Realtime publishers

"Leading the Conversation"

The Administrator Shortcut Guide™ To

Active Directory Security

SCRIPTLOGIC

Derek Melber and Dave Kearns

Introduction to Realtimepublishers

by Don Jones, Series Editor

For several yeas, now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 1: Directory Security

For all networks, systems administrators must keep track of who is accessing the network as well as control each user's access to the various network resources. In most networks, information about users and their access rights are stored in a directory that provides user authentication and access control services.

A directory service typically contains sensitive information about the user and service accounts that have access to the enterprise network and information regarding directory-enabled applications and services as well as other network resources. This information is sensitive in that the unregulated disclosure and/or disruption in the provision of this information and related services can interfere with business operations.

Directory security is fundamentally focused on protecting information, service, and resource assets accessible through the enterprise network. In addition to protecting information stored within the directory, the authorization and access control mechanisms provided by the directory service protect the services and information stored within your network.

Implementing security for the information contained in and the resources protected by Microsoft's directory service implementation—Active Directory (AD)—is not a simple task. Although AD provides powerful management capabilities, these features introduce complexities. You must understand AD, the network, the corporate environment, and the potential threats and vulnerabilities before you can effectively implement security.

In this chapter, we'll explore directory security at a high level before moving onto an exploration of the possible threats and approaches to managing the directory service and information from a security perspective. In later chapters, we'll delve into how the design of the directory impacts security and administration, then we'll take an in-depth look into Group Policies and delegation of directory administration.

Using Directories to Manage Network Access

In a network environment, you need to be able to control which people are able to access information and resources. To accomplish this control, authentication mechanisms must be used to ensure that only the designated people can access your directory, network, or other enterprise resources. To protect the resources on the network, access control mechanisms must be implemented to prevent unauthorized access to network resources and services as well as to prevent the illegitimate modification or deletion of information.

For most companies, a directory service integrated with their network operating system (OS) is the fundamental point of entry and access to all of the resources available on the enterprise network. The directory service handles authentication of users attempting to access the network and the authorization needed to access network resources by managing the users' rights and permissions.

Because the directory service plays a central role in controlling access to enterprise resources throughout the network, carefully securing the directory is essential to maintaining control of access to your information and operations. Directory-based security enables a high degree of granularity in managing user access to information and protects against the disclosure of confidential information to unauthorized users. Unlike some authentication systems, a directory service provides a hierarchical structure in which access permissions that are applied at a higher level can be inherited by directory objects, such as user accounts, that exist in organizational units (OUs) lower in the directory tree.

AD is a Lightweight Directory Access Protocol (LDAP)-compliant directory integrated with the Windows 2000 (Win2K) and Windows Server 2003 (WS2K3) OSs. AD leverages the Windows server security subsystem that provides authentication by validating the logons of users (and other security principals), and AD protects network resources by enforcing strict adherence to access control permissions assigned to resources. When access to a directory or network resource is requested, the user's security information is parsed against the security descriptors assigned to the resource; if a match is found between the user's security identifiers (SIDs) and the security descriptors, the user is provided with the level of access that has been granted.

AD further facilitates network security management by providing a pass-through authentication mechanism in which authentication via the directory service enables access to other enterprise resources. For example, logon authentication to an AD domain can provide authenticated access to Microsoft Exchange Server email and to all of the Microsoft SQL Server databases on the network.

AD also provides a policy-based implementation of the security constraints applied to computers or users. This implementation enables streamlined control of forest, domain, or OU-wide capabilities or restrictions.

Directory Security Protects Information and Service Assets

Securing your directory is critical in that the directory plays a central role in providing network security not only in the authentication of users but also in the operations of other network services and applications. Fundamentally, directory security is designed to protect against:

- Unauthorized access to the directory or network
- Disclosure of information
- Unauthorized modification of data
- Disruption of service

A directory service, such as AD, controls access to its objects and attributes by assigning security descriptors to each object or attribute, enabling administrators to provide differential access to each bit of information stored in the directory. The directory service also plays a central role in the management of identity information within your enterprise. The directory service is commonly responsible for storing identity information for enterprise network users as well as protecting this information by limiting access to authorized users and preventing unnecessary information disclosure.

AD is a distributed directory service that supplies centralized access to all of your information resources on the network. By using AD, you can search for and locate users, network devices, and shared information repositories.

Most directory services operate within a heterogeneous environment of platforms, services, and enterprise applications, so the need to support multiple security standards is common and some degree of pass-through authentication may be supported (particularly within a given platform). Increasingly, vendors of enterprise applications are writing their software to leverage the security mechanisms built-in to the directory service, thus increasing the ability to implement security for information and services from a centralized directory.

Why Directory Security Is Essential

Securing your network resources is important for a variety of reasons, not the least of which is the possible adverse impact on enterprise assets. The impact of a security breach could include disruption of service, destruction of enterprise information, and disclosure of sensitive information in ways that could damage investor or customer confidence—even a public perception of a lack of adequate security could negatively impact the confidence of your customers, investors, or other business partners. The protection of identity and directory information has also come under government regulation in recent years, which could lead to fines and even jail time for those responsible for any security breach. Therefore, maintaining effective security and promptly correcting any real—or perceived—vulnerability should be a constant priority.

Directory security mechanisms protect against unauthorized disclosure of information as well as modification or destruction of information. Directory security also protects the network services critical to your network operations against unauthorized tampering or disruption.

Securing AD is critical to your overall network and enterprise security, so you should give considerable thought to general AD security as well as the specifics of implementing AD security in your network environment. Not only do you have to determine how to initially implement effective security for your AD installation but you must also define procedures for maintaining that security on an ongoing basis. Additionally, you will need to plan for failure—when systems or services fail (and they will) or security breaches occur (and they may), which procedures do you have in place to contain the breach/failure and to recover from it?

Consider the administration of AD:

- Which services and/or data administrative tasks are assigned to whom and why?
- How are these administrative privileges and tasks delegated?
- How is the directory service monitored?
- How are security breaches detected and responded to?
- How are policy settings determined, deployed, and monitored?

These are the questions this guide will help you to answer.

Basic Security Mechanisms

Every directory uses the same basic security mechanisms to establish and maintain security—they all provide some means to authenticate validated users; control access to file shares, file systems, databases, network services, and other resources; and monitor the activities of user access, manipulation, and modification of these resources. Although the implementation might differ substantially between different directory services, the fundamental mechanisms include authentication, authorization, and auditing.

Authentication

Authentication is the process of determining that a user, computer, service, or application is actually the user, computer, service, or application that they claim to be. Authentication matches the submitted account name with the corresponding account name in the directory, and compares the logon credentials—account name and password, smart card, and so on—with the credentials stored in the directory for that account. If the submitted credentials match the corresponding credentials in the directory, the logon is authenticated and regulated access to the directory and network is granted. Authentication is not the same as validation, however. It is assumed that the identity is validated by external proofs when the account is created. Authentication then matches an asserted identity with one stored in the directory.

In AD, this authentication occurs during the logon process (see Figure 1.1). At a Windows workstation, the logon and authentication process begins when the user presses Ctrl+Alt+Delete, which invokes the logon screen (the graphic identification and authentication module). The user then inputs a username and password and selects a domain—these credentials are passed to the Winlogon service, which hands them off to the Local Security Authority. The LSA hashes the user's password and invokes the designated security support provider (by default, in Win2K and WS2K3, this provider is the Kerberos security support provider), which authenticates the submitted credentials with a domain controller. If the user credentials are authenticated with the domain controller, the user is allowed to access the directory and network.

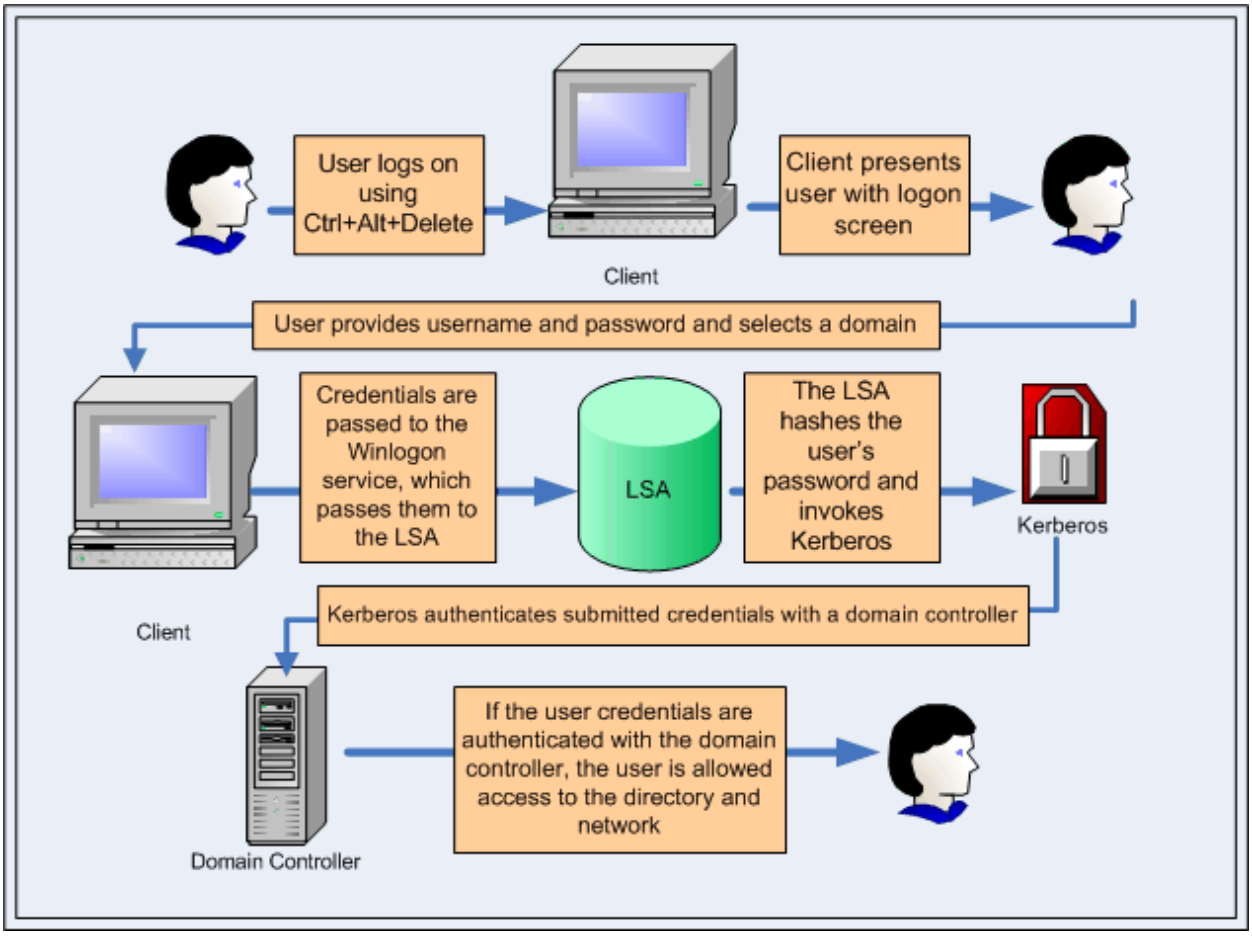

Figure 1.1: An overview of the AD authentication process.

Authorization

Authorization, also referred to as access control, is a bit more involved than authentication; authorization controls access to directory and network resources on a case-by-case, resource-specific basis. Upon logon of a security principal, the security subsystem works with AD to create an access token containing the SIDs of the user account and all security groups to which the user belongs. When a user attempts to access a protected resource, this access token is used to compare the information stored in the account's SIDs with the information stored in the security descriptor access control lists (ACLs) for each directory object or network resource the account attempts to access. Based on this comparison, the security subsystem allows or denies the specified types of access (read, modify, create, delete, take ownership, and so on) to the resource.

Auditing

Auditing is a mechanism that can be implemented by administrators to track user account logons, system events, and changes to directory objects and policy. Auditing is essential for maintaining security of your AD implementation and the security of access to your network.

In AD, auditing is implemented by first enabling the auditing capability within a Group Policy, then selecting the events to be audited for specific objects within the directory. To track changes to directory service access and objects, you must enable auditing within the scope of interest (domain, OU, and so on). To enable auditing on AD objects within a domain, you must first enable auditing within the default Domain Controller Policy Group Policy object (GPO—located in the Domain Controller OU). Then, to turn on auditing for any specific object within the directory, select the object within the directory, then access the object properties. Within the object's properties, select the Security tab, then select the Auditing tab, then specify the specific events—either success or failure—that you want to audit for that object. For the purpose of most auditing of directory-related events, you will usually want to select the Everyone group so that you can track changes made by any user to the objects in question.

Auditing in AD allows you to track both successful and failed attempts at access or modification of directory objects. Tracking all successful changes to directory objects will provide you with an audit trail for all actual alterations to the directory; whereas, tracking all failed attempts at changes can provide you with information indicating unauthorized or invalid attempts at access or directory modification. The following list highlights examples of events to audit:

- System events on domain controllers—particularly unexpected or unexplained reboots of the domain controller, which should always be investigated as they might indicate hacking attempts.
- Account management—auditing account management can provide you with an audit trail of changes to user or group accounts (when auditing success events) and can supply feedback indicating illicit access attempts (when auditing failure events).
- Excessive activity on directory partitions could indicate a Denial of Service (DoS) attack being launched by adding large amounts of data to the directory database, which could fill up the directory partition and render AD inoperative.

However, there is a caveat to auditing within AD: When you enable auditing for a given domain, every time the audited event occurs, an entry is made in the Security log (which you can see with Event Viewer). If events occur frequently, the Security log can rapidly fill up. Depending upon your audit policy settings for how to respond to excessive security log entries, this situation could result in either the overwriting—thus loss—of auditing information or the shutdown of the domain controller. When you use auditing in AD, you will need to set the Security log policies to increase the size of the log so that log entries are not overwritten if the log is full. In addition, monitor the Security event log for excessive or inappropriate entries.

How AD Provides Security

AD implements access control to network resources by managing which security principals have access to each specific resource. In AD, security principals can be users, computers, groups, or services (via service accounts) and are validated by way of the authentication process (for users, authentication occurs at logon, for computers, it occurs at startup).

A SID is assigned to security principals at the point of creation—when the object is created in the directory. Each SID is comprised of a domain identifier (common to all security principals within the domain) and a unique relative identifier (RID). When a user logs on to the network, an access token is created that contains the user's SID, the SIDs for each group to which the user is a member, and the assigned user rights or privileges.

All resources within AD (objects and their properties), network folder and printer shares, and folders and files within the NTFS file system are protected by the assignment of security descriptors—access control entries (ACEs) contained within access control lists (ACLs)—that are associated with each object or resource. A security descriptor is comprised of two distinct ACLs assigned to each object or resource: the discretionary access control list (DACL) and the systems access control list (SACL). In brief, the DACL contains a list of the SIDs of all security principals that are either granted or denied access and the degree of access that is allowed (read, modify, full, and so on). The SACL contains a list of all the SIDs of the security principals whose access or manipulation of the object or resource needs to be audited, and the type of auditing that needs to be performed.

When a user attempts to access a directory object or network resource, the security subsystem checks to see whether the SIDs for the user (or security groups to which the user is a member) match the security descriptors assigned to the resource. If they match, the user is granted the degree of access to the resource that is specified in the ACL. Most commonly, users are assigned to security groups within AD, and the security groups are granted varying degrees of access to the network resources or AD objects. By assigning users to groups and applying security descriptors to objects and resources, groups of users can be granted or denied access to or control over entire classes of objects and sets of resources.

Policy-Based Security

One of the strengths of AD is its support for policy-based networking. Through the use of the Group Policy feature, security and usage policies can be established for both computer accounts and user accounts separately. These policies can be applied at multiple levels: a policy can be applied that affects the computers or users in a specific AD site, an entire AD domain, or only the users or computers residing in a specific OU.

Although this Group Policy capability provides a substantial degree of control over the network environment through the use of hundreds of different policy settings for computers or users, it can be a bit complicated to assess which specific cumulative set of policies are controlling the environment for a specific user or computer. In an improvement over Win2K, WS2K3 provides the ability to track and report the Resultant Set of Policy (RSoP), which is essentially the net effect of each of the overlapping policies on a specific user or computer within the domain.

Even more challenging is trying to monitor and track changes to the multiple and overlapping Group Policies implemented throughout the forest and domains. When you are managing AD in a distributed enterprise in which you have multiple administrators with the authority to implement and alter Group Policies, changes to Group Policies might occur without all administrators being aware of what has changed, when it changed, and the implications of the change for directory and network operations. For this reason, and others we'll discuss later, it is a good idea to limit the number of people who manage Group Policy.

Threats, Vulnerabilities, and Attacks

Protecting against attacks on your enterprise information or operations requires you to understand the nature of the types of vulnerabilities, threats, and attacks that might and to implement appropriate prevention, detection, and recovery strategies. In general, the degree of protection implemented should be related to the degree of value of the enterprise information or operations. For example, in most networks you probably wouldn't need to or want to implement fingerprint and retinal scanning to control access to the average user's workstation. You might, however, want to implement the use of smart cards to control access to critical domain controllers. In this section, we'll first explore what constitutes a threat, vulnerability, and attack, then examine some of the most common forms of attacks conducted against enterprise assets such as networks, directories, and the associated information.

Threat

In its most generic sense, a threat is someone or something that has the capability or potential to compromise the security of your directory, network, or information. In general, three factors are commonly required in order for a person to be a threat to the security of your directory: motive, method, and opportunity.

