Windows Resource Kit Quick Reference

Author: Jialong He
Email: Jialong_he@bigfoot.com
http://www.bigfoot.com/~jialong_he

Console User Manager

Cusrmgr -u *UserName* [**-m** *ComputerName*] [{**-r** *NewUserName*| **-d** *NewUserName*}] [{**-p** | **-P** *Passwd*}] [**-rlg** *OldGroupName NewGroupName*] [**-rgg** *OldGroupName NewGroupName*] [**-alg** *LocalGroupName*] [**-agg** *GlobalGroupName*] [**-dlg** *LocalGroupName*] [**-dgg** *GlobalGroupName*] [**-c** *Comment*] [**-f** *FullName*] [**-U** *UserProfile*] [**-n** *LogonScript*] [**-h** *HomeDir*] [**-H** *HomeDirDrive*] [{+**s** | **-s** } *Property*]

-u *UserName*	user account to perform the operation on
-m *ComputerName*	Computer name
-r *NewUserName*	Rename the user specified with –**u**
-d *NewUserName*	Delete *NewUserName*
-P *Passwd*	Set password to *Passwd*
-rlg *OldGroupName NewGroupName*	Rename local group
-rgg *OldGroupName NewGroupName*	Rename global group
-alg *LocalGroupName*	adds user to local group
-agg *GlobalGroupName*	adds user to global group
-dlg *LocalGroupName*	deletes user from local group
-dgg *GlobalGroupName*	deletes user from global group
-c *Comment*	comment to the user given with **-u**
-f *FullName*	Full name
-U *UserProfile*	Path to user profile
-n *LogonScript*	Path to user's logon script
-h *HomeDir*	User's home directory
-H *HomeDirDrive*	User's home drive
{+**s** | **-s** } *Property*	MustChangePassword CanNotChangePassword PasswordNeverExpires AccountDisabled AccountLockout RASUser

Add a list of users to a computer

addusers [*computername*] { **/c** [**/p:**{**l | c | e | d**}] **| /d | /e** } *filename* [/s:*x*] [/?]

/c	Create user accounts
/d	Dump user accounts
/e	Delete user accounts
/**p**:{**l**|**c**|**e**|**d**}	**l** users do not have to change passwords at next logon. **c** users cannot change passwords. **e** passwords never expire (implies l option). **d** accounts are disabled

Filename contains a list of users, an example is:

[User]
User1,FullName,Password,Comment,HomeDir,Profile,Script
User2,FullName,Password,Comment,HomeDir,Profile,Script
[Global]
GlobalGroupName,Comment,User1, User2
[Local]
LocalGroupName,Comment,User1, User2

Add a list of users to a group

usrtogrp *filename*

filename contains the users to be added. For example,

```
domain: localmachine
globalgroup: Administrators
user1
user2
```

Note, add a single user to a local group, use NET command,
Net localgroupe Administrators user1 /add

Commonly Used Commands

pulist [*ComputerName*]	List running processes
whoami [*/options*]	Display current user information e.g., whoami /all
getmac [*computername*] [*computername.domain.com*]	Get Ethernet address
uptime [*server*] [**/s**] [**/a**] [{ /d:mm/dd/yyyy | /p:n }] [/heartbeat] [{ /? | /help }]	Display computer uptime
associate .*ext ExeFname* [/q] [/**d**] [/**f**] [/?]	Add association of an extension to program. /d delete association. E.g. associate .lst notepad.exe
sclist [-?] [**-r**] [**-s**] [*ComputerName*]	List installed services
perms [*domain*|*computer*\]*username filename* [/i] [/s] [/?]	Display access permission. E.g., *perms jialong c: /s*
instsrv *ServiceName PathToExecuteable* [**-a** *AccountName*] [**-p** *AccountPassword*] [*ServiceName* **Remove**]	Install or remove a service, for example: *instsrv MyService "srvany.exe"* net start MyService

