Quick Reference
Windows Server 2003 Commands

TechRepublic®
Real World. Real Time. Real IT.

SYSTEM

Driverquery

{System root}\system32

Displays a list of the installed drivers, types and dates.

```
driverquery  [/s computer] [/u domain\user /p password]
    [/fo {table | list | csv}] [/nh] [/v | /si]
```

No parameters: Provides a list of drivers with the credentials of the logged in user.
[/s *computer*]: Get a list of the drivers installed on ‘computer’. Do not use UNC notation - only the system name.
[/u *domain\user* /p *password*]: Use the user name specified by /u domain\user and password specified by /p password to run the command. Omitting this switch uses the credentials of the currently logged in user.
[/fo {table | list | csv}]: Change the way that the output information is displayed. Use table to show the results in tabular form, list to show a list with one piece of information per line and csv to display the results in a format that can be imported into Excel.
[/nh]: Specifies that column header should not display.
[/v]: Verbose
[/si]: Information about signed drivers.

Eventcreate

{System root}\system32

Creates a custom event in the event log.

```
eventcreate [/s computer [/u domain\user [/p password]]
    {[/l {application | system}] | [/so source]} /t {error |
    information | warning } /id eventID /d description
```

[/s *computer*]: The name or IP address of the system to which the event should be recorded.
[/u *domain\user* /p *password*]: Use the user name specified by /u domain\user and password specified by /p password to run the command. Omitting this switch uses the credentials of the currently logged in user. Used only with the /s parameter.
[/l {application | system}]: The event log to which the event should be written.
[/so *source*]: The source to use for the event. Can be any application or component.
/t {error | information | warning }: The type of event to create.
/id *eventide*: Any number between 1 and 1000. Used to identify the event.
/d *description*: The description of the event.

Relog

{System root}\system32

Exports performance counter logs into other formats for easy import into other programs.

```
relog [file [file ...]] [-a] [-c path [path ...]] [-cf file]
    [-b date [time]] [-e date [time]] [-f {bin | csv | tsv | SQL}]
    [-o {outputFile | DSN!CounterLog}] [-t value] [-config
    {file | i}] [-q]
```

[*file* [*file* ...]]: A list of path names/files to performance counter logs.
[-a]: Append information to the output file rather than overwrite it.
[-c *path* [*path* ...]]: A list of performance counter paths to log, each enclosed in quotes and separated by spaces.
[-cf *file*]: A file containing the performance log counters that should be included in the relog output. By default all counters are included.
[-b *date* [*time*]]: The time of the first record to relog in M/D/YYYY HH:MM:SS format.
[-e *date* [*time*]]: The time of the last record to relog in M/D/YYYY HH:MM:SS format.
[-f {bin | csv | tsv | SQL}]: Specifies the format of the output file. Csv is comma delimited, tsv is tab delimited and bin is binary.
[-o {*outputFile* | DSN!CounterLog}]: The output file name to which the relog data will be written. For SQL output, specify a DSN.
[-t value]: Allows a smaller subset of records by taking a sample of every x records where x is the value in -t.
[-config {*file* | i}]: A config file containing the command line parameters to use.
[-q]: Displays performance counters and times of the log files specified in the input file.

Runas

{System root}\system32

Allows a program to be run within the context of a different user.

```
runas [/env] [/netonly] [/profile | /noprofile] [/savedcreds]
    [/smartcard] [/showtrustlevels] [/trustlevel]
    /user:username program
```

[/env]: Uses the current network environment rather than the user’s local environment.
[/netonly]: The information provided is for remote access only.
[/profile | /noprofile]: /profile will load the user’s profile and is the default behavior. Specify /noprofile to avoid loading the user’s profile.
[/savedcreds]: Use this switch if the user’s credentials have been previously saved.
[/smartcard]: Use this switch if credentials will be supplied from a smart card.
[/showtrustlevels]: Shows the available trustlevel options.
[/trustlevel]: The level of authorization for which the program will run.
/user:*username*: The account under which the application should run in domain\user format.
Program: The program to run.

Shutdown

{System root}\system32

Shuts down or restarts the local machine or a remote system.

```
shutdown [/i | /a | /l | /s | /r | /p | /h | /e] [/f] [/m \\computer]
    [/t seconds] [/d [p:] major:minor [/c "comment"]]
```

[/i | /a | /l | /s | /r | /p | /h | /e]: The shutdown or restart method - each described below.
[/i]: Must be the first parameter if used. Displays a shutdown dialog box on the remote system.
[/a]: If within the shutdown timeout period, the shutdown is canceled. Can only be used with the /m switch.
[/l]: Logs the currently logged in user off the system with no warning. This switch cannot be used with /m or /t.
[/s]: Shuts down the specified system or the local system if none is specified.
[/r]: Restarts the specified system.
[/p]: Local system only: Immediately shuts down the system with no warning.
[/h]: Places the specified system into hibernation.
[/e]: Allows documentation for the reason for the shutdown.
[/f]: Closes running applications without warning.
[/m \\*computer*]: The computer to be shut down. When omitted, the local system is assumed.
[/t *seconds*]: The number of seconds to wait before shutting down. The default is 30 seconds, but can range from 0 to 600 seconds.
[/d [p:] major:minor [/c "*comment*"]]: Provides a reason for the shutdown. p: indicates that the shutdown is planned. Major is the major reason — a number from 0 to 255 and minor is the minor reason, a number from 0 to 65535.