> There are threats that do not have motive such as fire or flood; however, for threats that involve a person, motive is an applicable factor.

Another way to define the concept of a threat to your enterprise IT systems or information is as any action by a user, condition, or process that has the potential to disclose, damage, or disrupt your operations or information (see Figure 1.2). A user attempting unauthorized entry into your network, a fire that breaks out in the building that houses your network servers, and a virus that attempts to corrupt or delete needed information are all examples of viable threats to the security of your directory and your network.

Although threats to network security are commonly thought of as arising from external attackers exploiting some kind of vulnerability in your network or application software, it is not uncommon for both deliberate and inadvertent threats to the integrity of your network resources and operations to occur from people internal to your organization. According to some industry sources, internal threats are more prevalent than external ones.

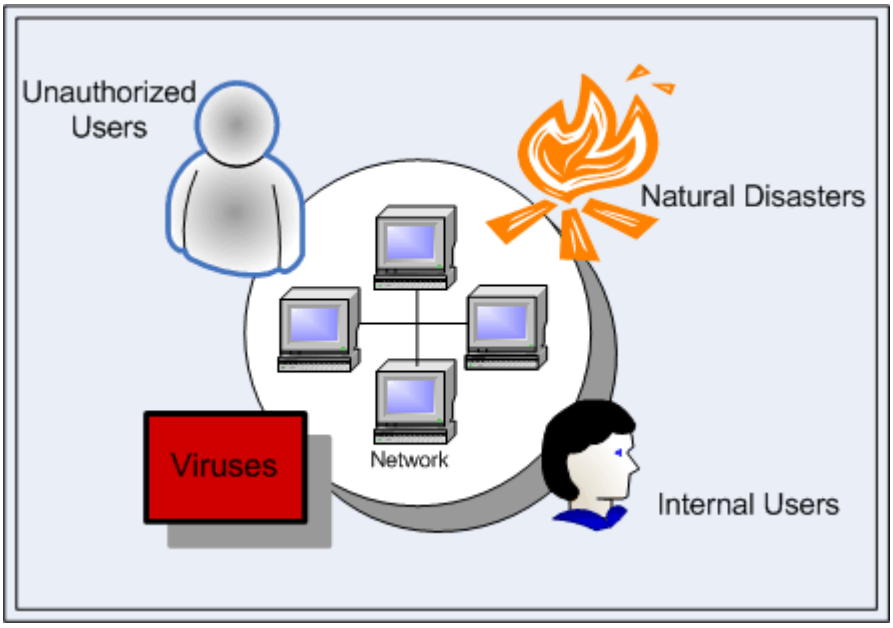

Figure 1.2: Threats to the security of your network.

Vulnerability

It seems that the IT industry magazines and even the mainstream press are constantly talking about new vulnerabilities discovered in software that is commonly used on workstations or services within your enterprise. Nevertheless, far fewer incidents are discussed by the press than exist, and it's rare for the general nature of such vulnerabilities to be discussed.

A vulnerability can be defined as any weakness in your security that provides an opportunity for an attack and that, by its utilization, can allow an attack to succeed. Vulnerabilities can occur in many different aspects of your network—software, hardware, social or physical environment—and you need to protect against all of them all of the time in order to ensure security. This requirement requires constant vigilance on many fronts—it sometimes seems as though there is a new weak spot revealed every day. It's not an easy task, but it is a critical one.

One of the most obvious areas of vulnerability is software, starting with the OS. If you are running Windows on your servers, you must ensure that each system has the latest service pack and patches, which requires you to monitor Microsoft's Web site for updates. To make this task a bit easier, you can subscribe to Microsoft's security updates newsletter and security update notification service (see the following resources for Web site information).

Useful Microsoft Security URLs

Microsoft Security Update at http://www.microsoft.com/technet/security/signup/default.mspx

Microsoft Security Bulletins at http://www.microsoft.com/security/security_bulletins/

Microsoft Security Guidance Center at http://www.microsoft.com/security/guidance/default.mspx

Microsoft Security Anti-Virus Information at http://www.microsoft.com/security/antivirus/

Microsoft Security Newsgroups at http://www.microsoft.com/technet/community/newsgroups/security/default.mspx

Patch Management, Security Updates, and Downloads at http://www.microsoft.com/technet/security/topics/patch/default.mspx

In addition to the Microsoft resources, be sure to check with vendors of other software that is deployed on your network and independent security organizations such as the System Administration, Networking, and Security Institute (SANS) at http://www.sans.org and the Computer Emergency Response Team (CERT) at http://www.cert.org, both of which issue bulletins about security problems arising from many vendors' products.

When it comes to network services, the fewer the better—install the minimum number of network services required. You should install the services you need, of course, but make sure you disable any unnecessary services and, if at all possible, avoid installing unnecessary services on AD domain controllers. Every service has its own soft spots (vulnerabilities)—the fewer weaknesses you need to keep track of, the easier your job will be.

Don't ignore physical security; all the software-based security in the world won't help you if someone can walk into the server room and lay hands on the machine. Physical access to a server means that it is open to a variety of forms of attack such as:

- Rebooting the server, possibly with another OS on a floppy disk or CD-ROM
- Attaching devices that allow capturing keystrokes or copying data from the server
- Adding or removing system components such as hard drives or network devices
- Copying data to removable media
- Picking up the entire computer and walking out with it (don't laugh, this has happened)

Attack

An attack is any action by a user or software process that, if successful, results in the disruption, disclosure, or damage to enterprise information, services, or operations. Attacks, like threats, share the characteristics of motive, method, and opportunity, which assume the intent on the part of the attacker to deliberately be attempting to damage or steal information or disrupt operations. In a directory context, an attack is an action that uses or exploits the directory to gain access to or deny service from the directory or network resource.

There are many forms of attacks that can be carried out against your network, directory, and information; there are also many sources of attacks—both intentional and unintentional.

User-Based Attacks

The most common source of attacks are those initiated by people—whether by anonymous users attempting external penetration of the enterprise network or by an authenticated user working from inside the network. User-based attacks can either be physical attacks on the equipment supporting your directory or network or based on using the network or directory environment. Physical attacks can be as simple as stealing the physical computers (workstations, servers, and domain controllers), damaging the physical computers, and/or damaging the physical network infrastructure.

Network and directory-based attacks can come from anonymous users, authenticated users, or even administrators. Each of these sources has its own approaches to an attack and associated potential risks, which we'll briefly explore.

Anonymous Users

Anonymous user attacks commonly attempt to use vulnerabilities in the network, service, or application software. An attacking user might gain access via scanning tools or by exploiting a well-known but not patched error condition in operating software. When a known vulnerability is patched, the software update is generally accompanied by a description of the weakness, often providing all the information needed to hack an unpatched system.

> ☞ It is critical to stay on top of released patches and security updates.

In an AD environment, an anonymous user might be able to use LDAP to flood domain controllers with lookup queries, read domain information, identify user account security policies, find account names and SIDs, and identify shares on domain computers. Although some of these anonymous attacks can be mitigated by tightening security settings, thwarting anonymous DoS attacks requires monitoring of the domain controllers for unreasonably high levels of LDAP queries.

Some anonymous attacks are amazingly easy to carry out. Breaking into the typical user account requires only two pieces of information—username and password. Every Windows installation has a default account named Administrator, providing half the information needed to gain enormous power over the system. Similarly, many Windows computers have well-known hidden file shares (C$, D$, and so on) for administrative purposes. Disabling these file shares and renaming the Administrator account are a couple of easy steps to take that will help protect you against attackers guessing or hacking passwords as a means of gaining access to your network.

Authenticated Users

Authenticated user-based attacks use an authenticated account as the starting point in the attack. These attacks might be from spoofed-account access (via hacking/cracking tools), the illicit use of a valid account (obtained through some social engineering scheme), or a valid user who has decided to attack information, services, or operations for some personal or professional reason.

One of the problems with attacks by authenticated users is that the accounts have legitimate access to a range of resources and information on the enterprise network; thus, it is more difficult to detect when such attacks are taking place. Authenticated users, for example, can validly start processes that will have the effect of creating DoS conditions by consuming inordinate amounts of service resources (for example, a flood of LDAP queries or connections) or disk space (for example, storing many extremely large objects in the directory). Security for attacks by authenticated users requires a significant degree of monitoring, analysis, and responsiveness to anomalies occurring in the directory.

Authenticated users can also identify members of sensitive security groups, for example, determine sensitive account information (names, addresses, phone numbers, password, delegation status, and so on), discover linkage of Group Policies, identify sites, identify the OSs of domain controllers, and discover and disclose much additional information stored in the directory. The ability to read most objects in the directory is also contained in permissions assigned to all authenticated users by default; thus, the possibility of information disclosure by authenticated users is high.

Administrators

Illicit administrator attacks include conditions in which an Administrator account has been spoofed, the account has invalidly elevated privileges, or a trusted administrator has decided to attack the directory or network. Attacks using an account with administrative capability present some of the most serious threats to the directory, the network, and to the enterprise information accessible via the network.

Although they do not offer the range of capability of service administrators, accounts with limited delegated administrative rights can modify permissions on objects within their scope, enable accounts to be trusted for delegation, change passwords on other user accounts to be used for further (spoofing and repudiation) attacks, and change security settings causing DoS conditions.

Software-Based Attacks

The directory information structure is defined in the directory schema, which specifies the objects, attributes, and syntax permissible within the directory. Because the AD forest and domain directory structure is based on a correctly specified schema, any software application that corrupts the schema could render the entire directory—and your enterprise network—inoperative.

Likewise, automated attacks via viruses or worms that are not necessarily directed against your company can nevertheless have a damaging or disruptive effect. Email attachments present a huge risk and user education doesn't seem to stop people from opening every attachment that shows up in their inboxes. If such is true in your company, consider having your messaging system block, or at least scan, all attachments. Additional measures, such as turning off preview panes that automatically display messages, converting HTML mail to plain text, and blocking email clients from accessing the Internet can save you many headaches.

Environment-Based Attacks

In the physical environment that houses the domain controllers, any condition that has the effect of damaging or destroying the server hardware (fire, flood, tornado, hurricane, lightning, and son on) could also render the AD environment inoperative. These types of threats to IT operations are consistent across platforms and are usually well addressed by IT management in planning and implementing strict backup and restoration procedures.

Make sure that your disaster preparedness and recovery plans include provisions for offsite data backups, then make sure that the backups are actually taken offsite, and consider a secondary physical site that is ready to go in case the worst happens and your primary site is disrupted for an extended period of time.

Threat Analysis

To prevent attacks, you must first determine the nature and purpose of the attacks you need to protect against. Threats to the security of a directory service and the information it contains are varied, yet they can be usefully subdivided into several common categories. There are types of attacks that rely upon false authentication and subsequent access to the directory information (including spoofing, repudiation, and information disclosure). Some attacks are focused on preventing normative access to the directory information or service (for example, DoS attacks). Other types of attacks involve deleting or corrupting information in the directory, network, databases, or other information repositories. Still other attacks are based on changing access rights to allow an unauthorized user to gain access to or control over directory information (elevation of privilege).

To discuss common threats to information systems such as directory services, databases, and networks, the acronym STRIDE is used to summarize the Spoofing, Tampering, Repudiation, Information disclosure, DoS, and Elevation of privilege types of attacks.

Spoofing

Spoofing commonly refers to the type of attack in which the attacker is pretending to be someone or some process that otherwise has legitimate access to the directory. In a spoofing attack, the attacker obtains and uses the account and password of another user or service that has sufficient permission to access the directory information. The attack might impersonate an actual user or software process, leveraging the account information and security credentials to conduct unauthorized or malicious actions.

To defend against such spoofing attacks, implement policies to protect the username and password information for all user and service accounts that have access to the directory. Most network administrators have seen passwords on sticky notes prominently stuck to the side of a monitor, so don't forget that users must be educated about your security policies as well as the consequences of ignoring them.

Stringent authentication measures can help provide some degree of protection against spoofing attacks. Use of biometrics, for example, in addition to the use of usernames and passwords can help insure that the user is who they claim to be.

In AD, the spoofing of Administrator accounts is the most serious risk. If the spoofed user account is a service administrator (member of the Enterprise Admins, Domain Admins, or Schema Admins security groups), the attacker could damage or disrupt domain-wide, or possibly forest-wide, directory operations. Because these service administrators can modify the configuration of the entire AD environment and especially domain controllers, the compromising of these accounts to an attacker is particularly problematic. Directory schema management, replication, DNS service configuration, and domain addition and deletion are directly under the control of the service administrators. Service administrators also manage the installation and configuration of all software (including the OS), patches, and updates, and configure the settings on all network servers. As a result, if an attacker gains entry to your directory via a service administrator account, they can wreak unparalleled havoc throughout your AD environment—and mostly likely much of the rest of your enterprise network.

🕮 We'll explore this topic in a bit more detail later in this chapter.

Although service administrator accounts are particularly sensitive, the compromising of data administrator accounts by spoofing can be just as disastrous. The data administrator accounts don't have the ability to change the directory configuration or operations; they are used to administer and modify user and group data contained within a portion of the directory and control the configuration of network file and printer shares. Spoofing of accounts that have been delegated administrative authority can allow the attacker to add or remove users and to modify user information. The last of these would allow the attacker to change a user's password and carry out additional attacks impersonating that user.

Even the spoofing of a domain user with nominal privileges can allow the attacker to access information stored on your enterprise network, potentially stealing, disclosing, or damaging important information. There are many horror stories of the chaos created by a single determined user; the same sorts of risks apply to a user account that is compromised by an external person.

Tampering

A tampering attack occurs when the information contained in the directory is changed, deleted, or corrupted by an unauthorized user in order to accomplish subterfuge, disrupt operations, or damage the directory information. A tampering attack might be conducted directly by an unauthorized user or indirectly by software constructed specifically to modify or damage the directory information (such as using a script that exploits a security flaw).

Keeping your security patches up to date in order to block inadvertent security holes in your applications, services, and OSs is a good starting point for protecting against such tampering attacks. In addition, lock down the directory service by using permissions that allow only necessary and authorized users to change directory information and access. Doing so will limit the window of vulnerability to unauthorized attacks.

Repudiation

Repudiation refers to the type of attacks that are designed to perform unauthorized operations wherein administrators of the attacked system are unable to prove who performed the attack. If changes to a directory or database are not being audited, for example, or the Security log is modified or deleted, any unauthorized change to the information the log contains wouldn't be traceable back to the source of the change.

To defend against a repudiation-based attack, both stringent authentication and auditing of the directory needs to be performed. Detailed event logging auditing access and changes to directory information can provide you with essential data to help track and stop such attacks. Consistent real-time off-server backups of the Security log need to be made in order to effectively track attempted repudiation-based attacks.

Information Disclosure

An information disclosure attack is designed to cause protected information to be exposed to one or more people who are not authorized to have access to that information. Information disclosure can take many forms; inappropriate access to documents in the file system; unauthorized access to databases containing sensitive user, financial, or medical information; and access to user accounts and other information stored in the directory. Information disclosure attacks can also occur when the information is on-the-wire—being transmitted across network connections. In such attacks, a network sniffer (or custom application with similar packet monitoring capabilities) is used to capture the information.

Use of network protocols that encrypt packets prior to transmission can protect against the latter type of attack, yet there are many ways that attackers can bypass standard security measures to inappropriately access information. Using permissions to control access to sensitive directory objects, file systems, and databases is a baseline necessity to defend against information disclosure attacks. Nevertheless, social engineering attacks—convincing an authorized user to unwittingly provide an attacker access—are a type of attack that technological mechanisms will not prevent. In addition to technical security mechanisms, security training needs to be provided to all people that have access to the directory and other sensitive data stores in order to prevent such information disclosure attacks from succeeding.

DoS

DoS attacks take many forms: as simple as remotely shutting down a server or as complex as an attack that hijacks many (tens, hundreds, thousands) of client systems and overloads a network service with bogus requests so that the network service cannot provide services to authorized users. In all of its variations, the purpose of a DoS attack is to render the network service unavailable to the users or systems that depend upon the service.

In the recent past, several high-profile DoS attacks have targeted the Web servers of well-known companies—attacks that have effectively prevented the normal operation and usage of their public Web sites. Within a company's internal network, DoS attacks can be substantially more problematic, potentially bringing all IT-dependent activities to a halt until the attack is neutralized. Real-time performance monitoring and automated alerts are a necessary starting point for defending against DoS attacks.

Elevation of Privilege

An elevation of privilege attack is one in which a user—authorized or not—has changed his or her access permissions to allow enhanced, or complete, control over directory, network, or file system settings. In this situation, an attacker can alter the permissions assigned to users, services, files, and directory objects. This attack could include turning off auditing, monitoring, or other tracking mechanisms, which would effectively allow subsequent attacks to be untraceable.

Although auditing can alert you to changes in privilege elevation, there is commonly significant delay between the action and the awareness by IT management that such a change has occurred. Even after a change has been discovered, staff must determine whether each specific privilege elevation was authorized or not. Use of intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) can greatly enhance the responsiveness of the network security team in identifying and preventing such attacks.

Managing the Directory Service

AD administration can be divided into two significant areas:

- Service administration
- Data administration

Both areas are critical and entail security risks and vulnerabilities; however, service administration requires a higher degree of access to the directory and you must take great care in determining who will do these tasks and how they will carry out the tasks.

Service administration involves managing AD operations, including replication, schema changes, domain creation and removal, and the delegation of tasks to data administrators. Because part of the job of a service administrator involves the installation and configuration of software—including service packs and other software updates on domain controllers—service administrators will need physical access to domain controllers.

