# 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 <u>CA Infrastructure</u>. 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          | per participation and the second   | BEGIN CERTI        | Web Server (WebServer)                     | eb Server (WebServer) 53000000235f1f 28-10-2022 ( |                            | 27-10-2024 09:07            |  |
| <b>-</b> 43 | THE RESIDENCE OF THE PARTY OF T | BEGIN CERTI        | Computer (Machine)                         | 530000002bba4                                     | 28-10-2022 15:14           | 28-10-2023 15:14            |  |
| <b>42</b>   | THE RESERVE AND ADDRESS OF THE PARTY OF THE  | BEGIN CERTI        | Computer (Machine)                         | 530000002a0f5                                     | 28-10-2022 15:13           | 28-10-2023 15:13            |  |
| <b>4</b> 1  | ALCOHOLD STREET  | BEGIN CERTI        | Administrator (Administrator)              | 530000002983e                                     | 28-10-2022 15:08           | 28-10-2023 15:08            |  |
| <b>4</b> 0  | NY CHRONOLOGIC CONTROL   | BEGIN CERTI        | Administrator (Administrator)              | 5300000028d8a                                     | 28-10-2022 15:03           | 28-10-2023 15:03            |  |
| 37          | NY DESCRIPTION OF THE PARTY OF  | BEGIN CERTI        | Computer (Machine)                         | 5300000025ccff                                    | 28-10-2022 09:10           | 28-10-2023 09:10            |  |
| ₹ 36        | THE RESERVE OF THE PERSON NAMED IN   | BEGIN CERTI        | Computer (Machine)                         | 53000000240c4                                     | 28-10-2022 09:09           | 28-10-2023 09:09            |  |
| <b>3</b> 29 | THE RESIDENCE OF THE PARTY OF T | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 530000001df8d                                     | 9-6-2022 11:58             | 9-6-2023 11:58              |  |
| <b>28</b>   | ALCOHOLOGY DATE:   | BEGIN CERTI        | SCCM Client Distribution Point Certificat  | 530000001c180                                     | 9-5-2022 15:08             | 9-5-2023 15:08              |  |
| <b>27</b>   | No. of Street, Street, Street, Street,   | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 530000001b7ca                                     | 9-5-2022 15:08             | 9-5-2023 15:08              |  |
| <b>2</b> 6  | NY CHIEF CONTROL OF THE  | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 530000001acd1                                     | 1-5-2022 11:43             | 1-5-2023 11:43              |  |
| <b>25</b>   | THE RESIDENCE OF THE PARTY OF T | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 5300000019ad7                                     | 1-5-2022 11:42             | 1-5-2023 11:42              |  |
| <b>=</b> 24 | THE RESERVE AND ADDRESS OF THE PARTY OF THE  | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 530000001860a                                     | 12-4-2022 07:11            | 12-4-2023 07:11             |  |
| <b>2</b> 3  | SCORPANICO SER   | BEGIN CERTI        | Domain Controller Authentication (Kerb     | 5300000017696                                     | 23-12-2021 08:34           | 23-12-2022 08:34            |  |
| <b>2</b> 2  | STATE OF THE PARTY | BEGIN CERTI        | Domain Controller Authentication (Kerb     | 53000000169d8                                     | 23-12-2021 08:30           | 23-12-2022 08:30            |  |
| 🕎 21        | NY CHRONICAS DE LA CONTRACTOR DE LA CONT | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 5300000015b4e                                     | 23-12-2021 01:40           | 23-12-2022 01:40            |  |
| <b>3</b> 20 | Control of the Contro | BEGIN CERTI        | Kerberos Authentication (1.3.6.1.4.1.311   | 5300000014b65                                     | 23-12-2021 01:11           | 23-12-2022 01:11            |  |
| <b>3</b> 19 | The state of the s | BEGIN CERTI        | Domain Controller Authentication (1.3.6    | 5300000013564                                     | 23-12-2021 01:11           | 23-12-2022 01:11            |  |
| 🕎 18        | SECURE OF SECURE | BEGIN CERTI        | Directory Email Replication (1.3.6.1.4.1.3 | 530000001254a                                     | 23-12-2021 01:11           | 23-12-2022 01:11            |  |
| <b>=</b> 17 | pro-contention across editors  | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2 | 5300000011c59                                     | 23-12-2021 00:01           | 23-12-2022 00:01            |  |
| <b>3</b> 16 | SECURIOR SEC | 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          | Control of the Contro | BEGIN CERTI        | CA Exchange (CAExchange)                   | 530000001ea0e                                     | 22-10-2022 14:31           | 29-10-2022 14:41            |  |
| <u></u> 9   | PROPERTY AND ADDRESS.  | BEGIN CERTI        | SCCM Web Server Certificate (1.3.6.1.4.1   | 53000000098ь5                                     | 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 <u>Certutil.exe</u>. 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

```
C:\>Certutil -backupDB c:\temp
Full database backup for CA-SUB-02.ditcompany.com\ditcompany-CA-SUB-02-CA.
Backing up Database files: 100%
Backing up Log files: 100%
Truncating Logs: 100%
Backed up database to c:\temp.
Database logs successfully truncated.
CertUtil: -backupDB command completed successfully.

C:\>_
```

