

Re: Bit of advice on current AD structure.

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01400

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxx>
 - *Date:* Wed, 17 Jan 2007 20:02:52 -0500
-

You set up OU's for two main purposes. AD security delegation and Group Policy. The simpler your design, the better overall. If you can do everything you need to do from a GPO and security standpoint there is no reason to move to something more complex. Tidying up the hierarchy because it makes it nicer to look at should not be a consideration. Nor should you be doing it to make it easier for humans to find things because that is what searching is for.

So you need to figure out what your security and group policy strategy is, then make your design.

One of the best designs, in my mind relies on having provisioning tools. In that case you set up a single OU for users and then if needed you set up a couple of sub-OUs for GPOs. I think many companies get crazy with GPOs handling all software delivery etc through it. I am really not on board with that design. Most companies, IMO, can go with 5-7 main GPOs for users and be done with it. And usually out of those they tend to use maybe 3, very little control, a little bit of control, and then kiosk. Companies that do more are usually doing things ad hoc and find themselves in a mess a few years down the road. I am really disliking native delegation of security for user objects more and more as new apps come out and having rights to the users gives you rights to harm the apps, things like Exchange come to mind here where an admin who can directly manipulate user objects can cause nightmares for folks managing the Exchange Service.

Then depending on how far you go with provisioning, hopefully you did groups too then you can have an OU for your groups. Computers are the one item I haven't seen a lot of provisioning systems for though I don't understand why as they can be handled that way as well. It is likely because people feel it is a hassle to precreate computer accounts. Anyway, assuming you don't have provisioning for those items, you break them out into OUs that match your delegation model. So for instance if you manage/delegate by division, you will break out by division. If you do it by site, break out by site. Overall between those two, I highly prefer geography over corporate structure as the latter can change rapidly.

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Re: Bit of advice on current AD structure.

daniel.dryhurst@xxxxxxxxx wrote:

Hiya

I have just inherited a domain as part of my new job. The framework is there but it's very messy and not organised. However, one thing that has been done is to have two separate OU's one for users and one for computers.

There are no further divisions below the top level. Shortly I am going to be restructuring the tree, but I have since found out that a lot of other applications like the AV etc. has been set up to read from AD and these particular OU's – same with WSUS.

I don't want to make a huge amount of admin work as I'm on my own, but is there any disadvantage to keeping users/computers separate and just replicating the function/location divisions through each OU? Or is it best to completely start from scratch and just use the one OU with divisions that include both users and computers?

i.e. Is there any disadvantage to preserving the current OU's but just tidying them up into sub containers?

Thanks for any advice.