to meet the need of large enterprises. Microsoft had a monumental task not just in upgrading its operating system, but also in developing the interrelationships of the OS with the directory. The tools provided by Microsoft meet the basic needs of knowledgeable network architects.

However, with the delegated management structure, network architects are not the only individuals within an organization who need access to the management and administration tools. For example:

- Department level administrators need to be able to investigate and resolve local problems, create and modify OU permissions, and add users, groups, and computers to their part of the network.
- Help desk workers need to be able to change passwords, assign individuals to existing groups, and troubleshoot Active Directory-related issues themselves.
- Application developers need to be able to directly manipulate directory objects during application development and deployment.

The features that make Active Directory reliable, flexible, and interoperable — multimaster replications, distributed management, etc. — are the very same features that create a complex labyrinth of access rights, dependent users, and network protocols.

Several ISVs from the Windows NT management space have developed management tools for Active Directory. These suppliers have two potential approaches when developing these tools: Adapt existing products for the new operating system and Active Directory or create new products from scratch specifically designed for Active Directory.

Adapting NT Domain Tools for Active Directory

Suppliers that adapt existing NT domain tools for Active Directory provide products with familiar interfaces and similar functionality. Most of these products provide a compromise solution to manage Active Directory domains in conjunction with the NT domains.

Unfortunately, adapted tools carry many limitations of NT into the Active Directory. The primary limitation is the fact that adapted tools do not respect the native Active Directory security model. Because NT is a flat domain system instead of a hierarchical domain, there are no delegated rights to track. To enable delegated administration, third-party NT management tools need to create an imposed, proprietary delegation infrastructure and maintain the information with the application — typically in a separate database.

If an enterprise uses a proprietary delegation infrastructure to manage Active Directory, it removes the option of using the native object management tools provided by Microsoft. In addition, the proxy-server approach compromises Active Directory's availability. It introduces a single point of failure into the network where, if the management proxy-server goes down, no one can administer the directory. NT management tools cannot dynamically extend to manage new objects and object attributes, which limits Active Directory's flexibility.

Adapted NT tools impose an unnecessary administrative layer between the administrator and Active Directory. In the name of delegated administration, these ap-

plications require that users go through proprietary interfaces in order to manage directory objects. Active Directory, though, already contains delegated administration capabilities.

New Management Tools Designed for Active Directory

Active Directory's multimaster model provides more scalability and availability than Windows NT ever offered. By embracing the new features of Active Directory, new management tools can address several requirements particular to the Active Directory environment:

- *Manage Access Control Lists:* Active Directory management tools must be able to locally group, grant, track, and represent the delegation rights to administrators. This ability will allow managers to proactively manage the directory with health checks and access verifications.
- *Expose Access Control Complexities with Graphical Interface:* To simplify management and enable quick audits of delegated rights, an Active Directory management tool must be able to visually represent the relationships within the Active Directory.
- *Respond to Changes in Active Directory:* Active Directory management tools must respond to schema or attribute changes made to the directory. Without this responsiveness, the enterprise would need to go back to the ISV whenever a change was made to Active Directory's design. Instead, the enterprise should choose a management tool that can be easily modified or, even better, can dynamically detect changes to Active Directory's structure and include them in directory management.

Include Active Directory Management in Migration Planning Process

Whether using an adapted or specialized management application, any enterprise understands the importance of tightly managing Active Directory. Based on the experiences of Active Directory early adopters, Aberdeen strongly recommends that enterprises include Active Directory management as part of the overall Windows 2000 migration and implementation strategy.

Many early adopters of Windows 2000 paid considerable attention to the administrative lockdown of the directory during the migration from Windows NT domains. Given the technical — and political — complexity of Active Directory design and migration, it is understandable that companies would want to simplify the migration process by incrementally increasing the number of users in Active Directory while maintaining a tight administrative regime.

While increasing the complexity of the migration planning, businesses must manage their design and migration for two main reasons:

1. The enterprise must be able to meet service level agreements (SLAs) with customers during the migration. The help desk must continue to respond to incoming customer requests. Without an integrated management plan, the enterprise will not be able to meet SLAs for applications that are shifted from NT to Active Directory during the migration.
2. The enterprise must maintain security of directory data during the migration. Management tools imposed after the migration leave the directory exposed for a period of time, which in some cases may be short (a few hours) and others very long (several months). Including management in migration planning allows firms to delegate rights management before the directory is populated, decreasing the risk of exposure once the data migration begins.

