(2011-10-23) Best Practices For The Default Domain Policy And The Default Domain Controllers Policy GPOs

Posted by Jorge on 2011-10-23

i
1 Vote

Every AD domain since Windows 2000 Server implements two default GPOs being the "Default Domain Policy" GPO and the "Default Domain Controllers Policy" GPO.

–

With regards to the domain related GPOs the following are best practices:

- Create a separate "Custom Domain Policy" GPO and link that also to the AD domain to be applied after the Default Domain Policy.
- Use the "Custom Domain Policy" GPO for all non-default settings you require to use, except for the password policy and account lockout policy settings

- For the password policy and account lockout policy settings still use the “Default Domain Policy” GPO. The reason for that is described in “(2010-09-27) Password Policies And Account Lockout Policies Within An AD Domain (Part 1)” and in “(2010-09-27) Password Policies And Account Lockout Policies Within An AD Domain (Part 2)”

–

With regards to the domain controllers related GPOs the following are best practices:

- Create a separate “Custom Domain Controllers Policy” GPO and link that also to the domain controllers OU to be applied after the Default Domain Policy.
- Use the “Custom Domain Controllers Policy” GPO for all non-default settings you require to use, except for the user rights settings.
- For the user rights settings still use the “Default Domain Controllers Policy” GPO OR you need to duplicate all user rights from the “Default Domain Controllers Policy” GPO into the “Custom Domain Controllers Policy” GPO. However, when installing applications with Domain Admin or Enterprise Admin equivalent permissions, some of those applications may automatically edit the “Default Domain Controllers Policy” GPO with regards to the user rights without any interaction. It is therefore better to still configure all user rights for domain controllers in the “Default Domain Controllers Policy” GPO. Because of this reason it is pointless to manage user rights settings in a “Custom Domain Controllers Policy” GPO.
- You may need to create an additional GPO that only targets Branch Office DCs through group filtering or WMI filtering so that Branch Office DCs do not register domain-wide SRV records
- You need to create an additional GPO that only targets the DC currently hosting the PDC FSMO role and any candidate DC to host the PDC FSMO role through WMI filtering. You can read more about that in “(2010-09-26) Configuring And Managing The Windows Time Service (Part 1)”, “(2010-09-26) Configuring And Managing The Windows Time Service (Part 2)”, “(2010-09-26) Configuring And Managing The Windows Time Service (Part 3)” and “(2010-09-26) Configuring And Managing The Windows Time Service (Part 4)”.

–

Cheers,
Jorge
———————————————————————————
* This posting is provided "AS IS" with no warranties and confers no rights!
* Always evaluate/test yourself before using/implementing this!
* DISCLAIMER: https://jorgequestforknowledge.wordpress.com/disclaimer/
———————————————————————————
############### **Jorge’s Quest For Knowledge** #############
######### http://JorgeQuestForKnowledge.wordpress.com/ ########
———————————————————————————