HCX Central CLI User Guide

Table of Contents

About this Guide

This document is the user guide for Central CLI in release 3.5. The purpose of Central CLI is to diagnose the managed WAN Interconnect Gateway without log into them over console/SSH.

There is no extra firewall rule required except the standard 9443 for RESTful channel. Once Remote Access mode is enabled, user can even SSH into the CGWs from management plane directly for advanced diagnostic.

Intended Audience

This document is intended for operators of the HCX service.

Support Resources

Please reach out to your assigned support channels to get further assistance.

Common

Start, Exit and Help

Central CLI can be started with admin user, simply like below. Type "**exit**" command or twice CtrlC to quit CCLI.

```
/dev$ ssh admin@<hcx-mgmt-ip>
Password:

[admin@onpremhcm1 ~]$ ccli
[admin@onpremhcm1] exit

[admin@onpremhcm1 ~]$ ccli
[admin@onpremhcm1] ^C

Input Ctrl-c once more to exit
[admin@onpremhcm1] ^C
Interrupted
```

Postfix "--help" after a command can print out the help information for a given command, which contains subcommands available and flags available.

```
[admin@onpremhcm1] show config --help
Configuration query commands.
Usage:

Available Commands:
  cgw         Show CGW configuration.
  ipsec       Show ipsec configuration.
```

```
Flags:
  -h, --help   help for config

Global Flags:
      --nopager   Don't pipe output into a pager

Use "[command] --help" for more information about a command.
```

By default, most commands' output are paged which is friendly for console. User can use "--nopager" to turn off paging output.

```
[admin@onpremhcm1] show config ipsec --nopager
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    # strictcrlpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.der
#      leftsendcert=never
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightcert=peerCert.der
#      auto=start
```

```
#conn sample-with-ca-cert
#       leftsubnet=10.1.0.0/16
#       leftcert=myCert.pem
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightid="C=CH, O=Linux strongSwan CN=peer name"
#       auto=start
```

Configuration

When CCLI is started, it will read managed gateway appliance information from database automatically. Type "**list**" command to view the managed appliances.

```
[admin@onpremhcm1 ~]$ ccli
[admin@onpremhcm1] list
|-------------------------------------------------------------------------------|
| Id | Node                     | Address            | State     | Selected |
|-------------------------------------------------------------------------------|
| 0  | CGW_fleet2000            | 192.168.4.201:9443 | Connected |          |
|-------------------------------------------------------------------------------|
| 1  | L2C-HT-taggableDvs-UMzo8 | 192.168.4.202:9443 | Connected |          |

|-------------------------------------------------------------------------------|
```

When add/remove/redeploy the gateway appliances, you need to type "refresh" command to reload the CCLI configuration:

```
[admin@onpremhcm1] refresh
Refresh central cli configuration.
 ...reading configuration from mongodb
 Reading CGW information from mongoDB...
Compiling the CCLI configuration...
Dumping to /home/admin/.ccli file...
Preparing ssh keys and config...
Dumping to /home/admin/.ssh/config ...
```

```
Done

 ...loading configuration file [/home/admin/.ccli]
 ...refreshing managed nodes
Done.
```

CLI Commands

Central CGW Commands

The central CGW commands allow you to run a subset of available CGW commands directly from manager without switching the current CGW back and forth. Those commands have the format ***show node nodeId <keywords and arguments>*** which is equivalent of running ***show <keywords and arguments>*** on the selected CGW.

Note: TAB completion is not supported after "node nodeId" in this mode. Encourage user to select the target CGW first by "go nodeId" first.

CLI	Description	Example
show node *nodeId* info	Show basic information of specified node.	[root@VcReleaseHCM] show node 0 info
show node *nodeId* config cgw show node nodeId config ipsec	Show CGW configuration (in JSON). Show ipsec configuration.	[root@VcReleaseHCM] show node 0 config cgw [root@VcReleaseHCM] show node 0 config ipsec
show node nodeId firewall	Show Firewall table	[root@VcReleaseHCM] show node 0 firewall
show node nodeId ipsec cert show node nodeId ipsec config show node nodeId ipsec conn show node nodeId ipsec sa	Show IPSEC service information in various aspects, such as config, certificates loaded, current connections, SA/SP etc.	[root@VcReleaseHCM:CGW-IQC4A] show node 0 ipsec cert

