

PowerShell 2.0

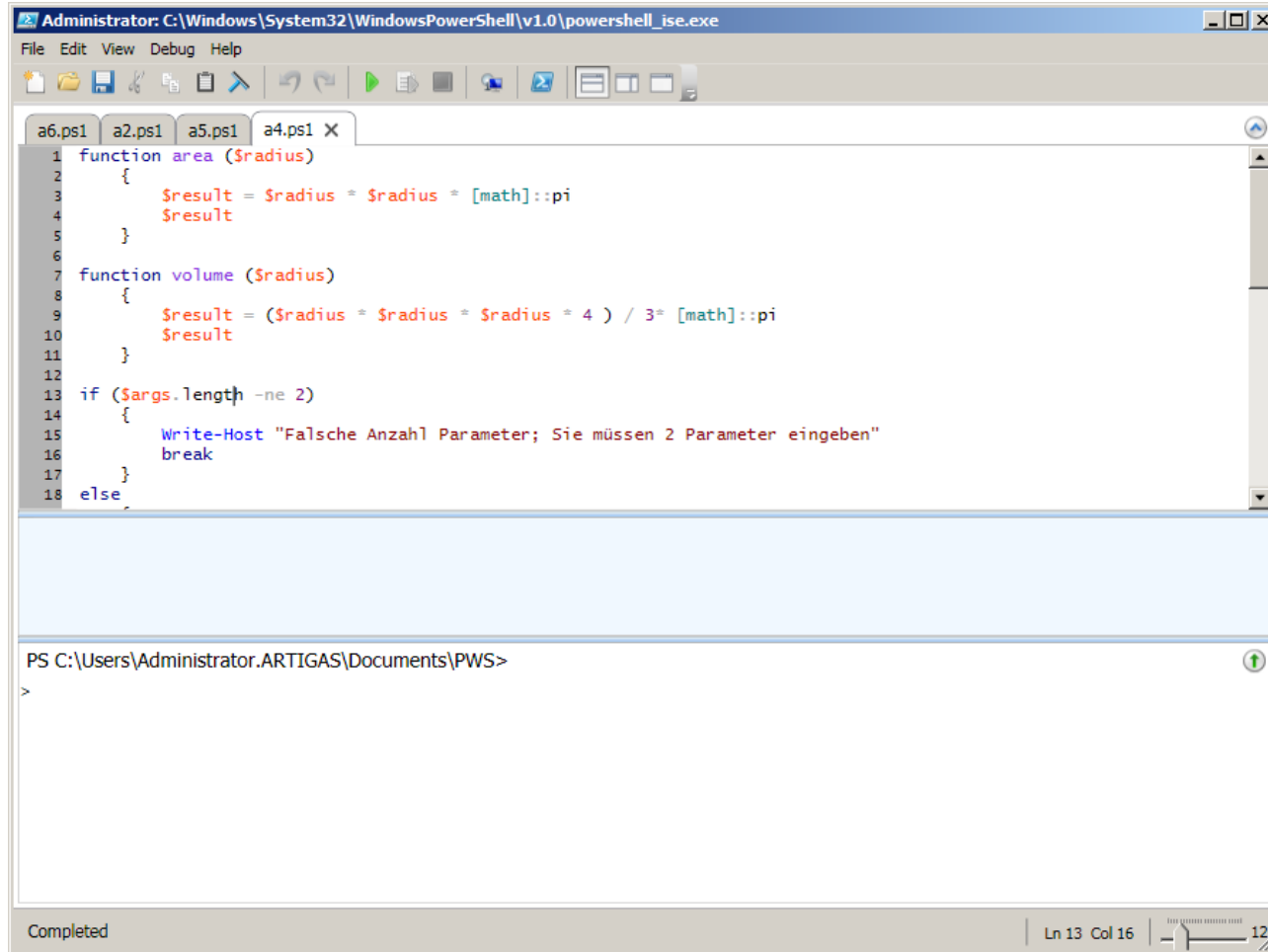
Übersicht & Neuigkeiten

Referent: Raúl B. Heiduk, Dipl. Ing. (FH)

