

Re: Scavenging Machine Accounts in AD

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-10/0973.html

From: Joe Richards [MVP] (*humorexpress_at_hotmail.com*)

Date: 10/16/04

Date: Sat, 16 Oct 2004 10:42:35 -0400

lol.

```
--
Joe Richards Microsoft MVP Windows Server Directory Services
www.joeware.net
Cary Shultz [A.D. MVP] wrote:
> Yes, Thank you, Joe!
>
> Yet another example of the fingers going too fast!
>
> And you have O - N - L - Y three of the five? Hard to believe. I thought
> it would have been all of them!
>
> Cary
>
> "Joe Richards [MVP]" <humorexpress@hotmail.com> wrote in message
> news:%23IQxLpysEHA.1216@TK2MSFTNGP10.phx.gbl...
>
>>Let me correct that URL... www.joeware.net
>>
>>if you want you can read about it in the current Windows IT Pro magazine.
>
> It is
>
>>one of 5 Best Tools for AD (I have 2 other tools in that list as well).
>>
>>  joe
>>
>>
>>--
>>Joe Richards Microsoft MVP Windows Server Directory Services
>>www.joeware.net
>>
>>
>>Cary Shultz [A.D. MVP] wrote:
>>
>>>Mutsa,
>>>
>>>A large part of the problem apparently is that the domain user account
>>>object is a member of the computer's local Administrators group. I
>
> suggest
>
>>>this as the only way that this action ( to rename a computer or to join
```

microsoft.public.win2000.active_directory: Re: Scavenging Machine Accounts in AD

```
>
> it
>
>>>to a domain/workgroup ) is available is if the domain user account
>
> object is
>
>>>a member of the local Administrators group ( or that the domain user
>
> account
>
>>>object being used to do this is a member of the Domain Admins or other
>
> 'top
>
>>>level' special groups ).
>>>
>>>A 'regular' domain user account object *should* not be a member of any
>
> of
>
>>>these groups. This problem very quickly goes away if this basic
>
> security
>
>>>policy is maintained and enforced ( as the ability to do this is not
>>>available ).
>>>
>>>There is also the behavioral problem ( which, again, would not be
>
> possible
>
>>>where basic security policies in place - but I do understand that this
>
> is
>
>>>not always possible politically. Which is always a horrible horrible
>>>horrible reason). Management and HR might need to be involved and your
>
> user
>
>>>base needs to be made aware that they are not to be messing with the
>>>computer account objects in any way, shape or form. However, this
>
> requires
>
>>>HR and Management to be in agreement with the IT Department's stance on
>>>this. This is not always the case ( as mentioned above ) so.....
>>>
>>>Now, while this is not an 'automagic' approach you can go to Joe
>
> Richard's
>
>>>website at http://www.joesware.net and look at his free utilities
>
> section.
>
>>>There is something called oldcmp that will do what you need. However,
>
> you
>
>>>do need to manually run this ( or set up something so that it runs on a
```

microsoft.public.win2000.active_directory: Re: Scavenging Machine Accounts in AD

```
>>>schedule ). Be advised that you must first disable any computer account
>>>objects before you can delete them. This is just one of the several
>>>safeguards that Joe wisely built in to this awesome utility.
>>>
>>>HTH,
>>>
>>>Cary
>>>
>>>"mutsa" <mutsa@roke.co.uk> wrote in message
>>>news:%232w2u$3rEHA.2168@TK2MSFTNGP10.phx.gbl...
>>>
>>>
>>>>Does any one know if there is an automatic way to scavenge and delete
>
> the
>
>>>>accounts of machines that have been taken permanently off-line but have
>>>
>>>>not
>>>
>>>>been cleanly removed from the domain.
>>>>
>>>>For example a machine is built using RIS which will automatically add
>
> that
>
>>>>client to AD. After that the user removes the machine from the network
>
> to
>
>>>>make it stand-alone, but does not inform me. I would like that machines
>>>>account to be either deleted automatically from AD after a set period of
>>>>time of say 60 days or disabled somehow.
>>>>
>>>>Is this possible and can anyone help.
>>>>
>>>>MMMSD
>>>>
>>>>
>>>>
>>>>
>
>
```