

Re: LDP client authentication fails

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-05/msg00167

- *From:* Romil Shah <RomilShah@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 3 May 2007 05:21:02 -0700
-

Thanks for your suggestions...

This is something I tried ...

I modified the schannel event log value to 7 so as to get all the details.

This is what I get if LDAP server is configured in serverclient authentication mode.

Event Type: Warning

Event Source: Schannel

Event Category: None

Event ID: 36875

Date: 5/3/2007

Time: 4:50:41 PM

User: N/A

Computer: LDUKE

Description:

The remote server has requested SSL client authentication, but no suitable client certificate could be found. An anonymous connection will be attempted. This SSL connection request may succeed or fail, depending on the server's policy settings.

I have copied the personal certificate as follows:

mmc -> Add/Remove Snap in -> Add -> certificate

Added certificate under "My user account" and "Computer account" under personal tab.

But even after all this I get the error mentioned above on connection to server using LDP.exe

As I mentioned earlier

" I am using Windows 2003 with SP1 installed.

I found that in Windows 2000 SP4 a bug on similar line is fixed . (811288)

Is this bug fixed in windows 2003 with SP1 installed ? "

- 1) is this a problem in 2003 sp1 ?
- 2) Or I am adding the personal certificate in wrong place .

Re: LDP client authentication fails

Appreciate your help in this regard.

–Romil Shah

"Paul Bergson [MVP–DS]" wrote:

Thanks I will let him know.

—

Paul Bergson
MVP – Directory Services
MCT, MCSE, MCSA, Security+, BS CSci
2003, 2000 (Early Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup
This posting is provided "AS IS" with no warranties, and confers no rights.

"Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:eKywdbOiHHA.680@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Client cert authentication in AD/LDAP is supposedly supported, but it is also undocumented black magic as far as I'm concerned. We don't have much detail on this in our book. Supposedly ADAM also allows you to do client cert authentication for Windows users, but I have no experience with that either.

A few years ago, someone at MS got this piece of feedback and said they were working on some docs to clarify how client cert auth works with LDAP binds. However, I don't think this document has seen the light of day yet. Very few people ask about it, so it isn't a hugely popular subject.

Thanks for the kind words on the book. Please tell you dev guy that if he has any questions, he's welcome to follow in one of the newsgroups or on the book's website: www.directoryprogramming.net. I hope you get a chance to play sometime as well. One of the nice things about our book is that even though it doesn't address PowerShell directly, everything you learn in there about .NET LDAP programming is applicable to PowerShell, so it probably makes the best detailed tutorial out there on how to actually do the LDAP stuff.

Joe K.

—

Joe Kaplan–MS MVP Directory Services Programming
Co–author of "The .NET Developer's Guide to Directory Services Programming"

Re: LDP client authentication fails

<http://www.directoryprogramming.net>

"Paul Bergson [MVP-DS]" <pbergson@xxxxxxxxxxxxxxxxxxxx> wrote in message

<news:%23ZZvMDOiHHA.5044@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

That surprises me, but is good to know.

Picked up Ryan's and your book the other day. I have a guy writing some AD code to create users and he loves the details you two have provided.

Hopefully this will get him over the hump. He was having some problems figuring some of this out. I wish I had the time to do it, but I don't always get to play.

Paul Bergson
MVP – Directory Services
MCT, MCSE, MCSA, Security+, BS CSci
2003, 2000 (Early Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup
This posting is provided "AS IS" with no warranties, and confers no rights.

"Joe Kaplan"
<joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:OgzK%23jNiHHA.4228@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Actually, AD does support client certificate authentication for binding and this can be done with ldap. It isn't well documented though. As long as the client certificate is available and SSL is being negotiated, the client certificate can be used. In general, the client certificate should be the "my" store for the current user and must be a certificate that is trusted by the server.

