Name :erfan ahmad beigi

Master:mr.milad nourian nasab

Subject: What are the components of Group Policy?

**Local Group Policy**

First, without an [Active Directory](https://blog.netwrix.com/2017/04/20/tutorial-learn-the-basics-of-active-directory/), there’s one Group Policy available — Local Group Policy — which affects only the workstation it is on. Local Group Policy requires you to perform desktop management in a decentralized way, by going to each machine individually. Therefore, Local Group Policy is belst used when Active Directory isn’t available, such as when you have machines that aren’t connected to a Windows domain.

The most expeditious way to edit the Local Group Policy on a machine is to click the “Start” button and run the command “GPEDIT.MSC” to start the Local Computer Policy Editor. Local Group Policy supports multiple local GPOs (MLGPOs), which enables you to decide which users get what options at the local level; for example, you can assign regular users one set of settings and administrators another set, or you can give one specific user a particular combination of settings.

Local Group Policy is stored in the “%windir%\system32\grouppolicy directory (usually, C:\windows\system32\grouppolicy). Each policy you create gets its own folder, named with the security ID (SID) of the corresponding user object.

## Group Policy in Active Directory

The other strategy is centralized Group Policy administration, which works only in conjunction with Active Directory on. You can think of an Active Directory network as having four constituent and distinct levels that relate to Group Policy:

* The local computer
* The site
* The domain
* The organizational unit (OU)

In Active Directory, each server and workstation must be a member of one (and only one) domain and be located in one (and only one) site. In Windows NT, additional domains were often created to partition administrative responsibility (like an ESAE forest architecture) or to rein in needless chatter between domain controllers. With Active Directory, administrative responsibility can be delegated using OUs, and the problem with needless domain bandwidth chatter has been brought under control with the addition of Active Directory sites, which are concentrations of IP (Internet Protocol) subnets with fast connectivity. There is no longer any need to correlate domains with network bandwidth — that’s what sites are for!

## Managing Group Policy

Administrators can manage Group Policy using the [Group Policy Management](https://blog.netwrix.com/2019/04/18/group-policy-management/) Console (GPMC). The GPMC wasn’t part of Microsoft Windows 2000, Windows Server 2003 and Windows XP, you had to download it separately. However, it has been part of every Windows Server operating system since Window Server 2008, so no extra effort is required to access it nowadays.

The GPMC was created to help administrators by providing a one-stop shop for all Group Policy management functions and a Group Policy–centric view of the lay of the land. GPMC does a great job of aligning the user interface of Group Policy with what’s going on under the hood. It consists of a Microsoft Management Console (MMC) snap-in and a set of programmable interfaces for managing Group Policy. The GPMC scripting interface allows just about any GPO operation. The older GPMC that works on XP and 2003 server has a way to script using VBScript. The newer GPMC can use VBScript or PowerShell.

## Group Policy Objects (GPOs)

A Group Policy object (GPO) is a collection of [Group Policy setting](https://blog.netwrix.com/2019/05/07/6-group-policy-settings-you-need-to-get-right/)s that define what a system will look like and how it will behave for a defined group of users. Every GPO contains two parts, or nodes: a user configuration and a computer configuration.

The first level under both the User and the Computer nodes contains Software Settings, Windows Settings and Administrative Templates. If we dive down into the Administrative Templates of the Computer node, we discover Windows Components, System, Network and Printers. Likewise, if we dive down into the Administrative Templates of the User node, we see some of the same folders plus some additional ones, such as Shared Folders, Desktop, Start Menu and Taskbar.

The Computer node contains policy settings that are relevant only for computers. That is, if a GPO that contains Computer settings “hits” a computer, those settings will take effect. These Computer settings could be startup scripts, shutdown scripts, and setting that control how the local firewall should be configured. Every setting is relevant to the computer itself, no matter who is logged on at a given moment.

The User node contains policy settings that are relevant only for users. Again, if a GPO contains User settings “hits” a user, those settings will take effect for that user. User settings make sense only on a per-user basis, like logon scripts, logoff scripts and availability of the Control Panel. Think of this as every setting relevant to the currently logged-on user; these settings follow the user to every machine they use.

