

## Re: How to re-join an NT domain without losing user profile data/s

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network\\_web/2004-10/2672.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2004-10/2672.html)

---

**From:** Matt DuBois [MSFT] ([mdubois\\_at\\_online.microsoft.com](mailto:mdubois_at_online.microsoft.com))

**Date:** 10/19/04

Date: Tue, 19 Oct 2004 15:44:00 -0700

Unfortunately, you can't specify the SIDs, which is one reason backups are so critical, especially of domain controllers.

Your other question isn't quite clear, so I want to make sure I understand what you're trying to accomplish. What I THINK you're after is this:

- A) You want the name of the PDC to be the same as it was originally once all the dust is settled, even though it is a different physical machine.
- B) You want the former PDC to be a BDC with the same name as the original BDC.

For clarity, Server01 will be the original PDC and Server02 will be the original BDC.

(Steps assume Server01 is offline – hardware failure, etc).

- 1) Promote Server02 to PDC
- 2) Bring Server01 back online (if possible) and demote it (see <http://support.microsoft.com/default.aspx?scid=kb:en-us:167248>)
- 3) Rename Server01 to a temporary name (follow <http://support.microsoft.com/default.aspx?scid=kb:en-us:150298> – remember its a BDC now)
- 4) Rename Server02 to the name you want the PDC to have (using the same rename article)
- 5) Rename Server01 to the name you want the BDC to have (using the same rename article)

If Server01 will be rebuilt instead of just switched around, replace steps 2 and 3 with "Delete the computer account for Server01", and replace step 5 with "Rebuild Server01 with the desired name".

Is that what you were after?

--

This posting is provided AS IS with no warranties, and confers no rights.  
"J\_Schneider" <[JSchneider@discussions.microsoft.com](mailto:JSchneider@discussions.microsoft.com)> wrote in message  
news:4D32A5E3-F7B8-43C4-84FA-C220840FC90B@microsoft.com...

