

Re: Certs for Domain Controllers–Trying to Prevent an Issue

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-03/msg00066.html>

- *From:* "Brian Komar \ (MVP)" <brian.komar.nospam@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 20 Mar 2008 10:04:29 -0500
-

Yes, I just finished the copy edits.
 Should be out in a few months
 Pre-orders are available at MSPress and Amazon
 Brian

"Jorge de Almeida Pinto [MVP – DS]" <SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxxxx>
 wrote in message [news:e\\$3ocamiIHA.1944@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:e$3ocamiIHA.1944@xxxxxxxxxxxxxxxxxxxxxxxx)

Hi Brian,

Just out of interest. I'm reading your w2k3 PKI book right now and like it very much. Will there be a w2k8 version?

--

Cheers,
(HOPEFULLY THIS INFORMATION HELPS YOU!)

Jorge de Almeida Pinto # MVP Windows Server – Directory Services

BLOG (WEB-BASED)--> <http://blogs.dirteam.com/blogs/jorge/default.aspx>
 BLOG (RSS-FEEDS)--> <http://blogs.dirteam.com/blogs/jorge/rss.aspx>

 * How to ask a question --> <http://support.microsoft.com/?id=555375>

- * This posting is provided "AS IS" with no warranties and confers no rights!
- * Always test before implementing!

 #####

"Brian Komar (MVP)" <brian.komar.nospam@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:ePdPEYmiIHA.6136@xxxxxxxxxxxxxxxxxxxxxxxx

Easiest would be to deploy a proper PKI (not piggy-backing a CA on a DC)
 You can use certutil -dcinfo deleteALL to replace the certs after the new PKI
 is deployed

Re: Certs for Domain Controllers–Trying to Prevent an Issue

You cannot restore the CA. If you read the installation warning, you cannot change the domain or NetBIOS name of the CA after installing Cert Services

Brian

"Christian" <nospam@xxxxxxxxxx> wrote in message

[news:VabEj.160559\\$3y2.117963@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:VabEj.160559$3y2.117963@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Reposting this issue. It was recommended that I post to this group from someone in the AD group.

We have three DC's, all running Windows Server 2003 w/SP2. DC1 is unstable, and needs to be demoted before there is a serious hardware failure. DC2 and DC3 have been brought online, and all of the FSMO roles have been moved to them. The one remaining issue is that DC1 issued the Domain Controller certs to DC2 and DC3. No other certs in our environment were created by DC1, just the Domain Controller certs for DC2 and DC3. What needs to be done in order to allow the demotion of DC1 out of AD without affecting the certs? This server will be salvaged after the demotion.

Thank you,

–Christian