

# Re: ADAM SP1 on Win2K3 SP1

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-09/msg00228](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg00228)

---

- *From:* Bo Zhu <[ffkiller@xxxxxxxxxxxxxxxxxxxx](mailto:ffkiller@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 05 Sep 2006 12:21:28 +0800
- 

Hi Lee,

Finally I figured out the reason why I can't make SSL work for non-administrative ADAM service account.

To use a domain user account as the ADAM service account for SSL communication, I have to request server authentication certificate using that account. Only when a certificate is requested and installed with that account will a private key file be created in C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys folder. If the certificate is requested and installed using an administrator account, the private key file will be created in C:\Documents and Settings\Administrator\Application Data\Microsoft\Crypto\RSA\MachineKeys folder instead. However, granting the ADAM service account READ permission to private key in Administrator MachineKeys folder doesn't work.

So the lesson is always requesting certificates using non-administrative accounts with an option to export private key.

Btw, thanks for the help in my quest for SSL setup.

Bo Zhu

Lee Flight wrote:

Hi

I think you are correct about the lack of a private key that is a common problem in SSL setups.

It looks like you need to set permission on the new key for the ADAM service account. Did you copy the cert or move it. I usually run the certificates snap-in for both the source cert store and the ADAM instance cert store and cut from one and paste to the other.

Lee Flight

"Bo Zhu" <[ffkiller@xxxxxxxxxxxxxxxxxxxx](mailto:ffkiller@xxxxxxxxxxxxxxxxxxxx)> wrote in message [news:O4m3Mr9zGHA.720@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O4m3Mr9zGHA.720@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Re: ADAM SP1 on Win2K3 SP1

The previous message is from ADAM Instance event log, the Schannel event is:

The SSL server credential's certificate does not have a private key information property attached to it. This most often occurs when a certificate is backed up incorrectly and then later restored. This message can also indicate a certificate enrollment failure.

My general cryptography knowledge tells me only the account used to request an SSL certificate should have a private key attached to it. And since I didn't enable exporting private key when requesting the original server authentication certificate, I recreated another server authentication certificate with an option to export private key. Then I exported that certificate with private key and imported them to the domain user account's personal certificate store. Of course I also copied that new certificate to ADAM instance personal certificate store, granted domain user account full control to every file in MachineKeys folder and restarted ADAM instance.

Now i get a different error from Schannel event log:

A fatal error occurred when attempting to access the SSL server credential private key. The error code returned from the cryptographic module is 0x80090016.

I also noticed that files in C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys didn't seem to be modified when I looked at the timestamp. Instead one file in C:\Documents and Settings\Administrator\Application Data\Microsoft\Crypto\RSA\S-1-5-21-3225114411-2335338089-454612937-500 folder has an update timestamp corresponding to the time I recreated the certificate.

This SSL setup is driving me nuts.

Lee Flight wrote:

Hi

is that the message from the schannel provider or from the ADAM Instance event log? It's the Schannel message that's of most interest and if that is it then the certificate is not being found.

If you have matched all the requirements FQDN of the cert matches the ADAM server name, cert appropriate to server auth etc., as in the notes I linked to then you could try moving the cert into the cert store of the ADAM Instance service from its current

Re: ADAM SP1 on Win2K3 SP1

location  
(probably the Computer cert store in your case?).

Lee Flight

"Bo Zhu" <ffkiller@xxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:OpUyowazGHA.744@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OpUyowazGHA.744@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

The log message I got from Windows Event  
Log is:

LDAP over Secure Sockets Layer (SSL) will  
be unavailable at this time because the server  
was unable to obtain a certificate.

Additional Data

Error value:

8009030e No credentials are available in the  
security package

I did a search on Google and didn't find  
anything particularly useful.

-zhubo

Lee Flight wrote:

Hi

did you restart the ADAM  
service after you added the  
read permission  
for the key?  
If it still fails after a restart  
then try bumping the  
debugging level of  
the Schannel provider

<http://support.microsoft.com/?id=260729>

set it to 0x7 and then (1)  
restart the ADAM instance  
service and  
(2) attempt the SSL  
connection and see what  
Schannel logs in the

Re: ADAM SP1 on Win2K3 SP1

system event log.

On the general question, add  
the permissions to the key  
and  
then change the account  
with dsdbutil and then  
restart the service  
should be OK.

Lee Flight

"Bo Zhu"

<ffkiller@xxxxxxxxxxxxxxxxxxxx>

wrote in message

[news:eZwDwRPzGHA.3568@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eZwDwRPzGHA.3568@xxxxxxxxxxxxxxxxxxxxxxxx)

The  
problem  
remains  
after I  
granted  
Read  
permission  
of every file  
in  
MachineKeys  
folder to the  
domain  
user.  
ldp.exe still  
fails with  
the same  
error code  
0x51 Server  
Down,  
which  
doesn't  
make any  
sense.

Now I have  
a general  
question.  
Assuming  
SSL on  
ADAM is

Re: ADAM SP1 on Win2K3 SP1

working  
fine and i  
want to use  
another  
domain user  
account as  
the ADAM  
service  
account. Do  
i only need  
to grant that  
account  
READ  
permission  
to machine  
keys and  
use dsdbutil  
to change  
the ADAM  
service  
account? Or  
I have to go  
through the  
entire  
process  
starting  
from  
requesting  
certificate  
all over  
again to use  
the new  
domain user  
account as  
the ADAM  
service  
account?

Previously  
what I did  
was that I  
went  
through the  
entire SSL  
setup  
process  
while  
logged on  
as a domain  
admin, and  
subsequently

Re: ADAM SP1 on Win2K3 SP1

picked a  
normal  
domain user  
account to  
run ADAM.

