Syslog日志 叶佳豪 2019-04-09 发表

# 组网及说明

## 1 配置需求及说明

## 1.1 适用的产品系列

#本案例软件管理平台适用于所有ACG1000系列产品

#### 1.2 ACG1000管理平台安装环境要求

产品系列	SecPath ACG1000日志分析与管理平台
硬件环境	X86服务器/Intel Xeon
内存	最低4G内存,建议采用16/32G内存
硬盘	最低100G存储空间,建议500G存储空间,最好是磁盘阵列
软件环境	Windows server 2003/Windows7/ Windows server 2008 (以 上为64位操作系统)
目标文件名称	SACG-7.0-R0303P02.zip
內存 更盘 软件环境 目标文件名称 ACG1000系列应用控制网关版 本号	R6606P01及以上 E6401及以上(ACG1000-AK200系列)

## 1.3 配置需求及实现的效果

#在一台windows服务器\电脑上安装ACG1000管理平台,接收ACG1040发送的日志信息,并在日志审 计平台上显示对应的审计记录。

#### 2 组网图



#### 配置步骤

3.1 官网下载软件安装包

#首先需要在华三官网 www.h3c.com.cn "产品支持与服务\软件下载\安全"下载安装软件"H3C SecPath ACG1000 日志分析与管理平台"。

首页,产品支持与服务,文档与软件,软件下载,安全,应用控制网关产品, H3C SecPath ACG1000 日志分析与管理平台 该版本需要安装在CentOS7.4软件环境下 th ACG1000 SACG 7.0 R0304 版本软件及说明书 🔒 → H3C SecPath ACG1000 SACG 7.0 R0303P02版本软件及说明书 B 以下版本可以安装在Windows软件环境 下戰 → H3C SecPath ACG1000 SACG 7.0 R0303P01 版本软件及说明书 🖬 下蛻 → H3C SecPath ACG1000 SACG 7.0 R0303 版本软件及说明书 @ 下的 → H3C SecPath ACG1000 SACG 7.0 R0302P01 版本软件及说明书 🔒 下载 → H3C SecPath ACG1000 SACG 7.0 R0302 版本软件及说明书 下較 → H3C SecPath ACG1000 SACG 7.0 R0301P01 版本软件及说明书 下舰

注: 软件版本下载账号: yx800 密码为: 01230123, 如果现场环境不具备CentOS7.4环境建议下载R 0303P02版本使用。

#下载完成后将版本文件解压到电脑上,然后双击"setup.exe"开始安装,请按照安装提示完成软件安装





安装

取消

< 上一步(B)

InstallShield



#### 3.2 管理软件登陆

#安装成功后,启动浏览器,输入登录信息。在PC上启动IE浏览器(建议使用IE9.0及以上版本),例如:安装服务器在地址栏中输入http://127.0.0.1或者用该服务器的IP地址<u>http://192.168.10.4</u>后单击"Ent er"键,即可进入下图所示的SecPath ACG1000日志分析与管理平台登录页面。

□ ACG1000日志分析与管理 × +		
$\leftrightarrow$ $\rightarrow$ O   127.0.0.1		
系统支持IE9及以上版本,Firefox浏览器,推荐显示器最佳屏幕分语车1366*768		
	HE	26 谷寻玄统
	meher	
	767-16	- super
	密码	A
	验证码	◎ swyyl 8wyy <sup>换一张</sup>
		登录

#输入系统缺省的用户名"super"和密码"super.123",并输入验证码,点击"登录"按钮即可进入ACG1000 Manager并进行管理操作。

<b>达</b> 通量监控 编辑型控 料导	<ul> <li>▲ 系统信息</li> <li>● 系统时间:2019-02-27 14:26:35 星期三</li> <li>● 软件版本:SACG7.0 R0303P02</li> <li>● 数据库大小6.18MB</li> <li>● 数据库太小K5.18MB</li> <li>● 数据库版本:MYSQL SERVER 5.1.40</li> <li>● 磁盘剩余空间/总空间:21.17GB/97.66GB</li> <li>● 在线设备/总设备:0/0</li> <li>● 接收值息:默认提供</li> <li>● 可管理最大设备数:3000</li> <li>● 約47日第2002</li> </ul>
--------------------------------	--

