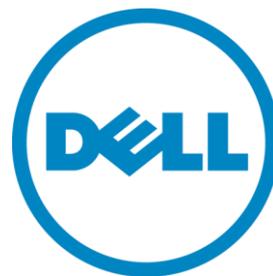


Mastering Active Directory Migrations: Controlling Critical Issues

*Use the right combination of tools and processes
to protect your core network operating system
during this critical process*



Abstract

With each release of Windows Server, Microsoft transforms and updates its network operating system (NOS)—Active Directory Domain Services—into one of the most comprehensive network-infrastructure engines in the industry. Each time, organizations are faced with a key question: is our existing Active Directory able to respond to the growth and changes the organization needs to go through with an update to the NOS? According to Microsoft, the answer is no for up to 80 percent of their customer base. For these customers, this means creating a new directory structure and migrating all data into it.

However, migrating a directory structure is no simple task. First, you need to find out where you can improve the current structure. Next, you need to discover the new features of the NOS and see if they apply to your organizational requirements. Then, you need to build the new directory structure. And finally, you need to move all data, services and objects from the old structure to the new. Daunting task you say? Yes indeed. But there is light at the end of the tunnel. Using a combination of best practices and the right migration tools may not make the pain go away, but this will definitely help smooth the process.

About the Authors

Nelson Ruest and **Danielle Ruest** are technology futurists focused on infrastructure design and optimization, as well as continued service delivery. They have been working with complex infrastructures for over 20 years. Their system designs include core application deployments such as email and collaboration. They also have been working with virtualization for more than ten years. Their recent books include [Configuring Windows Server 2008 Active Directory](#), an exam preparation guide for Microsoft Certification exam 70-640; [Deploying Messaging Solutions with Microsoft Exchange Server 2007](#), an exam preparation guide for Microsoft Certification exam 70-238; [Virtualization: a Beginner's Guide](#), a look at comprehensive virtualization infrastructure designs and [Configuring Windows Server Virtualization with Hyper-V](#), an exam guide for exam number 70-652. They both work for Resolutions Enterprises Ltd.



Table of Contents

Mastering AD Migrations: Controlling Critical Issues.....	1
1. Identify When to Migrate.....	2
2. Determine How to Migrate	3
The Parallel Network Migration Order	4
3. Prepare the New Directory Service	5
Migrate Security Principals	7
4. Perform the Migration	9
Using the Active Directory Migration Tool	9
Enable the Password Export Server	9
Create Domain Data Reports.....	10
Special ADMT Considerations.....	11
Use a Commercial Migration Tool.....	12
Final Thoughts.....	13

Mastering AD Migrations: Controlling Critical Issues

With each release of a new server operating system, Microsoft Corporate releases updates to its core network operating system (NOS): Active Directory Domain Services (AD DS). But with each release customer organizations are faced with a dilemma: Should we upgrade the server operating system (OS) and therefore upgrade our directory service? According to Microsoft, the answer is no in most cases. Why? Because IT administrators in general, with or without reason, do not trust the server upgrade process and often find that upgrading an NOS is just as challenging as upgrading a simple OS. This means that moving to a new server operating system will also imply moving to a new NOS or directory structure and migrating all existing data into it.

This is no simple task. Of all of the migration tasks organizations and IT departments are faced with, migrating the NOS is probably the most daunting and complex. But there is light at the end of the tunnel. Because Microsoft has released several different versions of its NOS — Windows 2000 Server; Windows Server 2003; Windows Server 2008, along with the R2 versions which provide considerable updates; and now, Windows Server 2012 — organizations have, by necessity, performed this migration a number of times and formed a body of knowledge and best practices around the entire process. The general process looks like this:

1. Begin by identifying when to migrate.
2. Determine how you will perform the migration.
3. Rely on directory best practices to create and deploy the new NOS.
4. Actually perform the migration, as well as decommission of the legacy NOS.

This process will help you move to the new environment and hopefully let your organization grow without having to repeat it again for quite some time.