Lee Flight  
wrote:

Hi

as  
you  
noted  
if  
running  
ADAM  
on  
a  
DC  
you  
should  
be  
using  
a  
standard  
doamin  
account  
not  
Network  
Service.

There  
are  
some  
notes  
on  
ADAM  
SSL  
configuration  
here:

<http://groups.google.co.uk/group/microsoft.public.windows.s>

In  
particular  
note  
that

Re: ADAM SP1 on Win2K3 SP1

you  
must  
set  
appropriate  
permissions  
on  
\*individual\*  
keys  
in  
Users\ApplicationData\Microsoft\Crypto\RSA\MachineKeys  
as  
the  
keys  
in  
that  
folder  
do  
not  
inherit  
permissions.

Lee  
Flight

"Bo  
Zhu"  
<ffkiller@xxxxxxxxxxxxxxxxxxxx>  
wrote  
in  
message  
[news:edYZ7XnyGHA.4104@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:edYZ7XnyGHA.4104@xxxxxxxxxxxxxxxxxxxxxxxx)

Okay,  
the  
second  
mystery  
is  
solved.  
I  
didn't  
use  
dsdbutil  
to  
change  
ADAM  
service  
account,

Re: ADAM SP1 on Win2K3 SP1

that's  
why  
I'm  
getting  
some  
JET  
DB  
related  
error.

The  
first  
problem  
remains  
there.

Bo  
Zhu  
wrote:

Hi,

I  
have  
two  
questions  
related  
to  
ADAM  
running  
on  
a  
domain  
controller.

1.  
SSL  
connection  
with  
non-administrative  
account  
I  
followed  
a  
pretty  
detailed  
step-by-step

Re: ADAM SP1 on Win2K3 SP1

guide  
(<http://www.oftedal.no/~erlend/?blogid=7>)  
on  
how  
to  
setup  
SSL  
certificate  
with  
ADAM,  
like  
generating  
a  
server  
authentication  
certificate,  
place  
the  
certificate  
in  
service  
account  
certificate  
store,  
granting  
read  
access  
to  
private  
key  
files,  
etc.  
But  
after  
all  
configuration  
steps  
were  
done,  
I  
was  
only  
able  
to  
connect  
to  
my  
ADAM  
instance  
through  
SSL

Re: ADAM SP1 on Win2K3 SP1

Re: ADAM SP1 on Win2K3 SP1

if  
ADAM  
is  
run  
by  
an  
Administrative  
account.  
If  
I  
run  
ADAM  
service  
with  
"NT  
Authority\Network  
Service",  
which  
is  
the  
default  
account  
selected  
during  
ADAM  
instance  
creation,  
ldp.exe  
always  
fail  
to  
connect  
with  
the  
following  
error  
message:

```
ld
=
ldap_sslinit("ffkillervm2k3.zb.encentuate.com",
50001,
1);
Error
0
=
ldap_set_option(hLdap,
LDAP_OPT_PROTOCOL_VERSION,
3);
Error
81
```

Re: ADAM SP1 on Win2K3 SP1

```
=  
ldap_connect(hLdap,  
NULL);  
Server  
error:  
<empty>  
Error  
<0x51>:  
Fail  
to  
connect  
to  
ffkillervm2k3.zb.encentuate.com.
```

I  
found  
something  
in  
one  
ADAM  
FAQ  
from  
Microsoft  
that  
says  
I  
can  
use  
"certutil  
-store  
my"  
command  
to  
see  
the  
file  
name  
of  
the  
private  
key  
whose  
Read  
permission  
should  
be  
granted  
to  
the  
service  
account

Re: ADAM SP1 on Win2K3 SP1

used  
to  
run  
ADAM  
service.  
But  
all  
I  
got  
for  
the  
"Key  
Container"  
attribute  
after  
running  
this  
command  
is  
the  
name  
of  
root  
CA  
certificate  
I  
generated  
earlier.  
I  
even  
granted  
Read  
permission  
of  
"C:\Documents  
and  
Settings\All  
Users\Application  
Data\Microsoft\Crypto\RSA\MachineKeys"  
folder  
and  
all  
sub-folders  
to  
"NT  
Authority\Network  
Service"  
account  
and  
still  
SSL

connection  
fails.

2.  
Running  
ADAM  
service  
with  
a  
domain  
user  
account  
ADAM  
Help  
states  
I  
should  
not  
run  
ADAM  
service  
with  
"NT  
AUTHORITY\NETWORK  
SERVICE"  
account  
if  
the  
instance  
is  
running  
on  
a  
domain  
controller.  
So  
I  
created  
a  
new  
domain  
user  
in  
my  
test  
AD  
and  
used  
that  
account

Re: ADAM SP1 on Win2K3 SP1

to  
run  
ADAM.  
I  
have  
also  
enabled  
"Log  
on  
as  
a  
service"  
and  
"Generate  
security  
audits"  
for  
the  
new  
domain  
user  
account  
in  
Default  
Domain  
Contollers  
Policy.  
Unfortunately  
I'm  
not  
able  
to  
start  
ADAM  
service  
with  
that  
new  
domain  
user  
account.

A  
quick  
examination  
of  
Windows  
events  
shows  
one  
error:

Active  
Directory  
could  
not  
be  
initialized.

The  
directory  
service  
cannot  
recover  
from  
this  
error.

User  
Action  
Restore  
the  
local  
directory  
service  
from  
backup  
media.

Additional  
Data  
Error  
value:  
-1032  
JET\_errFileAccessDenied,  
Cannot  
access  
file,  
the  
file  
is  
locked  
or  
in  
use

Any  
help  
is  
appreciated.

Re: ADAM SP1 on Win2K3 SP1

Best  
regards,

Bo  
Zhu