

Re: ADAM schema design

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-09/msg00951

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 20 Sep 2007 13:27:16 -0500
-

I've never played with groupOfNames, but I thought I'd point out that ADAM groups are not Windows security principals and have no effect on Windows security at all. They are security principals in ADAM only (so they can be used in ADAM ACLs and it will understand them).

One possible advantage of using group instead of groupOfNames is that you might be able to get nested group membership via tokenGroups. I'm not sure if groupOfNames supports that. If group membership will be nested, that is a handy convenience feature as you would not have to recursively expand through memberOf (ADAM will basically do it for you).

I'm not sure if putting millions of users in a group will work. I've never heard of anyone trying to do that at that scale. I think you might be better off building some sort of query-based group management function where you set attributes on the user to indicate their group memberships and determine membership dynamically (like the feature provided by the MS AzMan framework). However, you could certainly try it and see.

Note that if you have more than 1500 members in a group, you'll need to use range retrieval techniques to expand the membership (reading member on the group object) if you ever need to do that.

Best of luck!

Joe K.

Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

<amol4321@xxxxxxxx> wrote in message
news:1190301118.076596.311360@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I'm really impressed to see the discussions on group / groupOfNames / groupOfUniqueNames on this forum.

This is my first post in here and would really appreciate if you could respond to it with your guidance.

Re: ADAM schema design

We need to use ADAM as the WMM store for WebSphere Portal Server 6.0 which would essentially use ADAM for user authorization based on the group memberships. we have decided to use "groupOfNames" as we purely want to use these objects as application/functional groups and not windows sec principles.

I'm looking your guidance on the following scenario:

Where we are expected to have million+ users in a single group; which means the million DN entries in "member" attribute of group object

- Firstly how is it going to affect the user authorization calls made from portal to ADAM? (I believe, it should not as it should ideally lookup for user object and return the "memberOf" list back to the portal") but I would appreciate your thought on this.
- Secondly, how does this impact the group management functions where I need to add / delete any users from this large group?

Amol.