

# 天翼云・ 安全专区

# 用户使用指南

中国电信股份有限公司云计算分公司



目录

	目	录
1 业务控制台说明		5
1.1. 管理控制台说明		6
1.1.1. 系统信息		6
1.1.2. 账号口令管理		6
1.1.3. 网络管理		7
1.1.4. 日志配置管理		8
1.1.5. 系统工具		8
1.1.6. 日期时间管理		11
1.1.7. 数据库备份与恢复		11
1.1.8. 日志备份与恢复		12
1.1.9. 系统恢复		12
1.1.10. 重置平台初始化口令		12
1.1.11. 系统停止和重启		13
1.1.12. 系统参数配置		13
1.1.13. 配置管理		13
1.1.14. 下载运维日志		14
2 业务系统配置		14
2.1. 资产管理配置		15
2.1.1. 简介		15
		I



2.1.2. 常规设置	
2.1.3. 自定义资产添加	23
2.2. 日志标准化配置(必配)	26
2.2.1. 日志接入说明	26
2.2.2. syslog 方式(常见): linux 系统及网络设备接入	27
2.2.3. WMI 方式(常见): windows 系统接入	
2.2.4. 文件方式	42
2.2.5. 数据库方式	
2.2.6. 日志归并	46
2.2.7. 日志过滤	47
2.2.8. 流量引擎	
2.3. 关联策略配置(选配)	50
2.3.1. 关联策略说明	50
2.3.2. 具体配置	55
2.4. 审计策略配置(选配)	65
2.4.1. 审计策略说明	65
2.4.2. 具体配置	
2.4.3. 审计对象管理	72
2.5. 告警监控	
2.6. 实时监控	83
2.7. 报表管理	84
	11



2.7.1. 报表实例	
2.7.2. 报表任务	
2.8. 云端配置	
2.9. 拓扑图配置(选配)	
2.9.1. 具体配置	
3 事件查看	91
3.1. 安全仪表盘查看	
3.2. 日志列表	
3.3. 关联事件(选配)	
3.4. 审计事件(选配)	
3.5. 流量日志(选配)	
3.6. 导出任务管理	
4 日常维护	
4.1. 软件版本升级	
4.2. 修改密码	
4.3. 恢复出厂设置	
4.4. 系统巡检	
4.5. 修改 IP 地址	
4.6. 日志查看	
4.7. 日志备份与恢复	
4.8. 数据库备份与恢复	
	111



4.9. 身	〔群维护(选配)	116
4.10.	系统配置	118
4.11.	业务配置管理	120
4.12.	运维日志下载	121
4.13.	常用配置命令	121
5 实放	拖后设备运行检查	124
5.1	整体运行状态检查	124
5.2	设备日志检查	126
5.3	主要功能使用情况检查	126



# 1 业务控制台说明

用户对 LAS 系统的绝大部分操作主要通过业务控制台完成。通过业务控制台可以对 LAS 系统的具体业务模块进行设置、安全内容进行查看,主要包含授权更新、日志标准化设置、 资产管理、告警策略配置、安全事件查看等等。

▼ 安全概点	Ritting a			Time-						c	5.2
<ul> <li>安全监控</li> </ul>	810 44 E	44513001 HH513001	H 1 10075	33/00/2							<u>∧</u>
• 日志查询	1400310										74
<ul> <li>报表管理</li> </ul>	告警		关联事	件		审计事件			日志		
<ul> <li>策略管理</li> </ul>	1		12			4			4030		
<ul> <li>资产管理</li> </ul>	重点关注日志Top10										配置
<ul> <li>日志采集</li> </ul>											
> 系统管理	SU会话	SSHI] sen		rsyn	ctl	SSH会	SSHIE	删除用户	编建版户	用户口令	
	<b>82</b> 逝7日:82	<b>492</b> 近7日: 492 近7	002 8 : 1002	<b>1002</b> 近7日:1002	<b>1001</b> 近7日:1001	<b>164</b> 逝7日:164	<b>82</b> 逝7日:82	<b>41</b> 逝7日:41	<b>41</b> 近7日:41	<b>41</b> 近7日:41	
	重点设备				配置	重点资产 👔					配置
	172.16.0.10				4030	资产名称	风险等	踧 世	吉智分布		
						172.16.0.10	<b>(</b> 2)		0010		
	内部互连威胁		内部威胁分	市		外部安全					全部 ▼

使用 WEB 方式登录方式

操作步骤:

#### 单点登录日志审计

1、通过天翼云安全账号登录天翼云控制中心,进入天翼云等保安全专区安全管理平台,在
 平台中找到安全专区,点击【云日志审计】->【操作】登录。

<u></u>	、天蜀亡。											×	<b>•</b>	۳×
6 5	e cloud	安全管理中心	组合管理											_
		组供管	Į₩											
			λ±											
4 8	18957 ØT											EXHWR	Q BER	重用
	U全分析	云主机名称	。 関型 0	产品規格 ○	存储空间 0	地域 0	VPC 👳	₩JPIP ©	公同IP ⇔	許可信息 ≎	版本信息 🜼	状态	操作	
<b>1</b>	含管理	AQZQ-EDR est	-vpct 终端安全EDR	离可用架构 + 弹 性带宽		广州4	vpc-test	192.168.0.202		1000			42	
8.4		AQZQ-LAS	-vpct 云日志审计	高可用架約 + 弹 性带家		广州4	vpc-test	192.168.0.189		1000			@ ©	
ii 1 ⊗ s	J单管理 《统管理	AQZQ-OSN test	I-vpc 云堡垒机	高可用架构 + 弹 性带宽		广州4	vpc-test	192.168.0.24		1000			0	
		AQZQ-AF-v	pcte 云劼火墙	高可用銅約 + 弹 性带宽		广州4	vpc-test	192.168.0.153		1000			⇔ ©	
											共4条	< 1 → [	10 奈/页 > 跳至	1 页

2、从安全管理平台进行单点登录,无需密码,点击进入,即跳转进入。

Co 天賀石   LAS 3.	0.5			当前事件速率(Liceps) Q.企文检索	<u>)</u> cssp_t
导航菜单	安全概题 ③ 欢迎登录 日志市计系统	↓!当前时间: ,系统已运行 13天6小€	135分钟 。		-
▼ 安全概范	整体状况 审计分析 告誓纲况	事件分析 系统状态			0.2
<ul> <li>安全监控</li> </ul>	♀ 標示: 系统检测型终未开启审计策略。				×
<ul> <li>日志査询</li> </ul>	ergoz:				
> 报表管理	196.75.73 10				40.
策略管理	告警	关联事件	审计事件	日志	
资产管理	0	0	0	147842	
<ul> <li>日志乐集</li> </ul>	重点关注日志Top10				RE
> 系统管理					
	2005				
	9999+				
	近7日: 9999+				
	重点设备		配置 重点资产 🕢		配置
	192.168.0.61		3411716		
				智无数据	
	内部互连威胁	内部威胁分布	外部安全		全部 *

# 1.1. 管理控制台说明

# 1.1.1.系统信息

Cloud

展示产品硬件、版本等信息,如下:

导航荣单	系统信息		
▶ 系统信息			
账号口令管理		硬件标识	06E4C-8A438-7A526-CFC85-44C98
▶ 网络管理		软件版本号	3.0.4
▶ 索引配置管理			
<ul> <li>系统工具</li> </ul>		软件序列号	EF7CD-+47/7-C/EEA-2320F-D3CD4
日期时间管理		编号	Mzg4XzM0NzBfMzQ3MF8zNDcwXzM0NzBfMzQ3MF8zMzdfMzQ3MF8zNDcwXzM0NzBfMzQ3MF8zNDcw
<ul> <li>数据库备份与恢复</li> </ul>			
▶ 日志备份与恢复			
▶ 系统恢复			
▶ 重置平台初始口令			
▶ 系统停止和重启			
> 系统参数配置			
▶ 抹脓白检数据			

展示产品硬件、版本等信息。

# 1.1.2. 账号口令管理

用户可以修改管理的口令,如下:

导航单单	账号口令管理			
▶ 系统信息				
▶ 账号口令管理	账号	admin		
▶ 网络管理	原密码			
▶ 索引配置管理				
<ul> <li></li></ul>	新密码			
▶ 日期时间管理	确认密码			
<ul> <li>数据库备份与恢复</li> </ul>				
▶ 日志备份与恢复		_		
<ul> <li>         系统恢复     </li> </ul>			保存	
▶ 重置平台初始口令				
<ul> <li>系统停止和重启</li> </ul>				
> 系统参数配置				
<ul> <li>抹除自检数据</li> </ul>				

# 1.1.3. 网络管理

Cloud

1. 用户可以设置网络的地址、掩码、DNS、网关等(工作口配置任何网口都可用于流量接入口使用),如下:

导航荣单	<b>M</b>	名管理																							
<ul> <li>系统信息</li> </ul>	网络配置	路由國	昭置																						
▶ 账号口令管理																									
▶ 网络管理			主机名	local	lhost.localdomain																				
▶ 素引配置管理				172.16	50154 ×		① T作口	x eth1	1																
▶ 系统工具			<b>A</b> 2015	172.10	0.0.254		1111																		
<ul> <li>日期时间管理</li> </ul>			网关	172.1	16.0.1		DNS	8.8.8																	
<ul> <li>数据库备份与恢复</li> </ul>	<b>#0</b>	<i></i>			1997 4			199.46																	
<ul> <li>日志备份与恢复</li> </ul>	序号	名称			IPV4			IPV6																	
▶ 系统恢复			IPV4	地址	172.16.0.154		IPV6地址	2001::154																	
▶ 重置平台初始口令	1	eth0	IPV4	1掩码	255.255.255.0		子网前缀长度	64																	
<ul> <li>系统停止和重启</li> </ul>																									
▶ 系统参数配置	2		IPV4	1地址	10.251.251.128		IPV6地址																		
抹除自检数据	2	eurz	IPV4	4掩码	昭 255.255.255.0		子网前缀长度																		
					10.050.050.100		and call 11																		
	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3 eth2	eth2	eth2	eth2	IPV4	11611	10.252.252.128		IPV6181		
			IPV4	1把的	255.255.255.0		子阿丽摄长度																		
				IPV4	地址	10.253.253.128		IPV6地址																	
	4	eth3	IPV4	1摘码	255 255 255 0		子网前缀长度																		
					233,233,233,0			[]																	
			IPV4	4地址	10.254.254.128		IPV6地址																		
	5	etn4	IPV4	1掩码	255.255.255.0		子网前缀长度																		

### 2.路由配置工具:设置系统路由信息

导航菜单	网络管理									
▶ 系统信息	NikRE BinhRE									
<ul> <li>账号口令管理</li> </ul>	系统路由表									
<ul> <li>网络管理</li> </ul>	目的IP地址		网关	接口						
<ul> <li>&gt; 索引配置管理</li> </ul>	10.252.252.0		0.0.0.0	eth2						
<ul> <li>系统工具</li> </ul>	10 254 254 0		0000	eth4						
<ul> <li>日期时间管理</li> </ul>	47346.00		0.0.00	10						
<ul> <li>数据库备份与恢复</li> </ul>	172.18.0.0		0.0.0.0	ethu						
▶ 日志备份与恢复	10.253.253.0		0.0.0.0	eth3						
▶ 系统恢复	10.251.251.0		0.0.0.0							
• 重查半台初始口令	169.254.0.0		0.0.0.0							
> 系统停止和重局	169.254.0.0		0.0.0.0							
<ul> <li>新玩学校印刷</li> <li>1134014470197</li> </ul>	169.254.0.0		0.0.0.0							
* 34464CH1228/351	169.254.0.0		0.0.0							
	0000		172 16 0 1							
	静态路由表									
	目的IP地址	网关	接口	操作						
		当前无可用记录								
		♣新増静态路由								



# 1.1.4. 日志配置管理

配置日志库提交线程与性能,如下:

导航荣单	索引配置管理		
▶ 系统信息			
账号口令管理	索引线程数量	2	
<ul> <li>网络管理</li> </ul>	MARKET PLAN	10000	1
▶ 索引配置管理	#BARENE>CROM	10000	J
▶ 系统工具	30秒索引提交事件量	15000	
<ul> <li>日期时间管理</li> </ul>			
<ul> <li>数据库备份与恢复</li> </ul>	索引库分片数量	1	
<ul> <li>日志备份与恢复</li> </ul>	保活素引库天数	7	1
<ul> <li>系统恢复</li> </ul>			1
• 重置平台初始口令			
<ul> <li>系统停止和重启</li> </ul>			特政
> 系统参数配置			
▶ 抹脓自检数据			

详细说明:

参数项	优化说明
日志线程数量	<ol> <li>1、提交日志的线程数与 CPU 的线程数有关系,可以配置最 大线程数的一半</li> <li>2、可以提升事件的写入性能</li> </ol>
单线程提交数量	1、单线程的日志写入能力, 依赖 CPU 的性能, 默认配置 10000, 一般不建议修改
30 秒日志提交事件 量	1、 触发日志序列化的数据量大小,一般不建议修改
日志库分片数量	1、非集群项目不做修改
保活日志天数	<ol> <li>1、ES保持开启的最大日志库数量,默认 31 天,如果 业务上对 31 天以前的数据</li> <li>2、不频繁查询,不建议修改</li> </ol>

# 1.1.5. 系统工具

1. 检测工具:对目标地址进行 traceroute、ping、tcpdump 操作

导航单单	系统工具		
<ul> <li>系统信息</li> </ul>	他到1日 5512年9月17 预加带持下数 许可道理 或者的"穿 外营养法 用机比例		
▶ 账号口令管理			
▶ 网络管理	目标地址		
▶ 素引配置管理			
▶ 系统工具	cteuro and a second a		
<ul> <li>日期时间管理</li> </ul>			
<ul> <li>数据库备份与恢复</li> </ul>			
<ul> <li>日志备份与恢复</li> </ul>			
<ul> <li>系统恢复</li> </ul>	與行結果		
• 重置平台初始口令			
> 系统停止和重启	ping traceroute tcpdump 🖓		
> 系统参数配置			
▶ 抹脓白检数据			

2.SSL 证书制作:由于浏览器对 HTTPS 服务的非授权机构授权证书不信任,浏览器会弹出信 任警告并支持添加例外,用户也可以通过制作 SSL 证书并导入客

户端浏览器,使其信任该网站

loud

导航菜单	系统工具		
▶ 系统信息	● SSL证书制作功能为重新制作应用系统的SSL证书,制作成功底可在应用系统登录页面下载证书!		
▶ 账号口令管理	社会工具 SSL证书物件 原始带体下载 许可击弹 磁曲扩容 外質存储 接机绘图		
▶ 网络管理			
▶ 索引配置管理	1Piktuście A-		
<ul> <li>系统工具</li> </ul>			
▶ 日期时间管理	Prittinguade-		
▶ 数据库备份与恢复	Philuiddea		
日志备份与恢复			
<ul> <li>系统恢复</li> </ul>	中地址或超四		
▶ 重置平台初始口令	1P地址或综合五		
▶ 系统停止和重启			
系统参数配置			
▶ 抹除自检数据	证书制作		

3. 原始日志下载: 下载原始日志或者通用日志

导航菜单	系统工具
▶ 系统信息	检测工具 SSU证书制作 <b>经给押件下载</b> 许可猜理 视曲扩容 外置存益 持机绘则
▶ 账号口令管理	
▶ 网络管理	日本施择 ④ 所有日本 ③ 通用日本
▶ 索引配置管理	10 46 Hibb
<ul> <li>系统工具</li> </ul>	
▶ 日期时间管理	下磁床数 1000
<ul> <li>数据库备份与恢复</li> </ul>	原始日志文任 序号 文件名 大小(KB) 操作
▶ 日志备份与恢复	
<ul> <li>系统恢复</li> </ul>	
▶ 重置平台初始口令	开始
▶ 系统停止和重启	
> 系统参数配置	
抹除自检数据	

4. 许可清理:清理产品当前许可信息已便重新授权



大異 Cloud

> 5. 磁盘扩容: 当系统内置存储不足以支撑用户的存储需求时,可以通过该功能进行本地磁盘 扩容

导航荣单	系统工具		
系统信息	他與工具 SSL证书制作 原始事件下载 许可通道 <b>建位扩</b> 容 外景存载 持机绘制		
> 账号口令管理			
▶ 网络管理	불효상료 VelGroup-N_cpt151G,VelGroup-N_root40G		
▶ 索引配置管理	新聞總盘 请说师 •		
▶ 系统工具			
<ul> <li>日期时间管理</li> </ul>			
<ul> <li>数据库备份与恢复</li> </ul>			
<ul> <li>日志备份与恢复</li> </ul>			
<ul> <li>系统恢复</li> </ul>			
• 重置平台初始口令	趣交		
<ul> <li>系统停止和重启</li> </ul>			
<ul> <li>系统参数配置</li> </ul>			
<ul> <li>抹鯰自检数据</li> </ul>			

6. **外置存储:** 当系统内置存储不足以支撑用户的存储需求时,可以通过该功能进行外置存储 扩容(IP 地址: 172.16.0.171; 路径: /opt/nfstest)

导航荣华	系统工具
▶ 系统信息	也與工具 SSL证书制作 居始事件下载 许可请遣 袒血扩容 <b>分置存缩</b> 拷约处测
▶ 账号口令管理	
<ul> <li>网络管理</li> </ul>	存他方式 ④ NPS
> 索引配置管理	19%bù
<ul> <li>系统工具</li> </ul>	
<ul> <li>日期时间管理</li> </ul>	調会
<ul> <li>数据库备份与恢复</li> </ul>	
<ul> <li>日志备份与恢复</li> </ul>	
<ul> <li>系统恢复</li> </ul>	
▶ 重置平台初始口令	11年 29年
▶ 系统停止和重启	
<ul> <li>系统参数配置</li> </ul>	
<ul> <li>抹除自检数据</li> </ul>	

7. 拷机检测:硬件出厂前设备稳定性测试,一般不建议用户使用



# 1.1.6. 日期时间管理

大異 Cloud

用户可以修改时间、日期及时区信息(仅限平台服务器),如下:

导航菜单	日期时间管理		
<ul> <li>系统信息</li> </ul>			
▶ 账号口令管理	当前日期	2019-07-25	
▶ 网络管理	********	2-44-22	
▶ 索引配置管理	⇒man	2.99.23	
▶ 系统工具	当前时区	Shanghai 🔻	
<ul> <li>日期时间管理</li> </ul>			
<ul> <li>数据库备份与恢复</li> </ul>			
<ul> <li>日志备份与恢复</li> </ul>		_	
<ul> <li>系统恢复</li> </ul>			Q77
• 重置平台初始口令			
<ul> <li>系统停止和重启</li> </ul>			
> 系统参数配置			
<ul> <li>抹脓白检数据</li> </ul>			

## 1.1.7. 数据库备份与恢复

用户可以设置数据的备份方式(仅限平台服务器),如下:

导航单单	数据库省份与依复			
<ul> <li>系统信息</li> </ul>	● 出版媒体出现异常与较无法使用的情况,可以通过数媒体终其功能恢复到指定时间点。数据常备份社会;系统内置接触,用户自注义策略,历史统计数据等!			
▶ 账号口令管理	餐价 你算			
▶ 网络管理				
▶ 索引配置管理	备份编略 ③ 不备约 ④ 白定文 ③ 立即备约			
▶ 系统工具	500 · 0 · 0 · 0			
<ul> <li>日期时间管理</li> </ul>	mman a av a s			
<ul> <li>数据库备份与恢复</li> </ul>	备份方式 ⊛ SFTP ◎ NFS			
▶ 日志备份与恢复	1P Mah			
<ul> <li>系统恢复</li> </ul>				
• 重置平台初始口令	89			
<ul> <li>系统停止和重启</li> </ul>	\$FEA			
> 系统参数配置				
▶ 抹脓白检数据	) BO			
	90			
	447			

1.1.8. 日志备份与恢复

Cloud

导航荣单	日志备份与恢复		
<ul> <li>系统信息</li> </ul>	● 当日本文件丢失或者无法正常使用时,可以通过日本收留功能将某一天或某一局的数据进行收复,日本备合周期为每天时,会定期备份的一天的数据,备份周期为因时,会定期备份上一局的数据		
▶ 账号口令管理	<b>各</b> 份   位真		
<ul> <li>网络管理</li> </ul>			
▶ 索引配置管理	备份策略 ◎ 不备份 ● 自定义		
<ul> <li>系统工具</li> </ul>	<b>8</b> 40回题 @ 40天 ① 国		
▶ 日期时间管理			
<ul> <li>数据库备份与恢复</li> </ul>	备他方式 ④ SFTP ③ NFS		
<ul> <li>日志备份与恢复</li> </ul>	1P%bb		
<ul> <li>              系统恢复      </li> </ul>			
• 重置平台初始口令	10 C		
<ul> <li>系统停止和重启</li> </ul>	密码		
> 系统参数配置			
<ul> <li>抹除自检数据</li> </ul>	調發		
	829		

# 1.1.9. 系统恢复

用户可以将系统恢复至初始状态,即清除所有过往数据,故需慎用,如下:

导航单单	系统作复
<ul> <li>系统信息</li> </ul>	● 系统抗复至出厂设置,相应的生产数据将被消除,加带件配置有变化,图icense将不可用,清整新申请icense!
<ul> <li>账号口令管理</li> </ul>	
▶ 网络管理	
▶ 索引配置管理	
<ul> <li>系统工具</li> </ul>	如需 系统恢复,请点击下方按钮!
<ul> <li>日期时间管理</li> </ul>	
<ul> <li>数据库备份与恢复</li> </ul>	
<ul> <li>日志备份与恢复</li> </ul>	
<ul> <li>系统恢复</li> </ul>	
• 重置平台初始口令	<b>—</b>
<ul> <li>系统停止和重启</li> </ul>	
> 系统参数配置	
▶ 抹除白松酸精	
	系統的対

# 1.1.10. 重置平台初始化口令

重置 8443 页面 admin 用户密码,如下:

导航菜单	重责前台超级管理员告码			
<ul> <li>系统信息</li> </ul>	夏其時前自續後豐豐魚的前妻豊力初始後期			
<ul> <li>账号口令管理</li> </ul>				
▶ 网络管理				
▶ 索引配置管理				
▶ 系统工具	如需 重置 密码 (请点击下方按钮)			
▶ 日期时间管理				
<ul> <li>数据库备份与恢复</li> </ul>				
▶ 日志备份与恢复				
<ul> <li>          系统恢复      </li> </ul>				
▶ 重置平台初始口令				
<ul> <li>系统停止和重启</li> </ul>				
> 系统参数配置				
▶ 其意:白台歌娟	a			
	単語名称			



# 1.1.11. 系统停止和重启

重启或关闭机器,如下:

与航卒单	系统停止与重启		
<ul> <li>系统信息</li> </ul>	● 系统里启成系统停止过硬件系统起作用!		
▶ 账号口令管理			
▶ 网络普理			
▶ 索引配置管理			
▶ 系统工具		如需 系统重启、请点击下方按钮!	如需 系统停止,请点击下方按钮!
→ 日期时间管理			
▶ 数据库备份与恢复			
▶ 日志备份与恢复			
▶ 系统恢复			
▶ 重置平台初始口令			
▶ 系统停止和重启			
> 系统参数配置			
→ 抹放白检数据			
		<b>新桃室</b> 前	adarejit.

# 1.1.12. 系统参数配置

配置系统参数信息,如下:

导航菜单	系统參数配置			
▶ 系统信息	采集配置			
▶ 账号口令管理				
▶ 网络管理	釆集主端口	514		
▶ 索引配置管理	采集端ロー			
▶ 系统工具				
→ 日期时间管理	采集端口二			
▶ 数据库备份与恢复	6215403286	4		
▶ 日志备份与恢复	NTTI STERX	-		
<ul> <li>系统恢复</li> </ul>	过滤线程数	1		
• 重置平台初始口令	Charles and the second s			
> 系统停止和重启	()加速速度	⊕# ®≆		
> 系统参数配置	采集超负荷处理方式	◎ 仅存储原始	日志 💿 丢弃	
,抹除自检数据	采集机负载均衡配置		口能输入大于等于1的正常数	
	自身负载	1		
	6.8.9.0%			
	贝戴普户塔			
	SNMP服务配置			
	8770	о <b>п</b> . о <b>м</b>		
	是否开启	⊛# © ¥		
	团体名	BDSEC_20	16	
	6 M 400			

采集配置: 配置日志接受的端口;

采集机负载均衡配置:集群信息配置,(需要搭建集群环境);

SNMP 服务配置: 配置团体名信息(团体名: test; 允许的 IP: 172.16.0.171);

SYSLOG 服务配置: 配置转发第三方服务(服务 IP: 172.16.0.171);

SSH 服务配置: 配置是否可以使用 ssh 直接连接;

U-key 配置:指定 Ukey 服务器配置。

#### 1.1.13. 配置管理

配置管理功能适用于新旧产品配置迁移场景,迁移的新旧产品必须为同一版本。

分航菜单	配置管理	
▶ 系统信息	● 该功能只适用于新装的产品和进行系统恢复后的产品	
▶ 账号口令管理		
▶ 网络管理	<b>②配置文件</b> 请选择文件 选择文件	
> 素引配置管理		
▶ 系统工具		
日期时间管理		
<ul> <li>数据库备份与恢复</li> </ul>		
<ul> <li>日志备份与恢复</li> </ul>		
<ul> <li>系统恢复</li> </ul>		
▶ 重置平台初始口令		⇒入配置 ⇒出配置
<ul> <li>系统停止和重启</li> </ul>		
▶ 系统会数配置		
抹除自检数据		

### 1.1.14. 下载运维日志

下载系统组件运行日志,下载文件为加密文件,一般用于提供给技术人员定位问题。

# 2 业务系统配置

# 业务系统配置步骤简介

1、日志标准化(必配):

在 LAS 系统上首先设置需要接收、标准化具体设备/系统的安全事件/日志;它是安全事件管理的核心内容,也是系统安全事件/日志的唯一来源。LAS 上完成日志标转化后,能够识别各种设备日志,并进行标准化、模版化呈现、日志归并、日志过滤、关联告警等核心内容呈现,该项配置主要包含以下两项步骤:

- (1) 网络设备、服务器等日志指向 LAS 存储;
- (2) LAS 系统采集器配置,将接收的日志执行标准化。

2、安全策略关联配置(必配):

关联分析功能是系统中的重要功能之一,将标准化后的日志与系统内置安全策略相匹配 比对,如果符合关联策略,将以告警的形式在实时监控模块呈现给用户,用户可以对告警进行 相关的处理。该项配置主要包含以下内容:

(1) 启用系统内置关联策略库;

(2) 根据实际用户需求,手工增加策略(按需配置);

(3) 对安全策略产生的告警进行处理。

# 2.1. 资产管理配置

#### 2.1.1. 简介

1、资产管理便于 LAS 设备对当前设备进行识别及管理:

(1) 通过资产管理在 LAS 系统上登记了资产后,在 日志查询->日志列表中的相关日志 信息,将显示登记 ip 的资产名称;

	(2)	如未进行登记,	获取到的安全日志信息将只显示 ip 地址,	不显示设备名称。
--	-----	---------	-----------------------	----------

导航菜单	日志列表								
> 安全概题									
<ul> <li>安全监控</li> </ul>	设备日本最佳名列表								
▼ 日志查询	田期送帰: 2019-07-25 x 序号 1P地址 0 没备名件 「一旦 0 任日 0 低日 0 低日 0 低日 0 2数	•							
日志列表	1 172.16.0.10 172.16.0.10 0 0 299 1791 12820 14910								
关联事件									
审计事件	Windowsま形(0) 範疇のので、またので、 の語ので、								
流量日志	P Poula() ■ (b)/(#(0))								
导出任务管理	■ 端一載時電池(0) ▲ 入侵快速(0)								
· 报表管理	- 入侵防御販売(0)								
策略管理	■ 1=2mm84(0) ▲ VPN (0)								
<ul> <li>资产管理</li> </ul>	b防病毒(0) 物病毒(0)								
> 日志采集	■ KoOm+(·) ■ Web+即倒(0)								
<ul> <li>系统管理</li> </ul>	■ 健全計(0) ■ 内田転位(1)								
	■ 異它(0)								
	第二 100 - 名/P巻 第二 191 年 1 年 1 年 1 年 1 年 1 年 1 年 1 年 1 年 1	5							
	2017 ANN T READE								

2、资产管理支持批量资产导入导出,同时支持按视图对资产进行分类(资产分组):

导航菜单	资产管理		
> 安全概赏	资产管理 自定义履性 视图管理		
> 安全监控	资产列表		Q
<ul> <li>日志壹询</li> </ul>		◎ 视图查看	
▶ 报表管理	序号 一 资产名称	◆ 资产IP ◆ 系统类型 ◆ 资产类别 ◆ 创建日期	
▶ 策略管理	1 172.16.0.10	172.16.0.10 CentOS 服务器 2019-07-25 02:26:42	📆 🥜 🗰
▼ 资产管理			
资产管理			
网站管理			
拓扑管理 >			
网络管理			
资产发现			
→ 日志采集			
▶ 系统管理			
		000 - XI - U - NOD	
	显示 100 🔻 祭记录	显示1到1共1条记录	« < 1 > »

## 2.1.2. 常规设置

#### 一、单台资产添加

场景:添加1台 windows server2008 服务器, ip 地址为 5.5.5.5。

#### 二、具体配置

WEB 登录 LAS 业务控制台: <u>https://10.250.250.128</u>(软件版根据实际设定的 ip 地址进行 登录) 默认用户名: admin, 密码 admin。

(1) 增加 ip 地址段:

选择 资产管理->网络管理->IP 地址段列表, 点击新增。

							理	网络管	导航菜单
Q							表	IP地址段列	<ul> <li>安全概范</li> </ul>
							<b># 1919</b>	🖕 新増	<ul> <li>安全监控</li> </ul>
⇒ 操作	描述	采集控制器	所周网络	IP地址段	名称			序号	<ul> <li>日志査询</li> </ul>
*			缺當网络	10.250.250.0/24	4	缺曾网络-10.250.250.0/24		1	<ul> <li>报表管理</li> </ul>
*		CC-184b4c42-5c	缺當网络	10.251.251.0/24	4	缺曾网络-10.251.251.0/24		2	> 00100-0410
*		CC-184b4c42-5c	缺當网络	10.252.252.0/24	4	缺省网络-10.252.252.0/24		3	
*		CC-184b4c42-5c	缺當网络	10.253.253.0/24	4	缺省网络-10.253.253.0/24		4	· yt/~ Ete
		CC-184b4c42-5c	缺當网络	10.254.254.0/24	4	缺雪网络-10.254.254.0/24		5	<b>资产管理</b>
*		CC-184b4c42-5c	缺當网络	172.16.0.0/24		缺省网络-172.16.0.0/24		6	FIRE
*		CC-184b4c42-5c	缺省网络	2001::0/64		缺省网络-2001::0/64		7	RIPER
									PROTECT
									黄产夜现
									・日志米集
									<ul> <li>系统管理</li> </ul>
« < 1 > »			到7共7条记录	显示 1			▼ 条记录	显示 100	
< < 1			到 7 共 7 集记录	显示 1			▼ 祭记录	显示 100	<b>,</b> 系统管理

增加 5.5.5.0/24 网段,如下图配置。



注意:绝大多数情况下【所属网络】请务必选择缺省网络,否则将造成其他功能模块解 析异常。

(2) 增加具体资产:

大異 Cloud

点击资产管理->资产管理->新增

导航菜单	说产普理	
> 安全概范	<b>资产管理</b> 前级义是性 视频管理	
<ul> <li>安全监控</li> </ul>	5/ <sup>2</sup> /3	
<ul> <li>日志查询</li> </ul>		
· 报表管理	原号         更产名称         更产1P         系统类型         更产类别         创建日期         ●         风粘结况         資作	
策略管理	1 🔲 172.16.0.10 172.16.0.10 CentOS 服务器 2019-07-25 02:26:42 👧 🦯 😫	
▼ 资产管理		
演产管理		
网站管理		
拓扑管理		
网络管理		
资产发现		
<ul> <li>日志采集</li> </ul>		
• 系统管理		
	■ 量示 100 v \$ki2录 显示1到1共1条记录 ( < 1 )	»
	A'	

如下图进行配置:

● 基本信息				
资产编号		✤ 资产名称	5.5.5.5	
✤ 系统类型	x Windows 2008	✤ IP地址段	5.5.5.5 × ¥	
◈ 资产类别	服务器 X Y	※ 资产ⅠP	× 5.5.5.5	
系统版本		硬件型号		
序列号		用途		
MAC地址				注

意:红\*为必填项

资产名称: 根据实际网络、设备自定义取名

系统类型:选择 windows 2008

て で Cloud

ip 地址段:选择已有的 5.5.5.0;如果是新增的 ip 地址段,可以直接点击后面的+号

资产类别:此处选择服务器

资产 ip: 此处填写需要增加资产的实际 ip

通过"查询",按钮可以快速的查询当前已添加的资产

资产管理	理														
资产管	理	Ê	定义属性	视图管理											
资产列表															Q
资产名	称:					资产IP:	5.5.5.5			系统类型:	请选择			¥.	
资产类	别:	请选择			٣	创建日期:		-		责任人:					
风险情	况:	清选择			Y										
							- 0, Eij	€ 清空							
🖕 新増	<b>*</b> #	脉	長次	🕘 导出 🕶	🔍 视图查看										
序号				资产名称	资产IP	条 系统3	(型) 🔶	资产类别		创建日期		风险情况		操作	
1			5.5.5	5.5	5.5.5.5	Windows 2008	85	终器	2019-04-15	07:32:19		无	/ 🕷		

三、资产批量导入

场景: 批量导入 6.6.6.1->6.6.6.10 这十台设备。

注意:LAS 系统仅支持 CSV 格式的文件导入, 文件大小不能超过 5M。

(1) 增加 6.6.6.0/24ip 地址段:

导航菜单	网络管理					
> 安全概范	IP地址段列表					Q
<ul> <li>安全监控</li> </ul>	🖕 新道 🗱 副除					
<ul> <li>日志查询</li> </ul>	序号 📃	名称 🔺	IP地址段 💠 所属网络	采集控制器	描述	⇒ 操作
<ul> <li>报表管理</li> </ul>	1	缺省网络-10.250.250.0/24	10.250.250.0/24 缺當网络			*
▶ 策略管理	2	缺曾网络-10.251.251.0/24	10.251.251.0/24 缺當网络	CC-184b4c42-5c		*
▼ 资产管理	3	缺個网络-10.252.252.0/24	10.252.252.0/24 缺當网络	CC-184b4c42-5c		*
市产管理	4 🗉	缺省网络-10.253.253.0/24	10.253.253.0/24 缺省网络	CC-184b4c42-5c		*
网站管理	5 🗐	缺省网络-10.254.254.0/24	10.254.254.0/24 缺省网络	CC-184b4c42-5c		*
(石扑管理 →	6	缺省网络-172.16.0.0/24	172.16.0.0/24 缺省网络	CC-184b4c42-5c		*
网络普理	7	缺省网络-2001::0/64	2001::0/64 缺省网络	CC-184b4c42-5c		*
资产发现						
<ul> <li>日志采集</li> </ul>						
> 彩绘感得						
NOTION						
	显示 100 🔻 条记录		显示1到7共7条记录			« < 1 > »



注意:通常情况下【所属网络】请务必选择缺省网络,否则将造成其他功能模块解析异

(2) 建议操作:从 LAS 导出某一台设备的 csv 文件,作为模版;此处以设备 5.5.5.5 为例:

选中主机 5.5.5.5,并选择导出为 csv 文件。

Cloud

常。

导航菜单	忠~若理	
安全概范	(東产結果 而没义是性 织图管理	
<ul> <li>安全监控</li> </ul>	要产列表	Q
▶ 日志查询	수 新常 第3時 원 무사 원 무坦 - 《 經濟委품	
<ul> <li>报表管理</li> </ul>	身号         ●         算のF         第パーP         算板実型         第パーP         創業         創業         創業         目標         日 <th1< th=""> <th1< th=""> <th1< th=""></th1<></th1<></th1<>	ŧ
▶ 策略管理	1 172.16 創 Excel 72.16.0.10 CentOS 服务器 2019-07-25 02:26-42  (3) ノード (1) マード (1) マ	
▼ 资产管理	R Word	
资产管理	(B) CSV	
网站管理		
拓扑管理		
网络管理		
资产发现		
<ul> <li>日志采集</li> </ul>		
▶ 系统管理		
		الشبكة

(3) 打开本地保存的 csv 文件(导出文件名为"资产列表.csv"),参照 5.5.5.5 资产格 式,根据实际情况录入 6.6.6.1->6.6.6.10 这十台设备:

5.5.5.5 资产导出 csv 格式,如下图:

高产编号 资产名称 系统类型 PP站址段 资产P MAC地址 责任人 系统版本 序列号 用油 保密性 完整性 可用性 上架信息 资产类别 硬件型号 Min2008 Windows 2008 5550 5555 系统管理员 新统管理员 3 3 3 服务器

参照格式进行录入,如下图(登记完成后注意删除原有的 5.5.5.5 资产,否则 LAS 系统会因为资产重复报错,无法执行导入)。



(4) 查看导入后的资产:

大異口 e Cloud

导入成功,将会在页面右下角提示导入成功

成功	***	0	1 #	
✔ 10个资产	<sup>2</sup> 成功被	导入		

查看新导入的10台资产

资产管理													
资产管理	自	定义属性	视图管理										
资产列表													Q
资产名称	:				资产IP	6.6.6		系统类型:	请选择			*	
资产类别	请选择			Ŧ	创建日期:		-	责任人:					
风险情况	: 请选择			Ŧ									
						🔍 查询	前 清空						
🝦 新増 🔰	<b>\$</b> #19x	🔊 导入	🕗 导出 🕶	🔍 视图查看									
序号		ğ	8产名称 💧	资产IP	♦ 系统类型	资产类别	U I	创建日期	\$	风险情况	\$	操作	
1		6.6.6.6		6.6.6.1	CentOS	终端	2019-04-15 09:29:51			无	🥒 🗱		
2		6.6.6.7		6.6.6.2	CentOS	终端	2019-04-15 09:32:12				/ 🗱		
3		6.6.6.8		6.6.6.3	CentOS	服务器	2019-04-15 09:32:12				/ 🕷		
4		6.6.6.9		6.6.6.4	CentOS	服务器	2019-04-15 09:32:12				/ 🕷		

#### 四、视图(分组)配置

场景:将增加的10台6.6.6.1->6.6.6.10,以及5.5.5.5增加组别信息。

- 6.6.6.1->6.6.6.10: 父组【test】、子组【6 网段】;
- 5.5.5.5: 父组【test】、子组【5 网段】。
  - (1) 添加父组: test:

选择资产管理->资产管理->视图管理,点击 新增,如下图:





**大異** Cloud

导航架单	<b>资产管理</b>			
> 安全概范	天产管理 自定义发性 视频管理			
<ul> <li>安全监控</li> </ul>	Risbia			
• Bann	🖕 #F# 🗱 1959			
• 报表碰望	麻号 位 税幣名存	Mitaa	自用状态	: <b>N</b> IT
* 箱崎管理		当约无可用记录		
* 资产管理				
東戸管理				
阿站他理		參视图名称 test		
KIY管理 >		显示风绘道 • 否 🔘 是		
阿然管理				
<b>崇产</b> 友提		描述信息		
• 日志采集				
• 系统管理				
		anta data d		

(2) 添加子组 6 网段和 5 网段:

点击 节点管理

资产	會理								
资产	管理	自分	≧义属性	视图管理					
视图列表									
🝦 新増	<b>* #</b>	除							
序号				视图名称	描述信息	启用状态	Å	操作	
1			test			启用	۵ 🖉 🍓		

点击 新增

资产管	理										
视图信息											
	视图名称: 描述信息:	1	test				显示风险值:	否			
节点列表											
🝦 新増	😫 删除										
序号			节点名称	上级节点	安全等级			关联资产		操作	
1		test-1				6.6.6.6	5,6.6.6.7,6.6		🗔 🥖 🗰		
显示 10	▼ 条记录					显示1到1共	1条记录			« < 1	, > »
										j	150

增加6网段和5网段

操作

<del>天算云</del> e Cloud					用尸使用指厚
导助凝单	治产管理				
安全概念	视图信息				
<ul> <li>安全监控</li> </ul>	祝聞名称: test	<b>H</b>	示风险值: 否		
<ul> <li>日志直询</li> </ul>	描述信息:				
> 报表普理	节点列表				
▶ 腕吻恰理					
▼ 资产管理	序号 □ 节点名称	1级节点 新增节点	安全等级 🗙	关联资产	操作
资产管理	P2 100 #123	◆节点名称			
网站管理	32/5 100 + 3802/8				
死扑倍理 >		9 T G M M M M M M M M M M M M M M M M M M			<b>返回</b>
PP:0 言語 第二分冊		上级节点 请选择	v l		
> 日表采集					
▶ 系统管理					
		保存	取消 //		

(3) 将资产划入相应分组:

将 5.5.5.5 划入 5 网段;

test

节点名称

6节点

5节点

上级节点

资产管理 视图名称:

描述信息: 节点列表 🚔 新増 🕌 删除 序号

1 2

在 资产管理-> 资产管理-> 资产管理,选中 5.5.5.5 资产,进行修改,如下:

安全等级

资产管	理											
资产管	锂	自定义属性	视图管理	1								
资产列表												Q
🖕 新増	😫 删除	🔊 导入	🔊 専出 🗸	• 视图查看								
序号		)	资产名称	资产IP	♦ 系统	类型 💧	资产类别		创建日期	风险情况		E
1		5.5.5	.5	5.5.5.5	Windows 2008	服命	5 <b>8</b>	2019-04-15 07:32:19		无	1	

显示风险值:

6.6.6.6,6.6.6.7,6.6....

