

Re: Anonymous LDAP Access Problem

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-04/msg01273

- *From:* JayMG <JayMG@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 25 Apr 2006 05:26:02 -0700
-

Hi Joe,

Just got back into this after working on something else....

I need to authenticate using LDAP and I still am having some problems. I don't know if you may be able to help?

I've successfully managed to bind anonymously using openDSObject using the following :

```
Set oUser =  
oDSP.OpenDSObject(sRoot,vbNullString,vbNullString,ADS_SERVER_BIND AND  
ADS_NO_AUTHENTICATION)
```

Where sRoot is [LDAP://myServer/RootDSE](#)

I can now iterate through the attributes in oUser and print them out. This is of course the attributes at the root of our AD.

I now can't work out how to now do a search further down the tree once I'm bound to get information on other attributes not in the root.

Do you have any ideas on how to do this?

I will be able to do it as AD has been opened up for anonymous access.

The only examples I've managed to find are using ADODB Connection and Command objects to query. This doesn't seem to work as I need to maintain the anonymous bind and not set up a new connection.

I may be getting really confused now so I hope this makes sense.

Any ideas or help would be really appreciated.

Thanks,

Jason.

Re: Anonymous LDAP Access Problem

"Joe Kaplan (MVP – ADSI)" wrote:

It doesn't sound like you are accessing AD anonymously. It sounds like your ADSI code is authenticating with the current Windows user's credentials, which works when that is a domain account, but does not when that account is a local machine account.

AD in 2003 doesn't actually allow anonymous searches at all, so if you were to try that, it would probably not work. Doing anonymous auth requires using empty strings for your credentials in OpenDsObject and passing in the "anonymous" authentication flag.

It might be easier if you just enabled basic authentication in IIS rather than trying to do your own authentication in ADSI. That would immediately fix your problem here.

Another thing to consider is that you don't need the user's DN to authenticate them. Simply binding to RootDSE with their credentials will authenticate them. The only reason to get their DN is if you need to look up some additional information for them.

Joe K.

"JayMG" <JayMG@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:BB51272C-1BB4-46B0-B415-24B71B53730D@xxxxxxxxxxxxxxxxxxxxx

Hi,

I have an ASP application that I am using to authenticate users. The application takes a unique user id and searches LDAP anonymously to return the ADSPATH for the id. I then go back and authenticate the user using the ADSPATH and their password.

The problem is that the LDAP anonymous access search only works if I configure the anonymous account for my website (via IIS Manager) to a domain account. If I set it as a local IUSR account I cannot connect.

I spoke to the guys that administer AD here and they said that anonymous access should allow anyone to access LDAP and search to retrieve "allowed" attribute which is confusing me.

Can anyone confirm the default behaviour of anonymous access to LDAP? (i.e would I have to run my website with a domain account? or should it not matter?).

Re: Anonymous LDAP Access Problem

Many thanks,

Jay.