> Although Microsoft often describes a domain as a security boundary, this definition is only partially accurate. The domain boundary *does* act as a block to the inheritance of security policy data (such as password and account policies), but it does *not* protect against attacks by service administrators. Thus, you *must* trust your service administrators across the entire forest, even if you do not intend them to administer outside of a designated domain.

You *must* trust the people who will be service administrators absolutely—you will still want to implement auditing and other security controls, of course, but a rogue service administrator can wreak havoc on your directory, your network, and therefore your business. Only employees who have demonstrated that they are responsible and understand both AD and your business operations should be entrusted with these tasks. This job should not be outsourced, given to temporary staff, or, in most cases, delegated to a brand-new hire. For similar reasons, don't add user accounts from another forest to service accounts in your domain; security lapses in the other forest—which you cannot control—can easily compromise the security of your forest.

AD uses several built-in service administrator accounts, such as Enterprise Admins, Domain Admins, Schema Admins, and so on. Some groups, such as Schema Admins, should not have permanent members but should instead have membership granted only when those tasks need to be performed. The built-in Admin groups allow more access than you will necessarily want to provide, even to the people who need to do those tasks. In this case, create a custom group that provides only the specific access that is needed rather than using a default group.

Make sure that you define clear administrative policies and ethical standards, establish consequences for breaches, then educate administrators about these policies. Obtaining signed copies of critical policies from each administrator provides a paper trail so that people can't say, "I didn't know…" Senior administrators should set an example by adhering to both the spirit and the letter of these policies—it doesn't make much sense to expect compliance with policies that managers are ignoring.

Best Practices for Service Administrator Account Management

There are several best practices to ensure that service administrator accounts are not misused in any way. The following highlights these considerations:

- Limit the use of service administrator accounts to actual service administration tasks. Although it might be easier to simply log on with an account that provides all the privileges you might need, such an account introduces security risks. If a service administrator is also a data administrator, ensure that there is one account for each function, plus a standard user account for normal work logon.
- Restricting the computers that the service administrator accounts can log on to will provide further security by insuring that these accounts are only used on a limited number of workstations (perhaps in a secure environment) and not from just any computer. These workstations should have all the usual protective software such as antivirus, anti-spyware, and so on because a virus running on such a machine will be running with a high level of privileges and could cause much damage.

- Consider requiring strong authentication of some sort using a token or biometric identifier or even split credentials for service account logon. The use of split credentials means that two people are required to log on to a single service account. This process might involve giving the physical token to one person and the password to another or creating a complex password and telling each person half of it. Thus, access to the account requires that two people be present, further reducing the possibility of attacks because it is unlikely that someone will attempt an attack with someone literally looking over their shoulder.
- Create only the service administrator accounts that are actually needed. Every person with service administrator access is a potential security risk—even if the person associated with an account is 100 percent trustworthy, each account that exists is another account that could be hacked.
- Keep service administrator accounts restricted from unnecessary access and possible exposure by not providing Internet access, email accounts, and so on. Doing so can help limit the possible exposure of these accounts to hacking attempts and serves as a constant reminder to the administrator that he or she should be using a regular user account for non-administrative work.
- The built-in Administrator account is an obvious target, so make sure that you rename it. When you rename the account, make sure that all the information in the account is altered to resemble a standard user account—it won't do you much good to rename the account if the text in the description still identifies it as the Administrator account. You should also create an account that looks like the standard Administrator account but has no privileges to act as a decoy.
- Create an AD subtree that will contain all service administrator user and group accounts and the workstations from which they can perform service administration tasks. You should not allow a data administrator—or even numerous service administrators—access to service account management; only allow trusted service administrators to manage these accounts. Doing so will help protect against data administrators elevating their privileges. This subtree should be fully audited and audit logs should be checked regularly.
- Don't forget DNS! AD relies on DNS and you should monitor its correct operation as part of good directory management. When you design your internal AD namespace, use a namespace that is different from any of your public DNS names. AD-integrated DNS stores the data in the directory, which is more secure than standard zone files and supports secure DNS updates. Every authenticated user has the ability to create DNS resource records. WS2K3 supports quotas to ensure that a rogue user can't flood the DNS service with spurious or malicious DNS records as part of a DoS attack.

> 🕮 Microsoft has several whitepapers available that describe specific steps to take when securing AD (http://www.microsoft.com). Consult these resources when you are designing your directory and administrative practices.

Best Practices for Managing Directory Information

Data administrators manage the contents of the directory, user accounts, groups, network resources such as computers, and so on. Thus, you need to take the precautions when determining data management practices. Depending on the information that is being stored in AD, something as simple as the disclosure of user data could present serious risks. If, for example, the Human Resources department has decided to store confidential information such as pay grades and social security numbers in the directory, that information must be protected for reasons that range from internal policy (many companies forbid employees disclosing their compensation) to legal (if your staff's personal and financial data ends up on the Internet, you're in huge trouble).

Most of the people who will be administering your directory will be data administrators, and most of them will have access only to a limited subset of directory data. Some things are obvious—data administrators do not control delivery of the directory *service*, they don't need access to domain controllers, and, in general, they can do their work from any available workstation. In most organizations, the privileges afforded to a data administrator are restricted to a portion of the directory—a single OU representing a workgroup, for example, or only a printer and related services.

One of the major advantages to AD when compared with pre-Win2K versions of Windows Server products is this ability to delegate control of portions of the directory. It's a very simple process in practice; you create a group, add members, and provide the required privileges. This functionality is almost deceptively easy as it hides the risks that are inherent in delegating management of a portion of the directory.

Some types of data administration are fairly straightforward and easy to delegate securely. Printer management, for example, requires a limited set of rights to directory information and isn't likely to provide many security holes. GPO management, however, provides many opportunities for security breaches, either inadvertent or deliberate; even though GPO management might be considered data management, you might want to restrict this task to a few trusted service administrators. There are default groups available for a number of administrative tasks each with predefined sets of privileges. You can also create custom groups to accommodate the specific needs of your organization. When assigning data administration tasks, you will have to find a balance between enough access to do the job and too much access, which puts directory information or network security at risk. The following list highlights best practices for data administration:

- Limit data administrator's scope of access to the minimum required to accomplish the assigned tasks. AD allows highly granular assignment of security, so use it. It's better to create a group that has too few rights and go back and add an additional privilege later than to grant too many privileges initially and only discover after the fact that security has been compromised.
- A single person should be delegated management for each group, if possible, to avoid group membership conflicts that could occur if several people are changing members of the same group.
- The application of Group Policy has wide-ranging implications as it controls the application of security for the network. Accordingly, GPO management should be restricted to service administrators (not data administrators) in most cases.

- Watch for abuse of Creator/Owner status. When a directory object is created, the user creating that object owns that object as well as any objects created underneath it. Thus, a data administrator who has the right to create OUs can create a subtree and then block access to it. Although this problem is not permanent—members of the Administrators group can take back ownership—it is something to keep an eye on if for no other reason than it might indicate a person whose activities you should closely watch.
- Monitor user reports (and Security logs in Event Viewer) of odd behavior. An occasional occurrence might be nothing to worry about, it could be an indication of internal tampering—such as indicating that an administrator is resetting passwords to allow them to log on as another user. By doing so, the administrator can impersonate that user and carry out activities such as reading or even sending email from the user's account.

User Management in AD

A great deal of the administration of AD is focused around user and group management, generally referred to collectively as user management. User accounts provide the means of identifying and authenticating individuals, while the rights that are granted to each user are normally controlled by group membership. Even these simple user management tasks, however, have the potential to compromise the security of your directory if performed incorrectly.

If you've been managing Windows networks since before Win2K, the changes to the User account with AD will seem significant. User accounts in Windows NT had less than a dozen settings to configure; however, an AD user account has more than 250 possible attributes to deal with! Everything from extensive work-related information, such as a user's manager, to personal data, such as home address and phone number, can be securely stored in the directory.

All this configurability comes with a price: the complexity of user management has grown exponentially. Luckily, only about half a dozen attributes are mandatory and many of them are not even displayed in the standard AD management tool. In fact, quite a few are entirely hidden from the usual management tools and require special utilities to view and configure (although they can generally be included as part of a search in the standard UI).

To simplify the process of securing this information, there are default security settings applied to sets of user properties, which can be either good or bad. Using predefined property sets streamlines setting security; however, allowing access to the home phone number of a user, for example, also exposes the user's home address. You should study the details of user properties and consider the related security implications carefully rather than assuming that you understand how it all works.

Creating a User Object

There are three types of objects employed for user accounts in AD:

- User—This account is the standard user account and will be used most in corporate networks. A User object is a security principal and a member of the domain in which it is created.
- InetOrgPerson—The InetOrgPerson object was added in WS2K3 to facilitate the use of AD as an LDAP directory that complies with Request for Comments (RFC) 2789. The InetOrgPerson is a security principal and a domain member and functions in the same manner as a User.
- Contact—A contact object is used to represent a person who needs an email account but no other access to the network. It is not a security principal, so it cannot be used for a person who needs access to network resources. You might use a contact to allow the inclusion of a person in the directory for searching purposes—as a phonebook entry of sorts—or to include members of other forests in the global catalog. Exchange Server 2000 and later use contact objects for custom recipients, which are external email addresses that are included in the local address book.

To create a User, select the container in which you want the object to be created, then choose the option to create a new User, InetOrgPerson, or Contact object. Configure the various forms of name for the new user, making sure it is not a duplicate of another name in the domain and set other mandatory and desired properties such as password.

> ☞ A clear naming standard is useful to prevent the existence of duplicate names.

Set the values for other properties that need to configured. Doing so might require navigating through several property sheets to find all of the needed properties as well as going into the special properties that are available from the Advanced button on the Security tab. Next, add the new user account to the appropriate groups.

You can perform this add-user process manually or by using a bulk import method such as Ldifde or Csvde. Creating user accounts manually is quick and easy if you only have one or a few to add. If you are populating a new directory, however, or have many new users to add every week, automating the process is useful as it can lighten your workload and avoid many opportunities for error. Automated creation methods can also allow you to set hidden properties without the need for an additional tool.

Creating a Group

Before creating a group, you must make two decisions to determine which type of group you need. The two areas that you must consider are the type of group and its scope. The type of group determines what you can do with the group. There are two types of groups used in AD:

- Security groups provide a means to apply permissions and are the primary type of group used in AD.
- Distribution groups are used only by messaging systems that are integrated with AD, such as Exchange Server 2000. These groups provide no means of applying security permissions, but rather function solely as a collection of user accounts for email and other messaging products.

The group scope determines where it can be used and which object types can be a group member:

- Domain local—Applies to a single domain, can contain users as well as global and universal groups
- Global—Used within an entire AD forest, can contain users from the same domain and global groups
- Universal—Can be used throughout an entire forest and can contain users, global groups, and other universal groups; for compatibility reasons, Universal groups are only enabled in native-mode domains

> 🕮 We'll explore Universal groups in more detail in later chapters.

To create a group, Select the container in which you want to create the group, then choose the option to create a new group object. Next, name the group and select the type and scope of the new group. Finally, add user and group accounts to the new group.

Summary

In this chapter, we introduced you to how directory security works by looking at the big picture. After exploring some general security concepts, we took a look at how AD manages those aspects of security. Possible threats were discussed, and we talked a bit about best practices for managing both the directory service and directory data.

With this background on directory security and some ideas about how to approach secure management, we'll move on to the details of doing so. In the next chapter, we'll look at the big picture of directory administration starting with how the design of your AD tree impacts your management processes (hint: it's more than you might think), then explore the details of delegating administration. After that, we'll move on to an in-depth look at Group Policies and finish up with a chapter on delegating administration.

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.

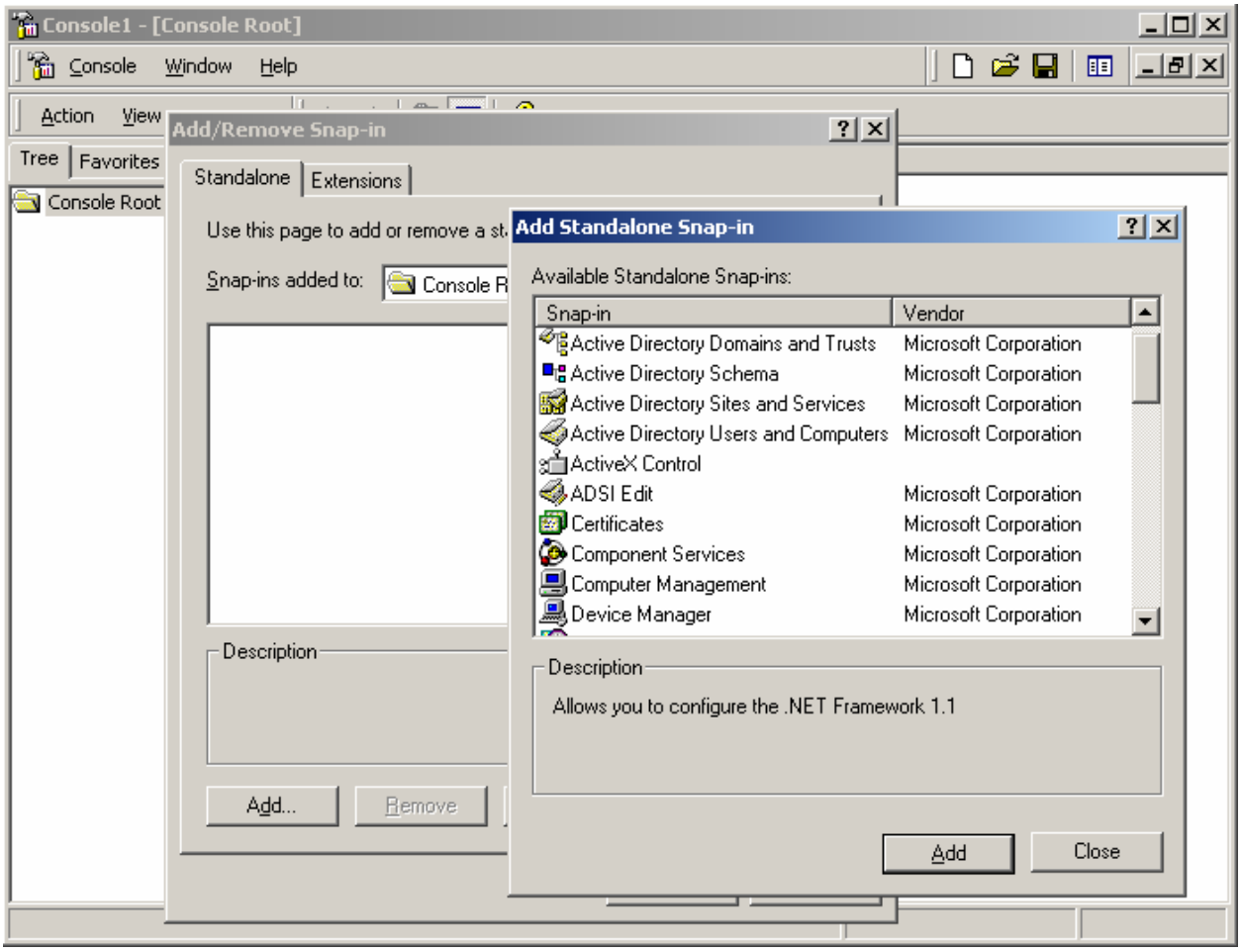

Figure 2.1: MMC with a list of snap-ins.

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.

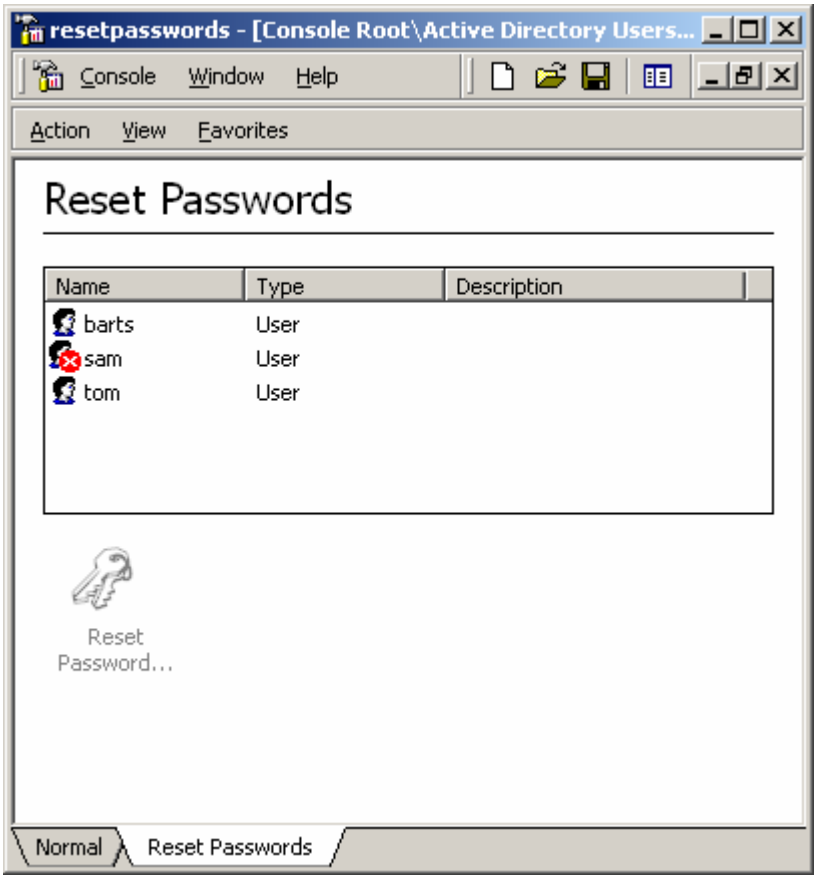

Figure 2.2: An MMC Taskpad providing the delegated administrator the ability to reset passwords.

