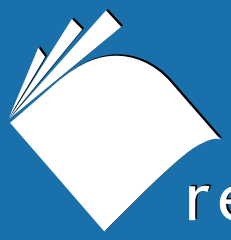

realtimepublishers.com™

The Administrator Shortcut Guide™ To

Active Directory Security

SCRIPTLOGIC

Derek Melber
and Dave Kearns

Copyright Statement

© 2004 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 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.

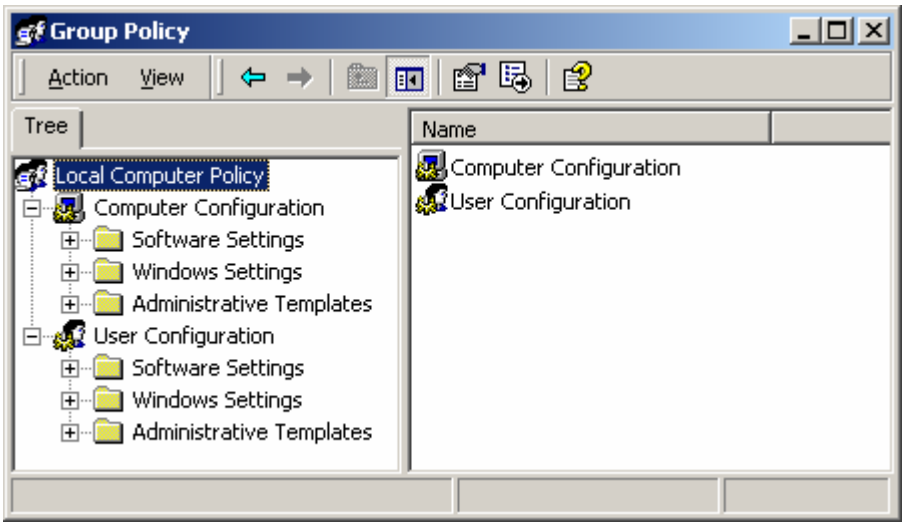

Figure 3.1: The Group Policy Editor showing the format of a typical GPO.

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.

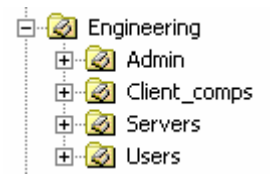

Figure 3.2: OU structure for scenarios.

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.

