

Re: Event ID 1000 (Userenv) Error and Event ID 8021 (BROWSER) Error

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2004-03/0102.html>

From: Ohaya (*ohaya_at_N_O_S_P_A_M_cox.net*)

Date: 03/02/04

Date: Mon, 01 Mar 2004 22:00:08 -0500

"Ace Fekay [MVP]" wrote:

>

> *In news:4043BF86.F36813F@N_O_S_P_A_M_cox.net,*

> *Ohaya <ohaya@N_O_S_P_A_M_cox.net> posted their thoughts, then I offered mine*

> > *"Ace Fekay [MVP]" wrote:*

> > >

> > > *In news:4042D440.FEF08EAC@N_O_S_P_A_M_cox.net,*

> > > *Ohaya <ohaya@N_O_S_P_A_M_cox.net> posted their thoughts, then I*

> > > *offered mine*

> > >

> > > > *Kevin,*

> > > >

> > > > *You have some good questions, and I only have answers to some of*

> > > > *them unfortunately :(...*

> > > >

> > > > *First of all, my desire/intention is to build this 2-machine network*

> > > > *such that it's kind of a standalone ("standalone", in a limited*

> > > > *sense) Windows domain, but physically connected to an external*

> > > > *network.*

> > > >

> > > > *The "machine A" runs an IIS web server, and we need "inward" access*

> > > > *(from clients on the external network) to this web server, but, in*

> > > > *general, we don't need, or want to allow, "outward" access (from*

> > > > *machine*

> > > > *A, or machine B) to the external network.*

> > > >

> > > > *The reason for the machine A/machine B configuration is that*

> > > > *machine B runs a database which is accessed by our web application*

> > > > *(which runs*

> > > > *on machine A), and also, we want to manage all the machines on this*

> > > > *internal network (consisting of machines A & B) using GPOs, etc.*

> > > > *from machine A.*

> > > >

> > > > *Now here's the way that I think that things work (and they are, for*

> >>> *the*
> >>> *most part, working):*
> >>>
> >>> *You noted that we don't define a gateway for either NIC2 on machine*
> >>> *A*
> >>> *or*
> >>> *NIC1 on machine B, but you'll also note that NIC2/machine A and*
> >>> *NIC1/machine B are on the same subnet (IP addresses 192.168.1.xx).*
> >>> *In addition, both NIC2/machine A and NIC1/machine B point to*
> >>> *machine B*
> >>> *for*
> >>> *their DNS server.*
> >>>
> >>> *[I'm being a bit vague here] When something in machine A wants to*
> >>> *connect to either machine A or machine B, since the DNS IP address*
> >>> *points to machine B, name resolution gets handled by the DNS server*
> >>> *on machine B.*
> >>>
> >>> *As to how it "gets out without a gateway", I think it works somewhat*
> >>> *akin to a 2-computer network using a cross-over cable (and without a*
> >>> *router) but, in our case, we're using a switch between the 2*
> >>> *computers (instead of a cross-over cable). My understanding is*
> >>> *that in such a configuration, packets with source/destination*
> >>> *address get sent out*
> >>> *the*
> >>> *NIC on the source machine, and the machine with the matching*
> >>> *destination address will simply receive those packets.*
> >>>
> >>>
> >>> *Here are the answers to some of your questions (I think):*
> >>>
> >>> *Q1) "How is the internal DNS resolving external names with out a*
> >>> *gateway?"*
> >>> *A1) We DON'T WANT the internal DNS (on machine B) to resolve*
> >>> *external names.*
> >>>
> >>> *Q2) "Do you have NAT on the member server?"*
> >>> *A2) No, we don't.*
> >>>
> >>> *Q3) "You have no gateways listed for any NIC, how do you get out*
> >>> *without*
> >>> *a gateway?"*
> >>> *A3) My guess is per what I wrote above.*
> >>>
> >>>
> >>> *BTW, you mentioned above that:*
> >>>
> >>> *"> You cannot have TCP/IP without DNS in Win2k if you leave DNS*
> >>> *blank*
> >>> *it*
> >>> *will*

> >>>> *pick up the loopback address or use DHCP to get the DNS server."*
> >>>
> >>> *Do you know that the above (that it will either default to the*
> >>> *loopback address or use DHCP to get the IP of the DNS server) is*
> >>> *true? The*
> >>> *reason that I'm asking is that this might be at least part of the*
> >>> *question in my earlier thread ("How is resolution working?").*
> >>>
> >>> *If so, can you point me to some documentation about this? Also, if*
> >>> *you*
> >>> *know, under what circumstances would it default to the loopback*
> >>> *address*
> >>> *vs. trying to get the DNS server IP from DHCP?*
> >>>
> >>> *Jim*
> >>
> >> *To add, if you want external communication, you'll need to specify a*
> >> *gateway, unless you do not want to have Internet communication from*
> >> *this machine?*
> >>
> >
> >
> > *Hi Ace et al,*
> >
> > *I was testing all weekend with my new test setup, and I think that*
> > *I've figured out what's going, at least partially, mainly with the*
> > *DNS part.*
> > *I still can't figure out what's going on with the subject of this*
> > *thread though (the Event ID problem).*
> >
> > *The explanation is going to be a bit complicated, but I'll try to*
> > *touch*
> > *on the main points.*
> >
> > *Basically, I started looking at what was happening to the routing*
> > *table ("route print") on the multi-homed machine when I made various*
> > *changes*
> > *to the GWY and DNS pointers on NIC1 and NIC2.*
> >
> > *It turns out that if the GWY is populated in both NIC1 and NIC2, two*
> > *default routes (Destination 0.0.0.0) get created in the routing table.*
> > *For example, if one NIC has IP 192.168.0.9, GWY 192.168.0.1 and the*
> > *other NIC has IP 192.168.1.111, GWY 192.168.1.110, the entries look*
> > *something like:*
> >
> > *0.0.0.0 192.168.0.1 192.168.0.109 1*
> > *0.0.0.0 192.168.1.109 192.168.1.110 1*
> >
> > *As I understand it, the routing logic will look for a match between*
> > *the destination address in a packet and the entries in the routing*
> > *table,*

