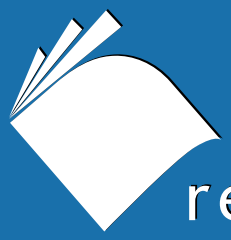

realtimepublishers.com™

The Administrator Shortcut Guide™ To

Active Directory Security

SCRIPTLOGIC

Derek Melber
and Dave Kearns

Copyright Statement

Chapter 2: Active Directory Security

AD security is not a single setting; it is a compilation of settings that is multifaceted and can become very complex. The default AD security settings handle the basic control of objects such as user accounts, group accounts, and computer accounts. For small companies, this default configuration might be sufficient. For larger companies, the built-in security will be quickly outgrown quickly and additional security settings and design must be considered and implemented. Regardless of the size of the company, a firm grasp of AD security settings is necessary to ensure a secure and stable IT infrastructure.

If security is not established early in the AD environment, the entire environment can spiral out of control quickly. This spiraling is a result of the number of security settings that can be set, which grows almost exponentially as additional objects and features are added to AD—consider that a single OU has nearly 1000 permissions that can be set to control its contents. This complexity requires consideration as early as possible in the implementation of AD. During the design phase of AD, the security of AD objects should be considered and documented. The objects that need to be considered for security include:

- Domain controllers
- Servers
- Client computers
- User accounts
- Group accounts
- OUs
- GPOs

The security that you design for AD must be implemented properly to be effective. Failure to follow your design documents can leave AD vulnerable to attacks from both within and outside of the LAN. In addition, AD security is very difficult to audit and track if not set up properly. In some cases, it will be easier to start over rather than to attempt to secure the AD environment after it has been installed and configured with many objects, settings, and features.

Another key aspect of AD security is management. The management phase is critical because it is at this stage that ongoing AD security must be maintained. Whether it is giving users the ability to add members to groups or locking down computers that are located in the reception area, the management of the security for AD must be procedural and consistent.

In this chapter, we will explore delegation of administration within AD as well as the implications of AD structural design on security. Determining the best AD design for your environment is an important part of effective security. In addition, a key factor in AD security is directory administration.

Directory Administration

Directory administration for Windows AD spans well beyond the AD database. With AD, security needs to be considered for all aspects of object management, GPO management, DNS management, and general domain controller management.

If you are coming from a Windows NT background, AD management might seem foreign, as the management of objects, policies, DNS, and domain controllers could not be segregated in NT. With NT, the objects were only controlled at the domain level; not at any level below the domain. This setup did not allow for delegation of administration to any objects in the domain. There were groups, such as the Account Operators and Server Operators, which allowed for some users to have control over a subset of objects in the domain. However, these groups did not allow for control over a subset of these objects, just the set of these objects as defined by the domain.

This mindset is dramatically changed with AD. In AD, delegation of administration allows for the domain administrators to delegate tasks to junior-level administrators and power users within a department. The same options are available for Account Operators and Server Operators as were available in NT, but with AD, these groups are not a suggested means to give delegated privileges. Instead, delegation of administration is provided at the OU level (it is also provided at the domain level, but the OU level is most common). This delegation is accomplished by configuring the ACL on an OU. As there are almost 1000 permissions associated with a single OU, these permissions allow granular control over which task and function the domain administrator will delegate to the user.

As you can imagine, the options of what can be delegated are almost endless. Thus, delegation of administration must be designed into the AD security and implementation early on. As we will explore, the security related to delegation depends on the OU design and object placement in those OUs. If the AD implementation is allowed to progress without considering the security related to delegation of administration, the process to rearrange the objects to support a desired delegation model becomes very difficult. There are general guidelines that you need to keep in mind as you consider the security of the directory administration:

- The rules that applied to NT usually don't apply to Win2K and WS2K3 AD. This idea is difficult for many companies and administrators to get past. Much of the failure to consider this reasoning is that the NT methods have been in place for years and seem to work well.
- The AD security design needs to take full advantage of the power of AD. It is a shame to have companies spend so much time, effort, and money moving from NT to Win2K and WS2K3 AD to then not take advantage of the power that AD provides. The power of AD is in the ability to reduce the number of domains, which in turn, reduces the number of domain controllers, administrators, and trusts (administrative overhead) and increases the ability to centrally administer the environment.

- The group design is essential for optimizing the security configuration of the directory. In some OSs, it is common to have built-in groups that provide widespread power over accounts, servers, and services. With AD, these groups can still be used, but it is better to also use other groups that will be delegated administrative control over specific aspects of AD. The reason this design is better is that the built-in groups many times have control over all user accounts or all servers. With the delegation model, groups have control over a subset of the user or computer accounts. In addition to the limitation of object scope, the delegated group usually has a limitation set on the capabilities over those objects as well.

As the security of AD is designed, it will be important to logically organize the administration model. These models are typically implemented through the OU design. There are numerous designs and considerations. The following list highlights common methods for breaking down the administration model in AD:

- Regional—It is common to have administration at the regional level (for example, West, East, Europe, Australia). Doing so provides administrators with the ability to control a larger group of accounts.
- Departmental—Like most companies, administration might be broken down into departments such as Human Resources, IT, Accounting, and Sales.
- Object function—Administration of the directory might also be broken down by object function. It makes sense that the administrator of the HR user accounts is not in charge of the Financial servers. Typical object categories include user accounts, employee computer accounts, IT user accounts, servers, domain controllers, and service accounts.

A poor decision that many administrators make is to duplicate the organizational chart for the company in an attempt to create the structure for security of the directory. Unfortunately, the organizational chart is not an effective AD security model because administration crosses too many boundaries that the organizational chart creates. This causes additional overhead in configuring and managing the directory security.

Create Usable Boundaries

There are many boundaries that are defined within AD. Some of the boundaries are hard coded and others can be created manually. The boundaries are usually defined based on where the delegation of administration is established. There are three primary drivers for delegation of administration of AD: organizational, operational, and legal. These delegation drivers must be included when the AD structure is created.

- Organizational—In this delegation model, parts of the organization share the infrastructure to save costs but must have the ability to operate independently from the rest of the organization.

- Operational—In this delegation model, a part of the organization or a specific application (or service) can create special constraints compared with the other components of AD. These constraints might include directory configurations, availability, or security. Examples of this model include military, hosting, extranets, and outward-facing AD environments.
- Legal—In this delegation model, a legal requirement forces a part of the organization to function in a more secure or specific way. This might require restricted access to AD services or data. Examples of this model include financial and government agencies.

