Check Point CLI Reference Card - 20120724

by Jens Roesen – email – www - twitter

Check Point Environment variables (most common ones)

$FWDIR	FW-1 installation directory, with f.i. the conf, log, lib, bin and spool directories.
$CPDIR	SVN Foundation / cpshared tree.
$CPMDIR	Management server installation directory.
$FGDIR	FloodGate-1 installation directory.
$MDSDIR	MDS installation directory. Same as $FWDIR on MDS level.
$FW_BOOT_DIR	Directory with files needed at boot time.

Basic starting and stopping

cpstop	Stop all Check Point services except cprid. You can also stop specific services by issuing an option with cpstop. For instance cpstop FW1 stops FW-1/VPN-1 or use cpstop WebAccess to stop WebAccess.
cpstart	Start all Check Point services except cprid. cpstart works with the same options as cpstop.
cprestart	Combined cpstop and cpstart. Complete restart.
cpridstop	Stop cprid, the Check Point Remote installation Daemon.
cpridstart	Start cprid, the Check Point Remote installation Daemon.
cpridrestart	Combined cpridstop and cpridstart.
fw kill [-t sig] proc_name	Kill a Firewall process. PID file in $FWDIR/tmp/ must be present. Per default sends signal 15 (SIGTERM). Example: fw kill -t 9 fwm
fw unloadlocal	Uninstall local security policy and disables IP forwarding.

Basic firewall information gathering

fw ver [-k] fwm ver vpn ver [-k] fgate ver	Show major and minor version as well as build number and latest installed hotfix of a Check Point module. Show additional kernel version information with -k switch.
cpshared_ver	Show the version of the SVN Foundation.
fw stat	Show the name of the currently installed policy as well as a brief interface list. Can be used with the -long or -short switch for more information.
cpwd_admin list	Display process information about CP processes monitored by the CP WatchDog.
cpca_client lscert	Display all ICA certificates.
fw ctl iflist	Display interface list.
fw ctl arp [-n]	Display proxy arp table. -n disables name resolution.
fw ctl pstat	Display internal statistics including information about memory, inspect, connections and NAT.
fw ctl chain	Displays in and out chain of CP Modules. Useful for placing fw monitor into the chain with the -p option.
fw ctl zdebug drop	Real time listing of dropped packets.
cp_conf sic state	Display current SIC trust state.
cp_conf finger get	Display fingerprint on the management module.
cp_conf client get	Display GUI clients list.
cp_conf admin get	Display admin accounts and permissions. Also fwm -p
cp_conf auto get <fw1|fg1|rm|all>	Display autostart state of Check Point modules.
fgate stat	Status and statistics of Flood-Gate-1.
fwaccel <stat|stats|conns>	Status and statistics or connection table of SecureXL.
cpstat <app_flag> [-f flavour]	Display status of the CP applications. Command has to be used with a application flag app_flag and an optional flavour. Issue cpstat without any options to see all possible application flags and corresponding flavours. Examples: cpstat fw -f policy – verbose policy info cpstat fw -f sync – Synchronisation statistics cpstat os -f cpu – CPU utilization statistics cpstat os -f memory – Memory usage info cpstat os -f ifconfig – Interface table
cpinfo -z -o <file>	Create a compressed cpinfo file to open with the InfoView utility or to send to Check Point support.
fw hastat	View HA state of local machine.
cphaprob state	View HA state of all cluster members.
vpn overlap_encdom	Show, if any, overlapping VPN domains.
fw tab -t <tbl> [-s]	View kernel table contents. Make output short with -s switch. List all available tables with fw tab -s. E.g. fw tab -t connections -s – Connections table.
avsu_client [-app <app>] get_version	Get local signature version and status of content security <app> where <app> can be "Edge AV", "URL Filtering" and "ICS". Without the -app <app> option "Anti Virus" is used by default.
avsu_client [-app <app>] fetch_remote -fi	Check if signature for <app> is up-to-date. See previous command for the possible values of <app>.
show asset hardware	View hw info like serial numbers in Nokia clish. Also see ipsctl -a and cat /var/etc/.nvram.
info device	View Edge Appliance information (hw, fwl, license..)
info computers	List active devices behind Edge Appliance.

