BOLL
IT Security Distribution

CHEATSHEET

FORTIANALYZER FOR 6.4

© BOLL Engineering AG, Cheat Sheet 1.1 10.08.2021)

General

Default Device Information

`admin / no password`	Default login
`192.168.1.99`	Default IP on port1, internal or MGT
`9600/8-N-1 / hardware flow control disabled`	Default serial console settings

System

Server Information

`get system status`	Status of FAZ device
`get system performance`	FAZ performance statistics
`diag system print [option]`	View different server information
`diag hardware info`	Hardware statistics for CPU, memory, disk and RAID
`diag dvm supported-platforms list`	Lists supported Forti-Devices (models and firmware versions)

Reset Information

`exec reset all-settings`	Erases configuration on flash
`exec reset all-except-ip`	Erases the configuration on flash, leaves the settings for IP and routes
`exec format disk`	Formats Log disk

Backup / Restore

`exec backup <all-settings|logs|reports> …`	Creates backup via FTP/SFTP/SCP
`exec restore <all-settings|logs|reports> …`	Restores a backup via FTP/SFTP/SCP
`exec migrate all-settings …`	For migration between different models (system settings are not migrated!)

High Availablity

`diag ha status`	Show HA status
`diag ha stats`	Show HA statistics
`diag ha failover`	Run on master, force HA failover
`diag ha force-cfg-resync`	Force HA to re-sync configuration
`diag ha restart-init-sync`	Run on master, restart HA initial sync
`diag ha load-balance`	Show HA load-balance status

Disk

Disk / RAID / Virtual Disk

`config system locallog disk setting`
`set diskfull nolog/overwrite`
	What happens with oldest logs

`diag system raid [option]`
`status, hwinfo, alarms`
	RAID information

`diag system disk [option]`
`info, health, errors, attr`
	Disk information

`exec lvm info`	provides a list of available disks (VM)
`exec lvm extend <disk nr.>`	Add disk (VM)

Network

Network Troubleshooting

`exec ping/traceroute [host]`	Ping / Traceroute utility
`show system route`	Displays routing table
`diag sniffer packet <if> <filter> <level> <timestamp>`	Packet sniffer

`conf sys fortiview settings`
`set resolve-ip enable`
	Resolve IP address to hostname

ADOM

ADOM operation

`config system global`
`set adom-status [ena/dis]`
	ADOM settings
	Enable or disable ADOM mode

`config system global`
`set adom-mode [normal/adv]`
	Set ADOM mode to normal or advanced /for VDOMs)

`config system global`
`set adom-select [ena/dis]`
	Displays ADOM window after login

`diag test appl oftpd 3`	Lists connected devices and IPs
`diag dvm adom list`	Lists enabled and configured ADOMs
`diag dvm device list`	Lists currently registered and unregistered devices/VDOMs
`execute sql-local rebuild-adom <ADOM-name>`	Rebuild ADOM database

Authentication Group

`config sys admin group`
`edit <new-group>`
	Group authentication server

Logging

Log Forwarding

`config system log-forward`
`edit <id>`
`set mode <realti, aggr, dis>`
	Forwarding logs to FortiAnalyzer / Syslog / CEF

`conf sys log-forward-service`
`set accept-aggregation ena`
	Configure the FortiAnalyzer that receives logs

Log Encryption

`config log fortianalyzer setting → set enc-algorithm {high*|high-medium|low}`	FortiGate's encryption level

`config system global`
`set enc-alg {high*|med|low}`
	FortiAnalyzer's encryption level

`config system global`
`set log-checksum …`
	Configure FAZ to record log file hash, timestamp and authentication code

Log Settings on Fortigate

`configure log fortianalyzer setting/filter`	Logging commands on FortiGate
`diag log test`	Generates dummy log messages
`diag test appl miglogd 6`	Dumps statistics for log daemon
`diag log kernel-stats`	Sent and failed log statistics
`exec log fortianalyzer test-connectivity`	Test connection to FortiAnalyzer

Log Troubleshooting

`diag test appl oftpd 8`	Daemon for receiving logs
`diag test appl logfiled 2`	Log file-related activitites
`diag log device`	Used disk space per ADOM
`diag system print df`	Logs and system files on drive
`diag fortilogd lograte[-…]`	Log receive rate per second
`diag fortilogd msgrate[-…]`	Message receive rate per second

Reporting

Hard Cache

`diag sql status sqlreportd`	SQL query conn and hcache status
`diag sql show hcache-size`	Hcache size on the file system
`diag test application sqlrptcached <level>`	State of the hcache
`diag test appl sqlreportd 2`	Diagnose hcache creation
`exec sql-report hcache-build <ADOM-name> <schedule-name> <start-time> <end-time>`	Rebuild hcache
`exec sql-report list-schedule <ADOM-name>`	View report grouping information

Database

`diag sql process list`	Current SQL processes running
`diag sql status sqlplugind`	SQL insertion status