AD can be structured with domains, trees, and forests. The domains are standalone entities that can be associated with other domains. When domains share the same DNS extension, they are referred to as a *tree of domains*. An example of a DNS extension that meets this criterion is auditingwindows.com. Domains that can exist within this tree include root.auditingwindows.com and company.auditingwindows.com. When one or more trees are spliced together, they form a *forest*. The forest is a grouping of trees. Each tree will have a unique DNS namespace.

Once AD structural boundaries are established, consider the AD security boundaries that are associated with the structural boundaries. The following list highlights common boundaries that are associated with AD security:

- Enterprise Admins group—A built-in group that has forest-wide scope, the Enterprise Admins group's capabilities include being able to administer any user, computer, service, or object in any domain within the forest. There is no higher security group than the Enterprise Admins group.
- Schema Admins group—This group is very important because it also has forest-wide scope. However, the capabilities are only for the schema. The schema controls the creation of the objects within the forest and dictates the properties of each object.
- Domain Admins group—This group has been around Windows domains for a long time, and the scope remains the same. The Domain Admins group can only administer the domain for which it is created. (There are other important groups that only have domain scope. These groups are not as powerful as the Domain Admins group.)
- Schema—The schema is the core structure underlying every new object that is created. As I previously mentioned, the schema determines the properties for each object. If a change is made to the schema, every object in the forest can be affected.
- Account policies—The account policies control the passwords for domain user accounts. The account policies include password policy, account lockout policy, and Kerberos policy. These settings do not pass the domain boundary. For example, if a password length of eight characters is set at the top-level domain in a tree, the other domains in the tree will not inherit the eight-character password. Instead, they have their own unique account policy that dictates this setting.
- GPO scope—GPOs are designed to control objects within their scope of influence. The different scopes of influence that a GPO can have include site, domain, and OU.

- Group scope—There are different types of groups within AD. The groups have a wide variety of scope based on the configuration of the domain. The different groups include domain local, global, and universal. Domain local groups are only available to computers in the domain in which the group is configured. (If the domain is still in mixed-functional level, the domain local groups will only be seen by the domain controllers, not any of the other domain members.) Global groups are designed to function within the same domain only. Universal groups are new to AD and are designed to cross domain boundaries.
- Delegation of administration—Delegation of administration is designed to have a boundary based on your needs of administration. Typically, delegation of administration is designed at the OU level, but that is not a strict rule. There are needs and reasons to design delegation of administration at different levels, including site, domain, and object.

When you are considering the boundaries and design of AD security, you need to have a clear understanding of what the delegation drivers are. Delegation drivers dictate how and why the AD structure is designed. Unfortunately, there is not an easy method of determining the delegation drivers and the final design of AD from those drivers. The benefit of the flexibility provided by this setup is that there is no wrong answer, simply degrees of effectiveness.

Thus, before AD is implemented, there needs to be a planning phase. This phase might take longer than you anticipate, with so many design considerations. Security is one of those considerations—especially the delegation model and the GPO implementation plan. I have seen planning phases that take as long as 6 months, but the time required depends on the size and complexity of the company network.

After the planning phase is the testing phase. The testing phase can determine whether the results of the planning phase are effective or, as is often the case, are not. This phase gives ample time to develop a new plan that can then be tested. I have seen testing phases that also last 6 months or longer. The longer test phases usually result from additional planning phases to work out any kinks in the design.

As the security boundaries of AD are considered in the planning and testing phases, thought must be given to the level of autonomy, isolation, or a combination of both:

- Autonomy—Provides administrators with the ability to independently manage all or part of the service management and/or the data stored in AD.
- Isolation—Provides the administrators with the ability to prevent other administrators from controlling or interfering with service management and/or the data stored in AD.

With delegation of administration, almost any level of autonomy can be accomplished within any one domain. Regarding isolation, there are some key questions to ask to determine the appropriate level:

- If there is a department that is asking for isolation from the other departments, what would be sufficient for them?
- Would a top-level OU in the domain be enough?
- Do they require their own domain?
- Is it required that they be a domain in their own forest?

These are decisions that must be made with consideration of all aspects of AD security. Autonomy is much easier to accomplish than isolation. The reason is that administrators who have autonomy understand that other, higher-level and ranking administrators have the ability to control the same information that they control.

Select the Proper Directory Structure

The directory structure will be one of the final decisions that come from the AD security and structure planning and testing. The directory structure for AD must go beyond the main directory and include DNS. DNS is an integral part of AD, so much so that AD can't effectively function without DNS. There are many directory structure options, each having advantages that relate to security for the enterprise:

- Single AD domain—This structure is the ideal structure for any environment. If every security consideration, service, object, and application can function in a single domain, it should be the structure that is selected. This structure provides a single point of administration that is easier to secure than a multiple-domain environment. With a single domain, there are no trust relationships or cross-domain permissions to manage.
- Single tree forest—A single tree is simply multiple domains that share a domain suffix. With a single tree, all of the benefits of a single domain are lost. There will be a trust relationship between all domains in the tree. User accounts from each domain will be able to access resources in all other domains, if they are given permission to do so. There will be multiple Domain Admins groups—one for each domain. There will be multiple account policies that need to be designed and maintained. The GPO administrative overhead increases with each new domain that is considered in the structure, because each domain keeps track of its own GPOs.
- Multiple tree forest—A multiple tree forest structure is identical to a single tree forest with regard to security considerations. There are simply more domains and domain suffixes that need to be implemented.
- Empty root—An empty root structure is one in which the first domain (root domain) is designed so that it does not include any user or computer accounts. The other child domains under the root domain will contain all of the user and computer accounts. This setup is beneficial from a security perspective in that the Enterprise and Schema Admins groups are isolated from other users and administrators. With this design, a few administrators can be selected to control the Enterprise and Schema Admins groups, and all other administrators reside in the child domains, configured to be Domain Admins.

