net.com
networking & communications

HOLGER SCHWICHTENBERG

2., aktualisierte Auflage

Windows PowerShell 2.0
Das Praxisbuch

Einführung und Lösungen für Windows-Administratoren

- Für Windows XP/Server 2003/Vista/Server 2008 & Windows 7
- Kommandozeile und Scripting
- Zahlreiche Praxisbeispiele

ADDISON-WESLEY

www.IT-Visions.de
Dr. Holger Schwichtenberg

CD

3 Einzelbefehle der PowerShell

Die PowerShell kennt folgende Arten von Einzelbefehlen:

- Commandlets
- Aliase
- Ausdrücke
- Externe Befehle
- Dateinamen

3.1 Commandlets

Commandlet

Ein „normaler" PowerShell-Befehl heißt *Commandlet* (kurz: *Cmdlet*) oder *Funktion* (*Function*). Hier in diesem Kapitel geht es zunächst nur um Commandlets. Eine Funktion ist eine Möglichkeit, in der PowerShell selbst wieder einen Befehl zu erstellen, der funktioniert wie ein Commandlet. Da die Unterscheidung zwischen Commandlets und Funktionen aus Nutzersicht zum Teil akademischer Art ist, erfolgt hier zunächst keine Differenzierung.

Ein Commandlet besteht typischerweise aus drei Teilen:

- einem Verb,
- einem Substantiv und
- einer (optionalen) Parameterliste.

Verb und Substantiv werden durch einen Bindestrich „–" voneinander getrennt, die optionalen Parameter durch Leerzeichen. Daraus ergibt sich der folgende Aufbau:

```
Verb-Substantiv [-Parameterliste]
```

Die Groß- und Kleinschreibung ist bei den Commandlet-Namen nicht relevant.

Ein einfaches Beispiel ohne Parameter lautet:

```
Get-Process
```

Dieser Befehl holt eine Liste aller Prozesse.

Die Tabulatorvervollständigung in der PowerShell-Konsole funktioniert bei Commandlets, wenn man das Verb und den Strich bereits eingegeben hat, z.B. `Export-` ↹. Auch Platzhalter kann man dabei verwenden. Die Eingabe `Get-?e*` ↹ liefert `Get-Help` ↹ `Get-Member` ↹ `Get-Service`.

Commandlet-Parameter

Parameter

Durch Angabe eines Parameters werden nur diejenigen Prozesse angezeigt, deren Name auf das angegebene Muster zutrifft:

```
Get-Process  i*
```

Ein weiteres Beispiel für einen Befehl mit Parameter ist:

```
Get-ChildItem c:\daten
```

`Get-ChildItem` listet alle Unterobjekte des angegebenen Objekts (*c:\daten*) auf, also alle Dateien und Ordner unterhalb dieses Dateiordners.

Parameter werden als Zeichenkette aufgefasst – auch wenn sie nicht explizit in Anführungszeichen stehen. Die Anführungszeichen sind optional. Man muss Anführungszeichen nur verwenden, wenn Leerzeichen vorkommen, denn das Leerzeichen dient als Trennzeichen zwischen Parametern:

```
Get-ChildItem "C:\Program Files"
```

Alle Commandlets haben zahlreiche Parameter, die durch Namen voneinander unterschieden werden. Ohne die Verwendung von Parameternamen werden vordefinierte Standardattribute belegt, d.h., die Reihenfolge ist entscheidend.

```
Get-ChildItem C:\temp *.doc
```

bedeutet das Gleiche wie:

```
Get-ChildItem -Path C:\temp -Filter *.doc
```

Wenn ein Commandlet mehrere Parameter besitzt, ist die Reihenfolge der Parameter entscheidend oder der Nutzer muss die Namen der Parameter mit angeben. Alle folgenden Befehle sind gleichbedeutend:

```
Get-ChildItem C:\temp *.doc
Get-ChildItem -Path C:\temp -Filter *.doc
Get-ChildItem -Filter *.doc -Path C:\temp
```

Bei der Angabe von Parameternamen kann man die Reihenfolge der Parameter ändern:

```
Get-ChildItem -Filter *.doc -Path C:\temp
```

