

iMC无法收到设备trap告警的排查思路

一、组网

使用iMC智能管理中心管理设备的网络。

二、问题描述

在配置好设备的SNMP参数并开启trap功能后，iMC就可以对设备工作状态和配置等进行管理，并且可以通过接收设备发送过来的trap报文来发现设备的异常情况，产生告警来提醒管理员。但是有时候由于配置或者其他方面的错误，导致iMC无法产生设备的告警信息，影响管理员对设备的管理。

三、问题分析

造成这种情况的原因通常是设备侧或者iMC侧配置的问题，排查时需要理解iMC产生告警的工作流程，并且顺着trap告警产生的流程来一步一步的进行定位，详细请见下文说明。

四、解决方法

1. 确认设备开启了SNMP功能，并且配置的SNMP读写团体字与iMC添加此设备时使用的一致。如果使用的SNMPv3还需要确认是否定义了正确的mib-view，usergroup，user和加密认证方式，并且相互之间的关联关系配置正确。

2. 确认设备配置的SNMP trap命令指定了正确的iMC地址和端口，并且trap源地址和iMC对设备的管理地址一致，及正确的securityname参数。如下所示为SNMP的配置：

SNMP V2C：

snmp-agent

snmp-agent local-engineid 800063A203000FE2456BC0

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info version all

snmp-agent target-host trap address udp-domain 172.16.0.2 params securityname public v2c

SNMP V3：

snmp-agent

snmp-agent local-engineid 800063A2033CE5A614D887

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info location Hangzhou,china

snmp-agent sys-info version all

snmp-agent group v3 gv3 read-view default write-view default

snmp-agent target-host trap address udp-domain 172.16.0.2 params securityname uv3 v3 privacy

snmp-agent mib-view included default iso

snmp-agent usm-user v3 uv3 gv3 cipher authentication-mode md5 \$c\$3\$cGTH6tjGCEPk2vNktubH4D6G6aC6j/ydJH+NO+FM0Gt8Q== privacy-mode aes128 \$c\$3\$svyPbl13iilGYX5DntKBUX603gXeffMc+6xQB1CkgLvvcG==

3. 确认设备的全局和各功能模块SNMP trap功能是否开启，设备的trap功能是可以针对某模块单独设置开启或关闭的，如果能收到设备的一部分trap信息，另一部分trap信息收不到，那很可能就是这个功能模块的trap没有开启，如下命令为开启OSPF接口状态变化trap：

[H3C]snmp-agent trap enable ospf ifstatechange

4. display trapbuffer查看设备有没有向iMC发送trap信息，如下：

[H3C]dis trapbuffer

Trapping buffer configuration and contents:enabled

Allowed max buffer size : 1024

Actual buffer size : 256

Channel number : 3 , channel name : trapbuffer

Dropped messages : 0

Overwritten messages : 0

Current messages : 127

#Apr 27 06:50:24:861 2000 H3C HWCM/4/TRAP:

1.3.6.1.4.1.25506.2.4.2.1 configure changed: EventIndex=6,Command Source=1,ConfigSource=2,ConfigDestination=4

#Apr 27 06:51:53:405 2000 H3C IFNET/4/INTERFACE UPDOWN:

Trap 1.3.6.1.6.3.1.1.5.3: Interface 9437188 is Down, ifAdminStatus is 1, ifOperStatus is 2

#Apr 27 06:52:47:596 2000 H3C HWCM/4/TRAP:

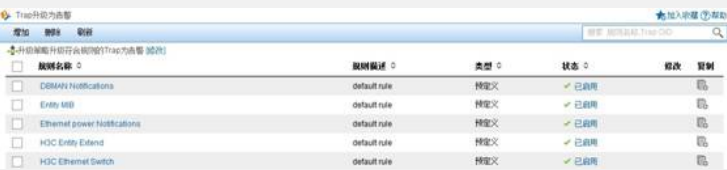
1.3.6.1.4.1.25506.2.4.2.1 configure changed: EventIndex=7,Comman

dSource=2,ConfigSource=4,ConfigDestination=2
如果这里确实已经显示设备向正确的接收地址发送了trap报文，侧证明设备的配置没有问题。
5.在iMC服务器上抓包查看是否收到了对应的trap报文，如果没有收到请检查网络中路由，防火墙等是否配置正确，iMC服务器是否使用了正确的端口来接收trap，并且此端口没有被其他进程占用。
6.以上步骤排查都没有问题后，就应该可以在iMC的trap浏览里面看到对应的trap记录了，注意这里的排序方式，最好使用设备IP地址，或者trapOID来搜索一下，如果确认没有，则可能是被所配的trap过滤规则过滤掉了，查看重复trap过滤，未知trap过滤和其他自定义的trap过滤规则是不是和当前要接收的trap匹配。确认trap是否为未定义可以到“trap定义一览表”里查看，如下图：



Trap名称	Trap OID	企业名称(企业ID)	Trap严重	Trap类型	设备信息	修改	删除
☐ 15分链路故障告警	1.3.6.1.4.1.2011.2.23.11.2.6.2...	S8016(1.3.6.1.4.1.2011.2.23.11...	告警	预定义	无		
☐ 24小时链路故障告警	1.3.6.1.4.1.2011.2.23.11.2.6.2...	S8016(1.3.6.1.4.1.2011.2.23.11...	告警	预定义	无		
☐ 400输入告警	1.3.6.1.4.1.2011.2.17.6.50	Huawei HEB0 Traps(1.3.6.1.4.1...	告警	预定义	无		
☐ 400输入告警配置	1.3.6.1.4.1.2011.2.17.6.51	Huawei HEB0 Traps(1.3.6.1.4.1...	告警	预定义	无		
☐ 802.1d用户认证成功	1.3.6.1.4.1.11.2.14.11.10.2.26...	HP Port Security Notifications...	警告	预定义	无		

7.如果trap浏览里已经可以看到trap记录了，但还是没有告警生成，那首先确认这条trap已经定义，并且trap升级为告警规则中已配置将这条trap升级为告警，如下图：



规则名称	规则描述	类型	状态	修改	复制
☐ DEFAULT Notifications	default rule	预定义	已启用		
☐ Entity MIB	default rule	预定义	已启用		
☐ Ethernet power Notifications	default rule	预定义	已启用		
☐ H3C Entity Extend	default rule	预定义	已启用		
☐ H3C Ethernet Switch	default rule	预定义	已启用		

8.如果以上各步都没有问题，还是收不到告警时，请收集具体信息联系业务软件二线进行定位。反馈设备软硬件版本及配置，iMC版本，无法产生告警的trapOID，iMC过滤规则，trap定义等配置截图，以及告警进程的debug级别日志。

日志收集方式为：

```
C:\Program Files\iMC\server\conf目录下打开qvdm.conf文件，修改其中字段
#setting log level (DEBUG, INFO, WARNING, ERROR, FATAL)
LogLevel = INFO      //该处将INFO修改为DEBUG
#setting log expire (its unit is day)
LogExpire = 15
```

在部署监控代理中重启imcfaultdm.exe进程，触发设备发送相应trap到iMC，完成后，将日志级别恢复到INFO级别，并重启告警进程。反馈C:\Program Files\iMC\server\conf\log下imcfaultdm.txt。