- Forest trust—New to WS2K3 is an option called the forest trust. The forest trust allows companies that have their own AD environment to "splice" their environments together. This splice does not share a schema, but it does allow all user and computer objects from one forest to access resources in the other forest. The forest trust has advanced hardware and OS requirements: All domain controllers need to be running WS2K3, and the domain and forest functional levels need to be increased to WS2K3 levels.
- DNS—DNS is the service that AD uses to resolve computer names and AD services for client computers, servers, and domain controllers. AD will not function without DNS. Therefore, it is essential to consider DNS in the design of AD and the security of AD. Some of the DNS security considerations with respect to AD include:
  - AD integrated zones—When a DNS zone is integrated with AD, it stores the DNS database in the AD database. The benefits of this functionality include fault tolerance, management, and authentication of computers attempting to update DNS records.
  - Secure dynamic updates—DNS now supports dynamic updates, which allows the computer to communicate with DNS to exchange computer name and IP address information to update the DNS database. The problem with this solution is that almost anyone can "spoof" the computer name and IP address, which will redirect communications from the valid computer to the spoofed computer. If secure dynamic updates are configured, the spoofing computer must be validated by the AD domain before it can update any records in the DNS database.
  - DNS ACLs—When a computer securely updates its DNS records, the records become the owner of the entry. This setup further protects DNS and AD, such that only the registering computer can update that record from then on.

Delegate Administration Whenever Possible

Delegation is one of the key security reasons to move from NT to Win2K or WS2K3 AD. The benefits that delegation provides are superior to any directory control mechanism that is available in NT. A chronic complaint about NT is that it does not provide any granular administration capabilities within the directory. The most granular administration possibilities are offered through Account Operators, Server Operators, Print Operators, and Backup Operators—groups that are built-in to the OS. There is the capability of creating additional groups within the directory and configuring special user rights for them. However, this feature only provides marginal improvements over the built-in groups, because the user rights do not allow control over a portion of the environment, only tasks within the environment.

AD delegation of administration provides granular control over objects within the directory. The following list highlights examples of common delegated tasks:

- Create user accounts—Provides the assigned delegate the ability to create user accounts. However, the delegate could not manage or delete the user accounts after the accounts are created. If this delegation were assigned at an OU, the delegate could only create user accounts in the specified OU.
- Delete user accounts—Provides the assigned delegate the ability to delete user accounts. The same rules apply as for the creation of user accounts in that the deletion of user accounts is the only task the delegate can perform, and the scope could be limited if applied to an OU.
- Manage user accounts—Management of user accounts is a common task. However, with delegation, the management scope can be limited to an OU, which include only a subset of user accounts in the domain.
- Reset passwords on user accounts—This task is one of the most prevalent Help desk call requests and can be delegated to the Help desk staff, management in a department, or a power user over a subset of users in the domain.
- Read all user information—Auditors, management, and security professionals need to have access to all account information to complete their jobs. However, this task of reading information is not for everyone, nor is it for these groups all of the time. With delegation capabilities, this task can be easily added and removed.
- Create, delete, manage groups—These tasks follow the same logic as the user accounts. They can be grouped together to give the delegate all three tasks or separated to provide the delegate with a narrower set of tasks for the groups in the domain.
- Modify the membership of a group—One of the specialized tasks included in managing a group is to add or remove members of that group. This is a good example of the granularity that can be accomplished with delegation of administration.
- Manage Group Policy links—GPOs have powerful results; thus, it is ideal to separate the roles of GPO management. AD delegation of administration enables an administrator to allocate one or many of the roles related to GPOs.

There many more capabilities of delegation of administration within AD to provide granular security control to any object. With all of this complexity, you can quickly see that planning will be crucial to a successful implementation of AD security with delegation. As we have already discussed, planning should not be bypassed. The testing phase will provide a time to verify that all security measures are upheld when the delegation of administration is implemented.

The design of delegation is, for the most part, integrated into the OU design. The reason for this integration is that delegation at the domain or site level has too broad of a stroke. Every user and computer account is included when delegation is performed at the domain level. The site delegation model has a similar problem, in that it encompasses too many objects to be a viable security solution. As OUs are the core to the logical structure of AD and to delegation of administration, great time and effort needs to be given to them during the planning and testing phases.

Certain tasks can even be delegated to non-IT personnel. For many, this concept is foreign and difficult to comprehend. However, after further consideration, you will find that it can improve efficiency, security, scalability, and ROI:

- Improved efficiency—Delegating administration to non-IT personnel can improve the efficiency of your IT staff. Instead of end users always calling the IT staff to get a common task accomplished, the users can call a coworker or manager to get the problem fixed.
- Security—When too many IT staff members have access to resources and AD objects, there can be vulnerabilities of rogue administrators and too many administrators. With delegation to non-IT staff, the burden can rest on the owner of the resource in many cases, by allowing control over groups and the resource itself to the owner of the resource.
- Scalability—AD by itself is very scalable. When the administration of common tasks is delegated to non-IT staff, the opportunity of growing the IT infrastructure without growing the IT staff becomes very possible.
- ROI—The ROI for installing AD and newer OSs on servers and client computers is very high as a result of delegation of administration. It is only with Win2K and later that users can be delegated administrative privileges because earlier OSs either can't function in a domain or have problems performing administrative tasks in AD.

Two Kinds of Administrators

As you consider how the delegation and overall security will be handled within AD, consider that there are two primary kinds of administrators: data administrators and service administrators. Each type of administrator has a role within AD, but the roles are quite different. Let's take a look at each type of administrator to get a feel for what the options are as you implement your security plan.

Data Administrators

Data administrators are responsible for maintaining data that is stored in AD. Here, the use of the term data might throw you off a bit. We are not talking about files and folders or typical database contents used to store company confidential information. Instead, we are referring to data that can be stored in AD. This includes user accounts, computer accounts, group accounts, and so on. However, this is not the same as what you might be familiar with from an NT domain. In an NT domain, you have control over all user, group, and computer accounts if you are in the Account Operators group. Instead, the focus of data administrators is on a subset of the domain objects. This subset delegation is accomplished by using the delegation of administration techniques that we have discussed and will explore in more detail in Chapter 4.

The computers that data administrators have control over must be domain members. This should encourage you to make all computers on the network members of the domain. If they are not members of the domain, they could easily become rogue computers that the data administrators don't have control over.

There are not data administrators created by default. There are some groups that could be considered data administrators groups, but these groups provide too broad of administrative privilege for most organizations. The process for creating these data administrators is to have the domain administrator create new user accounts and group accounts for these data administrators. The user accounts for data administrators should be different from the user accounts that are used for personal tasks such as checking email and writing memos. Once the data administrators' user accounts are placed into the data administrators groups, the administrators are ready to be given privileges to administer data in AD.

An important point is that data administrators don't create accounts for other data administrators; the data administrators are simply in charge of performing the administration work. We will see that the service administrators will be responsible for creating the groups for and managing the data administrators.

Once the data administrators groups are established, they should then be granted delegated administration over the subsets of data that is stored in AD. We have also reviewed how this is typically configured, which is at the OU level.