Service Operations

Netsvc *servicename* \\computername /cmd {/? | /help}

Example: *netsvc /list \\joes486*

List	lists installed services
Query	queries the status of a service
Start	starts the specified service
Stop	stops the specified service
Pause	pauses the specified service
Continue	restarts a paused service

Services Control

sc [*MachineName*] **Command** *ServiceName [OptionName=OptionValue...]*

Config	Changes the configuration of a service (persistent).
Continue	Sends a CONTINUE control request to a service.
Control	Sends a control to a service.
Create	Creates a service (adds it to the registry).
Delete	Deletes a service (from the registry).
Description	Changes the description of a service.
EnumDepend	Enumerates service dependencies.
Failure	Changes the actions taken by a service upon failure.
GetDisplayName	Gets the display name for a service.
GetKeyName	Gets the name of the registry key for a service.
Interrogate	Sends an INTERROGATE control request to a service.
Pause	Sends a PAUSE control request to a service.
Qc	Queries configuration for the service. To find out the name of the binary for any service and whether it shares a process with other services, run **sc qc** *ServiceName*.
Qdescription	Queries the description of a service.
Qfailure	Queries the actions taken by a service upon failure.
Query	Queries the status for a service, or enumerates the status for types of services.
QueryEx	Queries the status and extended information for a service, or enumerates the status and extended information for types of services.
SdShow	Displays a service's security descriptor using SDDL.
SdSet	Sets a service's security descriptor using SDDL.
Start	Starts a service.
Stop	Sends a STOP request to a service.
Boot	Values are {**ok** | **bad**} Indicates whether the last restart should be saved as the last-known-good restart configuration
Lock	Locks the Service Database
QueryLock	Queries the LockStatus for the SCManager Database

Registry Console Tool

REG ADD [*Computer*\]*Keyname* [**/v** *ValueName* | **/ve**] [**/t** *Type*] [**/s** *Separator*] [**/d** *Data*] [**/f**]
REG COMPARE [*Machine*\]*Keyname1* [*Machine*\]*Keyname2* [**/v** *ValueName*] | [**/ve**] [**/s**] [Output]
REG COPY [*Machine*\]*SourceKey* [*Machine*\]*DestinationKey* [**/s**] [**/f**]
REG DELETE [*Machine*\]*Keyname* [**/v** *ValueName* | **/ve** | **/va**] [**/f**]
REG QUERY [*Machine*\]*KeyName* [**/v** *ValueName* | **/ve**] [**/s**]
REG EXPORT *Keyname Filename* [**/nt4**]
REG IMPORT *FileName*
REG SAVE [*Machine*\]*KeyName FileName*
REG RESTORE [*Machine*\]*KeyName FileName*

REG LOAD [*Machine*\] *KeyName FileName*
REG UNLOAD [*Machine*\]*KeyName*

Root key name Abbreviation
HKEY_LOCAL_MACHINE *HKLM*
HKEY_CURRENT_USER *HKCU*
HKEY_CLASSES_ROOT *HKCR*
HKEY_CURRENT_CONFIGURATION *HKCC*

When use REG ADD, /t type include
REG_BINARY
REG_DWORD
REG_DWORD_LITTLE_ENDIAN
REG_DWORD_BIG_ENDIAN
REG_EXPAND_SZ
REG_MULTI_SZ
REG_NONE
REG_SZ

Example
REG ADD HKLM\Software\MyCo\ /v Data /t REG_BINARY /d fe340ead
Adds a value (name: Data, type: REG_BINARY, data: fe340ead).

