

Uwaga: By móc połączyć się ze zdalnym serwerem za pomocą PS'a musi być spełniony szereg czynników (odpowiednie uprawnienia, możliwość zmiany GPO etc.)

```
winrm quickconfig
```

```
cd wsman::localhost\client
```

To {wsman} jest „Provider”, o tym później

```
Set-Item TrustedHosts localhost
```

```
Restart-Service WinRm
```

```
Enable-PSRemoting
```

```
Enter-PSSession localhost
```

Prawdopodobnie się nie udało ;-(dlatego przedstawię slajd z MVA

Enable Remoting

PS WSMAN:\localhost>

```

Administrator: Windows PowerShell
PS C:\> Enable-PSRemoting

WinRM quick configuration
Running command "Set-WSManQuickConfig"
management through winRM service.
This includes:
  1. Starting or restarting (if already stopped) the WinRM service
  2. Setting the winRM service type to Remote
  3. Creating a listener to accept requests
  4. Enabling firewall exception for WinRM

Do you want to continue?
[Y] Yes [A] Yes to All [N] No [L] No to All (default is "Y"):y
    
```

The screenshot shows the Group Policy Management Editor window. The left pane displays a tree view of policies, with 'WinRM Service' selected under 'Windows Remote Management (WinRM)'. A red arrow points from the PowerShell console to this selection. The right pane shows a list of settings for 'WinRM Service', all of which are currently 'Not configured'.

Setting	State
Allow automatic configuration of listeners	Not confi...
Allow Basic authentication	Not confi...
Allow CredSSP authentication	Not confi...
Allow unencrypted traffic	Not confi...
Specify channel binding token hardening I...	Not confi...
Disallow Kerberos authentication	Not confi...
Disallow Negotiate authentication	Not confi...
Turn On Compatibility HTTP Listener	Not confi...
Turn On Compatibility HTTPS Listener	Not confi...

PowerShell Remoting is already enabled in Server 2012

Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management

Źródło: MVA

```

Administrator: Windows PowerShell
PS C:\> Enter-PSSession Server2.acme.local
[server2.acme.local]: PS C:\Users\administrator.ACME\Documents> cd\
[server2.acme.local]: PS C:\> Get-Service

Status      Name                               DisplayName
-----
Running     AeLookupSvc                       Application Experience
Stopped     AppMgmt                            Application Management
Running     BFE                                Base Filtering Engine
Running     BITS                               Background Intelligent Transfer Ser...
Stopped     Browser                            Computer Browser
Running     CertPropSvc                       Certificate Propagation
Stopped     clr_optimizatio...                Microsoft .NET Framework NGEN v2.0....
Stopped     COMSysApp                         COM+ System Application
Running     CryptSvc                          Cryptographic Services
Running     DcomLaunch                        DCOM Server Process Launcher
Stopped     defragsvc                         Disk Defragmenter
Running     Dhcp                               DHCP Client
Running     Dnscache                          DNS Client
Running     DPS                                Diagnostic Policy Service
Stopped     EFS                               Encrypting File System (EFS)
Running     eventlog                          Windows Event Log
    
```

Źródło: MVA

```
Administrator: Windows PowerShell
PS C:\>
PS C:\> Invoke-Command -ComputerName server1, server2, win7 -scriptBlock {
>> Get-EventLog -LogName Security -Newest 2 } |
>> Format-Table PsComputerName, EntryType, Source
>>
```

PsComputerName	EntryType	Source
server1	SuccessAudit	Microsoft-windows-Secu...
server1	SuccessAudit	Microsoft-windows-Secu...
server2	SuccessAudit	Microsoft-windows-Secu...
server2	SuccessAudit	Microsoft-windows-Secu...
win7	SuccessAudit	Microsoft-windows-Secu...
win7	SuccessAudit	Microsoft-windows-Secu...

