

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)

Group Policy, my favorite new Windows 2000 (Win2K) feature, gives me something that Windows NT never offered—centralized but granular control over users' desktops. Think of Group Policy as mature NT 4.0 system policies. Specifically, Group Policy Objects (GPOs) are Active Directory (AD)-based objects that let you centrally configure your Win2K desktops and servers. Group Policy functionality encompasses everything from NT 4.0-style desktop lockdown to security configuration to software installation.

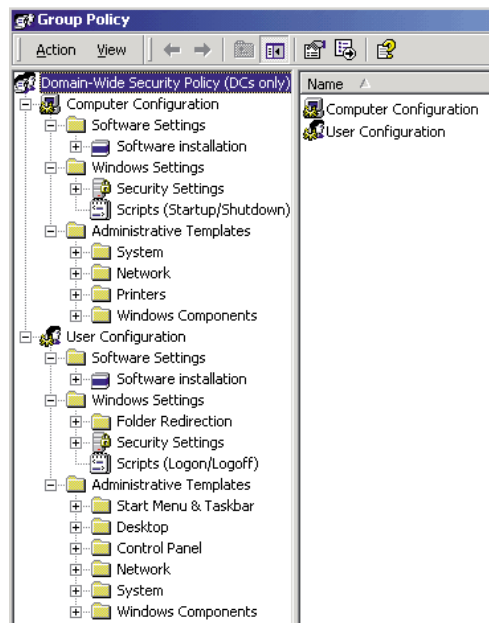
In this article, I show you how Group Policy works, what goes on inside the system, and how to deal with some of the challenges you're likely to face as you prepare to deploy the technology in your Win2K environment. Knowing how NT 4.0 system policies work will help you understand Group Policy's complexities.

What Is Group Policy?

The GPO is the physical policy that you associate with a domain, site, or organizational unit (OU). In NT 4.0, a single system policy file (i.e., ntconfig.pol) contained all the functionality to enforce policy, but that policy was limited to the enforcement of user and computer Registry settings. In Win2K, a physical GPO has both files and AD objects associated with it. With Group Policy, you can specify settings for

- Registry-based policy settings, using NT 4.0-style .adm template files
- Win2K security for local computer, domain, and network settings
- Software installation using the Windows installer, which lets you assign or publish software
- Folder redirection, which lets you redirect certain folders to the network
- Scripts, including computer startup and shutdown and user logon and logoff

You use the Microsoft Management Console (MMC) to manage GPOs. The MMC tool that Screen 1, page 62, shows uses the Group Policy Editor (GPE) snap-in, which is equivalent to poledit.exe in NT 4.0 system policies. Within the GPE snap-in, each node of functionality you see (e.g., Software Settings, Windows Settings, Administrative Templates) is an MMC snap-in extension. Extensions are optional management functionality tools in an MMC snap-in. If you're an application developer, you can extend GPO functionality with custom extensions that provide additional policy control specific to your application.



Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)

Table 1 summarizes the capabilities that GPOs support by default. These capabilities provide the infrastructure that supports much of Win2K's IntelliMirror technology. Only Win2K devices can process Group Policy. NT 4.0 and Windows 9x clients can't see or process GPOs with an AD infrastructure.

TABLE 1: Default GPO Capabilities	
Policy Feature	Function
Computer Configuration (specific to computer objects)	
Software Settings: Software Installation	Provides mechanism for assigning .msi application installation packages that the system applies to computer objects.
Windows Settings: Security Settings	Uses security configuration templates to deliver per-machine security configuration. Machine security settings include account policy, user rights policy, and auditing policy.
Windows Settings: Scripts (Startup/Shutdown)	Lets you define machine-based startup or shutdown scripts, such as simple batch files, executable files, or Windows Scripting Host (WSH) scripts. The script files reside in the GPT.
Administrative Templates	The system defines NT 4.0-style system policy settings here. Machine-specific administrative templates let you control HKEY_LOCAL_MACHINE Registry key settings.
User Configuration (specific to user objects)	
Software Settings: Software installation	Provides mechanism for publishing or assigning .msi and .zap application installation packages that the system applies to user objects.
Windows Settings: Folder Redirection	Provides the ability to redirect common Windows Explorer shell folders such as Desktop, My Documents, and Startup to server-based folders.
Windows Settings: Security Settings	Lets you define IP Security and Public Key policy that the system applies to user objects.
Windows Settings: Remote Installation Service	Lets you define how the Remote Installation Service (RIS) will request information from users using RIS to install Win2K.
Windows Settings: Scripts Logon/Logoff	Lets you define logon and logoff scripts that the system applies to user objects.
Administrative Templates	The system defines NT 4.0-style system policy settings here. User-specific administrative templates let you control HKEY_CURRENT_USER Registry key settings.

