# EventLog Analyzer 快速操作手册

产品快速使用指南



技术支持部

本文档旨在帮助用户快速熟悉产品使用的方法。

Tel: 400 660 8680

# 目录

1.安装和使用EventLog Analyzer	3
1.1 系统要求	3
1.2 安装步骤	4
<b>1.3</b> 启动 ······	6
2.连接EventLog Analyzer服务器	10
3.添加监控设备	11
3.1 Windows设备	11
3.2 syslog设备及其它设备	13
4.导入日志	16
5.使用预定义报表	18
6.创建自定义报表	18
7.日志搜索	19
8.创建告警配置文件	20
9.高级配置	22

# 1.安装和开始使用EventLog Analyzer

从下载页下载EXE文件: <u>https://www.manageengine.cn/products/eventlog/download.html</u>

下载 首页 » 下载			
	信息排	是交成功!	
	白金版	分布式版本	
	म	始下载 4\\\2.xxx/227MB	
	321	位 64位	
		升级包	

#### 1.1 安装

在运行产品之前,检查是否满足前提条件。

#### 硬件需求

32位, 安装和运行Evenglog Analyzer的最小系统要求如下:

- 1 GHz, 32-bit (x86)奔腾双核处理器或其他相同性能处理器
- 2 GB内存
- 5 GB磁盘空间

64位,安装和运行Evenglog Analyzer的最小系统要求如下:

2.80 GHz, 64-bit (x64) 志强 (Xeon<sup>®</sup> LV) 处理器或其他相同性能处理器

- 2 GB内存
- 5 GB磁盘空间

EventLog Analyzer要求使用1024x768或以上的屏幕分辨率。

#### 操作系统要求

Tel: 400 660 8680

EventLog Analyzer可以安装和运行在以下操作系统(32位和64位)的设备上:

#### Windows

Windows 2016 Server Windows 2012 Server Windows 2008 Server Windows 2000 Server Windows 8 Windows 7 Windows 2000 Windows Vista Windows XP Windows NT

#### Linux

- Linux RedHat RHEL
- Linux Mandrake
- Linux Mandriva
- Linux SuSE
- Linux Fedora
- Linux CentOS
- Linux Ubuntu
- Linux Debian

#### VMware

VMware environment 支持的Web浏览器

#### 支持的web浏览器

Internet Explorer 11 最新Firefox 最新Chrome

#### 支持的平台和设备

EventLog Analyzer可以对任意1设备进行日志的收集、索引、分析、归档、搜索和生产报表。默认支持以下操作系统和设备的日志:

Windows	Server	2016	
Windows	Server	2012	
Windows	Server	2008	R2
Windows	Server	2008	
Windows	Server	2003	
Windows	Server	2000	
Windows	8		
Windows	7		
Windows	2000		
Windows	Vista		
Windows	ХР		
Windows	NT		
Linux -	RedHat	9.0	
Linux -	Mandral	ke	
Linux -	Mandriv	va 🛛	
Linux -	SuSE		

Tel: 400 660 8680

Linux - Fedora Linux - CentOS Linux - Ubuntu Linux - Debian UNIX - Solaris, HP-UX IBM AS/400 - Variants V5R1、V5R2、V5R3、V5R4、V5R5和V6R1 IBM AIX Cisco交换机和路由器 VMWare - Syslog版本 Windows的SNARE<sup>^</sup>

#### 默认还支持以下应用的日志

IIS W3C Web服务器 IIS W3C FTP服务器 Apache Web服务器日志 MS SQL Server Oracle 10 G Release 2 (10.2.0.3) - 审计日志 DHCP Windows日志 DHCP Linux日志 打印机日志

