PLAT SNMP 张轩玮 2019-09-21 发表

组网及说明

1.1 适用产品系列

本案例适用于iMC PLAT 7.1及之后版本, V5版本设备。

1.2 适用场景与注意事项

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,计算出其相关网络拓扑,接收Trap,自动采集设备性能指标等操作 iMC 中的SNMP、Telnet、SSH 参数必须与设备上的配置保持一致

配置步骤

1 配置步骤

- 1.1 网络设备管理参数配置
- 1.1.1 Telnet、SSH参数配置

#启动设备Telnet 服务
[H3C]telnet server enable
#配置登录参数
[H3C]user-interface vty 0 15
[H3C-ui-vty0-15]user privilege level 3
[H3C-ui-vty0-15]protocol inbound all
[H3C-ui-vty0-15]authentication-mode password
[H3C-ui-vty0-15]set authentication password simple iMC123
#增加设备本地用户
[H3C]local-user test
[H3C-luser-test]password simple iMC123
[H3C-luser-test]authorization-attribute level 3
[H3C-luser-test]service-type ssh telnet

- 1.1.1 网络设备SNMP代理配置
 - #SNMP 代理配置 <H3C> <H3C>system [H3C]snmp-agent [H3C]snmp-agent community read public [H3C]snmp-agent community write private [H3C]snmp-agent sys-info version v1 v2c
- 1.2 iMC中增加设备
- (1) 选择"资源"页签,在左导航树中单击"资源管理 > 增加设备"菜单项,进入增加设备页面。
- (2) 输入设备的管理IP 地址"192.168.40.100"。
- 图1 增加设备

D TOWN CHANNER		
设备基本信息		
主机名或IP地址 *	192.168.40.100	
设备标签		
掩码		0
设备分组		• ?
登录方式	Telnet	• ?
✔将设备的Trap发送到本网管系统	充	
✔ 设备支持Ping操作⑦		
Ping不通也加入⑦		
将LoopBack地址作为管理IP		
◆配置SNMP参数		
➡配置Telnet参数		
◆ 配置SSH参数		
		确定取消
₩₩₩₩		
奴呪明: ♀♀枟恷・沿冬左 iMC 由見一的夕€	。 iMC 今白动涛取识冬的	Svenama作为设备行体。
又田1小立・ 以田仁 IVIC 中亚小山石が 奋码・ 设冬管理 IP 地址対応的埼码	iMC 会白动读取设备的	Systiallie 作为反面你觉, 罟的答理IP 地址对应的描码·
もう・ 反面自注 II 地址が述いもう。 学会方式・iMC 部署相关配署时体田	1000 去日幼族牧伎笛工乱	
导致ACLM。MVM 等组件不可用:		
条设备的 Trap 发送到本网管系统:	勾选后iMC 会自动将Trap f	=机配置到该设备上,以便设
将产生的Trap 发送到iMC 服务器上	, ,	

(3) 点击"配置SNMP 参数"链接或其左侧图标,展开SNMP 参数配置栏。 图2 设备管理参数

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

(4) 点击"设置"链接,弹出SNMP 参数配置页面,配置设备的SNMP 参数类型为"SNMPv2", 读写团体字分别为"public"和"private"。

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	

(5) 单击<确定>按钮,完成SNMP参数的配置。

(6) 点击"配置Telnet 参数"链接或其左侧图标,展开Telnet 参数配置栏。

(7) 点击"设置"链接,弹出Telnet 参数配置页面。认证模式选择"用户名+密码",输入Telnet 用户名"test"和密码"iMC123"。

●手工编辑Telnet参	▶数 ──从已有的Telnet参数模板中选取	
认证模式	用户名 + 密码 ▼	
用户名 *	test	
密码	•••••	
超时时间(1-60秒) *	4	
	确定 取消	

(8) 单击<确定>按钮,完成Telnet参数的配置。(9) 如果设备上开启了SSH 服务,可配置相应的SSH参数。(10) 单击<确定>按钮,完成设备的增加。

1.3 结果验证

1.3.1 查看拓扑

设备成功增加后,设备在拓扑中的链路会自动计算,同时在"我的网络拓扑"中可以查看到新增设备。

(1) 选择"资源 > 网络拓扑"页签,进入拓扑查看页面。

(2) 在左导航树中选择"自定义拓扑 > 我的网络拓扑"菜单项,打开我的网络拓扑页签,可看到 新增设备已经加入到对应的网络中。

图5设备所在拓扑



1.3.2 查看告警

设备产生的 Trap 会发送到iMC 上并生成相应的告警,可在全部告警中搜索相关设备查看告警。 (1) 选择"告警"页签,单击"告警浏览 > 全部告警"菜单项,进入全部告警页面。 (2) 在右上角的搜索栏中输入新增设备的IP 地址192.168.40.100 后回车,页面显示新增设备的告 警。 图6 设备告警

