

RE: NTDS.dit file is corrupt

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-12/1295.html

From: ptwilliams (ptw2001_at_hotmail.com.donotspam)

Date: 12/22/04

Date: Wed, 22 Dec 2004 01:01:01 -0800

How often is this server backed up?

You're best (and probably only) hope now is a relatively new restore...

--

Paul Williams

<http://www.msresource.net/>

<http://forums.msresource.net/>

"microsoft" wrote:

> We are currently facing a serious problem with one our client server.
>
> It is an only domain controller on the network, when we are trying to login
> to the server it has given an error before the login screen which is
>
> LSASS.EXE - System Error, security accounts manager initialization failed
> because of the following error: Directory Services cannot start. Error
> status 0xc00002e1.
>
> Please click OK to shutdown this system and reboot into directory services
> restore mode, check the event log for more detailed information.
>
> After rebooting the machine in directory services restore mode, I had
> followed the steps below; ntdsutil neither defrag Active Directory Database
> nor repair (ntds.dit). It is given the following error;
>
> file maintenance: integrity
>
> Opening database [Current].*** Error: DBInitializeJetDatabase failed with
> [Jet
>
> Error -1209].
>
> Error While Doing Soft Recovery
>
> file maintenance:"
>
>
>
> Right now I am not able to access the server's event viewer log as well.
> Please help me to resolve that above problem.
>
> Thanks
>
> Muhammed Imran
>

microsoft.public.win2000.active_directory: RE: NTDS.dit file is currrupt

```
>
>
> -----
> -----
>
> 1. Restart the domain controller.
> 2. When the BIOS information appears, press F8.
> 3. Select Directory Services Restore Mode, and then press ENTER.
> 4. Log on by using the Directory Services Restore Mode password.
>
> Note If you cannot log on, visit the following Microsoft Knowledge Base
> article:
>
> 249321 Unable to log on if the boot partition drive letter has changed
> 5. Click Start, select Run, type cmd in the Open box, and then click
> OK.
> 6. At the command prompt, type ntdsutil files info.
>
> Output that is similar to the following appears:
>
> Drive Information: C:\ NTFS (Fixed Drive ) free(533.3 Mb) total(4.1 Gb) DS
> Path Information: Database : C:\WINDOWS\NTDS\ntds.dit - 10.1 Mb Backup dir :
> C:\WINDOWS\NTDS\dsadata.bak Working dir: C:\WINDOWS\NTDS Log dir :
> C:\WINDOWS\NTDS - 42.1 Mb total temp.edb - 2.1 Mb res2.log - 10.0 Mb
> res1.log - 10.0 Mb edb00001.log - 10.0 Mb edb.log - 10.0 Mb
>
>
>
> Note The file locations that are included in this output are also found in
> the following registry subkey:
>
> HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
>
> The following entries in this key contain the file locations
>
> ..
>
> Database Backup path
>
> ..
>
> Database Log files path
>
> ..
>
> DSA Working Directory
>
>
> 7. Verify that the files that are listed in the output in step 6 exist.
> If the files do not exist, follow the steps in the following Microsoft
> Knowledge Base article:
>
> 240362 Directory Services does not start if Ntds.dit file is missing
> 8. Verify that the folders in the Ntdsutil output have the correct
> permissions. The correct permissions are specified in the following tables.
>
> Windows Server 2003
>
> Account
>
> Permissions
>
```

microsoft.public.win2000.active_directory: RE: NTDS.dit file is corrupt

```
> Inheritance
>
> System
>
> Full Control
>
> This folder, subfolders and files
>
> Administrators
>
> Full Control
>
> This folder, subfolders and files
>
> Creator Owner
>
> Full Control
>
> Subfolders and Files only
>
> Local Service
>
> Create Folders / Append Data
>
> This folder and subfolders
>
> Windows 2000
>
> Account
>
> Permissions
>
> Inheritance
>
> Administrators
>
> Full Control
>
> This folder, subfolders and files
>
> System
>
> Full Control
>
> This folder, subfolders and files
>
> Note Additionally, the System account requires Full Control permissions on
> the following folders:
>
> ..
>
> The root of the drive that contains the Ntds folder
>
> ..
>
> The %WINDIR% folder
>
> In Windows Server 2003, the default location of the %WINDIR% folder is
> C:\WINDOWS. In Windows 2000, the default location of the %WINDIR% folder is
> C:\WINNT.
> 9. Check the integrity of the Active Directory database. To do this,
> type ntdsutil files integrity at the command prompt.
```

