

Re: Enable LDAP over SSL

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-08/msg00950

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 21 Aug 2007 10:08:13 -0500
-

It doesn't sound like you have a private key associated with that certificate then. That would be your primary problem.

How did you request the certificate? Was it requested on the domain controller machine? If there is an outstanding certificate request (which would have a private key associated with it), you should be able to associate the request with the certificate that was given back to you by the CA and then get this working.

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>

—
"DavidL" <DavidL@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:68CFAF43-0BA2-4574-82AB-1B9698493038@xxxxxxxxxxxxxxxxxxxxx

I've looked on every tab after double clicking the certificate under "personal".

I don't see private key anywhere.

I was delivered were .crt and in text format in an email.

"Joe Kaplan" wrote:

On the DC, does the DC certificate say that it has a private key associated with it? It will say so at the bottom of the certificate property page when you open it up. If it does not have a private key associated with it, it will not work.

If there is no private key, then the method you used to install the certificate must not have worked. Do you have a p12 or pfx file for the certificate? How was it delivered to you?

Re: Enable LDAP over SSL

Also, is the subject name on the certificate the DNS name of the domain controller?

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>
—

"DavidL" <DavidL@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:2BD020D7-7F3E-4CFE-9177-DB31AEE3CFA7@xxxxxxxxxxxxxxxxxxxx>

If I look at the certificate with the certificate snap—in while
logged
on
to
the DC, they both say "This certificate is OK."

"DavidL" wrote:

Thanks for your efforts...
Answers in line..

"Joe Kaplan" wrote:

Ok, so you don't have a
valid certificate installed.

A few things:

The cert must be in the
personal container of the
local machine
store

It is

the subject name on the cert
must match the DNS name
of the DC

I think it is.

The cert must have the
server authentication EKU

Re: Enable LDAP over SSL

I see that checkmarked.

The cert must have a private
key (the certificate property
pages
will
tell
you if it does)

It says Public Key. (How do I change that?)

The cert must say that it is
valid (the full chain must be
valid and
the
dates must be valid)

I see this "This root certificate appears to be
trusted by the remote
computer. To ensure this root certificate is
valid on the remote
computer,
verify this root certificate on that computer."
And this "This certificate is OK."

If any of those are not true,
then you either didn't get a
proper
certificate from the CA you
used or you did not install
something
properly.

You can check this by
opening up the certificates
mmc snap-in and
checking.

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>

--

Re: Enable LDAP over SSL

"DavidL"

<DavidL@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:4DC6D7E8-A58B-457F-9E03-8346AE209AE5@xxxxxxxxxxxxxxxxxxxx

OK.... that
gives me
more to
chew on.
I see this in
the system
log.
Event Type:
Warning
Event
Source:
Schannel
Event
Category:
None
Event ID:
36872
Date:
8/20/2007
Time:
3:46:18 PM
User: N/A
Computer:
Description:
No suitable
default
server
credential
exists on
this system.
This
will
prevent
server
applications
that expect
to make use
of the
system
default
credentials
from
accepting
SSL
connections.
An example

Re: Enable LDAP over SSL

of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.

and this in the directory service log

Event Type:
Information
Event
Source:
NTDS
LDAP
Event
Category:
LDAP
Interface
Event ID:
1220
Date:
8/16/2007
Time:
3:51:10 PM
User: N/A
Computer:
Description:
LDAP over
Secure
Sockets
Layer (SSL)
will be
unavailable
at this
time
because the
server was

Re: Enable LDAP over SSL

unable to
obtain a
certificate.

"Joe
Kaplan"
wrote:

You
will
need
the
full
cert
chain
on
the
DCs,
but
you
should
not
need
the
full
chain
on
the
client
as
AD
should
provide
the
whole
chain
to
the
client
during
the
SSL
negotiation.

There
are
usually
useful
error
messages

Re: Enable LDAP over SSL

in
the
system
event
log
from
schannel
and
sometimes
errors
from
LDAP
in
the
Directory
Service
log
when
there
are
SSL
configuration
problems.

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

Re: Enable LDAP over SSL

in
message
news:u8NRwU34HHA.2312@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I
have
seen
this
fail
when
the
CA
cert
from
the
third
party
isn't
properly
imported
into
both
the
client
and
all
dc's
cert
stores.

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

<http://www.pbbergs.com>

Re: Enable LDAP over SSL

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.

"DavidL"
<DavidL@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote
in
message
news:E29AF6C3-FAE2-4BCD-AA1A-FBB5A3DA

I
followed
the
instructions
in
KB321051
to
install
a
certificate.
I
got
to
the
section
"Verifying
an
LDAPS
connection"

Re: Enable LDAP over SSL

and
cannot
connect
to
636
or
3269.
Error
<0x51>:
Fail
to
connect
389
works
fine.
I
don't
see
an
_ldap
entry
in
DNS.
The
domain
controller
I'm
working
with
has
no
IIS
and
our
network
has
no
CA

Re: Enable LDAP over SSL