#### 1.2 启动

A. 双击下载后的exe文件打开安装程序, 阅读并选中同意许可协议的条款和条件

	EventLog Analyzer	L
License Agreement		
Please read the following licens	se agreement carefully.	
Press the PAGE DOWN key to	see the rest of the agreement.	
Software License Agreement ManageEngine EventLog Ana	lyzer	^
This License Agreement detai Analyzer ('Licensed Software * Evaluation License * Commercial License * Technical Support Please read the following licen order or download of the Lice	Is the policy for license of ManageEngine EventLo ") on the following topics: nse carefully, before either (i) completing the elevinsed Software from an authorised website, or (ii	ctronic
Do you accept all the terms of select No, the setup will close, accept this agreement. tallShield	the preceding License Agreement? If you . To install EventLog Analyzer, you must	Print

Tel: 400 660 8680

#### 选择安装产品的文件夹

默认安装位置是C:\ManageEngine\EventLogAnalyzer。 B.可以通过浏览选项,修改安装位置

EventL	og Analyzer	n.	-
Destination Folder			
Select a folder where the application will be	installed		
Click Next to install in this folder.			
To install in a different folder, click Browse	and select anothe	er folder.	
You can choose not to install EventLog Ana Wizard	alyzer by clicking C	Cancel to exit the	Installation
Destination Folder	1	6	1
C: ManageEngine EventLog Analyzer			Browse
taisnield			
			105

C. 默认端口号是8400。确保默认和所选端口号没有被占用

Eve	ntLog Analyzer	×
Begin Installation Review settings and begin installation		
Setup has enough information to begin Next to begin the installation.	n the installation. Click Back to mak	e any changes. Click
EventLog Analyzer	gine EventLog Analyzer	^
Port: 8400 Available Disk Space : 72049 MB		
		¥
<		>
tallShield	< Back Next >	Cancel

D. 输入个人信息以便获取技术支持

Registration for Technical Su Enter Your Details below	upport (Optional)	
Name		
E-mail Id		
Phone		
Company Name		
Country	-Select-	*
tallShield		NUL 201
	< <u>B</u> ack <u>N</u> ext	> Skip

E. 安装完成后,安装向导显示自述文件并启动EventLog Analyzer服务器

EventLog Analyzer
InstallShield Wizard Complete
Setup has finished installing EventLog Analyzer on your computer.
<ul> <li>✓ Yes, I want to view readme file</li> <li>✓ Start EventLog Analyzer in console mode</li> <li>Technical support: eventlog-support@manangeengine.com</li> </ul>
< Back Finish Cancel

Tel: 400 660 8680

F. 安装完毕后可以直接双击桌面图标启动EventLog Analyzer



同时,我们建议您在安装完毕后将EventLog Analyzer安装为windows服务,以 windows2012为例步骤如下:

