

Re: Windows 2003 – Child domain cannot request certificate from root domain

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-01/msg00097.html>

- *From:* JulioHM <juliohm@xxxxxxxx>
 - *Date:* Thu, 24 Jan 2008 10:21:31 -0800 (PST)
-

Just read my own e-mail... I sound like a real foreigner!
(don't worry.. i really am one)

Gotta brush up my english.. hehehehe sorry :)

On Jan 24, 3:19 pm, JulioHM <juli...@xxxxxxxx> wrote:

I'm not quite sure what you mean by "properly"... we're not real experts on Windows network management. Where can I find more info on replication configuration for the windows network?

We've setup the network ourselves by the lack of a real expert for this in this project.

Things seem to be working fine now. We have automatic backups running every day, late at night, so if we need should be covered from any major disaster :)

Thanks for all the help!
Julio

On Jan 18, 9:53 pm, "Brian Komar" <brian.ko...@xxxxxxxxxxxxxxxxxxxx> wrote:

It sounds like you have replication problems (have you properly defined sites and subnets?)
Brian

"JulioHM" <juli...@xxxxxxxx> wrote in message

news:250f5491-a960-49e7-a861-9aa345c183f4@xx

Hi,

Thanks for the response. Eventually we got it working. We tried all kinds of permissions (your tip included)... and at the end of the day we found out that AD had not replicated permissions throughout the forest. Even though we completely shutdown and restarted ALL machines and domain controllers in the lab (several times), we had to force replication by using mmc snap-in "Active Directory Sites and Services".

Browse to "Sites > Default-First-Site-Name > Servers > YOUR_ROOT_DC > NTDS Settings"

Under that, you'll find your child domain controllers. Right click on each one and select "Replicate Now".

This got it all working. Now we know... all you need is the right permissions on the certificate template you want to use. Even though we changed permissions on the template, AD was taking much longer to replicate these settings throughout the forest (apparently this may take several hours).

Thanks a lot!
Julio

Re: Windows 2003 – Child domain cannot request certificate from root domain

On Jan 13, 6:49 am, "Brian Komar"
<brian.ko...@xxxxxxxxxxxxxxxxxxxx>
wrote:

The main thing is that you have to modify the permissions on the certificate templates you wish to issue. By default, permissions assume a single domain forest. You must change the permissions to allow users and computers from a child domain to request certificates from the CA>

- The certificate templates are edited using the Certificate Templates console (certtmpl.msc)
- By default, only Enterprise Admins and forest root Domain Admins have the permissions to edit the certificate templates.
- The certificate templates are stored in the Configuration naming context and replicated to all DCs in the forest (requiring the use of either global groups or universal groups for the permission assignments.

You can use of of two permission strategies.

- 1) Create a custom global group in each domain to represent the target users or target computers for the certificate template. Add both groups (based on the fact that you state you have a root domain and a child domain), and assign each group Read and Enroll permissions.
- 2) Create a custom global group in each domain to represent the target users or target computers for the certificate template. Add each global group to a custom universal group and assign the universal group Read and Enroll permission for the certificate template.

Certificate Request Wizard

The certificate request failed because of one of the following conditions:

- The certificate request was submitted to a Certification Authority (CA) that is not started.

- You do not have the permissions to request certificates from the available CAs.

OK

Apparently, as we have googled around, this message seems to have several possible reasons to show up. We've tried changing all kinds of permissions everywhere (templates, active directory) but without any luck.

Would anyone have any clue of how work around this?

Any help is appreciated.

Thanks
Julio