否

关联资产

#### 在所属视图中选中5网段,并保存

所屬视題	5网段			B 57 和四 回 10 <sup>2</sup> test 10 <sup>3</sup> 570段
	影除	全部删除	*	

同理将10台6网络设备加入【6网段】;

所屬視图 6	网段	^	日 尋 视图 日 编 test	
			· · · · · · · · · · · · · · · · · · ·	

#### (4) 点击 资产管理->资产管理->视图查看,可以查看当前已经建立的分组:

导航菜单	资产管理
安全概范	第 <b>件 特徴</b>   自意义理性 14回答理
<ul> <li>安全监控</li> </ul>	Q
<ul> <li>日志查询</li> </ul>	
▶ 报表管理	序号         更产名称         第一日         第二日         新先更型         第二日         第二日         前面         风险信息         操作
策略管理	1 172.16.0.10 172.16.0.10 CentOS 服务器 2019-07-25 02:26:42 🚺 🧪 🕷
▼ 资产管理	
资产管理	
网站管理	
拓扑管理	
阿須省理	
<ul> <li>) 日志采集</li> </ul>	
> 彩统管理	
	□ 日示 100 ▼ 条记录 日示1到1共1条记录 ( く 1 ) 3

按分组查看

资产管理				
资产列表				Q
日 尋視園	🕨 新増 😫 删除 🚽 导入 🖗 导出 🕶 🖡	列表查看		
网络监控(0)	序号 📄 资产名称 🗍 资产	P 🝦 系统类型 🔶 资产类别 🗧	创建日期	风险情况  操作
■ 6节点(4)	1 5.5.5.5 5.5.5.5	Windows 2008 服务器	2019-04-15 07:32:19	📧 🥖 🗰
5节点(1)				

# 2.1.3. 自定义资产添加

## 一、自定义厂商、产品、系统类型(非 LAS 默认自带)资产添加

场景:

添加一台防火墙:

ip 地址: 10.250.250.12

厂商: A 厂商

产品: A 产品



系统型号: A 系统

## 二、具体配置

(1) 添加厂商:

点击系统管理->内置对象->厂商->新增

导航菜单	内置对象		
<ul> <li>安全概節</li> </ul>	厂商 产品	系统类型	-
<ul> <li>安全监控</li> </ul>	厂商列表		Q
<ul> <li>日志査询</li> </ul>	🚔 新増 😫 激除		
· 报表管理	序号 🗌	名称 ・ 主页 ・ 地址 ・ 描述 ・ 是否内置	♦ 操作
▶ 策略管理	1	Adobe 内国	
资产管理	2	Alcatel(阿尔卡特 內面	
<ul> <li>日志采集</li> </ul>	3	Anachiva(安局华 内西	
▼ 系统管理	4	Apache PIR	
用户管理	5	Apple(甲栗公司) PB	
日志管理	6	Arbor P語	
系统参数	7	Aruba PAB	
内面对象	8	Blue Coat PBE	
升级管理	9	8000(22時(酒) (23日)	
许可证管理	10	CheckPoint Page	
云端配置	11 🔲	Cisco(思科) PAE	
云端升级	12	Citra(思志)	
业务配置	13	CrossBeam HE	
系统配置	14	DPtech()由音科技) 内国	
集群管理	15	EMC	
凝銑巡检	16	ERICSSON(數立第	
	17	Extreme netw PBR	
	显示 100 🔻 条记录	显示1到74共74条记录	< < 1 > »

#### 如下图进行配置:

内置对象	
新增厂商	
✤ 厂商名称	AŪ
厂商电话	
厂商web主页	
厂商地址	
描述	
	保存 戰消

(2) 增加产品:

点击系统管理->内置对象->产品->新增

导航菜单	内置对象					
> 安全概節	厂商	产品	系统类型			
> 安全监控	产品列表					Q
<ul> <li>日志査询</li> </ul>	🖕 新増 💲	制除				
<ul> <li>报表管理</li> </ul>	序号		产品名称	▲ 产品厂商	◆ 产品型号 ◆	是否内置 🕴 操作
▶ 策略管理	1		Alcatel Rout	Alcatel(阿尔卡特		内置
> 资产管理	2		Anachiva NGF	Anachiva(安启华		内西
<ul> <li>日志采集</li> </ul>	3		Apache	Apache		内置
▼ 系统管理	4		Apache Tomca	Apache		内置
用户管理	5		Arbor NTMS	Arbor		内置
日志管理	6		Arcsight	HP(惠晉)		内置
系统参数	7		Aruba AC	Aruba		内面
内面对象	8		Big Iron	Foundry(阿捷)		内置
升级管理	9		BIND	other(其它)		内置
许可证管理	10		Bluecoat上网代理	Blue Coat		内置
云端配置	11		Broker-FTP-S	other(其它)		内置
云端升级	12		CdomainFree	other(其它)		内置
业务配置	13		CentOS	other(其它)		内置
系统配置	14		CheckPoint	CheckPoint		内置
集群營理	15		Cisco ACS	Cisco(思料)		内置
系统巡检	16		Cisco ASA	Cisco(思料)		内面
	17		Cisco Guard	Cisco(思科)		内置
	显示 100 -	条记录		显示 1 到 100 共 182 条记录		« < <u>1</u> 2 > »



如下图进行配置,产品厂商选择刚建立的【A 厂商】:

内置对象				
新增产品				
✤ 产品名称	A产品	※ 产品厂商	Microsoft(微软公司)	× v
产品型号				
描述				
				保存 取消

(3) 增加系统类型:

点击 系统管理->内置对象->系统类型->新增

导航菜单	内置对象						
> 安全概范	厂商	产品	系统类型				-
<ul> <li>安全监控</li> </ul>	系统类型列表						Q
<ul> <li>日志查询</li> </ul>	🚽 新増 😫 🕷	除					
<ul> <li>报表管理</li> </ul>	序号		系统类型 ▲	产品 🕴	厂商 🔷	描述	是否內置 🕴 操作
策略管理	1		AIX 5	IBM AIX	IBM	IBM AIX 5	内置
<ul> <li>资产管理</li> </ul>	2		Alcatel Rout	Alcatel Rout	Alcatel(阿尔卡特	Alcatel Router/	内置
<ul> <li>日志采集</li> </ul>	3		Alcatel S12	Alcatel Rout	Alcatel(阿尔卡特	Alcatel S12	内置
▼ 系统管理	4		Alcatel Spat	Alcatel Rout	Alcatel(阿尔-#特	Alcatel Spatial	内置
用户管理	5		Anachiva NGF	Anachiva NGF	Anachiva(安启华	Anachiva NGFW	内五
日志管理	6		Apache	Apache	Apache	Apache	内置
系统参数	7		Arbor NTMS	Arbor NTMS	Arbor	Arbor NTMS	内置
内置对象	8		Arcsight Exp	Arcsight	HP(惠晉)	Arcsight Expres	内置
升级管理	9		Arcsight Log	Arcsight	HP(惠晉)	Arcsight Logger	内置
许可证管理	10		Arsight ESM	Arcsight	HP(惠晉)	Arcsight ESM	内置
云端配置	11		Aruba AC	Aruba AC	Aruba	Aruba AC	内置
云端升级	12		Big Iron	Foundry Rout	Foundry(网捷)	Big Iron	内置
业务配置	13		BIND	BIND	other(其它)	BIND	内置
凝绕配置	14		Bluecoat	Bluecoat上网代理	Blue Coat	Bluecoat	内置
集群管理	15		CentOS	CentOS	other(其它)	CentOS	内置
系统巡检	16		CheckPoint	CheckPoint	CheckPoint	CheckPoint	内置
	17		Cisco ACS	Cisco ACS	Cisco(思料)	Cisco ACS	内置
	显示 100 - 第	影记录		显示 1	到 100 共 183 条记录		< < 1 2 > »

如下图 进行配置,产品厂商选择刚建立的【A 厂商】,产品选择刚建立的【A 产品】:

内置对象					
新增系统类型					
	※ 厂商	Microsoft(微軟公司) × ×	* 产品	Windows	× v
	✤ 系统类型	A系统			
	描述				
					li
					保存取消

(4) 添加资产,调用新建的【A 系统】:

点击资产管理->资产管理->资产管理->新增

天 Tech	bud		
	导航菜单	· 资产管理	
	<ul> <li>安全概説</li> </ul>	茨方普課   自定义届性	
	> 安全监控		
	<ul> <li>日志查询</li> </ul>	◆新酒 第部除 ④ 导入 ④ 导出 ● ③ 切图差著	
	<ul> <li>报表管理</li> </ul>		风险情况 💧 操作
	▶ 策略管理	1 目 172.16.0.10 172.16.0.10 CentOS 服务器 2019-07-25 02:26:42	📧 🥖 🗰
	▼ 资产管理		
	资产管理		
	网站管理		
	拓扑管理 >		
	CT ( A A A T T T		

显示 100 🔻 条记录	显示1到1共1条记录	« < 1 > »

参照下图配置,系统类型选择刚建立的【A系统】,即可完成自定义资产的调用:

资产管理			
新增资产			
● 基本信息			
资产编号		✤ 资产名称	A资产
✤ 系统类型	× A系统	✤ IP地址段	缺省网络-172.16.0.0/24 × × 🔹
✤ 资产类别	服务番 × ▼	✤ 资产IP	× 172.16.0.11
系统版本		硬件型号	
序列号		用途	
MAC地址			

# 2.2. 日志标准化配置(必配)

#### 2.2.1. 日志接入说明

1、日志标准化

日志采集
 系统管理

在 LAS 系统上首先设置需要接收、标准化具体设备/系统的安全事件/日志;它是安全事件管理的核心内容,也是系统安全事件/日志的唯一来源。LAS 上完成日志标准化后,能够识别各种设备日志,并进行标准化、模版化呈现、日志归并、日志过滤、关联告警等核心内容呈现;该项配置主要包含以下两项步骤:

(1) 网络设备、服务器等日志指向 LAS 存储;

(2) LAS 系统采集器配置,将接收的日志执行标准化。

2、各种采集方式适用的场景不尽相同,在实际设置时应根据具体的被接入设备进行设置:

- (1) Syslog 方式:适用于大多数 Linux/Unix 类系统及多数网络和防火墙类设备;
- (2) SNMP Trap 方式:适用于一般的网络设备;
- (3) WMI 方式:适用于 Windows 系统的事件接入;

(4) 数据库方式:适用于部分数据库自身的审计日志接入以及一些仅能将日志保存在数据库中的软件系统,如 Symantec 网络防毒系统、趋势网络防毒系统等;

(5) 文件方式:适用于无法通过上述方式实时接入系统的或需集中审计(特别是事后审)计)的软件或应用系统所留存的日志信息;

(6) Socket 方式:适用于对日志信息丢失零容忍的场景,但相关被采系统需进行一定程度的改造以发出符合 LAS 要求的日志格式;(由于实施难度大,需要定制开发,不建议使用);

(7)SMB 方式: 用于 web 连接和客户端与服务器之间的信息沟通;

(8)CONSOLE 方式: 主动采集目标设备的原始日志具体采集方式由插件类型决定对应参数请根据系统要求填写;

(9) 日志导入:适用于对日志进行手动导入;

(10)流量镜像接入方式:采用旁路模式接受镜像流量,只需将网线插入对应的网卡接口, 通过网线接受镜像流量。

#### 2.2.2. syslog 方式 (常见): linux 系统及网络设备接入

一、场景:

LAS 系统上需要识别 2 台负载均衡、1 台防火墙、1 台天泰防火墙以及若干 linux 主机日志,进行标准化呈现:

2 台负载均衡地址: 172.16.32.11、 172.16.32.12;

防火墙地址: 210.x.x.x;

1 台天泰 waf 防火墙: 210.x.x.x;

若干台 linux 主机: 主机数量较多, 具体 ip 未统计, 需要一段周期的添加时间。

二、注意事项

网络通信正常:被采集设备与日志服务器之间网络可达,与日志采集器的 UDP: 514 端 口畅通。

日志编码格式正确: Syslog 编码需要文本格式, UTF->8 或者 GBK。

#### 三、各类设备配置:将 syslog 日志指向 LAS 系统。

1、常规网络、安全设备



在 web 界面或者命令行,将 syslog 服务器设置为 LAS 系统(采集器) ip 地址。

各类设备的 Syslog 或者 SNMP Trap 日志外发的配置方式,可以参见 LAS 系统里的"策略管理->知识库->日志配置类",针对不同设备有不同的配置方法,如下图:

导航菜单	知识库				
<ul> <li>安全概范</li> </ul>	日志配置类	日月	5英 安全经验英		· · · · · · · · · · · · · · · · · · ·
・ 安全監控	日志配置类	u			Q
<ul> <li>日志查询</li> </ul>	🚽 新増 🗰 😫	删除			
<ul> <li>报表管理</li> </ul>	序号		标题	创建时间	▼ 是否内置 💠 操作
▼ 策略管理	1		AIX日志配置	2019-07-25 01:05:18	内置
审计策略	2		FREEBSD日志配置	2019-07-25 01:05:18	内置
关联策略	3		LINUX日志配置	2019-07-25 01:05:18	内置
采集策略	4		CATALYST日志配置	2019-07-25 01:05:18	内置
知识库	5		REDBACK SE800日志配置	2019-07-25 01:05:18	内置
<ul> <li>资产管理</li> </ul>	6		JUNIPER ROUTER日志配置	2019-07-25 01:05:18	内置
<ul> <li>日志采集</li> </ul>	7		LINKTRUST SCANNER日志配置	2019-07-25 01:05:18	内置
<ul> <li>系统管理</li> </ul>	8		安奈特交换机日志配置	2019-07-25 01:05:18	内置
	9		CYBERWALL日志配置	2019-07-25 01:05:18	内置
	10		LINKTRUST IDS7.1日志配置	2019-07-25 01:05:18	内置
	11	知识库详情	LINKTRUST IDS7.2日志配置	2019-07-25 01:05:18	内置
	12		TOPSEC IDS日志配置	2019-07-25 01:05:18	内置
	13		SYMANTEC8/9/10日志配置	2019-07-25 01:05:18	内置
	14		SYMANTEC11日志配置	2019-07-25 01:05:18	内置
	15		LTIM日志配置	2019-07-25 01:05:18	内置
	16		WEBSPHERE V6日志配置	2019-07-25 01:05:18	内置
	17		LINKTRUST UTM日志配置	2019-07-25 01:05:18	内置
	显示 100 🔻	祭记录	显示 1 到 56 共 56 条记录		« < 1 > »

注意: 被采集设备的日志配置需要这些设备的系统管理员协助

2、Redhat Linux 系统

(1)登录到 Redhat 系统中,执行命令: "vi /etc/syslog.conf"(或者为 rsyslog.conf);

(2)在文件末添加如下内容: \*.debug @SyslogserverIP 其中 debug 和@符号之间是一个 Tab 键而不是空格, IP 地址填写收集 Syslog 接收服务器的地址(LAS 地址);

(3)保存配置文件:执行命令":wq";

(4)重新启动 syslog 服务:执行命令"service rsyslog restart"。

#### 四、LAS系统配置:日志标准化配置

2 台负载均衡、1 台防火墙、1 台天泰 waf、若干台 linux 主机已经将日志指向 LAS 系统, 需要在 LAS 系统上配置相应的标准化策略。

1、登录系统进入日志采集页面,点击"新增"按钮

24度回     第482048     第4828       24度回     1 FB00K.org/8/HE-VOLog/E - 行目を信意工具、用于WindowEI目事業 & MOLog/WindowEI目事業 & MOLog/WindowEIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	防菜单	日志采集							
22222         1 TERNOLOGIE	安全概题	采集控制器 存储配置							
建築調       ##2014(172.14.0.15/0)(前間間))         建築調       ##2014(172.14.0.15/0)(前間間))         建築調       ●用         中間       ●用         建築調       ●用         1       comm_fondingine         1       comm_fondingine         1       comm_fondingine         1       comm_fondingine         2       172.16.0.10         単株具機製(SYS00)       172.16.0.134         単株       ●用         単木       ●用         単木       ●用         単木       ●用         2       172.16.0.10         単木       ●用         単木       ●用         単木       ●用         単木       ●用         単木       ●用         単木       ●用         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●	安全监控	上下载NXLog客户端:NXLog是一个日志	18改集工具、用于Windows日志采集 🔺 NXLoo客A	- in					
	日志豊尚								
Radik	报表管理	Ideal FOIL BEAGE TALLACE AND	251 0/24 81-95 <sup>-</sup> 00 10	STARS. STAR					
四方相         一日         日日         日         日         日         日 <td>策略管理</td> <td>ABALLIR: De Biplie-10.231.</td> <td>231.0/24, 0/8/9/08-10</td> <td>ETTAS. ETTAS</td> <td></td> <td></td> <td>RCIE</td> <td>里局</td> <td>MIAK</td>	策略管理	ABALLIR: De Biplie-10.231.	231.0/24, 0/8/9/08-10	ETTAS. ETTAS			RCIE	里局	MIAK
2234年         時間         月間         前目的名称         東型         地址         送日秋の         東市           1         0         comm_fowErgine         洗品可量         127.16.0.154         100 * 第         *         <	资产管理	→新達 ▶ 启用 📕 停用							
I         Comm_flow/Engine         通過単         12/16.0154         Engine         ア           2         172.16.0.10         単中未規制(SSLOG)         172.16.0.154         Engine         ● ア           第         1         第         1         第         ●	日志釆集	序号	组件名称	类型	地址	运行状态		探(	ŧ.
2     172.16.0.10     単年二典規約(75L00)     172.16.0.154     Main File       第第 100 ● 銀紀葉     第第 1 動 2 共 2 新紀葉     (1)     (1)     (1)	系统管理	1	comm_flowEngine	流量引擎	172.16.0.154	运行正常	8	<b>- X</b>	
<u>第示 100 </u> ● <i>集G</i> 健		2	172.16.0.10	事件采集器(SYSLOG)	172.16.0.154	运行正常		<b>* *</b>	
				TO THE A THE ALL A AND A AND A					1.4
		<u>≅</u> ≉ <u>100</u> • Sic≉		量亦1割2共2第iGR					

#### 2、配置相关参数

loud

(1) 增加2合负载均衡: 172.16.32.11、172.16.32.12:

导航菜单	白金菜集	
> 安全概意	新聞來集員	
<ul> <li>安全监控</li> </ul>	◆ 名称 Sangforad	
<ul> <li>日志查询</li> </ul>	接入方式 ④ Syslog 0 💿 SNMP Trap 0 🔵 数据库 0 💿 文件 0 💿 SMB 0 💿 WML 0 💿 CONSOLE 0 💿 日志导入 0 💿 SOCKET 0	
<ul> <li>报表管理</li> </ul>		
▶ 策略管理	1P哈爾 × 172.16.32.11 × 172.16.32.12	
> 资产管理	◆ 标单化描略	
▼ 日志采集	日志配置加归车	
• 系统管理	a 🛛 🗸 🕤 The matrix	
	事件过述 · 语思评	
	最否如并 〇 是 ⑧ 否	
	展送	
		保存取消

名称: 自定义; 例如本例自定义取名为 Test\_AD;

类型:选择"事件采集器";

标准化策略:选择系统内置对应的模版,在对话框中输入厂商名称首几位,系统将自动关联。

	安全報答         新增采申請
	• इक्टेइंग्ले क दर्श sangforad
	日本通知     接入方式 ④ Syslog ④   SMMP Trap 0   影響等 ④   文件 0   SMB 0   WM 0   CONSOLE 0   日本導入 0   SOCKET 0
	探索管理
	· 補助體證 即管題 <u>× 172.16.32.11</u> × 172.16.32.12
	庚产检理         ◆ 标单化描略         san
	· 日本報集 日本記書和日本記書和日本記書和日本記書和日本記書和日本記書和日本記書和日本記書和
	· 系统普通 Sangfor FW Sangfor FW
	Sunger PLan Sangfor NGAF
	● 中田は anglor AD
	a Sangtor ALLOIR-00 Based B Sangtor ALLOIR-00
	Sandor Nackaru (T-8)
	Hite And
保存 取消	
90	新作業         an           日志将集         Sandor SS. 1/PN           月支持備         日志見第の供 記述自由日本           単大管理         Sandor SS. 1/PN           正式自由日本         Sandor SS. 1/PN           Sandor SS. 1/PN         Sandor SS. 1/PN           Sandor SS. 1/PN         Sandor SS. 1/PN           Sandor SS. 1/PN         Sandor SS. 1/PN           Sandor SO. 1/PN         Sandor SS. 1/PN           Sandor SO. 1/PN         Sandor SO. 1/PN           Sandor SO. 1/PN         Sandor SO. 1/PN           Sandor AC(ORE)         Sandor SO. 1/PN           Sandor AC(ORE)         Sandor SO. 1/PN           Sandor SO. 1/PN         Sandor SO. 1/PN           Interview         Sandor SO. 1/PN           Sandor AC(ORE)         Sandor SO. 1/PN           Sandor SO. 1/PN         Sandor SO. 1/PN </th

ip 范围:输入两台负载均衡的具体地址;此项可以为空系统将自动识别;建议填写准确 ip 以便系统能够识别。

(2) 添加防火墙标准化策略(参考负载均衡) 210.x.x.x:

导航菜单	日志采集	
> 安全概范	新增采集器	
<ul> <li>安全监控</li> </ul>	◆ 名称	WAF
<ul> <li>日志查询</li> </ul>	接入方式	● Sydog 0   SNMP Tap 0   数据库 0   文体 0   SMB 0   VMI 0   CONSOLE 0   目击导入 0   SOCKET 0
<ul> <li>报表管理</li> </ul>		
育略管理	IP范围	* 172.16.0.111
<ul> <li>资产管理</li> </ul>	✤ 标准化策略	* TITANSEC WAR
▼ 日志釆乗	日志配置知识库	
> 系统管理	过滤自身日志	● ■ ○ 否
	事件过滤	· 通送师 🔶
	是否归并	
	描述	
		914 E.A

(3) 添加天泰 WAF 防火墙:

loud

导航菜单	日志采集	
<ul> <li>安全概范</li> </ul>	新増釆集器	
<ul> <li>安全监控</li> </ul>	◆ 名称	WAF
<ul> <li>日志查询</li> </ul>	接入方式	④ Syslog 0 ⑤ SNMP Trap 0 ⑥ 炭農業 0 ⑥ 文件 0 ⑥ SMB 0 ⑥ Wh1 0 ⑥ CONSOLE 0 ◎ 日志号入 0 ◎ SOCKET 0
<ul> <li>报表管理</li> </ul>		
第二章	IPEE	× 177.16.0.111
<ul> <li>资产管理</li> </ul>	◈ 标准化策略	K TITANSEC WAF
▼ 日志采集	日志配置知识库	
<ul> <li>系统管理</li> </ul>	过滤自身日志	• R O A
	事件过速	第25時 🔶
	是否归并	○ 差 ⊕ 否
	描述	
		9763 IT33

(4) 添加若干台 linux 主机:



注意点:由于主机数量较多,需要一段的添加周期,故此处可以将 ip 范围留空(或者添加地址段),系统支持智能识别;其他配置与上述步骤相同。

导机菜单	日志采集	
安全概范	新增采集器	
> 安全监控		LINUX
<ul> <li>日志查询</li> </ul>	接入方式	③ Sydgo ③ SNMP Tap ④ ② 数据库 Ø ③ 文件 Ø ③ SM8 Ø ④ WML Ø ⑤ CONSOLE Ø ⑤ 目表导入 Ø ⑤ SOCKET Ø
▶ 报表管理		
▶ 策略管理	15/2/20	<u> K 1/2.160.1/24</u>
> 炭产管理	◈ 标准化策略	x Linx
▼ 日志采集	日志配置知识库	Linux日志配置
▶ 系统管理	过烤自身日志	• E 0 F
	事件过滤	- (13)2月 - (13)21 -
	是否归并	
	描述	
		保存 取滅

(5) 查看已配置标准化策略:

日秋草竹	日本司件					
L DARK	шажж					
* 女王锐向	采集控制器	存储配置				
<ul> <li>・ 安全监控</li> </ul>	▲ 下载NXLog客户	≒端:NXLog是一个日志收集工具,用于Windows日志采集 📥 NXLog客	户端			×
<ul> <li>日志查询</li> </ul>	采集控制器(172.10	6.0.154)[許可覺控]				
· 报表管理	Histori 60	3: 熱管回路。10.251.251.0/24. 熱管回路。10	运行状态: 运行下桌			777 (RC) (RH)
▶ 策略管理						
资产管理	🖕 新増 🕨 启用	用 📕 停用				
▼ 日志采集	序号	组件名称	类型	地址	运行状态	操作
<ul> <li>系统管理</li> </ul>	1	comm_flowEngine	流量引擎	172.16.0.154	运行正常	<b>×</b>
	2	172.16.0.10	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🎘
	3	sangforad	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🛠
	4	WAF	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗰 🛠
	显示 100 - 泉	记录	显示1到4共4条记录			« < 1 > »

注意:每种标准化策略只能添加一次,例如上例添加了 Test\_AD 后,再新增事件采集器时,就无法继续选择 Test\_AD,如下图显示。

导航菜单	日志采集				
> 安全概范	新增采集器				
<ul> <li>安全监控</li> </ul>	* 名称	SANFOR			
<ul> <li>日志查询</li> </ul>	接入方式	Syslog 0 SNMP T	rap 0 🔵 数据库 0 🔵 文件 0 🔵 SMB 0 🔵 WME 0 🔵	CONSOLE 0 _ 日志导入 0 _ SOCKET 0	
报表管理					
策略管理	IP范围	请输入			
资产管理	◈ 标准化策略	sang			
▼ 日志采集	日志配置知识库	Sangfor SSL VPN	-	·	
> 系统管理	讨法自身日本	Sangfor FW			
	1716日94日45	Sangfor NGAF			
	事件过滤	Sangfor AC(UTF-8)		+	
	是否归并	Sangfor NGAF(UTF-8)			
		Sangfor DAS			
	加之		· ·	•	
					10
				保存取	ä



如果有新的负载均衡加入,例如 172.16.32.13 加入,需要编辑原有的 sanfor->ad 标准化 策略,在 ip 地址范围添加上,如下图:

	日志采集								
<ul> <li>安全概念</li> </ul>	100 AT	2012070							
<ul> <li>安全监控</li> </ul>		171020020							
→ 日志香湖	▲ 下载NXLog客户端	I:NXLog是一个日志收集工具,用于	FWindows日志采集 📥 NXLog客户键	1					×
1-00三円 ) 返去無道	采集控制器(172.16.0	0.154)[許可豐控]							
> 30.00 m 18	地址段:	缺省网络-10.251.251.0/24, 缺省网	可络-10	运行状态:	运行正常			配置 重启	删除
· 3R41512	🛖 新増 🕨 启用	- 停用							
• 荧产管理	序号		组件名称	类型		地址	运行状态	操	作
* 日志来集	1	com	mm_flowEngine	流量引擎		172.16.0.154	运行正常	<b>×</b>	
▶ 系统管理	2		172.16.0.10	事件采集器(SYSI	.0G)	172.16.0.154	运行正常	🔳 🗰 🛠	
	3		sangforad	事件采集器(SYSI	.0G)	172.16.0.154	运行正常	🔳 🗰 🛠	
	4	0	WAF	事件采集器(SYSI	.0G)	172.16.0.154	运行正常	🔳 🗰 😒	
	显示 100 - 条记者	₹.		显示1到	4 共 4 条记录			(< )	1 > >
导航菜单	日志采集								
与航菜单 • 安全概念	日志采集 修改采集器								
<ul> <li>号結束単</li> <li>・ 安全報告</li> <li>・ 安全部目</li> </ul>	日志采集 修改采集器 ※ 名称:	sangforad							
<ul> <li>等結束単</li> <li>・ 安全電流</li> <li>・ 安全型符</li> <li>・ 日志査術</li> </ul>	日志采集 	sangforad							
日本市場           > 安全販売            > 安全販売            > 日本市場            > 田本市場	日吉采集 	sangforad syslog							
日前次单           ・安全或広           ・安全或広           ・日志直海           ・ 現志皆環           ・ 加速計算	日志采集 	sangforad syslog [x 172.1632.11] (x 172.163	2.12 × 172.16.6.123		1				
9款次单           > 安全概念           > 安全型程           > 日志直询           > 报表答理           > 現表答理	日志平集 (約37年集選 金 名称: 建入万式: 印電道 金 江海小海道	sangforad syslog ( <u>w 172.16.32.11</u> ) <u>w 172.16.33</u>	212 × 172.16.0.123		]				
1         安全概念           > 安全概念         安全航空           > 安全航空         日本市会務           > 探索循環         東岸福祉           > 東岸福祉         東岸福祉	日志平集 参え東集選 全 名称: 扱入方式: P范選 全 伝承に儀略	sangforad syslog [x 172.16.32.11] x 172.16.32 [x sangfor AD]	2.12 × 172.16.6.123		]	_	_		
545.20           · 安全截至           · 安全型位           · 日志告助           · 援助管理           · 援助管理           · 援助管理           · 夏の管理	日志平県 (学校天皇3) 会 名称: 扱入方式: 19で選 会 伝承化振時 日本記録や24。	sangforad ayslog [x 172.16.32.11] x 172.16.3 [x sangfor AD]	2.12 × 172.16.0.123		]				
日本         9           ・ 安全電気         ・           ・ 安全電気         ・           ・ 日本         日本           ・ 日本         日本           ・ 東水管理         ・           ・ 日本         日本           ・ 東水管理         ・           ・         日本           ・         東水管理           ・         日本	日本半集 (2)2) (2)2) (2)2) (2)2)2 (	sangforad syslog [x 172.16.32.11] (x 172.16.32 [x sangfor AD] • B II	2.12 × 172.16.0.123		]				
1045.00 単           ・ 安全転益           ・ 安全型型           ・ 日本直接           ・ 日本直接           ・ 「「「「」」」」           ・ 「「」」」           ・ 「「」」」           ・ 「」」」           ・ 「」」」           ・ 「」」」           ・ 「」           ・ 「」           ・ 「」           ・ 「」           ・ 「」           ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	日本本集 (初次年編集) (初次年編集) (日本)(日本) (日本)(日本)(日本) (日本)(日本)(日本) (日本)(日本)(日本)(日本) (日本)(日本)(日本)(日本)(日本) (日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)	angforad ayslog (x 172.1632.11) x 172.163 (x sangfor AD) (* Sangfor AD)	2.12 × 172.16.0.123		]		_	_	
日本         9	日本平単           使な栄養器           金 名称:           扱入方式:           少 石器           今 気邪:           日本記録の月本           送岸自由日本           要将过速	sangforad syslog (x 172.16.32.11) (x 172.16.32 (x sangfor AD) ④ 意 ③ 蔚 康志祥	2.12 x 172.16.6.123		]	_			
時期20           ・安全戦災           ・安全戦災           ・日本血物           ・現業管理           ・実業管理           ・実業管理           ・実業管理           ・実業管理           ・実施管理		sangforad pyslog [x 172.16.32.11] (x 172.16.32 [x sangfor AD]	2.12 × 172.16.0.123		]				
日本市内           9         安全或広           9         安全或広           9         日本市内           9         東大管理           9         東大管理           9         日本管理           9         東大管理           9         東大管理	日本半集 (223年編集)	sangforad oyslog (x 172.16.32.11) x 172.16.33 (x sangfor AD) ⊕ & ⊙ IT (#32.05 () & © IT	212 x 172.16.0.123		]				
9款设单           · 安全氣気           · 安全気災           · 日る直询           · 展表接接           · 累殊整理           · 国時整理           · 国家整理           · 日志采集           · 風病管理	日本年期	angforad syslog (x 172.16.32.11) x 172.16.3 (x sangfor AD) (* Sangfor AD) (* Sangfor AD) (* Sangfor AD)	2.12 x 172.16.0.123		]				
日本         日本	<ul> <li>業本は日</li> <li>第二日</li> <li>第二日<th>sangforad syslog [x: 172.16.32.11] (x: 172.16.32 [x: sangfor AD]</th><th>2.12 x 172.16.0.123</th><th></th><th>]</th><th></th><th></th><th></th><th></th></li></ul>	sangforad syslog [x: 172.16.32.11] (x: 172.16.32 [x: sangfor AD]	2.12 x 172.16.0.123		]				
時期200           ・安全戦災           ・安全戦災           ・日本当時           ・現業管理           ・実業管理           ・実業管理           ・実業管理           ・実業管理           ・実際管理           ・実際管理           ・気が管理	日本半集 使之学集器 金 名称: 現入方式: 17回盟 今 印度人類時 日本記録の内本 近球の曲日本 条件过途 高可祥 展派の井 展送	sangforad 9x80g [x 172.16.32.13] (x 172.16.32 [x sangfor AD] ④ 星 ④ 前 - 章 ● 前	2.12 × 172.16.0.123		]				
1         安全概念           > 安全概念         安全型空           > 日志走時         (日本市内市内市内市内市内市内市内市内市内市内市内市内市内市内市内市内市内市内市内	日志米県 (2000年1000年 (2000年10月1日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月11日) (1000年10月1111111111111111111111111111111	sangforad syslog (x 372.16.32.11) x 172.16.33 (x sangfor AD) (0 ∰ (0 ) ∰ (0 ∰ (0 ) ∰ (0 ∰ (0 ) ∰ (0 ) ∰ (0 ) ∰	2.12 x 172.16.0.123		]			86	Rin

#### 五、标准化日志查看

点击"日志查询"->"日志列表"界面,可以显示已添加设备的日志收集情况(按严重、高级、中级、低级、信息)显示:

日志列表									
概览 查询									
设备日志量排名列表									
日期选择: 2019-04-15 💥	<b>②重建</b> 素引								
	序号	IP地址	设备名称	严重	a 🔒 🛞 🔶		低级 🔶	信息 🔶	总数 🔻
日 📻 设备类型 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	1	172.16.0.10	172.16.0.10	0	0	5759	34550	247571	287880
Windows主机(0)	2	172.16.0.147	172.16.0.147	0	3	0	3	16800	16806
try>(用(1))     the(二系約管理(0))     人侵犯服系统(0)     人侵犯服系统(0)     日相編系(0)     日相編系(0)     ひ形(0)     防病兩(0)     致短葉(0)     Web中印刷(0)     星盘和(0)     星盘和(0)     星盘和(0)     星盘和(0)     星盘和(0)     星星和(0)     星星和(0)									
注意:									

<del>天翼云</del> e Cloud

日志按照原始设备日志等级,以严重、高级、中级、低级、信息级别显示;如果原始设备部携带日志等级信息,系统将按照默认的显示等级显示;

设备名称:设备在"资产管理"->"资产管理"中完成相应资产设置的,在此处将显示具体信息,如上图中的172.16.0.10;如果没有则留白不显示;

左键点击具体设备,可以显示设备当日具体日志信息,点击某一条日志,将显示具体的 日志信息。

🐑 导出 🔻	②配置引	列表默认字段 🛛 📗 离线分析	「「标准化优化建议						
序号		名称	类型	子类	严重级别 🔻	设备IP	时间	⊕ IRIP ⊕	目的IP 🔶
1		SU会话开启	访问控制	用户切换	中級	172.16.0.10	2019-04-15 03:13:47		172.16.0.10
2		SU会话开启	访问控制	用户切换	中級	172.16.0.10	2019-04-15 03:13:49		172.16.0.10
3		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:13:57		172.16.0.10
4		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:13:59		172.16.0.10
5		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:14:07		172.16.0.10
6		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:14:09		172.16.0.10
7		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:14:16		172.16.0.10
8		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:14:18		172.16.0.10
9		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:14:26		172.16.0.10
10		SU会话开启	访问控制	用户切换	中级	172.16.0.10	2019-04-15 03:14:28		172.16.0.10



#### 2.2.3. WMI 方式 (常见): windows 系统接入

#### 一、场景:

LAS 系统上需要识别1台 windows 10 主机的日志,进行标准化呈现:

• win10 主机的 ip 地址: 192.168.1.174

#### 二、注意事项

- 网络通信正常:被采集设备与日志服务器之间网络可达,用于WMI访问的135端口畅通 (例如没有被硬件防火墙阻断135端口);
- 被采集服务器自带防火墙允许 WMI 应用通过 windows 防火墙进行通信,如下图。

