

## Re: ADAM : Beginner and need help

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-12/msg00586](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg00586)

---

- *From:* "John Fly" <[JohnFlyTn@xxxxxxx](mailto:JohnFlyTn@xxxxxxx)>
  - *Date:* 7 Dec 2006 06:15:03 -0800
- 

Joe,

Thank you for your helpful reply. I wish I had stated earlier that I'm going to have to implement this solution for JAVA projects as well.

I'm going to look at Authorization Manager, thank you for the tip.

If I wanted to just set something very basic up in ADAM though could I have a structure like this(and have it make sense):

Users belong to Groups which belong to Permissions...

This would let me tie a user to a group with an easy LDAP query for memberOf, then check those groups memberOf attribute for permissions(which are really just groups themselves).

Does this make any sense?

Joe Kaplan wrote:

You can definitely do this with ADAM if you want. ADAM makes a pretty good store for users as it has nice support for objects that contain passwords and a reasonable way to authenticate with that password using and LDAP bind. ADAM can also support lots of password policy features that Windows supports like length, history and complexity requirements and provide account lockout if you want it.

ADAM also has support for groups and you can put whatever type of object you want in it.

To create some sort of support for an abstract concept like a "permission", you'd probably want to consider extending the schema to support something like that. LDAP schema is different from what you are used to with SQL (assuming you know SQL, which most application designer people do these

Re: ADAM : Beginner and need help

days), but it isn't too bad. Everything is just classes and attributes. It would probably be good to do some reading to find out more about this though. Extending the ADAM schema takes a bit more effort than changing the schema of a SQL database and is far more permanent than SQL, so it is a good idea to do a little more planning.

One thing you might want to consider is looking at Microsoft's application authorization framework (called Authorization Manager or AzMan). It actually has very strong support for role based security and has a very useful programming concept called an "operation", which is a granular unit that you use to apply security to what your application does. AzMan maps operations to tasks, tasks to roles and then roles into security principals, which are users and groups. Those can come from AD or ADAM.

I think you might be happier trying to apply AzMan to your programming problem than to reinvent the wheel (although maybe not :)).

Best of luck. Start doing some Google searches to learn more.

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>  
---

"John Fly" <JohnFlyTn@xxxxxxx> wrote in message  
<news:1165432705.333002.192400@xx>

Hello,

I've been playing with ADAM for about 3–4 days now, I'm trying to see if we can use it for user management for a number of software applications. I am mostly needing to store (Users, Groups, Permissions)

i.e A \*User\* is a member of one or more \*Groups\*. A \*Group\* is a set of one or more \*Permissions\*. A \*Permission\* might be "View open orders"

Is this a correct use of ADAM?

if so...

I have been able to setup ADAM on windows server 2003 R2, and have created an application partition.

Within the partition I have created a few users, and made these users member of the built–in Roles(Administrators, Users)

Re: ADAM : Beginner and need help

ISSUE:

I am not certain how to progress from here. In what way can I configure ADAM to best express my data in terms of Users/Groups/Permissions?

Where might I find some tutorials / examples or similar material for setting up ADAM in such a way?