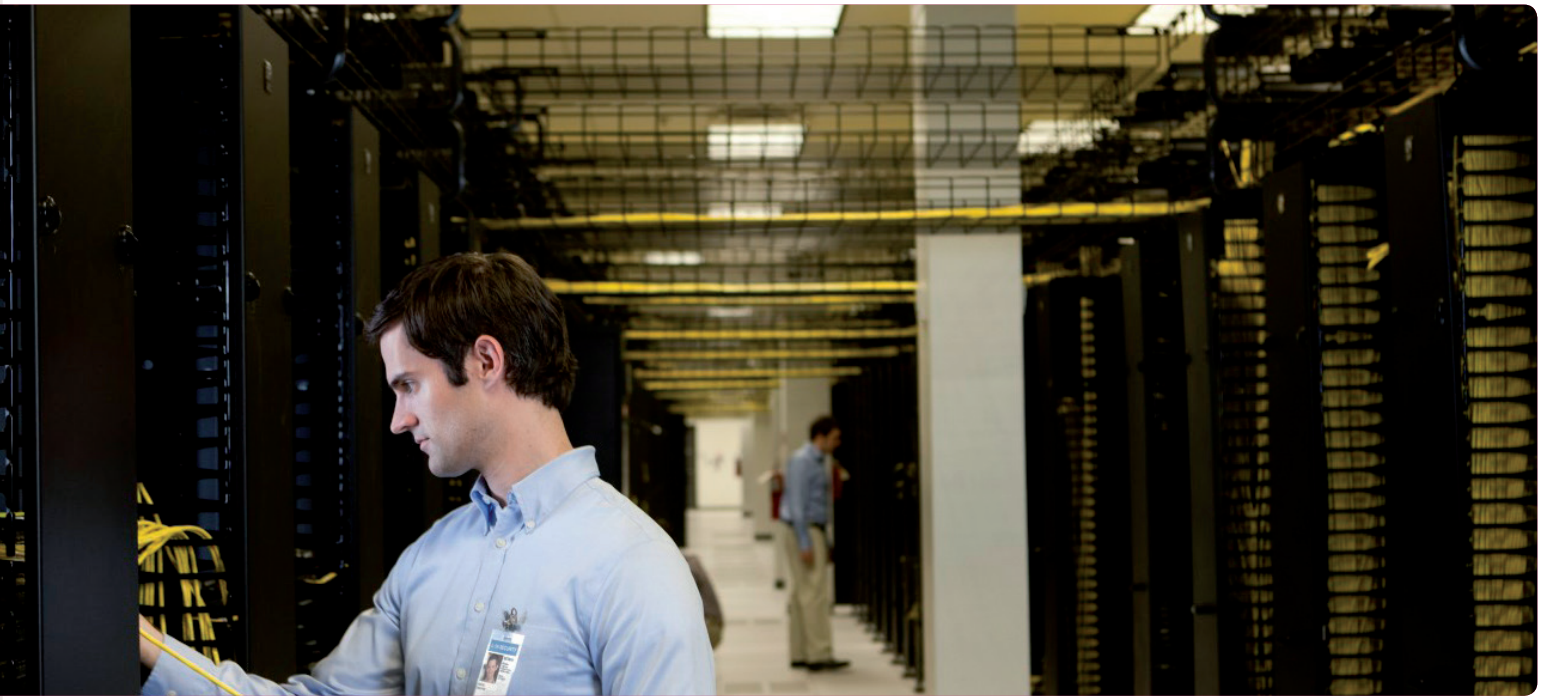
Restructuring, Consolidating or Merging Active Directory Domains



Introduction

Making changes to Microsoft® Active Directory® directory service domains can be a risky proposition. It is at the center of today's networks; mission-critical applications, such as email, rely on it and users need it to access almost every critical resource to do their jobs. This guide is designed to walk you through some of the challenges of restructuring, calling attention to critical planning decisions and considerations. Then it shows you how to perform a migration using an innovative third-party tool such as Migration Manager for Active Directory from Dell Software.

