PAW Security guide

azureblog.pl/2020/05/23/paw-security-guide

Robert Przybylski

Hi there,
It was a while since I wrote last post.
This time I'd like to talk about the Privileged Access Workstation (PAW) security guide.

As always there are some scripts that I've made to speed up the deployment https://github.com/przybylskirobert/ADSecurity/tree/master/PAW.

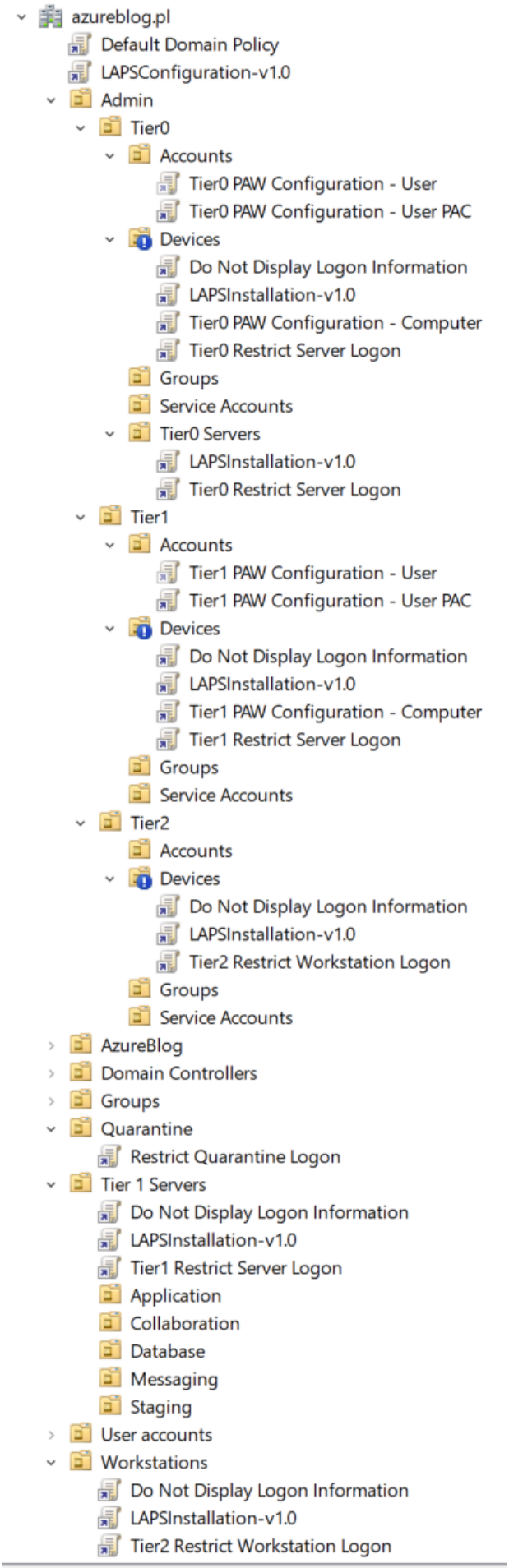
So what are we going to deploy today?
It will be a group of GPOs that will harden our PAWs.

GPO Overview

- **Do Not Display Logon Information** – this GPO will disable logon information on all resources under Admin, Tier 1 Servers and Workstations
- **Restrict Quarantine Logon** – This GPO will lockout the computer object if it will be created during the domain join process. Our goal is to Limit the possibility to add a computer to the domain only for limited groups Tier 1 Server Maintenance and Tier 2 Workstation Maintenance.
- **Tier0 Restrict Server Logon –** This GPO will deny access to the Tier 0 resources for users from Tier 1 and Tier 2
- **Tier1 Restrict Server Logon –** This GPO will deny access to the Tier 1 resources for users from Tier 0 and Tier 2
- **Tier2 Restrict Workstation Logon –** This GPO will deny access to the Tier 1 resources for users from Tier 0 and Tier 1
- **Tier0 PAW Configuration – Computer –** This GPO will configure who can log on locally, who can be a member of local groups, windows firewall settings,
- **Tier1 PAW Configuration – Computer –** This GPO will configure who can log on locally, who can be a member of local groups, windows firewall settings,
- **Tier1 PAW Configuration – Computer –** This GPO will configure who can log on locally, who can be a member of local groups, windows firewall settings,
- **Tier0 PAW Configuration – User –** This GPO will configure proxy settings to 127.0.0.1
- **Tier1 PAW Configuration – User –** This GPO will configure proxy settings to 127.0.0.1
- **Tier2 PAW Configuration – User –** This GPO will configure proxy settings to 127.0.0.1
- **Tier0 PAW Configuration – User PAC –** This GPO will configure proxy settings to use a custom proxy.pac file that will allow specific websites to be open.
- **Tier1 PAW Configuration – User PAC –** This GPO will configure proxy settings to use a custom proxy.pac file that will allow specific websites to be open.
- **Tier2 PAW Configuration – User PAC –** This GPO will configure proxy settings to use a custom proxy.pac file that will allow specific websites to be open.

