

microsoft.public.win2000.active_directory: Re: Restricting access to AD located in another domain

Re: Restricting access to AD located in another domain

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-11/0776.html

From: Cary Shultz [A.D. MVP] (cwshultz_at_mvps.org)

Date: 11/12/04

Date: Fri, 12 Nov 2004 09:35:45 -0500

Curtis,

I might rethink this. As Paul states, you should use the Delegation Wizard for your help desk people. I am not so sure that granting the Help Desk group Domain Admins is the best solution. This could be possibly very dangerous. The Delegation method will allow you to give them only what they need.

If they need to be members of the local Administrators on all of the WIN2000 + workstations then take a look at Restrictive Groups. Out of the box, this will purge the current members of the local Administrators group on all of the workstations (or whatever computer account objects you place in the OU to which you link this policy) so you might want to add two groups: the HelpDesk security group and the Domain Admins. If you do not want to do that (suffer from the 'purging membership' then take a look at the following MSKB Article:

<http://support.microsoft.com/?id=810076>

You will need to call MS-PSS (but will not be charged) and make sure that you get both the WIN2000 and the WIN XP patches. These will be e-mailed to you in zipped format (with a password), so make sure that you have WinZip available (as well as giving them a valid e-mail address). Apply the appropriate patch to all of your systems (even your Domain Controllers). Now, this GPO will simply 'add to' the current membership of the local Administrators group on all of the systems that fall under the SOM of this policy.

HTH,

Cary

"Curtis Fray" <curtis.fray@Xbssmail.nhs.uk> wrote in message news:uUQOxVByEHA.3120@TK2MSFTNGP12.phx.gbl...
> *Hi,*

Re: Restricting access to AD located in another domain

microsoft.public.win2000.active_directory: Re: Restricting access to AD located in another domain

>
> *I have two domains (DOM1 and DOM2). At the moment the Helpdesk staff have*
> *Domain Admin rights on DOM1. DOM2 is brand new and just being configured*
> *at*
> *the moment. I would rather not give them Domain Admin rights on this and*
> *just let them do everything they need using Group Policy. I currently log*
> *on*
> *to DOM1 and I've set up a trust between the two domains so I am able to*
> *use*
> *my AD Users and Computers mmc to access AD on DOM2.*
>
> *Do begin with I'd like to set this up so Helpdesk accessing DOM2's AD from*
> *DOM1 can only see one container I've set up called NewUsers. Is there*
> *anyway*
> *to restrict their view to exactly what I want, rather than being able to*
> *see*
> *everything?*
>
> *If you need any further info, or anything clarified please let me know.*
>
> *Thanks,*
>
> *Curtis.*
>
> =====
> *When replying by email please remove the X*
> =====
>
>