> Matt,  
>  
> Your explanation about promoting the BDC to PDC after the improper  
> installation is understandable. For our next installation, we'll be  
> certain  
> to start the installation correctly as a BDC for that domain. If we do  
> that  
> properly, can we add the BDC, synchronize the domain, promote the BDC to  
> PDC  
> and then rename the new PDC so that it is has the same name as the PDC we  
> are  
> replacing?  
>  
> Am I correct that the process to rename the newly promoted PDC is to  
> simply  
> change the computer name, then to delete the old record in the server  
> manager  
> for the previous PDC and re-add the new PDC (that now will have the same  
> name  
> as the old PDC) as a BDC, but it will automatically be added as a PDC? Is  
> there a reboot in the middle of this process--after changing the name of  
> the  
> new PDC, but before deleting the old PDC record and re-adding the new  
> record  
> in server manager?  
>  
> Also, I understand sometimes there can still be unforeseen problems with  
> this  
> process. If it happens and I have to start from scratch (or in the case of  
> a  
> complete D/R where the system cannot be recovered for whatever reason), is  
> there a way to use the getsid tool and another tool (forget the name) to  
> replace old SIDs with new SIDs on the nt machine so that I can match the  
> SIDs  
> of the computer accounts, NT PDC, and user accounts to what they were  
> before?  
>  
> BTW, regarding Exchange Server, thankfully I am using an internally  
> administered UNIX SENDMAIL server instead.  
>  
> Thanks for your help -- JS  
>  
>  
> "Matt DuBois [MSFT]" wrote:  
>  
>> You are right, the way you installed did cause the trust relationships  
>> not  
>> to be preserved. The Event Code 5513 you see tells you that the domain  
>> SID  
>> changed. The trick you used is unsupported for a reason, and what you  
>> are  
>> seeing is that reason. It may look like it works, but it is not the same  
>> as  
>> doing it right from the start.  
>>  
>> Your prior experience where you had to rebuild because you couldn't  
>> restore  
>> your backup is also exactly the same thing. You created a new domain with  
>> the same name, but the SID, of course, was different.  
>>  
>> If you install the OS as a BDC of the old domain from the start, then the  
>> domain SID will be preserved and you won't have this sort of trouble.

```
>>
>> The steps you had to take are also expected. The SIDs of the users
>> changed
>> also (remember that a full user SID is made up of a combination of the
>> user
>> SID and the domain SID) when the domain SID changed. So, even though the
>> name of the user was the same, the SIDs were different, so the user did
>> not
>> have access to the profile directory. Permissions aren't assigned by
>> user
>> name, though they are shown that way because it is more human readable,
>> they
>> are assigned by SID.
>>
>> There are actually a bunch of reasons Outlook might prompt. My guess is
>> that it did so for a similar reason as the profile directories -
>> mismatched
>> SIDs. If you are using a domain joined Exchange server, you may have
>> some
>> trouble brewing. Like the workstations, that server has probably lost
>> ITS
>> trust relationship too. Not to mention that the mailbox permissions are
>> probably set for the old accounts and not the new ones. You're likely to
>> have some trouble with that down the road. If you are not very familiar
>> with Exchange, you may either want to contact PSS and explain your setup
>> and
>> make sure everything is OK, or get a consultant to check things out
>> instead.
>> The last thing you want is for everything to blow up a little down the
>> road,
>> just when you think all the fallout is over.
>>
>> Go ahead and check the document out. It is relevant even with XP because
>> on
>> an NT 4 domain, XP uses NT 4 style domain policies. The profile stuff
>> has
>> also not changed that much, and its a pretty good description of profiles
>> and what's in them.
>>
>> --
>> This posting is provided AS IS with no warranties, and confers no rights.
>>
>>
>> "J_Schneider" <JSchneider@discussions.microsoft.com> wrote in message
>> news:AC29903E-1727-46BF-A185-69B6FAD9023D@microsoft.com...
>> > Thanks for the comprehensive explanations. However, I still have some
>> > questions and I want to clarify parts of my original post:
>> >
>> > First, I did make a BDC and promote it. However, this didn't preserve
>> > the
>> > trust relationships as I intended. However, I think this was because I
>> > setup
>> > the new server as a PDC by mistake. Therefore, I had used the trick of
>> > changing the registry key HKEY_LOCAL_MACHINE\Security\Policy\PolSrvRo
>> > from
>> > 03000000 to 02000000. Then I joined the domain with it as BDC and then
>> > promoted it. It seemed to work fine (all user and computer accounts
>> > tranferred, etc), except that as each WINXP PRO workstation logged in
>> > an
>> > EVENT CODE 5513 was logged in the SYSTEM event log with the
>> > description:
>> >
```

