

# Re: Basic Sec Template Design

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-11/msg00078.html>

---

- *From:* "Roger Abell [MVP]" <[mvpNoSpam@xxxxxxx](mailto:mvpNoSpam@xxxxxxx)>
  - *Date:* Thu, 9 Nov 2006 15:54:43 -0700
- 

Hi Adrian,

Sorry it took a couple days for me to revisit here.  
I attempt to comment inlined with your comments

--

Roger

"Adrian" <[Adrian@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Adrian@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:48D97964-32BE-414A-A2C9-C5A296621BE0@xxxxxxxxxxxxxxxxxxxx](mailto:news:48D97964-32BE-414A-A2C9-C5A296621BE0@xxxxxxxxxxxxxxxxxxxx)

I take it you mean upgrading of servers in place to W2k3, either with  
upgrades or (to me preferred) fresh builds, rather than moving domain to  
domain.

Yes we have to upgrade the servers in place, Im a fan of fresh installs  
but  
have been over ruled on this call.

'tis the life, no?

- All that you mention is
- 1) not changed W2k to W2k3
  - 2) defined in a GPO linked to the domain object to impact domain accounts
  - 3) effective over machine local accounts if a GPO sets these for OUs that hold machines
  - 4) effective for all accounts equally

Im not quite sure I understand.

## Re: Basic Sec Template Design

You were saying you wanted to define password policies, length, complexity, etc.

So I commented that these are not different for W2k vs W2k3 and that when set

in a GPO linked to the domain these affect domain accounts, and if set in GPOs

allowed to impact machines then these (also) impact the machine local accounts,

and finally, that these affect all accounts where they have any effect.

Ex. If set in a GPO linked to the domain then these affect domain accounts, and

if there is no OU linked GPO with these set differently, then machines in the OU

will also see these and have them impact the machine local accounts, whereas if there were a GPO with them set differently linked to the OU then those would

be effective.

servers will be migrated 1 at a time to Win 2003 I cant create a domain policy for the Win 2003 servers

I do not see the reasoning for this. Why not?

Is it possible to have different domain policies? One for the 2000 network and

one for the new 2003 network? If so I didnt realise I thought a domain policy

applied to all in the domain, I didnt know you could specify at the domain level which OS's it applies too.

No. Windows 2000 does not obey WMI filtering. Otherwise, for XP and above a WMI query could be used to detect OS version and control application of a GPO to only specific versions (but all W2k would try to apply the GPO's settings).

My point was, however, that I could see no reason whatsoever as to why you were seeing a need to make a policy apply just to W2k3 servers because, as you said, the servers would be migrated 1 by 1. I could not, and still do not, see what that has to do with it.

If your settings are in a domain linked GPO they are getting applied to all, at

least unless a more specific GPO alters them. They would apply to the W2k and to the W2k3 as soon as it is upgraded. If you wanted some settings to

## Re: Basic Sec Template Design

only apply to the W2k3 then place these in an OU with a GPO linked to it that carries settings only machines in that OU should be getting.

It is good you have familiarized yourself with the SCW.  
Have you also reviewed the security guides ?  
<http://go.microsoft.com/fwlink/?linkid=14845>  
<http://go.microsoft.com/fwlink/?linkid=15159>  
<http://www.microsoft.com/technet/security/guidance>

Thanks for the links Ill give them some time today and do some more reading up.

I am afraid they take a bit more than a day, at least for me.

It is better to import templates into GPOs, and control there application in the normal way via GPO hierarchy. Note that the templates in the guides are suggested settings and should be fully evaluated relative to specifics of a deployment.

So if can just spell this out for my own understanding. Say I get a Brand New 2003 server straight out of the box, can I just place that in the 2003 Server OU under in my 2000 domain. I then would apply the security template to that OU rather than to each server. SO I wouldn't have to any work in theory on the actual server (Apart from placing it in the OU).

Just place it into your W2k3 OU and have your security template imported into a GPO that is linked to that OU. Then, whatever can be done via GPO will be done as soon as that machine is rebooted or forced to refresh policy.

We are perhaps mixing words. You say security template. I say GPO, and use security template to be an inf file such as managed by the Security Config and Analysis MMC snapin. A security template can only set a portion of the possible settings of a GPO, can be imported into a GPO, etc. A security template can be applied to a machine (directly, with the previously mentioned

## Re: Basic Sec Template Design

snapiin or with secedit), or once imported into a GPO can be applied (and on need reapplied) to sets of machines that are in the scope of the GPO's application.

I prefer central control via AD base GPO.

Should I really be looking at creating policys in the following order.

1 Create a Domain Policy just for 2003 Servers, which would contain all the settings normally found under Local Security Policy, password, Audit etc

Depends.

If domain linked the account policies of this will impact domain account That is not at all related to what kinds of OS versions are involved.

If domain linked and not overwritten by OU linked GPO, then those settings would also apply to the machines in the OUs.

Account policies are unique in these regards, and in being all or none (you cannot set some accounts differently).

For most policies other than Account policies you normally set those at the highest level in the domain/OU hierarchy that makes sense based on what you want to be impacted with those settings.

It is beginning to sound liike your scenario is, that you do not want to affect

anything on the W2k that are waiting to be upgraded, but you want to control via GPO as much as possible on the machines as soon as they are W2k3.

In that case, I would not alter any Domain linked GPOs, but use a (perhaps temporary) W2k3 OU and make use of GPO linked to that, with the machines moved into the W2k3 OU as soon as they are upgraded and stable.

2 Then create separete policys for each "Child OU" of the "Server 2003 OU" for instance "Print Server OU", "ISA Server OU", "Web Server OU" which would

allow me to have diiferent policys for each Server role

That is a possibility. One also sees security group filtering used (ie. all machines

in one OU and some GPOs targetted to specific machines by use of a security group that has as members the computer accounts of the machines to be affected.

THanks for you help so far btw

Re: Basic Sec Template Design