# H3C SecPath D2000-G[AK][V]系列数据库审计系统

## 命令参考

# 目　录

# 1 Console 口的缺省参数

端口：COMx；

波特率：115200；

数据位：8；

奇偶校验：None；

停止位：1。

密码：sasdebug!@#

# 2 CLI 命令

## 2.1 arp

**arp** 命令用来显示 arp 缓存。

【命令】

**arp**

【相关命令】

- arpdel
- arpset

## 2.2 arpdel

**arpdel** 命令用来删除 arp 缓存。

【命令】

**arpdel** {host}

【参数】

**host**：表示删除指定地址的 arp 信息。

【相关命令】

- **arp**
- **arpset**

## 2.3 arpset

**arpset** 命令用来设置指定的主机的 IP 地址与 MAC 地址的静态映射。

【命令】

**apset** {host} {mac}

【参数】

**host**：表示需要设置的 IP 地址。

**mac**：表示需要修改成的 MAC 地址。

【举例】

**arpset** 10.4.8.198 aa:bb:cc:dd:ee:ff

## 2.4 clock

**clock** 命令用来查看和设置硬件时间。

【命令】

**clock set** {time} {day} {month} {year}

**clock show**

【参数】

**set**：表示设置硬件时间，需填写对应的时间格式。

**show**：表示展示硬件时间。

【举例】

#设置硬件时间为 2018 年 3 月 9 日 15:32:00

clock set 15:32:00 9 March 2018

## 2.5 date

**date** 命令用来显示当前设备的时间。

【命令】

**date**

## 2.6 df

**df** 命令用来查看磁盘挂载和使用情况。

【命令】

**df**

## 2.7 exit

**exit** 命令用来结束当前会话。

【命令】

**exit**

## 2.8 help

**help** 命令用来显示串口帮助信息。

【命令】

**help**

## 2.9 history

**history** 命令用来显示串口模式下最近执行过的命令记录。

【命令】

**history** [limit]

【参数】

limit：表示最多显示的记录行数。

## 2.10 ids_test

**ids_test** 命令用来手动运行监听进程。

【命令】

**ids_test**

【使用指导】

当发现系统各项配置正常，但是监听进程始终无法正常运行时，使用该功能，手动确认监听进程的运行情况。

## 2.11 ifconfig

**ifconfig** 命令用来查看和设置网卡信息,同 linux 系统 ifconfig 命令一致，最多支持 5 个参数。

【命令】

**ifconfig** [interface] [parameter1] [parameter2] [parameter3] [parameter4] [parameter5]

【参数】

Interface：表示指定的网卡名

parameter1： 参数 1

parameter2： 参数 2

parameter3： 参数 3

parameter4： 参数 4

parameter5： 参数 5

## 2.12 init_disk

init_disk 命令用来初始化数据硬盘，初始化成功后系统自动重启。

【命令】

init_disk

【使用指导】

因涉及用户数据安全，该命令请慎重使用。一般在设备第一次部署出现系统初始化失败时，可通过该命令强制格式化数据磁盘后，系统即可正常初始化。如果设备运行一段时间后执行该命令，则需在系统配置管理页面清空所有配置，以避免格式化数据盘部分配置被清空后导致审计系统使用出错。

输入该命令，需再输入密码“sasinitdisk!@#”后，系统提示是否进行初始化，y 表示进行初始化，n 表示否。

## 2.13 login

login 命令用来登录系统后台，并通过指定用户进行后台操作。

【命令】

login [user]

【参数】

user：为系统用户名，不填则默认 root。

## 2.14 logout

**logout** 退出串口。

【命令】

**logout**

## 2.15 netstat

**netstat** 命令用来查看网络状态，同 linux 下的 **netstat** 命令。

【命令】

**netstat** [var]

【参数】

var 有如下可能，可组合使用，为空时和-a 选项效果一样。

-a (all)：显示所有选项，默认不显示 listen（监听）服务相关。

-t (tcp)：仅显示 tcp 相关选项。

-u (udp)：仅显示 udp 相关选项。

-n：拒绝显示别名，能显示数字的全部转化成数字。

-l：仅列出有在 listen (监听) 的服务状态。

-p：显示建立相关链接的程序名。

-r：显示路由信息，路由表。

-e：显示扩展信息，例如 uid 等。

-s：按各个协议进行统计。

-c：每隔一个固定时间，执行该 netstat 命令。

## 2.16 ping

**ping** 命令用来测试主机之间网络的连通性。

【命令】

**ping** {dest}

【参数】

dest：表示需要测试连通性的 ip 地址。

## 2.17 ps

**ps** 命令用来查看进程状态，与 linux 下 **ps** 相同。

【命令】

ps [var]