View and manage logfiles

fw lslogs	View a list of available fw logfiles and their size.
fwm logexport	Export/display current fw.log to stdout.
fw logswitch [-audit]	Write the current (audit) logfile to YY-MM-DD-HHMMSS.log and start a new fw.log.
fw log -c <action>	Show only records with action <action>, e.g. accept, drop, reject etc. Starts from the top of the log, use -t to start a tail at the end.
fw log -f -t	Tail the actual log file from the end of the log. Without the -t switch it starts from the beginning.
fw log -b <starttime> <endtime>	View today's log entries between <starttime> and <endtime>. Example: fw log -b 09:00:00 09:15:00.
fw fetchlogs -f <file> module	Fetch a logfile from a remote CP module. NOTICE: The log will be deleted from the remote module. Does not work with current fw.log.
fwm logexport -i in.log -o out.csv -d ',' -p -n	Export logfile in.log to file out.csv, use , (comma) as delimiter (CSV) and do not resolve services or hostnames.

Display and manage licenses

cp_conf lic get	View licenses.
cplic print	Display more detailed license information.
fw lichosts	List protected hosts with limited hosts licenses.
dtps lic	SecureClient Policy Server license summary.
cplic del <sig> <obj>	Delete license with signature sig from object obj.
cplic get <ip host|-all>	Retrieve all licenses from a certain gateway or all gateways in order to synchronize license repository on the SmartCenter server with the gateway(s).
cplic put <-l file>	Install local license from file to an local machine.
cplic put <obj> <-l file>	Attach one or more central or local licenses from file remotely to obj.
cprlic	Remote license management tool.
contract_util mgmt	Get contracts from Management Server.

Basic configuration tasks, Administrators, Users, SIC, ICA

cpconfig	Menu based configuration tool for the most common tasks. Options depend on the installed products and modules.
cp_conf -h	Display cp_conf help. Options depend on the installed products and packages.
cp_conf admin add <user> <pass> <perm>	Add admin user with password pass and permissions perm where w is read/write access and r is read only. Note: permission w does not allow administration of admin accounts.
cp_admin_convert	Export admin definitions created in cpconfig to SmartDashboard.
fwm lock_admin -v	View list of locked administrators.
fwm lock_admin -u <user>	Unlock admin user. Unlock all with -ua.
cp_conf admin del <user>	Delete the admin account user.
fwm expdate <dd-mmm-yyy> [-f <dd-mmm-yyyy>]	Set new expiration date for all users or with -f for all users matching the expiration date filter: fwm expdate 31-Dec-2020 -f 31-Dec-2010.
cp_conf client get	Display GUI clients list.
cp_conf client <add|del> <ip>	Add / delete GUI client with IP ip. You can delete multiple clients at once.
fwm sic_reset	Reset internal Certificate Authority (ICA) and delete certificates. Initialize ICA afterwards with cpconfig or cp_conf ca init.
cp_conf sic init <key>	(Re)initialize SIC.
cpca_client	Manage parts of the ICA. View, create and revoke certificates, start and stop the ICA Web Management Tool.

fw monitor Examples

The fw monitor packet sniffing tool, is part of every FW-1 installation. For more info on this topic see the Check Point guide (http://bit.ly/fwmonref) or see my fw monitor cheat sheet (http://bit.ly/cpfwmon). fw6 monitor is working with GaiA.

Display traffic with 192.168.1.12 as SRC or DST on interface ID 2
(List interfaces and corresponding IDs with fw ctl iflist)

```
fw monitor -e 'accept host(192.168.1.12) and ifid=2;'
```

Display all packets from 192.168.1.12 to 192.168.3.3

```
fw monitor -e 'accept src=192.168.1.12 and dst=192.168.3.3;'
```

UDP port 53 (DNS) packets, pre-in position is before 'ippot_strip'

```
fw monitor -pi ipopt_strip -e 'accept udpport(53);'
```

UPD traffic from or to unprivileged ports, only show post-out

```
fw monitor -m O -e 'accept udp and (sport>1023 or dport>1023);'
```

Display Windows traceroute (ICMP, TTL<30) from and to 192.168.1.12

```
fw monitor -e 'accept host(192.168.1.12) and tracert;'
```

Capture web traffic for VSX virtual system ID 23

```
fw monitor -v 23 -e 'accept tcpport(80);'
```

Capture traffic on a SecuRemote/SecureClient client into a file.
srfw.exe in $SRDIR/bin (C:\Program Files\CheckPoint\SecuRemote\bin)

```
srfw monitor -o output_file.cap
```

