

RE: Move Ent. Certificate Authority from DC and keep certs

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.migration/2005-01/0180.html>

From: Jon (Jon_at_discussions.microsoft.com)

Date: 01/09/05

Date: Sat, 8 Jan 2005 21:07:01 -0800

Thanks for the reply Bob,

It's good to know that this procedure applies to DCs as well – I didn't catch that.

However, it does state that the computer name must be the same for the new CA as the old. Is there any other way around this?

I did not clearly state in my last post that we have two DCs in this forest. DC1 and DC2. DC1 is the CA and is slated for demotion (or virtualization if we can get it to succeed). DC2 holds most of the FSMO roles except Infrastructure and Schema, so it is more 'active' in the domain/forest. If we back up DC1's CA in preparation to move it to DC2 (or another DC), then it sounds like we will need to demote DC1 before taking it offline and bringing a new DC1 (same computername) online to restore the CA to.

With that in mind, how will the AD objects handle a new computer with the same name as the old CA? Are the CA objects in AD associated with the computer account for the CA (e.g. SID) ?

Any insights greatly appreciated!

"Bob Qin [MSFT]" wrote:

> *Hi Jon,*
>
> *Thanks for your posting here.*
>
> *To move a CA from a DC to another DC, you can refer to the article of*
> *298138.*
>
> *HOW TO: Move a Certification Authority to Another Server*
> *<http://support.microsoft.com/?id=298138>*
>
> *It also apply to Domain Controller.*

microsoft.public.windows.server.migration: RE: Move Ent. Certificate Authority from DC and keep certs

>
> *Have a nice day!*
>
> *Regards,*
> *Bob Qin*
> *Microsoft Online Partner Support*
>
> *Get Secure! – www.microsoft.com/security*
>
> =====
> *When responding to posts, please "Reply to Group" via your newsreader so*
> *that others may learn and benefit from your issue.*
> =====
> *This posting is provided "AS IS" with no warranties, and confers no rights.*
>
> -----
> *Subject: Move Ent. Certificate Authority from DC and keep certs*
> *Date: Thu, 6 Jan 2005 13:11:01 –0800*
> *Newsgroups: microsoft.public.windows.server.migration*
>
>
> *Is it possible to move an AD integrated CA installed on a DC to*
> *another*
> *computer (AD DC or otherwise?).*
>
> *Our requirement is to demote an old DC with Enterprise CA installed*
> *and*
> *rebuild the hardware for different production server roles.*
>
> *The only Articles I have been able to locate are:*
> *ID 5551515 – Manually remove Enterprise CA from 2000/3 domain*
> *ID 298138 – Move a CA to another server (Windows 2000, Stand-alone)*
> *ID 555012 – How to move a CA to a new [DC] (this article is written*
> *very*
> *poorly and requires three computers to accomplish).*
> *Much searching of newsgroups and such have not netted any positive*
> *results*
> *yet.*
>
> *We have tried using VSMT but have not been successful yet. Failing*
> *this, we*
> *may have to demote the CA server and likely revoke all active certs*
> *and issue*
> *new ones on the new Ent CA. This will cause interruption of active*
> *services*
> *that use certs for secure (tunnelled, authenticated) communications,*
> *which*
> *could impact many users, therefore we would like to avoid that.*
>
> *Moving the EntCA is a last resort option, but I want to research it*
> *before*

RE: Move Ent. Certificate Authority from DC and keep certs

microsoft.public.windows.server.migration: RE: Move Ent. Certificate Authority from DC and keep certs

- > *we potentially have to use it. Any ideas, feedback, or experience you*
- > *can*
- > *share would be helpful.*
- >
- > --
- > *-Jon*
- >
- >
- >