

Re: Question for Roger Abell

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-12/msg00426.html

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Thu, 28 Dec 2006 18:13:28 -0700
-

<void.no.spam.com@xxxxxxxx> wrote in message
<news:1167338188.100896.303520@xx>

Roger Abell [MVP] wrote:

Hey void,

I am not sure what prior threads you found, but it sounds as if it may have been one about how to imprint the same local policy on multiple stand-alone machines. Notice that "local security policy" only shows some of what gpedit can set (notably the adm templates and software restriction policy). Templates cover the security policy and some other things not available otherwise on a stand-alone (filesystem, services, reg, etc.)

I notice that my Local Security Policy contains Account Policies, Local Policies, Public Key Policies, and IP Security Policies on Local Machine. The security template only contains Account Policies (which includes a Kerberos Policy that the Local Security Policy does not have) and Local Policies, as well as Event Log, Restricted Groups, System Services, Registry, and File System. So the template doesn't save the Public Key Policies or IP Security Policies on Local Machine, although I don't think I'll change those, so it isn't a big deal.

If you just want to safeguard for rebuild, as you state, just keeping a copy of %windir%\system32\GroupPolicy can get you there.

It looks like that directory saves everything that I can change in gpedit.msc except for the Windows Settings > Security Settings (Account Policies, Local Policies, Public Key Policies, and IP Security Policies on Local Machine). So if I back up that directory and also use a security template for the things that aren't saved in the directory, then that will cover everything in gpedit.msc (except for the few things I mentioned earlier).

Re: Question for Roger Abell

So if I were to reinstall Windows, all I would need to do is restore the backup of my c:\winnt\system32\GroupPolicy directory, and then use the Security Configuration and Analysis snap-in to apply the security template I had saved?

Else, notice the adm folder within that location, where you could set different default values for the involved settings in the adm files and copy those in used in conjunction with a template for the security policy (this I like as it allows me to control some filesystem and services changes).

For SAFER (software restriction), as far as I know there is no good way in XP to copy just those definitions. One can just take the involved registry settings and import them into the reg of another machine, and they will be effective, but they will not show in the local policy of that system.

I'm not familiar with SAFER, and I'm running Windows 2000. Is that something I need to worry about?

Thank you Roger.

No problem.

SAFER is not in Windows 2000.

Kerberos does not exist in use on a stand-alone, it is used only with a domain environment.

The directory saves more than you indicated (the .pol files), and unless you are using some items, like registry, or filesystem sections, there is no real need to apply the template after a copy of the saved directory content in on the new system; but, you are correct that use of the template would make more clear that you do get what you want for settings other than Local Policy that a template covers. Keep in mind that applying a template is a one-time event, that is, it sets things as such but it does not enforce their remaining that way for these other sections.

IPsec policy and SAFER are late additions and are handled, well, rather uniquely. If you had XP or later you could use the ipsec context in the netsh command to save and restore IPsec definitions. There is (or was) a download for Windows 2000 for commandline configuration of IPsec ruleset (ipsecpol if I remember rightly) but there were issues with its use (one had to either use it exclusively

Re: Question for Roger Abell

or use the user interface exclusively).

.