

# Fortianalyzer diagnose and debug cheat sheet

[General Health](#)

[Communication debug](#)

[Logs from devices](#)

[Licensing](#)

## General Health

Command	Description
<b>get sys status</b>	Get general information: firmware version, serial number, ADOMs enabled or not, time and time zone, general license status (Valid or not).
<b>get sys performance</b>	Detailed performance statistics: CPU load, memory usage, hard disk/flash disk used space and input/output ( <b>iostat</b> ) statistics.
<b>exe top</b>	Display real time list of running processes with their CPU load.
<b>diag log device</b>	Shows how much space is used by each device logging to the Fortianalyzer, including quotas.
<b>exe iotop -b -n 1</b>	Display and update every 1 second READ/WRITE statistics for all the processes.
<b>diagnose system print cpuinfo</b>	Display hardware CPU information - vendor, number of CPUs etc.
<b>diagnose hardware info</b>	Even more hardware-related info.
<b>diagnose system print df</b>	Show disk partitions and space used. Analog of the Linux <b>df</b> .
<b>exe lvm info</b>	Shows disks status and size
<b>diagnose system print loadavg</b>	Show average system load, analog to the Linux <b>uptime</b> command.
<b>diagnose system print netstat</b>	Show established connections to the Fortianalyzer, as well as listening ports. Every logging device can (and usually does) have multiple connections established.
<b>diagnose system print route</b>	Show routing table of the Fortianalyzer.

# Communication debug

Command	Description
<b>diagnose test application oftpd 3</b>	List all devices sending logs to the Fortianalyzer with their IP addresses, serial numbers, <i>uptime</i> meaning connection establishment uptime, not remote device uptime, and packets received (should be growing).
<b>diagnose debug application oftpd 8 &lt;Device name&gt;</b>  <b>diagnose debug enable</b>	Real time debug of communicating with the <i>Device name</i> device.
<b>diagnose sniffer packet any "host IP of remote device"</b>	Sniff packets from/to remote device, to make sure they are sending each other packets. The communication is encrypted.
<b>diagnose sniffer packet any "port 514"</b>	Sniff all packets to/from port 514 used by Fortianalyzer to receive logs from remote devices.

## Logs from devices

Command	Description
<b>diagnose test application oftpd 50</b>	Show log types received and stored for each device.
<b>diag log device</b>	Shows how much space is used by each device logging to the Fortianalyzer, including quotas.
<b>diagnose fortilogd lograte</b>	Show in one line last 5/30/60 seconds rate of receiving logs.
<b>diagnose fortilogd lograte-adom all</b>	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).
<b>diagnose fortilogd lograte-device</b>	Show average logs receive rate per device for the last hour, day, and week.
<b>diagnose fortilogd lograte-total</b>	Show summary log receive rate for all devices on this Fortianalyzer.

## Licensing

Command	Description
<b>diagnose dvm device list</b>	Look for the line <i>There are currently N devices/vdoms count for license.</i>
<b>diagnose debug vminfo</b>	Show report on Virtual Machine license: whether valid or not, type, licensed storage volume, licensed log receive rate, licensed maximum device count.