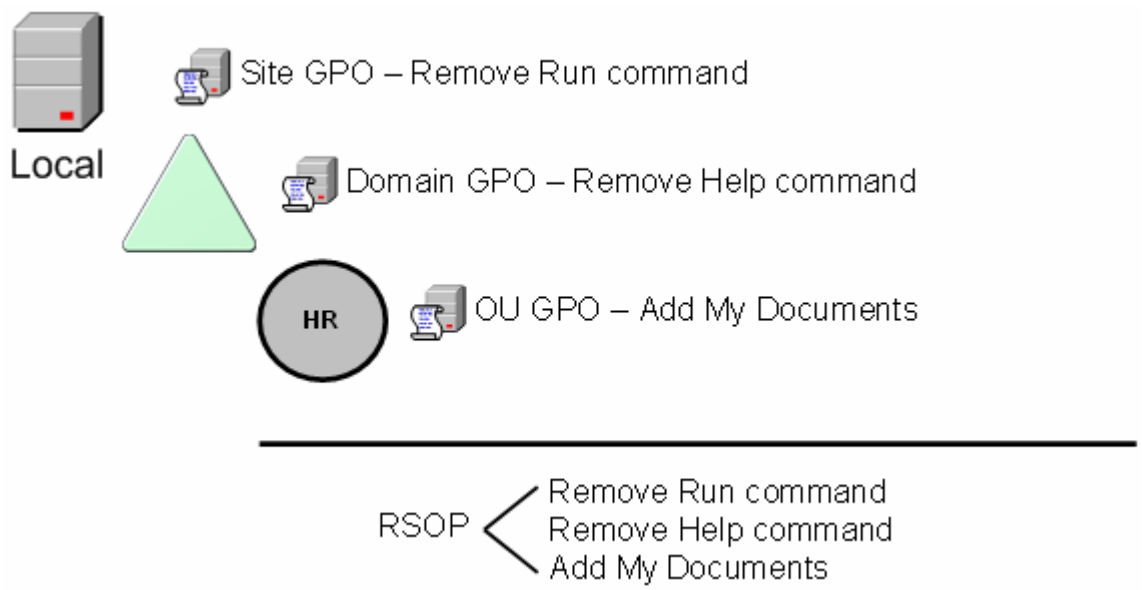

Figure 3.3: GPOs apply in the order of LSDOU; when there are no conflicts, all of the settings apply from each GPO.

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.

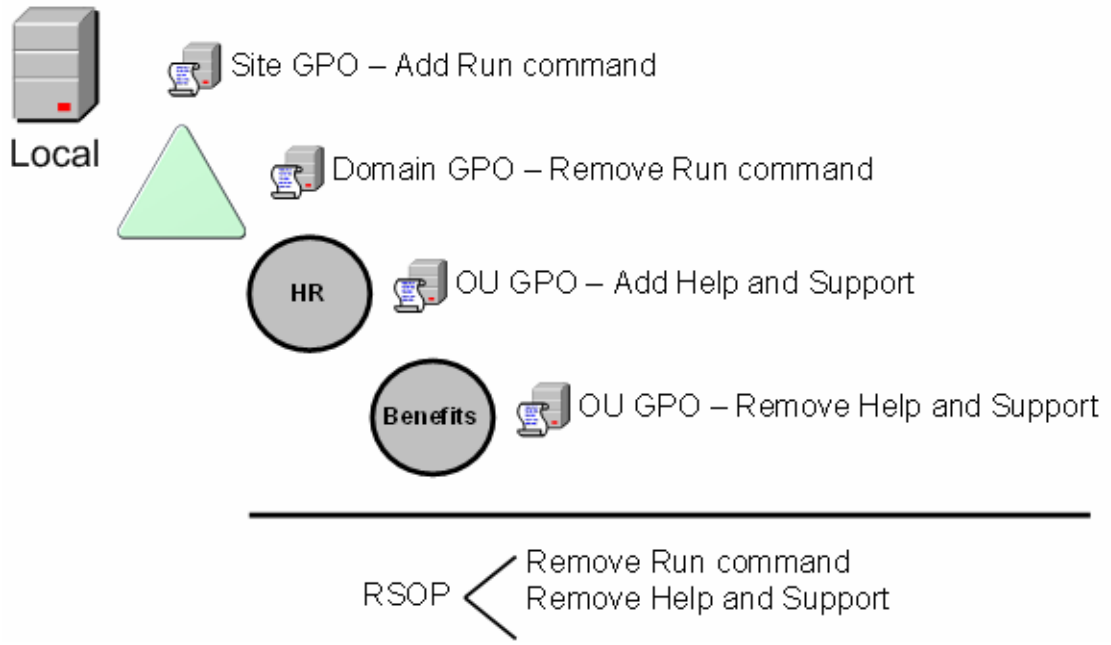

Figure 3.4: When a policy setting in two GPOs conflict, the setting with the highest priority will apply to the object.

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.

