ExtraHop Command-line Reference

Published: 2024-03-26

You can manage many administrative tasks on your ExtraHop system through a command-line interface (CLI). You will typically manage your ExtraHop system with the CLI when you connect from the USB connection on the appliance with a keyboard and monitor or when you connect through the IDRAC interface.

This reference provides information about accessing the CLI and a list of all available ExtraHop commands and sub-commands.

Authorization and access

You can log in to the CLI from the ExtraHop Administration settings or through a secure shell (SSH) terminal application. While you can run basic commands when logged in as any user with system and access administration privileges, you must have the password for the setup user account to run advanced commands.

Connect to the CLI through SSH

1. Open a secure shell (SSH) terminal application.
2. Type a command similar to the following example, substituting *example-extrahop.com* with the hostname or IP address of your ExtraHop system.

   ```
   $ ssh shell@example-extrahop.com
   ```

3. When prompted, type the password for the shell user account and then press ENTER.

After you connect, you can begin typing commands. Type a question mark (?) at the prompt to display a list of available commands. Type any command name followed by a question mark to show sub-commands, such as `show ?`.

Command modes

Commands are available in privileged and non-privileged mode. Any user with system and access administration privileges can access non-privileged commands, however the setup user account password is required to access privileged commands.

Non-privileged commands

These four commands require that you log in with a user account that has system and access administration privileges.

enable

Enables privileged commands. When this command is executed, you are prompted for the setup user account password.

ping

Sends a ping request to a specified device.

show

Displays the ExtraHop system configuration settings in view-only mode.

traceroute

Sends a traceroute request to a specified device.

Privileged commands

The following commands require the setup user account password.

configure
Enables configuration mode.

delete
Allows delete operations.

disable
Disables privileged mode.

enable
Enables privileged mode.

ping
Sends a ping request.

reload
Allows reload services operations.

reset
Allows reset services operations.

restart
Allows restart services operations.

show
Shows the current system configuration settings.

shutdown
Shuts down the ExtraHop system.

stop
Stops ExtraHop services.

support
Enables (or disables) the ExtraHop Support account.

traceroute
Sends a traceroute request.

configure

Puts the ExtraHop system into Configuration mode. After the configure command executes and the system is in Configuration mode, you can pass in any of the sub-commands listed below.

Syntax

```
extrahop#configure
```

Example

The following command sequence opens Configuration mode, enables the interface subcommands, sets a static IP address, DNS servers, and hostname for interface 2 on the ExtraHop system, and then exits Configuration mode:

```
extrahop#configure
extrahop(config)#interface 2
extrahop(config-if)#ip ipaddr <ipaddr> <netmask> <gateway>
extrahop(config-if)#ip dnsservers <ipaddr> <ipaddr 2>
extrahop(config-if)#ip hostname <name>
extrahop(config-if)#exit
extrahop(config)#exit
```

The configure command supports the following sub-commands:

diagnostics

Downloads and executes a signed diagnostics script.

Syntax

```
extrahop#configure
extrahop(config)#diagnostics <URI>
```

Parameters

URI

URI. Specifies the URI of a downloaded diagnostic script from ExtraHop Support to run on the ExtraHop system.

disk_cleanup

Frees disk space by compressing and deleting large ExtraHop log files. It is not necessary to run this command unless instructed to do so by ExtraHop Support. However, you can run this command at any time.

Syntax

```
extrahop#configure
extrahop(config)#disk_cleanup
```

dnsservers

Specifies the primary and secondary DNS servers.

Syntax

```
extrahop(config)#dnsservers <primary addr> <secondary addr>
```

Parameters

dnsservers

Configures the system DNS servers.

primary addr

Specifies the primary IP address of the DNS server.

secondary addr

Specifies the secondary IP address of the DNS server. This parameter is optional.

eula_reset

Reset the POC and EULA/TOS license agreements. Note that this command is intended for ExtraHop Support only.

Syntax

```
extrahop#configure
extrahop(config)#eula_reset
```

hostname

Specifies the system hostname for the ExtraHop system.

Syntax

```
extrahop(config)#hostname <name>
```

Parameters

hostname

Configures the system hostname.

name

Specifies the fully qualified domain name (FQDN) of the ExtraHop system.

install

Retrieves and uploads a firmware update from ExtraHop.

Syntax

```
extrahop#configure
extrahop(config)#install <uri>
```

Parameters

URI

Specifies the URI of a firmware update from ExtraHop Support that is uploaded to the ExtraHop system.

interface

Puts the CLI in Interface mode and provides sub-commands to specify how the ExtraHop system acquires an IP address and the hostname.

