Realtime
publishers

The Essentials Series: Tackling Active Directory's Four Biggest Challenges

Merging and Restructuring Domains without User Impact

by Greg Shields

Copyright Statement

Merging and Restructuring Domains without User Impact

In a Windows environment, it can safely be said that virtually everything relies on your Active Directory (AD). Every server is a member of AD. Every user stores their identity and credentials in AD. Nearly every group you create makes its home in your AD database. It's this near-universal reliance on AD that makes a Windows environment so critical to your environment, and it's this near-universal presence that makes merging and restructuring it such a pain in the neck.

The problem with AD's native resistance to major change is that businesses are dynamic. They grow, add divisions, merge with other businesses, and manipulate themselves time and time again to keep up with customer demand. As a result, many organizations find themselves merging and/or restructuring their AD infrastructures to follow the business. Microsoft provides a toolset that can handle some of these needs called the Active Directory Migration Toolkit (ADMT), the most recent version of which can be found at http://www.microsoft.com/downloads/details.aspx?familyid=AE279D01-7DCA-413C-A9D2-B42DFB746059&displaylang=en.

The Native Solution

The ADMT arrives as a set of scripts and installed code that manages the migration of objects from one domain or forest to another. Microsoft's ADMT toolkit can migrate user accounts, groups, and computers from a source to a trusted target domain. More complex objects such as Exchange attributes and mailboxes, clusters, application settings, and Group Policies cannot be migrated using this tool and must be copied over manually during the migration project.

To begin using the ADMT, download the tool and install it to a computer, which will become the host point for the migration. It is from this computer where all migration activities using the tool will take place. Either a two-way trust between both domains or a one-way trust from source to target domain must be created to provide the necessary authentication between the two domains.

Depending on the size of your domain, using the ADMT can take an extended period of time. Microsoft recommends that no more than 100 accounts are migrated at one time to keep the migration process manageable with this tool. To ensure that accounts can access resources that are in both domains—those that have and have not yet been migrated—Microsoft maintains historical security identifier (SIDhistory) information about each account throughout the course of the migration process.

Any domain merge or restructurting process will generally follow this list of steps:

- **Create a test plan with actual data.** Prior to beginning any domain merge or restructuring, it is a good idea to first create a completely separate environment to prototype the action. This environment should use data that is equivalent to the data you plan to migrate during the actual event. If you plan to use the ADMT, it can run a test migration of an empty group. It, however, cannot easily generate a complete set of test data.
- **Loosen security restrictions on Domain Controllers.** When merging down-level computers to a new domain whose Domain Controllers run Windows Server 2008, you must first loosen the security on those Domain Controllers. Do this by navigating to *HKLM\System\CurrentControlSet\Services\Netlogon\Parameters* and setting the DWORD value for *AllowNT4Crypto* to *1*.
- **Enable firewall exemptions for File and Printer Sharing.** If Vista or Windows Server 2008 machines in your source domain are using the Windows Firewall with Advanced Security for on-domain connections, create an exemption for File and Printer Sharing. Doing so enables the ADMT agent to properly interface with the client computer.
- **Create the Organizational Unit (OU) structure in the target domain.** This target OU structure can either match the source structure or be different. Such is the case because objects can be migrated into alternate OUs if desired.
- **Enable password migration.** The ADMT itself is unable to migrate passwords directly from source to target domain. Doing so requires the use of the Password Export Server (PES) service, which can be downloaded from http://go.microsoft.com/fwlink/?LinkId=147652. Install the PES service to a Domain Controller in the source domain, and ensure this service is only enabled during the period of the migration. Prior to starting a migration, you must first create an encryption key for passwords using the command *admt key /option:create /sourcedomain:<SourceDomain> /keyfile:<KeyFilePath> /keypassword:{<password>|*}*.
- **Migrate Universal and Global Groups.** Using the ADMT, all domain groups must be migrated at once. This ensures that a closed set of groups and the groups they contain has correctly been migrated from the source to the target domain. This process can be done either through the ADMT's GUI or via the command line with the command *ADMT GROUP /N "<group_name1>" "<group_name2>" /SD:" <source_domain>" /TD:" <target domain>" /TO:" <target OU>" /MSS:YES*.
- **Migrate user accounts.** Due to the closed-set limitations of the ADMT, it is a best practice to migrate all user accounts in the same period. Doing so ensures that no loss of resource access (for example, Exchange mailboxes) occurs during the migration and that all users along with their groups and subsequent users in those groups are correctly migrated. This can be done using the ADMT's GUI or with the command *ADMT USER /N "<user_name1>" "<user_name2>" /SD:" <source_domain>" /TD:" <target_domain>" /TO:"<target_OU>" /MSS:YES /TRP:YES /UUR:NO*.

