

Re: dsrm tool

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-05/msg00298

- *From:* "Paul Bergson [MVP-DS]" <pbbergs@xxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 7 May 2009 07:16:05 -0500
-

I'm with Florian, we also use oldcmp (Freeware) and I can disable and move depending on an aged date.

I have seen some Powershell scripts floating about as well. Of course you would need to load Quest AD CmdLet (Also Freeware)

Here is the meat for deleting inactive computer accounts.

```
# set the date to be used as a limit - in this example: 90 days earlier than the current date
$old = (Get-Date).AddDays(-90)
```

```
# get the list of computers with the date earlier than this date
Get-QADComputer -IncludedProperties pwdLastSet -SizeLimit 0 | where { $_.pwdLastSet -le $old }
```

A few variations to this depending on how you want to use the data:

```
# get a csv report
Get-QADComputer -IncludedProperties pwdLastSet -SizeLimit 0 | where { $_.pwdLastSet -le $old } |
select-object Name, ParentContainer, Description, pwdLastSet | export-csv c:\temp\outdated.csv
```

```
# move such computers to another OU
Get-QADComputer -IncludedProperties pwdLastSet -SizeLimit 0 | where { $_.pwdLastSet -le $old } |
Move-QADObject -to test.lab/obsolete
```

```
# remove the computer records from AD (caution: this actually deletes the records, run the command with
-whatif switch before running without it)
Get-QADComputer -IncludedProperties pwdLastSet -SizeLimit 0 | where { $_.pwdLastSet -le $old } |
Remove-QADObject -to test.lab/obsolete
```

Posted By:
Scha rique

—
Paul Bergson
MVP – Directory Services
MCTS, MCT, MCSE, MCSA, Security+, BS CSci
2008, 2003, 2000 (Early Achiever), NT4

Re: dsrm tool

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup This posting is provided "AS IS" with no warranties, and confers no rights.

"Florian Frommherz [MVP]" <florian@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:eg09A4tzJHA.1432@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Howdie!

uSlackr schrieb:

We just finished writing a windows cmd script to locate and delete aging computer accounts from AD. The script uses a combination of the ds* tools to find old accounts, check to see whether they have a flag to exclude their deletion and if not delete them from AD. We ran into a problem where some accounts had child objects (virtual server hosts for one) that requires us to use the -subtree option with dsrm. It works like a charm.

The script can be found here:

http://linux2.gmartin.org:82/tiki/tiki-view_blog_post.php?blogId=2&postId=138

I wonder why you didn't use joe's great oldCMP tool:

<http://joeware.net/freetools/tools/oldcmp/index.htm> — it's been around for a while and — as far as I can tell — got great feedback.

But it got me thinking, what if a bug in the script caused cn=computer,ou=servers,dc=corp,dc=com to drop the CN and leave the OU inplace. The subtree switch would allow dsrm to delete the OU and everything in it. So I have two thoughts.

Why would the subtree switch dsrm cause it to delete the OU? Having the switch on would let dsrm delete all objects and child objects of the base DN you specified:

CN=computer,OU=servers,DC=... it shouldn't touch the servers OU.

– We're going to set the "prevent accidental deletion" flag on all OUs. This is a good practice anyway. We found this script reference for that:

<http://msmvps.com/blogs/ulfbsimonweidner/archive/2007/09/25/protect-objects-from-accidental-de>

Yeah, that is a really good practice. You should go that way. That's what I recommend often.

– Second, would it make sense to ask MS to add a switch to dsrm that would prevent it from deleting OUs? That way, if you wrap it in a script you could specify the -noodelete switch and regardless of what you asked, it would

Re: dsrm tool

Re: dsrm tool

refuse to act.

I haven't used dsrm in a while so I cannot tell what switches it currently supports. From this perspective it would totally make sense to ask for a switch like that. A good place for that kind of suggestion would be connect.microsoft.com.

Cheers,
Florian

--

Microsoft MVP – Group Policy

eMail: [prename \[at\] frickelsoft \[dot\] net](mailto:prename@frickelsoft.net).

blog: <http://www.frickelsoft.net/blog>.

Maillist (german): <http://frickelsoft.net/cms/index.php?page=mailingliste>