

日志审计系统

用户使用指南

天翼云科技有限公司



■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有特别注明,版权均属 北京天翼云科技有限公司(简称天翼云)所有,受到有关产权及版权法保护。任何个人、机构未经天翼 云的书面授权许可,不得以任何方式复制或引用本文的任何片断。

■ 内容声明

您购买的产品、服务或特性等受合同和条款的约束,本文档中描述的部分功能可能不在您的购买或使用 范围之内。

本文档仅作为使用指导,实际产品可能会由于版本升级或其他原因,与文档描述有略微差异。

■ 免责声明

在使用产品之前,请详细阅读免责声明,一旦开始使用,即认可和接受本声明的全部内容。在使用过程中,天翼云不对以下情况承担任何责任:

- 因系统运维或管理人员未及时处理影响系统稳定性和可用性的告警,而造成的数据损失、系统可用 性降低等情况。
- 因业务量超过所规划硬件能力而造成的数据损失、系统可用性降低等情况。
- 因自然灾害(包含但不限于水灾、火灾、地震等)或外部原因(包含但不限于断网、断电等)而造成的数据损失、系统可用性降低或不可用等情况。

■ 格式约定

- 粗体字:菜单、命令和关键字
- 斜体字: 文档名、变量



说明:对描述内容的补充和引用信息



- 提示:使用设备时的技巧和建议
- - **注意**: 需要特别注意的事项和重要信息



警告:有可能造成人身伤害的警告信息





内容简介

章节	概述
1 设备简介	介绍 LAS 的产品简介。
2 设备管理方式	介绍 LAS 的两种管理方式和证书相关介绍。
3 帐号管理	介绍标品和涉密版的用户帐号管理方法。
4 系统配置	介绍主要的系统配置和网络配置方法。
5 日志接入	介绍各类日志接入的配置方法。
6 数据源	介绍数据源的管理操作方法。
7 枚举值	举例介绍枚举值的配置方法。
8 采集终端	介绍数据采集终端(采集器、天翼云设备和 Agent)的配置方法。
9 规则管理	介绍数据采集规则的配置方法。
10 资产管理	介绍资产的配置方法和管理方法。
11 日志分析	介绍日志信息的检索方法和日志监控信息的查看方法。
12 日志源管理	介绍日志源监控信息的查看方法和日志源拓扑的配置方法。
13 事件告警	举例介绍设备接入以及相关事件告警的查看方法。
14 报表管理	介绍报表的生成方法和管理方法。
15 数据管理/备份恢复	介绍数据备份、数据恢复、磁盘扩展、NFS 配置、超限管理和一键备机的操作方法。
16 消息中心	介绍系统消息的查看方法。
A 通信矩阵	介绍 Agent 支持的操作系统。

修订记录

日期	修订版本	修改记录
2025 01 22	02	1、系统配置-网路配置说明更新
2023-01-23	02	2、系统配置-取消短信和邮件服务器



日期	修订版本	修改记录
2024-04-25	01	初次发布。





1	设备简介	1
2	设备管理方式	2
	2.1 Web 管理	2
	2.1.2 Web 页面布局	2
	2.1.3 配置流程	.3
3	帐号管理	4
	3.1.1 创建用户帐号	.5
	3.1.2 查看用户帐号信息	6
	3.1.3 修改用户帐号信息	8
4	系统配置	9
	4.1 网络配置	.9
	4.1.1 配置网络接口	.9
	4.1.2 配置网络路由1	10
	4.2 NTP 配置1	1
	4.3 通知配置(FTP/SFTP 配置)1	.2
5	日志接入1	.4
	5.1 自动接入1	4
	5.2 天翼云设备日志接入1	17
	5.3 第三方安全设备/网络设备接入1	9
	5.3.1 场景1	9
	5.3.2 配置思路1	9
	5.3.3 配置步骤2	20
	5.3.4 结果验证2	21
	5.3.5 日志范式化说明	21
	5.4 Linux 主机日志接入3	32
	5.5 Windows 主机日志接入	35
	5.6 Web 服务器日志接入3	36
	5.7 数据库接入4	10
	5.8 虚拟化平台接入4	13

€₹

	5.9 网络设备流量接入	47
	5.10 文件日志接入	49
	5.11 其他日志接入	51
	5.12 主机审计日志接入	
	5.13 NAT 配置	
6	数据源	
	6.1 查看统计信息	60
	6.2 查看数据源处理信息	63
	6.3 数据源管理操作	63
	6.3.1 查询数据源	63
	6.3.2 编辑数据源	64
	6.3.3 删除数据源	64
	6.3.4 启用/停用数据源	65
	6.4 配置数据源	66
7	枚举值	
8	平隹终端	72
U	8.1 Agent	
	8.1.1 下载 Agent	
	8.1.2 安装 Agent	74
	8.1.3 查看 Agent	75
	8.1.4 数据采集配置	
	8.1.5 启用/禁用 Agent	
	8.1.6 升级 Agent	78
	8.1.7 强制更新 Agent	78
	8.1.8 卸载 Agent	79
	8.1.9 删除 Agent	80
9	规则管理	
10	0 资产管理	
	○ 欸/ 日·至···································	
	10.1.1 新建资产	
	10.1.2 资产导出	
	10.1.3 资产导入	
	10.2 资产发现	
	10.2.1 场景	
	10.2.2 配置步骤	87
11	1 日志分析	89



	11.1 日志检索	
	11.1.1 日志基本/高级搜索	
	11.1.2 快捷检索配置	
	11.1.3 保存检索条件	
	11.1.4 历史日志检索	
	11.1.5 快捷检索日志	
	11.1.6 重点关注日志	
	11.1.7 日志管理操作	
	11.2 主机审计分析	96
	11.3 Web 服务器日志分析	
	11.4 自定义仪表盘	
12	日志源管理	
	12.1 日志源监控	
	12.1.1 采集器维度日志源监控信息	
	12.1.2 资产维度日志源监控信息	
	12.2 采集资产监控	
	12.3 日志源拓扑	
13	事件告警	
14	报表管理	
14	报表管理 14.1 我的报表	
14	报表管理 14.1 我的报表 14.2 报表任务	112
14	报表管理	
14	报表管理	
14	报表管理	112
14	报表管理	112
14	报表管理	112
14	报表管理	 112
14	报表管理	112
14	 报表管理	
14	 报表管理	112 112 113 113 113 113 113 113 113 113 113 113 113 113 114 115 116 117 116 117 119 119 120
14	报表管理	112 112 113 113 113 113 113 113 113 113 113 113 113 114 115 116 117 119 119 120 121
14	报表管理 14.1 我的报表 14.2 报表任务 14.2 报表任务 14.2.1 新建报表任务 14.2.2 管理报表任务 14.3 模板管理 14.3.1 新建报表模板 14.3.2 管理报表模板 15.1 备份恢复 15.1.1 日志备份 15.1.2 日志恢复 15.1.3 文件备份 15.1.4 文件恢复	112 112 113 113 113 113 113 113 113 113 113 113 113 113 114 115 116 116 117 119 119 120 121
14	报表管理 14.1 我的报表 14.2 报表任务 14.2.1 新建报表任务 14.2.2 管理报表任务 14.2.2 管理报表任务 14.3 模板管理 14.3.1 新建报表模板 14.3.2 管理报表模板 15.1 备份恢复 15.1.1 日志备份 15.1.2 日志恢复 15.1.3 文件备份 15.1.4 文件恢复 15.2 磁盘扩展	112 112 113 113 113 113 113 113 113 113 113 113 113 113 113 113 113 115 116 116 117 117 119 119 120 121 121 121
14	报表管理 14.1 我的报表 14.2 报表任务 14.2 报表任务 14.2.1 新建报表任务 14.2.2 管理报表任务 14.3 模板管理 14.3.1 新建报表模板 14.3.2 管理报表模板 14.3.2 管理报表模板 15.1 备份恢复 15.1 目志备份 15.1.1 日志备份 15.1.2 日志恢复 15.1.3 文件备份 15.1.4 文件恢复 15.2 磁盘扩展 15.3 NFS 配置	112 112 113 113 113 113 113 113 113 113 113 113 113 113 113 113 113 115 116 117 116 117 119 119 120 121 121 121 122
14	报表管理 14.1 我的报表 14.2 报表任务 14.2 报表任务 14.2.1 新建报表任务 14.2.2 管理报表任务 14.2.2 管理报表任务 14.3 模板管理 14.3.1 新建报表模板 14.3.2 管理报表模板 14.3.2 管理报表模板 14.3.2 管理报表模板 15.1 备份恢复 15.1.1 日志备份 15.1.2 日志恢复 15.1.3 文件备份 15.1.4 文件恢复 15.2 磁盘扩展 15.3 NFS 配置 15.4 超限管理	112 112 113 113 113 113 113 113 113 113 113 113 113 113 113 113 113 115 116 116 117 119 119 120 121 121 121 121 122 123



A	通信矩阵	126
	A.1 Agent 支持的操作系统	126





随着企业信息化的不断发展,公司信息化资产数量日趋增多、系统的关联性和复杂度不断增强,然而当前信息安全形势日益严峻,信息安全防护工作面临前所未有的困难和挑战。目前国家的政策法规、行业标准等都明确对日志审计提出了要求,日志审计已成为企业满足合规内控要求所必需的功能。日志审计能够帮助用户更好监控和保障信息系统运行,及时识别针对信息系统的入侵攻击、内部违规等信息,同时日志审计能够为安全事件的事后分析、调查取证提供必要的信息。

天翼云日志审计系统(简称 LAS)是一个综合性的日志管理平台,可有效地管理网络资产输出的各种日志数据。LAS 的功能概述如下:

- 将分散、异构的日志进行统一范式化处理,并提供多维度的分析工具,方便用户对日志 进行全面、高效地运维。
- 帮助用户发现日志中蕴含的各种安全风险,便于用户对网络中的安全问题进行定位、追踪、取证,以确保用户网络及业务的顺畅运行。



2 设备管理方式

LAS 支持以下两种管理方式:

- Web 管理 最直观的人机交互管理方式,提供最全面的功能管理界面。
- Console 管理
 通过控制台以命令行方式对 LAS 进行简单配置和管理。

本章主要内容如下:

功能	描述
Web 管理	介绍 LAS 的 Web 管理方式。
配置流程	介绍 LAS 的启用配置流程。

2.1 Web 管理

LAS 的 Web 管理系统为用户提供了更直观的人机交互方式,用户通过 Web 管理页面实现对 LAS 的管理和配置。下面详细介绍 Web 管理的登录方法、页面布局以及常用操作。

2.1.2 Web 页面布局

各功能模块的页面布局相同,示例如图 2-1 所示。





图 2-1 页面布局



编号	区域	描述
1	菜单栏/导航栏	LAS 的一级功能菜单栏。将鼠标悬停在菜单上,出现对应的二级功能菜单。
2	快捷工具栏	 从左至右的具体说明如下: ● 【 仅支持首页大屏的全屏展示,按 Esc 键可以退出全屏模式。 ● 【 记入总控制台。 ● 【 记入消息中心,红色数字表示当前未读的信息数量。 ● 【 查看关于信息和在线帮助。 ● 【 查看关于信息和在线帮助。 ● 【 包括以下两个功能。 • 屏幕锁定:将 LAS 的 Web 界面锁定,暂时拒绝其他用户登录,只能由当前登录用户登录并解锁。 • 进入用户中心:管理当前登录用户的帐号信息。对于 admin 用户,还支持对所有帐号和角色进行管理。详细功能说明请参见《天翼云日志审计系统 V2.0R00F07 用户手册》第 3 章。
3	工作区	各类功能的配置、操作、浏览都在此区域进行。 若开启告警规则,将在工作区顶部滚动展示告警信息。告警规则的配 置方法请参见《天翼云日志审计系统 V2.0R00F07 用户手册》第13章。

2.1.3 配置流程

LAS 的整体配置及使用流程建议如图 2-2 所示。具体的配置及使用方法,请参见后面的章节。



图 2-2 LAS 整体配置/使用流程



3 帐号管理

LAS 用户由系统内置账号和自定义账号组成。系统内置账号为 admin,默认用户角色为 "系统管理员"和 "业务管理员",拥有账号管理的权限。本章主要内容如下:

功能	描述
创建用户账号	介绍如何创建 LAS 用户账号。
查看用户账号信息	介绍如何查看 LAS 用户账号信息。
修改用户账号信息	介绍如何修改 LAS 用户账号信息。



3.1.1 创建用户帐号

LAS 用户帐号的创建方法如下:

- 步骤 1 使用 admin 帐号登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在快捷操作栏中的A,选择【用户中心】,进入 **帐号管理 > 帐号**页面, 如图 3-1 所示。

图 3-1 帐号列表(LAS 标品)

我的账号	账号管理					
角色	账号					
						+新建账号
账号名	用户角色	邮箱	手机号	可登陆IP	账号状态	操作
admin	系统管理员 更多 ※			****	启用	/ O 🗎 🛞
< 1 >	每页10条,共1页,到第 1	页确定				

步骤 3 单击【新建帐号】,配置帐号参数,如图 3-2 所示。

- a. 密码:支持两种设置方式。其中,默认密码为**帐号名+@123456**(例如:帐号名为 admin1, 默认密码为 admin1@123456)。
- b. 可登录 IP 范围: 支持 IPv4 和 IPv6, 填写格式详见页面提示。



图 3-2 创建用户帐号(LAS 标品)

□ 账号新建			×
*账号名称	admin1		
*密码	 自定义密码 」 默认密码 		
主责任人	张三		
曲即箱	zhangsan@qq.com		
手机号码	16109227890		
*角色	🗌 业务管理员 💟 审计管理员 💟 系統管理员		
* 权限	名称	✓ 授权	
	账号管理		
	系统日志		
可登录 IP 范围			
			取消 确定

步骤 4 单击【确定】按钮,完成用户帐号创建。

----结束

3.1.2 查看用户帐号信息

用户帐号新建后,查看帐号信息的操作方法如下:

步骤 1 使用新建帐号登录 LAS 的 Web 管理页面。

首次登录时,需要修改密码,再重新登录,如图 3-3 所示。



图 3-3 首次登录修改密码(LAS 标品)

	2
旧密码	•
	● 密码可输入大小写英文字母、数字和特殊字符(~!@#\$%^&*()_++=),7 可包含用户名
新密码	请输入密码
确认新密码	请再次输入密码

步骤 2 密码修改成功后,重新登录 LAS 的 Web 管理页面,如图 3-4 所示。

	admin1	
	9wd	9 X v F 1174. 16-11 18 18
-		

图 3-4 Web 登录页面(LAS 标品)

步骤 3 将鼠标悬停在快捷操作栏中的A,选择【用户中心】,默认进入 我的帐号 页面,如 图 3-5 所示。

图 3-5 查看当前登录用户的帐号信息(LAS 标品)

100KG <mark>KGW</mark> H		
•	🛓 主責任人: admin1	â fini: (Komaz) (Burnaz)
admin1	🐱 前称:	0 服马属性: 前定义所导
	€ 手机号码:	IP 可登录 IP 范围: *****
	4、权限:《原母音录》《系统日志》	
	聚号体度 已设备 882	
	完美的际号信息可以将有更丰富更安全的功能体验。建议切能体及对先3	於号信息,於号信息此成,手引号,如何,可整是外王副等。
	会員案码 已设置 ● 時間 ※会社部地球部門(1年)4日第4会 時代が空間第3点中間	
	10000100 この2011月1日日 清仲本地以近、本地以近 + 近地以近 (uKey 以近) 、同种健長方式	



----结束

3.1.3 修改用户帐号信息

查看用户帐号信息 时,支持修改帐号信息、登录密码和登录方式。

修改帐号信息

如图 3-6 所示,包括邮箱、手机号码、可登录 IP 范围。

图 3-6 修改用户帐号信息(LAS 标品)

账号信息 设置中 修改	
完善的账号信息可以拥有更丰富更安全的功能	能体验,建议您能够及时完善账号信息。账号信息包括:手机号、卸箱、可登录时范围等。
自3箱	
手机号码	
可登录 iP 范围	
	取消 藏定

修改登录密码

如图 3-7 所示,建议定期更换登录密码,密码规则请参见页面提示。

图 3-7 修改用户帐号登录密码(LAS 标品)

登录家码 设置中 修改	
安全性高的密码可以便账号更安全,建议您	定期更佳密码。
旧密码	
	● 密码可输入大小写英文字母、数字和构称字符(1@#\$%^&℃_+-=),不可包含用户名
新密码	请输入密码
确认新密码	请再次输入密码
	取消 确定

修改登录方式

若要将登录方式改为**本地认证+证书认证**,操作方法如下:

- **步骤 1** 在 LAS 设备插入 uKey。
- 步骤 2 选择认证方式为"本地认证+证书认证",单击【确定】按钮,如图 3-8 所示。



图 3-8 修改用户帐号登录方式(LAS 标品)

登录方式 《登中_ 侍欲			
提供本地认证、本地认证 + 证书认证(uKey 认证),两种登录方式			
认证方式 💿 本地认证 🔷 本地认证 + 证	书认证 (uKey 认证)		
取消 稀定			

- 步骤 3 切换成功后退出登录。
- 步骤 4 再次登录时,客户端需要插入对应的 uKey 并安装认证程序。

----结束



本章介绍 LAS 运维管理的相关操作,主要内容如下:

功能	描述	
网络配置	分别介绍 LAS 硬件版、软件版和虚拟化版的网络配置方法。	
NTP 配置	介绍 LAS 的时间同步配置方法。	
通知配置(FTP/SFTP 配 置)	介绍 SFTP/FTP 服务器的配置方法。	

4.1 网络配置

4.1.1 **配置网络接口**

接口默认为 dhcp 不建议更改

网络接口的配置方法如下:

- 步骤 1 使用单点账号登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标³,进入 系统配置 > 网络配置 > 网络接口 页面,如图 4-1 所示。



图 4-1 网络接口列表

系統配置	
日志分析 「网络配置」「阿哈路田」	37/10HCP
日志渡管理 资产配置	
事件活答 * <u>当地配置</u>	虚拟化环境下,开启 DHCP, 前端页面配置网络不可操作,可以选择 关闭 DHCP, LAS 的 IP 恢复到10.1.1.1,页面将会强制退出
报表管理 · 安全配置	
· 统计管理 _ 统计管理	
速归配置	
NTP 配置	
SNMP 配置	
安全中心	

在如图 4-1 所示的页面中,单击【打开 DHCP】按钮,确认提示框中的信息后单击【确 认】按钮,即可开启 DHCP 功能。开启后,LAS 将自动分配平台 IP、网关和掩码信息。



----结束

4.1.2 配置网络路由

配置 LAS 网络路由的具体操作如下:

将鼠标悬停在总控制台图标^Ⅲ,进入 **系统配置 > 网络配置 > 网络路由**页面,初始状态下,只有默认路由。单击【新建】按钮,配置静态路由参数,参数说明如表 4-1 所示。 新建静态路由后,可以进行编辑和删除等操作。默认路由不支持编辑和删除。

配置项	描述
路由名称	填写静态路由的名称,取值范围为 1~20 个字符。 不能包含\/:* ?"<> =@#\$%^&;()'[]和空格等特殊字符。
目的 IP 地址	数据包要被送达的目的主机或目的网段的 IP 地址。支持 IPv4 和 IPv6。
子网掩码/IPv6 前缀	 若目的 IP 地址为 IPv4,填写数据包要被送达的目的主机或目的网段的子网 掩码。 若目的 IP 地址为 IPv6,填写数据包要被送达的目的主机或目的网段的 IPv6 前缀。IPv6 前缀的取值范围为 0~128 的整数。
度量	填写静态路由的度量值。取值范围为 1~9999 的整数。 度量值越低,优先级越高,优先使用度量值小的路由转发数据包。
路由类型	选择配置网关路由或接口路由。
网关地址	填写静态路由的网关地址,通常为下一跳设备的入口IP地址。支持IPv4和IPv6。
接口名称	从下拉菜单选择要配置路由的接口。



