

Re: Preventing users from connecting to shares NOT on the domain..

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-01/0416.html>

From: Miha Pihler [MVP] (*mihap-news_at_atlantis.si*)

Date: 01/21/05

Date: Fri, 21 Jan 2005 22:05:57 +0100

Hi,

I believe this would work under few conditions.

First condition would be to set "Require Security" policy to "Restricted OU". As Roger mentioned this would be a computer policy and would apply to all computers in this OU. I am guessing that "Require Security" policy would also need some modifications to exclude domain controllers, DHCP server, etc. These computers could be excluded by IP address, but you would have to edit the policy...

If you want your clients from "Restricted OU" to communicate with rest of the domain you will have to put the other computers in separate OU and set "Respond Only" policy to this OU.

Getting this right may not be an easy task. Best advice I can give you is to setup a small lab and test the settings out. If you have any questions, feel free to post back.

--

Mike

Microsoft MVP - Windows Security

"Javier J" <no.mail@please.no> wrote in message
news:uAhzqhw\$EHA.3256@TK2MSFTNGP11.phx.gbl...

> Hi!

>

> The servers might be located on the same subnet of some of the clients.

> Not sure about that, would have to check the precise topology.

>

> The idea is:

> These 30+ Client PCs should only be able to access resources on

> computers located on the Domain.

>

> IIRC, all the servers are located on the same OU, but as for their IP

> addresses, I don't know if they're on the OU or not.

>

> To be more precise, the setup is as follows:

>

> + AD

> - Users: Most users are placed on the default container

> |

> - OU=Restricted: Ou where we've placed the "secure" client PCs and

microsoft.public.win2000.security: Re: Preventing users from connecting to shares NOT on the domain..

> related users.
>
> The OU has two GPOs, one for "Machine" and one for user. The "Machine" GPO
> is set to apply to all Authenticated Users. The "User" GPO _only_ is applied
> to the members of a "Restricted" group.
>
> The users of the "Restricted" group "suffer" a desktop as locked down as
> I've managed to get (Redirected Folders, Roaming User Profiles deleted on
> logoff, no "All Users" programs and folders, etc). The _ideal_ setup would
> be one where the "restricted" can't connect to any non-domain PC, while a
> "normal" user doesn't have to suffer any more restrictions than
> necessary...
>
> The rest of the users/PCs on the domain should still be running "as is",
> that's why