Inhalt

- PowerShell Neuigkeiten
 - ISE
 - Sessions, Jobs
 - Remote Scripting
 - Modules
 - Transcripts, Transactions
- Einsatz von PowerShell
 - Verwaltung von Rollen und Features
 - Einführung in AD-CmdLets
 - Verwaltung von Freigaben, Druckern und TCP/IP
 - Überwachung und Optimierung von Windows Betriebssystemen

Integrated Scripting Environment (ISE)



```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
File Edit View Debug Help
a6.ps1 a2.ps1 a5.ps1 a4.ps1 X
1 function area ($radius)
2 {
3     $result = $radius * $radius * [math]::pi
4     $result
5 }
6
7 function volume ($radius)
8 {
9     $result = ($radius * $radius * $radius * 4 ) / 3 * [math]::pi
10    $result
11 }
12
13 if ($args.length -ne 2)
14 {
15     Write-Host "Falsche Anzahl Parameter; Sie müssen 2 Parameter eingeben"
16     break
17 }
18 else
19 {
20 }
21 }

PS C:\Users\Administrator.ARTIGAS\Documents\PWS>
>

Completed | Ln 13 Col 16 | 12
```

Integrated Scripting Environment (ISE)

- Farbige Kennzeichnung der Variablen, Funktionen, Cmdlets und Texte
- Haltepunkte können beliebig gesetzt werden (F9)
- Single Step (F11), Schritt überspringen (F10)
- Ausgabefenster für Resultate einzelner Kommandos
- Tooltips zeigen Variableninhalte an
- Scripts in unterschiedlichen Registern
- Jedes Register kann auch eine Remote Session darstellen

```
$m.From = "me@digicomp.ch"  
$m.To.add("rh@pobox.com")  
$m.Subject = "Test"  
$m.Body = "Das ist der eigentliche Text"  
$s.Send($m.Subject = Test)
```

