# Managing Active Directory at the command line **EX-DIRECTORY**

Professionally manage Active Directory users, groups, and other AD objects with Windows PowerShell Version 2.0. **BY ROLF MASUCH** 

he introduction of PowerShell [3] sees Microsoft finally implement long overdue changes to Windows scripting. Unfortunately, Power-Shell Version 1 was no big help for Active Directory (AD) administrators, but then Microsoft added PowerShell support to its "Common Engineering Criteria" (CEC), making it mandatory for all Redmond products to support it. This means Windows Server 2008 R2 and Windows 7 now have PowerShell Version 2 hard-wired.

# Revamped PowerShell for Active Directory

Microsoft developers have enhanced Active Directory support with a PowerShell provider and 76 additional cmdlets (say "commandlets"). The provider lets you change to an AD like changing a drive by typing *cd ad:*. The cmdlets are an additional, optional instruction set that you can use to manipulate individual Active Directory objects.

Although a script-based approach is possibly overkill for occasional work

with individual objects, it becomes essential if you need to handle several dozen or even thousands of objects. The PowerShell is a .Net implementation and thus object oriented throughout; objects can be processed in a structured manner through the use of pipes, removing the need to search text-based output for specific content.

Administrators can manipulate the object properties and methods directly. The introduction of this powerful scripting language is an important milestone for the management of Windows systems, whether clients or servers, and the applications installed on them.

# Requirements

Not every Active Directory will support the use of PowerShell. At least one of the domain controllers (DCs) in the AD has to run Windows Server 2008 R2. For "legacy" systems based on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008, the Active Directory Management Gateway Service [4] is available as a separate download.

After the installation, the Active Directory Web Services (ADWS) run on the

domain controller. To support ADWS, you need to allow TCP port 9389 on the domain controller running the service. If you use a group policy object to configure your firewall, you need to modify your group policies to allow this port for ADWS. The beta versions of the Gateway Service used a different port. Windows PowerShell Version 2 must be installed.

If you have Windows Server 2008 R2 fulfilling the *Active Directory Domain Services* role, the PowerShell module for Active Directory is preinstalled. This module is not installed on any other systems. Instead, the Remote Server Administration Tools (RSAT) module is used [5] [6].

The version for Windows 7 not only installs a full set of tools for GUI-based administration, but also a full set of PowerShell modules. Again, you need PowerShell v2 installed.

The minimum requirement for installing PowerShell is the .NET Framework 2.0. The PowerShell Integrated Scripting Environment (ISE) requires version 3.51 of the frameworks. ISE is the internal editor for PowerShell. All you need now is a user account with the required privileges for the management work you want to perform, and you are up and running.

# Accessing Active Directory

To manipulate user-type objects with PowerShell, you need a connection to your Active Directory and the *ActiveDirectory* PowerShell. Via the Start menu or ISE, launch a PowerShell console. To load the module with the *Import-Module* cmdlet, use:

#### Import-Module ActiveDirectory

Make sure *ActiveDirectory* has no embedded blanks. If your computer is connected to your Active Directory, the system will display a new drive labeled *ad:*. If the connection fails, a warning displays. PowerShell displays warnings in orange and errors in red.

If you want to connect to this drive, or to another domain, see Listing 1. The Get-Credential cmdlet retrieves the credentials used to establish the connection and stores it in the *\$cred* variable. The New-PSDrive cmdlet establishes the connection with the specified parameters. The PSProvider switch specifies the provider on which to establish the drive. The Name switch defines the name used to reference the drive later. The default here is *AD*, but you can change this to suit your own needs. The next two switches *Root* and *Server* define the server you want to connect to and the mountpoint, but more of that later. Finally, the Credential keyword passes in the login information. Without these details, PowerShell uses the data for the currently logged on user.

Because Active Directory is an LDAP directory, PowerShell also supports the functions and requirements of the LDAP protocol. When you establish a connection, it displays all the partitions at the topmost level, root. In the example here, running the *dir* command gives you the output in Listing 2.

