

序号	名称	状态	责任人
1	正常运行	正常	syslog管理
2	系统异常	异常	syslog管理
3	配置修改	异常	syslog管理
4	用户登录	异常	syslog管理
5	其它日志	异常	syslog管理
6	用户退出	异常	syslog管理

策略中心

- 监听配置
- 事件定义
- 对象管理
- 客户端信息
- 敏感信息
- 事件响应
- 三层关联
- 入侵检测规则
- 交换机信息
- 系统管理

17:17:03
星期日 2020-10-18

风险响应策略

响应策略配置

Windows告警配置

启用:

IP地址:

发送最小时间间隔(分钟):

测试 保存配置

syslog告警配置

启用:

IP地址: 10.1.1.8

端口: 514

测试 保存配置

H3C 数据库审计系统

序号	名称	策略	责任人
1	敏感信息	不可见	syslog管理
2	三层关联	中可见	syslog管理
3	入侵检测规则	不可见	syslog管理

测试连通性正常

策略中心

- 监听配置
- 事件定义
- 对象管理
- 客户端信息
- 敏感信息
- 事件响应
- 三层关联
- 入侵检测规则
- 交换机信息
- 系统管理

17:17:03
星期日 2020-10-18

风险响应策略

响应策略配置

Windows告警配置

启用:

IP地址:

发送最小时间间隔(分钟):

测试 保存配置

syslog告警配置

启用:

IP地址: 10.1.1.8

端口: 514

测试 保存配置

Ping测试正常



修改编码方式，日志正常



对于出现X日志的问题，依次点击设备上的按钮进行测试
最后发现点击测试的时候产生的该日志



在综合日志审计平台抓包查看发现接收到的就是X

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.24	10.28	Syslog	X
2	0.000002	10.24	10.28	Syslog	X
3	0.998952	10.24	10.28	Syslog	X
4	1.998996	10.24	10.28	Syslog	X
5	2.999001	10.24	10.28	Syslog	X

经确认，这个X是为了测试连通性，探测发送的信息，并没有特殊含义，无需在意。

解决方法

1、修改编码方式

名称:

设备类型:

设备型号:

采集器IP:

IP:

厂商:

采集器名称:

日志类型	端口号	编码	例外	编辑
<input type="checkbox"/> Syslog	514	gbk	无	<input type="button" value="编辑"/>

总记录 1 条 < 1 >

2、X日志为了测试连通性探测发送的信息，并没有特殊含义，无需在意。