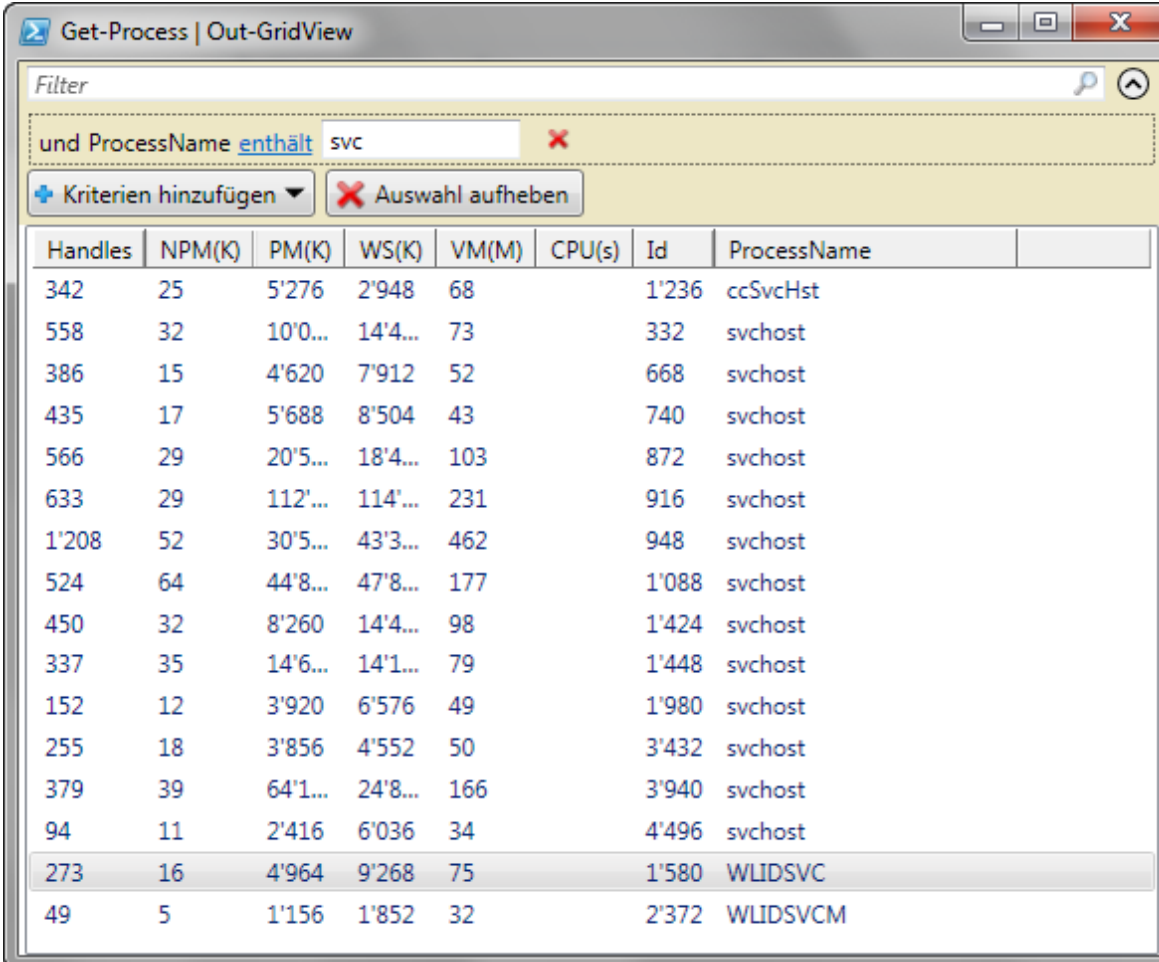
Über 60 neue Cmdlets

- `Add-Computer`, `Remove-Computer`
- `Rename-Computer`, `Stop-Computer`, `Restart-Computer`
- `Checkpoint-Computer`, `Restore-Computer`
- `Get-Counter`, `Import-Counter`, `Export-Counter`
- `Get-Hotfix`
- `Limit-EventLog`, `New-EventLog`, `Remove-EventLog`
- `Wait-Process`
- `Rename-Computer`, `Reset-ComputerMachinePassword`
- `New-WebServiceProxy`
- `Get-Module`, `Import-Module`, `New-Module`, `Remove-Module`
- `Connect-WSMan`, `Out-GridView`
- Und viele mehr...

Out-Gridview

- Erfordert .NET-Framework 3.5 mit SP1
- Spalten ein-/ausblenden
- Sortieren
- Schneller Filter
- Kriterienfilter
- Zeilen kopieren/einfügen, um die Daten in eine Excel-Arbeitsmappe zu übertragen