#在导航栏中选择"系统管理----》产品激活",可以查看到该管理平台在未注册前有90天的试用期,超过 试用期只能管理型号为ACG1000-B、ACG1000-C、ACG1000-S、ACG1005、ACG1005-PWR、AC G1010、ACG1010-X1、ACG1020、ACG1030、ACG1030-X1、ACG1040、ACG1050、ACG1050-X1、ACG1000-AK110、ACG1000-AK120、ACG1000-AK130、ACG1000-AK140、ACG1000-AK150、ACG1000-SE、ACG1000-SE-PWR、ACG1000-BE、ACG1000-BE-PWR、ACG1000-AK21 0、ACG1000-AK220、ACG1000-AK230、ACG1000-AK240、的设备,且最大可管理设备数量小 于10台。

	NG0.000 78.8	5				
問題	7.62.62.10	090%	<b>42</b> 28	0909	550U	10 C
	1 約里所収	该把权均设备型号无关	90 美	3000 台	1CH OF	8.050
1250 1929 2014973 2014973 2018 2019 2019 2019 2019 2019 2019 2019 2019	2 804000	AC30300-A AC40300-A AC3000-A AC3000-A AC3000-A AC3000-A AC3000-A AC3000-A AC3000-A AC3000-A AC30	10.8	NUTER CONTRACTOR	1018	

3.3 设备配置

#登录ACG1040的管理页面,进入"网络配置—>接口"选择ge3接口点击"操作"。

H3C	Sec	Path ACG	1000		A MARKAN AND AND A MARKAN AND AND AND AND AND AND AND AND AND A
H3C	物理將	口子接口	网桥接口 聚合接口	隧道接口 天	浅接口 安全域
- 1 监控统计		接口名称	描述	IP地址	IPv6地址
一〇 网络配置	1	ge0		10.88.142	135/24
一接口	2	ge1		10.1.1.254	/24
─ 端口镜像	3	ge2		192.168.0.	1/24
一路由表	4	ge3		192.168.10	0.1/24
一静态路由	5	ge4			
-ISP路由	6	ge5			

#配置ge3口的ip地址为"192.168.10.1",然后选择管理方式为"Center-monitor"然后点击"提交"。

本设置							
	名称	ge3	(3c:8c:4	10:4e:03:a4)			
	描述			(0-127 字	符)		
	启用						
	IP类型	IPv4 IPv6					
		地址模式	● 静态地址	ODHCP	O PPPOE		
		接口主地址	192.168.10.1/24	(例如: 192.168.1	.1/24)		
		从IIIPv4列表	④ 新建				
			地址		操作		
	管理方式	Https	Http	Ssh	Telnet	Ping	Center-monitor
202 T							
	协商模式	<ul> <li>自动</li> <li>〇</li> </ul>	强制				
	MTU	1500 (1	1280-1500)				
	AND THE REAL	+==	ALCO D				

#在"系统管理à日志设定à日志服务器"里勾选"启用"并配置服务器的IP地址192.168.10.4 点击"提交"。保 证服务器的地址和ACG1040设备能正常通信。

充管理 > 日志设定 > 日志服务	8		
H3C [Root]	日志服务署		
■监控统计			
日志查询		-	
网络配置	启用		
一接口	服务器1IP地址	192.168.10.4	加密: 🔲
一 🖬 路田	服务哭1端口	514	(1-65535)
-NAT	ands #Paralish		1-00
- DHCP 服务器	服穷器21P地址		加密: □
— IPv6网络	服务器2端口	514	(1-65535)
一链路负载均衡	服务器3IP地址		加密: 🗆
■ 网络优化	肥冬翠沙湖口	514	(1-65535)
■用户管理	加快力量高小的同口		(100000)
■対象管理	源IP地址		
■上附行为管理 ■ たんたけり			
コ 女主P/DfF コ V/DN		提交 重置	
系统管理			
一授权管理			
一 🖬 管理员			
一 🖬 系统设定			
一〇〇二月世			
一日志设定			
日志服务器			
一日志辺想			

