Group Policy Design Guidelines – Part 2

Posted by Alan Burchill on 27 July 2010, 7:00 pm

Linking GPO's

Essentially there are three ways ways you can link a GPO to an AD structure firstly is to apply it to a OU secondly is to apply it to an AD Site and finally is to link it to a domain.

LINKING TO AD SITE

I have to say that you should NEVER consider applying a Group Policy to an AD site EVER!!!. Not only does applying a GPO to an AD site make troubleshooting an absolute pain you frequently finding yourself inadvertently applying a user or workstation GPO to your servers (This can be VERY BAD). AD Sites are based on IP subnets and I agree it can be very handy to apply settings based on the IP address of the computer (see How to use Group Policy Preferences to dynamically map printers with Roaming Profiles) and thankfully there is a way to now do this with Group Policy Preferences. Any of the new preference settings can be targeted using Preference Item-Level Targeting which gives you 27 different ways you can target your setting. The IP Address Range Targeting and Site Targeting target options will allow you to achieve the same targeting as applying the GPO to an AD Site however you are far less likely to make a mistake using this method as the GPO should be linked to resource OU that limits the scope of the policy to only a particular type of AD Objects (e.g. just workstations not servers).

LINKING TO OU

Linking a GPO to an OU is by far and away the most popular method of linking a GPO. This method allows for easily change the users configuration my moving them into the appropriate OU structure to have them configured. This method also fits well with the resource OU structure (see Part 1) so that you can disable parts of the GPO that don't apply to the object that you are apply the policy.

LINKING TO A DOMAIN

Technically you can apply a GPO to the Domain however this is more or less like linking it to the Root Organisational Unit. Linking it here will apply the policy to the entire domain so make sure that you are very careful when link a policy to this location. Policies should only be linked to the domain if you have a setting that you want to be applied to all users and/or computer in your entire domain. (See "Edit Default Domain Policies Sparingly" section above). The other scenario that you might want to link a policy here is if you want to make sure that you have at least your core policy setting applied to your "Users" or "Computers" container. But I would also recommend that you redirect these default locations for new objects so that you don't have to setup GPO's at the domain to cover these objects.

REFERENCES

TechNet: Linking GPOs

> If, however, the settings do not clearly correspond to computers in a single site, it is better to assign the GPO to the domain or OU structure rather than to the site.

TechNet: Linking GPOs

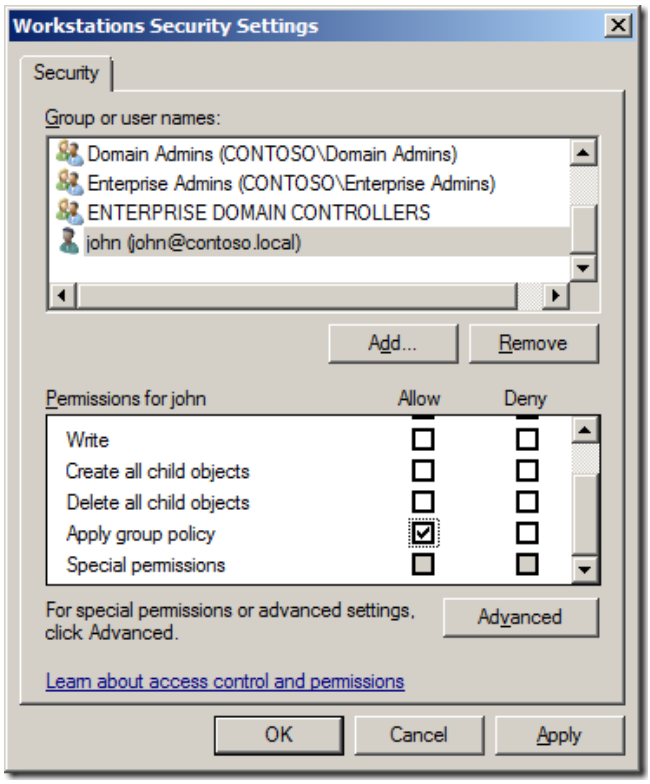
> Most GPOs are normally linked to the OU structure because this provides the most flexibility and manageability