CLI	Description	Example
show node nodeId ipsec sp show node nodeId ipsec status		
show node nodeId flow flowbalance config show node nodeId flow flowbalance state	Show flowbalance config and runtime state	[root@VcReleaseHCM:CGW-IQC4A] show node 0 flow flowbalance state
show node nodeId flow flowspec spec	Show current flows with specified flowspec query.	[root@VcReleaseHCM:CGW-IQC4A] show node 0 flow flowspec proto=tcp:dport=9443
show node nodeId log alert show node nodeId log event show node nodeId log syslog	Show /var/log/emessages, /var/log/system_events and journal logs of the CGW.	[root@VcReleaseHCM:CGW-IQC4A] show node 0 log event [root@VcReleaseHCM:CGW-IQC4A] show node 0 log syslog -u cgw -n 20
show node nodeId fou config show node nodeId fou state	Show FOU transport configuration and runtime state	[root@VcReleaseHCM:CGW-IQC4A] show node 0 fou state
show node nodeId network address show node nodeId network arp show node nodeId network route show node nodeId network socket show node nodeId network ping *target_address*	Show various network information on the CGW, such as IP addresses, ARP table, route table, socket lists. "ping" is used to do ICMP ping against the specified address.	[root@VcReleaseHCM:CGW-IQC4A] show node 0 network arp -i vNic_0 [root@VcReleaseHCM:CGW-IQC4A] show node 0 network address [root@VcReleaseHCM:CGW-IQC4A] show node 0 network ping 10.145.0.112
show node nodeId service all show node nodeId service cgw*state*|*status* show node nodeId service hbrsrv	Show the specified service runtime status. "cgw state|status" is used to display the internal config engine status.	[root@VcReleaseHCM:CGW-IQC4A] show node 0 service all [root@VcReleaseHCM:CGW-IQC4A] show node 0 service mobilityagent [root@VcReleaseHCM:CGW-IQC4A] show node 0 service cgw

CLI	Description	Example
show node nodeId service ipsec show node nodeId service lwdproxy show node nodeId service mobilityagent show node nodeId service sshd		[root@VcReleaseHCM:CGW-IQC4A] show node 0 service cgw state
show node *nodeId* system cpu show node *nodeId* system date show node *nodeId* system disk show node *nodeId* system load show node *nodeId* system memory show node *nodeId* system process show node *nodeId* system runtime	Show the system resources information.	[root@VcReleaseHCM:CGW-IQC4A] show node 0 system cpu

CGW Commands

The following table lists the CLIs available on the selected CGW over Central CLI.

TAB completion is supported for those commands.

CLI	Description	Example
list	List the managed CGWs.	[root@VcReleaseHCM] list
exit	Exit CCLI program.	[root@VcReleaseHCM] exit

CLI	Description	Example
go *node*	Select the CGW to diagnose against.	[root@VcReleaseHCM] go 0
help *cmd* --help	Show the help message. Show more information about a command.	[root@VcReleaseHCM:CGW-IQC4A] help [root@VcReleaseHCM:CGW-IQC4A] system --help
clear	Clear the screen.	[root@VcReleaseHCM:CGW-IQC4A] clear
refresh	Refresh CCLI configuration by populationg CGW information from mongodb.	[root@VcReleaseHCM:CGW-IQC4A] refresh
show info	Show basic node information (build, type etc.)	[root@VcReleaseHCM:CGW-IQC4A] show info
show config cgw show config ipsec	Show CGW configuration (in JSON). Show ipsec configuration.	[root@VcReleaseHCM:CGW-IQC4A] show config cgw [root@VcReleaseHCM:CGW-IQC4A] show config ipsec
show firewall	Show firewall table	[root@VcReleaseHCM:CGW-IQC4A] show firewall
debug coredump debug coredump *enable|disable* debug remoteaccess debug remoteacces *enable|disable* debug tcpdump *spec* debug techsupport --wanopt	Show coredump enablement status and history. Enable/Disable coredump Enable/Disable remoteacces mode "tcpdump" is used to capture packets on the CGW and fetch the pcap file back.	[root@VcReleaseHCM:CGW-IQC4A] debug coredump [root@VcReleaseHCM:CGW-IQC4A] debug coredump disable [root@VcReleaseHCM:CGW-IQC4A] debug remoteaccess enable [root@VcReleaseHCM:CGW-IQC4A] debug tcpdump -i vNic_0 -t 10 tcp and port 22 [root@VcReleaseHCM:CGW-IQC4A] debug techsupport --wanopt