1. Identify When to Migrate

When you're looking at a potential directory service migration, start by identifying the right time to migrate. Network operating system migrations can be overwhelming when undertaken without proper planning. Given all of the moving parts of a directory service migration, you will want to guarantee that your operational disruptions will be kept to an absolute minimum. Some common reasons to undertake a migration include:

1. **Operational** — Your users and administrators become aware that the current system is simply not providing the functionality that it should. Outdated systems often lack the ability to integrate with the latest client devices and operating systems, or simply can't provide the services that a mobile or remote workforce requires. It becomes obvious that the system can no longer keep up with the structural changes of a growing organization.
2. **Technological** — The technology used to run your operational systems is outdated and needs replacement, for example; when a new version of Windows Server is released. Microsoft has identified that 80 percent of their clients will perform an NOS deployment when implementing new versions of Windows Server and AD DS. This is no surprise, since very few organizations will trust the OS upgrade process when it comes to critical machines such as servers. Performing an NOS migration is a very significant endeavor, since it involves the replacement and update of all of the security principals in your network.
3. **Structural** — Complex technologies such as AD DS are sometimes deployed in fast-track patterns that do not result in optimum configurations. This often can be caused by a lack of centralized planning and coordination during the deployment process. In these situations, administrators choose to restructure this foundational building block to streamline structural configurations, simplify operations and improve service levels. This 'second surgery' approach will frequently require a complete overhaul of the infrastructure used to run these critical systems to provide better efficiency and manageability.
4. **Legal** — Directory services often require complete restructuring to meet updated security regulations. In this case, your best option is to create a completely new directory and migrate all objects from the legacy directory into the new one.
5. **Mergers and Acquisitions** — When organizations change and meld together, they often find that their existing directories do not meet the requirements of their new structure. In this case, they can either create a new directory structure or use one of their existing structures as the migration destination.

Any of these situations will have a direct impact on your directory system, since all require the upgrade or replacement of your directory servers.

2. Determine how to migrate

Migrating a directory service or network operating system means creating a new infrastructure and moving the objects, such as security principals, from the legacy network to the new network. The best way to do this is through the use of a parallel network — a new network that runs in parallel with the original environment until all objects have been migrated and the legacy network is decommissioned. Parallel networks gradually replace older systems as more functionality is integrated into the new network.

In addition, the creation of a parallel network is the perfect time to take advantage of virtual machine (VM) technology. Directory servers or domain controllers are ideal candidates for virtualization and should run within VMs to reduce the physical server footprint in the datacenter. If you haven't moved to a virtual environment yet, or even if you have a partial virtual environment, deploying a new NOS is the right time to fully embrace virtualization. Here's how the migration process works (see Figure 1):

- 1 Core host servers are formed from new acquisitions
- 2 Core of new network is built with virtual machines
Core network services are activated

