Exercices Powershell : Corrigé

# 1ère session

## Commandes

* Lister toutes les commandes de type « functions »
  + Get-Command –CommandType function
* Lister toutes les commandes se terminant par ‘path’.
  + Get-Command \*path

## Aide

* N'afficher que les exemples de l'aide en ligne pour la commande Get-Process
  + Get-Help Get-Process -examples
* Afficher de l'aide concernant For
  + Get-Help about\_for
* Que fait ce script :
  + Get-Command | Foreach {Get-Help $\_ -detailed |Out-File -FilePath C:\temp\$\_.txt –Encoding ASCII}
  + Il envoie le contenu de l’aide de chaque commande dans un fichier portant le nom de la commande en cours.

## Système de fichiers

* Lister tous les fichiers du répertoire C:\Windows\system32 et ses sous répertoires dont la taille est supérieure ou égale à 10 Mo
  + Get-ChildItem C:\Windows\System32 –recurse | Where-Object {$\_.length –ge 10MB}
* Copier l’arborescence (récursif) de ‘program files’ vers un répertoire de votre choix.
  + Copy-Item ‘C:\Program files’ ‘Repertoire’ –recurse –filter psiscontainer

## Système

* Récupérer tous les services arrêter et envoyer le résultat dans un fichier.
  + Get-Service | ? {$\_.status -eq 'stopped'} | Out-File C:\scripts\CESI\services.log
* Lister tous les id, des maj microsoft et envoyer le résultat dans un fichier.
  + Get-HotFix | Select-Object hotfixid > hotfix.log **ou**
  + Get-HotFix | ForEach-Object {$\_.hotfixid} > .\hotfix.log
* Récupérer les processus utilisant au moins 100 Mo.
  + Get-Process | Where-Object {$\_.workingset -ge 100MB}
* Récupérer dans le journal d’événements ‘Application’ , toutes les entrées en erreur.
  + Get-EventLog -LogName application -EntryType error

## 2ème session

## Les fournisseurs

* Récupérer dans une variable le contenu de la variable d'environnement « computername »
  + $var = (dir env:\computername).value
* Retrouver le chemin complet de la clé Winlogon dans le registre (HKEY Current User)
  + Get-ChildItem hkcu: -Recurse | Select-String Winlogon
* Crée une variable d'environnement nommer 'login' et affecter lui la valeur 'james.bond'
  + $env:login = 'james.bond'

## Affichage

* Afficher toutes les propriétés de la commande Get-Process
  + Get-Process | Format-List \*
* Puis choisir de n'afficher que les propriétés ID, Name et WorkingSet
  + Get-Process | Format-List id,name,workingset

## Système de fichiers

* Afficher les extensions de fichiers présentes dans le répertoire c:\windows de manière unique et dans l'ordre alphabétique (exclure les extensions ‘vides’)
  + Get-ChildItem C:\Windows | ? {$\_.extension -ne ''} | % {$\_.extension} | sort -unique
* Modifier la date d’accès d’un fichier.
  + (dir .\config.sys).set\_lastaccesstime($date = get-date -Year 2011 -Month 09 -Day 12 -Hour 12 -Minute 10 -Second 00)

## Système

* Afficher le nombre de services arrêtés et démarrés en seule ligne de commande
  + Get-Service | Group-Object status | Format-table count,name
* Afficher tous les processus fabricant (Microsoft, AMD, Intel, etc..) et trier en ordre décroissant leurs nombres.
  + Get-Process | Group-Object company | sort count -Descending | ft count,name
* Vérifier la présence d’une erreur disque dans les journaux d’évènements (id event 7)
  + Get-EventLog system | Where-Object {$\_.eventid -eq 7} | ft eventid

## Texte

* Mesurer le nombre de lignes, de mots et caractères d'un fichier texte.
  + Get-Content .\WmiExplorer.ps1 | Measure-Object -Line -Word -Character

## Condition

* Proposer à l’utilisateur de choisir un chiffre en 1 et 5 et afficher lui le chiffre choisi en toutes lettres – Pour exécuter un script : set-executionpolicy unrestricted
  + $Nombre = Read-Host ’Choisir une valeur entre 1 à 5’

Switch ($Nombre)

{

1 {Write-Host ’Le nombre saisi est un’}

2 {Write-Host ’Le nombre saisi est deux’}

3 {Write-Host ’Le nombre saisi est trois’}

4 {Write-Host ’Le nombre saisi est quatre’}

5 {Write-Host ’Le nombre saisi est cinq’}

Default {Write-Host ’Le nombre saisi est hors plage !’}

}

## Session3

## Boucle

* Créer une boucle visuelle avec la commande Write-Progress (Barre de progression)
  + for ($i = 1; $i -lt 30; $i++ ){

start-sleep 1

write-progress -activity "Boucle visuelle" -status "%Effectué:" -percentcomplete $($i\*100/30)}

