

Re: Renewing Kerberos ticket

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.scripting/2005-03/0032.html>

From: Amihai Bareket (*amihai73_at_hotmail.com*)

Date: 03/01/05

Date: Tue, 1 Mar 2005 08:41:55 +0200

Just to clarify –
Regular users don't run this script.

We use it to build new organizational units in AD.
Each OU we create is followed by a creation of several security groups and then a several folders which the new groups have permissions to.
The script adds the "Domain Admin" group to one of the newly created security groups, then I need to set ACL on the new folder only for the new group.

Can you think of another way of doing this?

"Roger Abell" <mvpNOSpam@asu.edu> wrote in message
news:eB6hNciHFHA.560@TK2MSFTNGP12.phx.gbl...
> *The account must log off and back on.*
> *There is no other way. Refreshing a ticket does not*
> *refresh the user token that is in use. Only getting a*
> *new TGT through login authentication does that.*
>
> *However, there is something that does not make sense in*
> *what you have said.*
> *The user runs a script that creates a group and adds themselves*
> *to the group. The script then attempts to alter an ACL but are*
> *denied due to permissions. You say that if their user token*
> *were refreshed to see the new group and their membership in*
> *it then they would not be denied. I do not see how that is so,*
> *but do see how that seems impossible.*
>
> --
> *Roger Abell*
> *Microsoft MVP (Windows Security)*
> *MCSE (W2k3,W2k,Nt4) MCDBA*
> *"Amihai Bareket" <amihai73@hotmail.com> wrote in message*
> *news:eQGERJiHFHA.3076@tk2msftngp13.phx.gbl...*
>> *I'm working with a script that's creating new AD Security groups and*
>> *changing their membership.*
>> *The user that runs the script is added as a member of the new groups.*

>> *Once the groups are created I need the script to create folders and set
> ACL
>> on these folders using the new groups.
>> Because the groups are newly created, the information that indicates that
>> the logged in user (the one that's running the script) is a member of the
>> new groups is not included in the Kerberos ticket he's been granted on
>> logon.
>> The permission change on the file system fails because of this with an
>> access denied message (makes sense...). I'm using XCACLS to set the
>> permissions on the new folders.
>>
>> Is there a way to request a renewal to a user's Kerberos ticket from a
>> script or batch so that he will receive a new or renewed ticket with the
> new
>> group information?
>>
>>
>>
>
>*