Syntax

```
extrahop#configure
extrahop(config)#interface <interface-number>
extrahop(config-if)#ip ipaddr <addr> <netmask> <gateway>
Parameters
```

Note: You can specify the interface you want to configure by entering the interface number when running the `interface` command. If you do not specify an interface, the command will configure the primary management interface.

The `interface` command includes the following sub-commands and parameters:

ip dhcp

Configures the ExtraHop system with the DHCP option.

ip dnsserver

Configures the system DHCP servers. This parameter requires the following values:

primary addr

Specifies the primary IP address of the DNS Server.

secondary addr

Specifies the secondary IP address of the DNS server. This parameter is optional.

ip hostname

Specifies the system hostname.

name

Specifies the hostname for the ExtraHop system.

ip ipaddr

Specifies the hostname for the ExtraHop system.

addr

A static IP address.

netmask

An address that specifies the subnet mask.

gateway

The IP address of the computer that is used by devices on the network to access another network or a public network.

ip6 dhcp

Enables IPv6 and configures the ExtraHop system with the DHCPv6 option with IPv6.

Note: If enabled, DHCPv6 will be used to configure DNS settings.

ip6 disable

Disables IPv6.

ip6 ipaddr

Enables IPv6 and sets a static IPv6 address. If specified without an IPv6 address, clears all previously configured static IPv6 addresses.

ip6 ra_dns

Enables the system to configure Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) information according to router advertisements,

ip6 slaac

Enables IPv6 and configures Stateless Address Autoconfiguration for IPv6.

disabled

Disables Stateless Address Autoconfiguration.

hwaddr

Configures the system to automatically assign IPv6 addresses based on the MAC address of the sensor.

stable_private

Configures the system to automatically assign private IPv6 addresses that are not based on hardware addresses. This method is described in RFC 7217.

license

Provides sub-commands to enter the license string to update the ExtraHop license. The license key text is sent by ExtraHop Support, and it is pasted into the CLI at the Enter license text prompt.

Syntax

```
extrahop#configure
extrahop(config)#license update
Enter license text: <license>
```

Parameters

The license command includes the following sub-commands and parameters:

update

Updates the ExtraHop system license. This parameter requires the following parameter values:

license

Specifies the license key.

reformat

Provides sub-commands to schedule or cancel a reformat.

Syntax

```
extrahop#configure
extrahop(config)#reformat
```

Parameters

The reformat command performs a reformat on the next boot and includes the following subcommand:

reformat cancel

Cancels the scheduled reformat.

remote_auth

Provides sub-commands to enable or disable remote authentication of users on the ExtraHop system. Note that the sub-commands `ldap`, `radius`, and `tacacs` put the CLI in the specific mode to accept parameters for the specified remote authentication method.

Syntax

```
extrahop#configure
extrahop(config)#remote_auth disabled
```

Parameters

The `remote_auth` command includes the following sub-commands and parameters:

disabled

Disables remote authentication.

ldap

Specifies configuration parameters to enable the LDAP remote authentication method. This command puts the CLI in `ldap` mode and requires the following parameter values:

basedn

Specifies the base of the LDAP search used to find users.

binddn

Specifies the Distinguished Name (DN) used by the ExtraHop system to authenticate with the LDAP server.

port

Specifies the listening port number of the LDAP server.

search

Specifies the search filter used when searching the LDAP directory for user accounts.

server

Specifies the hostname or IP address of the LDAP server (or servers).

show

Displays the current LDAP settings.

radius

Specifies configuration parameters to enable the RADIUS remote authentication method. This command puts the CLI in radius mode and requires requires the following parameter values:

delete_server

Deletes a specified RADIUS server host.

server

Specifies the hostname or IP address of the RADIUS server (or servers), the shared secret password, and an optional timeout value.

show

Displays the current RADIUS settings.

tacacs

Specifies configuration parameters to enable the TACACS remote authentication method. This command puts the CLI in tacacs mode and requires requires the following parameter values:

delete_server

Deletes a specified TACACS server host.

server

Specifies the hostname or IP address of the TACACS server (or servers), the shared secret password, and an optional timeout value.

show

Displays the current TACACS settings.

running_config

Provides commands to update and save settings in the running configuration file. The update command generates a prompt in the CLI to provide the updated configuration text. For more information about modifying the running configuration code, see the Running Config section.

Syntax

```
extrahop#configure
extrahop(config)#running_config edit
Enter configuration:
```

Parameters

The running_config command includes the following sub-commands and parameters:

edit

Provides an interface to make changes to sections of the running configuration.

update

Provides an interface to make changes to the entire running configuration. You are prompted to enter the running configuration text by the CLI.

save

Saves the changes made to the running configuration to disk.

revert

Reverts to the saved running configuration.

services

Provides commands to enable or disable the Administration settings, enable or disable the SSH service that supports the CLI interface, and enable or disable SNMP services.