When to filter

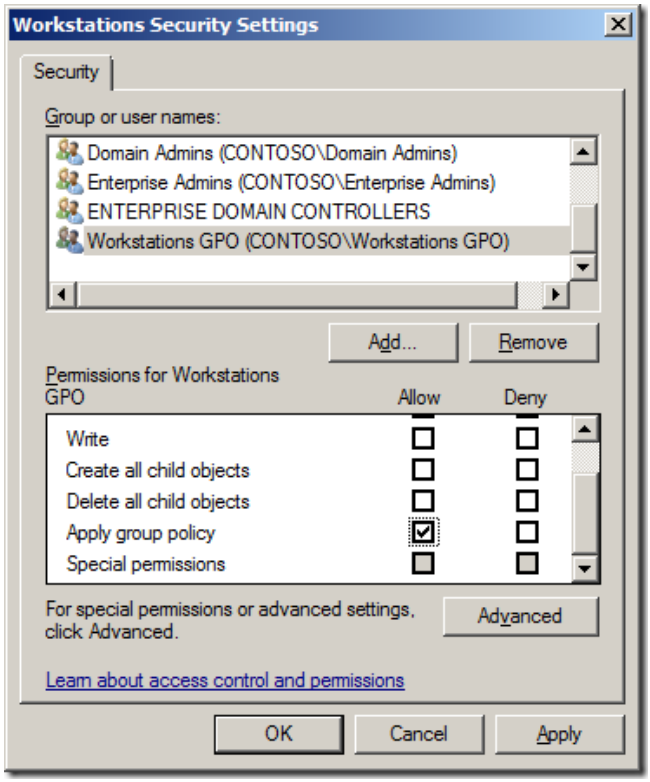
There are two ways you can filter your GPO when you apply then to your AD structure. Predominantly I find that Security Filtered Group Policy Objects is the most common way you can filter. Either way you should be filtering a GPO only when you want to exclude or include exceptions to the scope of the policy.

SECURITY FILTERED

This method allow you to apply Group Policy Objects to a cross section of users or computers in your organisation. I quite often have a security filtered policy that has my pilot users computers as members so that I can selectively apply settings to their computers first for testing (see "Create a Test Group Policy Structure" section above). As computers and users can also be a member of multiple GPO this also allows you to configure a users environment without having to spawn many number of levels of OU's that would other wise be necessary for every combination of GPO assignment (see "80/16/4 Example 3 & 4"). You can in theory apply a single user or computer to a GPO by adding them explicitly to the GPO under Advanced security (see image below).



However this is extremely poor practice and I would strongly recommend that you should always create a security group that has the "Apply Group Policy" permission assigned to it so that at a later stage you can assign users or computer to the GPO without modify the permission on the GPO itself (see image below).



I know the name "Workstation GPO" might seem to conflicting with the "Don't use the work "POLICY" or "GPO" in the GPO name" rule that however in this case "GPO" is justified as this is the name of a security group and so it is not obvious that a the security group is used as part of a Group Policy Object.

Recommendation: When removing "Authenticated Users" from the security filtering of a GPO ensure that you only remove the "Apply Group Policy" permission and not the "Read" permission as this will cause "Inaccessible GPO" error when any non domain admin tries to look a the GPO's via GPMC. See my previous post How to apply a Group Policy Object to individual users or computer for detail instructions on how to do this correctly.

REFERENCE

TechNet: Defining the Scope of Application of Group Policy

> If you have Read access to the domain, site, or OU, but not on one of the GPOs linked there, it will appear as **Inaccessible GPO**, and you will not be able to read the name or other information for that GPO

The exception to where you want to do this is if you have many GPO's that are security filtered and you want to ensure as fast a possible security processing then removing the read permission will "slightly" improve performance. So unless GPO processing time is an issues this doing removing the read is still not recommended.

TechNet: Determining the Number of Group Policy Objects

> If the Apply Group Policy permission is not set, but the Read permission is, the GPO is still inspected (although not applied) by any user or computer that is in the OU hierarchy where the GPO is linked. This inspection process increases logon time slightly.

Recommendation: You should only security filter GPO when the setting in the policy are mutually exclusive with all the other

GPO in your organisation. If you have two GPO's that are security filtered that configure the same setting and the user or computer are in both the group for that policy then only one policy will win out and you could end up with some fairly un-predictable results.

WMI FILTERS

WMI Filters have been around since Windows XP/2003 and are a great way to filter your Group Policy Objects based on the hardware of the computer that the policy is applied. However performing a WMI queries can take a substantial amount of time and if you have multiple WMI filters applying to your computers you have a significant performance decrease. Once again you can get around having to resort to using WMI Filters as Group Policy Preference Item-Level Targeting also have a number of options you can target hardware. Unlike WMI the Preference targeting engine has the performance advantage of being written in native code so it is much faster at determining what setting to apply.

They hardware targeting options are:

- Battery Present Targeting
- CPU Speed Targeting
- Disk Space Targeting
- MAC Address Range Targeting
- Operating System Targeting
- PCMCIA Present Targeting
- Portable Computer Targeting
- RAM Targeting
- As a legacy option you can even do WMI Query Targeting which allows you to easily port your pre-existing WMI queries into preferences. But be warned the WMI Query Targeting still suffers from the same performance issues.

