Fortigate CLI Reference - v 1.0.5

by André Otta - andreotta@gmail.com

System

get system status	basic infos about system SN included
exec date	show system date
exec time	show system time
diag autoupdate versions	show versions of engines
exec reboot	reboot the fortigate
exec shutdown	shutdown the fortigate
diag debug config-error-log read	show errors who are happened when load the config file

Performance

get system performance status	show performance usage and fw uptime
diag sys top 2 50	show top from 50 processes updating every 2 secs.
diag sys top-sum	show top grouped processes
diag hardware sysinfo shm	show shared memory information

High Availability

get sys ha status	show HA status		
get sys checksum status	show HA checksum		
exec ha manage <ha_unit_index>	manage other cluster member/ type ? instead of index to show all Ids		
diag sys ha hadiff status	show HA diff		
diag sys ha reset uptime	change the cluster active member		
diag sys ha cluster-csum		<5.2	Show sync checksum
diag sys ha checksum cluster		5.4 >	Show sync checksum
diag sys ha checksum cached (vdom or root)		5.4 >	Tshoot sync problems
diag sys ha ckecksum recalculate <vdom name | globa	force a checksum recalculation (sometimes this can solve sync proble		
diag sniffer packet any "ether proto 0x8890" 4	Sniffer HA heartbeat packets		
diag debug app hatalk -1			
diag debug app hastalk -1			
diag debug app hasync -1			
diag debug em			

VPN Ipsec

get vpn ipsec tunnel summary	list all ipsec tunnels
get vpn ipsec tunnel details	list details of ipsec tunnels
diag vpn ipsec tunnel list	list details of ipsec tunnels
diag vpn tunnel flush <p1 name>	flush tunnel Sas
diag vpn tunnel reset <p1 name>	flush tunnel Sas and reset NAT-T and DPD confs
diagnose vpn ike restart	Be careful! This command restart all tunnels.
diag debug reset	We need to run this 2 commands before all debug commands
diag debug enable (after finish always run disable)	
diag debug app ike -1	More common debug, show mismatch in PSK or in VPN phases
diag debug app ike 255	Output VPN handshaking.

User authentication

diag debug reset	We need to run this 2 commands before all debug commands	
diag debug enable (after finish always run disable)		Debug LDAP or Radius
diag debug application fnbamd -1		Option -1 enables all debug output
diag debug authd fsso list		Show FSSO authenticated users

Failure Troubleshooting

exec tac report	generate a TAC report with a lot of info
diag debug crashlog read	shows the crashlog in a readable format

Resseting a lost admin password

1. Connect a console cable to Fortigate
2. Run putty.exe with default settings
3. When the firewall respond with its hostname
4. Reboot the firewall
5. You have 30 seconds after shows the login again to use the recovery credencials
6. Back in login screen, type username: **maintainer**
7. The password is **bcpb+ serial no. of the firewall (ex: bcpbFGT60C3G10016011)**
8. Now you should be connected to the firewall
9. Change the admin password

```
config sys admin
edit admin
    set password XXXXXXXXX
end
```

10. Password changed

Network

get system arp	show fortigate arp table	
exec ping-options <source>	source = fortigate interface ip	
exec ping <host>	execute a ping	
exec traceroute <destination>		
exec traceroute-options <srcip> or <device>		
show system interface <port x>	show fortigate specific interface	
show system interface	show all fortigate interfaces	
diag hardware nic device info <port x>	show detailed infos about interface like errors/drops/packets	
diag sys session list	list active sessions	Filter options:
diag sys session filter src <ip>	filter active sessions of na specific IP	sintf Source interface.
diag sys session list	list active sessions from the filtered IP	dintf Destination interface.
diag sys session clear	clear active session from the filtered IP	src Source IP address.
		nsrc NAT'd source ip address
		dst Destination IP address.
		proto Protocol number.
		sport Source port.
get router info routing table all	show the (active) routing table	
get router info routing-table database	show the routing table with the worst routes too	
diag sniffer packet <interface> <filter> 3	verbose level 3: print header and data from Ethernet of packets	
diag sniffer packet <interface> <filter> 4	verbose level 4: print header of packets with interface name	
<filter> can be src host, dst host, host, arp, tcp ports, protocols and etc.		
More infos: http://kb.fortinet.com/kb/viewContent.do?externalId=11186		
get router info vrrp	show vrrp state, vrip, priority, vmac, etc.	
diag firewall fqdn list	show the resolved FQDNS objects	
diag sys link-monitor status	show status of links with link-monitor configured	

Network - Internet service database

Fortigate has a collection of IP Addresses and ports realted to applications over internet, working in a granularity of application control.

diagnose internet-service id | grep <application>	show the id of an specific application
diagnose internet-service id-summary <id>	show details (ip addresses and ports) related to this app

Network - Debug FLOW

diagnose debug disable	We need to run togheter, first clean old debugs, next apply a new one.
diagnose debug flow trace stop	It's possible to use only saddr or daddr instead of both.
diagnose debug flow filter clear	
diagnose debug reset	For more filters: diagnose debug flow filter ?
	proto Protocol number.
diagnose debug flow filter saddr x.x.x.x	addr IP address.
diagnose debug flow filter daddr x.x.x.x	saddr Source IP address.
diagnose debug flow show console enable	daddr Destination IP address.
diagnose debug flow show function-name enable	port port
diagnose debug flow show ipprobe enable	sport Source port.
diagnose debug console timestamp enable	dport Destination port.
diagnose debug flow trace start 999	negate Inverse filter.
diagnose debug enable	

Network - BGP

get router info bgp summary	Show summary info like AD, UP/Down info.
get router info bgp neighbors	Show neighbors informarion

Webfilter

diag debug urlfilter src-addr <host_IP_address>	Filtering by an specific IP, you can see details of the websites in realtime.
diag debug app urlfilter -1	Debug level (-1 shows all infos) It's very important to disable the debug, because consumes
diag debug enable	fortigate resources.

IPS

diag ips anomaly list	show details about DoS Policy
diag test application ipsmonitor <XX>	
1: Display IPS engine information	To tshoot you can run the commands with 1, 10 , 13 and finally 99 to restart.
10: IPS queue length	These diags collect some valuable information.
13: IPS session list	
97: Start all IPS Engines	
98 : Stop all IPS Engines	
99: Restart all IPS engines and monitor	

IMPORTANT

- Do not forget to disable the debugs, because consumes fortigate resources.
- In HA clusters the primary has the better priority.
- High CPU can cause HA problems.