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.

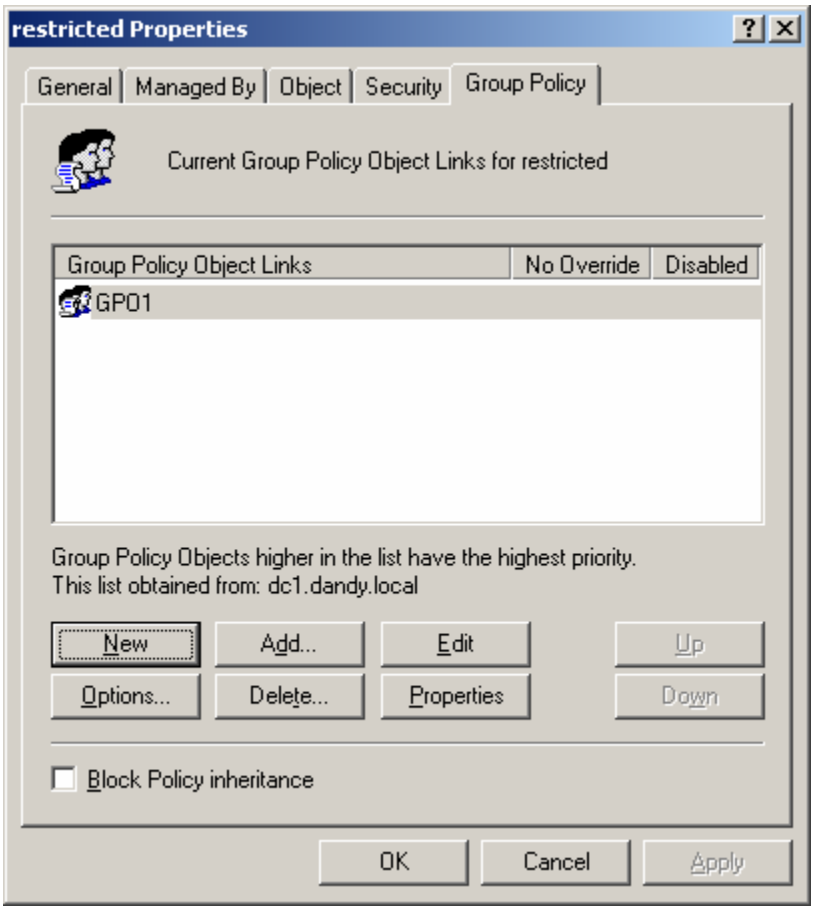

Figure 2.3: Win2K Group Policy tab, providing administration of GPOs.

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.

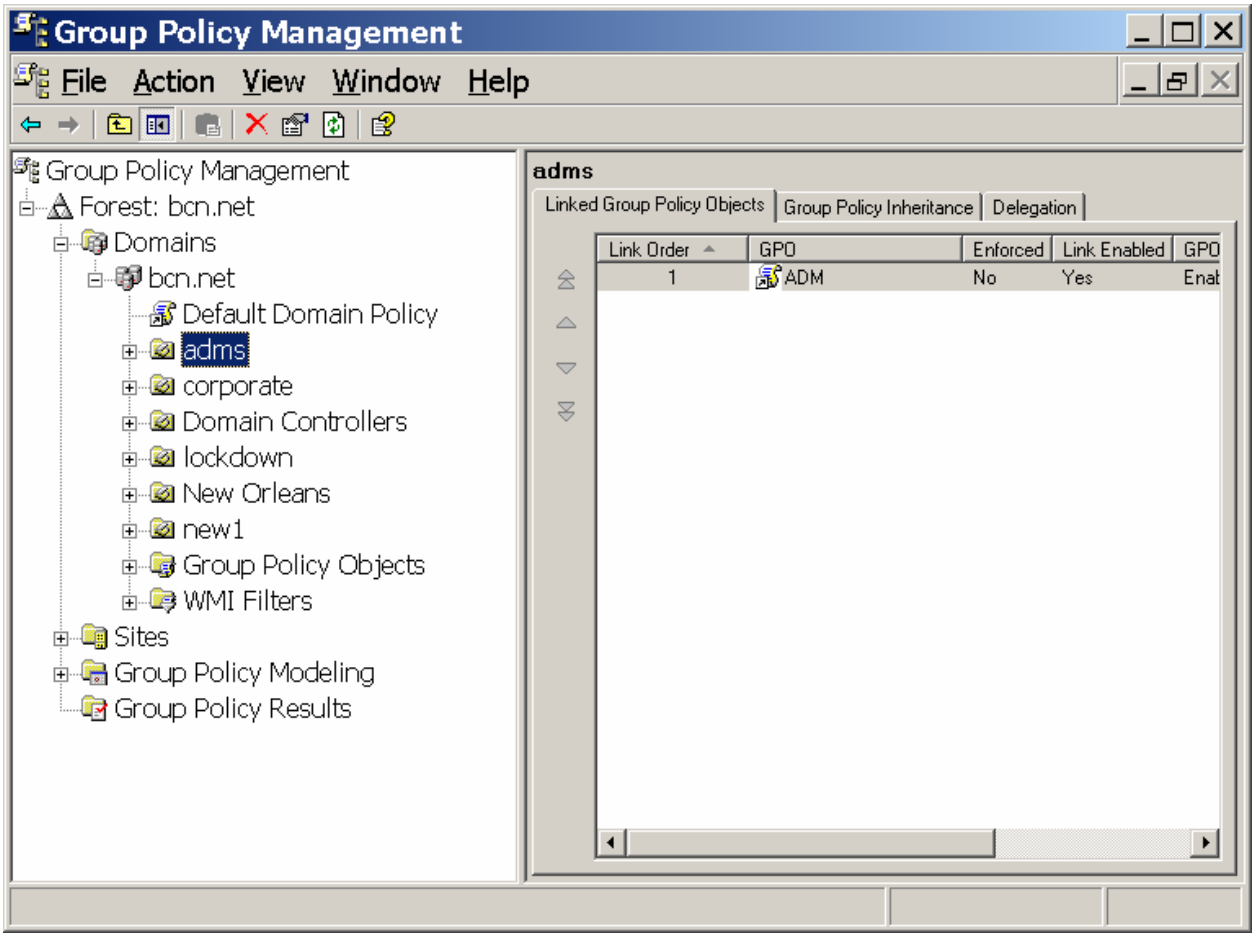

Figure 2.4: GPMC provides a simpler interface to control all aspects of GPOs.

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.

Chapter 3: Group Policies

So far, this guide has provided an introduction to a directory service as well as many of the security considerations that you must manage to keep all objects secure. In addition, we have explored Microsoft AD, with all of its security control mechanisms. You should have a good understanding of the AD infrastructure areas that will require the most attention in order to protect your assets. The assets that need to be protected include user accounts, group accounts, data files, databases, and OS files.

In the previous chapter, we discussed the various methods that administrators have at their disposal to control these AD assets. We focused much of the discussion on delegation of administration, which allows administrators to offload many routine and mundane administrative tasks onto junior administrators, Help desk workers, and other employees of the company. GPOs are of particular interest for delegation, as they enable administrators to control the ability to create, link, edit, and view GPOs.

Before we dive into who will manage GPOs—we will tackle the details of controlling the management of GPOs in the next chapter—we must first establish a foundation of knowledge by exploring the basics of GPOs. One of the most important aspects of a GPO is its ability to control security for user and computer accounts in the domain. A GPO has almost 1000 policy settings. The security settings are spread throughout the structure of the GPO, so simply finding a specific GPO setting can be a daunting task. This chapter will lay out the structure of a GPO, indicating where the essential security policies reside, allowing you to efficiently find the settings that you need.

Once you're familiar with how a GPO is structured, it is important to understand how the GPOs interact with one another. This interaction follows routine inheritance rules, which is an aspect of GPOs that can be very frustrating as a result of the complexity. We will explore when, why, and how to use the tools that control inheritance of GPOs, tackling terms such as no override, block policy inheritance, security group filtering, and Windows Management Instrumentation (WMI) filtering.

As in the previous chapter, we will stress the point that AD, security, and GPOs must be designed. Failing to consider security and GPOs during the design of AD almost ensures disaster. The reason is the complexity that results from GPO implementation. Let's begin by defining policy-based security.

Policy-Based Security

When you think about policy-based security, you most likely consider terms such as consistency, reliability, uniformity, and standardization. In addition to these, you can also throw in customization, mandatory, and absolute. Policy-based security is provided through GPOs. Such has not always been the case with Microsoft OSs, but policy-based security is standard with Windows AD. When the first domain controller is installed in the first domain, tree, and forest, GPO security is in control. Even the default GPOs provide the structure for policy-based security, in the following manner:

- Consistency—The structure of a GPO provides consistency for all security settings by the way that the GPOs are applied. The intent of GPOs is to ensure that every time a computer starts or a user logs on, security is applied the same every time. This consistency is accomplished during authentication with the domain controllers, which are in control of the AD infrastructure. As long as the computer is a member of the domain and a user account from the domain is used for authentication, the security settings will always be applied.
- Reliability—Because GPOs are controlled by AD, DNS, and authentication, they are out of the hands of the user at logon. This setup ensures a reliable application of the GPOs, which provides a secure environment that is out of the control of any user or computer.
- Uniformity—GPOs are applied to OUs, the domain, or sites. This application typically will affect multiple objects (either user or computer accounts). Each object that is affected by the GPO will receive the same settings by default. This application provides for an easy way to ensure that multiple objects have uniform security settings applied to them.
- Standardization—The security settings that are built-in to GPOs are the common security settings that any environment will require. This commonality provides a standard that all GPOs begin with. If such were not the case, each GPO might have different settings and options, resulting in a confusing and irregular application of security throughout the domain.
- Customization—GPOs provide an almost endless interface for custom policy and security settings. From registry values to software installation, GPOs provide a method to customize settings for target computers. In addition, WMI filters allow GPOs to target computers with specific credentials for hardware, OSs, configurations, and more.
- Mandatory—When a GPO is applied to a target object, the setting is mandatory for that object. In most cases, the local GUI grays out, ensuring that it cannot be changed by the local user. If the setting is enabled to be changed locally, there are methods that enable you to change those settings back to the GPO settings as often as every couple of seconds.
- Absolute—With the ability for a GPO to mandate policy and security settings, then force the settings down to the target object, the GPO has the final, absolute say on any setting. This is comforting from an administrative standpoint, because many manual settings are only suggestive, allowing the local user to make changes that can only be changed back with another administrative manual alteration.

What Group Policies Control

If you are new to AD and GPOs, you might be wondering: What does a GPO control? First, consider Figure 3.1.

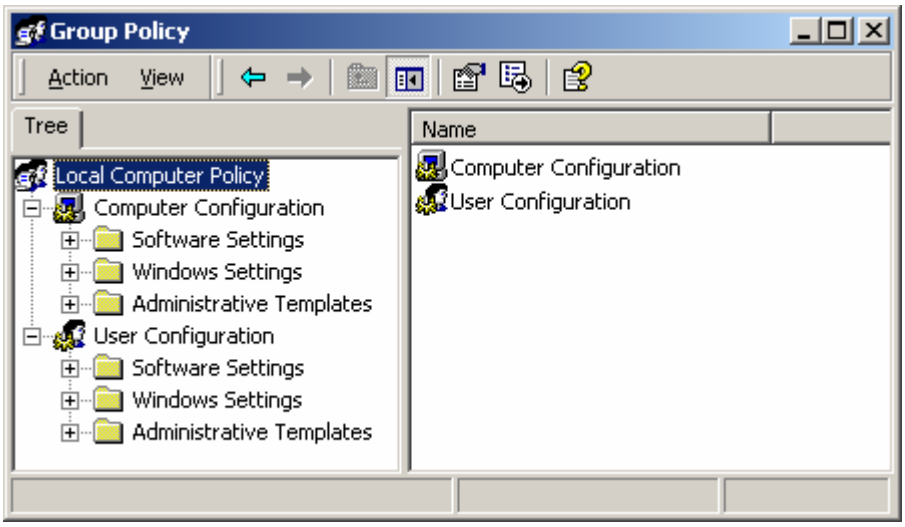

Figure 3.1: The Group Policy Editor showing the format of a typical GPO.

This figure represents the image that you should always conjure when you are asked what a GPO controls. The reason that this image is important is that it clearly answers the question. Notice that a GPO has two sections: Computer Configuration and User Configuration. These are the only two objects that GPOs can affect: computer and user accounts.

The next thing to consider when trying to answer this question is which object is being affected by the GPO policy that is configured. For this answer, you can also refer to Figure 3.1. If the policy that you set is under User Configuration, the policy will only affect user accounts. A policy that is set under the User Configuration section of the GPO can't affect a computer account. The same is true for the Computer Configuration section and policies in the GPO. These can only affect computer accounts.

If a GPO can only affect computer and user accounts, then what about the other objects? Can a GPO apply to an OU? Not exactly. An OU is an object that contains other objects, such as user and computer accounts. GPOs are linked to OUs; GPOs don't apply to OUs. A GPO linked to an OU will have an affect on all of the computer and user accounts in the OU and child OUs, but not to the OU itself. The same case can be made for the domain node and sites. GPOs are linked to these objects, they don't apply to these objects.

To make sure that this is clear, we will explore scenarios that will help you remember what GPOs apply to. All of the following scenarios will use the OU structure that Figure 3.2 shows.

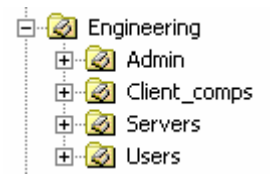

Figure 3.2: OU structure for scenarios.

All of the scenarios will also use the following GPOs and links listed in Table 3.1.

GPO Name	Linked To	GPO Policy	Section
No Run Option	Users OU	Remove Run menu from Start Menu	User Configuration
Legal Notice	Client_comps	Legal Notice Caption Legal Notice Text	Computer Configuration

Table 3.1: GPOs used in the example scenarios.

The scenarios will use the accounts and the account locations that Table 3.2 shows.

Account name	Account type	Location
TomT	User	Users OU
BettyF	User	Users OU
JoeB	User	Admin OU
Tom_PC	Computer	Client_comps OU
Betty_PC	Computer	Client_comps OU
Server4	Computer	Servers OU
Employees	Group	Users OU

Table 3.2: User and group accounts used in the scenarios.

Scenario 1: What will Tom see if he logs onto his own computer?

Answer: He will see the Legal Notice and won't have the run command.

Scenario 2: What will Betty see if she logs onto Toms' computer?

Answer: She will see the Legal Notice and won't have the run command.

Scenario 3: What will Joe see if he logs onto Betty's' computer?

Answer: He will see the Legal Notice and will have the run command.

Scenario 4: What will Tom see if he logs onto Server4?

Answer: He will not see a Legal Notice and won't have the run command.

Scenario 5: What will Betty see if she is a member of the Employees group and logs onto Server4?

Answer: She will not see a Legal Notice and won't have the run command.

Scenario 5: What will Joe see if he is a member of the Employees group and logs onto Server4?

Answer: He will not see a Legal Notice and will have the run command.

From these example scenarios, you can see clearly that the location of the user and computer accounts are essential and the membership in groups has no bearing with a default configuration of GPOs.

GPO Application

We saw in the last section that GPOs can only apply to computer and user accounts. When considering what the application of the GPO is, you will need to take into account the following three criteria: physical location, domain membership, and location in AD. All three of these criteria match perfectly with the different locations to which a GPO can be linked in AD:

- Physical location—AD site
- Domain membership—AD domain
- Location in AD—AD OU

An easy way to remember where a GPO can be applied is to use the acronym that is developed from these locations: SDOU. We will also see that this acronym is used for inheritance and precedence. As for the application of GPOs at each level in AD, there are different issues to consider for each.

GPOs at AD Sites

By default, there are no GPOs linked to any GPO site. The most likely reason for this default setup is that there is only one site in a default AD forest. This site would include every domain controller, server, and client. There are very few policies that should affect every single computer in the forest, so there are no GPOs linked here by default.

If you are considering whether to link a GPO to a site, bear in mind that all of the computer accounts that are physically located in the subnet that is defined by the site will be affected. This will include domain controllers, servers, and clients. For most GPO policies, this inclusion is too widespread influence. In most environments, domain controllers and clients need to be configured differently to accommodate their role in the domain. The rare cases in which GPOs are linked to sites might include configuring clients for RAS subnets and for Software Update Service (SUS).

GPOs at AD Domains

There is an existing GPO linked to every domain in the forest. This GPO is named Default Domain Policy. The main responsibility of this GPO is to configure the Account Policies for the domain user accounts. The account policies include the password policies, account lockout policies, and Kerberos policies. These policies will control how many characters a password contains, how often the password is changed, what happens if a user forgets his or her password, and the Kerberos ticket details.

Additional GPOs can be linked to the domain, but the same problem occurs at the domain level as it did at the site level. The domain includes domain controllers, servers, and clients, which means that all of these computer objects will be affected by the GPO that is linked to the domain. If the User Configuration section of the GPO is configured, all user accounts in the domain will be affected, including the Administrator account, other domain administrators, IT staff, executives, developers, and employees. In most cases, these user accounts need to be dealt with uniquely; thus, setting a policy that affects them all the same is not generally beneficial.