CLI	Description	Example
	"techsupport" is used to get techsupport bundle from CGW. "–wanopt" option is used to fetch debugDump bundle of WanOpt associated with the CGW together.	
show flow flowbalance config show flow flowbalance state	Show flowbalance config and runtime state	[root@VcReleaseHCM:CGW-IQC4A] show flow flowbalance state
show flow flowspec *spec*	Show current flows with specified flowspec query. Flowspec format is that same as conntrackd flowspec.	[root@VcReleaseHCM:CGW-IQC4A] show flow flowspec proto=tcp:dport=9443
show fou config show fou state	Show FOU transport configuration and runtime state	[root@VcReleaseHCM:CGW-IQC4A] show fou state
show ipsec cert show ipsec config show ipsec conn show ipsec sa show ipsec sp show ipsec status	Show IPSEC service information in various aspects, such as config, certificates loaded, current connections, SA/SP etc.	[root@VcReleaseHCM:CGW-IQC4A] show ipsec cert
show log alert show log event show log syslog	Show /var/log/emessages, /var/log/system_events and journal logs of the CGW.	[root@VcReleaseHCM:CGW-IQC4A] show log event [root@VcReleaseHCM:CGW-IQC4A] show log syslog -u cgw -n 20
show network address show network arp show network route show network socket show network ping *target_address*	Show various network information on the CGW, such as IP addresses, ARP table, route table, socket lists.	[root@VcReleaseHCM:CGW-IQC4A] show network arp -i vNic_0 [root@VcReleaseHCM:CGW-IQC4A] show network address [root@VcReleaseHCM:CGW-IQC4A] show network ping 10.145.0.112

CLI	Description	Example
	"ping" is used to do ICMP ping against the specified address.	
show service all show service cgw*state*|*status* show service hbrsrv show service ipsec show service lwdproxy show service mobilityagent show service sshd show service snmp show service sddc-daemon *state*	Show the specified service runtime status. "cgw state|status" displays the internal config engine status. "sddc-daemon state|status" displays the internal state/status of sddc-daemon.	[root@VcReleaseHCM:CGW-IQC4A] show service all [root@VcReleaseHCM:CGW-IQC4A] show service mobilityagent [root@VcReleaseHCM:CGW-IQC4A] show service cgw [root@VcReleaseHCM:CGW-IQC4A] show service cgw state [root@VcReleaseHCM:CGW-IQC4A] show service sddc-daemon state
show system cpu show system date show system disk show system load show system memory show system process show system runtime	Show the system resources information.	[root@VcReleaseHCM:CGW-IQC4A] show system memory
hc hc probe hc unit *all* | *ipsec* | *resource* | *service* | *fou* hc alert	Start healthchecking (both probing and self testing) Start probing healthchecking (probe VC/Lookup/Gateways) Start self-healthchecking (against specified unit) Show the alerts generated in latest healthcheck.	[root@VcReleaseHCM:CGW-IQC4A] hc [root@VcReleaseHCM:CGW-IQC4A] hc probe [root@VcReleaseHCM:CGW-IQC4A] hc unit all [root@VcReleaseHCM:CGW-IQC4A] hc alert

CLI	Description	Example
wanopt login | logout wanopt info wanopt *tunnel* | *flow* | *stats*	Login/Logout the associated WANOPT (if has). Query the system information of WANOPT. Query tunnel/flow/interface stats information of WANOPT.	[root@VcReleaseHCM:CGW-IQC4A] wanopt login [root@VcReleaseHCM:CGW-IQC4A] wanopt info [root@VcReleaseHCM:CGW-IQC4A] wanopt tunnel
dr details dr listdatastores dr listgroups dr listhosts dr printgroup dr printimage dr querygroupsstats dr queryhostsstats dr querylatestinstances dr queryserverstats dr status	show various detailed inforamtion of DR service.	[admin@onpremhcm1:CGW_fleet2000] dr status

RemoteAccess Mode

When RemoteAccess is enabled, user is able to SSH to the CGW directly from manager without prompting the password.

- Enable RemoteAccess on CCLI with below:

  debug remoteaccess enable
  Enabling remote access.
  Remote Access Enabled

- Now from manager, you can SSH to the target CGW by specifying "root@CGW-Name" as below

  # ssh root@CGW-IQC4A

  User is also able to SSH to WanOpt behind the associated CGW from manager. The hostname is in **<CGW_name>_WANOPT** convention. You need to know the username/password of the WanOpt.
  [root@VcReleaseHCM /opt/vmware/bin]# ssh admin@CGW-G6KQH_WANOPT