Checkpoint CP CLI Commands

Version 1.0

Dokument Name: Checkpoint_CP CLI Commands

Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

touch erstellt ein neues File, wenn dies schon vorhanden ist wird es modifiziert
md5sum Berechnet den md5 hash
chown ändert den Datei Besitzer
chgrp ändert die Benutzer Gruppe
chmod ändert die Berechtigungen
Ethtool:
ethtool ethX Zeigt Infos über die NIC und die Einstellungen
ethtool-S ethX Zeigt NIC Statistiken Zähler, mit Error Zähler
ethtool -s autoneg off Schaltet die autonegotiation aus
ethtool -s ethX speed 100 Sets die NIC auf 100Mbps Full Duplex
duplex full
ethtool -i ethX Zeigt Treiber Informationen an
ethtool -p ethX Läst die LED an der Nic blinken
Netstat:
netstat -i übersicht der Nic zähler (oder ifconfig -s)
cpview
Anzeige von div. Systeminfos mit -t kann der Zeitliche verlauf angezeit werden +-
fw unloadlocal
Unload aller Policys!!! z.B. nötig, wenn kein Zugriff mehr möglich ist
Expert Mode
vergleichbar Cisco enable
set expert-password
Expert PW setzen
exit
Expert mode verlassen
show configuration
Cisco like, auch hier ist es möglch die Config als Text zu kopieren und mit Notepade etc zu bearbeiten. Kann dann per Copy and paste auf ein anderes System übertragen werden.
[Expert@gw-d7e3b3:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.
Configuration Options:
(1) Licenses and contracts
(2) Administrator
(3) GUI Clients
(4) SNMP Extension
(5) PKCS#11 Token
(6) Random Pool
(7) Certificate Authority
(8) Certificate's Fingerprint
(9) Check Point CoreXL
(10) Automatic start of Check Point Products
(11) Exit
Enter your choice (1-11) :

Locale Rules löschen:
fw unloadlocal
Centrales Managment, IP Adressen fehler (Log und Rules)
A99000fw004> set security-management local-override-mgmt-addr true mgmt-address 91.132.180.209 send-logs-to local-override-mgmt-addr

Check Point CLI Reference Card – v2.1

by Jens Roesen

Useful Secure Knowledge articles

sk65385	List of "How To" Guides for all Check Point products.
sk97638	Check Point Processes and Daemons
sk52421	Ports used by Check Point software
sk98348	Best Practices - Security Gateway Performance
sk105119	Best Practices - VPN Performance

There also are a lot of valuable ATRGs (Advanced Technical Reference Guides) available. Search for "ATRG" and a suitable keyword. For instance "atrg ipv6".

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.

Reference Card Command Shell Indicators

Expert Mode	GAiA clish [c]	SPLAT cpshell [c]	IPSO clish [c]	IPSO shell [i]

A lot of the expert mode commands are also available within GAiA clish as "extended command". View complete list with the clish command "show extended commands".

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 cpridstart cpridrestart	Stop, start or restart cprid, the Check Point Remote Installation Daemon.
fw kill [-t sig] proc	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	Uninstalls local security policy and disables IP forwarding.

Basic firewall information gathering

fw ver [-k] fwm [mds] 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.
ver [cs]	Show CP version and build as well as kernel info.
cpshared_ver	Show the version of the SVN Foundation.
cpview	Tool combining several Check Point and Linux commands into a great text based tool providing both OS and software blade information. See sk101878.
fw stat fw stat <-l|--long> fw stat <-s|--short>	Show the name of the current policy and a brief interface list. Use -l or -s for more info. Consider using cpstat fw instead of -l or -s switch for better formatted output.
fw ctl iflist	Display interface list.
fw ctl arp [-n]	Display proxy arp table. -n disables name resolution.
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.

