

Re: LDAP query failing

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-01/msg01900

- *From:* "Lee Flight" <lef@xxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 28 Jan 2006 18:20:37 -0000
-

Hi

you will need to ask your AD admins what attribute being used for logon is (e.g. CN) and then modify your search to look for that if it is not (the same as) sAMAccountName.

Lee Flight

"kevinL" <kevinL@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:67465DCA-E5D4-4728-AE92-DE472855FDA3@xxxxxxxxxxxxxxxxxxxx>
> Thanks, I'll try those suggestions.

>

> All the users and groups are in the default Users container in the one domain in the forest.

>

> Any suggestions for options other than sAMAccountName to allow users to use the one word user name they are accustomed to using to logon = "user logon name."

>

> KevinL

>

>

>

> "Lee Flight" wrote:

>

>> Hi

>>

>> you need to speak to your AD admins and find a good search base to be using in your LDAP URL; you need to find where the user accounts are rooted.

>>

>> Also your search base format

>>

>> cn=users,dc=adsdnsname

>>

>> needs to be a distinguishedName so the leading part of the URL is:

>>

Re: LDAP query failing

>> ldap://myaddomain.com:389/cn=user.dc=myaddomain.dc=com
>>
>> With mod_auth_ldap you will need an AD account that you can use to run
>> the search. You will also need some discipline on how the user accounts
>> are searched for if sAMAccountName is what the user will be entering
>> that's
>> fine but if variations in the input e.g. userPrincipalName are likely you
>> will
>> probably need to parse those into sAMAccountNames or vice versa, this
>> could be tricky in a multi-domain environment and might need a global
>> catalog
>> search (your AD admins should be able to advise).
>>
>> A further thing that you will want to do is to run the LDAP connection
>> over
>> SSL so that the usernames and passwords that are presented for binding
>> do not pass over the network in cleartext. In the auth_ldap conf file you
>> can have a pointer to certificate store IIRC.
>>
>> If you google you should find plenty of mod_auth_ldap examples for
>> running
>> against
>> AD (and ADAM), it's quite widely used.
>>
>> Lee Flight
>>
>> "kevinL" <kevinL@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:DE9FFEE4-C12B-4E27-8C3E-E604C854CAFC@xxxxxxxxxxxxxxxxxxxx
>> > My organization is really beginning to see the value of AD as an
>> > enterprise
>> > directory and I want to encourage that.
>> >
>> > We make good use of IIS for a variety of applications but our intranet
>> > runs
>> > on Apache, v 2.0.52. Users provide user names and passwords to access
>> > various pages on the intranet. I'd like to have Apache
>> > authenticate/authorize against our 2003 functional level domain ldap
>> > for
>> > user
>> > name and pw hash as well as group membership authorization. We already
>> > have
>> > our Unix servers authenticating against our AD for logins.
>> >
>> > I am attempting to use an Apache module called mod_auth_ldap for our
>> > intranet auth/auth.
>> >
>> > The question:
>> >
>> > An ldap query to:
>> >
>> > ldap://adnsname:389/cn=users.dc=adnsname.?sAMAccountName?sub?(objectClass=user)

Re: LDAP query failing

>>>
>>> returns:
>>>
>>> "dap_search_ext_s() for user failed"
>>>
>>> Perhaps, the query is not landing at the right place in the LDAP
>>> structure?
>>> I'd like to query against their logon name, userprincipalname or
>>> samaccountname.
>>>
>>> 1)Any suggestions would be appreciated.
>>>
>>> 2)Does anyone know where I could find a graphical representation of the
>>> default LDAP structure of a 2003 AD? Trying to extrapolate from the
>>> detailed
>>> tools like ldp or dsquery is daunting?
>>>
>>
>>
>>

• **Follow-Ups:**

- ◆ **[Re: LDAP query failing](#)**
◇ From: kevinL

• **References:**

- ◆ **[Re: LDAP query failing](#)**
◇ From: Lee Flight
- ◆ **[Re: LDAP query failing](#)**
◇ From: kevinL

- Prev by Date: **[Re: Windows 2000 to Windows 2003 AD migration](#)**
- Next by Date: **[Re: Group Policy – Shutdown/Startup Scripts Question](#)**
- Previous by thread: **[Re: LDAP query failing](#)**
- Next by thread: **[Re: LDAP query failing](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**