Deployment Time!

So we all know what will be configured , let's start configuration



Linked GPOs to the OU

```
Administrator: Windows PowerShell
PS C:\tools\paw> Get-ChildItem


    Directory: C:\tools\paw


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        23.05.2020     19:44                GPO Backup
-a----        23.05.2020     18:59           2057 Create-Group.ps1
-a----        23.05.2020     18:58           1580 Create-User.ps1
-a----        03.05.2020     20:09            815 Groups.csv
-a----        23.05.2020     18:04           1006 Import-GPO.ps1
-a----        23.05.2020     19:42            766 Link-GpoToOU.ps1
-a----        23.05.2020     19:45           3983 PAW_steps.ps1
-a----        23.05.2020     18:26           3088 proxy.pac
-a----        23.05.2020     18:33            595 Users.csv
```

PAW Directory Structure

Let's prepare some stings before running scripts.

```
$location = Get-Location
Set-Location C:\Tools\PAW
```

```
Administrator: Windows PowerShell
PS C:\Tools\PAW> Set-Location C:\Tools\PAW
>> $location = Get-Location
PS C:\Tools\PAW>
```

Setup Location

As you can see my scripts for PAW configuration are stored under **C:\Tools\PAW** directory

```
$csv = Read-Host -Prompt "Please provide full path to Groups csv file"
.\Create-Group.ps1 -CSVfile $csv -Verbose
```

Groups Creation

The line above will create all the necessary groups to show you the PAW security idea.
The line below will create user accounts.

```
$csv = Read-Host -Prompt "Please provide full path to Users csv file"
.\Create-User.ps1 -CSVfile $csv -password zaq12WSXcde3 -Verbose
```

Users Creation

Probably you are now thinking:
Why this guy is using so simple password?

My answer is – **this is a lab only** 🙂

The next step is very important and you need to be very careful.
We are going to configure the migration table required for GPO import.
Migration table will allow you to change my lab, related groups, into the groups from your environment (they will have different SIDs)

Please open the **gpo_backup.migtable** file on the computer where you have a group policy management console.
Fil the proper values under the **Destination Name** column.

Migration Table Structure

Done?
If yes we are ready to go with GPO import.
Please run the following code

```
$BackupPath = Read-Host -Prompt "Please provide full path to GPO backups"
$GPOMigrationTable = Read-Host -Prompt "Please provide full path to GPO
Migration Table"
.\Import-GPO.ps1 -BackupPath $BackupPath -GPOMigrationTable $GPOMigrationTable
-Verbose
Set-Location C:\Tools\PAW
```

GPO Import

As you can see you will be asked to provide 2 values:

- Path to the directory where GPO Backup exists (GPO backup from my repository saved on your drive)
- Path to the migration table file

After GPO Import please copy **proxy.pac** file to:
\\Your_domain_Name\sysvol\scripts

