

Re: Non-Administrator users Can't do LDAP bind to AD

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-04/msg01153

- *From:* "Joe Kaplan \ (MVP – ADSI)" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 22 Apr 2006 14:18:26 -0500
-

Ah, I see what you are doing. In this case simple bind is your only good option is simple bind as it is probably the only lowest common denominator you have available. Apps using non-Windows LDAP stacks are the primary reason why you would ever want/need LDAP simple bind. As long as you are planning to use SSL/LDAP, you'll be fine.

I'd still suggest using ldp.exe for your tests/verifications. It is much easier to do exploratory stuff with it than using ldifde, which is really intended for doing import/export stuff. LDP can easily tell you all of the default partition info as well.

I also have a bias towards LDP as I use it all the time (3 instances open as we speak :)). I'm a programmer more than an infrastructure guy by a big margin though, so itake it for what its worth. Whatever works for you is what is most important.

Joe K.

"ohaya" <ohaya@xxxxxxx> wrote in message news:444A6A8F.864F572@xxxxxxxxxxx

Joe,

P.S. So you don't think that I was ignoring your comments about SSPI :)...

I am using this testing with ldifde and simple bind just to check that I can access the AD successfully via LDAP, and to verify the baseDN, etc.

I have an application that we'll be using, so once I get things working with ldifde, I know what to set the config parameters for my program to. My app, which will eventually be running on a Solaris box, supports both simple, clear binds, and simple, SSL binds, so the plan is to move to SSL-protected connection once we have checked everything out.

I think that it was a good thing that we took this approach, because if we do have a problem with the LDAP simple bind, hopefully this'll make it easier to pinpoint the cause before we move to using the app.

Re: Non-Administrator users Can't do LDAP bind to AD

Jim

ohaya wrote:

Joe,

I'll give your suggestions a try when I get a chance to get into the lab.

Thanks,
Jim

"Joe Kaplan (MVP – ADSI)" wrote:

I'm not sure what was wrong, but it could have been something as simple as an incorrect username or password specified. For example, this DN for the user is definitely wrong:

```
dc=test1,cn=users,cn=mydomain,dn=com
```

I'm guessing you just mistyped that, but I thought I'd point that out.

In any event, I'd check for bind failures with ldp.exe first. You also need to be certain that test1 was enabled, etc. LDP (and possibly AD U&C) are more useful for troubleshooting bind failures than ldifde.

I also really really recommend against using LDAP simple binds with AD. There is no reason to use them as AD supports SSPI based auth (even with credentials) and simple binds are a security risk (unless you combine with SSL). I realize this is just a test lab and all, but they are bad habit.

Note that if you do use SSPI auth, you can't use the DN as a

Re: Non-Administrator users Can't do LDAP bind to AD

username
syntax. You can use the NT name (domain\user) or UPN or
just the
username
though. AD also supports NT name and UPN for simple
binds, so I tend
to
recommend people use those 2 user name syntaxes with AD
to get the best
possible compatibility.

Best of luck,

Joe K.

"ohaya" <ohaya@xxxxxxx> wrote in message
<news:44497168.7EAAF6D9@xxxxxxxxxxx>

Joe,

Thanks for the suggestions.

The Win2K3 instance I mentioned in my
original post is in our lab,
and I
don't know for sure what "baseline" they
installed, so I'm not sure
if
that machine was locked down in any way.

So, I'm in the process of doing a clean install
of Win2K3 now, and
I'll
try to do the same test I did in the lab to see
if I have the problem
again.

If I do run into the problem, I'll try ldap as
you suggested, and I'll
also try to post details.

If I DON'T run into the problem, I still need
to figure out WHAT is
causing the ldifde from working in the lab,
so I guess in the
meantime,
while I wait for the installation to get done, I
am still wondering
what
could be causing the ldifde failure.

FYI, I was doing a simple basic ldifde

Re: Non-Administrator users Can't do LDAP bind to AD

export. Something like:

```
ldifde -f foo -d "dc=mydomain,dc=com" -a  
"dc=test1,cn=users,cn=mydomain,dn=com"  
*
```

ldifde was successful if I made user "test1" a member of the "Administrators" group. If I removed "test1" from the "Administrators" group, the ldifde would fail.

Will post back in a bit...

Thanks again,
Jim

"Joe Kaplan (MVP - ADSI)" wrote:

Are you sure it is the bind that is failing and not some other operation?
Any user with a valid password who is not expired, disabled, locked out, etc. should be able to do an LDAP simple (or preferably secure) bind.
Try it with ldp.exe.

You might also consider providing an example of what you were doing.

Joe K.

"ohaya"

<ohaya@xxxxxxxx> wrote
in message

news:1145639715.954223.239270@xx

Re: Non-Administrator users Can't do LDAP bind to AD

Hi,

I have a
Win2K3
Server with
AD. I am
trying to do
an LDAP
simple
bind
and am
testing
using ldifde.

I created a
new user
"test1" in
ADUC,
which is a
member of
Domain
Users, but
when I try
to use ldifde
with this
user using a
simple
bind,
I am getting
a failure.

If I make
the "test1"
user a
member of
Administrators,
the
ldifde/bind
works.

What do I
need to do
so that
"test1" can
successfully
do the
LDAP
bind?

Thanks,
Jim

Re: Non-Administrator users Can't do LDAP bind to AD