

组网及说明

被扫描端点与网络设备直连，且与扫描器网络可达。

问题描述

随着物联时代的发展，时刻都会有新的端点（笔记本电脑、智能手机和平板电脑，各种形式和规模的P物联网设备，服务器）加入网络。这些设备会增大网络的受攻击范围，并且许多安全设备都无法感知。

iMC EPS即鹰视系统是物联时代的准入系统，可以对PC终端、哑终端（摄像头、IP电话、门禁等）、网络设备、服务器等接入网络及时感知，并进行持续监控。可以精准识别接入网络的端点、设备的类型及详细信息，还可以对非法接入的端点、设备主动阻断。

阻断的方式根据其实现原理分为两类：1、EPS与EIA联动方式控制准入；2、EPS与扫描器联动通过SNMP方式控制准入。

本案例主要讲述iMC EPS与扫描器联动通过SNMP方式控制终端准入方案中，出现无法阻断问题的排查。

过程分析

故障定位思路：

- 1.检查iMC EPS所在服务器的硬件性能信息符合要求规范，iMC部署中各个组件与PLAT、扫描器的适配关系是否满足版本说明书的适配要求，然后保证iMC监控代理中jserver.exe进程、相关组件的业务进程正常和EPS扫描器的服务正常启动。
- 2.检查扫描器状态是否正常，扫描任务配置的条件是否满足要求。
- 3.需要确认端点详细信息中是否正常学习到上连设备的IP和接口信息，若未正常学习到该信息，需要确认设备命令行和对应的mib节点中是否能正常获取到MAC地址表情况

解决方法

1、iMC服务器安装部署规范检查

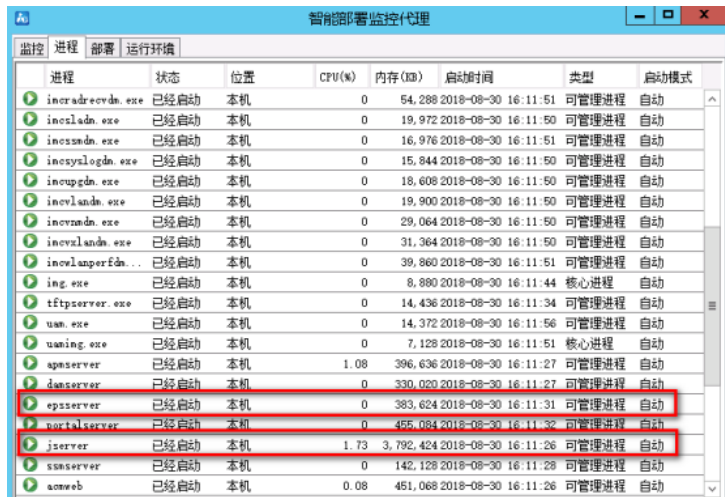
服务器性能是保证iMC认证系统稳定运行的基本要素，所以排查问题是首先需要确认服务器软硬件配置情况。请对照《智能管理中心（iMC）部署和硬件配置方案》查询这套iMC服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行iMC最基本的部署要求。（1）对照《方案》检查服务器CPU、内存、硬盘等是否合乎规格，如果扫描的端点数量大、扫描的实时性要求高，是否根据《方案》要求将组件分布式部署在性能良好的服务器上。重点需要检查内存占用是否过高，内存大小是否满足《方案》计算出的要求，操作系统是否是高性能的x64版本。

2、检查iMC部署中版本适配关系

iMC中各个业务组件与平台有依赖关系，部分业务组件之间也有依赖关系，各个业务组件版本与平台版本有一定的适配关系，针对这一问题在EPS组件的版本说明书中有明确的适配要求。以iMC EPS 7.3 E0601版本为例，其版本说明书中明确要求适配的PLAT版本为iMC PLAT 7.3 E0506P09以及其后续版本。