Group Policy and AD

To take full advantage of GPOs, you need to have an AD domain infrastructure in place. AD lets you define centralized policy that you can then deploy to all of your Win2K servers and workstations. However, every Win2K computer has a local GPO that you can't centrally manage (i.e., a local GPO resides on the file system of the local computer). Local GPOs let you assign policy on a per-workstation basis for machines that don't participate in an AD domain. For example, for security reasons, you might not want to install a publicly available kiosk machine on an AD domain. With a local GPO, you can modify local policy to provide security and desktop restrictions without the use of AD-based GPOs. To access the local GPO, you have two options. First, you can sit at the machine on which you want to manage the GPO, go to the Start menu, select Run, and type

`gpedit.msc`

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)

This operation is equivalent to using NT 4.0's `poedit.exe` and opening the local Registry. Second, you can edit a local GPO manually from an MMC console by selecting the GPE snap-in and selecting the local or remote computer. You edit a local GPO by focusing on a computer instead of an AD object.

In Win2K beta 3, when you view the local GPO using the GPE, you don't see the actual state of administrative template settings on the machine. If you try to view machine-specific or user-specific administrative template settings, you'll see a Not Configured message. This behavior deviates from that of NT 4.0, in which you can use `poedit.exe` to view the local effective policy.

Local GPOs support all the default extensions except software installation and folder redirection. Therefore, you can't perform these functions using only local GPOs. To get the full benefit of the GPO infrastructure, you need AD.

Multiple GPOs and Inheritance

Within AD, you can define GPOs at three different levels—domain, OU, or site. An OU is a container within an AD domain that lets you delegate administration of objects such as users, groups, and computers. A site is a collection of subnets on your network that high-speed links connect. Sites form replication boundaries for the AD. As Screen 1 shows, the GPO namespace is divided into Computer Configuration and User Configuration options. Only users and computers are subject to GPOs. For example, you can't apply a GPO to a printer object or even to a user group.

If you want to edit a policy on a domain or OU, you have several options. From the Active Directory Users and Computers MMC snap-in, you can right-click a domain or OU, choose Properties, then select the Group Policy tab. To edit site policies, you need to load the Active Directory Sites and Services snap-in and right-click the desired site to get to the GPO. Alternatively, go to the Start menu, select Run, and type

`mmc.exe`

to start the MMC. Choose Console, Add/Remove snap-in, and select the Group Policy snap-in, then select Browse. In the resulting window, you can see all GPOs defined within your AD domain and choose one to edit.

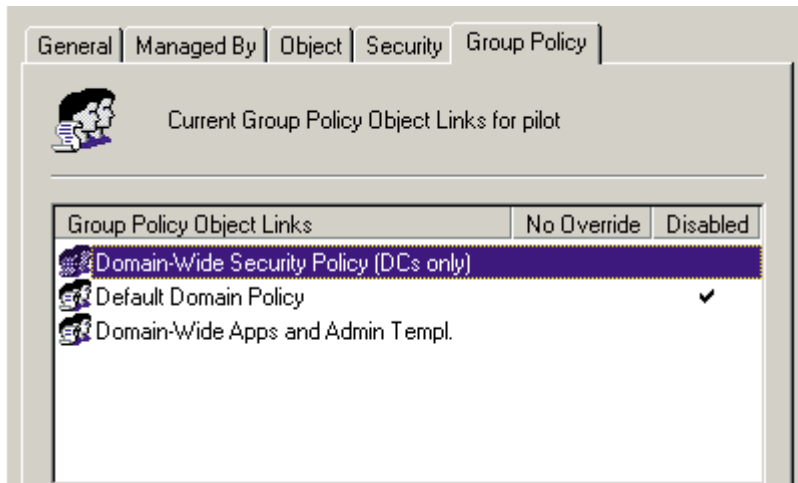
Several GPOs can apply to a user object or a computer object, depending on the GPOs' place in the AD namespace. GPOs are inherited just as other objects and properties in the domain are inherited. Win2K processes GPOs in the following way. First, the OS processes any existing local computer policy. Then, Win2K processes any defined site GPOs, domain-level GPOs, and OU-based GPOs.

