Cheat Sheet

FortiAnalyzer
FortiManager
for version 7.0

The cheat sheet from BOLL. Here you can find all important CLI commands for the operation and troubleshooting of FortiAnalyzer and FortiManager for version 7.0.

BOLL
IT Security Distribution

General

Default Device Information	
admin / no password	Default login
192.168.1.99	Default IP on port1 or management 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 leaves the settings for IP and routes
exec format disk	Formats Log disk

Server Information	
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
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] 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)
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

HA Information	
diag ha force-resync	On primary resync to all members, on secondary resync only this member

FortiAnalyzer Logging

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
execute sql-local rebuild-adom <ADOM-name>	Rebuild ADOM database

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 name|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 enc-algorithm {default*|high|low|disable}	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 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 sniff packet any 'port 514' 4	Sniffer for Syslog Traffic
diag test 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	Log receive rate per second
diag fortilogd msgrate	Message rate per second
diag fortilogd msgrate-total	Message rate in total
diag fortilogd msgrate-device	Message rate per devicee
diag fortilogd msgrate-type	Message rate for each log type

Cheat Sheet

FortiAnalyzer
FortiManager
for version 7.0

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 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

FortiManager

Configuration	
diag dvm device list	Currently registered and unregistered devices / VDOMs
config system admin setting set mgmt-addr <FMG NATed IP address>	Set FMG NAT-IP if setup is behind a firewall / NAT device
config system dm set fmfm-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 [enabled / normal / workflow]	Enable workspace or workflow session based administration

Replacement of devices	
exec device replace sn <devname> <new serialnum>	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 diag dvm lock → check for unexpected, locked proceses diag dvm proc list → check for a stuck process or task	Logoff all admins, unlock ADOMs and create FMG backup before executing database checks

Management Settings on FortiGate	
config system central-management set type fortimanager set fmg <FortiManager IP> end	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	
FDS (fdslinkd) FGD (fgdlinkd) FCT (fctlinkd) FGC (fgclinkd) FDN	FortiGate AV/IPS FortiGate Web-/Email filter FortiClient AV/IPS Forticlient Web-/Email filter FortiGuard Distribution Network
diag fmupdate view-serverlist [fds|fct|fgd|fgc|fmtr]	Show list of available update servers per service
diag fmupdate dbcontract [<optional fds|fgd> <optional device serial number>]	Verify FortiGate contract information on FMG
det system fortiguard-service status	Shows version, last update, contract expiration date
diag debug application update -1 diag debug enable exec update-now	Show realtime output of the update-now process and details on all FortiGates downloading updates from FMG

Troubleshooting ADOM Databases	
exec fmpolicy print-adom-package <ADOM> <System template type> <package> <category>	Troubleshoot provisioning templates
exec fmpolicy print-device-database <adom_name> [device_name>	Display device configuration
exec fmpolicy print-device-object <adom_name> [device_name> <vdom_name> <category_name>	Display individual object configuration
exec fmpolicy print-adom-database <adom_output_filename>	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 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 debugging: generates realtime log entries during upgrade
exec fmprofile [export-profile/import-profile] <ADOM name> <profile name> <output file name>	Perform profile related actions.
diag debug application depmanager 255 diag debug enable	Obtain real-time status of the FortiGate device being added in Add-Device-Wizard and debug script execution in real time
exec fmscript clean-sched	Delete scripts which are assigned to deleted devices
config system admin setting set show_tcl_script enable end	Enable TCL scripts to be executed on FMG
diag test deploymanager reloadconf <devid> (use Device ID from "diag dvm device list")	Shows which stage config reload is failing to update device-level db.

Version: 23.11.2021

BOLL