Proxy file placement

All good? Done without any problems?
Let’s go to next step – Linking GPO to the proper OUs

```
$GpoLinks = @(
$(New-Object PSObject -Property @{ Name = "Do Not Display Logon Information"
; OU = "OU=Devices,OU=Tier0,OU=Admin"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Do Not Display Logon Information"
; OU = "OU=Devices,OU=Tier1,OU=Admin"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Do Not Display Logon Information"
; OU = "OU=Devices,OU=Tier2,OU=Admin"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Do Not Display Logon Information"
; OU = "OU=Tier 1 Servers"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Do Not Display Logon Information"
; OU = "OU=Workstations"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Restrict Quarantine Logon" ; OU =
"OU=Quarantine"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier0 Restrict Server Logon" ; OU
= "OU=Devices,OU=Tier0,OU=Admin"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier1 Restrict Server Logon" ; OU
= "OU=Devices,OU=Tier1,OU=Admin"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier1 Restrict Server Logon" ; OU
= "OU=Tier 1 Servers"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier2 Restrict Workstation Logon"
; OU = "OU=Devices,OU=Tier2,OU=Admins"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier2 Restrict Workstation Logon"
; OU = "OU=Workstations"; Order = 1 ;LinkEnabled = 'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier0 PAW Configuration -
Computer" ; OU = "OU=Devices,OU=Tier0,OU=Admin"; Order = 1 ;LinkEnabled =
'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier0 PAW Configuration - User" ;
OU = "OU=Accounts,OU=Tier0,OU=Admin"; Order = 1 ;LinkEnabled = 'No'}),
$(New-Object PSObject -Property @{ Name = "Tier0 PAW Configuration - User
PAC" ; OU = "OU=Accounts,OU=Tier0,OU=Admin"; Order = 1 ;LinkEnabled =
'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier1 PAW Configuration -
Computer" ; OU = "OU=Devices,OU=Tier1,OU=Admin"; Order = 1 ;LinkEnabled =
'YES'}),
$(New-Object PSObject -Property @{ Name = "Tier1 PAW Configuration - User" ;
OU = "OU=Accounts,OU=Tier1,OU=Admin"; Order = 1 ;LinkEnabled = 'NO'})
$(New-Object PSObject -Property @{ Name = "Tier1 PAW Configuration - User
PAC" ; OU = "OU=Accounts,OU=Tier1,OU=Admin"; Order = 1 ;LinkEnabled =
'YES'})
)
.\Link-GpoToOU.ps1 -GpoLinks $GpoLinks -Verbose
```

GPO Link

GPO Link

We are almost done but…
You need to do some changes in the GPOs
Basically, you need to update the following settings:

- **Computer Configuration\Preferences\Control Panel Settings\Local Users and Groups\Administrators**
  Add Tier X PAW Maintenance Group to Administrators (if already added please remove and again)
- **Computer Configuration\Preferences\Control Panel Settings\Local Users and Groups\Remote Desktop Users**
  Add Tier X PAW Maintenance Group and Tier X PAW Users to Administrators (if already added please remove and again)

Replace X with the proper Tier level that you are editing.

Under the following GPOs

- Tier0 PAW Configuration – Computer
- Tier1 PAW Configuration – Computer
- Tier2 PAW Configuration – Computer

Now we are done, this is a time to do some tests.
Move our test machines to the Tier 1 Devices OU and Quarantine OU

