查看类：

查看 powershell 版本
$PSVersionTable

查看操作系统版本信息
Get-CimInstance -ClassName Win32_OperatingSystem -ComputerName . | Select-Object -Property Build*,OSType,ServicePack*

查看部分组策略
gpresult /Z

查看部分组策略(需要导出到文件)
secedit /export /cfg c:\sec_result

查看服务
Get-Service

查看运行中服务
Get-Service | Where-Object {$_.Status -eq 'Running'}

查看 IP
ipconfig /all 或者 Get-NetipConfiguration

查看进程
Get-Process

查看已安装补丁
Get-WmiObject -Class Win32_QuickFixEngineering 或者 wmic qfe list

查看使用 Windows Installer 安装的程序
Get-WmiObject -Class Win32_Product | Format-Wide -Column 1

查看 CPU 相关信息
get-wmiobject win32_processor

查看 CPU 使用率 2008/2012 通用
Get-WmiObject win32_processor | select SystemName, LoadPercentage

查看 CPU 使用率排名前 20
Get-Counter -ComputerName localhost '\Process(*)\% Processor Time' | Select-Object -ExpandProperty countersamples | Select-Object -Property instancename, cookedvalue| Sort-Object -Property cookedvalue -Descending| Select-Object -First 20| ft InstanceName,@{L='CPU';E={($_.Cookedvalue/100).toString('P')}} -AutoSize

查看系统版本/序列号
gwmi win32_OperatingSystem

查看总内存
Get-WmiObject win32_OperatingSystem TotalVisibleMemorySize

查看总内存（单位 GB）
gwmi Win32_PhysicalMemory | %{$sum = 0} { $sum += $_.Capacity } {Write-Host ($sum / 1GB) "GB"}

查看空闲内存
Get-WmiObject win32_OperatingSystem FreePhysicalMemory

查看磁盘总空间（单位 MB）
Get-WMIObject Win32_LogicalDisk |Where-Object{$_.Size}|Foreach-Object { 'Disk {0} has {1:0.0} MB totalspace' -f $_.Caption, ($_.Size / 1MB) }

查看防火墙状态
netsh advfirewall show currentprofile

查看 BIOS 信息
Get-WMIObject -Class Win32_BIOS

查看主板信息
Get-WMIObject -Class Win32_Baseboard

查看逻辑磁盘信息
Get-WMIObject -Class Win32_LogicalDisk

查看物理磁盘信息
Get-WMIObject -Class Win32_DiskDrive

查看桌面设置(屏保是否设置)
Get-CimInstance -ClassName Win32_Desktop

查看一个文件夹内的文件及目录
Get-ChildItem -Path C:\ -Force

管理类：

重启服务器
Restart-Computer　或者 Restart-Computer -Force 强制重启

关闭服务器
stop-computer

停止 spooler 服务
Stop-Service -Name spooler

启动 spooler 服务
Start-Service -Name spooler

重启 spooler 服务
Restart-Service -Name spooler

停止某个进程
stop-process -id 2792

锁定服务器
rundll32.exe user32.dll,LockWorkStation

新增注册表项
New-Item -Path hkcu:\software_DeleteMe

删除注册表项
Remove-Item -Path hkcu:\Software_DeleteMe

入门级别

1. 像文件系统那样操作 Windows Registry——cd hkcu:
2. 在文件里递回地搜索某个字符串——dir –r | select string "searchforthis"

3. 使用内存找到五个进程——ps | sort –p ws | select –last 5
4. 循环（停止，然后重启）一个服务，如 DHCP——Restart-Service DHCP
5. 在文件夹里列出所有条目——Get-ChildItem – Force

6. 递归一系列的目录或文件夹——Get-ChildItem –Force c:\directory –Recurse

7. 在目录里移除所有文件而不需要单个移除——Remove-Item C:\tobedeleted –Recurse

8. 重启当前计算机——(Get-WmiObject -Class Win32_OperatingSystem -ComputerName .).Win32Shutdown(2)

收集信息

9. 获取计算机组成或模型信息——Get-WmiObject -Class Win32_ComputerSystem

10. 获取当前计算机的 BIOS 信息——Get-WmiObject -Class Win32_BIOS -ComputerName .

11. 列出所安装的修复程序（如 QFE 或 Windows Update 文件）——Get-WmiObject -Class Win32_QuickFixEngineering -ComputerName .

12. 获取当前登录计算机的用户的用户名—— Get-WmiObject -Class Win32_ComputerSystem -Property UserName -ComputerName .

13. 获取当前计算机所安装的应用的名字——Get-WmiObject -Class Win32_Product -ComputerName . | Format-Wide -Column 1

14. 获取分配给当前计算机的 IP 地址——Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter IPEnabled=TRUE -ComputerName . | Format-Table -Property IPAddress

15. 获取当前机器详细的 IP 配置报道——Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter IPEnabled=TRUE -ComputerName . | Select-Object -Property [a-z]* -ExcludeProperty IPX*,WINS*

16. 找到当前计算机上使用 DHCP 启用的网络卡——Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter "DHCPEnabled=true" -ComputerName .

17. 在当前计算机上的所有网络适配器上启用 DHCP——Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter IPEnabled=true -ComputerName . | ForEach-Object -Process {$_.EnableDHCP()}

软件管理

18. 在远程计算机上安装 MSI 包——(Get-WMIObject -ComputerName TARGETMACHINE -List | Where-Object -FilterScript {$_.Name -eq "Win32_Product"}).Install(\\MACHINEWHEREMSIRESIDES\path\package.msi)

19. 使用基于 MSI 的应用升级包升级所安装的应用——(Get-WmiObject -Class

Win32_Product -ComputerName . -Filter "Name='name_of_app_to_be_upgraded'").Upgrade(\\MACHINEWHEREMSIRESIDES\path\upgrade_package.msi)

20. 从当前计算机移除 MSI 包——(Get-WmiObject -Class Win32_Product -Filter "Name='product_to_remove'" -ComputerName .).Uninstall()

机器管理

21. 一分钟后远程关闭另一台机器——Start-Sleep 60; Restart-Computer –Force –ComputerName TARGETMACHINE

22. 添加打印机——(New-Object -ComObject WScript.Network).AddWindowsPrinterConnection(\\printerserver\hplaser3)

23. 移除打印机——(New-Object -ComObject WScript.Network).RemovePrinterConnection("\\printerserver\hplaser3 ")

24. 进入 PowerShell 会话——invoke-command -computername machine1, machine2 -filepath c:\Script\script.ps1

PowerShell 常用命令：

一 Get 类

1.Get-Command ： 得到所有 PowerShell 命令，获取有关 cmdlet 以及有关 Windows PowerShell 命令的其他元素的基本信息。包括 Cmdlet、Alias、Function。

2.Get-Process ： 获取所有进程

3.Get-Help ： 显示有关 Windows PowerShell 命令和概念的信息

4.Get-History ： 获取在当前会话中输入的命令的列表

5.Get-Job ： 获取在当前会话中运行的 Windows PowerShell 后台作业

6.Get-FormatData ： 获取当前会话中的格式数据

7.Get-Event ： 获取事件队列中的事件

8.Get-Alias ： 获取当前会话的别名

9.Get-Culture ：获取操作系统中设置的当前区域性

10. Get-Date ：获取当前日期和时间

11. Get-Host ： 获取表示当前主机程序的对象