4.2 NTP 配置

将鼠标悬停在总控制台图标[€], 进入 系统配置 > NTP 配置 页面, LAS 支持三种时间同 步方式:

- 周期同步: LAS 平台周期性的与时间服务器进行同步, 如图 4-2 所示。
- 立即同步: LAS 平台立即与时间服务器进行一次同步, 如图 4-3 所示。
- 校正时间:手动配置 LAS 平台的时间,如图 4-4 所示。

图 4-2 NTP 配置(周期同步)

■ NTP 配置	
	O 2023-02-22 20:57:33
* 同步方式	 周期同步 立即同步 校正时间
* 启动周期同步	 ● 是 ○ 否
*同步周期	每天次 🗸 🗸 🗸
* 主服务器	ntp1.aliyun.com
备服务器	
	应用配置

图 4-3 NTP 配置(立即同步)

ID NTP 配置	
	Q 2023-02-22 20:57:51
*同步方式	○ 周期同步 ● 立即同步 ○ 校正时间
* 主服务器	ntp1.aliyun.com
备服务器	
	应用偏置



图 4-4 NTP 配置(校正时间)

		Ø 2023-02-2	22 20:58:06								
*	同步方式	○ 周期同步	○ 立即	司步 💿 校正	时间						
*	校准时间	2023-02-2	2 20:54:46								#
		应用配置			已选择	2023	-02-22	20:54:	46		确定
					<		-	月 202	23		>
					B		Ξ	Ξ	四	五	六
								1	2	3	4
					5	6	7	8	9	10	11
					12	13	14	15	16		18
					19				23	24	25
					26	27	28				
							时间	20:54	:46		
					时:	C				-	D

4.3 通知配置(FTP/SFTP 配置)

场景

若要将文件/数据上传至 SFTP/FTP 服务器进行备份,需要在 LAS 中对 SFTP 或 FTP 服务器进行配置。

配置步骤

SFTP/FTP 服务器的配置方法如下:

- 步骤 1 使用 admin 帐号登录 LAS 的 Web 管理页面。
- 步骤 2 将鼠标悬停在总控制台图标³³³,进入 系统配置 > 通知配置 > SFTP 服务器 页面,如图 4-5 所示。

图 4-5 SFTP/FTP 列表(初始状态)

□ 通知配置					
邮件服务器	短信服务器	SFTP 服务器			◆新建 SFTP
连接类型	名称	主机地址	备注	内容	操作
			1 智无数据		

单击【新建SFTP】按钮,在弹出的提示框中单击【已知晓】。



步骤 3 配置 SFTP/FTP 服务器参数,如图 4-6 所示。

□ 编辑	×
连接类型	● SFTP ○ FTP
*名称	SFTP
* 主机地址	10.65.189.157
*服务端口	22
号测氛登	root
* 密码	请输入用于登录该 FTP 的密码
上传模式	● 被动模式 ○ 主动模式
存储路径	Ĩ
备注	请输入该服务器的备注信息,不超过255个字符
	取消 确认

步骤 4 单击【确认】按钮,返回 SFTP/FTP 列表,如图 4-7 所示。

图 4-7 SFTP/FTP 列表 (完成配置)

邮件服务器	短信额务器 SFTP 服务器				+新建 SFTP
连接类型	名称	主机地址	备注	内容	操作
SFTP	SFTP	10.65.189.157		sftp://root*****@10.65.189.157:22/	1 8 %

- **步骤 5** 在 SFTP/FTP 列表中,单击操作列的¹,进行连通性测试,检验服务器网络是否可达。 连通性测试过程中,不可进行编辑和删除操作。
- 步骤 6 SFTP/FTP 服务器的连通性测试成功,完成配置。

----结束

图 4-6 配置 SFTP/FTP 服务器



5 _{日志接入}

日志接入是指接入各种日志对象,日志对象即按照日志来源进行分类的日志。

功能	描述
自动接入	以自动接入第三方安全设备的日志为例,介绍LAS自动接入日志的操作方法。
天翼云设备日志接入	介绍 LAS 接入天翼云安全设备日志的操作方法。
第三方安全设备/网络设备 接入	介绍 LAS 接入第三方安全设备的配置方法、验证方法和日志范式化方法。
Linux 主机日志接入	介绍 LAS 接入 Linux 主机日志的操作方法。
Windows 主机日志接入	介绍 LAS 接入 Windows 主机日志的操作方法。
Web 服务器日志接入	介绍 LAS 接入 Web 服务器日志的操作方法。
数据库接入	介绍 LAS 接入数据库数据的操作方法。
虚拟化平台接入	介绍 LAS 接入虚拟化平台日志的操作方法。
网络设备流量接入	介绍 LAS 接入网络设备流量的操作方法。
文件日志接入	介绍 LAS 接入文件日志的操作方法。
其他日志接入	介绍 LAS 接入其他日志的操作方法。
主机审计日志接入	介绍 LAS 接入主机审计日志的操作方法。
NAT 配置	介绍 NAT 配置的操作方法。

本章主要内容如下:

5.1 自动接入

以自动接入第三方安全设备的日志为例,配置方法如下:

步骤 1 登录 LAS 的 Web 管理页面。



步骤 2 将鼠标悬停在总控制台图标³³³,进入 **数据采集 > 日志接入**页面,展示接入日志对象的入口,如图 5-1 所示。

图 5-1 日志接入

请您选择接入对象。			
天现云安全设备日志 接入天调云和HBS的全设路日志,StIWAF、IPS/IDS、NF等设备	プ 第三方安全设备日志 扱入其它安全厂商的安全设备日志,如 WAF、IPS/IDS等	開始現象日志 時間の調波(地)人 (文実明、海由線、DNS、GTM/LTM)的日志 信号可調波(地)人	数据库数据 通过 JDBC 的方式主接到数据库管理系统,以拉案指统的数据
Windows 主机序件日志 風江茨県口市市準備 Agent 接入 Windows 2008、Windows 7 】 学生広報局であ	入 Linux 主机系统日志 遠江デ第三日志洋県 Agent 接入 Linux 包没行数本的系统日志	そ web 服务器日志 測定支援正日志来編 Agent 施入 Web 服务器产生的功利日志、 病現日を	▲ 直現化平分日志 除人系者素化不可約字型的日本
 	<u> 身に日あ</u> 可後入其它返用程序、中尚件、业务系统等产生的日志	♥ 文件日志 手动上何文本文件日巻	

- **步骤 3**(可选)单击"请您选择接入对象"的♥♥,设置禁止接入的 IP 范围,设定范围内的日 志源日志将不被自动接入 LAS。
- 步骤 4 第三方安全设备日志自动接入配置。
 - a. 在如图 5-1 所示的界面中,开启第三方安全设备日志的自动接入功能,如图 5-2 所示。

图 5-2 开启第三方安全设备日志的自动接入

请您选择接入对象。	
天翼云安全设备日志 接入天翼云科技的安全设备日志,如WAF、IPS/IDS、NF 等设备	▼ ● <

- b. 设置端口号并开启配置后,单击操作栏的,如图 5-3 所示。
- c. 单击【确认】按钮,完成自动接入配置。



图 5-3 第三方安全设备日志自动接入配置

	【第三方安全设备日志】 自	动接入配置					×
#	端口号		是否开启		操作		
1	88		● 开启	() 关闭	+		
0	不同接入对象可配置同一端 1、端口:日志发送的指定。 2、端口启用:端口开启,3 3、端口禁用:端口禁止对施 4、当自动接入端口已存在3	亂口,也可配置不同端口 ,其中: 滿口需与自动接入配置端口保持一致 对应接入对象日志自动接入,开始监听 应接入对象自动接入 真实数据源时,不再创建虚拟数据源	读取数据并进行	, 规则匹配,	匹配成功完成自动接入		
						取消	确认

步骤 5 进入 数据采集 > 数据源 页面,可以查看已自动接入的数据源,如图 5-4 所示。

图 5-4 自动接入的数据源

補选 达乐学业品水业后该学业品上的政策图		•			更多操作・
▲第三方安全设施日表_08	0/s 5842	*	0/5 70302	三位理(1) 水(2)(3) 編新先数(1)	=

步骤 6 单击数据源名称,进入该数据源的详情页,如图 5-5 所示。

当配置的 88 端口有日志上报时,自动接入产生日志的第三方安全设备,如图 5-6 所示。

图 5-5 数据源详情

					◆ 通回上级
第三方安全设备日志_88 10.65.189.175 (CU:10	1.65.189.175)				
他入政告 地入政策					
语输入关键问题词				配册后并规则	配置 日井和田
# 设备IP	厂商	关型	型号/版本		操作
1 🔺 255.255.255.255	42	Everal .	F01		τ α

图 5-6 数据源详情(有日志上报)

□ 数据影样情					▶ 美国上级
第三方安全设备日志_88 10.65.189.	.175 (CU:10.65.189.175)				
後入設備 接入配置					
语能入关键现查询				ERSARI	000000774000
# (段盤HP	Fai	类型	型号/版本		30/E
1 🛕 255.255.255.255	1938	dKRIR港	F01		τ 8
2 10.65.189.101	编为	AntiDDoS	8030		τ 0



----结束

5.2 天翼云设备日志接入

LAS 接入天翼云安全设备日志的操作方法如下:

- 步骤 1 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标 → 进入 数据采集 > 日志接入 页面,如图 5-1 所示。
- **步骤 3** 将鼠标悬停在【天翼云安全设备日志】,右上角浮现自动配置日志接入开关按钮,LAS 默认开启天翼云安全设备日志对象的自动配置功能,如图 5-7 所示。
 - a. 开关打开后,每当有天翼云安全设备接入,LAS可自动配置该天翼云安全设备对应的 日志来源设备,无需再按照以下步骤手动配置。
 - b. 开关关闭后,请按照以下步骤进行配置。

图 5-7 选择天翼云设备日志接入对象

请您选择接入对象。	
天翼云安全设备日志	又 第三方安全设备日志
接入天翼云科技的安全设备日志,如WAF、IPS/IDS、NF 等设备	接入其它安全厂商的安全设备日志,如 WAF、IPS/IDS等

- 步骤 4 选择采集器。
 - a. 单击【天翼云安全设备日志】,进入"已选择接入 天翼云安全设备日志"页面,如图 5-8 所示。

图 5-8 选择天翼云安全设备日志采集器

远洋安按入的木果斋	
10.65.133.3 (CU:10.65.133.3)	

- b. (可选)单击【重新选择】,返回如图 5-1 所示页面,重新选择日志的类型。
- c. 选择采集器,单击【继续】按钮。



步骤 5 配置天翼云安全设备信息。

- a. 进入"添加要接入日志的天翼云设备"页面,配置天翼云安全设备的设备 IP、设备 HASH、 设备类型和设备型号/版本,单击操作栏的➡,完成天翼云安全设备的添加,如图 5-9 所示。
- b. (可选)重复以上步骤,可以继续添加天翼云安全设备。

图 5-9 配置要接入日志的天翼云设备

					日本101年
	设备IP	设备 HASH	设备类型	设备型号/版本	18/11
3	10.65.7.120	492D-89D4-1863-ACO4	SA5-KS *	V6.0R11F00	1014 ST/8
_					
			上一步 完成输入		

- 步骤 6 单击【完成接入】按钮,完成天翼云安全设备的接入。
- **步骤 7** 进入 **数据采集 > 数据源**页面,可以查看接入天翼云安全设备的已处理日志数量,如 图 5-10 所示。

图 5-10 天翼云设备日志已接入



步骤 8 单击数据源名称,进入该数据源的详情页,如图 5-11 所示。

图 5-11 数据源详情

接入设备				
诸威人共振风致风				配置资料规则
# 设备 IP	设备 HASH	设备关型	设备型号/版本	19PT
1 10.65.7.120	492D-8904-1863-AC04	SAS-ICS	V6.0R11F00	

步骤 9 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看上一步接入天翼云 安全设备的日志详情,如图 5-12 所示。



图 5-12 已接入天翼云安全设备的日志检索

重点关注	筛选条件: 日	さば型 病毒化的日本			
Q	法律时间	〇 最近1小时 〇 最近24小时 〇 最近7天	• 最近 30 天 自定义 3分钟 V	•	
	法探测性	● 日志陽性 ○ 波介陽性			
	日志来源中		37 P		
	目的 P				
	自定文绘象	调输入张伟			
		保存检索条件		快速检索截至	抱木 売収技家 ヘ
	显示武表♥				
	最新日志数 🌒	6685 D			显示空中级 日志导出 检索结果统计
	日志来源 IP	日志产生时间	日志接收到间	日志論号	采集器编号
	10.65.7.120	2023-02-24 21:27:59	2023-02-24 21:27:59	e005b08f47714ed8b71e9372c882efdc	947A-5875-7CEA-EBE3
	10.65.7.120	2023-02-24 21:27:57	2023-02-24 21:27:57	2c27bb4a8d30404689c499d7bea38dee	947A-5875-7CEA-EBE3
	10.65.7.120	2023-02-24 21:27:55	2023-02-24 21:27:55	0b1944df884f4104a55082c13ab8fbc2	947A-5875-7CEA-EBE3
	10.65.7.120	2023-02-24 21:27:53	2023-02-24 21:27:53	eb82a8c367a94d70aadb12b8a6e85d02	947A-5875-7CEA-EBE3
	10.65.7.120	2023-02-24 21:27:51	2023-02-24 21:27:51	dc263b71c5de4e7d9129b5457b5966bc	947A-5875-7CEA-EBE3

----结束

5.3 第三方安全设备/网络设备接入

本节介绍第三方安全设备的接入方法。网络设备接入 LAS 的操作方法,与第三方安全设备的基本相同。

5.3.1 场景

第三方安全设备的示例信息如表 5-1 所示。

表 5-1 第三方安全设备接入示例

设备参数	信息
设备型号	启明星辰防火墙 3.6.0.9
设备 IP	10.65.189.101
设备 Syslog 端口	450

5.3.2 配置思路

- 确定 LAS 与第三方安全设备之间的网络连接正常。
- 确定第三方安全设备的 Syslog 端口。
- 确定第三方安全设备的版本信息。



5.3.3 配置步骤

第三方安全设备(示例如表 5-1 所示) 接入 LAS 的配置方法如下:

- 步骤 1 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标 → 进入 数据采集 > 日志接入 页面,如图 5-1 所示。
- 步骤 3 单击【第三方安全设备日志】,选择要接入的采集器,如图 5-13 所示。

图 5-13 选择第三方安全设备接入采集器

日志猿入	数振潮	枚举值	规则管理	采集终端		
-						
E	选择接	入第三	方安全设备	品日志		重新选择
					选择要接入的采集器	
					10.65.189.175 (CU:10.65.189.175)	
					現位	

步骤 4 配置第三方安全设备日志的接入方式,如图 5-14 所示。

图 5-14 配置第三方安全设备日志接入方式

已选择接入 第三方安全设备日志		重新选择
	配器接入方式	
振入协议	UDP -	0
振入地口	450	
	0 派纳施口不可占用	
截漏落式	Syslog	
批编编码	UTF-8 *	
	上一步 网络	

步骤 5 添加要接入日志的第三方安全设备,如图 5-15 所示。

图 5-15 配置第三方安全设备日志的设备信息

		添加要接入日志的第三方安全设备		
				日:南部 0 1
记备IP	厂商	送型	型号/版本	操作
10.65.189.101	启明星辰	▼ 防火増	▼ 3.6.0.9	+

步骤 6 (可选) 重复步骤 5, 继续添加第三方安全设备。

单击页面下方的【批量添加】,支持批量添加多台第三方安全设备。

步骤 7 单击【完成接入】按钮,完成第三方安全设备的日志接入,如图 5-16 所示。



图 5-16 完成第三方安全设备接入

日 地名人名法			
◎已完成接入	第三方安全设备日	志	
		第→ 第三方安全设备日志_450	
	接入更多日志	提供输入其它类型的日本以底量	
	配置委弃规则	丢弃不必要的数据,降低存储。计算资源的资度	
	搜索日志	前往最贵重看已線入的日志	
	创建统计项	前往创建更多统计项,用于生成很欢	



5.3.4 结果验证

第三方安全设备(示例如表 5-1 所示)接入 LAS 的验证方法如下:

- 步骤1 在防火墙进行产生日志的操作。
- 步骤 2 登录 LAS 的 Web 管理页面。
- **步骤 3** 将鼠标悬停在总控制台图标³³⁴,进入 数据采集 > 数据源 页面,如果数据源有接收速率和范式化速率,且存在已处理的日志数量,说明接入成功,如图 5-17 所示。

图 5-17 第三方安全设备接入 LAS 的验证

THE A P. LEWIS CO. N. LEWIS CO. CO. CO. CO.	· 输入资产	未识别日志	未知識這個語	解析失败日志	接收速率	范式化速率	入库速率
98*	3台(共3个日志源)	0 %	0 🛧	0.8	10 _{%/s}	14 8/5	0 亲/s
「「「「「「「「」」」」 「「「」」」 「「」」 「「」」 「「」」 「」」	新聞上的数据源		•				更多操作
Contraction of the local							
and Cheverge Edites		10/s			14/5	已处理 (74)	

----结束

5.3.5 日志范式化说明

对于第三方安全设备日志、网络设备日志、虚拟化平台日志和其他日志,可以按照字段 提取规则提取有效数据进行范式化,然后 LAS 对这些数据进行相应的展示。

5.3.5.1 字段提取

以第三方安全设备日志为例,同一个设备发出的日志格式不同,日志样本如下:

```
<124>Sep 10 17:33:01 H3C
data_type1=attack97;log_type1=alerti20;attack_name4=1510034030penSSL CVE-2014-0224
Man in the Middle Security Bypass Vulnerability
Scan7;app_protocol_name6=84021364HTTPS13;protocol7=656;segment_direct28=72;src_ip22
=221.122.179.191;src_port23=13450;dst_ip24=171.89.207.143;dst_port25=59627
```



<124>Sep 10 17:33:01 H3C data_type1=attack97;log_type1=alerti21;attack_name4=151003403OpenSSL CVE-2014-0224 Man in the Middle Security Bypass Vulnerability Scan7;app_protocol_name6=84021364HTTPS13;protocol7=656;segment_direct28=72;src_ip22 =221.122.179.191;src_port23=13450;dst_ip24=171.89.207.143;dst_port25=59627

字段提取规则的操作方法如下:

步骤 1 请参见 配置步骤,接入第三方安全设备,如图 5-18 至图 5-20 所示。

图 5-18 选择接入第三方安全设备日志的采集器

已选择接入 第三方安全设备日志			重新选择
	选择要接入的采集器		
	10.65.189.175 (CU:10.65.189.175)	×	
	他的		

图 5-19 配置第三方安全设备的接入方式

已选择接入 第三方安全设备日志				重新出译
		注意		
·····································	UDP	一个姚口只能以一种协议 (FTP 例外) 線入一种格式的数据!	- 0	
日本人間	38			
	0 系统第日不可占用			
此原格式	Syslog			
数运输59	UTF-8		•	
	1	步 继续		

图 5-20 配置第三方安全设备信息

E	选择接入第三方安全设备日志				重新选择
		添加	更接入日志的第三方安全设备		
-					已添加1台
	设备IP	厂商	类型	型号/版本	操作
1	10.65.68.108	厂商doc	授型doc	뤏号doc	/ 0
2	请输入设备P	请输入或选择厂商	清输入或选择供型	请输入或选择型号/版本	+
					批量添加
			上一步 完成输入		

