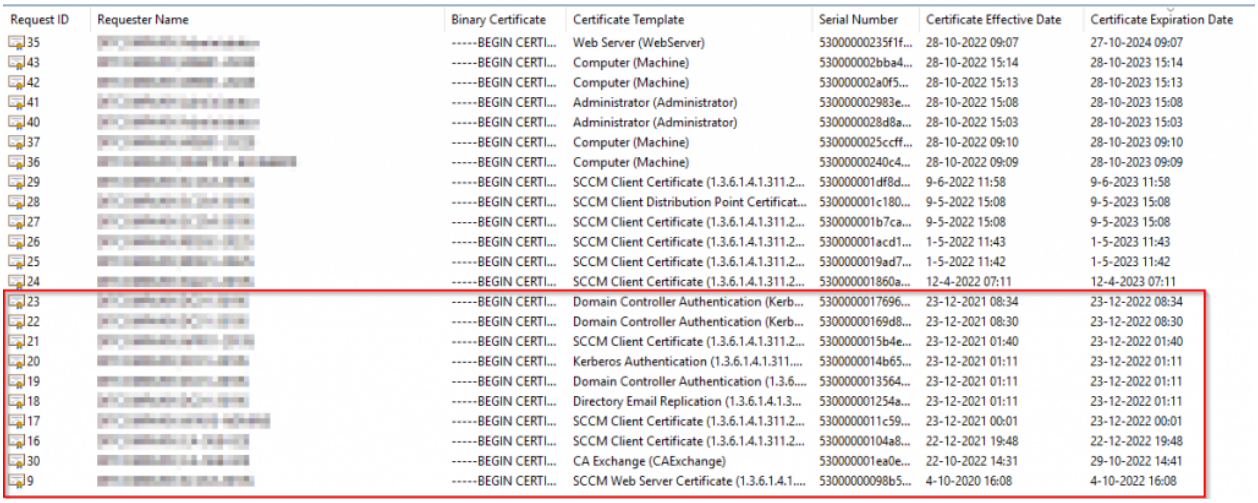
Clean and compact the CA Database

vmlabblog.com/2023/01/clean-and-compact-the-ca-database

Aad Lutgert January 8, 2023

In this blog I will show how you can clean and compact the CA Database. To regain overview in your CA Infrastructure. Depending on your environment, the CA Database can increase substantially in size over time. In addition, expired certificates remain in the Issued Certificates view.



Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
35	[redacted]	-----BEGIN CERTI...	Web Server (WebServer)	53000000235f1f...	28-10-2022 09:07	27-10-2024 09:07
43	[redacted]	-----BEGIN CERTI...	Computer (Machine)	530000002bba4...	28-10-2022 15:14	28-10-2023 15:14
42	[redacted]	-----BEGIN CERTI...	Computer (Machine)	530000002a0f5...	28-10-2022 15:13	28-10-2023 15:13
41	[redacted]	-----BEGIN CERTI...	Administrator (Administrator)	530000002983e...	28-10-2022 15:08	28-10-2023 15:08
40	[redacted]	-----BEGIN CERTI...	Administrator (Administrator)	5300000028d8a...	28-10-2022 15:03	28-10-2023 15:03
37	[redacted]	-----BEGIN CERTI...	Computer (Machine)	5300000025ccff...	28-10-2022 09:10	28-10-2023 09:10
36	[redacted]	-----BEGIN CERTI...	Computer (Machine)	53000000240c4...	28-10-2022 09:09	28-10-2023 09:09
29	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	530000001df8d...	9-6-2022 11:58	9-6-2023 11:58
28	[redacted]	-----BEGIN CERTI...	SCCM Client Distribution Point Certificat...	530000001c180...	9-5-2022 15:08	9-5-2023 15:08
27	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	530000001b7ca...	9-5-2022 15:08	9-5-2023 15:08
26	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	530000001acd1...	1-5-2022 11:43	1-5-2023 11:43
25	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	5300000019ad7...	1-5-2022 11:42	1-5-2023 11:42
24	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	530000001860a...	12-4-2022 07:11	12-4-2023 07:11
23	[redacted]	-----BEGIN CERTI...	Domain Controller Authentication (Kerb...	5300000017696...	23-12-2021 08:34	23-12-2022 08:34
22	[redacted]	-----BEGIN CERTI...	Domain Controller Authentication (Kerb...	53000000169d8...	23-12-2021 08:30	23-12-2022 08:30
21	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	5300000015b4e...	23-12-2021 01:40	23-12-2022 01:40
20	[redacted]	-----BEGIN CERTI...	Kerberos Authentication (1.3.6.1.4.1.311....	5300000014b65...	23-12-2021 01:11	23-12-2022 01:11
19	[redacted]	-----BEGIN CERTI...	Domain Controller Authentication (1.3.6....	5300000013564...	23-12-2021 01:11	23-12-2022 01:11
18	[redacted]	-----BEGIN CERTI...	Directory Email Replication (1.3.6.1.4.1.3...	53000001254a...	23-12-2021 01:11	23-12-2022 01:11
17	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	5300000011c59...	23-12-2021 00:01	23-12-2022 00:01
16	[redacted]	-----BEGIN CERTI...	SCCM Client Certificate (1.3.6.1.4.1.311.2....	53000000104a8...	22-12-2021 19:48	22-12-2022 19:48
30	[redacted]	-----BEGIN CERTI...	CA Exchange (CAExchange)	530000001ea0e...	22-10-2022 14:31	29-10-2022 14:41
9	[redacted]	-----BEGIN CERTI...	SCCM Web Server Certificate (1.3.6.1.4.1....	53000000098b5...	4-10-2020 16:08	4-10-2022 16:08

Pic 1: Example Expired Certificates Database

This can cause you to lose overview. Besides the Issued Certificates, this also applies to Revoked, Pending and Failed Requests. After you clean up the database, you need to compact it. The cleansing process creates white spaces in the database which can be removed by compacting the database.

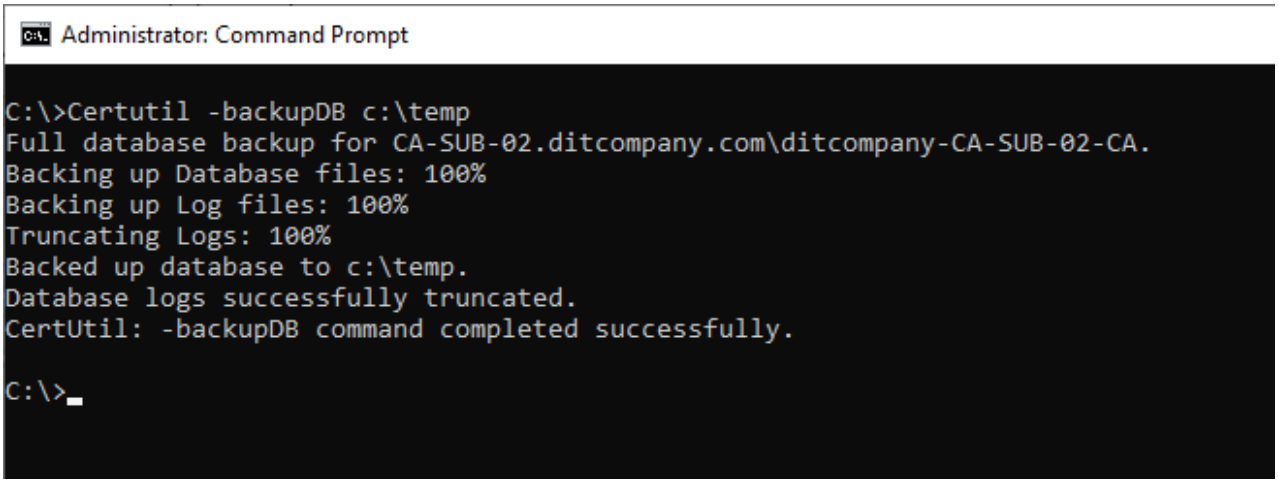
Backup the CA Database

To clean up the database, we use the command-line program Certutil.exe. This is installed by default when adding the Certificate Services role on the server. Before starting, it is important to make a backup so that it is possible to restore the CA database.

```
Certutil -backupDB <backupDirectory>
```

