Intro to Powershell

New IT Pros User Group

Sunny Chakraborty
@sunnyc7

- Please interrupt.
- Please ask questions.

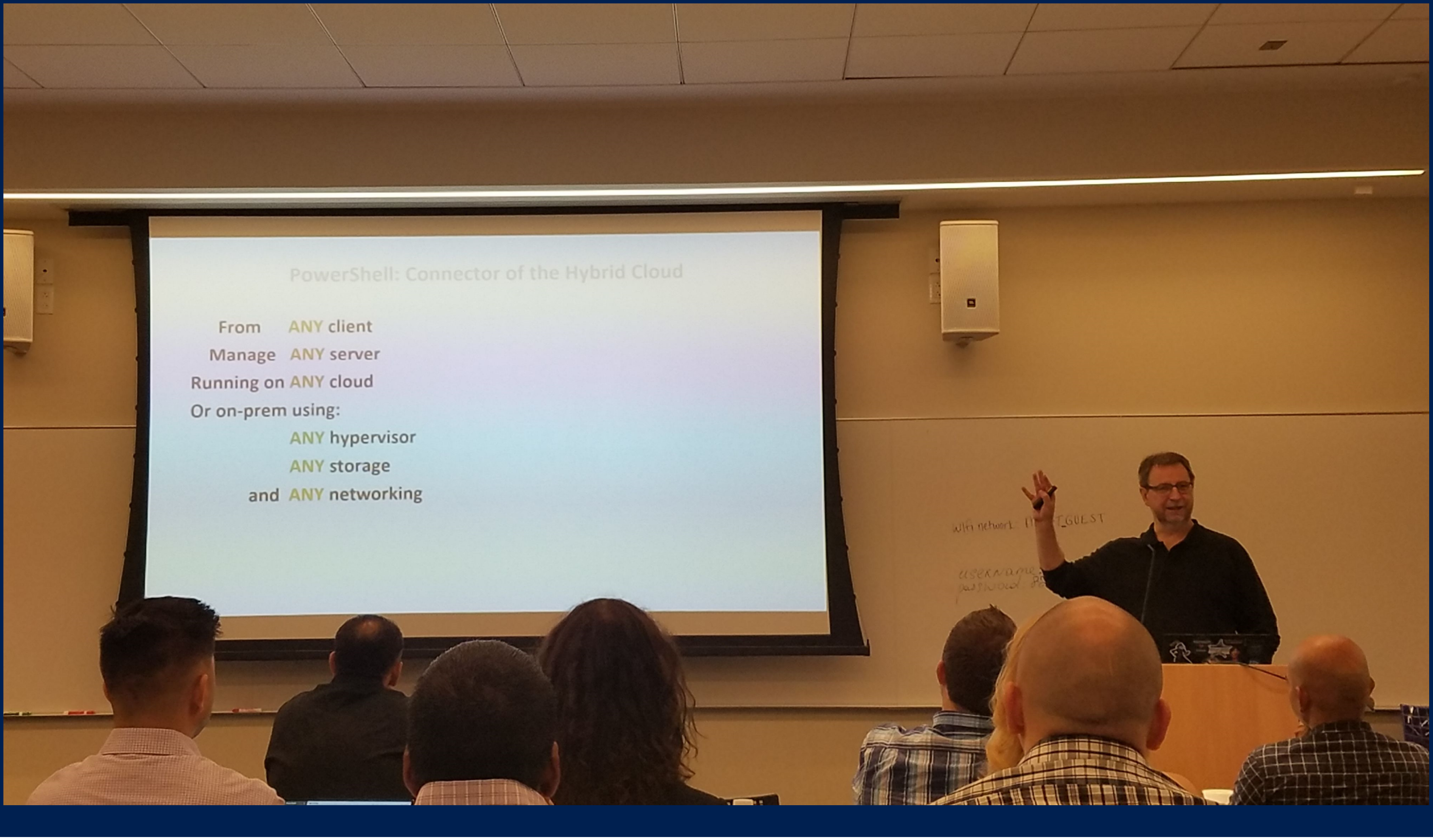
About Me:

- Yes, Yes – I am the substitute teacher.
- Sr. Infrastructure Engineer.
  - Windows, Exchange, SCOM, Citrix, VDI, Security blah blah.
  - Infrastructure as Code – Chef, TeamCity, Plaster, Psake, Chocolatey
- NYC Powershell UG.
- Reads the Monad Manifesto every year. - http://www.jsnover.com/Docs/MonadManifesto.pdf

What is Powershell:

- In the beginning, in a galaxy far far away – there were just Monad's.
- What is Powershell
  - Automation Model - .Net, WMI
  - Shell
  - Scripting Language (+ Classes)
  - MMC (think Exchange, VMWare, Sharepoint)
  - Remoting Engine (PSRP)

NYC Powershell UG



PowerShell: Connector of the Hybrid Cloud

From ANY client
Manage ANY server
Running on ANY cloud
Or on-prem using:
ANY hypervisor
ANY storage
and ANY networking

Powershell:

- Commandline shell / vs ISE Editor / vs VSCode

- .Net
- WMI
- Remoting

Warm-up

- Launch
  - ISE
  - Shell
- 64-bit / 32-bit
- CommandLine Switches –exec –prof –version
- $psversiontable
- Gci env:

Finding your way

- Get-Command
- Get-Member
- Get-help
- Get-Help –examples

Bicycle for the mind:

Scripts, Modules & Functions

- Script
- Modules
  - Text
  - Binary / DLL
- Functions

Automatic Variables

- $profile
- $psversiontable
- $pid
- $error
- $MyInvocation

- What is this ($_) ?

.Net / WMI

- .Net Framework
  - What is it ?
  - Why do you need it ?
- WMI
  - How to Access it
  - What is CIMV2, NameSpace, Classes, Methods, Properties
  - How to find more info ?
  - WMIExplorer - https://wmie.codeplex.com/
- PRO-Tip: ILSpy

Ideas

- .about_
- == -eq /-ne / -le
- Iteration
- Modularize for automation.
- Write-Output
- ErrorAction
- Do 1 thing, and 1 thing only.

SysAd Stuff: Active Directory

- Users
- Groups
- AD Cmdlets replaced LDAP/LDIFDE/LDP/ADSI
- AD Forensic Investigation - @GoateePFE

SysAd Stuff: Exchange

- Mailbox
- DAG
- DistributionGroups
- EWS
- SendMail

Reports

- Find X in all computers
- Find X in all users
- Query for X
- Export-CSV –
- Convert-OutputForCSV (@proxB)

CoreOS: Installed Programs

- WMI:
  - Get-WmiObject (GWMI)
    - Win32_ComputerSystem
    - Win32_OperatingSystem
- Process
  - Win32_Process
  - Get-Process
- Services
  - Win32_Service
  - Get-Service

Remoting

- Winrm qc
- WinRM
- DCOM
- Port 5985 / SSL – 5986
- WsMan
- PsSession

- Homework: PSRP

Remoting in Action

- Enter-PsSession
- New-PsSession
- -Session Parameter
- Invoke-Command

- Protocol DCOM /vs WsMan
- Invoke-Command / CimSession

Fun-Stuff

- Sapi Voice
- Process launch detection with events
- REST API Calls
- P/Invoke to save memory

Habits

- Read:Write –eq 10:1 ratio
- Read daily
- Write Daily
- Resources
  - Github www.github.com
  - ScriptCenter - https://technet.microsoft.com/en-us/scriptcenter/bb410849.aspx
  - Powershell Gallery - https://www.powershellgallery.com/
  - Hey Scripting Guy - https://blogs.technet.microsoft.com/heyscriptingguy/
- Google-Fu ! / StackOverflow / Slack

Resources.

- Book - Month of Lunches - Don Jones
- Learn from the best
  - Lee Holmes, Boe Prox, Doug Finke
  - Powershell Blog
  - Mattifestation
  - HSG
  - ScriptCenter
  - Security/InfoSec –Matt Graeber, Jared Atkinson, Will Schroeder, Carlos Perez

@sunnyc7
gist.github.com/sunnyc7
github.com/sunnyc7