So as you can see WMI Filters applied to the GPO object itself however just as in the "Where to Link" section above you will see Group Policy Preference will help you avoided having to rely upon WMI to often.

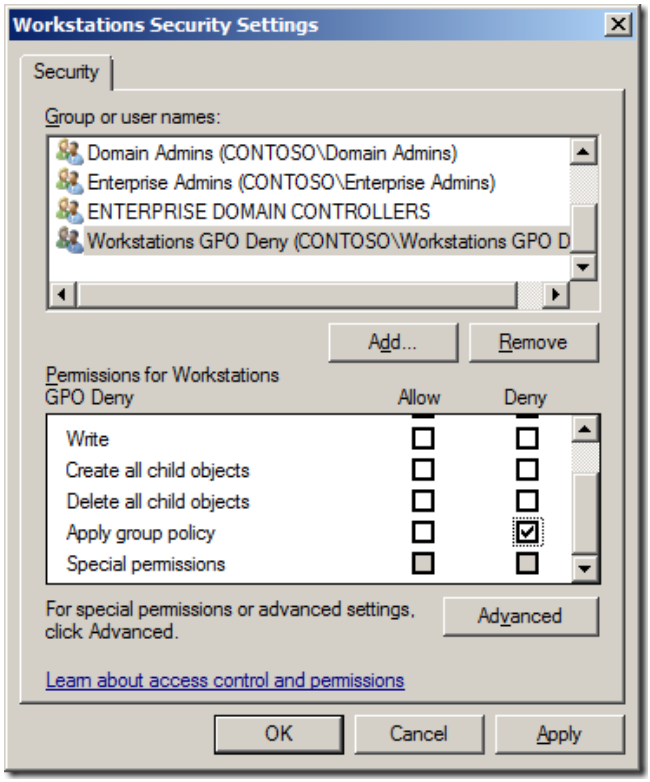
REFERENCE

TechNet: Applying WMI Filters

> WMI filters can take significant time to evaluate, so they can slow down logon and startup time.

Always create a deny "Apply group policy" security group

When creating a GPO always consider creating a security group and assigning it the Deny "Apply group policy" permissions (see image below) so that you have a simply way to exclude a particular user or computer from the policy in the future. Having this deny group applied to the GPO in advanced can save you a lot of time as it is often much easier and quicker to added a users to a security group than it is to modify the security on a GPO.

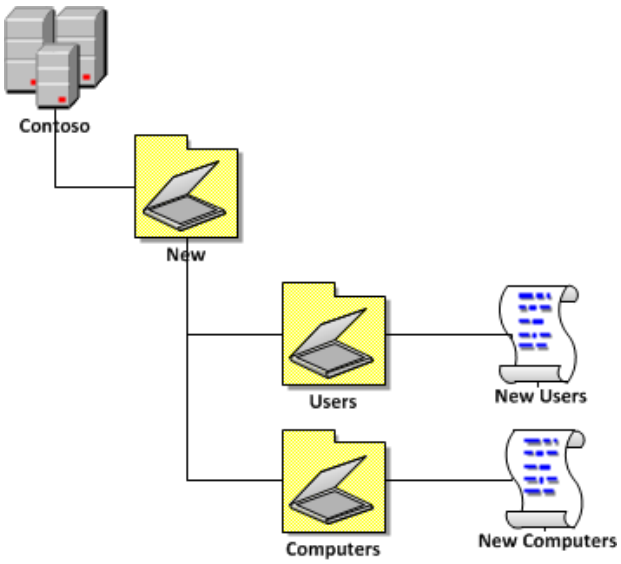


(Same as above) I know the name "Workstation GPO Deny" might seem to conflicting with the "Don't use the work "POLICY" or "GPO" in the GPO name" rule that however in this case "GPO" is justified as this is the name of a security group and so it is not obvious that a the security group is used as part of a Group Policy Object.

Apply GPO to New Users and Computers OU

In part 1 I recommended about setting up a new OU structure for any new user and computer that is created in your AD under the "Redirect New User and Computer Accounts" section. The reason why this was recommended was to enable you to easily apply a GPO to the default locations for these objects without having to resort to modifying the Default Domain Policy or by linking a new GPO to the entire domain.

It the example below I have created a simple GPO for each Users and Computers OU. Using this method your default user and computers will still receive the "Default Domain Policy" GPO and any additions settings in the two "New" GPO's.



I don't recommending linking the "People" or "Workstations" GPO's (See "Example Group Policy Designs" section below) as the New\Users and New\Computers OU as they could contain objects other than People and Workstations (e.g. Service Accounts or Servers). Instead I recommend that you only configured some basic security setting for the "New Computers" such as a default WSUS and patch install schedule so that any computers that are left in these OU's are at least kept up to date with security patches. Then for the "New Users" GPO you may want to configure a delayed logon script (see How to schedule a delayed start logon script with Group Policy) that notifies the users that they are not properly configured and they need to contact the help desk.

