iMC 设备管理及常见问题分析

随着互联网极大丰富，5G 时代的到来，运维的方便成为极大的竞争力。SNMP 作为业界大家认可及广泛使用的运维协议，已在 H3C 自研设备上实现。为了更好的帮助管理员管理设备，H3C 的 iMC 管理平台提供了完善的设备管理功能。通过对网络设备进行基本配置，将其增加到 iMC 中实现集中管理，iMC 可以自动完成识别设备、获取设备配置及运行信息、计算相关网络拓扑、接收 Trap 以及自动采集设备性能指标等操作。

一、SNMP 介绍

SNMP（Simple Network Management Protocol）是简单网络管理协议，广泛应用于管理设备对被管理设备的访问和管理。其工作方式主要分为三种，分别为 Get、Set 和 Trap。“Get”指令用于管理员向设备获取数据；“Set”指令用于管理员向设置执行设置操作；当设备发生重要状况改变时，需要向管理员通报事情的发生，此时需要“Trap”操作指令。

H3C 网络设备和 iMC 平台支持 SNMP 协议的三个版本，分别为 SNMPv1，SNMPv2c 及 SNMPv3。管理员可根据需要选择使用其中的任意一个版本，iMC 平台中，默认为 SNMPv2c 版本。图 1 给出了网络管理站与被管理设备之间通过 SNMPv2c 协议的通信报文信息。GetRequest、 GetNextRequest 和 SetRequest 是一种简单的请求加应答的操作方式，网络管理者使用随机源端口向网管代理的 UDP 端口 161 发送请求，网管代理使用 UDP 端口 161 作为源端口，向请求中的随机源端口发送回应 Get-response。SNMP Trap 由网管代理向网络管理者主动上报事件的操作，使用随机源端口向网络管理者的 UDP 端口 162 发送 Trap。

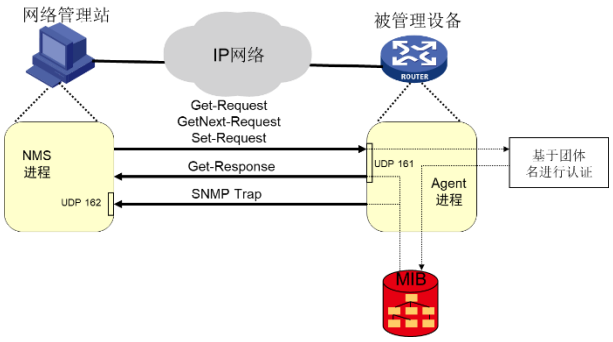


Figure 1

SNMPv1 和 SNMPv2c 使用团体来进行安全机制管理，每个团体通过团体名即一个字符串来区别，团体名实际上是一个相关权限的密码，规定了可以管理者可以访问的节点以及访问的类型（读/写）。要使用 iMC 平台的设备配置管理，则必须在 iMC 服务器和被管设备上配置一致的 SNMP 团体字。SNMPv3 相对于 SNMPv2c 最重要的改进，在于提出了一种全新的基于用户的安全模型，管理员可以通过配置认证和加密功能，使 SNMP 报文传输的安全性得到显著提高。要 iMC 平台与被管理设备之间通过 SNMPv3 通信，需要在两者上配置一致的用户

信息，加密和认证算法及密钥。SNMPv1, SNMPv2c 和 SNMPv3 版本对比如图 2 所示。

	PDU支持情况	安全级别	认证	加密
SNMPv1	Get、GetNext、Set、Trap、GetResponse	noAuthNoPriv	community	NO
SNMPv2c	Get、GetNext、Set、Trap、Inform、GetResponse、GetBulk	noAuthNoPriv	community	NO
SNMPv3	Get、GetNext、Set、Trap、Inform、GetResponse、GetBulk	noAuthNoPriv AuthNoPriv AuthPriv	MD5 SHA	DES AES

