Fortianalyzer diagnose and debug cheat sheet

Table of Contents

General Health

Command	Description
get sys status	Get general information: firmware version, serial number, ADOMs enabled or not, time and time zone, general license status (Valid or not).
get sys performance	Detailed performance statistics: CPU load, memory usage, hard disk/flash disk used space and input/output (`iostat`) statistics.
exe top	Display real time list of running processes with their CPU load.
diag log device	Shows how much space is used by each device logging to the Fortianalyzer, including quotas.
exe iotop -b -n 1	Display and update every 1 second READ/WRITE statistics for all the processes.
dia sys process list	list running processes, like `ps aux` in Linux.
dia sys process kill <kill signal> <process id>	Kill a process by its pid. Kill signal can be word or numeric, e.g. `dia sys process kill 9 27034`.
diagnose system print cpuinfo	Display hardware CPU information - vendor, number of CPUs etc.
diagnose hardware info	Even more hardware-related info.
diagnose system print df	Show disk partitions and space used. Analog of the Linux `df`.
exe lvm info	Shows disks status and size
diagnose system print loadavg	Show average system load, analog to the Linux `uptime` command.

Command	Description
dia sys print uptime	Show FAZ uptime.
dia sys admin-session <list/status/kill>	List, kill admin session(s).
dia sys ntp status	Show NTP status: IP of the NTP server synchronized to, its startum, etc.
dia dvm check-integrity	Check objects db integrity.

Communication debug

Command	Description
diagnose system print netstat	Show established connections to the Fortianalyzer, as well as listening ports. Every logging device can (and usually does) have multiple connections established.
diagnose system route list, **diagnose sys route6 list**	Show routing table
diagnose test application oftpd 3	List all devices sending logs to the Fortianalyzer with their IP addresses, serial numbers, *uptime* meaning connection establishment uptime, not remote device uptime, and packets received (should be growing).
diagnose debug application oftpd 8 <*Device name*> **diagnose debug enable**	Real time debug of communicating with the *Device name* device.
diagnose sniffer packet any "host *IP of remote device*"	Sniff packets from/to remote device, to make sure they are sending each other packets. The communication is encrypted.
diagnose sniffer packet any "port 514"	Sniff all packets to/from port 514 used by Fortianalyzer to receive logs from remote devices.

Logs from devices

Command	Description
diagnose test application oftpd 50	Show log types received and stored for each device.
diag log device	Shows how much space is used by each device logging to the Fortianalyzer, including quotas.

Command	Description
diagnose fortilogd lograte	Show in one line last 5/30/60 seconds rate of receiving logs.
diagnose fortilogd lograte-adom all	Show as table log receiving rates for all ADOMs aggregated per device type (i.e. rate for all Fortigates will be as one data per ADOM).
diagnose fortilogd lograte-device	Show average logs receive rate per device for the last hour, day, and week.
diagnose fortilogd lograte-total	Show summary log receive rate for all devices on this Fortianalyzer.

Disk and RAID health

Command	Description
diagnose sys raid status	General health of the RAID: RAID level used, RAID status, RAID size, health status of each physical disk in the RAID.
dia sys raid hwinfo	Detailed RAID controller info: IDs, slot numbers, link speed, media type, temperature, error counters, and more.
dia sys disk info	General physical disks info: model and maker for each physical disk, s/n, speed (RPM), media type, ATA/SATA versions supported.
dia sys disk health	Health state of the disks as read from S.M.A.R.T. info, greatly depends on the S.M.A.R.T. level support by the disk.
dia sys disk error	History of all errors along with the time of occurrence.
dia sys disk usage	Lists all folders (a lot) of the filesystem with their sizes on disk. Also available on VM FAZ.
dia sys flash list	List FAZ image stored in the flash, e.g.

Licensing

Command	Description
diagnose dvm device list	Look for the line *There are currently N devices/vdoms count for license*.

Command	Description
diagnose debug vminfo	Show report on Virtual Machine license: whether valid or not, type, licensed storage volume, licensed log receive rate, licensed maximum device count.
dia license list	List all applied lcienses on this FAZ.