

## Re: 1058 and 1030 errors revisited

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group\\_policy/2004-10/0153.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2004-10/0153.html)

---

**From:** perry (*perry-hart.sweetser\_at\_hornnes.vgs.no*)

**Date:** 10/06/04

Date: Wed, 6 Oct 2004 01:50:24 -0700

I will gather data and get back to you on this. However, from what I can see when I look at the event logs on all of the machines I have checked so far, this problem does not seem to be localized to any one machine – they all seem to show the same thing – with the exception of a client machine that has a gigabit adapter. That machine registers quite a few other errors as well, like 1054, 5719, 40960 and 40961 events. The 1054 events come about every ten minutes on that client. The 1030 and 1058 id pair share the same time stamp on all of the machines.

I watched the Network Monitor on the server adapters this morning, but they showed no more than a peak utilisation of 1% on the AD machine and 6% on the NAS machine (which has all the roaming profiles and home directories) when 30 pupils logged on simultaneously. So it does not seem to be a traffic problem.

But I will do a deep analysis of the time stamps of the errors during the last month and see if I can run a monitor around the times I see represented most. Then I'll be back with the data in a few days time.

>-----Original Message-----

>Very Interesting an issue I must say. I really cant pin it down to any

>one thing

>

>0. Are you sure about the symptoms ie when the 11th or 12th user logs

>in the error state occurs? Does it never happen when the 8th,9th or

>10th user is logging in? Does the issue occur only on some machines?

>

>1. To gather us some logs, UserEnvironment logging would be a good

>place to start with. If you can reproduce this error state at will,  
>then enable UserEnv logging on the 11th machine which freezes at  
>login. Let him take that 30–40 mins to log in and then examine the  
>UserEnv logs. These logs actually have the time and second stamp for  
>each event as it happens in the background at logon. This way we know  
>that hey when the computer was trying to do this–this–and–this, the  
>error state occoured.  
>  
>Enable UserEnv Logging:  
>Login locally to the box itself as the local admin, enable Logging as  
>per the below KB, rename the current UserEnv file to .old and then  
>attempt to logon as the 11th user to the domain from this box.  
><http://support.microsoft.com/default.aspx?scid=kb;EN-US;221833>  
>  
>Let me also have a look at the logs. Ill see if I find anything which  
>gives us a hint.  
>  
>2. A netmon trace would also help if the UserEnv doesnt.  
>  
>--  
>Gautam Anand  
>e: gautam at hotpop dot com  
>-----  
>"Perry" <perry-hart.sweetser@hornnes.vgs.no> wrote in message  
>news:298101c4aaf8\$a6b5a530\$a501280a@phx.gbl...  
>|I would also like to submit a problem with our Domain GPO  
>| and the notorious 1058 event. I have read everything about  
>| it on this site, the eventid site and on the Microsoft  
>| support site; however, the problem(s) described there do  
>| not correspond to our problems (Q842804 deals with  
>| computers resuming from standby of restart – ours are not  
>| in these modes when this happens); and, although I have  
>| tried all the suggestions mentioned at these sites, the  
>| problem still won't go away.  
>|  
>| But before I discuss this, I would like to contribute with

>/ a solution to a possible diagnosis of the origin of some  
>/ of the problems I have seen. This is because I  
>/ inadvertently managed to produce the 1058 event through  
a

>/ mistake in configuration. What happened was this: when I  
>/ first install a 2003 server I usually try to avoid virus  
>/ infection by immediately downloading and installing the  
>/ newest updates. However, the computer is exposed for a  
>/ very short time to the Internet without any protection.

So

>/ I usually turn on the firewall and turn off NetBios and  
>/ file-sharing on the NIC. Normally, I turn file-sharing  
>/ back on afterwards, but in this one case I forgot to do  
>/ so. Everything seemed ok, so I ran dcpromo and rebooted,  
>/ but then I got the infamous 1058 – 1030 event pair.