Figure 2

二、iMC 设备管理

在 iMC 中增加设备时，需要进行两步操作，一是配置被管理设备的 SNMP 参数；二是在 iMC 中增加配置设备，并将 iMC 中的 SNMP 版本及参数与被管理设备设置一致。当设备数量较少时，在 iMC 中可用手工增加设备；当被管理设备数量较多时，使用 iMC 自动发现功能系统能自动发现符合条件的可管理设备。以下所有 iMC 界面，均为 iMC PLAT 7.3 版本界面。

（一） 通过 SNMPv2c 进行设备管理

1. 配置设备的 SNMP 参数

如：将读团体字设置为 public，写团体字设置为 private，当设备发生重大情况时，上报给 ip 地址为 192.168.127.69 的网络管理站。

[] snmp
[] snmp community read public
[] snmp community write private
[] sys-info version all
[] trap enable
[] snmp target-host trap address udp-domain 192.168.127.69 params securityname public
[] save

2. iMC 中增加配置设备

以手工配置为例，在资源—资源管理—增加设备界面下，手动输入被管理设备的主机名或 ip 地址，并将 SNMP 的读团体字设为 public，写团体字设为 private。如图 3 所示

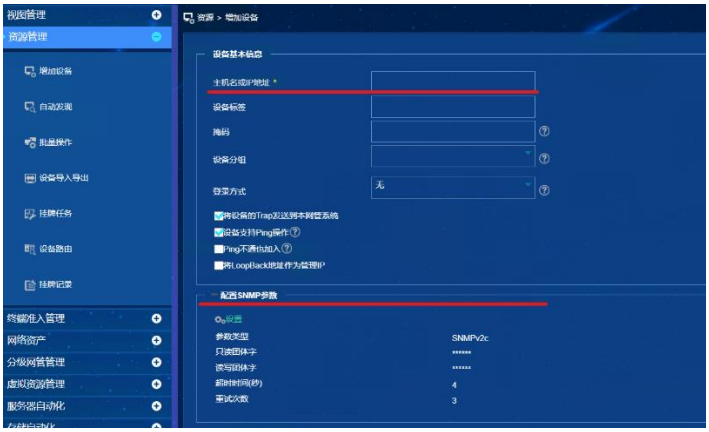


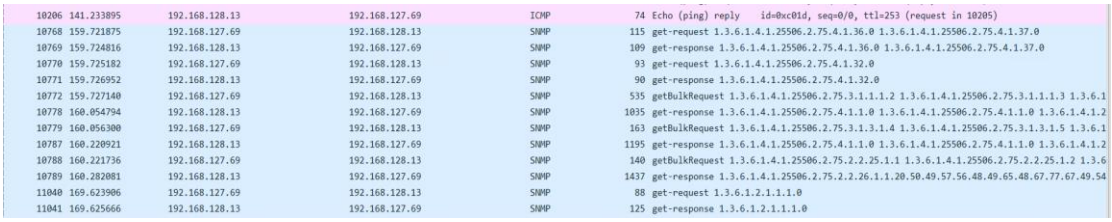
Figure 3

3. wireshark 抓包分析

iMC 服务器 ip: 192.168.127.69

被管理设备 ip: 192.168.128.13

正常通信时，iMC 发送一个请求报文，设备会给一个回应报文。



10206	141.233895	192.168.128.13	192.168.127.69	ICMP	74	Echo (ping) reply id=0xc01d, seq=0/0, ttl=253 (request in 10205)
10768	159.721875	192.168.127.69	192.168.128.13	SNMP	115	get-request 1.3.6.1.4.1.25506.2.75.4.1.36.0 1.3.6.1.4.1.25506.2.75.4.1.37.0
10769	159.724816	192.168.128.13	192.168.127.69	SNMP	109	get-response 1.3.6.1.4.1.25506.2.75.4.1.36.0 1.3.6.1.4.1.25506.2.75.4.1.37.0
10770	159.725182	192.168.127.69	192.168.128.13	SNMP	93	get-request 1.3.6.1.4.1.25506.2.75.4.1.32.0
10771	159.726952	192.168.128.13	192.168.127.69	SNMP	90	get-response 1.3.6.1.4.1.25506.2.75.4.1.32.0
10772	159.727140	192.168.127.69	192.168.128.13	SNMP	535	getBulkRequest 1.3.6.1.4.1.25506.2.75.3.1.1.1.2 1.3.6.1.4.1.25506.2.75.3.1.1.1.3 1.3.6.1
