

Re: Enable LDAP over SSL

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-08/msg00913

- *From:* DavidL <DavidL@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 20 Aug 2007 19:36:06 -0700
-

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 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 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.

Re: Enable LDAP over SSL

There are usually useful error messages 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 in message
<news:u8NRwU34HHA.2312@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

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>

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@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:E29AF6C3-FAE2-4BCD-AA1A-FBB5A3DA45A2@xxxxxxxxxxxxxxxxxxxx>

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