

Microsoft Windows 7 joining a Samba Domain Status

Last week Microsoft made available Windows 7 Build 7100 as a download for the general public. At the time of writing this operating system will not join a Samba domain. The error message is “The specified domain either does not exist or could not be contacted”.

This problem it appears has been known by Microsoft for some time.

On Sunday, January 11, 2009 3:20 PM a enquirer called Ender9 questions <http://social.technet.microsoft.com/Forums/en-US/w7itpronetworking>

Does this affect samba domains, too? If I try to join my domain at home, I get "The specified domain either does not exist or could not be contacted.", though my other computers (running Vista and XP) have no problems joining.

I only have 1 DC, and I can browse it if I enter it's name directly (that is Win+R -> \\deephthought - I don't see it if I browse the network, only my Vista machine and printer appear there; it asks me for credentials, and I can then access the shares on it normally). I have also tried disabling the Windows firewall, but it had no effect.

If I try joining the domain, I'm asked for the username and password, and after entering them, I get the error. I can see from the logs that there is some communication between Windows and Samba, but joining ultimately fails.

Ned Pyle [MSFT] – MS Enterprise Platforms Support Employee – Beta Team replies

“You will need a double-sided network trace to see what's happening here Ender9. The error only highlights what we already know, that there is a network problem. It's the DCLOCATOR process that's failing here, so it appears to be name resolution that's not working. I don't have a way to test this though, as I do not run SAMBA. You may also want to give them a shout to see if they have run into any issues with default Win7 in this Beta build or with the PDC M3 exit build.

So - network capture util on both servers (netmon 3.2 or Wireshark on the Win7, whatever you like on the Samba). Make sure you flush DNS and NETBIOS caches on the client (ipconfig /flushdns and nbtstat -R), then start both captures. Try to join, get error, stop captures, examine captures.”

Ender9 then posts the double-sided network trace but gets no response back from Microsoft.

Then on Fri Jan 16 07:27:47 GMT 2009 from Volker.Lendecke at SerNet.DE
Unable to join a domain with windows 7 beta1

On Thu, Jan 15, 2009 at 11:10:55AM -0800, Joshua-M wrote:

I have a Samba 3 / OpenLDAP system working with 2000, XP/2003 and Vista clients, but no go with 7, I will attach what information I have gathered.

Jim Pinkerton asked me to post this message from Microsoft:

Sincere apologies, but wanted to confirm that there is an issue with NT Domain support in Windows 7. We're trying to expeditiously track down exactly the issue(s), but the short of it is I wouldn't spend time trying to get this functionality to work. We'll get some sort of official notice out shortly (and I do mean shortly).

Jim Pinkerton Microsoft

Jim Pinkerton [Microsoft] replies on February 13th 2009 to the Samba Team

Jim Pinkerton

To: samba-technical@samba.org

CC: Nick Meier, Keith Hageman

Unable to join a domain with windows 7 beta1

Well, to quote the trailer in an email that Jeremy and I sent out for the SNIA SMB/CIFS interop event back in September: (... and yes, pigs can fly!... :-)) ... and now can actually post to external reflectors! What a concept. As we slooowly, but surely break down the accumulated walls that have built up over the years, today is a bit of a unique day in my experience - we (well, really Nick Meier, representing Microsoft's interop lab) filed bugs against Samba to help get over the interop issues we've seen with Windows 7 (and yep, we have bugs on our end as well (sigh)...).

The bugs are:

Samba 4 - Function NetrLogonDummyRoutine1 needs to return STATUS_NOT_IMPLEMENTED (bug 6109)

Samba 4 - NetrServerAuthenticate[2,3] returns inaccurate capabilities (bug 6108)

Samba 3.2 - Function NetrLogonDummyRoutine1 needs to return STATUS_NOT_IMPLEMENTED (bug 6100)

Samba 3.2 - NetrServerAuthenticate[2,3] returns inaccurate capabilities. (bug 6099)

Just so hopefully we all know what's going on, lemme attempt to explain what the heck happened (and no, to the best of my knowledge we're not trying to hose small business' as was theorized on this thread :-)). First, we've dropped support for NT Domains - thus it is no longer included in our test matrix. And as programmers often do, old things break as you introduce new things (like AES support, better diagnostics). Also, the crypto community pretty strongly deprecates 40 and 56 bit crypto, so the default minimum crypto required is 128 bit (overridden with a reg-key, if you don't need enterprise class security or interop is more important). That said though, the goal is interop. Period. But interop is never a constant target, as we both continue to put new features in our code bases.