#### 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

```
Administrator: Command Prompt

C:\>certutil -deleterow 01/01/2023 cert

Rows deleted: 10

CertUtil: -deleterow command completed successfully.

C:\>_
```

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.

| 🙀 Certification Authority (Local) | Request ID                               | Requester Name   | Binary Certificate | Certificate Template   | Serial Number  | Certificate Effective Date | Certificate Expiration Date      |
|-----------------------------------|--|--|--------------------|--|----------------|----------------------------|----------------------------------|
| Revoked Certificates              | 35 35 35 35 35 35 35 35 35 35 35 35 35 3 | OTO DEPOP AND DESCRIPTION  | BEGIN CERTI        | Web Server (WebServer)   | 53000000235f1f | 28-10-2022 09:07           | 27-10-2024 09:07                 |
| Issued Certificates               | <b>43</b>                                | ON OHROMANIA SIGN  | BEGIN CERTI        | Computer (Machine)   | 530000002bba4  | 28-10-2022 15:14           | 28-10-2023 15:14                 |
| Pending Requests                  | <b>42</b>                                | ON OHROMOUS DOOR   | BEGIN CERTI        | Computer (Machine)   | 530000002a0f5  | 28-10-2022 15:13           | 28-10-2023 15:13                 |
| Failed Requests                   | <b>41</b>                                | The state of the s | BEGIN CERTI        | Administrator (Administrator)  | 530000002983e  | 28-10-2022 15:08           | 28-10-2023 15:08                 |
| Certificate Templates             | <b>40</b>                                | The second second  | BEGIN CERTI        | Administrator (Administrator)  | 5300000028d8a  | 28-10-2022 15:03           | 28-10-2023 15:03                 |
|                                   | 37                                       | OT SHOP MAN SUS  | BEGIN CERTI        | Computer (Machine)   |                | 28-10-2022 09:10           | 28-10-2023 09:10                 |
|                                   | 36                                       | OU OWNER OR STATE OF THE PERSON NAMED IN   | BEGIN CERTI        | Computer (Machine)   | 53000000240c4  | 28-10-2022 09:09           | 28-10-2023 09:09                 |
|                                   | 29                                       | STORMANDON STR   | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2   |                | 9-6-2022 11:58             | 9-6-2023 11:58                   |
|                                   | 28                                       | ENGLISHED AND AND  | BEGIN CERTI        | SCCM Client Distribution Point Certificat  | 530000001c180  | 9-5-2022 15:08             | 9-5-2023 15:08                   |
|                                   | 27<br>26                                 | THE RESIDENCE OF THE PARTY OF T | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2<br>SCCM Client Certificate (1.3.6.1.4.1.311.2 |                |                            | 9-5-2023 15:08<br>1-5-2023 11:43 |
|                                   | <u>□</u> 25                              | OTO DEPOSITION OF THE PARTY OF  | BEGIN CERTI        |  |                |                            | 1-5-2023 11:43                   |
|                                   | <u>□</u> 23                              | 00 349 CO F CO   | BEGIN CERTI        | SCCM Client Certificate (1.3.6.1.4.1.311.2   |                |                            | 12-4-2023 07:11                  |
|                                   | ingi ∠4                                  |  | DEGIN CENTI        | occivi ciieni cerunicate (1.5.0.1.4.1.511.2  | J30000001000a  | 12-4-2022 07:11            | 12-4-2023 01:11                  |

