🔎 iMC EPS与扫描器联动无法实现SNMP阻断问题排查

iMC EPS 张鑫 2018-09-29 发表

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l 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。

故障定位思路:

过程分析

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 E 0601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。

h			î	明節署!	监控代理			l		x
监持	2 进程 部署 运行	环境								
	进程	状态	位置	CPU(%)	内存(128)	启动时间		类型	启动模式	
0	incradrecydm. exe	已经启动	本机	0	54, 288	2018-08-30	16:11:51	可管理进程	自动	^
0	incsladn. exe	已经启动	本机	0	19, 972	2018-08-30	16:11:50	可管理进程	自动	
0	incssmdn. exe	已经启动	本机	0	16, 976	2018-08-30	16:11:51	可管理进程	自动	
0	incsyslogdn. exe	已经启动	本机	0	15, 844	2018-08-30	16:11:50	可管理进程	自动	
0	incupgdn. exe	已经启动	本机	0	18, 608	2018-08-30	16:11:50	可管理进程	自动	
0	incvlandm. exe	已经启动	本机	0	19, 900	2018-08-30	16:11:50	可管理进程	自动	
0	incvnndn. exe	已经启动	本机	0	29, 064	2018-08-30	16:11:50	可管理进程	自动	
0	incvzlandn. eze	已经启动	本机	0	31, 364	2018-08-30	16:11:50	可管理进程	自动	
0	incwlanperfdm	已经启动	本机	0	39, 860	2018-08-30	16:11:51	可管理进程	自动	
0	ing. exe	已经启动	本机	0	8, 880	2018-08-30	16:11:44	核心进程	自动	
0	tftpserver.exe	已经启动	本机	0	14, 436	2018-08-30	16:11:34	可管理进程	自动	≡
0	uam. exe	已经启动	本机	0	14, 372	2018-08-30	16:11:56	可管理进程	自动	
0	uaning.exe	已经启动	本机	0	7, 128	2018-08-30	16:11:51	核心进程	自动	
0	apmserver	已经启动	本机	1.08	396, 636	2018-08-30	16:11:27	可管理进程	自动	
0	danserver	已经启动	本机	0	330, 020	2018-08-30	16:11:27	可管理进程	自动	
O	epsserver	已经启动	本机	0	383, 624	2018-08-30	16:11:31	可管理进程	自动	
D	portalserver	已经启动	太机	0	455.084	2018-08-30	16:11:32	可管理讲程	自訪	
0	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	
Ο	ssmserver	已经启动	本机	0	142, 128	2018-08-30	16:11:28	可管理进程	自动	
0	activeb	已经启动	本机	0.08	451,068	2018-08-30	16:11:26	可管理进程	自动	$\overline{\mathbf{v}}$

EPS扫描器侧服务正常启动,如下图所示。

9	EScan Config	又件(F) 违项(O) 董倉(V) 进程 性能 用户 详细信息 服务
服务器IP 192	168 . 111 . 176 服务器端口	名称 状态
本机与服务器通信IP:	192. 168. 111. 171	i WMI Provider Host ▶ 1 服务主机 本地服务(无网络) (3)
日志等级 调试	✓ 自动静脉之前的扫描结果和日志(天	■ Microsoft IME ▶] 録券主机: DCOM 服务職进程启动職 (6)
启动服务	停止服务	▶ ③ 服务主机: 近程过程调用 (2) ◎ ScanConfigWnd ② EScan Config
v w termsvcs		1349 0'220 13'1 MB

Þ	COM Surrogate	1972	0%	2.6 MB
1	WebCamScannerU WebCamScanService	2052	0%	3.8 MB
Þ	Microsoft 分布式事务处理协调器服务	2188	0%	1.7 MB

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。

議点採測管理 > 扫描動置 > 扫描器管理 扫描器管理			
扫描器名称 扫描时间从	0	I	
网络夹亚 全部 常加 删除 号入 扫描 网关信息	Ť		
	网络类型	NAT名称	版本号
在线 扫描器171(192.168.111.171)	普通		7.3 E0506H03
高线 ZX(192.168.214.35)	普通		-
离线 SLAVE(192.168.111.119)	普通		-

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。

1 MAGRO	馆理 > 扫描配置 > 扫描器管理 > 网	大国意				
网络瓜田						
	RAPELA			Ξ		
	PECOP					
84	111 121 - 811					
	開光名扉 ≑		REAPRIL +		NATER	设备类型
	192.168.111.254		192.168.111.254			用关
	192.168.111.164		192.168.111.164			交換机
月412	张记录,当前第1-2,第1/1页。					