To create a backup in the folder “C:\temp” you will need to create the folder “c:\temp” and enter:

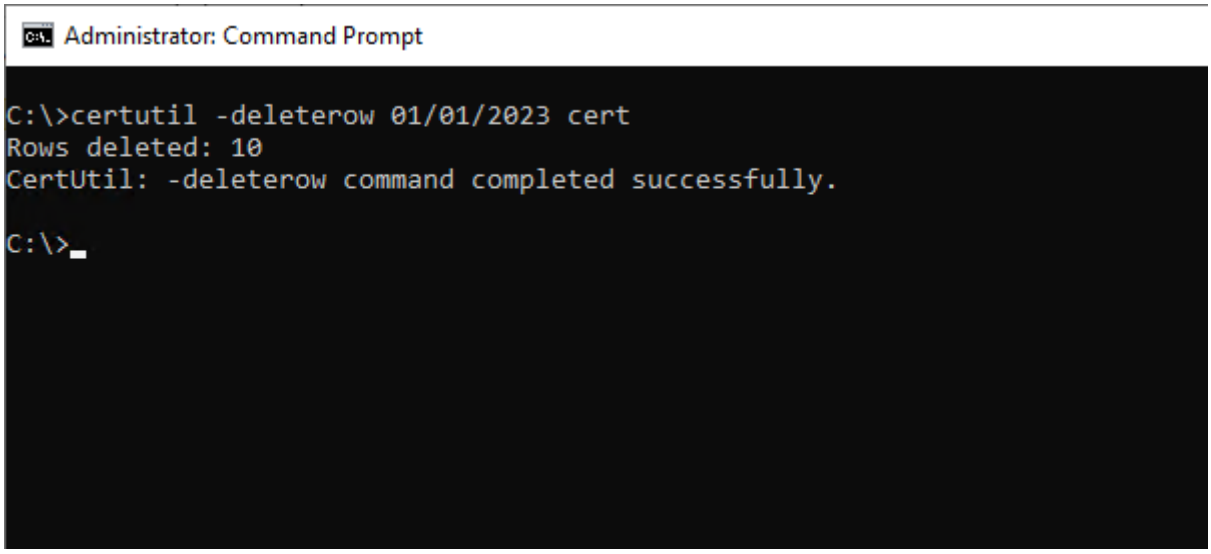
```
Certutil -backupDB c:\temp
```



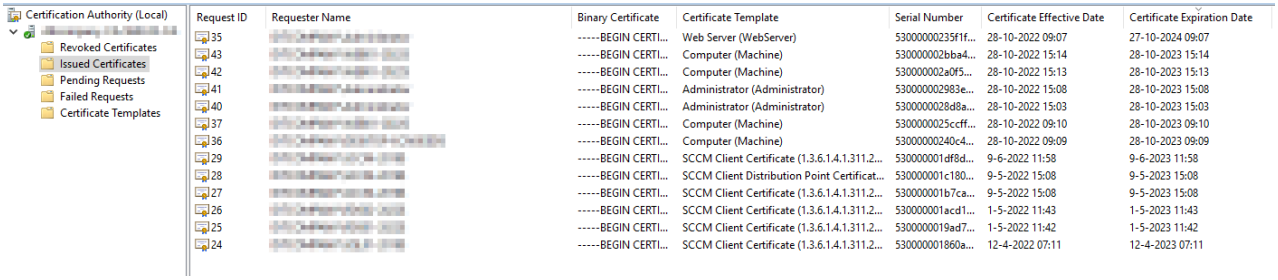
Remove the Expired and revoked certificates

Now that we have a backup of the CA database, we can start cleaning up the records. As with the backup, we will use Certutil.exe. To remove Expired and Revoked certificates, we specify the date until which they should be removed. For example, if you want all certificates expired and revoked through 01-01-2023, then enter 01-01-2023. Certificates expired or revoked on 02-01-2023 will remain in the database. In this example I will remove all certificate which are expired or revoked on 01-01-2023. To indicate that you want to remove expired and revoked certificates enter "**cert**".

