GROUP POLICY CENTRAL

Information about Group Policy for IT Administrators

Active Directory Structure Guidelines – Part 1

Posted by Alan Burchill on 23 July 2010, 8:00 pm

Isolate your Administrator Resources

If you are an organisation of any significant size you probably have a delegated cretin duties to specific teams (e.g. help desk or desktop support) via the way of administrator groups. This would allow you to easily grant the required permission for a IT support person to a specific user by only adding them to one group. However one of the permissions that is normally delegated is the ability to change group membership.

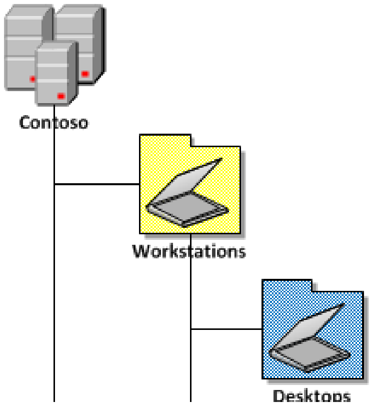
If all the groups in your organisation were in one location then a person who simply has the ability to add and remove member from group could in theory given them self more administrator access by adding them self to a higher level administrators group. To prevent this from happening you should segment all administrator or higher level permission group in the AD structure so that only the most trusted administrators can make changes to these admin groups.

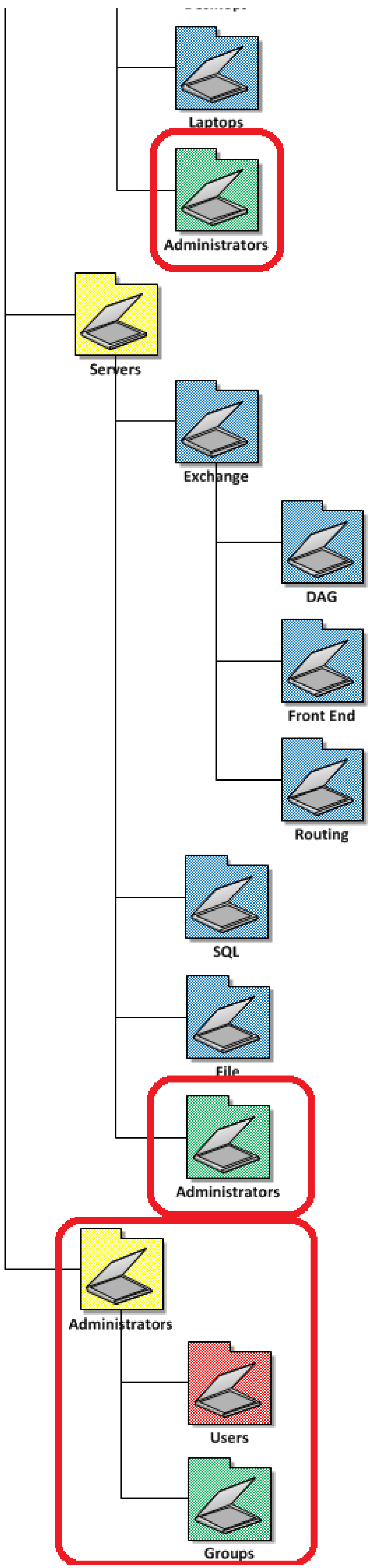
Also remember there is a difference from having administrator or delegated access to the Active Directory object and local administrator access to a computer. Therefore under each Workstations and Servers resources OU you may also want to consider creating an Administrators OU that contains the local administrator security group of the computers accounts in the top level OU's. This would also assist and being able to easily delegate administrator access to both the computers AD object but also local administration as they are all contained in the one location in AD.

Another reason to you have a dedicated Administrators OU at the top level is so that your administrator accounts are not subject to the same SOE Group Policy setting than the rest of your users. Administrator accounts should also be a separate accounts for IT administrators as their normal day to day accounts should be subject to the same configuration as the rest of the staff. While this is something that a lot of IT staff loath I think it is very good idea for IT staff to set the example as to how computers are configured and dogfood their own configuration. Ensuring that IT staff also have a separate administrator account also reduces greatly reduces the security risk associated with doing day to day operations (checking email, surfing web) with administrator permissions (see How to use Group Policy to make Windows 7 90% more secure).

For more information on assigning local administrator access to computers via group policy check out my other article How to use Group Policy Preferences to Secure Local Administrator Groups

Isolated Administrator OU Structure




Laptops
Administrators
Servers
Exchange
DAG
Front End
Routing
SQL
File
Administrators
Administrators
Users
Groups

