

Microsoft®

Solution guide

Getting a Quick Start with Active Directory

By Mike Spacey

Windows 2000 Server provides many benefits in addition to those offered by Windows NT 4.0, and even more benefits are available to organizations that deploy Active Directory. For instance, Win2K improves a number of features that existed in NT4 (e.g., disk administration and unattended installation) and adds many more: for example, file system enhancements such as encryption, user quotas, and mounted drives; Terminal Services; remote storage; plug and play; a more powerful command line; and a powerful scripting environment.

Add an AD structure, however, and you enable powerful tools for reducing total cost of ownership (TCO). Remote Installation Services lets you publish customized installations of Win2K over a network. The Installer Service can deploy applications automatically to users or computers from a central point based on Group Policies. Some of the best features of Distributed File System (DFS) depend on AD. Enabling AD makes it possible to organize servers and workstations so that

you can delegate computer and user account administration — an invaluable capability for managing large networks.

In other words, AD enables some of the best features that differentiate Win2K from NT4. If that's the case, why don't all networks using Win2K have AD in place? The answer is, simply, complexity of planning. AD requires proper planning to ensure effective deployment and this planning takes time.

AD Planning Challenges

Although planning an AD structure for a small network isn't too difficult, organizing a network into domains, organizational units, sites, and so forth is much more complicated for larger networks. And larger networks are the ones that really see the benefits of AD. Because reworking an AD structure, or any directory structure, after you've deployed it is problematic, you need to do it right the first time.

When a woman once asked Louis Armstrong to define jazz he replied, "If you have to ask, you'll never know." The same answer might apply to the question of why planning an AD structure is a challenge: If you don't know the pieces well enough to see why it's complicated, then it's impossible to appreciate the complexities of the task.

If you're unfamiliar with AD, you must come away with one point: AD is not just a bigger version of an NT4 SAM database. Both have domain controllers and user and machine accounts, but AD is more advanced because of its multi-level structure. In NT4, an account is in a group, and that group is part of a domain. If you want to change the way someone can use the network, you change the rights or permissions of that group (or, more rarely, the permissions of an individual account). Tweaking rights and permissions may not always be easy, and making domains

trust each other so that members of one domain can use the resources contained in another domain can be complicated, but the basic components are simple: individual accounts, groups, and domains.

Added Benefits of AD

With AD, you still have user accounts, machine accounts, groups, and domains, but you also have organizational units and sites. Organizational units (OUs) are key both to management delegation — you can make them into subdomains — and to the use of group policy objects for change and configuration management, because GPOs apply to OUs, domains, or sites, not to individual accounts or to groups. OUs and groups are not mutually exclusive; you will work with both to manage different aspects of the network. Sites are physical organizations of the network that you can apply to minimize network traffic and speed routing between subnets in the network. And that's just within domains — AD domains may be part of superstructures called trees (nested domains) or forests (groups of trees).

Even the parts of AD that you thought you recognized from NT4 are different. In NT4, you couldn't nest groups: local groups could contain global groups, but that was it. Win2K supports nested groups. In NT4, domains did not automatically trust each other and there were no transitive trusts. To extend trust between any two domains, regardless of their relationship with other domains, required a carefully timed two-step process of domain A permitting domain B to trust it, then making domain B trust domain A — and then reversing the whole

process to make domain A trust domain B, because trust one way did not imply trust the other way. AD trusts within the same tree are automatic.

Consider a simple example. You're designing an AD structure for a company with offices in Seattle, New York City, and New Milford, Connecticut. Seattle and New York have high-speed WAN access, but New Milford does not. Should you use sites to organize the subnets, and if you do how will this affect network traffic? Some people working in the New Milford office work with people in New York. Do you use groups or OUs to manage these separated teams? Should the people with administrative privileges for the Seattle office be able to manage the servers in the New York and New Milford offices? If not, how will you organize the network to share information without compromising the security at each office? Do you want to organize the network into a single domain, or should the network be organized into multiple trees, or even multiple forests? What if the rumored addition of a Johannesburg office takes place — how will you handle that? And just how does that Novell server fit into the equation?