步骤 2 完成第三方安全设备日志接入后,单击设备列表操作栏的【立即提取】,如图 5-21 所示。



图 5-21 立即提取字段

□ 接入完成						
♥ 已完成接入 第三方	ī安全设备E	目志				
	 成功创建数据 	源-> 第三方安全设备日志_33				
	山下设备信	无字段提取规则	総型	型号/版本	信息等理定	揭作
	10.65.68.108	, inc /™l®jdoc	类型doc	쀞룩doc		立即爆取
报	夏入更多日志	继续接入其它类型的日志\流量				
西 19	記置丢弃规则 寛索日志	丢弃不必要的数据,降低存储、计算? 前往搜索查看已接入的日志	资源的浪费			
ŧ	测建统计项	前往创建更多统计项,用于生成报表				

- 步骤 3 进入样本接入页面,输入样本数据,如图 5-22 所示。
 - 图 5-22 样本接入

] 学段想取 -> 第三方安全设备日志_33 -> 厂商doc - 关型doc - 型号doc		
#本娘入 ●	15.5.4.RE	入库配置
	输入样本	
rotscol7+666jsepnent_dfrect0l+72jsrc_lo22+221.122.129.191jsrc_port23+146	(at 1,244-171,10,387,10);at 1,2071559827;ifnam_int1646/0035;ifnam_unt17net1600;egre_cont1841;egre_offst404;via	1255 yanı: 126-00-01: d7 vec: d5 (40,000: 127-54) 75: 00-50: 1.d: (4: yappent, 1: 121-1; 1; 1

步骤 4 创建提取规则,选择日志样本,如图 5-23 所示。

图 5-23 字段提取:选择样本

字段提取 -> 第三方安全设备	記書表33→「Radoc-#聖君doc- 担告doc	
###		入非起来
李段譜取 李段转换	学校修正 学校/開稿	
		0
25974 12287	30713 EB00	
("recv_time":"1677242 ment_direct28=72;src_ 1","timestamp":"16628 name6=84921164HTTPS13 =54:75:d0:5b:1d:8c;ag	NBULY,"rew_data"/1205gs 10 1733/01 NC data_typedwated07/lgg_typetwlart101sttack_asset41300400pedSL OF-300+4204 Nos is the Hiddle Security Opass Volkerbillty Schr/ingp_protocol_ [ja2247112273.01];rc_part214584;dg_1ja2471.03.07.043;dt_part24598271[fram_joided00000;jfram_aud17wot000];aggr_contable_10ggr_dffet8450[had35=part24804];dt_act255 NBUMBW0".security""/">Not"Not"/"Not"/Not"/Not"/Not"/Not"/Not Not Not Not Not Not Not Not Not Not	ame8=84021364HTTPS13;protocol7=656;seg 54:75:d0:5b:1d:8c;agent_ip128=1.1.1 pass Vulnerability Scan7;app_protocol 125=;smmc128=00:01:d7:ec:e5:04;dmac127
下一步 取得		
(1) 10 10 10 10 10 10 10 10 10 10 10 10 10	8≓8878 <i>√</i>	
接收时间	Biologia Bio	
° ✓ 2023-02-24 20:47:08	classing at 11:11:11 at 6.41 (particular) (p	#72jsrc_1p22#221.122.179.191jsrc_port23#13468jd 18=72jsrc_1p22=221.122.179.191jsrc_port23=13450jdst 22=221.122.179.191jsrc_port23=13450jdst_jp24=171.1



步骤 5 按需选择要提取的字段,如图 5-24 所示。

图 5-24 字段提取:指定条件

字段提取 字段制	会 学校修正 学校编辑	0
10.1748 × 11	see allante Rillente	
样本数据	ne byd-etten?jjg-tyd-ader101jette: wee-018094050er83. Of-2014-824 Res is to Hade Socily byen vidersbilly Socijeg_prized,wee-48010647910jpriced-48010667910jpriced-480106670jpriced-480106670	
选择字段	remaining •	
限定条件	(1) 第35年27日2 (1) 第35年3月14日 (1) 11 14年3月14日 (1) 145年3月14日 (1) 145年5月14日 (1) 145年5月14日 (1) 145年5月14日 (1) 145年5月14日 (1) 145年5月14年5月14日 (1) 11 145年5月14日 (1) 145年5月14年5月14年5月14年5月14年5月14年5月14年5月14年5	清空条件
	✓ (2):8770 ✓	
接收时间	原始教授	
* v 2023-03-24 11	<pre>cl2066g10 0733300 HC data_typei-attack97iog</pre>	tirect28=72;src_ip22=21 tt_direct28=72;src_ip22=2 72;src_ip22=221.122.179.
	(E-#) (E-#)	

步骤 6 选择方法,此处选择【正则表达式】,如图 5-25 所示。

提取 log_type1 字段的值,重命名为 log_type。

图 5-25 字段提取:选择方法

字段提取 字段转	· ···································	
		0
BRATA R	asht 是明方法 R面规则	
样本数据	(は近視時に告知)2度境内の前向成時子 >>)	
	Are_typel=tetex09(1)s_typel_bient12 jetexc_med=15004050e850. (N-2014-824 Men in the Niarja Security Spans Winerability Scar7;agg_protocal_med=640421546017511;protocal7=665;segment_sirect38=72;prc_jp22=211.122.179.191;prc_port18=15469;adt_jp24=17 1.8.30.141;adt_port18=5427	
正则规则	(?un)(?(*);");?)?(?++(*dog,\$pp+*(*]+)	
验证结果	log_type = alert21	
< 脸证 兜	809	
	■ 一 二 二 二 二 二 二 二 二 二 二 二 二 二	
3886x03193 ✓ 2023-03-24 11:	2018/06/0 19 7331/81 ND data_type1+stack971/gg_type1+stack138/04/00/per55L OR-2014-8224 Nm in the Middle Security Sysax Vulnershilly Scar7.pgp_urotocl_seade44821464TT9313protocl7+665/segment_di 2231 security = 4 Joset = NE	irect28=72;src_ip22=22 _direct28=72;src_ip22=2 2;src_ip22=221.122.179.

步骤 7 验证,完成规则配置,如图 5-26 所示。



图 5-26 字段提取:验证

□ 字段提取 -> 第三方安全	ù∰Hdg_33->∫Γβ(doc - ∰Edoc	
14:2	WA REMARKE	入傘起置
字段提取 字段转转	A 李祝侍王 李祝裕雅	
		0
输入 用正	则 提取字段 remaining	輸出
□示行号 ✔ ● 数行展示	✓ 10.市場取字段 ✓	
接收时间	原始設備	
2023-03-24 11:29-46	(14054e 18 D7:33):01 HS_det_type1=stac697.log_type1=stac1321.pttrec_neme4-530034030penS31_CVE-2014-6224 Pan in the Middle Security Bypeas Vulnerability Scen7.ppg_protocol_neme4-64021954HTTP513perotocol74654;sep unemby = 4 log_type = ader12 lost = HSC piolity = 124 m	rent_direct28=72;src_ip22=221.12 rgment_direct28=72;src_ip22=221.1;
	(1 -#)(T -#)	

步骤 8 创建新规则,如图所示。

选择日志的样本数据和字段,配置限定条件。

图 5-27 字段提取: 创建新规则

字段提取 字段转	l 学校修正 学校增强	
		0
151941× 185	art 153年方法 152章(0)	
样本数据	(12036p 10 1713)00 HDC data_typel=track97)igg_typel=alert101pttace_wave4=45100300000550. OVE-2014-0224 Man in the Hiddle Security bypass Vulnerability Scan7.pap_protocal_mane4=6401164HTPS11protocal7=6563;segment_di ret18=72jarg_jg2221.112.1193.00jarg_per12=12464ptt_jg24=1_040_07.149jatg_per12=56627	
选择字段	ranç data 🔹	
限定条件	log_type	清空条件
< <u></u> ▼ →#	19	
(15.75 v)(16.78)		
接收时间	應給數据	
• 🗸 2023-03-24 11:3	C141/5ep 10 17:33:01 MC data_type1=attack97;log_type1=attack71;log_type1=attack71;log_type1=attack70;log_typ	irect28=72;src_ip22=21 t_direct28=72;src_ip22=2

步骤 9 选择 Key->Value 方式提取,如下图 5-29 所示。



图 5-28 K->V 方式提取日志(1)

字段提取 字段转	换 字段修正 字段增强					
						0
iðjārāta 🔪 Ak	29/1 2005.5 NUTRO					
样本数据	<pre><124>Sep 10 17:33:01 HSC data_type1=attack97;log rect28=72;src_ip22=221.122.179.191;src_port23=13</pre>	_type1=alerti21;attack_name4=151003403OpenSSL CVE- 550;dst_jp24=171.89.207.143;dst_port25=59627	2014-0224 Man in the Middle Security Bypass Vulnerability Scan7;	app_protocol_name6=84021364HTTPS13;	protocol7=656;segment_di	
K->V	Key1 =	Value1	: Key2		Value2	
验证结果	str. port23 = 13450 dst ip24 = 171,99,207,143 se	ament direct28 = 72	vne1 = attack97 log type1 = alerti21 protocol7 = 656 dst port2	5 = 59627 ann protocol pameñ = 840	21364HTTP513	
	src_ip22 = 221.122.179.191 attack_name4 = 151003	03OpenSSL CVE-2014-0224 Man in the Middle Security E	ypass Vulnerability Scan7			
	R7 265					
(11)(11)(11)						
接收时间	原始音教过展					
• 🖌 2023-03-24 11	<pre><124>Sep 10 17:33:01 H3C data_type1=attack97 30:35 severity = 4 log_type = alerti21 host = H3C raw_data = <124>Sep 10 17:33:01 H3C data_type1 facility = 15</pre>	<pre>;log_type1=alerti21;attack_name4=1510034030penSSL priority = 124 =attack97;log_type1=alerti21;attack_name4=1510034030</pre>	CVE-2014-0224 Man in the Middle Security Bypass Vulnerability S DpenSSL CVE-2014-0224 Man in the Middle Security Bypass Vulnerability	can7;app_protocol_name6=84021364HTTP Scan7;app_protocol_name6=84021364H	S13;protocol7=656;segment_direct28=72;src_f	.p22=2 ip22=1
						_
			(I-#) (F-#)			

图 5-29 K->V 方式提取日志(2)

□ 字段提取 -> 算	第三方安全设备日志_33 -> 厂 磅doc - 类型doc - 型号doc		
	释年接入 ●		入炮配置
李段提取	李段转换 李段博正 李段瑞路		
			0
輸入 🕂	用 正則 過取字段 remaining	当字段 log_type == alerti21 时, 用 k>v 週期字段 raw_data	輸出
		条件不通足时保存到 未伊朗日志	
显示行号 ~)	「 接行 展示・		
接收时间	原始数据		
2023-03-24	4113400 ("recv_tile": "187942884136", "tilestam": "1460281181308", "severity ("4", "4st_624", "171, 187, 287 4113400 severity = 4 (dst_624", "171, 187, 287 4113400 severity = 4 (dst_624", "171, 187, 287	.1417_110_type1'1^81ert1117_f81_port137198027_189_protocol_mem67196011040HT9517_1747_102717201.121.139.1917_ medi=84021160HT9511 sr_622=221.122.178.191 picniy=124 sr_6ort2)=13450 log_type=a4ert21 srgment_dir	priority":"124","src_port23":"134 rect28 = 72 <124>sep 10 17:33:01 F
		(L-#) (F-#)	

步骤 10 单击【上一步】按钮,输入日志样本后,单击【下一步】按钮,如图 5-30 所示。

图 5-30 字段提取: 输入日志样本

字段提取 字段线	換 李四修正 李段缩强	0
5841× 15	size SARATE EXERCIT	
样本遺靈	134469 10 70.1018 0C dot_type1-title0701gt_type1-size130.pttstome4-110034050ec011 Of-3014-8224 Max is the Middle Society Byses Wahersellity Scat_page-protocl_meet-4801044007901jprotocol=480jageet_gil return=7jprgi2-222_112_175_10jprgot151-0506(pt_1)protocol=480jageet_gil	
选择字段	medata •	
限定条件	log,type • = = • set 120 Michael Micha	長件
	2月 	
121XHOIM	memory in a starting of the starting of the starting of the starting and a starting of the starting of the starting in the sta	721000 1022-
✓ 2023-03-24 11:	12 control of a 12 control of	8=72;src_ip22



步骤 11 创建新规则,通过 Key-value 方式提取字段,如图 5-31 至图 5-35 所示。

图 5-31 字段提取: Key-value 方式(1)

	時換 予政修止	10.78.28						
								6
2.1847.# N	6294 84953	ALIERRAS						
样本数组	<124>Sep 10 17:33: rect28=72;src_ip22	1 H3C data_type1=attack97;log_type 221.122.179.191;src_port23=13458;c	el=alerti20;attack_name4=151003403OpenSSL C dst_ip24=171.89.207.143;dst_port25=59627	VE-2014-0224 Man in the Middle S	ecurity Bypass Vulnerability Scan7;a	pp_protocol_name6+84021364HTTP513;pr	rotocol7=656;segment_di	
K->V	Key1		Value1		Key2		Value2	
Second B								
< 登班 完	src_port23 = 13450 src_jp22 = 221.122.1 Rt和	det ip24 = 17188.207.143 segmen 9.191 attack_name4 = 1510034030	tr, direct28 – 72 ~124×eep 10 17/3301 blc da penSSL CVE-2014-0224 Man in the Middle Securi	ta, type1 = attack97 log, type1 = . ty Bypass Vulnerability Scan7	protocol7 = 656 dxt_port25 dxt_port25	= \$9627 app_protocol_name6 = 8402	1864HTTPS13	
< <u>验证</u> 完	src_port23 = 13450 src_jp22 = 221.122.1 取消 取消	dat 1948 = 171.88.207.143 segmen 8.197 attack_named = 1510034030	rt, direct28 = 72 (124-sep 10 1733)01 No.ds penSSL CVE-2014-0224 Man in the Middle Securi	ta type1 = attack97 log type1 = /	lent20 protocol7 = 656 dat port25	= \$9627 app_protocol_name6 = 8402	1364HTTPS13	
< 验证 完 法示任 > (約7%) 接收时间	src_port23 = 13450 src_jp22 = 221.122.1 取消 取消 成合数2元	det [242 = 171,88207,143] = segunes 8.191 attack_named = 1510024030p	e, direct28 = 72 : - (124-sep 10 178301 hJc da	ta type1 = attack97 log,type1 = /	len20 protocol7 = 656 dat port25	= \$9927 app_protocol_name6 = 8402	1364HTTPS13	
<	crc.por23 = 12450 wrc.jp22 = 221.122.1 wrc.jp22 = 221.122.1 Will Will	det jugi = 17.48.2021.42 segmen 2019 attack_nemes = 1310034430, 131/02 HC deta_type1arttack97,100 10.902 = deta_type1arttack97,100 10.902 = deta_type1arttack97,100 10.902 = deta_type1arttack97,100 10.902 = deta_type1arttack97,100	e_dimetal= 72 -122-92 h T73300 h bit-di genesis_CVE-2014-0224 Man in the Middle Securi 	ta yopel = attack97 log_typel = /	Interesting protocol? = 656 det_port25	59827 app_protocol_numed = 8402 nr/sop_protocol_numed=8402 an/sop_protocol_numed=84021064HT193	13644/TTP513 13jprotoco17x454jsegment_stirect	t28+72;src_ip22 ect28=72;src_ip22
< 登録 登録 登録 一 第 2023-03-24 11	ロ:: por23 = 12450	det_ip24 = 17.48.2021.42 append 2019 attack_numeri = 131024400, 13108 NC 4645 Appet=4ttac097,1248 Append = America (State 1997) attack Append = America (State 1997) attack Append = America (State 1997)	e_derect3 = 72 = 124.945 to 173302 halede persS1 CVF-2014-022 hAm in the M66de Securi 	In popel = attack97 log_tppel = / y Byparks Vulnerability Scien7 SSL CVE-2014-0224 Man in the Millio 000QpenSSL CVE-2014-0224 Man in	tle Security Bypass Vulnerability Sca	59827 app_protocol_maned = 8402 n1) 499_protocol_maned=84021564HT195 an3) 499_protocol_maned=84021364HT195	1364-fTF9513 13.jpratocol.7~656; segment_sfrect 19513:protocol.7=656; segment_dire	t28+72;src_ip22

图 5-32 字段提取: Key-value 方式(2)

	祥本塘入	70元で化記簿 ;	
字段提取	字段转换 字段修正 字段增强		
			0
输入	用 正對 總裁字段 remaining 🕇 🖋 🍵	当字段 log_type == alerti21 时, 用 k>v 把取字段 raw_data	输出
		当字段 log_type == alerti20 时, 用 k->u 图取字段 raw_data	
		条件不满足时保存到未识别日志	
(B):58 - (操行爆赤マ 医赤进取学校 イ		
據收时间	原始数据		
• 2023-03-24	("recv_time":"1679629442176","timestamp":"1662831181000","severity":"4","dst_ip24":"171.89.20", (1)4402 (severity = 4 dst_ip24 = 171.89.20",143 log_type1 = slerti20 dst_port25 = 59627 app_protocol_n	.437,"log_bysl":"slerti28","dst_port25","50027","sp_protocol_mame6":"64021344mT19513","src_b922":"221.122.179.191","priori ame6 = 840213644TTP513 ur_b92 = 221.122.179.191 priority = 124 pr_port23 = 13450 log_type = alert20 segment_diret28	ity":"124","src_port23":"134 = 72 <124>sep 10 17:33:01 F
		(<u>+</u> -+)	

图 5-33 字段提取: Key-value 方式(3)

」 宇宙標準 → 第三方安全设备日表_33 → 厂简doc - 是型doc - 型号doc				
	Reckie	入成配置		
英型: 类型doc	祭明/編本: 監守doc	高豪存入多报录》 试试多考虑的		
	当学说 log_type == alerti21 时, 用 k->v 绝版学级 raw_data	8.0		
	当字段 log_type == alerti20 时, 用 k->v 提取字段 raw_data			
	(held) (second)			
	oc - 型形doc 英音: 完型doc	東京: 東面doc 東京: 東面doc 東京: 東面doc 東京: 東面doc 東京: 東面doc 東京: 東面doc 東京: 東面doc 東京: 日本: 田田市市 田田市: 日本: 日本: 日本: 日本: 日本: 日本: 日本: 日本: 日本: 日本		



图 5-34 字段提取: Key-value 方式(4)

样本撮入		RESCRIED	入体設置
■: 厂司doc	資型: 対型doc	繁璧 /御本: 監号doc	将所有字段符入一部的
输入 用 regex 提取字段 remaining		当于限 log_type == alerti21 时, 用 k->v 證职于限 raw_data	8 0
		当字段 log_type == alerti20 时, 用 k->v 提取字段 raw_data	8.0

图 5-35 字段提取:存入多张表

样本接入		33.5KRE €	
1991: 厂町;doc	英型: 类型doc	聚 吗/称本: 至号doc	將所有李延持入一法法
输入 用 regex 提取字段 remaining		当字段 log_type == alerti21 时, 用 k->v 图取字段 raw_data	存入家 alerti21 中
		当字段 log_type == alerti20 时, 用 k->v 遵职字段 raw_data	研入素 alert20 中

- 步骤 12 完成字段提取,如图 5-36 所示。
 - 图 5-36 完成字段提取

□ 提取完成	
⊘ 已完成提取 第三方安全设备	日志
接入更多日志	(単位)を1000月10日をつける
配置去弃规则	些并不必要的政治,种 征 护德,计算的那的浪费
腹索曰志	前社境表面質已減入的日ボ
台级影响计项	带拉伽建贾多纳计语,用于生成报表