Hingegen ist Folgendes falsch, weil die Parameter nicht benannt sind und die Reihenfolge falsch ist:

```
Get-ChildItem *.doc C:\temp
```

Schalter-Parameter

Schalter-Parameter (engl. Switch) sind Parameter, die keinen Wert haben. Durch die Verwendung des Parameternamens wird die Funktion aktiviert, z.B. das rekursive Durchlaufen durch einen Dateisystembaum mit `-recurse`:

```
Get-ChildItem h:\demo\powershell -recurse
```

Berechnungen in Parametern

Parameter können berechnet, d.h. aus Teilzeichenketten zusammengesetzt sein, die mit einem Pluszeichen verbunden werden. (Dies macht insbesondere Sinn in Zusammenhang mit Variablen, die aber erst später in diesem Buch eingeführt werden.)

Der folgende Ausdruck führt jedoch nicht zum gewünschten Ergebnis, da auch hier das Trennzeichen vor und nach dem + ein Parametertrenner ist.

```
Get-ChildItem "c:\" + "Windows" *.dll -Recurse
```

Auch ohne die beiden Leerzeichen vor und nach dem + geht es nicht. In diesem Fall muss man durch eine runde Klammer dafür sorgen, dass die Berechnung erst ausgeführt wird:

```
Get-ChildItem ("c:\" + "Windows") *.dll -Recurse
```

Es folgt dazu noch ein Beispiel, bei dem Zahlen berechnet werden. Der folgende Befehl liefert den Prozess mit der ID 2900:

```
Get-Process -id (2800+100)
```

Weitere Beispiele

```
Get-Service -exclude "[k-z]*"
```

zeigt nur diejenigen Systemdienste an, deren Name nicht mit den Buchstaben „k“ bis „z“ beginnt.

Auch mehrere Parameter können der Einschränkung dienen. Der folgende Befehl liefert nur die Benutzereinträge aus einem bestimmten Active-Directory-Pfad. (Das Beispiel setzt die Installation der PSCX voraus.)

```
Get-ADObject -dis "LDAP://E02/ou=Geschäftsführung,
OU=www.IT-Visions.de,dc=IT-Visions,dc=local" -class user
```

Tabulatorvervollständigung klappt auch bei Parametern. Versuchen Sie einmal folgende Eingabe an der PowerShell-Konsole: `Get-ChildItem -` ⇆

Platzhalter

An vielen Stellen sind Platzhalter bei den Parameterwerten erlaubt.

Eine Liste aller Prozesse, die mit einem „i“ anfangen, erhält man so:

```
Get-Process i*
```

Weitere Aspekte zu Commandlets

Beachten Sie, dass bei den Commandlets das Substantiv im Singular steht, auch wenn eine Menge von Objekten abgerufen wird. Das Ergebnis muss nicht immer eine Objektmenge sein. Beispielsweise liefert

```
Get-Location
```

nur ein Objekt mit dem aktuellen Pfad.

Mit

```
Set-Location c:\windows
```

wechselt man den aktuellen Pfad. Diese Operation liefert gar kein Ergebnis.

Die Groß- und Kleinschreibung der Commandlet-Namen und der Parameternamen ist irrelevant.

Verben

Gemäß der PowerShell-Konventionen soll es nur eine begrenzte Menge wiederkehrender Verben geben: `Get`, `Set`, `Add`, `New`, `Remove`, `Clear`, `Push`, `Pop`, `Write`, `Export`, `Select`, `Sort`, `Update`, `Start`, `Stop`, `Invoke` usw. Außer diesen Basisoperationen gibt es auch Ausgabekommandos wie `Out` und `Format`. Auch Bedingungen werden durch diese Syntax abgebildet (`Where-Object`).

Prozessmodell

Die PowerShell erzeugt beim Start einen Prozess. In diesem Prozess laufen alle Commandlets. Dies ist ein Unterschied zum DOS-ähnlichen Windows-Kommandozeilenfenster, bei dem die ausführbaren Dateien (*.exe*) in eigenen Prozessen laufen.

3.2 Aliase

Namensersetzungen

Durch sogenannte Aliase kann die Eingabe von Commandlets verkürzt werden. So ist `ps` als Alias für `Get-Process` oder `help` für `Get-Help` vordefiniert. Statt `Get-Process i*` kann also auch geschrieben werden: `ps i*`.

