ACG1000日志分析与管理平台安装与使用方法

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

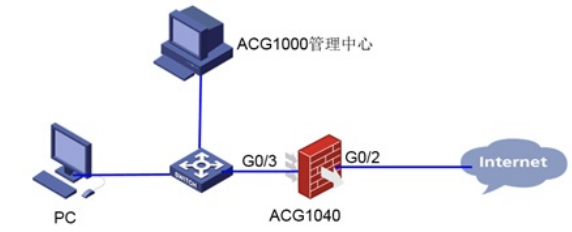
1.2 ACG1000管理平台安装环境要求

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
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

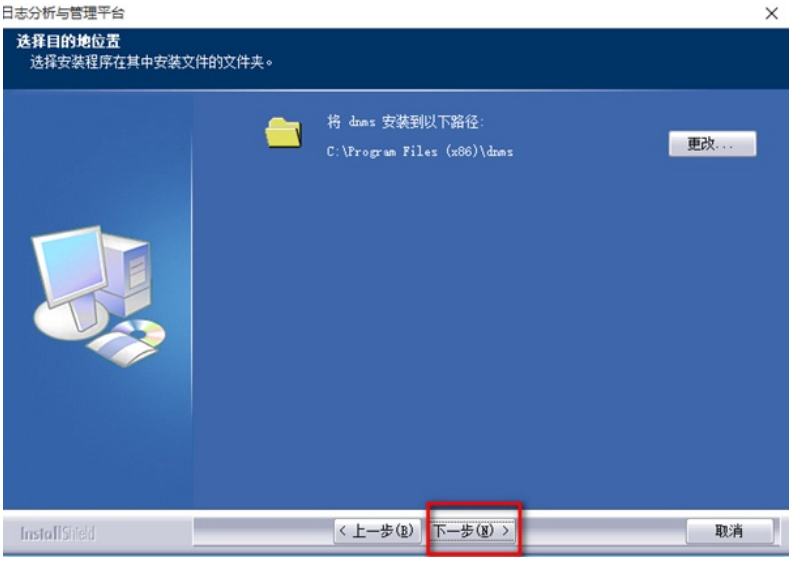
3.1 官网下载软件安装包

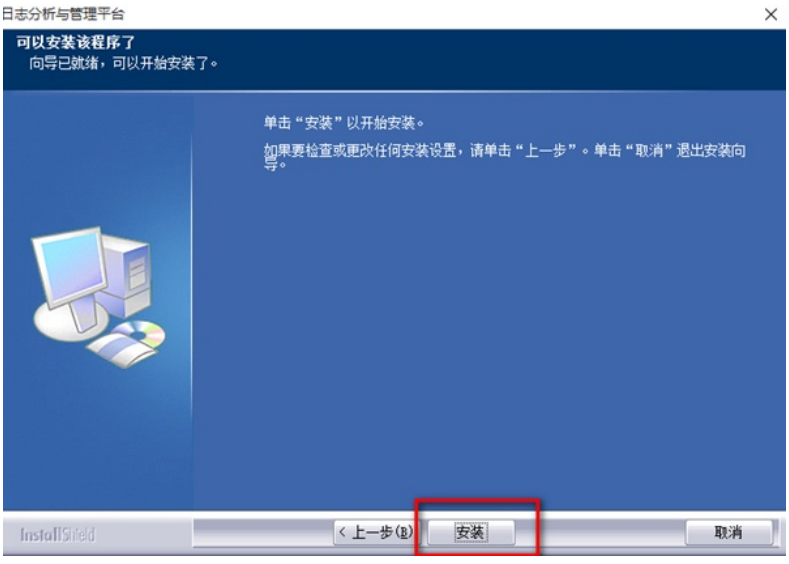
#首先需要在华三官网 www.h3c.com.cn “产品支持与服务\软件下载\安全”下载安装软件“H3C SecPath ACG1000 日志分析与管理平台”。

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R0303P02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。