GPOs at AD OUs

Like the domain level, there is a default GPO linked to the only OU in a new domain. The only OU is the Domain Controllers OU and the default GPO is named Default Domain Controller Policy. This GPO is designed to establish the default security for the domain controllers, which includes establishing the user rights and configuring some security options.

OUs are inherently designed to contain other objects, so it makes sense to use OUs to organize user and computer accounts. As we will soon see, the design of what is contained in the OUs is driven by the GPOs that will be linked to the OU and therefore apply to the objects in the OU. The other deciding factor for the OU design will be delegation of administration.

For most AD environments, the majority of all GPO links will be to OUs. Because the different types of objects that caused problems at the site and domain level can be organized into their own separate OUs, the GPO dilemma is solved when they are linked to OUs.

Inheritance

GPOs follow very strict rules, and obey the rules of inheritance. The rules of inheritance dictate that GPOs will apply in a certain order when there is more than one GPO to be applied. When talking about the inheritance of GPOs, it is important to understand all of the different GPO locations that must be considered. We have already discussed that a GPO can be linked to the site, domain, and OU. There is a fourth location that comes into play when discussing inheritance: the local GPO.

The local GPO is on every computer that runs Win2K and later. The local GPO can't be removed, but it can be blank, containing no policies that have been configured. By default, the local GPO is not configured.

Order of GPO Application

GPOs can be linked to sites, domains, and OUs. There is also a local GPO on every computer. So which has the highest priority when they are applied to a user and computer account? To answer this question, we must look at the acronym that we defined earlier—SDOU. We are going to add the local GPO to the mix, which now creates our final acronym of LSDOU. This acronym presents the order of application for GPOs.

First, the local GPO applies. Although this GPO resides directly on the computer that it will configure, it has the least priority when compared with the other AD GPOs. Next, the site GPOs apply. These will most likely be few, if any, GPOs. After the site GPOs, are the GPOs linked to the domain, which include the default GPO that is linked to the domain, which configures the domain user accounts' password restrictions. Finally, the OU GPOs apply and have the final say over all other GPOs. These are the GPOs that are closest to the computer and user objects that reside in AD.

Although GPOs apply in the order of LSDOU, it is important to fully understand how the concept of GPO application works. When a GPO applies to an object, the GPO policy settings are gathered in the order or least priority to most priority. If no GPO policy settings conflict, the order of application is inconsequential. It is only when the GPO policy settings conflict that the precedence of GPO application becomes a factor. Figure 3.3 illustrates how GPO precedence works and what the outcome of the GPO application should be.

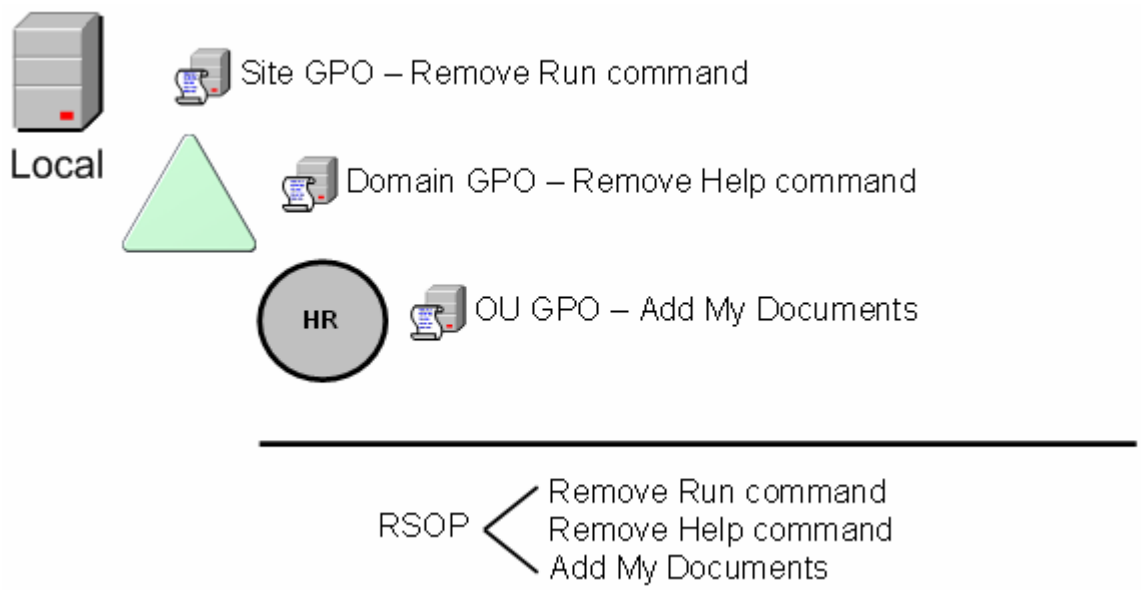

Figure 3.3: GPOs apply in the order of LSDOU; when there are no conflicts, all of the settings apply from each GPO.

It is when a policy setting in two different GPOs conflicts that the concepts of precedence and GPO application take affect. The policy setting from the GPO with the highest priority or precedence will be the one that applies to the object, when there is a conflict between two different GPOs. Figure 3.4 illustrates this behavior.

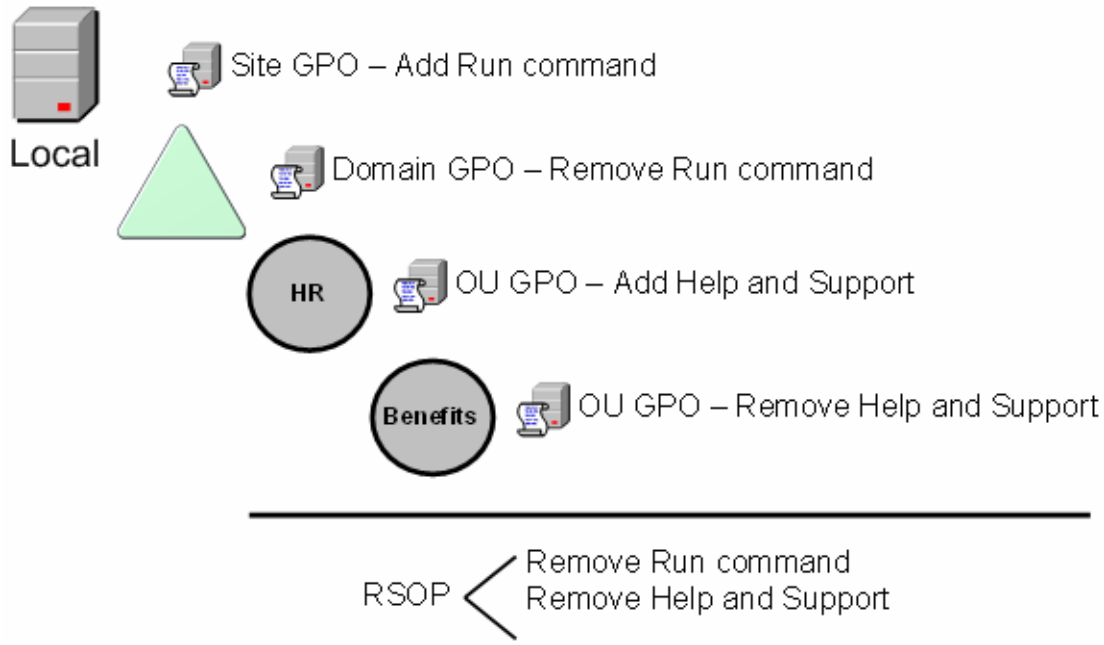

Figure 3.4: When a policy setting in two GPOs conflict, the setting with the highest priority will apply to the object.

Once you fully understand how GPO conflicts are handled from GPOs at different locations in AD, you might wonder what happens when there is more than one GPO at any one level. This situation is not possible at the local level. However, at the SDOU levels it is not only possible but also highly likely at the OU level. Figure 3.5 illustrates what GPOs at the same location would look like.

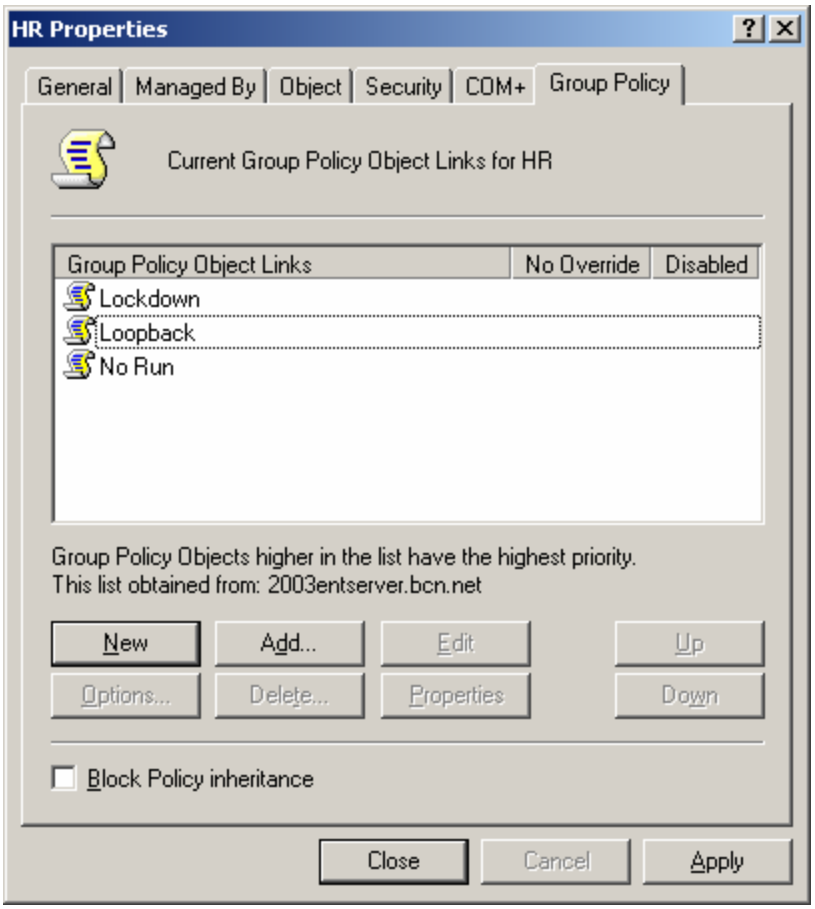

Figure 3.5: Sites, domains, and OUs can have multiple GPOs linked to them.

When there is more than one GPO linked to a single location in AD, the overall precedence does not change regarding the LSDOU. However, at each level, there is an additional calculation regarding which GPO has precedence at that level. From Figure 3.5, you can see that there are three GPOs. The one at the bottom of the list, No Run, has the least priority, and the one at the top of the list, Lockdown, has the highest priority.

We know that there are two considerations when applying GPO precedence. First, the LSDOU order is essential, with the GPOs linked closer to the target object receiving the highest priority. The second consideration is the order of the GPOs that are linked to the site, domain, or OU. Those at the top of the list will have a higher priority than those at the bottom of the list.

Controlling GPO Application Order

If the default permissions, settings, and hierarchy is left alone, there is little more to discuss with regard to GPO application. However, there are instances and situations that might require additional configurations to control how the GPO application occurs. In the following sections, we will discuss four methods to control the inheritance of the standard GPO application.

Block Policy Inheritance

The typical inheritance is to have the GPO settings append to one another from LSDOU, unless there is a conflict. Then, in the event of a conflict, the GPO with the highest priority wins. The block policy inheritance setting breaks those rules.

The block policy inheritance setting can be configured only at the OU and domain levels. The site level does not support the option to block any policy inheritance. It would only be blocking the local GPO, which it can't do. If the site GPO is to alter the local GPO, it must do so with a conflicting GPO setting. The local GPO is the first one to apply, so there would be nothing to block even if it could be configured at this level.

Thus, the only two locations that can block policy inheritance are at the AD level, so you will either need to be on the Group Policy tab on the property page of the domain or OU, or you can use the Group Policy Management Console (GPMC). If you are using the AD Users and Computers console, you will need to access the block policy inheritance option by following these steps:

1. Right-click on either the domain or OU level where the configuration will occur.
2. Click on the Properties menu option.
3. Select the Group Policy tab.
4. Select the Block Policy inheritance check box, as Figure 3.6 shows.

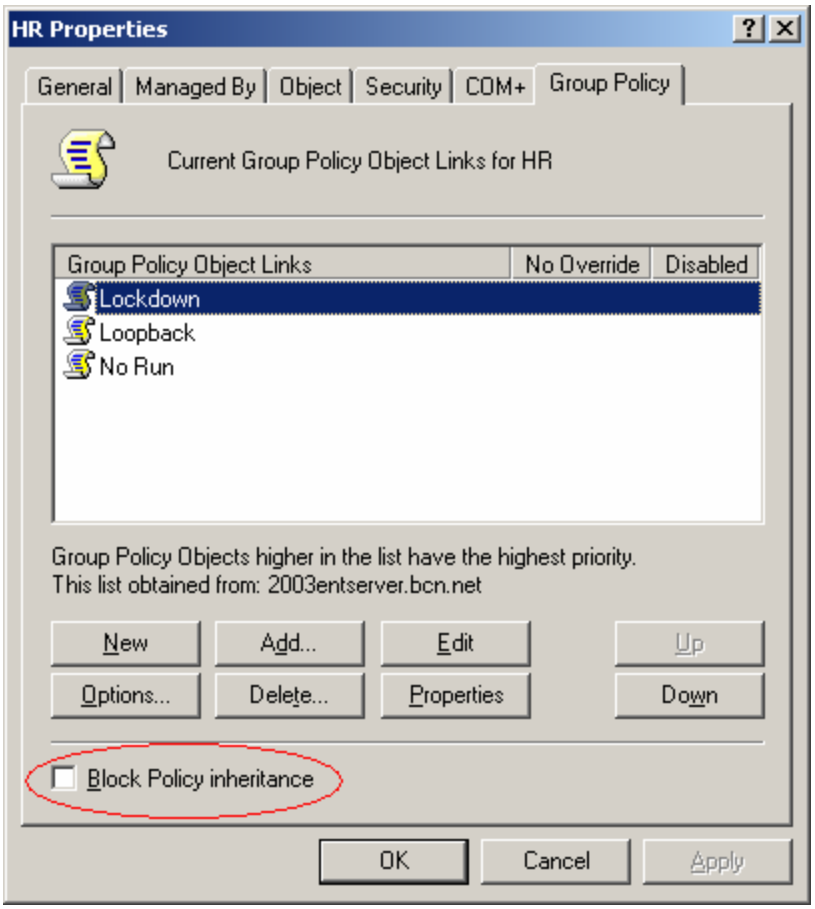

Figure 3.6: The domain and OU levels can block policies from lower in the GPO application order.

The result of this setting is that the policies at the local GPO and site GPOs (and the domain GPOs if the OU is configured) will not be a factor in the application of GPOs for the target objects in the configured location. The reason is that the blocking of policy inheritance blocks all other GPOs and policies at the other levels.

No Override

Imagine that a junior-level administrator has just configured the block policy inheritance setting at an OU three levels deep in the AD structure. You, as the domain administrator, have configured GPOs at the domain and top-level OUs to configure all aspects of security for both the computer and user accounts. You find out that the computer and user accounts are not receiving your GPO settings from the domain and OUs because they are being blocked.

As you can imagine, this spot is very compromising and can be scary and frustrating. However, there is no need to worry—there is a setting that can trump the block policy inheritance setting. This setting, the no override setting, can't be stopped by the blocking of policy inheritance. Unlike the block policy inheritance setting, which is global for all GPOs above the location of AD, the no override setting is GPO specific.

The no override setting can be configured for any GPO at the SDOU levels. It can't be configured at the local GPO level. To configure the no override setting, you can go to the same Group Policy tab while in the AD Users and Computers console, or you can configure the Forced setting inside the GPMC. To configure no override for a GPO from the Group Policy tab, follow these steps:

1. Select the GPO link that you want to force with the no override setting.
2. Click the Options button (or, you can just double-click the cell under the No Override column to get a check mark to appear)
3. Select the No Override check box, as Figure 3.7 shows.

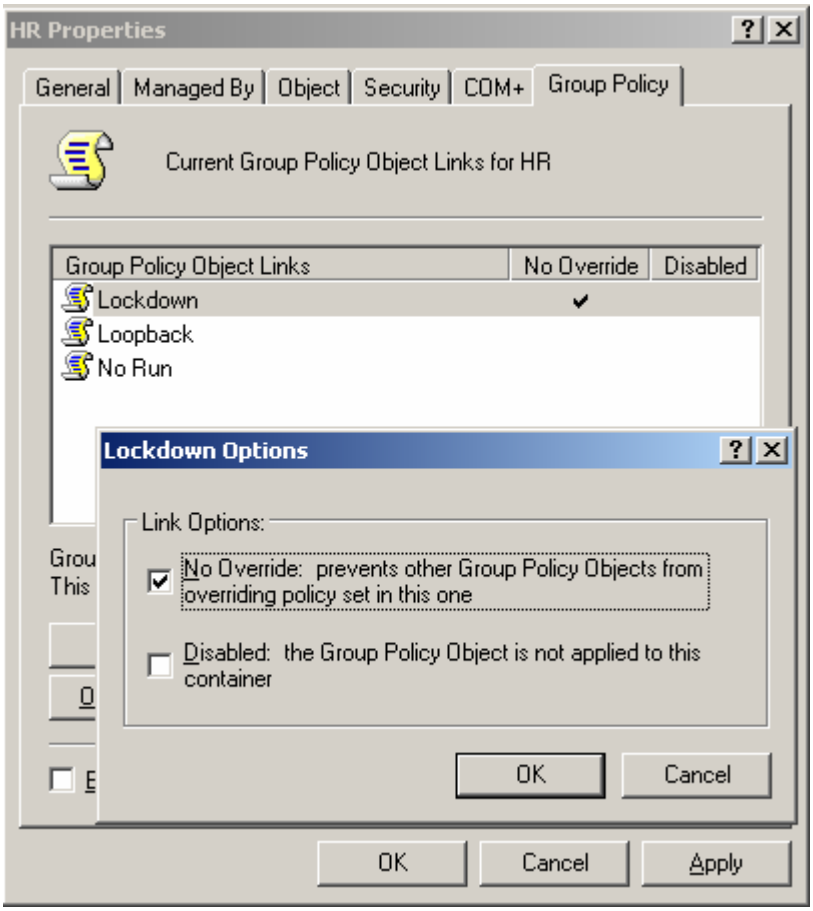

Figure 3.7: The no override setting at the site, domain, or OU takes precedence over the block policy inheritance setting at the domain or OU level.

