

RE: Permissions problem

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.migration/2004-08/0642.html>

From: Bob Qin [MSFT] (*bobqin_at_online.microsoft.com*)

Date: 08/23/04

Date: Mon, 23 Aug 2004 13:12:04 GMT

Hi Jeff,

Please try to add the new Technician account to the following accounts.

"ADMIN-03\Debugger Users"

"Domain\Reports - SCEDP"

"Domain\MSDSS Admins"

What is the result?

Regards,

Bob Qin

Microsoft Online Partner Support

Get Secure! – www.microsoft.com/security

=====

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.

=====

This posting is provided "AS IS" with no warranties, and confers no rights.

From: "Jeff B." <anonymous@discussions.microsoft.com>

Subject: RE: Permissions problem

Date: Fri, 20 Aug 2004 08:04:16 -0700

Newsgroups: microsoft.public.windows.server.migration

I'll answer each one at a time.

1. As I understand it a separate AD domain was created that existed along with the old NT domain. Trust was established then the machines and users were eventually migrated.

2. No memberships were changed.

3. As far as I can tell a couple of scenarios:

a. An average user who can add themselves to contact lists to which they have no rights or privileges to. New users with identical memberships and rights cannot accomplish this.

b. Technicians who were removed from domain admin group but can go in at will and add themselves back

4. I'll use the technicians as an example. We had a group called EDP technicians. This group at one time was a member of Domain Admin group. We later determined that the EDP technicians no longer needed the Domain Admin rights so we removed it from that group. However later that week we found out that a technician managed to perform functions which only Domain Admin or higher can perform. When pressed, he says he merely added himself back to the Domain Admin group. Sure enough we removed him and had him show us. At his PC, using his profile, he added himself to the group. We found out that all the other technicians were able to do the same. We checked all other groups which they were members of and none should have had the rights to do this. We made an identical copy of the technician's account and it was unable to do this. As far as we can tell both scenarios are only happening to the pre-migration users.

I ran the whoami with the technician and a copy of the technician. AD Users and Computers have neither one as Domain Admins.

Technician's group memberships:

Group 1 = "Domain\Domain Users"
Group 2 = "Everyone"
Group 3 = "ADMIN-03\Debugger Users"
Group 4 = "BUILTIN\Administrators"
Group 5 = "BUILTIN\Remote Desktop Users"
Group 6 = "BUILTIN\Users"
Group 7 = "Domain\San Antonio Technicians"
Group 8 = "Domain\EDP PC Techs"
Group 9 = "Domain\IBC Backup Operators"
Group 10 = "Domain\Internet Users"
Group 11 = "Domain\EDP Technicians"
Group 12 = "Domain\Spe-Apps"
Group 13 = "Domain\Platform Users"
Group 14 = "Domain\Platform Supervisor"
Group 15 = "Domain\Reports - SCEDP"
Group 16 = "Domain\Global Technicians"
Group 17 = "Domain\Domain Admins"
Group 18 = "Domain\Spe-Apps"

microsoft.public.windows.server.migration: RE: Permissions problem

Group 19 = "Domain\Platform User"
Group 20 = "Domain\Platform Supervisor"
Group 21 = "Domain\Internet Users"
Group 22 = "Domain\MSDSS Admins"
Group 23 = "Domain\SPE-APPS1"
Group 24 = "Domain\Oklahoma"
Group 25 = "Domain\ExUsrs"
Group 26 = "LOCAL"
Group 27 = "NT AUTHORITY\INTERACTIVE"
Group 28 = "NT AUTHORITY\Authenticated Users"

Copy of Technician account memberships:

Group 1 = "Domain\Domain Users"
Group 2 = "Everyone"
Group 3 = "BUILTIN\Administrators"
Group 4 = "BUILTIN\Users"
Group 5 = "BUILTIN\Remote Desktop Users"
Group 6 = "Domain\San Antonio Technicians"
Group 7 = "Domain\EDP PC Techs"
Group 8 = "Domain\IBC Backup Operators"
Group 9 = "Domain\Internet Users"
Group 10 = "Domain\EDP Technicians"
Group 11 = "Domain\Spe-Apps"
Group 12 = "Domain\Platform Users"
Group 13 = "Domain\Platform Supervisor"
Group 14 = "Domain\Reports - SCEDP"
Group 15 = "Domain\Global Technicians"
Group 16 = "Domain\Spe-Apps"
Group 17 = "Domain\Platform User"
Group 18 = "Domain\Platform Supervisor"
Group 19 = "Domain\Internet Users"
Group 20 = "Domain\SPE-APPS1"
Group 21 = "Domain\Oklahoma"
Group 22 = "Domain\ExUsrs"
Group 23 = "LOCAL"
Group 24 = "NT AUTHORITY\INTERACTIVE"
Group 25 = "NT AUTHORITY\Authenticated Users"

Thanks.

Jeff

>-----Original Message-----
>Hi Jeff,
>
>Thanks for your posting here.
>
>First let's confirm the following information:
>

- >1. Did you upgrade or migrate the NT domain to Windows 2003 domain?
- >2. Did you change the users' group during migration?
- >3. Do you mean that the normal domain user can change the group membership in domain or local computer?
- >4. Would you please provide a detailed scenario for the issue?

>
>Please run the "whoami /user /groups" command under the user with problem
>and the new user with out problem and copy the result in your post.

>
>Note: whoami.exe is an utility from Windows 2000 Resource Kit Tools. You
>can download it from

>
><http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/whoami-0>

>.asp

>
>Thank you!

>
>Regards,
>Bob Qin
>Microsoft Online Partner Support

>
>Get Secure! – www.microsoft.com/security

>=====

>When responding to posts, please "Reply to Group" via your newsreader so
>that others may learn and benefit from your issue.

>=====

>This posting is provided "AS IS" with no warranties, and confers no rights.

>
>-----

> From: "Jeff B."
> <anonymous@discussions.microsoft.com>
> Subject: Permissions problem
> Date: Wed, 18 Aug 2004 20:06:43 -0700
> Newsgroups:
> microsoft.public.windows.server.migration

>
> I am a consultant to a bank which four months ago
> migrated from an NT domain to a Windows 2003 native mode
> domain. Seems the users that existed prior to the
> migration have more rights and privileges than

- they
- > *should. At the root of the domain,*
the 'Authenticated
 - > *Users' group and 'Everyone' group have limited*
rights as
 - > *intended. However the effective rights of*
the 'Domain
 - > *Users' group who is not even included in the*
 - > *permissions/security of the domain, shows nearly*
all
 - > *rights. Users can manipulate files, folders,*
group
 - > *memberships etc. even when they are not intended*
to.
 - > *Likewise, we had a group of technicians who*
had 'Domain
 - > *Admin' rights which were removed after the*
migration can
 - > *add themselves back to the 'Domain Admin' group at*
will.
 - > *Any user accounts created after the migration have*
not
 - > *exhibited these problems. How do I correct this*
problem?
 - > *Thanks.*
 - >
 - >
 - >
 - >
 - >
 - >