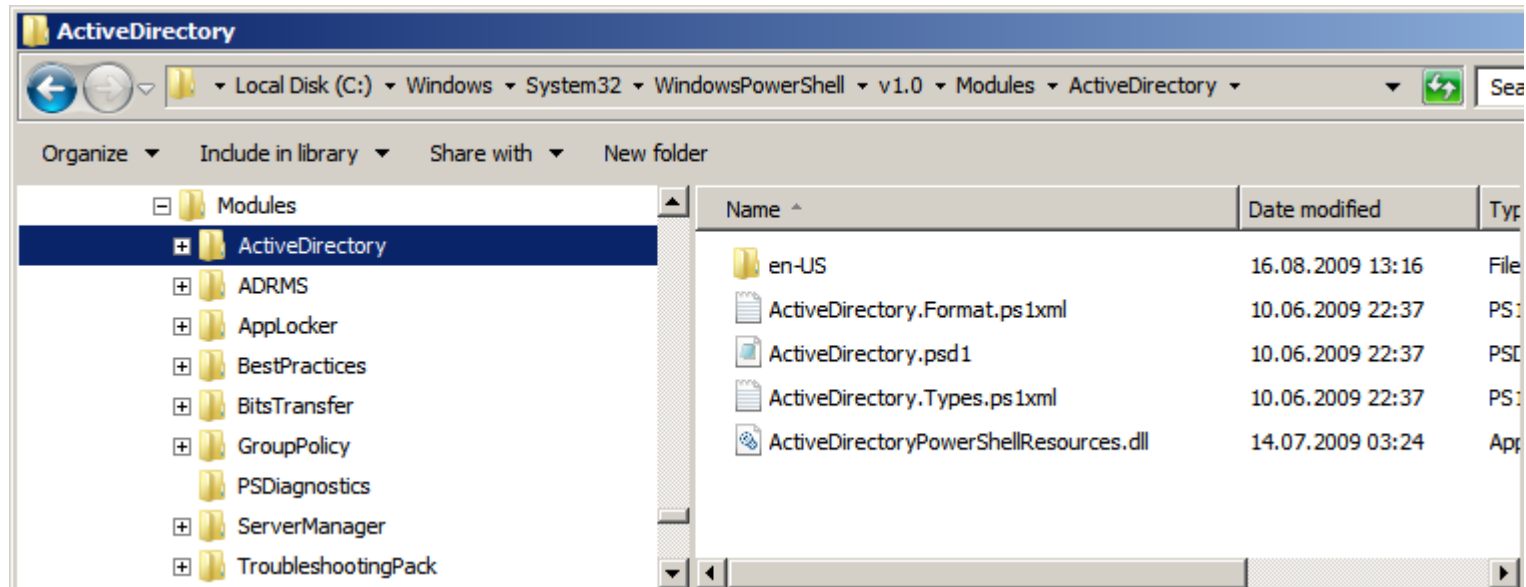
Out-GridView



The screenshot shows a Windows PowerShell window titled "Get-Process | Out-GridView". The window has a search filter set to "und ProcessName enthält svc". Below the filter, there are two buttons: "Kriterien hinzufügen" (Add criteria) and "Auswahl aufheben" (Remove selection). The main area displays a table of process information.

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
342	25	5'276	2'948	68		1'236	ccSvcHst
558	32	10'0...	14'4...	73		332	svchost
386	15	4'620	7'912	52		668	svchost
435	17	5'688	8'504	43		740	svchost
566	29	20'5...	18'4...	103		872	svchost
633	29	112'...	114'...	231		916	svchost
1'208	52	30'5...	43'3...	462		948	svchost
524	64	44'8...	47'8...	177		1'088	svchost
450	32	8'260	14'4...	98		1'424	svchost
337	35	14'6...	14'1...	79		1'448	svchost
152	12	3'920	6'576	49		1'980	svchost
255	18	3'856	4'552	50		3'432	svchost
379	39	64'1...	24'8...	166		3'940	svchost
94	11	2'416	6'036	34		4'496	svchost
273	16	4'964	9'268	75		1'580	WLIDSVC
49	5	1'156	1'852	32		2'372	WLIDSVCM

PowerShell Modules



PowerShell Module

- Script-Funktionen
 - Reserviertes Verzeichnis im Benutzerprofil oder im Systemverzeichnis für benutzerdefiniert Module
- .NET Assemblies
- PowerShell Snap-Ins
- Benutzerdefinierte Ansichten und Datentypen, die in .PS1XML-Dateien beschrieben sind

Sessions, Jobs und remote Scripting

- Einige CmdLets haben eingebauten Remotezugriff
 - WMI
 - Eventlog
 - Dienstverwaltung
 - Computerverwaltung (Restart, Remove)
- Mit WinRM lässt sich jedoch jedes CmdLet remote aufrufen
- Remote Sessions sind ebenfalls möglich

PowerShell für Remotezugriff einrichten

- PowerShell als Administrator starten (!)
- `Get-Service winrm`: ist der Dienst gestartet?
- `Enable-PSRemoting [-force]`: bereitet die Remotefunktion vor
- Falls der entfernte Computer nicht vertrauenswürdig ist:
 - `Winrm s winrm/config/client`
`'@{Trustedhosts="Client01"}'`

Remote-Kommandos

- `Invoke-Command`
 - `Invoke-Command -computename Client01 -scriptblock {Get-Process}`
- `New-PSSession`
- `Get-PSSession`
- `Enter-PSSession`
- `Exit-PSSession`
- `Import-PSSession`
- `Export-PSSession`

Remote Sessions aufrufen

- `$s = New-PSSession -computename client01`
- `Invoke-Command -session $s -scriptblock {Get-Process}`
- `Invoke-Command -session $s {powercfg.exe -energy}`
- Kommandos können auch als Hintergrundjobs aufgerufen werden
 - `Invoke-Command -session $s {powercfg.exe -energy} -AsJob`

Remote Jobs ausführen

- Job in einer Interaktive Session starten
- Background Job auf einem entfernten Computer starten, der ein Ergebnis auf dem lokalen Computer zurückgibt
- Background Job auf einem entfernten Computer starten, der ein Ergebnis auf dem entfernten Computer zurückgibt

Job CmdLets

- **Get-Job**: Anzeige gestarteter Hintergrund-Jobs
- **Receive-Job**: Liefert die Ausgabe und Fehler der Hintergrund-Jobs der aktuellen Sitzung
- **Remove-Job**: Löscht gestartete Jobs
- **Start-Job**: Startet einen Hintergrund-Job auf dem Lokalen Computer
- **Stop-Job**: Beendet Hintergrund-Jobs
- **Wait-Job**: Hält Hintergrund-Jobs an

