

Re: Domain unavailable for some logons

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-11/0052.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 11/05/05

Date: Fri, 4 Nov 2005 19:01:10 -0600

The info shown in the reports generated for netdiag contain all the info that is included in ipconfig /all. Your reports all look great in that the domain controllers and domain clients are configured correctly and communicating with each other [well at least after startup] . I believe the problem is your wireless network. What happens is that wireless network cards often do not initialize fast enough at startup to have network connectivity and contact a domain controller. One solution to fix the problem is to have the users that need to logon to the computer do so when it is connected to the network by cable. That should create a cached logon for that user and by default a domain computer can store 10 cached logons. This behavior is a security option controlled in Local Security Policy under local policies/security options – number of previous logons to cache. Once the user has a cached logon he can logon via the wireless network via the cached logon and then after the wireless network adapter initializes it will have network connectivity and the user will be able to use domain resources.

Beyond that you could contact the manufacturer of your wireless equipment and ask them if they have any solution which could be a driver upgrade or a registry change for the wireless adapter or you may be stuck with performance as is. There may be particular brand of wireless network adapters that work better in an Active Directory domain environment but I can't recommend any based on my experience. You might also want to post in the Active_directory newsgroup with a topic along the lines of "wireless domain user logon problems" to see if anyone there has any recommendations or experience with that problem. --- Steve

"zuke" <lgilmore@NO_SPAMrainbowgrocery.net> wrote in message news:u3Y166Z4FHA.700@TK2MSFTNGP15.phx.gbl...

> Hello,

>

> Here most of the requested logs. Any suggestion on producing a text file of the ipconfig/all output?

>

> Interestingly I can unjoin the wireless laptop from the domain and then join it again creating a new computer account with DNS entries. But then I cannot log onto the domain now, even with cached credentials. I can always log on using the NIC chip that runs the wire connection. Of course, I do not have both the wireless and the wired connection enabled at the same

> time.
>
> *It is interesting that there is enough connectivity with AD to delete or
> create a computer account wirelessly, but not enough to log on to the
> domain.*
>
> Thanks
> "Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message
> news:T-CdnfN527RKVPveRVn-gw@comcast.com...
>> *There is a problem with netdiag and that the kerberos error may not be of
>> any significance. It is OK to have a secure channel to any DC. If you
>> could
>> post the results of netdiag in a reply here of one of the domain
>> computers
>> where you can not logon as a domain user and also the results of netdiag
>> /test:kerberos /debug and netdiag /test:dsggetdc /debug. Also post
>> ipconfig
>> /all for each domain controller. --- Steve
>>
>>
>> "zuke" <lgilmore@NO_SPAMrainbowgrocery.net> wrote in message
>> news:uH5W0sn3FHA.2532@TK2MSFTNGP09.phx.gbl...
>>> Hello,
>>>
>>> So, I ran netdiag on the server, no problems.
>>>
>>> Then on the two machines (one wired; one wireless) hooked up to the
>>> Linksys netdiag returned a "failed" for [fatal] "Kerberos does not
>>> have
>>> a ticket for host..." All else passed. But these also say they have a
>>> secure channel, not to the PDC, but to the secondary DC.
>>>
>>> Is there any connection between Kerberos and joining the host to the AD
>>> domain?
>>>
>>> So, it appears I can go to the network from these hosts, but some data
>>> cannot come from the LAN to these hosts. I am using a backup software
>>> that also cannot find the host, whereas it could before.
>>>
>>> I have a lot of other machines that work fine logging on and off, so I
>>> doubt it is a DC config.
>>>
>>> Any suggestions?
>>> Regards,
>>> Zuke
>>>
>>>
>>> "Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message
>>> news:TsKdnezIoMamw_zeRVn-pw@comcast.com...
>>>> Hmm. Logon to that computer with a domain account that you can and run
>>>> the support tool netdiag on it to see if any problems are found with*