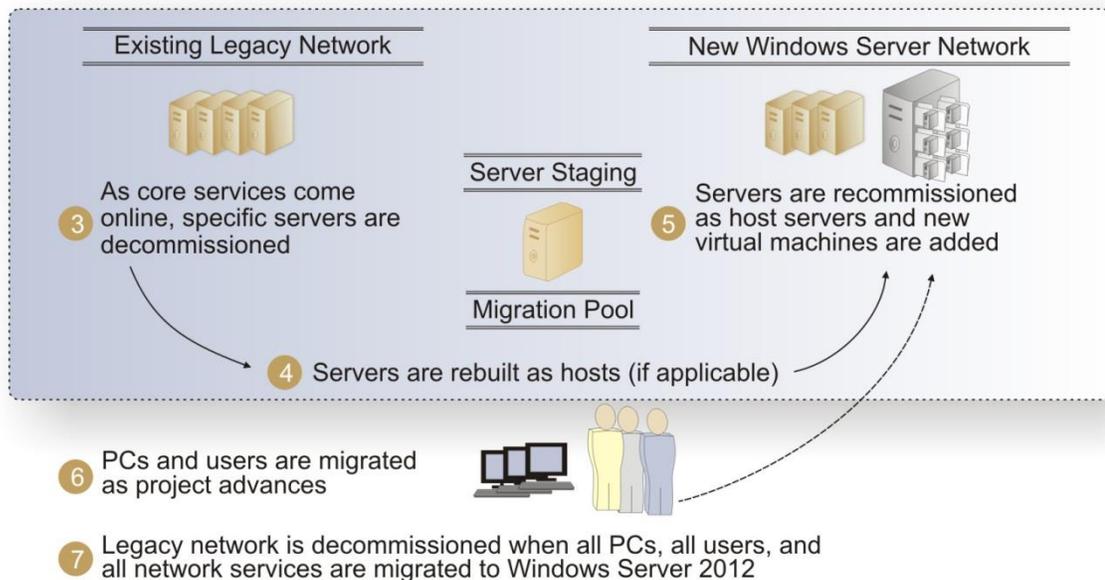


Figure 1. The parallel network migration approach

1. Acquire new servers to host the virtual machines that will form the core of your new network operating system.
2. Build the model VMs that will be used to clone all new machines and deploy the initial domain controllers for the new directory service.
3. Decommission physical or virtual machines from the legacy network as new services are made available within the new infrastructure.
4. If applicable (if the physical machines hosting the decommissioned legacy service are properly scaled and configured), redeploy them as host servers running the hypervisor service in support of additional VMs.

-
5. Build additional host servers and additional VMs to host more services within the new network.
 6. Migrate PCs when all services have been updated.
 7. Decommission the legacy network when all objects have been migrated.

Basically, you perform a server rotation throughout the entire parallel-network process. When you select a service to migrate, you should prepare the new virtual servers that will host this service first and ensure that you have a fallback solution in case of service failure. This is the advantage of the parallel network: The legacy network is always available for service fallback if you need it. But if you've done your homework right, you won't.

The Parallel Network Migration Order

When you're ready to move to the new infrastructure, you'll have to put together a migration strategy. This strategy must cover four major activities:

- **Security principal migration:** Migrating users and computers from the directory service in the legacy network to AD DS in the new network.
- **Member server migrations:** Migrating all services found on member servers, including file, print, management, collaboration and more. This includes special products, such as Exchange, SQL Server and other services that manage the back end of your network.
- **PC migrations:** Migrating PCs from obsolete operating systems to updated environments. This will involve capturing and restoring user data and preferences/profiles. This portion of the migration may already be done, depending on your approach to the maintenance of existing PC operating systems.
- **Custom application migrations:** This involves mostly conversions or redevelopment of both rich-client and Web-based in-house applications.

Each of these four stages is a mini-project of its own, and each will require its own resources. In the parallel network, you begin with the security principal migration. If you set up your environment right, you will be able to migrate user and computer accounts, as well as groups, at your own pace, giving yourself time to prepare the other aspects of the project. In addition, by using the parallel network approach, you won't affect the current production environment; therefore, users in either network will be able to share applications and services from both during the entire length of the migration.

3. Prepare the New Directory Service

Your network is now ready to be launched into the production environment. So far, every operation you have followed has been, or should have been, within a laboratory environment. Even the final procedures you'll use for the migration itself must be thoroughly tested before you move to the migration into the new production network. You'll begin by populating the directory in the new network.

Organizations have been preparing directory services in Windows ever since the release of Windows 2000 Server. Because of this, a body of best practices has been established and is available to anyone wanting to create a new directory running AD DS as the NOS. Consider the following when creating the new directory service in your parallel network:

AD DS Design Best Practices

For a comprehensive set of best practices for AD DS design, look up [The Complete Reference to Windows Server 2008](#) by Ruest and Ruest.

1. **Forest/Domain Strategy:** The forest strategy determines the overall boundary of your directory service. This strategy depends on your organization size and thus, the number of objects your directory will contain. If your organization is small — fewer than 1,000 objects — create a single domain forest to simplify ongoing management and administration. If your organization is large, or you require a more complex infrastructure because it spans several international territories, create a forest root domain (FRD) with a global child production domain (GCPD). Also include the trusts your forest will implement in this part of your design.
2. **Naming Strategy:** AD DS is very closely tied to the Domain Name System (DNS), since its entire naming structure relies on a DNS hierarchy. Two strategies exist for this:
 - **Split-brain DNS:** In a split-brain strategy, your internal directory name is the same as your external domain name presence. For example, an organization whose Internet domain name is TandT.MS uses the same name for its internal AD DS structure. This requires manual DNS maintenance to segregate the domain names both internally and externally. It also creates a potential security hole, since hackers and attackers can use the same root name both internally and externally.
 - **Whole-brain DNS:** In a whole brain strategy, your internal name differs from your external name. For example, an organization whose Internet name is TandT.MS will use TandT.WS as an internal directory name. Using a different name creates a natural segregation between internal and external networks. This strategy is more secure by far. The organization can rely on the User Principal Name (UPN) feature of AD DS to ensure all email and user accounts use the external or TandT.MS name.
3. **OU Structure:** Organizational units (OU) create the internal structure of your directory. There are four reasons to create an OU:
 1. **Administration:** OUs provide units of administration for the objects they contain. This is performed through Group Policy.
 2. **Collection:** OUs provide containers to collect objects of a similar type or in a given location.

