

知 某局点iMC PLAT将SSL VPN上线的syslog信息升级为告警，用户再次上线不告警

PLAT 李树兵 2019-06-09 发表

组网及说明

略。

问题描述

某局点做SSL VPN认证，设备上认证上线的信息通过syslog日志转发给iMC，iMC侧配置告警规则，将上线信息升级为告警，但是出现第一次上线的时候可以告警，但是用户下线之后再次上线，syslog可以收到，但是不会生成告警，告警也不转发。

过程分析

复现问题，收集debug级别的imcfaultdm日志，在日志中发现告警中存在此oid信息因为重复被过滤。

```
2019-05-27 15:34:46.257 [DEBUG (0)] [THREAD(98592)] [CTrapProcessorTaskMgr::processReceiveTrap] dev:2034 Trap oid: 1.3.6.1.4.1.25506.4.2.8.2.6.20
2019-05-27 15:34:46.257 [DEBUG (0)] [THREAD(99044)] [CTrapProcessorTask::dealTrapData] Trap deal start.
2019-05-27 15:34:46.257 [DEBUG (0)] [THREAD(99044)] [CTrapProcessorTask::dealTrapData] copy data.
2019-05-27 15:34:46.257 [DEBUG (0)] [THREAD(99044)] [CTrapProcessorTask::dealTrapData] Repeat filter.
2019-05-27 15:34:46.257 [DEBUG (0)] [THREAD(99044)] [CTrapProcessorTask::dealTrapData] Trap is repeat,fault_oid = 1.3.6.1.4.1.25506.4.2.8.2.6.20, dev_id = 2034
2019-05-27 15:34:46.347 [DEBUG (0)] [THREAD(91436)] [CDevTrapAdaptor::TrapCB()]
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CTrapProcessorTaskMgr::processReceiveTrap()] Receive A Trap.
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CTrapProcessorTask::convertPduToTrapData] Get Trap from [10.200.251.1]
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CDevBasicInfo::getDevInfo] itDevIPAddrInfo != m_oDevIPMap.end()
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CTrapProcessorTask::getDevIdByIP] iRet == SNACC::AsnDmErrCode::IRST_MSG_FAULT_OPERATION_SUCCESS
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CTrapDefAccessor::findDevTrapSeverity] get resultByDevId failed,dev_id = 2034
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CTrapProcessorTask::convertPduToTrapData] Final Trap source: [10.200.251.1]
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(100156)] [CTrapProcessorTaskMgr::processReceiveTrap] dev:2034 Trap oid: 1.3.6.1.4.1.25506.4.2.8.2.6.20
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(98420)] [CTrapProcessorTask::dealTrapData] Trap deal start.
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(98420)] [CTrapProcessorTask::dealTrapData] copy data.
2019-05-27 15:34:47.251 [DEBUG (0)] [THREAD(98420)] [CTrapProcessorTask::dealTrapData] Repeat filter.
2019-05-27 15:34:47.252 [DEBUG (0)] [THREAD(98420)] [CTrapProcessorTask::dealTrapData] Trap is repeat,fault_oid = 1.3.6.1.4.1.25506.4.2.8.2.6.20, dev_id = 2034
```

通过查看此oid信息确认为iMC Syslog的oid信息，故怀疑为iMC侧重复Trap过滤导致将这个Syslog的告警信息给过滤掉了。

选取Trap

Trap名称

Trap OID

1.3.6.1.4.1.2550

企业名称

企业ID

查询

重置

☒ iMC Syslog(1.3.6.1.4.1.25506.4.2.8.2)

确定

取消

10月13日 18:45

解决方法

在重复Trap过滤中将这个oid 1.3.6.1.4.1.25506.4.2.8.2.6.20 的Trap信息设置为不重复的Trap之后问题解决。

过滤规则 > 重复Trap过滤配置

重复Trap过滤配置

不过滤的重复Trap

Management

AC负载均衡使能(3Com 802.11 AC)

无线用户解除关联(3Com 802.11 Client)

无线用户下线(3Com 802.11 Client)

Syslog升级的告警(iMC Syslog)

选取Trap

删除Trap

☒ 升级为告警(系统收到超过阈值的重复Trap后产生一条新告警)

阈值(1-5000) *

1

☐ 过滤重复Trap(在指定时间窗和Trap队列长度内连续收到重复Trap只上报一次)

时间窗长度(1-1500 分) *

10

Trap队列长度(100-10000) *

5000

☒ 使用滚动时间窗

确定

取消