



Re: SID History and SID Filtering questions (netdom)

Oh and by the way the Technet doc on how to create a SID mapping file only applies to ADMT v2 and Not ADMTv3 it should be updated, I have now written a small app to export the Domain SID + User RID from the domain you are attempting to migrate so that you can use a SID mapping file.

Vincent Xu [MSFT] wrote:

Hi,

SID filtering is enabled automatically on any trust relationships created by domain controllers running Windows 2000 Service Pack 4 or Windows Server 2003. Or, you can manually enable it by using the Netdom trust command line utility with the /EnableSIDHistory:no command line switch. To disable SID filtering (and thus enable SIDHistory), use the /EnableSIDHistory:yes switch.

If even this level of SIDHistory accessibility is too much, you can impose even stricter limits on your trust relationships by enabling the Quarantine feature. (In this context, the Quarantine feature controls SID processing over trust relationships and shouldn't be confused with the Network Access Protection or Network Access Quarantine Control technologies that are used to control local and remote access connections.) By enabling Quarantine for a trust relationship, you are specifying that only SIDs from the exact domain on the other side of the trust are to be honored. In effect, enabling Quarantine on a trust relationship will break the transitivity of that trust, so that only the specific domains on either side of the trust are considered participants in the trust. Quarantine is disabled by default on all trust relationships; you can manually enable it by using the Netdom trust command line utility with the /quarantine:yes command line switch. Use the /quarantine:no switch to disable Quarantine on a trust relationship where it has already been enabled. I suspect that your problem is: you grant a group, which has the user account, the permission to access the old resource. After you migrate the user to the new domain, they are not part of the old group so that they lost the permission to access the old resource. Please feel free to correct me.

If so, please check the share permission and NTFS permission of the old resource and let me know if you grant the permission to the user directly.

If this is the issue, we need to re-ACL the resources.

Since OldDomain\User1 is a built-in group we cannot use ADMT to migrate it. Fortunately, we are able to use Security Translation Wizard with a SID Mapping file to add the NewDomain\"Domain Users\" group's SID to the resources.

To do so:

1. Get the SIDs of both OldDomain\"Domain Users\" and NewDomain\"Domain Users\". We can logon as OldDomain\User1, run

Re: SID History and SID Filtering questions (netdom)

"whoami.exe /all". From the return content, we can find the SID of OldDomain\ "Domain Users". Please use this method to get the SID of NewDomain\ "Domain Users".

Note: whoami.exe is an utility from Windows 2000 Resource Kit Tools. If you do not have it, please let me know.

2. Create a SID mapping file (should be a txt file). We can name it sidmapping.txt.

3. Edit the SID mapping file in Notepad and input the following content:

<SID of OldDomain\ "Domain Users">, <SID of NewDomain\ "Domain Users">

Note: Please put the correct SIDs in the above line.

4. Run ADMT, choose "Security Translation Wizard".

5. On the "Security Translation Options" page, choose "Other objects specified in a file" and browse to select the sidmapping.txt file created in Step 2.

6. Follow the wizard to translate resources on ServerA.

7. Please check if the NewDomain\User1 has access to <\\ServerA\Share>.

Let me know if you have any concerns or questions.

Best regards,

Vincent Xu  
Microsoft Online Partner Support

=====  
PLEASE NOTE: The partner managed newsgroups are provided to assist with break/fix issues and simple how to questions. We also love to hear your product feedback! Let us know what you think by posting from the web interface: Partner Feedback from your newsreader: microsoft.private.directaccess.partnerfeedback. We look forward to hearing from you!  
=====

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

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



Re: SID History and SID Filtering questions (netdom)

Which Group ? > 1, Verify whether the group has been migrated  
I also get access denied with 2

what is the difference between  
/quarantine:No and /enablesidhistory:yes?  
Vincent Xu [MSFT] wrote:

Hi,

Netdom Syntax:

```
Netdom trust
TrustingDomainName
/domain:TrustedDomainName
/quarantine:No
```

```
netdom trust trusted_domain
/domain:trusting_domain
```

/enablesidhistory:yes

since you get "Access denied" when you run "Netdom trust

TrustingDomainName

```
/domain:TrustedDomainName
/quarantine:No", 1, Verify
whether the group has been
migrated
2, Enable SID history by
running : netdom trust
trusted_domain
/domain:trusting_domain
/enablesidhistory:yes
```

Let me know if you still have concern.

Best regards,



Re: SID History and SID Filtering questions (netdom)

User-Agent:  
Mozilla  
Thunderbird  
1.0  
(Windows/20041206)  
X-Accept-Language:  
en-us,  
en  
MIME-Version:  
1.0  
Subject:  
SID  
History  
and  
SID  
Filtering  
questions  
(netdom)  
Content-Type:  
text/plain;  
charset=ISO-8859-1;  
format=flowed  
Content-Transfer-Encoding:  
7bit  
Message-ID:  
<ep3qkafXGHA.4988@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
Newsgroups:  
microsoft.public.windows.server.migration  
NNTP-Posting-Host:  
dsl-146-103-45.telkomadsl.co.za  
165.146.103.45  
Lines:  
1  
Path:  
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2  
Xref:  
TK2MSFTNGXA01.phx.gbl

microsoft.public.windows.server.migration:23283

X-Tomcat-NG:  
microsoft.public.windows.server.migration

Hi,

Re: SID History and SID Filtering questions (netdom)

Re: SID History and SID Filtering questions (netdom)

there  
seems  
to  
be  
very  
little  
in-depth  
technical  
docs  
on  
sid

history

and  
sid  
filtering  
and  
I  
need  
some  
help!

I  
am  
trying  
to  
get  
sidhistory  
to  
work  
between  
2  
domains  
a  
windows  
2000  
domain  
and  
a  
windows  
2003sp1  
domain,  
(we  
are  
moving  
from  
the

Re: SID History and SID Filtering questions (netdom)

windows  
2000  
domain)

I  
have  
domain  
admin  
rights  
in  
both  
domains  
(and  
Enterprise  
admin  
in

the

2003  
domain)

when  
I  
run  
the  
command  
(  
in  
either  
domain)  
netdom  
trust  
win2000domain  
/Domain:Win2003Domain  
/Quarantine

I  
get  
an  
Access  
Denied  
error.  
I  
have  
tried  
the  
/userO

Re: SID History and SID Filtering questions (netdom)

and  
/userD  
options

My  
questions  
are  
1)  
Exactly  
where  
am  
I  
getting  
access  
denied?

2)  
when  
you  
run  
the  
command  
with  
a  
/Quarantine:YES  
what  
attribute/s

are

changed  
where  
in  
AD?

and  
what  
is  
the  
difference  
between  
the  
/Quarantine:NO  
and  
the  
/EnableSidHistory:YES  
commands?  
Do  
I

Re: SID History and SID Filtering questions (netdom)

need  
to  
run  
both?  
What  
is  
the  
latest  
version  
of  
netdom?  
(I  
am  
using  
5.2.3790.0)

Oh  
and  
if  
anyone  
from  
Microsoft  
is  
reading  
this  
the  
following  
needs  
to  
be  
updated  
to  
incorporate  
ADMT  
v3

<http://support.microsoft.com/default.aspx?scid=kb:en-us:835>

Regards  
Riccardo  
Moretti

Re: SID History and SID Filtering questions (netdom)