## microsoft.public.windowsxp.network\_web: Re: How to re-join an NT domain without losing user profile data/s

```
>> > The computer COMPUTERTNAME tried to connect to the server DOMAIN_SERVER
>> > using
>> > the trust relationship established by the DOMAIN_NAME domain. However,
>> > the
>> > computer lost the correct security identifier (SID) when the domain was
>> > reconfigured. Reestablish the trust relationship.
>> >
>> > To recreate the trust relationship, I removed the PC from the domain
>> > and
>> > re-joined the domain. However, when logging into the XP PRO workstation
>> > as
>> > USERNAME, the user's local profile path (the settings for various
>> > application, desktop settings and my document redirections, etc) had
>> > changed
>> > from C:\Documents and Settings\USERNAME to C:\Documents and
>> > Settings\USERNAME.DOMAIN. No matter what I tried, I was unable to get
>> > XP
>> > PRO
>> > to user C:\Documents and Settings\USERNAME instead of C:\Documents and
>> > Settings\USERNAME.DOMAIN.
>> >
>> > Finally, I had to log in as the domain administrator (not local domain
>> > administrator) and add the domain user DOMAIN\USERNAME to the directory
>> > C:\Documents and Settings\Username (note that the ACL had a numeric
>> > entry
>> > representing the SID that the very same domain user had once been
>> > assigned).
>> > Then I had to change the registry entry HKLM/Software/MicroSoft/Windows
>> > NT/Current Version/Profile List/[user's_sid]/ProfileImagePath to
>> > represent
>> > the path C:\Documents and Settings\USERNAME instead of C:\Documents and
>> > Settings\USERNAME.DOMAIN. Even after doing this, I mentioned that
>> > Outlook
>> > still prompted for the email password. Probably having to do with the
>> > .PWL
>> > files (if that is still where windows stores stuff like that -- haven't
>> > check
>> > lately).
>> >
>> > I have also had this happen in a D/R situation where hardware changed
>> > and
>> > the D/R recovery was unable to recover the system volume and registry
>> > of
>> > the
>> > PDC and therefore it had to be rebuilt. When trying to join each
>> > workstation
>> > to the new PDC, they all had similar problems with the profile path. It
>> > just
>> > occurs to me there must be an easier way to perform this recovery.
>> >
>> > I'm not sure the guide To Windows NT 4.0 Profiles and Policies is
>> > applicable, because my problem seems to be with the profile that is
>> > stored
>> > on
>> > the XP PRO box, and its relationship to the sid in the user manager on
>> > the
>> > domain (but I'll reread it to check).
>> >
>> > And, I will check this guide you mentioned, because I haven't seen it
>> > before:
>> >>> EXTRACTING A USER PROFILE FOR USE ON ANOTHER DOMAIN OR MACHINE
>> >>> section
```

```
>> >>> in part 3 of the guide.
>> >
>> > I hope this clarifies my dilemma and can lead to further insights.
>> > Thanks
>> > again for your post Matt.
>> >
>> > _ JS
>> >
>> >
>> > "Matt DuBois [MSFT]" wrote:
>> >
>> >> A lot depends on what you mean by "replaced". If you promoted a BDC
>> >> to
>> >> PDC
>> >> then you're good and shouldn't have to do anything. However, it
>> >> sounds
>> >> as
>> >> if you created a new domain with the same name because something
>> >> happened
>> >> to
>> >> the old PDC, and you couldn't restore a backup for whatever reason.
>> >>
>> >> The important thing to know here is that even if one domain has
>> >> exactly
>> >> the
>> >> same name as another, they are still distinctly different. Each
>> >> domain
>> >> has
>> >> a domain SID that uniquely identifies it, and that SID is randomly
>> >> generated
>> >> when the domain is created. That SID is also associated with the user
>> >> profiles for the domain accounts. So, when you join the workstations
>> >> to
>> >> the
>> >> new domain (and it IS a new domain even if the name is exactly the
>> >> same
>> >> as
>> >> it was), the system recognizes that it is a new domain and creates a
>> >> new
>> >> profile directory for it since the profiles contain information
>> >> derived
>> >> from
>> >> the domain.
>> >>
>> >> So, the "proper" way to do this is to either have a BDC that you can
>> >> promote
>> >> or have a backup strategy that will let you recover. Creating a whole
>> >> new
>> >> domain is not recovering, it is starting over from scratch and comes
>> >> with
>> >> all the pain and work that entails. There IS a heavily manual process
>> >> you
>> >> can try now that you're in this position (see below), but it is not