Microsoft attaches the acronym LSDOU to this order of precedence (i.e., local, site, domain, then OU). You can define multiple GPOs at any level in this hierarchy. Screen 2 shows a set of three GPOs defined at the domain level within an AD domain called pilot. To view this list, start the Active Directory Users and Computers MMC tool, right-click the pilot domain, select Properties from the Context menu, then select the Group Policy tab. The GPO at the top of the list (i.e., Domain-Wide Security Policy) has the highest priority; therefore, Win2K processes it last. Because you can have GPOs at four different levels within the AD (including the local one) and because you can define any number of GPOs at each level except the local GPO, you'll experience problems if you don't strictly manage your GPOs.

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)



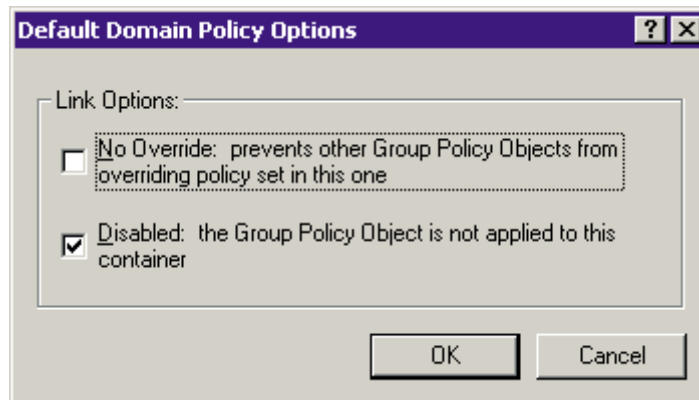
A GPO's inheritance model is significantly different from Novell's Zenworks approach to policy. In Zenworks, if you apply multiple policy packages at different points in the Novell Directory Services (NDS) tree, only the policy package closest to the user object applies. In Win2K, if you define four GPOs at different levels of the AD, the OS processes them using LSDOU, and the result for the user or computer is the accumulation of those four policies. In addition, settings you define in one GPO sometimes cancel out settings you've defined in another GPO. With AD GPOs, you have much more granular delegation of policy control. For example, suppose your company's security department is responsible for defining a security GPO at the domain level that applies to all devices. Using GPOs, you could leave control of software installation at the OU level to the administrator for that OU. In the Zenworks model, you would have to duplicate policy that you want to apply at each level of the tree. Zenworks doesn't require you to think about the effective policy that each user receives as a result of the inheritance of policies from higher in the tree.

To further control GPO application, Microsoft provides three settings to help you limit inheritance complexity. At each container level—site, domain, and OU—you can select a check box to block inheritance from higher-level GPOs. Similarly, on each GPO, you can choose default domain policy options, as Screen 3 shows. To get to this dialog box, start the Active Directory Users and Computers snap-in (or Active Directory Sites and Services if you're modifying a site-specific GPO). Right-click the domain or OU in which the GPO is defined, choose Properties from the context menu, then select the Group Policy tab. Highlight the GPO entry whose behavior you want to modify, and select the Options button. You can select No Override, or you can select Disabled to disable the GPO. When you choose No Override, the GPO will still apply even if you've selected the check box to block inheritance. This option is useful if you have a GPO that you want to apply everywhere (e.g., for domainwide security policy). If an administrator in an OU tries to block the inheritance of your security policy, the security GPO will still apply. The Disabled check box lets you completely disable a GPO. This option is useful when you're editing a GPO and don't want users to process it until you're finished.

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)



GPO Processing and Filtering

Only user and computer objects process Group Policy. At startup and shutdown, a Win2K computer processes policies that you define in the Computer Configuration portion of a GPO. At user logon and logoff, a Win2K user processes policies that you define in the User Configuration portion of a GPO. In fact, you can apply some policies manually within a logon session—for example, you can use the command-line utility `secdit.exe` to trigger security policy application. Additionally, you can use an Administrative Templates policy to define a periodic refresh of user and computer GPO settings. By default, this refresh occurs every 90 minutes. The refresh can significantly slow down a user attempting to tamper with a policy you have defined via Group Policy. However, software installation policy is exempt from the refresh interval. You don't want to periodically refresh a policy change that causes an application to uninstall, especially if someone is using the application. A computer or user processes software installation policy only at startup or user logon, depending on whether the application is machine-specific or user-specific.