To work with the typical tree structure, you can use the *cd* command to change to the domain partition. Alternatively, you can specify the required partition directly with the *Root* parameter. This then is your mountpoint. Before doing this, you might want to change the drive. When you specify the partition name, you must use X.500 notation. The use of canonical names, such as *woodgrove*- *bank.com,* is not currently supported. The command

#### cd ad:

cd "DC=WoodgroveBank, DC=com"

changes to the required partition.

## Working with User Accounts

The *ActiveDirectory* module includes 76 cmdlets for Active Directory. To discover the cmdlet useful for working with user accounts, ask PowerShell for help. The *Get-Command* cmdlet supports a wild-card search and the *Type* parameter to provide a filter function:

get-command \*user\* -type cmdlet | 2
format-table -autosize

This query results in five cmdlets (Listing 3).

With the exception of the *Get-ADUser-ResultantPasswordPolicy* cmdlet, which performs a resulting set of policy (RSOP) query against the password policies for a user, you can use all of these cmdlets for manipulating user objects. For example, the *New-ADUser* cmdlet adds a new user. To change user properties, you would choose *Set-ADUser*. The *New-ADUser* command creates a new user account for Mark Eting in the Marketing organizational unit (Listing 4). The *Name* option passes in the value for a user's *Common-Name* (CN). The display name is specified by the *DisplayName* switch. To manipulate the user object, you need to run the *Get-ADUser* cmdlet and store the object in a variable:

\$User = Get-ADUser MarkEting 2
 -Properties \*

Then you can use the object's individual properties to access the values. For example, *\$User.PasswordExpired* checks to see whether a user's password has expired. User accounts can be deleted either by passing in their unique names or by piping. The *Confirm* option sup-

## Listing 1: Access Active Directory

01 \$cred = Get-Credential

02 New-PSDrive -PSProvider ActiveDirectory -Name AD -Root ""

-Server "nyc-dcl.woodgrovebank.com" -Credential \$cred

Listing 2: AD LDAP Information				
01 Name	ObjectClass	DistinguishedName		
02				
03 WoodgroveBank	domainDNS	DC=WoodgroveBank,DC=com		
04 Configuration	configuration	CN=Configuration,DC=WoodgroveBank,		
05 Schema	dMD	CN=Schema,CN=Configuration,DC=Wood		
06 DomainDnsZones	domainDNS	DC=DomainDnsZones,DC=WoodgroveBank		
07 ForestDnsZones	domainDNS	DC=ForestDnsZones,DC=WoodgroveBank		

Listing 3: Filtering Commands for *user*						
01	CommandType	Name	Definition			
02						
03	Cmdlet	Get-ADUser	Get-ADUser -Filter <string></string>			
04	Cmdlet	Get-ADUserResultantPasswordP	Get-ADUserResultantPasswordP			
05	Cmdlet	New-ADUser	New-ADUser [-Name] <string></string>			
06	Cmdlet	Remove-ADUser	Remove-ADUser [-Identity] <a< td=""></a<>			
07	Cmdlet	Set-ADUser	Set-ADUser [-Identity] <adus< td=""></adus<>			

### Listing 4: Create a New User

01 New-ADUser -Name "Mark Eting" -SamAccountName "MarkEting" -GivenName "Mark"

-Surname "Eting" -DisplayName "Mark Eting"

-Path 'OU=Marketing,OU=NYC,DC=WoodgroveBank,DC=com'

-OtherAttributes @{'msDS-PhoneticDisplayName'="EtingMark"}

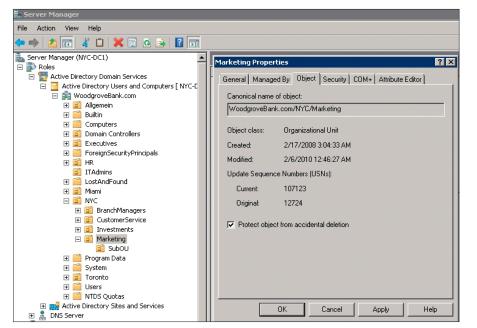
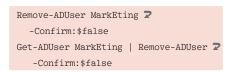


Figure 1: In the MMC user interface, you can disable the delete request.

presses the confirm dialog for the deletion.



