H3C Comware V7 平台设备通过 EAA 功能过滤自定义敏感词汇配置案例

EAA 产品特性 丁犁 2022-06-28 发表

组网及说明

需求：处于安全要求，网络管理人员不允许创建任何命名中，包含“H3C”（大写）关键字的资源。

配置步骤

通过部署 EAA CLI 监控策略，实现相关安全需求：

创建一个“not_use_h3c”名称的CLI监控策略
<Sysname> system-view
[Sysname] rtm cli-policy not_use_h3c
配置监控事件：监控包含“H3C”关键字。如果指定skip参数，则表示事件发生时，只执行CLI监控策略中的动作，不执行event cli中指定的命令；如果不指定skip参数，则表示事件发生时，CLI监控策略和event cli中指定的命令同时执行。
[Sysname-rtm-not_use_h3c] event cli async skip mode execute pattern H3C
事件发生时，发送优先级为1，日志记录工具为local1，信息为“Do not use sensitive words”的日志。
[Sysname-rtm-not_use_h3c] action 0 syslog priority 1 facility local1 msg Do not use sensitive words
配置CLI监控策略执行动作的持续时间为3秒
[Sysname-rtm-not_use_h3c] running-time 3
配置用户角色network-admin具有执行该策略的权限。
[Sysname-rtm-not_use_h3c] user-role network-admin
确认执行该策略
[Sysname-rtm-not_use_h3c] commit

通过display rtm policy registered查看，可以看到策略名为 not_use_h3c，策略类型为CLI的策略。
<Sysname>display rtm policy registered
Total number: 1
Type Event TimeRegistered PolicyName
CLI CLI Jun 28 16:06:18 2022 not_use_h3c

配置关键点

通过上述配置后，若网络管理员创建比如name中包含“H3C”关键字的ACL列表，设备将提示告警，且相关ACL列表不会创建成功。

```
[Sysname]acl number 3333 name dH3Cd
 [Sysname]%Jun 28 16:06:59:867 2022 Sysname RTM/1/RTM_ACTION: Do not use sensitive words
%Jun 28 16:06:59:872 2022 Sysname RTM/6/RTM_POLICY: CLI policy test is running successfully.
[Sysname]
[Sysname]display acl all   //创建name为dH3Cd自定义名称的acl不生效
[Sysname]
[Sysname]acl number 3333 name dH3C
[Sysname]%Jun 28 16:07:20:828 2022 Sysname RTM/1/RTM_ACTION: Do not use sensitive words
%Jun 28 16:07:20:832 2022 Sysname RTM/6/RTM_POLICY: CLI policy test is running successfully.
[Sysname]
[Sysname]display acl all   //创建name为dH3C自定义名称的acl不生效
[Sysname]
[Sysname]acl number 3333 name H3Cd
[Sysname]%Jun 28 16:07:40:109 2022 Sysname RTM/1/RTM_ACTION: Do not use sensitive words
%Jun 28 16:07:40:114 2022 Sysname RTM/6/RTM_POLICY: CLI policy test is running successfully.
[Sysname]
[Sysname]display acl all   //创建name为H3Cd自定义名称的acl不生效
[Sysname]
```