From an ROI position, the data administrator groups are important because they do not have to have the knowledge that the service administrators has. The data administrators only need to be responsible for the tasks that have been delegated to them, including managing user accounts, group accounts, and computer accounts. The data administrators are not responsible for knowing how to add new domain controllers, ensure replication has occurred, or how to add a new site to AD.

Service Administrators

Service administrators are responsible for more of the day-to-day tasks associated with managing and maintaining the AD infrastructure. They are also required to be more aware of the company security policy and procedures. The service administrators are responsible for more in-depth AD tasks than the data administrators are responsible for. Both the service administrators and data administrators are needed, but their job roles are significantly different.

The following list highlights tasks the tasks that the service administrators are responsible for:

- Install domain controllers—As the number of users and locations grow, there will be a need to install new domain controllers and place them where they will make the most impact.
- Manage DNS—As DNS is an integral part of AD, the service administrators is responsible for much of the management that is associated with DNS. This responsibility includes adding static records, performing backups and restorations, and troubleshooting any problems.
- Manage the Distributed File System (Dfs)—With Dfs providing more features and stability in Win2K and later, more and more companies have implemented this service. One of the useful features of Dfs is that it can be integrated with AD, which requires the service administrators to be responsible for the management of all the links and replicas that are configured in Dfs.

- Manage Global Catalog (GC) servers—The service administrators will be responsible for ensuring that all services and resources that rely on the GC have access to this service. With AD and Exchange relying heavily on the GC, management and availability of the GC servers is an important task.
- Manage the schema—The schema is vital to AD. When it is modified, the service administrators will be responsible for knowing what is being modified, how it is being modified, and keeping it available before and after any changes.
- Ensure directory availability—The service administrators are responsible for ensuring that AD is available at all times. This responsibility includes backups and restorations and disaster recovery. It also includes ensuring that AD is available for WAN links and remote access users. If AD is not available for the WAN and RAS users, GPOs and other key security settings might not be applied properly, leaving these client computers vulnerable to attack.
- Manage trusts—Trusts in AD are automatic, so the internal trusts require little to no management. However, the trusts that go outside of the forest follow the old NT rules. These trusts require management for creation, removal, and troubleshooting if the trust fails. Because a trust can allow a user from an outside domain access to an internal resource, trusts must be managed by the service administrators who are trained on what the vulnerabilities might be.
- Manage sites—Site management is not a day-to-day task, but it does fall into the scope of responsibility of the service administrators. Sites need to be managed if a new domain controller was brought into the domain, replication needed to be modified, new subnets were added, or a domain controller was being taken offline.

With all of these responsibilities, the service administrators will need to be a member of the AD deployment team. The service administrators will need to be well trained and skilled at all aspects of AD, even the tasks that the data administrators are responsible for. The service administrators will need to have a clear understanding of how security fits into the overall AD structure so that when any changes are made to AD, the security policies are maintained.

The service administrators will also need to have a complete understanding of GPOs. In many cases, the service administrators will be responsible for creating, linking, and/or maintaining the GPOs for the domains in the forest. Often, the security policy is implemented through GPOs. The service administrators will need to understand how the GPOs enforce security to user and computer accounts, including every nuance of security deployment to domain controllers, servers, and client computers, as well as IT staff, executives, and employees.

With the service administrators having broad, deep, and almighty powers in AD, these users must have a higher level of clearance than the data administrators or the typical employees have. A rogue service administrator can bring down a company, causing loss of data and income. All service administrators must have the highest level of trust with management. It is a good practice to have regular audits on the service administrators to ensure that they are performing their tasks properly and with the company's best interests in mind.

The number of service administrators should be limited, with the scope and power that they bring. The fewer service administrators you have controlling AD, the better. There should, however, be more than one service administrator, as one service administrator does not enable the environment of accountability that is required to maintain a secure AD.

Overlapping Administrators

It should be clear now what each type of administrator is responsible for. Data administrators keep tabs on the objects within AD, making sure users can log on, groups have the correct members, and computers are located in the correct OU. Service administrators work at a little bit higher level, making sure that AD is stable, available, and all services that work with AD are managed properly.

There can be an overlap between these two types of administrators if the company structure and plans allow for it. However, this overlap is only a one-way overlap. The one-way direction is on the side of the service administrators. A service administrator can perform the duties of a data administrator, but the data administrators can't perform the duties of a service administrator.

The service administrators are responsible for creating the data administrators' user and group accounts. The service administrators must then manage these accounts to ensure that the data administrators have the correct privilege and access to AD. This separation of duties is more important than just who can do what. From a company security standpoint, it is important to separate tasks so that one administrator does not have too much privilege.

Best Practices for Delegating Control in AD

You might be tired of me hounding you on the phases of planning and testing, but I can't stress enough how important these two phases are in the stability, security, and long-term effectiveness of your AD deployment. Thus, the initial best practice for AD delegation of control is planning and testing. The next best practice is to use the power of AD as much as possible by employing OUs for delegation, non built-in groups for delegation, and nested OUs for the optimum design of your delegation.

- OUs for delegation—OUs must be designed and implemented properly and the correct objects (user, group, computer) must be placed in them in order for delegation to be successful.
- Use of non built-in groups—Built-in groups give too wide of privilege in the domain, so the delegation design must include the creation and location of new groups designed solely for delegation.
- Use of special administrative accounts—For best security and autonomy of data administrators' and service administrators' tasks, it is ideal to create user accounts for when the user performs these tasks.
- Use of nested OUs—There will be various levels of data administrators within AD. Some will be delegated control over an entire data type, such as servers, and others might only be given a subset of the data type, such as file servers. This hierarchy is established by creating OUs and sub-OUs, with the delegated administration at the top having more privilege than those lower in the OU structure.

There are additional best practices and tips that have been successful for many organizations that use delegation of administration to control security of AD. One best practice while delegating administration is to not provide too much delegation. For example, suppose you are delegating administration to a user in the Sales department. You are giving the user the ability to control membership in the groups for the Sales department. The OU structure related to Sales might look something like

```
Sales
    Computers
    Groups
    Users
```

An easy solution for delegating the administration would be to create a new group in the Groups OU named Sales_Groups_Admins. You would then add the appropriate users from the Users OU to the Sales_Groups_Admins group. The final step would be to delegate at the Groups OU administrative control to change group membership to the Sales_Groups_Admins group.