4	全部管	雪雪				A	实时告警 ▼	ジ 过渡规则	🔂 浏览Trap	专加入收	藏⑦帮助
	恢复	确认	删除 …更多操作					[192.168.40.100		0,
		級别 ≎	告警来源 \$	类型 ≎	告警信息 🗘	恢复状态 \$	确认状态;	告警时问 😂	恢复时间 \$	持续时间	分析报告
		<mark>1</mark> 警告	NMS(127.0.0.1)	[⊒ iMC	智能管理中心告警系统从2015-12-21 13:18:13到2015-12- 21 14:58:14期间连续100次收到设备RDSI01- S5820v2(192.168:40.100)的事件(周期告警)。	4.未恢复	人 未确认	2015-12-21 14:58:14		1小时 25 分钟 48 秒	Eq.
		<u>1</u> 警告	NMS(127.0.0.1)	Банк	智能管理中心告警系统从2015-12-21 11:38:14到2015-12- 21 13:18:13期间连续100次收到设备RDSI01- S5820v2(192.168.40.100)的事件(周期告警)。	4.未恢复	🔒 未确认	2015-12-21 13:18:13		3小时 5 分钟 49 秒	Eq.
		▲ 警告	NMS(127.0.0.1)	Щімс	智能管理中心告警系统从2015-12-21 09:59:14到2015-12- 21 11:38:14期间连续100次收到设备RDSJ01- S5820v2(192.168.40.100)的事件(周期告警)。	4 未恢复	🔒 未确认	2015-12-21 11:38:14		4小时 45 分钟 48 秒	Eq.
	共有	F3条记录,	. 当前第1 - 3 , 第 1/1 页	ί.					« < 1	>	50 •
	数据新	郑取时间:	2015-12-21 16:24:02						俠	夏 确认	删除

1.3.3 查看新增设备的详细信息

设备加入 iMC 后,默认性能指标 (CPU 利用率、内存利用率、不可达比例等) 会自动采集,可通

过设备详细信息页面查看。在IMC 任一页面,通过右上角的设备搜索栏查找要查看的设备。 (1) 在设备搜索栏中输入172.18.24.100 后回车,搜索设备。

图7 搜索设备

HBC Intelligent Management Center		首页	資源			合整	ie a	系统管理					
视阳管理	\rightarrow	🐂 室砌设备											★加入收錄 ⑦ 帮助
资源管理	>												
终端准入管理	>	● 提示 学変通的統計		IN HEID ALL HA	100 DE Julio Hereiro	÷							
网络遗产	>	20 20 20 40 40 40 40 40 40 40 40 40 40 40 40 40	· 98.00.000										
虚拟资源管理	>	重要改算状态:	дар 🗸 /	-an - an 200.972	• Azi • 3	vn V ±R	_				_		
腦券器自动化	\rightarrow	📋 H H 🖬 📑	88 -	职消管理	Da⊭ Ca	(1)新 ▼ 更 :	>			💼 定制列	4 5	≝Exce	i 🖹 ≒±csv
存储自动化	>	──状态≎	꿗	新标签 ▲			- 코号 ≎		IP地址 ≎	类型 ♀			授作
CMDB管理	>	- 重要	10	0(172.18.24.10	10)		H3C \$5820V2-5	20	172.18.24.100	交换机			
性能管理	>	共有1条记录。	当前第1-1,	第1/1页+						«	< 1	>	» 50 •
		数据获取时间:20	017-06-05 15	:05:03									

(2) 点击设备标签链接,进入设备详细信息页面,可查看设备的详细配置及监视信息。 图8 设备详细信息

资源 > 10	0(172.18.24.100)						大 加入收藏 ()帮助
设备详细的	1息						动作	~
设备标签。 问地码 sysolD 设备型 系统描述 提牌信息	100 ●重要 172.18.24.100 255.255.05 H3C.50270-520 文執机 图1820 H3C.formare Path right reserved. 未註面[21620	■18株1 1.845 form Software, Software Versio	系统名称 联系人 位置 运行时间 最后轮明时间 型子方式 接口数里 n 7.1.045, Release 2311P05 H3C 5	100 [[영왕] Hangzhou H3C Tech Hangzhou, China 6天22-J:8148分钟 2017-06-05 13:08: Telnet [[代왕] 68歳口列表 5820V2-52Q Copyright (c) 2C	o, Co., Ltd.	3C Tech. Co., Ltd. All	 ○ 閂歩 ○ 閂歩 ○ 目4新 ○ 目4前 ○ Finet ○ Fine ○ Fine	
▶服务监	È	共有0条记录	R o			「定制	R SSH	
最近10条末	大恢复告警					更多…	性能监视	,
级别	告警信良		告答时间				设备配置管理	>
▲重要	轮询设备172.18.24.100时发现1	72.18.24.21为非法IP地址。	2017-06-05 13:08:26				VLAN管理	>
▲ ⊕ #	轮询设备172.18.24.100时发现2	2.22.22.5为非法IP地址。	2017-06-03 15:04:36				设备基本信息	>
	轮询设备172.18.24.100时发现20	4.24.24.100为非法IP地址。	2017-06-05 13:08:26	+	恢复失踪		协议管理	>
▲ (1) 要	轮询设备172.18.24.100时发现24	4.24.24.101为非法IP地址。	2017-06-03 13:04:26	20				
▲重要	轮询设备172.18.24.100时发现1	72.18.24.15为非法IP地址。	2017-06-05 13:08:26	10				
▲重要	轮询设备172.18.24.100时发现1	72.18.24.5为非法IP地址。	2017-06-05 13:08:26					
4 警告	接口Vlan-interface40的IP地址由	24.24.24.1\255.2	2017-05-17 16:24:27	0 原急	重要次要	警告		

(3) 单击右导航栏中的"性能监视 > 性能数据概览"菜单项,弹出设备性能监视信息页面。 图9 性能监视



配置关键点