3、检查相关进程是否正常启动

iMC EPS组件包含前台和后台以及扫描器三部分，其中前台进程为jserver，后台进程为epsserver，如图所示服务器侧进行正常启动。



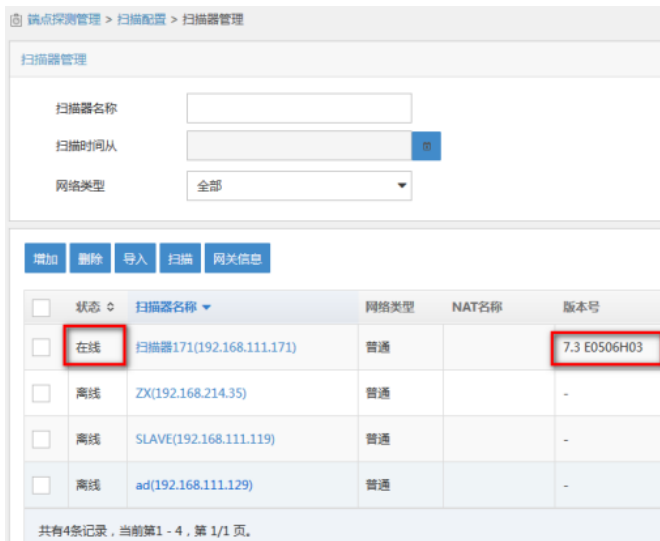
进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
incradreecd.exe	已经启动	本机	0	54,288	2018-08-30 16:11:51	可管理进程	自动
inectlnd.exe	已经启动	本机	0	19,972	2018-08-30 16:11:50	可管理进程	自动
incssnd.exe	已经启动	本机	0	16,976	2018-08-30 16:11:51	可管理进程	自动
incsyslogd.exe	已经启动	本机	0	15,844	2018-08-30 16:11:50	可管理进程	自动
incupgd.exe	已经启动	本机	0	18,608	2018-08-30 16:11:50	可管理进程	自动
inevlnd.exe	已经启动	本机	0	19,900	2018-08-30 16:11:50	可管理进程	自动
incvnd.exe	已经启动	本机	0	29,064	2018-08-30 16:11:50	可管理进程	自动
incvulnd.exe	已经启动	本机	0	31,364	2018-08-30 16:11:50	可管理进程	自动
incvlsuperfd...	已经启动	本机	0	39,860	2018-08-30 16:11:51	可管理进程	自动
ing.exe	已经启动	本机	0	8,880	2018-08-30 16:11:44	核心进程	自动
tftpsvr.exe	已经启动	本机	0	14,436	2018-08-30 16:11:34	可管理进程	自动
usn.exe	已经启动	本机	0	14,372	2018-08-30 16:11:56	可管理进程	自动
using.exe	已经启动	本机	0	7,128	2018-08-30 16:11:51	核心进程	自动
apsrver	已经启动	本机	1.08	396,636	2018-08-30 16:11:27	可管理进程	自动
dnsrver	已经启动	本机	0	330,020	2018-08-30 16:11:27	可管理进程	自动
epsserver	已经启动	本机	0	383,624	2018-08-30 16:11:31	可管理进程	自动
nortalsrver	已经启动	本机	0	455,084	2018-08-30 16:11:32	可管理进程	自动
jserver	已经启动	本机	1.73	3,792,424	2018-08-30 16:11:26	可管理进程	自动
ssnsrver	已经启动	本机	0	142,128	2018-08-30 16:11:28	可管理进程	自动
awweb	已经启动	本机	0.08	451,068	2018-08-30 16:11:26	可管理进程	自动

EPS扫描器侧服务正常启动，如下图所示。



4. 扫描器状态和配置检查

登录扫描器所在的操作系统，按照步骤3确认扫描器服务正常启动后，在iMC EPS服务器侧检查扫描器的状态信息。



扫描器状态栏显示扫描器的状态，若确认扫描器服务器已经启动，iMC EPS侧扫描器状态始终为离线，则需要检查如下信息：

1)扫描器到iMC EPS所在服务器的网络通信情况。确认扫描器到iMC EPS之间的网络可达，若扫描器与iMC EPS之间涉及防火墙等设备时需要注意放通对应端口，其中iMC EPS使用端口UDP 6060，扫描器使用端口为UDP 12000。

2)扫描器与iMC EPS之间的共享密钥配置一致。在【用户】|【端点探测管理】|【系统管理】|【系统参数】中，配置“共享密钥”的值。

5. 扫描任务配置检查

扫描任务基于其实现原理的不同，分为两种类型：

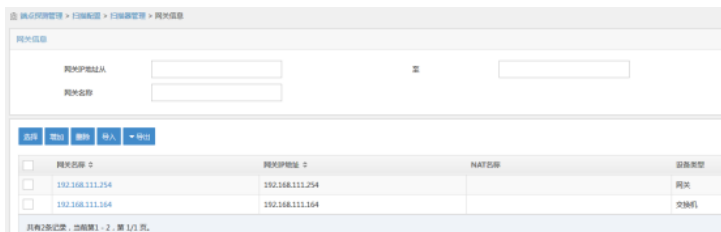
1)基于IP网段方式的扫描

即扫描的对象为IP网段，此时扫描器需要逐个探测网段中每个IP的通断情况和端点信息。配置任务时仅需要输入网段信息，扫描前需要进行自动发现，使用这种方式扫描时速度相对较慢，不能跨网段获取端点的MAC地址信息，也无法获取端点的上连设备IP和端口情况。

2)基于网关方式的扫描

即扫描的对象为终端的网关设备，此时需要在配置扫描任务前，将端点所有上连设备以及网关信息纳管至iMC EPS组件中，并在配置扫描任务时选择对应的上连设备和网关设备。扫描器通过获取设备的ARP等表项信息获取端点信息，使用这种方式扫描时速度相对较快，可以识别端点的MAC地址信息，也可以根据设备的表项获取端点的上连设备IP和端口，从而实现在判断该端点非法时，将端点的上联口shut down，阻断其接入至网络中。