Although this process would accomplish the goal, it also provides too wide of privilege for the members in the Sales_Groups_Admins group. As the Sales_Groups_Admins group is located in the Groups OU, all of the members of the Sales_Groups_Admins group can add or remove members to this group too. Thus, they could add employees to the group that should not have the privilege to modify group membership for the other groups in the OU.

A solution to this potential vulnerability is to create an Administrative OU at each level where delegation is performed. For example, the OU structure would now look like

```
Sales
    Administrative
    Computers
    Groups
    Users
```

You would still create the users in the Users OU, but you would not create the Sales_Groups_Admins group in the Groups OU. Instead, you would create this group in the Administrative OU. Then when you delegate administration for this group to control the group membership for groups in the Groups OU, it will not include the Sales_Groups_Admins group.

Another best practice when working with delegation is to perform regular audits on who has been given delegated administrative privilege to different levels in AD. There are two methods to audit this activity. If your company has the manpower and stamina to audit as the activity occurs, you will need to use the built-in auditing that is provided for the OS. If your company is running low on manpower and the IT staff already has too many things to do, it might be best to perform manual audits on the delegation in AD. This can be performed by first documenting where any delegation is configured. If documentation is available, tools such as dsacls.exe and acldiag.exe can acquire the delegation configurations at each level in AD. Then a quick comparison of the actual settings versus the documented settings can be performed.

Any delegation that performed at the domain level can typically be accomplished by using the built-in groups for domain administration. These groups include Domain Admins, DNSAdmins, DHCP Admins, RAS and IAS Servers.

Delegation control over sites and site replication is typically controlled at the forest level because site management is a forest-level function. You typically would not attempt to delegate specific site responsibilities because the service administrators responsible for site management would need to control all sites as a whole, not independently. Membership in the Enterprise Admins group would provide the typical site administration roles and responsibilities. If granular control over sites is needed, there are specific tasks that can be delegated.

Directory Tools

There are numerous directory tools that are available in a default installation of AD. These tools are essential to the core function, management, and troubleshooting of AD and its related services. There are also resource kit tools that help increase the management capabilities of the directory. As far as security-based tools, almost every tool can be tied back to security in some manner. Security is in almost every aspect of AD and the tools that manage it—from the files that run the directory to the accounts that reside in the directory to the sites that replicate the directory between domain controllers. Tables 2.1 provides the most common built-in, command-line, and resource kit tools.

Tool	Use	Security control
Built-In Tools		
Active Directory Users and Computers	Used by data administrators to manage all security principals, GPOs, contacts, AD shares, AD printers, and OUs	User accounts, group accounts, delegation administration, GPO management
Active Directory Domains and Trusts	Used by service administrators to create and manage trusts to external domains	Trusts that go outside of the forest
Active Directory Sites and Services	Used by service administrators to create and manage sites and replication	Controls replication schedule between sites and subnets associated with sites
Computer Management	Controls “computer” aspects such as hard drives, services, and the local Security Accounts Manager (SAM)	Local SAM (non-domain controller), services, shared folders, drivers

Tool	Use	Security control
DNS	Manage DNS	Secure dynamic updates, replication partners, manual DNS entries
Event Viewer	View tracked events for the system, applications, and security	View security logs
Routing and Remote Access	Manage routing and remote access services	Specify RAS protocols and security; determine RAS access for users
Command-Line Tools		
Adprep	Prepares your existing Win2K AD for WS2K3	Changes the schema to prepare for WS2K3
Ds* tools	Provides access to AD for creating, querying, deleting, and moving objects within the directory	Provides means for someone to access AD remotely from the command line
Shutdown	Allows the shutdown of a server remotely	Can shutdown a server or domain controller remotely from the command line
Bootcfg	Displays and modifies contents of the boot.ini file	Can change the main boot file of a server or domain controller remotely from a command line
Resource Kit Tools		
Dumpfsmos	Dumps Flexible Single Master Operations (FSMO) roles from AD	Provides location of all FSMO roles on each domain controller
EventCombMT	Gathers Event Viewer logs from the network computers and organizes them to files in a single folder	Access to security logs remotely
Lockoutstatus (Server 2003)	Dumps the lock out status of user accounts	Access to which accounts are locked out
Ntrights	Sets user rights on servers and domain controllers	Allows for remote user to set user rights from command line
Showacls	Displays the ACL for resources	Access to the ACL to see which users and groups have access

Table 2.1: Built-in, command-line, and resource kit tools for AD with the security controls that the tool provides.

For AD administration, the main tools are those that are built-in and provide a user-friendly graphical interface. These tools are designed to use the Microsoft Management Console. MMC allows for customization beyond the default Administrative Tools that are pre-built and available from the Start menu.

When an organization becomes too large or delegates administration to many different aspects of the AD structure, it becomes a necessity to build custom MMC consoles. Such consoles are easy to create and can be specific in what they show. When an MMC is customized, it is done so by importing snap-ins, which are the administrative tools themselves. There is a snap-in for almost any administrative task for the directory. The following list highlights common MMC snap-ins that are used to control AD and the security of AD:

- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers
- Active Directory Schema
- Active Directory Service Interfaces (ADSI) Edit
- Computer Management
- Dfs
- DNS
- Event Viewer
- Group Policy
- IP Security Policy Management
- Shared Folders
- System Information

Figure 2.1 shows the MMC and a list of snap-ins.

