The 12 Essential Tasks of Active Directory Domain Services

Using the right tools and processes helps reduce administrative overhead and ensures directory service is always available

By Nelson Ruest and Danielle Ruest

Sponsored by DELL

Sponsored by DELL

ABSTRACT

Active Directory Domain Services (AD DS) administration and management includes 12 major tasks. These tasks cover a wide breadth of business needs and are not all performed solely by AD DS administrators. In fact, administrators can and should delegate several tasks to other members of their technical community, technicians, help desk personnel, even users such as team managers and administrative assistants. While delegation is a way to reduce the amount of work administrators have to do when managing AD DS infrastructures, it really only addresses one or two of the 12 tasks, for example, user and group administration as well as end point device administration. The other ten tasks can be staggering in nature—security, networked service administration, OU-Specific Management, Group Policy Object management and many more—and because of this can take up inordinate amounts of time. You can rely on Microsoft's built-in tools to reduce some of this workload, but are the native tools enough? Perhaps it's time to reduce AD DS administration overhead by automating most tasks and tightening internal security. Address this by first, determining what the twelve essential labors of Active Directory are and then, see how you can reduce AD DS workloads through the implementation of proper management and administration tools.

Table of Contents

A Report by

Les Entreprises Resolutions Ltd. Enterprises

www.Reso-Net.com

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 more than 20 years. Their system designs include core application deployments such as e-mail and collaboration. They have also been working with virtualization for more than 10 years. Their recent books include *Configuring Windows Server 2008 R2 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.

ACTIVE DIRECTORY DOMAIN SERVICES ADMINISTRATION

Any systems administrator will agree that Active Directory Domain Services (AD DS) offers comprehensive services for network administration. In fact, AD DS goes beyond the simple Lightweight Directory Access Protocol (LDAP) services most manufacturers publish. An LDAP service is designed to provide an organized set of records, often using a hierarchical structure. For example, a phone book is a simple directory.

Active Directory Domain Services is a directory service that provides a means of securing and managing a Windows network. It also supports links and integration features with other Windows-based services. Because of this, AD DS is the primary directory that is designed to rule and manage users, computers and servers in a distributed network hierarchy.

However, AD DS is first and foremost based on a database—a hierarchical database (see **Figure 1**). As such, the directory database contains a schema—a database structure. This schema applies to every instance of AD DS, but it can be extended as when you integrate directory-aware applications such as Microsoft Exchange, Microsoft SharePoint and other into your network structure.

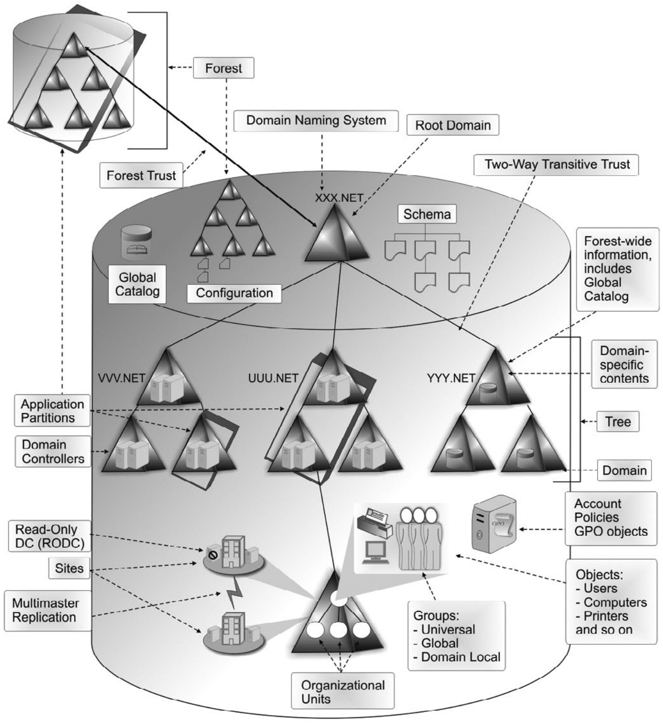

***Figure 1:** The Active Directory Domain Services database structure*

An AD DS instance is defined as an Active Directory forest. The forest is the largest single partition for any given database structure. Everyone who participates in the forest will share a given set of attributes and object types. Forests can be grouped together to share certain information. Windows Server 2003 introduced the concept of forest trusts, which allow forests to share portions of their Active Directory database with others and vice versa. This concept has since been improved in Windows Server 2008.

By default, the AD DS database includes over 200 object types and over 1,000 attributes. When you extend the AD DS database, you add more object types or attributes. For example, Microsoft Exchange practically doubles the number of objects and attributes in the forest when it is installed in an AD DS environment.

Like any database, AD DS categorizes the objects it contains, but unlike relational databases, the AD DS database structure is hierarchical because it is based on the Domain Naming System (DNS) structure. In a forest, the root point—analogous to the home page in a DNS structure—is the root domain. Every AD DS forest must contain at least one domain. Domains act as discrete object containers within the forest. Domains can be regrouped into trees. Trees are segregated from each other through their DNS name.

