



ANYSEC-日志审计快速配置手册



版权所有:深圳市中科网威科技有限公司



1、登录

E0 口登录地址: https://192.168.1.40

用户名: admin 密码: admin123456

	日志审计系统		
Field th			
2 用户名	9 密码	验证码 66 ⁰⁹	登录
请先登录			

● IP 地址修改

B MIRE ANYSEC	日志审计系统			未收到告罄(或日:	志无法导出),点击检证		¢	2	7 🛪		e •0
2020-04-28 20 58 02	₭ ④ 网络设置										
₩ 秋态	昭和-110月 日										
<u>네</u> 分析	>										
@ 审计	·	* IP3512	: 192, 168. 1. 40								
X 关系	6	* 子阿攏弱	: 255.255.255.0								
名 用户	>	±tes:	: 100.70.70								
■ 资产	\$1		2017 July 100 100 100								
◆ 規则	>	Million .	: 951 100, 70, 70, 70								
团 报表	s:				相文	- 取:前					
¶7 告誓	》 同卡列表										
● 网络	~ 同卡名称		环境址	子网编码	状态	± DWS	备 BHS)	R ft
相件状态 网络语言	+th0		192.168.1.40	255.255.255.0	ø					1	0
路由设置	ethi		192, 168, 2, 40	255 255 255 0	¥					j	0
通信设置	et32		192. 165. 3. 40	255.255.255.0	g)	0
भ्यतः सः भव	ath3		192° 1635 4 40	255 255 255 A	0						n



2、添加资产

资产-资产列表-右上角添加资产或批量导入资产

BHINK RNYS	EC日志审计系	哀鏡		未收到告警(或日	志无法导出),点击验证…		۵	😌 🎞 admin 🔒 🕫
2020-04-25 20:39:35	ĸ	④ 资产列表					E	1版下数 与入资产 与出资产
◎ 状态		12户组	资产列表 搜索关键词	Q.				× + ×
<u>旭</u> 分析	>	未分组	四 资产名称	書产ロ	資产素型	日志教學	资产分组	80
眉审计	>							
🐹 关系	•							
8 用户	×.							
■ 资产	~							
资产列表 资产类型								
资产监控								

▶ 添加 Linux_Syslog 资产参数

添加资产				
	* 资产名称	8	数据库服务器	
	* 资产IP	:	192. 168. 1. 10	
	* 资产类别	es.	Linux	
	* 资产类型	i)	Linux服务器_Syslog	
	* 资产主类	11	主机设备	
	* 日志编码	8	итг-в	
	业务类型	<u>;</u> ;	请选择业务类型 最多十项	
	业务端口	1:	请按Enter键输入端口	
	采集器名称	3	本机采集器	•
	资产组归属	8	请选择资产组 不选择则不分组	
			启用JIDBC 启用WMI 提交	取消

※ 总机电话-- 0755-83658009∰ http://www.anysec.com

 後 技术支持--0755-83658229

 後 24 小时技术值班热线-----135-1069-3536

 ※ 深圳市龙华区观澜街道观光路1301-80 号电子科技大学(深圳)高等研究院3号楼1401



添加 Windows syslog 资产参数

200 (0H 5 <)			
* 资产名称	¢	杀毒服务器	
* 资产IP	:8	192, 188, 1, 11	
* 资产类别	ŝ	Windows	•
* 资产类型	:	Windows客户端	•
* 资产主类	13	主机设备	
* 日志编码	:	NTF-8	•
业务类型	10	请选择业务类型 最多十项	
业务端口	ia:	请按Enter键输入端口	
采集器名称	į,	本机采集器 ————————————————————————————————————	•
资产组归属	18	请选择资产组 不选择则不分组	
		启用JIDBC 启用WMI 提交 取	肖

● 添加后的资产列表

资产列表	搜索关键词	٩				ाम + x
	资产名称	资产卫	资产类型	日志教堂	资产分组	操作
(FT)	▲ 新春服务器	192. 168. 1. 11	Windows客户谎	0	未分组	◎ 🖉 🛱
	解析规则已加载 1816 行		1			共计 1 条