(1) 点击左下角windows图标进入系统配置界面后点击左下角的箭头



(2) 找到Log360程序,首先点击Stop Log360停止程序运行,然后点击Install Log360 in Service。



Tel: 400 660 8680

(3) 安装成功后,可以在服务中看到该程序已经启动,之后每次启动操作系统时程序会随机启动。

		服3	F.				- 0
文件(F) 操作(A)	查看(V) 帮助(H)						
,服务(本地)	服务(本地)	-					
	ManageEngine Log360	名称 *	描述	袄态	自动类型	登录力	
		🔍 ManageEngine ADAudit	Activ	正在	自动	本地系统	
	停止此服务	🔍 ManageEngine ADAudit	Man	正在	手动	本地系统	
	<u>重用</u> 的此服务	🔍 ManageEngine ADMana	Activ	正在	自动	本地系统	
		S ManageEngine ADSelfSe	Activ		自动	adman	
	福沫	G ManageEngine DataSecu	Data	正在	自动	本地系统	
	A complete log management	AnageEngine DataSecu	Man	正在	手动	本地系统	
	solution	ManageEngine EventLog	Tool	正在	用助	本纳系统	
		C. ManageEngine Log360	A co	正在	自动	本地系统	
		ManageEngine Log360 U	User	正在	手动	本地系统	
		ManageEngine Office365	Com	正在	自动	本地系统	
		Microsoft iSCSI Initiator	首理		手动	本地系统	
		G Microsoft Online Service	启用	正在	自动	本地系统	
		🔍 Microsoft Software Shad	甘理		手动	本地系统	
		Microsoft Storage Space	Micr		手动	网络服务	
		🔍 Multimedia Class Schedu	基于		手动	本地系统	
		Net.Tcp Port Sharing Ser	揭供		禁用	本地服务	
		Q Netlogon	为用	正在	目动	本地系统	
		Retwork Access Protecti	网络		手动	网络服务	
		Retwork Connections	首理		手动	本地系统	
		Q Network Connectivity Ass	提供		手动(触发	本地系统	
		🔍 Network List Service	(RBI	正在	手助	本地服务	
		Average Network Location Aware	欲樂	正在	自动	网络服务	
		🔍 Network Store Interface	此程	正在	自动	本地服务	
		🗟 Optimize drives	通过		手动	本地系统	
		Q Performance Counter DL	使远		手动	本地服务	
		Reformance Logs & Aler	性能		手动	本地服务	
		C Dive and Diau	Jan L.	11.12	ni se	-1-1m 10/10	

# 2.连接EventLog Analyzer服务器

成功启动服务器后,按照以下步骤访问EventLog Analyzer。

- ●打开产品支持的web浏览器。键入链接URL: http://<devicename>:8400(其中<设备名称 > 是运行EventLog Analyzer的名称,8400是默认的web服务器端口。)
- ●使用默认的用户名/密码(admin/admin)登录EventLog Analyzer。
- ●点击"登录"按钮。



Tel: 400 660 8680

# 3.添加监控设备

#### 3.1 Windows设备

在所有的Windows设备,确保已启用WMI、DCOM,并且为各自的模块/对象启用日志。请使用第三方工具,如SNARE,转发syslog格式的Windows事件日志。

#### A.添加Windows设备

1.

1.选中配置选项卡,在左侧下拉菜单中选择设备管理,选中,点击添加windows设备选项 卡,点击右侧添加设备

EventLog Analyzer)	主页 报表 合规性 ?	意案 相关性 告誓 <mark>设置</mark> LogMe 支持					
	设备管理						
<b>父 配置</b> 管理设备	Windows设备 ⑦	Syslogi设备 ⑦ 其他设备 ⑦					
导入日志数据 管理应用源	透樺分类 全部设备	→ 配置域/工作組					+ 添加设备
管理文件完整性监视	Q 📀 📀 📽 🗄					1-1共1 10 *	添加/移除字段
管理风险源	abre 🗌	设备 ▼   显示P	下次目編	1210.974	秋志		
成的管理 管理派用数据 管理设备组 管理文件完整性模板 管理·Center	Fo /	10g340	2020-02-05 18:41:18	10 <del>531e</del>	<b>成</b> 功		

#### 2.在弹出的对话框中选择域/工作组,并添加搜索到的设备

) 不安全   47.10	04.189.192:8400/event/index2.doi	?tab=system&url=er	nberapp#/devicemanagement,	windows					
alyzer)	主页 报表 合规性 搜索	相关性 告答	添加设备			×			<b>26</b> 44
Q	设备管理		选择分类 adplus.cn	~		+ 手动配置			
			q		1-1共1 10 •	▼ 组织单位过滤器			
	Windows设备 ⑦	Syslog设备	268 〒	操作系统	组织单位				
	选择分类 全部设备		LOG360	Windows Server 2012 R2 D	D Domain Controll	ers			
観	Q 0 0 1 1								1-1
	动作	<b>设数 -  </b> 显示的					a ej fra		
	Eo /	log360					i310	成功	
板									
				添加 取消	í				