## Registre

* A l’aide du chemin de registre suivant, extraire le nom, les versions des Framework .net installés 🡪 "HKLM\software\microsoft\Net Framework setup\ndp"
  + Get-childitem 'HKLM:\software\microsoft\Net Framework setup\ndp' | select-object @{Name="Framework";Expression={$\_.PSChildname}},@{Name="Service Pack";Expression={$\_.getvalue("version")}} |format-table -autosize
* A l’aide du chemin de registre suivant, activer le bureau à distance de votre machine 🡪 "HKLM\SYSTEM\currentcontrolset\control\terminal server\ fdenytsconnections"
  + set-ItemProperty -name fDenyTSConnections -Path 'HKLM:\SYSTEM\CurrentControlSet\control\Terminal Server\' -Value 0
* A l’aide du chemin de registre suivant, lister toutes les clés usb connectés à votre machine hôtes 🡪 HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
  + Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\\*\\*' | Select-Object psChildname,FriendlyName,Class

## Active Directory

* Préparer un serveur Windows 2012 R2 et le promouvoir en contrôleur de domaine

***Pour utiliser les commandes ActiveDirectory les outils de gestion RSAT doivent être installés, dans le cas d’un DC, ils sont installés automatiquement. Cependant en dehors de cet exercice, il est vivement conseillé d’utiliser un poste de travail non serveur pour administrer ActiveDirectory.***

***Depuis Powershell v3, l’import d’un module dans la session courante est automatique :***

***Dans ce cas la commande implicite exécutée est Import-module ActiveDirectory lors du premier lancement du commande ActiveDirectory.***

* Créer une OU nommé Utilisateurs (en Powershell)
* Créer un utilisateur lambda avec une adresse mail et une ville à l’aide de la commande New-Aduser, puis lui ajouter un mot de passe. (dans l’OU créer précédemment)
* Créer un deuxième utilisateur avec mot de passe à l’aide d’une seule ligne de commande
* Lister tous les comptes dont le mot de passe n’a pas été changé depuis un mois. ***(dans le cadre du TP, une heure suffira étant donné la date de création des comptes)***
* A l’aide la commande précédente, forcer le changement de passe des comptes concernés
* A l’aide du fichier CSV fourni par le formateur, créez un grand nombre de compte tel que :
  + Login : prenom.nom (limité à 20 caractères) sans accent
  + Mot de passe : nombre aléatoire de 8 caractères
  + Email : [prenom.nom@votredomaine.xxx](mailto:prenom.nom@votredomaine.xxx) (sans limitation de caractère)
  + Forcer le changement de mot de passe à la première ouverture de session
  + Créer l’utilisateur dans l’OU précédemment crée

🡺 Pour la correction voir scripts fournis par le formateur

## Active Directory et MySQL

* Installer un WAMP sur votre machine et importer le fichier CSV fourni dans une base de données nommée RH
* Supprimer tous les comptes que vous avez créés précédemment.
* Importer directement tous les comptes dans l’AD depuis la base mysql tel que :
  + Login : prenom.nom (limité à 20 caractères) sans accent
  + Mot de passe : nombre aléatoire de 8 caractères
  + Email : [prenom.nom@votredomaine.xxx](mailto:prenom.nom@votredomaine.xxx) (sans limitation de caractère)
  + Forcer le changement de mot de passe à la première ouverture de session
  + Créer l’utilisateur dans l’OU précédemment crée
* Créer les dossiers personnels des utilisateurs avec les bons droits NTFS à l’aide du script fourni

🡺 Pour la correction voir scripts fournis par le formateur

## WMI

* Prérequis : 3 machine Windows virtuelles nommées Client1, Client2, Client3

Les VMs doivent pouvoir communiquer avec la machine hôte. (NIC Bridged ou host-only)

* Démarrer les VMs crées précédemment et nommées Client1, Client2, Client3 et configurer le mot de passe : P@ssword pour le compte administrateur – important pour la suite
* Sur chaque VM, lancer la commande suivante pour autoriser WMI et DCOM distant : Client1, Client2, Client3 :

netsh advfirewall firewall set rule group="Infrastructure de gestion Windows (WMI)" new enable=yes

* Sur l’hôte hébergeant les VMs, lancer une console powershell, puis la commande suivante :

