

Re: Administrators Group in Local Users and Groups

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-01/msg00040

- *From:* "Jorge de Almeida Pinto" <SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxxxx>
 - *Date:* Mon, 2 Jan 2006 20:22:35 +0100
-

Account Operators by default can logon to the DCs, can manage/create/delete users/groups/computers all over the place.

As Joe said, using the Account Operators group is doing your work like you in the NT4 domain days. We now have the AD days and the ability to delegate tasks to different people. That was not introduced for nothing, use it!

Some (high level) tips on setting up delegation:

- * create separate admin accounts to perform admin tasks, use normal accounts for mail and internet, etc
- * Define the admin roles in your organization
- * Define all the admin tasks performed by those roles in your organization
- * Create an OU for the Admin roles and the admin tasks
- * Do not delegate the management of the roles and the tasks to groups or persons other than the domain admins
- * Create an OU for the Admin accounts
- * Do not delegate the management of the admin accounts to groups or persons other than the domain admins
- * Create separate an OU for the Admin roles
- * Setup admin roles represented by security groups in AD
- * Setup all kinds of tasks represented by security groups in AD
- * Give the task groups the appropriate permissions in AD and on servers through the delegation of control wizard and through GPOs (restricted groups feature)
- * Make the role groups a member of the appropriate tasks
- * Make the admin accounts a member of the appropriate roles (most of the time 1 admin account only has one role assigned and when needed several tasks)
- * Protect the admin accounts OU, the admin roles and tasks OU

For delegating tasks see the following white papers. They are very good!

<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>

--

Cheers,
(HOPEFULLY THIS INFORMATION HELPS YOU!)

Re: Administrators Group in Local Users and Groups

Jorge de Almeida Pinto

BLOG --> <http://blogs.dirteam.com/blogs/jorge/default.aspx>

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

* Always test before implementing!

"Spin" <Spin@xxxxxxxx> wrote in message
news:41t6p5F1gaa6oU1@xxxxxxxxxxxxxxxxxxxx

> Hi Joe,

>

> I do not see a problem with adding junior admins to the Account Operators
> group. That gives them good privileges to the domain without giving them
> domain admin rights. I feel safe doing this. Why do you feel it is not
> safe?

>

> --

> Spin

>

> "Joe Richards [MVP]" <humorexpress@xxxxxxxx> wrote in message

> news:uO5Ox5LDGHA.2988@xxxxxxxxxxxxxxxxxxxx

>> 1. You can't have a group automatically added upon join. You can get them
>> added via a group policy though, look at restricted groups.

>>

>> 2. You can't add builtin groups from the domain to domain member's
>> builtin groups. Builtin groups have a well known sid, in the case of acc
>> ops it is S-1-5-32-548. That group will not work outside of domain
>> controllers. If you applied it to an admin group, it would give a
>> resolution error. However think of if it did work, that SID has no domain
>> affinity (i.e. no domain component of the SID) so ANY account operator of
>> ANY domain would then have admin rights to your workstations. That is why
>> it doesn't work at all.

>>

>> Finally, don't use account ops. It is a bad group to use for a multitude
>> of reasons. Consider it useful only during migration from NT4. Once you
>> have all 2K or better DCs, stop using it.

>>

>> joe

>>

>> --

>> Joe Richards Microsoft MVP Windows Server Directory Services

>> www.joeware.net

>>

>>

>> Mark Morrell wrote:

>>> Hi!

>>> I am trying to find out how to add in the domain group Account Operators
>>> to

>>> each workstations administrator group (without going to each computer).

Re: Administrators Group in Local Users and Groups

Re: Administrators Group in Local Users and Groups

>>>
>>> Domain Admins is added into each computer when it joins the domain.
>>> I want Account Operators to do the same.
>>>
>>> Running Server 2000 and 2003 native
>>> With Workstations 2000 and XP
>>> All updates as of yesterday.
>>>
>>> Thanks
>>> Mark
>>>
>

• ***Follow-Ups:***

- ◆ ***Re: Administrators Group in Local Users and Groups***
 ◇ *From: Spin*

• ***References:***

- ◆ ***Re: Administrators Group in Local Users and Groups***
 ◇ *From: Spin*
- Prev by Date: ***Re: Created users can't immediately login***
- Next by Date: ***Re: AD forest layout recommendations***
- Previous by thread: ***Re: Administrators Group in Local Users and Groups***
- Next by thread: ***Re: Administrators Group in Local Users and Groups***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***