# Working with Groups

Just like the cmdlets for manipulating user accounts, it makes sense to discover the cmdlets for working with Active Directory groups. Again the *Get-Command*  is a useful aid, but this time, use the *Module* option to restrict the search to cmdlets from this module. The results are more extensive than for user accounts (Listing 5).

The following command lists the members of the *NYC\_MarketingGG* group by their *CommonName*:

Get-ADGroupMember -Identity NYC\_2
MarketingGG | %{\$\_.Name}

The *New-ADGroup* cmdlet is used to create a new group. Don't forget to specify

Ele Edit View	<u>Go D</u> ebug <u>O</u> pti	ons <u>T</u> ools <u>H</u> elp				
) 🎯 🔲 🖉 🔿 1		글 일 [의, 의, ] 🕨 🥶 📲 🔳 🖪 😰 [전	nput script parameters here>	0		
Doord Investigant	. 면 profile.ps1 원					
76	[string] \$He					
77	[System.Man	agement.Automation.Host.FieldDesc	<pre>ciption[]] \$FieldDe:</pre>	scription		
78 🖂 🔰 🗎						
79						
		e = 'System.Collections.ObjectMod	el.Collection'l'			
		[Type] \$genericTypeName				
	closedType = \$	genericType.MakeGenericType([Type	'System.Management	t.Automation.Hos	t.FieldDescription'	)
83						
	descriptions =	[Activator]::CreateInstance(\$clo	sedType, \$false)			
85						
86 白 \$		on   ForEach-Object {				
87	<pre>&gt;descriptio</pre>	ns. Ad Synopsis: Performs an operation against each of a set of	to a share a			
		Definition				
90 \$	have and Descent	(\$Cap ForEach-Object Process <scriptblock[]> [Begin</scriptblock[]>	<scriptblock>] [InputObject</scriptblock>	<psobject>][End <script< td=""><td>Block&gt;][CommonParameters]</td><td></td></script<></psobject>	Block>][CommonParameters]	
	nosc.ul.Prompt	(ycap)				
91 - }						
92	ten Deed Greede					
92 93 funct	ion Read-Crede				-d-opiolo io pho di	-14
92 93 funct 94 ⊟ \$	result = Read-	Input 'Enter your credentials' 'P		uthentication cr	edentials in the fi	elds provided.
92 93 funct 94 ⊟ \$ 95 ⊨ 1:	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and %result['Password']	- {		edentials in the fi	elds provided.
92 93 funct 94 - \$ 95 - 1: 96	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P	- {		edentials in the fi	elds provided.
92 93 funct 94 = \$ 95 - 1: 96	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and %result['Password']	( -Password \$result		edentials in the fi	elds provided.
92 93 funct 94 = \$ 95 = 1: 96	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and %result['Password'] ial -Username %result['Username']	) ( -Password \$result Output	['Password']		elds provided. •
92 93 funct 94 5 95 1 96 4 4	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and %result['Password'] ial -Username %result['Username'] What is your name?	-Password \$result Output LCID	['Password'] Name	edentials in the fi DisplayName	elds provided.
92 93 funct 94 = \$: 95 i i: 95 i i: 96 i ≮I €Caption \$Message	result = Read- f (\$result['Us	Input 'Enter your oredentials' 'P ername'] -and %result['Password'] ial -Username %result['Username'] What is your name? Please enter your name in the fields provide	Output	['Password'] Name	DisplayName	
92 93 funct 94 \$ 95 1 96 1 * * * * * * * * * * *	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and &result['Password'] ial -Username &result['Username'] What is your name? Please enter your name in the fields provide System.Collections.DbjectModel.Collection	-Password \$result Dupput LCTD 1033	['Password'] Name		
92 93 funct 94 S 95 iii 96 iiii 96 iiiiiiiiiiiiiiiiiiiiiiii	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and %result['Password'] ial -Username %result['Username'] What is your name? Please enter your name in the fields provide System_Collections. DbjectModel.Collection System_Collections.DbjectModel.Collection	Cuput Output LCID  1033	['Password'] Name	DisplayName	