Syntax

```
extrahop#configure
extrahop(config)#services gui <enable/disable>
```

The `services` command includes the following sub-commands and parameters:

gui

Enables or disables the web service that supports the Administration settings. This command supports the parameter values `enable` to turn on the service and `disable` to turn off the service.

snmp

Enables or disables the SNMP service that supports SNMP monitoring. This command supports the parameter values `enable` to turn on the service and `disable` to turn off the service.

ssh

Enables or disables the SSH service that supports the command-line interface. This command supports the parameter values `enable` to turn on the service and `disable` to turn off the service.

systemsettings

Provides commands to work with core files.

Syntax

```
extrahop#configure
extrahop(config)#systemsettings corefiles lifetime <value>
```

The `systemsettings` command includes the following sub-commands and parameters:

corefiles enable

Enables the core files.

corefiles disable

Disables the core files.

lifetime

Sets the value for the core files lifetime.

value

Specifies the lifetime value.

time

Provides commands to set the ExtraHop system time, specified with the following datetime syntax: `<MMM DD YYYY H:M:S>`.

Syntax

```
extrahop#configure
extrahop(config-time)#time <time>
```

Parameters

time

Specifies the time in the following format: `MMM DD YYYY H:M:S`.

delete

Puts the ExtraHop system into Delete mode. After the delete command executes and the system is in delete mode, you can pass in any of the sub-commands listed below to remove files from the system.

Syntax

```
extrahop#delete
```

core

Provides commands to delete core files from the ExtraHop system. This command requires that you specify at least one core file name.

Syntax

```
extrahop#delete core <file>
```

Parameters

file

Specifies the name of the core file to delete.

disable

Removes the ExtraHop system from Enable mode. After the `disable` command executes and the system is disabled, you will need to execute the `enable` command to perform any operations that modify settings through the command-line interface.

Syntax

```
extrahop#disable
```

Example

The following command sequence disables the command-line interface:

```
extrahop#disable
```

eca

(Console only) Puts the ExtraHop system into eca mode. After the eca command executes and the system is in eca mode, you can pass in any of the sub-commands listed below to manage connected sensors, recordstores, and packetstores.

Syntax

```
extrahop#eca
```

Example

The following command sequence opens eca mode and lists the details of all connected ExtraHop sensors, recordstores, and packetstores:

```
extrahop#eca details
```

The `eca` command supports the following sub-commands:

delnode

Provides commands to remove a sensor from a console.

Syntax

```
extrahop[ECA]#eca delnode <nodeid>
```

Parameters

nodeid

Specifies the id of the sensor to remove.

details

Provides commands to list the configuration details of the connected sensor.

```
extrahop[ECA]#eca details <nodeid>
```

Parameters

nodeid

Specifies the id of the sensor.

Tip: Run the `eca details` command without the `nodeid` parameter to show the details of all connected sensors, recordstores, and packetstores.

disable

Provides commands to disable a sensor. When this connection is disabled, the console cannot access the sensor data.

```
extrahop[ECA]#eca disable <nodeid>
```

Parameters

nodeid

Specifies the id of the sensor.

enable

Provides commands to enable a sensor.

Syntax

```
extrahop[ECA]#eca enable <nodeid>
```

Parameters

nodeid

Specifies the id of the sensor.

listnodes

Provides command to list the id, name, status, firmware version, and license status of all connected sensors, recordstores, and packetstores.

Syntax

```
extrahop[ECA]#eca listnodes
```

setnickname

Provides a command to create a nickname for a connected appliance.

Syntax

```
extrahop[ECA]#eca setnickname <id> <nickname>
```

Parameters

nodeid

Specifies the id of the connected appliance.

nickname

The name to set

enable

Puts the ExtraHop system in Privileged mode. After the `enable` command executes and the system is fully enabled, you can enter and execute other commands to perform operations through the command-line interface. At the start of a session, this command is usually the first command issued. If you are prompted to enter a username and password, type the following credentials:

- Type `shell` as the user name.
- Type the number displayed on the service tag

Note: The service tag is on a pullout tab located on the front of the ExtraHop appliance, below the video connector on the 610 and below the power button on the 710.

Syntax

```
extrahop>enable
```

Example

The following command sequence enables the command-line interface and prompts for the system password:

```
extrahop>enable
password:
```

ping

Executes a command to ping a selected target to verify the ability to contact the specified host. Ping results specify the response packets received and the round-trip time.

