

# Re: General questions about LDAP, GC and access permissions

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-07/msg00421](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-07/msg00421)

---

- *From:* UncleRedz <UncleRedz@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Wed, 11 Jul 2007 00:40:03 -0700
- 

Hi,

Thanks for the quick reply. I'll try to clarify what my intentions are.

The application/service only needs read-only access to AD. This is used for two different tasks.

The first task, is as I described earlier, a user connects to the service using Windows Communication Foundation (WCF), resulting in a WindowsIdentity that we have to examine in order to determine what that user is allowed to do.

The examination process is supposed to figure out what groups the user (represented by the WindowsIdentity) belongs to and what groups those groups may belong to. This results in a list of groups.

The user and the list of groups is then matched against our database where users and groups have been assigned various permissions, the output of this is that we get a combination of all permissions that may be directly assigned to the specific user as well as those inherited through group memberships.

The second task that uses AD is the task of populating the database with users and groups and assigning various permissions to those. This requires us to create lists of all the available users and groups that the administrator can add to the database. (I think the answers provided by you and Richard is sufficient for solving this task.)

I'll checkout the book as well, if anything it might be handy to keep around for future issues.

"Joe Kaplan" wrote:

5. How do I deal with trusted domains? Will using GC instead of LDAP solve this?

Re: General questions about LDAP, GC and access permissions

It can be complicated and it depends on what you mean by this. What about trusted domains do you need to do?

For task 2, I need to be able to present all available users and domains that are valid on the machine that is running the service.

For task 1, I need to be able to resolve all the groups that the accessing user is a member of, and what groups those groups are members of, independent of what ever domain they may be from, as long as they are valid in the context of the machine running the service.

6. If the local machine is running in domain X and the user is from the trusted domain Y, should I still use the X domain when constructing the LDAP/GC query? Or should I use the Y domain instead?

Are these domains in the same forest or an external forest?

I have no idea, this service and application will be running at various customers with very varying network configurations. Although I think there has to be a limit to how flexible the service and application is.

Don't forget that when you are using Windows auth, Windows itself will calculate a user's group membership in the user's logon token. It is best to not try to get the user's group membership via LDAP if Windows is going to do it for you.

Well, this sound most interesting, if the information that can be gained is enught, then this would be the easiest solution. Do you have any pointers to where I should look in order to get the memberships from the token?

Cheers,  
UncleRedz

.