3、客户端主动推送设置

收集 Windows 日志: 需要在系统-插件中心内下载 windows agent 客户端并安 装到设备上。

他ANYSEC日志审	计系统	未收到告警(或日志无法导出),点击绘证…		🗘 💔 🏛 admin
14-25 20 44 21 K	€ ④ 捕作中心			
ēr , [城井列表			
現回 >	文件名称	版本号	獅迷	操作
旧表 >	vindows agent	V 2.1 build 2019-09-10	采集windows系统日志/网络数据图/应用文件日志	Ð
5 E >	Windows agent server 2003 支持包	V 1.0 bmild 2019-07-10	zerver 2003 PowerShell 支持包	Ð
	windows agent ap 支持回	V 1.0 bmlld 2019-07-10	xp PowerShell1支持包	Ê
158				
系统 ~		1		共计:
形種设置 對接索引信息				
采集器管理				
插件中心				
to flat				
ows日志采集程	译序 v2.1			
				
器地址 192.1	168.1.40	端口 5145	识别资产IP: 192.168.1.11	
经口士亚律	· 大田の住 - 六川の住	——— 日志审计IP地址,端口默ù	人 木和	D.
第四心不亲 [流里禾集 又曰禾集		41/0	
开启系统日志	采集引擎			
-	山ヶ住へ	如乏休口十 法具项律和节进项律		
/]全选	収 朱王	即杀统日心,	远挥开后,可以主部开	
Application			·	
HardwareEven	nts			
Internet Explored	rer		_	
Key Manageme Media Center	ent Service		=	
Security				
V System				
Vindows Powe	erShell			
ForwardedEve	ents			
Microsoft-Wind	dows-API-Tracing/Operational			
Microsoft-Wind	dows-Application Server-Application	ac /Admin		
Microsoft-Wind	dows-Application Server-Application	ns/Operational		
Microsoft-Wind	dows-Application-Experience/Proble	em-Steps-Recorder		
Microsoft-Wind	dows-Application-Experience/Progr	am-Compatibility-Assistant		
Microsoft-Wind	dows-Application-Experience/Progr	am-Compatibility-Troubleshooter		
Microsoft-Wind	dows-Application-Experience/Progr	am-Inventory		
Microsoft-Wind	dows-Application-Experience/Progr	am-Telemetry		
Microsoft-Wind	dows-AppLocker/MSI and Script			
Microsoft-Wind	dows-Audio/CaptureMonitor			
Microsoft-Wind	dows-Audio/Operational			
Microsoft-Wind	dows-Authentication User Interfac	e/Operational		
Microsoft-Wind	dows-Backup			
Microsoft-Wind	dows-biometrics/Operational dows-Bitl ocker-DrivePreparationTo	ol/Admin		
Microsoft-Wind	dows-BitLocker-DrivePreparationTo	ol/Operational		
	dows-Bits-Client/Analytic	na Anna Anna Anna Anna Anna Anna Anna A		
Microsoft-Wind			2010	
Microsoft-Wind	dows-Bits-Client/Operational		T	
Microsoft-Wind	dows-Bits-Client/Operational			÷
Microsoft-Wind Microsoft-Wind 用最后点	dows-Bits-Client/Operational		示为空,请退出程序后安装PowerShell支持点击几	立用
☑ Microsoft-Wind ☑ Microsoft-Wind ■ 果最后点	dows-Bits-Client/Operational	启动,需要手动开启权限";	示为空,请退出程序后安装PowerShell支持点击顶 计后方法	这 用

收集 Linux 日志, 打开 Linux 服务器命令行界面, 按如下步骤执行:

vi /etc/rsyslog.conf 编辑 rsyslog.conf 配置文件

. @192.168.1.40 192.168.1.40 是日志审计设备的 IP 地址

systemctl restart rsyslog 重启日志服务

※ 总机电话-- 0755-83658009∰ http://www.anysec.com

 · 技术支持--0755-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-83658
 · 25-83658
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836



4、日志查询及审计



5、可能遇到的问题

Windows 采集引擎未启动,,需要手动开启系统日志推送服务



 · 技术支持--0755-83658229
 · 公24 小时技术值班热线-----135-1069-3536
 · 河浦市龙华区观澜街道观光路1301-80 号电子科技大学(深圳)高等研究院3号楼1401



@rtt www.tggs	采集器地址 192.168.1.40 滅口 5145	识别资产IP: 192.168.1.11
as C:\Windows\system32\cmd.exe - winlogbeat.exe -c winlogbeat.yml	系统日志采集 流里采集 文件采集	
C:\>cd C:\Program Files (x86)\WindowsAgent\Windows_Agen	☑ 升启系统日志米廉引擎 ☑ 全法	
C: Vrognan Files (x86)-WindowsAgent-Windows_Agent_v2.1\ -c winlogbeat.yml	Marcosoft-Windows UAC/Operational Marcosoft-Windows UAC/Operational Marcosoft-Windows 2004;000/T/Operational	
这个窗口不要关,关了就不推送日志了		
	Microsoft-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows	
	可以看到服务已经启动了提示:如列表显示	示为空,请避出程序后安装PowerShell支持
	系統日志采集引擎:已自动 流量采集引擎:未启动	文件采集引擎:未启动 应用 週出