Tel: 400 660 8680

#### B.手动添加Windows设备

您还可以通过点击手动配置链接,手动添加设备。1.输入设备名称或IP地址。

2.使用管理员凭证,输入用户名和密码,点击验证登录链接。

3.点击"添加"按	钥。
-----------	----

手动配置		←返回 ×
	设备	
	添加为syslog设备	
	用户名	
	密码 脸证等	禄
<u></u>		
	添加 添加并关闭 取消	

Tel: 400 660 8680

#### 3.2 syslog设备及其它设备

1.选中配置选项卡,在左侧下拉菜单中选择设备管理,选中,点击添加syslog设备选项 卡,点击右侧添加设备

EventLog Analyzer)	主页 报表 合规性 搜索 相关性 告發 设置 し	agMe 支持		- 「開始時間 日本語の後裔 🦺 ? - 😁 
良重接来	设备管理			
<ul> <li></li></ul>	Windowsik 🕸 🕐 Systogik 📽 🔿	Meije ()		* #1012ff
管理文件完整性监视	Q 🌣 配蓋目初日志純友 📀 🤗 🖥			1-1共1 10 -
管理风险源	₩ <b>₩₩ ●</b>   显示P	最后派息时间 ▼	状态 ▼	
期別管理 管理原同数据 管理公論组 管理文件先整性模板 管理文件先整性模板	one one one one	×	重新日志	

2.添加Syslog设备窗口,点击发现&添加链接。您可以根据IP范围(开始IP至结束IP)或 CIDR,发现您网络中的Syslog设备。

添加Syslog设备			×
	设备	輸入主机,使用英文逗号隔开发现并添加	
		<mark>添加</mark> 取消	

3.输入开始IP和结束IP或CIDR范围,发现Syslog设备。

	(1) [1] [1] [1] [1] [1] [1] [1] [1] [1] [1]	Ē		(		范围			
开始IP	172	-	31	]-	79	]-[	0		
结束IP	172		31		79	-	255		

发现 - 选择发现时使用的SN	MP凭证		×
			➡ 添加凭证
Q <sup>€</sup> ∎			
✓ 名称	类型	描述	
<b>public</b>	SNMP V1	Default SNMP credential	
		返回	扫描

4.选择SNMP凭证,自动发现您网络中的Syslog设备。默认下,公共SNMP凭证可用于 扫描 您网络中的Syslog设备。或者,您可以通过点击添加凭证按钮 "+",添加SNMP 凭证。选择SNMP凭证后,点击"扫描"按钮,自动发现指定IP或CIDR范围内的Syslog 设备。

漆加SNMP先证		
凭证类型	SNMP V1	~
*名称	public	
描述	描述	
*SNMP读	public	
*SNMP端口	161	
	保存并继续添加	

5. 选中配置选项卡,在左侧下拉菜单中选择设备管理,选中,点击其它设备选项卡,点击 下方添加设备按钮

」资授素 C	设备管理			
父 配置				
言理设备	Windows设备 ⑦	Syslogi设备() 具他设备()		
导入日志数据				
會理应用源				
實理文件完整性监视				
官理风险源				
成肪管理				
「理漏洞数据	4		10-18780-1045 (BPT)-1045	
言理设备组	1		近有1000000000000000000000000000000000000	
會理文件完整性模板			◆ 添加设备	
會理vCenter			A	
日志收集器				