步骤 13 当该设备的日志发送到 LAS 平台后,进入 日志分析 > 日志检索 页面,查询相关日志, 如图 5-37 和图 5-38 所示。


图 5-37 第三方设备的日志检索(1)

OKOBIGLAR MUNICH	< PRAR(1+: DEPS	Easterizo			
Q	法援助问 🕠 🕿	版1小时 〇 最近24小时 〇	最近7天 〇 最近30天 〇 自定3	2 3分钟 🖌 🕨	
88	地探漏性 💌 日	志属性 〇 资产属性			
19日志	日志来源 P		源 P		
志 ぎ	源调口		目的P		
"登录日志	目的地口				
日志	自定义检末 调整	认 图件			
0(V3070)日志	(9,79	检索条件		快捷检索配置	投索 高级搜索 *
志 3志	豊示鑑表♥				
15	最新日志数 6555	3 1			显示空宇段 日志导出 检索结果统计
5火塘日志 《墙	日志来源 IP	日志产生时间	日志接收时间	日志编号	采集器编号
	10.65.68.108	2023-03-24 11:00:01	2023-03-24 10:54:59	76bc7dc2470947aeb8d6edd36fc7d8fa	F0ED-629A-9686-94A2
旧志	10.65.68.108	2023-03-24 11:00:01	2023-03-24 10:54:59	cdc81117232a4403802a4b39008ddee3	F0ED-629A-9686-94A2
	10.65.68.108	2023-03-24 11:00:01	2023-03-24 10:54:59	2177d487b6054a8ca7f6af30ff87f58f	F0ED-629A-9686-94A2

图 5-38 第三方设备的日志检索(2)

快速检索 重点关注	< 除透発件: 日	市典型alerti21	-0		
Q	antential	• 最近1小时 〇 最近24小时 〇	最近7天 ○ 最近30天 ○ 自定5	2 3分钟 🗸 🕨	
6日 市	远择属性	• 日志漏性 〇 遊产漏性			
5	日志家道中		38 IP		
15 15	源油口		目的IP		
用户登录日志	Rear				
志	EISTMIN .				
5	自定义检索	请输入条件。			
PS日志					
070(V3070)日志		保存检索条件		快速检索配置	· 夜索 高级搜索 ▲
印志					
日志	显示图表¥				
□●/+□◎ も日志	最新日志数	8546 2			显示空宇宙 日志导出 检索结果统计
00防火場日志		2000 A	2	2448	
防火場	日空油酒中	D40%,T3316)	Delinatio	D-09-2	14.12.02.94.73
志	10.65.68.108	2023-03-24 11:00:01	2023-03-24 11:03:49	5187dea214174c76a2576f342d4a6586	F0ED-629A-9686-94A2
/PN日志	10.65.68.108	2023-03-24 11:00:01	2023-03-24 11:03:49	10352354662e45949592eb7c0b95dfd9	F0ED-629A-9686-94A2
日志					

步骤 14 执行 字段修正。

步骤 15 进入入库配置页面,如图 5-39 所示。

图 5-39 字段提取:准备入库配置

#平镜入 ●	76		
¶e: /™Mjdoc	用题: 問題doc	聖明/献奉: 聖問doc	
義入 用 k->v 證明字段 raw_data			E 0



步骤 16 单击<mark>告</mark>,指定日志类型,如图 5-40 所示。

图 5-40 字段提取:指定日志类型

٥	指定日志类型			×
	日志类型命名规则: 1. 只允许包含数字、小 如: anti_av_log	写英文字母、下划线(); 2. 只允许	以英文字母开头; 3. 长度不超过30个字符	
	日志类型	logdoc	从已有日志类型中选取	
	日志别名	as_logdoc		
				取消 确认

步骤 17 单击【完成提取】按钮,完成日志提取,如图 5-41 和图 5-42 所示。

图 5-41 字段提取:日志提取结束

日本後入	2014通道 ()		
s /"medoc	用版: 如 届doc	服号/編本: 股号doc	
th III k. to MERCHID you date			存入版 logdoc 中

图 5-42 字段提取:完成日志提取

□ 提取完成	
已完成提取 第三方安全设备日	±
擒入更多日志	继续输入其它类型的日本流量
配置丢弃规则	丢弃不必要的敢强,降低存储、计算资源的流费
搜索日志	前往搜索查看已接入的日志
创建统计项	前往创建更多统计项,用于生成资源



5.3.5.2 字段修正

配置字段修正规则,用于删除无用字段、修改字段名称或修改字段类型。操作方法如下: 步骤 1 根据提示配置修正规则,如图 5-43 所示。



图 5-43 准备配置字段修正规则

₩ キ接 入 ②			
▲ 摄歌学校中存在无效的学校家。 需要 配置修正规 则 方	ilitistat		
▲ 開助学校中存在无效的学校会、 编要 配器特证规则 方 ■: 「■doc	開始の1	聖明/國家 : 五年doc	

步骤 2 删除无效的字段,如图 5-44 所示。

图 5-44 删除无效字段

释 和 液入			2	
* 李骏玄称		李段别名	字段类型	操作
10 🛕 <124+sep 10 17:35:01 h3c data_type1			string	10
	(1-#)(T-#)			

----结束

5.3.5.3 字段转换

配置字段转换规则,用于将提取的字段范式化为指定格式。

进入字段转换页面,配置转换规则,单击【确定】按钮,进入下一步配置,如图 5-45 所示。

图 5-45 字段转换

□ 字钮细眼 -> 第三方安全设备日志_33 -> 厂 异doc - 美型doc - 型号doc		
ната). С		入市総置
李紀縣歌 李伯明語 李伯修正 李紀樂語		
		0
特特加学经	<124>sep 10 17:38:01	*
和如果是	e) #@offe	•
atiGitast	yyyy-MMe-dd	*
	8014 80(H	
	(F-#)(T-#)	



5.3.5.4 字段增强

只有第三方安全设备日志、网络设备日志、虚拟化平台日志、其他日志和文件日志支持配置字段增强规则。

进入字段增强页面,单击+,添加一个自定义的字段增强,完成字段提取,如图 5-46 所示。

图 5-46 字段增强

新子·独入			入 5 章	2	
李段摄歌 李段转换 李段修正 李段增强					
Endourne (d) 🖌 🖉 (Althéorem (d) 🖌					0
◎ 字段名称	字段别名	字段类型	字段圆定值	操作	
10 data_type1	data_type	string	和月 日日	/ 0	
11 请输入新增生经济的	资格入制增少股份 有	\$31874825	• BRYRIGHTER	+	

5.4 Linux 主机日志接入

Linux 主机日志接入的操作方法如下:

步骤 1 下载 Linux Agent。

- a. 登录 LAS 的 Web 管理页面。
- b. 将鼠标悬停在总控制台图标☉,进入数据采集 > 采集终端 > Agent 页面。
- c. 单击【下载 Agent】, 进入 Agent 下载页, 如图 5-47 所示。
- d. 在 Agent 列表中,单击平台端下载栏的之,将对应的 Agent 下载到本地。 根据目标主机的操作系统架构选择对应的 Agent:
 - X86:选择 Linux-x86。
 - ARM:选择Linux-arm。
 - SunOS:选择 SunOS。



图 5-47 Agent 下载页

志接入	数据》	原 枚举值	规则管理	采集终端					
🗖 Agent T	载								▶ 返回上级
❶ 为确保) Agent i	Agent 正常 卸载方式:	會使用,请开放 UDP 协议 1、在管理页面中远程卸程	的 514	下载配置中的 UDP、 ent读本地密码卸载	TCP 第口。 查看具体操作详情)				
									♦ 下载配置
平台		支持版本			安装包	MD5	版本	大小	平台端下载
Wind	lows	Vista or later/All Wind	ows release		NSFOCUS-Agent-Windows-1.0.1.msi	4d209bf731a85b1b16fdbc8426e3f37c	1.0.1	280.52Kb	*
👌 Linux	x-x86	CentOS/Redhat/Ubunt	u/Debian or other	r Linux 2.7 or later	NSFOCUS-Agent-Linux_x86-1.0.1.run	1b651698879b170dfca82a8a623982b9	1.0.1	282.36Kb	*
👌 Linux	k-arm	CentOS/Redhat/Ubunt	u/Debian or other	r Linux 2.7 or later	NSFOCUS-Agent-Linux_arm-1.0.1.run	34090dc4a8d74b0e9812adc52f4c4132	1.0.1	268.57Kb	±
👌 SunO	S-i386	SunOS5.10/Solaris10 c	or later		NSFOCUS-Agent-SunOS_i386-1.0.1.tar.gz	f65e7ff57376e8979ed1fdf912016405	1.0.1	267.52Kb	±

步骤 2 登录目标主机,上传 Agent 安装包,如图 5-48 和图 5-49 所示。

图 5-48 上传 Agent 安装包(1)

h

图 5-49 上传 Agent 安装包(2)



步骤 3 赋予可执行权限并安装 Agent, 如图 5-50 所示。

chmod +x CTYUN-Agent-Linux x86-1.0.1.run



图 5-50 安装 Agent

[root@localhost ~]# ./NSFOCUS-Agent-Linux_x86-1.0.1.run
[ok] nsfocusagent.service start
agent install successfully in /usr/local/nsfocusagent/nsfocusagent
[root@localhost ~]#

步骤 4 返回 **数据采集 > 采集终端 > Agent**页面,等待几分钟后,目标主机上安装的 Agent 已上线,如图 5-51 所示。

状态为"已最新",说明 Linux Agent 安装成功。

图 5-51 数据采集 Agent 列表

□ 采集终端						
采集器 设备 Agent						▲下號 Agent
总数 💶			请输入IP地址、主机名称、操作系统进行重调			
IP 地址 全部▼	主机名称	主机信息	状态	注册时间一	最后道信时间一	操作
10.55.189.142	DESKTOP-M4I46U3	Windows 10 Pro x64 desktop	日報新の	2023-02-24 14:47:25	2023+02+24 14:54:02	¢ % ≡
Q 10.65.68.108	localhost.localdomain	CentOS Linux x64 server	日爆新の	2023-02-24 14:47:13	2023-02-24 14:54:09	¢ % ≡
10.65.4.206	SHIZHISHANG	Windows 11 Pro x64 desktop	日最新 2	2023-02-24 08:58:40	2023-02-24 14:54:00	\$ % ≡
₫ 10.65.189.175	las-1666257429	CentOS Linux x64 server	日母新の	2023-02-23 17:00:21	2023-02-24 14:54:04	¢ % ≡
< 1 > 每页10条,共1页,到第 1	页 跳应					

步骤 5 进入 数据采集 > 数据源 页面,可以查看已处理的日志数量,如图 5-52 所示。

图 5-52 数据源(Linux 主机日志)

Linux 主机新纳日志_514	ර) නමා		0/s 183518		Ξ
------------------	-----------	--	---------------	--	---

步骤 6 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看接入 Linux 主机的日 志详情,如图 5-53 所示。



图 5-53 日志检索(Linux 主机日志)

选择时间	 最近1小时 	○最近 24 小时 ○最近 7天 ○最近 30 天	· ○ 自定义 3分钟 ▼ ▶				
选择属性	• Bankte O	逆产属性					
日志来源 P		日志名	10				
自定义检索	请临入资件						
	保存检索条件			侠	教授委委团		18:20 R 18:0
显示图表¥							
量示图表♥ 最新日志数(12) 12				1	显示空学段 日志	時出 检索
显示语表* 最新日志数(日志产生时间	2 1	设备型号/版本	日志中選印	日志名称	主机名	显示空子段 日志 告留等级	時出 检索器 遊程名
■示題表× 最新日志数 (日志产生时间 2023-02-24 1	™ 17:32:05	设能型号/版本 CentOS Linux release 7.9.2009 (Core)	日本中期IP 10.65.68.108	日志名称 audīt	主机名 localhost.localdomain	<u>豊示な守</u> 役 日ま <u>負責等項</u> 6	75世 1228 进程名
型示信表* 最新日志数 (日志产生时间 2023-02-24 1 2023-02-24 1	2 II 17:32:05 17:32:05	设备理 归/xs本 CentOS Linux release 7.9.2009 (Core) CentOS Linux release 7.9.2009 (Core)	日志中選手 10.55.68.108 10.65.68.108	日志名称 audīt audīt	主机将 iocalhosLiocaldomain iocalhosLiocaldomain	日本 合計学校 合	988 检察 8 进程名
型示道表* 最新日志教 2023-02-24 2023-02-24 2023-02-24	17:32:05 17:32:05	設備型号/版本 CentOS Linux release 7.9.2009 (Core) CentOS Linux release 7.9.2009 (Core) CentOS Linux release 7.9.2009 (Core)	日志中選P 10.65.68.108 10.65.68.108 10.65.68.108	B&SAN audit audit audit	主時名 iccalhost.localdomain iccalhost.localdomain iccalhost.localdomain	■示法字段 日載 名言を決め 6 5 6 6	29931 12993 連程名
■示認表・ 最新日志数 (日志产生时间 2023-02-24 1 2023-02-24 1 2023-02-24 1 2023-02-24 1 2023-02-24 1	 I I7:32:05 I7:32:05 I7:32:05 I7:32:05 	UBST 19/166 # CentOS Linux release 7.9.2009 (Core) CentOS Linux release 7.9.2009 (Core)	Eldu#@P 10.65.68.108 10.65.68.108 10.65.68.108 10.65.68.108	Eld:SAN audit audit audit audit	主略客 Iocalhost.localdomain Iocalhost.localdomain Iocalhost.localdomain	第示公子段 日息 の出る好	₩ 进程名

----结束

5.5 Windows 主机日志接入

Windows 主机日志接入的操作方法如下:

- **步骤 1** 下载 Windows Agent。
 - a. 登录 LAS 的 Web 管理页面。
 - b. 将鼠标悬停在总控制台图标 , 进入 数据采集 > 采集终端 > Agent 页面。
 - c. 单击【下载 Agent】, 进入 Agent 下载页, 如图 5-47 所示。
 - d. 在 Agent 列表中,单击 Windows 平台端下载栏的盖,将对应的 Agent 下载到本地。
- 步骤 2 鼠标双击 Agent 文件,安装 Windows Agent。
- 步骤 3 返回 数据采集 > 采集终端 > Agent 页面, 查看 Windows 主机是否在线。

Windows 主机已接入,如图 5-54 所示。

图 5-54 数据采集终端列表

采集器 设备 Agent						▲下載 A
BR (4)			谢输入IP地址、主机高称、操作系统进行查询			
P 地址 全部 ▼	主机名称	主机曲眼	状态	注册时间一	最后通信时间 -	操作
10.65.189.142	DESKTOP-M4I46U3	Windows 10 Pro x64 desktop	已衆新の	2023-02-24 14:47:25	2023-02-24 17:40:52	• •
∆ 10.65.68.108	localhost.localdomain	CentOS Linux x64 server	日最新の	2023+02+24 14:47:13	2023-02-24 17:40:43	• •
10.65.4.206	SHIZHISHANG	Windows 11 Pro x64 desktop	日最新 2	2023-02-24 08:58:40	2023-02-24 17:40:44	• •
A 10.65,189,175	las-1666257429	CentOS Linux x64 server	日最新 2	2023-02-23 17:00:21	2023-02-24 17:40:40	0%



步骤 4 进入 数据采集 > 数据源 页面,单击上一步接入的 Windows 主机,可以查看接入的设备信息,如图 5-55 所示。

图 5-55 接入的主机信息(Windows 主机日志)

	▶ 返回上级
Windows 主机事件日志_514 10.65.189.175 (CU:10.65.189.175)	
· 御入主机 · 御入配置	
新新人/58月世份	配置归并规则
* ±00P	操作
1 10.65.188.142	8

步骤 5 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看接入 Windows 主机 的日志详情,如图 5-56 所示。

图 5-56 日志检索(Windows 主机日志)

选择时间	 最近1小时 〇 最 日志属性 〇 田村 	近24小时 〇 最近7天 〇 最近 蜀姓	E30天 自意义 3分钟 ▼ ▶				
日志来源中	10.65.189.142		周中				
操作			日志名称				
自定文检索	请输入条件。						
	保存检索条件			(*18%)#			22 2622 ×
显示图表-							
最新日志数(1 7998	R 8888 🖬
日志产生时间		日志来還IP	主机	操作	日志名称	风险等级	告誓等级
2023-02-24 1	6:47:55	10.65.189.142	DESKTOP-M4I46U3	Special Logon	Security	o	6
	647.64	10.65 189 1.62	DESKTOR, MARKER	Special Lopon	Carceller	0	6

----结束

5.6 Web 服务器日志接入

以 Window IIS 服务器(采集路径为 C:\Users\Public\web.log)为例,Web 服务器日志接入的操作方法如下:

步骤 1 下载 Windows Agent (若已在 Web 服务器中安装 Agent,请忽略该步骤)。

- a. 登录 LAS 的 Web 管理页面。
- b. 将鼠标悬停在总控制台图标 , 进入 数据采集 > 采集终端 > Agent 页面。
- c. 单击【下载 Agent】, 进入 Agent 下载页, 如图 5-47 所示。
- d. 在 Agent 列表中,单击 Windows 平台端下载栏的盖,将对应的 Agent 下载到本地。

步骤 2 进入 数据采集 > 日志接入 页面,单击【Web 服务器日志】,如图 5-57 所示。



图 5-57 选择日志接入对象(Web 服务器日志接入)

¢		
DS、NF等	取 第三方安全设备日志 接入其它安全厂商的安全设备日志,如 WAF、IPS/IDS等	网络设备日志 各厂商的网络设备(交换机、路由器、DNS、GTM/LTM) 的日志信息可通过此接入
	入 Linux 主机系统日本	名gent Web 服务実日主
В、	通过绿盟日志采集 Agent 接入 Linux 各发行版本的系统日志	通过感望日志采集 Agent 接入 Web 服务器产生的访问日志、错误日志

- 步骤 3 选择 Web 服务器日志接入的采集器,如图 5-58 所示。
 - 图 5-58 选择 Web 服务器日志接入的采集器

已选择接入 Web 服务器日志			重新选择
	选择要接入的采集器		
	10.65.189.175 (CU:10.65.189.175)	7	
	继续		

步骤 4 填写 Web 服务器日志接入的端口号 (不可填写系统端口号),如图 5-59 所示。

图 5-59 配置 Web 服务器日志接入方式

已选择接入 Web 服务器日志		重新改革
	配置接入方式	
摄入协议	UDP	
摄入端口	.11	
	0 新桃园不可占用	
数据情式	Syslog	
数据编码	UTF-8 •	
	上一步 如本	

步骤 5 单击【添加 Web 服务器】按钮,添加接入日志的 Web 服务器,如图 5-60 所示。



图 5-60 添加接入日志的 Web 服务器

已选择接入 Web 服务器日志			王和选择
	添加要接入日间	S的 Web 服务器	
			已添加 0 名
# 服务器 IP	服务器类型	日志格式	操作
	0	无政策	
			透加 Web 服务器
	上一步	完成撮入	
注意:			
1。用户必须具有管理员权限			
2、Web服务器日志接入,参考 配置文档,进行相关操作			

- 步骤 6 配置接入日志的 Web 服务器参数。
 - a. 配置完成,单击【确定】按钮,如图 5-61 所示。
 - b. 单击【完成接入】按钮, Web 服务器日志完成接入, 如图 5-62 所示。

