



---

---

---

---

---

---

---

### What is a PowerShell Provider?

Software that translates data storage into a PowerShell-friendly format

Typically hierarchical data structures

- FileSystem
- Registry
- Certificate store
- Active Directory

TRAINSIGNAL

---

---

---

---

---

---

---

### What is a PowerShell Provider?

But also configuration sources

- WSMAN
- IIS
- Environment

Additional providers may be added via modules

Run Get-PSProvider to view installed providers

Read help topic about\_providers

TRAINSIGNAL

---

---

---

---

---

---

---

## Using Providers

### Common providers

- FileSystem
- Registry
- Certificate
- WSMAN

Data storage exposed as a PSDrive

Provider translates cmdlet actions to the "drive"

Providers may expose dynamic parameters

Providers may expose dynamic help examples

TRAINSIGNAL

---

---

---

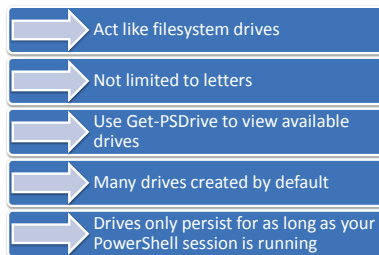
---

---

---

---

## PSDrives



```
PS C:\> Get-PSDrive
```

TRAINSIGNAL

---

---

---

---

---

---

---

## Creating a PSDrive

### Use New-PSDrive

- Specify drive name
- Specify provider
- Specify path
- Options: credential, persistence

The drive name does not include the colon

Drives are scope specific

Drives not necessarily seen by Windows

Add drive settings to your PowerShell profile script

```
PS C:\> New-PSDrive IT FileSystem \\chi-fp01\IT
```

TRAINSIGNAL

---

---

---

---

---

---

---

## Navigating PSDrives

- Use the colon when accessing a drive
- Use same set of cmdlets
- Some providers require ItemProperty cmdlets
- Some PSDrives require elevated privileges

TRAINSIGNAL

---

---

---

---

---

---

---

## FileSystem

- ▶ Use traditional file system commands
- ▶ PowerShell should detect mapped Windows drives
- ▶ Create persistent drives
- ▶ External drives automatically mapped
- ▶ **Tip:** Create your own shortcut drives

TRAINSIGNAL

---

---

---

---

---

---

---

## FileSystem

```
PS C:\scripts> dir B:\.xml

Directory: C:\scripts

Mode                LastWriteTime         Length Name
----                -
d-----          11/18/2010   2:54 PM           55086 bestpractices.xml
d-----          9/19/2012    6:08 PM           1158 Books.xml

PS C:\scripts> cd \work
PS C:\work> dir -directory

Directory: C:\work

Mode                LastWriteTime         Length Name
----                -
d-----          10/20/2012   9:35 AM             atomic
d-----          10/17/2012   2:03 PM             foody
d-----          12/20/2012  10:10 AM             images
d-----          12/20/2012  10:08 AM          resources
d-----          10/20/2012   9:27 AM             shell
d-----          1/23/2013   4:27 PM             test
d-----          2/21/2013   8:32 AM          Test sig 2
d-----          1/23/2013   4:27 PM             test2
d-----          7/15/2013   9:53 PM          Ubuntu12
d-----          12/20/2012   9:57 AM          widgets
d-----          12/20/2012  10:16 AM          _derived

PS C:\work>
```

TRAINSIGNAL

---

---

---

---

---

---

---

## Registry

Only works locally

Default drives to HKLM and HKCU

Technically no filtering...but there are ways

Some information stored as an Item property

TRAINSIGNAL

---

---

---

---

---

---

---

## Registry

```
PS C:\> get-psdrive -PSProvider registry

Name      Used (GB)  Free (GB) Provider      Root
-----
HKCU      0.0000000  0.0000000 Registry      HKEY_CURRENT_USER
HKLM      0.0000000  0.0000000 Registry      HKEY_LOCAL_MACHINE

PS C:\> cd HkLM:
PS HkLM:\> cd .\SYSTEM\CurrentControlSet\Services\Browser
PS HkLM:\SYSTEM\CurrentControlSet\Services\Browser> dir

Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser

Name      Property
-----
Parameters ServiceDllUnloadOnStop : 1
              MaintainServerList : Auto
              ServiceDll : C:\Windows\System32\browser.dll

TriggerInfo

PS HkLM:\SYSTEM\CurrentControlSet\Services\Browser> get-ItemProperty .

Name      Property
-----
Start      : 3
DisplayName : @systemroot\system32\browser.dll,-100
ErrorControl : 1
Group      : NetworkProvider
ImagePath  : C:\Windows\System32\svchost.exe -k netsvcs
Type       : 32
Description : @systemroot\system32\browser.dll,-101
DependsOnService : (LanmanWorkstation, LanmanServer)
ObjectName : LocalSystem
Permissions : (132, 3, 0, 0...)
PSPath      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM
```