#在"上网行为管理à策略配置àlPv4策略"里点击"新建",动作默认选择"审计",然后在"应用审计"再点击"

新建",应用审计选择"所有应用",日志级别选择"信息",其他都保持默认,点击"提交"。

186558	1057	> DVIEW															
R HBC		A IPVIE	6														
「日田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田																	
日本語を開		542		_	•												
-90			10	0.82	Ogath	Ose			Catera	9							8
-90.00			8K270	0	(0-10	000000/E.B.	·重型0、如果70	网络个的									
-305	E .		振送							RRE							
-#c3	10		85	Ø						15.5				(0-	63)		
-15P(8)	8	58.9	体							应用审计	乐教应用	-		~			
-832			Re.	any						相关行为	形有行为	▼ #H6:	1.5g (東))所	* v	1		
-NAT			RACIN	any land			energiese land			DEMO		OBR			·		
-DNS			and the second	and			and any				包金マ	所有			¥ 15	(关键字	
-0HCP Ed	14		1852	any X						0.820	4/#	~				ALCORE I.	
一众就均衡			目的地址	any X						日本語句	an						
-CONS			1010	always													
一日用户管理			IE 6	any				/									
日対象管理				and a			/	-									
	511 10		122/0	anyx		-											
-248	18					/										182	200
- 9/68		£4%			/	-											
- 料定策略	ī .		1	Colori									0				
一会派管理				●転遣	EREST : O	金石配〇順	宇宙配										
	872			創	行力	内容	活成	关键字	(0.9)	动	85 58	5 <u>1</u> /1					
○ siz ○ m	B8 9,1	PA 0 49	<b>O</b> MR <b>2</b>	XAD 👌	西部北部市平	Stutene *	feil: ① 約88	=#ił	- <del>2</del> #if = 1	540							
	18:25	1D 388	0 88	180	3.64	monest	100		88	,	un .	医肥大的	5882	114	88	走行时间	發作
1	0	1 any	an		any	any	any		any	a	ny	6822		always		0	Ø O
15	mine	URLIER															
	应用		行力		内容	趣》	9	关键字	10.5	н	幼作	88		Rif.			
1	1 新有	应用	所有行为		所有行为内容	63	£	any	信用	8	允许	۲		11			
	_																
12		4 4 44 4	and a													10	

#### 3.4 配置ACG日志分析与管理中心

#在ACG日志分析与管理中心的页面的导航栏中选择"设备管理—>设备管理",选择添加"设备"来添加ACG1040设备。



#输入设备的IP地址"192.168.10.1",账号密码为"admin/admin"点击"确定"。

名称:	ACG1040	
描述:		
设备IP:	192.168.10.1	
用户名:	admin	
密码:	•••••	
设备组:	未分组设备 🔹 👻	

#如下图显示,为成功添加ACG1040设备,可以查看到ACG1040的 CPU、内存以及磁盘的信息,在管理平台上点击"WEB管理"可以直接进入被管理的ACG1040的管理页面。