92 94 = \$ 95 = \$ 95 = \$ 96 = \$ 96 = \$ \$Caption \$Message \$genericTypeName \$genericType	result = Read- f (\$result['Us	Input 'Encer your credentials' 'P ername'] -and Gresult('Password') ial -Osername Gresult('Username') What is your name? Please enter your name in the fields provide System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection	d -Password %result Output LCID LCID 1033	['Password'] Name  en-US	DisplayName  English (United :	
92 93 funct 94 8: 95 1 1: 96 1 96 1 96 1 96 1 96 1 96 1 96 1 96 1	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and Sresult('Desruca') ial -Username &result('Username') What is your name? Please enter your name in the fields provide System.Collections.DbjectModel Collection System.Collections.DbjectModel Collection System.Collections.DbjectModel Collection System.Collections.DbjectModel Collection	d -Password %result Output LCID LCID 1033	('Password') Name en-US E c:\WINDOWS\spsjps	DisplayName  English (United : m.log	
92 93 funct 94 \$ 95 1 96 \$ 96 \$ Scaption \$ SenericTypeName \$ genericType	result = Read- f (\$result['Us	Input 'Encer your credentials' 'P ername'] -and Gresult('Password') ial -Osername Gresult('Username') What is your name? Please enter your name in the fields provide System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection	Output LCID 1033 First name: ''	['Password'] Name en-US D c:\WINDOWS\spslpar C:\WINDOWS\spslpards	DisplayName  English (United : m.log	
92 93 funct 94 ⊕ 8; 95 ⊕ 3; 96 ⊨ 1 96 ⊨ 1 96 ⊨ 1 \$2apton \$Message \$genericTypeName \$closedType \$closedType \$closedType \$host B Name	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and %result('Password') ial -Username %result('Username') What is your name? Please enter your name in the fields provide System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection System.Collections.DbjectModel.Collection System.Management.Automation.Internal.HC PowerGUIScriptEdioHold	Corput CCID  lo33 First name: '' Initial: ''	('Password'] Name en-US C:\WINDOWS\spake C:\WINDOWS\spake c:\WINDOWS\spake	DisplayName  English (United : m.log	
92 funct 94 € 3; 95 1 1; 96 1 96 1 96 1 96 1 96 1 96 1 96 1 96 1	result = Read- f (\$result['Us	Input 'Inter your credentials' 'P ername'] -and Sresult('Desruca') ial -Username %result('Username') What is your name? Please enter your name in the fields provide System Collections. DbjectModel Collection' System Management.Automation.Internal.Ho PowerGUISciptEdioHott	Cuput Cuput LCID LCID 1033 First name: '' Tour favorite fo First name: ''	('Password') Name en-US E c:{WINDOWS}spats E c:{WINDOWS}spats C:{WINDOWS}schas c:{WINDOWS}sh	DisplayName  English (United : m.log & xc.log &	
92 93 funct 94 8; 95 1 1; 95 1 1; 95 1 1; 95 1 1; 95 2; 11 2; 95 2; 12 2	result = Read- f (\$result['Us	Input 'Enter your credentials' 'P ername'] -and iresult('Bassword') ial -Username iresult('Username') What is your name? Please enter your name in the fields provide System. Calections. DhjectModel. Collection System. Calections. DhjectModel. Collection System. Calections. DhjectModel. Collection System. Calections. DhjectModel. Collection System. Management. Automation. Internal. HC PowerGUIScredEdioHot 1.51.4%	Couper Co	('Password'] Name en-US C:\WINDOWS\spskps C	DisplayName English (United : m.log sv.log st	
