

## Re: Lab Domain Layout – SOS

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2004-09/0232.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-09/0232.html)

---

**From:** Adrian Marsh (NNTP) (*marsh\_remove\_\_at\_lucent.com*)

**Date:** 09/02/04

Date: Thu, 02 Sep 2004 16:19:57 +0100

Hi Al,

login scripts are assigned to the GPO only, not NT4-style to the individual users (I've no NT boxes, so I'm trying to adopt the 2000 methods).

So the Servers and Workstation GPOs DO have logon scripts assigned at the User Configuration level. But because the labadmin user is assigned to the uk-lab\users container, it doesn't run any of the logon scripts when logging into a Servers PC (I'm guessing because the user is defined in a higher-level OU than Servers). Heres the problem. if I move the labadmin user –say– to the Servers GPO, then it'll run the scripts under Servers, but I don't think it'll be able to login to the Workstations.

I thought about a similiar layout as below:

```
domain
|_Lab
  |_Servers
  |_Workstations
```

...putting the labadmin user into the \_Lab OU/container and defining logon scripts at the \_Lab level, but then those scripts would run on both the \_Servers and \_Workstations – whereas I'd want it to run different scripts.

If I try to detect the OU within the logon script, then that beats the point of defining the scripts per GPO, and I may as well go back to having a logon script per user (NT style).

Reason for wanting the labadmin to be able to login to the Workstations as well is for backup.

I suspect theres another way of doing all this, using Group assignments, but can't see how.

Adrian

Al Mulnick wrote:

> *Hard to follow exactly, but in your situation there are no login scripts*  
> *assigned for the labadmin user, correct?*  
>  
> *I can't think why you'd want to put the labadmin account in the workstations*  
> *OU. That doesn't make any sense at all (to me anyway).*  
>  
> *I would think you might want to do something similar to the follow for OU*  
> *layout*  
>  
> *domain context*  
> *|\_Admins*  
> *|\_Corp*  
> *|\_Servers*  
> *|\_Workstations*  
> *|\_Users*  
> *|\_Groups*  
> *|\_Builtin*  
> *|\_computers*  
> *|\_Users*  
>  
> *Etc...*  
>  
> *That way you can attach user-specific and machine-specific GPOs to the*  
> *users. Your labadmin would reside in the corp/admins OU, while labuser*  
> *would be in corp/users OU. Assign the scripts appropriately remembering*  
> *that some settings are user-specific and some are workstation specific*  
> *meaning you may need a master script that checks which OU a user is in or*  
> *what groups etc and then making a decision as to which sub-functions to run*  
> *based on that information. Depends on what the scripts do.*  
>  
>  
> *"Adrian Marsh (NNTP)" <marsh\_remove\_@lucent.com> wrote in message*  
> *news:es9PVsOkEHA.3536@TK2MSFTNGP12.phx.gbl...*  
>  
>> *Hi,*  
>>  
>> *I'm trying to sort out my domain structure before deployment, but I'm*  
>> *hitting some snags. Main problem is in sorting out where in the structure*  
>> *User accounts should exist, and what groups they should be a member of,*  
>> *and how that affects the logon scripts.*  
>>  
>> *Heres the current Layout:*  
>> -----  
>> *uk-lab*  
>> *Builtin*  
>> *Computers*  
>> *Domain Controllers (OU)*  
>> *ForeignSecurityPrincipals*  
>> *Servers (OU) (Server Admins)*  
>> *Users (labadmin)*

>> *Workstations (OU) (labuser, labusergroup)*  
>> *Desktops A (OU)*  
>> *Desktops B (OU)*  
>> *Desktops C (OU)*  
>> *laptops (OU)*  
>> *test machines (OU)*  
>>  
>> *here are the users:*  
>> *labuser – part of the Workstations OU. member of the "labusergroup". Also*  
>> *a member of Domain User.*  
>> *labadmin – part of the Users container. member of "server admins group".*  
>> *Also a member of Domain Admin.*  
>>  
>> *here are the groups:*  
>> *labusergroup – Part of the workstations OU*  
>> *Server admins – Part of the Servers OU*  
>>  
>> *I have 5 GPO policies:*  
>>  
>> *uk–lab domain policy (top level)*  
>> *DC policies*  
>> *Servers Policy*  
>> *Workstations Policy*  
>> *test machines policy*  
>>  
>> *(Workstation policy will be inherited into child–OUs : laptops, etc.*  
>> *Intended to be able to setup different Automatic Update schedules, and*  
>> *test different settings on test machines).*  
>>  
>> *Seperate logon scripts are defined for both the Server OU, and Workstation*  
>> *OU.*  
>>  
>> *labuser is a member of Restricted Group (Administrator) under the*  
>> *Workstation OU.*  
>>  
>> *labadmin is a memeber of the Domain Admins.*  
>> -----  
>> *Heres my issue:*  
>>  
>> *I want labadmin to be able to logon anywhere (which is why I left it in*  
>> *the default users container). i only want labuser to be able to logon to*  
>> *computers held in the Workstations OU and below.*  
>>  
>> *At the moment, when labuser logs into Workstation PCs, all works well.*  
>>  
>> *But if labadmin logs into a machine on the Server OU, then none of the*  
>> *server logon scripts run. If i move the lab admin account into the*  
>> *Servers account, then will that account be able to log into the*  
>> *Workstation PCs??? Will the logon scripts for labadmin work?*  
>>  
>> *I want labadmin to be able to logon anywhere, but have the logon scripts*

>>run in reflection of the OU policy (i.e. Servers run "server" type  
>>scripts, Workstations run different sets).  
>>  
>>What am I missing about the setup of labadmin to be able to have it logon  
>>everywhere, and have appropriate scripts run?  
>>  
>>I've tried:  
>>  
>>– Moving the logon scripts for sever into the top–level OU (uk–lab), but  
>>then those scripts also run on any Computers in Workstation and below.  
>>– Moving the labadmin account into Servers. But then I'm unsure if  
>>labadmin is still able to logon to Workstation accounts. And how would  
>>logon scripts run?  
>>  
>>I just can't work out which OU to put labadmin in. Whichever OU I move him  
>>too i think he'll not be able to log into the other. obviously I've missed  
>>something simple ??  
>>  
>>Adrian  
>  
>  
>