microsoft.public.win2000.active_directory: RE: NTDS.dit file is corrupt

>
> If the integrity check indicates no errors, restart the domain controller in
> normal mode. If the integrity check does not finish without errors, continue
> to the following steps.
> 10. Perform a semantic database analysis. To do this, type the following
> command at the command prompt, including the quotation marks:
>
> ntdsutil "sem d a" go
> 11. If the semantic database analysis indicates no errors, continue to
> the following steps. If the analysis reports any errors, type the following
> command at the command prompt, including the quotation marks:
>
> ntdsutil "sem d a" "go f"
> 12. Follow the steps in the following Microsoft Knowledge Base article
> to perform an offline defragmentation of the Active Directory database:
>
> 232122 Performing offline defragmentation of the Active Directory database
> 13. If the problem still exists after the offline defragmentation, and
> there are other functional domain controllers in the same domain, remove
> Active Directory from the server, and then reinstall Active Directory. To do
> this, follow the steps in the section titled "If the domain controller
> cannot start in normal mode" in the following Microsoft Knowledge Base
> article:
>
> 332199 Using the DCPROMO /FORCEREMOVAL command to force the demotion of
> Active Directory domain controllers
>
> Note If your domain controller is running Microsoft Small Business Server,
> you cannot perform this step, because Small Business Server cannot be added
> to an existing domain as an additional domain controller (replica). If you
> have a system state backup that is newer than the tombstone lifetime,
> restore that system state backup instead of removing Active Directory from
> the server. By default, the tombstone lifetime is 60 days.
>
> For additional information about how to restore a system state backup, click
> the following article number to view the article in the Microsoft Knowledge
> Base:
>
> 240363 How to use the Backup program to back up and restore the system state
> 14. If no system state backup is available, and there are no other
> healthy domain controllers in the domain, we recommend that you rebuild the
> domain by removing Active Directory and then reinstalling Active Directory
> on the server, creating a new domain. You can use the old domain name again
> or use a new domain name. You can also rebuild the domain by reformatting
> and reinstalling Windows on the server. However, removing Active Directory
> is quicker, and effectively removes the corrupted Active Directory database.
>
> If no system state backup is available, there are no other healthy domain
> controllers in the domain, and you must have the domain controller working
> immediately, perform a lossy repair by using either Ntdsutil or Esentutl.
>
> Note Microsoft does not support domain controllers after Ntdsutil or
> Esentutl is used to recover from Active Directory database corruption. If
> you perform this kind of repair, you must rebuild the domain controller for
> Active Directory to be in a supported configuration. The repair command in
> Ntdsutil uses the Esentutl utility to perform a lossy repair of the
> database. This kind of repair fixes corruption by deleting data from the
> database. Only use this kind of repair as a last resort.
>
> Although the domain controller may start and may appear to function
> correctly after the repair, its state is unsupported because the data that
> is deleted from the database can cause any number of problems that may not

microsoft.public.win2000.active_directory: RE: NTDS.dit file is currrupt

> surface until later. There is no way to determine what data was deleted when
> the database was repaired. As soon as possible after the repair, you must
> rebuild the domain to return Active Directory to a supported configuration.
> If you only use the offline defragmentation or semantic database analysis
> methods that are referenced in this article, you do not have to rebuild the
> domain controller afterward.

> 15. Before you perform a lossy repair, contact Microsoft Product Support
> Services to confirm that you have reviewed all possible recovery options and
> to verify that the database truly is in an unrecoverable state. For
> information about how to contact Microsoft Product Support Services, visit
> the following Microsoft Web site:
>
> <http://support.microsoft.com/default.aspx?scid=fh;EN-US;CNTACTMS>
>

> To use Ntdsutil to recover the Active Directory database, type ntdsutil
> files repair at a command prompt in Directory Service Restore Mode.

> 16. After the repair operation is complete, rename the .log files in the
> NTDS folder by using a different extension such as .bak, and try to start
> the domain controller in normal mode.

> 17. If the repair operation does not appear to finish, you can try to
> repair the database by using Esentutl.

>

> Windows 2000 Server:
>

> At the command prompt, type the following command:
>
> esentutl /p path\ntds.dit /!10240 /8 /v /x /o
>

> For example, on a Windows 2000 server where the Active Directory database
> resides in the default location of C:\WINNT\NTDS, use the following command:
>
> esentutl /p c:\winnt\ntds\ntds.dit /!10240 /8 /v /x /o
>

> Windows Server 2003:
>

> At the command prompt, type the following command:
>
> esentutl /p path\ntds.dit
>

> For example, on a Windows Server 2003-based computer where the Active
> Directory database resides in the default location of c:\WINNT\NTDS, use the
> following command:
>
> esentutl /p c:\winnt\ntds\ntds.dit
>

> After the command has finished running, rename the .log files in the NTDS
> folder by using a different extension such as .bak.
>
>
>
>