

Re: Using Ldapsearch to find things in the active directory

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01433

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 18 Jan 2007 11:05:01 -0600
-

I'd ask them for the errors they are getting. I'm guessing OpenSSL is in the mix on the client end and there should be some sort of log somewhere (or something you can turn on) that will say why it is failing.

You could also look for schannel errors in the system event log on your DC, but the error is probably on their side.

Make sure they trust the certificates you are using. That is a common cause of SSL server auth failure.

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>

--

"Sabo, Eric" <sabo_e@xxxxxxx> wrote in message
<news:C2ED8F6F-9232-42E9-8F19-BB0899003D2F@xxxxxxxxxxxxxxxxxxxx>

Joe,

I have installed the SSL certificates on my server, the only I have put two names in the certificate (DC name and an DNS name), Microsoft helped me with this. We can use ldp.exe to connect to both names correctly.

but the vendor is saying that it does not work. Through our firewall we enabled SSL (port 636) and they are hitting the hole correctly.

At this point, it is a blaming game. I just want to make sure that my active directory is setup correctly. Is there anything else I might have missed?

Re: Using ldapsearch to find things in the active directory

"Joe Kaplan" wrote:

I generally agree with this (using Kerb where possible), but in some cases LDAP auth must be accomodated. In that case, make sure you are using SSL/LDAP exclusively with these apps as there is a very high likelihood they will be using LDAP simple bind for authentication and that is not secure. It must be secured at the protocol level with SSL (or IPSEC).

In my experience, LDAP auth against AD is pretty common, especially in IT scenarios that must accomodate a wide variety of platforms.

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>

--

"Tomasz Onyszko" <T.onyszko_nospam_@xxxxxx> wrote in message
<news:eaoarOpOHHA.4604@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Sabo wrote:

I forgot to mention we are using an SSL connection to our LDAP server.

This is good practice – however if You want to use AD to authenticate users on linux \ unix You should take a look at Kerberos modules available for these platforms

--

Tomasz Onyszko

<http://www.w2k.pl/> – (PL)

<http://blogs.dirteam.com/blogs/tomek/> – (EN)