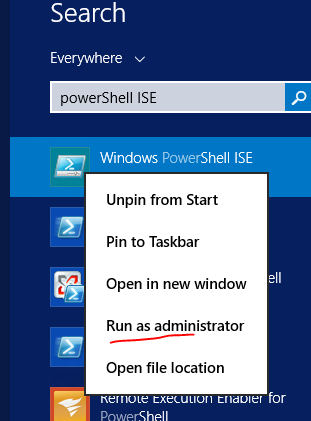
**Powershell on CW- introduction:**

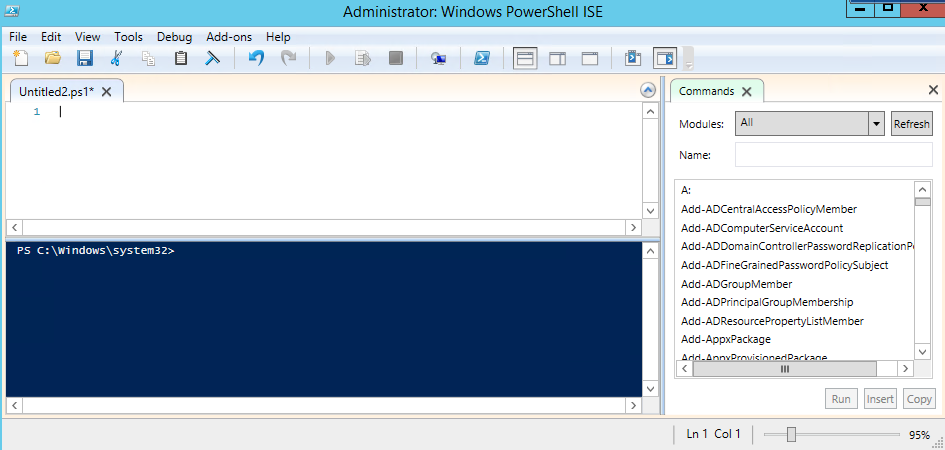
In order to use remote scrips log on any jumpbox (example 10.130.0.11 or cw-svr-ter2)

You can use either windows powershell console or Windows PowerShell which is much more user friendly.

Please mind that most scripts will require you to open PowerShell console as administrator



Once opened this way you can either copy paste prepared previously scripts or write your own in white tab.

Results and errors will be written in blue console bellow:

**Access to different devices:**

When it comes to access those are some things you are able and not able to on cw domain:

1. Servers: You have no limitations for using scripts on servers like: viscin1 or dc1. If you can do something by MSTSC you can do it by PowerShell as well. You have no access to dc2.

This is due to fact that most of windows servers come with powershell enabled on them by default. However your domain account has no administrative right on production-hosted domain.

1. POS: You are able to use read only scripts, for example to check process that are running currently on remote devices.

In order to work with scripts that would change something on a till (for example change something on registry while till is logged on user) you would need to enable remote access on the till first, more info on how to do this:

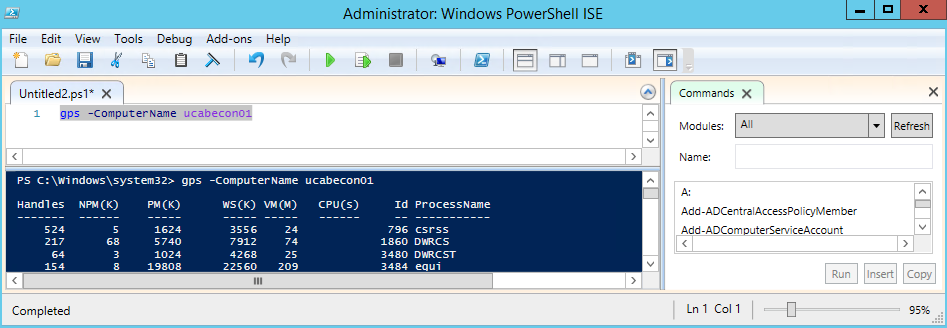
<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-5.1>

1. Manager PC’s: same as POS.
2. ATM- You won’t have any use for remote scripts on ATM’s even if you enable remote scripts on them.

**Useful scripts and how to use them:**

1. **Check processes/services running on remote devices.**

Get-process –computerName ucabecon01



Simply write get-process –computername (name of the till/manager pc).

This is useful for example if you are not sure if vista is slowly starting or haven’t started yet on a till. You can see processes on remote device which you would be unable to due to gps on a till.