Finding Some Help

Do you have answers? Good. Now comes the hard part: Can you justify those answers to your peers and bosses in the other two offices?

Unless you have more spare time than most people to study the pieces of AD and your company's organizational and political structure, you would probably welcome some help identifying and designing your company's AD

structure. One source of help is Microsoft's QuickStart program.

Addressing Deployment Barriers

The MS QuickStart program has been developed to help customers — a Microsoft survey shows that three-quarters of the Win2K clients are in the process of deploying AD — overcome barriers to deployment for various Microsoft enterprise offerings. The program combines the experience of Microsoft Consulting Services and Microsoft Partners in deploying Microsoft technologies with a prescriptive, fixed-price, fixed-term packaged service. These highly structured and efficient consulting engagements are designed to help customers determine if Microsoft products and technology can meet their needs, and then to accelerate the deployment process while minimizing risk. Programs are available to address both the evaluation of, and planning for, Win2K and AD deployment:

- The Microsoft QuickStart for Evaluating Windows 2000 Service is a pre-sales workshop designed to assess a customer's needs and determine if Win2K and AD are the right solution.
- The Microsoft QuickStart for Planning Windows 2000 Service provides fixed-duration, packaged services that rapidly produce a first-pass architecture design, identify risks for full deployment, and provide the transfer of knowledge to the customer's IT staff by involving them in critical key decisions around AD, networking, and security.

Typically, when a customer chooses the MS QuickStart program the process works something like this.

The project begins with a review of the business requirements and an agreement about the vision and scope of the project. The customer might already have identified specific project criteria and these must be considered in the context of the business objectives. Establishing the vision and scope focuses the project to produce more valuable results, in less time and with less risk.

Then, one or two Microsoft and Microsoft Partner consultants guide the customer's IT staff through a structured consulting services engagement focused primarily on transferring knowledge and identifying risks. The consultants work with the customer's IT staff in a series of technical design sessions over a four- to six-week period. In addition to transferring knowledge, these sessions lead to creation of a high-level architectural plan that addresses important key decisions related to AD, networking, and security. This stage of an implementation is extremely important because the amount of time and focus spent on planning may determine the success or failure of the overall deployment project. Interoperability with existing systems, including the design of an AD structure capable of interoperating with non-Windows servers and clients, as is the case with most enterprise networks today, is also a key deliverable from the project.

The Microsoft and Microsoft Partner consultants document the customer's environment and map the AD structure, keeping the project's executive sponsor and lead IT manager apprised of progress. Time is taken during planning to educate the IT staff about key aspects of Win2K and AD. Unlike general classroom training, these

interactive design sessions focus less on the general understanding of various topics and more on how these topics (e.g., data structures and server configurations, application compatibility, standard operations, and overall issues and risks) apply directly to the customer's workplace. The MS QuickStart program is beneficial both to those organizations and individuals with Win2K experience and to Win2K novices; the difference lies mainly in the time required to establish the appropriate knowledge base with the customer.

The keys to the value of the MS QuickStart program include transferring knowledge, identifying

obstacles and risks, accelerating deployment, and achieving better results through careful, experienced planning. Typically, the overall cost of a MS QuickStart engagement is much less than an ad hoc consulting engagement because the program leverages the experience gained from a large number of deployments, and it is a highly structured engagement, which leaves little room for scope creep. The final deliverable is a complete, high-level architectural plan that documents key decisions made by the customer during the project. This architectural plan provides the CIO with the knowledge needed to scope the remainder of the

Yale's Experience with the MS QuickStart Program

Yale University wanted to build an Active Directory (AD) structure for its 400 servers and 20,000 client computers running Windows NT 4.0 and Windows 2000, but even for their Win2K experts, planning for a network of this size wasn't a simple matter. Technical problems, such as designing the interface with an existing Kerberos 4 infrastructure, stalled the planning and it was important to keep disruptions to a minimum. The number of groups involved in decision-making also complicated the process.