So the beta interop issue was pretty much what betas are for - we've tested it enough in our labs, time to put it out in the big-bad real world. And of course we found a few holes in our test plan... interop testing with Samba was minimal (we've fixed this going forward). We scurried around internally to figure out how bad it was, and then sent out an email with full status, plus had a sanity-check con-call with a few Samba folks (I'm going to botch it if I try to say everyone that was on, but a few of the usual suspects, like Tridge, Volker, Andrew, James Peach...). On our end were devs from the AD team, netlogon team, and the SMB team. This resulted in the above bugs being filed.

So in short, we have a plan. Fix the above bugs on your end, we'll fix a few on our end, and we'll meet in the Microsoft Cambridge Interop lab (well, virtually meet) with privates ASAP to verify there aren't any other hidden issues (hopefully before we ship the next Windows 7 beta update). Below is the gory details, sent out by Keith Hageman before the con-call, including thoughts around interop matrices (i.e. what will work by default, what won't but has defaults that can be over-ridden, etc).

Hope this helps. A bit long winded, but hopefully worthwhile.

Jim

And the Samba Teams reply

Following is our current understanding of the issue you have reported to us including additional testing that was recently completed. We welcome your input here and would like to start an active dialog to resolve these issues.

Summary:

- We have done quite a bit of testing with Samba 3.2.7. Spotty on other versions (help appreciated.)*
- Have found issues with AD, crypto, and netlogon, due to non-testing of NT interop and upgrading of security requirements. Going forward (post win7) strongly encourage Samba team to move off the NT Domain, since we stopped supporting it a while back (and thus aren't testing it as thoroughly as we used to).*

- o We're up for fixing the issues on our side to interoperate with Samba, however a couple of the issues we're recommending be fixed in the Samba code, because to fix it on our end opens us to man-in-the-middle attacks.*

Summary of outstanding technical issues:

- We think there are two bugs in Samba (which we'll file bug reports for):*

- o [MS-NRPC]NetrServerAuthenticate[2,3] Message output, NegotiateFlags field – need to set negotiated flag to the intersection of what they support and what the client supports (currently it appears to just be echoed back, falsely advertising capabilities that Samba doesn't support).*

- o [MS-NRPC]NetrLogonDummyRoutine1 (for win7 this is renamed NetLogonGetCapabilities) - i.e. opnum 21.*

- § Function call to test for a man-in-the-middle attack - first implemented in win2k.*

- § If Samba supported the end-point, but not the method, and returned "status not implemented", then the response is secure and we would downgrade to prior behavior.*

- § Approach that would open us up to man-in-the-middle attacks - If "RPC procnum out of range" error was returned. This is because it is not signed, thus it opens us up to man-in-the middle attacks.*

Here is the proposal for the interop matrix with Windows 7 (after all changes have been done for Windows 7 and for Samba):

- Samba as a domain joined file server*

- o With current Samba and the proposed modifications to Windows 7, full interop.*

- o Downlevel interop may require setting of registry keys on Windows 7.*

- Note: this means that a Win7 client must substantially degrade it's security configuration to achieve this functionality.*

(See below for Win7 Client registry settings information)

- Samba as a domain joined SMB client*

- o Would interoperate*

- Samba as a DC

o would require installation of security patches as defined above.

If they are not installed, then Windows 7 would not interoperate.

- Samba in non-domain joined environments (i.e. SMB server or client)

o Would interoperate

Configuration changes potentially required on Win7 client to interoperate with downlevel Samba DC (unknown yet which versions of Samba require which settings - arguably just set them all):

* WS08/Win7 clients perform DNS name resolution validations to enable detection of misconfigured environments early. This must be disabled via client registry policy for NT4 domains as they don't have DNS names.

o HKLM\System\CCS\Services\LanManWorkstation\Parameters DWORD DNSNameResolutionRequired = 0

* NT4 does support NTLM v2, Win7 client's require it by default:

o Gpedit.msc / Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Policies - "Network security: LAN Manager authentication level" needs to be relaxed to one of the levels that accepts LM & NTLM but doesn't require NTLM v2 otherwise NTLM auth fails with errors like 1326 ERROR_LOGON_FAILURE.

* Two Win7 client registry policies that must be disabled as NT4 does not support them.

o HKLM\System\CCS\Services\Netlogon\Parameters DWORD RequireSignOrSeal and RequireStrongKey = 0

* Win7 requires NTLM 128bit:

o Gpedit.msc / Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Policies - Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

§ Uncheck: Require 128-bit encryption.

Stuff left to examine:

- Unsecure domain join (using a pre-created computer account in the domain). This does not work against an NT 4 machine, but we haven't yet tested against Samba. Since Samba supports 128 bit crypto, this may work - but need to validate.