Simply put, you can't afford to make any mistakes when changing Active Directory domains. Whether you're restructuring domains to align with new business directions or add efficiency, consolidating domains to reduce administrative overhead and streamline IT, or merging domains as part of an acquisition or reorganization—you'll need to consider several important details before you start clicking buttons.

Planning considerations

While the benefits of Active Directory restructuring projects are expected to outweigh the challenges, successful migrations require significant planning and effort. Addressing the following critical considerations up front helps streamline the process to meet business and organizational goals as quickly and efficiently as possible.

Size and complexity

A restructuring project requires you to manage changes to a large number of users and resources. You probably have many objects that need to be migrated, either within forests or between forests. In addition, your resources might be widely distributed across your network.

User impact

Ideally, changes to your directory should occur without disrupting user productivity or requiring calls to the help desk. Users should have continuous access to all appropriate

Native tools and most third-party tools do not handle all aspects of Active Directory restructuring. Active Directory does not include tools to automatically merge two or more domains, split domains, move objects between domains and forests, or perform other Active Directory reconfiguration procedures.

resources during and after the restructuring project, without needing to log off.

IT administration

When executing inter-forest migrations—in other words, moving accounts and resources between forests—there's inevitably a period of time when both the old and new environments are intact. In large environments, it might take months before everyone is migrated and the old environment can be decommissioned. During that time, any changes made in one directory have to be made in the other as well, virtually doubling administrative tasks during the transition period.

Resource limitations

Restructuring projects can test the limits of an overworked IT department. Administrators may be called upon to work nights or weekends, and overtime could be required. And the restructuring project could take many weeks or even months to complete.

Suitable tools

Native tools and most third-party tools do not handle all aspects of Active Directory restructuring. Active Directory does not include tools to automatically merge two or more domains, split domains, move objects between domains and forests, or perform other Active Directory reconfiguration procedures. In addition, native tools and most third-party tools do not migrate all types of Active Directory objects and attributes. Nor do they update permissions across Microsoft Exchange Server, Microsoft SQL Server®, and Active Directory platforms, for example. You might face several restructuring issues that cannot be addressed with your existing tools.

Politics

Organizations often overlook the effect of internal political issues on their directory design. Certain groups or departments may prefer to be set up separately, or administrators may want to limit access to their areas of responsibility. This could lead to disagreements about when to create separate organizational units (OUs), domains, and forests. Underestimating these factors can add time and effort to your restructuring project.

Remote locations

Portions of your Active Directory might be controlled by remote administrators with exclusive access. It is essential to gain permissions for all remote locations or ensure that project standards are followed.

Risk

Changes made directly to your production environment can be risky. You need a way to restructure your directory that also allows you to preview and test changes before applying them to your network. You also need a way to selectively roll back changes if something unexpected occurs.

Security

During restructuring, existing security measures, such as passwords and permissions, must be preserved. To maintain a secure environment, you need to clean up security identifier (SID) history and track and delete source objects that have migrated. These tasks are not easily accomplished with native tools.

Assessing the infrastructure

It is essential that you have a clear understanding of your infrastructure to help see the whole picture and make good design decisions. Start by mapping out key infrastructure elements.

Infrastructure diagrams

Now is the time to create or update and verify diagrams with inter-site connections speeds, Active Directory design, OU hierarchy, domain controller placement, Flexible Single-Master Operations (FSMO) role placement, and Microsoft BackOffice Server location, along with other infrastructure elements.

Disabled and inactive accounts

You might also want to determine which user accounts have been inactive, with no logons for an extended period of time, to avoid moving them to the new environment.

Preparing source and target environments

The source and target environments must be properly prepared before starting a migration project. We have outlined some key things to do, as well as certain things you should consider, to prepare your environment.