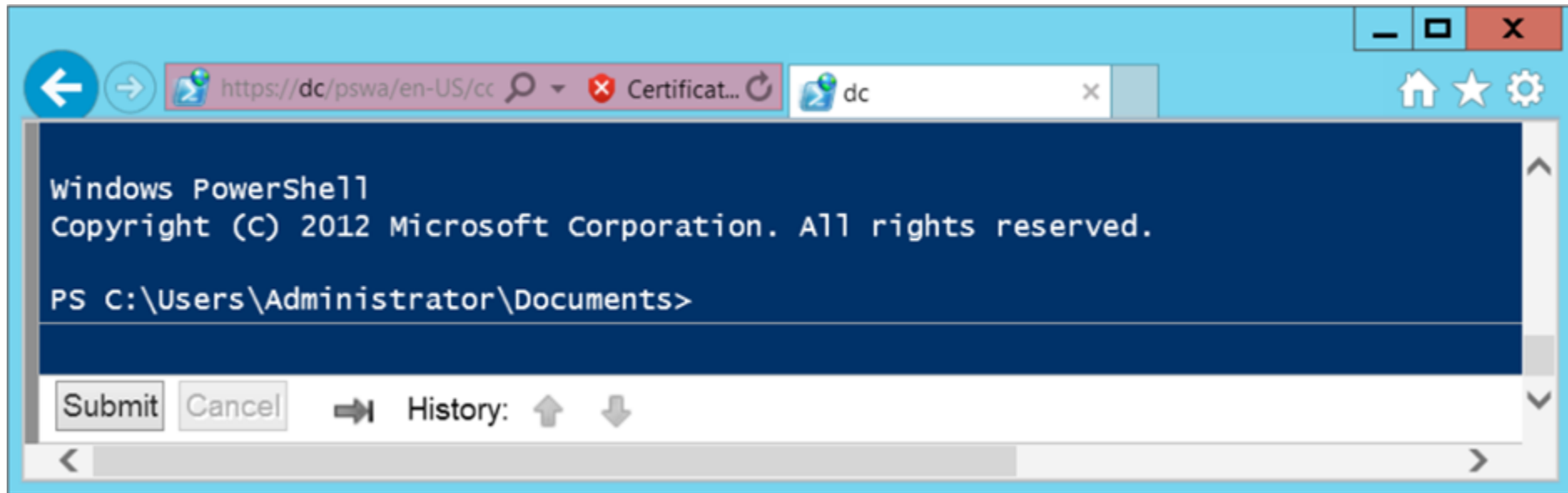
```
Administrator: Windows PowerShell
PS C:\>
PS C:\> Invoke-Command -UseSSL -Port 443 -ThrottleLimit 64 -ScriptBlock{
>> Get-Service} -ComputerName server1, server2 -credential (Get-credential)
>>
```

Istnieją jeszcze inne sposoby na zarządzanie zdalne za pośrednictwem PS'a:

- Przez Web, po zainstalowaniu WindowsPowerShellWebAccess i do konfigurowaniu serwera IIS, przygotowaniu odpowiedniego PKI (Wicie co to jest PKI :

https://pl.wikipedia.org/wiki/Infrastruktura_klucza_publicznego?)

można zarządzać maszyną poprzez stronę WWW:



- I co najfajniejsze za pośrednictwem DSC (Desired State Configuration). Jest to platforma do zarządzania, dużych środowisk Windowsowych. Umożliwia dwa tryby pracy „push” i „pull”. Jej zadaniem jest jak sama nazwa wskazuje osiągnięcia pożądanego stanu konfiguracji. Umożliwia scenariusze np.: po wpięciu nowego czystego serwera do „konfiguracji” na serwerze zostanie zainstalowany i skonfigurowany IIS, oraz zostanie przeprowadzona instalacja aplikacji. A wszystkimi zmianami można sterować centralnie ;-)

Uwaga! Ponieważ za pomocą PS można naprawdę dużo zrobić, dlatego Execution Policy powinno być ustawione na AllSigned lub RemoteSigned.

Dlatego polecałem na drugich zajęciach:

<https://blogs.technet.microsoft.com/heyscriptingguy/2010/06/17/hey-scripting-guy-how-can-i-sign-windows-powershell-scripts-with-an-enterprise-windows-pki-part-2-of-2/>

Ktoś przeczytał?

Set-ExecutionPolicy -ExecutionPolicy AllSigned

Robimy skrypt:

```
$yourName=Read-Host "What is your name?"  
Write-Host "Hello $yourName"
```

Zapisujemy gdzieś jako 3.ps1, i próbujemy odpalić: .\3.ps1

Ja uzyskałem:

```
.\3.ps1 : File D:\ps\zsl\3.ps1 cannot be loaded. The file  
D:\ps\zsl\3.ps1 is not digitally signed. You cannot run this script on  
the current system.
```


Ok coś o kluczu, że nie jest digitallyly signed... Dobra ale najpierw:

get-psdrive

Mamy :

Cert

Certificate \

Psdrive to jest provider, mamy tam zarówno dyski tradycyjne C:\ D:\ etc. jak i WSMAN i HKLM HKCU (dostęp do rejestru).

[https://msdn.microsoft.com/en-us/library/ee126186\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ee126186(v=vs.85).aspx)

A Windows PowerShell provider allows any data store to be exposed like a file system as if it were a mounted drive. For example, the built-in Registry provider allows you to navigate the registry like you would navigate the c drive of your computer.