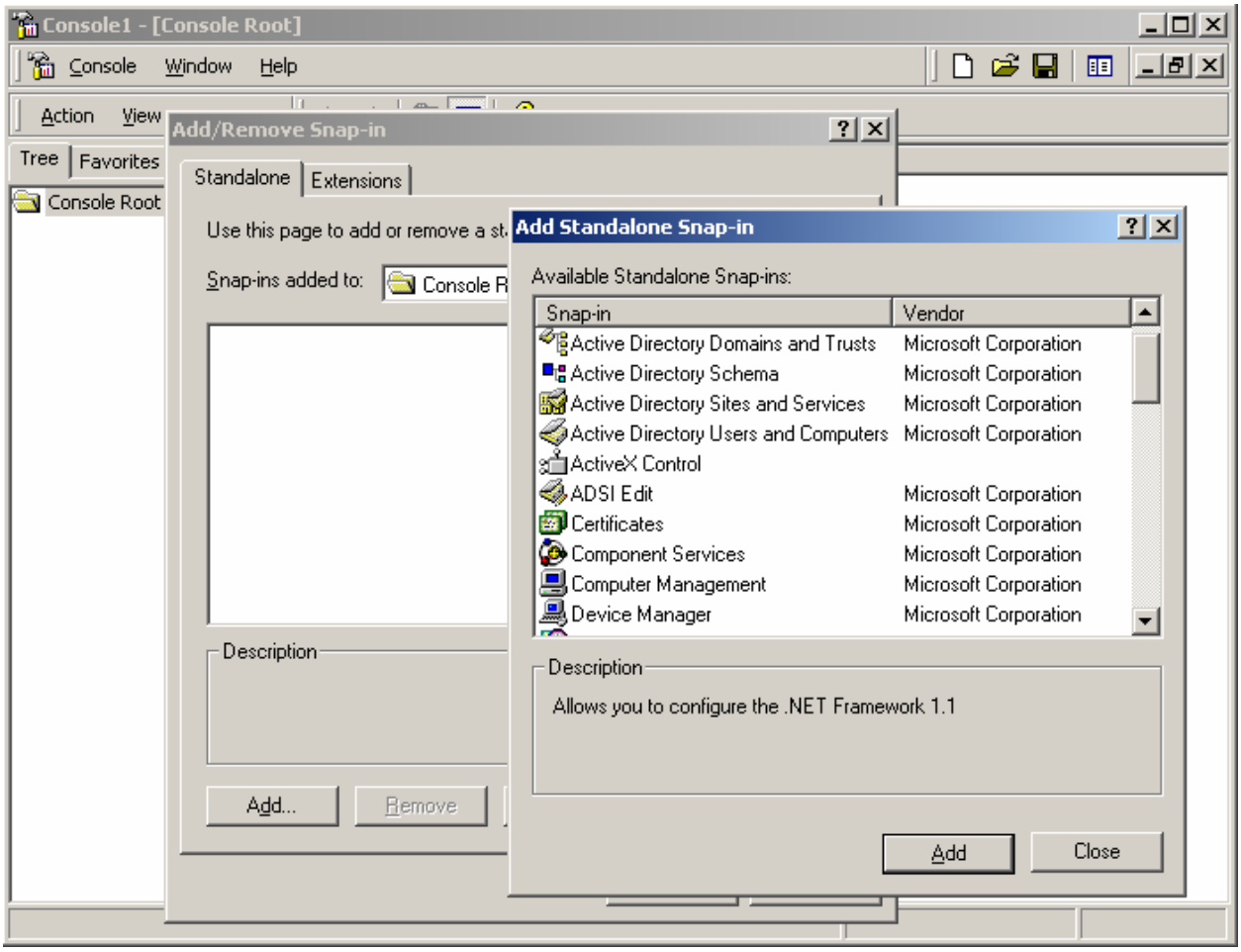

Figure 2.1: MMC with a list of snap-ins.

The benefit of the MMC is that the essential snap-ins can be grouped in a single interface, then saved in the MMC. After it is saved, it can be shared on a central server or sent via email to an administrator that has been delegated administrative access to resources within the snap-in.

For most organizations that use this method, the administrator or non-IT employee will need to have the tools that administer domain controllers, servers, and AD installed. This installation is easily accomplished, as the suite of tools is available on all domain controllers. The file that contains the suite of tools is called adminpak.msi. This installation package can be shared on a central server for installation across the network, sent via email to the administrator, or pushed out through a GPO. After the installation package is installed, the user will have the full list of administrative tools necessary to complete the delegated administrative task.

For some administrators, especially those that are non-IT employees, the full-blown administrative tool that comes with the adminpak.msi can be too much. Thus, instead of teaching and encouraging these administrators to use the tools, you can create Taskpads that narrow the scope of what they see in the interface. Taskpads are created within each snap-in and can be very specific with their focus.

An example of a Taskpad is providing delegated administrators the ability to see only user accounts and giving them the option to only reset the accounts' passwords. This option is useful for a non-IT employee that has been delegated the privilege to reset passwords for an OU full of user accounts. Typically, administrators must open Active Directory Users and Computers, then navigate to the correct OU. Once they arrive at the OU, they see all of the objects in the OU, including groups, computer accounts, other contacts, printers, shares, and other OUs. This view can be quite confusing. The Taskpad will show them a single view of the user accounts in the OU in which they have been delegated the ability to reset passwords. They will then have one option, which is to reset passwords for these user accounts. Figure 2.2 shows a Taskpad for resetting passwords for an OU.

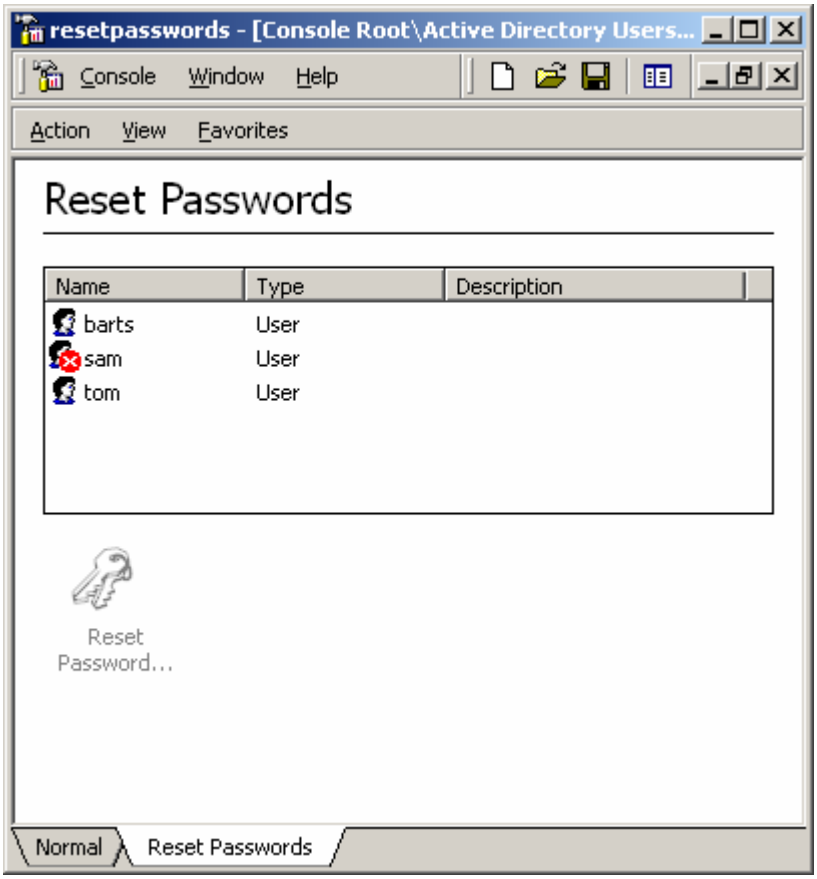

Figure 2.2: An MMC Taskpad providing the delegated administrator the ability to reset passwords.