Trusts

Plan to establish two-way trusts between all domains that will participate in your project. Trusts make it possible to resolve SIDs between domains, helping ensure that resource access and other elements are handled properly. If you choose to proceed without these trusts in place, you will not be able to use a single administrative account for the migration. You'll most likely have to migrate users and all their resources—including workstations—at the same time, rather than in a phased approach. And without these trusts, many migration assistance tools may not be able to use automated features that ease the migration process and reduce risk considerably.

SID filtering

If your target domain controllers are running Microsoft Windows® 2000 SP3, Windows 2003, or later you should turn off SID filtering for each source domain to be migrated. You should also disable SID filtering if source accounts were previously migrated and contain SIDs from other domains in their SID history. By default, SID filtering is turned on. To disable SID filtering, you must be a domain administrator.

Exchange Server ramifications

Because Exchange Server is inextricably linked to Active Directory, a domain migration of any kind often impacts Exchange Server. You'll need to consider:

- Redirecting mail between the source and target Exchange Server organizations to ensure that users receive mail during the migration
- Associating offline folders (OST files) in Microsoft Outlook® messaging software with an Exchange Server mailbox; an innovative third-party tool such as Migration Manager can be used to keep existing OST files without having to re-sync the entire file when a user's mailbox is switched

Third-party applications

Check your source environment for all third-party business applications, such as enterprise resource planning (ERP) or customer relationship management (CRM) applications, prior to the migration. Also consider infrastructure components, such as metadirectories, and business services, such as fax servers. These applications should be deployed in a test lab first and then properly tested in your migrated environment.

Ensure that these applications will function correctly in the target environment. For example, moving a server from one domain to another may require you to reassign permissions for service accounts, users, or other elements of the application. In some instances you may need to re-install the third-party application; in others, you may not need to take any actions at all.

Network attached storage (NAS)

Network attached storage (NAS) that assigns permissions to Active Directory security principals will need to be considered a part of the migration. Migration Manager can update NAS and storage area network (SAN) devices, using either the command-line permissions updating tool (Vmover.exe) or the Migration Manager console.

NAS and SAN devices typically store a large amount of data, and are often in almost continuous use by a large number of users. That means you need to carefully plan the time frame and

Check your source environment for all third-party business applications, such as enterprise resource planning (ERP) or customer relationship management (CRM) applications, prior to the migration... These applications should be deployed in a test lab first and then properly tested in your migrated environment.

An advanced third-party tool such as Recovery Manager for Active Directory provides granular, online backup and restore capabilities for Active Directory, up to and including complete forest recovery (when using the Recovery Manager for Active Directory Forest Edition).

procedures for updating these devices. Test these devices in a lab, if possible, to ensure you can update them properly. Be sure to maintain verified backups of all data throughout the migration, and have a recovery plan in place should a problem arise during the migration.

Disaster recovery

In a carefully planned, thoroughly tested, and properly managed migration, you should have no problems or lost data. However, waiting until you lose data is a bad time to start thinking about how to recover it! So be sure to back up your source and target Exchange Server and Active Directory infrastructures prior to implementing Migration Manager. Active Directory should be backed up at least twice a day during the migration; ideally, you should back up a domain controller's System State prior to beginning any step in the migration project. An advanced third-party tool such as Recovery Manager for Active Directory provides granular, online backup and restore capabilities for Active Directory, up to and including complete forest recovery (when using the Recovery Manager for Active Directory Forest Edition).

Infrastructure services and operation

You need to ensure that core infrastructure services are operating properly, including Domain Name System (DNS); Windows Internet Naming Service (WINS), if in use; and Dynamic Host Configuration Protocol (DHCP). Resolve any Active Directory replication issues before beginning your migration activities.

Also ensure that any migration-related traffic can pass through your network's infrastructure and locally installed firewalls, including the Windows Firewall. Migration tools might have traffic requirements above and beyond normal Active Directory use, file sharing, and other traffic; learn these requirements and conduct tests to be sure they are met before beginning your migration activities.