This action has removed 10 rows



On my demo server there are only some expired Issued Certificates. As you can see in the screenshot, all certificates that expired on or before 01-01-2023 have been removed.

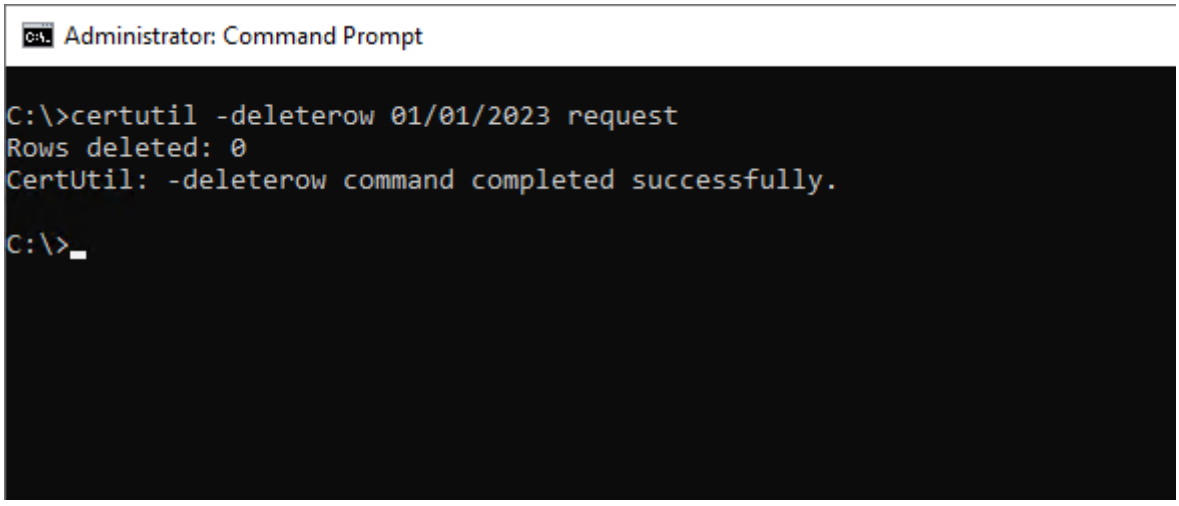


Since I don't have revoked certificates I can't show this, but the same goes for revoked certificates.