The use of Taskpads can save many calls to the Help desk or the administrative staff, as users who have not been educated in the finer points of the administrative tools can quickly access the tasks that they need to perform. These Taskpads can also be placed on a central server, emailed, or manually copied to provide access to all administrators.

These tools and features perform useful services for data administrators and service administrators, but they can be clumsy for large organizations and fall short when there are too many resources, objects, servers, or users. Many of the tools have built-in limitations to show only 10,000 AD objects. These limitations can be overcome, but when an organization has 20,000 users, 50,000 groups, and 25,000 computer accounts, the list of objects can take a very long time to refresh in these graphical tools. At this stage, it can become a task in itself to try and find the object that you are looking for.

In addition to the lack of scalability of these tools, there is another limitation. The MMC can't import or support all of the features required to administer the domain and AD. Both data administrators and service administrators need a tool that can combine every feature that they might need to control, along with fully customizable interfaces. Such a tool would provide a one-stop shop for all of their needs, with the robust interface capable of supporting the customization required to make the job easy. There are many third-party tools available that provide such features. These solutions meet almost any need for data administrators and service administrators, including:

- AD migrations
- Active templates for easy delegation
- Auditing
- GPO administration and migration
- Cross-platform integration and management
- Built-in recovery for AD
- Advanced ADSI management
- Advanced AD querying

If your company is struggling to keep on top of AD security and management tasks, these tools can help centralize those tasks, making administration and delegation for everyone involved easier and more efficient.

Group Policy Management Console

The Microsoft Group Policy Management Console (GPMC) provides an interface that simplifies administering GPOs. This new tool has limitations—for example, it runs only on Windows XP Professional and WS2K3—however, these limitations are easy to overcome. Even in a pure Win2K AD environment, GPOs can be administered from a single Windows XP computer running the GPMC.

What advantage does this tool provide over the old method of managing GPOs? The answer is clear if you have ever used the old method of managing GPOs. The old method relied upon the Group Policy tab located on the properties sheet of a site, the domain, and all OUs. This one tab, which Figure 2.3 shows, gave a masked view of the entire GPO picture, which caused much confusion among most administrators.

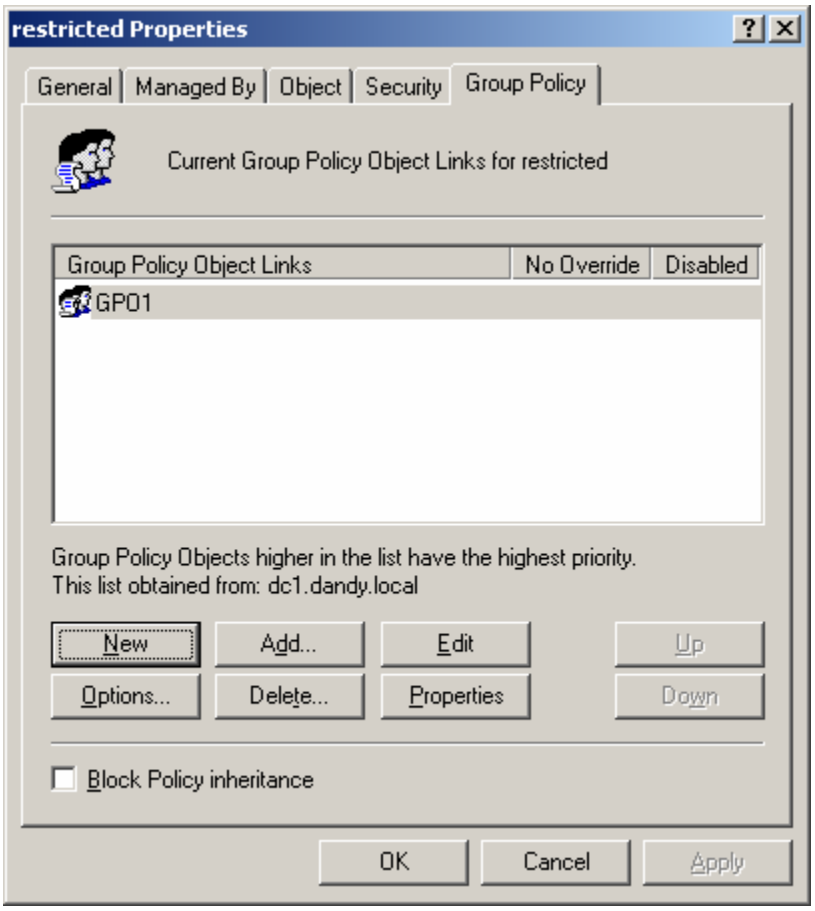

Figure 2.3: Win2K Group Policy tab, providing administration of GPOs.

The GPMC is much easier to use, and the control over GPOs is more efficient. The tool provides for the same features as all the other GPO tools and interfaces provided with Win2K in one tool. The GPMC provides for routine creation, management, and deletion, as well as archiving, resultant set of policies (RSoP), and modeling. Figure 2.4 shows the GPMC interface.