Registry Script Tool
Regini *ScriptFile*

ScriptFile contains registry settings, e.g.

```
\registry\user\software\microsoft\exchange\client\options
   DictionaryLangId = REG_SZ 1033
   PickLogonProfile = REG_SZ 0
```

Find a Registry Key
regfind [{**-m** *\\ComputerName* | **-h** *HiveFile HiveRoot* | **-w** *Win95Directory*}] [**-i** n] [**-o** *OutputWidth*] [**-p** *RegistryKeyPath*] [{**-z** | **-t** *DataType*}] [{**-b** | **-B**}] [**-y**] [**-n**] [*SearchString* [**-r** *ReplacementString*]]

Example: regfind -p "HKEY_CURRENT_USER\Control Panel" -t REG_DWORD

Backup a Registry
regback [*destination_dir*] [*filename hivetype hivename*]

Example: regback c:\backup

Shutdown (reboot) computer
Shutdown [*computername*] [**/l**] [**/a**] [**/r**] [**/t**:xx] ["*msg*"] [**/y**] [**/c**]

/L Specifies a local shutdown.
/A Quits a system shutdown.
/R Restart the computer.
/T:xx Sets the timer for system shutdown in xx seconds.
"*msg*" Specifies an additional message.
/y Answers questions with "yes".
/C Forces running applications to close.

Example: shutdown \\YourPC /R

Log events
logevent [**-m** *\\ComputerName*] [**-s** *Severity*] [**-c** *CategoryNumber*] [**-r** *Source*] [**-e** *EventID*] [**-t** *TimeOut*] "*Event Text*"

Severity
{**S|I|W|E|F**} = {Success, Information, Warning, Error, Failure}

Example:
logevent -m \\server -s E -c 3 -r "User Event" -e 42 "My message."

Dump events
dumpel **-f** *filename* [**-s** *\\server*] [**-l** *log* [**-m** *source*]] [**-e** *n1 n2 n3...*] [**-r**] [**-t**] [**-d** *x*]

-f *file* Output file
-s *\\server* computer name
-l {system|application|security}
-d x dumps events for the past x days.

Examples
dumpel -f event.out -s eventsvr -l system

Directory Usage
diruse {/s | /v} {/m | /k | /b} [/c] [/,] [/q:# [/l] [/a] [/d] [/o]] [/*] dirs

/s includes subfolders
/{m|k|b} displays disk usage in MB, KB, or Byte.
/d displays only folders that exceed specified sizes.
/* uses the top-level folders residing in the specified dirs.

Example:
diruse /s /k /* c:\users

Substitute User
Su *username* ["*cmdline*"] [*domain*] [[*winstation*\]*desktop*] [*options*] [{**-b** | **-i** | **-n** | **-s** }]

username	user name for the new process
"cmdline"	command line to execute as user, default cmd
-cb	does not create a new console.If the new process is a console process, it inherits the console of the caller
-dn	does not switch to a new desktop
-e	disables environment preparation
-g	Forces GUI option prompting with supplied command-line arguments
-l	disables loading of the user registry hive. Default is used instead
-v	displays verbose output to STDOUT
-w	Do not wait on child
-b	The target user must possess the SeBatchLogonRight logon type (batch)
-i	The target user must possess the SeInteractiveLogonRight logon type (the default logon type for SU) (Interactive)
-n	The target user must possess the SeNetworkLogonRight logon type (Network).
-s	The target user must possess the SeServiceLogonRight logon type (Service).

Send HTTP command
httpcmd *httpserver input.file* [**-k**] [**-u**:*username*:*password*] [**-a**:*AuthenticationScheme*] [**-e**] [**-t**] [**-h**]

-k Keep-connection
-a:AuthenticationScheme can be "Basic", "NTLM", or "MS-KERBEROS".
-e echo sends requests to STDOUT.
-t do HEX-HTTP for filter testing.

Example in input file
GET index.html HTTP/1.0

Sysdiff
Sysdiff */snap snap_shot.img*
Take a snapshot of current status of system, then install software and configure system.

Sysdiff */diff snap_shot.img sys_diff.img*
Create a difference file. sysdiff.inf is very important, must exclude folders in-use (locked).

Sysdiff */apply /m /q sys_diff.img*
Apply the sys_diff.img to an new system.

Sysdiff */dump sys_diff.img dump.txt*
Dump the difference in human readable format.