H3C SecCenter 安全威胁发现与运营管理平台

故障处理手册

资料版本：5W100-20200325

目 录

1 简介

本文档介绍 H3C SecCenter 安全威胁发现与运营管理平台常见故障的诊断及处理措施。

1.1 故障处理注意事项

注意

系统正常运行时，建议您在完成重要功能的配置后，及时保存并备份当前配置，以免设备出现故障后配置丢失。建议您定期将配置文件备份至远程服务器上，以便故障发生后能够迅速恢复配置。

在进行故障诊断和处理时，请注意以下事项：

- 当出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），收集信息越全面、越详细，越有利于故障的快速定位。
  - 记录您所使用的系统版本。
  - 记录具体的故障现象、故障时间、配置信息。
  - 记录完整的网络拓扑，包括组网图、端口连接关系、故障位置。
  - 记录现场采取的故障处理措施及实施后的现象效果。
- 故障处理过程中，如需更换程序文件或安装补丁，请参考软件对应的版本说明书，确保兼容性。
- 诊断和处理故障人员必须详细了解软件运行机制，并能熟练操作软件及其所依赖的程序和系统。

1.2 故障处理求助方式

当故障无法自行解决时，请准备好设备运行信息、故障现象等材料，发送给 H3C 技术支持人员进行故障定位分析。

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

2 资产问题处理

2.1 资产创建问题处理

2.1.1 创建资产时，提示“区域配置不正确，资产创建失败”

1. 问题描述

创建资产时，提示“区域配置不正确，资产创建失败”。

2. 问题处理步骤

(1) 检查资产信息配置是否存在错误，例如管理 IP 或名称与组内已有成员是否重复。如果是资产管理 IP、名称重复等错误，请根据提示修改相应配置信息。

(2) 检查区域配置是否正确，确保区域配置 IP 范围在父区域范围内，查看是否存在其它错误，例如 IP 范围或名称与组内已有成员是否重复。如果是区域 IP 范围、名称重复等错误，请根据提示修改相应配置信息。

(3) 如果区域未配置，请按照区域配置步骤配置区域信息。

(4) 如果上述操作完成后问题仍无法排除，请联系 H3C 技术支持工程师。

2.1.2 创建资产时，提示“创建失败，管理 IP 不一致”

1. 问题描述

创建资产时，提示“创建失败，管理 IP 不一致”。

2. 问题处理步骤

该问题是由于创建资产管理 IP 与区域 IP 范围不一致造成的。解决方法如下：

(1) 检查资产管理 IP 是否超出区域 IP 范围，如果未超出，查看信息配置是否存在错误，例如管理 IP 或名称与组内已有成员是否重复。如果是资产管理 IP、名称重复等错误，请根据提示修改相应配置信息。

(2) 检查区域配置是否正确，确保区域配置 IP 范围在父区域范围内，查看是否存在其它错误，例如 IP 范围或名称与组内已有成员是否重复。如果是区域 IP 范围、名称重复等错误，请根据提示修改相应配置信息。

(3) 如果上述操作完成后问题仍无法排除，请联系 H3C 技术支持工程师。

2.2 资产发现失败

2.2.1 问题描述

创建拓扑任务后，自动发现资产功能失效，资产发现失败。

2.2.2 问题处理步骤

该问题可能原因为区域配置错误、区域采集器异常或拓扑任务未启动。解决方法如下：

(1) 检查是否已部署区域采集器，如已部署，通过 ping 命令确认采集器是否能正常访问。

(2) 检查区域是否已正确配置，例如，区域名称是否重名，检查 IP 范围是否在区域采集器所在网段。

(3) 检查拓扑任务是否已启动，如果未启动请先启动任务。

(4) 如果上述操作完成后问题仍无法排除，请联系 H3C 技术支持工程师。

2.3 性能监控失败

2.3.1 问题描述

资产配置界面，资产的 CPU 利用率和内存利用率无数据展示。

2.3.2 问题处理步骤

(1) 通过终端登录到资产查看该资产是否配置 SNMP 功能，配置命令如下。

```
<sysname>display current-configuration | include  snmp
 snmp-agent
 snmp-agent local-engineid 800063A280000C2958CBDD00000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap address udp-domain 186.64.6.176 params securityname public v2c
```