Syntax

```
extrahop#ping <addr>
```

Parameters

addr.

Specifies the IP address of the device to ping.

Example

The following command sequence pings a device at the specified IP address:

```
extrahop#ping 192.164.111.10
```

reload

Executes a reload operation for the specified ExtraHop system component. After the reload command is invoked, you can reload any of the supported components identified by their subcommands.

Syntax

```
extrahop#reload
```

Example

The following command sequence activates Reload mode and reloads the ExtraHop bridge service:

```
extrahop#reload exbridge
```

The `reload` command supports the following sub-commands:

exbridge

Specifies the ExtraHop bridge as the component service to reload.

Syntax

```
extrahop#reload exbridge
```

excap

Specifies the ExtraHop capture as the component service to reload.

Syntax

```
extrahop#reload excap
```

reset

Executes a reset operation for the specified ExtraHop system component. After the `reset` command is invoked, you can reset the ExtraHop Datastore, which clears all current data from the Datastore.

Syntax

```
extrahop#reset
```

Example

The following command sequence activates Reset mode and clears data from the ExtraHop datastore:

```
extrahop#reset datastore
```

The `reset` command supports the following sub-commands:

datastore

Clears the saved data from the ExtraHop Datastore.

Syntax

```
extrahop#reset datastore
```

restart

Executes a restart operation for the specified ExtraHop system component. After the `restart` command is invoked, you can restart the ExtraHop component services identified by the following sub-commands.

Syntax

```
extrahop#restart
```

Example

The following command sequence activates Restart mode and restarts the ExtraHop bridge service:

```
extrahop#restart exbridge
```

The `restart` command supports the following sub-commands:

exbridge

Specifies the ExtraHop bridge as the component service to restart.

Syntax

```
extrahop#restart exbridge
```

excap

Specifies the ExtraHop capture as the component service to restart.

Syntax

```
extrahop#restart excap
```

exportal

Specifies the ExtraHop web portal as the component service to restart.

Syntax

```
extrahop#restart exportal
```

system

Specifies the ExtraHop system as the component to restart. This operation reboots the entire ExtraHop system.

Syntax

```
extrahop#restart system
```

webserver

Specifies the ExtraHop web server as the component service to restart.

Syntax

```
extrahop#restart webserver
```

show

Puts the CLI in View mode so that you can see the settings and parameter values associated with the ExtraHop system components. After the `show` command executes and the system is in View mode, you can look at the settings associated with every aspect of the ExtraHop system.

Syntax

```
extrahop#show
```

Example

The following command sequence puts the interface in View mode and shows the ExtraHop system time:

```
extrahop#show clock
```

The `show` command supports the following sub-commands:

clock

Specifies the ExtraHop computer current clock time as the setting to show.

Syntax

```
extrahop#show clock
```

controllers

Shows the settings for all the ExtraHop system active interfaces.

Syntax

```
extrahop#show controllers
```

cores

Shows the settings for the ExtraHop system core files.

Syntax

```
extrahop#show cores
```

dhcp

Shows whether DHCP is enabled or disabled on the primary management interface of the ExtraHop system.

Syntax

```
extrahop#show dhcp
```

diskmon

Shows the hard disk monitor statistics for the hard drive on the ExtraHop system.

Syntax

```
extrahop#show diskmon
```

diskmon_details

Shows the health details of the firmware SSD drive on the ExtraHop sensor.

Syntax

```
extrahop#show diskmon_details
```

dnsservers

Shows the DNS server configuration settings for the ExtraHop system.

Syntax

```
extrahop#show dnsservers
```

eula_accepted

Shows whether the EUSL/TOS and POC agreements have been accepted for the ExtraHop system.

Syntax

```
extrahop#show eula_accepted
```

firmware

Shows the firmware versions installed on the ExtraHop system.

Syntax

```
extrahop#show firmware
```

flash

Shows the content of the flash key for the ExtraHop system.

Syntax

```
extrahop#show flash
```

gateway

Shows the gateway configuration settings for the ExtraHop system.

Syntax

```
extrahop#show gateway
```

history

Shows the session command history for the current CLI session.

Syntax

```
extrahop#show history
```

hostname

Shows the system hostname for the ExtraHop system.

Syntax

```
extrahop#show hostname
```

interface

Displays information about a specific interface of the ExtraHop system.

Syntax

```
extrahop#show interface <interface-number> <sub-command>
```

The `interface` command includes the following sub-commands:

dhcp
Shows whether DHCP is enabled or disabled on the interface.

ipaddr
Shows the IP address and netmask for the ExtraHop system management port on the interface.

macaddr
Shows the MAC address for the interface.

inventory

Shows the firmware version, system BIOS version, serial number, dossier ID, and hostname for the ExtraHop appliance.