本文重点检查基于网关方式的扫描，在【用户】|【端点探测管理】|【扫描配置】|【扫描器管理】中，点击“网关信息”，确认端点上连设备和端点网关设备均纳管至其中。



同时需要确认网络设备的类型与实际组网一致，SNMP参数配置正确。

端点探测管理 > 扫描配置 > 扫描器管理 > 网关信息 > 修改网关信息

修改网关信息

基本参数

网关名称 *	192.168.111.254
网关IP地址 *	192.168.111.254
设备类型 *	网关
网络类型 *	普通

SNMP参数

SNMP参数类型 *	SNMPv2c
只读团体字	*****
读写团体字	*****
超时时间(1-60秒)	4
重试次数(1-20)	3

在配置扫描任务时，注意选择对应的网关设备和上连设备的信息。如下图所示，检查扫描IP网关/IP网段列表的配置情况，注意不允许出现仅配置IP网段的情况。

端点探测管理 > 扫描配置 > 扫描器管理 > 修改扫描器

扫描器名称: 扫描器171

扫描器类型: 普通

扫描器IP地址: 192.168.111.171

扫描器IP网段列表

扫描器IP网段名称	IP地址	网段	设备类型
192.168.111.164	192.168.111.164	-	交换机
192.168.111.254	192.168.111.254	192.168.111.1-192.168.111.254	网关

6. 端点详细信息学习情况检查

确认上述基础检查条件配置正常后，需要检查端点详细信息中设备上连设备的IP和端口学习情况，即在【用户】|【端点探测管理】|【所有端点】中搜索该端点的IP或MAC地址信息，点击端点的IP地址查看端点详细信息。在端点详细信息中确认接入交换机IP和接入交换机端口信息是否正常学习。

端点探测管理 > 端点详细信息

端点详细信息

IP地址	192.168.111.252	设备	配置
在线状态	离线	在线状态	配置
MAC地址	487ADAAAC813F	设备类型	PC
操作系统	Linux	端口	Linux
扫描时间	2018-07-17 05:11:03	更新时间	2018-06-21 11:26:17
接入交换机IP	192.168.111.*	接入交换机端口	-
基础MAC地址	487ADAAAC813F	基础设备类型	PC
基础操作系统	Linux	基础端口	Linux
设备类型	普通	NAT策略	
扫描器	SLAVE		

7. 设备学习情况检查

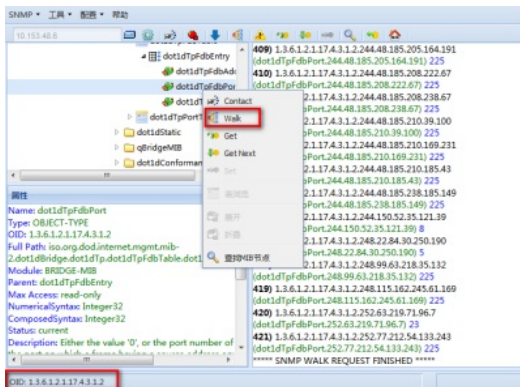
在设备侧确认ARP表项和MAC地址表学习情况，是否包含当前端点的IP地址。

```
[RT1]dis arp 192.168.1.123
Type: S-Static      D-Dynamic      A-Authorized
IP Address          MAC Address     VLAN ID         Interface       Aging Type
192.168.1.123      0cda-411d-0e76 N/A             GE0/1           10           D
```

iMC EPS在获取设备ARP表项的同时，还会获取设备的MAC地址表学习情况。由于设备版本不同，iMC EPS获取设备MAC地址表时使用的mib节点也不相同，以iMC EPS E0602版本为例，iMC EPS产品会先后获取的设备的1.3.6.1.2.1.17.7.1.2.2.1.2节点和1.3.6.1.2.1.17.4.3.1.2节点，确认通过该节点能否正常获取设备的表项信息。iMC PLAT有足够授权时，可以将该网关设备和端点上连交换机设备纳管至iMC PLAT中，配置与EPS相同的SNMP参数，在iMC PLAT前台页面右上角直接搜索设备IP，点击设备IP进入设备详细信息页面。并单击“mib管理”。



在弹出的页面中找到OID为1.3.6.1.2.1.17.4.3.1.2，然后鼠标右键选择walk该节点。此时右侧会出现该节点的返回值。如下图所示，该节点未返回任何信息，则表示当前无法从设备的该节点获取到设备的MAC地址学习情况。



类似地，找到OID为1.3.6.1.2.1.17.7.1.2.2.1.2的节点，确认该节点的返回值情况。