In any case even though you have configured these locations it is still very important that you establish some sort of regular process by which someone reviews the objects in these OU's and ensures they are moved into the appropriate locations so the proper policies are applied.

REFERENCES

Designing an OU Structure that Supports Group Policy

> …change the default location where new user and computer accounts are created so you can more easily scope GPOs directly to newly created user and computer objects

Use the 80/20 rule

Ok… this is the a rule in name only as it should also be considered as a guideline. Essentially you should try to put the vast majority of setting in a policy that applied to all your computer or users. Then you should apply the exception to the default policy to the subset only to the computers you want to apply these settings (see 80/20 Conceptual Design). If two scopes/levels of applying policies is not flexible for your organisation then you can even consider the 80/16/4 to give you more flexibility (4% equals 20% of 20%). Also note the smaller 4% scope does not necessarily need to be a complete subset of the 16% as it is possible that you want to apply location specific settings that have nothing to do with the organisational structure (see 80/16/4 Conceptual Design below).

When deciding what policy settings to put in the 80% of 20% GPO's make sure that you take another look at the "Monolithic vs. Functional GPOs" section above that talks about the different approaches you can take when configuration settings. As I said before the 80% policies are going lend them self to have more setting in them but they will probably be relatively static (i.e. Monolithic) where the 20% policies will have fewer settings but probably need to be updated more frequently (i.e.

Functional).

80/20 Conceptual Design	80/16/4 Conceptual Design
	

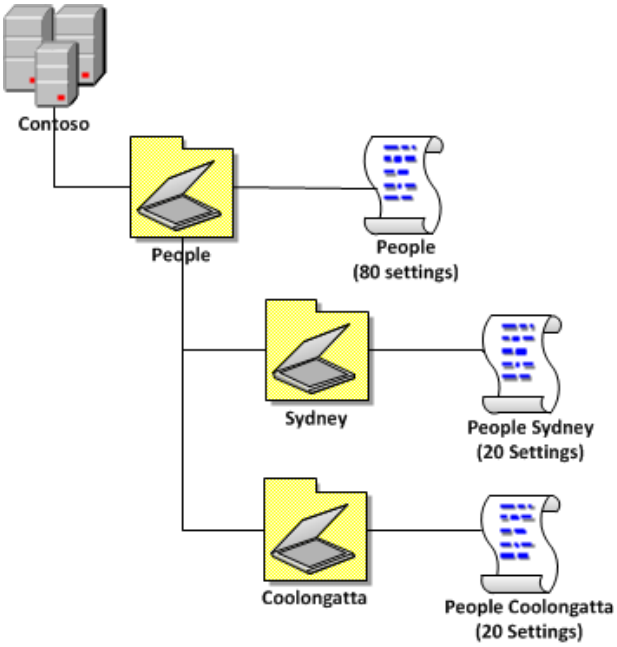
The conceptual designs above shows that there is only one level 2 and level 3 scopes to apply GPO but in reality there could be many different lower level policies that can be applied to your environment as seen in "80/16/4 Example 4".

Example Group Policy Designs

The organisation below that I use in the examples conveniently has 100 setting that they need to apply. Therefore they number of setting equals the percentage break down of the number of settings that are applied. In real world the number of setting are obviously going to vary greatly from single digits perhaps many thousands of settings.