Re: LDP client authentication fails

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>

--

"Paul Bergson [MVP-DS]"
<pbergson@xxxxxxxxxxxxxxxxxxxx> wrote in
message
<news:%23hO8tMiHHA.3512@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Inline

--

Paul Bergson
MVP - Directory Services
MCT, MCSE, MCSA,
Security+, BS CSci
2003, 2000 (Early
Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any
questions should be posted
in the NewsGroup
This posting is provided
"AS IS" with no warranties,
and confers no
rights.

"Romil Shah"
<RomilShah@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
<news:8272DF53-420B-4B42-939E-1141BAC93344@xxxxxxxxxxxxxxxxxxxx>

Hi Paul,
You are
right that
we need to
copy the
Root CA to
Trusted
Root
Certificate
Authority
store. I did

Re: LDP client authentication fails

this , but as
per the main
query I had
,does
Active
directory
client
ldp.exe
support
client
authentication?"

I am not positive but I
would say that ldp doesn not
support client
authentication.

Any idea as
to where to
store the
personal
certificate
of ldp.exe
client .
I dont find
any option
in the
ldp.exe tool.
So now the
question
comes as to
whether
ldp.exe AD
client
supports
client
authentication
. If not then
server can
never
authenticate
the client.

To store the client cert just
double click on the cert and
import it.
Or open up IE, Select Tools,

Re: LDP client authentication fails

Internet Options, Content
tab and click on
certificates and import
from there. This will add the
work station
cert for you, but I don't see
this working with LDP, but
I could be
wrong.

As LDAP
server is not
receiving
any
certificate
from client
side for
authentication
so I think
ldp.exe is
not
supporting
client
authentication

.
But not sure
if I am right
on this ..
Any idea ?

You could use ipsec and
have your machine
authenticate to the server.

Thanks.
Romil Shah

"Paul
Bergson
[MVP-DS]"

Re: LDP client authentication fails

wrote:

When
you
say
you
have
copied
the
personal
certificate
of
the
server
into
the
Trusted
Root
Certificates
Authority,
I
am
unclear
as
to
what
you
mean.
What
you
should
have
done
is
copy
the
Root
CA
of
the
server
certificate
into
the
clients
Trusted
Root
Certificate
Authority
Store.

Re: LDP client authentication fails

Does
the
client
also
have
a
cert
and
have
you
provided
the
server
with
the
clients
Root
CA
and
placed
that
in
its
store?

The
two
need
to
trust
one
another's
certificates
before
communications
will
occur.

--
Paul
Bergson
MVP
-
Directory
Services
MCT,
MCSE,
MCSA,
Security+,
BS
CSci

Re: LDP client authentication fails

2003,
2000
(Early
Achiever),
NT

<http://www.pbbergs.com>

Please
no
e-mails,
any
questions
should
be
posted
in
the
NewsGroup
This
posting
is
provided
"AS
IS"
with
no
warranties,
and
confers
no
rights.

"Romil
Shah"
<Romil
Shah@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote
in
message
<news:E46868D3-9D30-48F0-90F3-DA9B716E0F2C@xxx>

Hello,

I
am
using
LDP.exe
as
a
client

Re: LDP client authentication fails

to
communicate
with
LDAP
server.
LDAP
server
is
configured
to
use
SSL
with
client
server
authentication
.

I
have
copied
the
personal
certificate
of
server
into
the
Trusted
Root
Certificate
Authoroties.

I
found
that
ldp.exe
fails
to
connect
to
server.
SSL
handshaking
fails
.

The
queries
that
I

Re: LDP client authentication fails

have
are
as
follows:
1)
Does
LDP.exe
authenticates
to
server
(
client
authentication
is
supported
?
)
I
am
using
Windows
2003
with
SP1
installed.
I
found
that
in
Windows
2000
SP4
a
bug
on
similar
line
is
fixed
.
(811288
)
Is
this
bug
fixed
in
windows
2003
with
SP1

Re: LDP client authentication fails

installed
?

2)
If
client
authentication
is
supported
then
which
personal
certificate
does
ldp.exe
send
to
server
for
authentication
and
where
is
the
personal
certificate
stored
on
windows
?

Looking
forward
for
your
suggestions

.

Thanks,
Romil
Shah

Re: LDP client authentication fails