Aliase auflisten

Durch `Get-Alias` (oder den entsprechenden Alias `aliases`) erhält man eine Liste aller vordefinierten Abkürzungen in Form von Instanzen der Klasse `System.Management. Automation.AliasInfo`.

Durch Angabe eines Namens bei `Get-Alias` erhält man die Bedeutung eines Alias:

```
Get-Alias pgs
```

Möchte man zu einem Commandlet alle Aliase wissen, muss man allerdings schreiben:

```
Get-Alias | Where-Object { $_.definition -eq "Get-Process " }
```

Dies erfordert schon den Einsatz einer Pipeline, die erst im nächsten Kapitel besprochen wird.

Alias	Commandlet
%	ForEach-Object
?	Where-Object
Ac	Add-Content
Asnp	Add-PSSnapIn
Cat	Get-Content
Cd	Set-Location
Chdir	Set-Location
Clc	Clear-Content
Clear	Clear-Host
Clhy	Clear-History
Cli	Clear-Item
Clp	Clear-ItemProperty
Cls	Clear-Host
Clv	Clear-Variable
Compare	Compare-Object
Copy	Copy-Item
Cp	Copy-Item
Cpi	Copy-Item
Cpp	Copy-ItemProperty
Cvpa	Convert-Path
Dbp	Disable-PSBreakpoint
Del	Remove-Item
Diff	Compare-Object
Dir	Get-ChildItem
Ebp	Enable-PSBreakpoint
Echo	Write-Output
Epal	Export-Alias
epcsv	Export-Csv
epsn	Export-PSSession
erase	Remove-Item
etsn	Enter-PSSession

***Tabelle 3.1**: Vordefinierte Aliase in der PowerShell 2.0*

Alias	Commandlet
exsn	Exit-PSSession
fc	Format-Custom
fl	Format-List
foreach	ForEach-Object
ft	Format-Table
fw	Format-Wide
gal	Get-Alias
gbp	Get-PSBreakpoint
gc	Get-Content
gci	Get-ChildItem
gcm	Get-Command
gcs	Get-PSCallStack
gdr	Get-PSDrive
ghy	Get-History
gi	Get-Item
gjb	Get-Job
gl	Get-Location
gm	Get-Member
gmo	Get-Module
gp	Get-ItemProperty
gps	Get-Process
group	Group-Object
gsn	Get-PSSession
gsnp	Get-PSSnapIn
Gsv	Get-Service
Gu	Get-Unique
Gv	Get-Variable
Gwmi	Get-WmiObject
H	Get-History
History	Get-History
Icm	Invoke-Command
Iex	Invoke-Expression
Ihy	Invoke-History
Ii	Invoke-Item
Ipal	Import-Alias
Ipcsv	Import-Csv
Ipmo	Import-Module

***Tabelle 3.1**: Vordefinierte Aliase in der PowerShell 2.0 (Forts.)*

Alias	Commandlet
Ipsn	Import-PSSession
Ise	powershell_ise.exe
Iwmi	Invoke-WMIMethod
Kill	Stop-Process
Lp	Out-Printer
Ls	Get-ChildItem
Man	help
Md	mkdir
Measure	Measure-Object
Mi	Move-Item
Mount	New-PSDrive
Move	Move-Item
Mp	Move-ItemProperty
Mv	Move-Item
Nal	New-Alias
ndr	New-PSDrive
ni	New-Item
nmo	New-Module
nsn	New-PSSession
nv	New-Variable
ogv	Out-GridView
oh	Out-Host
popd	Pop-Location
ps	Get-Process
pushd	Push-Location
pwd	Get-Location
R	Invoke-History
rbp	Remove-PSBreakpoint
rcjb	Receive-Job
rd	Remove-Item
rdr	Remove-PSDrive
ren	Rename-Item
ri	Remove-Item
rjb	Remove-Job
rm	Remove-Item
rmdir	Remove-Item
rmo	Remove-Module