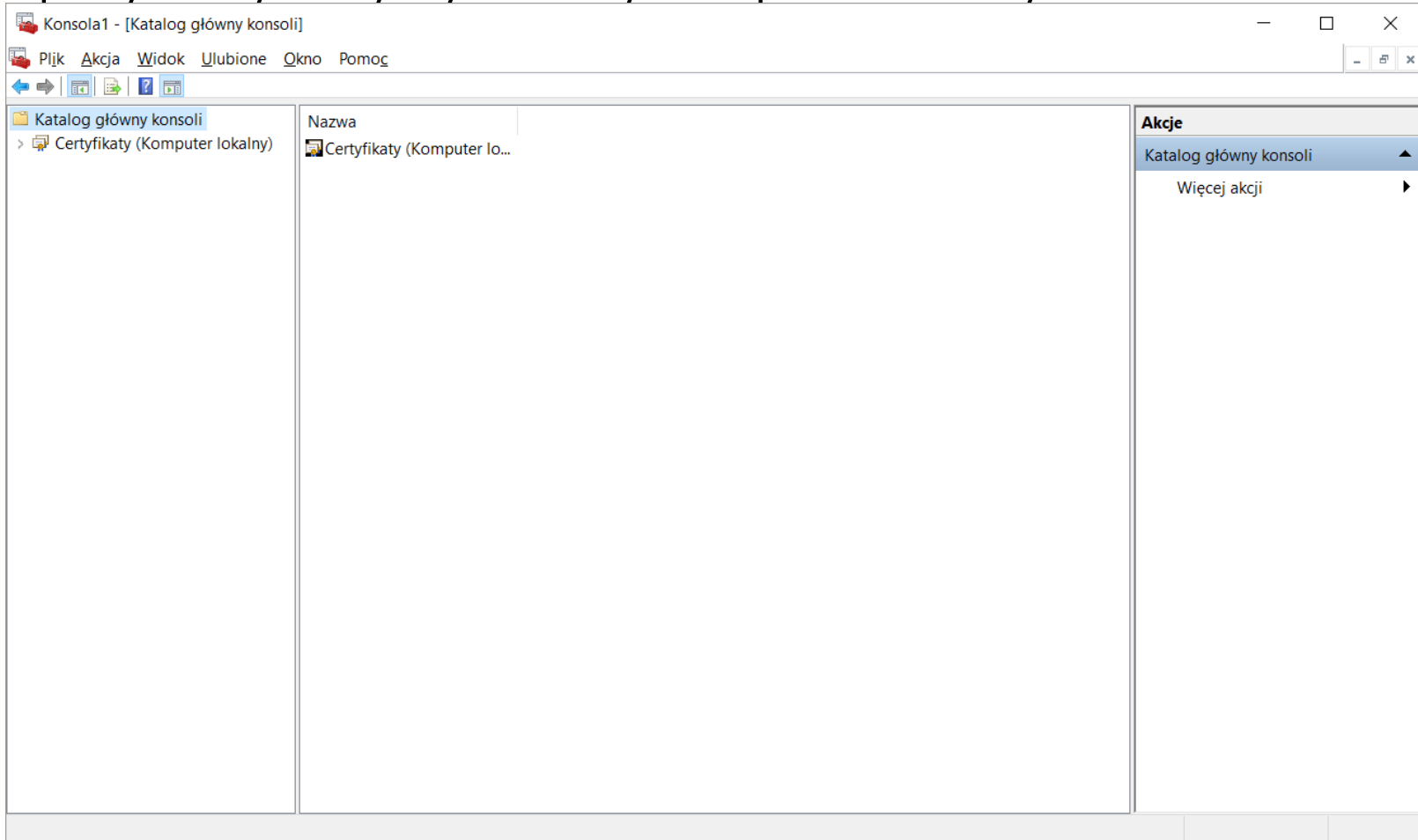
Czyli rozumiemy już polecenie:

```
dir cert:\LocalMachine\my\ -Recurse -CodeSigningCert
```

```
$cert = New-SelfSignedCertificate -DnsName test.aplitt.com -Type  
CodeSigning -CertStoreLocation Cert:\LocalMachine\My
```

```
Set-AuthenticodeSignature -FilePath D:\ps\zsl\3.ps1 -Certificate $cert
```

Prawdopodobnie trzeba będzie dodać nasz nowy certyfikat do zaufanych dostawców mmc.exe, pod plik-> dodaj usuń przystawkę dodajemy Certyfikaty wybieramy Komputer lokalny



W Certyfikaty (komputer lokalny) -> Osobisty -> Certyfikaty znajdujemy swój certyfikat i kopiujemy go do Zaufane główne urzędy certyfikacji:

