

## Re: Security Groups issue...

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-10/msg01660](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-10/msg01660)

---

- *From:* "Herb Martin" <[news@xxxxxxxxxxxxxxx](mailto:news@xxxxxxxxxxxxxxx)>
  - *Date:* Fri, 20 Oct 2006 02:08:36 -0500
- 

"Kshaeta" <[visual.eyes@xxxxxxxx](mailto:visual.eyes@xxxxxxxx)> wrote in message  
[news:u7S2Ak88GHA.4604@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:u7S2Ak88GHA.4604@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

\*\*\* Note, I posted this is the "security" group, but someone suggested I put it here to get an answer. \*\*\*

One reason I ask, is because of this problem. I have two security groups, within my domain, and two servers in my domain. One server is a domain server (DOM), the other is a member server (MEM).

I have 2 security groups. The difference between the two is one is a DLS group, the other is a GS group. The DLS one doesn't allow the security group to be set on servers other than the domain servers.

That is almost certainly because it is NOT actually a "Domain Local Group" (despite what the dialog box says or common usage of the term) due to your domain being in Mixed Mode (or Intermim.)

Technically, "Local Groups on the Domain" do not become "Domain Local Groups" unless you change the domain mode to one of the Native modes. (Win2003 or Win2000 native).

The terminology on this is extremely confusing (and whoever wrote the dialog box didn't even get the message — or they decided it wasn't worth the trouble to change the label as the mode changes, as do some other user properties do to distinguish Native/Mixed modes.)

ONLY true "Doman Local Groups" are truly visible/usable off the DCs — NT and mixed mode "Locals on the Domain" are only for DC usage.

That is, if you are on DOM and you create a directory, you can grant it "Information Systems\_DLS" security, or "Information Systems\_GS" security. But if you log on to MEM, and try that it won't work. You need to grant it "Information Systems\_GS". The option to grant any DLS doesn't even show up in the security selection on the member server.

## Re: Security Groups issue...

Mixed mode "feature" most likely.

I don't really grasp this. Should "Domain level Security" allow you to grant that security group to any member server?

Yes, and it will if you convert the domain to Native+ mode.

I know how security groups work together, how certain ones can't be part of others, etc. But I don't really understand how they work, or where and when to use them.

Use "Global Groups" primarily to create "bunches of users" — to represent a particular set of users.

Use Local Groups (either machine or on the domain) to represent "a set of resources" that should be given the same access.

Then place the PERMISSIONS on the (machine or domain) local groups and the users into the Globals on the domain. Now you put the Global group(s) into the various Local groups to grant the access.

Where are DLS (Domain Local Security) groups used, and why?

See above.

How about GS (Global Security) groups? Universal Security groups?

Ditto for Global Groups.

Universals can be best thought of as "super globals" and are not even available as Security Groups (only distribution groups) until you reach Native+ mode. (It would confuse any NT BDCs left over.)

Universals differ from Globals mainly (in a technical sense) in that they can include users from Multiple Domains where as Globals can only contain objects from the SAME domain (where the Global is created.)

Is there any good documentation that explains how these are used and why?

Re: Security Groups issue...

Yes, the Built-In Help, the Resource Kit books (paper or online), TechNet in specific and the other online Microsoft resources are the best.

(Unless you attend my class <grin>)

—  
Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

Thanks for any info.

—  
Bill Tkach  
MSP, A+  
visual{period}eyes{period}this{at}gmail{period}com