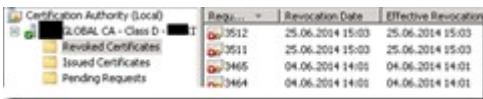


HowTo: Cleanup expired certificates from a Microsoft CA with Powershell and Shrink the DB Part 1 of 2

Written by:
12/18/2014
10:19:00 AM



Request ID	Revocation Date	Effective Revocation Date
3512	25.06.2014 15:03	25.06.2014 15:03
3511	25.06.2014 15:03	25.06.2014 15:03
3465	04.06.2014 14:01	04.06.2014 14:01
3464	04.06.2014 14:01	04.06.2014 14:01

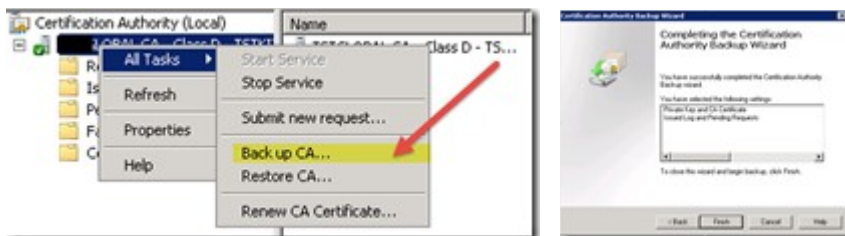
When you are running a Microsoft CA / PKI infrastructure, there are a few maintenance tasks like cleaning up expired or failed certificates from the database and then shrinking your DB at the end to “cleanup” the whitespace.

This article shows you , how to do this by using my powershell script “Cleanup_MSPKI_Cert_v1.1.ps1”.

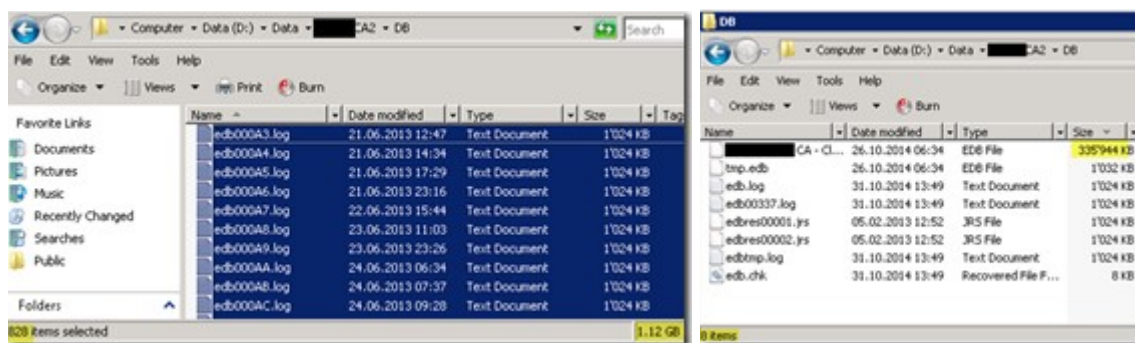
Regularly (depending on number of issued certificates) you have to perform a cleanup of expired certificates from your CA (Certification Authority) DB and then shrink the db to get rid of the “white space”.

You have to perform the following 3 steps in order:

1. make a backup of your CA DB (protected with a password) to another Server / medium



- this backup also "removes" the maybe hundreds of db log files (each of the has a size of 1 MB) – in my case 828



2. cleanup all expired certificates from all 4 categories with my PowerShell Script



- in a first step it's the best to run the script in a "view only" modus to see which certificates would be deleted

- **the script and all the details are explained in the 2nd part of this series!** => Klick following link for part 2: [Part 2 of 2](#)