Security Group Filters

Another way to control the typical inheritance of GPO application is to change the default behavior of security group filtering. What exactly is security group filtering? Security group filtering is a fancy word for modifying the access control list (ACL) of the GPO. Because the GPO is an object in AD, it has an ACL.

The process for modifying the ACL of the GPO is identical to that of a file, folder, or registry key. Of course, the detailed permissions are a bit different, because the GPO is a unique object type. The default permissions of every GPO provide the Read and Apply Group Policy permissions, which allow computer and user objects to receive GPO settings as Table 3.3 shows.

Access Control Entry	Permission
Authenticated Users	Read—Allow Apply Group Policy - Allow

Table 3.3: Default permissions allowing all computer and user accounts to receive GPOs.

Read and Apply Group Policy permissions are the only permissions required to receive a GPO. If either of these permissions is not provided for an object, the object will not receive the GPO settings for that GPO. Remember that the Authenticated Users group includes all computer and user accounts (all domain controllers and the Administrator account).

We need to combine two concepts to ensure that the concept of ACLs on GPOs is clear. Notice that the default ACL on the GPO provides a group for the filtering of the GPO. This particular group includes every computer and user account in the domain. However, we saw in the earlier scenarios that the computer or user account must be in the path of the GPO to receive the GPO settings.

If you refer back to Figure 3.2, Table 3.1, and Table 3.2, you can see that you were not concerned with the ACL of the GPO. The GPOs from Table 3.1 simply had the default permissions, which allowed every account in the path to receive the settings. What if you wanted to restrict BettyF from receiving the GPO settings linked to the Users OU? BettyF is currently receiving the GPO because she is a member of the Authenticated Users group. To restrict her from receiving the GPO, you can simply add her to the ACL explicitly, giving her Deny permissions to either Read or Apply Group Policy, or Deny her both permissions.

Make sure you consider the following key points when establishing GPO security group filters:

- The ACL that is configured for the GPO is a property of the GPO, not a property of the GPO link to the SDOU.
- Troubleshooting GPO filtering can be difficult. The GPMC and other third-party tools are needed to help find where GPO filtering is established.
- Security group filtering should be used as a last resort for solving a unique GPO application problem. The best way to avoid the use of security group filtering is to design your AD properly.

WMI Filters

A final method used to control the default behavior of GPO inheritance is the use of WMI filters. WMI is a remarkable tool that can not only help with GPO application but also with routine network administration. With regard to GPOs, the WMI filter helps determine whether a target account should receive the GPO settings.

For example, if the GPO is installing a software package that is larger than 250MB installed, it would be beneficial to find out if the target computer has enough hard drive space before the installation begins and subsequently fails. So, the WMI query determines whether there is more than 250MB of hard drive space. If the query says "yes," the software is deployed. If the query returns "no," the GPO is ignored for that target account.

WMI filters are individual files that contain the query. These files are then associated to the GPOs. To associate a WMI filter to a GPO from within the Active Directory Users and Computers console, follow these steps:

4. Select the Group Policy tab on the Properties window for the SDOU where the GPO is linked.
5. Select the GPO from the list, and click Properties.
6. Select the WMI Filter tab on the HR Properties window.
7. Select the "This filter" radio button, and click Browse/Manage.
8. Click Advanced on the Manage WMI Filters window, click New, and type a name for the WMI filter into the Name field.
9. Type the query that you will use into the Queries text area. An example might be to check for the installation of Windows XP Professional, which would use the following text

   ```
   Root\CIMV2; SELECT * FROM Win32_OperatingSystem WHERE Caption
   LIKE "Microsoft Windows XP"
   ```

10. Click Save, OK, OK again in the Properties windows, and OK one more time in the next Properties window.

The following list highlights additional key considerations when working with WMI filters:

- WMI filters only apply to WS2K3 and Windows XP; Win2K target computers ignore that WMI filter and apply the GPO.
- WMI filters are associated with the GPO, not the GPO link.
- If a WMI filter file is deleted, but the associate to the GPO is not, the GPO will not apply to any target. The WMI filter extension will return a set of null for targets that meet the query.

Effective OU Design Is Critical

With this knowledge of the key aspects of GPO basics, we're ready to switch directions to the foundation for implementing GPOs. Without an OU design and structure to link GPOs, there is little that can be done to control security, software, and other OS settings that are controlled by GPOs.

As you consider your OU design, don't forget about the overall AD design, which includes other domains and possibly other forests. You will need to consider how GPOs in these other domains will be updated and stay consistent across the entire company.

The OUs are the most important aspect of the AD design when considering the implementation of GPOs. We can't negate the other reason that OUs are organized and created, which is for delegation of administration. As you start to design your OUs, you will need to make a list of all of the delegation that needs to occur. This list will include delegation for user, group, and computer accounts, as well as for OU, GPO, and AD administration. The result of these considerations will be an OU structure. Next, the full list of GPOs and GPO settings will need to be established. This list will include categories of what needs to be controlled by GPOs. The following list provides all the areas that a GPO can control:

- Application management
- Disk quotas
- EFS recovery
- Folder redirection
- Internet Explorer (IE) settings
- IP Security (IPSec)
- Registry settings (administrative templates)
- Scripts
- Security

From these possible GPO areas of configuration, you will determine how the GPOs should be applied and to which target objects. You need to consider only the placement of computer and user accounts, because these are the only two objects that can receive GPOs. When you consider which GPO settings will affect which target objects, consider the following categories (and potential OUs) for organizing the GPO application:

Computer account categories

- Server role (IIS, Exchange, SQL, and so on)
- Client computers
- IT staff client computers
- Secured client computers
- HR servers
- Branch office client computers

User account categories

- IT staff
- Developers
- Executives
- Service accounts
- Employees
- Branch office employees

After considering both the delegation of administration and the GPO implementation factors for the OU design, the two OU structures need to be merged. For smaller organizations, this task will not be difficult if there are only a few delegations and GPO categories. For larger organizations, this task can result in a very complex structure that consists of many conflicting OUs, where an OU contains accounts for delegation reasons that break the GPO implementation strategy.

For areas of the AD design in which delegation and GPO considerations conflict, there are some possible solutions:

- Create a hierarchy of OUs in which the top-level OU consists of the delegation and the sub-OUs are where the GPOs are linked. This setup will provide a solution for both delegation and GPO implementation for specific accounts.
- Use GPO security group filtering to control which accounts in the OU will receive the settings in the GPO. This option is not the preferred method, but in some cases, it is the only possible solution.

When a conflict can't be resolved, the delegation should win the conflict, because GPOs can be filtered with security groups.

Even for the small AD implementations, the complexity of delegation and GPO administration can overwhelm the built-in administration tools. Microsoft has developed the GPMC to help with the administration of many of the GPO tasks, but there are still holes. To fill these holes, you should look into other GPO management tools from companies such as ScriptLogic, Full Armor, and Quest Software. These tools can provide options that the Microsoft tools lack. The following list highlights some of the capabilities that these tools can provide:

- GPO version control
- Offline GPO change management
- Documentation
- Auditing

In the next couple of sections, we will discuss the need for some of these capabilities and why they should be considered to ensure a secure AD environment.

Implementing Group Policy

A single GPO has 766 policy settings. The new Windows XP SP2 will include an astounding additional 609 GPO policy settings. With all of these settings, a test environment is essential. If you couple the raw number of GPO policy settings with the complex interaction of GPOs from LSDOU, block inheritance, and no override, you can clearly see that a test lab environment is essential for stable and correct GPO application. Unfortunately, native AD tools don't provide this lab environment to test settings before they are rolled out. The test lab environment will provide the following benefits for GPO implementation:

- Test complex LSDOU interaction before implementing to production
- Determine the Resultant Set of Policy (RSoP) for the user and computer accounts to ensure compatibility with applications and network access
- Verify inheritance and control of inheritance is correct before moving GPOs to the production environment
- Test different domain interactions with consistent GPO configurations
- Provide a "central" location for developing GPOs that will be consistent across multiple domains and forests
- Different versions of the same GPO can be tested and the RSoP can be evaluated for optimum control over security and other GPO policy settings before being released to production
- New GPO settings, distributed with service packs and applications, can be tested for compatibility and stability before being placed into production

Migrating Group Policy Between Domains

During the design of AD, you will be forced to have a single domain, multiple domains, or possibly multiple forests. These decisions can be forced for a variety of security or political reasons. Even though you might have multiple domains for these reasons, many of the GPOs that are implemented will need to be consistent across the domains. GPOs can be created in one domain, or even in the test lab environment. They will eventually need to be moved, or migrated, to all of the domains to ensure consistency of security settings across the entire AD infrastructure. The following sections include items to consider when migrating GPOs between domains.

GPO Consistency

If you have multiple domains, you will want to have GPOs consistent through all of the domains (as much as possible). For administrative, security, and sanity reasons, you will need to have a process in place to ensure that GPOs are all the same. The reasons that GPOs need consistency between domains include:

- Security—The only method that provides consistent security settings for all computers in the enterprise is the use of GPOs. With 1000 policy settings, you don't want to miss one single setting. The ability to migrate a single GPO for security to multiple domains will provide the coverage of security that the network deserves.
- Stability—Administrators are not without error, and with so many GPO policy settings to choose from, errors are easy to make. A single errant configuration can cause a computer to not communicate on the network, causing loss of time, money, and data.
- Efficiency—When it comes time to troubleshoot a network or application problem that is rooted with a conflicting GPO setting, administrators and Help desk professionals will benefit from consistent GPOs. When GPOs are migrated from one domain to another, allowing consistent configurations across all environments, the troubleshooting process is much easier.

GPO Tracking

When a GPO is created, it is given a unique identification number. This number is referred to as a Global Unique Identifier. GUIDs are not friendly to humans, as they are rather long. For example, the GUID for the Default Domain Policy GPO is {31B2F340-016D-11D2-945F-00C04FB984F9}. Each GPO is given a GUID as it is created in the domain so that it can be tracked by the OS. The OS must track two locations for GPOs. One is in the AD and one is in the SYSVOL folder on the domain controllers. Each location refers to GUIDs—not the name of the GPO—for tracking GPOs.

When a GPO is migrated from one domain to another, this GUID needs to be created by the OS. Creating a new folder for the new GPO and copying the contents of the source GPO to the new folder will not suffice for migrating a GPO from one domain to another. Doing so will not create the required GUID and embed it in the AD for tracking purposes.

Tools, such as the GPMC and other GPO management tools from third-party vendors, provide an easy method to migrate GPOs from one domain to another. These tools handle the registration of the GPO, affording the creation of the GUID and correct entries in AD for tracking.

GPO Permissions

When a new object is created in a domain, it must be tracked by the OS. There is more to an object in AD than a GUID. There is also a Security Identifier (SID) that helps control access to resources. GPOs don't have SIDs, but they do have an ACL, which contains lists of SIDs. This list of SIDs must be relative to the domain in which the object is created.

GPO management tools provide a seamless process to take care of this small, yet important detail. If the permissions for the GPO ACL were not fixed, the GPO would not be implemented to any computer or user account due to incorrect SIDs on the ACL.

GPO Management

After a GPO is migrated to the target domain or domains, there is still work that needs to be done. The GPO must be linked to the proper SDOU. Although the built-in tools provide this capability, they don't make the task easy. You must remember all the considerations for GPO management:

- Linking to SDOU
- Block policy inheritance
- No override
- Security group filtering
- WMI filtering

If you have a multitude of GPOs that either reside in a single domain or are migrated from domain to domain, the standard tools for these tasks can cause more harm than good due to their inability to easily control these GPO functions. Third-party tools can provide a significant advantage to the management of these functions. The GUIs are designed around GPOs and incorporate small icons, color changes, and menu options that make management of these features easier.

Auditing Group Policy

The concept of auditing has been around OSs and resources for a long time. However, the concept of auditing GPO management is new. There is, in essence, nothing built-in to AD or Win2K or later to help with auditing of GPO management.

Certainly, there is the Event Viewer and advanced GPO logging, but these tools are not centralized, produce less than coherent log results, and don't provide for the detailed information that is required for a good audit trail. The built-in tools also fail miserably when it comes to any form of reporting or alerting when an event does occur.

Therefore, when it comes to auditing GPOs, you are best off obtaining a third-party tool. Not even the illustrious GPMC can touch auditing of GPOs. What do these third-party tools provide that is so important for auditing of GPOs?

- Change management—This benefit includes tracking the old and new values of the GPO, who performed the change, when the change occurred, and archiving the old versions of the GPOs for future reference.
- Reporting—When you have a multitude of GPOs in AD, you will also have a multitude of changes that need to be queried and summarized. The reporting features should allow for custom searches, reports, and documentation based on a variety of variables, such as date, time, user, GPO name, domain controller, and policy.
- Alerting—If an errant or malicious change to a GPO occurs without notice, damage can be done long before the change is ever tracked and remedied. Alerting provides an immediate notification that something has changed, so the IT staff is aware of all possible vulnerabilities or outages based on GPO mistakes. These alerts can be via email, pager, or phone.

There Isn't Much Natively

The only capabilities that are provided natively in Windows include the basic event logs and additional capabilities for verbose logging. The native event logs are usually so cryptic, they are not worth the effort to decipher them. However, with enough experience and event ID tracking, they can be useful to an experienced administrator. For advanced logging, this does provide for advanced and detailed tracking of GPO management. However, the logs are not stored centrally, they are stored in different files for each log activity, and there is no reporting or alerting capabilities. The advanced logging is also difficult to configure on many computers, because they require registry updates to be triggered. The following list highlights the categories of the different logs that can be configured natively for GPO logging:

- GPO core logging
- Security logging
- Folder redirection logging
- Software installation logging
- Windows Installer logging
- GPMC error logging
- GPMC error and verbose logging
- GPMC editor logging

Change Management

When you are auditing GPO change management, you are highly concerned about what changed, who changed it, when it changed, what it was changed to, and what it was changed from. Any good GPO auditing tool will provide this information to ensure GPOs are tracked and can be audited. If any of this information is omitted, it is difficult to audit the process of GPO management, because at least one important piece of the puzzle would be missing. Most of the third-party GPO auditing tools will categorize the change management within a graphical interface, breaking down the information into the following areas:

- Date/time of the change
- User who performed the action or change to the GPO
- Domain controller on which the change originated
- GPO name and GUID of GPO
- Section of GPO that the change occurred
- Old value of policy setting
- New value of policy setting

These changes should be archived in a central location so that they can be referenced later. Also, there should be a query option built-in to the archive to allow for manipulation of the data, showing trends and dates when changes have occurred.

Reporting

The reporting tools for GPO auditing should interface seamlessly with the archived change management system. This system should provide access to all of the archived information, offering pre-built and custom reports on the data. The reporting tool should also incorporate a custom query function so that reports can be generated based on the information that is archived from the change management tool.

Another feature that is important for reporting on GPO auditing is to have the reporting tool support HTML. This support can provide a means to access the archive of information from any computer. When a problem arises that might be associated with GPOs, the administrator can quickly go online and determine whether any changes have occurred in the recent past. The HTML interface can also provide a means to access management reports and documentation.

Alerts

When a GPO is undesirably changed, bad things can happen—an executive might not have access to the Internet, security could be omitted from a server configuration, or an application could be removed from an HR workstation. If one of these problems occurs, or possibly a worse problem arises from a GPO configuration, you need to be alerted of the change that can cause the problem.

Many of the GPO auditing tools won't do so natively; they will instead rely on the existing real-time alert infrastructure that the network provides. This capability could be provided by ScriptLogic, Microsoft, NetIQ, Tivoli, or another third-party vendor. If the GPO auditing tool provides this functionality natively, that is just a bonus of the tool, because you won't need to implement another real-time alert tool or interface with your existing tool.

Other Capabilities

We have looked at a variety of GPO requirements, features, tools, and functions. There are even more considerations as you move forward with GPOs to secure your AD infrastructure. Most of these additional capabilities will not be supported in the built-in tools that Microsoft provides. You will need to head to the GPMC or a third-party vendor solution to get these features. However, once you see what these tools provide, you will quickly determine that it is not a want but a need for GPO management.

Rollback Capability

Many of the GPO management tools provide an archive of historic GPOs. These archived GPOs maintain their policy settings and can be brought back from the archive into production at any time. This feature is an excellent solution for a large organization that needs to implement the latest and greatest security changes, regardless of the compatibility issues they might cause. In this case, security is more important than functionality. However, if the changes from the GPO provide too strict an environment for any production to occur, the old GPO can be brought back online to the production environment.

