

Re: AD User Objects & Permission Inheritance

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-02/0380.html

From: Arcom (Arcom_at_discussions.microsoft.com)

Date: 02/01/05

Date: Tue, 1 Feb 2005 11:27:02 -0800

I went ahead and granted the Account Operators built in group rights on the adminSDholder object according to what I want the OU admins to have. I will add the OU Admins to the Account Operators built in group and this should solve the problem with the least amount of security weakening. If anyone sees a flaw in this thought process please mention it. Thanks in advance.

"Arcom" wrote:

> Thanks for all the help. I went ahead and enabled inheritance on the
> adminSDholder object to verify that this indeed was the cause and 60 minutes
> later all user objects began to inherit permissions again. At this point I
> will look into the best way to provide a "middle ground" solution so as not
> to open up all user accounts to inheritance but at the same time allowing the
> necessary OU admins the proper rights to its users. My only remaining
> question that I was not able to clearly answer through the responses or KB
> article is whether every single user under an OU that contains a protected
> user account gets inheritance disabled because of that one protected account?
> Reason I ask is because certain OU's contain only a handful of customer
> service users that have never been in a protected group yet they too were not
> inheriting permissions. Thanks again for all your time and information.

>

> "ptwilliams" wrote:

>

>> Personally, I don't think method two is suitable. The adminSDHolder object
>> is there for a reason. After all, this behaviour is by design. In many
>> environments, setting the inherit flag will add a lot of additional,
>> unnecessary permissions to the protected accounts.

>>

>> If you have the need to delegate control to a user or group to administer
>> users in an OU, and in that OU reside other protected users you have two
>> choices –remove them from those protected groups (most of the time they are
>> members for legacy reasons, and should no longer be in there); or delegate
>> the control to an existing admin-type person, i.e. one of the protected
>> group members –you can then grant that user or protected group to which he/
>> she belongs permissions to the adminSDHolder object.

>>

>> If neither of these suit your needs, I would apply the permissions that you

> > applied to the OU in question to the adminSDHolder object. This is better
> > than simply allowing the adminSDHolder to inherit permissions, as you are
> > still limiting access to these protected users.
> >
> > --
> >
> > Paul Williams
> >
> > <http://www.msresource.net/>
> > <http://forums.msresource.net/>
> >
> > "Desmond Lee" <mcp@donotspamplease.mars> wrote in message
> > news:BD1A4EDE-EE11-4979-9FB2-B5A6D42009F2@microsoft.com...
> > Do you have Win 2000 SP4 installed and the phenomenon happened recently /
> > intermittently?
> >
> > Are these admins also members of a security group within the OU delegated
> > rights to manage the OU?
> >
> > See
> > <http://support.microsoft.com/default.aspx?scid=kb;en-us:817433>
> >
> > Method 2 in the KB would be the less disruptive resolution to this
> > 'security' problem.
> >
> > Do let us know if it helps. Thanks!
> >
> > "Arcom" wrote:
> >
> > > I noticed something when one of the users in charge of an OU reported he
> > > could no longer modify the user objects. The user rights were not
> > > inheriting
> > > permissions from its parent OU's. I enabled the Inherit permissions check
> > > box
> > > and the next day it was disabled again. Then I went looking at all other
> > > user
> > > objects in the different OU's and some OU's had users with permission
> > > inheritance enabled and other OU's user objects had inheritance disabled.
> > > How
> > > would this be? Is there a setting in a GPO somewhere to control this? It
> > > seems so sporadic and it makes it hard to pinpoint.
> >
> >
> >