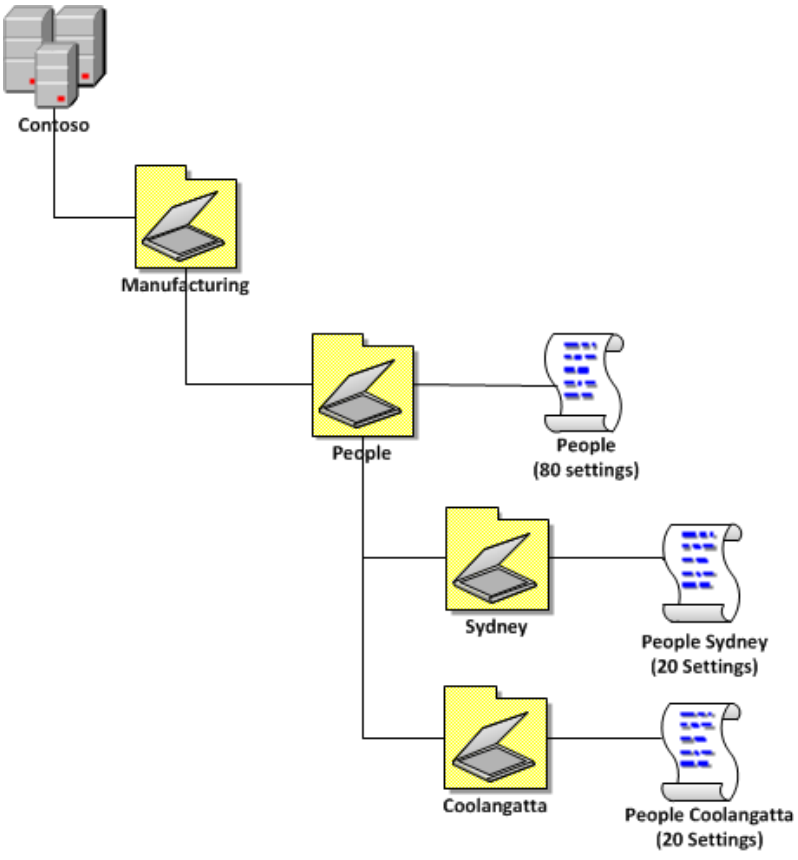
"80/20 Example" is a simple representation of how you would actually apply this in the real world. As you can see 80 setting are applied at the top level to all "People" OU and there then there are 20 settings site specific user settings. These location setting are typically drive and printer mapping setting that are specific to the site. While the "People" Group Policy Object will have setting that need to be applied to all users universally (e.g. screensaver time out value.)

80/20 Example 1



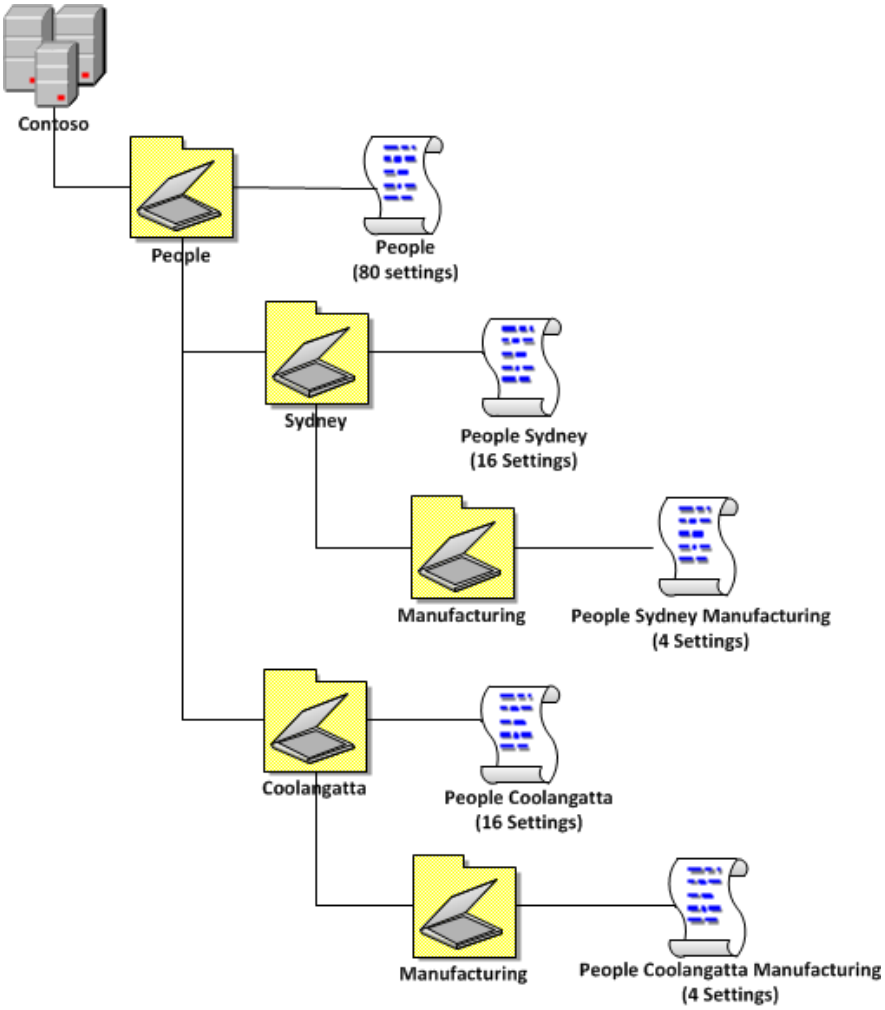
"80/20 Example 2" is the same as Example 1 except in this scenario the business has decided to have a top level organisational OU structure so that it will be easy in the future to separate parts of the organisation from the AD in the future. This illustrates that you do not need to have the same number of levels of OU's in your AD as the number of level of scope that you apply GPO's.

