Script Divers

Exchange

Récupérer la version d'Exchange

Source: Liens vers l'article Technet

A partir d'Exchange 2013:

Get-ExchangeServer | fl Name, Fqdn, ExchangeVersion, ServerRole, AdminDisplayVersion

Avant Exchange 2010:

Get-Command Exsetup.exe | ForEach-Object {\$_.FileVersionInfo}

Get-ClientAccessServer | fl Name, OutlookAnywhereEnabled, AutoDiscoverServiceCN, AutoDiscoverServiceInternalUri Get-ExchangeServer | Get-OutlookProvider | ft Server, Name, CertPrincipalName, TTL -auto Get-OutlookAnywhere | fl Server, Name, ExternalHostname, SSLOffloading, ClientAuthenticationMethod, IISAuthenticationMethods, MetabasePath

Get-WebServicesVirtualDirectory | fl Identity, Name, InternalNLBBypassUrl, InternalUrl, ExternalUrl Get-OwaVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl Get-ActiveSyncVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl Get-AutodiscoverVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl Get-EcpVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl Get-PowerShellVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl Get-PowerShellVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl Get-OabVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl, PollInterval Get-EcpVirtualDirectory | fl Identity, Name, InternalUrl, ExternalUrl

#Récupérer les certificats Exchange# Get-ExchangeCertificate | ft Thumbprint, Services, NotAfter, Subject -auto \$D=(Get-Date).AddDays(30); Get-ExchangeServer | %{\$S=\$_.ldentity;\$R=\$_.ServerRole; Get-ExchangeCertificate -Server \$S | Sort NotAfter | Select @{n='Server';e={'{0} ({1})' -f \$S,\$R}}, @{n='CertSubject';e={(\$_.Subject -split '(,)*..=')[1]}}, @{n='Expires';e={'{0.MM/dd/yyyy}' -f \$_.NotAfter}, @{n='IssuedBy';e={(\$_.Issuer -split '(,)*..=')[1]}}, @{n='Domains';e={\$_.CertificateDomains -join ','}},@{n='Alert';e={' !'[(Get-Date \$_.NotAfter) -le \$D]}},*} | ft -a Alert, CertSubject, Status, Expires, IsSelfsigned, IssuedBy, Services, Thumbprint, Domains -GroupBy Server | Out-String -Width 8192 #Récupérer le nombre de BaL par DB# Get-Mailbox | Group-Object -Property:Database | Select-Object Name,Count | Sort-Object Name | Format-Table -Auto #Summary of Mailbox Move Request Status# Get-MoveRequest | Group-Object -Property:Status | Select-Object Name,Count | Format-Table -Auto

MDB & DAG ### #A partir d'Exchange 2013# Get-DatabaseAvailabilityGroup | ForEach
{\$_.Servers | ForEach {Get-MailboxDatabase -status -Server \$_} | ft Name, Server, DatabaseSize,
AvailableNewMailboxSpace, LastFullBackup -auto} Get-DatabaseAvailabilityGroup | ForEach
{\$_.Servers | ForEach {Get-MailboxDatabaseCopyStatus -Server \$_} | ft Name, Status,
CopyQueueLength, ReplayQueueLength, LastInspectedLogTime, ActivationPreference,

ContentIndexState -auto} Get-DatabaseAvailabilityGroup | ForEach {\$_.Servers | ForEach {Test-ReplicationHealth -Server \$_} | ft -auto} Get-DatabaseAvailabilityGroup | ForEach {\$_.Servers | ForEach {Get-Queue -Server \$_} | ft Identity, DeliveryType, Status, MessageCount, LastError, LastRetryTime, NextretryTime, NextHopDomain -auto} #Sous Exchange 2010# Get-MailboxDatabase -Status -Server PROMES05 | ft Name, Server, DatabaseSize, AvailableNewMailboxSpace, LastFullBackup -auto Get-MailboxDatabase -Status -Server PROMES05 | ft Name, Server, AvailableNewMailboxSpace, LastFullBackup, LastIncrementalBackup, LastDifferentialBackup -auto Get-MailboxDatabaseCopyStatus -Server PROMES05 | ft Name, Status, ActiveDatabaseCopy, CopyQueueLength, ReplayQueueLength, ContentIndexState -auto Test-ReplicationHealth -Server PROMES05 | ft -auto Get-Queue -Server PROMES05 | ft Identity, DeliveryType, Status, MessageCount, LastError, LastRetryTime, NextretryTime, NextHopDomain -auto

