

SecPath ACG1000日志分析与管理平台添加ACG1000-P设备失败故障案例

ACG1000

日志采集器

其他

丁犁

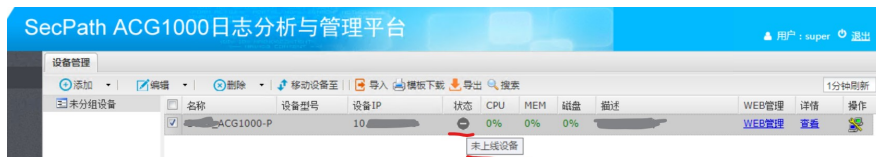
2019-01-21 发表

组网及说明

不涉及

问题描述

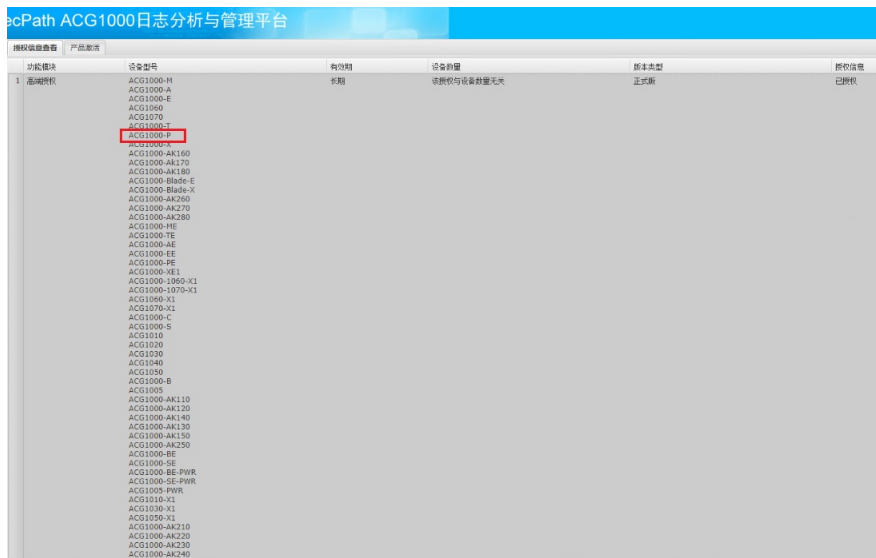
SecPath ACG1000日志分析与管理平台使用R0303P02版本，在其中纳管添加ACG1000-P设备（R6609P06）后，相关设备状态显示为“未上线设备”状态。



过程分析

1、检查ACG1000日志分析与管理平台所属服务器与ACG1000-P设备连通性：互ping正常，可通；服务器浏览器上web打开ACG1000-P管理界面正常。

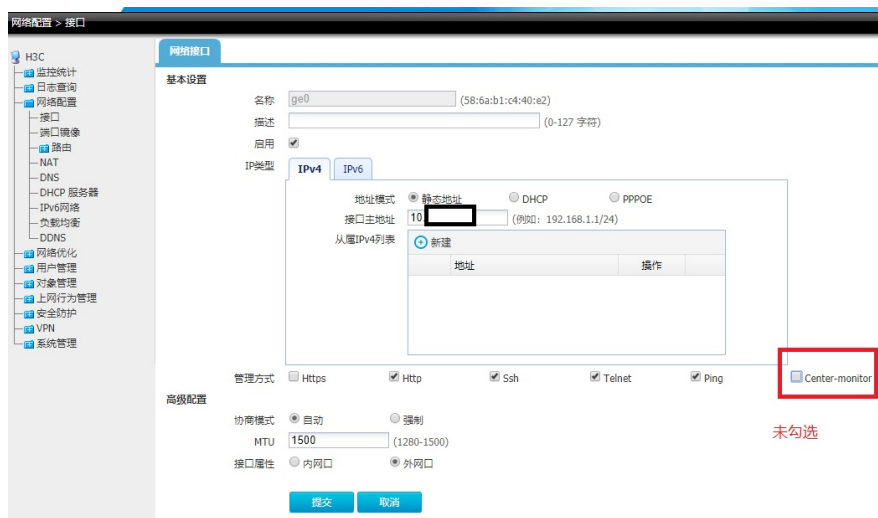
2、由于ACG1000-P型号属于高端产品，因此需要在ACG1000日志分析与管理平台上安装“高端授权”：平台已经安装成功，且非临时过期授权。



3、在ACG1000-P设备上抓包，确认ACG1000-P设备收到了日志分析与管理平台发送过来tcp目的端口=8888的发现报文，但是ACG1000-P设备没有回应任何报文：

tcp.port == 8888						
No.	Time	Source	Destination	Protocol	Length	Info
985	1.740726	10.10.10.1	10.10.10.1	TCP	66	51186 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
1344	8.459153	10.10.10.1	10.10.10.1	TCP	66	51188 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
1845	11.4600...	10.10.10.1	10.10.10.1	TCP	66	[TCP Retransmission] 51188 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
2238	17.4540...	10.10.10.1	10.10.10.1	TCP	66	51190 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
2569	20.4555...	10.10.10.1	10.10.10.1	TCP	66	[TCP Retransmission] 51190 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
2980	26.8429...	10.10.10.1	10.10.10.1	TCP	66	51192 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
3339	29.8461...	10.10.10.1	10.10.10.1	TCP	66	[TCP Retransmission] 51192 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
3690	32.9608...	10.10.10.1	10.10.10.1	TCP	66	51193 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0
3870	35.9610...	10.10.10.1	10.10.10.1	TCP	66	[TCP Retransmission] 51193 → 8888 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0

4、检查ACG1000-P设备接收tcp目的端口=8888相关接口配置，发现未勾选“Center-monitor”



解决方法

在ACG1000-P设备上，将相关接口的“Center-monitor”选项勾选提交后，问题解决。