

Re: failing to retrieve CRL from certificate server using new LDAP

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-08/msg00319.html>

- *From:* Mr555 <Mr555@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 30 Aug 2006 16:23:01 -0700
-

Hello S.Pidgorny

Once again thank you for your suggestion to my question.

we have 4 DC
2 running windows 2003
2 running windows 2000
Paul 192.168.1.2 is the Forest Root DC

Our CRL expire today. I tested again by specify the IP address of 192.168.1.2 "windows 2003 FSMO" and 192.168.1.4 "windows 2003 replicate DC" under our netscreen VPN server > certificate > LDAP server setting. it failing to retrieve a new CRL from the certificate sever using both 2003 LDAP server.

we have another window 2000 replicate DC Server it is call "Spoon. the ip address of spoon is 192.168.1.3, I specify the ip address of 192.168.1.3. on the certificate setting > LDAP on our netscreen VPN/ Firewall. the automatic CRL retrieve works.

after this test I suspect there may be some default security setting may have disallow Netscreen to communicate with our windows 2003. do you know or is there any setting i need to be aware of ?

Thank you

Mr555

"S. Pidgorny <MVP>" wrote:

Re: failing to retrieve CRL from certificate server using new LDAP

I'm not familiar with Netscreen gear and LDAP client of that but here's what I'd do:

1. Make CA publish new CRL into AD. If it's offline, bring it online and do that!
2. Using any LDAP client, check if CRL is in place on both new and old server.
3. Capture traffic between Netscreen and LDAP servers to see the requests and responses. Make sure you disable LDAP encryption.

That will allow to pinpoint the issue.

--

Svyatoslav Pidgorny, MS MVP – Security, MCSE

-- F1 is the key --

"Mr555" <Mr555@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:456DA499-8E8D-45F6-8DFD-AC258EABFD55@xxxxxxxxxxxxxxxxxxxx

Hello S. Pidgorny

I agreed with your comment, I thought I can specify any DC.

I have tried your suggestions previously it won't work. the CRL will automatically updates only if I put 192.168.1.1 under LDAP Server: settings

So you don't think there are any settings that may bind to our old DC "corp" server ? i need to specify on our new 2003DC

This is how I specify on our VPN netscreen 50 under certificate options >
CRL
settings

CRL Settings

URL Address:

<ldap:///CN=company1,CN=Paul,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Config>

LDAP Server: 192.168.1.1

Refresh Frequency: Daily

"S. Pidgorny <MVP>" wrote:

You should be able to use any domain controller and point the LDAP url

Re: failing to retrieve CRL from certificate server using new LDAP

accordingly, like:

ldap://192.168.1.2/CN=company1,CN=Paul,CN=CDP,CN=Public%20Key%20Services,CN=

--

Svyatoslav Pidgorny, MS MVP – Security, MCSE

-- F1 is the key --

"Mr555" <Mr555@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

news:A622E5A1-6E88-4693-A9BB-1D7A34A390DC@xxxxxxxxxxxxxxxxxxxx

Hello

Thank you so much for your input to my questions. I am new to certificate server, through I just enabled the certificate services will be OK. At the moment our VPN is operational. the only problem (serious problem) we are having is that it will only retrieve new CRL from the certificate server, if I specific the old LDAP server IP address which is 192.168.1.1 " corp server windows 2000" we are going to demote corp server soon, I got the feeling that some configuration is been done on corp server., possible I have to enable it on Paul Server 192.168.1.2 windows 2003. I am not sure what it is . so hopefully you will be able to help me with this. we are using netscreen 50 as our VPN server. under certificate options on our netscreen VPN server, a place where you have to specific the URL path, under the netscreen documentstions it saids I must copy it from the

Re: failing to retrieve CRL from certificate server using new LDAP

published
CRL locations "
URL=ldap:///CN=company1,CN=Paul,CN=CDP,CN=Public%20Key%20Services,CN
to that location, then I have specific the Ldap
ip address 192.168.1.1
to
work around

Thank you

Mr555

"S. Pidgorny <MVP>" wrote:

Which VPN server do you
use and how do you
configure it for CRL lookup
(if
applicable)?
What CDPs are defined in
the VPN client certificate
properties?
Not less important – what
CDPs are defined in the
VPN server
certificate?

==
Svyatoslav Pidgorny, MS
MVP – Security, MCSE
-- F1 is the key ==

"Mr555"
<Mr555@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
news:63E32FFE-E2B4-4477-B6B0-3895307DF3D3@xxxxxxxxxxxxxxxxxxxx

3 months
ago we
migrated to
windows
2003
Server.

We have
moved the
entire
FSMO role

Re: failing to retrieve CRL from certificate server using new LDAP

from our
old
windows
2000 server
"Corp"
to our new
windows
2003 Server
"Paul" Paul
is now the
forest root
of
our
network.
The ip
address of
Paul is
192.168.1.2

Few weeks
ago our
windows
2000
certificate
server
"Spoon"
die, we
decided
to
rebuild the
certificate
server to
windows
2003. The
new
certificate
server
is
now called
"Mugen"
and is
configured
as a
stand-alone
root CA
member
server.
The purpose
of this
certificate
server is to

Re: failing to retrieve CRL from certificate server using new LDAP

authenticate
VPN
connection
to
our network
and is
operate
together
with our
netscreen
VPN /
firewall.

15 days
ago, our
VPN /
firewall
failing to
retrieve
CRL from
certificate
server.
Therefore
VPN
connections
stop
working.

Under
extensive
investigation.
I have
discovered
we can only
make
our
VPN/firewall
to
automatically
obtain CRL
from the
certificate
server
"Mugen".
if we
specific the
old LDAP
server IP
address "
corp."
which is

Re: failing to retrieve CRL from certificate server using new LDAP

192.168.1.1.

if I enter the
ip address
of Paul
192.168.1.2
to the VPN/
firewall
certificate
settings, the
automatic
CRL
retrieve will
fail.

I have
checked
with the
firewall
support
team. They
said
netscreen
does
support
windows
2003
Server.
They
suspect I
have not
configured
our
certificate
server
correctly to
work under
"Paul"
LDAP
Server.

Questions:

Are there
any
configuration
or security
policy I
need to
configure
to

Re: failing to retrieve CRL from certificate server using new LDAP

allow
communication
between
LDAP
"Paul"
server and
certificate
server "
Mugen"?

I need to
specific
"Paul" as
the LDAP
server on
the VPN
setup
instead
of
corp.
Server.
please help

Thank you

Mr555