Cluster ### #A partir de Server 2008 R2# Get-DatabaseAvailabilityGroupNetwork | fl Get-ClusterQuorum | ft -auto Get-ClusterGroup | ft -auto Get-ClusterNode | ft -auto #En dessous de Server 2008# cluster group /status cluster node /status

HealthReport ### #Get-ExchangeServer | Get-ServerHealth -HealthSet "MailboxSpace" Get-ExchangeServer | Get-HealthReport | where { \$_.alertvalue -ne "Healthy" } Get-ExchangeServer | Test-ServiceHealth Get-Mailbox -Monitoring

Lync / Skype ### Get-CsManagementStoreReplicationStatus Test-CSGroupIM Test-CSDataConference Test-CSASConference Test-CSxmppIM Test-CSPersistentChatMessage Test-CSUCWAConference

#Récupérer les informations de version de l'AD# Import-Module ActiveDirectory Get-ADForest | fl Name,Domains Get-ADForest | fl Name,ForestMode Get-ADDomain | fl Name,DomainMode netdom /query fsmo

#Tester une relation d'approbation entre deux domaines Active Directory# nltest /trusted_domains

#Lister les DC d'un domaine# nltest /dclist:*domain*

#Analyser l'état des contrôleurs de domaine# dcdiag /Q cd %USERPROFILE%\Desktop && dcdiag /V /D /C /E > .\dcdiag.log #Diagnostiquer les problèmes de réplication Active Directory# repadmin /showrepl repadmin /replsummary cd %USERPROFILE%\Desktop && repadmin /showrepl *adc* /verbose /all > .\repl.txt #Synchroniser un contrôleur de domaine avec l'ensemble de ses partenaires de réplication# #/e: Enterprise; includes partners in all sites. #/d: Identifies servers by their distinguished names in messages. #/A: All; synchronizes all directory partitions that are held on the home server. #/P: Pushes changes outward from the home server. repadmin /syncall /e /d /A /P

Azure AD Connect ### Get-ADSyncScheduler #Lancer une synchronisation# Connect-MsolService Import-Module ADSync #Lancer une synchronisation différentielle# Start Delta Sync Start-AdSyncSyncCycle -PolicyType Delta #Lancer une synchronisation complète# Start Full Sync Start-AdSyncSyncCycle -PolicyType Initial

Réplication AD au niveau de la forêt ### repadmin /syncall /ADEP

#Tester l'état de la RA entre une machine et le domaine# Test-ComputerSecureChannel -verbose nltest.exe /sc_verify:domain.local Dfsdiag /TestDCs #Réinitialise la relation d'approbation entre un poste et son DC (no need to reboot the machine)# Test-ComputerSecureChannel -repair -credential (Get-Credential) -verbose Reset-ComputerMachinePassword -credential (Get-Credential)

#List DFS replication groups - use cmd# DfsrAdmin RG List /attr:RgName,RgDomain,ObjState #Determine which replication member is primary for a replication group - use cmd# DfsrAdmin Membership List /RGname:*ReplicationGroupName*

/attr:MemName,RFName,LocalPath,MembershipEnabled,IsPrimary #Determine the path & the size of the staging folder for a replication group - use cmd# DfsrAdmin Membership List /RGname:*ReplicationGroupName* /attr:MemName,RFName,LocalPath,StagingPath,StagingSize #Determine the path & the size of the "Conflict and Deleted" folder for a replication group - use cmd# DfsrAdmin Membership List /RGname:*ReplicationGroupName* /attr:MemName,RFName,LocalPath,CDPath,CDSize,MoveDelFiles