80/20 Example 2



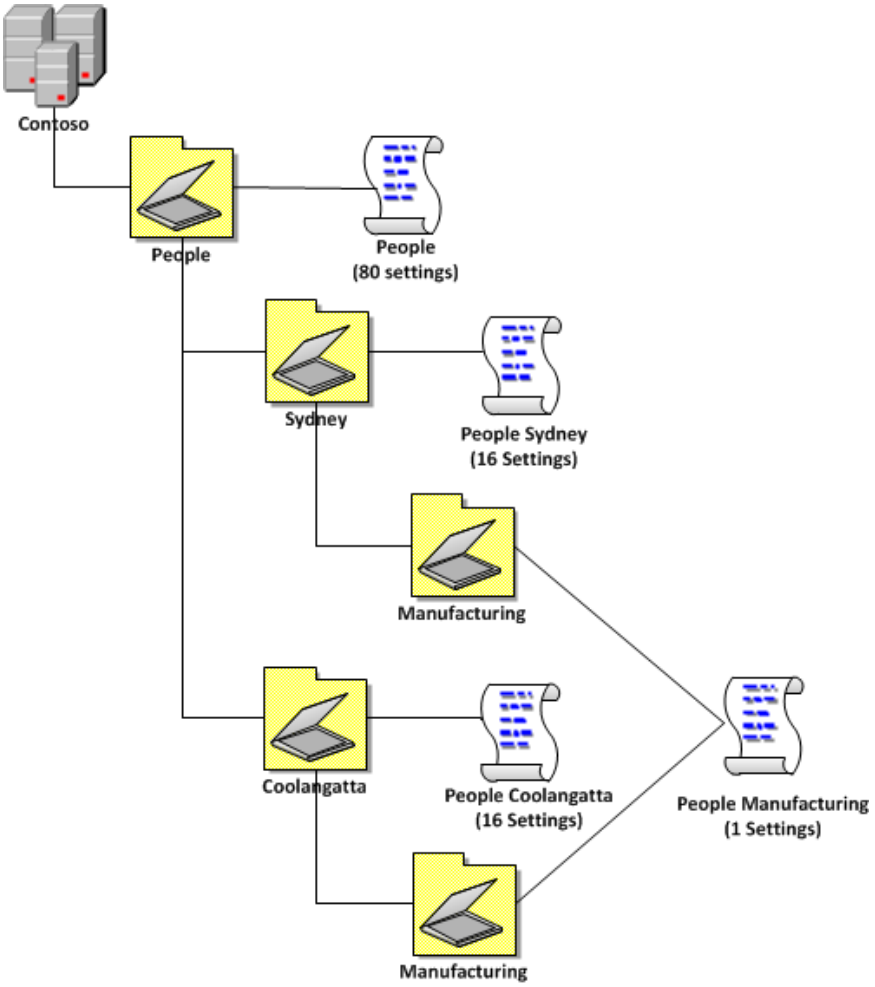
"80/16/4 Example 1" shows you how you would apply this to a "Three Tier OU Structure" (see part 1). The advantage of this model is that all setting are applied base on the OU structure and which means all policies are applied simple based on the location of the AD object in the OU structure. This is useful as you don't that you don't need to add and users (or computers) to security group.

80/16/4 Example 1



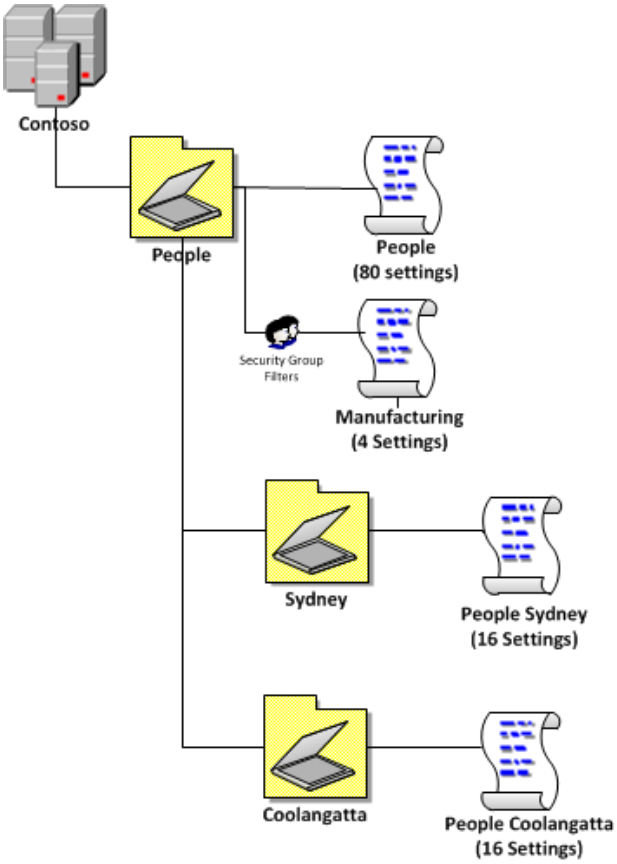
"80/16/4 Example 2" shows you what you can do when you only want to apply the same "Manufacturing" setting to all the users across all the sites. This takes into consideration the "Reuse GPO's where possible" rule (see above) and link a single manufacturing GPO