图 5-61 配置接入日志的 Web 服务器

添加 Web 服务器配置	
服务器 (P•	
10.65.189.142	
服务强大型。	
115	•
日志格式。	
Custom Log Format	
白定义模式。	
timestamp sitename dip method request query dport accountname sip user_agent status http_sub_code win32_code	
0 自定义指式参考股票	
15 服务器 timestamp sitename dip method request query dport accountname sip user_agent status http_sub_code win32_code	
Nginx 服务器 Sremote_uddr - Sremote_user [Stime_local] "Srequest" Sstatus Sbody, bytes_sent "Shittp_referer" "Shittp_user_agent" "Shittp_r_forwarded_for"	
Apache 服务器 "%h %i %u %t %T1%h1" %>s %b 1%i[Refered])" 1%i[User-Agent])""	

图 5-62 Web 服务器日志完成接入

□ 接入完成				
○ 已完成接入 Web 服务器日志				
0	成功创建数据	2課 -> Web 服务器日志_11		
接入更	10多日志	继续接入其它类型的日志小成量		
配置支	長奔规则	近弃不必要的败据,降低存储、计算资源的 流费		
搜索日	日志	游社搜索查查已接入的日志		
的建筑	充计项	前往创建遵多统计项,用于生成版表		

步骤 7 返回 数据采集 > 采集终端 > Agent 页面, 配置要接入日志的 Web 服务器。



- a. 单击数据采集终端列表操作栏的 , 配置 Web 服务器的应用服务日志参数, 如图 5-63 所示。
- b. 配置主机采集参数和应用服务日志参数,其中应用服务日志参数包括服务名、日志采集 路径、日志文件名全路径和端口号(即步骤4接入的端口),如图 5-64 所示。

图 5-63 数据采集终端列表(Web 服务器日志接入)

□ 采集终端						
采集器 设备 Agent						▲下载 Agent
总数 🕙			诸猿入户地址、主机名称、扁作系统进行黄词			
IP 地址 金郎▼	主机名称	主机信息	状态	注册时间一	最后通信时间 -	操作
10.65.189.142	DESKTOP-M4I46U3	Windows 10 Pro x64 desktop	日最新 2	2023-02-24 14:47:25	2023-02-24 17:58:08	● % ≡

图 5-64 数据采集终端配置(Web 服务器日志接入)

[10.65.189.142] Agent 数据采集配置				×	
 ● 支持采集 Windows / Linux 系统日志、软硬件配置变更、外围设备使用。 支持采集 Windows / Linux 环境下的的应用服务日志,需配置服务名,日志采集路径、日志文件名路径,及数据发送端口。 支持监控指定目录下,文件的添加、修改、删除等操作,需配置监控文件的路径信息(windows xp 和 server2003系统、Solaris、Fedora 暂不支持文件目录审核)。 启用注册表审核和主机审计相关配置,可产生相对应的绿盟终端日志(windows xp 暂不支持)。 支持配置指定日志类型加密传输策略,默认加密传输策略为否(不加密) 					
主机采集配置 ≈ 加密传输 是 ● 否 系统日志采集对象 转发事件 ☑ 应 ④ 如果系统日志采集对象没有选择,默认 应用服务日志 ≈	用程序 🕑 安全 人会开启应用程序、安全和	Setup ☑ 系统 系统。			
服务名	日志采集路径	日志文件名全路径	端口		
▼ 志日2II	C:\Users\Public	C:\Users\Public\web.log	11	Ô	
★添加					
示例:如 windows 下要监控 R 盘下以 * 在通配符写法中支持匹配 *(若干行	a' 开头的所有 txt 文件,可 '字符)、?(单个字符)。	「使用通配符写法 R:\a*.txt			

步骤 8 进入 数据采集 > 数据源 页面,当有日志上报时,可以查看已处理的日志条数,如图 5-65 所示。

图 5-65 已接入日志的 Web 服务器

· 第选 选择采集器来查看该采集器上	的数据源	•		更多操作 •
Web 服务器日志_11 —	0/s 勝攻	*	0/s 范武化	=



步骤 9 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看接入 Web 服务器的 日志详情,如图 5-66 所示。

图 5-66 日志检索(Windows 主机日志)

13月33月 ● 最近 1 小时 ● 最近 24 小时 ● 最近 7天 ● 最近 30 天 ● 自由文 39 钟 ▼ ▶ 13月31日 ● 日志編性 ● 田志編性 ● 資产編性 日志永源 P 100105本 100105本 100105本 100105本	
15月間性 ● 日本篇性 ① 前产篇性 日本演 ● 日本篇性 ② 前产篇性 日本来源 P	
日志未順 P 日志未順 P 約以約本 施太下キ	
(h)2/6法 唐文方注	
N VALUE NO V	
统志得	
自定又结素 网络入员中	
保存检索条件 快速检索管置	技术 高级技术
豊方憲表で	
最新日志教 💿 🧃	日志导出 检索结果
日志产生时间 日志来跟P 目标P 请求和部 潤P 请求方法	状态码说明
2023-02-24 18:15:49 10.65:189.142 10.128.137.142 123.151.42.52 GET	success
2023-02-24 18:15:49 10.65:189.142 10.128.137.142 123.151.42.52 GET	success

----结束

5.7 数据库接入

以 POSTGRES 数据库为例,数据库数据接入的操作方法如下:

- **步骤 1** 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标 →, 进入 数据采集 > 日志接入 页面, 单击 【数据库数据】, 如图 5-67 所示。

图 5-67	选择日志接入对象	(数据库接入)

	_		
	U		
	第三方安全设备日志	网络设备日志	数据库数据
	接入其它安全厂商的安全设备日志,如 WAF、IPS/IDS等	各厂商的网络设备(交换机、路由器、DNS、GTM/LTM) 的日志信息可通过此接入	通过 JDBC 的方式连接到数据库管理系统,以拉取指定的 数据
_			

步骤 3 选择数据库数据接入的采集器,如图 5-68 所示。



图 5-68 选择数据库接入的采集器

已选择接入 数据库数据			運動法は
	选择要接入的采集器		
	10.65.189.175 (CU:10.65.189.175)	•	
	短续		

- 步骤 4 配置数据库接入参数。
 - a. 添加要接入数据的数据库,如图 5-69 所示。
 - b. 配置数据库接入参数,如图 5-70 所示,主要参数说明如表 5-2 所示。
 - c. 单击【连接测试】按钮,如果连接测试通过,进入步骤5添加数据表;如果连接测试不通过,请检查数据库名称、连接帐号和连接密码是否正确。

图 5-69 添加要接入数据的数据库

已选择接入数据库数	文 据			重新选择
		添加要接入数据的数据库		
			从已有	育数据库(0)中选择
数据库 IP	数据库类型	数据库板本	数据库通口	
10.65.189.175	PostgreSQL	- 9.x	5432	
		上一步		

图 5-70 配置数据库接入参数

已选择接入 数据库数	女据					重新选择
			配置数据库接入参数			
鼓运库名称						+ 0
这场计与						
道建密码						
援入速率(条/分钟)	1000					0
BIGJELRE	S = 0 = 5					
已接入鼓运家	= 数据表	数据表别名		備移列	操作	
			O SERS			
					法投票款 活江改成来	
			上一步 完成接入			

表 5-2 数据库接入参数

配置项	描述
即时拉取	 是:从当前时间开始拉取后续新的日志数据。 否:第一次选择"否",表示从0开始拉取历史所有数据和后续新数据; 第N次选择"否",表示从上次拉取的时间开始拉取历史所有数据和后续 新数据。



步骤 5 单击【添加数据表】按钮,添加接入的数据表,此处以 public_auth_user 为例,如图 5-71 所示。

图 5-71 添加数据表

已选择接	そ入 数据库数据		重新选择
		添加教掘表	
	数乘表类型 ● 有主境 ○ 元主境 ○ 玩面		
	数据表"校量添加	数据表别名。	
	publicautr_user	tis user	

- 步骤 6 配置接入数据的数据库参数。
 - a. 配置完成,单击【确定】按钮,如图 5-72 所示。
 - b. 单击【完成接入】按钮,数据库数据完成接入,如图 5-73 所示。

图 5-72 数据库数据接入配置

已选择接入数据库数	 技 据					康新选择
		配置数据库接入参数				
数据库名称	100				+ 0	
這級防母						
连续空码						
接入速率 (条/分钟)	1000				Θ	
#78社会职	○是 ● 音					
已版人数据表	* 数据表	数据表别名	倫修列	爱作		
	1 public.auth_user	las_user		e		
				治投发试 添加数据表		
		上一步 完成没入				

图 5-73 数据库数据完成接入

□ 接入完成		
○ 已完成接入 数据/	库数据	
	◎ 成功创建数	据題 → 取振声弊設置_10.65.189.175
	接入更多日志	继续输入其它类型的日志\流量
	配置丢弃规则	丢弃不必要的数据,降低存储、计算资源的 浪费
	搜索日志	前往废卖查看已接入的日志
	创建统计项	前往创建更多统计项,用于生成服表

步骤 7 进入 **数据采集 > 数据源**页面,当 auth_user 表里有数据插入,可以查看已处理的日志 条数,如图 5-74 所示。



图 5-74 已接入日志的数据库

等选 资料平量基本查查该平量器上的数据源		•			更多操作。
	0/s		0/s	日秋澤(1)	-
Biter#4046_10.65.189.175	接收	~	潜式化	#2000 (0) 解析失效 (0)	=

步骤 8 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看接入数据库的日志 详情,如图 5-75 所示。

图 5-75 日志检索(数据库接入)

快速检索 重点从注	< 博选条件: 日志英型Ja	s_user			
Q	选择时间 💿 最近	1 小时 🔷 最近 24 小时	最近7天 0 最近30天 0 自定义	3分钟 ~ ▶	
Βð	选择属性 🔹 日志	属性 〇 资产属性			
备日志	日志来源中				
几事件日志	自定义检索 调编入	\$:#-			
廃日志 注志	保存检测	索条件		快速检索配置	技大 英级技术 <
	显示图表♥				
	最新日志数 🕦 🍱				显示空中段 日志导出 检索居黑统计
	日志来源 IP	日志产生时间	日志接收时间	日志编号	采集器编号
	10.65.189.175	2023-02-24 18:34:27	2023-02-24 18:34:27	923d6495-3260-46fd-88c5-985eb0cee24a	947A-5875-7CEA-EBE3
	< 🚺 > 每页 20 多	R, 共1页, 到篇 2 页	确定 0 可在1~1页之间相页		



----结束

5.8 虚拟化平台接入

以 ESXi 6.7 虚拟化平台为例,虚拟化平台接入的操作方法如下:

- 步骤 1 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标³³⁴,进入 **数据采集 > 日志接入**页面,单击【虚拟化平台日志】,如图 5-76 所示。



图 5-76 选择日志接入对象(虚拟化平台接入)

	U		
	第三方安全设备日志	网络设备日志	数据库数据
IF等	接入其它安全厂商的安全设备日志,如 WAF、IPS/IDS等	各厂南的网络设备(交换机、路由器、DNS、GTM/LTM) 的日志信息可通过此接入	通过 JDBC 的方式连接到数据库管理系统,以拉取指定的 数据
	٩	9	Agent
	Linux 主机系统日志	Web 服务器日志	虚拟化平台日志
	通过绿盟日志采集 Agent 接入 Linux 唇发行版本的系统日 志	通过绿盟日志采集 Agent 接入 Web 服务器产生的访问日 志、错误日志	接入昏虚拟化平台产生的日志

- 步骤 3 选择虚拟化平台日志接入的采集器,如图 5-77 所示。
 - 图 5-77 选择虚拟化平台日志接入的采集器

已选择接入 虚拟化平台日志		重新选择
	选择要接入的采集器	
	10.65.189.175 (CU:10.65.189.175)	
	913	

步骤 4 填写虚拟化平台日志接入的端口号(不可填写系统端口号),如图 5-78 所示。 ESXi 6.7 的外发固定端口号为 514。

图 5-78 配置虚拟化平台日志接入方式

已选择接入 虚拟化平台日志		重新选择
	配置接入方式	
能入防災	UDP	
接入递口	514	
	0 新秋风2不可人用	
設 ##Akut	Syrlog	
数据编码	UTF-8 *	
	上一步 想效	

- 步骤 5 添加要接入日志的虚拟化平台。
 - a. 填写平台 IP 并选择平台名称,如图 5-79 所示。
 - b. 单击【完成接入】按钮,虚拟化平台日志完成接入,如图 5-80 所示。



图 5-79 添加要接入日志的虚拟化平台

E	选择接入虚拟化平台日志		重新选择
	添加要接入日本的面积化平台		
			已质如 0 余
	平台 IP 平台名称	操作	
1	10.65.109.153 ESI 6.7 GA •	+	
			批量添加
	上一步 能能输入		

图 5-80 虚拟化平台日志完成接入

□ 接入完成							
⊘ 已完成接入 虚拟化平台日志							
	◎ 成功创建数据	□ 虚拟化平台日志_514					
1	夏 入更多日志	继续接入其它类型的日志、流量					
Ā	記置丢弃规则	云亮不必要的数据,降低存储、计算资源的映 费					
搜索日志 前往搜索查看已输入的日志							
Ê	创建统计项	前往创建更多统计项,用于生成报表					

步骤 6 进入 ESXi 6.7 虚拟化平台。

- a. 登录 ESXi 6.7 虚拟化平台,进入 系统 > 高级设置 页面,如图 5-81 所示。
- b. 搜索键: Syslog.global.logHost,结果如图 5-83 所示。
- c. 编辑选项,如图 5-84 所示。 格式为 udp://10.65.189.175:514,其中 10.65.189.175 为 LAS 平台 IP。

图 5-81 进入 ESXi 6.7 虚拟化平台

vmware: ESXi				root@10.65.18	19.153 + 務助・	1 Q.投索	
Welcome to localhost.localdomain	- XSB						ж
• □ 主机	系统 硬件 许可 软	件包 服务 安全和用户					
世現 意控	高级设置	/ 病病治疗 ♂ 刷新 ☆ 脱作				Q 提索	
- (3) dziki (40	自动启动	97 A	~ 名称	- a	BtiA	~ 己聚素	~
- 👸 242-F07SP测试环境勿删	5250	Annotations WelcomeMessage	直接控制台用户界面 (DCUI) 的初始屏幕中的欢迎消息。使用空			False	10
1819	的阿和日期	BufferCache FlushInterval	以此时间间隔(毫秒)刷新	30000	30000	False	
更多虚拟机		BufferCache.HardMaxDirty	如果脏睡存区过多(百分比), 会阻塞写入器	95	95	False	
· 🛛 🕫 🖬 🚺 🚺		BufferCache PerFileHardMaxDirty	如果给定文件的新爆冲区过多(百分比)。会阻塞写入器	50	50	False	
1 <u>Q</u> M/S		BufferCache SoftMaxDirty	如果脏睡存区过多(百分比)、则立即则新	15	15	Falso	
		CBRC DCacheMemReserved	CBRC 数据缓存清耗的内存(以 MB 为单位)	400	400	False	
		CBRC.DCacheSize	CBRC 数据缓存的大小(以 MB 为单位)。如果 CBRC Enable 设	32768	32768	False	
		CBRC:DigestJournalBootinterval	暂时禁用摘要日志以免影响引导过程的时间间隔(以分钟为单位)	10	10	False	
		CRRC Frahla	由用其干肉豆的透過在	falsa	falsa	Falsa	
		快速荡进器					1059 瑛
	1 近期任务						
	任务	✓ 目标 < 启动者	✓ 已接以时间	◇ 结果 ▲		完成时间 🔻	



图 5-82 系统高级配置

选项	描述
Syslog.global.defaultRotate	要保留的存档的最大数目。可以在全局范围内设置该数目,也可以为单个子记录器设置 该数目。
Syslog.global.defaultSize	在系统轮换日志之前,日志的默认大小 (KB)。可以在全局范围内设置该数目,也可以 为单个子记录器设置该数目。
Syslog.global.LogDir	存储日志的目录。该目录可以位于挂载的 NFS 或 VMFS 卷中,只有本地文件系统中的 /scratch 目录在重新引导后仍然存在,将目录指定为[数据存储名称]文件路径,其 中,路径是相对于支持数据存储卷的 root 目录的路径。例如,路径 [storage1] /systemlogs 将映射为路径 /vmfs/volumes/storage1/systemlogs。
Syslog.global.logDirUnique	选择此选项将使用 ESXi 主机的名称在 Syslog.global.LogDir 指定的目录下创建子目 录。如果多个 ESXi 主机使用同一个 NFS 目录,则唯一的目录非常有用。
Syslog.global.LogHost	向其装发 syslog 消息的远程主机,以及远程主机在其上接收 syslog 消息的端口。可以包括协议和端门,例如 ssī: //hostNane1:1514。支持 UDP(仅在端门 514 上)、 TCP 和 SSL,远程主机必须安装并正确配置 syslog 以接收转发的 syslog 消息。有关 远程主机配置的详细信息,请参见远程主机上安装的 syslog 服务的文档。
	您可以使用无限数量的远程主机来接收 syslog 消息。

图 5-83 搜索键的结果

系统	硬件	许可	软件包	服务	安全和用户							
高级设	12		/ iii	續造项	C Riff 🏠 🎘	ήΈ.				Qs	yslog.global.log	gHost X
白动启	目动		52 A				0	名称	(道) ~	獣认 〜	已要盖	~
时间和	印印期		Syslo	g.global.l	logHost			将日志输出至的远程主机。为空时重置为默认值。支持多个主机	udp://10.65.189.222:514,udp:/		True	
			快速	筛选器		*						1顶

图 5-84 编辑选项

🗋 localhost.localdomain - 管理							
系统 硬件 许可 软件	地 服务 安全和用户						
高度设置	/ 编辑选项 ℃ 副新	O IBIT				Q Syslog global logHost x	
自动启动	程 .		🙍 \$18	e @	~ \$KU.	→ 已蔵魚 →	
動同和日期	Syslog global logHost		将日志输出至的远程主机。	为空时重要为默认信。支持多个主机 udp://10.65.16	9 175:514	True	
	快速用悲襲						
	Û	Syslog global logHost 《 新聞品版 - Syslog global.logP 新儀	ost udp./10.65.189.175.514 (序符章)	2月多个王明、400月回号(1)年201月7,993 	2. udp./hostName1.514. hostNam	n2, ssl/hostName31514	

步骤 7 进入 数据采集 > 数据源 页面,可以查看已处理的日志条数,如图 5-85 所示。

图 5-85 已接入日志的虚拟化平台



步骤 8 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看接入虚拟化平台的 日志详情,如图 5-86 所示。



图 5-86 日志检索(虚拟化平台日志接入)

筛选条件:	日志英型vsphere虚拟机日志			
选择时间	 最近1小时 〇 最近24小时 〇 最 	近7天 〇 最近 30 天 〇 自定义	3分钟 🖌 🕨	
选择属性	● 日志属性 ○ 资产属性			
日志来源 IP				
自定义检索	请输入资件			
	保存检索条件		快速检索配置	技 索 高级接索 *
显示图表▼	(82) E			显示空宇段 日志导出 检索结果统计
日志来源 IP	日志产生时间	日志接收时间	日志集号	采集器编号
10.65.189.1	53 2023-02-24 19:37:49	2023-02-24 19:37:53	079ddcb83c9c4ca2a37015dbd9dbc0bd	947A-5875-7CEA-EBE3
10.65.189.1	53 2023-02-24 19:37:17	2023-02-24 19:37:20	eb2c4ef0ed97420da06f31bee3a198e7	947A-5875-7CEA-EBE3
10.65.189.1	53 2023-02-24 19:36:45	2023-02-24 19:36:48	c01c9d280ce84be382ffbc8ca2f33786	947A-5875-7CEA-EBE3
10.65.189.1	53 2023-02-24 19:32:50	2023-02-24 19:38:18	a1f1b441f9044cf2b2151b0080b84135	947A-5875-7CEA-EBE3
10.65.189.1	53 2023-02-24 19:32:48	2023-02-24 19:38:15	593227a26ff840b29bb7d1a14e2ccbc3	947A-5875-7CEA-EBE3

