

Re: Remote site BDCs won't auth clients when T1 to AD 2003 is down LTLM?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-01/1061.html>

From: Richard McCall [MSFT] (richmcc_at_online.microsoft.com)

Date: 01/16/04

Date: Fri, 16 Jan 2004 08:43:38 -0500

Depending on what clients you have if you do not have additional W2K DCs then w2k and XP client will not revert to authentication from a NT4 DC if the only W2k\w2k3 DC is not available. You could have used the registry entry below to prevent that behavior until you had more w2k\w2k3 dc up. However at this point you have two options.

1. Make the registry change on the W2k\W2k3 DC and then use netdom to rejoin all the XP\W2k clients out and back into the domain.
2. Put a W2K DC at every site the you want authentication to continue if the WAN link is down.

284937 Windows 2000-Based Clients Connect Only to the Domain Controller That

<http://support.microsoft.com/?id=284937>

298713 How to Prevent Overloading on the First Domain Controller During Domain

<http://support.microsoft.com/?id=298713>

--

Richard McCall [MSFT]

"This posting is provided "AS IS" with no warranties, and confers no rights."

<Cappy@Aol.com> wrote in message news:5o0dnRXJQa293JrdRVn2jQ@giganews.com...

> (Sorry for Multiple Posts- Have Pitty, I'm Old)

> I am totally screwed, I think. I need some adult supervision for my next step at solving a problem.

> We did an in place upgrade from NT4 PDC to 2003 Server w/ Mixed/Hybrid Mode

> Active Directory. We took our PDC and upgraded it. We upgraded a second machine (BDC) and all seemed wonderful (DNS included). Now, due apparently

> to the structure of our domain, lack of through testing, and following

> Microsoft's directions to a tee, we are in a HUGE MESS!

> We have a main site which has our PDC emulator and several legacy BDCs. We

> have several remote sites that connect via to the main campus over speedy

> links. (You already know what I am going to say, right?) We have a BDP at

> each of the remote sites that have not been upgraded to 2000.

> Currently whenever we lose one of our T1 links overnight, in the morning

> nobody at the remote site can authenticate to the domain even though a

> domain controller (NT4BDC) is on the same subnet and replication

thought-out

> the domain is going perfectly. I have done several packet captures and it

microsoft.public.security: Re: Remote site BDCs won't auth clients when T1 to AD 2003 is down LTLM?

> looks as if the clients are ignoring the local domain control and wanting
> to
> authenticate themselves to an active directory box. It is as if they will
> not stand for NTLM authentication anymore having tasted the fruits of
> Kerberos. I have tried forcing the AD controller to do NTLM only- but that
> still didn't work. If I remove one of the computers from the domain and
> re-add it then it works if I force the AD to do NTLM. (this of course will
> not work if the machines are not able to get to the main campus in an
> outage
> situation.) I have tried flipping the machine's registry for NTLM to 1 but
> that didn't work either.
> Please, Please, Please HELP ME! Am I going to have to remove EVERY MACHINE
> IN THE ENTIRE ENTERPRISE FROM THE DOMAIN AND RE-ADD THEM??? If so, please
> let me know so I may kill myself.
> Your Old Hippy/ ex Cobol Programmer Friend.
> CappyClam