GAiA clish

ver	Show GAiA Version.
show configuration	Show running configuration.
save config	Save running configuration.
history	Show command history.
show commands	Show all commands you are allowed to run.
lock database override	Acquire read/write access to the database.
start transaction	Start transaction mode. All changes made will be applied at once if you exit transaction mode with commit or discarded if you exit with rollback.
show version os edition	Show which OS edition (32 or 64-bit) is running.
set edition default 32-bit|64-bit	Switch between 32 and 64-bit kernel. 64-bit needs at least 6GB of RAM (or 1GB running in a VM).
expert	Switch to bash and expert mode.
show extended commands	Show all defined extended (OS level) commands
add command df path /bin/df description "list free hdd space"	Add f.i. Linux command df to the list of extended commands. You can also use all options of an ext. command from within clish: clish> df -h

IPSO clish (Better go and read the documentation. Clish is mighty ;)

You can enter clish commands either in the clish itself or from the shell using clish [-s] -c "<command>". The -s option runs save config afterwards.

show summary	Show system configuration summary.
show asset hardware	Show hardware information. See also output of ipsctl -a and cat /var/etc/.nvram.
show images	Show available IPSO images.
show image current	Show current IPSO image.
show package all|active	Show all available/active packages.
show interfaces	Show all interfaces and their configuration.
set package name <name> <on|off>	Activate or deactivate a package.
set ssh server log-level <level>	Set sshd log verbosity to quiet, fatal, error, info (default), verbose or debug.
show vrrp [interfaces]	View VRRP (interface) status.
reboot image <img> save	Reboot into <img> and run save before booting.
rm /config/active	Kind of factory default reset. Reboot afterwards.
set voyager daemon-enable <1|0> ssl-port 8443 ssl-level 168	Enable (or disable) Voyager on SSL port 8443 using 3DES crypto. Also works with true, false, on or off. save config afterwards.

VPN & VPN Debugging

vpn ver [-k]	Check VPN-1 major and minor version as well as build number and latest hotfix. Use -k for kernel version.
vpn tu	Start a menu based VPN TunnelUtil program where you can list and delete Security Associations (SAs) for peers.
vpn shell	Start the VPN shell.
vpn debug ikeon|ikeoff	Debug IKE into $FWDIR/log/ike.elg.
vpn debug on|off	Debug VPN into $FWDIR/log/vpnd.elg.
vpn debug trunc	Truncate and stamp logs, enable IKE & VPN debug.
vpn drv stat	Show status of VPN-1 kernel module.
vpn overlap_encdom	Show, if any, overlapping VPN domains.
vpn macutil <user>	Show MAC for Secure Remote user <user>.

You can analyze the generated files ike.elg and vpnd.elg with the IKEView tool provided by Check Point.

Provider-1

mdsconfig	MDS replacement for cpconfig.
p1shell	Start the P1Shell if it's not the default shell.
mdsenv [dms_name]	Set the environment variables for MDS or DMS level.
mdsstart [-m|-s]	Starts the MDS and all DMS (10 at a time). Start only MDS with -m or DMS subsequently with -s.
mdsstop [-m]	Stop MDS and all DMS or with -m just the MDS.
mdsstat [dms_name]|[-m]	Show status of the MDS and all DMS or a certain customer's DMS. Use -m for only MDS status.
cpinfo -c <dms>	Create a cpinfo for the customer DMS <dms>. Remember to run mdsenv <dms> in advance.
mcd <dir>	Quick cd to $FWDIR/<dir> of the current DMS.
mdsstop_customer <dms>	Stop DMS dms.
mdsstart_customer <dms>	Start DMS dms.
mds_backup [-l] [-d directory]	Backup binaries and data to current directory. Change output directory with -d, exclude logs with -l. You can exclude files by specifying them in $MDSDIR/conf/mds_exclude.dat.
./mds_restore <file>	Restore MDS backup from file. Notice: you may need to copy mds_backup from $MDSDIR/scripts/ as well as gtar and gzip from $MDS_SYSTEM/shared/ to the directory with the backup file. Normally, mds_backup does this during backup.
mdscmd <subcmds> [-m mds -u user -p pass]	Connect to a (remote) MDS as CPMI client and configure or manage it. See mdscmd help.
vsx_util <subcommand>	Perfom VSX maintenance from the main DMS. See vsx_util -h for subcommands.