6.选择设备类型,输入设备名称后点击添加

	设备类型	ESXi		~	
	设备名称				
		8			
事件日志服	B务器运行在: lo	g360(172 31 79 124)			
オマチャートしょう					
在添加Uni. 在/etc/sysl	x设备前,请先配 log.conf文件中添	Services and the service of the ser			
在添加Uni 在/etc/sysl *.* @ever	x设备前,请先配 log.conf文件中添 ntloganalyzer	置syslog。 加:		_	
在添加Uni: 在/etc/sysl *.* @ever 在/etc/sen 軍改了端口	x设备前,请先配 log.conf文件中添 <b>ntloganalyzer</b> vices中更改syslo ]号后,在Unix设	■ 置syslog。 加: g服务的端口号为上面提 备中重新启动syslog后台	到的Syslog监听端[ 3程序。	].	
在添加Uni: 在/etc/sysl *.* @ever 在/etc/sen 更改了端口	x设备前,请先配 log.conf文件中添 ntloganalyzer vices中更改syslo ]号后,在Unix设	Bysiog。 加: g服务的端口号为上面提 备中重新启动sysiog后台	到的Syslog监听講口 a程序。	].	
在添加Uni. 在/etc/sysi *.* @ever 在/etc/sen 更改了端口	x设备前,请先配 log.conf文件中添 <b>ntloganalyzer</b> vices中更改syslo ]号后,在Unix设	■ m: g服务的端口号为上面提 备中重新启动syslog后台	到的Syslog监听講E a程序。	٦.	
在添加Uni 在/etc/sysi *.* @ever 在/etc/sen 更改了端口	x设备前,请先配 log.conf文件中添 ntloganalyzer vices中更改syslo ]号后,在Unix设	Besyslog。 加: g服务的端口号为上面提 备中重新启动syslog后台	到的Syslog监听端[ }程序。	].	

# 4.导入日志

EventLog Analyzer可以让您导入任何常用日志,并为Windows(EVTX格式)、syslog设备、应用程序和归档文件提供预定义报表。

1. 选中配置选项卡,在左侧下拉菜单中选择导入日志数据,点击右侧导入数据按钮

Others Q	导入日志文件							
父 配置	选择 日志美型 所有格式	~						◆ 9入日也
管理设备	Q 0 0 8							1-2共2 10▼ 面
导入日志数据	文件名称 🚽	设备	這程设备 协议	210/0/6	上次扫描时间 🚽	下次扫描时间 🚽	状态	能表
管理应用源 管理文件完整性监视	hsf.log	log360	27.211.1 68.122	一次导入	2020-01-06 17:48:33	ii.	导入成功	童春报表
2 理风险原 成粉管理 管理規模数据 管理设备组 管理文件杂制性模板	schedule.log	log360	27.211.1 68.122	一次导入	2020-01-06 17:29:27		导入成功	280x

 2.选择导入日志的方式(以本地导入为例),选择本地路径→浏览→找到在本地的日志 并导入

ManageEngine Eventlog Analy	< 🕀		1414/101010-0001-00000-0	<del>~</del>	
← → C ▲ 不安全   47.10	04.189.192:8400/event/index2.c	do?tab=system&url=emberapp#/log-import/configu	re		
EventLog Analyzer)	主页 报表 合规性 搜	索 相关性  告警 <mark>设置</mark> LogMe  支持			
设置投末へへ	导入配置		打开		×
父 配置	浏览文件	本地路径 共享路径 远程路径 云		<ul> <li>◆</li> <li>◆</li></ul>	P
管理设备		透影	组织▼ 新建文件夹 Goog	le Chrome	•
导入日志数据				35 8	
管理应用源			重 桌面 grand	Theft Auto V	
管理文件完整性监视			>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	et 快捷方式 F节	
管理风险源			a filos	9	-
威胁管理			■ 视频 文本文 0.25节	档	
管理漏洞数据			M 图片 Kingd	om Come Deliverance	
管理设备组			■ 文档	et 快速方式	
管理文件完整性模板				-12	*
管理vCenter			文件名(N): hsf.log	▼ 所有文件	•
日志收集器				打开(0) 取消	
2。管理设置			· · · · · · · · · · · · · · · · · · ·		
<b>二</b> 系统设置					