When I

>/ tried to run the gpfix utility I got a "network path  
not

>/ found" error which tipped me off to the fact that I had  
>/ forgotten to switch file-sharing back on. I did so and  
>/ rebooted the pc, but this didn't help at all. The point  
>/ is: it seems that having file-sharing off when running  
>/ dcpromo messes up AC somehow. I ran dcpromo again to  
>/ uninstall AC rebooted and reinstalled AC. At this point  
>/ everything worked just fine. A hint to the programmers

at

>/ Microsoft: have dcpromo check the pc to see if all of  
the

>/ conditions (like filesharing) for AC are met before  
>/ installing AC.

>/

>/ Now to our problem:

>/

>/ We have very successfully run a w2k domain at our school  
>/ for the last three years or so. We have four servers to  
>/ share the workload: one for AD, one for Exchange 2000,  
one

>/ for ISA 2000 and one for NAS. There are about sixty  
client

>/ pc's running XP Pro and these all connect through high  
>/ capacity HP Procurve switches. The clients all have 100  
>/ Mbps NICs, whereas the servers all have two gigabit  
>/ adapters each. We have never experienced any networking  
>/ problems – the switch monitors show few or no packets  
>/ dropped, and, with the exception of the occasional  
printer

>/ error, the event logs on both clients and servers have  
>/ been error free for the last three years – which is  
>/ impressive, considering that we are talking about a  
school

>/ here.

>/  
>/ *However, the servers were beginning to show their age – we had run an NT network on them before – so we opted to replace the four servers with newer ones with more processing power (dual CPUs) more memory, SCSI raid storage and (continued) multihomed gigabit NIC capacity. When we bought the machines, we also decided to upgrade the server software to Windows 2003, Exchange 2003 and ISA 2004. At the same time, we installed Service Pack 2 on the XP clients.*  
>/  
>/ *We printed out our old w2k GPOs and used these to configure the new servers pretty much the same as the old ones were. Everything works fine – just as before – with one exception. When more than approximately ten people try to log on to the network at the same time, those client machines that attempt the logon freeze for about 30 minutes. When this happens, we get the 1058 – 1030 userenv event pair – usually for user SYSTEM on both the DC and the client machine application logs. Sometimes this is also followed by the same id pair for user ADMINISTRATOR – on the DC and the logon username on the client. Eventually, the users get logged in, but this makes the entire network unusable for classroom teaching, where up to 50 users log on simultaneously at the start of each classroom hour.*  
>/  
>/ *Note that the system works fine otherwise. The GPOs are applied correctly. This seems to be a network issue. We noticed that after applying Service Pack 2 on the XP clients that the application event log on client machines is always full of MrxSmb event id 3019 errors that were never there before. We have no unusual shares anywhere, and certainly none on the client machines. We assume it has something to do with this, but we are not sure. As I mentioned before, our network infrastructure, which worked fine under w2k, has not changed, and our switch monitors show no noticeable traffic overload nor dropped packets. I have tried the solutions mentioned elsewhere on this forum, but I have not read of anyone having this problem in exactly the same manner. I have even tried something*

>/ that no one else has tried: I noticed that it is the  
>/ Default Domain Policy that is listed in the event id  
>/ error – not any of the other GPOs – so I disabled it and  
>/ moved some of the more important stuff down to the other  
>/ GPOs. That did not help – I still got the same errors  
with  
>/ the same Domain GPO SID listed.  
>/  
>/ There is one thing I have not tried which was mentioned  
>/ here in this forum. I have not turned on file sharing on  
>/ the clients and offline folders are switched off. This  
was  
>/ the way the clients were configured before (this is a  
>/ school, after all, where file sharing cannot be allowed  
>/ under any circumstances because of tests and exams,  
which  
>/ are all taking on the computer) and it worked fine under  
>/ w2k. I cannot see that this should affect the network  
load  
>/ which the AD machine is placed under in anyway. The AD  
>/ runs integrated DNS and DHCP. There are no other  
services  
>/ running on the AD machine besides LanSafe (UPS) and  
>/ TrendMicro Server Protect, but the SYSVOL folder is  
>/ excluded in its entirety from virus scans.  
>/  
>/ Perhaps someone in this forum can see something that I  
am  
>/ missing. I would appreciate any advice.  
>/  
>  
>  
>  
>  
>