Group Policy Technical Overview

Windows 2000 introduced Group Policy as a rework of NT 4.0 system policies. Group Policy essentially configures and modifies Registry settings (among other things) automatically. Along with user profiles, group policies are used to control the user environment. Group Policy can also be used to deploy software.

Types of Group Policy Settings

Group policy settings are broken down into two categories: computer configuration policies and user configuration policies. Computer configuration policies are enforced based on the computer object and are generally `HKEY_LOCAL_MACHINE` (HKLM) Registry settings. User configuration polices are enforced based on the user account and are generally `HKEY_CURRENT_USER` (HKCU) settings. The general computer configuration categories in Windows Server 2003 are

- **Software Installation**—For deploying software to computers (assigning)
- **Windows Components**—For configuring various computer configuration settings for applications and services
- **Security**—For configuring local security settings
- **Administrative Templates**—For configuring HKLM Registry settings

The general user configuration categories in Windows Server 2003 are

- **Software Installation**—For deploying software to users (assigning or publishing)
- **Windows Components**—For configuring various user configuration settings for applications and services
- **Administrative Templates**—For configuring various HKCU settings

Administrative Templates are special in that in addition to the existing default policies, you can create and install your own administrative templates. Anything that can be configured in HKLM or HKCU can be loaded as an administrative template to apply the Registry keys.

Security Settings (under `Computer Configuration\Windows Settings`) are also special in that they are the only policies that can be imported and exported, at least with the built-in tools.

Tip The Group Policy Management Console that is supposed to be released concurrently with Windows Server 2003 has the capability to import and export group policies.

Group Policy Structure

Group policies are configured in Active Directory and are composed of two components: the Group Policy Template (GPT) and the Group Policy Object (GPO). The Group Policy Template is stored on the `SYSVOL` share on domain controllers and is the actual policy files. It contains the files and configuration settings necessary to implement the updates in the Registry and so on. The Group Policy Object is an object stored in Active Directory that is a reference to the GPT. Because the GPO is an object in Active Directory, it can be linked to various locations to determine where the policy will apply.

Group Policy Processing

Administrators define the scope of a Group Policy by linking it to certain objects in Active Directory. The *scope* determines which objects are affected by the particular Group Policy. Group Policies can be linked to sites, domains, and organizational units (OUs). Any object within the scope of where the object is linked is potentially affected by the Group Policy. For example, by linking a Group Policy at the domain level, all objects (users and computers) in that domain potentially get the settings configured in that Group Policy.

Group Policies are processed in a very specific order. The order in which the polices are processed determines the net effect of all the polices on the computer or user. If multiple policies configure the same setting, the last policy to apply wins. Group policies are processed in the order of local group policy, site, domain, OU. If multiple OUs exist, policies are processed first at the top OUs and then down to the child OUs. So, any group polices applied to the OU in which the object resides gets processed last and thereby wins.

When a Windows 2000 or later machine boots up on the network, it queries Active Directory to determine which policies are applied to the computer account. The polices applied are based on the location of the computer account in Active Directory. For example, if the computer account is in the Sales OU which is in the North America OU in the `braincore.net` domain, it processes all the policies applied to the `braincore.net` domain, the North America OU, and the Sales OU. It then determines the computer configuration settings that are set by these group polices and applies them to the computer. It does all this before you even get the logon screen.

Eventually, a user logs on. When that happens, the system goes through the same process, but this time it processes user configuration policies based on the location of the user account. Once again, they are processed in the order of local, site, domain, OU, OU, OU, and so on.

Controlling Group Policy Behavior

This processing of group policies is pretty powerful. However, you might not always want the policies to process in this way. Fortunately, there are ways to control the Group Policy processing behavior.

First, you can prevent policies linked to higher levels (such as the domain) from propagating to lower levels (such as an OU) by *blocking inheritance*. You can use blocking of inheritance to allow lower-level administrators to control their portions of the Active Directory hierarchy.

However, some policies might exist that you want to apply everywhere no matter what. You can do so by specifying No Override, which causes a policy to be applied even if you're blocking inheritance.

You can further restrict the scope of the application of a Group Policy with filtering. *Filtering* allows you to designate certain types of users or computer within the scope of the policy to apply (or not). A permission called Apply Group Policy is used. Its default is to be allowed to authenticated users, which means the Group Policy applies, thus causing the settings to be effective. By deselecting to allow (or denying) the Allow Group Policy permission, you can prevent the policy from applying to certain users, computers, or groups—even if they fall within the scope of the policy.

Another property of the GPO that can be used to control the application of the settings is to simply disable the policy. The GPO link itself can be completely disabled. Additionally, you can disable each of the two portions of the Group Policy independently (the computer configuration settings or user configuration settings). This can be used for troubleshooting to ensure that a particular policy is being applied. It is also recommended that you disable those portions of the policy that are not being used to speed up processing of the policy. For example, if a policy specifies only computer configuration settings, you can disable the user configuration section.

The final method for controlling the behavior of Group Policy is by configuring the following Group Policy settings:

- **Loopback processing**—Causes the user configuration settings to be applied from the policies applying to the computer account. (Remember, ordinarily only the computer configuration settings are applied from the computer account GPOs and user configuration settings are applied from the user account GPOs.) The two options with Loopback processing are Merge and Replace. Merge applies user configuration settings from both the user and computer GPOs (the computer's GPO settings would win a conflict). Replace applies the user configuration settings from computer account GPOs and ignores the user configuration settings from the user account GPOs.
- **Slow WAN link detection and behavior**—You can use Group Policy to specify what a slow WAN link is (56K, 128K, and so on). Additionally, other policies can determine what to do or not do over slow WAN links—for example, whether to process roaming profiles.

Group Policy provides a powerful, centralized way to consistently apply a variety of configuration settings to users and computers throughout a domain. In fact, because Group Policy is so powerful and flexible, it requires a great deal of planning to properly implement. Windows Server 2003 includes a new feature called Resultant Set of Policies (RSOP), which can help in planning Group Policy deployment. RSOP is discussed in Chapter 5, "Active Directory."