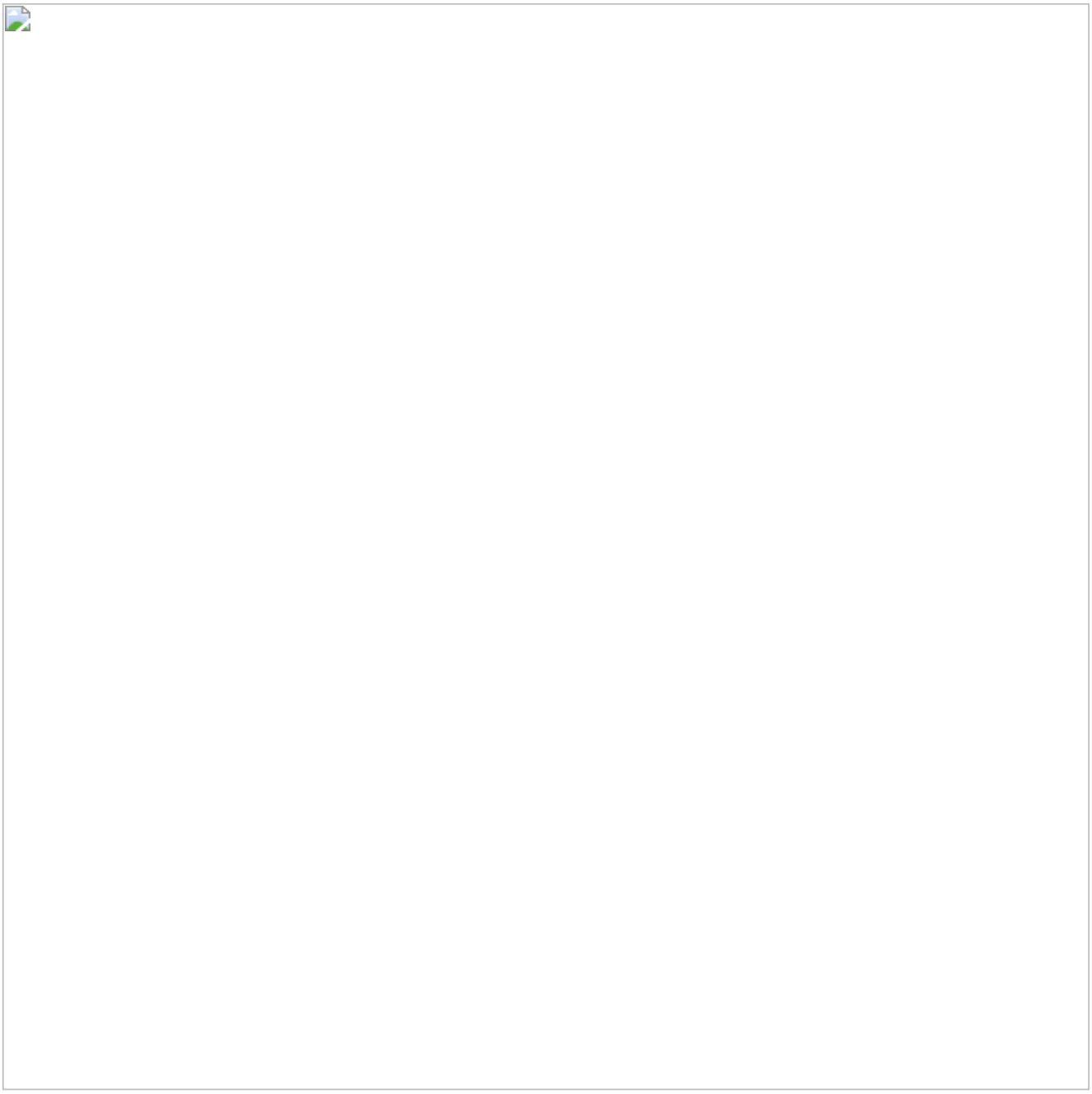
```
Get-ADComputer -Identity W10 | Move-ADObject -TargetPath
"OU=Quarantine,DC=Azureblog,DC=pl"
Get-ADComputer -Identity SRV01 | Move-ADObject -TargetPath
"OU=Devices,OU=Tier0,OU=Admin,DC=Azureblog,DC=pl"
Get-ADCOmputer -Identity W10
Get-ADComputer -Identity SRV01
```

Computers Movement

Test time!

