

Re: Prevent some Domain Admin Account from creating USERS, Groups, OUs

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2008-01/msg00005.html

- *From:* "Jorge de Almeida Pinto [MVP - DS]"
<SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxxxx>
 - *Date:* Sun, 6 Jan 2008 20:46:38 +0100
-

DAs can do anything and there is NOTHING to prevent it

for some of the tasks you can delegate it, for some you can't and some you won't

Working with DENY permissions on objects for DAs does not work

either someone is a DA or isn't.

If that person is a DA everything is possible. if that person is not a DA or shouldn't be, delegate. Don't handover trusted tasks to non-DAs like installing software on DCs or installing DCs or stuff like that

also see:

<http://blogs.dirteam.com/blogs/jorge/archive/2006/12/28/Granting-admin-level-access-for-the-OS-on-DCs-but-no>

Cheers,

(HOPEFULLY THIS INFORMATION HELPS YOU!)

Jorge de Almeida Pinto # MVP Windows Server - Directory Services

BLOG (WEB-BASED)--> <http://blogs.dirteam.com/blogs/jorge/default.aspx>

BLOG (RSS-FEEDS)--> <http://blogs.dirteam.com/blogs/jorge/rss.aspx>

* How to ask a question --> <http://support.microsoft.com/?id=555375>

* This posting is provided "AS IS" with no warranties and confers no rights!

* Always test before implementing!

#####

<coco07@xxxxxxxxxx> wrote in message

news:abcd420e-b5e2-4772-9b9c-8a297884afb8@xx

Re: Prevent some Domain Admin Account from creating USERS, Groups, OUs

How Can I PREVENT some specific Domain Admin Accounts from creating User Account, Security Groups, OUs and modifying those object properties??

These Domain Admin Account handle administrative tasks over Domain Controllers Servers such as: Install/Uninstall Software, Add Server Roles, Promote New Domain Controller, Configure AD Replication, DNS Configuration, DHCP Configuration, Manage Event Viewer, Troubleshooting related Tasks, Restart Services, etc... As far as I know the only way they can do all those things in a domain Controller Server is making those Users Account Domain Admins....

Im almost sure that the "Delegate Control" Concept doesnt work in this case, please correct me if Im wrong....

I Tried Restrict loading of Active Directory Users & Computers snap-in into MMC.... but the users already know how to manage Users or Groups using Command – Line Tools or Scripts....

I Tried removing those Account from Domain Admins Group.... I created a group where I place all of those user accounts, then I placed these group as member of other Built In Security Group Such as: DHCP Administrators, DNS Administrators, Server Operators, Network Configuration Operators, etc.... I Also gave most of the Privileges that Domain Admin Group Has... and yes.. I prevented these users from managing Users, Groups or OUs.. but that also I prevented these users from Installing/Uninstalling software, Restarting Services, Adding Roles, they couldnt handle AD Replication, etc.... So at the end it didnt work the way I wanted....

And finally I tried to place these accounts in two Security Groups: Domain Admins and a group called "LEVEL1". Using ADUC Permissions TAB, I configure "LEVEL1" group with DENY permissions over USER, GROUP and OUs Objects... hoping that "the most restrictive permission would apply"... but sadly... it didnt work neither....

So I really hope you can guide how to achieve this goal.