● 可以查看到日志了

COMMENT ANY	YSEC日志审计系统		未收到告誓(或日志	无法导出),点击论证一			😎 🏛 _{admin} 🖨 🔊
2020-04-26 21 17 1	11 任 ① 资产列表					E	1後下数 男人流产 男出流产
🔤 状态	are tu	與产列表 被常关键词	Q.				±+×
■ 分析	→ 未分組	□ 黄产名称	资产IF	黄产类型	日志教學	黄产分组	發作
國 单 f	3		192.168.1.11	Windows客户庸	20	未分组	©2†
各州户	2	Medium/undritigned 1010 (L		1			MT 1 M
为广兴里							
DITERS ANYS	SEC日志审计系统		未收到告警(或日志	无法导出),点击绘证一		٥	💎 🎞 _{adain} 🔒 🕫
2020-04-26 21:17:21	5EC日志审计系统 长 ④ 资产列表		未收到告警(或日志	无法导出),点击检证一		٩	😎 🎞 _{adain} 🔒 🗐 tettet Sliff, Sliff,
【2000-04-26 21:17:21 回 状态	5600日志审计系统 长 ④ 菜产则表 菜产瓶	資产列表 相關共補用	未收到告誓(或日志 Q	无法导出),点击管证一		٩	♥ 戸 adain ▲ ♥ 18万枚 第入版字 第出版字 止 + ×
 ○ 秋恋 □ 分析 	SEC日志审计 長校	資产減去 图示光谱用 - 资产软件	未收到告警 (咸日志 Q. 资产III	无法导出),点击给证— 资产类型	日志教堂	↓ 黄产分组	ゴス adain 全 の マの マ マ マの マ マの マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ
 2000-04-26 21:37 21 回 状态 山 分 折 - 公 亩 计 	aec日本時計長校 K- ① 京戸列表 文件編 ・ ・ 分類 : ・ ・	 資产列表 単空火線ボ 資产利本 資产名称 27 未要指許書 	末秋时告誓(城曰志 Q 現 戶17 182.184.1.11	私有知力、高市地理一 資产負責 Tinder要用項	日本教學 20	Q 資产分類 未分類	♥ 元 sain â q) RETR. 93.85 SLOFF 24 + X Br @ 2 @
 ○ 2020-04-26 21:37:21 □ 状态 山 分析 △ 由计 ○ 关系 	SEC日本部计研究 K- ① 用产列表 本分組 : > >	 第二条列為 単立大法方 第二条列条 27 共振振発音 新行取用に加加 1016 行 	未收到代費(項日志) Q 武产IF 182 189 J.11	私名称的。Alleで一 資产者間 Tadeo若月編	日本高度 20	டு துசதி ய சுற்பு	♥ ፲ stars
◎社(SX RNY= 2000-04-35 21:17:33 回 状态 山 分析 創 申計 ス 关系 各 用户	ACC日本単計 新校 K・① 第戸列為 本分類: > > >	 第4時期 第4時期 第4時期 第5時期 	未收到估費(減日志 成产	現在教授的。AIL的ロー	日志教聖 20	டு துசத்தி சுற்கு	♥ 22 state ● ● ● ● ● ● ● ● A ⁺ : S
 (111:03: FINYE 1000-00-28 31:17 31 び 大売 ・ ガ	SEC日本単計 新校 K・① 第戸列第 本分類: 2 2 3 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5	 第二人列為 新安美術店 第二人列入 第二人列入	未收到估費(編日志 文) 武产17 322 108.3.11	私名称的。ALL会议一 資产条型 Tradeo第月版 1	日本高望 20	ட துசுதின் சுற்கு	♥ 22 state 0 0 19783 (3)20 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020 2020
 ぜは25 PNV5 なか かが なか かが なか かが かが かが かが かか 	ACCID 点形計 新校 K・① 原产知識 参加 参加 参加 参加 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	 第二人列為 新安美術店 第二人列入外第 27 大学報告書 第千規則已加載 1936 行 	未收到估費(編日志 文) 近217 122 108.1.11	私名称的。ALL会议一 資产条型 Tradeo第月版 1	日本魚聖 20	ட துசதின் சுற்கு	♥ 24 state 0 0 19783 (3)400 (3)400 24 + X 86 0 21 Hit : 8