

## Re: ntds corrupted?

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2004-02/0287.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-02/0287.html)

---

**From:** mmac (mmac\_at\_junkmail.bin)

**Date:** 02/08/04

Date: Sat, 7 Feb 2004 16:50:01 -0800

Sorry to duplicate post, I just want to be sure to thank everyone personally. This was a big deal to have all you guys be so helpful. Thank you.

After 3 1/2 hours of actual phone time (after 2 hours waiting = 5 1/2 hours with a phone in my ear) we got it back as far as I can tell. It came down to running the ntdsutil and then eseutil in a certain sequence. and it recovered. The same for the exchange database. a specific sequence of eseutil and isinteg switches, that is not outlined specifically enough in any single KB article which was found in a message (they called it an object I think, something that may someday become a KB article?) the pss guy walked me through it and it did everything it said it would and it is now running again. I had all the pieces but the ordering was critical.

I don't know how much I lost because it was 3am this morning that I left it with the disk just churning away (Exchange trying to to catch up perhaps?) But when I checked my mail today I might have lost the day it crashed but thats all.

Next I move the stuff off this thing and rebuild after a graceful demotion. But that will wait a few days, I gotta get some sleep. Thank you all for so much help!

"Dmitri Gavrilov [MSFT]" <dmitrig@online.microsoft.com> wrote in message news:uwsicUV7DHA.2404@TK2MSFTNGP11.phx.gbl...

- > *Aha, that makes more sense. -550 means you got no logs. You must have copied*
- > *ntds.dit, but did not copy the logs. Edb.log is always created.*
- >
- > *If you can find the logs (wherever they used to be, in the same folder with*
- > *ntds.dit by default), then you can recover, by copying them into the ntds*
- > *folder.*
- >
- > *If you need to rebuild the DC, then, sorry, I am not at work, and I am no*
- > *support person either :)*
- >
- > *These KBs contain instructions on removing a dead DC:*
- > <http://support.microsoft.com/default.aspx?scid=KB;EN-US;216498>
- > <http://support.microsoft.com/default.aspx?scid=KB;EN-US;332199>
- >
- > --

> *Dmitri Gavrilov*  
> *SDE, Active Directory Core*  
>  
> *This posting is provided "AS IS" with no warranties, and confers no rights.*  
> *Use of included script samples are subject to the terms specified at*  
> *<http://www.microsoft.com/info/cpyright.htm>*  
>  
> *"mmac" <no@thank.you> wrote in message*  
> *news:ezW\$AzU7DHA.2056@TK2MSFTNGP10.phx.gbl...*  
> *> the error using ntdsutil files integrity is "inconsistent" is there*  
> *another*  
> *> command I can use to give you more info?*  
> >  
> *There are is an edb.log file present*  
> >  
> *What you say in the last paragraph will need handholding. Can you walk me*  
> *> through it. (or pick up the phone if you are at work ;)*  
> >  
> >  
> *"Dmitri Gavrilov [MSFT]" <dmitrig@online.microsoft.com> wrote in message*  
> *news:OqyOdeU7DHA.1052@TK2MSFTNGP12.phx.gbl...*  
> *> No, copying the DIT from another DC is a bad idea. Very bad.*  
> > >  
> *> Are you sure about the jet error? -1030 is JET\_errAlreadyInitialized,*  
> *> which*  
> *> should not be the case. Can you double check?*  
> > >  
> *> Most probably, you lost log files, and the db is left in inconsistent*  
> *> state,*  
> *> and jet can not restore the consistency by replaying the logs. So,*  
> *unless*  
> *> you find the logs (edb\*.log), you are screwed.*  
> > >  
> *> If you got another DC, then the easiest way out is to force-demote the*  
> *DC*  
> *> (basically, rebuild it), and then re-promote as a replica. If it held*  
> *any*  
> *> FSMOs, then you'll have to seize them to another DC. You'll also have to*  
> *> cleanup metadata (from ntdsutil) to get rid of the remnants of the*  
> *> decommissioned dc.*  
> > >  
> > > --  
> *> Dmitri Gavrilov*  
> *> SDE, Active Directory Core*  
> > >  
> *> This posting is provided "AS IS" with no warranties, and confers no*  
> *> rights.*  
> *> Use of included script samples are subject to the terms specified at*  
> *> <http://www.microsoft.com/info/cpyright.htm>*  
> > >

microsoft.public.windows.server.active\_directory: Re: ntds corrupted?