(2) 在资产配置页面查看是否配置 SNMP 参数，并且配置参数必须资产配置保持一致，具体配置如下图。

(3) 进入拓扑发现任务页面查看拓扑任务是否为启动状态，若未启动请单击操作列的启动按钮启动任务。

(4) 通过命令行方式发送 ping 命令检查资产与平台是否网络连通。

(5) 进入资产配置界面，查看是否展示 CPU 和内存利用率数据。

(6) 若执行上述操作后仍无数据，请联系 H3C 技术支持工程师。

2.4 资产模板导入失败

2.4.1 问题描述

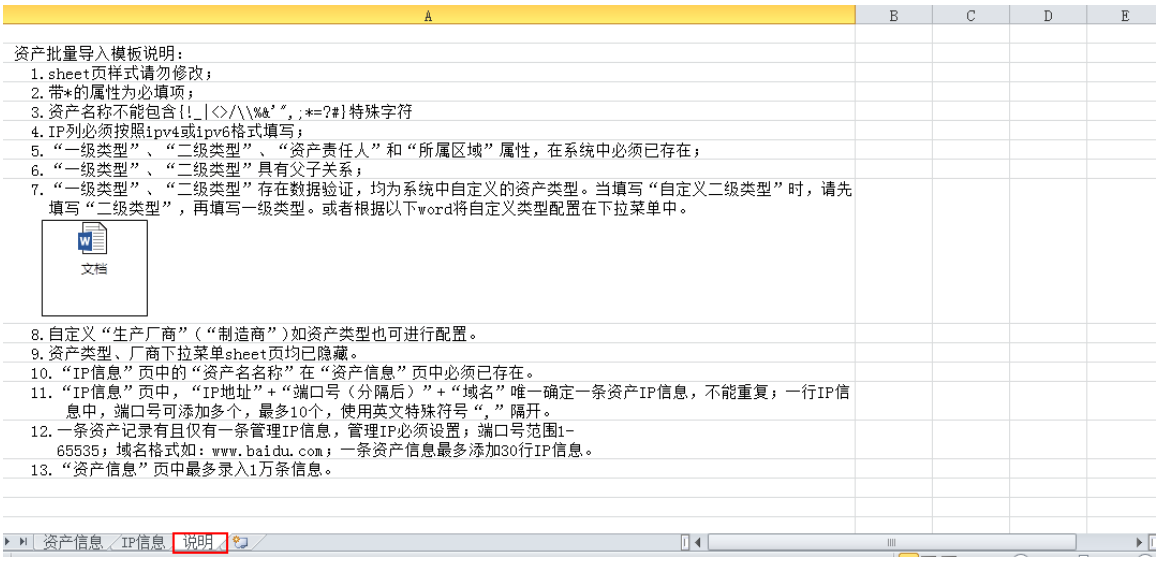
按照资产模板要求导入资产信息时，提示导入失败。

2.4.2 问题处理步骤

(1) 在下载的资产模板中，按照模板列表信息填写完整资产信息，其红色“*”为必填项。排查填入模板的信息是否符合“说明”sheet 页面的要求。

说明

不同版本资产导入的条件不一样，请以实际情况为准。



(2) 若满足要求，请在资产配置界面，单击<导入>按钮选择“导入信息”查看失败原因，并按提示信息更改资产导入模板中的信息。