-
3. **Delegation:** OUs provide a delegation point for the administration of specific objects.
 4. **Obfuscation:** OUs can be used to hide objects within the directory from searches by normal users. For example, objects of a technical or sensitive nature should be hidden from view at all times.

If an OU does not meet one of the above four reasons, then it is not necessary.

4. **AD DS and Other Directories:** You may require interaction with other directories, such as with the directories of partner or client organizations. There are several strategies that meet this requirement and it is important to consider them while designing your directory. Avoid long-term Forest Trusts if at all possible. Use technologies such as Active Directory Federation Services instead, because they provide support for partner and client interactions through normal Internet TCP/IP ports.
5. **Service Positioning:** This aspect of your directory will focus on the positioning of key directory servers. These include:
 - **Flexible Single Masters of Operations (FSMO):** FSMOs are key server roles that support the operation of the directory. Proper positioning is crucial to the long-term operation of the directory.
 - **Global Catalog Servers:** These servers provide support for directory searches. They should be widely dispersed within the directory.
 - **Domain Controllers (DC):** DCs are the main server role in an AD DS infrastructure and should be positioned to provide login support for all users and other directory objects.
 - **DNS Servers:** DNS is the main naming system that supports directory operations. The DNS server role should be married to the DC, since DNS data is stored within the directory. All DCs should be DNS servers.
 - **Read-Only Domain Controllers (RODC):** RODCs provide protected login support for remote offices. Position them accordingly.
6. **Site Topology:** Directory server operations are based on replication. AD DS relies on a multi-master replication strategy, which means that all standard DCs can initiate a replication. Your site topology should reflect this fact and ensure that replication priorities are located in your administrative offices first and foremost.
7. **Schema Management:** AD DS is a network operating system, since it can be used both for secure access to networked resources and remote object management (through Group Policy). Because of this, it is essential that every deployment of this directory service include a database schema administration policy. The NOS directory should only be modified by essential services, such as Microsoft Exchange Server, because while modifications can be deactivated, they cannot be reversed or deleted. Careful consideration should be given to any product that requires an NOS schema modification, especially since you can provide directory extensions that do not affect your NOS structure through services such as Active Directory Lightweight Directory Services.

The result of this undertaking should be a world-class directory structure that can grow to support your organization in any situation.

Migrate Security Principals

Now you're ready to perform the actual directory object migration. Start by migrating user accounts, PC accounts and data into the new directory. To do so, you'll need to perform the following steps:

- **Create trusts:** The first step is to create a two-way trust relationship between the new production domain and your legacy domain. This two-way trust serves to support the operation of both networks at the same time. It is transitive; i.e., it will not remain in place forever, but it will need to remain in place until the migration is complete.
- **Nest groups:** The second step is to nest the appropriate global groups into the local groups that are required to grant joint access to resources from both domains. For example, if you are migrating a select group of users and the migration cannot be completed all at once, you need to ensure that both sets of users — the ones located in the legacy network and those already migrated to the new network — have access to joint resources, so they can continue to work together for the duration of the migration. This approach will need to be extended to all users of shared folders, because they must share resources for the duration of your migration.
- **User account migration:** Next, you'll need to migrate user accounts from the legacy network to the new environment. You'll need to use a special tool, for example, the Active Directory Migration Tool (ADMT) available from Microsoft, or a third-party migration tool, to perform this operation. This is an excellent opportunity to clean up your legacy directory database as it is imported into the new production domain.
- **Service account migration:** You shouldn't need to migrate service accounts; instead, they should be recreated in the new network as new services are activated.
- **User data migration:** You can then proceed to migrate user data that is located on network shares, such as home directories, or better yet, through Folder Redirection Group Policy Objects (GPOs). This is where it is important to use the proper tool for user account migration, because each account that is migrated is assigned a new security identifier (SID). The new SID is different from the SID used to create the information in the legacy network. This means there's a risk that users might lose access to their data once it has been moved if you don't manage the migration properly. Migration tools can either maintain an SID history when used to migrate a user account, giving the account the ability to present a legacy SID when accessing the legacy network; or it can perform SID translation, replacing the legacy SID with the new SID on the object to avoid this problem.
- **PC account migration:** Next, you'll need to migrate PCs. If PCs do not need to be restaged (they are already running a current version of the Windows client OS), then you can use the migration tool to migrate computer accounts and reset security descriptors on each system. If, on the other hand, they are not up to date and need to be restaged, you will need to first recover all user data

from the system, reinstall the system, join it to the new domain during reinstallation, and then restore user data to the system.