## #管理平台成功管理到ACG1040后,可以在管理平台里查看ACG1040审计到下面终端相关日志。

(2) Stife	041 () 1/122-017							-					
H	3C 🖊	SecF	Path AC	G1000日志	分析与管理								
.11			BATELE										
	SCHNHT155	0, 2	用 直治条件: 创建	时间 后近一天 转换两型	WELLINK;								
		库电	设备名称	1810	WHATCH	III ISSP	万法口	0.8/3.6/4	ED IN INC.	NATES	19 K	11A	100
~	NATES	1	ACG1040	192.168.10.4	172.20.10.2	180.163.32.152	53598	53598	80	snat	TCP	2016-08-16 19:47:28	1
•	LRGABS	2	ACG1040	192.168.10.4	172.20.10.2	180.163.32.152	53599	53599	80	snat	TCP	2016-08-16 19:47:28	2.5
tπ.		2	ACG1040	192.168.10.4	172.20.10.2	219.133.60.243	53597	53597	36688	unat	TCP	2016-08-16 19:47:23	2
		4	ACG1040	192.168.10.4	172.20.10.2	180.163.32.152	53595	53595	80	snat	TCP	2016-08-16 19:47:23	2
ן ס	PEREKALS	3	ACG1040	192.168.10.4	172.20.10.2	180.163.32.152	53596	53596	80	snat	TCP	2016-08-16 19:47:23	2
	法撤销新日本	6	ACG1040	192.168.10.4	172.20.10.2	114.114.114.114	50675	50675	53	snat	UDP	2016-08-16 19:47:23	2
		7	ACG1040	192.168.10.4	172.20.10.2	183.3.226.111	53594	53594	36688	snat	TCP	2016-08-16 19:47:18	2
		8	ACG1040	192.168.10.4	172.20.10.2	180.149.144.169	53593	53593	80	snat	TCP	2016-08-16 19:47:18	1
		9	ACG1040	192.168.10.4	172.20.10.2	114.114.114.114	52192	52192	53	snat	UDP	2016-08-16 19:47:18	1
18		10	ACG1040	192.168.10.4	172.20.10.2	74.125.23.113	53592	53592	80	snat	TCP	2016-08-16 19:47:13	
		11	ACG1040	192.168.10.4	172.20.10.2	10.63.5.223	53582	53582	443	snat	TCP	2016-08-16 19:47:03	2
		12	ACG1040	192.168.10.4	172.20.10.2	125.88.193.243	53579	53579	80	snat	TCP	2016-08-16 19:46:58	1
-		13	ACG1040	192.168.10.4	172.20.10.2	183.134.16.86	53581	53581	80	snat	TCP	2016-08-16 19:46:58	2
		2.4	ACG1040	192.168.10.4	172.20.10.2	114.114.114.114	61243	61243	53	snat	UDP	2016-08-16 19:46:58	1
		15	ACG1040	192.168.10.4	172.20.10.2	183.134.16.86	53580	53580	80	snat	TCP	2016-08-16 19:46:58	1
*		16	ACG1040	192.168.10.4	172.20.10.2	115.239.210.27	53578	53578	80	snat	TCP	2016-08-16 19:46:58	1
818		17	ACG1040	192.168.10.4	172.20.10.2	114.114.114.114	64129	64129	53	snat	UDP	2016-08-16 19:46:58	2
		18	ACG1040	192.168.10.4	172.20.10.2	74.125.23.102	53575	53575	80	snat	TCP	2016-08-16 19:46:53	1
		19	ACG1040	192.168.10.4	172.20.10.2	10.63.5.223	53576	53574	443	snat	TCP	2016-08-16 19:46:48	23
		20	ACG1040	192.168.10.4	172.20.10.2	74.125.23.138	53568	53568	80	snat	TCP	2016-08-16 19:46:33	21

C @ http://127.6.0.1/index.html StH(7) R&D EB(Y) C&R(A) I&(7) Nbot C @ edmats @ R^bbs.comats SecPath ACG1000日志分析与管理平 H<sub>3</sub>C Rush 82Rush 82Rush 82 観天日古 \$819M 244885 HEBS \$5\$\$B 用户(用户根) 192.168.10.4 192.168.10.4 192.168.10.4 192.168.10.4 厚地址 192.168.10.4 192.168.10.4 192.168.10.4 192.168.10.4 192.168.10.4 
 目的地址
 自用

 43.250.14.49
 民間/土田花用

 115.231.171.09
 芳宁県約

 180.149.134.184
 新市月

 190.149.134.184
 新市月

 190.122.250.172
 芳宁県約
 9.69.0 84 2**8**45 08 748 748 748 748 364 24 RHEE 1813 1813 KK

## 配置关键点

1. ACG1000管理平台安装路径若包含中文字符时则会安装失败;规避方法是默认路径或安装路径均为 英文字符

2. ACG1000管理平台的默认防火墙需要关闭,保证管理平台和ACG1040设备网络可达,可以正常通信

3. 确保IPv4策略里面应用审计规则里的日志级别为信息,如果为不记录则审计不到日志