(3) 重新检查并修改资产模板的资产信息，确认信息无误后再次导入。

(4) 如果按上述操作执行完成后问题仍无法排除，请联系 H3C 技术支持工程师。

3 拓扑问题处理

3.1 拓扑发现任务不能发现网络拓扑

3.1.1 问题描述

添加拓扑发现任务后，不能发现网络拓扑，如图所示。

图3-1 网络拓扑无数据展示

3.1.2 问题处理步骤

造成问题的原因可能是拓扑发现任务添加步骤有误，或者拓扑发现任务参数配置有误。正确配置步骤如下：

(1) 配置资产信息。请在资产配置页面查看是否已添加资产及资产信息是否正确。

(2) 配置拓扑发现任务。在拓扑发现任务界面配置任务，确认任务扫描区域，SNMP 参数及定时发现设置等信息是否正确。

(3) 任务配置成功后返回任务列表页面，单击<启动>按钮。

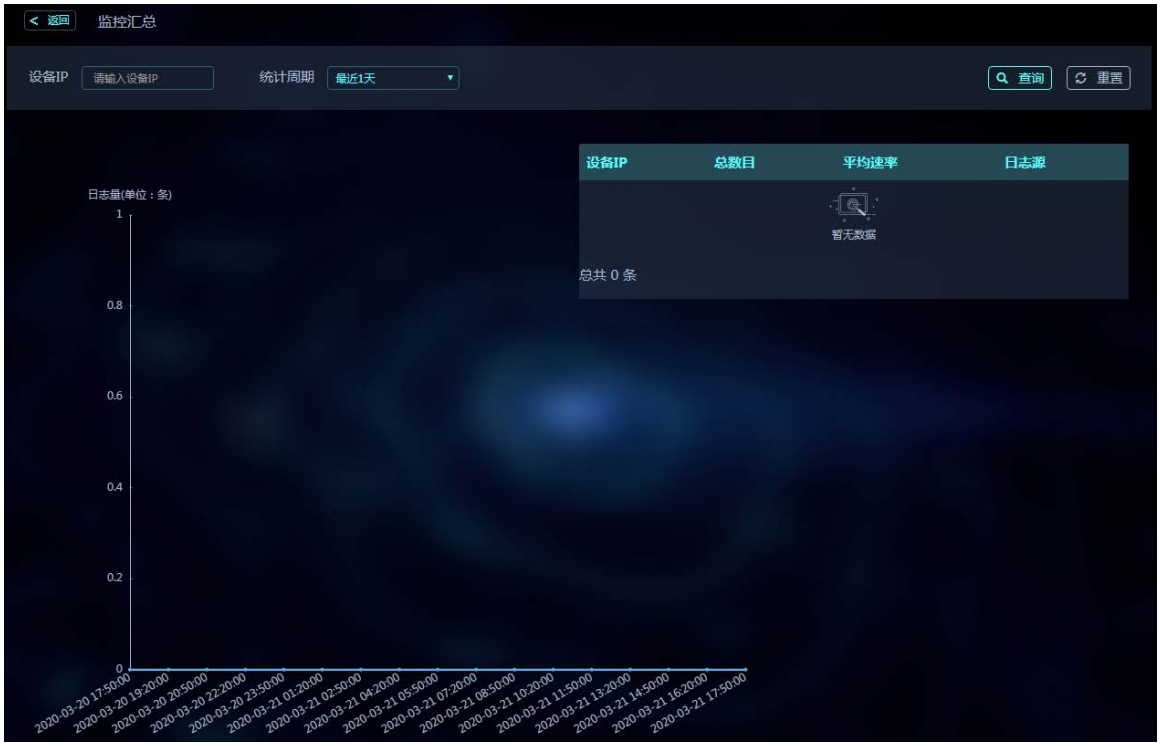
(4) 如果按上述步骤执行完成后仍不能排除问题，请联系 H3C 技术支持工程师。