【参数】

var 有如下可能，为空时和-w 选项效果一样。

-A：列出所有的进程

-w：显示加宽可以显示较多的资讯

-a：显示现行终端机下的所有进程，包括其它用户的进程；

-u：以用户为主的进程状态 ；

-x：通常与 a 这个参数一起使用，可列出较完整信息。

## 2.18 resumeifconfig

**resumeifconfig** 命令用来在异常情况下重置检修口的 ip 地址，保证 ip 为 1.0.0.1。

【命令】

**resumeifconfig**

## 2.19 set_listen_eth

**set_listen_eth** 命令用来设置监听口。

【命令】

**set_listen_eth** {var}

【参数】

var：表示需要被设置为监听口的网卡名，如果有多个请用’,'隔开。

【举例】

set_listen_eth GE0-2,GE0-3

## 2.20 show_DB_log

**show_DB_log** 命令用来查看最近 50 条系统日志。

【命令】

**show_DB_log** [num]

【参数】

num：需要展示的日志条数，不填则默认 50。

## 2.21 show_rule_configure

**show_rule_configure** 命令用来查看数据库审计规则。

【命令】

**show_rule_configure**

## 2.22 telnet

**telnet** 命令用于登录远程主机，对远程主机进行管理。

【命令】

**telnet**

【使用指导】

输入 telnet 命令后根据需要进行操作。

## 2.23 top

**top** 是 Linux 下常用的性能分析工具，能够实时显示系统中各个进程的资源占用状况，常用于服务端性能分析。

【命令】

**top**

## 2.24 set_ipconfig

**set_ipconfig** 命令用来配置网卡，请注意，通过此命令配置的内容，在系统重启后会失效。

【命令】

**set_ipconfig** {ethname} {host} {nmask}

【参数】

ethname：表示需被配置的网卡。

host：表示需配置的 ip 地址。

nmask：表示需配置的掩码。

## 2.25 show_ipconfig_file

**show_ipconfig_file** 命令用来查看网卡的配置列表。

【命令】

**show_ipconfig_file**

【使用指导】

查看或者确认当前网卡配置列表，可配合 set_ipconfig_file 来修改。

【相关命令】

set_ipconfig_file

## 2.26 set_ipconfig_file

**set_ipconfig_file** 命令用来修改指定网卡信息的配置文件。

【命令】

**set_ipconfig_file** {var}

【参数】

var：表示网卡的配置文件名。

【使用指导】

注意，通过此命令修改的配置文件重启后继续生效。

【相关命令】

show_ipconfig_file

## 2.27 traceroute

**traceroute** 命令是用来确认信息从审计设备到指定 IP 的通信路径。

【命令】

**traceroute** {dest}

【参数】

dest：表示需要确认的目标 IP 地址。

## 2.28 restore_pass

**restore_pass** 命令用来重置系统用户的密码为出厂状态。

【命令】

**restore_pass** {username}

【参数】

username：表示指定还原密码的系统用户名，仅支持默认的登录用户名 admin、sec、mon、audit。

【举例】

#重置 sec 账户的密码为出厂状态
restore_pass sec

## 2.29 reboot

**reboot** 命令用来重启设备。

【命令】

**reboot**

## 2.30 halt

**halt** 命令用来关闭设备。

【命令】

**halt**

## 2.31 display

**display** 命令用来显示当前设备版本、设备使用时长、SN 号、BIOS 版本、内存、硬盘、默认网口识别号、扩展网口识别号、网口接线状态等信息。

【命令】

**display [device]**

【参数】

**Device**：固定为 device

## 2.32 setip

**setip 用来修改网卡配置并且重启后有效，包括 IP、子网掩码、网关信息。**

【命令】

**setip** [interface] [ipaddr] [netmask] [gateway]

【参数】

Interface：网卡名

ipaddr ：要设置的 IP 地址

netmask：子网掩码

gateway：网关