关于ACG1000-SE-PWR 应用审计日志不显示解决方法

刘嘉炜 2018-04-11 发表

目前现场ACG1000-SE-PWR（F6608）之前使用日志显示正常，在客户执行配置初始化后，发现所有审计日志均无法显示。但是审计功能也正常并且ipv4策略有匹配条目。

1、在设备命令行下查看硬盘正常，存储空间未占满，数据库没有应用审计日志记录，在查看网站的同时，隔一段时间看没有增长。

```
H3C> display datab

disk capacity:458.3G  usage: 0%
-------------------------------------------------------------------------------------------
Log Type        Table Count   Current Table                    Count          Success
-------------------------------------------------------------------------------------------
web_access      2             t_log_webaccess_20180411         0              0
malware_app     2             t_log_malware_app_20180411       0              0
net             2             t_log_net_20180411               0              0
content         2             t_log_content_20180411           0              0
vid             2             t_log_vid_20180411               0              0
im              2             t_log_im_20180411                0              0
social_log      2             t_log_bbs_20180411               0              0
search_engine   2             t_log_search_engine_20180411     0              0
mail            2             t_log_mail_20180411              0              0
command_log     2             t_log_command_20180411           0              0
file_transfer   2             t_log_file_transfer_20180411     0              0
relax_stock     2             t_log_relax_stock_20180411       0              0
other_app       2             t_log_other_20180411             0              0
key_event       2             t_log_ucc_key_event_20180411     0              0
ucc_account     2             t_log_ucc_account_20180411       0              0
```

2、进入web_access的应用审计日志表中查看没有记录。

```
H3C# display database table
  web_access     Log of web_access
  malware_app    Log of malware_app
  im             Log of im
  social_log     Log of social_log
  search_engine  Log of search_engine
  mail           Log of mail
  command_log    Log of command_log
  file_transfer  Log of file_transfer
  relax_stock    Log of relax_stock
  other_app      Log of other_app
  key_event      Log of key_event
  ucc_account    Log of ucc_account
H3C# display database table web_access
  <cr>
  [all]  show all table count
H3C# display database table web_access

--------------------------------------
Table Name                  Count
--------------------------------------
t_log_webaccess_20180411    0
```

3、重置并清除数据库后将设备恢复出厂设置重启，日志硬盘还是没有存入日志。

H3C# clear database

Are you sure clear log database? Please enter "y/n" to confirm: y

H3C# recover database

H3C# reboot

4、目前设备配置正常没有问题

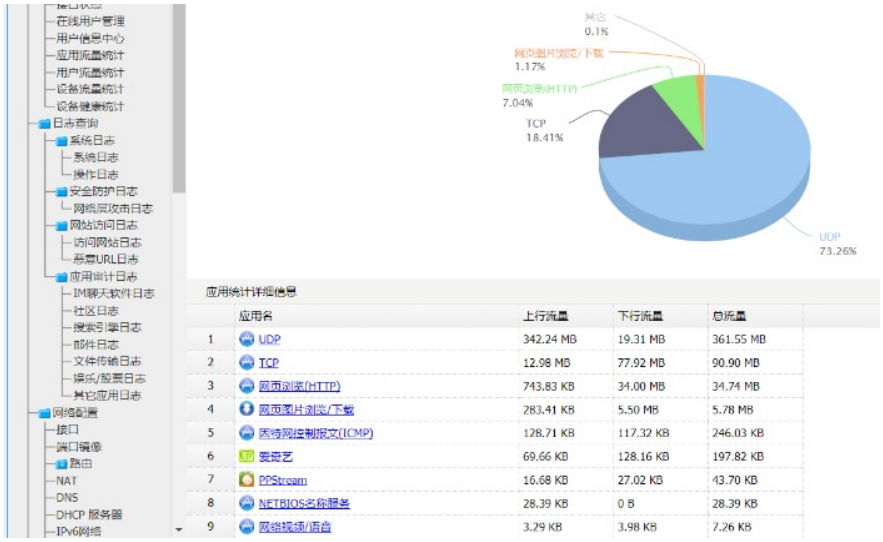
H3C# recover database

H3C# reboot

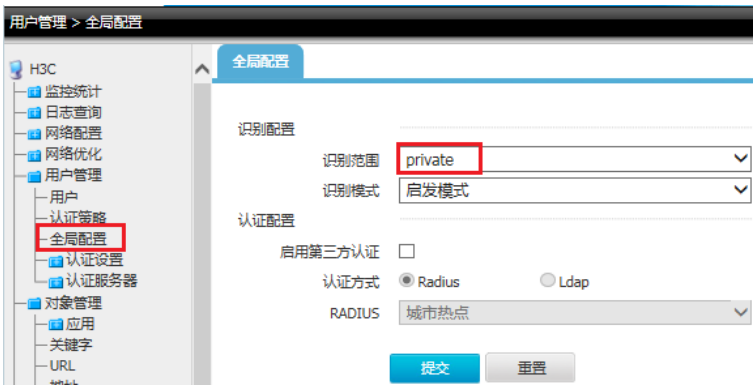
H3C# dis run policy

```
policy any any any any any any any always audit 1
app-policy 1 application any any any keyword include any accept info FilterIMLoginAction
app-policy enable 1
website-policy malware enable
website-policy 1 any accept info FilterUrl
website-policy enable 1
policy default-action permit
policy white-list enable
!
!policy-decrypt
!
!
```

5、在应用流量统计中应用审计正常。



排查发现客户将全局配置中的识别模式调整为private，导致无法识别输出审计日志。



将识别模式修改为any后问题解决。