80/16/4 Example 2



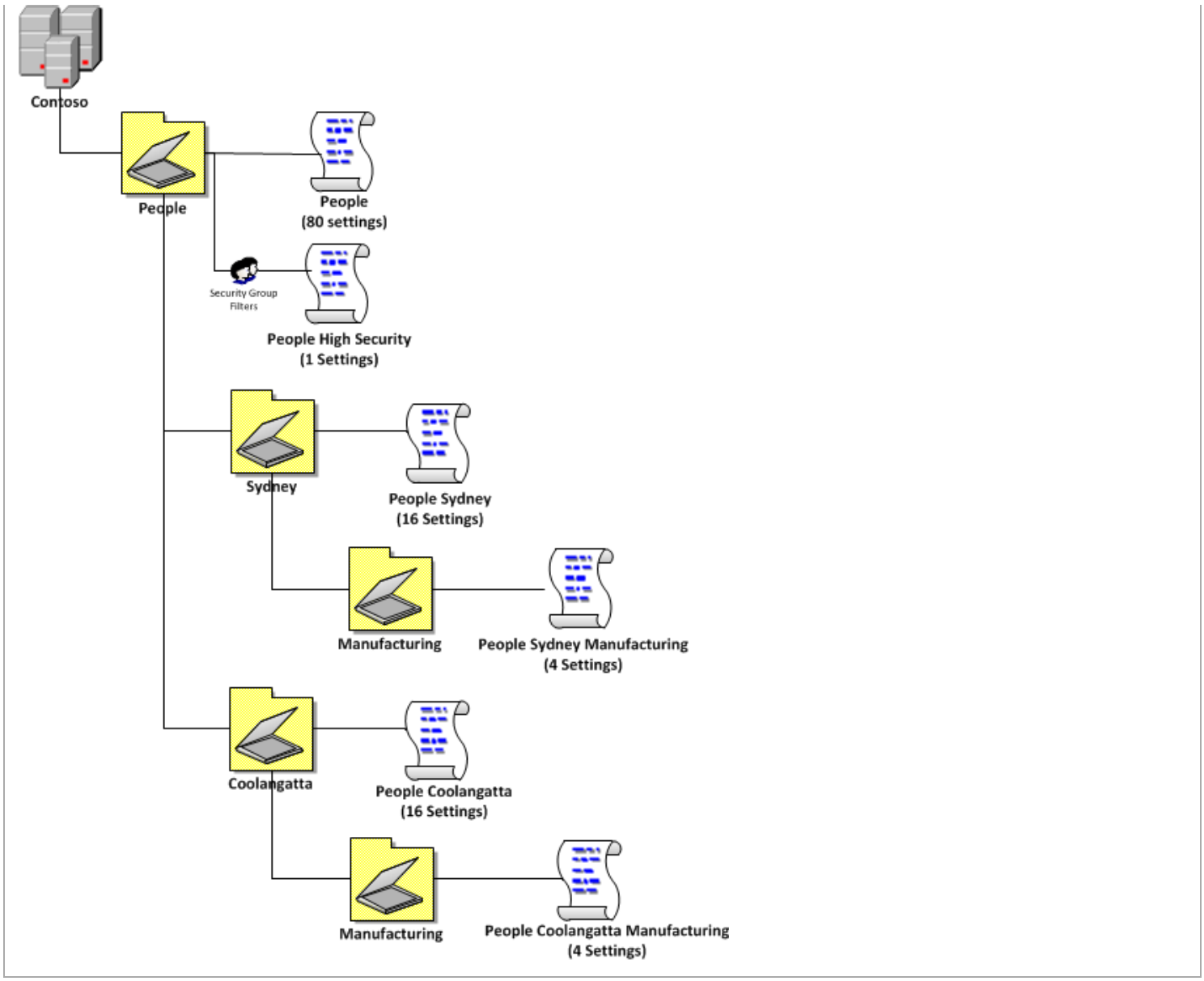
"80/16/4 Example 3" shows you how you could apply the policy differently using a single security group filtered policy at the top level but still have the same affect as the "80/16/4 Example 1". This is an example of applying a 3 level GPO structure to a 2 level OU structure as the "Manufacturing" simple by applying it at the top level but then applying a security group filter. The advantage of doing it this way is that you don't need to have as many OU deep (see "Go Wide not Deep" in part 1) and it avoids having to create a new Group Policy for the manufacturing users at each site (especially when they might be the same settings).