Systeminfo

{System root}\system32

Provides detailed information about the system specified including OS, security information, RAM, disk properties, etc.

```
systeminfo [/fo {table | list | csv}] [/nh] [/s computer
    [/u domain\user [/p password]]]
```

[/fo {table | list | csv}]: Change the way that the output information is displayed. Use table to show the results in tabular form, list to show a list with one piece of information per line and csv to display the results in a format that can be imported into Excel.
[/nh]: For table and csv output suppress column headers.
[/s *computer* [/u *domain\user* [/p *password*]]]: /s specifies the name or address of a remote computer for which to get information while /u and /p specify a username and password combination to use to log on to the system.

Taskkill

{System root}\system32

Kills a task or process.

```
taskkill [/s computer] [/u domain\user [/p password]]
    {/fi filter [{/pid process | /im image}] | /pid process |
    /im image} [/f] [/t]
```

[/s *computer*]: The name of the computer which has the task that needs to be killed.
[/u *domain\user* [/p *password*]]: Use the credentials specified to run the command. When omitted, runs as the logged in user.
{/fi *filter*}: The type of processes to include in the command.
[{/pid *process* | /im *image*}]: /pid is the process ID of the process to kill while /im indicates the name of the process to kill. Use * to specify all image names.
[/f]: Forcefully terminate the process.
[/t]: Kill child processes of the killed process.

Tasklist

{System root}\system32

Displays the tasks running on the specified machine.

```
tasklist [/s computer] [/u domain\user [/p password]]
    [{/m module | /svc | /v}] [/fo {table | list | csv}] [/nh]
    [/fi filter [/fi filter2 [ ... ]]]
```

[/s *computer*]: The name of the computer which has the task that needs to be killed.
[/u *domain\user* [/p *password*]]: Use the credentials specified to run the command. When omitted, runs as the logged in user.
[/m *module*]: Displays tasks with DLL modules matching the pattern provided.
[/svc]: Displays service information for each process.
[/v]: Verbose. Display full details of the adapter and transport.
[/fo {table | list | csv}]: Change the way that the output information is displayed. Use table to show the results in tabular form, list to show a list with one piece of information per line and csv to display the results in a format that can be imported into Excel.
[/nh]: When using table or CSV output, disables headers from being displayed.
[/fi *filter* [/fi *filter2* [...]]]: The types of processes to include in the command.

FILE SYSTEM

Cipher

{System root}\system32

Show or modify the state of encryption on files and folders.

```
cipher
```

No parameters: Shows the encryption status of every file in the current directory.

```
cipher [/d | /e] [/s:directory] [/a] [/i] [/f] [/q] [/h]
    [pathname [...]]
```

/d: Decrypts the specified folder.
/e: Encrypts the specified folder marking it such that all files added to the folder are also encrypted.
/s:*directory*: Recurses the /d or /e operation into all subfolders of the specified directory.
/a: Performs the operation on both files and folders.
/f: Forces the operation on all objects.
/h: Displays files with attributes of system or hidden. These files are not encrypted.
/I: Continues the operation even if errors are encountered.
/q: Reports only critical information during the operation.

```
cipher /k
```

/k: Creates a new encryption key for the current user. All other options are ignored.

```
cipher /r:path+filename
```

/r:*path+filename*: Generates a new recovery agent certificate and stores it in the path+filename specified.

```
cipher /u /n
```

Updates the encryption key for the user or recovery agent to the current ones for all encrypted files and folders on the drive and prevents the key from being updated. /u and /n need to be used together.

```
cipher /w:path
```

/w:*path*: Removes data on unused portion of the volume specified by the path.

```
cipher /x[:encrypted file] [filename]
```

Identifies certificates and keys for the currently logged in user and backs them up to the location specified by filename. If the encrypted file is included, the certificate used to encrypt it will also be backed up.

Compact

{System root}\system32

Manages the compression of files and folders on an NTFS volume.

```
compact
```

No parameters: displays the compression parameters for the current folder.

```
compact [/c | /u] [/a] [/f] [/i] [/q] [/s[:directory]] [targetname[...]]
```

/c: Compress the files or folders specified.
/u: Uncompress the files or folders specified.

Continued on next page