#Check what DFSR is doing at the moment# dfsrdiag replicationstate /A /V #Get DFRS Replicated Folder informations - State: 0: Uninitialized, 1: Initialized, 2: Initial Sync, 3: Auto Recovery, 4: Normal, 5: In Error# Get-CimInstance -Namespace root/MicrosoftDfs -ClassName DfsrReplicatedFolderInfo #Check Backlog# dfsrdiag backlog /rgname:*ReplicationGroupName* /rfname:*ReplicatedFolderName* /sendingmember:*sending_server* /receivingmember:*receiving_server* /v #Example: dfsrdiag backlog /rgname:gds.local\ssr_pra\replication /rfname:COMMUN /sendingmember:DC1-PSSRDFS01 /receivingmember:DC2-PSSRDFS02 /v #Example: dfsrdiag backlog /rgname:gds.local\ssr_pra\replication /rfname:COMMUN /sendingmember:DC2-PSSRDFS02 /receivingmember:DC1-PSSRDFS01 /v #Check SYSVOL backlog when DFS-R SYSVOL replication is enabled# dfsrdiag backlog /rgname:"Domain System Volume" /rfname:"SYSVOL Share" /smem:*DC1* /rmem:*DC2*

#Set the primary member during the initial replication# DfsrAdmin Membership Set /RGName:*ReplicationGroupName* /RFName:*ReplicatedFolderName* /MemName:*member you want to be primary* /IsPrimary:True #Example: DfsrAdmin Membership Set /RGName:gds.local\ssr_pra\replication /RFName:ARCHIVES /MemName:DC1-PSSRDFS01 /IsPrimary:True

#Determine the Reference domain controller# WMIC /namespace:\\root\microsoftdfs path DfsrReplicatfionGroupConfig get LastChangeSource #Force DFS to poll Active Directory for configuration change# dfsrdiag pollad Update-DfsrConfigurationFromAD #Checking domain controller configuration# DFSDiag /TestDCs DFSDiag /TestSites /DFSPath:\\gds.local\dfs DFSDiag /TestDFSConfig /dfsroot:\\gds.local\dfs DFSDiag /TestDFSIntegrity /dfsroot:\\gds.local\dfs DFSDiag /TestReferral /DFSPath:\\gds.local\dfs

#Cleanup All "ConflictAndDeleted" Folder# Get-CimInstance -Namespace root/MicrosoftDfs -ClassName DfsrReplicatedFolderInfo | Invoke-CimMethod -name cleanupconflictdirectory #Cleanup Specific Replication Groupe Name "ConflictAndDeleted" Folder# Get-CimInstance -ComputerName *hostname* -Namespace root/MicrosoftDfs -ClassName DfsrReplicatedFolderInfo -filter "ReplicationGroupName = '*ReplicationGroupName*'" | Invoke-CimMethod -name cleanupconflictdirectory

#Compare a file hash for a single file# Get-DfsrFileHash -Path '\\DC1-PSSRDFS01\d\$\PERSONNEL\DC2-PSSRDFS01.txt' | Format-Table -Auto -Wrap Get-DfsrFileHash -Path '\\DC2-PSSRDFS02\d\$\PERSONNEL\DC2-PSSRDFS01.txt' | Format-Table -Auto -Wrap #Compare file hashes for a folder# Get-DfsrFileHash -Path '\\DC1-PSSRDFS01\d\$\APPS\IT*' | Format-Table -Auto -Wrap Get-DfsrFileHash -Path '\\DC2-PSSRDFS02\d\$\APPS\IT*' | Format-Table -Auto -Wrap