Active Directory Management Leads Move to Directory-Enabled Applications

Active Directory-enabled management tools demonstrate how directory-enabled applications can leverage a centralized enterprise directory in the Windows 2000 architecture. Application developers do not need to recreate replication and logging functionality. Directory-enabled applications can store their own rules and policies in Active Directory itself. Active Directory then takes care of replicating additions or changes throughout the network. Thus, these new directory-enabled management applications inherit the fault tolerance inherent to Active Directory.

An example of this type of exploitation of Active Directory's architecture comes from an ISV with substantial Windows NT and directory experience: FastLane Technologies. FastLane has taken a full step toward appreciating the complexity and comprehension of Windows 2000 by dropping its native NT designs to create new Active Directory-focused management products that use native Active Directory facilities.

Aberdeen research indicates that adopting tools and applications based on Active Directory will grease the skids for more Microsoft and ISV directory-enabled applications later. Advances in Active Directory deployments create the opportunity for stronger tools and the value of role management. Aberdeen strongly encourages firms to consider adopting directory-enabled management applications, rather than remain tied to the management products that arose from Windows NT.

FastLane Technologies Builds on Active Directory

Initially founded in 1993 to assist in the management of Banyan's StreetTalk directory, FastLane Technologies (a division of Quest Software) soon expanded its focus to support the growing Windows NT environment. Today, FastLane provides enterprise directory management products and professional services primarily for the Windows NT, Windows 2000, and Exchange 2000 environments. FastLane also provides products and services to plan, deploy, and manage migration from Window NT to Windows 2000 and from Exchange 5.5 to Exchange 2000.

In June 2000, FastLane became a wholly owned subsidiary of Quest Software, a provider of management and monitoring software for business-critical applications. FastLane operates the Microsoft solutions unit of Quest Software.

Recognizing the complexity of directory management, FastLane developed the DM/LifeCycle, which addresses the planning, consolidation, migration, and on-going administration demands of NT and Active Directory environments. FastLane's products address these steps as part of the DM/Suite: DM/Administrator, DM/Consolidator, DM/Developer, DM/Manager, and DM/Reporter.

DM/ActiveRoles: 'Role-Based Administration for Active Directory'

FastLane's newest product, DM/ActiveRoles, is specifically designed to simplify and enhance the management of Active Directory. The product untangles the spider's web of delegated administration rights into a straightforward graphical representation of the administrators, the objects for which they are responsible, and the associated security settings that are applied to those objects. As a snap-in module to the Microsoft Management Console (MMC), network administrators can use the familiar MMC user interfaces.

In addition to exposing attributes of Active Directory, DM/ActiveRoles goes one better. This product allows administrators to create templates for delegation rights and apply them to new or existing objects within Active Directory. FastLane has created a list of typical "roles" for administrators or directory objects, called "ActiveRoles," but enterprises can extend and modify existing roles as necessary.

The objects and attributes within DM/ActiveRoles reflect the directory schema of the particular business. Any additions or new object classes in Active Directory are automatically reflected within DM/ActiveRoles. The additions are then available to be included in any ActiveRole.

While DM/ActiveRoles manages objects in the directory, it fully leverages the replication and object management capabilities of Active Directory. Figure 3 depicts the relationship between DM/ActiveRoles and an Active Directory environment.

Organizations using DM/ActiveRoles experience several major benefits:

- DM/ActiveRoles decreases Active Directory management costs in that the number of administrators needed to manage users and resources is less than when using native Windows 2000 tools.
- Because administrators can graphically view complex rights relationship within Active Directory, DM/ActiveRoles decreases the occurrence of improper or inaccurate rights delegations in Windows 2000 environments.
- The graphical view also improves network security, because the overall organization's rights delegation topology can be monitored.

- ActiveRoles templates allow firms to accelerate the rate at which they can take advantage of Active Directory's inherent delegation capabilities.