Remove the Pending and failed requests

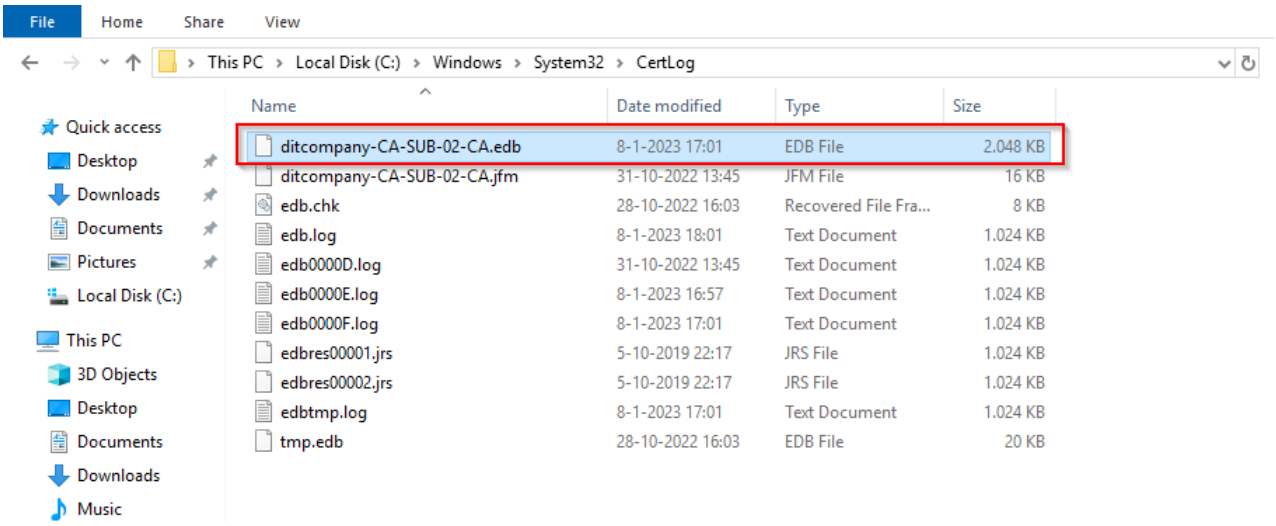
Now that the expired and revoked certificates have been removed we continue with the pending and failed requests. As with the previous work we use Certutil.exe. Unlike the expired and revoked certificates, the pending and failed requests require you to enter the submission date. If you want to remove pending and failed requests created up to and including January 1, 2023, enter 01/01/2023. To indicate that you want to remove failed and pending requests enter "**request**".

Since I don't have pending and failed requests I can't show this. As you can see in the screenshot, no rows have been deleted.



Compact the CA Database

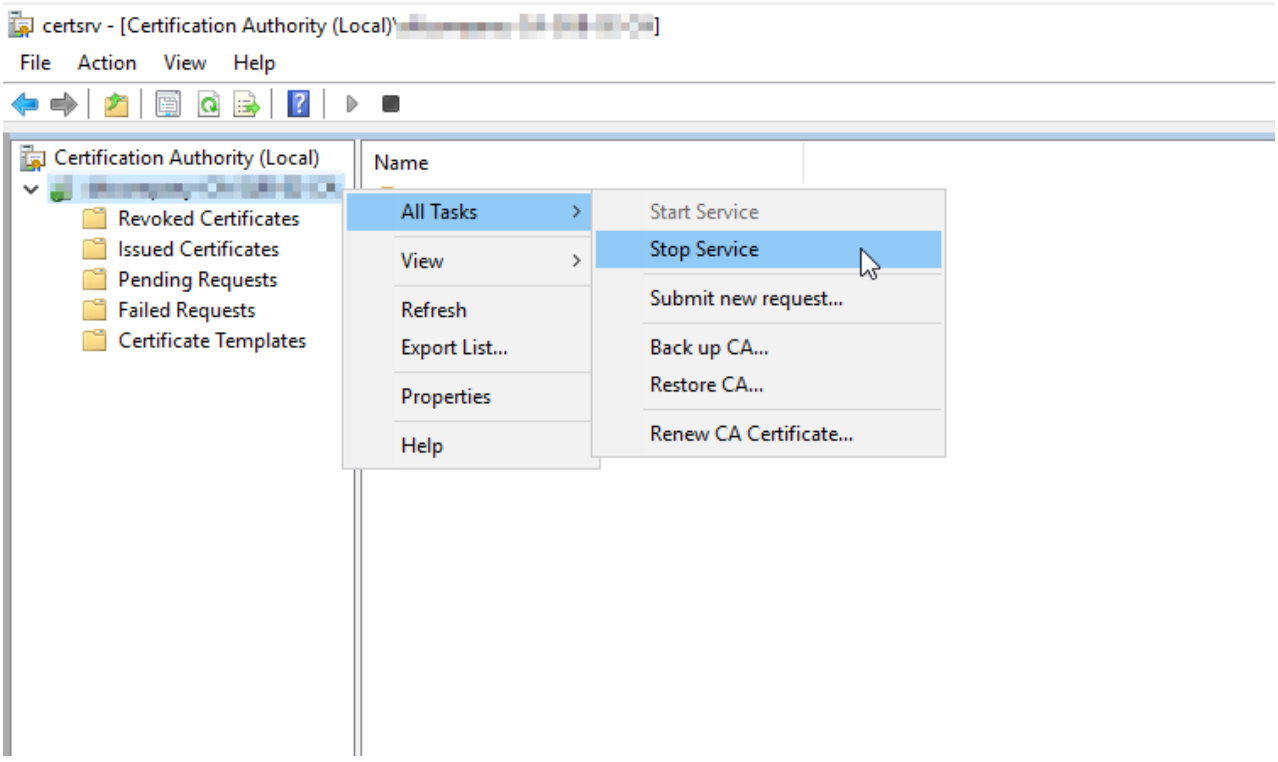
Now that we are almost at the end, we need to perform one more step and that is to extract the white spaces (defragmentation) from the database. To do this we use Esentutl. First we need to find out the path to the database. By default, the database is located in the folder "C:WindowsSystem32CertLog". The database has the extension "*.edb". In my demo environment, the database is called "ditcompany-CA-SUB-02-CA.edb".