4 日志适配问题处理

4.1 采集器模块

4.1.1 问题描述

采集器未收到日志，在“配置管理 > 数据来源 > 采集器管理”界面，单击“统计信息”列的统计进入监控汇总界面，查看页面无数据，如下图所示。



4.1.2 问题处理步骤

1. 查看采集器状态

(1) 在“系统配置 > 数据来源 > 采集器管理”页面查看采集器状态。

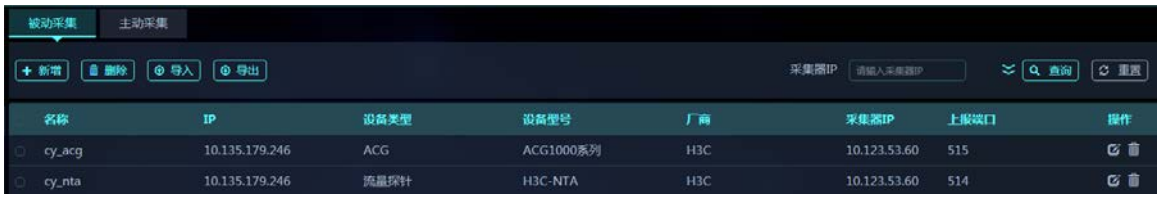
(2) 若采集器为离线状态，登录 cyber5 主机，执行如下命令重启采集器：

```
[root@cyber5 /]# cd /home/adapter-deploy-docker/
[root@cyber5 adapter-deploy-docker]# ./start_docker.sh all restart
```

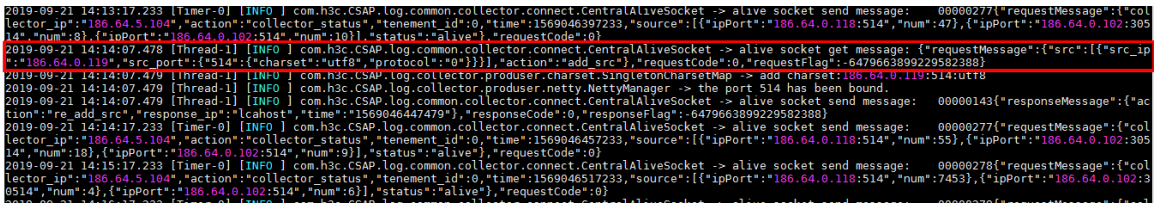
(3) 如重启后仍为离线状态，请联系 H3C 技术支持工程师。

2. 检查该采集器是否关联了日志源

(1) 在“系统配置 > 数据来源 > 日志源管理”页面，查看是否添加了日志源并正确关联了采集器。若未配置日志源，请<新增>按钮添加日志源并关联采集器。



(2) 正确添加日志源后，执行 **cd /data/collector/collector/logs/collector/20xx-xx-xx/info.log** 命令查看采集器日志，若日志显示添加的日志源编码且端口已被监听说明日志源添加成功。如下图所示。



说明

添加日志源或重启采集器均会产生日志源添加日志。

---

3. 日志源添加成功仍接收不到日志

(1) 排查设备侧配置问题。在平台上将设备添加为日志源后，还需在将设备的日志主机配置为平台的采集，检查设备日志主机是否配置为正确采集器、是否发送了日志。

(2) 排查平台路由问题。确保平台与设备之间网络互通。

通过命令行登录平台 cyber5 主机，使用 tcpdump（默认安装）抓包检查网卡是否能接收到 UDP 报文，如果设备收不到 UDP 报文，则应该为网络问题。抓包命令如下，指定要抓取报文类型、目的 IP 地址（日志源 IP 地址）和目的端口。

```
[root@host4 conf]# tcpdump -v dst 182.9.6.211 and udp port 514
tcpdump: listening on br0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

(3) 如以上操作均无法解决，请执行如下命令重启采集器。重启后，大约两分钟后查看是否有采集到日志。若仍不能排除问题，请联系 H3C 技术支持工程师。