1. **Site is down- basic troubleshoot**

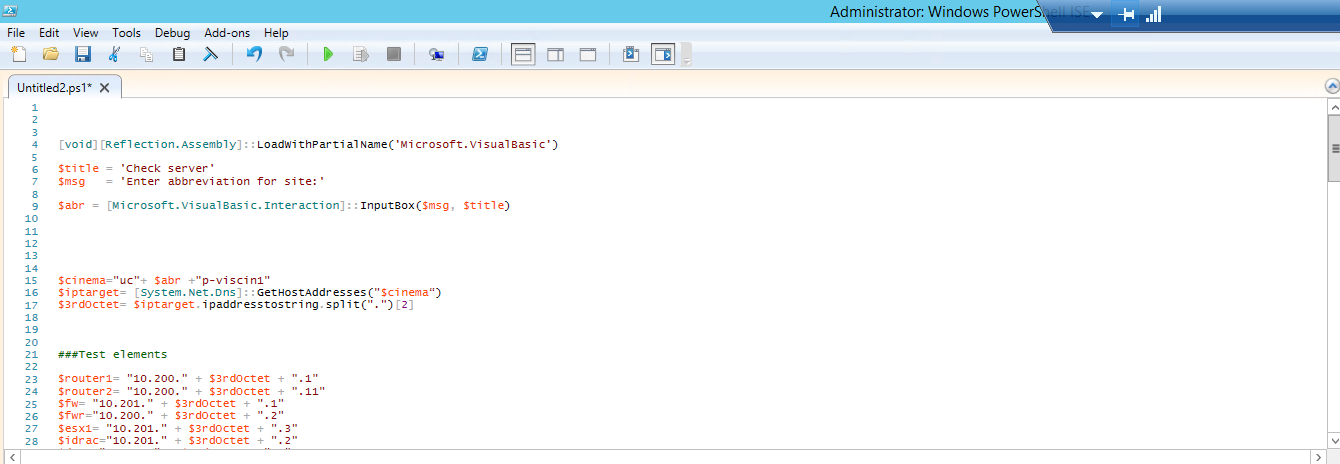
**Script name: TestSite.ps1**

This one will ping routers/firewalls/esx1/idrac/dc1/dc2 and check if IIS and SQL server agent is running on the remote server (using wmi).

After that it will write down the results in console.

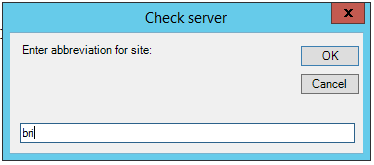
In order to use it:

* Open powershell ISE on jumpbox.
* Copy script to the white window



-press green arrow to run the script

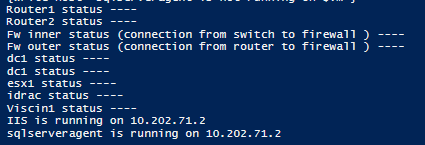
-window will prompt asking for 3 letter abbreviation for site (example bri for Brighton):



-press ok.

-script will run for some time you can recognize it is running by red stop button activated in the top prompt.

-Those will be results for fully working site:



Horizontal lines represent ping reply’s from site.

On bottom there is information if IIS and SQL server are running.

1. **Check dsp settings on mrx1.**

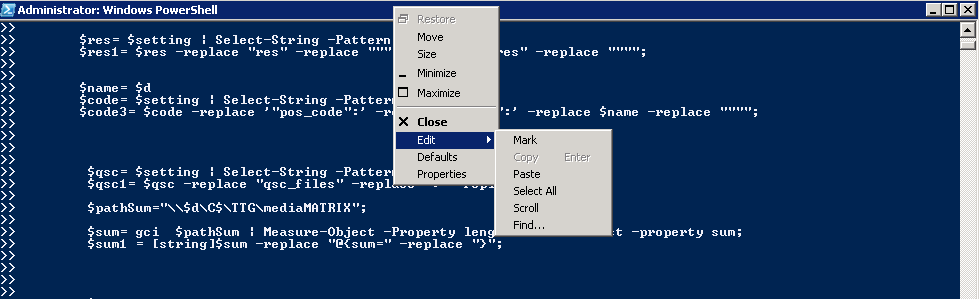
Script name: DSPCheck Parameters.txt

This will export some useful data regarding DSP’s on site to csv file.