- **Decommission the legacy network:** The last step will consist of decommissioning the legacy network. This will be the step that identifies when the migration is complete.

Once these steps are complete, your migration will be finalized and you'll be ready to move on to the administration and optimization of your new network (see Figure 2).

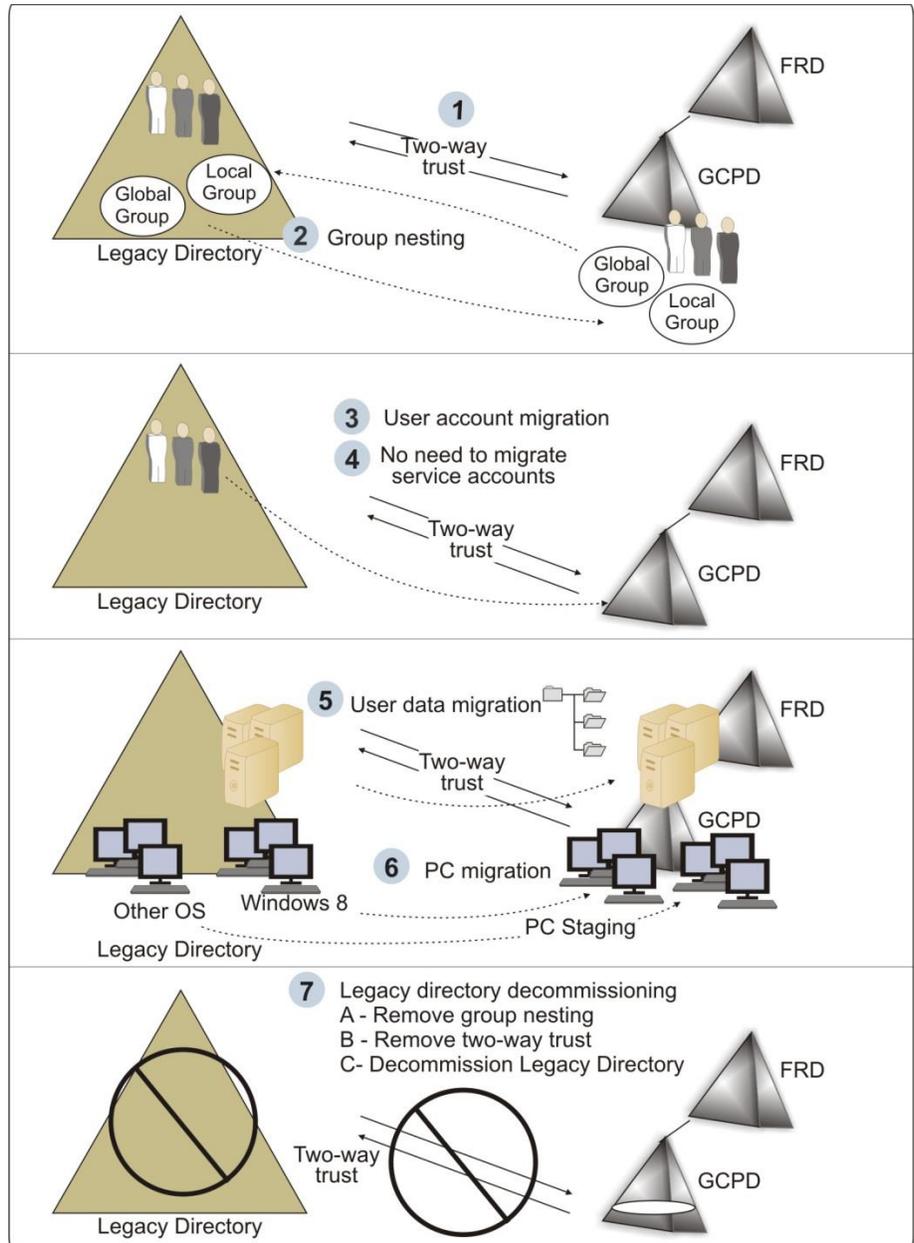


Figure 2: The user account, data, and PC account migration process

4. Perform the Migration

You must use a migration tool to perform a directory service migration. You have two choices: Use the Microsoft Active Directory Migration Tool (ADMT), or use a third-party tool. Microsoft's ADMT is a free tool that provides just enough features to perform a migration. Using a commercial migration tool helps you avoid many migration hassles, because it takes all of the migration situations into account and can often make the process considerably simpler and smoother.

Using the Active Directory Migration Tool

The ADMT is a downloadable tool that offers most of the features required to perform a directory migration. You don't have to install it on a target server, but you might find it easiest to do so. Also, you'll need domain administration credentials in both the source and target domains. ADMT requires a database for use. You can use SQL Server Express Edition, but you also can use a full copy of SQL Server to store and maintain the database. If you use SQL Server Express, it must be installed locally on the same machine as ADMT.

Active Directory Migration Tool

Find the ADMT at

<http://www.microsoft.com/en-ca/download/details.aspx?id=8377>.

Find the ADMT Migration Guide at

<http://www.microsoft.com/en-ca/download/details.aspx?id=19188>.

Once installed, you can launch the ADMT console by moving to Administrative Tools and selecting Active Directory Migration Tool. The operation of the ADMT basically consists of using the right mouse button to click Active Directory Migration Tool, accessing the context menu, and selecting the appropriate wizard. ADMT offers several wizards:

- User Account Migration
- Group Account Migration
- Computer Migration
- Security Translation
- Reporting
- Service Account Migration
- Password Migration

The operation of the wizards is fairly simple. You need to identify the source domain, the target domain, the objects you want to migrate, the container you want to migrate them to, and then how you want to perform the migration.

When ADMT migrates a group, it can also migrate the users that are contained within it, making it easier for you to determine what to migrate. But before you can move users and computers from one network to another, you need to ensure that the data you will migrate is filtered and that all obsolete records are removed. You don't want to input obsolete data into your brand new network!

Enable the Password Export Server

