BOLL
IT Security Distribution

CHEATSHEET

FORTIANALYZER FOR 6.0

General

Default device information	
admin / [no password]	Default login
192.168.1.99/24	Default IP on port1
9600/8-N-1 hardware flow control disabled	Default serial console settings

Basic commands	
get system status	Current status of FortiAnalyzer
show system interface	Displays the network interface configuration
show system route	Displays static routing table entries
show system dns	Displays DNS server address
show system ntp	Displays automatic time settings using a network time protocol (NTP) server
get system ntp	Displays how often FortiAnalyzer synchronizes its time with the NTP server
execute shutdown / restart	Shutdown and Restart command

Server information	
get system performance	FortiAnalyzer performance statistics
diagnose system print [option] certificate, cpuinfo, df, hosts interface, loadavg, partitions, route, rtcache, slabinfo, sockets, uptime, netstat	View different server information
diagnose hardware info	Hardware statistics for CPU, memory, disk and RAID

Reset Information	
execute reset all-settings	Erases the show configuration on flash, containing IP and routes
execute reset all-except-ip	Erases the configuration on flash, leaves the settings for IP and routes
execute format disk	Formats Log disk

Network

Network Troubleshooting	
execute ping [host]	Ping utility
execute traceroute [host]	Traceroute utility
diag sniffer packet <interface> <filter> <level> <timestamp>	Packet sniffer
config system fortiview settings set resolve-ip enable	Resolve IP address to hostname

Logging

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

Log Backup	
execute backup logs <device name | all> <ftp | sftp | scp> <server ip> <user name> <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 system global set enc-algorithm {high | medium | low*}	FortiAnalyzer's encryption level
config system global set log-checksum {md5 | md5-auth | none}	Configure FortiAnalyzer to record log file hash value, timestamp and authentication code

Logging settings on Fortigate	
configure log fortianalyzer setting / filter	Logging commands on FortiGate
diagnose log test	Generates several dummy log messages
diagnose test appli miglogd 6	Dumps statistics for log daemon
diagnose log kernel-stats	Sent and failed log statistics
execute log fortianalyzer test-connectivity	Test connection to FortiAnalyzer

Logging Troubleshooting	
diagnose test application oftpd 8	Daemon for receiving logs
diagnose test application logfiled 2	Log file-related actitivites
diagnose log device	Used disk space per ADOM
diagnose system print df	Logs and all system files on mounted drive
diagnose fortilogd lograte	Log receive rate per second
diagnose fortilogd msgrate	Message receive rate per second
diagnose fortilogd msgrate-total	Message receive rate totals
diagnose fortilogd msgrate-device	Device message rate
diagnose fortilogd msgrate-type	Message rate for each log type

Disk

Disk / RAID / Virtual Disk	
config system locallog disk setting set diskfull nolog / overwrite	What happens with oldest logs
diagnose system raid [option] status, hwinfo, alarms	RAID information
diagnose system disk [option] info, health, errors, attributes	Disk information
execute lvm info	For virtual machines: provides a list of available disks
execute lvm extend <disk nr.>	For virtual machines: Add disk

ADOM

ADOM operation	
config system global set adom-status [en/dis]	ADOM settings Enable or disable ADOM mode
config system global set adom-mode [normal/advanced]	Set ADOM mode to normal or advanced / for VDOMs)
config system global set adom-select [en/dis]	Displays ADOM window after login
diagnose dvm adom list	Enabled and configured ADOMs
diagnose dvm device list	Currently registered and unregistered devices and VDOMs
execute sql-local rebuild-adom <ADOM-name>	Rebuild ADOM database

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

Reporting

Hard cache	
diagnose sql status sqlreportd	SQL query connections and hcache status
diagnose sql show hcache-size	Hcache size on the file system
diagnose test application sqlrptcached <level>	State of the hcache
diagnose test application sqlreportd 2	Diagnose hcache creation
execute sql-report hcache-build <ADOM-name> <schedule-name> <start-time> <end-time>	Rebuild hcache
execute sql-report list-schedule <ADOM-name>	View report grouping information

Database	
diagnose sql process list	Current SQL processes running
diagnose sql status sqlplugind	SQL insertion status

Report errors, suggestions or comments to info@boll.ch

BOLL
IT Security Distribution