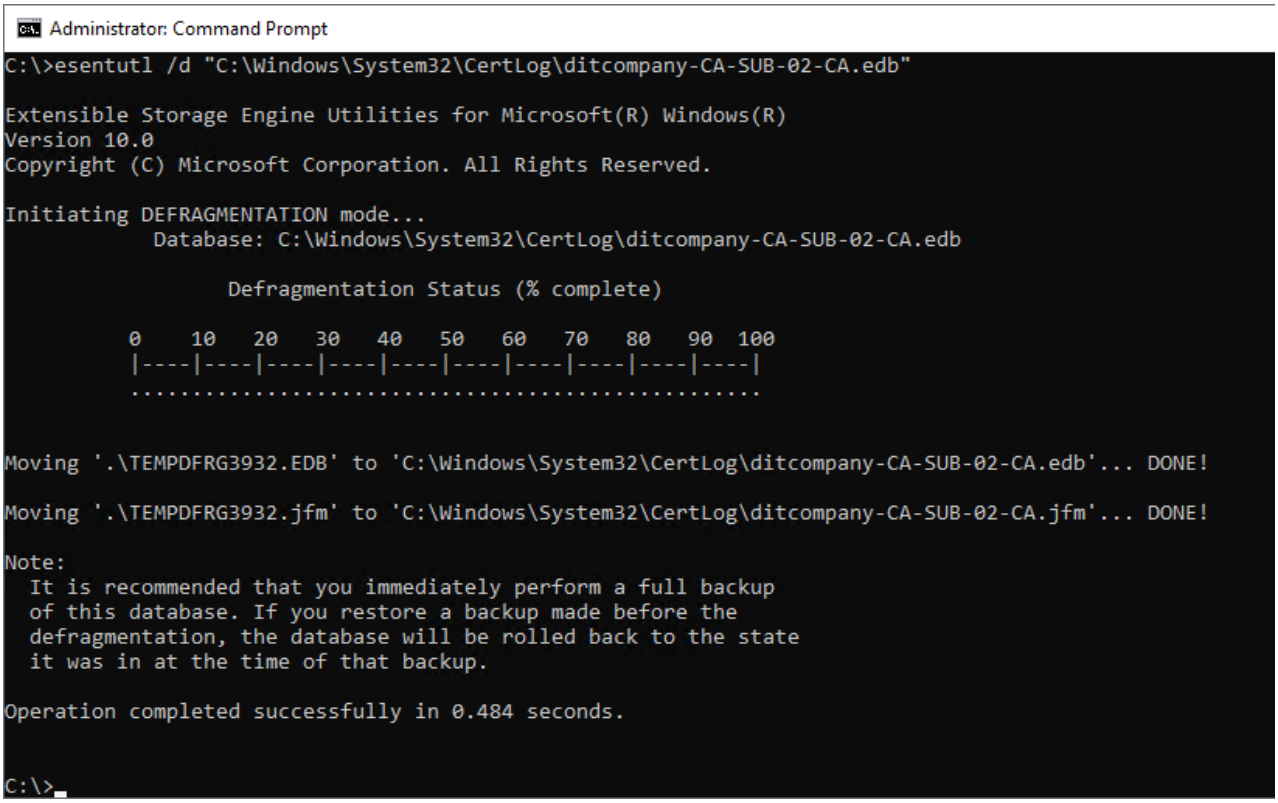
To remove the white spaces we are going to defragment the database. We do that with the command below:

```
Esentutl /d "<database path>"
```

