

RE: Delegation of duties to junior administrator

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-05/msg01449

- *From:* Richard Crandall <RichardCrandall@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 19 May 2006 16:35:02 -0700
-

As AD delegation goes Sanjay Tandon wrote an excellent whitepaper on this a few years back. This will help you to be able to customize the delegation wizard that Hutch mentioned and get some very good use out of it. You should know that you can manually edit the delegwiz.inf file from any machine that you use to launch the delegation wizard in ADUC. This file will allow you to define templates for use in this wizard. As you can imagine there are several approaches for how to build these templates including templates by group (help desk, tier I, tier II, etc) or templates by functional task (computer maintenance, user maintenance, etc), etc. Read through the whitepaper and use the appendix to build your own template and you will find that delegation is much more robust than it is out of the box. If you have any questions after reading those two docs and playing with the delegwiz a bit let me know and I will be glad to help out. One additional word of caution, as you are learning to use delegation and you are working out your delegation architecture use a test environment. You will find that your original plan is likely not going to be your final plan.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3&DisplayLa>
<http://www.microsoft.com/downloads/details.aspx?FamilyID=29dbae88-a216-45f9-9739-cb1fb22a0642&DisplayLa>

/rich

"Hutch" wrote:

I don't have much in the way of links, but the following should be helpful, specifically to your original question:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:315676&sd=tech>

http://www.microsoft.com/WINDOWS2000/techinfo/reskit/deploymentscenarios/scenarios/ou_delegate_admini

http://www.computerperformance.co.uk/w2k3/W2K3_OU_Delegate.htm

On another note, you can see what the delegation wizard does, when you use it on an OU. It is very similar to file/folder permissions with AD users & groups. Open ADUC, go to View, and make sure Advanced Features is selected. Then right click on an OU...you should have a new tab available, labelled

RE: Delegation of duties to junior administrator

Security.

That will let you see what groups have rights to that OU. Our domain isn't all the complicated so I haven't fully checked/tested, but I believe the rights flow down, the same as in a file/folder structure, i.e. parent to child.

Hope the above helps.

"Hutch" wrote:

What we have done is the following:

Created a Group in AD. Using the Restricted Groups GPO (be very careful with this one..if not setup properly, you can remove the Domain Admins group from everything), we have made this Group a member of the local Admins group, on all PC's (Not Servers). That gives members in this group, full admin rights to all PC's.

All Computer accounts are in a specific OU (not the default container, but we created a separate one). Delegated permissions to the Group, to allow for adding PC's, renaming, etc....essentially full admin rights.

With computers being separate from servers, this only allows the members to have full access to PC's, which we are not overly concerned about. I have made sure that all Domain Controllers, Servers, and any other essential PC, are not in this OU, nor does the Restricted Groups GPO have access to them.

The other reason the separate Computer OU works for us, is we use RIS to image our PC's. It automatically places the new computer account into this OU.

However, if you want to continue using the default computer container, you can delegate permissions on this one as well. As mentioned, I would just make sure that anything you don't want touched by this junior admin, does not have it's machine account in this container.

"sektor" wrote:

Hello everyone.

I was hoping to get some recommendations on how I can accomplish the following:

I have a Junior Administrator that will be starting soon for

RE: Delegation of duties to junior administrator

me. I need to figure out how to give him just enough access to perform some duties, without giving him full blown Administrative privileges. I came from the Unix/Linux world where I used "sudo" to give just the right permissions needed.

What is the best way to go about doing this? Here are some basic duties he would need to do:

- join computers to the domain
- when renaming computers, he will need the admin password (because it asks for it, just like when you join computers to the domain)
- patching computers

But I definitely do not want to give out full administrative access. I setup a policy to not even use the admin account for anything, unless absolutely necessary.

Anyone have some recommendations? Maybe a article or how-to to accomplish just what im trying to?

Thanks,