10778	160.054794	192.168.128.13	192.168.127.69	SNMP	1035	get-response 1.3.6.1.4.1.25506.2.75.4.1.1.0 1.3.6.1.4.1.25506.2.75.4.1.1.0 1.3.6.1.4.1.2
10779	160.056300	192.168.127.69	192.168.128.13	SNMP	163	getBulkRequest 1.3.6.1.4.1.25506.2.75.3.1.3.1.4 1.3.6.1.4.1.25506.2.75.3.1.3.1.5 1.3.6.1
10787	160.220921	192.168.128.13	192.168.127.69	SNMP	1195	get-response 1.3.6.1.4.1.25506.2.75.4.1.1.0 1.3.6.1.4.1.25506.2.75.4.1.1.0 1.3.6.1.4.1.2
10788	160.221736	192.168.127.69	192.168.128.13	SNMP	140	getBulkRequest 1.3.6.1.4.1.25506.2.75.2.2.25.1.1 1.3.6.1.4.1.25506.2.75.2.2.25.1.2 1.3.6
10789	160.282081	192.168.128.13	192.168.127.69	SNMP	1437	get-response 1.3.6.1.4.1.25506.2.75.2.2.26.1.1.20.50.49.57.56.48.49.65.48.67.77.67.49.54
11040	169.623906	192.168.127.69	192.168.128.13	SNMP	88	get-request 1.3.6.1.2.1.1.1.0
11041	169.625666	192.168.128.13	192.168.127.69	SNMP	125	get-response 1.3.6.1.2.1.1.1.0

Figure 4

（二） 通过 SNMPv3 进行设备管理

1. 配置设备的 SNMP 参数

如：创建 mib 视图，名字为 cmibview, 包含 mib 库中 iso 下的所有内容，并创建 v3 组，名字为 cv3group, 将 mib 库 cmibview 加入到该组中，开通读、写和通知权限。在 cv3group 中加入用户 cicysnmp,并设置验证和加密传输算法，密钥均为 adminkey。最后，设置 trap 的目标主机为 192.168.127.68

[] snmp

[] snmp-agentsys-info version all

[] snmp-agent mib-view included cmibview iso

[] snmp-agent group v3 cv3 group read-view cmibview write-view cmibview notify-view cmibview

[] snmo-agent usm-user v3 cicysnmp cv3group simple authentication-mode md5 adminkey privacy-mode des56 adminkey

[] snmp-agent trap enable

[] snmp-agent target-host trap address udp-domain 192.168.127.68 params securityname cicysnmp v2 privacy

2. iMC 中增加配置设备

对于 SNMPv3 版本，首先需要在系统管理—资源管理—访问参数模板—SNMP 中增加 SNMPv3 模板，如图 5 所示，用户名，认证和加密算法和密码与被管理设备中参数一致。