Next steps:

- We both do code changes.

- We would like to test interoperability with Samba ASAP (i.e. not wait for the next major release) in the Windows Interop lab in Cambridge to validate all the above (both for uplevel (i.e. bug fixed) Samba DC and for the other scenarios).

Here is a picture of Ender9's server capture file posted Monday Jan 12 2009

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.29	192.168.0.255	BROWSER	Local Master Announcement WIN7VM, Workstation
2	14.411797	Vmware_e6:56:bb	Broadcast	ARP	Who has 192.168.0.1? Tell 192.168.0.29
3	14.411824	IntelCor_13:dc:49	Vmware_e6:56:bb	ARP	192.168.0.1 is at 00:1b:21:13:dc:49
4	14.412038	192.168.0.29	192.168.0.1	NBNS	Name query NB YGGDRASIL<1c>
5	14.412265	192.168.0.1	192.168.0.29	NBNS	Name query response NB 192.168.0.1
6	14.412588	192.168.0.29	192.168.0.255	SMB_NETL	SAM LOGON request from client
7	14.412887	192.168.0.29	192.168.0.1	SMB_NETL	SAM LOGON request from client
8	14.413002	192.168.0.1	192.168.0.29	SMB_NETL	SAM Response - user unknown
9	14.413250	192.168.0.1	192.168.0.29	SMB_NETL	SAM Response - user unknown
10	19.410588	IntelCor_13:dc:49	Vmware_e6:56:bb	ARP	Who has 192.168.0.29? Tell 192.168.0.1
11	19.411372	Vmware_e6:56:bb	IntelCor_13:dc:49	ARP	192.168.0.29 is at 00:0c:29:e6:56:bb
12	20.804676	192.168.0.29	192.168.0.255	SMB_NETL	SAM LOGON request from client
13	20.804823	192.168.0.29	192.168.0.1	SMB_NETL	SAM LOGON request from client
14	20.805334	192.168.0.1	192.168.0.29	SMB_NETL	SAM Response - user unknown
15	20.805562	192.168.0.1	192.168.0.29	SMB_NETL	SAM Response - user unknown
16	20.903320	192.168.0.29	192.168.0.255	SMB_NETL	SAM LOGON request from client
17	20.903465	192.168.0.29	192.168.0.1	SMB_NETL	SAM LOGON request from client
18	20.903680	192.168.0.1	192.168.0.29	SMB_NETL	Response to SAM LOGON request
19	20.904067	192.168.0.1	192.168.0.29	SMB_NETL	Response to SAM LOGON request
20	21.012794	192.168.0.29	192.168.0.1	NBNS	Name query NB YGGDRASIL<1b>
21	21.013032	192.168.0.1	192.168.0.29	NBNS	Name query response NB 192.168.0.1
22	21.013437	192.168.0.29	192.168.0.1	SMB_NETL	Query for PDC from WIN7VM
23	21.014804	192.168.0.1	192.168.0.29	SMB_NETL	Response from PDC: host DEEPTHOUGHT, domain Y
24	28.431025	192.168.0.29	192.168.0.255	SMB_NETL	SAM LOGON request from client
25	28.431218	192.168.0.29	192.168.0.1	SMB_NETL	SAM LOGON request from client
26	28.431347	192.168.0.1	192.168.0.29	SMB_NETL	SAM Response - user unknown
27	28.431635	192.168.0.1	192.168.0.29	SMB_NETL	SAM Response - user unknown