-Log as admin on mrx1 server

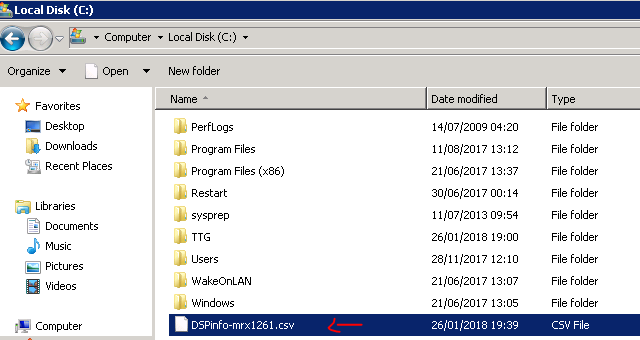
-Run powershell or powershell ise as administrator (multiple mrx1s wont have ISE yet).

-Copy script to shell (you can do this in similar fashion that you copy text to CMD right click on blue ribbon, edit-> Paste):

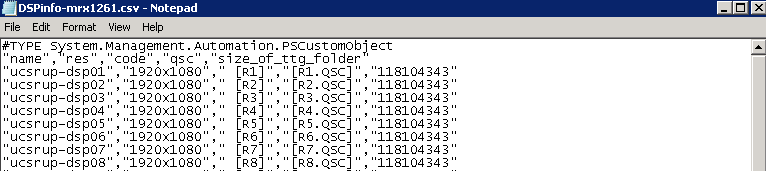


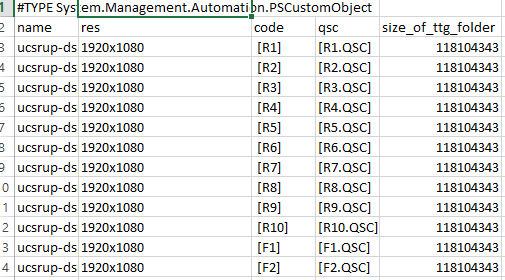
-press enter.

-It should create a cvs file on mrx1 c: drive:



You can open it either in notepad or copy on your desktop and open in excel for better view:





This will read info in TTG folder and put it in a handy list informing you:

-Which dsps are offline.

-What are resolution settings in TTG.

-Which screen numbers are those DSP’s

- Last row shows you the size of TTG folders (in most cases they should be the same)

1. **Check why user gets locked out.**

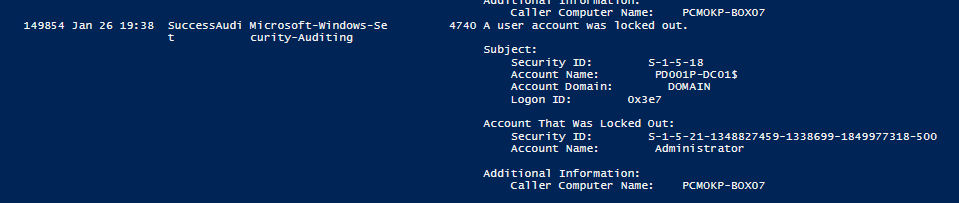
Script name: LastLockedUsers.txt

In case when you unlock somebody’s account and it gets instantly locked in AD it may be that this user is logged on another server/pos/pc with his old login and this will cause him to get insta locked.

You can check quickly last couple event viewer logs regarding logged accounts with this simple script:

Get-EventLog -ComputerName 10.130.1.12,10.130.1.11 -LogName Security -Newest 10 -After "9.4.2017 10:00" -InstanceId 4740 | Format-Table -Wrap

This will show you whom and where was locked out recently:



You can modify also in which time frame account was blocked, check wider range of logs by simple modifications done to this script etc.

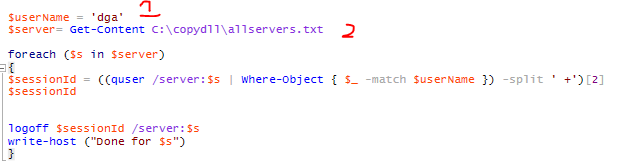
1. **Log off one user from multiple servers.**

Scrip name: LogMeOff.txt and AllServers.txt

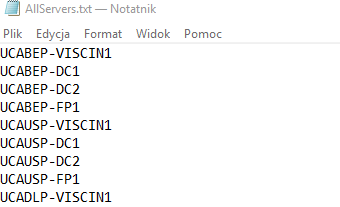
If you were working on many servers recently, and you want to make sure you logged yourself from all of them, you may want to use this script.

You will need however to specify two things in the script

1. your domain account:
2. what is the path to file AllServers.txt with information which are the server the script will be logging you from.