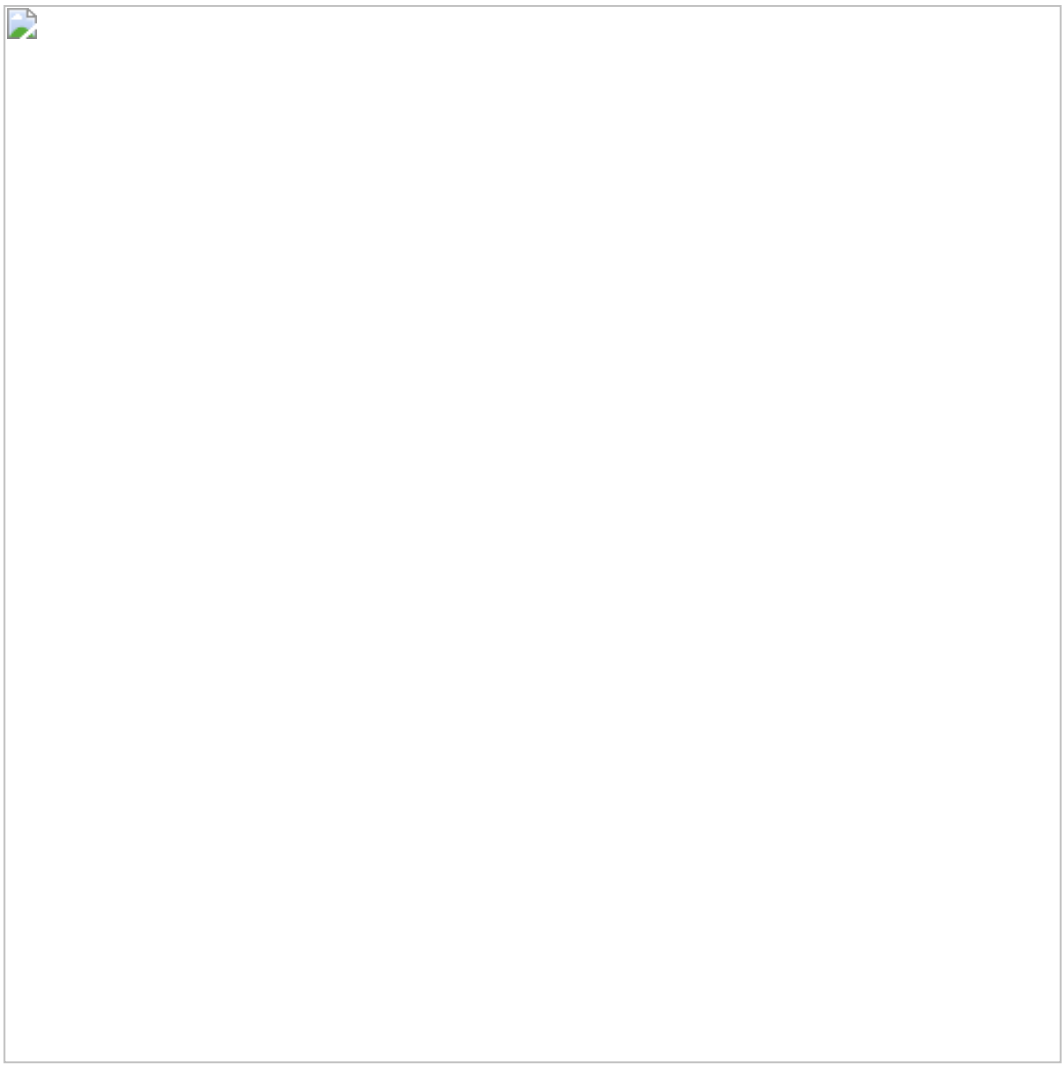
Please reboot those machines (we do not want to wait until GPOs will refresh)

Try to log on to the W10 machine (placed under Quarantine OU)



Computer in Quarantine

Nice, our test computer was moved and new GPO was applied.
When you try to log on you will receive the following message



Quarantine Lock

That means only Tier 2 Workstation Maintenance group members will be able to log in to this machine. If you want to fix it please move the object to the proper OU.

Now it is the time to check how is our SRV01 doing.
Try to log with **Tier 0 PAW User** account.

Tier 0 PAW User group membership

AS you can see our user is not a member of Administrators group. That means he will be able to work on this computer but without any “major” changes like software installation, reconfiguration etc.

Failed user creation

Is it secure?
Yes and it is not the end because for this user a custom proxy file was applied.

Tier 0 PAW user proxy settings

Now let’s try same steps with Tier 0 PAW Maintenancer account.

Tier 0 PAW Maintenancer group membership

Local user creation

Proxy configuration

Same way of work is for Tier 0, Tier 1 and Tier 2 PAW devices.
Of course you can take it or leave it it depends on you 🙂