Get-WmiObject win32\_bios -ComputerName client1 -Credential administrateur

* À l’aide de la commande précédente, créer un script qui va interroger toutes les VMs à l’aide d’une boucle.
* $computers = "client1","client2","client3","client4"

$credentials = Get-Credential -UserName 'administrateur' -Message 'Mot de passe ?'

foreach ($computer in $computers) {

Get-WmiObject win32\_bios -ComputerName $computer -Credential $credentials

}

* Adapter votre script pour détecter le système d’exploitation
* $computers = "client1","client2","client3","client4"

$credentials = Get-Credential -UserName 'administrateur' -Message 'Mot de passe ?'

foreach ($computer in $computers) {

Get-WmiObject win32\_Operatingsystem -ComputerName $computer -Credential $credentials

}

* Adapter le script pour afficher, le nom de la machine, le nom du système d’exploitation, sa version et son architecture (x64 ou x86).
* $computers = "client1","client2","client3","client4"

$credentials = Get-Credential -UserName 'administrateur' -Message 'Mot de passe ?'

foreach ($computer in $computers) {

Get-WmiObject win32\_Operatingsystem -ComputerName $computer -Credential $credentials | format-table PSComputerName

}

* À l’aide de la classe Wmi win32\_LogicalDisk afficher la taille et l’espace libre des partitions de votre hôte.
  + Get-WMIObject win32\_LogicalDisk| Format-Table Name, freespace, Size
* Affiner la sortie de la commande précédente pour afficher en tableau les colonnes suivantes : Name, Espace Libre (en GB) et taille (en GB). Garder ce script pour la prochaine partie.

$Fs=@{Label='Free Space (GB)'; expression={($\_.freespace)/1gb};formatstring='n2'}

$Sz=@{Label='Size (GB)'; expression={($\_.Size)/1gb};formatstring='n2'}

Get-WMIObject win32\_LogicalDisk| Format-Table Name, $fs, $Sz -autosize

## Rapport HTML et envoi de message

* À l’aide de la commande send-mailmessage, envoyez-vous un mail de test (adaptez les paramètres de la commande en fonction de votre fournisseur de messagerie : SSL ?, Port 25 ou 587…)

Send-MailMessage -From baptiste.deneuve@outlook.com -To baptiste.deneuve@rouen.archi.fr -Subject "PSV2" -Body "test" -Port 587 -SmtpServer smtp-mail.outlook.com -Credential (Get-Credential) -UseSsl

* À l’aide du script de la dernière partie (concernant Win32\_LogicalDisk), envoyer la liste des partitions de vos 3 VMs à votre adresse mail.

$Fs=@{Label='Free Space (GB)'; expression={($\_.freespace)/1gb}}

$Sz=@{Label='Size (GB)'; expression={($\_.Size)/1gb}}

$body = Get-WMIObject win32\_LogicalDisk| Select-Object Name, $fs, $Sz

$body = $body | Out-String

$body = $body -join '`n'

Send-MailMessage -From baptiste.deneuve@outlook.com -To baptiste.deneuve@rouen.archi.fr -Subject "PSV2" -Body $body -Port 587 -SmtpServer smtp-mail.outlook.com -Credential (Get-Credential) -UseSsl

* Répétez l’opération précédente en convertissant le retour du script en HTML.

#Fichier HTML

$Fs=@{Label='Free Space (GB)'; expression={($\_.freespace)/1gb}}

$Sz=@{Label='Size (GB)'; expression={($\_.Size)/1gb}}

$body = Get-WMIObject win32\_LogicalDisk| Select-Object Name, $fs, $Sz

$body = $body | ConvertTo-Html

OU

#Envoi en HTML

$Fs=@{Label='Free Space (GB)'; expression={($\_.freespace)/1gb}}

$Sz=@{Label='Size (GB)'; expression={($\_.Size)/1gb}}

$body = Get-WMIObject win32\_LogicalDisk| Select-Object Name, $fs, $Sz

$body = $body | ConvertTo-Html

$body = $body | Out-String

$body = $body -join '`n'

Send-MailMessage -From baptiste.deneuve@outlook.com -To baptiste.deneuve@rouen.archi.fr -Subject "PSV2" -BodyAsHtml $body -Port 587 -SmtpServer smtp-mail.outlook.com -Credential (Get-Credential) -UseSsl

## Transformer le retour d’une commande texte en objet

* Transformer le retour de la commande netstat.exe en objet

NETSTAT.EXE |Select-Object -Skip 4 | ConvertFrom-String | select @{n='Protocol';e={$\_.p2}}, @{n='Adresse locale';e={$\_.p3}}, @{n='Adresse distante';e={$\_.p4}}, @{n='Etat';e={$\_.p5}}