In order to migrate user accounts with their passwords, you must enable the Password Export Server (PES). Migrating user accounts with passwords is a lot easier on both users and administrators, because you do not need to provide users with temporary passwords, and users do not need to reset their passwords before they log on. You can, however, get them to reset their passwords at first logon as part of a security policy for your new environment.

Password Export Server

Find the x64 edition of PES at <http://www.microsoft.com/en-ca/download/details.aspx?id=1838>.

The PES must be installed on any domain controller in the *source* domain. This DC must support 128-bit encryption — the default in most versions of Windows Server. The tricky part is that you need to have an encryption key to perform the PES installation. This key must be generated with ADMT, but this time, it must be on the *target* domain.

Make sure you install ADMT on a DC in the target domain. Then generate the key with the following command:

```
admt key /option:create /sourcedomain:SourceDomain /keyfile:KeyFile  
/keypassword:*
```

This will prompt you for a password that will not be displayed on the screen. Note that *SourceDomain* is the name of the source domain and *KeyFile* is the name of the file to generate. Place the file on either a very secure file share or a Universal Serial Bus (USB) device to secure it.

You should also create a service account in the target domain. This account needs domain administration rights. Make sure you also grant this account local administration rights on the source DC. This account will be used to run the password migration service.

On the source DC, locate the PES installation file. It will be under `%SYSTEMROOT%\ADMT\PES` and is called `PWDMIG.MSI`. Double click it to launch the installation. Specify the account to run the service under, point to your encryption key file, and then provide the password to unlock it and complete the installation.

Once the service is installed, you need to start it. Go to the Services console, locate the Password Export Server service, and start it. It is a good idea to leave it on manual start, because this way, you can start it only when you need it. Stop it again once you have performed the migration of the passwords.

Create Domain Data Reports

To filter data from your source domain, you need to use the ADMT Reporting Wizard. This tool can support the creation of several different report types to summarize the results of your migration operations:

- Migrated Users and Groups
- Migrated Computers
- Expired Computers
- Account References
- Name Conflicts

The Expired Computers report lists the computers with expired passwords. The Name Conflicts report does the same with potential objects that will have the same name in the target domain. The Account References report lists the different accounts that have permissions to access resources on a specific computer.