```
[root@cyber5 /]# cd /home/adapter-deploy-docker/
[root@cyber5 adapter-deploy-docker]# ./start_docker.sh all restart
```

4.2 日志适配异常

4.2.1 问题描述

添加日志源后，该日志源上报的日志都归类到网元系统日志或其他日志，同时可能存在解析乱码现象。

4.2.2 问题处理步骤

(1) 确定日志源设备类型、编码格式等配置是否正确，以 H3C IPS（V7）设备配置为例，其配置如下图所示。

(2) 若日志源配置正确，请记录归类错误详情，如，攻击日志归类到其他。

(3) 请查看日志适配表，确定日志源设备是否与平台适配过。对于第三方厂商设备，目前不能及时跟进设备版本迭代，若其日志字段调整需重新适配。

(4) 未适配过的设备，需要按第三方日志适配流程进行适配：

a. 购买日志适配服务

b. 提供第三方设备日志手册

c. 将第三方日志设备接入本平台，设备类型选择其他，适配过程中，配合 H3C 技术人员反馈适配结果。

4.3 日志解析错误

4.3.1 问题描述

日志解析错误，例如，日志类型分类错误，暴力破解类日志解析为漏洞利用类，或字段映射错误。

4.3.2 问题处理步骤

请联系 H3C 技术支持工程师，并提供原始日志及解析错误详细描述。

5 安全事件分析

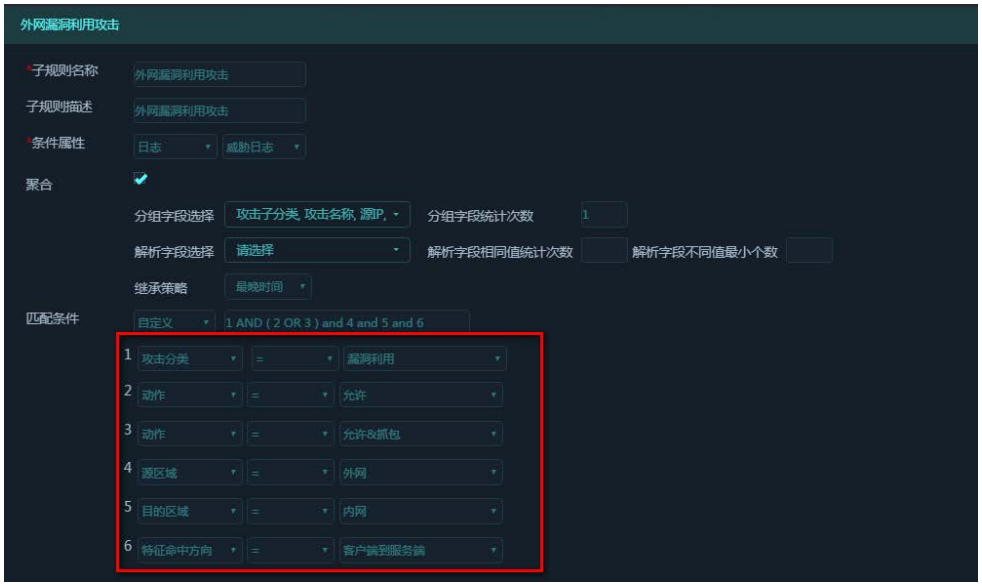
5.1 平台已采集到攻击日志，但无安全事件生成

5.1.1 问题描述

平台已采集到攻击日志生成但未生成安全事件。

5.1.2 问题处理步骤

(1) 确认日志是否满足关联规则匹配条件，如下图（以外网漏洞利用攻击为例），查看攻击日志是否符合匹配条件。



(2) 查看上报该攻击日志的日志源的系统时间与平台时间是否一致，若时间不一致将导致日志解析错误，从而导致安全事件匹配功能异常。

5.2 通过响应联动策略下发安全策略失败

5.2.1 问题描述

通过响应联动下发安全策略到目标设备失败。

5.2.2 问题处理步骤

(1) 平台仅支持对 H3C 防火墙和入侵防御系统设备下发响应联动策略，请确认目标设备是否为 H3C 防火墙和入侵防御系统

(2) 查看 H3C 防火墙和入侵防御系统版本，对照平台版本说明书，确认设备版本是否正确。

5.3 导入漏扫报告到平台后，平台解析的报告内容为空或比实际扫描IP少

5.3.1 问题描述

导入漏扫报告到平台后，平台解析的报告内容为空或比实际扫描 IP 少。

5.3.2 问题处理步骤

本平台仅分析内网资产存在的漏洞情况，对于非内网资产的扫描 IP（外网 IP 和内网用户 IP）均不分析。

6 流量分析

6.1 异常流量页面没有数据

6.1.1 问题描述

日志正常上报，但异常流量页面没有数据。

6.1.2 问题处理步骤

查看上报该攻击日志的日志源的系统时间与平台时间是否一致，若时间不一致将导致日志解析错误，从而导致异常流量分析功能异常。