>>>> *dns,*
>>>> *dc discovery, domain membership, or trust/secure channel and post the*
>>>> *results in a reply here. Also run netdiag on the domain controller.*
>>>> *The*
>>>> *error message usually means there is a problem finding or contacting*
>>>> *the*
>>>> *domain controller. --- Steve*
>>>>
>>>>
>>>>
>>>> *"zuke" <lgilmore@NO_SPAMrainbowgrocery.net> wrote in message*
>>>> *news:OkNR6%23y2FHA.472@TK2MSFTNGP15.phx.gbl...*
>>>>> *I can ping the DC's FQDN from the laptop over the air.*
>>>>>
>>>>> *RE: logging on with cached credentials, I was guessing that too, but*
>>>>> *it*
>>>>> *is strange that one of the user logons that returns the "..domain*
>>>>> *unavailable" complaint has logged on to this machine many times over*
>>>>> *the*
>>>>> *wire and so also should have cached credentials.*
>>>>>
>>>>> *I have no DHCP servers and yes, the routers' DHCP has been disabled..*
>>>>>
>>>>> *My client hosts' preferred DNS server settings already point to my two*
>>>>> *DNS servers(one primary, the other a backup), and NOT to the ISP.*
>>>>>
>>>>> *Regards,*
>>>>> *Zuke*
>>>>>
>>>>> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message*
>>>>> *news:%23zj4zon2FHA.1396@TK2MSFTNGP15.phx.gbl...*
>>>>>> *You probably have a dns problem and the computer that you can not*
>>>>>> *logon*
>>>>>> *to with the domain account can not find the domain controller. My*
>>>>>> *guess*
>>>>>> *is that the reason you can logon with some accounts is because you*
>>>>>> *are*
>>>>>> *logging on with "cached" domain credentials which is enabled by*
>>>>>> *default. Try pinging the domain controller by it's fully qualified*
>>>>>> *domain name to see what happens, run the support tool netdiag on that*
>>>>>> *domain computer and the domain controller, and use Event Viewer to*
>>>>>> *check the logs on the domain computer and domain controller. The link*
>>>>>> *below shows how dns MUST be configured for an AD domain to work*
>>>>>> *correctly and NEVER configure any domain computer to use the IP*
>>>>>> *address*
>>>>>> *of an ISP dns server as a preferred dns server anywhere in the list.*
>>>>>> *You can however configure your domain controller/dns server to*
>>>>>> *forward*
>>>>>> *to your ISP dns server so that all domain computers can resolved*
>>>>>> *internet names as explained in the KB dns article. Make sure that*
>>>>>> *DHCP*

microsoft.public.win2000.security: Re: Domain unavailable for some logons

>>>>> is disabled on your router device so that only your domain controller
>>>>> is used for DHCP. You can use the command ipconfig /all on any
>>>>> computer
>>>>> to see the current IP configuration and what computer/device is
>>>>> acting
>>>>> as the DHCP server. You only need to configure your DHCP scope or
>>>>> manually configure computers with static IP addresses like your
>>>>> domain
>>>>> controller to use the IP of your router as the default gateway. ---
>>>>> Steve
>>>>>
>>>>>
>>>>>
>>>>> [tp://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B291382](http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B291382) ---
>>>>> AD dns FAQ.
>>>>> <http://support.microsoft.com/default.aspx?scid=kb;en-us:321708> ---
>>>>> Netdiag
>>>>> <http://support.microsoft.com/kb/301423/> --- how to install support
>>>>> tools
>>>>>
>>>>> "zuke" <lgilmore@NO_SPAMrainbowgrocery.net> wrote in message
>>>>> news:uT%23lJKn2FHA.3744@TK2MSFTNGP10.phx.gbl...
>>>>>> Hello,
>>>>>>
>>>>>> I've got a W2K AD network with static IP addresses all round. I use
>>>>>> just a couple logon accounts for most of the 25 PC's. I have a
>>>>>> couple
>>>>>> logons for individuals.
>>>>>>
>>>>>> I just set up a Linksys WRT54G wireless router/access point behind my
>>>>>> firewall. I set it up using WPA/AES, the network is bridged, not
>>>>>> routed (as in a gateway). I have, at the moment, just one laptop
>>>>>> with
>>>>>> wireless enabled, with an Atheros WiFi chip and using the Atheros
>>>>>> driver. I have physical connectivity. I can log onto the domain with
>>>>>> my Enterprise/Domain Admin account. I can log on with just one of my
>>>>>> Domain/User accounts.
>>>>>>
>>>>>> Other Domain/User accounts return the following message at the logon
>>>>>> prompt:
>>>>>> "This system cannot log you on now because the Domain "X" is not
>>>>>> available"
>>>>>>
>>>>>> But I can just enter my Domain/Admin logon account or the one
>>>>>> Domain/User account and it logs on, no error. If I use the incorrect
>>>>>> password I get the usual suggestion to "check my user name and
>>>>>> password".
>>>>>>
>>>>>> Any suggestions?
>>>>>>
>>>>>> Zuke

Re: Domain unavailable for some logons

microsoft.public.win2000.security: Re: Domain unavailable for some logons

>>>>>>>
>>>>>>
>>>>>>
>>>>>
>>>>>
>>>>
>>>>
>>>>
>>>
>>>
>>>
>>
>>
>>
>>
>
>
>