

Managing Complex Enterprise Windows Networks Requires Research, Planning, and the Right Tools

By MARTY SCHER

You probably would not be surprised to learn that enterprise Windows networks are becoming increasingly more complex to design, implement, and manage. Many Windows NT veterans will remember when

designing an enterprise NT network was mostly a matter of specifying domain trusts and group memberships. Implementation was not much more complex than installing a domain controller at each site and management required only proficient use of User Manager and Event Viewer. But times are changing. Companies are finally planning migrations to Windows 2000 servers and the Active Directory (AD) service. And with the release of Windows XP, we now have a Windows client with more features, functionality, and complexity than ever before. In addition, many IT departments migrating to AD may also be contemplating upgrading back office systems, including migrating messaging systems to Exchange 2000. To best handle the complex nature of implementing and managing these new technologies, you might find it worthwhile to prepare designs and to research tools and methodologies so that you ensure implementation of a well designed and secure Windows network.



Educational Resources

As your company prepares for the upgrade to Win2K and the implementation of AD, your understanding of AD will be crucial. Many resources are available to educate yourself about AD and the knowledge you gain will ease the decision-making process during the design phase.

A good starting point for gathering information about AD is the Web. One of the best places to start is the Microsoft Web site, which offers white papers that outline AD technology and network design considerations. You will find many other Web resources, including user discussion forums where you can post questions or search for solutions about specific topics.

Another valuable Web resource is case studies, which offer a quick way to gather information, evaluate products, and learn about successful business solutions. Microsoft, for one, has learned the value of showcasing how you can combine and integrate the company's multitude of individual products to create a customized business solution. Microsoft has devoted generous Web site resources to offer hundreds of case studies indexed by solution or industry type. Most of the case studies use a similar format, which usually outlines a particular customer's needs, some possible solutions, what the final solution was and the achieved results. Browsing through these case studies may yield ideas to solve your particular needs and can be a valuable part of any system design process.

In addition, several publishers offer books that step you through the nuances of AD. And Microsoft offers the "Domain Migration Cookbook," which you can download at <http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/cookbook.asp>.

Migration Tools

After you've completed the AD design phase, tools are available that can make

migration less nerve-wracking and ensure that your once rock-solid NT network will now be a rock-solid Win2K network.

AD migration tools are available for every need, with both features and prices rising in a linear fashion. At the low end (free), Microsoft offers an AD Migration (ADM) tool that is stable, but that may lack some of the enhanced features of third-party tools. At a caliber higher than most of Microsoft's free utilities, the ADM tool (a product licensed from Mission Critical Software-<http://www.missioncritical.com>) contains enough features to complete many NT domain-to-AD migrations, and it is relatively easy to use. For companies whose migration plans are extremely complex or have additional requirements, the enterprise-scale package Controlled Migration Suite from Aelita Corporation

AD migration tools are available for every need, with both features and prices rising in a linear fashion. At the low end (free), Microsoft offers an AD Migration (ADM) tool that is stable, but that may lack some of the enhanced features of third-party tools. At a caliber higher than most of Microsoft's free utilities, the ADM tool (a product licensed from Mission Critical Software-<http://www.missioncritical.com>) contains enough features to complete many NT domain-to-AD migrations,



(<http://www.aleita.net>) contains additional functionality and features (such as total migration backout and enhanced reporting). Tools are also available for NetWare and Exchange migration.

Larger, more complex networks may benefit greatly from advanced features, including enhanced premigration resource discovery and post-migration reporting, that many third-party tools offer. The bottom line is that having any tool will greatly reduce the AD migration time and effort for Windows networks.

Management Tools

The migration to AD and consolidation of network objects won't eliminate the need to manage these resources and, in fact, may increase the need, as you migrate once-separated domains (and



all their resources) to AD. The managed client count may increase and you may need to manage security centrally. One of the biggest hurdles to overcome in managing clients is controlling and updating software applications. Today, applications become outdated in months, not years, and software patches must be implemented regularly. Without an automated software distribution process, implementing software patches can mean a lot of legwork for small networks and be nearly impossible in larger networks.

If your problem is the distribution of applications or patches only, some powerful, reasonably priced tools exist. Prism Deploy, from Lanovation (<http://www.lanovation.com>), is designed to create application install packages and distribute these packages to clients according to a schedule. When these tools are used properly, thousands of clients will have software upgrades in a matter of hours, in stark contrast to having to install these upgrades via sneaker net.

Another need when supporting clients is “being there” to assist in system troubleshooting or user training. This issue is compounded when you need to support a client at a remote location. Remote control packages, which have been available for many years, give you the ability to connect remotely to another PC (attended or not) and have total control as if you were sitting in front of the PC. One of the most popular tools for managing remote clients is

PC Anywhere from Symantec Corp. (<http://www.symantec.com>). With this tool, a support person can “take over” a remote PC screen, having total system control, if needed, to perform troubleshooting or assist a user.

Many third-party tools offer added features, such as improved file transfer, and tighter, domain-level security. Windows XP offers the remote desktop, which allows similar remote control functionality and can be very useful if, for instance, you need a specific application that is not installed on the XP client where you are sitting.

Other useful tools are those that manage client software inventory and software licenses. You can purchase such tools separately or as part of a suite. If your requirements (and budget) warrant, you can get the functionality of all the above tools (and many others) in one package: Microsoft’s Systems Management Server (SMS). Although SMS might require more administrative resources, it packs the power and scalability to manage windows clients and servers in numbers that could be in the thousands or tens of thousands. SMS is an enterprise-ready management tool and one that is constantly evolving to keep pace with other emerging Microsoft technologies, such as .NET.

Managing Security

Until recently, Windows network and user security was possibly one of the most under-managed technology areas for many companies. Mainframe and midrange systems were usually pretty tight; but often, Windows networks operated with a kind of implied trust, in which rights for folder access or assigning domain administration rights were simply doled out upon request.

Today, companies are finding it increasingly important that security be managed thoroughly – and, most likely, centrally – from the smallest networks to enterprise NT/2000

networks. A multitude of security management tools are available, with various prices and features. One tool for managing enterprise security is NetPulse 2000, from Labcal Corp. (<http://www.labcal.com>). NetPulse gives you the ability to configure the most user security settings within a single software application. NetPulse lets an administrator define a security policy and approve values to control user access. This application also includes security analysis utilities, which can scan user accounts and resources to determine levels of security. Enhancing network security and defining security policies should be a top priority in all Windows networks.

If the job of building (or upgrading) an NT/2000 network seems daunting, feel fortunate that many tools and resources are available to assist you every step of the way. Doing the homework during an AD design phase will reduce or eliminate many surprises during implementation or migration. Take advantage of someone else’s experience by researching case studies for your needed solutions. Use AD migrations tools to ease the transition. Long-term management does not have to be a nightmare, if the proper tools that fit your needs are implemented and used regularly. Improved security is in everyone’s best interest, so get to work defining, implementing, and enforcing these much-needed policies. ■

About the Author

Marty Scher

(martyscher@earthlink.net), an Information Technology manager for Fleet Credit Card Services, has more than 15 years of computer and network experience. He is also a freelance technology writer and product reviewer, covering Microsoft technologies and digital photography.