

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

## Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-12/msg01344](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg01344)

---

- *From:* "Alex" <[newsgroups@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:newsgroups@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 19 Dec 2006 11:16:15 -0000
- 

Hi Jorge. Thanks again, I can't thank you enough for all the help you and the other MVPs have given me over the last few weeks. I've followed the instructions on the links last night to enable debugging. At 01:07 last night DC1 (2000) logged the same SAM error again. I've searched through the netlogon.log on both DC1 and DC2 (DC2 is 2003 and has all FSMO Roles) and there is only one single entry with the 0xC000006A Failure code but this is a normal user mistake. On manually look through the logs I have listed below the entries which I am concerned about, in particular these batches of [CHANGELOG] entries which occurred at 01:06 last night and the SAM error was then logged at 01:07 need to look into further are below. Since there are no 0XC000006A Failure codes does this suggest the SAM 12994 event error isn't necessarily due to incorrect authentications otherwise they would have been logged ?

These entries ARE ONLY on DC1 (server with SAM Error) and have Names of servers and user accounts and are generated for 2 minutes solid every 2-3 hours. There are lots of entries for the 'Administrator' account and lots of repetition for the entries over the period of time. I'm slightly concerned these are only on DC1 and not DC2, is this related to the SAM 12994 event error ?

.....

```
[CHANGELOG] DeltaType .....
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2080 Rid: 0x527
Name: 'Administrator'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2801 Rid: 0x527
Name: 'Administrator'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2802 Rid: 0x527
Name: 'Administrator'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2803 Rid: 0x527
Name: 'Administrator'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2804 Rid: 0x527
Name: 'Administrator'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2805 Rid: 0x925
Name: 'DC2$'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2806 Rid: 0x326
Name: 'User1'
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2807 Rid: 0x872
```

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

Name: 'User2'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2808 Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 2809 Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280a Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280b Rid: 0x158  
Name: 'Server1'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280c Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280c Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280c Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280c Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType AddOrChangeUser (5) SerialNuber: 0 280c Rid: 0x527  
Name: 'Administrator'  
[CHANGELOG] DeltaType .....  
.....

These entries are generated quite often:

DC1 (2000)

[CRITICAL] Ping from DC1 for domain dc1.domain.net (null) for (null) on  
<Local> is invalid since we don't host the named domain.  
[CRITICAL] NetpDcGetNameIp: dc1.domain.net: No data returned from DnsQuery  
[CRITICAL] NetpDcGetName: dc1.domain.net: IP and Netbios are both done.

DC2 (2003):

[CRITICAL] Ping from DC1 for domain dc1.domain.net (null) for (null) on  
<Local> is invalid since we don't host the named domain.  
[CRITICAL] NetpDcGetNameIp: dc1.domain.net: No data returned from DnsQuery  
[CRITICAL] NetpDcGetName: dc1.domain.net: IP and Netbios are both done.

Thanks,  
Alex.

"Jorge de Almeida Pinto [MVP – DS]"  
<SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxx> wrote in message  
[news:uDeGciuIHHHA.3872@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uDeGciuIHHHA.3872@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

the license service can be disabled

I assume "something" with the wrong password is "attacking" your domain  
administrator with the wrong password.

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

use netlogon debugging to start tracing the account lockout....start at the PDC

Enabling debug logging for the Net Logon service

a.. HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DBFlag

b.. DBFlag = 0x2080FFFF (in: %windir%\debug\netlogon.log)

and follow what is mentioned here:

<http://www.eksternkompetanse.no/blog/PermaLink.guid.576846a0-ac14-47d4-8057-c117a9e2ec1c.aspx>

<http://www.eksternkompetanse.no/blog/PermaLink.guid.43f143b3-f389-4946-9bdf-21a1b787f5cb.aspx>

<http://www.eksternkompetanse.no/blog/PermaLink.guid.3e28462e-f4c9-499a-8cc9-43acc47a779.aspx>

--

Cheers,

(HOPEFULLY THIS INFORMATION HELPS YOU!)

# Jorge de Almeida Pinto # MVP Windows Server – Directory Services

BLOG (WEB-BASED)--> <http://blogs.dirteam.com/blogs/jorge/default.aspx>

BLOG (RSS-FEEDS)--> <http://blogs.dirteam.com/blogs/jorge/rss.aspx>

\* This posting is provided "AS IS" with no warranties and confers no rights!

\* Always test before implementing!