在增加设备界面中，在“配置 SNMP 参数”界面下，参数类型选择自己创建的模板，如图 6 所示

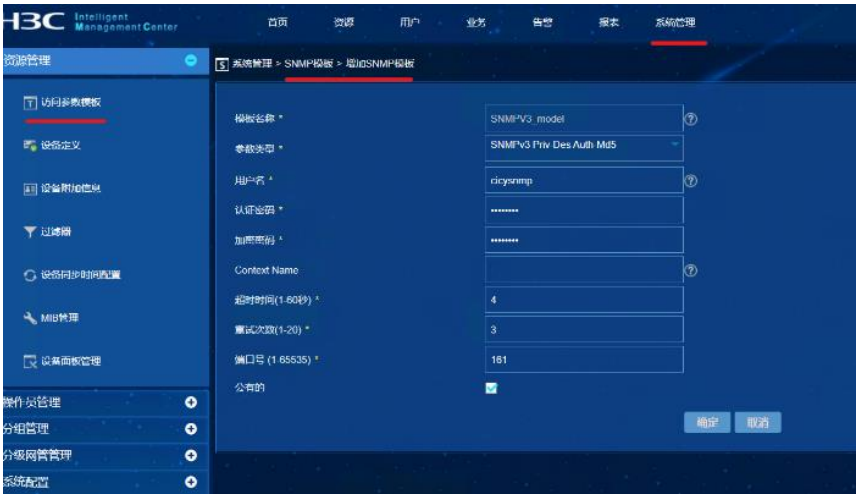


Figure 5

Figure 6

3. Wireshark 抓包分析

由于设置了加密算法，所以报文以密文信息传输，显示 encryted PDU: Privkey Unknow.

26435	547.957366	192.168.128.13	192.168.127.68	SNMP	211	encryptedPDU: privKey Unknown
26550	551.970048	192.168.128.13	192.168.127.68	SNMP	211	encryptedPDU: privKey Unknown
26598	553.943363	192.168.127.68	192.168.128.13	ICMP	74	Echo (ping) request id=0x2022, seq=19208/2123, ttl=128 (reply in 26599)
26599	553.945077	192.168.128.13	192.168.127.68	ICMP	74	Echo (ping) reply id=0x2022, seq=19208/2123, ttl=253 (request in 26598)
26651	555.958211	192.168.128.13	192.168.127.68	SNMP	211	encryptedPDU: privKey Unknown
26659	556.069567	192.168.127.68	192.168.128.13	SNMP	214	encryptedPDU: privKey Unknown
26663	556.075944	192.168.128.13	192.168.127.68	SNMP	209	encryptedPDU: privKey Unknown
26761	559.959325	192.168.128.13	192.168.127.68	SNMP	211	encryptedPDU: privKey Unknown