80/16/4 Example 3



"80/16/4 Example 4" shows a combination of "80/16/4 Example 1" and "80/16/4 Example 2" where the organisation has generally the same requirements of "Example 1" however they need to apply 1 high security setting (e.g. shorter screensaver timeout) that need to be applied to the managers computer because they normally deal with sensitive corporate information. This also illustrates that you can have multiple level 2 and level 3 GPO in the same environment and that level 3 GPO policies do not necessarily need to be a subset of level 2 policies (see conceptual circles above).

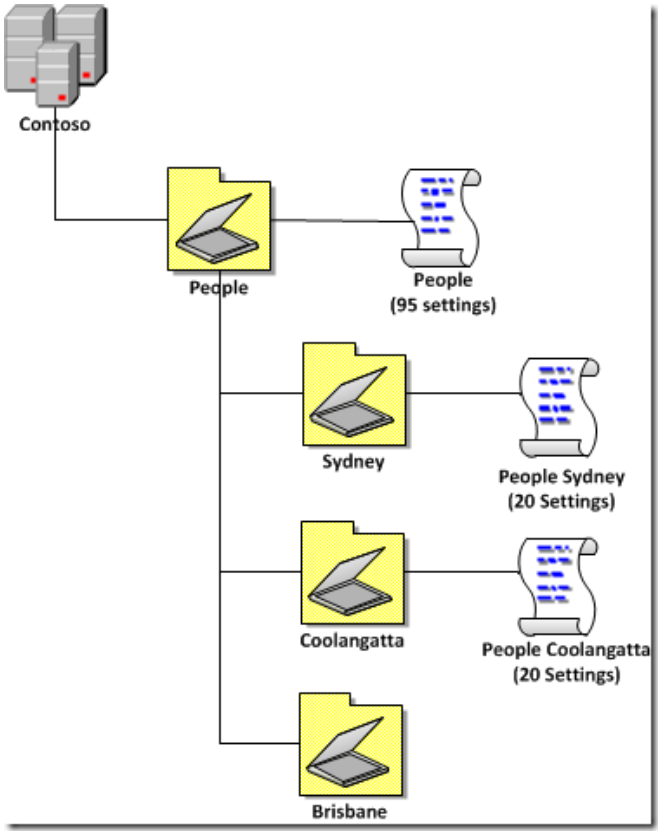
80/16/4 Example 4



Apply default settings on your 80% level one policy just in case

I know I have just gone though above that you should apply 80% of your settings in the highest policy however there is one problem with this. If for some reason a computer or users is placed in a top level OU or a second level OU is created without a policy applied to it or a user or computer has not been added to the correct security group this could leave gaps with the coverage of settings. So to get around this issue be sure that your level one 80% policies are configured with a default setting to cover your more essential configurations such as Screensaver timeout or WSUS servers.

In the example below we have 95 settings (or 95%) of the setting being applied to the users with the 20% being applied at the second level policy. Effectively only 80 settings (or 80%) will be actually be applied to the users from the top level policy as there is a 15% overlap of settings the settings. However a user in the "People" or the miss configured "Brisbane" OU will at least get 95 setting (or 95%) of the settings applied. This might not be a perfect configuration for them however it will at least mean they are compliant to the mandatory corporate configuration settings (e.g. Screensaver on and WSUS server configured).



In closing I hope this documents has helped you design your Group Policy infrastructure in your environment. If you have any other questions you want covered or you simply have a question about what I talked about above please feel free to post a comment…

Other References

Here is a list of link to other web sites that I have found useful in guiding my design decisions with group policy.

- Appendix A: GPO Scenario Policy Settings
- TechNet: Designing a Group Policy Infrastructure

Change Log

I plan for this to be a dynamic article that I will change over time and I am sure there will be a few errors along the way that will need correcting so below are the list of changes that I made to this article since it was originally published:

28/07/2010 – Add section for "Monolithic vs. Functional GPOs" from http://technet.microsoft.com/en-us/magazine/2008.01.gpperf.aspx by Darren Mar-Elia via Mike Kline

28/07/2010 – Corrected error in the WMI Filter sections that said they had been around since Windows 2000 (Should have said XP/2003). Thanks to Aaron Parker

2/08/2010 – Added mention to "How to Link" that you can link to the domain. Added more references to Microsoft TechNet articles. Added "Create a Test OU Structure"

3/08/2010 – Added “Apply GPO to New Users and Computers OU” section.

24/10/2011 – Added refrencec to Best Practices for DefautI Domain policies…

© 2016 Group Policy Central
Powered by WordPress | Theme F2 Metro.