ClusterXL

cp_conf ha enable|disable [norestart]	Enable or disable HA.
cphastart cphastop	Enable / Disable ClusterXL on the cluster member. Issued on a cluster member running in HA Legacy Mode cphastop might stop the entire cluster.
fw hastat	View HA state of local machine.
cphaprob state	View HA state of all cluster members.
cphaprob -a if	View interface status.
cphaprob -ia list	View list and state of critical cluster devices.
cphaprob syncstat	View sync transport layer statistics. Reset with -reset.
cphaconf set_ccp <broadcast|multicast>	Configure Cluster Control Protocol (CCP) to use unicast or multicast messages. By default set to multicast. Setting survives reboot.
clusterXL_admin [-p] <up|down>	Perform a graceful manual failover by registering a faildevice. Survives a reboot with -p switch set

Note: DO NOT run any cphaconf commands other than cphaconf set_ccp.

SecurePlatform cpshell

cd_ver or ver	View SecurePlatform build number.
sysconfig	SPLAT OS configuration and CP Software installation tool.
webui <enable|disable> [port]	Enable the WebUI on HTTPS port 443 or port [port] or disable the WebUI.
showusers	Display a list of configured SecurePlatform administrators.
adduser <user>	Add an admin account. Delete with deluser <user>.

SecurePlatform cpshell

backup	Backup system config to /var/CPbackup/backups file backup_host.domain_DD_MM_YYYY_hh_mm.tgz. backup works with the following switches: --scp <ip> <user> <pass> -path <path> <file> --tftp <ip> -path <tftpboot/subdir> file --ftp <ip> <user> <pass> -path <path> <file> If you do not specify file or path the default naming scheme and/or the homedir of the account will be used. A relative path results in a backup to a subdirectory of home.
restore <file>	Restores a backup from file <file>. Pretty much works with the same switches as backup.
snapshot	Take a snapshot of the entire system. Without options it's menu based. **Note: cpstop is issued!** Examples: snapshot --file <file> snapshot --tftp <ip> <file> snapshot --scp <ip> <user> <pass> <file> snapshot --ftp <ip> <user> <pass> <file>
revert	Reboot system from snapshot. Same switches as snapshot.
patch add cd <patch>	Install the patch <patch> from CD.
addarp <ip> <MAC>	Add a static ARP entry for ip. Survives a reboot. Use delarp with the same syntax to delete a ARP entry.
dns [add|del <ip>]	View DNS server setting or add/delete DNS servers.
log list	Show index of available system and error log files.
log show <nr>	View log file number <nr> from the log list index.
passwd	Change password. In standard mode (cpshell) it changes the admin password, in expert mode passwd is an alias for /bin/expert_passwd and changes only the expert pass. As expert use /usr/bin/passwd <user> for other users.
chsh -s /bin/bash admin	Change the login shell for the user admin to always be in expert mode after login.

VSX R67 (Commands for R75.40VS Expert Mode are in *italics*)

vsx stat [-v] [-l] [id]	Show VSX status. Verbose with -v, interface list with -l or status of single VS with VS ID <id>.
vsx get *vsenv*	View current shell context.
vsx set <id> *vsenv <id>*	Set context to VS with the ID <id>.
vsx sic reset <id>	Reset SIC for VS <id>. For details see sk34098.
vsx sicreset	Reset SIC in current context in R75.40VS.
cpinfo -x <vs>	Start cpinfo collecting data for VS ID <vs>.
vpn -vs <id> debug trunc	Empty & stamp logs, enable IKE & VPN debug.
fw -vs <id> getifs	View driver interface list for a VS. You can also use the VS name instead of -vs <id>.
fw tab -vs <id> -t <table>	View state tables for virtual system <id>.
fw monitor -v <id> -e 'accept;'	View traffic for virtual system with ID <id>. Attn: with fw monitor use -v instead of -vs
cphaprob -vs <id> state	View HA state for Virtual System id when "Per Virtual System HA" mode is configured.
cphaprob -vs <id> register	Register a faildevice and switch VS <id> to the next cluster member (only in Per VS HA/VSLS).
$linux_command -z <id> traceroute -Z <id>	In R67 set context for ifconfig, ip, arp, ping or netstat. Uppercase "z" for traceroute.

In general, a lot of Check Point's commands do understand the -vs <id> switch.