午应用进行通信有哪些风险?	の更	这设置	(N)
允许的应用和功能(A):			_
名称	专用	公用	-
□Wi-Fi Direct 网络发掘	Π.		_
Windows Management Instrumentation (WMI)		$\mathbf{\nabla}$	
□ Windows Media Player			~
□ Windows Media Player 网络共享服务			
□ Windows Media Player 网络共享服务(Internet)			1
□ Windows 对等协作基础			
□ Windows 防火墙远程管理			
☑ Windows 聚焦		$\blacksquare$	
☑ Windows 默认锁屏界面		$\checkmark$	
□ Windows 协作计算机名注册服务			
D Windows 远程管理			

使用 WMI 方式进行日志收集。WMI 为针对 Windows 系列设备的专用接入方式,适用于 Windows2003、2008、2012 系统。注意事项如下:

1、确认设备的 WMI 服务处于运行状态;

2、LAS 上需要录入具有 WMI 权限的账号进行日志采集:

(1) 可以使用 administrator 账号进行采集,administrator 带有 WMI 权限,仅需要开启 WMI 服务即可(参考下文【三、windows 配置 WMI,允许 LAS 采集日志】第1步);

(2) 如果用户由于涉密无法提供 administrator 账号,可以通过<mark>创建具有 WMI 权限的账</mark> 号进行日志采集。

3、本文以创建具有 WMI 权限的 wmitest 账号为例,采集 windows 主机审核日志。

三、windows 配置 WMI, 允许 LAS 采集日志

1、确保设备的 WMI 服务处于运行状态

(1)在运行对话框输入 services.msc:

E	Windows 将根据你所 文件夹、文档或 Inter	输入的名称,为你打 net 资源。	J开相应的程序、
打开(0):	services.msc		B
	使用管理权限创建	書此任务。	

(2).确保 WMI 服务处于"正在运行"的状态,如未处于"正常运行",右键点击该服务,选择"

启动":

0 服务	-					
WMI Performance Adapter	名称	A	描述	状态	启动类型	登录为
	Q. Windows	Event Collector	此服		手动	网络服务
停止此服务	A Windows	Event Log	此服	正在	自助	本地服务
重言动此服务	Windows	Firewal	Win	正在	自动	本地服务
	(a) Windows	Font Cache Ser	通过	正在	手动	本地服务
描述	Windows	Image Acquisiti	为妇		手助	本地服务
向网络上的客户读提供 Windows Management Instrumentation (WMI) 提供程序中的性能库信息。只 本在教室7分组织研究和主社 才会行	Windows	Installer	添加		手动	本地系统
	Windows	Management I	揭供	正在	自动	本地系统
	Windows	Media Player N_	便甩		手动	网络服务
行此服务。	() Windows	Modules Install	启用		手助	本地系统
	() Windows	Presentation Fo_	通过	正在	手动	本地服务
	C: Windows	Push Notificati	此.碳		手切	本地系统
	& Windows	Remote Manag_	Win		手助	网络服务
	() Windows	Search	为文		慧用	本地系统
	A Windows	Store Service (	为 W		手动(触发	本地系统
	🔍 Windows	Time	律护		禁用	本地服务
	Q. Windows	Update	倉用		手动(触发	本地系统
	🔄 Windows	移动热点服务	揭供		手动(触发	本地服务
	WinHTTP	Web Proxy Aut	Win		手动	本地服务
	Wired Aut	oConfig	有线		手动	本地系统
	THE AN AN	loConfig	MILA	正在	8.0	****
	認 WMI Perf	ormance Adapt	间祸	正在	田政	相信系统
	Work Fold	ters	此版	1	手动	本地服务
	C. Workstati	on	停田	正在	自助	网络服装

(3).如果用户可以提供 adminstrator 账号,则直接就可以在 LAS 系统上进行日志标准化配置操作;

(4).如果用户由于涉密无法提供 administrator 账号,下文以创建具有 WMI 权限的 wmitest 账号为例。

2、创建账号 wmitest 账号, 并赋予 wmi 权限

(1) 在运行对话框中输入 lusrmgr.msc,创建账号 wmitest;
٦	Windows 将根据你所输入 文件夹、文档或 Internet }	的名称,为你打 资源。	开相应的程序、
打开(O):	lusrmgr.msc		~
	使用管理权限创建此伯	务。	
	确定	取消	浏览(B)

(2).在弹出的窗口中,右键点击"用户",选择新用户;

🜆 lusrmgr - [	本地用户和组(本地	售)\用月	≏]	
文件(F) 操作	(A) 查看(V) 朝	計助(H)		
🗇 🏟 🖄 🖥	1 🗟 🗗	•		
🍠 本地用户和約	目(本地)	2	称	全名
周月	新用户(N)	11	Administrat	
	查看(V)	>	Guest	
	刷新(F)			
	导出列表(L)			
	帮助(H)			

(3).设置账号 wmitest,设定密码,同时勾选用户不能修改密码、密码永不过期两个选

项;

loud

用户名(U):	wmitest	
全名(F):		
描述(D):		
密码(P):	•••••	
确认密码(C):	•••••	
用户下次登录	时须要改密码(M)	
☑ 用户不能更改	<b>玄码(S)</b>	
2 密码永不过期(	W)	
□帐户已蒸用(B)		

(4).给 wmitest 用户 WMI 授权;



(5).控制面板->管理工具->计算机管理->服务和应用:右键 WMI 控件属性->安全标签安 全设置->为用户添加所有权限;



(6).组件服务->计算机属性->com 安全->启动激活权限;



(7).打开本地安全策略;

略。

控制面板->管理工具->本地安全策略->本地策略->审核策略,根据实际需要开启相关策



(8).最后赋予 wmi 账号"管理审核和安全日志"权限;

用户使用指南

	□ 彩色は空気をつけるいは豊む		Guest		
	一 将工作1560594			電级(A)	執定 取満
	口如此和印教设备报动程序	1650(H)	Administrators		
) 為 系統軍統策略,本地組策略対象	【二、任憲文件和目录】	THEFT (M)	Administrators, Backu		
∧ □ 第位率相端報告書	日間電車総合金日本	( Internet of the second secon	USER-20161009HH/w-		
3 IP 安全策略,在本地计算机	1. Will E 10		Administrators, Users,		
> 🛄 应用程序控制图题	更改系统时间		LOCAL SERVICE, Admi	wmitest	检查名称(C)
> 二 款件语制链路	更於时区		LOCAL SERVICE, Admi		
	以法理系统强制关机		Administrators	输入对象名称未选择(示型)(E):	
> III 电线变量 Windows 初大用	MARRINGECT 第11		Everyone, Administrat		and the second s
	[]从扩编编上取下计算机		Administrators, Users	USER-20161009HH	(0番(1)
1 用户数据分数	①创建水久共享对象			<b>三次(八三(</b> )):	
2 思北诺姆	————————————————————————————————————		Administrators	300 PT 10- 800 10-7	
∧ 📴 本招麗羅	11 台灣一个令牌75章		1112/003102010200002310301031	NU WURKTIM	对象类型(O)
> 📑 第三百姓的	(4)建全局对象		LOCAL SERVICE.NET	田白砂内墨安全主体	STO PLANTON
> 🥶 信任策略	(1) 利達符号碼接		Administrators	选择此X7象地型(S):	
◇ 🔜 朱戸無恵	1. 鲁伯文件和目录		Administrators, Backa	Constraints - Representation	
· 查多份量	策略		本表信器	Fine Country	

用户使用指南

### 四、LAS 系统配置:日志标准化配置

1. 点击日志采集->新增,新增采集器,如下图所示:

导航菜单	日志采集									
> 安全概范	采集控制器	存储配置								
・ 安全监控	▲ 下载NXLog客户	に 戸靖:NXLog是一个日志攻集工具,用于Windows日志采集  ▲ NXLog	客户请			×				
<ul> <li>日志查询</li> </ul>	彩化的制器(172.1)	<b>学电控制网(172160.150)</b> 件可带的								
<ul> <li>报表管理</li> </ul>										
▶ 策略管理	-54172				H					
<ul> <li>资产管理</li> </ul>	●新道 ▶ 启用	3月 🧧 停用								
▼ 日志采集	序号		英型	地址	运行状态	操作				
▶ 系统管理	2	172 15 0 10	高休公告報(SVSLOG)	172.16.0.154	たちての					
	3	sanoforad		172.16.0.154	正在東島					
	4	WAF	事件采集臻(SYSLOG)	172.16.0.154	运行正常					
	显示 100 - 条道		显示1到4共4条记录			< < 1 > »				

2. 按照下图进行设置,设置完毕后点击接入设备列表处的"新增"按钮:

导航菜单	日志采集	
> 安全概范	新燈乐集器	
<ul> <li>安全监控</li> </ul>	◆ 名称 wmi	
<ul> <li>日志查询</li> </ul>	援入方式 🕠 Syslog 0 🔵 SNMP Trap 0 🔵 数据库 0 💿 文件 0 💿 SMB 0 💿 WML 0 💿 CONSOLE 0 💿 日志导入 0 💿 SOCKET 0	
▶ 报表管理		
策略管理	接入设备列表 <ol> <li>建章:设备上限50台,建议控制在30台以内。</li> </ol>	×
资产管理	🚽 新塔 😫 翻除 🥜 推量修改口令	
▼ 日志采集	<b>隊号</b> - 接入设备IP地址 用户名	操作
▶ 系统管理	◆ 标准化策略 x Microsoft Windows	
	日志範遭知识库	
	Trensing ( ) II	
	事件过端 请忠序 🖕	
	星香铅并 () 星 () 香	
	機式	
		13
		保存 取消

名称: 自定义

类型:选择事件采集器

接入方式: WMI

标准化策略:选择 Microsoft Windows(输入首几位字母,系统将自动检索);



输入目标主机的信息,包括 ip 地址、账号(具有 wmi 权限)、密码等,点击"检测"; 如通信正常,主机将提示检测成功,如下图:

导航菜单	日志采集					
> 安全概意	新增采集器					
> 安全监控	会 名称					
<ul> <li>日志査询</li> </ul>	援入方式	🔘 Syslog 🛛 🔘 SNMP Trap 🛈	② 数据库 0 ② 文件	😧 🔿 SMB O 💿 WMI O 🔿 CONSOLE O 🔾 🗄 🗟	≣λ 0 ◯ SOCKET 0	
> 报表管理						
> 策略管理	接入设备列表	建章:设备上限50台,建议控制				
> 资产管理		·····································	2日令			
▼ 日志采集		廖号 □		接入设备IP地址	用户名	操作
> 系统管理	◆ 标准化策略	x Microsoft Windows	设备信息		×	
	日本配書知识案		✤ 接入设备IP地址	172.16.0.193		
			◈ 用户名	administrator		
	过渡日景口志		* 0\$			
	事件过滤			20.00 98.01 00.00	-	
	是否归并	○是 ● 香		松田 4月1、 40月		
	描述					
						194 (F (F )

检测通过后点击确认,完成 windows 主机添加:

导航菜单	日本以供									
> 安全概点	平衡均制器	友將配帶								
<ul> <li>・安全监控</li> </ul>		17 SHILLAR								
▶ 日志査測	本 N载NXLog客户	▲ NEMXLog器户输入NLog器一个日本改良工具,用于Windows日本来展 ▲ NoLog客户端 ×								
> 指表協復	采集控制器(172.10	保控制器(172.16.0.154)(许可爱控)								
> 第86日	地址段	: 缺省网络-10.251.251.0/24, 缺省网络-10	运行状态: 运行正常		R55	王 王宗 制味				
→ ※·	🝦 新増 🗼 启用	月 📕 停用								
▼ 日志受任	序号	日 组件名称	类型	地址	运行状态	操作				
	1	comm_flowEngin	e 流量引擎	172.16.0.154	运行正常	<b>R</b>				
, walkin	2	172.16.0.10	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🛠				
	3	sangforad	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🛠				
	4	WAF	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🛠				
	5	🗆 wmi	專件采集碼(WMI)	172.16.0.154	运行正常	📕 🗰 🎘				
	显示 100 - 祭道	己录	显示 1 到 5 共 5 条词	显示1到5共5条记录						

注意:添加多台 windows 有两种方式

方式 1: 编辑原有的采集器策略进行添加



导航菜单	日志采集	
安全概節	修改采集器	
<ul> <li>安全监控</li> </ul>	※ 名称:	wmi
<ul> <li>日志查询</li> </ul>	擦入方式:	WART
报表管理	200000	
▶ 策略管理	接入设备列表	<ul> <li>         (重) 注重:设备上限50台,建设控制在30台以内。         ×     </li> </ul>
资产管理		◆ 新酒 業部時 // 批量得改口令
▼ 日志采集		序号         總入设备IP地址         用户名         操作
斯统管理		1 🔲 172.16.0.193 administrator
	♦ 标准化策略	x Microsoft Windows(WMJ)
	日志配置知识库	Microsoft Windows(WM)日志配置
	过渡自身日志	
	事件过滤	请选择 🔶
	屋否归并	○ 最 ● 否
	描述	
	1000	
		1812 60.03

#### 方式 2: 新增采集器进行添加

天翼云 e Cloud

> 两种方式的区别在于: 方式1添加较为便利, 方式2多采集器处理性能更高; 建议使用 方式2进行添加; 当每台 windows 主机日志量较小时可以使用方式1。

DMAM	Dente								
· <u>東主</u> 解語 • <u>東</u> 会形式	米集投制器 存储配置								
· <u>火土ml</u> x • 日本本治	▲ 下载NXLog客户端:NXLog是一个	下種NKLog當戶編NKLog當戶小日告收集工具,用于Windows日告末集 ▲NKLog富戶時 ×							
	采集控制器(172.16.0.154)[许可受	該新羅(172.16.0.154)(許可要投)							
10.00 to 10     10.00 to 10	地址段: 缺省网络-10.3	251.251.0/24, 缺省网络-10	运行状态: 运行正常			配置 重启 日	削除		
· 演唱已正 • 签立然语	- 新増 🕨 启用 📕 停用								
▼ 日本受住	序号 📄	组件名称	类型	地址	运行状态	操作			
LINGATURE AND A REAL PROPERTY OF	1	comm_flowEngine	流量引擎	172.16.0.154	运行正常	2			
· MOTISIE	2	172.16.0.10	事件采果器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 😤			
	3	sangforad	事件采果器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 📯			
	4	WAF	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 📯			
	5	wmi	事件采集器(WMI)	172.16.0.154	运行正常	📕 🗱 😤			
	显示 100 - 祭记录		显示 1 到 5 共 5 条记录			« < 1	> >		

### 五、标准化日志查看



点击"日志查询"->"日志列表"界面,可以显示已添加设备的日志收集情况(按严重、高级、中级、低级、信息)显示:

日志列表									
概賞 童洵									
设备日志量排名列表									
日期选择: 2019-04-15 ×	◎重建索引								
	序号	IP地址	♦ 设备名称	严重	\$ <b></b>	🔶 中級	(低级	(信息)	总数 🔻
日 🧰 医胃突空 III Unix/Linux主机(1)	1	172.16.0.10	172.16.0.10	0	0	5877	35258	252655	293790
<ul> <li>➡ Windows主机(1)</li> <li>➡ 网络设备(0)</li> <li>➡ 防火増(0)</li> </ul>	2	172.16.0.147	172.16.0.147	0	3	0	3	17060	17066
	3	172.16.0.193	172.16.0.193	0	0	0	5	64	69
<ul> <li>● 病一載診管理(0)</li> <li>→ 入侵防御系統(0)</li> <li>→ 入侵防御系統(0)</li> <li>⇒ 扫描報(0)</li> <li>⇒ 以下用(0)</li> <li>⇒ 数据集(0)</li> <li>⇒ 数据集(0)</li> <li>⇒ 数据集(0)</li> <li>⇒ 数据集(1)</li> <li>&gt; 其定(2)</li> </ul>									

注意:

日志按照原始设备日志等级,以严重、高级、中级、低级、信息级别显示;如果原始设备部携带日志等级信息,系统将按照默认的显示等级显示。

设备名称:设备在"资产管理"->"资产管理"中完成相应资产设置的,在此处将显示具体信息。如果没有则留白不显示;

点击具体设备,可以显示设备当日具体日志信息,点击某一条日志,将显示具体的日志 信息:

P↓ 目的IP ↓
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
172.16.0.10
-

# 2.2.4. 文件方式

一、场景说明

适用于无法通过 Syslog 等方式实时接入系统的或需集中审计(特别是事后审计)的软件 或应用系统所留存的日志信息。

### 二、注意事项

Cloud

LAS 提供目标主机使用 sftp 登录的方式,实现文件传输。

LAS 系统 SFTP 具体登录方式: (1) ip: LAS 系统地址; (2) 用户名: uplogs; 密码: upload-logs-by-this-user。

目标主机上需要有相应的 SFTP 客户端,可以实现日志上传 LAS 系统的功能。

### 三、配置步骤

1、登录系统进入日志采集页面,点击"新增"按钮

・ 全全信点         「東島拉麻酒」「存油店満菜」」           ・ 安全信点         ▲ 下BINCLogS/ALL/OLLogIIII,用开WindowsBISLIKE ▲ NOLogS/ALL/OLLogIIII,用开WindowsBISLIKE ▲ NOLogS/ALL/OLLogIIIII,用开WindowsBISLIKE ▲ NOLogS/ALL/OLLogIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	• 92483       • #80%8       • 74828         • 92483       • #80%8       • 74828         • 92483       • 84843       • 84843         • 16584       • 84843       • 84843         • 93483       • 84843       • 84843         • 93483       • 84843       • 84843         • 93483       • 84843       • 84843         • 93483       • 8484       • 849443         • 93483       • 8484       • 849443         • 93483       • 8494       • 8494         • 93483       • 8494       • 8494         • 93483       • 949434       • 8494         • 93483       • 949434       • 8494         • 93483       • 949434       • 849434       • 8494         • 949434       • 949434       • 849434       • 949434         • 949434       • 949434       • 849434       • 949434         • 1       • 000000000000000000000000000000000000	导队菜单	日志采集									
• 24280         ▲ TRINU-opEricaLIG_IR_PUVnoveEdatig_LAUxtopEricALIG_IR_PUVnoveEdatig_LAUxtopEricALI		> 安全概范	采集控制器	存储配置								
・ 日点色点面     #単振物識(12.21.60.150(前句習知)       ・ 振動音振     ・ 振音振	• I Stading         • I Stading         • I Stading         • Stading	<ul> <li>安全监控</li> </ul>	→ T¥ENALogS/PE(#2010.0)是一个日志改革工具,用于Windows日志洪幸 ▲ NALooS客户論 × ×									
· 集報提         · 集報         · 集報         · 集         · ξ          · ξ         · ξ	・ 読者留       ************************************	<ul> <li>日志查询</li> </ul>	「年前時間(12)16016回回()									
· 就報程         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · 正         · · 正         · · · · · · · · · · · · · · · · · · ·	• State       • Ref	<ul> <li>报表管理</li> </ul>										
教史管理         学校型         学校型         学校型         学校型         学校型         地址         空行状 2         部時代         変型         地址         空行状 2         空行状 2         第二         日本         第二         日本         第二         日本         第二         日本         第二         日本         第二         第二 <th>• yr #di       • yr #di       * yr #di       <t< th=""><th>▶ 策略管理</th><th>ADALIA: U</th><th></th><th>EDVO: EDV</th><th></th><th>HC</th><th></th><th></th></t<></th>	• yr #di       * yr #di <t< th=""><th>▶ 策略管理</th><th>ADALIA: U</th><th></th><th>EDVO: EDV</th><th></th><th>HC</th><th></th><th></th></t<>	▶ 策略管理	ADALIA: U		EDVO: EDV		HC					
日本平血         月号         田田谷谷         安型         地址         店内は         田田谷           • 新知田         1         0 comm_flowing/one         月風目雪         12.16.0.154         日田谷         第           • 新知田         2         17.21.60.104         第日本県教(VSLOG)         172.16.0.154         日田公         第         ※           3         3         3         3         3         3         10000000         172.16.0.154         日田区         第         ※           4         4         WAF         毎日未単常教研究のの         172.16.0.154         日田区         第         ※           5         9         9         1000000000000000000000000000000000000	• 日志年載     府号     日前日谷中     支型     地址     ビドパル     資所       • 風焼醤     - ののm_0%/mpm     洗品1年     121.00.141     ビロゴム     デ       2     - 172.16.010     季は三葉着(5/15.00)     122.16.0144     ビロゴム     デ       3     - 3     3     3     3     日本町市公     デ       4     WAF     香は三葉着(5/15.00)     172.16.0144     ビロゴム     デ       5     - 9     wmi     香は三葉着(5/15.00)     172.16.0144     ビロゴム     デ       第     - 9     - 9     - 9     - 9     - 9     - 9     - 9       5     - 9     wmi     - 9     - 9     - 9     - 9     - 9       10<     - 泉谷栗     - 10     - 10     - 10     - 10     - 10	资产管理	🖕 新増 🕨 启用	- 停用								
・ 新築措置		▼ 日志采集	序号 0	组件名称	美型	地址	运行状态	操作				
1         171,000,107         1	・     ・     121.00.154     ・     121.00.154     ・     121.00.154     ・     121.00.154     ・     121.00.154     ・     121.00.154     ・     121.00.154     ・     121.00.154     ・     ・     121.00.154     ・	> 系统管理	2	172.16.0.10	加速21字 海(4式会話(SVGLOG)	172.16.0.154	EDER					
	4     日     100 (* 約23)     <		3	sandhrad	事件采用器(513200) 事件采用器(57510G)	172.16.0.154	ETTER .					
	5     Wml<		4	WAF	事件法律器(SYSLOG)	172.16.0.154	运行正常					
	□ 100 + 条2录 显示 1 10 5 共 5 条2录		5	wmi	事件采集器(WMI)	172.16.0.154	运行正常					
					a				-			

2、配置相关参数

导航菜单	日志采集	
安全概念	新培采集器	
<ul> <li>・ 安全监控</li> </ul>	◆ 名称 file	le
<ul> <li>日志查询</li> </ul>	接入方式 🔘	Syslog ①
报表管理	_	
策略管理	♦ 接入设备IP地址 17.	
· 资产管理	◆ 标准化策略 😠	e Linux
▼ 日志采集	日志配置知识库 Lin	nx日志取豊
• 系统管理	过滤自身日志 ④	A () A
	事件过滤 南	
	是否归并 ○	局 ● 否
	描述	
		,
		977 IN 3

### 3、保存配置

点击"保存"按钮。

4、使用 uplogs 用户 sftp 登录到采集服务器的/opt/sftp/uplogs 目录下的 172.16.0.193 目录, 将日志传入此目录。

# 四、功能验证

Cloud

1、检查采集器状态是否正常:

导航菜单	日志采集								
> 安全概節	采集控制器 存储配置	2							
<ul> <li>安全监控</li> </ul>	▲ <b>TRENIL 100</b> 近日第100日年日 月 用于Windows日本平台 ▲ N11005 中等 ×								
<ul> <li>日志查询</li> </ul>	5400484773260180/02/2001								
· 报表管理	7-3672-0588(272.20.0.204)[174]		5570						
> 策略倍理	地址版: 訳智利培-1	0.251.251.0/24, 統當阿路-10			A.	置 重启 删除			
资产管理	🚽 新増 🕨 启用 📕 停用								
▼ 日志采集	序号 📄	组件名称	类型	地址	运行状态	操作			
<ul> <li>系统管理</li> </ul>	1	comm_flowEngine	流量引擎	172.16.0.154	运行正常	<b>×</b>			
	2	172.16.0.10	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🛠			
	3	sangforad	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗱 🛠			
	4 🗉	WAF	事件采集器(SYSLOG)	172.16.0.154	运行正常	📕 🗰 玲			
	5	wmi	事件采集體(WMI)	172.16.0.154	运行正常	📕 🗱 🛠			
	6	file	事件采集譜(FILE)	172.16.0.154	运行正常	📕 🗱 🛠			
	显示 100 🔻 条记录		显示1到6共6条记录			« < 1 > »			

2、检查是否收集到设备日志(日志查询->日志列表):

日志列表										
概览 查询										
设备日志量排名列表	1									
日期选择: 2019-04-15 ×	◎重建索引									
	序号	IP地址		严重	(2)	) 🕴 (Hu	) ÷	(IEB)	信息 🕴	总数 🔻
日	1	172.16.0.10	172.16.0.10	0	0	597	1	35822	256707	298500
Windows主机(1)	2	172.16.0.147	172.16.0.147	0	3	0		3	17288	17294
▶ 阿姆皮爾(0) ▶ 防火壇(0)	3	172.16.0.193	172.16.0.193	0	0	0		43	1322	1365
<ul> <li>→ 人便於憲英統(の)</li> <li>→ 人便於憲英統(の)</li> <li>→ 打振騰(0)</li> <li>→ 打振騰(0)</li> <li>→ 打振儀(0)</li> <li>→ 数据集(0)</li> <li>→ 数据集(0)</li> <li>→ 延振集(0)</li> <li>→ 延振集(0)</li> <li>→ 其它(3)</li> </ul>										

🔊 登田 🔺	②配置列	刘表默认字段 🛛 📗 高线分析	后标准化优化建议						
序号		名称	♦ 类型	♦ 子类 ♦	严重级别 🔺	设备IP	♦ 时间	↓ 源IP	♦ 目的IP ♦
1		Windows 过滤平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.145
2		Windows 过濾平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.147
3		Windows 过滤平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	172.16.0.193	172.16.0.196
4		筛选平台已允许绑定本地端口	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	0.0.0	
5		Windows 过滹平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.141
6		Windows 过滹平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.179
7		Windows 过滹平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.160
8		Windows 过滹平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.176
9		Windows 过滤平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	255.255.255.255	172.16.0.153
10		Windows 过滹平台允许连	配置状态	状态跟踪	信息	172.16.0.193	2019-04-15 11:22:03	2001::193	ff02::1:ff00:1

# 2.2.5. 数据库方式

一、组网要求

1、被采集设备与日志服务器之间网络可达,用于数据库访问的相关端口畅通,比如 MySQL 的 3306, Oracle 的 1521;

2、需要提供被采日志数据库的表(视图)名、数据库登录参数。

二、组网拓扑

loud

无

### 三、配置要点

适用于部分数据库自身的审计日志接入以及一些仅能将日志保存在数据库中的软件系统,如 Symantec 网络防毒系统、趋势网络防毒系统等。

支持 SQLServer、DB2、Oracle、MySQL、Sybase。

#### 四、配置步骤

1、登录系统进入日志采集页面,点击"新增"按钮:

导航菜单	日志采集					
安全概范	采集控制器 存	律配置				
<ul> <li>安全监控</li> </ul>	土 下载NXLog客户请:NXLog	□是一个日志收果工具,用于Windows日志采集 📥 NXLog客户镜				×
<ul> <li>日志查询</li> </ul>	采集控制器(172.16.0.145)	[许可受控]				
▶ 报表管理	地址段: 缺省网	]络-172.16.0.0/24	运行状态: 运行正常			記聞 重良 删除
▶ 策略管理	A see b nm	- -				
▶ 资产管理		学用	M1 (70)	iih tu	1017142/0	19.04
▼ 系统管理	1	comm_flowEngine	流量引擎	172.16.0.145	今部	- 1341 F
用户管理	2	test	事件采集器(SYSLOG)	172.16.0.145	运行正常	
日志管理	3	123124	事件采集器(SYSLOG)	172.16.0.145	运行正常	<b>* *</b>
系统参数	4	windows_agent	事件采集器(SYSLOG)	172.16.0.145	运行正常	<b>= * </b> ×
内置对象	5	syslog采集器	事件采集器(SYSLOG)	172.16.0.145	运行正常	<b>= *</b> ×
升级管理	6	WAF	事件采集器(SYSLOG)	172.16.0.145	运行正常	<b>X</b> X
件可让管理	7	LINUX	事件采集器(SYSLOG)	172.16.0.145	运行正常	📕 🗱 🙊
二級水準	8	SANFOR	事件采集器(SYSLOG)	172.16.0.145	运行正常	📕 🗰 🙊
安装升版	9	wmi	事件采集器(WMI)	172.16.0.145	运行正常	📕 🗰 📯
业类配置的理	10	file	事件采集器(FILE)	172.16.0.145	运行正常	📕 🗱 🙊
集群管理	11	数据库	事件采集器(DATABASE)	172.16.0.145	运行正常	📕 🗱 🙊
系统巡检	12	奥试保存1	事件采集器(SYSLOG)	172.16.0.145	运行正常	📕 🗱 🙊
	13	hs-waf	事件采集器(SYSLOG)	172.16.0.145	运行正常	📕 🗱 📡
	显示 100 • 条记录		显示 1 到 13 共 13 条记录			« < 1 > »

### 2、配置相关参数:

导航菜单	日志采集		
> 安全概范	新增采集器		
<ul> <li>安全监控</li> </ul>	※ 名称	MySQL	
<ul> <li>日志查询</li> </ul>	接入方式	○ Syslog 0 ○ SNMP Trap 0 ④ 数据库 0 ○ 文件 0 ○ SMB 0 ○ WMI 0 ○ CONSOLE 0 ○ 日	志导入 0 💿 SOCKET 0
<ul> <li>报表管理</li> </ul>			
策略管理	✤ 接入设备IP地址	172.16.0.154 余 数据库类型	MySQL *
资产管理	* 账号	smc * 미숙	
▼ 日志采集	◆ 端口	3306 🔶 数据库名称	smc
<ul> <li>系统管理</li> </ul>	★ 表文前相图文	t evt. analysinoPolicy init	policyName
	查询字段	policyName	
	✤ 标准化策略	× MySQL	
	日志配靈知识库	Linux日志配豐	
	过滤自身日志	● 量 ○ 百	
	事件过滤	病法経	
	是否归并	○ 분 ● 점	
	描述		
			测试保存取消



#### 3、保存配置

点击"保存"按钮。

### 五、功能验证

1、检查采集器状态是否正常:

日志采集									
采集控制器 存住	<b>亚</b> 556								
本 T\$\$P\$X1.0g\$P\$#x9X.0g8一个日本改集工具,用于Windows日本采集 本 N0Log客户牌 ×									
采曲约制器(172.16.0.154)(许可管约)									
ADALLAX: UT IPS	en 10.231.231.0/27, exempler 10	21746. 220.00		86	皇 里后 別妹				
●新増 ▶ 启用 ■ 6	<b>亭用</b>								
序号 📃	组件名称	类型	地址	运行状态	操作				
1	comm_riowEngine		172.16.0.154	西行止常					
2	1/2.16.0.10	●仟米東韓(SYSLOG)	172.16.0.154	运行正常					
3	sangrorad	每件采果mb(SYSLOG)	172.16.0.154	医疗正常					
4	WAP	争件采来m(SYSLOG)	172.16.0.154	医疗止累					
5	wmi	●(牛米東橋(WMI)	172.16.0.154	运行止常					
6	tie	●件采集輯(FILE)	172.16.0.154	运行止常					
7	MySQL	●件采集器(DATABASE)	172.16.0.154	运行止常					
显示 100 • 条记录		显示1到7共7条记录			« < 1 > »				
	BERK         PH           #E2048         PH           #E2048 <th>日本年度</th> <th>日本年世           F40058         Practage           F400588         Practage           A TASOCOLOGE/TELESCEDE         ESTRETA: LOSSED: 0.00%           F400586         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F400586         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRET: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0</th> <th>P 年年年           P 株106k         P #82000           ▲ P K810000         P C B 80000         B 60000         B 600000         B 60000         B 60000         B 600000         B 6000000         B 60000000         B 60000000000         B 600000000000         B 6000000000000000000000000000000000000</th> <th>Parage           Parage           Paragee           Paragee           Paragee           Paragee           &lt;</th>	日本年度	日本年世           F40058         Practage           F400588         Practage           A TASOCOLOGE/TELESCEDE         ESTRETA: LOSSED: 0.00%           F400586         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F400586         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRET: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%         ESTRETA: LOSSED: 0.00%           F4005         ESTRETA: LOSSED: 0	P 年年年           P 株106k         P #82000           ▲ P K810000         P C B 80000         B 60000         B 600000         B 60000         B 60000         B 600000         B 6000000         B 60000000         B 60000000000         B 600000000000         B 6000000000000000000000000000000000000	Parage           Paragee           Paragee           Paragee           Paragee           <				

2、检查是否收集到设备日志(日志查询->日志列表):

日志列表									
概览 查询									
设备日志量排名列表									
日期选择: 2019-04-15 ×	◎重建索引								
	序号	IP地址	⇒ 设备名称	严重	\$ <b></b>	\$ <b>1</b> 00	\$ <b>(11.82)</b>	<ul> <li>信息</li> </ul>	🔶 总数 🚽
日 🧰 设备类型	1	172.16.0.10	172.16.0.10	0	0	6090	36533	261797	304420
Windows主机(1)	2	172.16.0.147	172.16.0.147	0	3	0	3	17626	17632
▶ 防火墙(0)	3	172.16.0.193	172.16.0.193	0	0	0	126	4781	4907
<ul> <li>         ・読む管理(0)         ・         ・         ・</li></ul>									

# 2.2.6. 日志归并

### 一、配置要点

归并策略是应用在采集器上的,而且一个采集器只能有一个归并策略。

### 二、配置步骤

1、登录系统进入日志采集,选择一个采集器,点击"修改"按钮。

新増策略									
* 策略	名称 22								
* 过滤									
									9
	- & 4								
* -	动作 🔿 丢弃 🎧	转发syslog 🦳 转发	bsyslog并继续处理	<ul> <li>设置属性</li> </ul>	E并继续处理				
				<u> </u>					
ł	街述	条件设置				×			
		※ 条件名称:	名称		Ŧ				
		※ 运首符・	绘干		<b>*</b>				
		- 24413							
		※ 条件值:	× 攻击						
				(D # 1	HT 244			保存	取消
				1朱仔	取/月	1.			
采集器管理									
* 名称:	10								
接λ <del>方式</del> :	svslog								
107519	. 172 16 0 10								
	x 1/2.10.0.10								
<ul> <li>你在化策略</li> </ul>	× Linux								
日志配宣知识库									
过滤自身日志									
事件过滤	× 11				+				
是否归并	◎ 是 ⑧ 否								
描述									
								Q=	107:25
								沐仔	HOH

2、保存配置

点击"保存"按钮 。

#### 三、功能验证

- 1、检查采集器状态是否正常。
- 2、检查收集到设备日志是否已归并了相关日志。

### 2.2.7. 日志过滤

# 一、配置要点

1、过滤策略是应用在采集器上的,而且一个采集器可以包含多个过滤策略。二、配置步骤

1、登录系统进入策略管理->采集策略->过滤管理页面,点击"新增"按钮:



2、配置相关过滤参数:

大異口 e Cloud

(1).点击"过滤器"右侧条件按钮:

采集策略	
修改策略	
	标注为公编员,转发inskoja通用于转发少量量点关注事件,转发事件量过大会影响采集器性能 ×
※ 策略名称	11
<ul> <li>ジェル</li> </ul>	<ul> <li>◆</li> <li>● 毎件子类 等于 木马(有害限序)</li> </ul>
※ 动作	● 丢弃 ○ 转发syslog ○ 转发syslog并继续处理 ○ 设置尾性并继续处理
描述	
	保存 取消



(2).保存配置:

点击"保存"按钮。

(3).应用策略到采集器:

点击"日志采集",选择一个采集器,修改。

采集器管理		
修改采集器		
※ 名称:	10	
接入方式:	syslog	
IP范围	× 172.16.0.10	]
✤ 标准化策略	x Linux	]
日志配置知识库	Linux日志配置	
过滤自身日志	<ul> <li>● 是 ○ 否</li> </ul>	
事件过滤	× 11	<b>]</b> ♣
是否旧并	○ 是 ④ 否	
描述		
		保存 脱游

#### 三、功能验证

- 1、检查采集器状态是否正常。
- 2、检查收集到设备日志是否已过滤了相关日志。

# 2.2.8. 流量引擎

一、流量引擎介绍

产品安装完成,流量引擎打开,系统可接收流量的镜像。当流量引擎旁路时,系统不再 接收流量镜像。

#### 二、流量引擎的启停

1.打开系统日志采集->流量引擎,查看流量引擎状:

导航菜单	日志采集												
> 安全概范	采集控制器 存储配置												
<ul> <li>安全监控</li> </ul>	▲ 下载NXLog客户端:NXLog是一个日志收集	王具 , 用于Windows日志采集 🔺 NXLog客户録	4			×							
<ul> <li>日志查询</li> </ul>	并承担制稿(172.16.0.154)[许可尝约]												
▶ 报表管理	#####2: ###回终,10.251.251	地址段: 計畫同語-10-251.251.074, 計畫同語-10 油行物志: 西方正式 単名 単数											
> 策略管理		AP 1 PORTING AND			HUE	TENEL BURN							
》 资产管理	●新達 ▶ 屈用 ■ 停用	BHAC		14.41	STATU INF	49.0-							
▼ 日志采集	1	知行內存 comm_flowEngine	· · · · · · · · · · · · · · · · · · ·	地址	运行状态	IRTF							
▶ 系统管理	2	172.16.0.10	事件平集器(SYSLOG)	172.16.0.154	运行正常								
	3	sangforad	事件采集器(SYSLOG)	172.16.0.154	运行正常	<b>X X</b>							
	4	WAF	事件采集器(SYSLOG)	172.16.0.154	运行正常	<b>X X</b>							
	5	wmi	事件采集器(WMI)	172.16.0.154	运行正常	📕 🗱 🛠							
	6	file	事件采集器(FILE)	172.16.0.154	运行正常	<b># %</b>							
	7	MySQL	事件采集器(DATABASE)	172.16.0.154	运行正常	📕 🗱 🛠							
	显示 100 🔻 条记录		显示1到7共7条记录			< < 1 > >							
						Z							

流量引擎的启停:流量引擎默认为开启状态,用户安装产品完成时,流量引擎处于开启状态。用户可根据自身需求是否开启流量引擎,关闭方式如下:

导航菜单	日志采集													
> 安全概意	采集控制器 存储配置	K&20468 744823												
<ul> <li>安全监控</li> </ul>	本下核NXLog客户端:NXLog是	· 个日志收集工具,用于Windows日志采集 ▲ NXLog客户	诗					×						
日志查询	采集控制器(172.16.0.154)[许可	米肥存納高(72166.015/0)作可型20												
报表管理	曲が母・社会団進。1													
▶ 策略管理	Autor 40.007201.41	CERTER TO T 1 NO. TO LOT				BLB	36.70	MARK.						
资产管理	🛶 新増 🕨 启用 📕 停用													
▼ 日志采集	序号 📄	组件名称	类型	地址	运行状态		19	effe						
<ul> <li>系统管理</li> </ul>	1	comm_flowEngine	流量引擎	172.16.0.154	运行正常		2							
	2	172.16.0.10	事件采集器(SYSLOG)	172.16.0.154	运行正常		* 🕅							
	3	sangforad	事件采集器(SYSLOG)	运行正常	📕 🗰 🛠									
	4	WAF	事件采集器(SYSLOG)	172.16.0.154	运行正常		<b>X X</b>							
	5	wmi	事件采集器(WMI)	172.16.0.154	运行正常		* 🕫							
	6	file	審件采集器(FILE)	172.16.0.154	运行正常		* 🕫							
	7	MySQL.	事件采集器(DATABASE)	172.16.0.154	运行正常		* 🔊							
	显示 100 🔻 条记录		显示1到7共7条记录	显示1到7共7条记录										