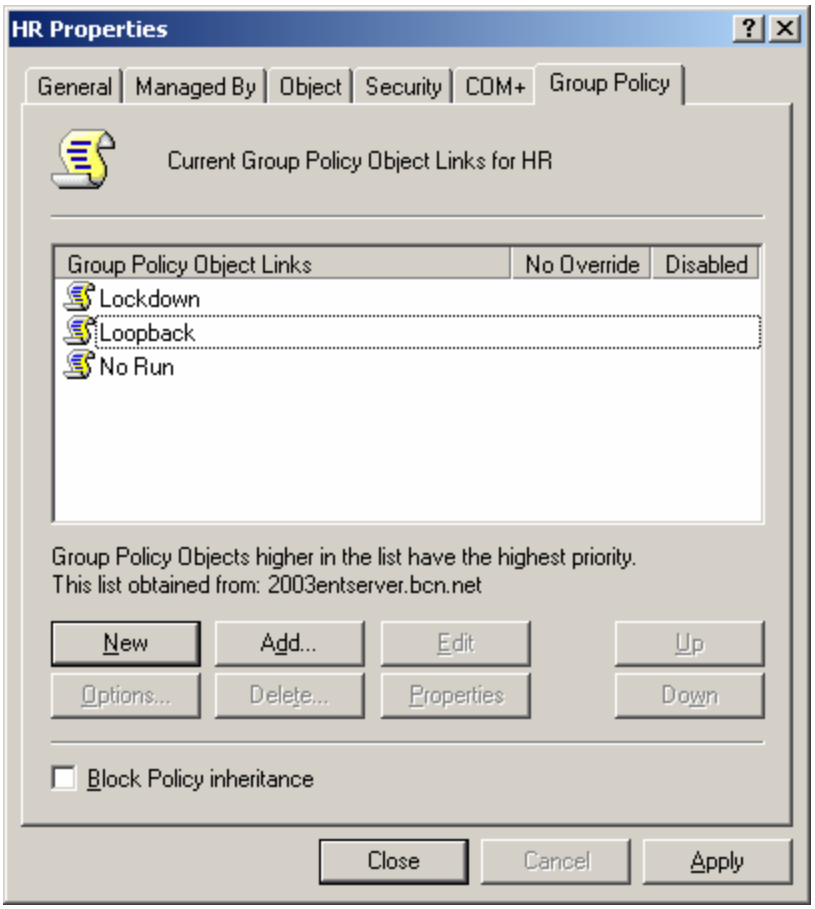

Figure 3.5: Sites, domains, and OUs can have multiple GPOs linked to them.

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.

