Software

Powershell: Benutzer und Gruppen

Powershell ISE starten, ggf. Script-Ausführung aktivieren.

Benutzer ermitteln:

• unformatierte Langform (lokal):
Get-CimInstance -ClassName Win32_ComputerSystem -Property UserName
Get-CimInstance -ClassName Win32_ComputerSystem -Property UserName | Format-Table -Property UserName

• Kurzform (lokal)
Benutzername ohne Domain: $env:UserName

• Lokal und Remote:
qwinsta /server:remotePC

AD Gruppen auslesen:

get-adgroup

Check ob User in einer Gruppe ist:

```
$user = $env:username
$group = "DeineSoftwaregruppe"
$members = Get-ADGroupMember -Identity $group
 -Recursive | Select -ExpandProperty Name

If ($members -contains $user) {
      Softwareinstallation, weil User ist in Gruppe
      Am Ende: Remove-
ADGroupMember -Identity DeineSoftwaregruppe -Members $user
 } Else {
       User ist nicht in Gruppe, tue XY
}
```

User zu Gruppe hinzu fügen:

```
PS: Add-ADGroupMember -Identity Gruppenname -Members Username
```

CMD:

```
net localgroup /add administrators Domain\adminuser
net localgroup /add administratoren Domain\adminuser
```

Gruppe entfernen:

```
Remove-ADGroupMember
```

Letzte angemeldete User auslesen:

get-eventlog -newest 10 -logname security | Format-List

Support-Admin Konto auktivieren, Remotesitzung, anschließend Konto deaktivieren:
- mittels PS-Script: GenerateRandomPassword.ps1
- lokalen Admin anlegen, Konto deaktivieren
- per Script Konto aktivieren, Zufallspasswort setzen, RDP anmelden, Konto wieder deaktivieren
Quelle:
https://administrator.de/tutorial/sicherer-umgang-mit-supportkonten-262066.html

@echo off
set /p target=Auf welchen PC willst Du?: %=%
for /f %%a in ('powershell \\server\share\GenerateRandomPassword.ps1') do net user admin%target% %%a /domain /active
/workstations:%computername%,%target% & cmdkey /add:TERMSRV/%target% /user:netbiosdomainname\admin%target% /pass:%%a
start /wait mstsc /v:%target%
pause
net user admin%target% /active:no /domain

PowerShell Remoting
https://docs.microsoft.com/de-de/powershell/scripting/learn/remoting/running-remote-commands?view=powershell-7

Windows Remoteverwaltung konfigurieren:
WINRM QUICKCONFIG - Firewall: Port 5985, Dienststart...

Inaktive Benutzerkonten per Powershell finden.
Bsp: Nutzer haben sich > 90 Tage nicht angemeldet

Search-ADAccount -AccountInactive -UsersOnly -TimeSpan 90.00:00:00 |

```
Where {$_.Enabled -eq “True”} |
Sort -property LastLogonDate -desc |
ft UserPrincipalName, LastLogonDate -autosize
```

Eindeutige ID: #1391
Verfasser: Uwe Kernchen
Letzte Änderung: 2024-02-05 21:58