# 3、流量引擎配置:流量引擎默认为开启;用户可以配置自己想要的协议类型流量。

日志采集												
采集控制器 存	總配班											
下载NXLog客户端:NXLo	20月二一个日志收集工具、用于Windows日志采集 📥 NXLog客户講				×							
采集灯時薪(172.16.0.154)[作可受切]												
ABALAX: UKEP												
新増 🕨 启用 📕	停用											
序号 🗌	组件名称	类型	地址	运行状态	操作							
	comm_nowengine	三元里り 年	172.16.0.154	BOER								
2	172.10.0.10	中午米米爾(515003) 事件が体験(515003)	172.10.0.154	EGER								
	Sangrorau	単十未未未出(313003) 第(4月本長(201002)	172.10.0.154	EDEX								
•	VINE	(中国)(中国)(1003)	172.10.0.154	EDEX								
, ,	WTH Pla	中非未完整(1701)	172.16.0.154	EDEX								
•	110	中1+米米類(FILE) 末(+ごき取(2)までの)	172.16.0.154	医疗正常								
/	MySQL	中午米表面(UATABASE)	172.10.0.154	RUFX								
100 - 98,679		亚小1到/共/梁尼東										
	tana ana ana ana ana ana ana ana ana ana	19:35年 平線20:46 中端記(10:05年) 年48:05:46 年4:05:05年) 10:05年 10:055	ままま ###記(### ##############################	3 2 3 2 3 2 3 3 3 2 3 3 3 2 3 3 2 3 3 3 2 3 3 2 3 3 3 2 3 3 3 2 3 3 3 2 3 3 3 2 3 3 3 3 2 3 3 3 3 2 3 3 3 3 2 3 3 3 3 2 3 3 3 3 2 3 3 3 2 3 3 3 3 2 3 3 3 3 2 3	Prata Dia segura di la segura di							

导航菜单	日志政策
> 安全概范	流動引導配置
> 安全监控	数据率金承期行: ● 开 ○ 失
<ul> <li>日志查询</li> </ul>	ℓ mysql 3306 ℓ erade 1521 ℓ sqlærver 1433
▶ 报表管理	
策略管理	RIVERSE O II O II
》资产管理	
<ul> <li>▼ 日志采集</li> </ul>	V pops 110 V smp V map
<ul> <li>系统管理</li> </ul>	文件傳輸会議報紙: ④ 开 〇 英
	3/2/2019年1月11日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日
	(d) telnet 23
	這程差接合成解析: ● 开 ◎ 关
	(r) ssh
	远程传载会点编标: ● 开 ○ 关
	(d) tis
	选程周用金级附行 ● 开 ○ 关
	(f) deepc
	网站动身金旗帜Fi ④ 开 关
	(v) http

# 2.3. 关联策略配置(选配)

# 2.3.1. 关联策略说明

一、功能简介:

loud

关联分析告警功能是系统中的重要功能之一,对于分析所产生的结果将在关联事件中呈现,如果符合关联策略,将以告警的形式在实时监控模块呈现给用户,用户可以对告警进行相关的处理。完成日志标准化策略后,建议直接启用 LAS 内置的关联告警策略。

LAS 系统主要根据基于规则和基于统计的方式,关联安全事件并产生告警。

1、基于规则:

Cloud

(1)基于规则的关联条件是这样一种状态机制,它包括若干个状态及关联运算符,且每两 个状态之间均有一个关联运算符(即它是一个二元算子),但与一般的关系运算不同的是,它 有两种属性;

时序:后续发生或后续不发生;

关联过滤条件:可选;前后状态之间的关联关系定义。

其形式类似下图:



其中, F,G,(D,N)为一状态, F 表示过滤器, G 表示分组字段(支持多个), 而 D 表示持续时间(以秒为单位,必须设置), 而 N 为重复次数(可不设)。

(2) 规则关联告警举例:waf (web 防火墙)攻击日志关联防火墙访问日志,产生告警:

条件 1: 【状态 1: waf (web 应用防火墙) 60 秒内产生过源主机 a 到目标服务器 b 的一次网络攻击告警日志】;

条件 2: 【状态 2: 防火墙 60 秒内产生 10 条源主机 a 到目标服务器 b 的访问日志】;

条件 3: 【状态 1 发生之后接着发生了状态 2】。

如果同时满足以上三条条件,则产生异常访问告警(一个攻击行为的源对目标进行持续 访问,可能是一种探测行为)



2、基于统计:

(1)基于统计的关联需要有基线数据;基线类型包括日基线和周基线;其中日基线包含 最近若干天,每个时段(以小时为单位)的基于指定聚合字段的统计数据,而周基线包括最 近若干周每周几的基于指定聚合字段的统计数据;

下图周基线为例 (假定学习了最近4周的数据):





从上图可以看出,过去最近四周,周三的平均事件量为 500 条,而刚过去的一日为 1000 条,与基线相比,超出了 100%,如触发条件设定为 100,则触发响应。响应的类型包括如产 生告警、邮件、Syslog 等。

(2) 基于统计的告警举例:

满足条件【1分钟内产生100条 a 主机访问 b 服务器连接拒绝的防火墙日志】,则产生异常访问告警:

	● -&与	•
	<ul> <li>              谷称 匹配 拒绝          </li> <li>             设备类型 等于 防火堆      </li> </ul>	
天动列表:		
<b>派条件</b> :	★応1	•

3、基于流量:

基于流量的关联策略只针对事件子类为流量(连接)的,它包括如下属性:

- (1) 归并字段: 根据不同数据来源, 对原始数据进行分组统计;
- (2) 触发条件: 1->100 之间的整数值, 超过该值时触发告警;
- (3) 统计时间: 5->300 之间的整数值, 单位秒, 统计该时间段内的流量情况;
- (4) 统计字段: 按照不同的维度进行统计, 可选项为发送流量、接收流量、总流量。

新增关联制	<b>食略</b>	
◆ 策略名称	話于沈厳	
+ 1148	<ul> <li>○ 基于成时 ○ 基于优量 ○ 基于优更事件</li> <li>● 本(小子供 等于 洗量(连接)</li> </ul>	•
<ul> <li>KIRCLER</li> </ul>	<ul> <li>●</li> <li>● 源地址 等于 172.16.0.109</li> </ul>	•

4、基于历史事件:

基于历史事件的关联策略统计在一定时间片段内(比如5秒),没发生某种事件却发生了 此日志,产生告警。它包括如下属性:

(1) 事件 1: 必选项, 从某台设备收集到的事件;

(2) 事件1之前 X 秒内不发生: 5->300 之间的整数值, 单位秒;

(3)事件 2: 必选项,事件 1 之前发生的事件,如果在设置的时间范围内,没有收集到该事件,则产生告警。

<ul> <li>过濾器</li> </ul>	●   - & 与   ● 事件子类 够于 洗量(连接)		9
历史事件	事件1           月井字段: 源地址           -         金 与           予測地址         第25,17,9	•	
	事件1之前 15 秒	●新還历史事件 内不炭生	
	事件2           -         & 与           -         2           -         2           -         2           -         2           -         3           -         -           -         3           -         3           -         3           -         3           -         3      <	• •	

#### 5、总结:

用户可以定义各类告警产生的策略(系统内置了部分策略);在策略中可以设定对于安全数据的筛选条件、归并字段、时长和次数以及命中后产生何种响应;响应包括包含发送邮件、发送 Syslog 或 SNMP Trap、执行外部程序或脚本、暂存数据(用户可以将数据保存在临时表中作为其它策略的输入)等。

系统的关联策略不仅支持以预定义规则的方式进行关联,还支持基于模式发现方式的关联;系统不仅支持短时间内的序列关联,还支持长时间的关联(最长可达 30 天)。

# 2.3.2. 具体配置

Cloud

### 一、启用默认告警策略

点击"策略管理"->"关联策略"

导航菜单	美联策略 ⑤ 关联结略语	用于与多谈	(备关联,)	a于时序、状态、统计等复杂攻击	场星的检测,	如:痰得猜测成功,了	「鮮東多清参考: <u>关联策略実施</u>			
安全概	关联策略列表									Q ^
<ul> <li>安全监控</li> </ul>	日 🇁 策略分组	🚔 新増	🗱 2009	🥥 启用 🥌 停用 🔊 長入	1000日 100000000	自命中统计				
<ul> <li>日志查询</li> </ul>	□ 芯厚软件	序号		策略名称	⇒ 状态	更新时间	▼ 策略描述	↓ 是否内置	命中次数	操作
▶ 报表管理	● 信息破坏	1		10	启用	2019-07-25 02:28:14		自定义	48289	• / 🗅 🗱 📲
▼ 策略等理	□设备故障	2		Microsoft-IIS攻击	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 、 IPS …	内置	0	• •
2014 Mills	□ 灾难	3		同源异常登录尝试	启用	2019-07-25 01:05:26	【依赖外部日志源】:所有设备的登录日志	内置	0	• •
単い家和	□ 蒸于统计类	4		数据库表删除	启用	2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	• •
安伊 388		5		数据库表创建	启用	2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	• •
10000		6		Oracle SYS用户远程登	启用	2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	• •
A SELECTOR		7		Unix系统重启	启用	2019-07-25 01:05:26	【依赖外部日志源】: Unix日志 【触发	内置	0	
· 97 BIE		8		Unix系统关闭	启用	2019-07-25 01:05:26	【依赖外部日志源】:Unix日志 【触发	内置	0	i)
· 口心水来		9		管理员登录失败	启用	2019-07-25 01:05:26	【依赖外部日志源】: Unix日志、win	内置	0	
* 系就管理		10		親口令扫描	启用	2019-07-25 01:05:26	【依赖外部日志源】: Unix日志、win	内置	0	• •
		11		密码猜测成功	启用	2019-07-25 01:05:26	【依赖外部日志源】:主机设备、安全设备、	内置	0	D
		12		发现病毒告答	启用	2019-07-25 01:05:26	【依赖外部日志源】:IPS/IDS/防病	内置	0	• •
		13		安全设备登录失败	启用	2019-07-25 01:05:26	【依赖外部日志源】: IPS/IDS/安全	内置	0	• •
		14		登录认证异常	启用	2019-07-25 01:05:26	【依赖外部日志源】:所有设备的登录日志	内置	0	• •
		15		Microsoft-远程服务攻	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	
		16		Microsoft-NETBI	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	• •
		17		UNIX- Mail攻击	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	•
		18		缓冲区溢出攻击	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	• •
								-		
	显示 100 🔻 祭记录				显示	1到100共282条记录			« <	1 2 3 > »

### 勾选绿色状态灯的规则,点击启用。

导航菜单	关联策略 ④ 关联策略运	用于与多说	·荷关联,基	于时序、状态、统计等复杂攻击	场景的检测,	9:蜜科猜测成功,了1	將更多請参考: <u>关联策略实施</u>			
> 安全概范	关联策略列表									Q
<ul> <li>安全监控</li> </ul>	□ = 策略分组	🐈 新増	<b>\$1</b> 1919:	📦 启用  🔮 停用 🛛 😜 尋入	<u>کې اوچک</u>	命中统计				
<ul> <li>日志查询</li> </ul>	□ 志康秋神	序号		策略名称	⇒ 状态>	更新时间 🔻	☆ 策略描述 🔶	是否内置	命中次数	操作
<ul> <li>报表管理</li> </ul>	<ul> <li>信息破坏</li> <li>内容安全</li> </ul>	1		10	启用	2019-07-25 02:28:14		自定义	48289	• / • *
▼ 策略管理	🗋 设备故障	2		Microsoft-IIS攻击	启用	2019-07-25 01:05:26	【依赖外部日志源】: IDS 、 IPS	内置	0	• •
审计策略	□ 灾难	3		同源异常登录尝试	启用	2019-07-25 01:05:26	【依赖外部日志源】:所有设备的登录日志	内置	0	I
关联策略	🗋 基于统计类	4		数据库表删除	启用	2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	• •
采集策略		5		数据库表创建	启用	2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	IN
知识库		6		Oracle SYS用户远程登	启用	2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	• •
资产管理		7		Unix系统重启	启用	2019-07-25 01:05:26	【依赖外部日志源】:Unix日志 【触发	内買	0	•
<ul> <li>日志采集</li> </ul>		8		Unix系统关闭	启用	2019-07-25 01:05:26	【依赖外部日志源】: Unix日志 【触发	内置	0	• •
<ul> <li>系统管理</li> </ul>		9		管理员登录失败	启用	2019-07-25 01:05:26	【依赖外部日志源】: Unix日志、win	内置	0	
		10		弱口令扫描	启用	2019-07-25 01:05:26	【依赖外部日志源】: Unix日志、win	内置	0	• •
		11		密码猜测成功	启用	2019-07-25 01:05:26	【依赖外部日志源】:主机设备、安全设备、	内置	0	• •
		12		发现病毒告答	启用	2019-07-25 01:05:26	【依赖外部日志源】:IPS/IDS/防病…	内置	0	• •
		13		安全设备登录失败	启用	2019-07-25 01:05:26	【依赖外部日志源】: IPS/IDS/安全	内置	0	0
		14		登录认证异常	启用	2019-07-25 01:05:26	【依赖外部日志源】:所有设备的登录日志	内置	0	• •
		15		Microsoft-远程服务攻	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	
		16		Microsoft-NETBI	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	• •
		17		UNIX- Mail攻击	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发祭件】	内置	0	
		18		缓冲区溢出攻击	启用	2019-07-25 01:05:26	【依赖外部日志源】:IDS 【触发条件】	内置	0	

查看策略状态:已启用

四本部門	关联篇明表											(
30.10.0410		AL DOM	-		DBa	B-der						
安全监控		- Br. Silves	<b>A</b> 4394		614m	NU PD-4	-57011					
日志查询	□ 网络攻击	序号		服婚名称	0 8	£8	更新时间		張順描述	是白内置	命中次数	深竹
报表管理	日本の	1	U	PCRat/Ghostati注意: h	H	2	019-03-28 19:35:33			PAR	0	• •
策略管理	2 设备故障	2		Microsoft-IIS攻击	启	用 2	019-07-25 01:05:26	【依較外部日志源】	: IDS , IPS	内置	0	• 0
1011-100 MR		3	0	审明为文本文件但实际发送Win	启	用 2	019-03-28 19:35:33			内置	0	• 6
ATTY SAME	3 基于统计关	4		同源异常登录尝试	启	用 2	019-07-25 01:05:26	【依赖外部日志源】	:所有设备的登录日志	内置	0	
		5	8	可疑的内部Oracle数据库	启	用 2	019-03-28 19:35:33			内置	0	
米東田市		6	0	数据车表删除	启	用 2	19-07-25 01:05:26	[依赖外部日志源]	: 数据库设备审计日志	内置	0	• 6
XUDUE		7		可疑的内部MSSOL数据库1	启	用 2	19-03-28 19:35:33			内西	0	
资产管理		8	-	教室を用いる		i⊞ 2	110-07-75 01-05-76	1次時从朝日本漢1	- 教探療设备室计日本	0000	0	
用志采集		0	-	C MANUFACING THE LAS		-	10 07 20 10 27 27 27	Fuckey ( main dama ]	- RORPE OF REALT PLACE	(111)		
系统管理		9	63	及来的1955以前通常 193	E	111 21	119-03-28 19:35:33				0	• 0
		10		Oracle SYS用户选择登	居	用 2	019-07-25 01:05:26	【依赖外部日志源】	:数据库设备审计日志	内置	0	• •
		11	0	反常的MSSQL数据库 143	启	用 2	019-03-28 19:35:33			内置	0	• 0
		12		MSSQL注入(闭合的字符串后	启	用 2	019-03-28 19:35:33			内置	0	00
		13	0	極似Apache Struct	启	用 2	019-03-28 19:35:33			内置	0	
		14	0	Unix系统重启	启	用 2	019-07-25 01:05:26	[依赖外部日志源]	: Unix日志 【触发	内置	0	
		15		疑似CVE-2014-3704	启	用 2	19-03-28 19:35:33			内置	0	• 15
		16	0	Unix系统关闭	启	用 2	019-07-25 01:05:26	【依赖外部日志源】	: Unix日志 【触发	内置	0	
		17	0	Apache Struts m	启	用 2	19-03-28 19:35:33			内西	0	
		19		會理思결문学院	Ē	用 2	19-07-25 01:05:26	【依赖外部日志源】	: Unix日書, win	内西	0	

#### 二、配置手工策略(按需配置)

手工关联告警举例:waf (web 防火墙)攻击日志关联防火墙访问日志,产生告警。

条件 1:【状态 1: waf (web 应用防火墙) 60 秒内产生过源主机 a 到目标服务器 b 的一次网络攻击告警日志】 2.2.2.2;

条件 2: 【状态 2: 防火墙 60 秒内产生 10 条源主机 a 到目标服务器 b 的访问日志】, 防火墙 ip 地址: 3.3.3.3;

条件 3: 【状态 1 发生之后接着发生了状态 2】。

如果同时满足以上三条条件,则产生异常访问告警(一个攻击行为的源对目标进行持续 访问,可能是一种探测行为)。

1、选择"策略管理->关联策略->网络攻击",点击"新增":

导航菜单	关联策略 ③ 关联策略	适用于与多议	街关联,1	「于时序、状态、统计等复杂攻击	场景的检测	9,如:蜜码猜测成功,了	7解更多请参考:关联策略实施				
<ul> <li>安全概范</li> </ul>	关联策略列表									Q	^
<ul> <li>安全监控</li> </ul>	日 🇁 策略分组	🐈 新増	🗱 細除	🥘 启用 🛑 停用 🛛 🖗 🖶 🗎	日本の	10000000000000000000000000000000000000					
<ul> <li>日志查询</li> </ul>	□ 网络攻击	序号		策略名称	÷ *	(志) 更新时间	∲ 策略描述	↓ 是否内置	命中次数	操作	
<ul> <li>报表管理</li> </ul>	自思破坏	1		PCRat/Gh0st回连遭讯	启	用 2019-03-28 19:35:33		内置	0	• 🗈	
* \$2186.00 TB	2 设备故障	2		Microsoft-IIS攻击	启	用 2019-07-25 01:05:26	【依赖外部日志源】:IDS 、 IPS …	内置	0	• •	
1223-1-2018B	□ 灾难	3		申明为文本文件但实际发送Win	启	用 2019-03-28 19:35:33		内置	0	• 🗅	1
父母父英帝	□ 英市 3	4		同源异常登录尝试	启	用 2019-07-25 01:05:26	【依赖外部日志源】:所有设备的登录日志	内置	0	• 🗈	
平佳菜館		5		可疑的内部Oracle数据库	启	用 2019-03-28 19:35:33		内置	0	• 🗅	
10000		6		可疑的内部MSSQL数据库 1	启	用 2019-03-28 19:35:33		内置	0	• 🗈	
<ul> <li>         ·</li></ul>		7		反常的MSSQL数据库 143	启	用 2019-03-28 19:35:33		内置	0	• •	
) () min		8		Oracle SYS用户远程登	启	用 2019-07-25 01:05:26	【依赖外部日志源】:数据库设备审计日志	内置	0	• •	
		9		反常的MSSQL数据库 143	启	用 2019-03-28 19:35:33		内置	0	• •	
, WALFIE		10		MSSQL注入(闭合的字符串后	启	用 2019-03-28 19:35:33		内置	0	• •	
		11		擬似Apache Struct	启	用 2019-03-28 19:35:33		内置	0	• •	
		12		<b></b>	启	用 2019-03-28 19:35:33		内置	0	• •	
		13		Apache Struts m	启	用 2019-03-28 19:35:33		内置	0	• •	
		14		管理员登录失败	启	用 2019-07-25 01:05:26	【依赖外部日志源】: Unix日志、win	内置	0	• •	
		15		Apache Struts g	启	用 2019-03-28 19:35:33		内置	0	• •	
		16		關口令扫描	启	用 2019-07-25 01:05:26	【依赖外部日志源】: Unix日志、win	内置	0	• 🗈	
		17		Microsoft IIS远程	启	用 2019-03-28 19:35:33		内置	0	•	
		18		密码猜测成功	启	用 2019-07-25 01:05:26	【依赖外部日志源】:主机设备、安全设备、	内置	0	• •	
						_		-			
	显示 100 🔻 条记录				5	显示 1 到 100 共 253 条记录		<.	< 1 2	3 > >	•

2、设定关联策略类型:

Cloud			
	关联策略		
	新增关联策略		
	※ 策略名称	5 关联策略	
		● 基于规则 ○ 基于统计 ○ 基于流量 ○ 基于历史事件	

策略名称:取名任意,此例为 waf 设备日志关联防火墙日志产生告警,取名"WAF 关联防火墙";

数据来源:本例要对 WAF 产生的攻击日志与防火墙产生的连接日志进行关联,这里选择 "事件";

- 事件: 根据来源于目标设备产生的安全日志进行告警策略设置;
- 基于规则:可以基于不同设备间的安全日志进行关联,本需对设备设备关联,此处选择"基 于规则";
- 基于统计:基于事件频率进行关联报警。

3、设置过滤器:

过滤器可以对日志等级、设备名称、时间、源目 ip、端口进行筛选,选取合适的日志信 息进行关联。

本例中对日志信息等级进行筛选,防火墙的连接日志可能属于正常连接,故这里日志级 别选择较低级别的"信息",对于日志信息大于或者等于级别为"信息"的日志,我们就进行关联 分析。

点击运算符&符号,如下图:

※ 过滤器		· · ·	۹ ۱۱ <u>۵</u>
点击增加,	如下图		
- & 5			æ <b>∏</b> ₽

条件设置如下图:对于安全日志信息级别属于"信息"及以上级别的,就进行关联分析。

用户使用指南



4、关联条件设置

そ E Cloud

点击"新增关联状态",如下图:

关联条件	●新聞关联状态

点击&运算符,如下图:

关联条件	♥ 新唱大味	47.¢	
		状态1	<b>811 ×</b> 9
	-	在 60 秒内发生 2 次	
		归并字段:	

点击+号按钮,增加条件:

关联条件	🗢 新増美歌	状态	
	-	状态1	9
	4	在 60 秒内发生 2 次	
		归并字段:	
		- & 与	& III 🖶 🗶
			<b>U</b>

关联 WAF 防护系统的主机 ip 地址: 2.2.2.2:

导航菜单	关联策略	
<ul> <li>安全概范</li> </ul>	新增关联策略	
> 安全监控	◆ 策略名称	
<ul> <li>日志查询</li> </ul>		<ul> <li>基于规则</li> <li>基于统计</li> <li>基于流史事件</li> </ul>
> 报表管理		
▼ 策略管理	☆ 过滤器	
审计兼略		- &=
关联策略		Mittade a
采集策略		◆ 象件: 渡地址 ▼
知识库	21 EV 45.01	<ul> <li>● 正算符: 等于 ▼</li> </ul>
<ul> <li>资产管理</li> </ul>	2000R1+	★ 各性価・ ↓ 2222]
<ul> <li>日志采集</li> </ul>		T AUTO T
▶ 系统管理		
		· 保存 取消 // // // // // // // // // // // // //
		○ 产生音響 ○ 株型外系统 ○ 共行程序
	关联事件名称	
	* ************************************	v v
	10° X 40° 911 + 6000	1927*
	知识库	82.5 * <b>4</b>
		1887:

# 在状态1继续点击新增

Cloud

关联条件	● 新增关系	(状态	
	-	状态1	0
	-	在 60 秒内发生 2 次	
		旧并字段:	0
		<b>一 &amp;</b> 与	& 🖬 🖶 B
		◎ 源地址 大于等于 2.2.2.2	

#### 关联 WAF 防护系统的"网络攻击"事件类型

导航菜单	关联策略						
> 安全概赏	新增关联策略						
<ul> <li>安全蓋控</li> </ul>	※ 策略名称						
<ul> <li>日志查询</li> </ul>		<ul> <li>● 基于规则</li> <li>○ 基于统计</li> <li>○ 基于流量</li> </ul>	◎ 基于历史事件				
> 报表管理							
▼ 策略管理	※ 过逝器						
审计策略		- 25	Ar HLVIUM				×.
关联策略			*****			•	
采集策略			※ 祭件:	事件类型		×	
知识库	21 EV 44 /4	▲ 新道关联状态	※ 运算符:	等于		Ŧ	
<ul> <li>资产管理</li> </ul>	Xuukir		♦ 条件值:	×网络政击			
<ul> <li>日志采集</li> </ul>							
▶ 系统管理							
					保存	取消	
	※ 响应方式	□ 产生告答 □ 转发外系统 □ 执行程序					
	关联事件名称						
	※ 关联事件级别	请选择					
	知识库					*	
		描要:					

# 设置发生频率为 60s 发生 1 次

状态1	
在 60 秒内发生 2 次	
旧并字段:	A DECK
- & 与	
◎ 源地址 等于 2.2.2.2	
-& 5	
◎ 專件类型 孽于 网络攻击	

设置状态1的归并字段为源地址、目标地址(归并字段用于两个字段间进行匹配)

	用户使用指南
e Cloud	
状态1	0
在 60 秒内发生 1 次	
<b>日并字段:####</b> #	1
- & 9	
◎ 源地址 等于 2.2.2.2	
- & 与	
事件关型等于网络攻击	

# 同理,新增状态2,设置防火墙日志属性,如下图

ta	
状态1	
在 60 秒内发生 1 次	
归并字段:	
- & 与	
颜地址等于 2.2.2.2	
- & 与	
◎ 專件类型 等于 网络攻击	
	★ 大 な 4 年60 砂内发生 1 次 日井字段: - & 長 ● 認地址 等于 2.2.2 - & 与 ● 事件炎型 等于 网络攻击

完成的设置结果如下图

关联条件	⇒ 新増关Ⅰ	版状态	
	<b>&gt;</b>	状态1       在 60 秒內没生 1 次       四并字段: 源地址,目的地址       - & 与       ● 源地址 等于 2.2.22       - & 与       ● 事件类型 等于 网络攻击	Q
	<b></b>	状态1 之后 发生 状态2 - & 与	Ŷ
	<b>&gt;</b>	状态2 在 60 秒内没生 10 次 相井字段: 源地址,目的地址 - & 与 ◎ 源地址 等于 3.3.33 ◎ 事件类型 等于 访问控制	٩

设置状态1和状态2之间的关联关系:状态1中的源地址、目的地址等于状态2中的源地 址、目的地址:

点击&符号

状态1	
在 60 秒内发生 1 次	
旧并字段:	
- & 与	
◎ 源地址 等于 2.2.2.2	
- & 与	
◎ 事件类型 等于 网络攻击	
↓ 秋态1之后发生状态2	
状态2	
★ 状态2 在 60 秒0次均年 2 次	
★ 状态2 在 60 秒内没生 2 次 旧社会印 ···	
状态2           在 60 秒内没生 2 次           归井字段:	
状态2       在 60 秒内没生 2 次       归并字段:       一 & 与	
★ 状态2 在 60 珍内发生 2 次 归井字段: - & 与 ◎ 源地址 等于 3.3.3.3	

# 点击+号(如果状态1、2中没有设置归并字段,此处将报错提示无法添加)

	状态1 之后 发生 状态2 - & 与	¢ ⊭ي
-	状态2	<b>9</b>

# 设置状态 1、2 的关联条件: 源、目的 ip 相同

	关联策略			
> 安全概念	新增关联策略			
<ul> <li>安全监控</li> </ul>	♦ 策略名称			
<ul> <li>日志查询</li> </ul>		<ul> <li>● 基于规则</li> <li>○ 基于统计</li> <li>○ 基于流星</li> </ul>	充量 〇 基于历史事件	
报表管理				
* 策略管理	※ 过滤器	•		
审计策略		- & 5	8.Ph09	
关联策略				
采集策略			* 9974 : 1975 g	
利用印度	关联条件	🔹 新增关联状态	★ 运算符: 每于 请输入源IP地址 ▼	
			* 条件值: × 源地址	
· 口心不来 • 彩绘美丽				
DOM IN A				
			(277 B)'H	
	◈ 响应方式	◎ 产生告警 ◎ 转发外系统 ◎ 执行程	元电学 · · · · · · · · · · · · · · · · · · ·	
	关联事件名称			
	※ 关联事件级别	唐洗柽		
	知识库		· •	
		<b>抽要</b> :		
		歸决方案:		

$\bigcirc$	状态1 之后 发生 状态2	<b>e</b>
	- & 5	
	◎ 状态1.源地址 等于 状态2.源地址	

# 再增加目的 ip 相同

**e** Cloud

> 状态1.源地址等于 状态2.源地址	
- 8 =	
状态1 之后 发生 状态2	۵



设置完成的界面如下图

大異口 e Cloud

	<ul> <li>● 20地址 号于 2.2.2</li> <li>● &amp; 与</li> <li>● 那件类型 等于 网络攻击</li> </ul>	
<b>(</b>	状态1 之后 发生 状态2 - & 与 ◎ 状态1.源地址等于 状态2.源地址 ◎ 状态1.目的地址等于 状态2.高的地址	Ŷ
<b>e</b>	<b>状态2</b> 在 60 秒内发生 10 次 归并字段:源地址,目的地址	Ŷ

最后设置响应方式:告警

响应方式:选择告警

级别:选择严重(实际实施中结合用户实际情况)

告警子类等非必选项根据实际项目勾选

*	响应方式	✔ 产生告答	转友外系统	

产生告答								
友情提示:当告	警名称生成方式选择"自动"时,产生告答的事件名称将作为告警名称。	>						
告警名称生成方式	<ul> <li>● 自动 ③ 自定义</li> </ul>							
※ 级别	请选择 マ							
※ 告警大类	- 講送降 ▼							
告警子类	请选择 ▼							
知会资产责任人	Email							
其他邮箱								

设置关联事件名称

关联事件名称	关联防火墙	
✤ 关联事件级别	警告	Ŧ



点击保存,即生成自定义的关联策略(添加的自定义策略,默认为启用状态)

导航菜单	关联策略 ③ 关联策略适	用于与多议	(备关联,)	「「「」」「「「」」」、「「」」、「「」」、「「」」、「」」、「」」、「」」、	占场景的检	浏,如	:密码猜测成功,	了解	更多请参考:关联策略实施			
安全概范	关联策略列表											Q
<ul> <li>安全监控</li> </ul>	日 🇁 策略分組	🝦 新増	🗯 删除	🧼 启用 🛑 停用 🚽 导入	1914	<b>iii</b> #	中统计					
<ul> <li>日志查询</li> </ul>	□ 恐思软件	序号		策略名称	÷ 1	状态	更新时间		策略描述	是否内置	命中次数	操作
<ul> <li>报表管理</li> </ul>	☐ 信息破坏	1		10	JE	3月 2	2019-07-25 02:28:14			自定义	56739	• 🥖 🕥 🗱
▼ 策略管理	1 设备故障	2		Microsoft-IIS攻击	Æ	3月 2	2019-07-25 01:05:26		【依赖外部日志源】: IDS 、 IPS	内置	0	•
审计策略	<ul> <li>一 支進</li> <li>一 算伸</li> </ul>	3		同源异常登录尝试	后	調 2	2019-07-25 01:05:26		【依赖外部日志源】:所有设备的登录日志	内置	0	
关联策略	□ 基于统计类	4		数据库表删除	JE	3月 2	2019-07-25 01:05:26		【依赖外部日志源】:数据库设备审计日志	内置	0	• •
采集箱略		5		数据库表创建	后	調用 2	2019-07-25 01:05:26		【依赖外部日志源】:数据库设备审计日志	内置	0	
知识库		6		Oracle SYS用户远程登	启	3月 2	2019-07-25 01:05:26		【依赖外部日志源】:数据库设备审计日志	内置	0	• •
<ul> <li> ※产管理</li> </ul>		7		Unix系统重启	眉	3月 2	2019-07-25 01:05:26		【依赖外部日志源】: Unix日志 【触发	内置	0	
→ 日志妥佳		8		Unix系统关闭	后	開 2	2019-07-25 01:05:26		【依赖外部日志源】: Unix日志 【触发	内置	0	i)
N STALSANDR		9		管理员登录失败	启	3用 2	2019-07-25 01:05:26		【依赖外部日志源】: Unix日志、win	内置	0	0
. WONELE		10		關口令扫描	<i>j</i> e	3用 2	2019-07-25 01:05:26		【依赖外部日志源】: Unix日志、win	内置	0	• •
		11		密码猜测成功	Æ	調 2	019-07-25 01:05:26		【依赖外部日志源】:主机设备、安全设备、	内置	0	•
		12		发现病毒告警	Æ	3用 2	2019-07-25 01:05:26		【依赖外部日志源】:IPS/IDS/防病	内置	0	0
		13		安全设备登录失败	Æ	周 2	2019-07-25 01:05:26		【依赖外部日志源】: IPS/IDS/安全	内置	0	•
		14		登录认证异常	后	調用 2	2019-07-25 01:05:26		【依赖外部日志源】:所有设备的登录日志	内置	0	•
		15		Microsoft-远程服务攻	唐	3用 2	2019-07-25 01:05:26		【依赖外部日志源】:IDS 【触发条件】	内置	0	• •
		16		Microsoft-NETBI	Æ	3用 2	2019-07-25 01:05:26		【依赖外部日志源】: IDS 【艘发条件】	内置	0	• •
		17		UNIX- Mail攻击	Æ	調用 2	2019-07-25 01:05:26		【依赖外部日志源】:IDS 【触发条件】	内置	0	•
		18		缓冲区溢出攻击	JE	3用 2	2019-07-25 01:05:26		【依赖外部日志源】:IDS 【触发条件】	内置	0	•
						-				-		
	显示 100 🔻 条记录					显示 1	到 100 共 282 条记录	<del>2</del>			« (	1 2 3 >

### 三、告警信息查看

1、告警通知:

如果有新的告警产生,将会在 web 上方的消息处弹出气泡提示:

导航菜单	告罄益拉											
<ul> <li>安全概説</li> </ul>	待处理告望 已	确认告答 已归档告答										
<ul> <li>安全监控</li> </ul>	待处理告答列表 💎 过滤	精管理 💿 监控设置										2
告警监控	❤ 确认 警 油除 👘	7 清选择过海器 - 👂 尋出 - 🌾 标题	· •								•	
实时整控	序号 📃	音響名称	关联策略	<b>\$\$21</b> 💠	対象名称 🕴	对象IP 🝦	系统类型	実別 💠	更新时间 🔻	总次	授作	ŧ
网站监控	1 0	堡垒机绕行登录	這差机幾行登录	-	172.16.0.111	172.16.0.111	CentOS	审计	2019-07-16 11:40:12	292	🖌 🗊	
<ul> <li>日志豊御</li> </ul>	2	图得猜测成功	图码猜测成功	<b>*</b> ±	172.16.0.111	172.16.0.111	CentOS	网络攻击	2019-07-16 11:40:12	146	🖌 🖞	
▶ 报表管理	3	root登录	非工作时间访问		172.16.0.111	172.16.0.111	CentOS	审计	2019-07-16 11:40:12	121	🖌 T	
▶ 策略管理	4 🗉	UNIX服务量Root账号登录	UNIX服务器Root账号登录		172.16.0.111	172.16.0.111	CentOS	审计	2019-07-16 11:40:11	146	¥ 8	
<ul> <li>資产管理</li> </ul>	5 🗐	密码错误	管理员登录失败		172.16.0.111	172.16.0.111	CentOS	市计	2019-07-16 11:40:10	584	48	
<ul> <li>日志采集</li> </ul>	6	同源异常登录尝试	同源异常登录尝试		172.16.0.111	172.16.0.111	CentOS	网络攻击	2019-07-16 11:40:10	584	48	
<ul> <li>系统管理</li> </ul>	7 🗉	密码错误	非工作时间访问	-	172.16.0.111	172.16.0.111	CentOS	审计	2019-07-16 11:40:10	1442	🖌 🗊	
	8	朝口令扫描	<b>第</b> 日今扫描	<b>P±</b>	172.16.0.111	172.16.0.111	CentOS	网络攻击	2019-07-16 11:40:07	293	🖌 🗊	
	9 📄	用户登录	非工作时间访问		172.16.0.111	172.16.0.111	CentOS	审计	2019-07-16 11:39:55	120	¥ 1	
	10	南码错误	登录认证异常		172.16.0.111	172.16.0.111	CentOS	市计	2019-07-16 07:40:49	2	¥ 8	
	显示 100 🔻 祭记景		显示1到:	10 共 10 条记机	R.					« (	1 >	»

点击"消息"将会显示告警信息摘要

Q 全文检索	Ω	系统管理员					
个人工作台							
<b></b>	<b>a</b>	<b>23</b>					
密码错误 创建时间:2019-04-15 11:52:50 告警名称:密码错误 相关资产: 172.16.0.1							
同源异常登 创建时间:2 告警名称:  产:172.16	同源异常登录尝试 创建时间:2019-04-15 11:52:50 告警名称:同源异常登录尝试 相关资 产:172.16						
弱口令扫描 创建时间:2019-04-15 11:52:50 告警名称:弱口令扫描 相关资产: 172.16.0							
密码猜测成 创建时间:2 告警名称:3 172.16.0	密码猜测成功 创建时间:2019-04-15 03:12:59 告警名称:密码猜测成功 相关资产: 172.16.0						

、 **買**し Cloud

# 点击摘要,将会跳转显示具体的告警信息内容

待处理告警			
基本信息			-
🥪 确认 🍵 清除	■ 査看知识率		
	告罄编号: 2	告警名称:	密码错误
	级别: (一般)	对象名称:	172.16.0.10
	对象IP: 172.16.0.10	类别:	审计
	系统类型: CentOS	策略名称:	管理员登录失败
	总次: 228	产生时间:	2019-04-15 11:52:50
	更新时间: 2019-04-15 12:02:12		
	<ul> <li></li></ul>		

2、告警信息查看及处理:



### 所有的告警信息均可以在"安全监控->告警监控"中进行查询

导航菜单	告誓监控			
> 安全概范	待处理告望 已确认告答 已归档告答			
<ul> <li>安全监控</li> </ul>	待处理告答列表 🏹 过速器管理 🐵 监控设置			1
告警查控	🛩 MAA 🗑 油粉 💎 油运探过场第一 🔊 寻出 - 🌾 M	ši •		<u> </u>
实时整控	○ 告留名称	关联策略 💠 级团 🗄 对象名称	◆ 対象IP      ◆ 系统类型 美別     ◆ 更新时间	▼ 总次 操作
网站监控	1	運差机除行登录 <u>一般</u> 172.16.0.111	172:16:0.111 CentOS With 2019-07-16 11:40:12	292 🖌 🕄 🗐
▶ 日志豊尚	2 密码猜测成功	密码猜测成功 (产生) 172.16.0.111	172.16.0.111 CentOS 网络攻击 2019-07-16 11:40:12	146 🖌 🗑 📕
▶ 振表管理	3 root 登录	非工作时间访问 (一篇) 172.16.0.111	172.16.0.111 CentOS 审计 2019-07-16 11:40:12	121 🥩 🗑 📓
▶ 策略管理	4 UNIX服务職Root所号登录	UNDX服务器Root泳号登录 ————————————————————————————————————	172.16.0.111 CentDS 审计 2019-07-16 11:40:11	145 🖌 🗑 📓
<ul> <li> 資产管理</li> </ul>	5 回 密码错误	管理员登录失敗 (一般) 172.16.0.111	172.16.0.111 CentOS 审计 2019-07-16 11:40:10	584 🖌 🗑 📓
▶ 日志采集	6 同源异常登录尝试	同源异常登录尝试 -172.16.0.111	172.16.0.111 CentOS 网络攻击 2019-07-16 11:40:10	584 🖌 🖁 📓
▶ 系统管理	7 富丽错误	#工作时间访问	172-16-0-111 CentOS 审计 2019-07-16 11:40:10	1442 🕜 🖞 📕
	8 0 000000	第四令扫描 (产型) 172.16.0.111	172.16.0.111 CentOS 网络攻击 2019-07-16 11:40:07	293 🗳 🗑 📓
	9 用户登录	非工作时间访问 ————————————————————————————————————	172.16.0.111 CentOS 审计 2019-07-16 11:39:55	120 🖌 🗑 📓
	10 面码错误	登录认证异常 (一般) 172.16.0.111	172.16.0.111 CentOS 审计 2019-07-16 07:40:49	2 🥩 🗑 📓
	显示 100 ▼ 祭记录	显示 1 到 10 共 10 祭记录		« ( 1 )