Every forest will include at least one tree and one domain. The domain is both a security policy and administrative boundary within the forest. It is required to contain objects such as users, computers, servers, domain controllers (DCs), printers, file shares, applications, and much more. If you have more than one domain in the forest, it will automatically be linked to all others through a transitive two-way trust.

The domain is defined as a security boundary because it contains rules that apply to the objects it contains. These rules can be in the form of security policies or Group Policy Objects (GPOs). Security policies are global domain rules, but they can be refined through fine-grained password policies and applied to specific groups of objects within the domain. GPOs tend to be more discrete and must be applied to specific container objects. While domains are discrete security boundaries, the forest will always remain the ultimate security boundary within an AD DS structure. The domain is termed an administrative boundary because, the policies that apply to its objects do not cross the domain boundary.

Domain contents can be further categorized through grouping object types such as organizational units (OUs) or groups. Organizational units provide groupings that can be used for administrative or delegation purposes. Groups are used mainly for the application of security rights or email distribution lists.

Forests, trees, domains, organizational units, groups, users, and computers are all objects stored within the AD DS database. As such, they can be manipulated globally or from a local Domain Controller. One major difference between Active Directory and a standard database is that in addition to being hierarchical, it is completely decentralized. Information resides in each domain controller and all DCs—except Read Only Domain Controllers (RODCs)—can initiate changes which will be replicated to others through the multi-master replication model.

As you can see, an AD DS environment can become quite complex and can be quite a burden to manage.

In addition, there are two clear contexts of administration within an AD DS database:

- Service administration which ensures that the AD DS environment functions properly, and

- Data administration which provides the entities that rely on AD DS—users, applications, services and more—with the information they need to properly perform their work.

AD DS administrators and technicians usually manage Service administration. Data administration is often delegated to other members of the organization such as individual users, managers, and, in the case of data fed to applications or services, the application developers and administrators.

Twelve Categories of AD DS Administration

When you understand the complexities of AD DS database contents and interaction, you can see that there are several different types of operations required to ensure an AD DS environment operates efficiently and reliably. In fact, Active Directory Domain Services administration or management covers 12 major activities. These activities and their breadth of coverage are described in **Table 1**, which also outlines which tasks focus on data or content management and which are concentrated on service administration, or which can be delegated and which require high-level administration rights.

Depending on the size of your network, each of the activities included in **Table 1** may be a fulltime role in many organizations. Delegation of this work, both across organizational and geographical boundaries help to spread the work effort and develop skill sets in the resource pool. However, the primary tools supplied by Microsoft do not lend themselves well to this distributed model that is required in todays' enterprises. Delegation, audit logging, reporting, and managed controls are all required for effective IT operations, and are primarily driven by audit controls mandated by the leadership of your company. All of the 12 primary AD DS management efforts must be auditable, reportable, controllable and manageable.

Managing the 12 Task Categories

Managing these tasks takes a lot of work. This is why it is so important to automate as many of the tasks as possible. Windows

Table 1: The Twelve Tasks of AD DS Administration, continued on page 3

Task	Description	Service	Data
1. User and group account administration	This includes user password resets, user creation and deactivation, user group creation, and membership management. • Password changes should be delegated to the help desk. • Massive account changes and service account administration should be the responsibility of administrators. • Global group memberships should be managed by user delegates.	☐	☑
2. Endpoint device administration	All computers in a Windows network environment must have a computer account. This is how they interact with the directory and how the directory interacts with them. • Should be delegated to technicians.	☐	☑
3. Networked service administration	This includes publication of network file shares, printers, Distributed File System (DFS shares, application directory partitions, possibly Exchange email, and so on. • Should be delegated to the administrator of each service type.	☑	☑
4. Group Policy Object (GPO) management	GPOs provide the most powerful model for object management in Windows Server. • Should be delegated to appropriate technicians. • A central GPO steward should control GPO proliferation.	☑	☐
5. DNS administration	DNS is closely tied to the directory, and the operation of the directory service is based on a properly functioning dynamic DNS infrastructure. • Because DNS is integrated with the directory, directory DNS administration is the responsibility of the domain administrator.	☑	☐
6. Active Directory topology and replication management	Replication is at the very core of the directory service operation. It covers the configuration of subnets, sites, site links, site link bridges, and bridgehead servers. You should rely heavily on the Knowledge Consistency Checker (KCC)—a service that automatically generates replication topologies based on the rules and guidelines you give it—to control replication. • This is the responsibility of the domain administrator.	☑	☐

PowerShell is a great help and so is the Active Directory Administration Console (ADAC), however, this all depends on how your network is organized and how many users or computers you need to manage. Small networks can be managed by a single person. Medium networks begin to require more than one person and also require delegation. Large networks or world-wide networks require a strong division of tasks and responsibilities, maximum delegation and complete automation.

Yes, you can perform most of these tasks with the native tools and the native automation features of Windows Server, but you'll also have to take the time to become a PowerShell expert and fully understand the intricacies of your AD DS environment.

