

Commandline

Process Information



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

File search

Search directory structure for a file in a specific directory: C:\> dir /b /s [Directory]\[FileName]
Count the number of lines on StandardOut of [Command]: C:\> [Command] | 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

Counting Loop: C:\> for /L %i in ([start],[step],[stop]) do [command]

Iterate over file line by line: C:\> for /F %i in ([file-set]) do [command]

Tools

Netstat

Useful Netstat Syntax
Show all TCP and UDP port usage and process ID: C:\> netstat -nao
Look for usage of port [port] every [N] seconds: C:\> netstat -nao [N] | find [port]
Dump detailed protocol statistics: C:\> netstat -s -p [tcp|udp|ip|icmp]

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`

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