CmdLets die den Parameter `-AsJob` erkennen

- `Invoke-Command`
- `Invoke-WmiMethod`
- `Test-Connection`
- `Restart-Computer`
- `Stop-Computer`

Ohne WinRM Remote-Befehle ausführen

- `Get-WinEvent`
- `Clear-EventLog, Show-EventLog, Write-EventLog, New-EventLog, Get-EventLog, Limit-EventLog, Remove-EventLog`
- `Get-WmiObject`
- `Set-Service, Get-Service`
- `Stop-Computer, Add-Computer, Restart-Computer, Remove-Computer, Rename-Computer`
- `Reset-ComputerMachinePassword`

Transactions

- Transactions dienen dazu, eine Serie von Kommandos als Einheit anzusehen, die entweder komplett ausgeführt oder rückgängig gemacht wird
- Transactions werden üblicherweise in Datenbanken angewendet, wo sicher gestellt werden soll, dass erst wenn die Kommandos korrekt sind, ausgeführt werden
- Nicht alle Kommandos in PowerShell unterstützen Transactions
 - Provider: Provider, die Transactions unterstützen sollen, müssen dafür geeignet sein
 - `Get-PSProvider | where {$_.capabilities -like "*transactions*" }`
 - CmdLet: Nur bestimmte CmdLets unterstützen Transaktionen
 - `New-Item, Set-Item, Clear-Item, Copy-Item, Move-Item, Remove-Item`
 - `Get-Help * - Parameter UseTransaction`

Transactions

- Transaction wird gestartet
 - `Start-Transaction`
 - `Get-Transaction`
- Kommandos werden ausgeführt, aber nicht endgültig appliziert
 - Parameter `-UseTransaction` muss explizit angegeben werden
- Transactions werden bestätigt oder rückgängig gemacht
 - `Complete-Transaction`
 - `Undo-Transaction`
 - `User-Transaction`
- Kein Lock-Feature vorhanden, d.h. andere Kommandos können parallel zu den in Transaction befindlichen Objekten Veränderungen durchführen
- Nur eine Transaction kann pro PowerShell-Sitzung aktiv sein

Steuerelemente im Script

- Kommentare werden zwischen den Steuerzeichen <# und #> angegeben und können sich über mehrere Zeilen erstrecken
- Der Bezeichner **#Requires** legt fest, welche Komponenten oder Versionen vorhanden sein müssen, damit das Script funktionieren kann
 - **#Requires -version 2.0**
 - **#Requires -ShellId "Microsoft.PowerShell"**
- **#Requires** muss in der ersten Programmzeile eines Scripts stehen

Serververwaltung

■ Konfigurationsoptionen Windows Server 2008

Windows Updates:	Install updates automatically using a managed updating service	Run Security Configuration Wizard Configure IE ESC
Last checked for updates:	Yesterday at 22:57	
Last installed updates:	Today at 03:12	
IE Enhanced Security Configuration (ESC):	Off for Administrators On for Users	

Roles Summary	Roles Summary Help
<input type="checkbox"/> Roles: 3 of 17 installed	Go to Roles

Features Summary	Features Summary Help
<input type="checkbox"/> Features: 8 of 42 installed	Add Features

Resources and Support	Resources and Support Help
Help make Windows Server better by participating in the Customer Experience Improvement Program (CEIP).	Participate in CEIP
Report issues to Microsoft and get solutions to common problems by turning on Windows Error Reporting.	Turn on Windows Error Reporting
Browse technical resources for Windows Server, including how-to help, guides, web casts, and tools.	Windows Server TechCenter
Get connected with other Microsoft customers through online community resources.	Windows Server Community Center
Send us your feedback and feature suggestions to help make Windows better.	Send Feedback to Microsoft
Search the Microsoft Update Catalog for product updates, add-ons and optional software.	Search the Microsoft Update Catalog
Browse product changes and retired Windows Server features.	Product Changes and Retired Features

Serververwaltung

- `Import-Module servermanager`
 - `Get-WindowsFeature`
 - `Add-WindowsFeature`
 - `Remove-WindowsFeature`