Review and Compare Old GPOs

After many changes to GPOs, you will have a large archive of GPO versions. There will be cases in which you want to investigate the settings that have occurred over time, comparing and contrasting different settings that are set in the different GPOs. Most GPO management tools provide a mechanism to compare one or more GPOs. This functionality can help track down a problem that a computer or user is having on the network, for example. If a virus or worm has entered your network, this feature can also provide insight into where the vulnerability might have come from, based on the archive of GPOs that were in production at the time of the attack.

RSoP

RSoP is essential for troubleshooting and evaluating new GPO settings. Almost every tool provides two views of the RSoP from the GPOs. The RSoP will accommodate for the inheritance, blocked policies, forced GPOs, security group filters, and WMI filters. If you were to try to manually evaluate all of these permeations for GPO application after the introduction of a new GPO, it would take many hours and cause much frustration.

Most tools provide two options for the RSoP evaluation. The first is used for troubleshooting. This feature will evaluate a specific computer account and user account, providing the final policies that affect the different accounts. The evaluation result will also indicate where the final policy settings were applied from, and in some cases, the result will include all GPOs where the policy was set, indicating any alterations to the default inheritance behavior of the GPOs.

The second RSoP feature is related to changes to computer and user account location in the AD. If a computer account is going to be moved to a different OU, it is ideal to first evaluate what the final GPO settings will be on the object before the move. The evaluation will help indicate any potential compatibility, security risk, or access issues that might occur due to the interaction of GPOs.

Backup and Restore GPOs

It is a great idea to have good documentation and a physical backup for GPOs. In Win2K AD, there are only a few tools that provide backup and restore options for GPOs. This capability is a routine function for all of the GPO management tools. As we investigated the migration of the GPOs earlier, you were introduced to different aspects of the GPO that can cause problems when moved from one environment to another. Likewise, when a GPO is backed up, it must be treated with care upon restoration.

The tools that you will use to backup and restore GPOs take this additional care, but in case there is a problem, you might need to step in and assist with the situation. If you need to assist with the restoration of a GPO, you will want to check the following characteristics of the GPO to ensure a valid restoration:

- GUID—The GUID must be the same for the GPO stored in AD and the one stored in the SYSVOL. Not only on one domain controller, but all domain controllers. If there is a mismatch or one portion of the GPO is missing, you might need to force replication of the AD or the SYSVOL to converge the restoration.
- GPO version—Each section of the GPO, computer and user, are managed by the version number of the GPO. When a change occurs to the section, the version number is incremented. Be sure the version numbers match for the GPO parts stored in AD and in SYSVOL. Like the GUID, if there is a mismatch, be sure to force replication.
- GPO timestamp—When dealing with a backed up GPO, you are dealing with an older version of the GPO. Be sure to verify that the restored GPO has replicated to all domain controllers or you will experience strange behavior and results on some of the computers that receive GPO settings from the domain controllers that have not received the replicated changes to the GPOs.

Troubleshoot Client-Side GPOs

When a problem arises from the application of a GPO on the client, it is logged on the client. These logs are not always useful, but if verbose logging is enabled, they can be helpful in diagnosing the problem. Some third-party tools allow for the advanced capability of viewing these remote logs on client computers. They also provide capabilities for configuring the advanced logging on one or more remote client computers. This feature provides the consistency and capability required to troubleshoot GPO problems that come up due to client-side issues.

Summary

In this chapter, we focused on GPOs and how they provide security control for computer and user accounts in the enterprise. We saw that GPOs are extremely logical, but have many features, settings, and options that make them a bit complex. With the built-in tools, GPOs can become a bit overwhelming to manage. There are plenty of good GPO management tools that can help implement, manage, troubleshoot, and monitor GPOs.

Next, we will finish off talking about AD security by taking an in-depth look into delegation of administration. We will need to refer back to parts of this chapter, as the interaction of delegation and GPO implementation overlap.

Chapter 4: Delegating Administrative Control

Delegation of administrative control might be the sole reason you moved from your old directory service to AD. Many want to move to AD to take advantage of the efficiency, security, scalability, and ROI that delegation provides. The ability to provide detailed task privileges to all areas of the IT staff, as well as to non-IT professionals, is why delegation is so useful.

There are many tasks that can be delegated within AD, but they can all be broken down into two categories: data administration and service administration. Data administrators control the resources that are stored in AD, such as user, group, and computer accounts. They also control member servers and the resources that reside on these computers. The administrative responsibilities that are associated with these tasks are broken down into categories to help organize the delegation that must occur to get all of the tasks done. Once the categories are created and the AD design finalized to include data administration, the delegation of these tasks can be completed. Delegation of data administration is provided within AD by giving data administrative groups permission over the objects that they will control.

Service administration and the delegation of the related tasks differ greatly from data administration. Service administration controls the directory service, ensuring it is configured properly, available, and stable. Service administration is typically delegated by adding user accounts to existing groups that already have privileges to control aspects of AD administration. These groups and additional groups are configured with user rights on domain controllers to give them additional delegated privileges. These delegated tasks are assigned from categories that organize the different AD administration tasks necessary to keep AD running.

You must begin delegating within AD early in the directory implementation. This best practice is one of many that you will be introduced to with regard to delegation of administration in AD. This chapter will also explore additional AD delegation best practices in areas such as logical and structured designs, the use of roles, and a clear understanding of your delegation model.

Once the delegation is implemented, the job is not done. You will still need to monitor and control the delegation for the production environment. This task typically can be broken down into three areas: logging, monitoring, and auditing. Each area is critical to ensuring that security within AD is maintained. Finally, we will take a look at tools that can help you complete your delegation within AD.

Data Administration

Data administration is not only the administration of data—it entails almost every delegation aspect outside of supporting the directory service itself. Data administration includes the following responsibilities:

- Creation of user, group, and computer accounts
- Assignment of user rights to user and group accounts
- Management of group membership
- Management of resources (data, application, and services) on member servers
- Management of client computers

The common thread among all of these responsibilities is controlling privilege access to a resource. In some cases, the resource is a file and in other cases the resource might be an entire server. Regardless, the structure of allowing, or delegating, these responsibilities must be designed, implemented, and maintained.

Delegating GPO Administration to Data Administrators

Data administrators are responsible for clients and servers, so there is the potential for them to control GPOs, which offer an ideal means of controlling all computers in the domain for security and configuration settings. As we have seen, GPOs provide control that is targeted and final. However, should a data administrator have control over GPOs that are targeted to clients and servers? This question can only be answered by the individual company and IT department. Take caution when considering this decision as you are giving data administrators a great deal of power when you give them control of a GPO.

GPOs can control security permissions on the target computer, group membership on the target computer, security settings, and much more. If a data administrator is delegated control to create, link, and edit GPOs, there is nothing that administrator can't do with or to the target computer. Also, if there are any user accounts in the OUs to which the data administrator has been delegated privilege, the administrator will also have control over these user accounts on the network. Ideally, you will not give any data administrator the ability to create or edit GPOs, instead delegating only the ability to link a GPO to an OU.

Delegating Object Creation Administration to Data Administrators

It is a common delegation to provide data administrators with the ability to create objects, such as user and group accounts. However, it is often overlooked that once this delegated privilege is given to a user, the user has full control over that object because the user owns the object (as with files and folders, the user that creates an AD object becomes the owner of the object). Thus, if you do want users to have full control access over the objects in AD, do not provide them with the ability to create the object. Alternatively, you can implement a process to change object ownership once an object has been created by a user.

Categories and Roles of Data Management Delegation

As you think about the overall design of data management delegation, consider the myriad options that you have available. The following lengthy list highlights data management categories and the delegation responsibilities that might fall under each role:

Account Administrator

- Create user accounts
- Delete user accounts
- Move user accounts
- Reset a user's password
- Unlock user accounts
- Modify user account properties
- Authorize access to user and group accounts
- Link GPOs to user account OUs

Workstation Administrator

- Create computer accounts
- Link GPOs to computer account OUs
- Have membership in local Administrators group
- Have permission to control workstation remotely

Server Operators

- Create computer accounts
- Link GPOs to computer account OUs
- Have membership in local Administrators group
- Have permission to control server remotely

Resource Administrator

- Control access to data
- Control service and service account on server
- Control application on server

Security Group Administrator

- Create security groups
- Modify the membership of security groups
- Delete security groups

Help Desk Operators

- Reset passwords on user accounts
- Unlock user accounts
- Control non-security–related user account properties

Application-Specific Administrator

- Control services and service accounts
- Modify the membership of security groups
- Have membership in local Administrators group

How to Delegate Data Administration

It is ideal to delegate data administration at the OU level, which allows for the greatest control over who is able to delegate and which objects a user can control. As a guideline for the data administration delegation process, the following list suggests steps that will need to be performed for every delegation that occurs within AD related to data administration:

11. Implement OUs based on the specific data administration model that was designed.
12. Move user, group, and computer accounts into the proper OUs.
13. Create groups that will be used for the delegation process. For example, you might create a group named Sales_PW_Reset that will be used to reset passwords for Sales employees.
14. Add the user accounts to the groups that were created for delegation.
15. Configure delegation for all groups based on the data administration design model that you developed. (You can use any number of tools for this procedure, as we will explore later in this chapter.)

After you delegate administrative privileges to users in the environment, you will need to provide them with tools so that they can perform administrative tasks. The preferred tool for administering user and group accounts is the Microsoft Management Console (MMC) Active Directory Users and Computers console. This tool can be installed on client computers by installing the Adminpak, which is on the server installation media as well as under the system files on any domain controller.

Another option is to create Taskpads, which are individual tasks created from the original Active Directory Users and Computers console but have a narrow scope to control what the user has access to. These Taskpads are discussed in more detail in Chapter 2.

Service Administration

Service administrators configure and manage AD and domain controllers, ensuring the directory service is functional and available. They have privileges that can cross domain boundaries, with the forest acting as the security boundary. Service administrators can act as data administrators, but data administrators cannot perform directory service administrative tasks. The overall mission of the service administrator is to make sure AD is running smoothly and efficiently.

With the scope of the service administrator controlling such important aspects of the company and network, there should be very few service administrators for any given task. Some companies have a team of 5 to 10 IT professionals that control service administration tasks, which allows for separation of duties as well as coverage in case an employee leaves or is promoted out of the role.

Categories and Roles of Service Management Delegation

Service management delegation is slightly more complex than data management delegation. Service administration tasks have greater ramifications if performed incorrectly and the AD configurations can be more difficult. The following lengthy list highlights service management categories and the delegation responsibilities that might fall under each role.

- Installation management—This role's tasks include the installation of new domains and domain controllers for the existing AD infrastructure as well as for the overall network
- Schema management—This role's tasks include control over any and all schema changes, modifications, additions, or considerations—involving not only direct changes to the schema but also to applications that extend the schema
- Trust management—This role's tasks include control over all trusts that can be created within or outside of the AD infrastructure (cross-link, Windows external, Kerberos external, and cross-forest trusts are included)
- Operations master roles management—This role's tasks include management of all the operations master roles in the entire forest and the roles in each domain; involves moving and seizing the roles between domain controllers
- Backup and restore management—Specific to the domain controllers and the AD database, this role's tasks include the backup of the system state, Sysvol, and all policies and logon scripts associated with the AD enterprise
- LDAP policy management—If there are any LDAP policies, this role is responsible for the creation and management of the policies and what the policies control
- Replication management—This role's tasks involve all functions related to the replication of AD, GPOs, logon scripts, and Dfs data
- Functional level management—This role's tasks include the control over the functional level at both the domain and forest level and the associated details that control this behavior
- Directory database management—This role's tasks include the optimization, security, location, and recovery of the AD database and the associated files to keep AD up and running

- Security policy management—This role focuses on the two default GPOs at the domain and domain controller OU levels (primarily including the Account Policy settings and the user rights configuration for domain controllers)
- DNS management—With DNS playing such an integral part of AD and the location of resources, an entire role is dedicated to the administration of DNS; this role's tasks involve the interaction of DNS with AD, security of DNS, and replication of DNS
- Domain controller management—This role's tasks include the control over installation and configuration of the domain controllers, which involves the management of services, applications, and data that is stored on the domain controllers

Service Administration Groups and Privileges

Service administration is delegated by adding user accounts to administration groups. These groups have default privileges, but they can also be given additional privileges through user rights. The following list provides suggested service administration group models and their privileges:

Forest Configuration Operators

- Creating and deleting child domains
- Creating, deleting, and managing all trust relationships for the forest
- Creating, deleting, and managing cross-reference objects
- Transferring and seizing the forest-wide operations master roles
- Raising the forest functional level

Domain Configuration Operators

- Managing replica domain controllers
- Managing operations master roles
- Managing the default Domain Controllers OU
- Managing the content stored in the System container
- Restoring AD from backup when required

Security Policy Administrators

- Managing Password policy settings
- Managing Account Lockout settings
- Managing Kerberos Policy settings

Service Administration Managers

- Managing service administration user accounts
- Managing service administration security groups

Domain Controller Administrators

- Managing software
- Managing service packs and security updates
- Managing GPO settings, for both security and control
- Managing event logs
- Managing directory service files and Sysvol

Replication Management Administrators

- Managing sites
- Managing subnets
- Managing site links and site-link bridges
- Managing the replication schedule and replication interval on site links
- Managing manual site connections

DNS Administrators

- Installing the DNS Server service on domain controllers
- Managing and configuring DNS recursion methods
- Managing forest-wide zones
- Managing DNS application partitions

How to Delegate Service Administration

Like data administration delegation, service administration delegation needs to be considered early in the AD design process. Although some of the delegation can be achieved by group membership, service administration still requires some OUs for controlling group membership and other delegation tasks. The following is a suggested process for how to delegate your service administration:

16. Create an OU to place the security groups that represent the service administration roles.
17. Create new groups that will be used for each of the service administration roles (where a default administration group does not cover those responsibilities).
18. Add the appropriate security group to all resource ACLs to provide the group with the sufficient access to perform the administrative task (this might include additional permissions given to a group for system files and folders).
19. To allow the service administration group to perform their tasks, configure appropriate user rights on all domain controllers and servers that run directory service applications.
20. Configure delegation for all groups based on the service administration design model and roles that you developed. (You can use any number of tools for this procedure, as we will explore later in this chapter.)
21. Add the appropriate user accounts to the security groups for each role.

At this point in the process, you need to provide the appropriate tools to the service administrators.

Best Practices

What is a best practice? In this context, we are going to define a best practice as a suggestion or recommendation from a valued, experienced source. A best practice is something that can be quantified, based on experience and analysis. The best practices here are from years of experience with AD, security, and delegation. Any good delegation strategy or best practice must be based on structured and logical thought processes, including a methodology of separating and organizing the different tasks into categories that are easily tracked and understood. Both of these factors will be molded into a model, which can then be implemented. The implementation stage is just as important as the design phase because mistakes here result in security issues down the road. In the following sections, we cover all of these areas of best practice delegation.

Delegation Needs to Be Structured and Logical

When you develop the model for your delegation, it must be structured and logical so that it can be implemented and managed with ease. Best practices that you should follow as you develop your delegation model include:

- Have a good understanding of all aspects of AD management
- Understand the administrative needs of departments, applications, and services that are associated with the Windows network
- Ensure that the delegation model has multiple users controlling each administrative task
- Always work from the least privilege aspect of any task and add permissions and privileges on an as-needed basis

Delegate Around Roles

As you design the delegation model, consider using roles as the core structure for the administration task. Roles categorize the different tasks so that you can either provide full access to each task in a role or partial access to a few of the tasks. We have already broken down the data and service administration delegation options into roles. You can either use these roles or develop your own roles as a basis for your delegation model.

Delegation Model

As a best practice for delegation, you need to develop a delegation model. This model will be the underlying structure for your AD design and how the objects in AD are organized. You will need to consider all of the different aspects of how your company is organized, especially with regard to the IT administration staff. You will need to work this consideration into the delegation model. In the end, the delegation model will provide the foundation for the overall AD structure and specific delegation for data and service administration. A good delegation model will

- Make sure all aspects of data and service administration are covered
- Provide separation of duties and isolation of duties where needed
- Ensure that data and service administration tasks are equally divided among the users performing these tasks
- Ensure that the delegation for all tasks is implemented using the least-privilege concept
- Restrict delegated tasks to only a few individuals

Best Practice Implementation

As you deploy and implement the delegation, there are some best practice considerations that you should keep in mind. Some of these can cause more initial work, but the time that they save in the long run is well worth the initial effort. When you implement delegation, make sure you consider the following:

- Every data and service administration role is covered by a security group
- Do not use security groups that were designed for delegation for any other purpose (this includes ACL permissions, user rights, and GPO filtering not associated with delegation)
- For delegation management of AD objects such as user and group accounts, make sure you delegate at the OU level
- Avoid configuring delegated management at the individual user or group account level
- Delegate with limited access in mind; doing so will require using resources that specify delegation configurations and testing for your environment

Logging, Monitoring, and Auditing

It is foolish to design, implement, and manage delegation without some way of ensuring that the desired delegation is the actual resulting delegation. To do so, you can have different levels of checking on the delegation of AD administration. First, you can establish a log that tracks changes to delegation as well as the use of delegation privileges. Next, you can monitor, either manually or automatically, the activity that occurs as a result of delegation of tasks. Finally, an audit needs to be done to ensure that the documented delegation is the current delegation.