***Tabelle 3.1**: Vordefinierte Aliase in der PowerShell 2.0 (Forts.)*

Alias	Commandlet
rni	Rename-Item
rnp	Rename-ItemProperty
rp	Remove-ItemProperty
rsn	Remove-PSSession
rsnp	Remove-PSSnapin
rv	Remove-Variable
Rvpa	Resolve-Path
Rwmi	Remove-WMIObject
Sajb	Start-Job
Sal	Set-Alias
Saps	Start-Process
Sasv	Start-Service
Sbp	Set-PSBreakpoint
Sc	Set-Content
Select	Select-Object
Set	Set-Variable
Si	Set-Item
Sl	Set-Location
Sleep	Start-Sleep
Sort	Sort-Object
Sp	Set-ItemProperty
Spjb	Stop-Job
Spps	Stop-Process
Spsv	Stop-Service
Start	Start-Process
Sv	Set-Variable
Swmi	Set-WMIInstance
Tee	Tee-Object
Type	Get-Content
Where	Where-Object
Wjb	Wait-Job
Write	Write-Output

***Tabelle 3.1**: Vordefinierte Aliase in der PowerShell 2.0 (Forts.)*

Neue Aliase anlegen

Set-Alias, New-Aliase

Einen neuen Alias definiert der Nutzer mit `Set-Alias` oder `New-Alias`, z.B.:

```
Set-Alias procs Get-Process
New-Alias procs Get-Process
```

Der Unterschied zwischen `Set-Alias` und `New-Alias` ist marginal: `New-Alias` erstellt einen neuen Alias und liefert einen Fehler, wenn der zu vergebende Alias schon existiert. `Set-Alias` erstellt einen neuen Alias oder überschreibt einen Alias, wenn der zu vergebende Alias schon existiert. Mit dem Parameter `-description` kann man jeweils auch einen Beschreibungstext setzen.

Man kann einen Alias nicht nur für Commandlets, sondern auch für klassische Anwendungen vergeben, z.B.:

```
Set-Alias np notepad.exe
```

Beim Anlegen eines Alias wird nicht geprüft, ob es das zugehörige Commandlet bzw. die Anwendung überhaupt gibt. Der Fehler würde erst beim Aufruf des Alias auftreten.

Man kann in Aliasdefinitionen keinen Parameter mit Werten vorbelegen. Möchten Sie zum Beispiel definieren, dass die Eingabe von „Temp" die Aktion „Get-ChildItem c:\Temp" ausführt, brauchen Sie dafür eine Funktion. Mit einem Alias geht das nicht.

```
Function Temp { Get-Childitem c:\temp }
```

Funktionen werden später (siehe *Kapitel 6 „PowerShell-Skripte"*) noch ausführlich besprochen. Die Windows PowerShell enthält zahlreiche vordefinierte Funktionen, z.B. `c:`, `d:`, `e:` sowie `mkdir` und `help`.

Die neu definierten Aliase gelten jeweils nur für die aktuelle Instanz der PowerShell-Konsole. Man kann die eigenen Alias-Definitionen exportieren mit `Export-Alias` und später wieder importieren mit `Import-Alias`. Als Speicherformate stehen das CSV-Format und das PowerShell-Skriptdateiformat (*.ps1* – siehe spätere Kapitel) zur Verfügung. Bei dem PS1-Format ist zum späteren Reimport der Datei das Skript mit dem Punkt-Operator (engl. „Dot Sourcing") aufzurufen.

	Dateiformat CSV	**Dateiformat .ps1**
Speichern	`Export-Alias c:\meinealias.csv`	`Export-Alias c:\meinealias.ps1 -as script`
Laden	`Import-Alias c:\meinealias.csv`	`. c:\meinealias.ps1`

Die Anzahl der Aliase ist im Standard auf 4096 beschränkt. Dies kann durch die Variable `$MaximumAliasCount` geändert werden.

Aliase für Eigenschaften

Aliase sind auch auf Ebene von Eigenschaften definiert. So kann man statt

```
Get-Process processname, workingset
```

auch schreiben:

```
Get-Process  name, ws
```

Diese Aliase der Attribute sind definiert in der Datei *types.ps1xml* im Installationsordner der PowerShell.

