

## Re: Clustering Certificate Authority Server

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-11/0214.html>

---

**From:** Amihai Bareket ([amihai73\\_at\\_hotmail.com](mailto:amihai73_at_hotmail.com))

**Date:** 11/22/05

Date: Tue, 22 Nov 2005 08:26:05 +0200

Base CRL – Publish every 1 week, Valid for 2 weeks.

Delta CRL – Publish every 24 hours, Valid for 48 hours.

This means that I potentially have 24 hours to restore the CA in case of a crash before the CRL becomes invalid.

My organization requires high availability of each component where implementing, so a restore of the CA is a good solution for DRP, but wouldn't provide me with redundancy and availability.

A second CA would be a totally separate CA and cannot assume the functions of the first CA.

Are there any best-practices for achieving these goals?

Amihai

"Miha Pihler [MVP]" <[mihap-news@atlantis.si](mailto:mihap-news@atlantis.si)> wrote in message news:eV15jPu7FHA.740@TK2MSFTNGP11.phx.gbl...

> *Question: What did you set your CRL publication interval to?*

>

> --

> *Mike*

> *Microsoft MVP – Windows Security*

>

> "Amihai Bareket" <[amihai73@hotmail.com](mailto:amihai73@hotmail.com)> wrote in message

> news:eg\$%23M4t7FHA.2012@TK2MSFTNGP14.phx.gbl...

>> *Hi,*

>>

>> *Problem with a second CA as you've described it is that the certificates*

>> *issued by the CA are signed by him and he is the only one that's able to*

>> *revoke them.*

>> *Also, the CRL file is signed by that CA.*

>> *Can you think of a way that the second CA will be able to revoke*

>> *certificates or sign the CRL using the private key of the first CA?*

>> *This is the main goal I'm trying to achieve with CA redundancy.*

>>

>> *Amihai*

>>

>>  
>> *"Miha Pihler [MVP]" <mihap-news@atlantis.si> wrote in message*  
>> *news:uuz049p7FHA.3416@TK2MSFTNGP15.phx.gbl...*  
>>> *Hi,*  
>>>  
>>> *no, you can't cluster CA server with Windows 2003 server. I believe*  
>>> *there were some solutions on UNISYS...*  
>>>  
>>> *For redundancy -- you can set up more than one Enterprise CA. If you set*  
>>> *up e.g. two -- either of two can issue any certificate based on*  
>>> *configured templates. Templates are stored in Active Directory so either*  
>>> *of two CA servers can read them and issue certificates.*  
>>>  
>>> *--*  
>>> *Mike*  
>>> *Microsoft MVP – Windows Security*  
>>>  
>>>  
>>> *"Amihai Bareket" <amihai73@hotmail.com> wrote in message*  
>>> *news:uQJppYo7FHA.3976@TK2MSFTNGP15.phx.gbl...*  
>>>> *Is it possible to cluster Certificate Authority (CA) server using*  
>>>> *Windows Server 2003 cluster?*  
>>>> *The CA is an Enterprise CA.*  
>>>> *If possible, Is there a whitepaper that explains how to do it?*  
>>>> *If not, what other redundancy/availability options are possible for*  
>>>> *CAs?*  
>>>>  
>>>>  
>>>>  
>>>  
>>>  
>>  
>>  
>  
>