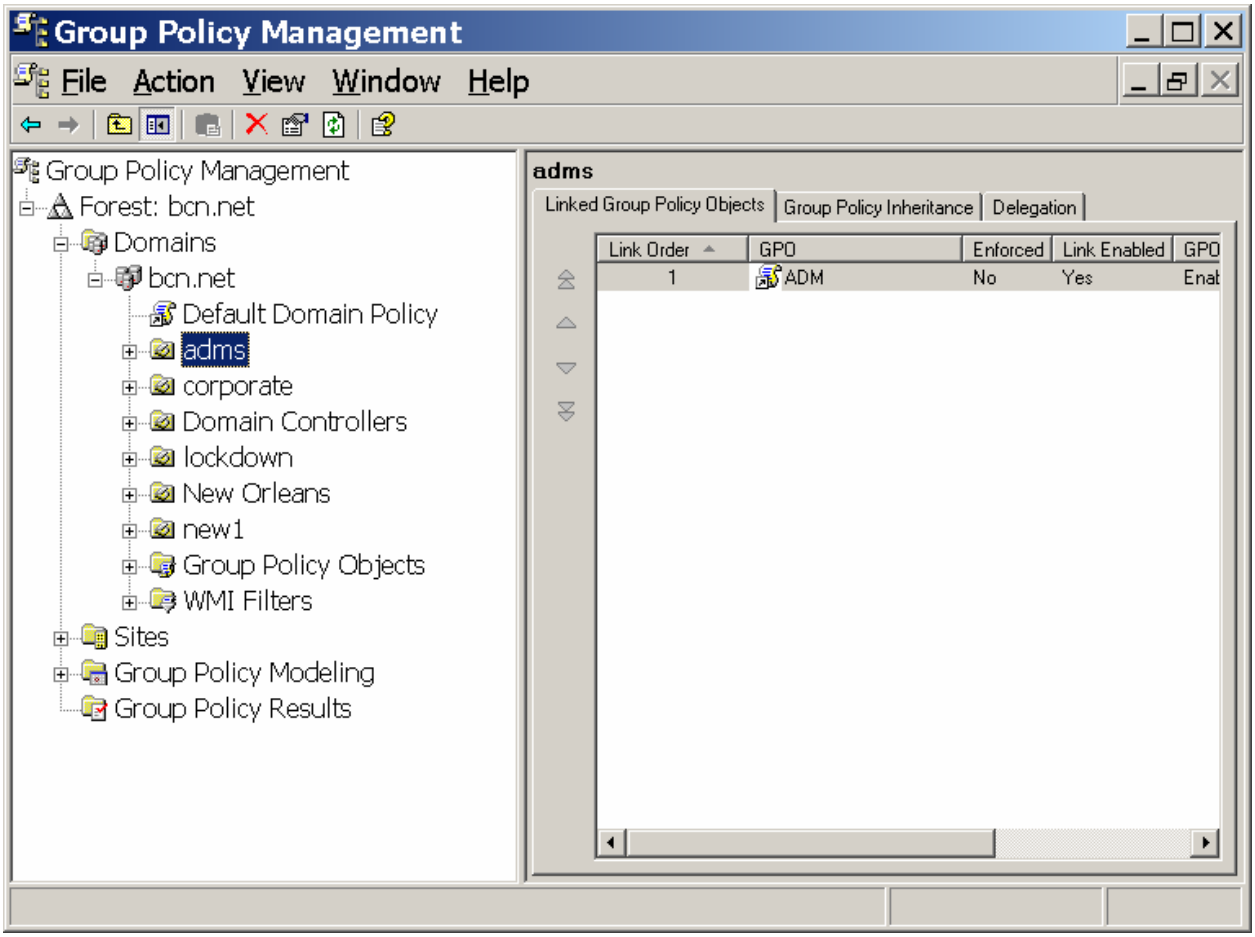

Figure 2.4: GPMC provides a simpler interface to control all aspects of GPOs.

Key features provided by the GPMC include:

- Controlling inheritance—The GPMC offers complete control over both Block Policy Inheritance and No Override. These features can be very complex if using the built-in tools, but the GPMC makes this easier to see and administer.
- GPO Filtering—Filtering of GPOs can be a complex and laborious task. With the GPMC, the listing of the GPOs provides a logical view of the GPOs, which makes the administration of the GPO ACL an easier task.
- Delegating GPO administration—There are actually two ways to delegate GPO administration. One is at the GPO level and the other is at the Container level (site, domain, or OU). The GPMC helps to see this delegation and will provide for better control because of the clearer view.
- Reporting on GPO settings—When an administrator needs to know all of the settings in a GPO, he or she must open the GPO and start to scan through the sea of settings manually. With the new reporting tool, you can quickly see all of the settings in the GPO without the added headaches.

- GPO operations—The GPO operations within Win2K had to come from a third-party tool. However, the new GPMC provides robust and easy control over GPOs, including the ability to import them from another domain or archive, duplicate GPOs, and more. These are essential functions for AD and GPO implementation.
- WMI filters—WMI filtering is going to take the concept of OU and GPO design to the next level. With WMI filtering, you are able to target specific computers, not based on location in the AD but based on characteristics of the computer itself.
- GPO modeling and results—The RSoP is crucial to an administrator who is attempting to move user and computer accounts from one OU to another. The RSoP is also important for administrators who are attempting to troubleshoot why a user does or does not have a particular setting. GPOs can get out of control and can be very complex. These reporting tools help demystify the complexity.
- Searching—The search capabilities in the GPMC are a refreshing change from hacking through the GPO interface to attempt to find the setting that you are looking for. GPMC allows for searches on GPO name, GPO links, configuration categories, and the GUID.

All of these functions help control GPOs, which help control the security of all user and computer accounts in the domain. The management of the GPOs also needs to be controlled, which is not all that easy in Win2K. With the delegation tab at every level in the GPMC, management can be easily configured, verified, and managed. Typically, there are five main tasks that need to be controlled and managed for GPO management:

- Creating GPOs—In Win2K, giving a user the ability to create GPOs is not a complex task, just confusing. With the GPMC, a user can be given the privilege to create GPOs by using the delegation tab associated with the GPOs node. This allows for separation of duties within the GPO world. A user that can create GPOs can't link them to an object.
- Linking GPOs—To give a user the ability to link GPOs in Win2K, the delegation wizard was required. With the GPMC, the delegation tab on the site, domain, or OU where the user will have the linking capability provides easy configuration for this task.
- Managing GPOs—This category is a broad definition that really includes editing, deleting, and modify GPO settings—there is no equal configuration tool in Win2K. The GPMC provides this option at each GPO.
- Editing GPOs—There is no need to give administrators more power than they need, and this setting ensures that doesn't happen. This delegated GPO task gives the administrator just the ability to edit the GPO settings, but nothing else. This is not a global setting, it is associated with each GPO individually.
- Viewing GPOs—There are two levels of viewing GPOs within the GPMC, which is two more than with Win2K GPO management. The delegated user will only be able to view the single GPO, or, if the domain or OU is delegated view options, the administrator can perform a model analysis on the GPO to see what the settings would be for a user and/or computer.

Summary

In this chapter, we focused on security and control of AD. We looked at many aspects of security that are crucial to AD and its related components. Determining the reasons for delegation and the needs for administration drives the design and structure of AD. We also explored how the OU design is essential to a secure environment that includes delegation of administration and GPO deployment.

With this solid foundation of AD security knowledge, it is time to go deeper into the understanding of GPO deployment and delegation of administration to secure the AD environment. In Chapter 3, we will take what we have learned in the previous two chapters and apply it to GPO design and implementation. We will also take planning and testing to the next level of implementing delegation of administration for AD.