- **Migrate workstations and servers.** As with user accounts, this should be done in small batches of no more than 100 at a time. The ADMT will reconfigure each computer and reboot when complete. Textual log files are created for each computer on the ADMT computer, one for each computer, in the folder Windows\ADMT\Logs\Agents. Each file should be monitored for success. As with users, it is possible to migrate computers using the command *ADMT COMPUTER /N "<computer_name1>" "<computer_name2>" /SD:" <source_domain>" /TD:" <target_domain>" /TO:" <target_OU>" /RDL:5*.
- **Re-migrate user accounts, workstations, and groups.** As the previous process can take an extended period of time, Microsoft recommends a re-migration of user accounts and workstations to ensure any changes during the migration period are correctly migrated as well. The same holds true for workstations and groups.
- **Clean up ACLs.** For migrations that make use of SIDhistory, migrated accounts will retain old ACL information from the source domain. This information must be translated to reflect the object's interactions with the target domain. Do this with the ADMT GUI or using the command *ADMT SECURITY /N "<computer_name1>" "<computer_name2>" /SD:" <source_domain>" /TD:" <target_domain>" /TO:" <target_OU>" /TOT:Replace*.
- **Migrate other data.** As stated earlier, the ADMT is limited in the types of information it can migrate. The result at this point in your migration will be the movement of accounts, groups, workstations, and some ACLs to the target domain. However, ACLs within applications, mailboxes, and other settings must also be individually confirmed and/or converted to reflect the object's positioning in the new domain. This process involves a manual verification of settings within each of these objects.
- **Decommission the source domain.** Once each of these steps is complete, demote the source domain's Domain Controllers and decommission the domain.

As you can see, Microsoft's ADMT solution provides a rudimentary mechanism for transferring many types of objects out of one domain and into another for a merge or restructuring activity. It can successfully transfer user and computer accounts as well as their privilege information between those domains.

The Need for Better Tools

Yet there are a number of problems inherent to the structure of the ADMT solution. It is designed to be a one-time solution for a one-time problem, enabling the migration of a source domain to a target domain. Merging or restructuring multiple domains requires multiple migration workspaces. If your organization is constantly restructuring itself due to acquisitions and mergers, there is no process for quickly completing the necessary activities. Each migration is a major project in and of itself, with little or no reuse of the effort from the previous project.

Making projects like these even more challenging are their potential for impact on your users. With each migration is also the virtual assurance that users will experience downtime associated with the move. During the migration, users can lose access to un-migrated resources, or even the use of their accounts entirely.

It is for these reasons and others that organizations considering complex migrations should look to outside tools for an added assurance of success. These tools exist to improve the process of completing large-scale actions such as domain merges and restructures, in many of the following ways:

- They create an entire migration infrastructure that includes real-time and bi-directional synchronization of objects to prevent the need for re-migrations.
- They provide guaranteed rollback functionality in the case of a failed object migration.
- They include workflow elements that ensure teams correctly complete their actions in the right order.
- They enable levels of reporting that go above and beyond simple log files.

Most importantly, organizations must remain up and operational irrespective that large-scale activities such as these are occurring in the background. As such, smart organizations demand tools that are seamless to the user and ensure a zero-impact result to their users and their business.