Abbildung 3.1 types.ps1xml

3.3 Ausdrücke

Mathematik

Ebenfalls als Befehl direkt in die PowerShell eingeben kann man Ausdrücke, z.B. mathematische Ausdrücke wie

```
10* (8 + 6)
```

Oder Zeichenkettenausdrücke wie:

```
"Hello "+ " " + "World"
```

Microsoft spricht hier vom Expression Mode der PowerShell im Kontrast zum Command Mode, der verwendet wird, wenn man

```
Write-Output 10* (8 + 6)
```

aufruft.

Command Mode versus Expression Mode

Die PowerShell kennt zwei Verarbeitungsmodi für Befehle: einen Befehlsmodus (Command Mode) und einen Ausdrucksmodus (Expression Mode). Im Befehlsmodus werden alle Eingaben als Zeichenketten behandelt. Im Ausdrucksmodus werden Zahlen und Operationen verarbeitet. Als Faustregel gilt: Wenn eine Zeile mit einem Buchstaben oder den Sonderzeichen kaufmännisches Und (&), Punkt (.) oder Schrägstrich ("\") beginnt, dann ist die Zeile im Befehlsmodus. Wenn die Zeile mit einer Zahl, einem Anführungszeichen (" oder '), einer Klammer ("(") oder dem @-Zeichen („Klammeraffe“) beginnt, dann ist die Zeile im Ausdrucksmodus.

Befehls- und Ausdrucksmodus können gemischt werden. Dabei muss man in der Regel runde Klammern zur Abgrenzung verwenden. In einen Befehl kann ein Ausdruck durch Klammern eingebaut werden. Außerdem kann eine Pipeline mit einem Ausdruck beginnen. Die folgende Tabelle zeigt verschiedene Beispiele zur Erläuterung.

Beispiel	Bedeutung
`2+3`	Ist ein Ausdruck. Die PowerShell führt die Berechnung aus und liefert 5.
`echo 2+3`	Ist ein reiner Befehl. „2+3“ wird als Zeichenkette angesehen und ohne Auswertung auf dem Bildschirm ausgegeben.
`echo (2+3)`	Ist ein Befehl mit integriertem Ausdruck. Auf dem Bildschirm erscheint 5.
`2+3 | echo`	Ist eine Pipeline, die mit einem Ausdruck beginnt. Auf dem Bildschirm erscheint 5.
`echo 2+3 | 7+6`	Ist eine unerlaubte Eingabe. Ausdrücke dürfen in der Pipeline nur als erstes Element auftauchen.
`$a = Get-Process`	Ist ein Ausdruck mit integriertem Befehl. Das Ergebnis wird einer Variablen zugewiesen.

***Tabelle 3.2**: Ausdrücke in der Windows PowerShell*

Beispiel	Bedeutung
`$a | Get-Process`	Ist eine Pipeline, die mit einem Ausdruck beginnt. Der Inhalt von $a wird als Parameter an Get-Process übergeben.
`Get-Process | $a`	Ist eine unerlaubte Eingabe. Ausdrücke dürfen in der Pipeline nur als erstes Element auftauchen.
"Anzahl der laufenden Prozesse: (Get-Process).Count"	Es ist wohl nicht das, was gewünscht ist, denn die Ausgabe ist: Anzahl der laufenden Prozesse: (Get-Process).Count
"Anzahl der laufenden Prozesse: $((Get-Process).Count)"	Jetzt ist die Ausgabe "Anzahl der laufenden Prozesse: 95", weil $(…) einen Unterausdruck (Subexpression) einleitet und dafür sorgt, dass Get-Process ausgeführt wird.

***Tabelle 3.2**: Ausdrücke in der Windows PowerShell (Forts.)*

3.4 Externe Befehle

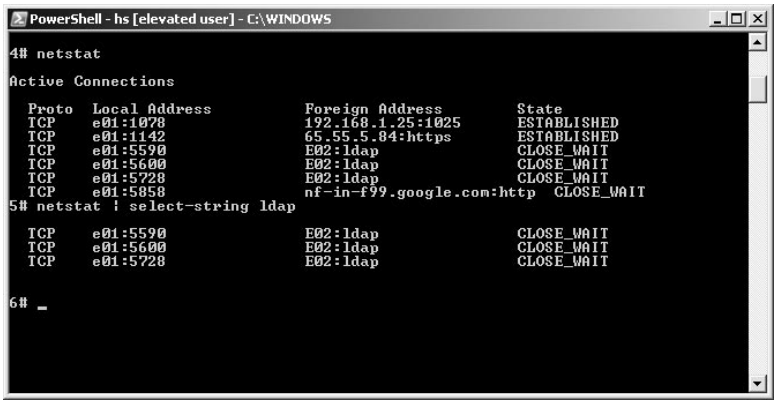
Windows-Anwendungen, DOS-Befehle, WSH-Skripte