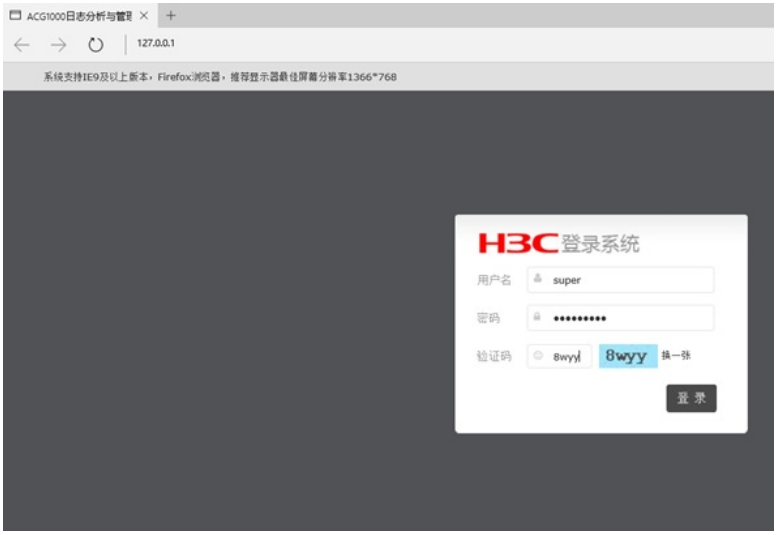

此电脑 › TOOL (E:) › ACG1000
名称
data1.cab
data1.hdr
data2.cab
engine32.cab
layout.bin
setup.exe
setup.ibt
setup.ini
setup.inx
setup.skin
日志分析与管理平台
欢迎使用日志分析与管理平台
将在计算机中安装，升级日志分析与管理平台。
若要继续请单击“下一步”
InstallShield
< 上一步(B)
下一步(N) >
取消


日志分析与管理平台
选择目的地位置
选择安装程序在其中安装文件的文件夹。
将 dnms 安装到以下路径:
C:\Program Files (x86)\dnms
更改...
InstallShield
< 上一步(B)
下一步(N) >
取消


日志分析与管理平台
可以安装该程序了
向导已就绪，可以开始安装了。
单击“安装”以开始安装。
如果要检查或更改任何安装设置，请单击“上一步”。单击“取消”退出安装向导。
InstallShield
< 上一步(B)
安装
取消

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http://192.168.10.4 后单击“Enter”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。



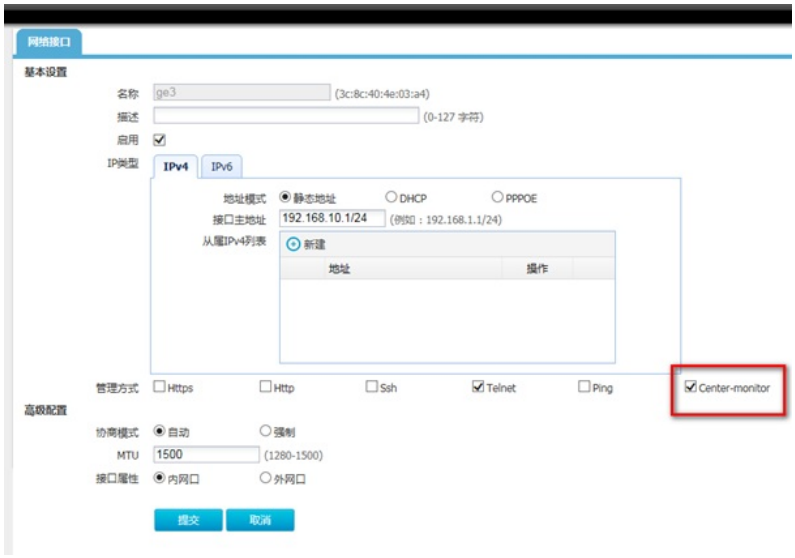
#输入系统缺省的用户名“super”和密码“super.123”,并输入验证码，点击“登录”按钮即可进入ACG1000 Manager并进行管理操作。

#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、ACG1010、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-AK210、ACG1000-AK220、ACG1000-AK230、ACG1000-AK240、的设备，且最大可管理设备数量小于10台。

