

Re: Converting local groups to domain local groups

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-12/msg00095.html>

- *From:* Trilix <Trilix@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 29 Dec 2006 00:40:01 -0800
-

Thanks for the explanation both of you. But it seems that our local groupnames are too long.

I'm going to build them from scratch on the domain and repopulate them.

"Roger Abell [MVP]" wrote:

As Joe said there is no conversion path.
However, there are some rather simple paths.
Consider
net localgroup
lists the local groups on the member
suppose this shows you
grp1 grp2 grp3 grp4
grp5 grp6 etc.
That that output and transform it in a file to
net localgroup grp1
net localgroup grp2
etc
Those commands will result in a listing of the
members in each group
Now, transform a copy of the file to
net localgroup grp1 /add
net localgroup grp2 /add
etc
If you now run that on a DC all of the domain local
groups will be defined.
Now, transform it again so that it is
net localgroup grp1 domain\grp1 /add
net localgroup grp2 domain\grp1 /add
etc
If you run that on the member then the new domain
local is added to the corresponding machine local.

Now, when you ran on the member the first file

Re: Converting local groups to domain local groups

```
net localgroup grp1
net localgroup grp2
etc
```

you got a list of members of each group

Transform that to

```
net localgroup grp1 user1 /add
net localgroup grp1 user2 /add
net localgroup grp2 user5 /add
net localgroup grp2 user6 /add
etc
```

etc for each user account that is a domain account.

When this is run on a DC the membership of the new domain local groups is made to be as close as possible to the member's local groups

```
net localgroup grp1 domain\user1 /delete
net localgroup grp1 domain\user2 /delete
net localgroup grp2 domain\user5 /delete
net localgroup grp2 domain\user6 /delete
etc
```

When this is run on the member these domain user accounts are removed (they still have access via the domain global).

If you are savvy in notepad or similar with global replace (ex "net localgroup " replacing a couple lines of comment, etc) making the two base files is not that much drudgery if the number of groups and memberships is reasonably small, and actually turns out much quicker than writing and testing a script to do the same.

Now, you would still have the machine locals in the ACLs where there were, and these would still carry any machine local accounts they may have had, but you would have domain locals that carry as much as can be carried by them. If you need to replace the machine locals with the domain locals then look at using such as SubInAcls and look at the impact of this removing access for any machine local accounts that might be in the machine locals being replaced.

Roger

Now, finally transform this to

"Trilix" <Trilix@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:54A8CDB2-15CD-4980-86FC-150B3636D5C8@xxxxxxxxxxxxxxxxxxxx

Hi,

We need to get rid of our local groups, because of our WAFS implementation, so I think the best way is to make domain local groups. Is there an easy way to convert local groups to domain local groups? A freeware util maybe?

Re: Converting local groups to domain local groups

Kind regards