Alle Eingaben, die nicht als Commandlets oder mathematische Formeln erkannt werden, werden als externe Anwendungen behandelt. Es können sowohl klassische Kommandozeilenbefehle (wie *ping.exe*, *ipconfig.exe* und *netstat.exe*) als auch Windows-Anwendungen ausgeführt werden.

Die Eingabe `c:\Windows\Notepad.exe` ist daher möglich, um den „beliebten" Windows-Editor zu starten. Auf gleiche Weise können auch WSH-Skripte aus der PowerShell heraus gestartet werden.

Die folgende Bildschirmabbildung zeigt den Aufruf von *netstat.exe*. Zuerst wird die Ausgabe nicht gefiltert. Im zweiten Beispiel kommt zusätzlich das Commandlet `Select-String` zum Einsatz, das nur die Zeilen ausgibt, die das Wort „LDAP" enthalten.

***Abbildung 3.2** Ausführung von netstat*



Wenn ein Leerzeichen im Pfad zu einer .exe-Datei vorkommt, dann kann man die Datei so nicht aufrufen (hier wird nach einem Befehl „T:\data\software\Windows“ gesucht):

```
T:\data\software\Windows Tools\ImageEditor.exe
```

Auch die naheliegende Lösung der Verwendung von Anführungszeichen funktioniert nicht (hier wird die Zeichenkette ausgegeben):

```
"T:\data\software\Windows Tools\ImageEditor.exe"
```

Korrekt ist die Verwendung des kaufmännischen Und (`&`), das dafür sorgt, dass der Inhalt der Zeichenkette als Befehl betrachtet und ausgeführt wird:

```
& "T:\data\software\Windows Tools\ImageEditor.exe"
```

Grundsätzlich könnte es passieren, dass ein interner Befehl der PowerShell (Commandlet, Alias oder Function) genauso heißt wie ein externer Befehl. Die PowerShell warnt in einem solchen Fall nicht vor der Doppeldeutigkeit, sondern die Ausführung erfolgt nach folgender Präferenzliste:

- Aliase
- Funktionen
- Commandlets
- Externe Befehle

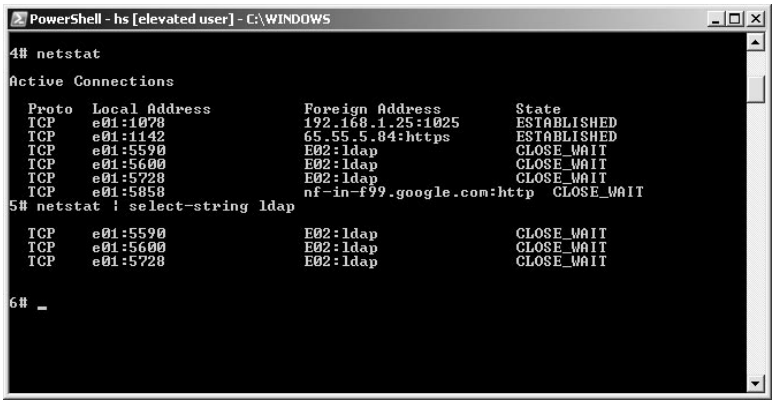


Abbildung 3.3
Ausführung von netstat

3.5 Dateinamen

Beim direkten Aufruf von Datendateien (z.B. `.doc`-Dateien) wird entsprechend den Windows-Einstellungen in der Registrierungsdatenbank die Standardanwendung gestartet und damit das Dokument geladen.

Dateinamen und Ordnerpfade müssen nur in Anführungszeichen (einfache oder doppelte) gesetzt werden, wenn sie Leerzeichen enthalten.

Abbildung 3.4
Anführungszeichen bei Pfadangaben