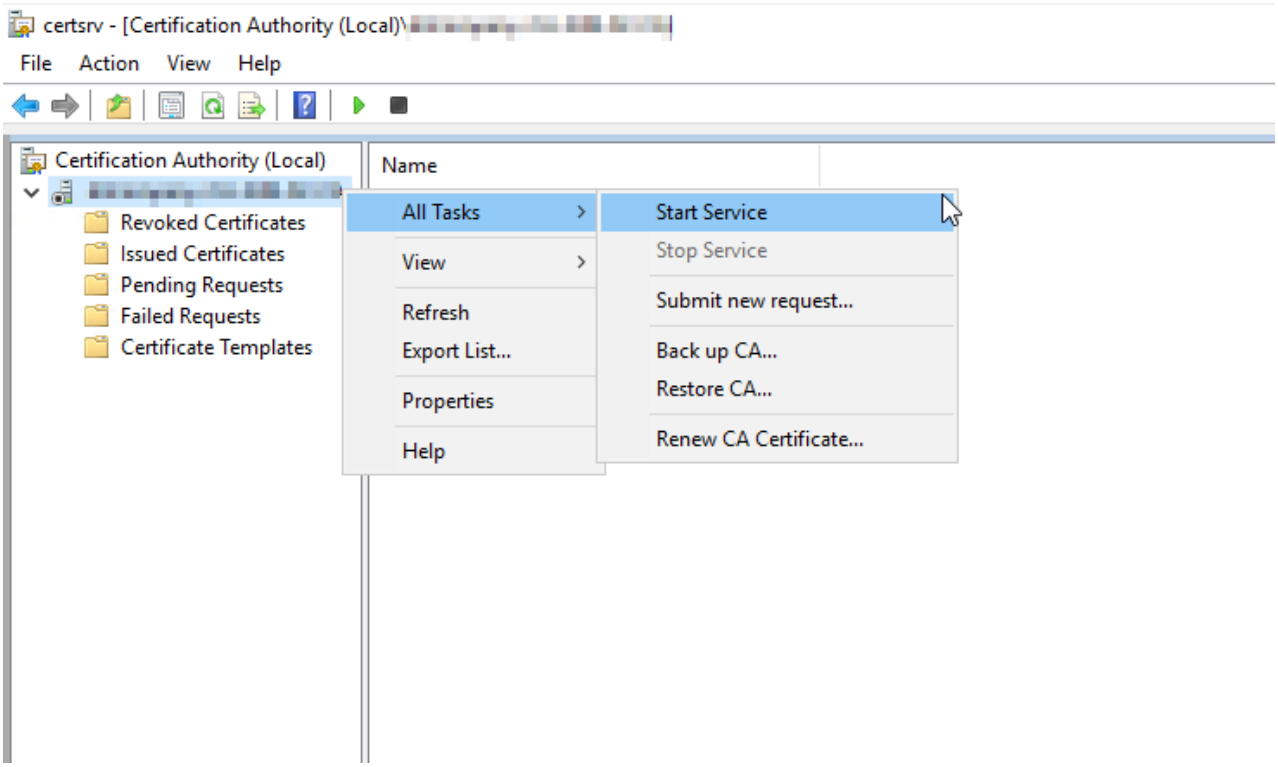
But before defragmenting the database, you must first stop the service. Keep in mind that because you stop the service, certificates cannot be temporarily issued either.