----结束

5.9 网络设备流量接入

网络设备流量接入的操作方法如下:

- 步骤 1 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标³³³,进入 **数据采集 > 日志接入**页面,单击【网络设备流量】,如图 5-87 所示。

图 5-87 选择日志接入对象(网络设备流量接入)

	٨
Windows 主机事件日志	Linux 主机系统日志
通过绿盟日志采集 Agent 接入 Windows 2008、 Windows 7等主机系统日志	通过绿盟日志采集 Agent 接入 Linux 各发行版本的系统日 志
	an C
网络设备流量	其它日志
接入网络设备 Netflow V5/V9的流量数据	可接入其它应用程序、中间件、业务系统等产生的日志

步骤 3 选择网络设备流量接入的采集器,如图 5-88 所示。



图 5-88 选择网络设备流量接入的采集器

已选择接入网	络设备流量	重新选择
	选择要接入的采集器	
	20.65.153.4(U.10.65.133.4)]

- 步骤 4 填写网络设备流量接入的端口号(不可填写系统端口号),如图 5-89 所示。
 - a. 数据格式仅支持 Netflow V5 和 Netflow V9。
 - b. 一个端口只能以一种协议接入一种格式的数据。

图 5-89 配置网络设备流量的接入方式

已选择接入 网络设备流量		重新选择
	配置接入方式	
接入协议	UDP	
接入端口	回航人统人旅客	
	● 系統調口不可占用	
数据格式	Netflow V5 ·	
	上一步 继续	

步骤 5 添加接入流量的网络设备,如图 5-90 所示。

- a. 配置网络设备的设备 IP、厂商、类型和型号/版本后,单击+。
- b. 单击页面下方的【批量添加】,支持批量添加网络设备。

图 5-90 配置网络设备参数

已选择接入 网络设备流	量				重新选择
	添加	叩要接入流量的网络设备			已添加 0 台
# 设备IP	厂商	类型	型号/版本	操作	
1 请输入设备IP	请输入或选择厂商	请输入或选择类型 ▼	请输入或选择型号/版本 ▼	+	
					批量添加
		上一步 完成接入			

步骤 6 单击【完成接入】按钮,完成网络设备流量接入,如图 5-91 所示。



图 5-91 接入完成(网络设备流量)

□ 接入完成		
♥ 已完成接	入网络	设备流量
0	成功创建数据源	₹-> 网络设备流量_515
接入	更多日志	继续接入其它类型的日志\流量
配置:	丢弃规则	丢弃不必要的数据,降低存储、计算资源的浪费
搜索:	日志	前往搜索查看已接入的日志
01 5 23	统计项	前往创建更多统计项

----结束

5.10 文件日志接入

文件日志接入的操作方法如下:

- 步骤 1 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标³³³,进入 **数据采集 > 日志接入**页面,单击【文件日志】, 如图 5-92 所示。

图 5-92 选择日志接入对象(文件日志接入)



步骤 3 选择文件日志接入的采集器,如图 5-93 所示。



图 5-93 选择文件日志接入的采集器

已选择接入文件日志		重新选择
	选择要接入的采集器	
	10.65.189.168 (CU:10.65.189.168)	
	健地	

步骤 4 填写文件日志接入的端口号(不可填写系统端口号),如图 5-94 所示。

图 5-94 配置文件日志的接入方式

已选择接入文件日志		重新选择
	配置後入方式	
描入幼识	UDP	0
统入建口	44	
	0 彩砂湖江不可占用	
数据传统	Syslog	
数据编码	UTF-8 •	
	1-# 885	

- 步骤 5 添加接入的文件日志来源设备,如图 5-95 所示。
 - a. 配置文件日志来源设备的设备 IP、厂商、类型和型号/版本后,单击+。
 - b. 单击页面下方的【批量添加】,支持批量添加文件日志来源设备。

图 5-95 配置文件日志来源设备参数

已选择接入 文件日	志			重新选择
		添加要接入的文件日志来源		135M 0.4
# 设备IP	厂商	类型	型号/版本	操作
1 10.10.10.10	厂商	- #2	•	- +
		上一步 完成油入		批量源和

步骤 6 单击【完成接入】按钮,完成文件日志来源设备的接入。

- 步骤 7 请参见 字段提取, 配置提取规则。
- 步骤 8 导入文件日志。
 - a. 进入 **数据采集 > 数据源**页面,单击文件日志来源设备名称,进入文件日志数据源详 情页面。
 - b. 单击文件日志来源设备列表操作栏的 1,弹出上传日志文件对话框,如图 5-96 所示。
 - c. 单击【点击选择文件】按钮或者将日志文件拖拽到指定区域,单击【导入】按钮,完成 文件日志的导入。



图 5-96 导入文件日志

□ 上传日志文件	×
	10 10 10 10 10 10 10 10 10 10 10 10 10 1
点击选择文件	
或将日志文件拖拽到这里完成上传,支持(*.txt)格式的文件	-
等待上传文件: filelog.txt	

	取消导入

步骤 9 进入 数据采集 > 数据源 页面,可以查看已处理的文件日志条数,如图 5-97 所示。

图 5-97 已接入的文件日志

精选 这样采出是这个世界这次是第上的政策原		٠			更多操作 •
	0/s		Q/s	已处理(4)	
又非出意_44	接收	~	蒲式化	第23回(1) 解析失敗(0)	=

----结束

5.11 其他日志接入

LAS 接入其它日志可以通过 UDP、FTP 和 KAFKA 协议进行。其中, UDP 和 FTP 协议的接入方法与接入第三方安全设备日志的基本相同,请参见 第三方安全设备/网络设备接入。

本节仅介绍 KAFKA 协议接入其它日志的配置。



KAFKA 日志接入是 LAS 主动去对端的 KAFKA 上拉取数据, 所以需要接入一个可以 成功连接的 KAFKA 环境。

通过 KAFKA 协议接入其他日志的操作方法如下:

- **步骤 1** 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标³³³,进入 **数据采集 > 日志接入**页面,单击【其它日志】, 如图 5-98 所示。



图 5-98 选择日志接入对象(其他日志接入)

	۵.
Windows 主机事件日志	Linux 主机系统日志
通过绿盟日志采集 Agent 接入 Windows 2008、 Windows 7等主机系统日志	通过绿盟日志采集 Agent 接入 Linux 各发行版本的系统日 志
&	Agent ①
网络设备流量	Agent ① 其它日志

步骤 3 选择其他日志接入的采集器,如图 5-99 所示。

图 5-99 选择其他日志接入的采集器

已选择接入其	它日志	重新选择
	选择要接入的采集器	
	10.65.189.176 (CU:10.65.189.176)	
	继续	

步骤 4 配置其他日志的接入方式,如图 5-100 所示。

- a. 填写文件日志接入的端口号(不可填写系统端口号).
- b. 接入协议选择 KAFKA。

图 5-100 配置其它日志的接入方式

已选择接入 其它日志		重新选择
	配置接入方式	
运 办公式	калка •	
接入端口	9092	
	0 新胡和二本可占用	
鼓扇格式	JSON	
数运编码	UTF-8 •	
	上一步	

步骤 5 配置其它日志的来源设备。

- a. 配置 KAFKA 设备 IP, 如图 5-101 所示。
- b. 配置 KAFKA 接入参数,如图 5-102 所示。
- c. 单击【连接测试】按钮,添加其它日志的主题,如图 5-103 所示。



图 5-101 配置 KAFKA 设备 IP

已选择接入 其它日志	重新改成
日即中課 [P	※已和KAFKA (0) 中語解
	L-# 98

图 5-102 配置 KAFKA 接入参数

已选择接入其它	目志			重新选择
		配置KAFKA接入参数		
限自時可接立規定	○是 ● 吾			
采集限速 (魚/秒)	0			0
认证方式	无			
已接入从节点	◎ 从罚点 IP	第日会	操作	
		1 新元政策		
			添加从节点	
已接入主题	# 主题	主题别名	操作	
		1 如无政语		
			连接 测试 添加主题	
		上一步 完成接入		

图 5-103 添加其它日志的主题

已选择接入 其它日志			重新选择
	添加主题		
18. sas_log_parse	tasiga	•	

步骤 6 单击【完成接入】按钮,其它日志完成接入,如图 5-104 所示。



图 5-104 其它日志完成接入

□ 接入完成				
○ 已完成接入 其它日志				
•	J建数据源 -> 其它日志_9092			
接入更	志 继续接入其它类型的日志\流量			
配置去	则 丢弃不必要的数据,降低存储、计	计算资源的源费		
搜索日	前往搜索查看已接入的日志			
创建纳	前往创建更多统计项,用于生成	段表		

步骤 7 进入 数据采集 > 数据源 页面,可以查看已处理的其它日志条数,如图 5-105 所示。

图 5-105 已接入的其它日志

· 佛西 · 历得华度器中自新演学生表	器上的影响器				更多操作。
N26#_9092	0/s (860)	>	0/s 18:5342	日田連 3 未定期(の) 解析先致(の)	=

----结束

5.12 主机审计日志接入

以 Linux 主机审计日志为例, 主机审计日志接入的操作方法如下:

- 步骤 1 请参见 Linux 主机日志接入,接入 Linux 主机日志。
- **步骤 2** 将鼠标悬停在总控制台图标 →,进入 **数据采集 > 采集终端 > Agent**页面,单击 Agent 列表操作栏的 →,弹出 Agent 数据采集配置对话框,配置主机审计参数,如图 5-106 所示。



-

图 5-106 Agent 数据采集配置

● 支持采典 Windows / Linux 系统日志、软硬件配置变更、外围设备使用。							
支持采集 Windows / Linux 环境下的的应用服务日志,需配置服务名,日志采集路径、日志文件名路径,及数据发送端口。							
支持监控指定目录下、文件的添加、修改、删除等程作、需配置监控文件的路径信息(windows xp 和 server2003系统、Solaris、							
Fedora 暂不支持文件目录审核)。							
启用注册表审核和主机审计相关配置,可产生相对应的绿盟终端日志(windows xp 暂不支持)。							
支持配置指定日志类型加密传输策略,默认加密传输策略为否(不加密)							
系统日志							
务日志 ≪							
服务名							
+ 添加							
住通即将与法平文持匹配"(石干1子符)。(平1子符)。							
录审核 ≪							
加密传输 🔘 是 💿 否							
文件路径 请输入监控文件的路径信息							
+配置 ☆							
加密传输 💿 是 🔘 否							
配置项 🕑 移动存储审计 🛛 硬件变更审计 🔽 软件变更审计 🔽 账号变更审计 🔽 密码变更审计							
🔽 用户登录审计 🛛 进程创建审计 🔽 网络连接审计							
TOWN							

步骤 3 进入 日志分析 > 日志检索 页面,通过日志类型的筛选,可以查看主机审计的日志详 情,如图 5-107 所示。



图 5-107 日志检索(主机审计日志)

筛选条件:	日志英型网络连接审计					
遗择时间	 最近1小时) 最近 24 小时 () :	最近7天 〇 最近30天	○ 目定义 3分钟 V ▶		
选择属性	 日志履性 	资产属性				
日志来源 IP						
自定义检索	请输入条件					
	保存检索条件				快速检索配置	技会 高级投资 A
显示图表♥						
最新日志数	1 12 1					显示空字段 日志导出 检索结果统计
动作	连接状态	连接协议	连接方向	日志产生时间	外部地址	日志来遵IP
连接	连接	tcp	连出	2023-02-24 19:56:09	10.65.68.108	10.65.68.108
断开	85开	tcp	连入	2023-02-24 19:56:09	10.65.68.108	10.65.68.108
连接	连接	tcp	连出	2023-02-24 19:56:05	10.65.68.108	10.65.68.108
连接	连接	tcp	连入	2023-02-24 19:56:05	10.65.68.108	10.65.68.108
连接	连接	tcp	连入	2023-02-24 19:54:23	10.65.7.120	10.65.68.108

----结束

5.13 NAT 配置

当接入 LAS 的数据源设备使用 NAT (Network Address Translation, 网络地址转换)将真实 IP 地址进行了转换,在 LAS 中可以进行 NAT 配置,记录数据源真实 IP、NAT 转发服务器 IP 和数据源设备 Tag,作为数据源设备的唯一标记。

NAT 配置的步骤如下:

- **步骤 1** 登录 LAS 的 Web 管理页面。
- **步骤 2** 将鼠标悬停在总控制台图标 → , 进入 数据采集 > 数据源 页面。
- **步骤 1** 单击【更多操作 > NAT 配置】按钮,进入已选择接入页面,选择要接入的采集器,如图 5-108 所示。



图 5-108 选择要接入的采集器

□ 日志接入	
已选择接入	
	选择要接入的采集器
	10.65.169.101 (CU:10.65.169.101)
	继续

步骤 2 单击【继续】按钮, 配置 NAT 接入方式, 如图 5-109 所示。

图 5-109	配置接入方式
---------	--------

□ 日志接入		
已选择接入		
	NAT 配置接入方式	
接入	协议 UDP	*
接入)) 5140	
数据	格式 Syslog	*
	上一步 继续	



步骤 3 单击【继续】按钮,配置 NAT 转换数据源设备参数,添加通过 NAT 地址转换接入 LAS 的数据源设备,参数说明如表 5-3 所示。

表 5-3 NAT 转换数据源设备参数

配置项	描述
NAT IP	数据源使用的 NAT 服务器 IP 地址。
设备 IP	数据源的真实 IP 地址。



配置项	描述
设备 Tag	从数据源设备日志中选择可以唯一标记该设备类型的字符串作为设备 Tag。

- **步骤 4** 单击 完成数据源设备添加。
- **步骤** 5 单击【完成接入】按钮,保存数据源设备 NAT 配置。

----结束





对于 日志接入 的日志对象,LAS 采集器会根据相应的字段提取规则来对其输出的日志 进行提取。完成提取后,在数据源下可以对所有日志数据的各个环节进行集中管理和配 置。

本章主要内容如下:

功能	描述
查看统计信息	介绍数据源统计信息的查看方法。
查看数据源处理信息	介绍数据源日志的处理内容。
数据源管理操作	介绍数据源几种常见的管理操作方法。
配置数据源	举例介绍数据源的配置方法。

将鼠标悬停在总控制台图标³³³,进入 **数据采集 > 数据源**页面,可以查看所有数据源的总体统计信息,并对各个数据源进行管理,如图 6-1 所示。

图 6-1 数据源

↓ 当前位置: 总拉台 > 数据采用	t • > 数据源 •							
日市接入 数1622	牧举语 规则管理 采集终端							
^{接入日志类型} 92 _类	接入资产 4 给 (共 10 个日志源)	未近的日本 0 条	*201数据源 0 个	解析失败日志 O 条	據收速率 0 葉/s	而式化速率 O m/s	加密速率 3	入库速率 0 _{氛/s}
神道 这样不是最大支部的	采集器上的数据图			•				更多操作 *
第三方安全设备日志。1234		0/s 接收) 0	0/s 范式化		日は週 (44,776) 未の則(5) 解析天政(5)	=
導盟安全设备日志		0/s 接收		*	0/s 描述化		日此理 (sk.367) 未识別 (0) 解析例文 (1)	=
周塘设 备 日志_1717	-	0/s 論収		> •	0/s 推示(化		日秋港(Massa 未明約(m) 線研研数(m)	
网络设备日志_1716		0/s 操改) 0	0/s 范式化		●此署 mono 未回 m 解析実验活 \ 新町 (2)	Windows 圏"以親話 Windows,
		0.04			0.ir		已於理 向1974	101 21



6.1 查看统计信息

如图 6-1 所示,页面顶部显示所有数据源的统计数据,单击数据进入对应的列表页,可以查看更多详情。单击页面右上方的【返回上级】,可以回到数据源页面。

查看接入日志类型

进入已接入日志类型详情页,页面左侧展示所有已经接入 LAS 的日志类型,将鼠标悬停 在日志类型上,可以在页面右侧查看该日志类型包含的子日志类型,如图 6-2 所示。

图 6-2 已接入日志类型

□ 已接入日志类型			◆ 返回上級
过滤 您可以通过日志类型。日志别名的关键字进行	子陈选		
線歷安全设备日志		advance_threat_file_event_log (陳威威許年本日志)	
第三方安全设备日志	18 +	applog (应用管理日志)	8
网络设备日志	(3) ×	audit (南计日志)	
数据库数据	360	authlog (以征日志)	
Windows 主机事件日志	(D) >	avlog (防衛適日思)	
Linux 主机系统日志	. (3) ×	cc_event_log (C&C遵信日本)	8
Web 服务器日志	(II) >	database_audit_log (說張库审计日志)	8
虚拟化平台日本	36	ddoslog (把她握得攻击日志)	
网络设备流量	(11) ->	dnsblacklistlog (DNS全局需省单日志)	
其它日本	2	email_audit_log (即件审计日志)	
文件日志	÷		
線整线時日本	(II) ×		

查看接入资产

进入已接入设备页面,可以对已接入设备(日志源)进行查看和管理。单击操作栏的**、**,可以查看对应设备的详情,如图 6-3 所示。

图 6-3 已接入设备(日志源)详情

秘数 💶 (共 10 个日志源)		请输入设备 IP 对接入设施列申进行筛选	
设备 IP	接入采集器	治 入类型	握
10.65.133.254	10.65.189.171 (CU:10.65.189.171)	绿盟安全设备日志	^
球型安全设备日本 (1997年期, 1997年, 1997年, 1997年)	10		
#22安至安勝日志 投稿支型: SAS→ICS 投稿型号/顺本: V5.6. 播入编曰: 5004 播入的说: TCP 8	10 19時前式: XML		
球型空光に分割日辺 (投動変更): SAS-ICS (投動変更): SAS-ICS (設動変更): SAS-ICS (設動変更): SAS-ICS (設備変更): SAS-ICS () SAS-ICS (10 198805: XML 1085.100.71 (CU10.55.100.77) 20.8 20.71 (CU10.55.100.77)	第二万安全公開日日 第二十一日 マックロー	

查看未识别日志

进入未识别日志页面,可以查看与现有规则不匹配及尚未配置字段提取规则的日志信息, 仅展示最新的 1000 条数据,如图 6-4 所示。

单击操作栏的[▼],执行 字段提取 操作,此时会自动将日志原文作为样本,无需手动配 置样本。

单击【导出全部】按钮,可以将所有未识别日志导出到本地。



单击【全部清空】按钮,可以将所有未识别日志删除。

图 6-4 未识别日志

•	未识别日志			• 3	医回上级
		来源 IP	请输入日志来源 查询	ib	
日志	总条数 1100	•		身出全部	部清空
#	来源 IP	接收	女时间	原始数据	操作
1	10.65.169.101	. 201	8-09-29 15:38:52	<124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=1510034030penSSL CVE-2014-0224 Nan in the Middl e Security Bypass Wulnerability Scan%d;app_protocol_name(6)=8402136AHTTPS%d;protocol(7)=6%d;segment_direct(28)=%d;src _jn(22)=61.12;e.61.%d;src_prot(23)=%d;dx_jn(24)=171.89.207.%d;dst_port(25)=%d;fname_in(16)=xeth0/0;ifname_out(17)=xeth0/0;ifname_out(26)=1;aggre_offset(43)=0	T
2	10.65.169.101	. 201	8-09-29 15:38:52	<pre><124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=1510034030penSSL CVE-2014-0224 Nan in the Niddl e Security Bypass Wulnerability Scan%d;app_protocol_name(6)=E4021364HTPS%d;protocol(7)=6%d;segment_direct(28)=%d;src jn(22)=61.12,9.61.Xd;src_port(23)=%d;dst_jn(24)=171.89.207.%d;dst_port(25)=%d;fname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0</pre>	•
3	10.65.169.101	. 201	8-09-29 15:38:52	<pre><124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=1510034030penSSL CVE-2014-0224 Man in the Middl e security Bypass Wulnerability Scan%d;app_protocol_name(6)=E4021364HTPS%d;protocol(7)=6%d;segment_direct(28)=%d;src _in(22)=61.12;e.61.Kd;src_port(23)=%d;dx_in(24)=171.89.207.%d;dst_port(25)=%d;fname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0</pre>	Ŧ
4	10.65.169.101	. 201	8-09-29 15:38:52	<	7
5	10.65.169.101	. 201	8-09-29 15:38:52	<124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=1510034030penSSL CVE-2014-0224 Man in the Middl e Security Bypass Wulnerability Scan%d;app_protocol_name(6)=E4021364HTTPS%d;protocol(7)=6%d;segment_direct(28)=%d;src _jn(22)=61.12;e.61.Kd;src_prot(23)=%d;dst_jn(24)=171.89.207.%d;dst_port(25)=%d;ifname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0	Ŧ

