Cheat Sheet

FortiAnalyzer
FortiManager
for version 7.4

The cheat sheet from BOLL. Here you can find all important CLI commands for the operation and troubleshooting of FortiAnalyzer and FortiManager for version 7.4.

General

Default Device Information

admin / no password	Default login
192.168.1.99	Default IP on port1 or mgmt port
9600/8-N-1 hardware flow control disabled	Default serial console settings

Reset Information

exec reset all-settings	Erases the configuration on flash, containing IP and routes
exec reset all-except-ip	Erases the configuration but preserves IPs and routes
exec format disk	Erases device settings, images, databases, and log data on disk, but preserves IPs and routes
diag cdb upgrade summary	Upgrade history

Server Information

get system status	General device status
get system performance	Performance statistics
diag system print [option]	View different server information
diag hardware info	Hardware statistics for CPU, memory, disk and RAID

Network

exec ping [host]	Ping utility
exec traceroute [host]	Traceroute utility
diag sniffer packet <interface> <filter> <level> <timestamp>	Packet sniffer
diag sniff packet any 'port 514' 4	Sniffer for log traffic
config sys fortiview settings set resolve-ip enable	Resolve IP address to hostname

Disk / RAID / Virtual Disk

config sys locallog disk setting set diskfull nolog/overwrite	What happens with oldest logs
diag system raid [option]	RAID information
diag system disk [option]	Disk information
exec lvm info	list of available disks (VM)
exec lvm extend <disk nr.>	Add disk (VM)
diag sys fsck harddisk	Check and repair file system after crash or power loss

Process Information

get system performance status	General performance infos
diag debug crashlog history	Crash statistics
diag debug crashlog read	Crash log
exec top	CPU/Memory intense processes Sort with P (CPU) / M (Memory)
exec iotop	Processes with high I/O

Firmware Upgrade Order

FortiAnalyzer → FortiManager → FortiGate

FortiAnalyzer Logging

Device and ADOM Operation

config system global set adom-status [en/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 [en/dis]	Displays ADOM window after login
diag dvm adom list	Enabled and configured ADOMs
diag dvm device list	Currently registered and un-registered devices and VDOMs
diag test appl oftpd 3	Currently connected devices/IPs
diag test appl oftpd 9	Currently unregistered devices
exec reset adom-settings <ADOM name> 6 4 0	Reset the ADOM version to 6.4
exec device replace sn <devname> <new sn>	Replace device with new device

Log Forwarding

config system log-forward edit <id> set mode <realtime, aggr, dis>	Forwarding logs to FortiAnalyzer / Syslog / CEF
conf sys log-forward-service set accept-aggregation enable	Configure the FortiAnalyzer that receives logs

Log Backup

exec backup logs <device|all> <ftp|sftp|scp> <serverip> <user> <password> <location on server>	Backup logs to external storage
exec restore <options>	Restore commands

Log Encryption

config log fortianalyzer setting set reliable enable set enc-alg {high-med|high*|low}	FortiGate's encryption level
config sys global set enc-alg {high* | med | low}	FortiAnalyzer's encryption level
config system global set log-checksum {md5 | md5-auth | none}	Configure FAZ to record log file hash value/timestamp and authentication code

Log Settings on FortiGate

config log fortianalyzer setting config log fortianalyzer filter	Logging commands on FortiGate
diag log test	Generates dummy logmessages
diag test appl miglogd 6	Dumps statistics for log daemon
diag test appl fgtlogd 4	Logging statistics, cache size
diag log kernel-stats	Sent and failed log statistics
exec log fortianalyzer test-connectivity	Test connection to FortiAnalyzer

Log Troubleshooting

diag debug appl oftpd 8	Daemon for receiving logs
diag test appl logfiled 2	Log file-related activities
diag log device	Used disk space per ADOM
diag system print df	Logs and system files on drive
diag fortilogd lograte / -total	Log receive rate
diag fortilogd lograte-device/-type	Log receive rate per device/type
diag fortilogd lograte-adom	Log rate for all/specific ADOM
diag fortilogd logvol-adom	Log volume for all/spec. ADOM
diag fortilogd msgrate / -total	Message rate
diag fortilogd msgrate-device/-type	Message rate per device/type

