

## RE: restricted groups?

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2005-07/msg00542](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-07/msg00542)

---

- *From:* "skip" <[skip@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:skip@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 7 Jul 2005 13:47:07 -0700
- 

the way mutiple domain and multiple tree's in a forest work is there is a transitive trust relationship between all domain in the forest, this enables users from domainB to access resources in domainA and vice versa, but because each domain in a forest is a separate security boundary, then domain admins from domainA (if they are not in the local admin group on a client machine in domainB) cant manage machines in a separate domain, because of the security boundary, but if you add the domai nadmins group from domainA to the local built in administrator group in domainB then this will solve the issue

This would work I was under the  
> impression that you create a Universal Group and add the Domain Admins from  
> Domain A and then put that Group inside the Domain Local Administrators group  
> from Domain B.  
but doing it this way creates more steps

"lforbes" wrote:

- > Hi,
- >
- > Actually yes, I am understanding. Now I haven't done this because I only
- > have one Domain (so someone correct if I am wrong) however, I was under the
- > impression that you create a Universal Group and add the Domain Admins from
- > Domain A and then put that Group inside the Domain Local Administrators group
- > from Domain B.
- >
- > Here is the Group Rules in Native Mode according to MS. As you can see a
- > Domain Group cannot contain a Domain group from another Domain. You have to
- > use Universal Groups to do that.
- >
- > ~From Microsofts website~
- > [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/nesting\\_in\\_native\\_mode.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/nesting_in_native_mode.asp)
- >
- > A universal group can contain other universal groups, global groups and
- > accounts from any domain in any forest. A universal group cannot contain any
- > domain local groups.
- > A global group can contain other global groups and accounts from the same
- > domain that the group belongs to. A global group cannot contain any universal
- > groups, or any global group or account from another domain.

## RE: restricted groups?

> A domain local group can contain universal groups, global groups and  
> accounts from any domain or forest. A domain local group can also contain  
> other domain local groups from the same domain that the group belongs to. A  
> domain local group cannot contain other domain local groups from any other  
> domain or forest.  
>  
> Cheers,  
>  
> Lara  
>  
> "skip" wrote:  
>  
>> you are not understanding what i am trying to do. I want the domain admins  
>> group from domainA to be in the domain admins group in domainB  
>>  
>> "lforbes" wrote:  
>>  
>>> Hi,  
>>>  
>>> I only have a One Domain Forest/Tree. However, I think that you should  
>>> investigate Universal groups. They give you the option of "Cross domain  
>>> access"  
>>>  
>>> Cheers,  
>>>  
>>> lara  
>>>  
>>>  
>>> "skip" wrote:  
>>>  
>>>> Hi all  
>>>>  
>>>> I have a forest root that contains a separate tree and domain. I would like  
>>>> to add the domain admins group from the forest root domain to every machine  
>>>> that is in the separate domain. Can i use restricted groups to do this? i  
>>>> need to scan all machines on the network for missing patches but i cant scan  
>>>> the machines in the domainb.com domain because the domain admins group from  
>>>> domainA.com is not listed in the local admin group on the machines  
>>>>  
>>>> Example  
>>>>  
>>>> DomainA.com is the forest root, DomainB.com is a separate tree in the forest  
>>>> root.  
>>>>  
>>>> Thanks

- 
- *Follow-Ups:*
    - ◆ *Re: restricted groups?*

RE: restricted groups?

◇ *From:* Paul Williams [MVP]

◆ ***RE: restricted groups?***

◇ *From:* lforbes

• *References:*

◆ ***restricted groups?***

◇ *From:* skip

◆ ***RE: restricted groups?***

◇ *From:* lforbes

◆ ***RE: restricted groups?***

◇ *From:* skip

◆ ***RE: restricted groups?***

◇ *From:* lforbes

- Prev by Date: ***Re: AD Proxy***
- Next by Date: ***Re: 2 Way Trust***
- Previous by thread: ***RE: restricted groups?***
- Next by thread: ***RE: restricted groups?***
- Index(es):
  - ◆ ***Date***
  - ◆ ***Thread***