查看未知数据源

若有未进行过日志接入配置的设备 IP 向 LAS 发送日志数据,该设备会被 LAS 归类为未知数据源。

进入未知数据源页面,可以查看未知数据源的详细信息,包括来源 IP、端口、接收时间和原始数据,如图 6-5 所示。

同时支持对未知数据源进行如下操作:

- 通过来源 IP 地址,查询指定的未知数据源。
- 每一个未知来源 IP 只保留最近的一条日志。
- 单击【全部清空】按钮,可以清除所有未知数据源。
- 单击【日志接入】,跳转至日志接入页面,可以根据未知数据源的实际情况,进行日志 接入配置,详细的配置方法请参见日志接入。



图 6-5 未知数据源

•	人口数据源			今 返回上版
		来源 IP	请输入未知数据源 IP	
			查询	
总数	0			Http://
#	来源 IP	端口	接收时间	质hapar
1	10.65.11.147	514	2019-11-11 12:56:02	(1870)の1111255(4)2007001111255(4)20070011112(150-1114)(55-1000015)/アウマを5100015-1.1-0015(Pertitione-roos)(Ategory-es)Surfage-yee) in Control Namagery&CondUnero432473)Societudos:fype-発展した自己に見いませた。 WI Performance Adapter 俗止;ComputerName-SURYANG)1E;EventIdentifier-0;User-

查看解析失败日志

进入解析失败日志页面,可以查看与现有字段提取规则匹配但解析失败的日志信息,如 图 6-6 所示。

查看解析失败日志,主要是用来验证己配置的字段提取规则是否已涵盖所有上传的日志, 若未完全涵盖,可以单击操作栏的^(*),执行 字段提取 操作,修改字段提取规则。

单击【导出全部】按钮,可以将所有解析失败的日志导出到本地。

单击【全部清空】按钮,可以将所有解析失败的日志删除。

图 6-6 解析失败日志

	Ņ	附先败日志				医回上级
			来源 IP	请输入日志来源 查询	IP	
E	志	总条数 801				部清空
	#	来源 IP	接收	如前间	原始数据	操作
	1	10.65.169.101	201	8-09-29 15:37:55	<124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=1510034030penSSL CVE-2014-0224 Man in the Middl e Security Bypass Vulnerability Scan%d;app_protocol_name(6)=84021364HTPS%d;protocol(7)=6%d;segment_direct(28)=%d;src jp(22)=611.961.4%g;src_port(23)=%d;dst_jp(2)=171.89.207.%d;dst_port(25)=%d;ifname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0	Ŧ
	2	10.65.169.101	201	8-09-29 15:37:55	<pre><124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=151003403OpenSSL CVE-2014-0224 Man in the Middl e Security Bypass Vulnerability Scan%d;app_protocol_name(6)=E4021364HTP5%d;protocol(7)=6%d;segment_direct(28)=%d;src _jn(22)=61.39;src_port(23)=%d;ds:jn(24)=171.89.207.%d;dst_port(25)=%d;ifname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0</pre>	۲
	3	10.65.169.101	201	8-09-29 15:37:55	<pre><124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=151003403OpenSSL CVE-2014-0224 Man in the Middl e Security Bypass Vulnerability Scan%d;app_protocol_name(6)=E4021364HTP5%d;protocol(7)=6%d;segment_direct(28)=%d;src jp(22)=61.19.61.%d;src_port(23)=%d;dst_ip(24)=171.89.207.%d;dst_port(25)=%d;ifname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0</pre>	T
	4	10.65.169.101	201	8-09-29 15:37:55	<124>%s H3C data_type(1)=attack%d;log_type(2)=alerti%d;attack_name(4)=1510034030penSSL CVE-2014-0224 Man in the Middl e Security Bypass Vulnerability Scan%d;app_protocol_name(6)=E4021364HTTP5%d;protocol(7)=6%d;segment_direct(28)=%d;src jp(22)=61.19.61.%d;src_port(23)=%d;dscip(24)=171.89.207.%d;dst_port(25)=%d;ifname_in(16)=xeth0/0;ifname_out(17)=xe th0/0;aggre_count(26)=1;aggre_offset(43)=0	۲
	5	10.65.169.101	201	8-09-29 15:37:55	<	T



查看运行速率

数据源页面顶部实时展示 LAS 接收日志的速率、范式化字段的速率以及将字段入数据库的速率,如图 6-7 所示。

图 6-7 查看运行速率

接收速率	范式化速率	入库速率
4 267	4 200	4 4 4 0
4,20/ 条/s	4,200 条/s	4,44 ∪ _{条/s}

6.2 查看数据源处理信息

数据源页面中,展示已接入数据源对相应日志的接收速率、范式化字段的速率以及已处理/未识别/解析失败的日志的数量,如图 6-8 所示

图 6-8 查看数据源处理信息

筛选 选择采集器来查看该采集器上的	数据源					更多操作▼
▲ 第三方安全设备日志_222 ——	0/s 接收	>>	0/s 范式化	\longrightarrow	已处理(0) 未识别(0) 解析失败(0)	≡
网络设备流量_515	0/s 接收	>	0/s 范式化		已处理(0) 末识别(0) 解析失败(0)	Ξ

6.3 数据源管理操作

在如图 6-8 所示的区域中,用户可以对数据源进行以下操作:

6.3.1 **查询数据源**

以采集器 10.65.189.171 为例,在筛选区域选择采集器,列表将只展示属于该采集器的数据源,如图 6-9 所示。



图 6-9 查询数据源

· 通過 10.65.189.171 (CU:10.65.189.171)		•			更多操作。
重三方安全设备日志。1234	0/5 播吹	*	0/s 范式化	日処理(00.4.776) 来沢服(の) 解析決敗(の)	=
W20108	0/s 接收	>•	0/s 102516	은요한편 (64,367,948) 제2만편 (0) 編위도한 (0)	=
用带设备日志_1717	0/s 接收	*	0/s 范式化		=
网络设备日志_1716	0/s 接吹	>	0/s 范式化	● 日廷理(1882) 131,576(未回期(19)) 解析考察()活 Windo 等为(1)(第1)(180)	₩S 5 Windows,

6.3.2 **编辑数据源**

单击☰,然后单击【编辑】按钮,仅支持编辑数据源的名称,如图 6-10 所示。

图 6-10 编辑数据源

□ 编辑数据源名称	×
第三方安全设备日志 1234	
	取消确认

6.3.3 **删除数据源**

单击**三**,然后单击【删除】按钮,可以删除相应的数据源,如图 6-11 和图 6-12 所示。 删除后,采集器将不再接收和解析相应的日志信息。

图 6-11 删除数据源




图 6-12 删除数据源确认框



6.3.4 **启用/停用数据源**

单击**三**,然后单击【启用/停用】按钮,可以开启/关闭相应的数据源。停用数据源后, 采集器将不再接收和解析相应的日志信息。

1. 数据源启用后,操作栏为【停用】,如图 6-13 所示。

图 6-13 停用数据源

第三方安全获载日本_1234		th BEE	已記還 (84,776) 朱纪敏 (0) 解析天世 (0)	三 (夜月)
	0/5	0/6	EREW (54,367,948)	编辑

2. 数据源停用后,数据源置灰,如图 6-14 所示。

图 0-14 数据源停用后 (1))
-------------------	---



3. 数据源停用的时候,操作栏为【启用】,如图 6-15 所示。

图 6-15 数据源停用后(2)



4. 数据源启用之后,恢复正常。



6.4 **配置数据源**

在如图 6-8 所示的区域中,单击数据源名称,可以查看和更改该数据源的相关配置。 每类数据源的管理方法类似,下面以第三方安全设备日志_1234 为例进行介绍,如图 6-16 和图 6-17 所示。

图 6-16 数据源

第三方安全设备日志。1234	0)s ලැබ	**	0/s 范式化	日記篇(16,776) ★ (20回(17) 解析形式(7)
線型安全设备日志			0/s 范式化	BIOE (64.367.948) 第 未分類(0) 重 解析決地(0) 重
网络设御日志_1717	0/s #x7	**	0/s 范式68	
网络总管日本_1716	05 1802	*	0/5 353576	Better info.131876 #1月日 (1) 新時期間近 Windows 報知の設置いる時がindows。

图 6-17 数据源详情

第三方安全设备日志_1234 10.65.189.	171 (CU:10.65.189.17	1)		
滚艇入关键闭查询				配置低非规则 配置归并规则
# iQ&IP	厂商	类型	型号/版本	操作
1 10.65.189.189	test	test	test	то

下面介绍配置丢弃规则的操作方法,归并规则和丢弃规则的操作方法类似,详情请参见 《天翼云日志审计系统用户手册》。

通过配置丢弃规则,可以丢弃某些不需要的字段,分为两种:

- 前置丢弃规则: 在采集器根据字段提取规则解析字段之前, 就丢弃整条日志。
- 后置丢弃规则: 在采集器根据字段提取规则解析字段之后, 才丢弃 Syslog 中的某个特 征字符串。

以前置丢弃规则为例,具体操作方法如下:

步骤 1 单击【配置丢弃规则】按钮,进入丢弃规则的前置丢弃规则页签,如图 6-18 所示。

图 6-18 前置丢弃规则(1)

丢	弃规则 第三方安全设备日志_1234			
前	医 奈弗规则 后 派 丢弃规则			0
#	目标设备	匹配方式 / 匹配值		操作
1		· 请选择匹配方式	谈输入匹配值	+



步骤 2 选择目标设备、匹配方式及其匹配值,单击操作栏的一,前置丢弃规则配置完成,如图 6-19 所示。匹配方式参数说明如表 6-1 所示。

图 6-19 前置丢弃规则(2)

丢	· 弃规则 第三方安全设备日志_1234			
m	王 恶弃规则 后置恐弃规则			
				0
	目标设备	匹配方式 / 匹配值		操作
1	10.65.189.189	startsWith; test ×		٠
2	请选择目标设备	· 通话将匹配方式 ·	请输入匹配值	+

表 6-1 前置丢弃规则匹配方式参数

配置项	描述
startsWith	以匹配值开始。
endsWith	以匹配值结束。
Contains	包含匹配值。

步骤 3 前置丢弃规则生效,在LAS 采集器根据字段提取规则解析字段之前,完成整条日志丢弃。 ----结束

修改接入配置

接入配置是指配置数据源的接入参数。修改接入配置的具体操作如下:

步骤 1 进入 接入配置 页面,如图 6-20 所示。

图 6-20 数据源的接入配置页

第三方安	全设备日志_1234
接入设备 接入面	E
接入协议	UDP *
接入端口	1234
数据格式	Syslog
数据编码	* 8-7TU
	编辑武量

步骤 2 单击【编辑配置】按钮,修改接入配置,如图 6-21 所示。 仅支持修改接入端口、数据格式和数据编码,接入协议置灰。



图 6-21 修改数据源的接入配置

第三方安	全设备日志_1234
接入设备接入面	ίΞ
接入协议	VDP *
接入端口	1234
数据格式	Syslog
数据编码	UTF-8 •
	<u> 应用和国</u> 取消



7 _{枚举值}

枚举值用于将各类日志对象输出日志中的字段名及该字段 key 值映射为一个简单易懂的 value 值。

将鼠标悬停在总控制台图标³²³,进入 数据采集 > 枚举值 页面,页面左侧展示 LAS 支持的 11 个日志对象类别,页面右侧列表展示对应日志对象类别已有的枚举值,如图 7-1 所示。

图 7-1 枚举值

□ 枚举值							
日志接入枚举	举值管理						
	总数 (261) 📋			请违择设备规型		▼ 讀选择设备型号/版本	· •
绿盟安全设备日志	李段名	Key	Value	设备类型	设备型号/版本	数据表	操作
第三方安全设备日志	nisk	1	任风险	NF		防火塘日志	1 1
网络设备日志	alerted	1	不告誓	NF		内容过滤日志	/ 0
Windows 主机事件日志	alerted	0	告誓	NF		内容过滤日志	/ 0
Unux 主机系統日志 Web 服务器日志 虚拟化平台日志 网络设备洗量	dropped	1	國進行	NF		防病毒日本 UR(分娩日患 防火衛日患 VPN日患 VPN日患 PR重日患 内容过端日本	× 5
其它日志 文件日志 標題终端日志	dropped	0	非短期	NF		防療審日志 URL分娩日志 防火焼日志 VPD日志 VPD日志 PP読量日志 入機物炉日本 内留近線日本	1 0
	risk	5	赛风险	NF		防火塘日志	/ 0
	risk	4	較獲风险	NF		防火塘日志	Ø 🖞

各类日志对象的枚举值管理操作方法基本相同,下面以天翼云安全设备日志为例进行介绍。

- **步骤 1** 请参见 天翼云设备日志接入,接入天翼云安全设备 NIPS/NIDS,并向 LAS 发送入侵防护 日志。
- 步骤 2 进入 数据采集 > 数据源 页面, 查看已接入的 NIPS/NIDS 信息和已处理日志情况。
 - a. 展示天翼云安全设备 NIPS/NIDS 的已处理日志条数,如图 7-2 所示。
 - b. 单击数据源名称,进入 接入设备 页面,展示天翼云设备信息,如图 7-3 所示。



图 7-2 数据源统计信息

	_0				C
0/s	-	0/s	EXELE (64,367,948)		2
接收		范式化	第2日第(0) 解析失敗(0)	-	
	-				

图 7-3 天翼云设备信息

	意入记录				
	自输入关键词查询				配置括车规则
1	设备 IP	រដូម HASH	设备类型	设备型号/版本	銀作
1	10.65.133.254	8626-95A0-7FA1-CFB9	SAS-ICS	V5.6.10	8
	10.66.246.113	108D-9284-15E2-DEC4	NIPS/NIDS	V5.6R10F00	8

步骤 3 进入 **数据采集 > 枚举值**页面,设备类型选择 NIPS/NIDS,查看 NIPS/NIDS 设备的日志 枚举情况,gr_type 字段的 Key 和 Value 如图 7-4 所示。

图 7-4 枚举值 (gr_type 字段转义)

总数 70	ů			NIPS/NIDS	•	请选择设备型号/版本	• +
	李段名	Кеу	Value	设备类型	设备型号/版本	数据表	操作
	gr_type	5	网络监控类功能	NIPS/NIDS		应用管理日本 防病毒日志 URL分授日志 承级防护日志 人侵防护日志 值誉日本	/ 0
	gr_type	4	可發网络活动機	NIPS/NIDS		应用管理日志 防病毒日志 URL分类日志 電级防护日志 人優防护日志 信誉日志	/ 8
	gr_type	3	信息搜集英攻击	NIPS/NIDS		应用管理日志 防病毒日志 URL分散日志 液级防护日志 人侵防护日志 值誉日志	/ 0
	gr_type	2	凝取权限美政击	NIPS/NIDS		应用管理日志 防病毒日志 URL分娩日志 高级防护日志 人侵防护日志 信誉日志	/ 0
	gr_type	1	拒绝服务类攻击	NIPS/NIDS		应用管理日志 防病毒日志 UR(分类日志 高級防护日志 入侵防护日志	激活 Windows 特到"设置"以激活 Windows。 タ 音

步骤 4 以 gr_type 字段为例,介绍日志详情的查看方法。

a. 进入 数据采集 > 枚举值 页面, gr_type 字段的值是 5, 如图 7-5 所示。

图 7-5 日志接入枚举值列表(gr_type 字段的值)

总数 🗝 🔒				NIPS/NIDS •				诸选择设备型号/版本	•
	字段名	Key	Value	121	备类型	设备型号/版本	数	据表	操作
	gr.type	5	网络监控舆功能	NIP	PS/NIDS		应防UR部入信	特徴日志 特徴日志 (2)供日志 起防約日志 豊石志	/ 0

b. 进入 **日志分析 > 日志检索** 页面,通过日志类型的筛选,可以查看 NIPS/NIDS 产生的 入侵防护日志详情,如图 7-6 所示。



图 7-6 日志检索(入侵防护日志)

筛选条件:	日志樂型:入侵防护	38						
0 截止2023	-02-07 之前的日志日	建氟硅银存、如果检查	8. 请先重载离线日志					
选择时间	〇 最近1小时	〇 最近 24 小	时 🖲 最近7天	〇 最近 30 天 〇	自定义 3分钟 🖌	Þ		
选择属性	• 日志属性	○ 资产属性						
日志来源 IP				源 IP				
目的 IP								
自定义检索	请输入条件							
	保存检索条件					快速检索配置	技发	高级搜索。
显示图表★								
最新日志数	332802						显示空宇段 日志导出	检索结果统计
日志产生的	P	设备类型	日志来源IP	源IP	目的IP	事件篇要描述		动作说明
2023-02-2	0 20:01:20	NIPS/NIDS	10.66.246.113	182.122.220.209	123.59.168.203	POP3服务用户登录认证成功		允许
2023-02-2	0 20:01:19	NIPS/NIDS	10.66.246.113	111.47.226.118	10.200.215.139	Web服务登录请求	激活 Windows 转到"设置"以激活 Wi	nthttivs。

c. 查看详细的日志信息,并且关注 gr_type 字段的内容。 日志原文中,gr_type 字段的值是 5,这里已经转义为"网络监控类功能",如图 7-7 所示。

图 7-7 日志检索(gr_type 字段已转义)

2023-02-20 20:01:20	NIPS/NIDS	10.66.246.113	182.122.220.209	123.59.168.203	POP3服务用户登录认证成功	允许					
日志接收时间: 2023-02-20 20	:00:48				服务类型:5						
级联节点编号: 2efd3b04-35ae	-48fb-be71-31b9	44fbfdc2			Raw信息的长度: 96						
源端口: 63643					告警事件规则ID: 50043						
目的端口: 110					网卡名: G1/2						
协议: 未知					发生时间的毫秒数:0						
目的mac: 90:E7:10:B6:C7:01					协议返回信息: POP3 CLIENT						
源mac: 00:1C:54:FF:08:0A					日志时间: 2023-02-20 20:01:20						
流行程度:1					以整型记录的源IP: 3061505233						
漏洞id: 0					以整型记录的目的IP: 2067507403						
事件持续次数:1					源资产id: 0						
攻击手段说明:网络监控类功能					目的资产id: 0						
操作系统:1					设备hash: 10BD-92B4-15E2-DEC4						
危险程度说明:低					gr_type : (ff:						
原始的包信息: kOcQtscBABxL	/wgKCABFAAA6b	b9AAHMG4qu2etzRe	zuoy/lbAG6Uy5JL8y0Qp	ooAYQPmJmQAAA	攻击手段:网络监控类功能						
QEICGBIC/4rsunnawikbAuk					动作: 允许						
消息关闭: 30721					源安全区: VWireZone						
事件对应的模块:0					目的安全区: VWireZone						
事件结果: 2					设备厂商: NSFOCUS						
技不手段:512					设备型号/版本: V5.6R10F00	1010098					
实际所完成的动作:1					资产名称: 10.66.246.113	221013030					