Cheat Sheet

FortiAnalyzer
FortiManager
for version 7.4

FortiAnalyzer 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 appl 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
exec sql-local rebuild-adom <ADOM-name>	Rebuild ADOM database

FortiAnalyzer HA

HA	
diag test appl oftpd 81	Show HA info
diag ha status / stats	Show HA status / statistics
diag ha failover	Run on master, force failover
diag ha load-balance	Shows HA load balance status
diag ha force-cfg-resync	Force HA to resync config
diag ha restart-init-sync	Run on master, restart HA initial sync

FortiManager

Configuration	
diag dvm device list	Currently registered and unregistered devices / VDOMs
config system admin setting set mgmt-addr <FMG NAT-addr> set auto-update disable set show_schedule_script enable	Set FMG NATed-IP if setup is behind a firewall / NAT device & disable automatic update on FGT configuration change & enable to schedule scripts
config system dm set fgfm-sock-timeout <sec> set fgfm_keepalive_itvl <sec> set rollback-allow-reboot enable	Adjust FGFM tunnel timeouts and ttl as well as enable FGT-reboot recovery logic on tunnel disconnect
config system global set workspace-mode [disabled / normal / per-adom / workflow]	Enable workspace or workflow session-based administration

Replacement of devices	
exec device replace sn <devname> <new sn>	Replace device with new device
exec fgfm reclaim-dev-tunnel <optional device name>	Reclaim tunnel (optional)
exec device replace pw <device name> <password>	(optional)

Backup FortiManager	
diag dvm check-integrity diag cdb check adom-integrity diag cdb check adom-revision diag cdb check policy-package diag cdb check update-devinfo	Logoff all admins, unlock ADOMs and create FMG backup before executing database checks
diag dvm lock	check for unexpected, locked proceses
diag dvm proc list	check for stuck process or task

Management Settings on FortiGate	
conf system central-management set type fortimanager set fmg <FortiManager IP>	FortiGate configuration for linking FGT to model-device
exec central-mgmt register-device <fmg-serial-no> <fmg-register-password>	Run on FGT to link model device to real device

Troubleshooting FortiGuard	
exec ping fds1.fortinet.com	Verify DNS to FortiGuard
FDS (fdslinkd) FGD (fgdlinkd) FCT (fctlinkd) FDN	FortiGate AV/IPS FortiGate Web-/Email filter FortiClient AV/IPS FortiGuard Distribution Network
diag fmupdate view-serverlist [fds/fgd]	Show list of available update servers per service
diag fmupdate update-status [fds/fct/fgd]	Display update status per FortiGuard service
diag fmupdate dbcontract <optional device serial number>]	Verify FortiGate contract information on FMG

Troubleshooting ADOM Databases	
exec fmpolicy print-adom-package <adom> < template type> <package> <category>	Troubleshoot provisioning templates
exec fmpolicy print-device-database <adom> <device >	Display device configuration
exec fmpolicy print-device-object <adom> <device> <vdom> <category>	Display individual object configuration
exec fmpolicy print-adom-database <adom_output_file>	Display entire ADOM database
exec fmpolicy print-adom-package <adom> <policy/template> <package> <category> <object>	Display firewall policies on policy package
exec fmpolicy print-adom-object <adom> <category>	Display individual ADOM object

Troubleshooting	
diag debug application fgfmd 255 diag debug enable	Show keepalive communication including checksum information and IPS version
diag sniff packet any 'port 541' 4	Sniffer for management traffic
diag fgfm session-list	Verify tunnel uptime, display connecting IP and link-level addresses.
diag sys admin-session list diag sys admin-session kill <session_id>	Show currently logged-in admins and kill command to delete admin with “session_id”
diag debug service cdb 255 diag debug enable	ADOM upgrade: Show realtime debug output during upgrade
exec fmprofile [export-profile / import-profile] <ADOM name> <profile name> <output file>	Perform profile related actions.
diag deb appl devmanager 255 diag debug enable	real-time info of FGT being added in Add-Device-Wizard and debug script execution
exec fmscript clean-sched	Delete scripts which are assigned to deleted devices
diag test deploymanager reloadconf <devid>	Shows info about config reload to update device-level db

Something missing?

Please contact us for comments, corrections or ideas regarding our cheat sheet at support@boll.ch