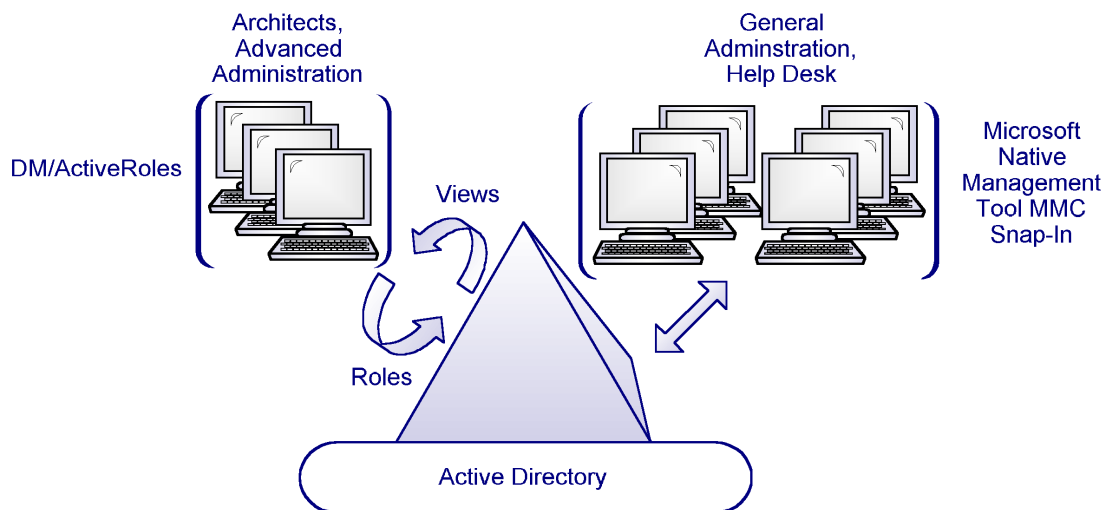
Aberdeen Conclusions

The promise of directory-enabled applications has been widely touted for many years, if not decades. However, the implementation, scale, and administration challenges of a directory-guided IT infrastructure has prevented mass adoption of the technology. Instead, directories have been deployed to support specific applications or to underpin a network operating system.

With Active Directory, Microsoft is on the verge of realizing the potential of enterprise-scale directories. Aberdeen predicts that a mass adoption of Windows 2000 will finally cause enterprisewide adoption of a directory-guided IT infrastructure, given the interdependencies of the operating system and the directory. Even though early deployments of Active Directory serve primarily to support Windows 2000 servers, third-party application developers and even Microsoft itself are employing a centralized directory design in other applications such as Exchange 2000. Microsoft's recent .NET initiative relies heavily on a completely and properly deployed Active Directory infrastructure.

Aberdeen recommends that, when evaluating Active Directory management applications — or any directory-enabled applications, for that matter — enterprises should look for applications that leverage the directory's native functionality. FastLane's DM/ActiveRoles is one such product. DM/ActiveRoles can help firms

Figure 3: DM/ActiveRoles and Active Directory



Source: FastLane, September 2000

increase enterprisewide communication and collaboration by diffusing the complexities of Active Directory's rights delegation process. FastLane leverages Active Directory's capability for multimaster replication and delegated rights management to provide a solution with low implementation costs and short deployment time. The concept of "roles" as embodied by an "ActiveRole" is an important one. Administering Active Directory through "roles" can significantly simplify the delegation and administration of management rights within Active Directory. The fact that DM/ActiveRoles can dynamically manage objects that are added to Active Directory structure is a definite benefit. The mechanism of storing the 'role' definitions in Active Directory allows for local access of the role definitions to administrators at the business unit level.

Aberdeen recognizes that the new architecture of Active Directory presents drastically different management requirements from the previous Windows NT environments. The hierarchical structure imparts the need to manage the rights delegation within the organization. While Microsoft's tools are adequate in some cases, enterprises will need applications developed by third-party software suppliers in order to simplify and clarify delegation rights management within Active Directory. These firms should consider FastLane's DM/ActiveRoles as a fully directory-enabled Active Directory management application.

*Aberdeen Group, Inc.
One Boston Place
Boston, Massachusetts
02108
USA*

*Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com*

*© 2000 Aberdeen Group, Inc.
All rights reserved
December 2000*

Aberdeen Group is a computer and communications research and consulting organization closely monitoring enterprise-user needs, technological changes and market developments.

Based on a comprehensive analytical framework, Aberdeen provides fresh insights into the future of computing and networking and the implications for users and the industry.

Aberdeen Group performs specific projects for a select group of domestic and international clients requiring strategic and tactical advice and hard answers on how to manage computer and communications technology.