Syntax

```
extrahop#show inventory
```

ip

Provides sub-commands to show IP address configuration settings for the ExtraHop system.

Syntax

```
extrahop#show ip arp
```

Parameters

The `ip` command includes the following parameters:

arp
Shows ARP resolution for the device and any computers connected to the device.

interface
Shows information for every IP interface on the connected computer.

sockets
Shows all active Internet connections for the device.

traffic
Shows the IP, ICMP, ICMP msg, TCP, UDP, UDP lite, TCP Ext, and IP Ext traffic for the device.

ipaddr

Shows the IP address and netmask for the ExtraHop system management port on the primary management interface.

Syntax

```
extrahop#show ipaddr
```

ldap

Shows the LDAP configuration settings for the ExtraHop system.

Syntax

```
extrahop#show ldap
```

license

Shows the licensed modules for the ExtraHop system and which ones are enabled or disabled.

Syntax

```
extrahop#show license
```

log

Provides sub-commands to show the logs for the ExtraHop system.

Syntax

```
extrahop#show log
```

Parameters

The `log` command includes the following parameters:

exbridge
Shows the ExtraHop system bridge component logs.

excap
Shows the ExtraHop system capture logs.

exportal
Shows the ExtraHop system web portal logs.

macaddr

Shows the MAC address for the primary management interface of the ExtraHop appliance.

Syntax

```
extrahop#show macaddr
```

memory

Shows the total, used, free, shared, buffers, and cached memory as well as Swap information for the ExtraHop system.

Syntax

```
extrahop#show memory
```

nics

Shows all NICs (network interface controllers) as well as their link status and link speed for the ExtraHop appliance.

Syntax

```
extrahop#show nics
```

processes

Shows the status of all ExtraHop system processes.

Syntax

```
extrahop#show processes
```

radius

Shows the RADIUS configuration settings for the ExtraHop system.

Syntax

```
extrahop#show radius
```

remote_auth

Shows the remote authentication configuration settings for the ExtraHop system.

Syntax

```
extrahop#show remote_auth
```

running_config

Shows the running configuration file settings for the ExtraHop system.

Syntax

```
extrahop#show running_config
```

systemsettings

Shows whether the core files are enabled and if the offline capture setting is enabled for the ExtraHop system.

Syntax

```
extrahop#show systemsettings
```

tacacs

Shows the TACACS configuration settings for the ExtraHop system.

Syntax

```
extrahop#show tacacs
```

users

Shows the user accounts for the ExtraHop system.

Syntax

```
extrahop#show users
```

version

Shows the base firmware version and the currently running firmware version on the ExtraHop system.

Syntax

```
extrahop#show version
```

shutdown

Initiates the system shutdown operation for the ExtraHop system.

Syntax

```
extrahop#shutdown
```

Example

The following command sequence initiated the ExtraHop system shutdown:

```
extrahop#shutdown
```

stop

Stops the specified ExtraHop system components. After the stop command is invoked, you can halt the operation of specific system component services without shutting down the entire ExtraHop system.

Syntax

```
extrahop#stop
```

Example

The following command sequence puts the interface in Stop mode and halts the operation of the ExtraHop bridge component service:

```
extrahop#stop exbridge
```

The `stop` command supports the following sub-commands:

exbridge

Specifies the ExtraHop bridge as the system component service to stop.

Syntax

```
extrahop#stop exbridge
```

excap

Specifies the ExtraHop capture as the system component service to stop.

Syntax

```
extrahop#stop excap
```

exportal

Specifies the ExtraHop web portal as the system component service to stop.

Syntax

```
extrahop#stop exportal
```

webserver

Specifies the ExtraHop web server as the system component service to stop.

Syntax

```
extrahop#stop webserver
```

support

Provides commands to enable or disable the ExtraHop system support account. After the `support` command is invoked, you can enable or disable the support account.

Syntax

```
extrahop#support
```

Example

The following command sequence puts the interface in Support mode and it activates the support account:

```
extrahop#support enable
```

The `support` command includes the following sub-commands:

enable

Turns on the ExtraHop system support account.

Syntax

```
extrahop#support enable
```

disable

Turns off the ExtraHop system support account.

Syntax

```
extrahop#support disable
```

traceroute

Executes the traceroute command on the ExtraHop system to measure packet delays across the network.

Syntax

```
extrahop#traceroute <addr>
```

Parameters

addr.

Specifies the IP address of a network device.

Example

The following command executes the traceroute command to measure network packet loss for the route to and from the specified IP address:

```
extrahop#traceroute <addr>
```