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。

8] 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。

-104.00							
归助器名称*	F3M68171				PRE *	192.168.111	.171
网络黄型	11.0				NATER		
归满器分组	未分组	-	1820		扫描场景	板盘	
第二派官	轻度		Ð		他议深度	轻度	
位置			eð -		经纬度		
编述							
R No 9	19地址			MD			设有关型
168.111.164	192.168.111.164			-			交換机
100010100	192.168.111.254			192.168.111.1-192.168.11	1.254		用关
108.111.234							

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。

H 1844	19月前日 > 鉄ぶ井田田島			
8.5	1910			
	第三体理			
	mahia	103168111 303	4 .	
	在緣然為	南线	合環球恋	1072 E
	MACREE	48/7A/DA/AC/81/7F	· · · · · · · · · · · · · · · · · · ·	PC
	操作系统	Linux	厂商	Linux
	或点型号		联系人	
	10.44 maas		电子邮箱	
	白编时间	2018-07-17 05:11:03	发现到问	2018-06-21 11:26:17
	NGEM	192.168.111.x	医捕食素人	28
	渡入交換机IP		接入交换机械口	
	基15MAC地址	48.7A/DA/AC/81:7F	基线病点类型	PC
	基线操作系统	Linux	基地厂商	Linux
	車批时间		审批人	
	网络类型	如 湯	NATSR	
	19 6 2	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。

[RTI]dis arp I	95.108.1.152			
	Type: S-Static	D-Dynam	ic 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, iM C 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"。

动作	
〇同歩	
C 刷新	
🛃 取消管理	
前 删除	
🗔 Teinet	
Neb网管	
···· Ping	
🔛 路由跟踪	
😪 拓扑走位	
🔧 MIB管理	
以 Telnet/SSH代理	
🔁 打开设备面板	
SSH	

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。此时右侧会出现改 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M AC地址学习情况。

10.153.48.6 🖬 😳 🐋 🔌 🖡		A 130	4= ++ Q, ++ 🏠
dot1dTpFdbE	intry *	409) 1.3. (dot1dTp	6.1.2.1.17.4.3.1.2.244.48.185.205.164.191 FdbPort.244.48.185.205.164.191) 225
and deated for	db.Day	idot1dTo	EdbPort 244 d8 185 208 222 67 225
detatdfield detatdfie	Contac Contac Get Get Ne Get Ne Set		2.1.17.4.1.2.2444.8185.2082385.7225 2.1.7.4.3.1.2.2444.8185.2082386.7225 2.1.7.4.3.1.2.2444.8185.2082386.7225 2.1.7.4.3.1.2.2444.8185.210.39.100 2.5.7.1.7.4.3.1.2.2444.8185.210.186.211 2.1.7.4.3.1.2.2444.8185.210.186.21 2.1.7.4.3.1.2.2444.8185.210.186.31 2.2.1.7.4.3.1.2.2444.8185.210.186.31 2.2.1.7.4.3.1.2.2444.8185.210.186.31 2.2.1.7.4.3.1.2.2444.8185.210.186.31 2.2.1.7.4.3.1.2.2444.8185.210.186.31 2.2.1.7.4.3.1.2.244.8185.208.185.34 2.2.1.7.4.3.1.2.244.8185.238.185.345 2.2.1.7.4.3.1.2.244.822.84.90.258 2.1.1.7.4.3.1.2.244.822.84.90.259.190 2.1.1.7.4.3.1.2.244.284.525.205.103.04 2.1.1.7.4.3.2.244.284.525.205.103 2.1.1.7.4.3.2.244.284.252.90.190 2.1.1.7.4.3.2.244.284.252.90.190 2.1.1.7.4.3.2.244.284.254.90.200.100 2.1.1.7.4.3.2.244.284.254.90.200.100 2.1.1.7.4.3.2.244.284.254.90.200.100 2.1.1.7.4.3.2.244.284.254.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.284.90.200.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.3.2.244.90.100 2.1.1.7.4.
Adot1dBridge.dot1dTp.dot1dTpFdbTable.dot1	Q. 查找时日刊点		Port.248.22.84.30.250.190) 5 2 1 17 4 3 1 2 248 99 63 218 35 132
Module BRDG5-MB Parent dotLTPrdBethty Max Access: read-only NumericalSymbol Integer32 ComposedSyntax Integer32 Status: current Description: Either the value '0', or the port numb	er of .	(dot1dTp 419) 1.3.0 (dot1dTp 420) 1.3.0 (dot1dTp 421) 1.3.0 (dot1dTp 	67dbPort.248.99.63.218.35.132) 225 66.12.117.43.1.2.748.115.162.745.61.09) 225 66.12.117.43.1.2.748.115.162.745.61.09) 225 66.12.117.43.1.2.752.63.219.71.967 748 66.12.117.43.1.2.252.77.212.54.133.243 37dbPort.252.67 212.54.133.243) 225 Weiker Keyles Finishele *****

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。