TRAINSIGNAL

---

---

---

---

---

---

---

## Certificate

Access certificate store for local user and computer

Hierarchical storage of certificate objects

Certificates as "files"

Objects can be deleted

TRAINSIGNAL

---

---

---

---

---

---

---

## Certificate

```
PS C:\> cd cert:
PS Cert:\> dir

Location      : CurrentUser
StoreNames    : {SmartCardRoot, Root, Trust, AuthRoot...}

Location      : LocalMachine
StoreNames    : {TrustedPublisher, ClientAuthIssuer, Remote Desktop, Root...}

PS Cert:\> cd .\CurrentUser\My
PS Cert:\CurrentUser\My> dir

Directory: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                Subject
-----
BC28F8FE2B3F36A0B081AD5097D05A70366F3B91  CN=jeff

PS Cert:\CurrentUser\My> dir | del -whatif
What If: Performing operation "Remove certificate" on Target "Item: CurrentUser\My\BC28F8FE2B3F36A0B081AD5097D05A70366F3B91".
PS Cert:\CurrentUser\My>
```

TRAINSIGNAL

## Environment

Access environmental variables

Use for read-only references

Access common settings as variables:

\$env:computername

\$env:userdomain

\$env:username

\$env:temp

TRAINSIGNAL

## Environment

```
PS C:\>
PS C:\> dir env:

Name                Value
----
ALLUSERSPROFILE      C:\ProgramData
APPDATA              C:\Users\jeff\AppData\Roaming
CLASSPATH            C:\Program Files (x86)\Java\jre7\lib\ext\QT...
CommonProgramFiles   C:\Program Files (x86)\Common Files
CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
CommonPrograms64     C:\Program Files\Common Files
COMPUTERNAME         SERENITY
ComSpec              C:\Windows\system32\cmd.exe
DevicePath           C:\
FP_NO_HOST_CHECK     NO
HOMEDRIVE            C:
HOMEPATH             \Users\jeff
JAVA_HOME            C:\Program Files (x86)\Java\jre7
LOCALAPPDATA         C:\Users\jeff\AppData\Local
LOGONSERVER          \\SERENITY
NUMBER_OF_PROCESSORS 8
OS                  Windows_NT
Path                C:\Program Files (x86)\VMware\VMware vSphere ...
PATHEXT              .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;...
PROCESSOR_ARCHITECTURE AMD64
PROCESSOR_IDENTIFIER Intel64 Family 6 Model 30 Stepping 5, Genuine...
PROCESSOR_LEVEL      6
PROCESSOR_REVISION   1a05
ProgramData          C:\ProgramData
ProgramFiles          C:\Program Files
ProgramFiles(x86)     C:\Program Files (x86)
Programs64           C:\Program Files
ModulePath            C:\Users\jeff\Documents\WindowsPowerShell\Mod...
```

TRAINSIGNAL

## Removing a PSDrive

- ☐ User defined drives end with session
- ☐ Use Remove-PSDrive to manually removal
- ☐ Can't remove Windows or fixed drives
- ☐ Don't try to remove your current drive
- ☐ Remove persistent drive mappings

```
PS C:\> Remove-PSDrive X
```

TRAINSIGNAL

---

---

---

---

---

---

---

## PowerShell Provider Demos

---

---

---

---

---

---

---

## Provider Sources

Additional providers may be added from modules, server features, or third party tools

- Active Directory
- IIS
- SQL Server
- PowerShell Community Extensions
- VMware PowerCLI



TRAINSIGNAL

---

---

---

---

---

---

---

**Lab**

1. Create a new PSDrive called TEMP that is mapped to the %TEMP% environmental variable
2. Change to the new drive and recursively list all files and folders
3. Using the registry find the value for ProductName under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

**TRAINSIGNAL**

---

---

---

---

---

---

---