Event: Service 1002 - DFS Replication service is starting 1004 - DFS Replication service has started 1006 - DFS Replication service is stopping 1008 - DFS Replication service has stopped 1102 - DFS Replication service has temporarily stopped replication because another application is performing a backup or restore operation 1104 - DFS Replication service successfully restarted replication after a backup or restore operation 1206 - DFS Replication service successfully contacted domain controller to access configuration information 4102 - DFS Replication service initialized 4104 - DFS Replication service successfully finished initial replication 4114 - The replicated folder has been disabled Staging Area 4202 - DFS Replication service has detected that the staging space in use is above the high watermark 4204 - DFS Replication service has successfully deleted old staging files & the staging space is now below the high watermark. 4206 - DFS Replication service failed to clean up old staging files 4208 - DFS Replication service detected that the staging space usage is above the staging guota 4210 - DFS Replication service cleaned up the oldest staging files 4212 - DFS Replication service could not replicate because the staging path is invalid or inaccessible 4302 - DFS Replication service has been repeatedly prevented from replicating a file due to consistent sharing violations encountered on the file 4304 - DFS Replication service has been repeatedly prevented from replicating a file due to consistent sharing violations encountered on the file 5002 - DFS Replication service encountered an error communicating with partner 5004 - DFS Replication service successfully established an inbound connection with partner 5012 - DFS Replication service failed to communicate with partner 5014 replication mode on the connection to partner has changed

#Nettoyer les tickets Kerberos# klist -lh 0 -li 0x3e7 purge

#Déterminez si une machine est une VM# (get-item "HKLM:\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters").GetValue("HostName")

Certificats ### #Vérification de l'expiration des certificats (- de 60 jours)# #A partir de Server 2008 R2# Get-ChildItem -Path "Cert:*" -Recurse -EXPIRINGINDAYS 60 | FL #En dessous de Server 2008# Get-ChildItem -Path "Cert:*" -Recurse | where { \$_.notafter -le (get-date).AddDays(60) -AND \$_.notafter -gt (get-date)} | fl thumbprint, subject, notafter, extensions

Windows Update ### #Répertoire des logs Windows Update & WSUS# %WINDIR%\WindowsUpdate.log %ProgramFiles%\Update Services\LogFiles\SoftwareDistribution.log #Vérifier les date de la dernière \ prochaine détection, du téléchargement et de l'installation des MaJ# (get-item

"HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Detect").GetValue("LastSuccessTime") (get-item "HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update").GetValue("NextDetectionTime") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Download").GetValue("LastSuccessTime") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install").GetValue("LastSuccessTime") #Vérifier la configuration registre de Windows Update# reg query "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" #Réinitialiser la connectivité d'un client WSUS et réactiver sa détection# wuauclt.exe /resetauthorization /detectnow #Réinitialiser l'ID WSUS (en cas de doublon d'ID WSUS lors de clone / ghost)# net stop wuauserv reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v AccountDomainSid /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v PingID /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientId /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientId /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientIDValidation /f net start wuauserv wuauclt /resetauthorization /detectnow #Lancer le processus de mise à jour# wuauclt.exe /UpdateNow #Forcer la détection des MaJ côté client + Mettre à jour le client WSUS dans la console WSUS# wuauclt.exe /DetectNow /ReportNow

#Getting Hotfix Information# Get-WMIObject Win32_QuickFixEngineering

reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" ((value "InstallDate" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" of native registry as integer) * second) + ("01 Jan 1970 00:00:00" as local time) (get-item "HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion").GetValue("InstallDate")

NTP ### #Vérifier la configuration du service NTP# (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters").GetValue(" Type") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient").GetValue("SpecialPollInterval") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config").GetValue("Anno unceFlags") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters").GetValue(" NtpServer") w32tm /query /status w32tm /query /peers w32tm /query /source w32tm /monitor

#Retrouver le PDC# Import-Module ActiveDirectory Get-ADDomain | Select-Object PDCEmulator #Resynchroniser l'horloge dès que possible# w32tm /resync /rediscover #Reset time service net stop w32time w32tm /unregister w32tm /register net start w32time