You should try to identify obsolete contents of the original directory before you begin to migrate contents. You can perform this removal in several ways:

- You can remove the objects from the source domain and then migrate the accounts.

-
- You can create new groups that contain only valid objects in the source domain and migrate objects by using these groups.
 - You can move the accounts to a specific OU in the target domain, clean them up, and then move them to their destination OUs.

The last approach may be your best bet, since the ADMT will allow you to control the way accounts are treated after the migration. In fact, you can ensure that no account is activated until after you perform a cleanup operation on the newly migrated accounts.

Reports must be generated before you can view them. Many reports are generated from information that is collected from computers throughout your network. This will affect their performance; therefore, you may decide to use dedicated servers for this function. Also, reports are not dynamic; they are point-in-time reports and must be regenerated to get an updated picture.

Special ADMT Considerations

There are a few items you must keep in mind when using the ADMT. The first is related to the SID. As mentioned earlier, all of a user's data is associated with the SID that represents the user at the time the user object is created; therefore, all of a user's data will be associated with the user's *legacy* SID. When you transfer this data to the new network, you must use a special technique that will either carry over the user's legacy SID or translate it to the user's new SID (the one generated by the new network).

The best way to do this is to ensure that the user's legacy SID is migrated to the new domain (using the appropriate check box in the Account Migration wizards) and then to use SID translation. The latter is performed through the use of the ADMT Security Translation Wizard. But in order for security translation to work properly, you *must make sure that all of a user's data has been migrated to the new network first*; otherwise, you will need to perform the SID translation again once this is done.

It is also important to note that, for SID history migration to work, the Password Export Server is required. As mentioned earlier, the PES is installed on a domain controller in the legacy network. It is best to use a dedicated server for this operation because it is resource-intensive. Therefore, you should stage a new domain controller and dedicate it to this task.

Your network also needs to meet the following conditions before you can perform password migration or SID translation:

- Auditing must be enabled on the source domain. If it isn't, ADMT will offer to turn it on during the migration.
- Your target domain must be in full-functional mode, but this shouldn't be an issue, since it is a brand new directory.

There are other prerequisites you must take care of before performing a migration (such as the service-pack level for the source domain machines). ADMT will also require some additional settings, but it can automatically perform the modifications during a migration operation.

Use a Commercial Migration Tool

While ADMT offers some powerful features, you may find that it is cumbersome to work with. Third-party manufacturers, such as Dell™, have more comprehensive commercial tools to support migrations from one network environment to another. For example, **Dell™ Migration Manager for Active Directory** offers full workflow integration, letting you move through a step-by-step process in support of the migration. It also supports complete coexistence between the source and the target directories. In addition, Dell™ Migration Manager for Active Directory is designed for Windows Server 2012. It also provides the following features:

- Support for the migration of users during business hours, since it has little or no impact on operations.
- Automatic updates for the permissions and resources of each security principal, including updates in AD DS, Exchange Server, Internet Information Server, File and Print servers, SQL Server and much more, removing the need to perform these updates manually.
- Support for controlled synchronization, allowing you to identify which DCs should be used for this purpose.
- Delegation for multiple types of migration activities, allowing you to designate support staff for the process without having to grant them ultimate privileges in your network.
- Support for the mirroring of a test environment to allow you to fully prepare for the migration process without impacting production networks.

These and other features can make it worthwhile to perform the migration with the assistance of a professional tool designed for the purpose of migration support. Find out more by downloading a free version of Dell™ Migration Manager for Active Directory at <http://www.quest.com/migration-manager-for-active-directory/>.

Final Thoughts

Directory structures for network operating systems are complex even in the simplest organization configurations. When you integrate them with additional network services, you add levels of complexity. The best way to ensure that this vital structure continues to work at its best during a migration is to rely on a specialized tool that is solely designed for the purpose of supporting the migration process.

Directory structures are the lifeline that organizations rely on to make their IT operations hum. Moving security principals from one system to another can make or break this lifeline. Using the right tools, focusing on the right issues and using the very best migration process can help you move on to the next generation of network operating systems and services with Active Directory Domain Services, as well as help make the move seamless and stress free.