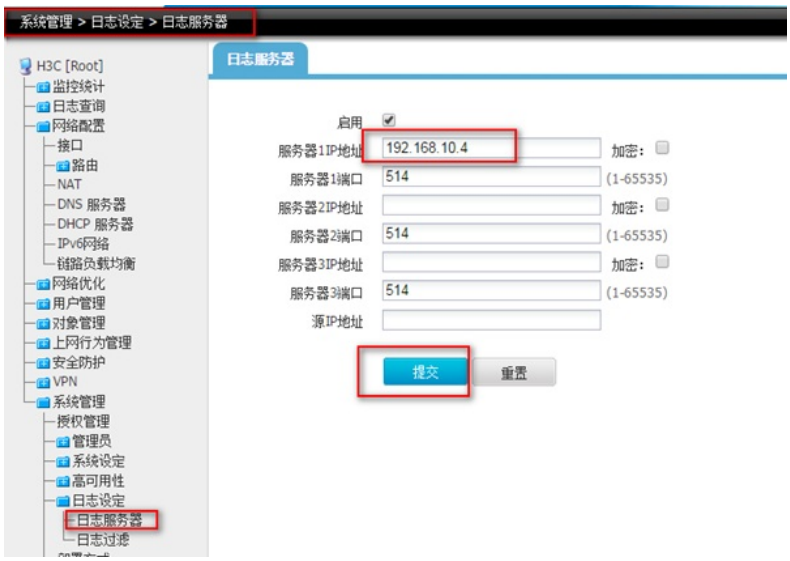
3.3 设备配置

#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”。

#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”。

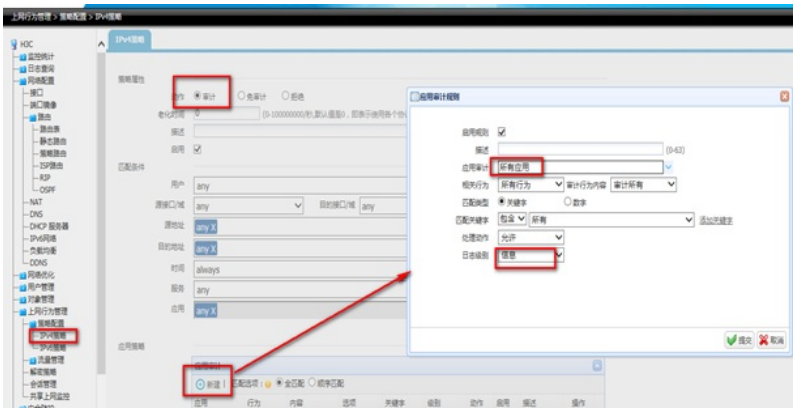


#在“系统管理à日志设定à日志服务器”里勾选“启用”并配置服务器的IP地址192.168.10.4 点击“提交”。保证服务器的地址和ACG1040设备能正常通信。



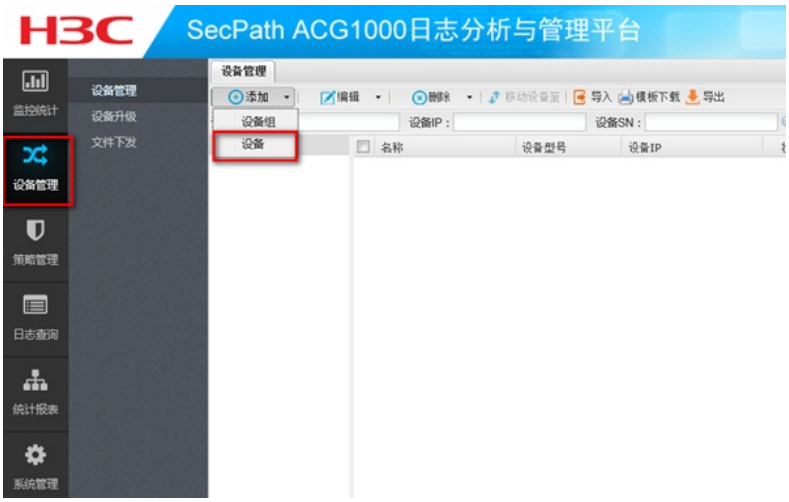
#在“上网行为管理à策略配置àIPv4策略”里点击“新建”，动作默认选择“审计”，然后在“应用审计”再点击“

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”。



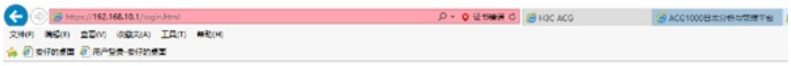
3.4 配置ACG日志分析与管理中心

#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。

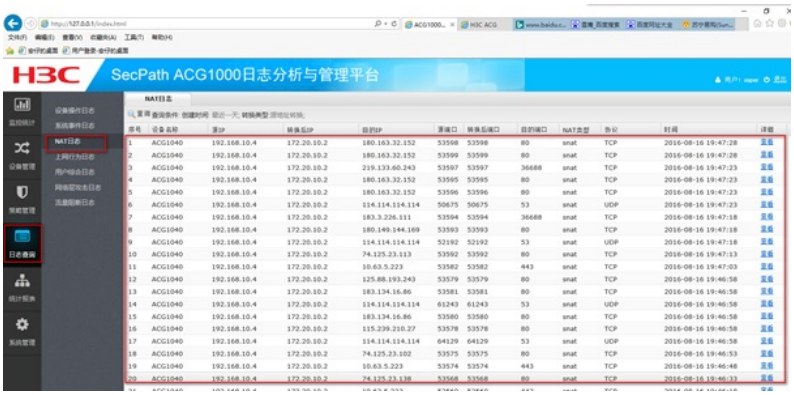


#输入设备的IP地址“192.168.10.1”，账号密码为“admin/admin”点击“确定”。

#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。



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