3. Shrink your CA database to get rid of the "whitespace"

- for this you use the **esentutl** tool with the "/d" (= defragmentation) option

```
C:\>esentutl
Usage Error: No mode specified.

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

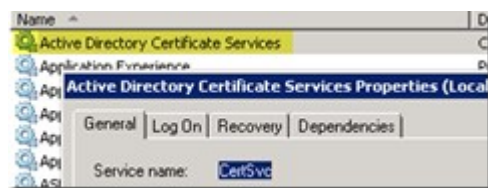
DESCRIPTION: Database utilities for the Extensible Storage Engine for Microsoft(R) Windows(R).

MODES OF OPERATION:
  Defragmentation: ESENTUTL /d <database name> [options]
  Recovery:       ESENTUTL /r <logfile base name> [options]
  Integrity:      ESENTUTL /g <database name> [options]
  Checksum:       ESENTUTL /k <file name> [options]
  Repair:         ESENTUTL /p <database name> [options]
  File Dump:      ESENTUTL /n[mode-modifier] <filename>
  Copy File:      ESENTUTL /y <source file> [options]

<<<<< Press a key for more help >>>>>
D=Defragmentation, R=Recovery, G=integrity, K=checksum,
P=repair, M=file dump, Y=copy file
=> _
```

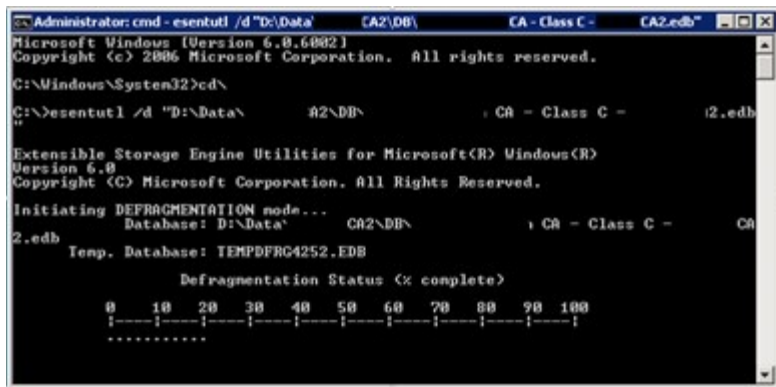
before executing the esentutl command stop the AD Certificate service and disable it

```
C:\>net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.
```

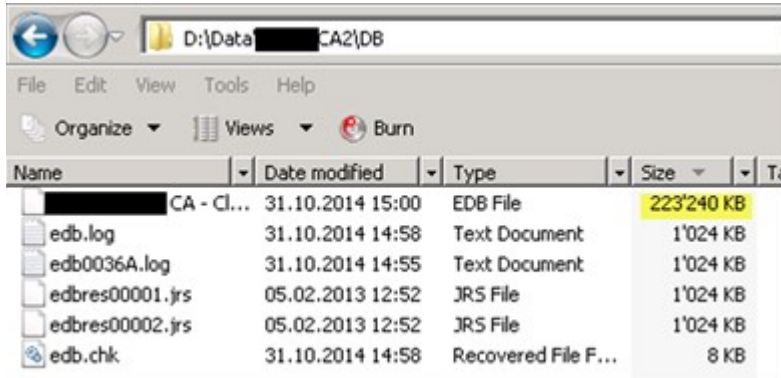


- run the following command with the path to the .edb DB file

```
esentutl /d "D:\Data\CA1\DB\CA - Class C - CA2.edb"
```



- at the end the db - file is more than 100 MB smaller than before!



- at this point you have to enable and start the CA Service again!

[The PowerShell Script from the 2nd step to easily cleanup the different expired certificates from the CA DB is explained in the following post:](#)

[HowTo: Powershell Script to cleanup expired certificates from a Microsoft CA Part 2 of 2](#)

[Further Information about the maintenance of a large CA database:](#)

“The Case of the Enormous CA Database”

<http://blogs.technet.com/b/askds/archive/2010/08/31/the-case-of-the-enormous-ca-database.aspx>