>> >> from
>> >> painless or automatic.
>> >>
>> >> I don't have any older domain clients around right now to confirm for
>> >> sure,
>> >> but with XP, disjoining and rejoining the domain does not create new
>> >> profiles. I've even disjoined a computer from a (Windows 2000)
>> >> domain,
>> >> changed its name, rejoined the same domain, and come right back to my
```

```
>> >> profile when I logged back into my domain account afterwards.
>> >>
>> >> The netdom command you mention only migrates the computer to the new
>> >> domain,
>> >> it does not migrate the user profile. There are a separate set of
>> >> tools
>> >> for
>> >> migrating user profiles from an NT4 domain to a Windows 2000 or 2003
>> >> domain,
>> >> but those don't apply here since the "new" domain is still NT4.
>> >>
>> >> If you want to learn more about NT 4.0 profiles, you can check out the
>> >> Guide
>> >> To Windows NT 4.0 Profiles and Policies
>> >> (http://support.microsoft.com/default.aspx?scid=KB;EN-US;161334). One
>> >> thing
>> >> you might try from there is to modify the steps in the EXTRACTING A
>> >> USER
>> >> PROFILE FOR USE ON ANOTHER DOMAIN OR MACHINE section in part 3 of the
>> >> guide.
>> >> That is a tremendously manual process and does not scale to lots of
>> >> machines - but might be workable for you if you have a small
>> >> environment.
>> >> To try in your case, you would postpone step 5 until after step 6.
>> >> After
>> >> copying the profile structure in step 6, you would rename the original
>> >> profile to something else, so that when you do step 5, the profile is
>> >> created with the correct profile path. I haven't ever tried it, but
>> >> it
>> >> looks as if it should work for you.
>> >>
>> >> Since you mentioned Windows XP in your post, you'll notice there is no
>> >> System control panel on Windows XP. To get to the profile copy
>> >> interface
>> >> on
>> >> XP, right click on My Computer, select Properties, go to the Advanced
>> >> tab
>> >> and click on the "Settings" button under User Profiles. Also, the
>> >> article
>> >> doesn't say it straight out, but you shouldn't be logged into the
>> >> account
>> >> for which you are copying the profile, even if it IS an Administrator
>> >> on
>> >> the
>> >> machine.
>> >>
>> >> Hope this helps shed some light on why you're seeing what you're
>> >> seeing.
>> >>
>> >> -Matt
>> >> --
>> >> This posting is provided AS IS with no warranties, and confers no
>> >> rights.
>> >>
>> >>
>> >> "J_Schneider" <JSchneider@discussions.microsoft.com> wrote in message
>> >> news:C3472F6E-F170-420B-8795-8DD0816C367F@microsoft.com...
>> >> > I've NEVER seen this answered completely and correctly. I hope it
>> >> > can
>> >> > be
>> >> > here. It is an important topic for network administrators like
>> >> > myself:
```

```
>> >> >
>> >> > I've recently replaced and NT4 PDC. The trust relationships with the
>> >> > workstations were broken and have to be recreated. What is the
>> >> > proper
>> >> > way
>> >> > to
>> >> > do this so that the user's profile and profile_path are retained?
>> >> >
>> >> > From my experience, if you remove the PC from the domain and then
>> >> > rejoin
>> >> > it
>> >> > the user will have a new locally cached profile_path created called
>> >> > username.domain (or username.domain.000 if the username was first
>> >> > using
>> >> > a
>> >> > profile_path of username).
>> >> >
>> >> > I've gotten around this somewhat by resetting security on the user's
>> >> > previous profile path and then editing the registry key under
>> >> > HKLM/Software/MicroSoft/Windows NT/Current Version/Profile
>> >> > List/[user's
>> >> > sid].
>> >> > But, this doesn't seem correct. Especially since MS Outlook prompts
>> >> > for
>> >> > the
>> >> > user's email account password the next time it is launched.
>> >> >
>> >> > I've also played with the NETDOM.exe tool from the XP support tools
>> >> > from
>> >> > one
>> >> > workstations, but had not much luck. Should I be using the
>> >> > netdom.exe
>> >> > tool
>> >> > from the server (the NT version)? Is this tool still available now
>> >> > that
>> >> > the
>> >> > NT Resource Kit has been discontinued?
>> >> >
>> >> > Help! This is a very troublesome issue that I cannot seem to find a
>> >> > definitive answer to. Thanks a ton to the genius who shed's light on
>> >> > it
>> >> > for
>> >> > me.
>> >> >
>> >> > Much thanks! -- JS
>> >>
>> >>
>> >>
>>
>>
>>
```