Active Directory design

It is necessary to create an Active Directory design (logical structure and site topology) before any migration. It is also recommended that your delegation model be engineered ahead of the project in order to identify business rules that must be enforced.

Creating a migration test environment

A test environment is an absolute must for a successful migration. It may seem like a hassle to set up an environment just for testing but rest assured, you will uncover—and solve—problems that you wouldn't want to face in your production environment.

Your test environment should resemble your production environment as closely as possible. With the ready availability of powerful virtualization solutions, you should be able to create a reasonable test environment with relatively few hardware resources. Remember, the test environment does not need the performance and power of your production environment—it merely needs to look like it. Consider the following techniques:

- Move one of your live domain controllers into the isolated network that will become your test lab and assign it the Primary Domain Controller (PDC)–emulator role. You may want to create an additional domain controller in production and then use it for testing purposes in the lab. Note that you will also have to seize all FSMO roles to this domain controller and make it a global catalog after you move it into the isolated network.
- Create an image of your live domain controllers and Exchange servers using third-party tools and restore the image to another box with a similar hardware configuration in the lab.
- Export the source Active Directory into a comma-separated value (CSV) or Lightweight Directory Access Protocol Data Interchange Format (LDIF) file using tools such as Microsoft CSV Data Exchange (CSVDE), Microsoft LDIF Directory Exchange (LDIFDE), or Softerra LDAP

Browser, and then import it into the test environment.
- Restore the directory data from backup into the test environment.

Performing the migration

An Active Directory migration involves user and group accounts, as well as their resources—including end-user client computers, file and print servers, and other Microsoft server products. You'll be moving these from one domain to another domain in either the same or a different forest. For the purposes of this discussion, Exchange Server is not a concern in an Active Directory migration project. You should perform the following steps during an Active Directory migration; be aware that there would be additional ones for projects that also include an Exchange Server migration.

Migration process

It is important to understand five steps in the Active Directory migration process:

1. **Pre-migration:** In this step you prepare the source and target environments, keeping in mind the earlier discussions in this white paper.
2. **Directory synchronization and account migration:** This step establishes synchronization between the two domains, and migrates accounts to the target domain. Synchronization ensures that all changes made during the coexistence period are reflected in both directories, including password changes or group membership changes. For migrations that occur over a very short period of time, you can skip synchronization.
3. **Resource updating:** This step processes distributed resources, re-assigning permissions. Servers are moved to the new domain as well.
4. **User switch:** In this step, end-user client computers are moved to the target domain and processed to reassign permissions. Migrated users start logging into their accounts in the target domain.
5. **Post-migration:** At this point, any synchronization agents that were used during the migration are removed. Source directory accounts are disabled, and SID history attributes are cleaned up in the target domain. Legacy account permissions are removed from resources, and the source environment is decommissioned.

In large environments, these five steps may be repeated multiple times, with a small portion of the environment being migrated during each cycle. The following sections explore how Migration Manager for Active Directory can avoid common pitfalls while helping to simplify and automate the overall process.

Import lists

An import list is a text file listing accounts to be migrated with Migration Manager, along with attribute values for each account. If you are going to perform a one-time migration and plan to migrate all users and groups at once, an import list is not necessary—the information can be read directly from the source domain. However, import lists should be used when migrating large environments (over 2,500 users). It makes the migration process more manageable, accurate, and efficient. In addition, using import lists can help you easily track migration activities by site, region, location, or any other criteria set up during the planning phase. You can also use import lists to modify target object attributes.

You can easily create an import list using Migration Manager's Import/Export feature when you open a new migration session. Migration Manager allows you export information about the accounts from the selected OU and save it in a plain-text, tab-delimited format. You also can select what attributes to export. Then you can open the file in a Microsoft Excel® spreadsheet, modify the attribute values as needed, and import the list back. The modified attribute values will be applied to the target objects during migration.