点击具体条目,可以查看具体告警信息

待处理告警			
基本信息			-
🖋 确认 🍵 清除	> 查看知识库		
	告啓紛号: 2	告警名称:	密码错误
	级别:	对象名称:	172.16.0.10
	对象IP: 172.16.0.10	类别:	审计
	系统类型: CentOS	策略名称:	管理员登录失败
	总次: 276	产生时间:	2019-04-15 11:52:50
	更新时间: 2019-04-15 12:04:12		
	<ul> <li></li></ul>		

对于告警信息有:确认、清除两种动作:

"确认"操作:不在 LAS 上继续对告警信息进行处理,确认后的告警信息将会被移动到"已 确认告警";

"清除"操作:不在 LAS 上继续对告警信息进行处理,清除后的告警信息将会被移动到"已 归档告警";

"查看知识库":可以对告警条目进行解释,并提供建议操作。

# 2.4. 审计策略配置(选配)

### 2.4.1. 审计策略说明

一、功能简介:



审计管理能是系统中的重要功能之一,审计管理侧重于发现日志中相关要素是否和预定的审计策略相符,如时间、IP地址、人员、方式等,对于相符合的结果,系统将在审计事件中呈现给用户,如果符合定制的审计策略,也会在实时监控模块以告警形式展现给用户。

导航菜单	审计事件									
> 安全概范	审计事件列表									Q
<ul> <li>安全监控</li> </ul>	田 = 审计类型(2)	🔊 専出	•							
▼ 日志查询	田 == 車订東略(3) 田 == 审计人员(0)	序号	事件名称	対象IP		事件级别	产生时间	更新时间		总次
日志列表	田 == 审计目标地址(1)	1	SU会活开启	172.16.0.10			2019-07-25 02:26:50	2019-07-25 04:07:12		1192
关联事件	田 📄 审计行为来源(0)	2	用户口令修改	172.16.0.10		警告	2019-07-25 02:26:50	2019-07-25 04:07:10		596
审计事件	田 田 田 市 日 ー ー 日 ー	3	删除用户	172.16.0.10			2019-07-25 02:26:50	2019-07-25 04:07:10		596
流量日志	田 ====================================	4	新建账户	172.16.0.10			2019-07-25 02:26:49	2019-07-25 04:07:10		596
导出任务管理										
▶ 报表管理										
▶ 策略管理										
》 资产管理										
<ul> <li>日志采集</li> </ul>										
<ul> <li>系统管理</li> </ul>										
	显示 100 🔻 条记录				显示	1到4共4 魚记	录		« (	1 > >

审计管理为审计人员、系统管理人员提供了一个统一的审计工具,减少人、财、物的投入,降低了综合审计成本。

审计管理能够方便的自定义审计人员、行为对象、审计类型、审计策略等基本配置;并 能够自定义审计策略模板,审计管理内置了大量审计策略模板,涵盖了常见的、对企业非常 实用的审计策略模板,如主机、防火墙、数据库、萨班斯审计策略模板等。

审计策略模板							
审计策略模板							Q
🗆 💼 审计策略模板组	分析增	●移除	<b>詳</b> 删除				
Windows王利 Linux/Unix主机	序号		策略模板名称	更新时间 🔻	策略描述	◆  是否内置◆	操作
🎍 防火増	1		登录成功审计	2019-04-13 06:22:27	针对计算机用户登录成功记录的审计策略	内置	🗔 + 🗈 🥜
● 扫描器 ▶ IDS/IPS	2		登录失败审计	2019-04-13 06:22:27	针对计算机用户登录失败记录的审计策略	内置	🗔 +E 🥜
▶ 防病毒	3		用户注销审计	2019-04-13 06:22:27	针对计算机中帐号登录注销动作记录的审计策	内置	
● 欧洲半	4		帐户变更审计	2019-04-13 06:22:27	针对计算机中帐户修改记录的审计策略	内置	🗔 +lž 🥖
🍌 等级保护	5		口令变更审计	2019-04-13 06:22:27	审计用户修改帐号囗令的行为。用户利用系统	内置	
	6		帐户权限变更审计	2019-04-13 06:22:27	针对计算机中帐户修改记录的审计策略	内置	🗔 +lž 🥖
	7		策略修改审计	2019-04-13 06:22:27	审计用户修改系统审计策略的行为。用户改变	内置	
	8		系统文件删除审计	2019-04-13 06:22:27	审计用户删除系统文件的行为。	内置	🗔 +lž 🥖
	9		可执行文件安装审计	2019-04-13 06:22:27	审计用户安装可执行文件动作。	内置	
	10		启动进程审计	2019-04-13 06:22:27	对系统应用程序启动的审计。	内置	🗔 +lž 🥜

### 2.4.2. 具体配置

一、启用默认告警策略

点击"策略管理"->"审计策略"

导航菜单	审计策略	© #1	策略是针对审计	國象进行	的分析,多	用于内部违规语	的审计算	服,如:	非工作时间	塑料,了解3	更多请参考:审计策略实施						
> 安全概赏	审计策略列表																Q
<ul> <li>安全监控</li> </ul>	🚔 新増 🚔 🦂	人模板创建策	略 🗰 🍀 删除	● 启用	🛑 停用	三 调整策略执行	行顺序	の行入	記録出会部	审计对象							
<ul> <li>日志查询</li> </ul>	序号				策略名称			状态			处理方式	处理顺序	*	是否内置	÷	操作	
▶ 报表管理	1		登录成功审计					启用	停止	处理其他策略		1		内置	• •	·	
▼ 策略管理	2		登录失败审计					眉用	(学)」	20世界他策略		2		四直	•	~	
审计策略	3		启动进程审计					眉用	停止	20/埋具他策略		3		内置	• •	r	
关联策略	4		SU失败动作审计					眉用	停日	20世具他策略		4		内資	• •		
采集策略	5		拒绝可疑连接行;	与审计				启用	停止	处理其他策略		5		内置	• • •		
知识库	6		su root动作审计					启用	停止	处理其他策略		6		内置	•		
资产管理	7		SU成功动作审计					启用	停止	处理其他策略		7		内置	•		
<ul> <li>日志采集</li> </ul>	8		普通病毒感染告	昏寒汁				启用	停止	处理其他策略		8		内置	•		
▶ 系统管理	9		高风险病毒感染	5警审计				启用	停止	处理其他策略		9		内置	- • • ·	2	
	10		用户注销审计					启用	停止	处理其他策略		10		内置	•	-	
	11		帐户变更审计					启用	停止	:处理其他策略		11		内置	- • • <i>•</i>	P	
	12		口令変更审计					启用	停止	处理其他策略		12		内置		P	
	13		帐户权限变更审计	+				启用	停止	处理其他策略		13		内置	- O 1	P	
	14		策略修改审计					启用	停止	处理其他策略		14		内置	- e i	1	
	15		可执行文件安装	Fit -				启用	停止	处理其他策略		15		内置	- O 2	2	
	16		系统重启审计					启用	停止	处理其他策略		16		内置	- • • ·	1	
	17		网络蛔虫行为审计	t				启用	停止	处理其他策略		17		内置		2	
	18		网络探测威胁行》	り审计				启用	停止	处理其他策略		18		内置		0	
	显示 100 v 1	条记录							显示1到;	30 共 30 条记录	2			1.000	-	e < 1	

勾选绿色状态灯的规则,点击启用。

loud

导航菜单	审计策略 🙂 🛱	计策略是针对审计对象进行的分析,参	用于内部违规操作审计场景,如:非	工作时间登陆,了解更多请参考:审计策略实施	包	
安全概	审计策略列表					۹ 🗠
<ul> <li>安全监控</li> </ul>	新增	第略 業 削除 📦 启用  ● 停用	這 調整策略执行顺序	月出全部 审计对象		
<ul> <li>日志查询</li> </ul>	序号 📃	策略名称	♦ 状态	处理方式	处理顺序 ▲	是否内置
<ul> <li>报表管理</li> </ul>	1 💌	登录成功审计	启用	停止处理具他策略	1	
▼ 策略管理	2	登录失败审计	启用	停止处理其他策略	2	
审计策略	3 🕑	启动进程审计	启用	停止处理其他策略	3	
关联策略	4 🗹	SU失败动作审计	启用	停止处理其他策略	4	内置 🔴 🦯
采集策略	5	拒绝可疑连接行为审计	启用	停止处理其他策略	5	内置 🔴 🥖
知识库	6	su root动作审计	启用	停止处理其他策略	6	内国 🔴 🥖
<ul> <li>资产管理</li> </ul>	7	SU成功动作审计	启用	停止处理其他策略	7	1933 🔴 🥖
<ul> <li>日志采集</li> </ul>	8	普遷病毒感染告替审计	启用	停止处理其他策略	8	内国 😑 🧪
> 乳体管理	9	高风险病毒感染告警审计	启用	停止处理其他策略	9	内国 😑 🧪
MABLE	10	用户注销审计	启用	停止处理其他策略	10	内置 😑 🥖
	11 🔲	帐户变更审计	启用	停止处理其他策略	11	内国 😑 🧪
	12	口令变更审计	启用	停止处理其他策略	12	内置 🔴 🧪 📕
	13	帐户权限变更审计	启用	停止处理其他策略	13	内置 🔴 🥖
	14	策略修改审计	启用	停止处理其他策略	14	内置 🔴 🥖
	15	可执行文件安装审计	启用	停止处理其他策略	15	内置 🔴 🥖
	16	系统重启审计	启用	停止处理其他策略	16	内置 🔴 🥖
	17	网络蠕虫行为审计	启用	停止处理其他策略	17	内置 🔴 🥖
	18	网络探测威胁行为审计	启用	停止处理其他策略	18	内置 🔴 🥖
	显示 100 🔻 条记录		- 00. S	显示 1 到 30 共 30 条记录		« < 1 > »

# 查看策略状态:已启用

导航菜单	审计策略 😁	审计策略是针对审计对象进行的分析,多	用于内部违规操作审计场星,如:非3	【作时问登陆,了解更多请参考: <u>审计策略实施</u>		
> 安全概念	审计策略列表					Q
<ul> <li>安全监控</li> </ul>	🖕 新增 🖕 从模板创建	建築略 🗰 勤除 🛛 📦 启用 🛑 停用	三 调整策略执行顺序 《导入 》	导出全部 审计对象		
<ul> <li>日志查询</li> </ul>	序号 📄	策略名称	<ul> <li>秋志</li> </ul>	处理方式	处理顺序 A 显否内i	豊 ∲ 操作
报表管理	1	登录成功审计	启用	停止处理其他策略	1 内資	•
▼ 策略管理	2	登录失败审计	启用	停止处理其他策略	2 内資	
审计策略	3	启动进程审计	启用	停止处理其他策略	3 内資	
关联策略	4	SU失效动作审计	启用	停止处理其他策略	4 内置	• /
采集策略	5 🗌	拒绝可疑连接行为审计	扇用	停止处理其他策略	5 内置	
知识库	6	su root动作审计	扇用	停止处理其他策略	6 内置	
<ul> <li>资产管理</li> </ul>	7	SU成功动作审计	启用	停止处理其他策略	7 内置	• /
<ul> <li>日志采集</li> </ul>	8	普遷病毒感染告營审计	启用	停止处理其他策略	8 内置	• /
<ul> <li>NIGATE</li> </ul>	9 🗉	高风险病毒感染告替审计	启用	停止处理其他策略	9 内置	
- 207 B 18	10 🗐	用户注销审计	启用	停止处理其他策略	10 内置	• /
	11 🗌	帐户变更审计	启用	停止处理其他策略	11 内置	• /
	12 🗐	口令变更审计	启用	停止处理其他策略	12 内置	• /
	13 🖂	帐户权限变更审计	启用	停止处理其他策略	13 内置	•
	14 🔲	策略修改审计	启用	停止处理其他策略	14 内置	
	15	可执行文件姿貌审计	启用	停止处理其他策略	15 内資	• /
	16 🔲	系统重启审计	启用	停止处理其他策略	16 内資	• /
	17 🗐	网络鳗虫行为审计	启用	停止处理其他策略	17 内面	• /
	18 🖂	网络探测赋肋行为审计	启用	停止处理其他策略	18 内置	• /
			÷			
	显示 100 * 条记录			示 1 到 30 共 30 条记录		< < 1 > »

# 二、配置手工策略(按需配置)

方法一: 从审计策略模板创建

进入审计策略->审计对象->审计策略模板页面

油、菜单	审计策略									
安全概范	审计策略模板 审计	英型 审计,	人员	审计行为对象 审计	+行为执行者对象	审计行为来源对象	审计时间段对象	审计目标对象		
安全监控	审计策略模板									0
日志查询	日 💼 東计策略模板組	<b>₩</b> 新増	₩1639	業務除						
报表管理	Windows主机 Linux/Unix主机	序号		策略模板名积	<b>3</b> 0	更新时间	Ŧ	策略描述	是否内置	操作
策略管理	防火場	1		登录成功审计	2019	-07-25 01:05:26	针对计算机用户登录	成功记录的审计策略	内置	E. 12 /
审计策略	IDS/IPS	2	0	登录失败审计	2019	-07-25 01:05:26	针对计算机用户登录	失败记录的审计策略	内置	18 /
关联策略	→ 防病毒	3	8	用户注销审计	2019	-07-25 01:05:26	针对计算机中帐号型	影注明动作记录的审计策	内置	🗔 +E 🥖
采集策略	▲ 萨班斯	4	0	帐户变更审计	2019	-07-25 01:05:26	针对计算机中帐户修	议记录的审计策略	内置	Co +E 🥖
知识库	🎍 等级保护	5		口令变更审计	2019	-07-25 01:05:26	审计用户修改帐号口	令的行为。用户利用系统	内置	🗔 +E 🥖
资产管理		6	0	帐户权限变更审计	2019	-07-25 01:05:26	针对计算机中帐户例	改记录的审计策略	内置	-12 /
日志采集		7		策略修改审计	2019	-07-25 01:05:26	审计用户修改系统审	计策略的行为。用户改变	内置	-12 /
系统管理		8		系统文件删除审计	2019	-07-25 01:05:26	审计用户删除系统文	样的行为。	内置	-18 🥖
		9		可执行文件安装审计	2019	-07-25 01:05:26	审计用户安装可执行;	文件助作。	内置	🗔 +E 🥖
		10		启动进程审计	2019	-07-25 01:05:26	対系统应用程序启动	的审计。	内置	-12 /
		11		系统重白审计	2019	-07-25 01:05:26	系统关闭、启动、重	自动信息的审计。	内置	-18
		12	0	拒绝可疑连接行为审计	2019	-07-25 01:05:26	审计系统中对网络连	要拒绝的信息日志,如防	内置	🗔 +E 🥖
		13		网络蟾虫行为审计	2019	-07-25 01:05:26	审计IDS系统告替信息	中國主级剧告管行为	内置	E +E 🥖
		14		SU成功动作审计	2019	-07-25 01:05:26	审计用户执行su操作	, 改变访问帐号成功的	内置	
		15	0	SU失败动作审计	2019	-07-25 01:05:26	审计用户执行su操作	, 故变访问帐号失败的	内置	🗔 +E 🥖
		16		su root动作审计	2019	-07-25 01:05:26	审计用户通过su命令!	来获得root权限的	内置	-12 +12 🥖
		17		网络探测威胁行为审计	2019	-07-25 01:05:26	对网络进行篇词扫描	行为审计。	内置	🗔 +E 🥖
	显示 100 - 条记录					显示1到40共40条	记录			< < 1

1、策略模板组:可以选择后进行模板的增删改查。也可以点击<sup>+1</sup>,对模板组内的模板进行 分组调整。

2、对模板组内的模板进行新增、移除和删除操作。

3、从模板创建策略:利用模板内的配置,创建新的策略。

4、将策略模板进行策略组调整。

5、修改策略模板。

点击从模板创建,根据实际情况对策略内容进行调整后保存即可

导航菜单	审计策略 🕀 🖶	计策略是针对审计对象进行的分析	,多用于内部违规操作审计场量,如:	非工作时间登陆,了解更多清	<b>修考:重计策略实施</b>		
> 安全概念	审计策略列表						Q ^
<ul> <li>安全监控</li> </ul>	新增	策略 💥 到除 🕘 屈用 🛑 停用	调整策略执行顺序 🚽 🖗 🖓 🖗 入	一等出全部 审计对象			
<ul> <li>日志査询</li> </ul>	序号 📄	策略名#	*	处理	15式 处理顺序	▲ 是否内置 ↓ 操作	
<ul> <li>报表管理</li> </ul>	1	登录成功审计	启用	停止处理其他策略	1		_
▼ 策略管理	2	登录失败审计	8用	停止处理其他策略	2		
审计策略	3	启动进程审计	启用	停止处理其他策略	3	内置 🔵 🥖	
关联策略	4	SU失败动作审计	启用	停止处理其他策略	4	内置 🔴 🥖	
采集策略	5	拒绝可疑连接行为审计	启用	停止处理其他策略	5	西置 🔴 🥖	
知识库	6	su root动作审计	启用	停止处理其他策略	6	内置 🔴 🥖	
> ※产管理	7	SU成功助作审计	眉用	停止处理其他策略	7	内置 😑 🥜	
<ul> <li>日志采集</li> </ul>	8	普通病毒感染告誓审计	肩用	停止处理其他策略	8	内置 🔴 🥖	
> #545ab10	9	高风险病毒感染告警审计	启用	停止处理其他策略	9	内置 🔴 🥖	
· 3705 to 18	10	用户注销审计	启用	停止处理其他策略	10	内置 🔴 🥖	
	11	帐户变更审计	启用	停止处理其他策略	11	内置 🔴 🥖	
	12 📃	口令变更审计	启用	停止处理其他策略	12	内置 🔴 🥖	
	13 🔲	帐户权限变更审计	启用	停止处理其他策略	13	内容 🔴 🥖	
	14 🔲	策略修改审计	启用	停止处理其他策略	14	内音 🔴 🥖	
	15	可执行文件安装审计	启用	停止处理其他策略	15	内資 🔴 🥖	
	16	系统重启审计	启用	停止处理其他策略	16	内置 🔴 🥖	
	17 🔲	网络鳗虫行为审计	启用	停止处理其他策略	17	西国 🔴 🥖	
	18	网络探测威胁行为审计	启用	停止处理其他策略	18	内政 🔴 🥖	
	PT 100 4/23	100 ( as 100 ( as 100 as 100 ) ( as 1	-				
	200 Y 100 Y 100			重小1四30共30重化度		« (	<u> </u>

日航苗曲	(T)07.00	
→ 安全順常	新增审计等略	
<ul> <li>安全监控</li> </ul>	※ 策略名称	登录成为审计
▶ 日志查询	22.08.01.29	
▶ 报表管理	東南内音	· · · · · · · · · · · · · · · · · · ·
▼ 策略管理		审计行为 屬于 行为助作 login, 行为结果: 成功
审计策略	* 过滤器	104 10 104 10 104 10 10 10 10 10 10 10 10 10 10 10 10 10
关联策略		中作大型         访问控制         ×         中作大杂         用户显示         ×         ×
采集策略		<b>审计操作对象</b> 审计目标 审计行为 常计行为执行者 审计行为来源 审计有效时间段 其他条件
知识库		<ul> <li>● 居于 ○ 不堪于</li> </ul>
▶ 资产管理		
▶ 日志采集		2017が第天型 2017が第二号 2017年1月1日 2017年1月1日 1日 1
▶ 系统管理		· · · · · · · · · · · · · · · · · · ·
	合并条件	前法师 在 約内发生 次
	响应方式	○ 产生雪響 □ 转发外系统
	命中后继续	
	审计名称	
	◆ 审计类型	· 衛忠师 *
	◆ 审计级别	请选择 *

# 方法二、新建自定义审计策略

oud

举例:访问控制日志审计

192.168.100.101 的 root 帐号属于运维人员张鹏, 当 192.168.100.101 的 root 登录系统 时, 审计事件将显示审计人员为张鹏。

1、选择"审计策略->审计对象->审计人员",新增审计人员:

导航菜单	审计策	略 🙂 审计	计策略是针对审计	國象进行	的分析,参	用于内部违规操作审	计场景,如	:非工作日	<b>拘登陆,了解</b>	更多请参考:审计策略实施					
> 安全概節	审计策略列	し表								_					Q ^
<ul> <li>安全监控</li> </ul>	🖕 新増	小模板创建的	ene 💥 Elle	🔵 启用	🛑 停用	├ 调整策略执行顺序	5 🔊 导入	「今日日	論 审计对象	k					
<ul> <li>日志查询</li> </ul>	序号				策略名称		<u>्</u> भ	态		经理方式	处理顺序	▲ 是否内證	\$	操作	
<ul> <li>报表管理</li> </ul>	1		登录成功审计				肩	用 1	亨止处理其他策略	ē	1	内置		/	
▼ 策略管理	2		登录失败审计				E	用 1	守止处理其他策略	8	2	内置		/	
<b>审计策略</b>	3		启动进程审计				Ē	用(	等止处理其他策略	Ê	3	内置		1	
关联策略	4		SU失败动作审计				JE	用 1	亭止处理其他策略	ň.	4	内置		1	
100384	5		拒绝可疑连接行为	均审计			扇	用 1	亭止处理其他策略	ĥ	5	内置		1	
4niOrd:	6		su root动作审计				E	用(	<u>等止处理其他策略</u>	ê	6	内置		1	
	7		SU成功动作审计				JE	用(	<u>學止处理其他策略</u>	ĥ	7	内置		1	
· 页广省理	8		普達病毒感染告報	音串计			ß	用(	多止处理其他策略	ñ	8	内置		1	
1 日后米米	9		高风险病毒感染的	- 警察计			JE	用 (	P止处理其他策略	8	9	内置		1	
/ 系统管理	10		用户注销审计				E	用(	亨止处理其他策略	2	10	内置	•	1	
	11		帐户变更审计				E	用(	亨止处理其他策略	ž	11	内置	•	1	
	12		口令变更审计				Æ	用(	亭止处理其他策略	ň	12	内置	•	1	
	13		帐户权限变更审;	t			唐	用(	亭止处理其他策略	ñ	13	内置		1	
	14		策略修改审计				后	用(	亨止处理其他策略	ň	14	内置		1	
	15		可执行文件安装的	₽i+			启	用(	亨止处理其他策略	8	15	内置		1	
	16		系统重启审计				E	用(	守止处理其他策略	8	16	内置		1	
	17		网络鳗虫行为审议	ŧ			度	用	守止处理其他策略	8	17	内置		1	
	18		网络探测威胁行》	力审计			启	用(	守止处理其他策略	8	18	内置		/	
		4/77					-			-			-		
	量示 100	▼ 第記录						显示 1	<b>酉 30 共 30 禁</b> 论	SNR				< <	

导航菜单	审计策略		
> 安全概節	审计策略模板 审计类型	<b>审计人员</b> 审计行为对象 审计行为执行者对象 审计行为来源对象 审计时间能对象 审计目标对象	1
<ul> <li>・ 安全监控</li> </ul>	审计人员列表		Q
<ul> <li>日志查询</li> </ul>	日 = 审计人员组	→新選 業務除	
▶ 报表管理	「「「「「」」「「「」」「「「」」「「」」「「」」「「」」「「」」「」」「「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」」「」」」「」」」「」」」「」」」「」」」「」」」「」」」」	床号         聚号名称         设备地址         申计人员         描述         操作	φ.
▼ 策略管理		当前无可用记录	_
审计策略			
关联策略			
采集策略			
知识库			
> 资产管理			
<ul> <li>日志采集</li> </ul>			
▶ 系统管理			
			- 1
			- 1
	显示 100 🔻 条记录	显示 0 到 0 共 0 祭记员 《 《	> >



天翼**二** e Cloud

导航菜单	审计策略							
<ul> <li>安全概范</li> </ul>	审计策略模板 审计类型	审计人员 审计行为对	象审计行为执行者对象	审计行为来源对象	审计时间段对象	审计目标对象		
▶ 安全监控								
<ul> <li>日志查询</li> </ul>								
▶ 报表管理		◎ 🕞 🔹	账号名称	设备地址		审计人员	描述	操作 🔶
▼ 兼略管理				È	当前无可用记录			
审计策略								
关联策略		新增审计规	枵		×			
采集策略		* 1	张号名称: 192.168.100.101					
知识库		* 1	<b>设备地址:</b> 192.168.100.101					
▶ 资产管理			8418· 22					
▶ 日志采集			#117.0% (258)					
▶ 系统管理			描述:					
				确认	取消			
	显示 100 文 奈诺泉			显示 0 到 0 共 0 菜记家				

导航菜单	审计策略					
> 安全概范	审计策略模板 审计类型	审计人员 审计行为对象	审计行为执行者对象	审计行为来源对象 审计时间段对象	审计目标对象	· · · · · · · · · · · · · · · · · · ·
<ul> <li>安全监控</li> </ul>	审计人员列表 Q					
<ul> <li>日志查询</li> </ul>	日 늘 审计人员组	🚽 新塔 💢 删除				
<ul> <li>报表管理</li> </ul>	二品油堆 288	席号 📃	账号名称	▼ 设备地址	◎ 审计人员	描述 操作 ≬
▼ 策略管理		1 192.168.100.1	01	192.168.100.101	运進	/*
审计策略						
关联策略						
采集策略						
知识库						
<ul> <li>资产管理</li> </ul>						
<ul> <li>日志采集</li> </ul>						
▶ 系统管理						
	显示 100 🔻 条记录			显示1到1共1条记录		< < 1 > >

2、选择"策略管理->审计策略",新增访问控制日志审计:

导航菜单	审计策略	) 审计策略是针对审计对象进行的分析,多	用于内部违规操作审计场显,如:非工作时间登陆,	了鮮更多请参考: <u>审计策略实施</u>	
<ul> <li>安全概范</li> </ul>	审计策略列表				Q
<ul> <li>安全监控</li> </ul>	🚔 新増 🔮 从模板创	川建策略 渊 削除 🛛 📦 启用 🜘 停用	三 清整策略执行顺序 全导入 全导出全部 审	计对象	
▶ 日志查询	序号 🔲	策略名称	♦ 状态	处理方式 处理顺序	▲      最否内置       最近内置       操作
<ul> <li>报表管理</li> </ul>	1	登录成功审计	启用 停止处理具	他策略 1	
▼ 第略管理	2	登录失败审计	启用 停止处理其	他策略 2	内置 🔴 🧪
审计策略	3	启动进程审计	启用 停止处理其	他策略 3	内国 🔴 🧭
关联策略	4	SU失败动作审计	启用 停止处理具	他策略 4	内西 🔴 🥕
采集策略	5	拒绝可疑连接行为审计	启用 停止处理其	他策略 5	内置 🔴 🥜
知识库	6	su root动作审计	启用 停止处理其	他策略 6	内国 🔴 🥜
<ul> <li>) 资产等理</li> </ul>	7	SU成功动作审计	启用 停止处理其	他策略 7	内五 🔴 🥖
	8	普通病毒感染告替审计	启用 停止处理其	他策略 8	内置 🔴 🥖
· 山心木朱	9 🗉	高风险病毒感染告答审计	启用 停止处理莫	他策略 9	内国 🔴 🥜
* 新筑管理	10	用户注销审计	启用 停止处理其	他策略 10	内五 🔴 🥜
	11	帐户变更审计	启用 停止处理其	他策略 11	内国 🔴 🥖
	12	口令变更审计	启用 停止处理冥	他策略 12	内置 🔴 🧪
	13	帐户权限变更审计	启用 停止处理其	他策略 13	内五 🔴 🦯
	14	策略修改审计	启用 停止处理其	他策略 14	内国 ● /
	15	可执行文件安装审计	自用 停止处理具	他領略 15	内百 ● /
	16	系统重启审计	自用 停止处理其	仲策路 16	(内容) () () () () () () () () () () () () ()
	17	网络睡中行为审计	白田 停止が増減	位策略 17	
	18	図線探測成時行も審決		4000% 17 4000% 18	
	10			10 10	
	显示 100 🔻 条记录		显示 1 到 30 共 3	0 条记录	« < 1 >

导航菜单	审计策略	
> 安全概意	新聞市計預略	
<ul> <li>安全监控</li> </ul>	<ul> <li>              金 館略名称</li></ul>	
<ul> <li>日志查询</li> </ul>	無職内容 ■计行力规行者 圖子 人员名称 运进	
▶ 报表管理		_
▼ 策略管理	♥ 以應請 事件类型 请选择 ▼ 事件子类 请选择 ▼	
审计策略		1
关联策略	第计操作对象 审计目标 审计行为 审计行为执行者 审计行为承援 审计有效时间段 其他条件	
采集策略		
知识库	人员名称 ▼	
<ul> <li>资产管理</li> </ul>		
<ul> <li>日志采集</li> </ul>		
系统管理	◆ 新计人员列表 日 ☑ ● 第计人员组	
	会相条件         班回照         班         时的发生         次	

合并条件	済送経 在 約内发生 次	
响应方式	□ 产生苦馨 □ 转发外系统	
命中后继续		
审计名称	访问控制审计	
※ 审计类型	访问控制审计 x x	
※ 审计级别	활동 · · · · · · · · · · · · · · · · · · ·	
描述		
		10
	保存 戰消	

点击保存即可生成审计策略。

loud
导航菜单	审计策略	🙂 市	策略是针对审计对象进行	的分析,≸	5用于内部违规操作审计	场星,如:	非工作时间登陆,了解更多请参考:重	计策略实施			
<ul> <li>安全概览</li> </ul>	审计策略列表										
<ul> <li>安全监控</li> </ul>	🔶 新增 🝦	从橫板创建開	戦略 😫 勤除 🛛 📦 启用	🔴 停用	] 調整策略执行顺序	●每入	每出全部 审计对象				
<ul> <li>日志查询</li> </ul>	序号		1	意略名称		状态	处理方式	处理顺序 ↓	是否内置	▲ ±	作
<ul> <li>报表管理</li> </ul>	1		新增访问控制审计			启用	继续处理其他策略	31	自定义	۰ 🖉 🖌	
▼ 常納祭神	2		登录成功审计			启用	停止处理其他策略	1	内置	• /	
(1)+998	3		登录失败审计			启用	停止处理其他策略	2	内置	۰ 🖉	
学民族的	4		启动进程审计			启用	停止处理其他策略	3	内置	• 🖉	
平佳范略	5		SU失败动作审计			启用	停止处理其他策略	4	内置	۵ 🖉	
4010 kg	6		拒绝可疑连接行为审计			启用	停止处理其他策略	5	内置	• /	
※产售用	7		su root动作审计			启用	停止处理其他策略	6	内置	• 🖉	
97 BE	- 8		SU成功助作审计			启用	停止处理其他策略	7	内置	۵ /	
16米来	9		普通病毒感染告管审计			启用	停止处理其他策略	8	内置	• /	
从外营生	10		高风险病毒感染告警审计			启用	停止处理其他策略	9	内置	• /	
	11		用户注销审计			启用	停止处理其他策略	10	内置	• /	
	12		帐户变更审计			启用	停止处理其他策略	11	内置	• /	
	13		口令变更审计			启用	停止处理具他策略	12	内置	• /	
	14		帐户权限变更审计			启用	停止处理其他策略	13	内置	• /	
	15		策略修改审计			启用	停止处理其他策略	14	内置		
	16		可执行文件安装审计			启用	停止处理其他策略	15	内置		
	17		系统重启审计			启用	停止处理其他策略	16	内晋		
	18		网络睡中行为审计			唐田	停止处理其他策略	17	内容		
	显示 100 🔻	条记录					显示 1 到 31 共 31 条记录				< 1

#### 2.4.3. 审计对象管理

#### 一、审计对象说明

审计对象用于创建审计策略时调用的审计对象,可在多条审计策略中重复调用。

包括审计人员、审计行为、审计行为执行者、审计行为来源、审计时间段、审计目标。

1、审计人员:将系统帐号和自然人进行关联;

2、审计行为: 如登录动作 login、攻击动作 attack 等;

3、审计行为执行者:行为动作的帐号,如源用户,可选择已定义的审计人员,或者直接定义 设备地址和帐号;

4、审计行为来源:行为的源地址;

5、审计时间段: 审计行为发生的时间段;

6、审计目标:行为的目标地址、主机设备等。

### 2.4.3.1. 审计人员

#### 一、审计人员配置说明

步骤一、进入审计策略->审计对象->审计人员页面:

导航菜单	审计策略	© #ilf	帘略是针对市计	国象进行的	分析,多1	用于内部违规操作审计	场景,如	:非工作时间公	2队,了解更多请参考	: <u>审计策略实施</u>			
<ul> <li>安全概范</li> </ul>	审计策略列表												Q
<ul> <li>安全监控</li> </ul>	🚔 新増 🖕 从	橫板创建策略	5 💥 1999	● 启用 ●	停用	[三 调整策略执行顺序	<b>》</b> 导入	日本部     日本部     日本部     日本     日本	审计对象				
<ul> <li>日志查询</li> </ul>	序号			策略	名称		状态		处理方式	处理顺序 🔺	是否内置	0	操作
▶ 报表管理	1	. 3	登录成功审计				启用	停止处理其	他策略	1	内置	• 🖉	
▼ 策略管理	2	. 3	登录失败审计				启用	停止处理其	他策略	2	内置	• /	
审计编辑	- 3	III 1	自动进程审计				启用	停止处理其	他策略	3	内置		
关联策略	4		50失败动作审计				启用	停止处理其	他策略	4	内置	• 🖉	
采集箱路	5	. 1	拒绝可疑连接行?	ち审计			启用	停止处理其	他策略	5	内置	• 🖉	
ADIEP RE	6		su root动作审计				启用	停止处理其	他策略	6	内置	• 🥖	
※ ※ 产 签 语	7		5U成功动作审计				启用	停止处理其	他策略	7	内置	۰ 🌔	
	8	- i	普通病毒感染告望	警审计			启用	停止处理其	他策略	8	内置	• 🥖	
1 山心木東	9	. 7	高风险病毒感染的	吉警审计			启用	停止处理其	他策略	9	内置	• /	
* 新筑管理	10		用户注销审计				启用	停止处理其	他策略	10	内置	• /	
	11		账户变更审计				启用	停止处理其	他策略	11	内置	• /	
	12		□令変更审计				启用	停止处理其	他策略	12	内面	• /	
	13		帐户权限变更审;	+			启用	停止处理其	他策略	13	内西	• /	
	14		蜜略修改审计				启用	停止处理其	他策略	14	内置		
	15		可执行文件安装的	E1+			启用	停止处理其	位策略	15	内西		
	16		彩绘重启审计				息用	停止处理其	他暗路	16	内西		
	17		网络幔中行为审计	+			息用	停止处理其	· // 倍略	17	内西		
	18						(1)(1)	はいいでは	An dat alt	17	152		
	10		~9485#26588897437					171130494	12.04.40	10			
	显示 100 - 象	和最						显示 1 到 31	L 共 31 条记录				≪ < 1 >

导航菜单	审计策略							
<ul> <li>安全概览</li> </ul>	审计策略模板 审计类型	审计人员 审计行为对象	审计行为执行者对象	审计行为来源对象	审计时间段对象	审计目标对象		
<ul> <li>安全监控</li> </ul>	审计人员列表							Q
<ul> <li>日志查询</li> </ul>	🕌 审计人员组	🛖 新増 😫 <b>謝除</b>						
报表管理		序号 📄	账号名称	设备地址		审计人员	描述	操作 🔶
▼ 策略管理				=	前无可用记录			
审计策略								
关联策略								
采集策略								
知识库								
▶ 资产管理								
<ul> <li>日志采集</li> </ul>								
> 系统管理								
	显示 100 🔻 条记录			显示 0 到 0 共 0 条记录				< < > »

### 1、增加审计人员组:

Cloud

(1)点击右侧+号

导航菜单	审计策略														
安全概算	审计策略模板	审计类型	审计人		前计行为对象	审计行为执	行者对象	审计行为来源对	R	审计时间段对象	审计目标对	<i>\$</i> .			
<ul> <li>安全监控</li> </ul>	审计人员列表													Q	
<ul> <li>日志查询</li> </ul>	山 审计人员组 🕄		中新增	<b>1</b> 2019:											
<ul> <li>报表管理</li> </ul>			序号		9	账号名称	v	设	地址		氠	十人员	描述	操作	
▼ 策略管理									当前	元可用记录					
审计策略															
关联策略															
采集篇略					新增节点					×					
知识库					*	1080: U	549			<u>^</u>					
资产管理															
▶ 日志采集					*	节点类型:	#计人员组		٣						
▶ 系统管理								确认	取消						
						_	_			1.					
		-													
	显示 100 🔻 条记	家						显示 0 到 0 共 0	菜记录						

(2)点击新增节点右侧+号,创建审计人员节点

-99A@0	
· *****	新計算物通貨    新計算机    新計合力対象    新计合力的合理分象    新计分为供存分象    新计分均均均数    新计目标分象     新计目标分离     新加速     新
<ul> <li>其未世活</li> <li>其他情況</li> <li>其他情況</li> <li>天然風雨</li> <li>大然風雨</li> <li>大然風前</li> </ul>	単型         単

2、修改或者删除审计人员:

 SCH04
 #1178

 9 Sch03
 #1178

 9 Sch03
 #1175

 9 Sch03
 #11157

 9 Sch03
 #11157

步骤一、选中审计人员节点,点击新增按钮,输入绑定的系统账号和 IP 地址

步骤二、点击"确认"按钮,保存审计类型。

#### 二、功能验证

1、审计人员创建成功,新增和修改审计策略时,选择审计行为执行者,在审计人员列表 中能够选择人员。

### 2.4.3.2. 审计行为

#### 一、审计行为配置说明

1、进入审计策略->审计对象->审计行为对象页面:



2、点击新增按钮:

天翼**云** e Cloud

审计策略		
新增审计行为对象		
♦ 行为对象名称		
描述		
		10
审计行为	● 展于 ○ 不属于	
	行为助作 不考虑结果 * ◆ 添加	
	身号 行为动作 行为结果 ↓ 招作	
	当約元可用记录	
	像存 取造	
	審计規制 新聞審计行为対象 中 行为対象名称 描述 第十行为	2011年8月       1011年1月1日       1011年1日       10111年1日       10111年1日       10111年1日       10111年1日       10111年1日       10111年1日       10111日       10111日       10111日       10111日       10111日       10111日       10111日       101111日       10111日       10111日

3、点击"保存"按钮,保存审计行为对象。

#### 二、功能验证

1、审计行为对象创建成功,新增和修改审计策略时,选择审计行为,在审计行为预定义里能
 够选择此对象:

导航菜单	<b>车</b> 计集略	
> 安全概范	新聞來计論略	
<ul> <li>安全监控</li> </ul>	☆ 策略名称	
<ul> <li>日志查询</li> </ul>	<b>油喷</b> 内容	
报表管理		
▼ 策略管理	♥ 以高の 事件类型 语近岸 * 事件子类 第近岸 *	
审计策略		
关联策略	新计组的效率 新计目标 斯计行为》 新计行为地方者 新计行为地质 新计行为规则 新计有效时间段 其他条件	_
采集策略		
知识库	· 新选择	*
<ul> <li>资产管理</li> </ul>		Ч
<ul> <li>日志采集</li> </ul>	会开条件 🔄 医作行为对象	
<ul> <li>系统管理</li> </ul>	明磁方式 💭 产生音響 📄 转发外系统	
	命中后继续	
	<b>前</b> 计名称	
	<ul> <li>◆ 前计奖型 语迅序</li> </ul>	
	◆ 解計数別 第25年 ▼	
	描述	
	保存 取消	



### 2.4.3.3. 审计行为执行者

#### 一、审计行为执行者配置说明

1、进入审计策略->审计对象->审计行为执行者对象页面 :

导航菜单		
<ul> <li>安全概范</li> </ul>	第计预通信板 审计类型 审计行为过金 审计行为执行贪对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行为免疫对金 审计行机公式 审计目标对金 医非白素素 医子子 医子子子 医子子子 医子子子 医子子子 医子子子 医子子子 医子	
<ul> <li>安全监控</li> </ul>		Ē
<ul> <li>日志查询</li> </ul>	◆ #38 業 部除	
· 报表管理	序号         行为执行客时象名称         ▼         描述         操作	
▼ 策略管理	二 前約元可用记录	
审计策略		
关联策略		
采集策略		
知识库		
资产管理		
<ul> <li>日志采集</li> </ul>		
▶ 系统管理		
	显示 100 v 称记录 显示 0 3 0 共 0 负10 内10 负10 负10 负10 负10 负10 负10 负10 负10 负10 负	
	A	_

2、点击新增按钮:

导航菜单	审计策略											
> 安全概范	新增审计行为执行者对	in in the second se										
> 安全监控	会 名称	♦ 名称 test										
<ul> <li>日志查询</li> </ul>	描述											
· 报表管理												
▼ 策略管理	审计行为执行者	1 = 0 2										
审计策略		人风春秋										
关联策略		<ul> <li>属于 〇 不属于</li> </ul>										
采集策略		☆ 审计人员列表	日間。雪け人気傷									
知识库												
> 资产管理												
• 日志采集												
> 系统管理												
			保存 戰	ň								

3、点击"保存"按钮,保存审计行为执行者对象。

#### 二、功能验证

1、审计行为执行者对象创建成功,新增和修改审计策略时,选择审计行为执行者,在审计行 为执行者预定义里能够选择此对象。

导航菜单	审计策略										
<ul> <li>安全概范</li> </ul>	新增审计策略										
<ul> <li>安全监控</li> </ul>	※ 策略名称										
▶ 日志查询	策略内容										
▶ 报表管理	A 245658										
▼ 策略管理	* 过路路	事件类型	请选择			w.	事件子类	请选择			v
审计策略						1	1	1	1		
关联策略		审计操作》	阿象 审计目标	审计行为	审计行为执行者	审计行为来源	审计有效时间段	其他条件			
采集策略		◎ 自定义	<ul> <li>预定义</li> </ul>								
知识库		请选择									*
<ul> <li>资产管理</li> </ul>		4									
<ul> <li>日志采集</li> </ul>	合并条件	谱 test									
<ul> <li>系统管理</li> </ul>	响应方式	○ 产生背容 [	转发外系统								
	命中后继续										
	审计名称										
	◆ 审计类型	请选择				٣					
	※ 审计级别	请选择				¥					
	描述										
										R	存取消

### 2.4.3.4. 审计行为来源

loud

### 一、审计行为来源配置说明

1、进入审计策略->审计对象->审计行为来源对象页面:

导航菜单	
> 安全概念	第计算機模型 事计共型 事计人员 事计行力均余 事计行力均匀素 事计行力方法意对象 审计行为完成对象 审计行为完成对象 事计行为规定者 非计目标对象
<ul> <li>安全监控</li> </ul>	审计行为中面对象列表         Q
<ul> <li>日志査询</li> </ul>	◆ 所得 業部除
<ul> <li>报表管理</li> </ul>	<u>度号</u> 一 万分平道名枠 マ 描述 費作
▼ 策略管理	当新无可用记录
审计策略	
关联策略	
采集策略	
知识库	
<ul> <li>资产管理</li> </ul>	
<ul> <li>日志采集</li> </ul>	
▶ 系统管理	
	■ 素 100     -     ★ \$\$R\$     \$\$B\$,0 \$\$0,0 \$\$0,0 \$\$0,0 \$\$R\$     €     < >     >

2、点击新增按钮:



3、点击"保存"按钮,保存审计行为来源对象。

#### 二、功能验证

大異口 e Cloud

> 1、审计行为来源对象创建成功,新增和修改审计策略时,选择审计行为来源,在审计行为来 源预定义里能够选择此对象:

导航菜单	· 审计策略
<ul> <li>安全概説</li> </ul>	新增高计算端
<ul> <li>安全监控</li> </ul>	☆ 策略名称
<ul> <li>日志查询</li> </ul>	策略内容
▶ 报表管理	
▼ 策略管理	◆ U.a.a 事件类型 遠語师 ▼ 事件子英 遠語师 ▼
审计策略	
关联策略	审计操作对象 审计目标 审计行力 审计行力 排行力 推行力力执行者 With 173为来源 审计有效时间段 其他条件
采集策略	○ 自定义 ● 焚電义
知识库	· · · · · · · · · · · · · · · · · · ·
<ul> <li>资产管理</li> </ul>	
<ul> <li>日志采集</li> </ul>	ch### 🖬 🔤
• 系统管理	
	命中近继续 💿
	审计名称
	<ul> <li>◆ 审计类型 请范洋</li> </ul>
	<ul> <li>◆ 审计段别 第送承</li> </ul>
	編述
	保存 取法

### 2.4.3.5. 审计时间段

#### 一、审计时间段配置说明

1、进入审计策略->审计对象->审计时间段对象页面:



2、点击新增按钮:

天翼**云** e Cloud

导航菜单	审计策略						
> 安全概范	新增审计时间段对象						
・ 安全监控	◆ 名称	时间					
<ul> <li>日志査询</li> </ul>	描述						
• 报表管理							6
▼ 策略管理	# 时间段	(e) (\$\fill E\$	○ 早期 ○ 日期				
审计策略							
关联策略			× - ×				
采集策略		④ 属于 (	◎ 不履于				🛖 添加
如识库		序号	审计时间段对象类型		审计时间段对象值		操作
》资产管理		1	物日	06:25至07:00		*	
<ul> <li>日志采集</li> </ul>							
▶ 系统管理						保存	取消

3、点击"保存"按钮,保存审计行为来源对象。

#### 二、功能验证

1、审计时间段创建成功,新增和修改审计策略时,选择审计时间段,在审计时间段预定义里
 能够选择此对象:

导航菜单	审计策略	
> 安全概范	新增审计策略	
<ul> <li>安全监控</li> </ul>	◆ 策略名称	
<ul> <li>日志查询</li> </ul>	策略内容	
<ul> <li>报表管理</li> </ul>		
▼ 策略管理	(1) 100 km	<b>事件类型</b> 前选择 マ 事件子类 前选择 マ
审计策略		
关联策略		审计操作效象 审计目标 审计行为 审计行为先行者 审计行为来源 审计有效图列组织 具他条件
采集策略		
知识库		諸語経
<ul> <li>资产管理</li> </ul>		
<ul> <li>日志采集</li> </ul>	合并条件	
系统管理	响应方式	产生音答 — 转发外系统
	命中后继续	
	审计名称	
	參 审计类型	<b>海辺坪</b> *
	◆ 审计级别	<b>海遊</b> 帰 Y
	描述	
		8 <del>1</del>
		14-17 IU.01



### 2.4.3.6. 审计目标

#### 一、审计目标配置说明

1、进入审计策略->审计对象->审计目标对象页面:

导航菜单	
▶ 安全概范	审计预期提供 审计规型 审计人员 审计行为对象 审计行为执行者对象 审计行为地质者对象 审计行为电质对象 审计行为电质对象 审计行为电质对象 审计行为电流对象 审计行为电流对象 中计引起对象
<ul> <li>安全监控</li> </ul>	□ ■計目版対象列表 Q
<ul> <li>日志查询</li> </ul>	◆ 新油 業 期後
▶ 报表管理	<u>ゆ号</u> 目标対象名称 v 描述 提作
▼ 策略管理	当新无可用记录
审计策略	
关联策略	
采集策略	
知识库	
▶ 资产管理	
<ul> <li>日志采集</li> </ul>	
▶ 系统管理	
	■示     100 ×     MC录     ■示 0 利 0 共 0 和C录     <     <     <     <     >>
	■示 100 × 約2映 ■示 0 約 0 共 0 新 2 共 ●示 0 新 2 共 0 計 0 新 2 共 0 計 0 新 2 共 0 計 0 新 2 共 0 計 0 新 2 共 0 計 0 新 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

### 2、点击新增按钮:

导航菜单	审计策略			
> 安全概念	新增审计目标对象			
<ul> <li>安全监控</li> </ul>	◆ 名称	目标对象		
<ul> <li>日志查询</li> </ul>	描述			
▶ 报表管理				
▼ 策略倍理	♦ 目标対象	<ul> <li>● IP###: ○ 主机设备 ○ 視問告产</li> </ul>		
审计策略				
关联策略		IP地址 审计目标对象		
采集策略		<ul> <li>雇于 〇 不属于</li> </ul>		🚔 法加
如识印库		<b>帝旦</b> 常は日に対象米刑	▲ 常社日に対象値	A 19946
▶ 资产管理		1 IP#di	172.16.0.101	2611-
▶ 日志采集				
▶ 系统普理				保存 取消

IP 地址: 直接输入 IP 地址;

主机设备:选择系统内资产。

宙计目标对象			
新增审计目标对象			
※ 名称	目标对象	]	
描述			
✤ 目标对象	<ul> <li>○ IP地址 ● 主机设备 ○ 视图资产</li> </ul>		
	设置规型: Unix/Linux主创	* * IPHEN: 172.16.0.10	× Y
	<ul> <li>雇于 〇 不雇于</li> </ul>		🛉 添加
	<b>序号</b> 审计目标对象类型	⇒ 审计目标对象值	↓ 操作
		当前无可用记录	
			保存取消

视图资产:选择系统内视图。

Cloud

审计目标对象	
新增审计目标对象	
※ 名称	目标对象
描述	
◈ 目标对象	◎ IP地址 ③ 主机设备 ④ 视图均产
	57日点 * * * * * * * * * * * * * * * * * * *
	保存 戰诺

3、点击"保存"按钮,保存审计目标对象。

#### 二、功能验证

1、审计目标对象创建成功,新增和修改审计策略时,选择审计目标,在审计目标段预定义里
 能够选择此对象:

导航菜单	审计策略
安全概点	新國市计論語
<ul> <li>安全监控</li> </ul>	◆ 頒贈名称
<ul> <li>日志查询</li> </ul>	<b>第86</b> 方容 审计目标(PP%地) 展于 172.16.0.123
▶ 报表管理	A 1968
▼ 策略管理	* U2篇 事件类型 语志师 * 事件子类 谎话师 *
审计策略	
关联策略	
采集策略	
知识库	test X
<ul> <li>资产管理</li> </ul>	
▶ 系统管理	http:// Tellerianstationst
	瞬度方式 🤤 产生音警 🦲 被没外系统
	命中區鐵獎 📃
	前计名称
	<ul> <li>◆ 前計委里 第88年</li> </ul>
	<ul> <li>◆ 前计假别 清洗洋</li> </ul>
	描述
	保存 取消

## 2.5. 告警监控

功能介绍

对于您关心的事件,可以在配置审计策略或关联策略时选中产生告警,使其在产生事件 的同时生成告警,进入策略配置页面,设置相关的条件:

#### 具体配置

Cloud

(1) 进入 LAS 系统->策略管理->关联策略:

900 <b>8</b> 4	关股指導 © 关联指增在目志要素、単件的基础上,进行统计分析,进一步生成告偿,详体消点点未算整洁的发生。													
> 安全概范	关联策略列表												0	2 *
・ 安全监控	日 5 策略分组	- 新道	制修	🔘 启用 🛛 📵 停用	<b>夏</b> 寿入	御御田	10 命中统计							
<ul> <li>日志查询</li> </ul>	の緒攻击	序号		前略	88		② 更新时间	Ŧ		陷地描述	是否内置	命中次数	操作	
> 报表做理	自意破坏	1		流量1		停	₹ 2019-07-16 08:06	:23			自定义	0	0 / 🗅 🕷	( ) (
* 12:00 MTH	□ 内容安全 □ 设备故障	2		Microsoft-IIS攻击		停	∃ 2019-07-15 04:29	:08	【依赖外部日志源】	: IDS _ IPS	内置	0	i 🖗	
	東雅	3		同源异常登录尝试		停	目 2019-07-15 04:29	:08	[依赖外部日志源]	:所有设备的登录日志	内置	792		
	□ 具他 □ 基于统计类	4	10	数据库表删除		停	₹ 2019-07-15 04:29	:08	[依赖外部日志源]	: 数据库设备审计日志	内直	0		
大新新期		5	8	数据库表创建		停	₿ 2019-07-15 04:29	:08	【依赖外部日志源】	: 数据库设备审计日志	内置	0	0	
A SHITLE		6		Oracle SYS用户运程到	ž	停	用 2019-07-15 04:29	:08	【依赖外部日志源】	: 数据库设备审计日志	内置	0		
> 38:02:4618		7		Unix系统重启		停	司 2019-07-15 04:29	:08	[依赖外部日志源]	: Unix日志 【触发	内置	0		
- SO MIR		в		Unix系统关闭		傳	€ 2019-07-15 04:29	:08	【依赖外部日志源】	: Unix日志 【触发	内面	0		
· ANOTHER		9		曾建员登录失败		傳	€ 2019-07-15 04:29	:08	【依赖外部日志源】	: Unix日志、win	内置	792	0	
		10		第日令扫描		停	E 2019-07-15 04:29	:08	【依赖外部日志源】	: Unix日志、win	内置	397		
		11		密码猜测成功		停	₹ 2019-07-15 04:29	:08	[依赖外部日志源]	: 主机设备、安全设备、	内置	198		
		12		发现病毒告答		停	₹ 2019-07-15 04:29	:06	[依赖外部日志源]	: IPS/IDS/防病	内置	0	0	
		13	8	安全设备登录失败		傳	₹ 2019-07-15 04:29	:08	[依赖外部日志源]	: IPS/ID5/安全	内置	0	o 💿	
		14		登录认证异常		停	司 2019-07-15 04:29	:08	[依赖外部日志源]	:所有设备的登录日志	内置	2		
		15		Microsoft-远程服务攻	L	傳	₹ 2019-07-15 04:29	:08	【依赖外部日志源】	: IDS 【粮发条件】	内置	0		
		16		Microsoft-NETBI		停	€ 2019-07-15 04:29	:06	[依赖外部日志源]	: IDS 【被发祭件】	内置	0	0	
		17		UNIX- Mail攻击		傳	目 2019-07-15 04:29	:08	[依赖外部日志源]	: IDS 【触发条件】	内置	0	0	
		18	0	循中区溢出攻击		傳	€ 2019-07-15 04:29	:08	[依赖外部日志源]	: IDS 【触发条件】	内置	0	0	
				10.5%							-		C. C.	
	臺亦 100 ▼ 祭记录					1	記示 1 到 100 共 282 角	11092				< (	1 Z 3	2 2

#### (2) 点击新增

<ul> <li>・ 安全網篇</li> <li>◆ 単的方式 (《 产生音響 』 祥文外系统 』 現け担求</li> <li>・ 安全監約</li> <li>・ 日本直询</li> </ul>
・ 安全監約         产生告答           ・ 日本直询         ・
・日本意識         「二十四留」
报表管理 ② 友情描示:当告誓名称生成方式选择"自动"时,产生告告的事件名称将作为告告名称。
★ <b>放畅管理</b> 自然名称生成方式 ● 自动 ○ 自定义
(前) 第
关联領路 ※ 取引 両辺州 /
采集描述         令 告留大英 请选择         诉选择         *
如明辉 音響子英 谦逊学 🔹
> 资产管理
▶ 系统管理 知会资产责任人 U Elital
其他部項

#### (3) 进入"安全监控->> 告警监控",可以查看产生的告警:

告警监控															
待处理告	19 Eð	私告答	已归档告警												
待处理告誓列	表 🌹 过渡器	管理 🛞 🛛	监控设置												2
🛩 确认 🔰	冒清除 🛛 🏹	请选择过滤器	• • 膨 导出 •	┡ 标签 🕶											
序号			告警名称		关联策略	级别	♦ 対象名和	в – ф	对象IP	系统类型	类别	更新时间	•	总次	操作
1		密码猜测成功	6		密码猜测成功	严重	172.16.0.10		172.16.0.10	CentOS	网络攻击	2019-04-15 06:52:48		1312	🛩 🗑 🗐

#### (4) 点击告警名称,可以查看告警基本信息及历次发生情况:

待处理告警			
基本信息			-
✓ 确认 前 清除	查署知识库		
	告誓编号: 1	告警名称:	密码猜测成功
	级别: 📻	对象名称:	172.16.0.10
	对象IP: 172.16.0.10	类别:	网络攻击
	系统类型: CentOS	策略名称:	密码猜测成功
	总次: 1314	产生时间:	2019-04-15 03:12:59
	更新时间: 2019-04-15 06:53:09		
	<ul> <li>講述: 告告各称: 電码通過成功</li> <li>相关技声: 172.16.0.10</li> <li>告告契約: 戸理</li> <li>問題及想: 戸理</li> <li>相关: 長期日期</li> <li>1.313</li> <li>相关: 長期日期</li> <li>日期日期</li> <li>日期日期</li> <li>日期日期</li> <li>日期日期</li> <li>日期日期</li> <li>日期日期</li> <li>日期12.168.10.136</li> <li>目期時は: 172.16.0.19</li> <li>其二目     <li>其2.168.10.136     <li>目期時は: 172.16.0.19</li> <li>其二、日期日期     </li> </li></li></ul>		

## 2.6. 实时监控

#### 功能介绍

Cloud

如果您想进行实时监控,可以使用监控规则将原始事件筛选出来,使其生成实时事件, 进入"安全监控->实时监控->规则设置",设置相关的条件:

#### 具体配置

(1)如果您想进行实时监控,可以使用监控规则将原始事件筛选出来,使其生成实时事件,进入"安全监控->实时监控->规则设置",设置相关的条件:



(2)进入"安全监控->实时监控",选择监控规则,点击开始按钮,可以查看产生的实时事件:

实时监控							
安全事件实时监控列表 🚳 規则设置							2
10	×	<b>1 16 🖉 </b> 🖗 🖓 🕀 🗄	1				
接收时间	名称	类型	子类	严重级别	设备IP	源IP	目的IP
2019-04-15 06:55:45	sendmail服务信息	配置状态	状态跟踪	信息	172.16.0.10		172.16.0.10
2019-04-15 06:55:46	通用日志	其它	其它	信息	172.16.0.10		
2019-04-15 06:55:46	新建账户	账户管理	账户新建	信息	172.16.0.10		172.16.0.10
2019-04-15 06:55:46	用户口令惨改	账户管理	口令变更	信息	172.16.0.10		172.16.0.10
2019-04-15 06:55:46	删除用户	账户管理	账户删除	信息	172.16.0.10		172.16.0.10
2019-04-15 06:55:46	通用日志	其它	其它	信息	172.16.0.10		
2019-04-15 06:55:47	SSH会话关闭	连接	连接断开	信息	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:47	密码错误	访问控制	用户登录	低级	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:47	密码错误	访问控制	用户登录	低级	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:47	密码错误	访问控制	用户登录	低级	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:47	SSH会话关闭	连接	连接断开	信息	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:48	密码错误	访问控制	用户登录	低級	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:48	密码错误	访问控制	用户登录	低级	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:48	SSH会话关闭	连接	连接断开	信息	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:48	root登录	访问控制	用户登录	信息	172.16.0.10	192.168.100.136	172.16.0.10
2019-04-15 06:55:48	SU会适开启	访问控制	用户切换	中级	172.16.0.10		172.16.0.10
2019-04-15 06:55:49	ctl_mboxlist	配置状态	状态跟踪	信息	172.16.0.10		172.16.0.10

### 2.7. 报表管理

#### 功能介绍

您可以从模板中选取需要生成报表,并且可以实时查看或定义任务生成报表。开启报表 实例后,可根据报表时间统计报表,于每日凌晨2点统计前一天的报表数据,报表实例可根 据用户需要自行新增。

### 2.7.1. 报表实例

具体配置

(1) 点击报表管理->报表实例

导航菜单	报表管理		
<ul> <li>安全概览</li> </ul>	报表实例 报表任务		
<ul> <li>安全监控</li> </ul>	报表实例列表		Q
<ul> <li>日志查询</li> </ul>	日 🧁 报表分组	🖕 新培 😫 删除 🔘 启用 📵 停用 🚳 个性化配置	
▼ 报表管理	日 🧰 日常报表	序号 📄 实例名称 ▲ 报表时间 更新时间	⇒操作
策略管理	□ 主机类	1 Unix英主机日志分布日报 时间范围:每日 2019-07-25 01:05:18	lin 🔵 🧷
资产管理	□ 网络设置突 □ 防火墙类	2 Windows英主机日志分布日报 时间范围:每日 2019-07-25 01:05:18	r 🕒 🥔 🥖
<ul> <li>日志采集</li> </ul>	<ul> <li>数据库类</li> <li>0 の用業</li> </ul>	3 主机访问控制分布日报-Linux 时间范围:每日 2019-07-25 01:05:18	lin 🥌 🥖
<ul> <li>系统管理</li> </ul>		4 1 主机访问控制分布日報・Windows 时间范围:毎日 2019-07-25 01:05:18	li 🕒 🥖
	萨班斯报表 第60保拍报表	5 目 其它美日志分布日报 时间范围:每日 2019-07-25 01:05:18	r 🕒 🥟
		6 安全告替分布情况日报 时间范围:每日 2019-07-25 01:05:18	r 🕒 🥟
		7 应用类日志分布日报 时间范围:每日 2019-07-25 01:05:18	li 🔵 🧷
		8 应用访问控制分布日报 时间范围:每日 2019-07-25 01:05:18	li 🕒 🥖
		9 _ 数据库美日志分布日报 时间范围:每日 2019-07-25 01:05:18	li 🕒 🥖
		10 副 数据库访问控制分布日报 时间范围:每日 2019-07-25 01:05:18	li 🕒 🥖
		11 日志总体分布周报 时间范围:每周 2019-07-25 01:05:18	li 🕒 🥖
		12 日志总体分布日报 时间范围:每日 2019-07-25 01:05:18	R 🔵 🧷
		13 日志总体分布月报 时间范围:每月 2019-07-25 01:05:18	li 🔵 🥖
		14 用户登录分布日报 时间范围:每日 2019-07-25 01:05:18	R 🔵 🧷
		15 用户登录失败分布日报 时间范围:每日 2019-07-25 01:05:18	li 🔵 🥖
		16 登录失败分布日报 时间范围:每日 2019-07-25 01:05:18	R 🔵 🧷
		17 登录成功分布日报 时间范围:每日 2019-07-25 01:05:18	li 🔵 🧷
	显示 100 🔻 条记录	显示 1 到 44 共 44 祭记录	« < 1 > »

#### (2) 点击新增

报表管理			
新增报表实例			
◆ 实例名称	test	]	
♠ 权振关别	安全事件报表 X ¥	♦ 欄版名称	安全事件分布统计
事件名称		时间范围	每日 *
事件类型	溝透準	事件子类	×
设备类型	· 请选择	事件严重说别	講進择
源地址		目的地址	
目的端口		源用户	
目的用户		采集器地址	
◆ 分组字段	事件名称	♦ 列表字段	x 事件名称
排序字段	·病选择	]	
描述			
			ß
			保存 取消

(3) 查看报表实例详情

大異口 e Cloud



详细	详细列表											
序号	事件名称	事件类型	事件严重规制	设备地址	教證							
1	计划任务执行	其它	信息	172.16.0.173	242							
2	计划任务执行	其它	信息	172.16.0.221	242							
3	postfix服务信息	配置状态	信息	172.16.0.173	120							
4	postfix服务信息	配置状态	信息	172.16.0.221	120							
5	系统计划任务执行	其它	信息	172.16.0.173	60							
6	系统计划任务执行	其它	信息	172.16.0.221	60							

### 2.7.2. 报表任务

#### 功能介绍

报表实例可根据用户需要自行新增。

报表任务可以设置定时执行报表实例,并将执行结果发送给配置的收件人(需在系统参





数中配置邮箱信息)。

#### 具体配置

(1) 点击报表管理->报表任务

导航菜单	规表普通
> 安全概览	报表实例 报表任务
・ 安全监控	报表任务列表 Q
日志查询	
▼ 报表管理	原号         日         名称         任务类型         更新时间         课件
▶ 策略管理	1 test 32809.47
<ul> <li>资产管理</li> </ul>	
▶ 日志采集	
<ul> <li>系统管理</li> </ul>	

#### (2) 点击新增

报表管理					
报表实例 报表任务					
报表任务列表					Q
♣新増 業 删除					
序号 🗌 名称 🔺	任务类型		更新时间	↓ 操作	
新增振行	田务	×			
*	任务名称				
*	<b>实例选择</b> 请选择				
*	<b>任务类型</b> 立即执行	v			
*	发送类型 PDF	<b></b>			
•	◎ 收件人 请选择				
P	枷收件人				
	描述				
		18			
		保存取消			

## 2.8. 云端配置

#### 功能介绍

客户端在连接到云端后,会接收来自云端发布的威胁情报,安全资讯和云端升级等信息。

#### 具体配置

1.用户在"是否接入云端"下拉选项选择"是",并连接云端测试成功后,再去选择升级方式,是否 自动执行重大事件任务,所属行业,云端上传数据等选项勾选"我已仔细阅读免责声明"后点击 保存按钮完成云端配置,如下图所示:

导航菜单	云满配置	
> 安全概范	云端配置	
・ 安全监控	是否接入云端是	▼ 连接云端测试
<ul> <li>日志查询</li> </ul>	升级方式 不升级	v
<ul> <li>报表管理</li> </ul>		
▶ 策略管理	选择所属行业: 高赦	×
▶ 资产管理	开启上传云端数据	
• 日志采集	序号 开启 数据项	上传数据内容
▼ 系统管理	1 整体安全	系统定期上传安全整体情况,包括风险值、资产数、原始日志数等统计数值。
用户管理	2 组件状态	系统定期上传组件运行状态信息。
日志管理	3 异常信息	系统自动触发式上传组件异常和业务异常信息
系统参数	4 硬件资源	系统定期上传硬件资源使用情况。
内置对象	5 升级记录	系统定期上传升级记录信息。
升级管理	6 资产	系统定期上传资产的系统关型分布统计数据。
许可证管理 云端配置 云端升级	7 原始日志	1. 系統定題上4個勝佔古忠意業,未兼新日本比例。epoi邀重,攻击未遵及攻击目标分布統计数据; 2. 云安全中心触发式上传未解所要由目表: 3. 用中也可以还原始日本意调试中主政员统承担化优化建议。
业务配置	加入云端数据反馈,有助于我们为您	履供更好的产品体验,谢谢!
系统配置		
集群管理		因于 我已仔细阅读 <u>免费声明</u>
系统巡检		保存

## 2.9. 拓扑图配置(选配)

#### LAS 拓扑图配置步骤简介

1、资产管理:

在 LAS 系统上首先需要将设备加入资产列表,资产是创建拓扑图的数据来源,配置步骤 参见 2.1.资产管理配置。

2、拓扑配置:

创建资产间的网络关系, 网元从资产清单里选择, 通过连线的方式, 将系统内各个资产 串联起来。

包括拓扑图的新增、修改、删除、隐藏等。

3、拓扑查看:

选择需要展示的拓扑图进行展示。

#### 2.9.1. 具体配置

一、创建拓扑

场景:将资产管理里的1台防火墙、1台路由器、1台Linux、1台Tomcat用拓扑图展示出来。

#### 二、具体配置

(1) 进入 LAS 系统->资产管理->拓扑管理->拓扑管理:



(2) 点击"新增"按钮,进入拓扑图编辑页面:

拓扑管理			
工具栏	文字栏	微件栏	~
〕 友情提示	: 在设备类图元、 道	£线、人员和视图	上长按鼠标
	背景类		
	÷		
	设备类		
		e	3
63	_		
	- 10		0
*	A		
-			
	÷		
	其它类		
	<b>-</b>		
	_	_	_
文字			
	÷		

(3) 从左边图元里拖拽一个防火墙进入右边空白区域:

拓扑管理												
工具栏	文字栏 微件档		0					<b>H</b> 8	制除图元		☐ 保存	取消
● 友情提示:	: 在设备类图元、连线、人		;左键可编辑履性,双:	图元名称可进行	修改,修改图元名	称后需要按回	Q车键才能生效。					
	背景类											
L												
	设备类		资产选择			a second	×					
	<b>a</b>	23	资产选择	102			× *					
			资产名称:	02								
<b></b>			系统类型:	AIX 5								
			资产IP:17	2.16.0.209								
	e,		资产类别:	服务器								
			IP地址段:	快省网络-172.16	.0.0/24(172.16.0.)	0)						
	其它类											
	170											
						确认	关闭					
124								1				



(4) 重复以上的方法,将 Linux 服务器、Tomcat、路由器创建出来:



(5) 创建个设备间的关系:

天翼**云** e Cloud

成分型建					
IAC	文字纪 微洋	H2 > (	0 N 5 N 6 6 0	用 御神蔵元	A 90 83
O ARES: 0	DRAZE, BR.	ARGERLAND	· · · · · · · · · · · · · · · · · · ·	s.	
1	NRM	_			
	28.4				
		3			
		3			
۲					
	0		2	3	
	HDa .				
-	-	-			
<u></u>					
	0		301	102	



(6) 拓扑查看:

点击资产管理->拓扑查看->拓扑管理,选择创建的"系统拓扑":







## 3.1. 安全仪表盘查看

### 一、安全事件仪表板查看

仪表板默认包含:整体状况、事件分析、审计分析、告警概况、系统状态 5 个部分内容,也可自定义添加需要关注内容。

整体状况 事	伸分析 审计分析	f 告警概况	系统状态						٥
既况分布									今日
告警 2		÷	<sup>关联事件</sup> 12		审计事件 <b>12</b>		9 9	5 610	
重点关注日志Top10									i
SU会话	SSH□	ctl	send	rsyn	SSH会	SSHIR	删除用户	新建账户	用户口令
<b>192</b> 近7日:238	<b>1152</b> 近7日:1428	<b>2404</b> 逝7日:2955	5 <b>2403</b> 5 ₺7日: 2955	<b>2403</b> 近7日:2955	<b>384</b> 逝7日:476	<b>192</b> 近7日:238	96 近7日:119	<b>96</b> 近7日:119	96 近7日:119
里点设备				配置	重点资产 🕢				I
172 16 0 10				11840					
Egg 172.10.0.10				11040	资产名称	风险等	取 告告分	<b>帝</b>	
					1/2.16.0.10	T			



1、系统状态:

大異口 e Cloud

- 仪表板默认显示系统状态,该模块可以查看; •
- 设备基本信息:设备型号、版本号、软件序列号;
- 当前关键组建的运行状态:业务管理器、响应中心、数据分析器使用情况; •
- 系统资源占用情况: CPU、内存以及硬盘使用情况: 系统运行时间。 •

整体状况 事件分析 审计分析 告誓	術 系统状态					• Z
响应中心 🗳 重启	数据分析器	🤣 重启	业务管理器	🤣 重启	数据存储	🖬 存储计算
<b>IP地址:</b> 172.16.0.151	IP地址: 172.16.0.151		<b>IP地址:</b> 17	72.16.0.151	存储已用: 4	G/150G(2%)
运行状态: 运行正常	运行状态:运行正常		运行状态:	國行正常	历史数据: 1	Æ
运行组件:数据分析器 采集控制器 响应中心 业务管理器 采集	器 流量引擎					Ø
<b>服务器名</b> : localhost.localdomain[172.16.0 运行时间: 0天15小时43分钟 运行状态: 采集控制器 运行研究	.151]			磁盘使用情况 留 20.13/341.09GB (5.9%) 2	检查使用情况 0.13/341.09GB (5.9%)	
	CPU					100%
CPU 1 % RAM 4.66/7.81GB(60%) Swap 0/8GB(0%)						
TARAL						
网卡 MAC地址 (运行	行状态 🕴 MTU 🍦 接收包	数 0	发送包数 丢包数	x ↓ 接收字节	♦ 发送字节	
eth0 00:1E:67:F8:FE:D4	UP 1500 721355	167	20856418 0	113832497358	141990097	80 1000Mb/s
eth1 00:1E:67:F8:FE:D5	UP 1500 2054301	1799	0 0	1847669934828	0	1000Mb/s

2、整体安全概况:



点击各个模块,可以显示更详细的日志信息。

3、日志查询:

大異し e Cloud

> 事件类型 TOP5: 柱状图显示今日整网安全日志类型数量,例如接收到的连接、配置 状态、网络攻击类日志数量;

> 事件种类 TOP5: 柱状图显示今日整网安全日志种类(类型里的细分项)数量,例如
>  接收到的连接接受、连接拒绝、系统内核信息日志数量;

 今日设备事件类型 TOP5: 柱状图显示今日各设备类型产生的安全日志数量,例如防 火墙设备、网络设备、主机设备产生的日志数量;

今日事件严重级别分布统计: 饼图显示今日安全日志的等级分布, 如信息、低级、
 中级等;

关联事件 Top10 列表: 按关联事件名称显示关联事件列表, 包含关联策略和事件数量;



事件发生趋势(30天):以日期和数量作为横纵轴,显示近 30天每天接收到的安全
 日志趋势;



● 点击各个模块,可以显示更详细信息。



4、审计分析:

今日审计事件 TOP5: 柱状图显示今日整网审计事件数量,例如登录日志、行为审计等日志数量;

审计类型统计 Top5: 柱状图显示今日整网审计事件类型数量,例如接访问控制审
 计、网络攻击审计、账户管理审计的数量;

审计事件:按审计事件名称分类显示审计事件列表,包含审计策略、审计类型和事件数量;

审计事件发生趋势(30天):以日期和数量作为横纵轴,显示 30天内审计事件数量
 趋势;

● 点击各个模块,可以显示更详细信息。



5、告警概况:

大異口 e Cloud

告警类别:按照告警内容,饼状图显示当前所有告警信息类型分布情况,例如网络
 攻击、安全漏洞类型的数量分布;

告警严重级别分布统计:按告警严重级别,饼状图显示所有已产生的告警分布,例如
 严重、警告的告警数量及分布;

告警严重级别分布统计(最近 24 小时):按告警严重级别,柱状图显示近 24 小时产
 生的告警分布,例如严重、警告的告警数量及分布;

最近 30 天安全事件发生趋势:以日期和数量作为横纵轴,显示 30 天内告警数量趋势。



# 3.2. 日志列表

#### 日志查看

大異 Cloud

日志查询 -> 日志列表:

查看所有接收到的日志,可根据设备类型筛选。

导航菜单	日志列表								
安全概范	概范 查询								
<ul> <li>安全监控</li> </ul>	设备日志量排名列表								
▼ 日志查询	日期选择: 2019-07-25 ×	序号 IP地址	设备名称	<b>严重</b> 🔶	<b>(a)</b>	中級 🔶	低级 🔶	(信息) 💠	总数 🔻
日志列表	日 🎦 没备类型	1 172.16.0.193		0	0	0	19131	497971	517102
关联事件	Lunix/Linux主机(1)	2 172.16.0.10	172.16.0.10	0	0	2720	16320	116949	135989
审计事件	■ Windows王秋(1) ■ 网络设备(0)								
流量日志	▶ 防火増(0) ▶ 统一或助管理(0)								
导出任务管理	▲ 入侵检测系统(0)								
▶ 报表管理	▲ 入授防御糸統(0) → 扫描器(0)								
▶ 策略管理	VPN (0) 除病毒(0)								
资产管理	数据库(0)								
▶ 日志采集	↓ Web中间件(0) ↓ 堡垒机(0)								
▶ 系统管理	▶ 应用系统(0)								
	· → +E(1)								
	显示 100 - 条记录		显示 1 致	1) 共 ) 名记录					1
	SEA TOO A WHY		亚小 1 王	I Z >< Z JRHJR				(	× · //

点击 IP 地址,即可查看该 IP 地址当天的所有日志,如下:

日志列表										
概范	查询									
日志列表										Q
友情提示	: 请尽量编入	精确查询条件,查询时系统将返回前1	0,000条记录。							×
普通模式	安家林	載式						⊟ 查询条件	请选择	¥
时间段类型:	自定义		Ψ	日期范围: :	2019-07-17 00:00:0	00	- 2019-07-17 23:59:59	)		
采集器:	请选择		v	名称:				严重级别:	请选择	×
设备IP:	172.16.0.1	93		源IP:				目的IP:		
设备类型:	请选择		w.	执行动作账号:				动作对象名称		
动作对象类型										
商級查询	1									
				- ( <u>)</u> Ex	10 <b>1</b> 12	🔒 保存查询条件				🗹 极速模式 👔
御御田	() 和量列表量	以字段 🌆 高线分析 📑 标	世化优化建议							
序号		名称	<ul> <li>类型</li> </ul>	1 🕴 子类	严里级别	设备IP	\$ BB		源IP	目的IP
1		过罐平台允许连接	配置状态	いい おうない おうちょう おうちょう しんちょう しんち	信息	172.16.0.193	2019-07-17 00:02:4	0 25	5.255.255.255	172.16.0.146
2		过滤平台允许连接	配置状态	: 状态跟踪	信息	172.16.0.193	2019-07-17 00:02:4	0 20	01::193	ff02::1:ff00:1
3		过减平台允许连接	配置状態	状态跟踪	信息	172.16.0.193	2019-07-17 00:02:4	1 25	5.255.255.255	172.16.0.145
4		篩选平台已允许绑定本地端□	配置状態	: 状态跟踪	信息	172.16.0.193	2019-07-17 00:02:4	14 0.1	0.0.0	
5		过速平台允许连接	配置状态	: 状态跟踪	68	172.16.0.193	2019-07-17 00:02:4	14 17	2.16.0.193	172.16.0.196
显示 100 -	祭记录		显示 1	到 100 共 7,813	条记录 (实际查询到	7,813 条)			ĸ	< 1 2 3 4 5 > »