REFERENCE

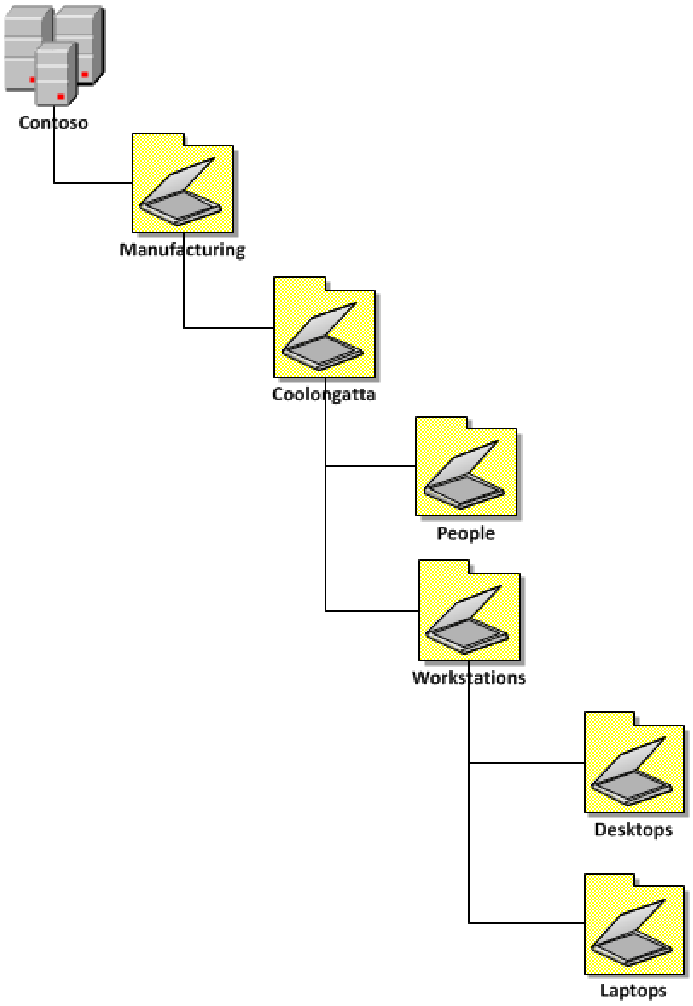
TechNet: Using Security Filtering to Apply GPOs to Selected Groups

> Create a separate OU for administrators and keep this OU out of the hierarchy to which you apply most of your management. In this way administrators do not receive most of the settings that that you provide for managed users.
>
> Have administrators use separate administrative accounts for use only when they perform administrative tasks. When not performing administrative tasks, they would still be managed.

Do you REALLY need more than 4 levels?

Below is an example of a combined Organisational / Location / Resources / Sub Resource model that you could consider for 4 level deep this structure or a variation of these levels should pretty much handle most any requirements of any organisation. As you can see from my examples below you would be fairly pushed to require an OU structure more than 4 level deep so ask yourself this question if you start to contemplate a 5+ level structure.

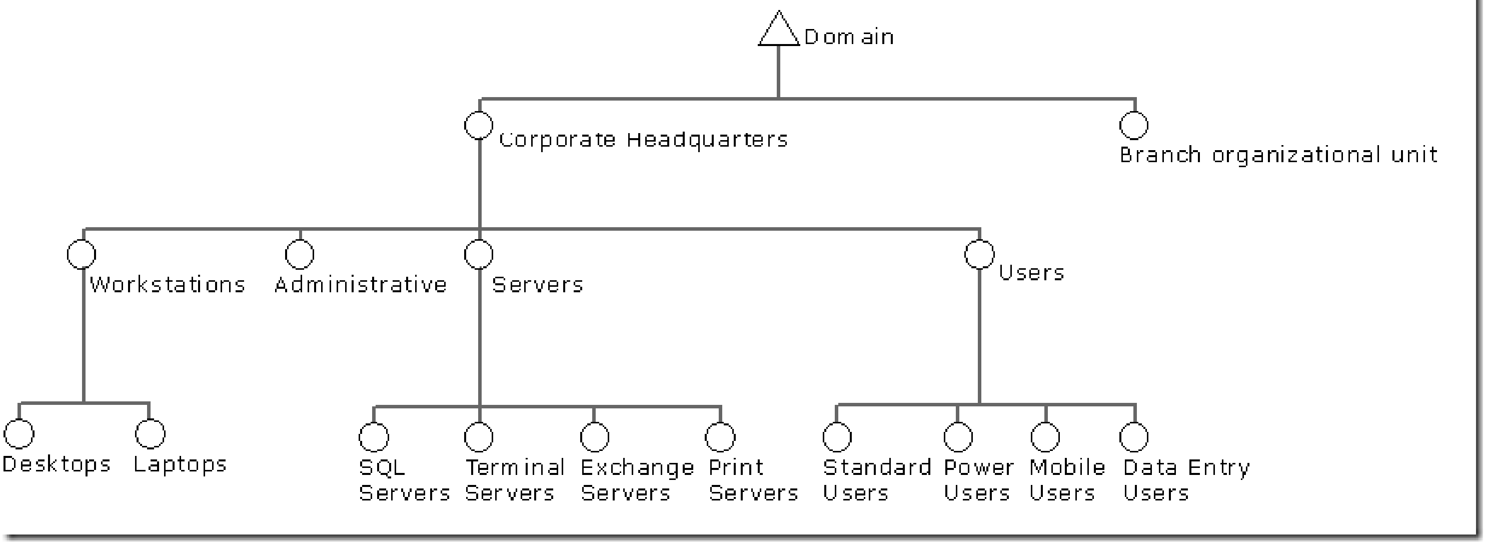
4 Level OU Structure



I am so confused… how about you just tell me what OU structure to use?

Ok. So your brain is probably about to explode with all the different OU types and you just don't know where to start. Well in the TechNet article Designing an OU Structure that Supports Group Policy we see a really good OU structure in Figure 2.3 Example OU Structure (see image below). You should be able to see how this is an three level OU structure combining Location/Resource/Sub-Recourse and that the naming convention of the structure match closely with guidelines we discussed above. You may find that this example will fit all your needs exactly or you may end up customising the design over time but either way this is a pretty good design that I have seen work in may organisations.

Figure 2.3 Example OU Structure



I hope the above AD design ideas have helped you design your organisations OU structure. Certainly there is no one size fits all model and you need to carefully consider your requirements before committing to a design.

Now I recommend that you you should visit the second part in this series where I list my Group Policy design rules which heavily depend upon. This should hopefully show you how designing a good OU structure can help you substantially make administering Group Policy (and your entire AD) a lot more easier.

Other References

- TechNet: Designing an OU Structure that Supports Group Policy
- Designing an OU Structure that Supports Group Policy

NEXT > Best Practice: Group Policy Design Guidelines – Part 2