Checkpoint `cpstat` diagnostics and information tool cheat sheet

Author: Yuri Slobodyanyuk, https://www.linkedin.com/in/yurislobodyanyuk/

NOTE	The tool is to be run in Expert mode. It is available on both Management Server and Gateway. The available **flavor** options depend on the blades enabled and their subscription status, also on platform used. To know what options are available on your specific Checkpoint - run `#cpstat` without any switches.

status: Work in Progress.

blades

Flavor	Description
fw	Statistics: Packets accepted, packets dropped, Peak number of connections, current Number of connections, Top Rule Hits (shows rules with IDs with the most hits),

os

Flavor	Description
default	Product Name, SVN Foundation Version String, SVN Foundation Build Number, SVN Foundation Status (`OK`), OS Name (e.g. `Gaia`), OS Major Version (`3`), OS Minor Version (`10`), OS Build Number/SP Major/SP Minor/Version Level, Appliance SN (Serial Number), Appliance Name, Appliance Manufacturer.
ifconfig	Interface information: Name, IP Address, MTU, State, MAC address, RX Bytes (Received), TX Bytes (Transmitted), RX/TX Errors, RX/TX Drops, TX/RX Packets.
routing	Routing info - IPv4 routing table.
routing6	IPv6 routing table.
memory	Physical/virtual memory specs: Total/Active Virtual Memory, Total/Active/Free Real Memory, Memory Swaps/sec, Memory to Disk Transfers/sec.

Flavor	Description
cpu	CPU load stats (analog of Linux `top`): CPU User Time (%), CPU System Time (%), CPU Idle Time (%), CPU Usage (%), CPU Queue Length, CPU Interrupts/Sec, CPUs Number.
disk	Local hard disk stats: Disk Servicing Read\Write Requests Time, Disk Requests Queue, Disk Free Space (%), Disk Total Free Space (Bytes), Disk Available Free Space (Bytes), Disk Total Space (Bytes).
perf	Combined output of flavors `memory`, `cpu`, and `disk` above.
multi_cpu	CPU load as in `cpu`, but per processor/core.
multi_disk	Disk partitioning info, analog of `df -h`: Partition Name, Size, Used (%/bytes), Free Total (%/bytes), Free Available.
raidInfo	RAID disks and volumes info: Volume id, Volume type, Number of disks, Max LBA, Volume state, Volume flags, Volume size (GB), Volume id, Disk id, Disk number, Disk vendor, Disk product id, Disk revision, Disk max LBA, Disk state, Disk flags, Disk sync state, Disk size (GB).

mg

Flavor	Description
default	Show management sessions info: administrator username currently connected, Windows domain name of the administrator PC or its IP address, and general Checkpoint Management server info like Product Name, Major/Minor versions, Build number, whether started or not, status (`OK`).
log_server	Log server stats and info: Log Receive Rate, Log Receive Rate Peak, Log Receive Rate Last 10 Minutes, Log Receive Rate Last Hour, Log Server Connected Gateways, their state (`connected`/`not connected`), Last Login Time, Log Receive Rate.

Flavor	Description
indexer	Log Indexer stats: Total Read Logs, Total Updates and Logs Indexed, Total Read Logs Errors, Total Updates and Logs Indexed Errors, Updates and Logs Indexed Rate, Read Logs Rate, Updates and Logs Indexed Rate (10min), Read Logs Rate (10min), Updates and Logs Indexed Rate (60min), Read Logs Rate (60min), Updates and Logs Indexed Rate Peak, Read Logs Rate Peak, Read Logs Delay.

fg

Flavor	Description
all	QOS version, kernel build, QOS Policy name, QOS Policy install time, interface table with statistics for average Bps/conns/packets, per interface limits.

https_inspection

Flavor	Description
default	State of HTTPS Inspection: On/Off.
hsm_status	Status of Hardware Security Module (HSM): Enabled/Disabled, HSM partition access, status for outbound HTTPS Inspection: HSM on/HSM off/HSM error.
all	Combined output from `default` and `hsm_status` flavors.

antimalware

Flavor	Description
default	Status of the antimalware blade (0 - disabled, 1 - enabled).
subscription_status	Subscription status for each Anti-Bot/Anti-Virus/Anti-Spam component. Info includes status, expiration date, description.

Flavor	Description
update_status	Antimalware blade updates status for Anti-Bot/Anti-Virus/Anti-Spam. The info includes status (`up to date`), Database version, package date, whether the next update is scheduled to run.
ab_prm_contracts	Anti-Malware premium contracts information: contract state, update status, DB version.
av_prm_contracts	Anti-Virus premium contracts information: contract state, update status, DB version.
scanned_hosts	Statistics for number of Scanned Hosts for Hour/Day/Week. Stats for number of Infected Hosts for Hour/Day/Week.
scanned_mails	Number of scanned mails.

dlp

Flavor	Description
default	DLP status code.
dlp	Version, License status, LDAP Status, Traffic scans, DLP incidents, Scanned e-mails, E-mail incidents, Last E-mail scan, Quarantined messages, Size of quarantined messages, Sent e-mails, Expired e-mails, Discarded e-mails, Postfix queue length, Postfix errors, E-mails in queue older than 1 hour, Size of messages in queue, Free space in queue, Free space for quarantine, Quarantine status, HTTP scans, HTTP incidents, HTTP last scan, FTP scans, FTP incidents, FTP last scan, Bypass status, UserCheck clients, Last policy install status, Last scan time.
fingerprint	Fingerprint Current/Completed Tables DB info: Repository Id, Data Type Uid,Repository Root Path, Scan Id, Start Time, Repository Total Size, Repository Files, Repository Total Files Scanned, Duration,Status, Status Description, Repository Total Directories, Repository Unreach Total Directories, Fingerprinted Total Files, Total Skipped Files, Total Scanned Directories, Total Errors, Description, Data type name, Next Scheduled Scan Date.

Flavor	Description
exchange_agents	Status of Exchange agents: Name, Status, Total messages, Total scanned, Dropped, Uptime, Time since last message, Agent queue length, Exchange queue length, Avg. time per message, Avg. time per scanned message, Version, CPU usage, Memory usage, Policy timestamp.

ctnt - Content Awareness

Flavor	Description
default	Is Content Awareness blade active: True/False. Total files scanned, total data types detected.