

Re: isolating a subdomain in AD

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-01/msg00212

- *From:* "chriss3 [MVP]" <removethis_christoffer@xxxxxxxx>
 - *Date:* Thu, 5 Jan 2006 15:41:52 +0100
-

Yes that is what the article is about, but his question in particular was to deny the enterprise admin to have any rights within a child domain ;)

--

Regards
Christoffer Andersson
Microsoft MVP – Directory Services

No email replies please – reply in the newsgroup

<http://www.chrisse.se> – Active Directory Resources

"Jorge de Almeida Pinto"

<SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxx> wrote in message
news:ONfdxmeEGHA.272@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

> EVERY domain admin in the forest can take over control, not just the
> enterprise admins

>

> --

>

> Cheers,

> (HOPEFULLY THIS INFORMATION HELPS YOU!)

> # Jorge de Almeida Pinto #

> BLOG --> <http://blogs.dirteam.com/blogs/jorge/default.aspx>

>

> * This posting is provided "AS IS" with no warranties and confers no
> rights!

> * Always test before implementing!

>

>

>

>

> "chriss3 [MVP]" <removethis_christoffer@xxxxxxxx> wrote in message

> news:eK9yFHZEGHA.1120@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>> Hello,

>> Dave is right!

>>

Re: isolating a subdomain in AD

>> Here is a few words that explains way it's not secure.
>>
>> Can a Domain Admin become a Enterprise Admin within a Forest
>> <http://www.chrisse.se/MAOB.asp?ID=51>
>> (Enterprise Admins are owners within the forest and can always take
>> ownership)
>>
>> If you want to look at real isolation have a look at the Multiple Forest
>> Consideration white paper:
>>
>> <http://www.microsoft.com/downloads/details.aspx?FamilyID=b717bfcd-6c1c-4af6-8b2c-b604e60067ba&DisplayLa>
>>
>> --
>> Regards
>> Christoffer Andersson
>> Microsoft MVP – Directory Services
>>
>>
>> No email replies please – reply in the newsgroup
>> -----
>> <http://www.chrisse.se> – Active Directory Resources
>>
>> "Dave Shaw [MVP]" <dhshaw@xxxxxxx> wrote in message
>> <news:%23mvJWsYEGHA.648@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
>>>I hate to tell you this, but there is no effective means to isolate a
>>>single domain within a forest from the Enterprise Admins. They have
>>>complete control over the forest.
>>>
>>> Here is the very best paper ever written on the subject –
>>>
>>> <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/actdid1.msp>
>>>
>>>
>>> -ds
>>>
>>>
>>> "John Czahor" <John.Czahor@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>>> <news:33DBA94F-CB41-4804-A793-7B935657902F@xxxxxxxxxxxxxxxxxxxx>
>>>>I have been asked to completly isolate a subdomain in AD. The Data is
>>>>very
>>>> sensitive and cannot be view by anyone includingthe enterprise admins.
>>>> There
>>>> will be only one admin to administritor to this sub domain (me). How do
>>>> I do
>>>> this? these users will still need to access thing within the forest.
>>>> Please
>>>> let me know.
>>>>
>>>> John
>>>>
>>>>

>>
>>
>
>

.

• *Follow-Ups:*

- ◆ [Re: isolating a subdomain in AD](#)
◇ *From:* Jorge de Almeida Pinto

• *References:*

- ◆ [Re: isolating a subdomain in AD](#)
◇ *From:* Dave Shaw [MVP]
- ◆ [Re: isolating a subdomain in AD](#)
◇ *From:* chriss3 [MVP]
- ◆ [Re: isolating a subdomain in AD](#)
◇ *From:* Jorge de Almeida Pinto

- Prev by Date: [Re: Mapped F Drive – group policy update problem](#)
- Next by Date: [Re: Old DHCP Server \[WildPacket\]](#)
- Previous by thread: [Re: isolating a subdomain in AD](#)
- Next by thread: [Re: isolating a subdomain in AD](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)