Figure 7

（三） 设备详细信息

添加单台设备后，在 iMC 中查看到的设备详细信息如图 8 所示

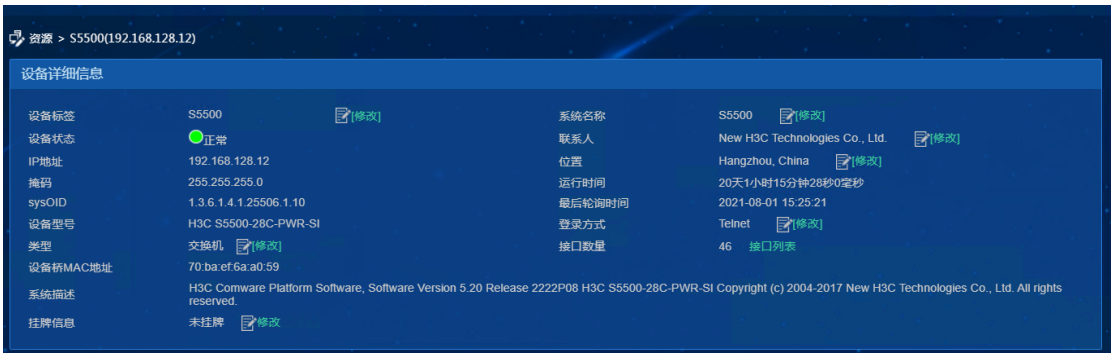


Figure 8

三、iMC 设备管理常见问题分析

（一）设备数量超出 License 限制

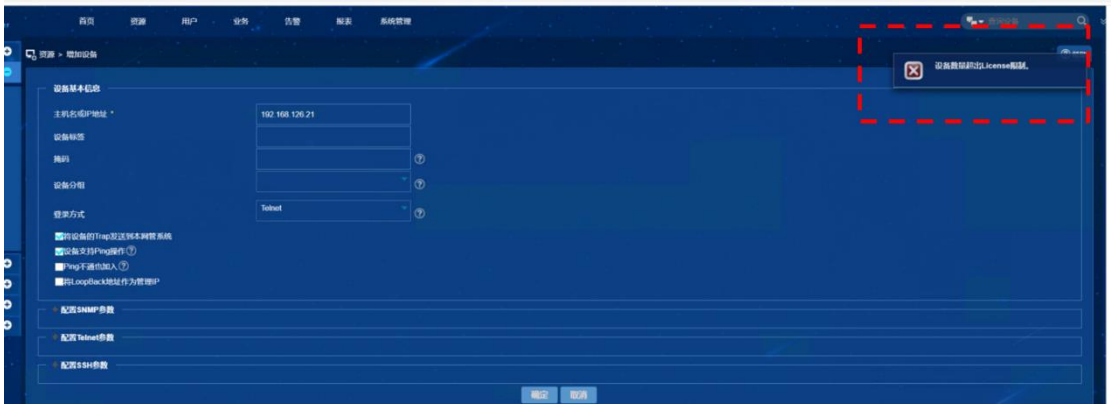


Figure 9

解决方案：

a. 申请注册更多 iMC PLAT 节点数的 License
b. 在设备视图中删除已有设备

（二）设备识别为 ICMP

事实上，添加设备为 ICMP 时可以依次检查以下配置：

a. 设备上有没有正确启用 SNMP；
b. 设备上的 SNMP 参数是否与服务器保持一致，包括 SNMP 版本，SNMP 读写团体字；
c. 设备到防火墙之间有无 ACL 或防火墙屏蔽 UDP 161/162 端口的通信。

以下为一些常见错误的案例分析。

1. 设备识别为 ICMP—SNMP 读写团体字配置错误或未配置

如被管理交换机上未设置读写团体字。

通过 wireshark 抓包分析，发现交换机向 iMC 服务器上报 Trap 信息。查看任意一条 Trap 报文，Trap 类型为 4，表示 SNMP 协议报文中的团体字无效。

23409	623.539377	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23434	624.612324	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23504	627.554047	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23529	628.611498	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23621	631.583889	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23648	632.613205	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23672	633.524635	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
23893	636.612005	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10
24298	642.636901	192.168.128.12	192.168.127.68	SNMP	89 trap iso.3.6.1.4.1.25506.1.10

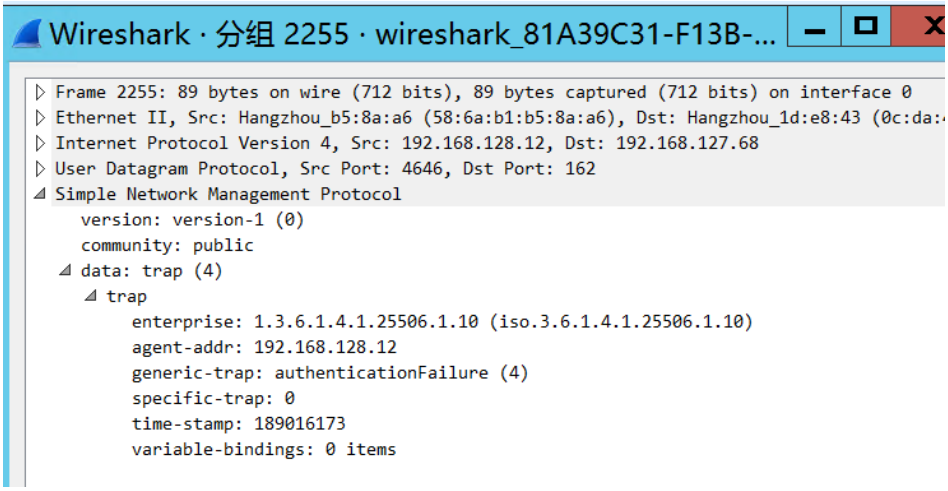


Figure 10

解决方案：将 iMC 管理平台与被管理设备的团体字设置一致。

2. 设备识别为 ICMP—iMC 平台与被管理设备 SNMP 版本不一致。

如在 iMC 服务器上添加设备设置 SNMP 参数为 SNMPv3，但在被管理设备上只进行了 SNMPv2c 相关参数的配置。

通过 wireshark 抓包分析，iMC 服务器(192.168.127.68)发送请求及报文和加密报文，但设备端(192.168.128.12)回应的报文，缺少了用户名，加密及认证信息。iMC 服务器与设备端发送的报文信息不一致，不能正常通信。