You can specify which servers you want the script to check. You may add more if you want to the existing list:



1. **DHCP scopes/ leases -Check all hosts and their IP**

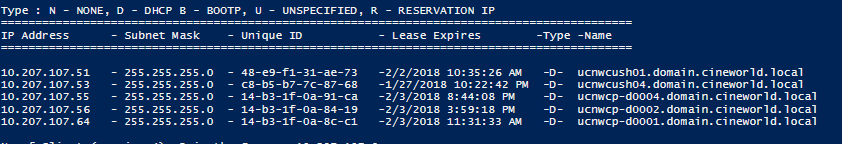
Scrip name: check all dhcp scopes and all devices.txt

It will check all hostanems/ip adreses, lease expiry date/ subnet mask for all ip scopes on domain controllers you will specify.

!!Note that you need to run PowerShell ise as admin, **also you won’t get info from any DC2 unless you are domain admin for prod-hosted1!!**

You also need to specify path to file abr.txt where names of all sites it will check are in. (you can find this file in misc folder)

Example results for one scope:

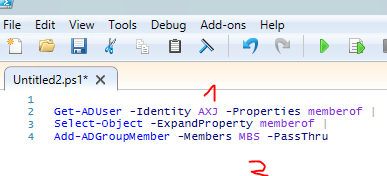


1. **Add the same member of’s another user has:**

Script name: AD copy Member Off.txt

If you have fresh user created and you want to quickly copy members of from one user to another.

Please mind the script will simply attempt to add members of from one user to another. It won’t remove existing ones.



1. **Check dot net**

If you need to check .net framework version from regedit.

Useful for ATM’s if they have 4.5+ version on them

**Other scripts/less usefull:**

1. **Vx820 copy and other copying scripts**

This script will check if all viscin1’s specified have same/current vx820 installation files that folder on C: drive has.

I used it to update install files on all viscin 1s and make it copy current drivers if they were missing.

It could be used if you want to copy something to multiple servers whiteout the risk of copying it multiple times.

1. **working atm check.txt**

It checks ATM’s if they use same current cml files for loyalty config.

It writes you report on which ones have old config at the end/ how many were checked, which ones are offline.

1. **Working email.txt**

If you need to add a script that will be automatically sending email at end of its run.

1. **Check all users members off and ou.txt**

Creates list of all users and workstations in domain and lists their OU and location in ad tree.

1. **Comparingregs.ps1**

Compares specific registry branches between two servers.

It will show you differences between two registry braches.

!Notice the bigger the branch selected (ex if you would select whole hkcu) the longer it will run.

1. **Startregs.txt**

Will update regedit on multiple server (same as running regedit file on machine localy so you need first copy the file to server before using it).

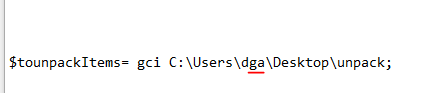
1. **xmls from site.txt**

This needs to be run on uh001p-vishodb2

If you run vista export from site. it will create unique zip file with xmls like cash inventory tickets.

If you write down this number inside “$numberOfZipFiles=” variable it will check if they have been delivered.

It will unpack also those files to your desktop. (you just need to change my domain name with yours):



1. **Powershell Job loggoff.rar**

This is bigger script that was designed to run as task.

It requires separate module to be installed for powershell on server that runs, and installed on powershell (which is part of the script).

Parts of this script include:

#####Scrip Synopsis###

####1--Variables for general settings

##1.1 Location of folder with settings, change it so it points to location of "Powershell Job loggoff" folder

###1.2 Path to list of servers that will be checked

###1.3 How long usser must be disconnected to be kicked off

###1.4 Which users will NOT be kicked off (domain names)

###1.5 Those ussers will not recive any emails

###1.6 Sending email details

###2 Checking servers and kicking users- main loop

###2.1 Error Handling and logs for getting sessions

###2.2 Pipline for getting ussers that are | disconnected | Above certain time| And are not certain ussers whitlisted in NeverLogOff folder

###2.3 Error Handling and logs for stopping sessions

###2.4 Stopping gathered sessions

###2.5 collecting information inside Variable on server and time when usser was logged of

###a) ading member so we will send email with this info later

###b) adding time of logging out

###3 gathering Mail information for all disconnected sessions

###3.1 Gathering mail detail for logged off ad user

###3.2 If there is no mail for this user, try to find his second domain account and get his mail

###4 This part writes an email takin under consideration data gathered in object

###4.1 create a email body using data stored

###4.2 send email only if its certain user (I have narrowed it down to T1 members for now for testing purposes)

###!To change this just change -contains to -not contains

###5 rapport

##5.1 Grouping all users by their ad account and sorting by amount of dc session2

##5.2 creating email body

##5.3 send rapport to fixed email

##END############