#### 3.选择在弹出的对话框中选择设备后点击导入即可

置捜索の	导入配置	
く配置	浏览文件	本地路径 共享路径 远程路径 云 🗸 🗸
理设备	所选文件	文件名 日志格式 自动验证 👻
入日志数据		hsf.log.txt
理应用源		
里文件完整性监视		
理风险源	相关设备	
协管理	1日天议画	one.one.one +
理漏洞数据	L	· · · · · · · · · · · · · · · · · · ·
里设备组		注意:导入的日志数据将存储两天。
理文件完整性模板		
		<b>弓)</b>
里vCenter		

Tel: 400 660 8680

#### 5.使用预定义报表

EventLog Analyzer提供固有报表,帮助分析网络安全和审计内部用户的活动。报表提供超过750种日志来源的信息,包括:

- ●网络设备,如防火墙、路由机、交换机和IDS/IPS
- ●应用程序包括Oracle和MSSQL服务器数据库
- ●Web服务器
- ●Windows和Linux/Unix机器

●IBMAS400系统

报表组包括Windows、应用程序、网络设备、漏洞、vCenter、我的报表、收藏夹 和基于 用户的报表。

#### 6.创建自定义报表

1.点击报表→管理报表→添加新报表

EventLog Analyz	zer)	±页 报表	合脫性	技家	相关性	告誓 设3	E LogMe	支持											+ <b>西加</b> Q 日日
1296 🗸	Windows	Unix/Unux	IBM A5/400	Cisco	SonicWal	Fortinet	juniper	Sophos	Meraki	PaloAlto	WatchGuard	Barracuda	Huawei	NetScreen	CheckPoint	HP	pfSense		
<b>q</b> matter		管理自定	义服表																+ 35.00755
Windows <del>事件</del>	•																		图 普通规定公
Windows严重性报表	•																		
Windows严重报表	•																		
Windows系统事件	•																		
威胁检测	•																		
移动硬盘审计	•											我不到自宠	2招表.						
网络策略服务器	,											y service and							
注册表更改	•																		
Windows备份和恢复	•																		
应用崩溃	•																		
Windows防火增审计	•																		
来自杀毒软件的威胁检测																			
基础架构报表	· · · ·																		
Hyper-V服务器事件																			
Windows防火這威胁	•																		
应用白名单	•																		
程序清单	•																		
过事件																			
Hyper-V虚拟机关联																			
- distant																			

2.在弹出的页面中依次填入报表名称,选择好设备及其它信息后,点击添加即可

EventLog Analyze	r) ±	75 18#	A8#	10-01	10.54	44 <b>5</b> 3	2011 Lov	Ma the											B244230		
12.11	Windows	Unix/Linux	IBM AS/400	Cisco	SonicW	all Fortin	net Junip	er Sophi	is Mera	ki PaloAlto	WatchGuard	Barracud	a Huawel	NetScreen	CheckPoint	HP	pfSense	•		100.055	★ 収蔵
Q METRER		创建自定	义报表																		
Windows事件	•	* 报表名称			测试								选择设备		UnixGroup	p		+			
Windows严重性报表		报表组			默认道			~					报表类型		表格视图			~			
Windows影快事件		报表标准																			(*)
威胁检测	•								Г						1.00						0
移动硬盘审计	,									严重性	~	等于	*	未过举任何内容	~						
网络策略服务器 注册表示改	,	标准模	武:((严重性:))																		+ 第20道
Windows备份和恢复	,											27.10	Decisi.								
应用崩溃												Herter.	秋川村								

# 7.日志搜索

EventLog Analyzer的日志搜索功能非常简单,您可以搜索任何信息。默认下,在日志中查 找输入的搜索项。搜索结果可以保存为PDF和CSV格式。



要搜索日志,请点击搜索选项卡,选择好设备及日志类型后点击搜索即可

Tel: 400 660 8680

### 8.创建告警配置

EventLog Analyzer可以配置为,当发生指定的安全事件时,产生告警。您可以:

- ●从500多种预定义告警中选择或自定义告警
- 当发生任何需要关注的事件时,通过电子邮件或短信获取实时通知。
- ●指定生成告警时运行的程序。
- ●配置事件监控的设备或设备组。
- 指定触发告警事件发生的次数和时间段。
- ●对任何合规策略事件进行告警。
- ●接收相关性告警,例如,两件或多件相关事件,需要进一步调查。

#### 需要创建告警配置文件:

1.点击告警选项卡,选择右侧添加告警配置文件

推案	q	管理告警配	置文件					+ 添加吉留創造文的
全部告警							2020-09-07 11:12	12 2020-09-07 13:12:12
民的告誓		Q 0 (	富 更多选项 •					1-10共103 <b>&gt; &gt;&gt;</b> 10 •
未指派的告誓			音響名称 🚽	東京	严重性	设备/组配置	通知典型	
alert.default.threat			123	相关配置文	件 High	基于相关性规则定义		0
*重告答			SAP密码变更	自定义	Low		1	0
基于配置文件的告答 相关性告答配置文件	•		SAP攻击	自定义	High	12	2	0
	- 1		SAP配置变更	自定义	High	*)		0
6 告答配置	-		网络设备Fan失败	自定义	High	. 60		0
管理告尝配置文件			网络设备失败的登录	自定义	High	one.one.one		0
工单系统配置			网络设备攻击	自定义	High	one.one.one	2	0
指派规则			网络设备管理员已添加	自定义	Low		8	0
lert.default.manageworkf	low		网络设备系统关闭	自定义	High	1.02		0
			网络设备配置变更	/ 自定义	High			0

2.在弹出的对话框中输入告警名称,所需要的告警的设备,以及需要选择告警的类型,并 选择好告警通知管理员的方式。

Evention Analyzer ) and any	離時到日志接枚器 🦺 ? - 😁 -
王····································	・ 福加 Q 日志理索
<u>まま</u> Q 添加店等配置文件	< 返用
全部告答 - 동동2余 (ct/l)	
我的告诉	
指派的告答 严重性 蕊 💙	
未报版的告答 * 法理设备 UnixGroup,WindowsGroup +	
alert.default.threat / · ·································	
P#AS	
基于影雷文件的伤害 , 高明起雷 ,	
相关性告告和意义并 , 通知设置 运行程本 工作点	
<b>8</b> 告告起责 -	
管理管理配置文件 发送费印 所有告答 V	
alert.default.manageworkflow ① 请赴重的年轻多得以应用影片告告。 配量供应服务器	
SMS200 (?)	
<ul> <li>() 律型重545级名编ULE用5455年8. 配置54558条制</li> </ul>	
denation to a	

# 3.单击保存配置文件的按钮后,即可生成新的配置文件

	04.100.41.92		cogine 3030				A 18 440 878 878 77
R.R. Q	日田日子	nca.x#					+ AGUNTHERXS
全部告答						2020-09-07 11:12:12	2020-09-07 13:12:12
我的告答	Q 0	意 更多透现。					1-10共104 <b>&gt; &gt;</b> 10 •
未指派的告答		舌間名称 🗸	異型	严重性	设备/图配查	通知美型	计数
alert.default.threat		123	相关配置文件	High	基于相关性规则定义		0
严重告答		SAP攻击	自定义	High	~		0
基于配置文件的告答	- D	SAP配置变更	自定义	High	*		0
相关性告誓配置文件	1	奧试	预定义的	High	WindowsGroup,UnixG	(* <sup>-</sup>	0
♣o 告答配置 •		网络设备Fan失败	自定义	High	5	÷	0
管理告答配置文件		网络设备失败的登录	自定义	High	one.one.one	1.	0
工单系统配置		网络设备攻击	自定义	High	one.one.one		0
推派规则		网络设备管理员已添加	自定义	Low	-	52.	0
alert.default.manageworkflow		网络设备系统关闭	自定义	High			0
		网络设备配置变更	自定义	High	*		0