> > and when it finds the best match, that determines which interface the
> > packet will be sent out on (ok, that explanation is somewhat
> > simplistic).
> >
> > In my case, I always had Metric set to 1, so basically what I found
> > was
> > the ORDER that these routes were being added to the routing table
> > would depend on the ORDER in which I added the GWY pointers to the
> > NICs.
> >
> > If I just happened to get the order one way, so that the 0.0.0.0
> > destination route entry with the 192.168.0.1 GWY was higher priority,
> > then pings to the external network would be able to get to the
> > external network via the "Default Gateway" of 192.168.0.1 (which was
> > a router on
> > the external network), and from there to the open Internet.
> >
> > If I just happened to get the order the other way, so that the 0.0.0.0
> > destination route entry with the 192.168.1.109 GWY was higher
> > priority,
> > then all outgoing traffic, including pings to the external network,
> > would instead be routed through the 192.168.1.110 NIC back into my
> > small network. Remember, the only other machine on this small
> > network was
> > machine B, so basically, these packets would get responded to with an
> > "unreachable".
> >
> >
> > An additional item is that it appears that if any of the NICs in the
> > machine have a specific IP address (e.g., 192.168.1.110), a route to
> > the entire subnet gets added that looks some like:
> >
> > 192.168.1.0 192.168.1.110 192.168.1.110 1
> >
> > Note that the above route will, by itself, provide a way for packets
> > with destination addresses on the 192.168.1 subnet to get to the
> > 192.168.1 subnet. Since this is the case, this means that even I
> > don't
> > have a default route that can get me to the 192.168.1 subnet, I can
> > still get to the 192.168.1 subnet via the above route. This is why I
> > was able to still resolve the names of machines on my internal network
> > (served by the DNS server on machine B) even when I didn't have a GWY
> > setting on the NIC.
> >
> > As I said above, a bit complicated :(...

> >
> > Ok, now that I've figured that out, there's still the matter of the 2
> > Event IDs in my original post.
> >
> > I've figured out one of them, the warning about the browser, by

> > *disabling the Alerter and the BITS service, but I'm still getting the*
> > *Event ID 1000 (userenv).*
> >
> > *Before we get into that, can someone explain what this error is*
> > *exactly? It looks like it's saying that the machine can't access a*
> > *certain file (registry.pol) on my DC?*
> >
> > *If that is correct, what is the ramification of this? What kind of*
> > *problem will it cause?*
> >
> > *Also, as I mentioned in one of my original posts, yes, I can click*
> > *through My Network Places to the DC, then to SYSVOL directory, then on*
> > *downward all the way to the registry.pol file on my DC.*
> >
> > *Since I *can* do that, doesn't that imply that this machine CAN access*
> > *registry.pol on my DC? And if THAT is correct, then why am I still*
> > *getting this error??*
> >
> > *If it's an access problem, as I mentioned earlier, I've already added*
> > *Everyone to that whole tree (just to try to get this working)...*
> >
> > *Thanks for all your patience!!*
> >
> > *Jim*
>
> *Just to let you know, Event ID 1000 is normally caused (99% of the time) by*
> *using the incorrect DNS server in IP properties that is not hosting the AD*
> *zone name, hence the need to use the internal servers only in any AD design.*
> *See this for more info:*
> *<http://www.eventid.net/display.asp?eventid=1000&source=>*
>
> *As for the dual gates, that is why we only usually put in one default*
> *gateway on one or the other NIC (unless I misinterpreted your post). Would*
> *have rather seen an actual ipconfig /all of this machine....*
> :-)

Ace,

Yes, I think we agree about 1 GWY for the machine with 2 NICs. That part makes sense now to me (as I tried to explain in my earlier post :)!). Until I realized what was going on in the route table, I couldn't figure out how traffic was getting out to my 192.168.1 subnet without the 2nd GWY.

Sorry about not posting the ipconfig. I've been making so many changes, back and forth, that I didn't know which one would be representative. I hope that you understand.

I'm waiting on a test now of the Event ID thing, and will post back in this thread.

microsoft.public.win2000.networking: Re: Event ID 1000 (Userenv) Error and Event ID 8021 (BROWSER) Error

BTW, is there any way to reduce the time between whatever is causing the Event ID 1000? I'm seeing between 90–100 minutes between these errors in the Event log, so testing any changes is a bit time-consuming...

Jim