#####  
#####

"Alex" <newsgroups@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:uuKOKOtIHHA.780@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uuKOKOtIHHA.780@xxxxxxxxxxxxxxxxxxxxxxxx)

Hi Paul. Thanks for the information. Unfortunately the process we went through to create our test network was different to what you have suggested on your site. Our live network at the time only had one 2000 DC. We took a NTBackup of the DC and restored it onto a server with the same hardware. There were no errors apart from the decomissioned signature for the first DC. I have ran dcdiag, netdiag and repadmin testing throughout the test upgrade to 2003 and have not had any errors. When we started having problems with the test network at the point of demoting the 2000 DC we stopped any parallel upgrades on the Live network. Subsequently both networks now have one 2000 DC and one 2003 DC, the 2003 has all the roles.

Unfortunately we aren't having much luck with this upgrade. The new 2000/2003 have been running without problem but over the weekend we have started generating LicenseService (ID 213) warnings on what appears to be a random selection of member servers (License Service is running on the 2003 DC and AD Sites & Services Licensing Site Settings points to DC2).

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

More concerning we have also started to get NTDSReplication ID 1083, NTDS Replication ID 1955 and SAM 12294 for the Domain Administrator account. I have just posted about this in a new post but if I could resolve these two issues on the Live network I don't think we would have any further problems with the demotion and addition of new 2003 DC.

Thanks,  
Alex.

"Paul Bergson [MVP-DS]" <pbergson@xxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:O89OrWjIHH.1248@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O89OrWjIHH.1248@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

How did you build the test network. Have a look at a build doc I have and see if you missed out on any steps.

<http://www.pbbergs.com>  
Select articles and click on Create a Test Domain

Once you have the domain created run diagnostics against it

If you don't have the tools installed, install them from your server install disk.  
d:\support\tools\setup.exe

Run dcdiag, netdiag and repadmin in verbose mode.  
-> dcdiag /e /c /v /s:DC\_Name /f:c:\dcdiag.log  
-> netdiag.exe /v > c:\netdiag.log (On each dc)  
-> repadmin.exe /showrepl dc\* /verbose /all /intersite > c:\repl.txt

If you download a gui script I wrote it should be simple to set and run (DCDiag and NetDiag). It also has the option to run individual tests without having to learn all the switch options. The details will be output in notepad text files that pop up automagically.

The script is located in the download section on my website at  
<http://www.pbbergs.com>

Just select both dcdiag and netdiag make sure verbose is set.  
(Leave

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

the default settings for dcdiag as set when selected)

When complete search for fail, error and warning messages.

—  
Paul Bergson  
MVP – Directory Services  
MCT, MCSE, MCSA, Security+, BS CSci  
2003, 2000 (Early Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the  
NewsGroup  
This posting is provided "AS IS" with no warranties, and  
confers no  
rights.

"Alex" <newsgroups@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message  
[news:uHnDDHfIHHA.2456@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uHnDDHfIHHA.2456@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi. We have been having a problem with a  
test network which we are  
using to test an upgrade from 2000 to 2003.  
The network was built from  
a restored 2000 DC image before the first  
2003 DC was added. The  
restore completed successfully on slightly  
different hardware with no  
errors and everything working correctly. On  
running repadmin /showsig  
the 2000 DC (DC1) has generated a new  
signature and the old signature  
has been retired. Unfortunately although  
repadmin is showing this DC as  
having and using a new signature, it registers  
it's CNAME entry in DNS  
with the old signature and the NTDS  
Replication DNS Alias (visible from  
AD Sites and Services on the 2003 DC) is  
also listing the old  
signature. Subsequently when we attempt to  
demote this server the  
demotion is not clean. BUT even after we  
clear out any left over DNS  
and AD entries for the 2000 DC (no server  
entry is left from the  
demotion in ntdsutil), when we then install  
2003 on the same server

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?

hardware, same IP address and same name, after running dcpromo and rebooting the server it generates replication errors. These errors are indicating that the 2003 DC(DC2) is attempting to replicate with the now new 2003 DC1 but they fail to authenticate with each other because the 2003 DC2 appearing to be trying to contact DC1 using its old retired signature. I have posted about this in a similar post previously and Jorge made the suggestions below but this is still occurring:

- \*Clear the DNS cache
  - rightclick the DNS server and clear the cache.
  - run from cmd: ipconfig /flushdns
- \*delete the files netlogon.dnb and netlogon.dns from  
%systemroot%\system32\config
- \*run ipconfig /registerdns
- \*restart the netlogon service, confirm the creation of the files netlogon.dnb and netlogon.dns on  
%systemroot%\system32\config
- \*run netdiag /fix

Check again the DNS entries.

This is only happening on our test network. When I run repadmin /showsigs on the live network the current 2000 DC has only 1 signature with non retired and the newer 2003 DC also has 1 signature. I would really like to cleanup the test network so I can confirm the demotion and addition of the replacement 2003 DC works successfully.

Thanks,  
Alex.

Re: Where are DC signatures stored in AD ? Can then be edited using adsiedit ?