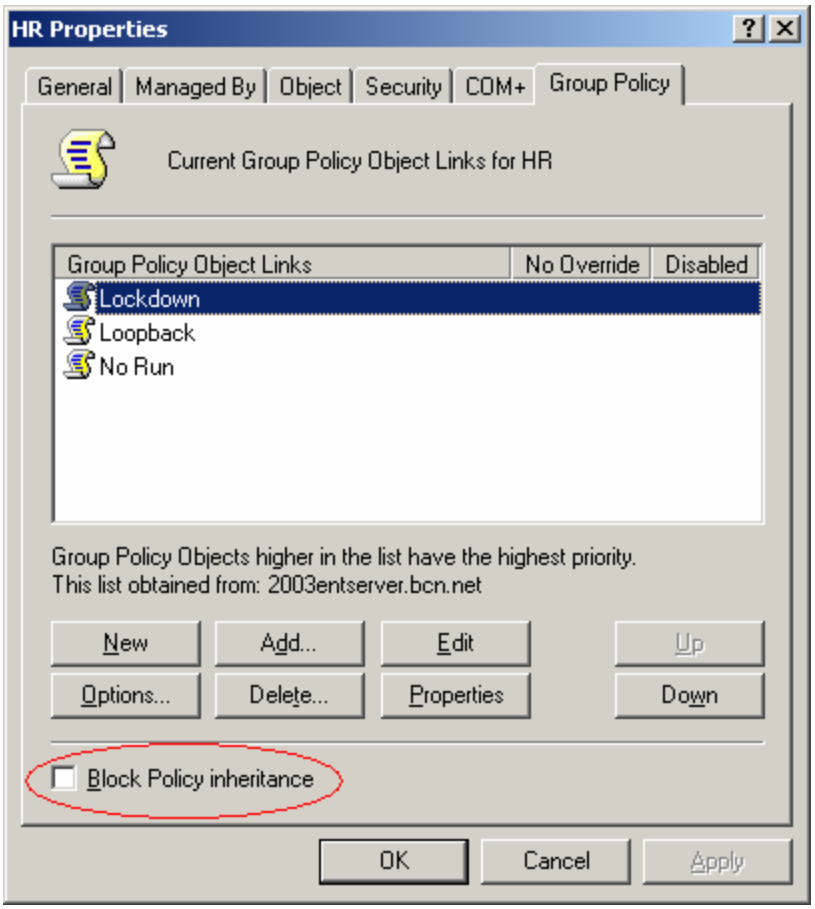

Figure 3.6: The domain and OU levels can block policies from lower in the GPO application order.

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.

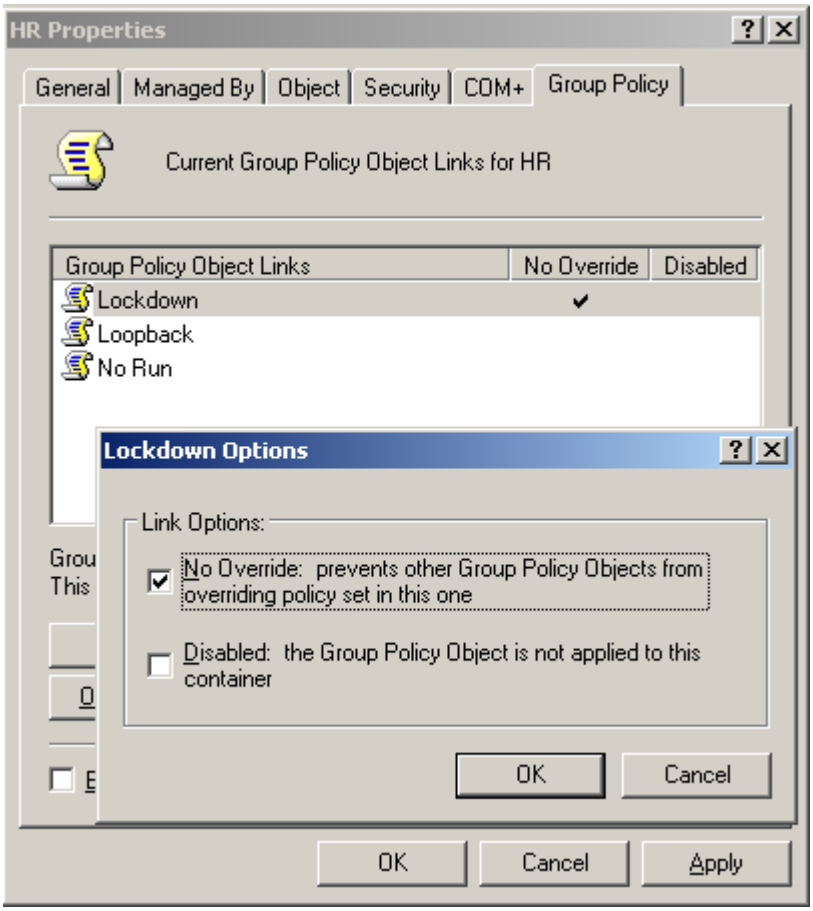

Figure 3.7: The no override setting at the site, domain, or OU takes precedence over the block policy inheritance setting at the domain or OU level.

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:

1. Select the Group Policy tab on the Properties window for the SDOU where the GPO is linked.
2. Select the GPO from the list, and click Properties.
3. Select the WMI Filter tab on the HR Properties window.
4. Select the "This filter" radio button, and click Browse/Manage.
5. Click Advanced on the Manage WMI Filters window, click New, and type a name for the WMI filter into the Name field.
6. 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"
   ```

7. 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.