

Re: Create certificate with makecert for LDAPS on a DC ?

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-12/msg00061.html>

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 12 Dec 2007 09:43:10 -0600
-

Is this for a test environment? Self-signed certs are ok for dinking around, but they are almost never appropriate to be used for real.

Note that you can get a perfectly good publicly rooted SSL cert from many different places now for about \$20. It isn't a big deal.

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>

--

"bigstyle [MVP]" <news:mn.62d37d7cfd7a2c5e.70874@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

Finally it works !

I have deleted every certs then I have created them by using the command quoted below.

After a reboot of the DC, the LDAP over 636 is working fine !

Thank you

Hi,

I would like to use LDAPS on my DC.

I have already read this article :

<http://support.microsoft.com/default.aspx/kb/321051> ...

but I am not able to create my self-signed certificate with certreq as I dont have any CA in my domain to submit the "request.req" file.

1. So I tried to create my own certificate with makecert by using this command :

"makecert -r -pe -n "CN=FQDN_OF_DC.domain.local" -b 01/01/2000 -e

Re: Create certificate with makecert for LDAPS on a DC ?

```
01/01/2036 -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localMachine -sky  
exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12"
```

The certificate is created in Personal\Certificates (under Computer) but when I watch the certificate status, I have a warning saying : "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."

2. I have also tried to create a trusted root CA certificate by using this command :

```
"makecert -n "CN=TempCA" -r -sv TempCA.pvk TempCA.cer"
```

Then I have created a server certificate trusted by this "TempCA" by typing this command :

```
"makecert -sk PourDC -iv TempCA.pvk -n
```

```
"CN=FQDN_OF_DC.domain.local" -ic
```

```
TempCA.cer PourDC.cer -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localMachine  
-sky
```

```
exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12"
```

When I try to connect (locally)to my LDAPS using ldp.exe (port 636 but without SSL option marked) , I have an error "Error <0x51>: Fail to connect to FQDN_OF_DC.domain.local."

Do I need to install a CA only for my testing purpose ?

I think it is possible by using makecert and I would like to find how !

:D

Thank you

P.S: Sorry for my english

--

bigstyle
MVP Windows Server – Directory Services
MCSE 2000/2003 Security