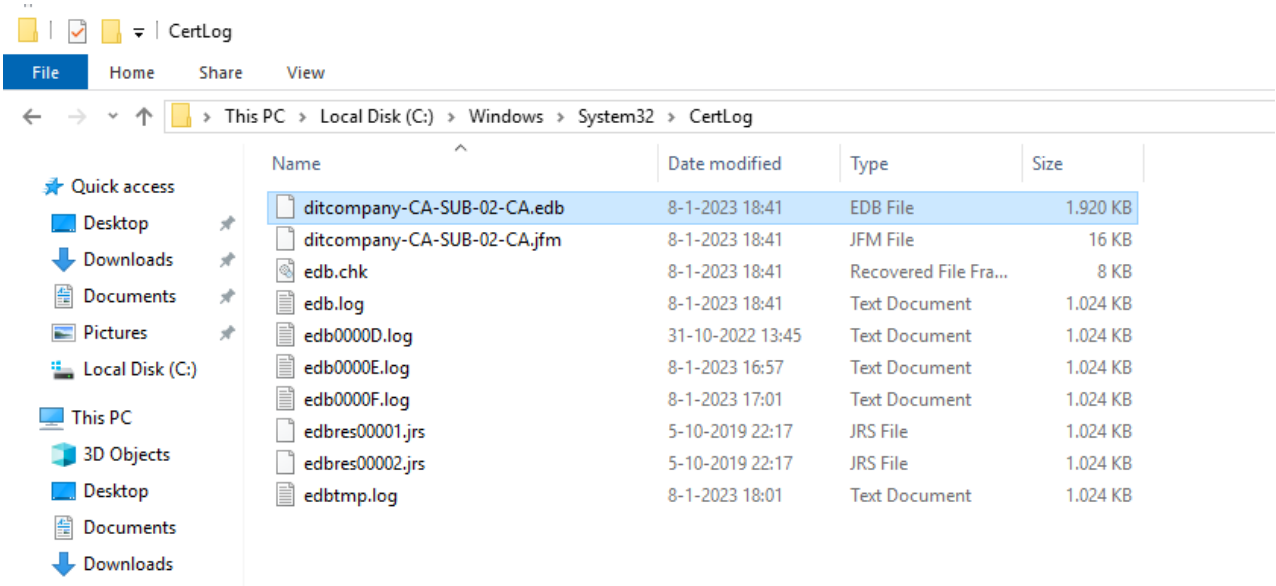
Now you can run the defragmenter by using esentutl /d.



After defragmenting is done successfully, you can restart the CA service.



Because I performed the work in a demo environment with only 10 certificates deleted, the results are not that great. Only 128 KB were freed. If you have an environment with thousands of certificates then you can imagine that the result is much bigger.


CertLog
File
Home
Share
View
This PC
Local Disk (C:)
Windows
System32
CertLog
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
This PC
3D Objects
Desktop
Documents
Downloads
Name
Date modified
Type
Size
ditcompany-CA-SUB-02-CA.edb 8-1-2023 18:41 EDB File 1.920 KB
ditcompany-CA-SUB-02-CA.jfm 8-1-2023 18:41 JFM File 16 KB
edb.chk 8-1-2023 18:41 Recovered File Fra... 8 KB
edb.log 8-1-2023 18:41 Text Document 1.024 KB
edb0000D.log 31-10-2022 13:45 Text Document 1.024 KB
edb0000E.log 8-1-2023 16:57 Text Document 1.024 KB
edb0000F.log 8-1-2023 17:01 Text Document 1.024 KB
edbres00001.jrs 5-10-2019 22:17 JRS File 1.024 KB
edbres00002.jrs 5-10-2019 22:17 JRS File 1.024 KB
edbtmp.log 8-1-2023 18:01 Text Document 1.024 KB