Best Practices for an Active Directory Migration

Written by Derek Melber, MCSE, MVP, president, BrainCore.Net AZ, Inc.

Abstract

This white paper details the major challenges of Microsoft® Active Directory® directory service migrations, and explains how choosing the right migration tools can speed your migration and help ensure its success.

Minimize loss of data and downtime with AD migration best practices

The goal for Active Directory migration projects is to provide seamless access to data and services for all users during and after the migration, and minimize the impact of on the production environment. Following best practices helps organizations ensure success, particularly for challenging scenarios involving multiple domains, complex site topologies and non-trusted domains.

Millions of dollars can be lost with a single resource or server failing to migrate successfully. Therefore, organizations need a management system that can track each migration step, ensure that nothing is missed, and provide a way to recover back to the original environment if a serious issue arises.

Assessing the source environment

The first step in a migration is assessing the current environment to determine the scope of your project and properly plan for resources required in the target environment. Most organizations will want to gather the following information:

- **Accounts that have never logged on and inactive accounts:** These accounts may not need to be migrated.
- **Computer account status:** Organizations often discover dead computer accounts that do not need to be migrated.
- **Duplicate users and groups:** If you identify duplicate users between domains, you might want to merge or rename some of these objects during the migration.
- **File shares by computer:** Some shared file resources might require a permissions update as part of the migration process.
- **Account policies, audit policies, and password policies:** You should assess the level of consistency between the source and target environments for each type of policy. Assessing password policies for domains, for instance, is important because when user accounts with weak passwords are migrated into a domain with a stronger password policy, those user accounts are automatically disabled by the operating system and the "must change password at next logon" flag is set.

Unfortunately, collecting this information and developing appropriate reports manually can be difficult and is prone to error. Many organizations find they do not have the time to assess their source environment properly, and they often face migration issues later that could have been avoided. Consider investing in a third-party tool, such as Reporter software from Dell, to automate the assessment process and help ensure you have a complete and accurate picture of your source environment.

Managing the migration

Most organizations have two important requirements for their Active Directory migration projects. The first is to minimize disruption for users, both during and after the migration, and the second is to minimize the impact to the production environment, also both during and after the migration. Although we all want the migration process to take a day, most migrations take weeks or even months to complete. During this time, users must be able to access the data and applications they need; servers must be available; and domain membership and resource permissions must be correct. If any of these fail during the migration, the ramifications can be staggering. Millions of dollars can be lost with a single resource or server failing to migrate successfully.

Therefore, organizations need a management system that can track each migration step, ensure that nothing is missed, and provide a way to recover back to the original environment if a serious issue arises. The following aspects of migration require particular attention.

Re-permissioning of resources

During the migration process, re-permissioning of resources needs to be tracked and verified. Re-permissioning must take into consideration the domain structure of all domains being migrated. Old user and group accounts and new user and group accounts need to be rationalized.

SID history migration

The security identifier (SID) history of migrated users needs to be understood, managed, and tracked to ensure seamless access to resources during and after the migration.

Coexistence

Most migrations are done in waves or phases; this is called a rolling migration. Ensuring that everything is kept in sync during these phases is critical to keeping business operations up and running. Some of the key synchronization efforts include:

- Continuous synching of user passwords from the originating domain and the target domain.
- Continuous updating of group membership

from the original domain to the target domain.
- Ensuring proper access to resources in both the original domain and the target domain.

Reporting

Administrators need regular statistics and reports so they can always know the status of the migration. Reports should indicate the percentage of the migration completed and detailed statistics on the number of successful and failed migrations of users, groups, servers, resources, permissions, etc.

Cleanup

After migration, you need to update permissions and resources, including Active Directory, Microsoft SharePoint® collaboration software, Microsoft Exchange messaging software, Microsoft Internet Information Services (IIS), file and print services, Microsoft SQL Server® database software, cluster servers, Microsoft Systems Management Server (SMS), and Microsoft System Center Configuration Manager (SCCM).

Rollback

A final key aspect of any migration is dealing with errors and failures. Rollback in case of error is complex and confusing because so many aspects of the environment need to be considered. Attempting to perform a rollback manually is just begging for something to go wrong.

Choosing the right tool

Managing a migration manually is usually not practical, and it introduces considerable risk of mistakes and omissions. Investing in a migration management tool can save you time and money and help reduce the risk of a failed migration. Look for a tool that:

- Enables you to control all migration processes from a single management console.
- Automates the migration of servers and resources.
- Provides up-to-the-minute statistics to ensure you always know the current status of the migration project.
- Ensures true coexistence between migrated and unmigrated users, so users can continue working totally unaware of the migration project. The tool should be able to synchronize all changes made during the coexistence period in both directions (from source to target and from target to source), including changes to passwords, group membership, and resource permissions.
- Automatically updates permissions and resources after migration.
- Detects errors during migration and provides automated rollback. The tool should be able to pinpoint which users are causing the issues and roll back only those users.

