

Commandline

Process Information

tasklist	List all processes currently running
tasklist /m	List all processes currently running and the DLLs each has loaded
tasklist /m [dll]	Lists all processes currently running which have the specified [dll] loaded
tasklist /svc	List all processes currently running and the services hosted in those processes
sc query	Query brief status of all services
sc qc [ServiceName]	Query the configuration of a specific service
taskkill <task>	

File handling

dir	
copy	
move	
del	
type	
more	
fc	compare two files
echo	
md, cd, rd/rmdir	directories
xcopy, robocopy	copy file trees (or other complex copy operations)

File search

dir /b /s [Directory]\[FileName]	Search directory structure for a file in a specific directory
[Command] find <string>	Find <string> in command output
[Command] find /c <string>	Count <string> in command output
find /c /v ""	Finds the count (/c) of lines that do not contain (/v) nothing (""). Lines that do not have nothing are all lines, even blank lines, which contain CR/LF

Loops

for /L %i in ([start],[step],[stop]) do [command]	Counting Loop
for /F %i in ([file-set]) do [command]	Iterate over file line by line

Tools

Netstat

<code>netstat -nao</code>	Show all TCP and UDP port usage and process ID
<code>netstat -nao [N] find [port]</code>	Look for usage of port [port] every [N] seconds
<code>netstat -s -p [tcp udp ip icmp]</code>	Dump detailed protocol statistics

Reg



`reg add [\\TargetIPAddr][RegDomain][Key]`

`reg export [RegDomain][Key] [FileName]`

`reg import [FileName]`

`reg query [\\TargetIPAddr][RegDomain][Key] /v [ValueName]`

recurse with /s

wmic



`wmic [alias] [where clause] [verb clause]`

[aliases]: process service share nicconfig startup useraccount qfe

Example [where clauses]: where name="nc.exe" where (commandline like "%stuff") where (name="cmd.exe" and parentprocessid!="[pid]")

Example [verb clauses]: list [full|brief] get [attrib1,attrib2...] call [method] delete

List all attributes of [alias]: C:\> wmic [alias] get /?

List all callable methods of [alias]: C:\> wmic [alias] call /?

`wmic process list full`

`wmic /node:[TargetIPAddr] /user:[User] /password:[Passwd] process list full`

Netsh



Interacting with the Network Using Netsh Turn off built-in Windows firewall: C:\> netsh firewall set opmode disable Configure interface "Local Area Connection" with [IPAddr] [Netmask] [DefaultGW]: C:\> netsh interface ip set address local static [IPAddr] [Netmask] [DefaultGW] 1 Configure DNS

server for "Local Area Connection": C:\> netsh interface ip set dns local static [IPAddr] Configure interface to use DHCP: C:\> netsh interface ip set address local dhcp

Administration

schtasks /CREATE /SC DAILY /TN "Backup" /TR "C:\Backup.bat" /ST 12:00	Schedule task
schtasks	List scheduled tasks
shutdown -s -t 0	shutdown now (time in sec 0)
runas /USER:Administrator "notepad.exe"	You guess!

GUI



Invoking Useful GUIs at the Command Line Local User Manager (includes group management): C:\> lusrmgr.msc Services Control Panel: C:\> services.msc Task Manager: C:\> taskmgr.exe Security Policy Manager: C:\> secpol.msc Event Viewer: C:\> eventvwr.msc Control Panel: C:\> control

Template

