

Re: AD Design

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-05/msg00123

- *From:* Meinolf Weber [MVP-DS] <meiweb(nospam)@gmx.de>
 - *Date:* Mon, 4 May 2009 21:00:42 +0000 (UTC)
-

Hello John,

Within a new domain the domain admins can administer the complete domain, nothing else. If you add them to the Enterprise admins, they are able to administer the complete forest.

Domain admins:

Members of this group have full control of the domain. By default, this group is a member of the Administrators group on all domain controllers, all domain workstations, and all domain member servers at the time they are joined to the domain. By default, the Administrator account is a member of this group. Because the group has full control in the domain, add users with caution.

Enterprise admins(only appears in the forest root domain):

Members of this group have full control of all domains in the forest. By default, this group is a member of the Administrators group on all domain controllers in the forest. By default, the Administrator account is a member of this group. Because this group has full control of the forest, add users with caution.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! http://www.blakjak.demon.co.uk/mul_crss.htm

Hi Meinolf,

Thanks for your reply.

Just so I am clear – you are saying a new domain tree in the existing forest or a child domain of the existing domain are two options that would allow the local administrators access to manage their domain and not give them any permissions to any existing domains? A new domain is the best way to go I think as this is a new part to the business and would like its own identity and namespace.

Good point that I would need to run the exchange domain prep – forgot about that!!

Re: AD Design

Regards

John

"Meinolf Weber [MVP-DS]" wrote:

Hello John,

If they should not have any permission to the main domain, you can create a new forest tree or a child domain in the existing domain tree. For Exchange and mailbox access in the domain without exchange installed run exchange domainprep.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers

no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! http://www.blakjak.demon.co.uk/mul_crss.htm

Hi All,

I hope this is the correct place to ask my question.

We have a single forest active directory with two domain trees. We

are now starting another company within the business thousands of miles

away from our company head office. The new business will have its

own

IT department but some IT related work will still be done from HQ.

The IT team in the remote office will not need access to any resources

in the head office domain. We also have Exchange 2007 in the head

office that will hold the mailboxes for the users based in the new

company office.

My question is what is the best practice for creating a new domain

for the new business?? We don't want the IT team in the new office

to have any control / admin permissions to the network / users etc

based at the head office.

I was thinking that a new domain in the existing forest would be

best. We can give some members of the IT Team domain

Re: AD Design

admin
permissions to the domain for the remote office but they
would not
have permissions to the head office domain unless their
account was
added to existing groups or they were delegated permissions.

Another option I was looking at was to create a new forest
but that
would create a new global catalogue / schema etc and
increase the
complexity of the network.

I am looking for views and opinions on how others would
implement AD
in this situation

Regards
John