# 9.高级配置

#### 数据库维护

在数据库维护中可以设置当前存储大小,定义收集的原始日志将保留在数据库中的天数、 相关性保留期定义格式化日志数据将保留在数据库中的天数、告警保留期定义告警将在数 据库中保留的天数。

在设置选项卡中单击数据库维护设置即可看到,并可以在相应位置设置您需要保留的 天数。

EventLog Analyzer)	主页 服表 合规性 微素 相关性 告誓 <mark>设置</mark> LogMe 支持	跟我我们到日本跟我们的潜入。
设置投票	DB保留设置	
父 配置	当朝存储大小: 32 天	
2。管理设置	相关性保留期: 90 夫	
管理代理 管理存档 技术员和角色	告告读 <b>这时</b> 90 天 1111	
登录设置 域和工作组 工作时间设置 产品设置	<b>被助</b> 方 · 编码存得这小信义公司的原始目前将存留石放振荡中的汗我,将预除号子配置的最长真的目中,默以虚为2万, · 相关性保留相信义统式化启在放振符得留在放集中的污我,做式学子能量做的目在将被删除。默以虚为20万,	
数据库增护设置 日志收集过滤器 日志收集放輝告警	* 告告将某种艺术告告所在初期每年将推荐力功。在1982元初之前发出的古台所被型牌。和从188480万以大。	
授表配置文件 完制日志解析		
地域の 時私设置 标签 Log360 元		

#### 归档设置

EventLog Analyzer可以定期归档日志。您可以配置归档间隔和保留期限,归档日志为加密 和设置时间戳的日志。

在设置选项卡中单击管理存档后,在上方选择设备,即可看到相应的数据

EventLog Analyzer	主页 报表 合规性 搜讨	素相关性 告發 📴 LogMe	支持				說時到	日志接收器 뵞 ? \varTheta
役官授業	归档日志							<b>\$</b> 193
父 配置	选择设备 UnixGroup,Window	vsGroup + 滴理						点击选择日期范围。 🕍
	<b>日</b> 加速机械							1 - 39 共 39
管理代理	2 28 -					完整性		
管理存档	log360	Windows	2019-12-30 18:47:04	2019-12-30 23:46:33	185 KB	◎ 验证	数据已可用。	
技术员和角色	log360	Windows	2019-12-30 23:47:48	2019-12-31 23:46:10	628 KB	0 ktiž	数据已可用,	
登录设置	log360	Windows	2019-12-31 23:47:00	2020-01-01 23:46:12	619 KB	0 kie	数据已可用。	
域和工作组	log360	Windows	2020-01-01 23:49:59	2020-01-02 23:46:42	681 KB	0 RE	数据已可用。	
工作时间设置	log360	Windows	2020-01-02 23:48:00	2020-01-03 23:46:54	652 KB	• 10E	数据已可用。	
产品设置	log360	Windows	2020-01-03 23:46:54	2020-01-04 23:46:48	622 KB	◎ 独证	数据已可用。	
数据库维护设置 口十次传 计运转	log360	Windows	2020-01-04 23:47:18	2020-01-05 23:46:17	546 KB	• 121E	数磁已可用。	
日本後年が開始期	log360	27.211.168.122_schedule.log	2019-12-24 06:08:00	2019-12-26 15:40:01	205 KB	<ul> <li>Mole</li> </ul>	數據已可用。	
报表配置文件	log360	Windows	2020-01-05 23:47:02	2020-01-06 23:46:19	612 KB	• 10E	数据已可用。	
定制日志解析	log360	27.211.168.122_hst.log	2019-12-26 10:29:45	2019-12-26 16:07:34	19 MB	0 ME	数据已可用,	
隐私设置	log360	Windows	2020-01-06 23:47:39	2020-01-07 23:46:20	567 KB	0 ME	数据已可用。	
标签	log360	Windows	2020-01-07 23:48:06	2020-01-08 23:51:09	528 KB	0 ME	数据已可用。	