Basic firewall information gathering

fgate stat	Status and statistics of Flood-Gate-1.
fwaccel <stat|stats|conns>	View status, statistics or connection table of SecureXL.
fw getifs	Show list of configured interfaces with IP and netmask.
cpstat <app_flag> [-f flavour]	View OS, HW and CP application status. Issue cpstat without any options to see all possible application flags <app_flag> and corresponding flavours. Examples: cpstat fw -f policy – verbose policy info cpstat os -f cpu – CPU utilization statistics
cpinfo -y all	List all installed patches and hotfixes.
cpd_sched_config print	Show task scheduled with CPD scheduler.
enabled_blades	View enabled software blades
avsu_client [-app <app>] get_version	Get signature version and status of content security <app>. Without the -app option "Anti Virus" is used.
show configuration [c]	Show running system configuration.
show commands [c]	Show all commands you are allowed to run.
show asset all [c]	Display general hardware information.
show sysenv all [c]	Display system component status (fans, power supply...)
asset	View hw info on IP Series Appliances running GAiA.
show asset hardware [c]	View hw info like serial numbers in Nokia clish.
ipsctl -a [i]	View hw info. Also see cat /var/etc/.nvram output.

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>	Detach license with signature sig from object obj.
cplid db_rm <sig>	Remove license <sig> from repository after detaching.
cplic get <ip host|-all>	Retrieve all licenses from a certain gateway or all gateways to synchronize SmartCenter license repository with gw(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.

View and manage log files

fw lslogs	View a list of available fw log files and their size.
fwm logexport	Export/display current fw.log to stdout.
fw repairlog <logfile>	Rebuild pointer files for <logfile>.
fw logswitch [-audit]	Copy 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>.
fw fetchlogs -f <file> module	Fetch a logfile from a remote CP module. NOTE: The log will be deleted from the remote module. Does not work with current fw.log.
fwm logexport -i <file> -o out.csv -d ',' -p -n	Export logfile <file> to file out.csv, use , (comma) as delimiter (CSV) and do not resolve services or hostnames (-n).
log list [c]	Show index of available system and error log files.
log show <nr> [c]	View log file number <nr> from the log list index.

Basic troubleshooting

cpview	View OS and software blade statistics. See sk101878.
cpinfo	Collect diagnostic data for CP support cases. See sk92739.
sar	System monitoring tool (GAiA) generating monitoring data every 10 minutes, keeping the data for 7 days. E.g.: sar -n EDEV - Interface errors from today sar -u -f /var/log/sa/sa04 - CPU stats from the 4th.
cpsizeme	For 24h, monitor gw resource utilization every minute and generate a CSV report to use for sizing considerations or troubleshooting. See sk88160 for additional information.
ethtool -S	View interface statistics and counters.
emergendisk	Create a bootable system on a USB device for system or password recovery and secure HDD wiping.
cpinfo -z -o <file>	Create a compressed cpinfo file to open with the InfoView utility or to send to Check Point support.
cst ecst	Configuration Summary Tool and its enhanced version. Packs IPSO config, logs, core dumps etc. into a single file. [i]
fw ctl zdebug drop	Real time listing of dropped packets.
cpwd_admin list	Display PID, status and starting time of CP WatchDog monitored processes.
cpca_client lscert	Display all ICA certificates.
fw tab -t <tbl> [-s]	View kernel table contents. Make output short with -s switch. List all available tables with fw tab -s. Example: fw tab -t connections -s – View connection table.
fw ctl multik stat	Show connection statistics for each kernel instance.
fw ctl pstat	Display internal statistics including information about memory, inspect, connections, synchronization 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.
cp_conf sic state cp_conf sic init <key>	Display SIC trust status or (re)initialize SIC. Also see sk30579 for additional hints on SIC troubleshooting.
fwm sic_reset	Reset Internal Certificate Authority (ICA) and delete certs. Reinitialize ICA with cpconfig or cp_conf ca init.
cpca_client	Manage parts of the ICA. View, create and revoke certificates, start and stop the ICA Web Tool. Examples: cpca_client lscert -stat Valid cpca_client search <searchstring>
fwaccel <off|on>	Disable/enable SecureXL.
cpmonitor	Statistics and analysis of snoop/tcpdump/fw monitor traffic capture files. See sk103212 for download link and usage.

sk98348 - Best Practices - Security Gateway Performance
sk98799 – Kernel Debug
PDF - How to Troubleshoot NAT-related Issues
tcpdump101 – Generate fw monitor and kernel debug CLI commands online.

fw monitor Examples

The fw monitor packet sniffer is part of every FW-1 installation. For more detailed info see my cheat sheet (http://bit.ly/cpfwmon). Disable SecureXL (fwaccel off) prior to sniffing.