日志列表页面包含两部分,上方为查询部分,可根据日志的字段信息搜索想要关注的日 志信息,下方展示搜索结果。

点击事件名称即可进入事件详细信息页面,展示该条日志的详细信息,如下:

日志列表			
详细信息			-
<ul> <li>基本信息</li> </ul>			
名称:	信息世報的沪 标准事件	\$编号:	
事件编号:	1438791f-d5bb-5410-9b33-469a76b10c0f		
详细信息	Oct 21 16:18-47 localhost welf bagrwell, log, webere site, jel:1380/781194 protect, jd:2380/701660 det, jor:172.16.0.180 det, jor:180 urc, jp:172.1 pot:13482 method/GET domaing/ing.ddd.gov.cn uri/indod/gillib/pawr/jaardine/dark event, type:1rbs_1ask strt, tyme:2017. Jose, juli-20172 method/GET domaing/ing.ddd.gov.cn uri/indod/gillib/pawr/jaardine/dark event, type:1rbs_1ask strt, tyme:2017. Jose, juli-20172 method/GET domaing/ing.ddd.gov.cn uri/indod/gillib/pawr/jaardine/dark/event, type:1rbs_1ask GNEEL-wedgeNet_TXXIIID-Method/GENGENGENER/BELG	16.0.175 10-23 16 GFibGUN 1UeXBIC RtbD48a IhcmlseS 3VuYW5j _info:Nor	l arc_ 18:46 (CAbd 0802X 07/02 RVmmF 288b Mc Øa
类型:	网络攻击	子类:	其它
级别:	(A)	會级別:	Alert
设备类型:	防火油 设备	昏地址:	172.16.0.30
设备名称:	localhost P&	諸名称:	Nsfocus WAF
产品版本:	188	如间:	2019-04-16 02:28:27
原始时间:	2017-10-23 16:18:46	可信度:	50
O 22			
源地址:	172.16.0.175 遊主	E机名:	
<b>逆消口</b> :	19462 運動組	上掩码:	
遭MAC:	3	夏区域:	
避用户:	(1)	三营商:	
源操作系统:	83	间览器:	

## 3.3. 关联事件(选配)

Cloud

查看关联策略(2.3 管理策略配置)所触发的事件列表,通过关联策略所触发的事件都会 在此列表展示,如下:

1	-1									
导航菜单	关联研	<b>F</b> 件								
<ul> <li>安全概范</li> </ul>	关联事件	列表								Q
<ul> <li>安全监控</li> </ul>	● 専出	•								
▼ 日志查询	序号	事件名称	⇒ 策略名称⇒	事件类型 🝦	事件子类	对象IP	⇒ 事件级别	⇒ 产生时间	● 更新时间	▼ 总次 🗧
日志列表	1	rsyncd	10	配置状态	状态跟踪	172.16.0.10	整告	2019-07-25 02:28:15	2019-07-25 06:19:31	34285
关联事件	2	ctl_mboxlist	10	配置状态	状态跟踪	172.16.0.10	警告	2019-07-25 02:28:15	2019-07-25 06:19:31	34286
审计事件	3	sendmail服务信息	10	配置状态	状态跟踪	172.16.0.10	「「「「「「」」」	2019-07-25 02:28:15	2019-07-25 06:19:31	34286
流量日志	4	SU会话开启	10	访问控制	用户切换	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:26	2742
导出任务管理	5	SSH服务日志	10	连接	连接跟踪	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:26	2742
<ul> <li>报表管理</li> </ul>	6	SSH口令猜测	10	连接	连接跟踪	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:26	16452
▶ 第略管理	7	SSH会话关闭	10	连接	连接断开	172.16.0.10	警告	2019-07-25 02:28:21	2019-07-25 06:19:26	5484
→ ※产等理	8	useradd日志	10	连接	连接跟踪	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:24	1372
	9	新建账户	10	账户管理	账户新建	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:24	1371
	10	用户口令修改	10	账户管理	口令变更	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:24	1371
/ 永靖官理	11	删除用户	10	账户管理	账户删除	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:24	1371
	12	userdel日志	10	连接	连接跟踪	172.16.0.10	警告	2019-07-25 02:28:20	2019-07-25 06:19:24	1371
	显示 100	) 🔻 条记录				显示 1 到 12 共	12 条记录		[	« < 1 > »

#### 点击事件名称即可进入、该条事件类型的详细页面,如下:

Cloud

关联事件												
关联事件详情												
事件名称	#IA	时间访问审计				策略名	称: 非工作	时间访问审计				
事件类型	访问拉	체				事件子	<b>类:</b> 用户器	£₽				
事件级别	24					创建时	<b>向:</b> 2019-1	07-17 00:00:08				
原始事件内容:	圖論学样內容: Mar 2 19:57:55 RGOG-128 sehd[7016]: Accepted password for root from 192.168.100.136 port 54933 seh2											
事件列表												
时间段类型	自定义		Ŧ	日期范围:	2019-07-11 0	0:00:00 -	2019-07-1	7 23:59:59				
名称:				严重级别:	请选择		Ψ.	遼1P:				
目的IP:				类型:	请选择		¥	子类:	请选择	Ψ.		
批次:												
					0	<b>童询 🔋 清</b> 空						
序号 打	比次	名称	严重级别	设备地	d <u>it</u>	臣	间		激地址	目的地址		
1 7	358	示 (100mg) 示 (100mg) 示 (100mg)	信息	172.16.0.111		2019-07-17 01:19:50		192.16	8.100.136	172.16.0.111		
2 7	357	密码错误	低级	172.16.0.111		2019-07-17 01:19:48		192.16	8.100.136	172.16.0.111		
3 7	356	密码错误	低级	172.16.0.111		2019-07-17 01:19:47		192.16	8.100.136	172.16.0.111		
4 7	355	密码错误	低级	172.16.0.111		2019-07-17 01:19:46		192.16	8.100.136	172.16.0.111		
5 7	354	密码错误	低級	172.16.0.111		2019-07-17 01:19:44		192.16	8.100.136	172.16.0.111		
6 7	353	密码错误	低级	172.16.0.111		2019-07-17 01:19:43		192.16	8.100.136	172.16.0.111		

该页面展示触发该事件的策略信息,以及该类型事件的列表,点击名称即可进入详细信 息页面,如下:

事件详情		
事件详情		
● 基本信息		
名称:	密码错误 标准事件编号:	XT_General-LINUX_00033
事件编号:	c815f9be-8ce8-5c7a-a831-01fadcea5b7a	
详细信息:	Mar 2 19:57:46 RGOS-128 sshd[7013]: Failed password for root from 192.168.100.136 port 54931 ssh2	
类型:	访问控制 <b>子类:</b>	用户登录
緞别:	(低級) 服始報約:	7
设备类型:	Unix/Linux主fi, 设备地址:	5.5.5
设备名称:	RG05-128 产品名称:	LINUX
产品版本:	提收应约问:	2019-07-17 03:30:30
原始时间:	1551527866 可信度:	50
● 源		
源地址:	192.168.100.136 濃主机名:	
源端口:	54931 滚地址编码:	
源用户:	<b>返运营商</b> :	
源操作系统:	適測 <b>茵</b> 識:	

## 3.4. 审计事件(选配)

Cloud

查看审计策略(<u>2.4 审计策略</u>)所触发的事件列表,通过审计策略所触发的事件都会在 此列表展示,如下:

导航菜单	审计事件										
<ul> <li>安全概范</li> </ul>	审计事件列表										Q
<ul> <li>安全监控</li> </ul>	田 == 审计类型(2)	ه 🕑	• •								
▼ 日志查询	田 == 审订策略(3) 田 == 审计人员(0)	序号	事件名称		对象IP		事件级别	产生时间	更新时间	•	总次 🕴
日志列表	田 == 审计目标地址(1)	1	SU会话开启	3	172.16.0.10			2019-07-25 02:26:50	2019-07-25 06:22:59		2802
关联事件	田 = 审计行为(0) 田 = 审计行为来源(0)	2	新建账户	1	172.16.0.10		一般	2019-07-25 02:26:49	2019-07-25 06:22:57		1401
审计事件	田 == 审计行为执行者(0)	3	用户口令修改	3	172.16.0.10		警告	2019-07-25 02:26:50	2019-07-25 06:22:57		1401
流量日志	由 = 前引引援(0) 由 = 前计目标对象(0)	4	删除用户	1	172.16.0.10		一般	2019-07-25 02:26:50	2019-07-25 06:22:57		1401
导出任务管理											
▶ 报表管理											
▶ 策略管理											
<ul> <li>资产管理</li> </ul>											
<ul> <li>日志采集</li> </ul>											
系统管理											
	显示 100 🔻 条记录					显示 1	创 4 共 4 条记录	₹		« <	1 > »

点击事件名称即可进入、该条事件类型的详细页面,如下:

用计学件						
事件名称	: 密码错误		审计类型:	访问控制审计		
事件级别	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		产生时间:	2019-07-17 02:30:17		
审计策略	: root登录审计		爭件会话编号:	7013		
执行者账号	: root		执行者地址:	192.168.100.136		
操作对象名称			操作对象类型:			
审计行为	: login		审计行为结果:	失败		
审计行为来源	: 192.168.100.136		审计目标地址:	5.5.5.5		
审计行为详细信息	:					
事件列表						
时间段类型	自定义	日期范围: 2019-07-	-11 00:00:00 - 201	9-07-17 23:59:59		
名称:		<b>严重级别:</b> 请选择		* 源IP:		
目的IP:		<b>类型:</b> 请选择		▼ 子类:	请选择	¥
批次:						
			이, 查询 (1) 清空			
<b>広号</b>	批次 名称 严重级别	设备地址	时间		逐地址	目的地址
1	1150 TEL:		2010 07 17 02-29-27	11	02 168 100 126	

该页面展示触发该事件的策略信息,以及该类型事件的列表,点击名称即可进入详细信 息页面,如下:

事件详情		
事件详情		
● 基本信息		
名称:	1001登录 标准事件编号:	XT_General-LINUX_00027
事件编号:	a8c03ef5-ad52-588d-b1d8-0e0297527f1c	
详细信息:	Mar 2 19:57:55 RGOS-128 sshd[7016]: Accepted password for root from 192.168.100.136 port 54933 ssh2	
类型:	访问控制 子集:	用户登录
銀別:	<b>使日本</b> 原始戰别:	7
设备类型:	Unix/Linux主机 设备地址:	5.5.5.5
设备名称:	RG05-128 产品名称:	LINUX
产品版本:	操收时间:	2019-07-17 03:31:30
原始时间:	1551527875 可信度:	50
0 19		
源地址:	192.168.100.136 源主机名:	
避靖口:	54933 還地址掩码:	
源用户:	<b>迎运苦商</b> :	
源操作系统:	運動試錯:	

## 3.5. 流量日志(选配)

#### 一、场景说明

适用于流量接入后,产生会话;通过查询条件可以查看各种类型的会话以及客户端地 址、服务器地址、服务端口等详细信息。可支持的类别有数据库会话、流量日志、http 会 话、DNS 会话、TLS 会话等。

#### 二、流量日志的查看

1.进入日志查询->流量日志 :

导航菜单	1	6월日志												
・ 安全概览	流量	日志												Q
・ 安全监控	日期	:	2019-07-25		时间段:	00:00:00		- 23:5	9:59		会话	<b>类别:</b> 网络会话	v.	Ŧ
▼ 日志查询	安白	·注册 hF·			服冬粥抽屉						服务	彩建口:		
日志列表		MANDAIL -	L		DRYS HHADAL.			_			10095			
关联事件						Q. 査询		t						🕑 极速模式 🕜
审计事件	序号		客户端地址	服务器地址	服务器家	11 协议	应用协议	流入包	数 流出包数 波	象入字节数	流出字节数	开始时间	结束时间	操作
流量日志	1	1	72.16.0.155	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 01:48:44	2019-07-25 01:49:15	童看
导出任务管理	2	1	72.16.0.155	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 01:58:30	2019-07-25 01:59:01	查看
<ul> <li>报表管理</li> </ul>	3	1	72.16.0.157	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 03:21:01	2019-07-25 03:21:32	查看
策略管理	4	1	72.16.0.157	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 03:31:31	2019-07-25 03:32:02	查看
<ul> <li>资产管理</li> </ul>	5	1	72.16.0.157	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 04:21:01	2019-07-25 04:21:32	查看
<ul> <li>日志采生</li> </ul>	6	1	72.16.0.157	8.8.8.8	53	udp	dns	0	2	0	148	2019-07-25 04:31:31	2019-07-25 04:32:02	查看
<ul> <li>素成成原</li> </ul>	7	1	72.16.0.157	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 05:21:01	2019-07-25 05:21:32	查看
* 新汽管理	8	1	72.16.0.157	8.8.8	53	udp	dns	0	2	0	148	2019-07-25 05:31:31	2019-07-25 05:32:02	查看
	9	1	72.16.0.193	172.16.0.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:02	2019-07-25 01:54:33	查看
	10	1	72.16.0.101	255.255.255.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:02	2019-07-25 01:54:33	查看
	11	1	72.16.0.178	255.255.255.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:03	2019-07-25 01:54:34	查看
	12	1	72.16.0.161	255.255.255.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:03	2019-07-25 01:54:34	查看
	13	fe80:0	000:0000:0000:	ff02:0000:0000:0000:	5355	udp	hostmon	0	2	0	168	2019-07-25 01:54:04	2019-07-25 01:54:35	查看
	14	19	92.168.0.193	224.0.0.252	5355	udp	hostmon	0	2	0	128	2019-07-25 01:54:04	2019-07-25 01:54:35	查看
	15	fe80:0	000:0000:0000:	ff02:0000:0000:0000:	0	icmpv6	unknown	0	3	0	210	2019-07-25 01:54:17	2019-07-25 01:54:36	查看
	16	1	72.16.0.169	255.255.255.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:05	2019-07-25 01:54:36	查看
	17	1	72.16.0.193	172.16.255.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:06	2019-07-25 01:54:37	查看
	18	1	72.16.0.160	255.255.255.255	1947	udp	unknown	0	1	0	82	2019-07-25 01:54:06	2019-07-25 01:54:37	查看
	19		0.0.0.0	ff02:0000:0000:0000:0000:0000:0000:0	016 0	icmpv6	unknown	0	1	0	90	2019-07-25 01:54:27	2019-07-25 01:54:38	查看
	显示	100 -	条记录		显示	1到100共	10,000 条i	2录(34	[际查询到 10,	120条)			« < 1 2	3 4 5 >

#### 2. 通过条件对已有的流量日志进行列表查询:

Cloud

导航菜单	流生	出志	通过时间进行	行查询	4	话类别	<b>查询</b>		1	会话类别	子洗垣			
	流量日	2 2	4					1				各广墙的地址进行值询		Q
> 安全概览	时间	2019-04-24	00:00:00 至	23:59:59	*	活类别	网络会话	v		×	客户端地址			
▶ 安全监控	服务领地	ti:			16	务器端口						/		
▼ 日志查询	目的知	也地址进行 <del>查询</del>		通道	过端口	号进行了		意词	f) 清空					
日志列夷	序号	客户端地址	服务器地址	服务器端口	协议	应用协议	流入包数	讀出包数	流入字节数	讀出字节数	开始时间	↓ 结束时间		操作
	1	210.47.244.249	10.0.0.107	1521	tcp	oracle	123	126	61099	51408	2019-04-24 15:20:59	2019-04-24 15:21:10	<u>ㅎ</u> ~	
关联事件	2	192.168.122.120	172.16.0.170	3306	tcp	mysql	12	13	4523	1030	2019-04-24 15:21:18	2019-04-24 15:21:19	査査	
审计事件	3	192.168.0.254	192.168.0.254	3306	tcp	mysql	22	35	2654	2977	2019-04-24 15:21:18	2019-04-24 15:21:19	<u>호</u> 종	
	4	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	15	11	3009	1459	2019-04-24 15:21:19	2019-04-24 15:21:20	查吞	
流量日志	5	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1147	1601	2019-04-24 15:21:19	2019-04-24 15:21:20	宣音	
导出任务管理	6	192.168.100.51	192.168.100.30	1433	tcp	sqiserver	372	85	182757	23465	2019-04-24 15:21:19	2019-04-24 15:21:20	查查	
12=盆田	7	192.168.100.51	192.168.100.30	1433	tcp	sqiserver	18	17	3428	4498	2019-04-24 15:21:19	2019-04-24 15:21:20	<u>8</u> 8	
10070512	8	192.168.100.51	192.168.100.30	1433	tcp	sqiserver	8	9	1333	1419	2019-04-24 15:21:19	2019-04-24 15:21:20	查石	
▶ 策略管理	9	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1134	1713	2019-04-24 15:21:19	2019-04-24 15:21:20	宣告	
<ul> <li>溶产答理</li> </ul>	10	192.168.100.51	192.168.100.30	1433	tcp	sqiserver	14	11	2983	1459	2019-04-24 15:21:19	2019-04-24 15:21:20	直音	
▶ 系统管理														

### 3. 点击列表中会话查看会话详情:

序号	客户端地址	服务器地址	服务器端口	协议	应用协议	流入包数	流出包数	流入字节数	流出字节数	开始时间	♦ 结束时间	♦ 操作
1	210.47.244.249	10.0.0.107	1521	tcp	oracle	123	126	61099	51408	2019-04-24 15:20:59	2019-04-24 15:21:10	查看
2	192.168.122.120	172.16.0.170	3306	tcp	mysql	12	13	4523	1030	2019-04-24 15:21:18	2019-04-24 15:21:19	查看
3	192.168.0.254	192.168.0.254	3306	tcp	mysql	22	35	2654	2977	2019-04-24 15:21:18	2019-04-24 15:21:19	查看
4	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	15	11	3009	1459	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
5	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1147	1601	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
6	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	372	85	182757	23465	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
7	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	18	17	3428	4498	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
8	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1333	1419	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
9	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	8	9	1134	1713	2019-04-24 15:21:19	2019-04-24 15:21:20	查看
10	192.168.100.51	192.168.100.30	1433	tcp	sqlserver	14	11	2983	1459	2019-04-24 15:21:19	2019-04-24 15:21:20	查看

4.会话详情查看(应用协议、协议、应用子协议、源区域、应用协议类型、流入流出、总字节 数等):

流量日志			
流量日志			
客户端地址	210.47.244.249	服务器地址	10.0.0.107
客户端端口	49197	服务器端口	1521
源区域	中国	目的区域	
源城市	大连	目的城市	
协议	tcp	应用协议	oracle
应用子协议	其它协议	应用协议类型	其它
威胁类型	0	情报类型	0
流入字节数	61099	流出字节数	51408
总字节数	112507	流入包数	123
流出包数	126	总包数	249
用户名	Administrator		
SQL语句	select null from dual; select ingth(chr(200000000)) H, length(chr(2000000)) H, length(chr(20000)) H, 'c' cL from dual; select ingth(chr(20)), nchr(20) from dual; select did, serulaf from VSession where audial = userenv(SESSIONID'); select * from V_TC_GZ_GZFFB ; select o;		
			关闭

## 3.6. 导出任务管理

#### 一、场景说明

loud

对于你关心的日志事件,可以在日志查询中导出任务;导出完成可以在导出任务管理中查看 导出结果;进而你可以继续导入本地查看详细信息。

1. 进入"日志查询->日志列表"菜单。

导航菜单	日志列表										
> 安全概览	概范	查询									<u>^</u>
・ 安全监控	日志列表										Q
▼ 日志查询	<ol> <li>友情提示:</li> </ol>	: 请尽量输入	青确查询条件,查询时系统	将返回前10,000条记录	ł.						×
日志列表	普通模式	专定措	÷					[] 查询条	(#	書洗择	<b>*</b>
关联事件		1 4 10 100								9427	
审计事件	时间段类型:	自定义		*	日期范围:	2019-07-25 00:00:00	- 2019	9-07-25 23:59:59			
流量日志	采集器:	请选择		Ŧ	名称:			严重级别	: 请选择		le 🗌
导出任务管理											
▶ 报表管理	设备IP:	172.16.0.193			源IP:			目的IP:			
兼略管理	设备类型:	请选择		Ŧ	执行动作账			动作对象	名		
》 资产管理	-11/123166米				号:			称:			
> 日志采集	2011FA38809C										
<ul> <li>系统管理</li> </ul>	〇 高级查询	)									
					0, 查询	🔋 清空 🗧 层 保	存查询条件				🗹 极速模式 🕜
	Som 4			院に進化が							
	6号	- BUEZ SACAN	222	金 米刑	A 7*	▲ <b>正田</b> 纲211▲	沿谷TD 💧	etial 💧		酒TD 💧	Elétre é
	1	0 1	:知事件	其它	其它	信息 172.	16.0.193 2019	-07-25 04:07:20		Rect I	HINDAY V
	2		知事件	其它	其它	信息 172.	16.0.193 2019	-07-25 04:07:20			
	3	0 E	退出进程	配置状态	状态变更	i 🔃 🕅 🕅 172.	16.0.193 2019	-07-25 04:07:20			
	4	. 3	用特权服务	配置状态	状态跟踪	: 信息 172.	16.0.193 2019	-07-25 04:07:20			
	5		创建新进程	配置状态	状态跟踪	i ( <u>fill</u> ) 172.	16.0.193 2019	-07-25 04:07:20			
	6	. v	indows 过滤平台允许连.	配置状态	状态跟踪	: 信息 172.	16.0.193 2019	-07-25 04:07:20	255.255.255.255	5 172.16	i.0.141
	7	. v	Indows 过滹平台允许连.	配置状态	状态跟踪	: 信息 172.	16.0.193 2019	-07-25 04:07:20	255.255.255.255	5 172.16	i.0.178
	8		indows 过滤平台允许连.	配置状态	状态跟踪	: (信息) 172.	16.0.193 2019	-07-25 04:07:20	255.255.255.255	5 172.16	6.0.157
	显示 100 -	条记录		显示1到	100 共 10,000	) 条记录 (实际查询到 59	8,619 条)			« < 1 2 3	4 5 > »

2. 进入"日志查询->导出任务管理"菜单。

								́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́	史用指
異口									
Cloud									
导航菜单	日山江久苦神								
→ 安全概察	导出任务列表								Q
<ul> <li>安全监控</li> </ul>	業 删除								
▼ 日志査询	序号 🛛	任务名称	任务类型	查询类型	查询时间范围	查询条件	任务状态	创建时间	▼ 操作
日志列表	1 🗆	默认导出任务	日志列表	普通模式	2019-07-25 00:00:00~2019-07-25 23:59:59	设备IP: 172.16.0.111	完成	2019-07-25 06:33:37	<b>#</b>
关联事件	2 🛛	默认导出任务	日志列表	普通模式	2019-07-25 00:00:00~2019-07-25 23:59:59	设备IP: 172.16.0.193	进行中	2019-07-25 06:32:33	×
审计事件									
流量日志									
导出任务管理									
<ul> <li>报表管理</li> </ul>									
策略管理									
<ul> <li>资产管理</li> </ul>									
日志采集									
<ul> <li>系统管理</li> </ul>									

# 4日常维护

### 4.1. 软件版本升级

一、设备升级的目的(主程序及补丁包)

显示 100 - 条记录

- 1、获取新功能。
- 2、解决软件缺陷。

#### 二、升级注意事项

1、升级不会导致配置、日志文件、库文件、license 丢失。

2、主程序升级需要重启设备,会造成断网,请避开业务高峰期升级。

3、主程序升级有一定风险,请务必保证升级过程中,设备供电稳定。

4、主程序升级前,请认真阅读版本发行说明及升级指导,同时注意比对下载的升级文件 MD5 值是否与发行说明提供的一致,避免因升级文件损坏造成升级失败。

显示 1 到 2 共 2 条记录

#### 三、具体步骤

1、登录 Web, 进入系统管理->升级管理, 界面如下图所示:

导航菜单	升级管理									
<ul> <li>安全概范</li> </ul>	系统升级									
<ul> <li>安全监控</li> </ul>	基础库:	Pro.2019.07.17.0031	98		6	法律化库: Evt.2	019.07.17.001765			
<ul> <li>日志查询</li> </ul>	文件保存路径:	请洗择文件	选择文件 罰							
报表管理										
▶ 策略管理					升级					
资产管理	升级列表							 		
<ul> <li>日志采集</li> </ul>	序号	升级内容		升级前版本	升级后版本		升级结果	升级时间	*	操作
▼ 系统管理										
用户管理										
日志管理										
系统参数										
内置对象										
升级管理										
作可让管理										
云端孔图										
业务配置										
系统配置										
集群经理										
系统巡检										
		3			민준이 왜 이 밖 이 솟긴 곳					
	E4 100 + 20C1	R			 重小 U 到 U 共 U 禁记派			 		

(1) 在"系统升级处"处,单击"选择"按钮,选择本地 PC 机上的升级文件包(升级包后缀为.zip,前缀命名可任意,如 Las\_305.xxx.xx.zip,一般用下载时的升级文件名字即可,不需修改)。

(2) 点击"升级"按扭提交设置后,升级文件开始上传到设备上,上传成功后,设备会自动完成升级。

### 4.2. 修改密码

#### 一、业务控制台密码修改:

1、登录业务控制台 WEB 页面, 输入 http://10.250.250.128 :

默认用户: admin

默认密码: admin

▼ 安全概范	整体状况 事件	均析 审计分析	告誓概兄	系统状态						
> 安全监控	概况分布									0
<ul> <li>日志查询</li> </ul>	/1-15k		M EK III.	114-		303-1-30-04			+	
· 报表管理			大吠中	1+		#JT #P1+			» Е7336	22
> 策略管理	1		12			4		4	5/330	
步 资产管理	重点关注日志Top10									用户名: 系统管理员
<ul> <li>日志采集</li> </ul>										所雇用户组: 超级管理员组
> 系统管理	SUQ35	SSH[]	已退出进	Wind	ctl	send	rsyn	if\$980.it	錦造平台	电话号码:
	<b>2336</b>	99999+	9999+	9999+	9999+	99999+	9999+	99999+	9999	郎福: juminfo@1
										手机号码:
	<b>重小10年</b>				52 M	#4987 O				修改密码
	1982,4723,634,889				-	ALMONT U				实施描导
	172.16.0.193				340539	资产名称	风险等	级 告告分	術	下翻译使日本
	I72.16.0.10				116799	172.16.0.10	₹	0	000	- PHILANELIAN
										注纳
	内部互连威胁		内部細胞分	布		外部安全				

2、点击右上角"系统管理员"->"个人信息":



3、点击"保存",密码修改成功:

4、重新登录,验证密码。

**e** Cloud

- 二、管理控制台密码修改:
- 1、登录业务控制台 WEB 页面, 输入 http://10.250.250.128:8082 :

默认用户: admin

默认密码: admin

导航革单	账号口令管理			
<ul> <li>系统信息</li> </ul>	· · · · · ·			7
> 账号口令管理		影号	admin	
<ul> <li>网络管理</li> </ul>		原来码		
> 索引配置管理				
<ul> <li>              新焼工員      </li> </ul>		新密码		
日期时间管理		确计算机		
<ul> <li>数据库备份与恢复</li> </ul>		THE CLE IN		
<ul> <li>日志备份与恢复</li> </ul>				
<ul> <li>         系统恢复     </li> </ul>				保持
• 重置平台初始口令				
<ul> <li>系统停止和重启</li> </ul>				
> 系统参数配置				

2、点击"保存", 密码修改成功。

3、重新登录,验证密码。

## 4.3. 恢复出厂设置

一、恢复出厂配置:

1、登录管理控制台 WEB 页面, 输入 <u>http://10.250.250.128:8082</u>:



2、点击"系统恢复"->"系统恢复"按钮。

等待系统恢复完成。

3、重新登录,验证恢复结果。

### 4.4. 系统巡检

巡检功能获取服务器状态,生成巡检报告。

		_						
导航菜单	系统巡检							
> 安全概览	系统巡检							Q
<ul> <li>安全监控</li> </ul>	✔ 巡检执行	<b>#</b> 896	\$ 					
<ul> <li>日志查询</li> </ul>	序号		巡检任务名称	执行时间 🔻	执行用户	执行结果	操作	F
<ul> <li>报表管理</li> </ul>	1		巡检任务1564004970278	2019-07-25 05:49:30	系统管理员	成功	🖬 🗰	
> 策略管理								
<ul> <li>资产管理</li> </ul>								
<ul> <li>日志采集</li> </ul>								
▼ 系统管理								
用户管理								
日志管理								
系统参数								
内置对象								
升级管理								
许可证管理								
云端配置								
云端升级								
业务配置								
系统配置								
集群管理								
系统巡检								
	显示 100 *	条记录		显示1到1共1条记录			٠ .	1 > >

系统管理->系统巡检。

点击执行



巡检任务大致运行一分钟。

大異 Cloud

巡检结束后点击任务后方查看报告按钮,查看报告。

系统巡检										
🚾 导出HTML	与出PDF									
巡检报告										-
<b>立</b> 日K+/6向	VE0.52		十個索利日		C 54454 42225					
产面版本信息	V5.0.5.2		土机序列亏	R1438-4E3RE-5431	C-544FA-4332F					
巡检时间	2019-05-14 10:03:49									
巡校结里	不会格		巡路會田	诸古吾川下红色标	Rency					
ALTECHA	ALC: NO PERSONNEL CONTRACTOR OF		All the second s							
● 设备负载										
cnu田白杰占田家	1 096		cpu山核态占田來	0.6%						
oportor "Cicitate			-pur3ixの口彻辛							
cpu系统占用率	16.0%		内存占用率	41.0%						
load average	0.52, 0.24, 0.24		磁盘占用率	0.54%						
wa	1.8%		系统缓存	Free:8656MB, Buff	ers:20MB, Cached	:OMB				
cpu个数	1									
1//14./***	6.HT		1004							
巡检结米	音格		巡检意见	设督贝戴巡检结果	止吊					
<ul> <li>网络连通性</li> <li>发包信申</li> </ul>	岡卡 억희[RY/TY] FRR원[RY/T		路由表信	章 日标册址	网关	海码	Flage	Metric 6	oflico	TÍ
	eth0 31793 0			172.16.0.0	*	255.255.255.0	0 U	0 0	0	e
	eth1 15 0	0		172.16.254.0	*	255.255.255.0	) U	0 0	0	e
				link-local	*	255.255.0.0	U	1002 0	0	e
				default	svn.juminfo.org	0.0.0.0	UG	0 0	0	e
域名解析情况	异常									
	-									
·	小首格		巡检貨	包光 网络连通性计	2检结果存在异常	,啃重看红色标	北湖建议			
■ 系統运行状态										
系统运行时间	0天0小时34分钟		当前田	前 2019-05-141	0:04:06					
検査出行の主	+# .A. \\+#20	BX++	144 20 PM		Sel2+10		_			
核心理性列表	ない世柱	是 首 仔 任 存在	世程数	· · · · · · · · · · · · · · · · · · ·	湖结米			-		
	业务管理器	存在	1	F	格					
	数据分析器	存在	1	É	格					
	采集控制器	存在	1	É	格					
	流量引擎 	存在	1	ŧ	格					
	采集器 亚曲器	存在	1	É	格			-		
	★★## 业务系统	存在	1	1	格		_			
		存在	1	É	楷			1		
		1								
巡检结果	合格		巡检到	<b>記</b> 系统运行状态	巡检结果正常					
# 4.5. 修改 IP 地址

一、修改 IP 地址:

Cloud

注意: 设置 IP 地址将导致系统重启,请勿在业务高峰期操作(工作口配置任何网口都可用于流量接入口使用)。

1、登录管理控制台 WEB 页面, 输入 http://10.250.250.128:8082 :

默认用户: admin

默认密码: admin

点击"网络管理"修改 IP 信息

与航菜单	网	络管理								
▶ 系统信息	网络配置	i 路由酒	置							
▶ 账号口令管理		0			1				1	
▶ 网络管理			主机名	localh	host.localdomain					
> 索引配置管理			Milescome	172.16	0.154		五十年日     日	x eth1		
▶ 系统工具			<b>3</b> 29914	1/2.10	10.104		1111			
▶ 日期时间管理			网关	172.1	16.0.1		DNS	8.8.8.8		
▶ 数据库备份与恢复	<b>*D</b>	<b>71</b>						10.14	1	
<ul> <li>日志备份与恢复</li> </ul>	185	省称			IPV4			IPV6		
▶ 系统恢复			IPV4	地址	172.16.0.154		IPV6地址	2001::154		
▶ 重置平台初始口令	1	eth0	IPV4	権码	255.255.255.0		子网前缀长度	64		
▶ 系统停止和重启										
> 系统参数配置	2	eth1	IPV4	地址	10.251.251.128		IPV6地址			
▶ 抹除自检数据	~		IPV4	掩码	255.255.255.0		子网前缀长度			
			THE COLOR		10.050.050.100		and so that			
	3	eth2	IPV45	REFEC	10.252.252.128		IPV6四班			
			IPV4	能码	255.255.255.0		子网前缀长度			
			IPV4#	Bitt	10 253 253 128		IPV6ibbl			
	4	eth3	TRV/48	NA LO		_	乙酮酸磷化酶			
				17 9 49	168-1	255.255.255.0		J Patrickinge		
			IPV4	地址	10.254.254.128		IPV6地址			
	5	eth4	IPV4	阉码	255 255 255 0		子网前缀长度			
					233.233.233.0					
					170100000					

2、点击"保存"按钮:

导航菜单			同关					DNS	8.8.8.8	
▶ 系统信息										
▶ 账号口令管理	序号	名称			IPV4				IPV6	
▶ 网络管理			IPV4炭	the 172.16.0.1	54			IPV6地址	2001::154	
▶ 索引配置管理	1	eth0	IPV4擁	码 255.255.25				子网前缀长度	64	
▶ 系统工具										
▶ 日期时间管理			IPV4地	址 10.251.251	1.128			IPV6地址		
▶ 数据库备份与恢复	2	ethi	IPV4擁	岡 255.255.25				子网前缀长度		
▶ 日志备份与恢复					确认提示		×			
<ul> <li>系统恢复</li> </ul>	2	oth 2	IPV4地	址 10.252.252	▲ 修改网络配置后系统将重启	, 确定要修改吗 ?		IPV6地址		
▶ 重置平台初始口令		ettiz	IPV4擁	弱 255.255.25				子网前缀长度		
▶ 系统停止和重启										
▶ 系统参数配置	4	eth3	IPV4地	the 10.253.253				IPV6地址		
▶ 抹除自检数据			IPV4拖	码 255.255.25		The	BD/H	子网前缀长度		
			TPVAH	the 10.254.254	1128	VBAE	100113	IRV6Httl		
	5	eth4		10.234.234				11 10 10 10		
			IPV4/%	255.255.25				于阿肋跋长度		
		eth5 ( 85	IPV4世	ut 172.16.254				IPV6地址		
	6 理口)	理口)	IPV4擁	暇 255 255 25				子网前缀长度		
								1		
						62,77				
								-		

等待系统重启完成 IP 地址的修改。

3、登录新的 IP 地址。



# 4.6. 日志查看

- 一、查看系统日志:
- 1、登录管理控制台 WEB 页面。
- 2、点击"系统管理"->"日志管理":

导航菜单	日志管理			
<ul> <li>安全概范</li> </ul>	用户日志	系统日志		
<ul> <li>安全監控</li> </ul>	用户日志列表	·		Q
▶ 日志查询	友情提示:	导出全部日志可能激	如偏巨大,请输入查询条件后再导出。	×
▶ 报表管理	🕗 导出 🕶			
▶ 策略管理	序号	日志级别	日志內容	日志产生时间
》 资产管理	1	信息	来自客户端(172.16.0.26),用户(系统管理员)證录系统成功	2019-07-25 05:49:40
<ul> <li>日志采集</li> </ul>	2	信息	来自喜户端(172.16.0.26),用户(系统管理员)登录系统失败	2019-07-25 05:49:33
▼ 系统普理	3	信息	来自喜户端(172.16.0.28),用户(系统管理员)登录系统成功	2019-07-25 05:46:04
用户管理	4	信息	来自客户馈(172.16.0.26),用户(系统管理员)登录系统成功	2019-07-25 05:39:55
日志普理	5	信息	来自秦户端(172.16.0.28),用户(系统管理员)超时退出系统	2019-07-25 04:42:07
系统参数	6	信息	来自客户端(172.16.0.28),用户(系统管理员)待处理告誓列表	2019-07-25 04:04:43
内置对象	7	信息	来自客户端(172.16.0.28),用户(系统管理员)待处理告誓列表	2019-07-25 04:04:38
升级管理	8	信息	来自餐户端(172.16.0.28),用户(系统管理员)新增事件过滤策略	2019-07-25 03:42:39
许可证管理	9	信息	来曲客户號(172.16.0.28),用户(系统管理员)新端采集器	2019-07-25 03:39:22
云端配置	10	信息	来且客户端(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:34:02
云端升级	11	信息	来自客户诗(172.16.0.28),用户(系统管理员)事件查询	2019-07-25 03:29:56
业务配置	12	信息	来自客户端(172.16.0.28),用户(系统管理员)修改采集器	2019-07-25 03:28:15
系统配置	13	信息	来目客户端(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:26:19
集群管理	14	信息	来自客户端(172.16.0.26),用户(系统管理员)超时退出系统	2019-07-25 03:22:39
系统巡检	15	信息	来自畜户端(172.16.0.28),用户(系统管理员)修改采集器	2019-07-25 03:22:14
	16	信息	来自客户馈(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:15:33
	显示 100 - 第	记录	显示 1 到 40 共 40 条记录 (实际查询到 40 条)	< < 1 > »

这里记录了系统各组件的运行日志,包括异常故障日志。

# 4.7. 日志备份与恢复

## 一、日志备份与恢复

1、登录业务控制台 WEB 页面, 输入 https://10.250.250.128:8082(假设当前设备 IP 为 10.250.250.128)。

默认用户: admin

默认密码: admin

进入【日志库备份与恢复】

2、备份策略:不备份(系统默认不备份日志库),不会备份日志库。



3、自定义备份日志:可以选择每周、每月备份一次当前的日志库。

i、备份方式: SFTP

Cloud

IP 地址: 172.16.0.176 (需要备份到的 SFTP 服务器)。

账号: uplogs(备份 SFTP 服务器的账号)。

密码: Yourpassword (备份账号的密码)。

路径: /upload (备份 SFTP 服务器的路径)。

点击保存后,系统将立即向 SFTP 服务器备份一次日志库。

导航荣单	日志養俗与吹夏
▶ 系统信息	● 当日志文件经失成者无法正常使用时,可以通过日本状质功能将某一天成某一局的激展进行代表。日本最后限能力得不对,会定期最合会一天的数据,是后限能力用时,会定期最合上一局的数据
<ul> <li>账号口令管理</li> </ul>	· · · · · · · · · · · · · · · · · · ·
▶ 网络管理	
> 索引配置管理	备份据增 ◎ 不备份 ● 自定义
<ul> <li>         系统工具     </li> </ul>	各份周期 · · · · · · · · · · · · · · · · · · ·
▶ 日期时间管理	
<ul> <li>数据库备份与恢复</li> </ul>	當做方式 ④ SFTP ③ NFS
→ 日志备份与恢复	172.16.0.176
<ul> <li>         系统恢复     </li> </ul>	
▶ 重置平台初始口令	账号 uplogs
<ul> <li>系统停止和重启</li> </ul>	<b>密码</b>
<ul> <li>         ·        系统参数配置         </li> </ul>	
› 抹芯目检数粥	Material States and St
	677

ii、备份方式:NFS

IP 地址: 172.16.0.176 (需要备份到的 NFS 服务器)。 路径: /opt/nfstest (备份 NFS 服务器的路径)。 点击保存后,系统将立即向 NFS 服务器备份一次日志库。