> > > "mmac" <no@thank.you> wrote in message  
> > > news:e9ehBhS7DHA.2168@TK2MSFTNGP12.phx.gbl...  
> > > > I have no ieda what problems the file from one DC would do to another  
> > > DC.  
> > > > Thats why I ask if it's a good idea. I just don't know. I could open a  
> > > > working dc and copy the file to the non working one. But what would  
> > > > happen?  
> > > > I can envision it fouling up both machines but just because thats the  
> > > way  
> > > my  
> > > > luck has been running...  
> > > >  
> > > > "Christian Schindler" <christian.schindler@ntx.at> wrote in message  
> > > > news:O%23%23HCcQ7DHA.1852@TK2MSFTNGP10.phx.gbl...  
> > > > > I don't say that there's no way – but is it worth the time you  
> > > invest?  
> > > > >  
> > > > > Why would copying from a working one be a bad idea?  
> > > > >  
> > > > > Christian  
> > > > >  
> > > > > "mmac" <no@thanks.com> wrote in message  
> > > > > news:%23QEpMUQ7DHA.3704@tk2msftngp13.phx.gbl...  
> > > > > > Does that mean that there is no way to recover the ntds.dit file  
> > > at  
> > > all?  
> > > > > Copying from a working one wouldnt' be a good idea I would  
> > > imagine.  
> > > I  
> > > > > shudder at the thought of installing exchange 55 again. but my  
> > > first  
> > > > > concern  
> > > > > is getting the machine working again. I'll deal with ex later.  
> > > > >  
> > > > >  
> > > > > "Christian Schindler" <christian.schindler@ntx.at> wrote in  
> > > message  
> > > > > news:uQmG1JQ7DHA.2736@TK2MSFTNGP10.phx.gbl...  
> > > > > > If you have no EX backup thats bad news. But to give you an idea  
> > > what  
> > > > > I  
> > > > > > would do(or  
> > > > > > try...):  
> > > > > >  
> > > > > > My plan would be to completely rebuild the server(same name) but  
> > > only  
> > > > > as  
> > > > > a  
> > > > > > member server. You mentioned that there are two other DC/GC's.  
> > > So  
> > > you

Re: ntds corrupted?

>>>>> loose  
>>>>> nothing in terms of AD...  
>>>>>  
>>>>> All you have to do afterwards is clean up the metadata in AD  
>> that's  
>>> left  
>>>>> from the server  
>>>>> with the corrupt ntds.dit. And perhaps seize FSMO roles.  
>>>>>  
>>>>> Then you'll have to do an Exchange recover(and now we have the  
> old  
>>>>> problem –  
>>>>> no backup).  
>>>>>  
>>>>> If you need the new server to play the DC role – just promote it  
>> and  
>>>>> your'e  
>>>>> done.  
>>>>>  
>>>>> I know it sounds so easy although it isn't – I think the big  
>> problem  
>>>>> is not the corrupt ntds.dit. It's the missing EX backup...  
>>>>>  
>>>>> Good luck!  
>>>>>  
>>>>> Christian  
>>>>>  
>>>>>  
>>>>> "mmac" <no@thanks.com> wrote in message  
>>>>> news:OgLa5RP7DHA.3304@tk2msftngp13.phx.gbl...  
>>>>>> entirely possible in going in circles but it feled more like a  
>>> wall  
>>>> to  
>>>>> me.  
>>>>>> yes it is running ex55 too. But that issue was before I killed  
>>>>> ntds.dit  
>>>>>> I have ex2k also on that domain but few users are on it.  
>>>>>> I have no exbackup. I was using the repair tools for exchange  
>> when  
>>> I  
>>>>> just  
>>>>>> ran out of room and had to add another drive to contain the  
>> tempdb  
>>>>>> created.  
>>>>>>> Thats when the floor dropped out on me.  
>>>>>>>  
>>>>>>> This morning I put the original NTDS.DIT back in place and  
>> what  
>>> I  
>>>> get  
>>>>> now

microsoft.public.windows.server.active\_directory: Re: ntds corrupted?

>>>>>> at  
>>>>>> boot time is what I had before I put the other one there:  
>>> LSASS.exe  
>>>>> error  
>>>>>> 0xC00002e1 reboot and start directory services restore ...  
>>>>>> so I can't read the event logs unless I use directory services  
>>>>> restore.  
>>>>>> I have gone through Q258062, 240362,249321 after it remapped  
> my  
>>>> drive  
>>>>>> letters.  
>>>>>> when I run ntdsutil / file / integrity, I get  
>>>> DBInitializeJetDatabase  
>>>>>> failed jet error 1030.  
>>>>>>>  
>>>>>>>  
>>>>>>>  
>>>>>>> "Christian Schindler" <christian.schindler@ntx.at> wrote in  
>>> message  
>>>>>>> news:%23009dnO7DHA.1632@TK2MSFTNGP12.phx.gbl...  
>>>>>>> Seems you're moving around in circles...  
>>>>>>>>  
>>>>>>>> The DC is also running Exchange 5.5, correct?  
>>>>>>>>  
>>>>>>>> Do you have a valid and functioning EX backup?  
>>>>>>>>>  
>>>>>>>>> --  
>>>>>>>>> Christian Schindler  
>>>>>>>>> MCSA / MCSE / MCT / CCEA  
>>>>>>>>>>  
>>>>>>>>>> Senior Consultant  
>>>>>>>>>>>  
>>>>>>>>>>> NTx BackOffice Consulting Group Austria  
>>>>>>>>>>> mailto:cns@ntx.at  
>>>>>>>>>>>>  
>>>>>>>>>>>>  
>>>>>>>>>>>> "mmac" <mmac@junkmail.bin> wrote in message  
>>>>>>>>>>>> news:uhnMZPM7DHA.360@TK2MSFTNGP12.phx.gbl...  
>>>>>>>>>>>>> Oh man am I in trouble.  
>>>>>>>>>>>>>> In an effort to simply add another drive to my server in  
>> order  
>>>> to  
>>>>>> fix  
>>>>>>> an  
>>>>>>>>>> exchange 55 database corruption, I installed the nearest  
>> drive  
>>>>> under  
>>>>>>> the  
>>>>>>>>>>>> impression that I would just format it and use it.  
>>>>>>>>>>>>>> It turned our to be a cloned drive from a couple years  
>> ago

Re: ntds corrupted?