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 0 -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);'
```

Basic administration and configuration tasks	
`cpconfig`	Menu based configuration tool. Options depend on the installed products and modules.
`sysconfig`	Start SPLAT OS and Check Point product configuration tool.
`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 account administration.
`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 `-f` for all users matching the expiration date filter: `fwm expdate 31-Dec-2020 -f 31-Dec-2014`.
`cp_conf client add <ip>` `cp_conf client del <ip>`	Add/delete GUI clients. You can delete multiple clients at once.
`cpca_client`	Manage parts of the ICA. View, create and revoke certificates, start and stop the ICA Web Tool.
`patch add cd <patch>`	Install the patch `<patch>` from CD.
`lvm_manager`	Manage partition sizes on GAiA. See sk95566 for info and download link.
`show users`	Show configured users and their homedir, UID/GID and shell.
`add user <user>`	Add a new user with username `<user>`.
`set user <user> shell <shell>`	Set the login shell of user `<user>` to `<shell>`. Setting it to `f.i. /bin/bash` will log in `<user>` directly into expert mode.
`set user <user> password`	Set new password for `<user>`.
`set selfpasswd`	Change your own password.
`set expert-password`	Set or change password for entering expert mode.
`save config`	Save configuration changes.
`showusers`	Display a list of configured SecurePlatform administrators.
`adduser <user>`	Add a new user with username `<user>`.
`chsh -s <shell> <user>`	Change the login shell for `<user>` to `<shell>` on SPLAT .
`passwd`	Change your own password.
`passwd`	Change expert password in expert mode on SPLAT systems.
`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).

VPN	
`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 `$FWDIR/log/ike.elg`. Analyze `ike.elg` with the IKEView tool. See sk30994.
`vpn debug on|off`	Debug VPN into `$FWDIR/log/vpnd.elg`. Analyze `vpnd.elg` with the IKEView tool. See sk30994.
`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>`.

sk60318 - How to troubleshoot VPN issues in Site to Site
sk89940 - How to debug VPND daemon
sk33327 - How to generate a valid VPN debug, IKE debug and FW Monitor

Backup and Restore	
`add backup`	Create backup in `/var/CPbackup/backups/` or on a remote server (scp/ftp/tftp). Also see sk91400. E.g.: `add backup local` `add backup scp ip <ip> path </pa/th/> username <user> interactive`
`set backup restore`	Restore backup. Also see sk91400. Examples: `set backup restore local <TAB>` `set backup restore scp ip <ip> path </pa/th/> file <file> username <user> interactive`
`show backups`	List locally stored backups.
`add snapshot` `delete snapshot`	Add and delete sytstem snapshots. Example `add snapshot <name> [descr <"my destription">]`
`set snapshot revert` `set snapshot export` `set snapshot import`	Export/import or revert to a certain system snapshot. E.g.: `set snapshot revert <name>` `set snapshot export <name> path <path> name <name>`
`show snapshots`	Show list of local snapshots.
`upgrade_export <file>` `migrate export <file>`	Tool from `$FWDIR/bin/upgrade_tools`. Saves only Check Point configuration (policy, objects...) and no OS settings.
`upgrade_import <file>` `migrate import <file>`	Import config package generated with migrate tools.
`backup`	Create backup in `/var/CPbackup/backups/` or on a remote server (scp/ftp/tftp). Also see sk54100. Examples.: `backup [-f <file>]` `backup --scp <ip> <user> <pass> [-path </pa/th/> <file>]`
`restore`	Restore backup from local package or via scp/ftp/tftp. Delete local backup packages. Menu based.
`snapshot`	Take a snapshot of the entire system. Without options it's menu based. **Note: cpstop is issued!** Examples: `snapshot --file <file>` `snapshot --scp <ip> <user> <pass> <file>`
`revert`	Reboot system from snapshot. Same syntax as `snapshot`.

ClusterXL configuration and troubleshooting – and some VRRP	
`cphaprob state`	View HA state of all cluster members.
`cphaprob -a if`	View interface status and CCP state.
`cphaprob -ia list`	View list and state of critical cluster devices.