1242…	2038.857573	192.168.128.12	192.168.127.68	TCP	60 [TCP Keep-Alive] 23 → 50976 [ACK] Seq=3331 Ack=222 Win=32768 Len=0
1242…	2038.857612	192.168.127.68	192.168.128.12	TCP	54 [TCP Keep-Alive ACK] 50976 → 23 [ACK] Seq=222 Ack=3332 Win=62836 Len=0
1250…	2044.287946	192.168.127.68	192.168.128.12	SNMP	109 get-request
1250…	2044.315186	192.168.128.12	192.168.127.68	SNMP	153 report 1.3.6.1.6.3.15.1.1.4.0
1250…	2044.327212	192.168.127.68	192.168.128.12	SNMP	186 encryptedPDU: privKey Unknown
1250…	2044.335909	192.168.128.12	192.168.127.68	SNMP	161 report 1.3.6.1.6.3.15.1.1.3.0
1252…	2045.037863	192.168.127.68	192.168.128.12	TELNET	56 Telnet Data ...

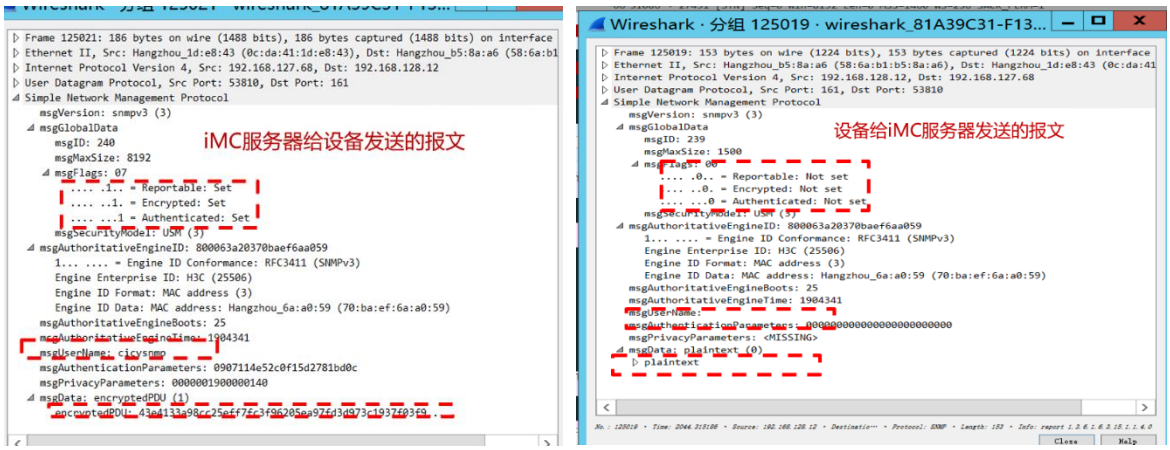


Figure 11

解决方案：将 iMC 管理平台与被管理设备的 SNMP 版本及参数设为一致。

3. 设备识别为 ICMP—设备上设置 acl 过滤

设备到防火墙之间设置 ACL 过滤，如以 SNMPv2c 版本为例

[] acl number 2002

[] rule deny source 192.168.127.68 0

[] snmp-agent community read public acl 2002

[] snmp-agent community write private acl 2002

此时，通过 wireshark 抓包可发现，由于设备拒绝了来自 iMC 服务器的报文，所以尽管 iMC 服务器不停的发请求报文，但被管理设备无响应报文回复。该故障与防火墙屏蔽 UDP 161/162 端口的通信故障相同。

Figure 12

解决方案：更改 acl 过滤条件或防火墙信息，允许来自 iMC 服务器的访问。

（三）设备型号为其他 SNMP 设备

iMC 平台支持对不同种类、不同厂家和不同型号的设备进行管理，对于友商的设备，导入 iMC 平台之后，会识别为其他 SNMP 设备，此时可在系统管理—设备定义—增加设备型号中，手动选择已导入的设备定义。