Import lists can also be used for renaming accounts. For example, you may want the names in the target to meet new corporate standards. To assign the target account a different name on the fly (this can be a name, or sAMAccountName), you can add a

Migration Manager allows you export information about the accounts from the selected OU and save it in a plain-text, tab-delimited format. You also can select what attributes to export. Then you can open the file in a Microsoft Excel® spreadsheet, modify the attribute values as needed, and import the list back. The modified attribute values will be applied to the target objects during migration.

Migration Manager includes Resource Updating Agents that perform tasks such as re-assigning permissions for local resources on server and client computers.

new column to the exported list right after the first column and populate it with the new object names (name or sAMAccountName). This is an excellent way to handle duplicate accounts, as discussed earlier. The new names are applied to the newly created target objects during migration.

You can also use import lists to merge source and target accounts that have different names. To do this, create an import list containing at least two columns (source sAMAccountName and target sAMAccountName), and specify the actual names for the source and target accounts in the columns. Source and target accounts will be matched by their sAMAccountNames and merged into a single account during the migration when using import lists created in Migration Manager.

Linked attributes and group migration

When you migrate a group from source to target, the target group membership should also be updated. This means that the user and group objects in the target domain that correspond to the user, and group objects in the source domain that are also members of the source group, should be added to the target group membership list. Since group membership is a list of so-called linked attributes, this process is called link resolution.

Migration Manager resolves links when you migrate or synchronize objects. However, if the objects that should be added to the target group membership or set as a manager for other objects have not been migrated yet, group membership and manager information will not be updated for those objects. Instead, those objects will be placed into an unresolved links queue. To resolve the links in the future, once all group members are migrated to the target, you can either re-migrate and merge groups or run full resynchronization.

For groups containing more than 5,000 members, you should rely on primary group membership to ensure correct synchronization.

Skipped attributes

You can skip certain attributes from directory synchronization. However, although Migration Manager allows you skip the majority of object attributes from its interface, you should never skip the following attributes from synchronization:

- The Directory Synchronization Agent service attributes (extensionAttribute15, extensionAttribute14, adminDescription, and adminDisplayName, by default)
- objectClass
- objectGUID
- userAccountControl
- objectCategory
- objectSID
- msExchMasterAccountSID
- msExchMailboxSecurityDescriptor

Skipping these attributes may lead to problems during directory synchronization.

Pre-installation of resource updating agents

Migration Manager includes Resource Updating Agents that perform tasks such as re-assigning permissions for local resources on server and client computers. These agents are normally installed to the computer when you start processing from the Resource Updating Manager. However, if desired, Resource Updating Agents can be pre-installed using Windows Group Policy or Microsoft Systems Management Server (SMS). Pre-installing the agents allows you to ensure you have enough rights over the workstation or server to perform the update, and that Windows Firewall is turned off on these computers. Pre-installation can also save time later by helping the Resource Update Manager to operate more quickly.

Conclusion

Active Directory migrations involve significant upfront planning and effort, especially in distributed environments. Proper preparation can make all the difference in the world: a thorough discovery process, detailed documentation, and a well-written migration plan, together with thorough and realistic testing. Migration Manager for Active Directory is designed to accelerate business outcomes and contain costs through heightened efficiencies—helping to simplify the process and integrate workflow while automating tedious administrative tasks.

For more information

Migration Manager for Active Directory empowers you to migrate efficiently and restructure your Active Directory. Migration Manager ensures coexistence between migrated and un-migrated users. Migration Manager simplifies migration processes and integrates workflow—from pre-migration analysis through setup, object migration, resource updating and post-migration cleanup. For more information, visit quest.com/migration-manager-for-active-directory.

Migration Manager for Active Directory is designed to accelerate business outcomes and contain costs through heightened efficiencies—helping to simplify the process and integrate workflow while automating tedious administrative tasks.

For More Information

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.