Relying on Third-Party Tools

While Microsoft has done a good job of bringing AD DS administration together under one roof with the new tools introduced in Windows Server 2008, there is still a lot left out. Making AD DS administration easier is the goal of the third-party products such as Quest ActiveRoles Server (see http://www.quest.com/activeroles-server/).

Your goal when looking to third-party tools should be to reduce administration overhead and ensure complete AD DS lockdown.

Table 1: The Twelve Tasks of AD DS Administration, continued

Task	Description	Service	Data
7. Active Directory configuration management	Configuration administration involves forest, domain, and organizational unit (OU) design and implementation. It also involves Flexible Single Master Operations (FSMO) role, global catalog servers, and DCs placement, including RODCs. One additional activity that is related to configuration management is time synchronization. AD DS relies on the PDC Emulator role to synchronize time in the network. • These tasks are the responsibility of the forest and domain administrators.	☑	□
8. Active Directory schema management	AD DS is a database, albeit a distributed one. As such, it includes a database schema. Schema modifications are not done lightly because added objects cannot normally be removed, although they can be deactivated, renamed, and reused. • This is the responsibility of the forest administrator.	☑	□
9. Information management	This refers to the population of the directory with information about the objects it contains. User objects, shared folders, and computer objects can include owners; groups can include managers; printers and computers can include location tracking information. The Active Directory Schema Management console can be used to add or remove content from the global catalog and determine whether an object should be indexed. You can also assign NTDS quotas to make sure no one adds or extracts more information than permitted in the directory. • Delegate as many of the information management tasks as possible to appropriate personnel within your organization.	□	☑
10. Security administration	Security administration covers everything from setting Domain Account and fine-grained password policies, assigning user rights, managing trusts as well as access control list (ACL) and access control entry (ACE) administration. • This is the responsibility of the domain administrator or designated operators to whom it has been delegated.	☑	□
11. Database management	Database management involves Ntds.dit maintenance as well as AD DS object and GPO protection. Includes managing the LostandFound and LostandFoundConfig containers, which are designed to collect homeless objects in your directory. Also includes compacting the directory database on each DC. Although AD DS regularly compacts its own database automatically, it is good practice to compact it manually. This also includes object recovery from the AD DS Recycle Bin. • This is the responsibility of the domain administrator.	☑	□
12. AD reporting	Generate reports from your directory to know how it is structured, what it contains, and how it runs. There is no default centralized reporting tool, but you can export data at several levels of the directory. You can also generate GPO reports with the Group Policy Management console. • This is the responsibility of the domain administrator and the GPO steward.	☑	☑

This is why you need a product that will first, address each of the 12 task categories, and second, provide support for delegation as well as full system automation. Ideally, the tool will offer the majority of the following functions:

1. Automatic user and group provisioning, reducing group and object management overhead.
2. Automatic computer account provisioning.
3. Controlled delegation to ensure networked services and other tasks can be completely and confidently delegated to appropriate personnel in your organization.
4. Group Policy integration to reduce GPO administration overhead.
5. DNS Management integration to simplify hierarchical database structure administration.
6. Topology and replication management tools to ensure the directory is always working at its best.
7. Configuration administration to help graft and prune the forest as needed as your organization changes.
8. Control over the schema modification process to ensure AD DS database stability.
9. User self-service and automation to support information management within the directory.
10. Complete security administration of the directory, creating a sort of firewall around the directory structure to protect it.
11. Database management capabilities to ensure the NTDS. DIT database runs at its best.
12. Full reporting both online and offline to ensure you are always up to date on the structure and operation of your directory service.

These twelve features focus on the 12 essential tasks of AD DS, however, there should also be additional features such as:

Automation, integrating the management tool with Windows PowerShell to help generate new scripts automatically.

Change control, ensuring that the proper authorities provide sign off on major service changes and to guarantee that all changes are tracked.

Extensibility to integrate automation and administration tasks to further simplify directory administration.

In the end, you'll see that using a single, integrated tool will greatly simplify the administration of large directory structures and provide an easy way to manage such a complex environment.

FINAL THOUGHTS

Managing large directory structures can be unwieldy, especially if you don't have the tools to properly delegate, manage and audit actions. Even so, when you try using the various built-in tools Microsoft makes available to perform the work, you end up having to become an expert in at least twelve different task categories and risk not being able to conform to other requirements such as: auditing, reporting and management of distributed or external resources.

Given the need today to do more with less and given the little free time most administrators have on their hands, the very best approach is to rely on one single tool set that can tackle all directory tasks in a standard interface. This is where tools such as Quest ActiveRoles Server can help. ActiveRoles Server can greatly simplify AD DS management and administration tasks for you while keeping your directory completely secure. Better yet, ActiveRoles Server can help you automate the most routine tasks you must undertake to keep your directory service humming. Isn't it time you took a proactive step in reducing your workload? Download a free trial and find out more at http://www.quest.com/activeroles-server/. Better yet, review their active community site at http://communities.quest.com/community/activeroles