

## Re: Active Directory / Policies questions

**Source:**

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2005-01/0224.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-01/0224.html)

---

**From:** Nicolas Heyer (*NicolasHeyer\_at\_discussions.microsoft.com*)

**Date:** 01/05/05

Date: Wed, 5 Jan 2005 04:37:07 -0800

First of all tanks for your reply.

Question 1: I will check the rights. Q251335 does not mention so many rights to be defined...

For the local admin problem, when we tried to install something it stated we need administrative rights to do so.

For question 3 concerning the domain name used when entering credentials for joining a computer to a domain, I have some precisions:

- the main site has only Windows 2003 domain controllers
- all the other sites have one Windows 2000 DC server.

The sites have been declared in the Active Directory reflecting their physical location. Each PC is installed with Windows 2000, receives an IP address from its local Windows DC server. Its first DNS server is also the local Windows DC server.

There is (or should not be) no WINS or NetBios though we simply do not need it (no old Windows NT domain, there was also no domain upgrade from NT). So I really see no difference other than the main site using Windows 2003 while the others still run on Windows 2000.

For the last question, I really mean DNS entries for the NIC connexion.

Kind regards  
Nicolas

"Gary Simmons" wrote:

- > *Hi..*
- >
- > *In-line*
- >
- > *Cheerio*
- > *Gary Simmons*

>  
> *gsimmons.uk@gmail.com*  
>  
> *On Wed, 5 Jan 2005 02:21:04 -0800, "Nicolas Heyer" <Nicolas Heyer@discussions.microsoft.com> wrote:*  
>  
> *>Have some questions concerning Active Directory and Policies.*  
> >  
> *>- Right to create/delete computer objects.*  
> *>I set this parameter for the "Authenticated Users" on the "Computer"*  
> *>container in "Active Directory Users and Computers". It seemed to work for a*  
> *>while. Users could join their Windows 2000 computer to the domain when they*  
> *>needed to reinstall their PC. But I realized in the last weeks that I needed*  
> *>to give the user admin rights for this operation because it did no longer*  
> *>work. What is wrong or what should I also check ? Or is that different with*  
> *>Windows 2003 servers ? (my source: Q251335)*  
>  
> *By default upto 10 anon users can add computers to the domain, you*  
> *need to delegate the exact rights to the target container in order to*  
> *permit non-AD admins the ability to add a computer account... With*  
> *these rights in-place you dont need to assign the "Add Computers to*  
> *the domain" in the domain security policy..*  
>  
> *Rights requiried..*  
>  
> *For 2003AD:*  
> *Object Perms:*  
> *Apply Onto: This object and all Child Objects*  
> *Allow Perms: Create Computer*  
>  
> *Properties Perms:*  
> *Apply onto: Computer*  
> *Allow Perms: Read Account Restrictions*  
> *Write Account Restrictions*  
> *Reset Password*  
> *Validated Write to DNS host name*  
> *Validated Write to service principal name*  
>  
>  
>  
> >  
> *>- Domain Users are member of the local Administrator group of each workstation*  
> *>This has been set according the Q320065 Microsoft article that describes how*  
> *>to configure a global group local to be member of the Administrators group of*  
> *>all workstations by using restricted groups configuration in a policy. That*  
> *>works fine for mostly all the computers but we found out that we could not*  
> *>install software on some computers when using a domain user account. We*  
> *>verified on the local workstation that the domain user group was member of*  
> *>the administrator group and it was. So why ?*  
>  
> *What was the error given during the install processes ? Have you set*

> *up object auditing to see where the failures are ?*  
>  
>>  
> >– *xxx.local or xxx domain*  
> >When joining a workstation (and create a WS account) to the domain, we found  
> >out that we had to enter "xxx.local" as the domain name in some locations  
> >(Windows 2003 DC servers) and only "xxx" in other locations (Windows 2000 DC  
> >servers) when entering credentials. Why ?  
>  
> *This is generally a name resolution issue, using the FQDN (xxx.local)*  
> *utilises DNS and the site model in order to locate a DC. This other*  
> *uses WINS and netBIOS.. Where possible always use the DNS method.. If*  
> *this isnt working then check the clients use of DNS to see whether it*  
> *can enumerate the domain (NSLookup etc)*  
>  
>>  
> >– *Are computer/user informations stored somewhere in AD ?*  
> >We have the impression that some informations like DNS entries of a computer  
> >are stored somewhere in AD because when we reinstall the whole PC, these  
> >informations are still available even if the default installation does not  
> >contain such informations (these informations were manually added). We do not  
> >use profiles. How can we explain this ?  
>  
> *Not sure what you mean, do you mean the network adapters DNS*  
> *settings?*  
>>  
> >Thanks for any reply  
> >Nicolas  
>  
>