Directory Services Cannot Start After Restoring NTDS & SYSVOL on a Single DC Fixing STOP Code 0xC00002E2

This guide explains how to recover from the Windows Server Blue Screen:

```
STOP CODE: 0xC00002E2
STATUS_DS_INIT_FAILURE
```

This typically occurs when:

- `ntds.dit` was restored manually
- SYSVOL was restored manually
- BurFlags may have been set
- The server was freshly promoted as a new DC
- The NTDS database state does not match the system registry metadata

On a **single domain controller**, this issue is fully recoverable using an NTDS hard repair.

⚠ Requirements

This procedure is safe **ONLY** when:

- You have a **single Domain Controller** (no other DCs in the domain)
- There is **no AD replication** to other servers

If you have more than one DC, **stop here** — this procedure can cause USN rollback in multi-DC environments.

---

1. Boot into Directory Services Restore Mode (DSRM)

1. Restart the domain controller.
2. During system startup, press **F8** (or use your hypervisor / cloud console “Send F8” function).
3. Select:

   ```
   Directory Services Restore Mode
   ```

4. Log in using the **DSRM password** (set when the DC was promoted).

---

2. Perform a Hard Repair of NTDS.dit

Open **Command Prompt (Administrator)** while in DSRM and run:

```
esentutl /p "C:\Windows\NTDS\ntds.dit"
```

You will be prompted:

```
Proceed with repair (Y/N)?
```

Type:

```
Y
```

This performs a “hard repair” of the AD database. This is only safe because this is a **single DC** domain.

---

3. Run an Integrity Check

Still in DSRM, run:

```
esentutl /g "C:\Windows\NTDS\ntds.dit"
```

Expected output should end with something similar to:

```
Integrity check successful
```

If errors appear, stop and record the output before proceeding.

---

4. (Optional but Recommended) Defragment the Database

Defragmenting the database can reclaim space and further clean up after the repair:

```
esentutl /d "C:\Windows\NTDS\ntds.dit"
```

Wait for the operation to complete before continuing.

---

5. Clean Up NTDS Log Files

Navigate to the NTDS folder:

```
C:\Windows\NTDS
```

Delete **only** the following file types:

- `*.log`
- `*.jrs`
- `edb.chk`

Do NOT delete:

- `ntds.dit`
- `temp.edb`
- any other `*.dit` files
- any `*.jfm` files

Removing the log and checkpoint files ensures AD does not try to reuse invalid transaction logs after the repair.

---

6. Reboot the Server Normally

Restart the server in normal mode:

```
shutdown /r /t 0
```

Expected outcome:

- The server boots normally (no more STOP 0xC00002E2)
- The Active Directory Domain Services service starts
- You can log in normally with a domain account

---

7. Verify SYSVOL and NETLOGON Shares

After logging in, open Command Prompt and run:

```
net share
```

You should see entries for:

```
SYSVOL
NETLOGON
```

If those shares exist, SYSVOL is being published correctly.

---

8. Re-Initialize SYSVOL (FRS) Authoritatively

If you manually restored SYSVOL content, you should re-initialize FRS so that this DC treats its SYSVOL as authoritative.

Set the BurFlags value:

```
reg add
"HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Proce
ss at Startup" /v BurFlags /t REG_DWORD /d 0xD4 /f
```

Then restart the File Replication Service:

```
net stop ntfrs
net start ntfrs
```

FRS will now rebuild its replication state using the restored SYSVOL as the authoritative source.

---

9. Validate Domain Health

Run a domain controller diagnostic:

```
dcdiag /v
```

Review the output for:

- Netlogon-related errors
- SYSVOL or FRS errors
- General AD DS health issues

If there are issues you are unsure about, you can paste the relevant sections into ChatGPT for analysis.

Final Result

When all steps are complete, you should have:

- A domain controller that boots without STOP 0xC00002E2
- A repaired and consistent `ntds.dit` database
- SYSVOL correctly restored and shared
- FRS synchronized to the restored SYSVOL (BurFlags D4)
- Active Directory fully operational in a single-DC environment

You can now proceed with normal operations and, if desired, plan for adding additional domain controllers, proper backups, and disaster recovery procedures to avoid similar issues in the future.

Revision #3
Created 2025-11-30 13:46:53 UTC by joliveira
Updated 2025-11-30 13:50:41 UTC by joliveira