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.

```
Administrator: Command Prompt

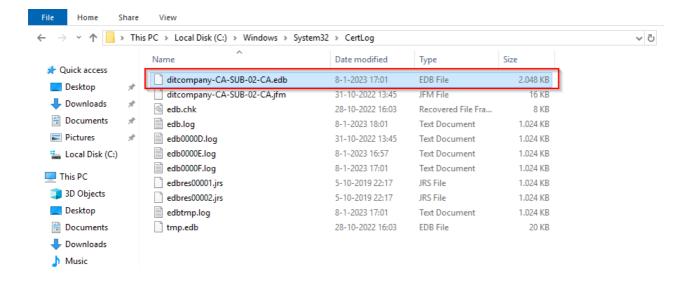
C:\>certutil -deleterow 01/01/2023 request
Rows deleted: 0

CertUtil: -deleterow command completed successfully.

C:\>_
```

## Compact the CA Database

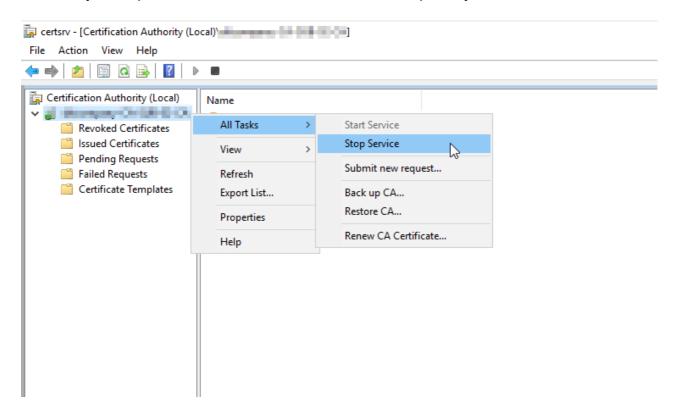
Now that we are almost at the end, we need to perform one more step and that is to extract the white spaces (defragmentation) from the database. To do this we use <u>Esentutl</u>. First we need to find out the path to the database. By default, the database is located in the folder "C:WindowsSystem32CertLog". 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>"

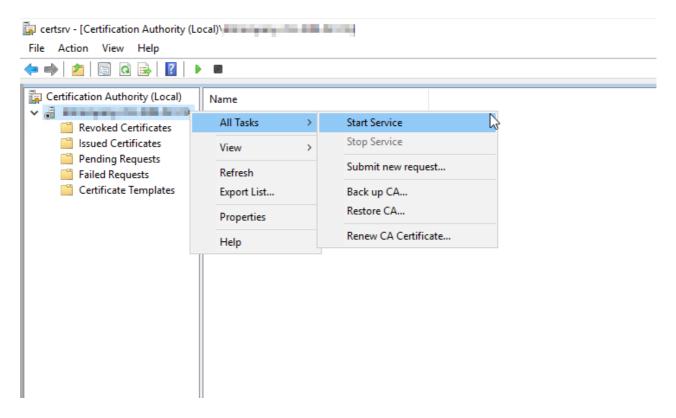
But before defragmenting the database, you must first stop the service. Keep in mind that because you stop the service, certificates cannot be temporarily issued either.



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

```
Administrator: Command Prompt
C:\>esentutl /d "C:\Windows\System32\CertLog\ditcompany-CA-SUB-02-CA.edb'
Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.
Initiating DEFRAGMENTATION mode...
            Database: C:\Windows\System32\CertLog\ditcompany-CA-SUB-02-CA.edb
                   Defragmentation Status (% complete)
                     20 30 40 50 60 70 80 90 100
Moving '.\TEMPDFRG3932.EDB' to 'C:\Windows\System32\CertLog\ditcompany-CA-SUB-02-CA.edb'... DONE!
Moving '.\TEMPDFRG3932.jfm' to 'C:\Windows\System32\CertLog\ditcompany-CA-SUB-02-CA.jfm'... DONE!
Note:
 It is recommended that you immediately perform a full backup
 of this database. If you restore a backup made before the defragmentation, the database will be rolled back to the state
  it was in at the time of that backup.
Operation completed successfully in 0.484 seconds.
```

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.