92 funct 94 ⊡ \$: 95 funct 95 funct 96 funct 96 funct 96 funct \$Capion \$Message \$Message \$Message \$Message \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Advertige \$Ad	result = Read- f (\$result['Us	Input 'Inter your credentials' 'P ername'] -and Sresult('Desavocd') ial -Username %result('Username') What is your name? Please enter your name in the fields provide System Collections. DbjectModel Collection' System Management.Automation.internal.Ho PowerGUISciptEdRoHot	<pre>{     Password fresult     Output     LCID     LCID     Total     First name: ''     Thitial: ''     Last name: ''     Thitial: ''     Last name: ''     Thitial: ''     Last name: '' </pre>	('Password'] Name en-US C:\WINDOWS\spstpsr C:\WINDO	DisplayName English (United : m.log 2 xv.log st k	
92     93	result = Read- f (\$result['Us	Input: 'Enter your credentials' 'P ername'] -and iresult('Dessword') ial -Username iresult('Username') What is your name? Please enter your name in the fields provide System. Collections. DhjechModel Collection System. Collections. DhjechModel Collection System. Collections. DhjechModel Collection System. Management. Automation. Internal. Hc ProverGUIScript Giothout 1.51.4% er31e65326347db+355c0740Jsed271 System. Management. Automation. Internal. Hc ProverGUIScript Giothout Carnot piccess argument because the value of age.	Coput LCID LCID Initial: '' Last name: '' first name: '' four favorite fo ap First name: '' Last name: '' Last name: '' Last name: '' Last name: '' Last name: ''	('Password'] Name en-US C:\WINDOWS\spake C:\WINDOWS	DisplayName English (United : m.log sv.log st t	
92 93 €unct 94 € 3; 95 6 1; 96 8; 96 9; 96 9	result = Read- f (\$result['Us	Input 'Inter your credentials' 'P ername']	Coput LCID LCID Initial: '' Last name: '' first name: '' four favorite fo ap First name: '' Last name: '' Last name: '' Last name: '' Last name: '' Last name: ''	('Password'] Name en-US C(WINDOWS/souppe	DisplayName English (United : m.log sv.log st t	
92 tunct 94 ≣ tunct 94 ≣ \$; 95 ∐ 1; 96 ∐ 1; 96 ∐ \$Caption \$Message \$GenericType \$closedType \$host 9 Name 9 Version 10 Instanceld 10 LurentUl/Lutar PrivateDat 2 GurentUl/Lutar 10 SteletCharge	result = Read- f (\$result['Us	Input: 'Enter your credentials' 'P ername'] -and iresult('Dessword') ial -Username iresult('Username') What is your name? Please enter your name in the fields provide System. Collections. DipectModel Collection System. Collections. DipectModel Collection System. Collections. DipectModel Collection System. Collections. DipectModel Collection System. Management. Automation. Internal. He ProverGUIScript dioHold 1.51.4% errUS control process argument because the value of args. System. Management. Automation. Host. Field	Coput LCID LCID Initial: '' Last name: '' first name: '' four favorite fo ap First name: '' Last name: '' Last name: '' Last name: '' Last name: '' Last name: ''	('Password'] Name en-US C:\WINDOWS\spake C:\WINDOWS	DisplayName English (United : m.log sv.log st t	
92 93 ±unct 94 ± \$; 95 95 10 \$000 \$000 \$000 \$000 \$000 \$000 \$000	result = Read- f (\$result['Us	Input: 'Enter your credentials' 'P ername'] -and iresult('Dessword') ial -Username iresult('Username') What is your name? Please enter your name in the fields provide System. Collections. DhjechModel Collection System. Collections. DhjechModel Collection System. Collections. DhjechModel Collection System. Management. Automation. Internal. Hc ProverGUIScript Giothout 1.51.4% er31e65326347db+355c0740Jsed271 System. Management. Automation. Internal. Hc ProverGUIScript Giothout Carnot piccess argument because the value of age.	<pre>{     Password fresult     Output     LCID      Io33     First name: ''     Initial: ''     Lest name: ''     Your favorite fo     Pirst name: ''     Your favorite fo </pre>	' Password']           Name              en-US           C (WNDOWStapping	DisplayName English (United : m.log sv.log st t	