#Configuration of PDC w32tm /config /manualpeerlist:"0.pool.ntp.org,0x9 1.pool.ntp.org,0x9 2.pool.ntp.org,0x9 3.fr.pool.ntp.org,0x9" /syncfromflags:manual /reliable:yes /update W32tm /resync /rediscover net stop w32time && net start w32time #Configuration of Non-PDC w32tm /config /syncfromflags:domhier /update W32tm /resync /rediscover net stop w32time && net start w32time

GPO ### #Forcer l'application des GPO# gpupdate /force #Afficher les données RSOP# gpresult /R #Enregistrer le rapport RSOP# gpresult /h %USERPROFILE%/Desktop/GPO.html

#SYN_SENT# netstat -a | findstr -i "SYN_SENT" #tester un port# http://portquiz.net:XXXX

#Vérifier l'intégrité du système# sfc /scannow cmd cd %USERPROFILE%\Desktop && findstr /c:"[SR]" %windir%\logs\cbs\cbs.log > .\sfcdetails.txt sfc /scannow

Réparer une image système Windows ### #Analysez & Vérifier si une image est réparable# DISM.exe /Online /Cleanup-Image /ScanHealth DISM.exe /Online /Cleanup-Image /CheckHealth #Réparer une image# DISM.exe /Online /Cleanup-Image /RestoreHealth

#Nettoyage de disque# cleanmgr /sageset:1 cleanmgr /sagerun:1

#Analyser la taille du magasin de composants (dossier WinSxS)# DISM.exe /Online /Cleanup-Image /AnalyzeComponentStore #Supprimer toutes les versions obsolètes de chaque composant dans le magasin de composants# DISM.exe /Online /Cleanup-Image /StartComponentCleanup /Resetbase

WMI ### #Vérifier le WMI# winmgmt /verifyrepository #Réparer le WMI# winmgmt /salvagerepository #Réinitialiser le WMI# winmgmt /resetrepository

#Vérifier l'état du disque# chkdsk C: chkdsk D: #Corriger les erreurs détectées sur le disque# chkdsk C: /F /R

WinRM ### #Activer WinRM for remote management# winrm quickconfig -q #Lister tous les listeners WinRM# winrm enumerate winrm/config/listener

McAfee ### #Répertoire des logs McAfee# %deflogdir% C:\ProgramData\McAfee\Common Framework\Task #Lancer I'UI si invisible dans le systray# powershell . "C:\Program Files (x86)\McAfee\Common Framework\McTray.exe" . "C:\Program Files (x86)\McAfee\Common Framework\UdaterUI.exe" . "C:\Program Files\McAfee\Common Framework\McTray.exe" . "C:\Program Files\McAfee\Common Framework\UpdaterUI.exe" . "C:\Program Files (x86)\McAfee\Common Framework\x86\McTray.exe" . "C:\Program Files (x86)\McAfee\Common Framework\x86\UpdaterUI.exe" . "C:\Program Files (x86)\McAfee\Common Framework\x86\UpdaterUI.exe" . "C:\Program Files (x86)\McAfee\Common Framework\x86\UpdaterUI.exe" . "C:\Program Files\McAfee\Agent\x86\McTray.exe" . "C:\Program Files\McAfee\Agent\x86\UpdaterUI.exe" #Suppression de l'agent McAfee# %ProgramFiles%\McAfee\Common Framework\frminst.exe /remove=agent %ProgramFiles%\McAfee\Common Framework\frminst.exe /forceuninstall rmdir "C:\Program Files (x86)\McAfee" /S /Q rmdir "C:\ProgramData\McAfee" /S /Q #Test Antivirus X50!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

#Proxy configuration# NETSH WINHTTP SHOW PROXY #Get Proxy server# (get-item "HKCU:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings").GetValue("ProxyServer") #Get Proxy Exceptions# (get-item "HKCU:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings").GetValue("ProxyOverride") set proxy proxy-server="http=myproxy;https=sproxy:88" bypass-list="*.contoso.com"

Package Microsoft ### #Exemple suppression d'IE 9, 10 et 11# FORFILES /P %WINDIR%\servicing\Packages /M Microsoft-Windows-InternetExplorer-*9.*.mum /c "cmd /c echo Uninstalling package @fname && start /w pkgmgr /up:@fname /quiet /norestart" FORFILES /P %WINDIR%\servicing\Packages /M Microsoft-Windows-InternetExplorer-*10.*.mum /c "cmd /c echo Uninstalling package @fname && start /w pkgmgr /up:@fname /quiet /norestart" FORFILES /P %WINDIR%\servicing\Packages /M Microsoft-Windows-InternetExplorer-*10.*.mum /c "cmd /c echo Uninstalling package @fname && start /w pkgmgr /up:@fname /quiet /norestart" FORFILES /P %WINDIR%\servicing\Packages /M Microsoft-Windows-InternetExplorer-*11.*.mum /c "cmd /c echo Uninstalling package @fname && start /w pkgmgr /up:@fname /quiet /norestart" #Suppresion d'un package# dism /online /remove-package

/packagename:Package_for_KB2706045~31bf3856ad364e35~amd64~~6.1.1.0

KMS / RDS ### #Find all the KMS server on the network# nslookup -type=SRV
_vlmcs._tcp.<FQDN> #Display license information# slmgr.vbs /dli cscript
C:\Windows\System32\slmgr.vbs /dli all > c:\windows\temp\KMS_dli.txt #Display detailed license

#Find License Servers & Licensing Mode# #OS from 2003 to 2008 R2# (get-item "HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services").GetValue("LicenseServers") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TermService\Parameters\LicenseS ervers").GetValue("SpecifiedLicenseServers") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM\Licensing Core").GetValue("LicensingMode") #Value = 2 for Per device, Value = 4 for Per User #OS from 2012 to newest# (get-item "HKLM:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services").GetValue("LicenseServers") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM\Licensing Core").GetValue("LicensingMode") #Value = 2 for Per device, Value = 4 for Per User #RDS farm# (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TermService\Parameters\LicenseS ervers").GetValue("SpecifiedLicenseServers") (get-item

"HKLM:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM\Licensing Core").GetValue("LicensingMode") #Value = 2 for Per device, Value = 4 for Per User #WMI version# \$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting \$obj.LicensingType #Value = 2 for Per device, Value = 4 for Per User \$obj.LicensingName \$obj.GetSpecifiedLicenseServerList().SpecifiedLSList #Set License Servers & Licensing Mode# \$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting \$obj.SetSpecifiedLicenseServerList("myservername.fqdn") \$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting \$obj.ChangeMode(4)

Profile ### #Windows# HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Session Data #Office# HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles HKCU:\Software\Microsoft\Office\15.0\Outlook\Profiles HKCU:\Software\Microsoft\Office\16.0\Outlook\Profiles

Modify Network Connection Profile ### Get-NetConnectionProfile Set-NetConnectionProfile -InterfaceIndex <index number> -NetworkCategory {Public | Private | DomainAuthenticated}

netsh dhcp server show mibinfo

###A APPROFONDIR### #displays users logged in to a RD Session Host, along with information about whether at the console or via an RDP session qwinsta #query users quser #https://docs.microsoft.com/en-us/powershell/module/nettcpip/set-netoffloadglobalsetting?view=win1 0-ps Get-NetOffloadGlobalSetting netsh interface tcp show globa #https://technet.microsoft.com/fr-fr/library/jj130859(v=wps.630).aspx Get-NetAdapterRss Enable-NetAdapterRss -Name *

Reset Windows Update Client

cls gpupdate /force reg query "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" net stop wuauserv reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v AccountDomainSid /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v PingID /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientId /f reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientIDValidation /f net start wuauserv wuauclt.exe /resetauthorization /detectnow wuauclt.exe /UpdateNow wuauclt.exe /DetectNow /ReportNow netstat -a | findstr -i "8530"

From: http://poste2travail.free.fr/dokuwiki/ - **Poste2Travail**

Permanent link: http://poste2travail.free.fr/dokuwiki/doku.php?id=script:divers

Last update: 2020/08/10 23:07

×