The following sections explore each of these areas to ensure that delegation at all steps in the process is covered and correct. If you are not satisfied with the built-in capabilities of the Windows OS with regard to these tasks, investigate tools from ScriptLogic, Aelita, NetPro, and BindView. These tools provide more robust and efficient solutions.

Logging

You can produce logs of delegation activity with the built-in logging feature of Windows. With this feature, you can track almost every activity that occurs to an object, service, or setting within the OS. Ideally, you will set up logging on the domain controllers to track when data administrators manage the objects contained in AD. If there are any servers that contain resources, you will also need to enable logging on those servers. For service administrators, you will primarily establish the logging only for the domain controllers, because these computers are the only servers that control AD.

The logging settings that need to be enabled to track delegation and the use of delegated privileges include:

- Account management—Tracks account management events that occur on the local SAM of servers and within AD
- Directory service access—Tracks when a user, group, or computer accesses an AD object; the object must also have auditing configured on the System Audit Control List (SACL), which is unique per object
- Object access—Tracks when a user, group, or computer accesses a resource; the resource must also have auditing configured on the SACL, which is unique per resource object (objects can include files, folders, registry keys, printers, and AD objects)
- Policy change—Tracks changes to user rights, audit policy, or trusts
- Privilege use—Tracks when a user performs a task that uses a user right on the computer
- System events—Tracks when the client is restarted or events that affect system security or the Security Log

To ensure consistent and persistent configuration of the logging settings, it is best to use GPOs to deploy these settings. For domain controllers, use a GPO linked to the Domain Controllers OU. For all other computers, create a new GPO, link it to the appropriate OU containing the computer accounts, then configure the audit policy settings in the GPO.

The logs generated from these settings are tracked in the Security Log of the Event Viewer. The security logs are kept in the log until they are archived or overwritten by newer events. Each OS configures the size of the security log differently, but it is a good idea to increase the size of this log to more than 10MB for domain controllers to ensure that all of the information is captured between archiving of the log. If there is a lot of traffic on the domain controller or there are numerous resources being tracked, it might be a good idea to increase the security log size to 50MB or more to ensure that no events are lost.

Monitoring

Once you have the logging and tracking established, you need to be made aware of when a critical event occurs. Even if the event is not logged, you still want to be made aware of the event occurring. Unfortunately, Microsoft does not have any such tool built-in to the Windows OS and really don't have many options that provide such monitoring. The Microsoft Operations Management (MOM) product provides some good monitoring over the OS; however, you might want to look at other tools that can provide you with more advanced monitoring capabilities over AD and the delegation that you have established over tasks.

When you evaluate your need for monitoring, you will need to consider the following features that some tools, none built-in, provide:

- Real-time monitoring
- Real-time alerting via email, phone calls, or pager messages
- Centralized management and storage of monitored events
- Documentation tracking of what was changed, when it was changed, and who changed it

Auditing

Once the logs have been established and there is a monitoring tool in place, auditing needs to be performed to make sure that nothing is missed. Also, auditing provides a process in which the events that are logged can be reviewed to find trends of security attacks or vulnerabilities. The first step to auditing is to create an audit trail. We have already discussed this step in the logging section earlier.

Employing a centralized tool is very beneficial when it comes to auditing. It can take days to track down the events from all of the domain controllers and servers in the organization. Tools such as EventCombMT from Microsoft can help, but this tool does not provide the efficient interface and query mechanisms that are really needed to ensure that a good audit can be performed on the event logs. Be sure to investigate tools from ScriptLogic, Aelita, NetPro, and BindView to help solve these issues.

Make sure that you also include the delegation audit. This audit includes the reporting of the delegation of administration on OUs and the membership in groups that you need to know in order to provide a good audit on delegation in AD. For these additional control checks, you will need to obtain a tool that allows you to efficiently list and organize ACLs of AD objects. You will then need to quickly access the membership of groups, especially those that were created specifically for delegation. Finally, you will need to audit the service administration default groups, which provide control over AD-related functions.

Delegation Tools

There are plenty of tools that can be used to help develop and report on the delegation of administration for AD and the objects in AD. It cannot be stressed enough how important it is to have the design of the delegation well thought out and implemented first. A poor delegation model is very difficult to administer regardless of the delegation tool.

Although there are plenty of tools that are available to help implement your delegation model in AD, we will explore the Delegation of Control Wizard, which is a free, built-in tool that is part of the Active Directory Users and Computers console. This tool offers many of the standard delegation tasks already configured for you to just click for an easy implementation. However, with many configurations required for a large organization and the need to report on the delegation that is in place, other tools are also needed to ensure successful delegation. The different tools that can be used to delegate administration in AD include:

- Delegation of Control Wizard
- ACL Editor
- Ldp.exe
- Dsacls.exe
- Acldiag.exe
- Dsrevoke.exe

We will discuss each tool and talk about their benefits and weaknesses. I must also stress that this is not an exhaustive list of tools that can be used for delegation of administration in AD. The tools not listed might provide a better solution because they offer GUI-based solutions, which can help with the overall implementation and reporting of the delegation in such a complex environment.

Delegation of Control Wizard

The Delegation of Control Wizard is built-in to the Active Directory Users and Computers console, where most of the administration of AD objects takes place. The wizard is designed to walk you through the decisions to configure the permissions on the objects in AD. Of course, the wizard is also designed to help configure the large number of permissions on objects in AD. The wizard will begin by asking questions about

- User or group to receive the delegation task
- Administrative task to be delegated
- Specific object type and property control (if standard administrative task is not selected)

When the wizard is finished asking questions, it configures the ACL on the object in which the wizard was initiated as well as down through the AD structure following the rules of inheritance that are configured for the objects being affected.

Although I have only mentioned that the Delegation of Control Wizard is available in the Active Directory Users and Computers console, it is also available to configure delegation to objects located in the AD Sites and Services console. In each AD tool, the Delegation of Control Wizard provides a default list of administrative tasks that configure the permissions on the objects automatically. These default administrative tasks differ slightly between Win2K Server and WS2K3 domain controllers, due to the updated list that the WS2K3 domain controllers provide. The following list summarizes the WS2K3 domain controller offerings of default administrative tasks in each AD tool:

Active Directory Users and Computers

- Create, delete, and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete, and manage groups
- Modify the membership of a group
- Generate Resultant Set of Policy (Planning)
- Generate Resultant Set of Policy (Logging)
- Create, delete, and manage inetOrgPerson accounts
- Reset inetOrgPerson passwords and force password change at next logon
- Read all inetOrgPerson information
- Join a computer to the domain (Domain node)
- Manage Group Policy links
- Create, delete, and manage WMI Filters

AD Sites and Services

- Manage Group Policy links

To use the Delegation of Control Wizard to delegate the resetting of passwords on an OU, you would follow these steps:

22. Right-click the OU and select Delegate Control, then click Next.
23. On the Users or Groups page, click Add.
24. On the Select Users, Computers, or Groups page, in the *Enter the object names to select* box, type the name of the user or security group to which you want to delegate tasks.
25. Click OK, then click Next.
26. On the Tasks to Delegate page, select the *Reset user passwords and force password change at next logon* check box.
27. Click Next, then click Finish.

This process will configure the needed permissions on the user accounts in the OU so that the configured users can reset the password and check the box to force the password to be changed when the user logs on again.

If an administrative task is not listed, yet you want to delegate that task to a user or group, you can create a custom task in the wizard. This task can be very daunting because there are literally hundreds of detailed permissions that can be set on any one object in AD. Rather than create a custom task, you can modify the underlying file that configures the default list of administrative tasks. This file, Delegwiz.inf, can be customized to include any set of permissions to make up an administrative task.

> 🕮 For more information about how to complete this customization, refer to the Microsoft article "HOW TO: Customize the Task List in the Delegation Wizard" at http://support.microsoft.com/default.aspx?scid=kb;en-us;308404.

As you can see, the Delegation of Control Wizard is easy to use and extremely efficient. However, there is one flaw with the tool. The tool can only "add" delegation permissions, it can't remove permissions. We will look at other tools—such as ScriptLogic's Active Administrator (AA)—that can report on and remove the delegated permissions if you have configured too much to a user or group.

ACL Editor

The ACL Editor is the rawest tool for establishing the delegation on an object in AD. The editor allows you to view, modify, and add the security configurations of objects in AD, just like you can for files and folders. The Delegation of Control Wizard is a GUI-based tool that performs this same task.

A benefit of the ACL Editor is the additional detailed configurations that can be made to the security description of the object. The permission that controls access to an object is just one of many settings associated with the overall security of an object. You can also configure the following security-related settings by using the ACL Editor:

- Security auditing—The SACL establishes which users or groups will be tracked in the Security Log when accessing the object. Figure 4.1 shows the SACL interface for a typical object in AD. The ability to track access to an AD object is essential to the overall delegation model, because it is the only way to track when a user fails or succeeds at modifying the objects in AD.

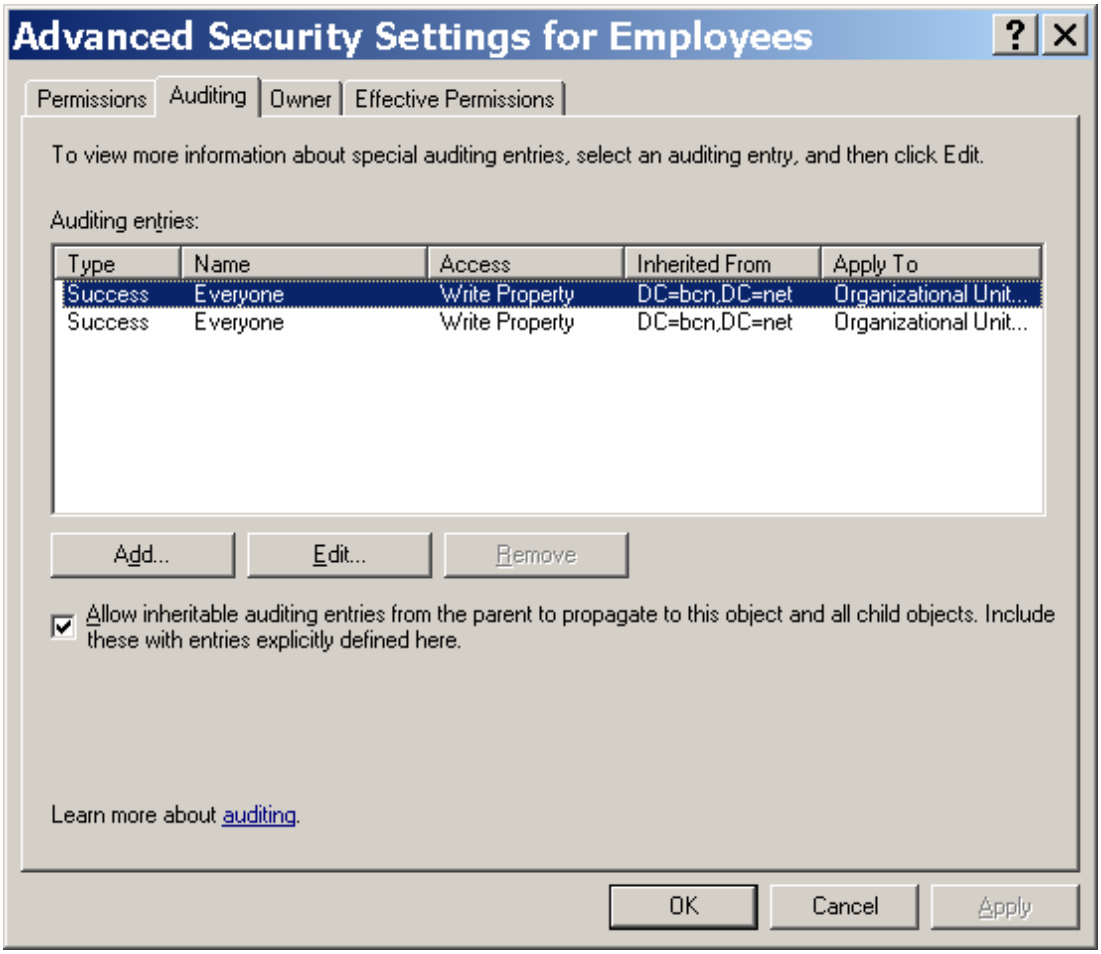

Figure 4.1: SACL settings configure auditing for objects in AD.

- Object ownership—The owner of an object can perform any task on that object. Therefore, the owner of AD objects is a critical part of overall security of that object and other objects that can be affected by the owner of an object. The user or group that creates an object becomes the owner of the object; thus, this configuration might need to be evaluated periodically to ensure that the optimum security configurations for object ownership are maintained over time.

The ACL Editor can be accessed from either the default administrative tools (Active Directory Users and Computers and AD Sites and Services) or from ADSI Edit, which is a GUI-based tool that allows you to see the objects located in AD.

> ADSI Edit is a free tool that comes on the Windows installation CD-ROM. You can find the tool, adsiedit.msc, under the Support Tools directory. Ideally, you will install the entire suite of support tools, which will make the ADSI Edit tool available from the Start menu.

If you are using Active Directory Users and Computers to access the ACL Editor, you might find that it is not available by default. If such is the case, to access the ACL Editor, you will first need to enable the Security tab on the objects that exist in AD. To enable the ACL Editor, click View on the toolbar in the Active Directory Users and Computers console, then select the Advanced Features menu option. The Security tab (which shows the ACL Editor) will be accessible for the objects in AD. To access the ACL Editor, follow these steps, right-click an object in the Active Directory Users and Computers console, select the Properties menu option, then select the Security tab on the Properties sheet for the object you are viewing.

The majority of administrative tasks that you will need to delegate won't show up on the initial Security tab, because the standard permission shown on this tab are more geared toward typical access of the object—not delegation of administration to the object. To access the permissions that relate to the administrative tasks associated with delegation, follow these steps once you are on the Security tab of the object.

28. Click Advanced, then find or create an entry for the user or group to which you are delegating administrative authority.
29. With the correct user or group entry selected, click Edit.
30. Configure the appropriate detailed permissions to allow the desired administrative task to be performed.
31. Click OK on each of the open ACL editor sheets to accept the settings and close the windows.

You will find that the options for configuring delegated administration are almost overwhelming using this method. The following list provides guidelines that will help you configure the delegation more efficiently using the ACL Editor:

- Configure the scope of inheritance on permissions—When you are working with the detailed permissions in the ACL Editor, configure the Apply onto setting, which will narrow the permissions inheritance. There are four main categories that you can choose from:
    - This object only—This setting will stunt the inheritance, only configuring the permission on the object itself
    - This object and all child objects—This setting will set the permissions on the current object and will allow the standard inheritance of permissions to flow down to the child objects located in the object
    - Child objects only—This setting will not set the permissions on the object itself but will affect the child objects located in the object to which the permissions are being set
    - <Specific object class> objects—This setting allows for a very narrow and specific scope of where the permissions will apply; this configuration targets the permissions to only the objects that are configured

- Use a guide—There are too many permissions with too much detailed control to think that you can configure all of the correct permissions without some form of reference. Rely on the work of others to help and guide you through specifying your own permissions. Refer to the Microsoft document Best Practices for Delegating AD Administration at http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3&displaylang=en for detailed listings of permissions for each administrative task.

Ldp.exe

The Ldp.exe tool allows you to access the raw data and objects located in AD. The tool uses the Lightweight Directory Access Protocol (LDAP) operations to view, manage, and create objects in AD. Like the ADSI Edit tool, this tool is part of the Support Tools located on the installation media.

The tool requires you to connect to a domain controller, then bind to the AD database, and finally view the contents of the database. After you have used the tool one time, you will see that it is rather simple. However, first use of the tool can be a bit confusing. Refer to the Microsoft article "Using Ldp.exe to Find Data in the Active Directory" at http://support.microsoft.com/default.aspx?scid=kb;en-us;224543 for all of the steps and details on accessing and modifying objects using Ldp.exe.

Dsacls.exe

Dsacls.exe can take much of the manual labor out of reporting the existing delegation on any object in AD. The other tools that have been reviewed can update and view the existing permissions on any object in AD, but using them to get a complete list of all permissions that are configured on the objects can be very time consuming. Dsacls.exe is a command-line tool that reports and modifies permissions more efficiently than any of the other tools mentioned. This tool is also available from the Support Tools on the installation media.

Acldiag.exe

Acldiag.exe is another command-line utility that reports on the permissions of AD objects, helping track the delegation that has been configured on the objects. Acldiag.exe will also delineate between inherited and explicit permissions, helping track where delegation might have been configured on individual objects, instead of at higher levels such as OUs or the domain. Acldiag.exe is part of the Support Tools suite, like the other tools mentioned.

Dsrevoke.exe

Dsrevoke.exe is a new tool for Win2K and WS2K3 domain controllers and is designed to work in conjunction with the Delegation of Control Wizard. As we have already discussed, the wizard is not capable of removing any permissions, only adding them to an object. The Dsrevoke.exe tool is a free tool from Microsoft that was designed to remove delegated administrative authority.

Summary

With the complexity of AD administration, you will need to provide other administrators and non-IT professionals with the ability to help manage all of the tasks required to keep AD running. Some tasks are for controlling the core objects in AD and other tasks ensure that the directory is secure, stable, and available. In addition to following the suggested best practices, it is important to remember that delegation needs to be maintained and audited to ensure a secure AD environment.

This guide has walked you through the implementation of security for the information contained in and the resources protected by AD. Although this task is complex, by following the suggested best practices, you can attain and maintain a secure AD environment.