Figure 2: PowerGUI is one of the free editors with built-in PowerShell support.

the *-GroupType*, or you will be confronted with a dialog without options. The supported values for this option are *Global*, *Universal*, and *DomainLocal*.

New-ADGroup -GroupScope DomainLocal **2** -Name NYC\_all

Adding new members to existing groups is also really easy. Just grab the required user account with the *Get-ADUser* cmdlet and then pipe it to the *Add-ADGroup-Member* cmdlet.

Get-ADUser MarkEting | 2
%{Add-ADGroupMember 2
NYC\_MarketingGG \$\_}

It is simpler to specify the username directly in the call to the cmdlet:

Add-ADGroupMember NYC\_MarketingGG **2** MarkEting

The command for removing users from groups is just as simple:

Remove-ADGroupMember NYC\_MarketingGG **2** MarkEting -confirm:\$false

As with deleting a user, *Confirm* suppresses the confirmation dialog.

# **Managing Other Objects**

Active Directory gives you many other object types besides users and groups; for example Computers, Organizational Units (OUs), Group Policies, and so on. To find the right cmdlets for these ob-

## Listing 5: Commands for \*group\*

01 Get-Command \*group\* -Module
 ActiveDirectory
02
03 Name

04 ----

- Add ADC
- 05 Add-ADGroupMember
- 06 Add-ADPrincipalGroupMembership
- 07 Get-ADAccountAuthorizationGroup
- 08 Get-ADGroup
- 09 Get-ADGroupMember
- 10 Get-ADPrincipalGroupMembership
- 11 New-ADGroup
- 12 Remove-ADGroup
- 13 Remove-ADGroupMember
- 14 Remove-ADPrincipalGroupMembership
- 15 Set-ADGroup

**THE AUTHOR** 

Rolf Masuch works as a product manager with ABSC GmbH. He has been a Microsoft Certified Systems Engineer for Windows Server 2003, Messaging Specialist, and Microsoft Certified Trainer since 1996. He is also a Microsoft Certified IT Professional for Enterprise Desktop Administrator Windows 7 and Enterprise Administrator Windows Server 2008. As the founder of the German-language PowerShell user group D/A/CH, Rolf is in a perfect position to plumb the depths of the

jects, you again need the *Get-Command* cmdlet with the appropriate wildcards. The search keys here are \*Computer\*, \*Org\*, \*Policy\*, or even \*Server\*. If you don't find a cmdlet for your task, you can use the generic cmdlets for objects. Note that these cmdlets might not have such a rich selection of options as the cmdlets optimized for special object types. The search key for the generic cmdlets is \*Object\*, of course.

command-line tool.

This search also returns the *Re-store-ADObject* cmdlet, which restores accidentally deleted objects. With the *Get-ADObject* cmdlet and its *IncludeDe-letedObjects* option, you can identify deleted objects and pipe them to *Re-store-ADObject*, which restores the objects.

Organizational units have four cmdlets. To create an OU, use the New-ADOrganizationalUnit cmdlet with the name of the new OU. Remove-ADOrganizationaUnit lets you delete an OU. Watch out for the Active Directory version. If you use Windows Server 2008, the new OU will automatically be flagged Protect ob*ject from accidental deletion*. To enable this feature, you might need to go to the MMC GUI in Active Directory Users and Computers in the View menu's Advanced Features item. After doing so, you can click the *Object* tab and remove the flag (Figure 1). Until you have entered the following, you will not be able to delete:

Remove-ADOrganizationalUnit **2** -Identity 'OU=Marketing,OU=NYC,**2** DC=WoodgroveBank,DC=com'

Unfortunately, you can't use the *Confirm* switch here.