Here is a picture of my server capture file taken Sunday May 10 2009

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::ffff:ffff:ffe	ff02::2	ICMPv6	Router solicitation
2	0.187884	fe80::8000:f227:30d1	fe80::ffff:ffff:ffe	ICMPv6	Router advertisement
3	0.188335	2001:0:cf2e:3096:3010	ff02::1	IPv6	IPv6 no next header
4	5.187740	SunrichT_06:59:75	Msi_8f:4e:b6	ARP	Who has 192.168.124.110? Tell 192.168.124.1
5	5.187846	Msi_8f:4e:b6	SunrichT_06:59:75	ARP	192.168.124.110 is at 00:16:17:8f:4e:b6
6	9.469994	192.168.124.110	192.168.124.255	SMB_NETL	SAM LOGON request from client
7	9.470161	192.168.124.110	192.168.124.1	SMB_NETL	SAM LOGON request from client
8	9.470284	192.168.124.1	192.168.124.110	SMB_NETL	SAM Response - user unknown
9	9.470429	192.168.124.1	192.168.124.110	SMB_NETL	SAM Response - user unknown
10	13.976296	Msi_8f:4e:b6	SunrichT_06:59:75	ARP	Who has 192.168.124.1? Tell 192.168.124.110
11	13.976323	SunrichT_06:59:75	Msi_8f:4e:b6	ARP	192.168.124.1 is at 00:0a:cd:06:59:75
12	26.452593	192.168.124.110	192.168.124.255	SMB_NETL	SAM LOGON request from client
13	26.452692	192.168.124.110	192.168.124.1	SMB_NETL	SAM LOGON request from client
14	26.452826	192.168.124.1	192.168.124.110	SMB_NETL	SAM Response - user unknown
15	26.452947	192.168.124.1	192.168.124.110	SMB_NETL	SAM Response - user unknown
16	26.550290	192.168.124.110	192.168.124.255	SMB_NETL	SAM LOGON request from client
17	26.550394	192.168.124.110	192.168.124.1	SMB_NETL	SAM LOGON request from client
18	26.550473	192.168.124.1	192.168.124.110	SMB_NETL	Response to SAM LOGON request
19	26.550578	192.168.124.1	192.168.124.110	SMB_NETL	Response to SAM LOGON request
20	26.658844	192.168.124.110	192.168.124.1	SMB_NETL	Query for PDC from EVALWIN7
21	26.658979	192.168.124.1	192.168.124.110	SMB_NETL	Response from PDC: host BIZUXA, domain STRALOCK
22	27.313671	192.168.124.110	192.168.124.255	SMB_NETL	SAM LOGON request from client
23	27.313766	192.168.124.110	192.168.124.1	SMB_NETL	SAM LOGON request from client
24	27.313884	192.168.124.1	192.168.124.110	SMB_NETL	SAM Response - user unknown
25	27.313995	192.168.124.1	192.168.124.110	SMB_NETL	SAM Response - user unknown

Look pretty similar don't they? You could almost be forgiven by assuming that Microsoft have done absolutely nothing about resolving the problem. But where does this leave business in evaluating Windows 7 as an eventual replacement for Windows XP Professional? And so it seems that both camps need to make changes before Microsoft's new operating system will be accepted by business.

Update from Joel Osburn Sat May 16, 2009 3:20 am

With version Samba 3.2.11; that is to say, the Windows 7 RC 7100 will join the Samba domain, report the DNS error, and then function correctly. At least it looks good so far!

Make these changes to the registry

HKLM\System\CCS\Services\LanmanWorkstation\Parameters

Add the following:

DWORD DomainCompatibilityMode = 1

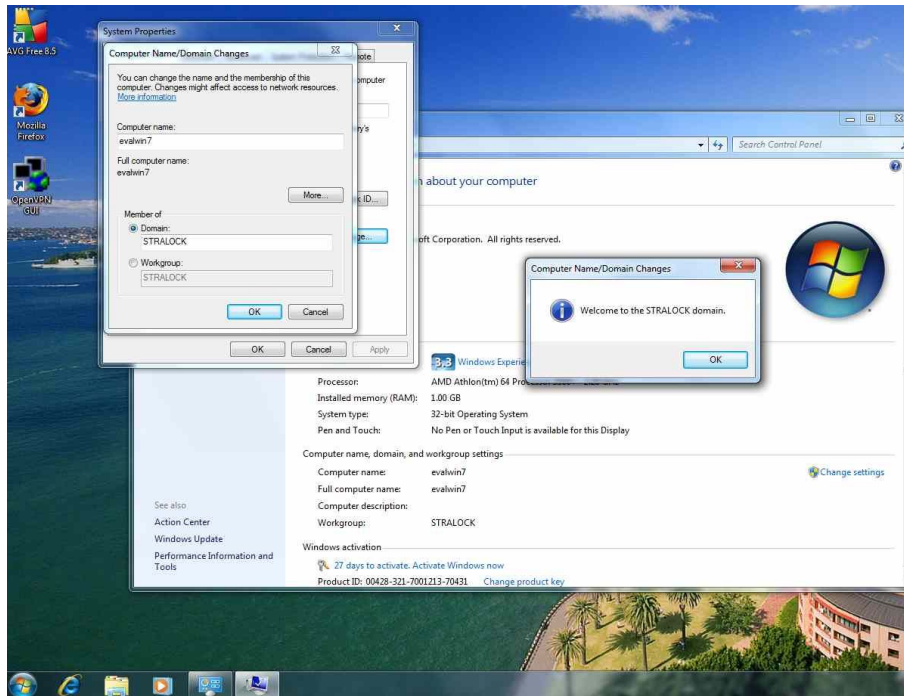
DWORD DNSNameResolutionRequired = 0

Modify the following:

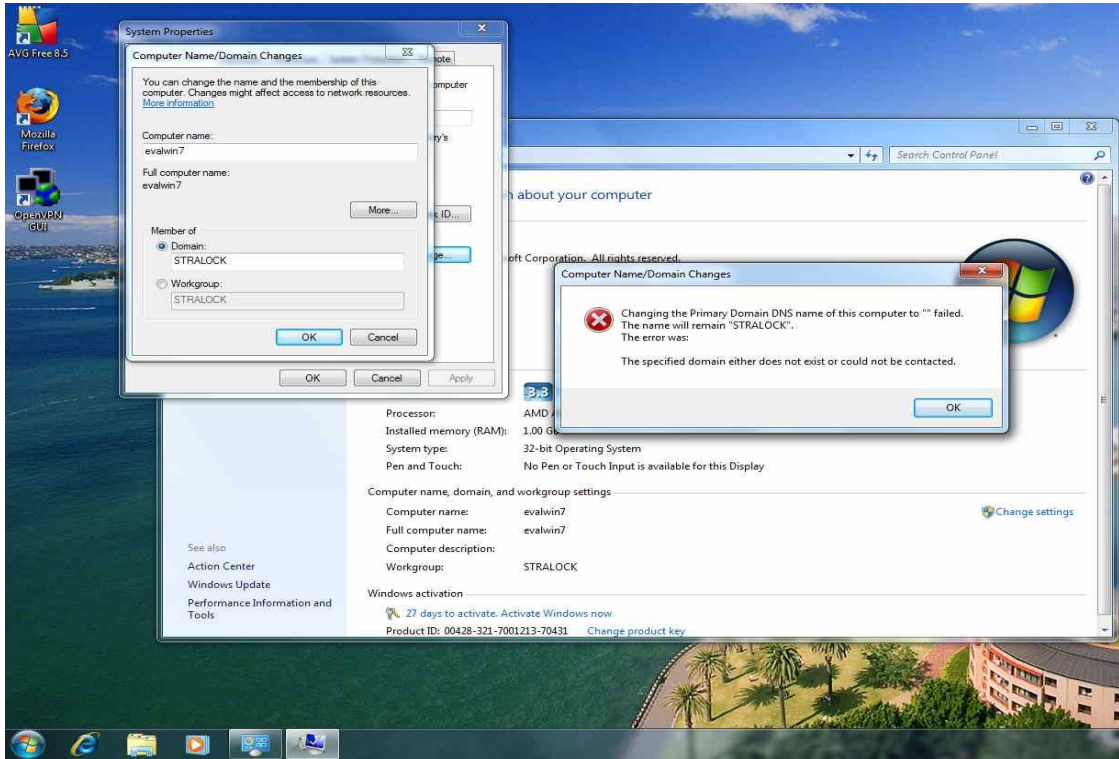
HKLM\System\CCS\Services\Netlogon\Parameters

DWORD RequireSignOrSeal = 0

DWORD RequireStrongKey = 0



then the DNS error



After the domain DNS error it seems that Windows 7 might support Domains and Samba after all.

win7	2 items	folder	Tue 19 May 2009 19:56:37 EST
profile	14 items	folder	Mon 27 Apr 2009 14:11:03 EST
profile.V2	14 items	folder	Tue 19 May 2009 18:49:55 EST
AppData	1 item	folder	Tue 19 May 2009 18:44:53 EST
Contacts	2 items	folder	Tue 19 May 2009 18:45:36 EST
Desktop	1 item	folder	Tue 19 May 2009 18:45:36 EST
Documents	1 item	folder	Tue 19 May 2009 18:45:37 EST
Downloads	1 item	folder	Tue 19 May 2009 18:45:37 EST
Favorites	5 items	folder	Tue 19 May 2009 18:45:43 EST
Links	4 items	folder	Tue 19 May 2009 18:45:38 EST
Music	1 item	folder	Tue 19 May 2009 18:45:36 EST
Pictures	1 item	folder	Tue 19 May 2009 18:45:36 EST
Saved Games	1 item	folder	Tue 19 May 2009 18:45:37 EST
Searches	3 items	folder	Tue 19 May 2009 18:45:37 EST
Videos	1 item	folder	Tue 19 May 2009 18:45:36 EST
ntuser.ini	250 bytes	unknown	Tue 19 May 2009 18:49:57 EST
NTUSER.DAT	512.0 KB	program	Tue 19 May 2009 18:49:55 EST

Showing the profile.V2 directory on the samba server for user win7