Planning Active Directory migration scenarios

If your migration involves migrating only users, groups, and computers from one domain to another, the process will not be that complicated. However, most Active Directory migrations are complex, and having the right tools to manage the migration is critical. If your migration involves scenarios like the following, consider investing in a quality migration management tool such as Migration Manager for Active Directory.

Intra-forest migration

An intra-forest migration is typically done to reduce the number of domains. This can help relieve the stress of managing the overall Active Directory environment and deliver cost savings, since you'll need fewer operating system server licenses and less hardware. The biggest stumbling block with an intra-forest migration is ensuring that the users have continuous access to their resources; users will want daily network activity to function as normal.

Inter-forest migration

An inter-forest migration is typical when one company purchases another and wants a centralized Active Directory environment rather than forest trusts. In an intra-forest migration, permissions are a key concern. First, the existing forest domain administrators must have

Administrators need regular statistics and reports so they can always know the status of the migration. Reports should indicate the percentage of the migration completed and detailed statistics on the number of successful and failed migrations of users, groups, servers, resources, permissions, etc.

You can simplify and speed up your migration—and ensure a cleaner target environment—by migrating only the accounts that are needed in the target domain. A tool like Migration Manager for Active Directory can identify expired, disabled, and system accounts and omit those accounts from the migration.

permission to migrate the users, groups, and computers from the external domain. Second, users being migrated to the new domain will likely need access to resources in their old external domain for some period of time, and this requires that the external domain provide appropriate permissions.

Managing this access manually is time-consuming and prone to error. A migration tool like Migration Manager for Active Directory can help ensure that all required access is available throughout the migration.

Site topology migration

Migrations that involve migrating and collapsing Active Directory domains and forests into one another are also complex. At the top level, considerations for network IP ranges will need to be solved, including any VLAN configurations. Next, the site topology for replication will need to be analyzed and potentially updated. If one of the domains currently fits into a hub-spoke site topology and the other domain fits into a complete mesh, the migration of the one domain into the other will need some attention to ensure that the domain controllers, DNS servers, DFS servers and resources, and desktops are migrated from one environment to another.

A tool such as Migration Manager for Active Directory can help you successfully execute a site topology migration by providing the detailed information you need.

Non-trusted domain migration

When an external domain must be migrated into an existing domain in an Active Directory forest, trust relationships are normally established to facilitate the migration. In some instances, however, security restrictions prevent creation of this trust relationship, making the migration more difficult.

Some third-party tools, including Migration Manager for Active Directory, can handle this migration scenario, allowing all of the objects from the external domain to be migrated into the Active Directory domain without the establishment of a trust.

Advanced user and group object property migration

You can simplify and speed up your migration—and ensure a cleaner target environment—by migrating only the accounts that are needed in the target domain. A tool like Migration Manager for Active Directory can identify expired, disabled, and system accounts and omit those accounts from the migration. You will have more time to verify that the accounts you need were properly migrated because you won't be wasting time trying to clean up accounts that were unnecessarily migrated from the source domain.

Migrated object property customization

In most migration scenarios, the source domain and target domain have different philosophies, management styles, user property requirements, and databases that help manage user account properties. Manually updating the migrated user properties would take more time than the migration itself, so having a tool to automate the process is invaluable.

If the source domain does not have the same user properties as the target domain, but there is an external database or configuration file that lists the desired properties, Migration Manager for Active Directory can import these additional user properties into the migrated user property details during the migration, saving you considerable time and effort.

Active Directory delegation migration

Powerful delegations can be granted in Active Directory in order for different users or administrators to control different Active Directory accounts. Delegation typically occurs at an organizational unit (OU) level, which grants control over the objects

contained within the OU. In most cases, groups are granted delegated control of functions such as resetting passwords, user management, group membership management, and overall group management. Since these delegations occur at the OU level and are configured for groups, these delegations must be documented, tracked, and validated during and after the migration.

Trying to manage the migration of delegation manually is a daunting task. Instead, consider using a tool such as Migration Manager for Active Directory, which provides seamless control and management of this level of detail to help you successfully migrate the delegation of control over accounts in OUs.

Migrating resources

The migration of resources from one domain to another, or from multiple domains into a single domain, presents some of the most challenging issues in a migration, including the following considerations.