## Summary

PowerShell Version 2 and the *ActiveDi*rectory module finally bring Active Directory management to the command line. PowerShell's strict object orientation makes it possible to manipulate elements in the Active Directory directly and to use all the methods and properties of the objects in question. Whereas other languages such as VBS previously

<b>.</b>	er maiscript - Choocuments and settings winningtrator wy bocuments istripts caustackdemo.ps i
<u>File Edit View Project Build Script De</u>	bug <u>T</u> ools <u>W</u> indow <u>H</u> elp
i 🗅 - 🚅 - 🔜 🥔 🕤 🖾 💁 🔋 i X	. 🐚 🖎 🔊 🝽 (漆) (御) 🔚 🚍 😩 (物) 👔 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘
i ab 🔡 🔩 🗉 🖃 🚹 😑 🗖 🕹 🕨	■
Tools Browser 🌐 🔍	Start page ActiveXposh.vbs Calistackdemo.ps1 ×
Admin Tools	1 #
	2 #
	3 # Microsoft PowerShell Source File Created with SAPIEN Technologies PrimalScrip 4 #
.NET Configuration 1.1	5 # NAME:
	6 #
Certificates	7 # AUTHOR: Alex , SAFIEN Technologies, Inc.
	8 # DATE : 6/20/2008
	10 # COMMENT:
Computer Management	11 #
	12 #
Device Manager	14 pfunction write-something({argument)
<b>1</b>	15 (
Disk defragmenter	16 Write-Host \$argument
2012	17 L) 18
	19 Function do-something(\$action)
Disk Management	20 (
ļ	21 if(%action -eq 1) 22 (
Event Viewer	22 muite compthing/IDaing and thing!)
Ťa –	
Group Policy	Command Window
<b>N</b>	Windows PowerShell Copyright (C) 2006 Microsoft Corporation. All rights reserved.
<b>2</b>	PS C:\projects\AEWIN> get-process pr*
.NET Tools	Handles NPM(K) PM(K) WS(K) VM(M) CPU(s) Id ProcessName
Admin Tools	724 21 40340 53564 511 35.39 3940 PrimalScript 31 2 496 1976 18 0.02 2788 ProtectionProcessorCleanup.0001
Flash Tools	
General	PS C:\projects\AEWIN>
SAPIEN Tools	
Script Tools	
-	
🖄 Sampl 🛅 File Br 🔀 Tools 📧 Object	Query Output Debug Help Command Window
i @ 🖉 🖳 I 🔍 🗈 👷 🗿 🌑 🗷 🗃 🏠	·

Figure 3: PrimalScript is a commercial editor with built-in PowerShell support.

had to address each individual object separately before manipulating it, a simple *dir* for a user OU in PowerShell will output all the user objects in the OU so that you can pipe them for ongoing processing. The integrated ISE editor is a useful tool to display scripts, your input, and the resulting output.

The RSAT tool lets you perform all of these tasks from a Windows-based client system, in which you can set up your personal scripting environment. This could include more powerful editors such as the free PowerGUI by Quest (Figure 2) [7] or the commercial PowerShell Plus variant by Idera [8] or PrimalScript by Sapien (Figure 3) [9]. At the end of the day, PowerShell helps administrators, especially in larger Active Directory environments with large numbers of objects, manage their Active Directory with less clicking, and the results are documented up front and more easily reproducible thanks to scripting.

### INFO

- [1] PowerShell community: http://powershellcommunity.org/
- [2] PowerShell user group: http://www.powershell-ag.de/ps
- [3] Download PowerShell version 2.0: http://support.microsoft.com/kb/ 968930
- [4] Active Directory Management Gateway Service (Active Directory Web Service for Windows Server 2003 and Windows Server 2008): http:// www.microsoft.com/downloads/ details.aspx?displaylang=en& FamilyID=008940c6-0296-4597-be3e-1d24c1cf0dda
- [5] Remote Server Administration Tools for Windows 7: http://www. microsoft.com/downloads/details. aspx?familyid=7D2F6AD7-656B-431 3-A005-4E344E43997D& displaylang=en
- [6] Description of Remote Server Administration Tools for Windows 7: http://support.microsoft.com/kb/ 958830/en-us
- [7] PowerGUI: http://powergui.org/ downloads.jspa
- [8] PowerShell Plus: http://powershellplus.com/
- [9] PrimalScript: http://www.primaltools.com/ products/info.asp?p=PrimalScript