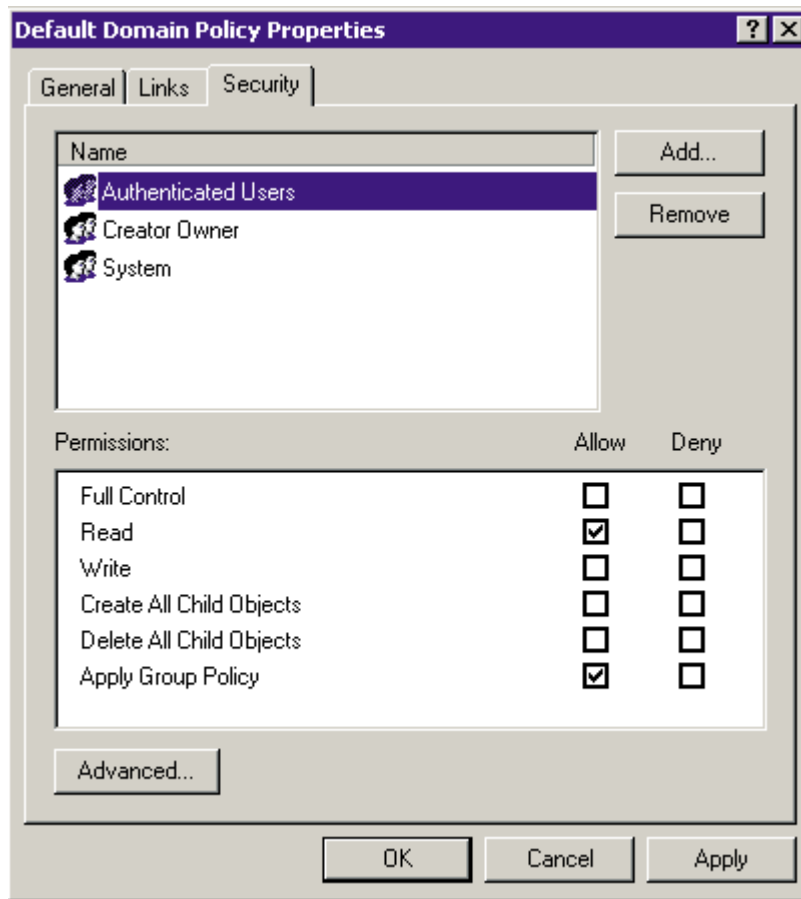
Although only user and computer objects in the AD process GPOs, you can filter the effects of the GPOs. Using Win2K security groups and Apply Group Policy—a new security right in Win2K—you can prevent a particular user group from processing a GPO, as Screen 4 shows. To view the GPO's current security settings, right-click the GPO's name in the MMC, select Properties, then select Security. In Screen 4, the Authenticated Users group has the Apply Group Policy right enabled, which means that all users subject to this GPO will process it. In Win2K, security groups can contain user and computer objects. Therefore, security groups give you fine-grained control over which users and computers will process a given GPO. You can also apply security to individual applications you publish or assign with the Software Installation portion of a GPO. For example, suppose you publish 10 applications in one GPO, which has security that lets all authenticated users process that GPO.

You can specify that only the Finance Users user group can read five of those applications. When other users log on to the domain, they won't see those five applications.

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)



The Guts of a GPO

A GPO has two components—the Group Policy Container (GPC) and the Group Policy Template (GPT). The GPC is the instantiation of a GPO within AD. A 128-bit globally unique ID (GUID) represents the GPC, which resides in a special container called System. Screen 5 shows GPCs in a domain. To view the System container, start the Active Directory Users and Computers snap-in, and select View, Advanced Features from the MMC menu, then drill down under the domain name to System, Policies. The GPT is the manifestation of Group Policy in Win2K's file system. The files associated with a GPO reside in the GPT. For example, the GPT contains