As Nick Rawlings, director of technology and planning for Information Technology Services for Yale, observed, "We tried to plan the structure on our own, but the technical problems we encountered and the need for buy-in from disparate groups over a large number of choices convinced us that we needed outside help. Our best chance for success was to have an independent outsider lead us through the decision-making process. In that way, no one of us won or lost any battle — we all won the war." In this case, the independent outsider was Microsoft, which offered help with the AD planning through the MS QuickStart program.

The entire process took about four months and the implementation of the completed AD structure went smoothly, with no problems. All in all, the program was a success. Yale prefers not to endorse vendors, but Rawlings was pleased that Microsoft participated in the planning process — "It worked for us."

deployment, thus avoiding risks and paving the way for success and a great return on investment.

Moving Forward with Deployment

Once your plan is done and you've received buy-in to move forward, you may choose to contract with MCS or partner consultants (from companies such as Compaq) to manage the actual deployment, work with you to do lab work and test the AD structure, and help to deploy AD. In other words, Microsoft develops the AD structure using the MS QuickStart program, but partner consultants may take that structure and synchronize it with your Human Resources system to draw user account names from new employee records. The consultants are not restricted to using Microsoft software, but may bring in any tools they consider necessary for a successful deployment. From beginning to end, the entire deployment program may take anywhere from a couple of months for a smaller network to perhaps six months for a large one, but Microsoft is committed to making the MS QuickStart program work within the original budgeted cost.

Although the MS QuickStart program has existed for almost a year, it's just now gaining momentum. According to Robert Dring, Microsoft QuickStart Lead, the MS QuickStart program is being rolled out worldwide, with adoption in the U.S., Canada, U.K., Venezuela, Peru, and South Africa.

The MS QuickStart program hasn't been developed solely for Win2K and AD (or Exchange — that's another MS QuickStart program) planning. In coming months, Microsoft will overhaul the material for .NET Server as needed, and the company is considering a short, two-day program to help people migrate from Win2K to .NET Server, if there's anything a consultant can add that more traditional .NET classes cannot. Microsoft has also developed MS QuickStart programs to help customers plan and deploy a secure network.

Why Use the Microsoft Program?

Since the release of Win2K in February 2000, there has been no shortage of consultants willing to help Microsoft customers plan their AD structure. Given that, it might not be immediately clear why you'd use a Microsoft packaged service offering instead of ad hoc consulting. The answer is simple. Microsoft recognizes that it is human nature to add objectives to the original scope of a project, often resulting in longer, more expensive engagements that may not adequately address the original goals. In addition, even experienced consultants may not be familiar with all the nuances of AD planning. The MS QuickStart program addresses both these

If you're interested in finding out more about the MS QuickStart program, go to <http://www.microsoft.com/business/services/QuickStart.asp>.

problems. MS QuickStart is a fixed-price, highly structured, very prescriptive program that delivers the high-level, first-pass architectural design for Win2K. Items that fall outside the scope of the project are documented so that they can be addressed separately and do not derail the effort. Because of MS QuickStart's fixed price, customers will not run into unexpected expenses, and they will get a Win2K AD design based on Microsoft's experience with other customers and backed by the complete Microsoft knowledge base. With the MS QuickStart program, customers receive a solid AD design that meets their business needs from the company that developed AD. Early investment in a great architectural plan will pay off during the rest of the deployment and will provide a higher overall return on the customer's investment in Microsoft technology.

The benefits of AD are one of the main reasons to move to Win2K, but many Microsoft customers — even those using Win2K — find planning the AD structure too complicated to handle in the limited time available. If that's the case for you, consider getting help from Microsoft's QuickStart program. This program ensures that you're taking the time to plan AD, and it lets you benefit from the experience of others when it comes to seeing what problems you might encounter and how to resolve them.

Microsoft®
www.microsoft.com/servers