

Re: Authentication Failure

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-09/0064.html>

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 09/09/05

Date: Thu, 8 Sep 2005 20:29:02 -0500

You mention that you are using image installs which is fine but the imaging method/program ideally should have a way to make sure each computer gets a unique sid though I don't know if that would be related to your problem or not offhand. If you think that may be happening SysInternals makes a program that can change the sid for a computer. The fact that a domain administrator can logon also makes me suspect that there may be a problem with the domain computer contacting a global catalog server if the domain is in native mode since regular domain user logon in a native mode domain would require access to a global catalog server. Double check that only domain controllers for the domain are listed as preferred dns servers in the tcp/ip properties of the domain computers and that nslookup affirms such and can resolve domain names to CORRECT IP addresses including the domain controllers and domain itself as in mydomain.com and that the global catalog server can be pinged by its fully qualified domain name on a problem computer. I would also run netdiag and dcdiag on your domain controllers and verify that dns is configured correctly for your domain as per KB link below.

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B291382> ---- AD dns FAQ

If you happen to be using ipsec in your domain keep in mind that domain controllers must be exempt from ipsec negotiation for AH/ESP for traffic between domain members and domain controllers. A network trace showing the packet sequence for an authentication attempt from the host domain computer may also be helpful though non server operating systems do not have a built in packet sniffer like netmon though you can install a free one such as Ethereal. ---- Steve

"Sam Spade" <sams@not.real.actually.fake> wrote in message news:Xns96CB6CEC74AA2Samisnotactuallyreal@207.46.248.16...

> *Hi Steven,*

>

> *We're on the same wavelength - I'd already saved and cleared the logs.*

> *There is nothing showing in the event logs on the DC. I'm really*

> *confused! I'm going to re-image the two affected machines today (yes, a*

> *4th one has gone now!) then I'll turn on MORE auditing to see if I can*

> *discover what's causing this VERY annoying problem!*

>
> *Thanks for the advice so far....*
>
> *Sam.*
>
> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in*
> *news:OKm1\$H8sFHA.908@tk2msftngp13.phx.gbl:*
>
>> *This may be a longshot but next time try logging on as a local*
>> *administrator and clearing the security log. The reason being if you*
>> *have crashonauditfail security option enabled in the security policy*
>> *it could prevent any user other than a local administrator from*
>> *logging onto the computer when the security log becomes full but*
>> *usually the computer blue screens when this is enabled and the*
>> *security log becomes full. Also look in the security logs of your*
>> *domain controllers to see if any failed logon events are recorded for*
>> *those domain users that may provide more information. You would want*
>> *to make sure that auditing of "account logon" events and account*
>> *management are enabled in Domain Controller Security Policy and that*
>> *the security logs have been increased in size from default quite a bit*
>> *to say at least 20MB. --- Steve*
>>
>>
>> *"Sam Spade" <sams@not.real.actually.fake> wrote in message*
>> *news:Xns96CA9DF3C35F7Samisnotactuallyreal@207.46.248.16...*
>>> *Steven,*
>>>
>>> *Thanks for the reply. Netdiag shows no problems except no default*
>>> *gateway is defined – not a problem as all Internet traffic is forced*
>>> *through the ISA Server.*
>>>
>>> *I can log onto the affected workstations as Local Administrator _OR_*
>>> *as Domain administrator. As Domain Admin. I have full connectivity.*
>>>
>>> *I am perplexed. Any other suggestions?*
>>>
>>> *Sam.*
>>>
>>>
>>> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in*
>>> *news:#j8kGQ2sFHA.3088@TK2MSFTNGP12.phx.gbl:*
>>>
>>>> *Next time that happens see if a local administrator can logon to the*
>>>> *computer and then run the support tool netdiag on it to see if it*
>>>> *reports any problems with dns, dc discovery, kerberos, secure*
>>>> *channel/computer account, etc. Make sure your domain computers*
>>>> *point only to domain controllers as their preferred dns servers.*
>>>> *--- Steve*
>>>>
>>>>
>>>> *"Sam Spade" <sams@not.real.actually.fake> wrote in message*

microsoft.public.win2000.security: Re: Authentication Failure

>>>> *news:Xns96C97390F2B18Samisnotactuallyreal@207.46.248.16...*
>>>>> *Group,*
>>>>>
>>>>> *Bit of a weird one here....*
>>>>>
>>>>> *I have set up an entirely Win2K network and locked the permissions*
>>>>> *down hard.*
>>>>>
>>>>> *Occasionally, and this has now happened on three of the*
>>>>> *workstations, when a user tries to logon we get:*
>>>>>
>>>>> *security event 533*
>>>>> *Reason: User not allowed to logon at this computer*
>>>>> *Logon process User32*
>>>>>
>>>>> *Nothing has changed on the users permissions or group policy, they*
>>>>> *are all domain users and can log on to any other workstations.*
>>>>>
>>>>> *I have cured this in the past my re-imaging the drive – a fairly*
>>>>> *simple process but I'd actually like to know what is going wrong.*
>>>>>
>>>>> *Any ideas anyone?*
>>>>>
>>>>> *TIA,*
>>>>>
>>>>> *Sam.*
>>>>
>>>>
>>>>
>>>
>>
>>
>>
>