Resource permissions

In Active Directory, permissions are assigned to users via access control lists (ACLs). Each list contains references to SIDs of the accounts to which the permissions are granted. To ensure that all resources are still available after the migration, these ACLs need to be updated with the new SIDs for the target domain. This is not an easy task, considering the volume of users and groups that need to access a single resource in one domain, with potentially hundreds of groups listed on a single ACL, containing potentially tens of thousands of users. A tool like Migration Manager for Active Directory automatically provides these updates.

Service accounts

Service accounts and the accounts used to run scheduled tasks must also be migrated to the corresponding target accounts to ensure that services and scheduled tasks will run correctly after their corresponding service accounts have been migrated. A tool such as Migration Manager for Active Directory can automatically update service accounts.

Desktops

Migrating desktops from one domain to another has always been a pain point because of the work that must be done to each desktop. The migration of the computer account in Active Directory is relatively easy; the difficult part is changing the domain membership on the desktop itself so that the user can log on as a user in the target domain. This has historically required configuring the desktop to change the domain membership and then rebooting the desktop.

The right tool can greatly simplify desktop migration. With Migration Manager for Active Directory, for instance, users need only to log off and then log back on to see the new domain and log on with their newly migrated user accounts. Migration Manager handles all of the domain configurations on the desktop, including the new domain being listed on the logon prompt for the user.

Laptops

Laptops are a stumbling block in most migrations because they are not normally connected to the corporate network. In most cases, the laptop is not migrated until it can successfully connect back to the physical network, which might be months for some mobile users and their laptops.

Migration Manager for Active Directory addresses this issue by providing logon scripts that alter the laptop domain configuration to make the user—even when he or she is still remote—part of the target domain and no longer associated with the source domain.

Servers

In addition to desktops and laptops, servers also need to be migrated. This includes not just resource servers,

The right tool can greatly simplify desktop migration. With Migration Manager for Active Directory, for instance, users need only to log off and then log back on to see the new domain and log on with their newly migrated user accounts.

Investing in tools like Reporter and Migration Manager for Active Directory can save you time and money and reduce migration risk by automating migration tasks and providing detailed migration reporting and centralized management.

which were addressed above, but servers running Microsoft Windows® operating system–based services that are Active Directory domain aware and specific. Services—like Exchange, SQL Server, SharePoint, IIS, SMS, and SCCM—and even NAS/SAN devices need to be updated to be migrated to the new domain. Migration Manager for Active Directory automates all of these processes to simplify your migration.

Cleanup

As part of the post-migration cleanup, the source domain SID (which became the SID history on the target domain user account) needs to be deleted. Although this is not a highly complex task, it is necessary in order to ensure the security of the new domain. A tool like Migration Manager for Active Directory can automatically clean up this property for all migrated users, eliminating human errors that could introduce security risks.

Conclusion

Active Directory migrations can be challenging, complex, and time-consuming, but having the right tools can speed your migration and help ensure its success. Begin your migration with a careful inventory of your current environment. Collecting this information and developing appropriate reports manually can be difficult and is prone to error, so consider using a third-party tool such as Reporter to automate the process and ensure you have an accurate picture of your source environment.

Once the migration begins, there are many moving parts that need to be managed, in order to minimize interruption to business operations. All migrated accounts should constantly be updated and verified so that access is not restricted or denied during the migration; this means that all servers, resources, and permissions need to be fully tracked and migrated. Every file and folder must be examined, and the groups associated with the old ACL must be updated to represent the new groups that exist in the target domain. In addition, all of the servers that run Exchange, SharePoint, IIS, SMS, SCCM, etc. must also be migrated from the source domain to the target domain in order to ensure seamless access to resources.

Migration is even more complex if you are migrating multiple domains into a single domain, migrating complex site topology structures, or migrating domains that can't have trusts established. Investing in tools like Reporter and Migration Manager for Active Directory can save you time and money and reduce migration risk by automating migration tasks and providing detailed migration reporting and centralized management.

About the author

Derek Melber, MCSE and MVP, is president of BrainCore.Net AZ, Inc., independent consultant, and speaker, as well as author of many IT books. Derek educates and evangelizes Microsoft technology, focusing on Active Directory, Group Policy, security, and desktop management. As one of only eight MVPs in the world on Group Policy, Derek's company is often called upon to develop end-to-end solutions regarding Group Policy for companies. Derek is the author of *Windows Group Policy Resource Kit* from Microsoft Press, which is the authoritative book on the subject. Derek is also author of Group Policy Video Mentor from Pearson, the perfect resource for learning Group Policy basics. You can hire Derek to perform Windows security audits and also train your team on the finer points of Windows security. You can reach Derek at derekm@braincore.net.

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.

WP-BPActiveDirMig-US-TG-2013-01-09