`fw hastat`	View HA state of local machine.
`cp_conf ha enable| disable [norestart]`	Enable or disable HA.
`cphastart` `cphastop`	Enable / Disable ClusterXL on the cluster member. On HA Legacy Mode `cphastop` might stop the entire cluster.
`cphaprob syncstat`	View sync transport layer statistics. Reset with `-reset`. See sk34475 for detailed description.
`fw ctl pstat`	View sync status and packet statistics. See sk34476.
`fw ctl setsync <off|start>`	Stop or start synchronization in a cluster.
`fw -d fullsync <member-ip>`	Start a full synchronization with debugging output.
`cphaconf set_ccp <broadcast|multicast>`	Configure Cluster Control Protocol (CCP) to use unicast or multicast messages. By default set to multicast.
`cphaconf debug_data`	View multicast MAC addresses used.
`clusterXL_admin [-p] <up|down>`	Perform a graceful manual failover by registering a faildevice. Survives a reboot with `-p` switch set.
`show vrrp interfaces`	Detailed status of VRRP interfaces. For a brief overview you can also use `show vrrp` in the `iclid` shell.
`cphaprob tablestat`	View IPs and interface IDs for all cluster members.
`cphaprob igmp`	View IGMP status for CCP multicast mode.

sk93306 - Advanced Technical Reference Guide: ClusterXL R6x and R7x
sk56202 - How to troubleshoot failovers in ClusterXL
sk62570 - How to troubleshoot failovers in ClusterXL - Advanced
sk43984 - Interface flapping when cluster interfaces are connected through several switches

Multi-Domain Security Management (Provider-1)	
`mdsconfig`	MDS replacement for `cpconfig`.
`mdsenv [dms_name]`	Set the environment variables for MDS or DMS level.
`mdsstart [-m|-s]` `mdsstop [-m]`	Starts/stops the MDS and all DMS (10 at a time). Start only the MDS with `-m` or DMS subsequently with `-s`.
`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>`	Change directory to `$FWDIR/<dir>` of the current DMS.
`mdsstop_customer <dms>`	Stop single DMS `<dms>`.
`mdsstart_customer <dms>`	Start single DMS `<dms>`.
`mds_backup [-l] [-d directory]`	Backup binaries and data to current directory. Change output directory with `-d`, exclude logs with `-l`, do a dry run with `-v`. You can exclude files by specifying them in `$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.
`cma_migrate`	Import and if necessary upgrade an `export_database` created management server or DMS database package.
`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.

sk95329 – Advanced Technical Reference Guide: Multi-Domain Security Management
sk33207 - How to debug FWM daemon on Provider-1 DMS / CMA

VSX (When two commands are given, the first applies to R68 and the second to R75.40+)	
`vsx stat [-v] [-l] [id]`	Show VSX status. Verbose with `-v`, interface list with `-l` or status of single VS with VS ID `<id>`.
`show virtual-system all`	List all VS with their VS ID and name.
`vsx get` `vsenv`	View current shell context. Second line applies to VSX on R75.40VS and up.
`vsx set <id>` `vsenv <id>`	Set context to VS with the ID `<id>`. Second line applies to VSX on R75.40VS and up.
`set virtual-system <id>`	Set context to VS ID `<id>`.
`fw -vs <id> unloadlocal` `vsenv <id>; fw unloadlocal`	Unload policy from a VS. To unload policies on all VS use `fw vsx unloadall`. See sk33065 for details.
`vsx sic reset <id>` `vsenv <id>; fw vsx sicreset`	Reset SIC for VS `<id>`. For details see sk34098. Second line applies to VSX on R75.40VS and up.
`cpinfo -x <id>`	Start cpinfo collecting data for VS ID `<id>`.
`vpn -vs <id> debug trunc`	Empty & stamp logs, enable IKE & VPN debug.
`fw -vs <id> getifs` `vsenv <id>; fw 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>` `vsenv <id>; fw tab -t <table>`	View state tables for virtual system `<id>`. Second line applies to VSX on R75.40VS and up.
`vsx vspurge`	Remove unused VSX systems and fetch VS config.
`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 R68 set context for `ifconfig`, `ip`, `arp`, `ping` or `netstat`. Uppercase "Z" for `traceroute`.

A lot of Check Point's commands up to R68 do understand the `-vs <id>` switch. With newer versions you often have to change context with `vsenv <id>` before issuing the commands.