### Creating and Linking GPOs

When Group Policy is created at the local level, everyone who uses that machine is affected. However, once you [step up and use Active Directory](https://www.netwrix.com/what_is_active_directory_ebook.html?itm_source=blog&itm_medium=context&itm_campaign=group-policy&itm_content=none&cID=70170000000kgEZ), you can have nearly limitless Group Policy objects, with the ability to selectively decide which users and computers will get which settings. Actually, you can have only 999 GPOs applied and affecting a user or a computer before the system gives up and won’t apply any more.

When we create a GPO, two things happen: We create some brand-new entries within Active Directory, and we automatically create some brand-new files on our domain controllers. Collectively, these items make up one GPO.

Creating a GPO merely makes it available, or ready to be used within the domain where it was created. To apply a GPO’s settings, you link it to one or more sites, domains or OUs:

* If a GPO is linked at the site level, its settings affect all user accounts and computer accounts in that specific site, no matter which domain or OU a given account is in. This is based on the IP subnet the users computer is a part of and is configured using Active Directory Sites and Services.
* If a GPO is linked at the domain level, it affects all users and computers in the domain, across all OUs beneath it.
* If a GPO is linked at the OU level, it affects all users or computers in that OU and all OUs beneath it (which are called child OUs or sub-OUs).

When you tell the system: “I want a new GPO to affect this OU.” The system automatically creates the GPO in the fixed location, and then associates that GPO with the level at which you want this GPO apply its settings, OU in our example. That association is called linking. In Active Directory, multiple levels can be linked to a specific GPO. Thus, any level in Active Directory can leverage multiple GPOs, which are standing by in the domain ready to be used. Remember, though, unless a GPO is specifically linked to a site, a domain, or an OU, it does not take any effect.

Giving inheritance of settings from higher levels to lower levels, you might wonder what happens if two policy settings conflict. Perhaps a policy at the domain level specifies one setting but another policy at the OU level species reverse. The result is simple: Policy settings further down the food chain take precedence. In our example, the OU-level setting would trump the domain-level setting. This might seem counterintuitive at first, but just remember that the golden rule with Group Policy is “last writer wins.” Read [Group Policy best practices](https://www.netwrix.com/group_policy_best_practices.html?itm_source=blog&itm_medium=context&itm_campaign=group-policy&itm_content=none&cID=70170000000kgEZ) to learn more about how to organize your Group Policy for maximum clarity and effectiveness.

If you want to link one GPO to more than one domain, you must do one of the following:

* Create exactly the same GPO in each domain using the GPMC.
* Create the GPO in one domain and copy it to the other domains using either the using the GPMC or a third-party tool.
* Use cross-domain policy linking. However, this is generally recognized to be a bad practice.

### Group Policy Preferences

Group Policy Preferences (GPPrefs) are a relatively old part of the Group Policy world but a lot of admins still don’t use them in their infrastructure; some don’t even know that they exist. GPPrefs are an extension or node that extends Group Policy’s reach and capabilities. They are not policies; they are advanced settings administrators can deliver. However, they must be fully understood and used with caution so you don’t accidentally shoot yourself in the foot.

Group Policy Preferences are located in the updated GPMC. You’ll need to either use Windows Server 2008 and higher or install the RSAT tools on an earlier Windows system, and then navigate to “Computer Configuration ->Preferences”. The new Preferences node has 21 new categories you can apply. The node is split into Windows Settings and Control Panel Settings, as detailed below.

#### Control Panel Settings

Here are the extensions in the Control Panel node:

* **Data Sources**— Lets you set connections to Open Database Connectivity (ODBC) data sources via Group Policy.
* **Devices**— Enables you to disable a single device or device class.
* **Folder Options** — Lets you associate a file extension with a particular class.
* **Local Users and Groups**— Enables you to add or remove users from groups, change users’ passwords, lock out accounts, and set password expirations.
* **Network Options**— Allows you to configure the following connection types:
* Virtual private network (VPN) connections
* Dial-up networking (DUN) connections
* **Power Options**— Allows you to manage Power settings. You can set things like the hard disk spin downtime or how long until the monitor goes into standby mode.
* **Printers**— Allows you to manage shared printers.
* **Scheduled Tasks**— Enables you to set scheduled tasks.
* **Services**— Enables you to manage just about every aspect of a client computer’s services. This is especially useful if the target is a server machine and you have one service that’s running on multiple machines but you haven’t gotten around to changing the service account.
* **Internet Settings**— Lets you specify Internet Explorer settings.
* **Regional Options**— Enables you to change local settings depending on who the user is.
* **Start Menu**— Provides a very easy way to make changes to the Start menu.