4、自定义备份日志库:用户可以根据每天、每周通过使用 SFTP 和 NFS 备份:

i、选择每天:每天凌晨1点左右会备份一次日志库。

大異口

导航单单	日志备份与恢复
<ul> <li>系统信息</li> </ul>	● 当日本文件任先或者无法正常使用时,可以通过日本恢复功能将某一天或某一期的数据进行恢复,日本独分质期为每天时,会迎期最份会一天的武器,最份原则为原时,会迎期最份上一类的数据
> 账号口令管理	· · · · · · · · · · · · · · · · · · ·
<ul> <li>网络管理</li> </ul>	
> 太引配置管理	备份预略 ③ 不备份 ● 自定义
<ul> <li>系统工具</li> </ul>	各世期期 @ 他子 @ 周
<ul> <li>日期时间管理</li> </ul>	
<ul> <li>数据库备份与恢复</li> </ul>	儲价方式 ④ SFTP 🕘 NFS
<ul> <li>日志备份与恢复</li> </ul>	172.16.0.176
<ul> <li>系统恢复</li> </ul>	
重置平台初始口令	繁号 uplogs
<ul> <li>系统停止和重启</li> </ul>	860
> 系统参数配置	
<ul> <li>抹除自检数据</li> </ul>	關础 /upload
	677

	11,	远 作 同 :	<b>可</b> 远 挥 同 一	- 全周日的仕恵-	─大,	一向备份一	-次
--	-----	---------	------------------	-----------	-----	-------	----

导航单单	日志書份与你复
▶ 系统信息	● 当日本文件先先或者无法正常使用时,可以通过日本状发动能将某一天或某一期的发展进行依契。日本备给用用力得天时,会迎期指台前一天幼政策,备约用期为限时,会迎期指台上一期的政策
▶ 账号口令管理	· 新田 · 古道
<ul> <li>网络管理</li> </ul>	
> 素引配置管理	备份指端 ◎ 不备份 ● 自定文
<ul> <li>              系统工具      </li> </ul>	各他回期 —— 每天 ·> 目
→ 日期时间管理	
<ul> <li>数据库备份与恢复</li> </ul>	율(thiship) 年尚 · · · · · · · · · · · · · · · · ·
→ 日志备份与恢复	
▶ 系统恢复	
• 重置平台初始口令	177
<ul> <li>系统停止和重启</li> </ul>	展号 UD 五
> 系统参数配置	
▶ 抹脸白检数据	密码 <sup>日</sup>
	mRe /upload
	(147

二、日志恢复

1、进入硬件管理平台->【日志备份与恢复】->【恢复】界面,可查看历史日志库备份的结果。

与机束单	日志备份	与恢复				
<ul> <li>         新航信息     </li> </ul>	● 当日志文件丢	失或者无法正常使用时,	可以通过日志恢复功能将某一天或某一周的数据进行		1,会定期备份上一周的数据	
> 账号口令管理	备份 恢复	7				
▶ 网络管理						
> 素引配置管理	备份数据列表					
▶ 系统工具	序号	备份方式 SETD	备份服务器地址 172.16.0.176	备份时间 2019-07-25-01-10-01	状态	操作
▶ 日期时间管理	1	arte	172.10.0.170	2019-07-23 011001	10 AKAU	171.692
▶ 数据库备份与恢复						
→ 日志备份与恢复						
· 形态能力						
- 新田市(4月10日本						
「生日十日初知日マ						
• 新知仲正和里后						
<ul> <li>         新祝参数配置     </li> </ul>						
<ul> <li>抹除自检数据</li> </ul>						

2、对于备份成功的结果,可以进行日志库恢复,点击【恢复】按钮,输入相关信息(与立即 备份操作类似),即可进行恢复日志库,若当前系统日志库已存在会覆盖恢复。

<b>966</b> 年年	日志藝份与你复
▶ 系统信息	● 四日本文件各先成素无法正常使用时,可以通过日本依有功能时某一天或某一用的数据进行恢复。日本曾经原明为每天时,会定期曾份前一天的数据,曾经原则为原时,会定期曾份上一类的数据
▶ 账号口令管理	<b>自分 你</b> 其
▶ 网络管理	
▶ 索引配置管理	备的数据列表
▶ 系统工具	序号 著切方式 <u>名加速な合計 良加振動</u> 状态 資作 1 STP <u>Dubute</u> 1 STP <u>Dubute</u> 目 STP
▶ 日期时间管理	
<ul> <li>数据库备份与恢复</li> </ul>	※告告式 5570
→ 日志备份与恢复	
<ul> <li>         系统恢复         </li> </ul>	172.16.0.128
• 重置平台初始口令	ELE cont
> 系统停止和重启	
▶ 系统参数配置	
▶ 抹脓自检数据	
	tude /ob/i/Terruni/
	恢复 取得

# 4.8. 数据库备份与恢复

## 一、数据库备份

Cloud

1、登录业务控制台 WEB 页面, 输入 https://10.250.250.128:8082(假设当前设备 IP 为 10.250.250.128)。

默认用户: admin

默认密码: admin

进入【数据库备份与恢复】

2、备份策略:不备份(系统默认不备份数据库),不会备份数据库。



3、立即备份数据库:一次生效,立即备份一次当前的数据库。

i、备份方式: SFTP

Cloud

IP 地址: 172.16.0.176 (需要备份到的 SFTP 服务器)。

账号: uplogs(备份 SFTP 服务器的账号)。

密码: Yourpassword(备份账号的密码)。

路径:/upload(备份SFTP服务器的路径)。

点击保存后,系统将立即向 SFTP 服务器备份一次数据库。

教派体验的与终发
新設選挙出現异常物設元法使用的情况,可以通过数据条线复功超的发展的回时间点,数据条备台包含;系统力量策略,用小自定义策略,历史统计数据等:
· · · · · · · · · · · · · · · · · · ·
备份指端 💿 不备份 🛞 自定文 💿 立即备份
Shullan — 每天 — 月 — 月
备份方式 ④ SFTP 💿 NFS
IP#844 172.16.0.145
展号 root
8日
IR62 /opt/admin/
822

ii、备份方式:NFS

IP 地址: 172.16.0.176 (需要备份到的 NFS 服务器)。 路径: /opt/nfstest (备份 NFS 服务器的路径)。 点击保存后,系统将立即向 NFS 服务器备份一次数据库。



导航荣单	教現中各份与改复
▶ 系统信息	● 出版展库出现异常导致无法使用的情况、可以通过数据库收益功能的发展指导时间点、数据本等给包含:系统内置转电、用户自定交集电、历史统计数据等!
账号口令管理	
▶ 网络管理	
▶ 索引配置管理	备份策略 💿 不备份 🛞 自定文 💿 立即备份
▶ 系统工具	<b>40回题 金 研天 白 田 白 日</b>
▶ 日期时间管理	
<ul> <li>数据库备份与恢复</li> </ul>	备份方式 💿 SFTP 🛞 NFS
▶ 日志备份与恢复	172.16.0.176
<ul> <li>         系统恢复     </li> </ul>	
▶ 重置平台初始口令	BG /opt/nfstest
▶ 系统停止和重启	
▶ 系统参数配置	677
▶ 抹意自检数据	alla se a

4、自定义备份数据库:用户可以根据每天、每周、每月通过使用 SFTP 和 NFS 备份(备份方 式与立即备份一致)。

i、选择每天:每天凌晨1点左右会备份一次数据库。

导航荣单	
▶ 系统信息	当該集集社現界常导致无法使用的情况,可以通过数据集体复功据恢复到指定时间点、数据库算份包含;系统内置策略、用户自定义策略、历史统计数据等!
▶ 账号口令管理	各份 依須
▶ 网络管理	
▶ 索引配置管理	备份策略 💿 不备份 🐵 自定义 💿 立即备份
▶ 系统工具	各份图题 ● 每天 ◎ 周 ◎ 月
▶ 日期时间管理	
▶ 数据库备份与恢复	备份方式 🐵 SFTP 🕘 NFS
▶ 日志备份与恢复	172.16.0.145
<ul> <li>系统恢复</li> </ul>	
• 重置平台初始口令	勝号 root
▶ 系统停止和重启	869
▶ 系统参数配置	
<ul> <li>抹肽白检数据</li> </ul>	路径 /opt/admin/
	877

ii、选择周:可选择周一至周日的任意一天,一周备份一次。

导航单单	数据库备份与恢复
▶ 系统信息	● 自動環境中型現界常勢充法法使用的情景,可以通过動現成率或超越的支援期間型目向点,数据常备份包含(系統內面積),用户自由交景積,否止低计数据等()
> 账号口令管理	备份 你算
▶ 网络管理	
> 索引配置管理	备份温略 💿 不备份 🛞 自定文 💿 立即备份
<ul> <li>         新焼工員         </li> </ul>	86000 0 67 + 0 0 D
<ul> <li>日期时间管理</li> </ul>	
<ul> <li>数据库备份与恢复</li> </ul>	备创封问 书词 本
日志备份与恢复	
<ul> <li>         系统恢复     </li> </ul>	
• 重置平台初始口令	
> 系统停止和重启	
> 系统参数配置	
抹除自检数据	2869 ••• <sup>日</sup>
	歸径 /opt/admin/
	627

iii、选择月:可选择1号至28号的任意一天,一个月备份一次。



导航菜单	教派奉旨份与庆复
▶ 系统信息	● 出数据库出国界常导校无法使用的描述,可以通过数据年终我功能的复数指定时间点,数据库备合性会:系统外置指笔,用户自定义指笔,历史他计数据等!
▶ 账号口令管理	· · · · · · · · · · · · · · · · · · ·
<ul> <li>网络管理</li> </ul>	
▶ 索引配置管理	备份捐赠 💿 不备份 🛞 自定文 💿 立即备份
<ul> <li>              新焼工具      </li> </ul>	
▶ 日期时间管理	MI COMPANY ( 10 10 10 10 10 10 10 10 10 10 10 10 10
<ul> <li>数据库备份与恢复</li> </ul>	备份时间 每月 1号 x
▶ 日志备份与恢复	
▶ 系统恢复	MUD2A = 1 25
▶ 重置平台初始口令	177 39 Am
▶ 系统停止和重启	19 10
▶ 系统参数配置	
▶ 抹脓自检数据	<b>2</b> 時 7号
	84 IRitiz /opyraamuy
	Qtit

## 二、数据库恢复

1、进入硬件管理平台->【数据库备份与恢复】->【恢复】界面,可查看历史数据库备份的结果。

越	国库备份与恢复				
<ul> <li>当数据/</li> </ul>	车出现异常导致无法使用的情	况,可以通过数据库恢复功能恢复到指定时间点。数据	漆备份包含:系统内置策略、用户自定义策略、历史统计数据等!		
备份	佐夏				
备份数据	列表				
序号	备份方式 SFTP	备份服务器地址 172.16.0.145	各份时间 2019-07-25 06:37:23	状态	操作
-			A & A & A & A & A & A & A & A & A & A &	ME 102 700-102	
	取3	取須申告付 均均契 ● 加加須年出版月年日 ひ し か 使用(の) 年日 各位数部列表 厚日 各かの式 1 5FTP	取扱単価の与め.数	取扱業 当初 5 年後 (1) 取扱業 当初 5 年後 (1) 日本 5 年 (1) 1 日本 5 年 (1) 1 日本 5 年 (1) 1 日本 5 年	取扱用         取用         2019         2019

2、对于备份成功的结果,可以进行数据库恢复,点击【恢复】按钮,输入相关信息(与立即 备份操作类似),即可进行恢复数据库,若当前系统数据库已存在会覆盖恢复。

96.44	数据库备份与恢复			
▶ 系统信息	● 当数据库出现异常导致无法使用的情况,可以	通过数据库恢复功能恢复	到指定时间点。数据库备份包含:系统内置策略、用户自定义策略、历史统计数据等!	
> 账号口令管理	· · · · · · · · · · · · · · · · · · ·			
▶ 网络管理				
▶ 索引配置管理	备份数据列表		1	
▶ 系统工具	序号 叠切方式 1 SFTP	當切服务部地址	10000000000000000000000000000000000000	状心 操作
▶ 日期时间管理		2011/11/2	8	
<ul> <li>数据库备份与恢复</li> </ul>		你有方式	CETP	
▶ 日志备份与恢复		(AB/)-6		
<ul> <li>系统恢复</li> </ul>		IP地址	172.16.0.145	
• 重置平台初始口令		RK P.	root	
▶ 系统停止和重启		×-5	1001	
> 系统参数配置		废码		
<ul> <li>抹脸自检数据</li> </ul>			fact factor factor	
		開住	/opt/admin/	
			恢复取消	
		L		J

## 4.9. 集群维护(选配)

### 测试场景:

搭建集群: 主节点: 192.168.100.173

子节点: 192.168.100.171

(备注)

登录硬件管理平台: https://192.168.100.171:8082

登录业务控制平台: https://192.168.100.173:8443

#### 一、集群状态查看:

登录业务控制台页面进行集群维护。【系统管理】->【集群管理】查看当前集群状态。

导航菜单	
> 安全概念	集群記證證件参譯: 1.集群市点 [网络管理] 配置上级市点 今2.导出信任文件 +3.所有集群市点与入信任文件 +4.开会集群维护 +5.集群配置 +6.同步集群能置 +7.重合集群服务
<ul> <li>安全监控</li> </ul>	all units
<ul> <li>日志查询</li> </ul>	(取税志: [13])     (加)     (     (加)     (     (加)     (     (加)     (
▶ 报表管理	节点总数: 1 数据节点总数: 1 分片总数: 85 正致分片比例: 100.0%
▶ 策略管理	
资产管理	
<ul> <li>日志采集</li> </ul>	多月或语人之中。 《 如何 是 如何
▼ 系统管理	序号         服务室IP         核の服务器         集研設合         集研ی合         集研ی合         集研ی合         <
用户管理	1 194.106.100.1/3 22 正元、53回72 元法 第二次 53回72 元法 19回7 日本 1912 日本 1912
日志曾理	
系统参数	异烷表引席维护
内置对象	● 关闭 案 删除
升级管理	<u>除号</u> 素引库 第31年 第4日 第4日 第4日 第4日 第4日 第4日 第4日 第4日
许可证管理	国際元利用に次
云端配置	显示     100 ▼     余记录     显示 0 ≦0 共 0 条记录     <     <     <
云端升级	
业务配置	
系统配置	
集群管理	
系统巡检	

### 二、集群配置操作步骤:

登录业务控制台系统管理->集群管理查看操作步骤配置集群。

集群配置操作步骤:1.集群节点【网络管理】配置上级节点→2.导出信任文件→3.所有集群节点导入信任文件→4.开启集群维护→5.集群配置→6.同步集群配置→7.重启集群服务

### 三、集群维护:

数据节点配置上级节点后可在此列表查看已注册的数据节点,通过页面顶端的配置步骤 可快速配置集群,所有集群节点的集群状态更新为"已加入集群",集群即可配置成功。若集群 配置失败,可通过点击列表上的【下载日志】下载相关日志。

	u										
<b>集群管</b>	理										
集群配置	<b>御記置操作歩戦: 1.半期</b> 行点 [网络管理] 配置上级节点 → 2.号出信任文件 → 3.所有集群节点导入信任文件 → 4.开启集期维护 → 5.集務配置 → 6.局步集群配置 → 7.重启集群服务										
集群状态											
ţ	「「「「「「「「」」」	5	群名称: cluster1556453827754	主节点名称: node-172.16.0.170	主节点IP	172.16.0.170					
1	5点总数: 2	数据于	5点总数: 2	<b>分片总数:</b> 6	正常分片比例	100.0%					
集群维护											
長田信	任文件 👗 开启集群维护	日步集群配置 ② 重启集群服	き 🕣 下載日志								
应是	服务器IP	♦ 核心服务器	♦ 集群角色	◆ 集群配置状态	集群状态	操作					
10.0	172.16.0.170	是	主节点、数据节点	已完成	已加入集群						
1											
1	172.16.0.144	否	数据节点	已完成	已加入集群	导入信任文件					

### 四、修改集群节点:

大異

开启集群维护后可通过点击各节点的【修改】按钮来修改"是否作为主节点"是否作为数据节点"等配置,点击【确定】后即可成功配置。

注意:至少选择一个节点作为主节点。

集群管理					
集群配置操作步骤: 1.集群节点 [网络管理] 配置上级节点 → 2.	导出信任文件 → 3.所有集群节点导入信任文件 → 4.开启集群	#維护 → 5.集群配置 → 6.同步集群	記豊 → 7.重启集群服务		
集群状态					
集群状态:	集群名称:	主节点名称:		主节点IP:	
节点总数:	数据节点总数:	分片总数: 正常分片比例:			
集群维护					
- 导出信任文件 A.开启集群维护 的步集群配置 (	回 重启集群服务 🛛 下载日志				
序号 服务器IP ♦ 核心服务器 《	集群角色	◆ 集群配置状态	集群状态		操作
1 172.16.0.170 是	主节点(备选)、数据节点	已完成	集群服务停止	修改 网络配置	
2 172.16.0.144 否	数据节点	巴奈成	生難服务停止	修改 网络配置 导入信任文件 删	除
	修改集群中品 星态作为主节点, 目		*		« < 1 >
异常素引库维护	200 (P) 22 (P) (C) 26				
🔴 关闭 🗱 删除	是否作为数据节点: 是		·		
廖号 □ 素引库	开启状态		▼ 份因子	文档数量	存储占用 操
		保存取	ii		
显示 10 🔻 条记录		显示 0 到 0 共 0 条记录			<b>«</b> < )

## 五、网络配置**:**

开启集群维护后可以通过点击各节点【网络配置】按钮来修改节点的网络配置信息,修 改后点击【确定】即可成功应用。

集群配置操作步骤: 1.集群节点 [网络管理 集群状态	] 配置上级节点 🗲 2.号	計信任文件 → 3.所有集群节点导入信任文件 •	◆4.开启集群维护 → 5.	集群配置 → 6.同步集群	配置 <b>&gt;</b> 7.重启集開			
集群状态:		集群名称:		主节点名称			ŧ	节点IP:
节点总数:		数据节点总数:		分片总数			正常分	计比例:
集群维护								
- 导出信任文件 - 开启集群维护	同步集群配置 G	)重启集群服务 🕢 下载日志						
序号         服务器IP         ↓           1         172.16.0.170         身	核心服务器	集群角色	÷	集群配查状态	集體	¥状态 ×	修改网络配置	操作
2 172.16.0.144		localhost	DNS :	172.16.0.8			修改 网络配置 导入信任	至文件 删除
	eth0							
异常素引库维护	IP地址:	172.16.0.170	掩码:	255.255.255.0				
🔘 关闭 🛛 😫 删除	网关:	172.16.0.8	]					
◎ 索引库	ethl						文档数量	存储占用
	IP地址:	172.16.254.11	掩码:	255.255.255.1				
显示 10 🔻 祭记录					保存	取消		

## 六、删除节点:

开启集群维护后可以通过点击各节点【删除】按钮来删除节点,弹出框点击【确定】即 可删除此节点。删除的节点可以通过重启此节点业务系统后重新加入。

用户使用指南

集群维护	A								
● 导出	信任文件	🚢 开启集群维护	📑 同步集群配置	◎ 重启集群服务	1 下载日志				
序号		服务器IP	核心服务器		集群角色	↓ 集群配置状态	集群状态		操作
1	172.16.0.	170	是	主节点 ( 备选	)、数据节点	已完成	集群服务停止	修改 网络配置	
2	172.16.0.	144	裕	数据节点		已完成	集群服务停止	修改 网络配置 导入信任	文件 删除
					确认	×			
异常索引	库维护					多数探手生 确实地行到除吗?			
● 关闭	) 🛛 💥 Mile	÷				为如道去大,明阳初初期际吗?			
序号		□ 索引	库	开启状态			备份因子	文档数量	存储占用
						是否			
显示 10	0 🔻 条记	录				显示 0 到 0 共 0 条记录			

### 七、异常日志库维护:

loud

通过关闭、删除对异常日志库进行维护操作。关闭或删除异常日志库后"集群状态"会更 新为"正常"

集群管	理										
集群配置	<b>聚作步骤:</b> 1.4	集群节点 【网络管理】 配J	置上级节点 → 2.导出信任	主文件 → 3.所有集群节点	导入信任文件 🗲 4.开启集群	¥维护 → 5.集群配置 → 6.同	日步集群配置 → 7.重启集	群服务			
集群状态	_										
#	群状态: 🧲	結		集群名称: cluste	r1556528578	主节	点名称: node-1		主节点IP:	172.16.0.183	
ŧ	a总数: 1 数据节点总数: 1 分片总数: 31 正常分片比例: 75.6%										
集群维护											
「「 同步集	#R2 💿	) 重启集群服务 🛛 下!	戦日志								
序号		服务器IP		核心服务器		集群角色		集群配置状态		集群状态	操作
1	172.16.0.	183	是		主节点、数据节点		待時	步	已加入集群		
						显示1到1共1条记录					≪ < 1 >
异常索引库	維护										
🔵 关闭	💢 删除										
序号		索引库	开启状态	健康状态	主分片	备份因子	文档数量	存储占用		操作	
1		test	开启	警告	5	1	0	1.1kb	分片详情 关闭 删除		
2		test1	开启	警告	5	1	0	631b	分片详情 关闭 删除		
显示 10	▼ 条记录					显示1到2共2条记录					« < 1 >

# 4.10. 系统配置

硬件管理功能既是当用户登录业务管理控制台;可直接跳转到硬件管理平台。

系统管理->系统配置:当用户已经登录过硬件管理平台即可直接跳转到硬件管理平台页

面

▼ 安全概范	整体状况 事	件分析 审计分析	告誓概况	系统状态						• 2
<ul> <li>安全监控</li> </ul>	概况分布									今日 •
<ul> <li>日志査询</li> </ul>	4+ 55k		MINT	- 11h-				_	+	
・ 报表管理			大联手	414-		甲汀爭忤			™ 740047	
<ul> <li>策略管理</li> </ul>	L L		12			4		- 1	/4821/	
> 炭产管理	重点关注日志Top10									配益
<ul> <li>日志采集</li> </ul>										
▼ 系统管理	SU会话	已退出进	SSH□	Wind	计算机减	筛选平台	send	cti	rsyn	已创建新
用户管理	4622	9999+	9999+	9999+	9999+	9999+	9999+	9999+	9999+	9999+
日志管理	<b>浙7日:4622</b>	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日: 9999+
系统参数		<u> </u>								
内置対象	里点设备				配置	里点资产 🕢				配置
升级管理										
件可业管理	(m) 172.16.0.193				1508611	资产名称	风险等	級 告替分	市	
云湖配直	I72.16.0.10				231048	172.16.0.10	无	0	010	
10月71日10日 山本記書	A 172.16.0.111				8558					
系统部門										
朱獻祭運										
系统巡检										
	内部互连威胁		内部威胁分	分布		外部安全				全部、



天翼云 e Cloud

当用户未登录过硬件管理平台时,点击硬件管理会直接跳转到修改密码的页面。

导航菜单	⇒☆振花 🙂	欢迎登录 深信服日志	审计系统 ! 当前时间	: 2019-07-25 08:56	36 ,系统已运行 0月	(7小时3分钟 。				
▼ 安全概览	整体状况 事件	:分析 审计分析	告警察况	系统状态						0.2
<ul> <li>安全監控</li> </ul>	概况分布									今日、
<ul> <li>日志查询</li> </ul>	###		~ ~ ~ ~	10					o+	
▶ 报表管理	1		10	14		甲汀弗什			1740217	
・ 策略管理	-		12			4			1/4021/	
》 资产管理	重点关注日志Top10									Ris .
• 日志采集										
▼ 系统管理	SU会话	已退出进	SSHC]	Wind	计算机试	筹选半台	send	cti	rsyn	已创建新
用户管理	4622	9999+	9999+	9999+	9999+	9999+	9999+	9999-	+ 9999+	9999+
五條參数	近7日:4622	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+	近7日:9999+
内置対象										
升级管理	里点设备				配置	里点资产 🕜				R:E
许可证管理	4 172.16.0.193				1508611	资产名称	风险等	報 告	管分布	
云端配置	172.16.0.10				231048	172.16.0.10	无	C		
云端升级	- -				0550					
业务配置	Lag 1/2.16.0.111				8008					
金和谷澤										
系统巡检										
	内部互连威胁		内部威胁分	怖		外部安全				全部、

SUPPORT	用户名 

# 4.11. 业务配置管理

配置管理功能即是可将当前系统环境信息中,自定义信息完整导出,可在新环境导入,以做 环境迁移。

配置导出:

**e** Cloud

导航菜单	业务配置
> 安全概题	• 友護爆示该功率円述用于新統的产品和进行系统恢复指的产品         ×         ×         ×
<ul> <li>安全监控</li> </ul>	导入业务经营
<ul> <li>日志查询</li> </ul>	◆ 配置文件 请法报文件 書標文件 留 导入配置
> 报表管理	
▶ 策略管理	9.11.25克西
> 资产管理	200 <sup>2</sup> 82 m 2 82
▶ 日志采集	
▼ 系统管理	
用户管理	
日志管理	
系统参数	
内置对象	
升级管理	
许可证管理	
云调配置	
云端升段	
M SIGN	
C PYMIE	
新作品加合	
and the second s	

### 点击导出配置按钮,下载获得

导航菜单	业务影響
> 安全概范	<ul> <li>          ま機構示法功調内透明手新練的产品和出行系統恢复成的产品      </li> </ul>
<ul> <li>安全监控</li> </ul>	导入业务配置
<ul> <li>日志查询</li> </ul>	◆ 配置文件 清压淬文件 割拌文件 目 与入配置
<ul> <li>报表管理</li> </ul>	
> 策略管理	导动业务配置
资产管理	
▶ 日志采集	
▼ 系统管理	
用户管理	
日志管理	
系统参数	
内置对象	
升级管理	
许可证管理	
云端配置	
云端升级	
业务配置	
系统配置	
来時官理	
<b>第4303</b> 四十至	
©2017-2019 深值服科技股份有限	公司問題が所有 問題が行う、戦止2019-10-24 曲頼版本: 3.0.4
las_config_export.zip	金都显示 X

配置导入:

在新的环境中打开此界面即可导入下载的配置数据。导入成功后,系统将会自动重启。

导航菜单	业务处理	
• 安全概范	◎ 友情描示:该功能只适用于新闻的"是科型任何系统优型系的" ● 品	×
・ 安全监控	每入 <u>业务起来</u>	
<ul> <li>日志查询</li> </ul>	● 配置文件 通信外文件 通信文件 罰 导入配置	
▶ 报表管理		
> 策略管理	导出业务公司	_
> 资产管理	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
<ul> <li>日志采集</li> </ul>		
▼ 系统管理		
用户管理		
日志普理		
系统参数		
内置对象		
2710/2012		
大端配置		
云端升级		
业务配置		
系统配置		
集群管理		
系统巡检		

# 4.12. 运维日志下载

如设备出现故障,可在个人工作台中下载运维日志,下载方式如下图标识:

▼ 安全概范	整体状况 事	件分析 审计分析	告警概兄	系统状态							
> 安全监控	概况分布										
<ul> <li>日志査询</li> </ul>	生数		- +	11×11×11		市计事件			Π±		
▶ 报表管理	1		<u> </u>			ф, ј <del>у</del> ј т			E2	002	ンイ
> 策略管理	-		<u> </u>	. 2		4			55	903	
> 资产管理	重点关注日志Top10										用户名: 系统管理员
<ul> <li>日志采集</li> </ul>		_									所属用户组: 超级管理员组
> 系统管理	SU食語	已退出进	SSH[]	Wind	send	cti	rsyn	119981245		算选平台	电话号码:
	258 逝7日:258	<b>397</b> 逝7日: 397	<b>250</b> 逝7日:250	<b>157</b> 近7日:157	<b>98</b> 运7日:98	<b>62</b> 逝7日:62	<b>45</b> 逝7日:45	<b>24</b> 逝7日:24		13 逝7日:13	邮稿: juminfo@1
											手机号码:
	重点设备				配置	重点资产 🕜					修政密码
											<b>企</b> 选指导
	172 16 0 193				3969	Very day day of the		- 40			2012/2017/2
	172.16.0.193				3969	资产名称	风险等	级	告誓分布		下载运维日志
	172.16.0.193 172.16.0.10				3969 374	<b>资产名称</b> 172.16.0.10	风险等	极	告誓分布 ① ①	0	工業运進日志
	<ul> <li>172.16.0.193</li> <li>172.16.0.10</li> </ul>				3969 374	资产名称 172.16.0.10	风险等	级	告誓分布 ① ①	0	下戰运進且志注將
	172.16.0.193 172.16.0.10				3969 374	资产名称 172.16.0.10	风险等	极	告替分布 ① ①	0	下重运弹且志 注例
	<ul> <li>172.16.0.193</li> <li>172.16.0.10</li> </ul>				3969 374	资产名称 172.16.0.10	风险器		告誓分布 (1) (1)	0	Induinte 下數這進品素 注例
	<ul> <li>172.16.0.193</li> <li>172.16.0.10</li> </ul>				3969 374	资产名称 172.16.0.10	风始制	级	告替分布 ① ①	0	Induitor 王致道道王王 注例
	□ 172.16.0.193 □ 172.16.0.10 □ 172.16.0.10 □ 0.001		内海	运动外东	3969 374	资产名称 172.16.0.10	风险器	题	告替分布 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		<u>工程道理日本</u> <u>工程道理日本</u> 注例

# 4.13. 常用配置命令

## 常用命令:

用户可以使用命令行对系统进行简单管理(使用 ssh 登录),初始用户名和口令分别为 syscli、Test@123,界面如下:



输入相应序号,则可进入相应选项

1、 User Account Setting: 用户账号设置, 用于修改 CLI 用户密码, 根据提示修改密码:

```
old password:
new password:
repeat the new password:
```

2、 Component Status Query: 查看系统组件状态:

```
data_analyser 0k! PID:[2599]
business_manager 0k! PID:[2704]
response_center 0k! PID:[2883]
file_store 0k! PID:[3491]
database 0k! PID:[2102]
web_server 0k! PID:[28985]
collector 0k! PID:[26844]
Done.
```

- 3、 Component Restart: 组件重启:
- 4、 System Shutdown: 关机:
- 5、 System Restart: 设备重启:



- 6、 Enter Console: 输入管理员密码, 进入系统后台:
- 7、 Reset WEB\_User:admin password: 重置 WEB 管理员密码:



8、 Reset WEB\_Manager:admin password: 重置管理控制台密码:

```
Rest AdminUser password
new password:
repeat the new password:
```

- 9、 Version: 查看版本号:
- 10、 Running Time: 查看系统运行时间:



- 11 Show the beginning: 查看开机时间:
- 12 Show network :



13 Setup IP address (工作口配置任何网口都可用于流量接入口使用):



14 Setup IPV6 address: 修改 IPV6 地址:

**e** Cloud



15 Change Console access port:修改硬件管理平台访问端口:



16 Change WEB access port: 修改 web 访问端口:



# 5 实施后设备运行检查

## 5.1 整体运行状态检查

## 一、基础检查

操作方法:

1、在"安全概览"->"系统状态"查看设备运行时间、CPU、内存、硬盘利用率 :

 
 整体状况
 事件分析
 审计分析
 告警概况
 系统状态
 o 2 🤣 重启 业务管理器 🤣 重启 数据存储 🧱 存储计算 数据分析器 🤣 重启 响应中心 IP地址: 172.16.0.155 **IP地址:** 172.16.0.155 IP地址: 172.16.0.155 存储已用: 3G/150G(2%) 运行状态:运行正常 运行状态: 运行正常 运行状态:运行正常 **历史数据:** 1天 网络吞吐(pp 网络吞叶(fp: 网络吞吐化 • 总量: 0.18 Mbps • 总量: 0.12 Kpps 网络吞吐: 21 fps 运行组件: 数据分析器 采集控制器 响应中心 业务管理器 采集器 流量引擎 服务器名: localhost.localdomain[172.16.0.155] はた体田住口 运行时间: 0天0小时44分钟

运行状态:	采集控制器运行正常						9.86/190.	日元 17GB (5.18%)			
			CPU								100%
CPU											
3 %											
RAM											
7.48/7.81GB(96%)											
Swap											
1.23/8GB(15%)											
											<u> </u>
			•								
工作网卡											
同卡 🔺	MAC地址	\$ 运行状态	MTU	接收包装	改 🔶 发送包数	÷ +	丢包数 🔶	接收字节	\$ 发送字节	\$	速率 🔶
eth0	52:54:00:87:29:F1	UP	1500	23459	1714674		0	39263259	736832322		100Mb/s
显示 10 🔻 条记录				显示1到13	も1条记录					« <	1 > »

2、在菜单日志采集查看采集器运行状态:

导航菜单	日志采集					
<ul> <li>安全概認</li> </ul>	采集控制器 存储配置					
<ul> <li>安全监控</li> </ul>	本 下核NXLog客户端:NXLog是一行	・ 日志牧隼工具,用于Windows日志採集 よNXLog客户演				×
<ul> <li>日志查询</li> </ul>	妥告於創業/172 16 0 154)[注司告	501				
▶ 报表管理	Hereit 2 - 2100 (21 - 1)	251 251 0/24 \$5%77% 10	法行建办 运行正义		2198	and the
策略管理	ABALLAX, UKEPART-10.	2312310/27, 4029/30-10			BCEL	重后 励味
<ul> <li>资产管理</li> </ul>	🖕 新増 🕨 启用 📕 停用					
▼ 日志采集	序号 📃	组件名称	类型	地址	运行状态	操作
• 系统管理	1	comm_nowEngine	が重り厚	172.16.0.154	西行止常	
	2	172.16.0.10	●件采集器(SYSLOG)	172.16.0.154	运行止常	
	3	sangtorad	墨件采集器(SYSLOG)	172.16.0.154	运行止常	
	4	WAF	夢件采集聲(SYSLOG)	172.16.0.154	运行正常	<b>* *</b>
	5	wmi	事件采集器(WMI)	172.16.0.154	运行正常	2 * *
	6	file	事件采集器(FILE)	172.16.0.154	运行正常	2 * 2
	7	MySQL	事件采集器(DATABASE)	172.16.0.154	运行正常	<b># X</b>
	显示 100 v 条记录		显示 1 到 7 共 7 条记录			« < 1 > »

二、检查标准:

大異し e Cloud

- 1、检查个组件运行是否正常;
- 2、硬盘利用率低于 80%是正常的, 高于 80%则会自动清理硬盘;
- 3、CPU 和内存稳定运行时不高于 80%是正常的, CPU 或内存达到 80%以上, 需要关注:
- ①设备是否正在高 EPS 的情况下接收日志: EPS 越高, CPU 利用率会越高。

# 5.2 设备日志检查

#### 一、基础检查

操作方法:

- 1、登录管理控制台 WEB 页面。
- 2、点击"系统管理"->"日志管理"。

导航菜单	日志管理				
<ul> <li>安全概范</li> </ul>	用户日志	系统日志			-
<ul> <li>安全監控</li> </ul>	用户日志列表				Q
<ul> <li>日志查询</li> </ul>	友情提示:	导出全部日志可能数	<b>原巨大,请输入查询条件后再导出。</b>		×
▶ 报表管理	🕗 导出 🕶				
▶ 策略管理	序号	日志级别	日志内容	♦ 日志产生时间	•
》资产管理	1	信息	来目客户端(172.16.0.26),用户(系统管理员)登录系统成功	2019-07-25 05:49:40	
<ul> <li>日志采集</li> </ul>	2	信息	来目晷户端(172.16.0.26),用户(系统管理员)登录系统失败	2019-07-25 05:49:33	
▼ 系统普理	3	信息	来自客户簿(172-16.0.28),用户(系统管理员)登录系统成功	2019-07-25 05:46:04	
用户管理	4	信息	来目客户端(172.16.0.26),用户(系统管理员)登录系统成功	2019-07-25 05:39:55	
日志普理	5	信息	来目響戶端(172.16.0.28),用户(系統管理员)超时還出系统	2019-07-25 04:42:07	
系统参数	6	信息	来自客户舖(172.16.0.28),用户(氢纯管理员)待处理告誓列表	2019-07-25 04:04:43	
内置对象	7	信息	来目客户端(172.16.0.28),用户(系统管理员)待处理告誓列表	2019-07-25 04:04:38	
升级管理	8	信息	来目晷户端(172.16.0.28),用户(系统管理员)新增事件过速策略	2019-07-25 03:42:39	
许可证管理	9	信息	来自客户端(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:39:22	
云端配置	10	信息	来自客户端(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:34:02	
云端升级	11	信息	来自客户诫(172.16.0.28),用户(系统管理员)事件查询	2019-07-25 03:29:56	
业务配置	12	信息	来自客户端(172.16.0.28),用户(系统管理员)修改采集器	2019-07-25 03:28:15	
系统配置	13	信息	来自客户端(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:26:19	
集群管理	14	信息	来自齋戶請(172.16.0.26),用戶(系統管理员)超时退出系统	2019-07-25 03:22:39	
系统巡检	15	信息	来自喜户涛(172.16.0.28),用户(系统管理员)修改采集器	2019-07-25 03:22:14	
	16	信息	来目客户端(172.16.0.28),用户(系统管理员)新增采集器	2019-07-25 03:15:33	
	显示 100 - 第	条记录	显示 1 到 40 共 40 条记录 (实际查询到 40 条)	« (	1 > >

这里记录了系统各组件的运行日志,包括异常故障日志。

### 二、检查标准:

1、检查系统日志里是否有异常日志,系统运行的日志都会在这里显示。

## 5.3 主要功能使用情况检查

### 一、基础检查

操作方法:

- 1、登录管理控制台 WEB 页面。
- 2、查看"日志查询"->"日志列表"是否有设备日志。
- 3、查看"日志查询"->"关联事件"是否有匹配关联策略的关联事件产生。
- 4、查看"日志查询"->"审计事件"是否有匹配审计策略的关联事件产生。
- 5、查看"安全概览"下各个仪表盘是否有相应的统计报告产生。

#### 二、检查标准:

操作方法:

1、事件列表展示系统接收到的设备日志。

Cloud

- 2、关联事件列表展示符合关联策略的关联事件。
- 3、审计事件列表展示符合审计策略的审计事件。
- 4、安全概览下个仪表盘显示正常,统计数据正确。