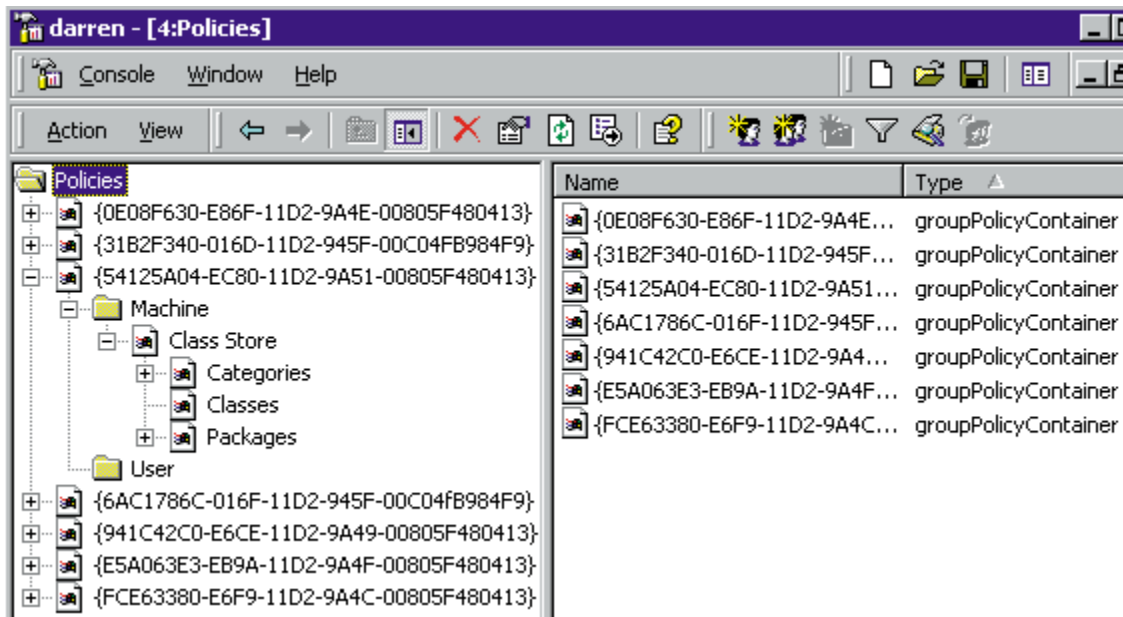
- all .adm files that GPOs' Administrative Templates feature uses
- the registry.pol file, which is Win2K's version of NT 4.0's system policy file
- security templates for some of the Security Settings features
- logon, logoff, startup, and shutdown scripts defined within the GPO

Win2K stores the GPT file structure on domain controllers in the OS's new Sysvol share. Sysvol is a set of folders automatically replicated between Win2K domain controllers using the NT File Replication Service (NTFRS). Sysvol replaces NT 4.0's Netlogon share. To find the GPT file structure on a domain controller, look in `\\%systemroot%\sysvol\sysvol\domain name\policies`.

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)



GPO Challenges

GPOs are rich in features and functionality, but they pose challenges. One major challenge you're likely to face is how to determine an effective policy to apply to users or computers in your domain. This determination is difficult because GPOs can exist at many levels of your AD hierarchy. Also, because you can delegate control of a GPO (e.g., at the OU level), you might not know what someone else has done with a GPO in a container that you have no control over. Therefore, calculating the Resultant Set of Policy (RSoP) that a user or computer object receives is difficult. Although Microsoft won't immediately provide tools to help you calculate RSoP, Full Armor plans to release such a product when Win2K ships. The company already builds tools to help manage NT 4.0 system policies. For Win2K, Full Armor will extend these capabilities to include GPO management, including a feature to help determine RSoP for a given user or computer object.

Another challenge is GPO processing. If you have GPOs at many levels of your AD hierarchy, the system must process the GPOs each time a user logs on or a machine starts up. In Win2K, Microsoft introduces a few features to optimize performance. First, a GPO's version information resides in the workstation and in the GPO. If a GPO doesn't change, the system doesn't process it. Also, on the Properties page in the GPE, you can disable user or computer configuration processing. Suppose you create a GPO to distribute shutdown and startup scripts. The user configuration portion of the GPO is unused; therefore, disabling the user configuration portion prevents the workstation from trying to parse through the GPO and determine whether anything has changed.

Your final challenge arises from the fact that the GPC and GPT are separate entities. Because the GPC is an object in the AD, the GPC replicates on a different schedule than do the files that the GPT contains. This difference means that when you create the GPO, the GPC might have already started to replicate through your AD infrastructure before the GPT has completely replicated all files to all Sysvol shares on all domain controllers.

Compounding the problem, AD uses a multimaster replication model. You could potentially edit a GPO on one domain controller while another administrator edits the same GPO on another domain controller—and cancel out each other's changes. Therefore, when you bring up the GPE, by default you're focused on only the domain controller that serves the PDC role within the Operations Master.

Introducing Group Policy

Darren Mar-Elia

(Reprinted from WindowsItPro Magazine)

(The Operations Master roles are a set of mandatory functions within your AD infrastructure. A server with the PDC role acts as the PDC to downlevel NT and Win9x devices.) This condition limits convergence problems you might experience when administrators edit GPOs from multiple domain controllers. However, grant GPO-editing responsibilities to only a few administrators, and make sure that everyone knows when someone is making a change. Additionally, remember to disable a GPO while you're editing it, then reenable the GPO after your changes propagate throughout your network.

Good News and Bad News

The good news is that GPOs give you flexibility and unprecedented control over your Win2K environment. The bad news is that increased complexity accompanies increased flexibility. How successfully will enterprises leverage this new technology and manage its complexity as more companies adopt Win2K? Stay tuned for answers.