Get-WindowsFeature

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.ARTIGAS> Import-Module SERVERMANAGER
PS C:\Users\Administrator.ARTIGAS> Get-WindowsFeature

Display Name                                     Name
-----
[ ] Active Directory Certificate Services         AD-Certificate
[ ] Certification Authority                       ADCS-Cert-Authority
[ ] Certification Authority Web Enrollment         ADCS-Web-Enrollment
[ ] Online Responder                             ADCS-Online-Cert
[ ] Network Device Enrollment Service            ADCS-Device-Enrollment
[ ] Certificate Enrollment Web Service          ADCS-Enroll-Web-Svc
[ ] Certificate Enrollment Policy Web Service    ADCS-Enroll-Web-Pol
[X] Active Directory Domain Services             AD-Domain-Services
[X] Active Directory Domain Controller           ADDS-Domain-Controller
[ ] Identity Management for UNIX                ADDS-Identity-Mgmt
[ ] Server for Network Information Services      ADDS-NIS
[ ] Password Synchronization                   ADDS-Password-Sync
[ ] Administration Tools                       ADDS-IDMU-Tools
[ ] Active Directory Federation Services         AD-Federation-Services
[ ] Federation Service                         ADFS-Federation
[ ] Federation Service Proxy                   ADFS-Proxy
[ ] AD FS Web Agents                           ADFS-Web-Agents
[ ] Claims-aware Agent                         ADFS-Claims
[ ] Windows Token-based Agent                  ADFS-Windows-Token
[ ] Active Directory Lightweight Directory Services ADLDS
[ ] Active Directory Rights Management Services  ADRMS
[ ] Active Directory Rights Management Server    ADRMS-Server
[ ] Identity Federation Support                 ADRMS-Identity
[ ] Application Server                          Application-Server
[ ] .NET Framework 3.5.1                       AS-.NET-Framework
[ ] Web Server (IIS) Support                    AS-Web-Support
[ ] COM+ Network Access                         AS-Ent-Services
[ ] TCP Port Sharing                           AS-TCP-Port-Sharing
[ ] Windows Process Activation Service Support  AS-WAS-Support
[ ] HTTP Activation                             AS-HTTP-Activation
[ ] Message Queuing Activation                  AS-MSMQ-Activation
[ ] TCP Activation                              AS-TCP-Activation
[ ] Named Pipes Activation                      AS-Named-Pipes
[ ] Distributed Transactions                    AS-Dist-Transaction
[ ] Incoming Remote Transactions                AS-Incoming-Trans
[ ] Outgoing Remote Transactions                AS-Outgoing-Trans
[ ] WS-Atomic Transactions                      AS-WS-Atomic
[ ] DHCP Server                                DHCP
[ ] DNS Server                                  DNS
[ ] Fax Server                                  Fax
[X] File Services                              File-Services
[X] File Server                                FS-FileServer
    
```

Modul ActiveDirectory

- Das Modul wird geladen mit `Import-Module ActiveDirectory`
- AD-Objekte abrufen: 22 CmdLets
- AD-Objekte erstellen: 7 CmdLets
- AD-Objekte entfernen: 12 CmdLets
- AD-Schreibvorgänge durchführen: 15 CmdLets
- AD-Objekte hinzufügen: 5 CmdLets
- AD-Objekte und optionale AD-Funktionen de-/aktivieren: je 2 CmdLets
- AD-Objekte verschieben: 3 CmdLets
- AD-Objekte Dienstkennworte zurücksetzen: 1 CmdLet
- AD-Objekte wiederherstellen/umbenennen: je 1 CmdLet
- AD-Objekte suchen: 1 CmdLet
- AD-Objekte Dienstkonto in-/deinstallieren: je 1 CmdLet
- AD-Objekte entsperren: 1 CmdLet

Inventarisierung

- `Get-Hotfix`
- `Win32_ComputerSystem`
- `Win32_OperatingSystem`
- `Win32_UserAccount`
- `Win32_Group`
- `Get-Hotfix`

Freigaben, Drucker TCP/IP

- Win32_Share
- Win32_Printer
- Win32_TCPIPPrinterPort
- Win32_NetworkAdapter
- Win32_NetworkAdapterConfiguration



DIGICOMP

Fragen & Antworten

Drive your life.