8 采集终端

本章主要内容如下:

功能	描述
Agent	介绍 Agent 的各类操作方法。

8.1 Agent

Agent 可以在 Windows 主机、Linux 主机、Web 服务器、虚拟化平台或其他日志中安装。 支持对 Agent 进行查看、下载、安装、卸载、数据采集配置、Agent 关联、启/禁用、卸载、删除和强制更新等管理操作。

8.1.1 下载 Agent

Agent 的下载方法如下:

- **步骤 1** 将鼠标悬停在总控制台图标 →, 进入 数据采集 > 采集终端 > Agent 页面, 如图 8-4 所示。
 - 图 8-1 Agent 列表

□ 采集终端						
采集器 设备 Agent						▲下载 Agent
总数 🕕			请输入IP地址、	主机名称、操作系统进行查	D	Q
IP 地址 全部▼	主机名称	主机信息	状态	注册时间 -	最后通信时间 -	操作
		1 智无数据				

步骤 2 单击【下载 Agent】,进入 Agent 下载页,如图 8-5 所示。



图 8-2 Agent 下载页面

志接入	数据源	枚举值	规则管理	采集终端					
□ Agent T	载								┑ 返回上約
❶ 为确保) Agent i	Agent 正常使用 即载方式:1、 {],请开放 UDP 协议 王曾理页面中远程卸	的 514	「薮配置中的 UDP、1 ent 端本地密码卸载(CP 第日。 查看具体操作评情)				
									♦ 下载配置
平台	技	寺版本			安装包	MD5	版本	大小	平台端下载
Wind	ows Vist	ta or later/All Wind	ows release		NSFOCUS-Agent-Windows-1.0.1.msi	4d209bf731a85b1b16fdbc8426e3f37c	1.0.1	280.52Kb	±
👌 Linux	- <mark>x86</mark> Cer	ntOS/Redhat/Ubunt	tu/Debian or other	Linux 2.7 or later	NSFOCUS-Agent-Linux_x86-1.0.1.run	1b651698879b170dfca82a8a623982b9	1.0.1	282.36Kb	±
👌 Linux	-arm Cer	ntOS/Redhat/Ubunt	tu/Debian or other	Linux 2.7 or later	NSFOCUS-Agent-Linux_arm-1.0.1.run	34090dc4a8d74b0e9812adc52f4c4132	1.0.1	268.57Kb	±
👌 SunO	S-i386 Sur	OS5.10/Solaris10 c	or later		NSFOCUS-Agent-SunOS_i386-1.0.1.tar.gz	f65e7ff57376e8979ed1fdf912016405	1.0.1	267.52Kb	±

步骤3下载配置。

单击页面右上角的【下载配置】, 配置平台端 Agent 下载参数, 用于 Agent 与 LAS 平台通 信, 如图 8-6 所示, 平台端 Agent 下载参数说明如表 8-4 所示。

图 8-3 平台端 Agent 下载配置

日石線人 数用牌	tone andre Collin	平台编 Agent 下载配置		×			
		通信配置 (UDP, TCP 编口, F	目于 Agent 与平台读通信,雪保证或口开放)				
		* 曾彊中心 IP 10.65.18	9.171				
O 7588R Agern IERIER Agent Rift Folly 1, -B	- 通行法 UDF 1952的 514 (約1) - UDF THATE THO UDF - 109 (約1). 11月1日日 - 5月16日 (月日) - 2、Agen (日本10月1日日)(日本月に5月11日)	* UDP (HD) 17046					
		* TCP 18E1 17047					OTHER
		服料配置				16:22	TeaTe
		服务工作组 nsfocus					
		股景谷町 nefocuta	iaent				
	CentOS/Redhat/Ubuntu/Debian or other Linux 2.7 or later				23692H2De7cbc4ace15		4
	CentOS/Ardhat/Ubuntu/Cebian or other Linux 2.7 or later	安装配置 (产品标识明于解决多 产品标识 () 量	产品Agent客户端共存利缴) ● 音				
	Sur/Q53.10/Solaris10 or later				8:50x26c+fc881d324170		
			取消	812			

表 8-1 平台端 Agent 下载参数

配置项	描述
管理中心 IP	Agent 的 IP 地址。不填写,表示默认下载的是平台的 agent;如果配置了 IP,下载的是配置 IP 的 Agent。
UDP 端口	Agent 客户端与 LAS 通信用的 UDP 端口号,默认为 17046。
TCP 端口	Agent 客户端与 LAS 通信用的 TCP 端口号,默认为 17047。
产品标识强校验	判断 Agent 共存的标识。默认为"否"。 选择"是",表示 LAS Agent 可以与扫描器、UES 等 Agent 共存。
服务工作组	Agent 在客户端的服务中显示的服务工作组名称, 默认为 CTYUN, 不支持修改。
服务名称	Agent 在客户端的服务中显示的服务名称,默认为 CTYUNagent,不支持修改。



步骤 4 下载 Agent。

返回 Agent 列表,单击平台端下载栏的之,将对应的 Agent 下载到本地(请根据安装平台选择 Agent)。

----结束

8.1.2 安装 Agent

安装 Agent 分为三种情况:在 Windows 系统中安装、在 Linux 系统中安装、在 Unix 系统中安装。

Agent 支持的操作系统均为 64 位,暂不支持 32 位。

在 Windows 系统中安装

鼠标双击或右键单击安装包 CTYUN-Agent-Windows-1.0.1.msi,选择"安装",确认安装 后,弹出安装环境检查对话框,环境满足后,自动完成配置及安装。

在 Linux 系统中安装

- 步骤 1 登录 Linux 主机,切换为 root 权限。
- **步骤 2** 执行命令 "chmod 755 CTYUN-Agent-Linux_x86-1.0.1.run" 赋予 Linux 系统 755 权限,如 图 8-7 所示。

图 8-4 在 Linux 系统中安装 Agent: 赋权

```
[root@lasdot101 opt]#
[root@lasdot101 opt]#
[root@lasdot101 opt]#
[root@lasdot101 opt]# chmod 755 NSFOCUS-Agent-Linux_x86-1.0.1.run
[root@lasdot101 opt]#
[root@lasdot101 opt]# ll | grep Agent
-rwxr-xr-x 1 root root 289161 Nov 19 17:40 NSFOCUS-Agent-Linux_x86-1.0.1.run
[root@lasdot101 opt]#
```

步骤 3 执行命令 "./ CTYUN-Agent-Linux_x86-1.0.1.run", 安装 Agent, 如图 8-8 所示。

图 8-5 在 Linux 系统中安装 Agent: 执行安装

```
[root@lasdot101 opt]#
[root@lasdot101 opt]#
[root@lasdot101 opt]# ./NSFOCUS-Agent-Linux_x86-1.0.1.run
current machine x64
[ ok ] nsfocusagent.service start
agent install successfully in /usr/local/nsfocusagent/nsfocusagent
[root@lasdot101 opt]# ■
```

步骤 4显示 "agent install successfully",表示安装成功。



在 Unix 系统中安装

- **步骤 1** 登录 Solaris 10 主机。
- 步骤 2 执行命令 "gzip -d Setup.tar.gz" 解压 Setup.tar.gz, 得到 Setup.tar 压缩包, 如图 8-9 所示。

图 8-6 在 Unix 系统中安装 Agent:获得压缩包

gzip	- d	Setup.tar.gz		
ls				
	gzip ls	gzip -d ls	gzip -d Setup.tar.gz ls	gzip -d Setup.tar.gz ls

步骤 3 执行命令"tar xf Setup.tar"解压 Setup.tar,得到 Setup 文件夹,如图 8-10 所示。

图 8-7 在 Unix 系统中安装 Agent: 获得 setup 文件夹

bash-3.2#	
bash-3.2#	tar xf Setup.tar
bash-3.2#	ls
Setup	Setup.tar
bash-3.2#	

步骤 4 执行命令 "cd Setup", 进入 Setup 文件夹。

步骤 5 执行命令"./install.sh",进行安装 agent,直至安装完成。

----结束

8.1.3 查看 Agent

将鼠标悬停在总控制台图标[™],进入 **数据采集 > 采集终端 > Agent**页面,展示已经 安装的 Agent 信息,如图 8-11 所示。单击某行 Agent,可以展开查看该 Agent 的配置信 息。

图 8-8 Agent 列表

开篇篇 设备 Agent									
总数 🜗		请输入IP地址、主机名称	1、操作系统进行查询			Q			
IP 地址 全部 ▼	主机名称	主机信息		状态	注册时间 -	最后通信时间—	操作		
10.65.189.142	DESKTOP-M4I46U3	Windows 10 Pro x64 desktop		已离线	2023-02-20 15:02:21		◊ % ≡		
< 1 > 每页10条,共1页,到第 1 页	夏 魂地								

8.1.4 数据采集配置

Agent 安装后,还需对其进行数据采集配置,Agent 才能将日志数据发送到 LAS。 以 Windows 系统为例,数据采集配置方法如下:



步骤 1 在 Agent 列表中,单击操作栏的*,弹出 Agent 数据采集配置对话框,如图 8-12 所示。

图 8-9 Agent 数据采集配置

[10.65.189.171]	Agent 数据采集配置 X
0 支持采集 Win 支持系集 Win 支持监控指定 Fedora 智不支 启用注册表审相 支持配置指定	dows / Linux 系统日志、欽硬件配置变更,外覆设备使用。 dows / Linux 环境下的的应用服务日志、毫距置服务名、日志采集路径、日志文件名路径,及数据发送端口。 显录下,文件的添加。传改、删除等强作,需配置监控文件的路径信息(windows xp 和 server2003系统。Solaris、 持文件目录审统)。 统和主机审计相关配置,可产生相对应的曝塑终误日志(windows xp 都不支持)。 目走类型加密传输振器,默认加密传输策略为否(不加密)
主机采集配置 «	
加密传输	· 퉆 · • · · · · · · · · · · · · · · · ·
系统日志	
应用服务口心 <	日本或集隊級 日本文任文全領級 織口
100.55 TH	
示例:如 wi 在通 文件目录审核 &	ndows 下要监控 R 盘下以 'a' 开头的所有 txt 文件,可使用通配符写法 R\a'.txt E符写法中支持匹配 "(若干个字符),?(单个字符),
加密传输	○ 是 ● 否
文件路径	诸输入监控文件的路径信息
主机审计配置 ≪	
加密传输	○ 是 ● 否
配置项	 移动存储审计 硬件交更审计
	取消尚 研究法

步骤 2 配置主机采集参数,参数说明如表 8-5 所示。

表 8-2 主机采集参数

配置项	描述
是否加密传输	数据传输过程中,是否使用加密传输策略。
系统日志	 默认采集应用程序、安全和系统。 开启后,LAS支持采集的系统日志对象包括转发事件、应用程序、安全、Setup和系统。

步骤 3 配置应用服务日志。

- a. LAS 支持采集 Windows/Linux 环境下的应用服务日志。
- b. 单击【添加】,配置应用服务日志参数,参数说明如表 8-6 所示。支持添加多个应用服务日志。

こ 美美 の

表 8-3 应用服务日志参数

配置项	描述
服务名	 内置服务包括以下六种: Nginx 日志:对应 Web 服务器的 Nginx 接入格式。 Linux 主机系统日志:对应 Linux 主机的系统日志。 Apache 普通日志:对应 Web 服务器接入的 Apache 服务类型的 Common Log Format, Common Log Format。 Apache Error 日志:对应 Web 服务器接入的 Apache 服务类型的 Error log。 Weblogic 日志:对应 Web 服务器接入的 Weblogic 服务类型的 Custom Log Format。 IIS 日志:对应 Web 服务器接入的 IIS 服务类型的 Custom Log Format。 IIS 日志:对应 Web 服务器接入的 IIS 服务类型的 Custom Log Format。 第二、对应 Web 服务器接入的 IIS 服务类型的 Custom Log Format。 第二、对应 Web 服务器接入的 IIS 服务类型的 Custom Log Format。
日志采集路径	日志文件的上一级文件夹路径。
日志文件名路径	日志文件的具体路径。
端口	用于日志采集数据发送的端口号。取值范围为 1~65535。

步骤 4 配置文件目录审核参数,参数说明如表 8-7 所示。

LAS 支持监控指定目录下文件的添加、修改、删除等操作。

表 8-4 文件目录审核参数

配置项	描述
是否加密传输	数据传输过程中,是否使用加密传输策略。
文件路径	监控文件的路径信息。支持多个路径,用回车符分隔。

步骤 5 配置注册表审核。

- a. 注册表审核默认开启。
- b. 注册表方式可选项有全局、自定义,选择自定义时,还需配置监控注册表的路径。
- 步骤 6 配置主机审计参数,参数说明如表 8-8 所示。

表 8-5 主机审计参数

配置项	描述
是否加密传输	数据传输过程中,是否使用加密传输策略。
配置项	可选项有移动存储审计、硬件变更审计、软件变更审计、帐号变更审计、密码 变更审计、用户登录审计、进程创建审计、网络连接审计,支持多选。



步骤7 单击【确定】按钮,保存配置。

----结束

Agent 关联

通过 Agent 关联,可以按照 Agent 来查看日志信息。

在 Agent 列表中,单击操作栏的条,选择【查看日志】,跳转至日志检索页,展示该 Agent 相关的日志信息。后续操作方法请参见 日志检索。

8.1.5 启用/禁用 Agent

在 Agent 列表中,单击操作栏的**三**,选择【启用】/【禁用】,确认后即可启用/禁用对 应的 Agent,如图 8-13 所示。禁用后, Agent 状态栏中显示"已离线"。

对于离线状态的 Agent,不支持禁用功能。

图 8-10 启用/禁用 Agent

□ 采集终端						
采集器 设备 Agent						▲下载 Agent
总数 🌗			语输入IP地址、主机名称、操作系统进行查询			
IP 地址 全部▼	主机名称	主机信息	状态	注册时间一	最后通信时间 -	操作
10.65.189.142	DESKTOP-M4I46U3	Windows 10 Pro x64 desktop	日幕线	2023-02-20 15:02:21		0 % ≡
< 1 > 每页10条,共1页,到簿 1	页 确定					禁用 卸戦 删除

8.1.6 升级 Agent

对于离线状态的 Agent,不支持升级功能,如图 8-14 所示。

在 Agent 列表中,单击状态栏的之,开始进行 Agent 版本同步;若 Agent 有新版本,自动进行更新;更新完成后,状态栏显示"已最新"。

图 8-11 离线 Agent 不支持升级

□ 采集终端						
采集器 设备 Agent						▲下载 Agent
总数 💶			请输入IP地址、主机名称、操作系统进行重调			۹
IP 地址 全部▼	主机名称	主机值服	Agent 已來說,請检查设錄或网络 当該	注册时间一	最后通信时间一	操作
10.65.189.142	DESKTOP-M4I46U3	Windows 10 Pro x54 desktop	已氟级	2023-02-20 15:02:21		○ % ≡
< 1 > 每页10条,共1页,到第 1	页 确定					

8.1.7 强制更新 Agent

对于离线状态的 Agent,不支持强制更新功能。

在 Agent 列表中,单击状态栏的€,或者单击操作栏的**三**,选择【强制更新】,即可更 新对应的 Agent。状态栏显示实时的更新进展,如表 8-9 所示。



表 8-6 Agent 更新状态

Agent 更新状态	描述
检查中	表示正在检查 Agent 是否有更新版本。
更新中	表示正在更新 Agent 版本,通过进度条显示更新进度。
更新失败	表示本次更新失败。
己更新	表示已经更新到 Agent 最新版本。

8.1.8 卸载 Agent

对于离线状态的 Agent,不支持卸载功能。

卸载在线 Agent

在 Agent 列表中,单击操作栏的**三**,选择【卸载】;确认卸载后,提示卸载成功,完成 卸载;卸载完成后,状态栏显示"已卸载"。



卸载离线 Agent

卸载 Windows 系统和 Linux 系统中的离线 Agent 有所区别,下面分别予以介绍。

卸载 Windows 系统中的离线 Agent

- **步骤 1** 卸载 Windows 系统中的离线 Agent 之前,请联系天翼云科技的技术支持人员获取离线卸载包。
- 步骤 2 以管理员权限启动 cmd.exe。
- 步骤 3 在 cmd 界面输入如下命令,按回车键。

rundll32.exe C:\Windows\System32\服务名].dll,u[卸载密码]

例如: Agent 安装后,服务名为 nsfagent,此时在 cmd.exe 中输入 rundll32.exe C:\Windows\System32\nsfagent. dll,u 5ba010200b3dd72b7ca33c9102eccd38,按回车键后, 完成卸载。

步骤 4 卸载完成后, Agent 列表中对应的 Agent 状态栏显示"已卸载"。



卸载 Linux 系统中的离线 Agent

卸载 Linux 系统中的离线 Agent 的具体操作如下:

- **步骤 1** 登录 Linux 主机。
- 步骤 2 卸载 Agent, 如图 8-15 所示。
 - a. 执行命令"./ CTYUN-Agent-Linux_x86-1.0.1.run"找到 agent 安装包。
 - b. 根据提示输入"y",输入卸载密码,选择卸载 agent。

图 8-12 执行卸载



步骤 3显示 "agent uninstall successfully", 卸载成功。

----结束

8.1.9 删除 Agent

在 Agent 列表中,单击操作栏的 ,选择【删除】,确认后,即可删除对应的 Agent。

	• 在线状态的 Agent 删除后,若进行刷新操作, Agent 会重新出现在 Agent 列表 中。
注意	• 只有离线状态的 Agent 可以被彻底删除,删除后不可恢复,请谨慎删除离线状态的 Agent。



9 _{规则管理}

在规则管理页面,可以查看并导入或导出日志规则。

将鼠标悬停在总控制台图标^Ⅲ,进入 **数据采集 > 规则管理**页面,初始状态下,展示 内置的日志规则,如图 9-1 所示。

图 9-1 规则管理

□ 规则管理			
規則数 (392) 🖕		▲ 規則導入 可能入規則信息対 [規	则) 形地进行制造 Q.
接入对象 全部 ▼	规则信息	内置规则 全部 -	撮作
绿盟安全设备日志	设备类型: NIPS/NIDS 设备型号/版本: V5.6R10F00	8	查看 深生 影除
绿壁安全设备日志	设备类型: NIPS/NIDS 设备型号/版本: V5.6R11F00	5	查看 深生 删除
绿壁安全设备日志	设备线数: NTA 设备数号/低本: V4.5R89F00	8	28 Re 200
绿壁安全设备日志	设备关键: NIPS/NIDS 设备型号//后本: V5.6.7	8	夏春 深生 新除
绿壁安全设备日志	设备被型: NIPS/NIDS 设备型号/版本: V5.6.8	8	夏夏 深生 動脉
绿壁安全设备日志	设备被型: NIPS/NIDS 设备型号/版本: V5.6.9	8	查看 派生 影除
傳歷安全设备日志	设备类型: TAC 设备型号/版本: V2.0801F00	8	夏夏 深生 肥料
總證安全设备日志	设备类型: SAS 设备型号/版本: V5.6.7	鬼	建 石 游生 肥料
志日番份全安證制	设备地型: SAS 设备型号/版本: V5.6.8	2	20 X± 200
總盟安全设备日志	设翰美型: SAS 设赖型号/版本: V5.6R10F00	£	20 ike Bik
總盟安全设备日志	後輪美型: NF 後輪型号/版本: V6.0R03F00	A.	11 1 2 1 10
柳盟安全设备日志	设备进型: WAF 设备型号/版本: V6.0R06F00	A	立石 派生 肥除
總豐安全设备日志	设备通知: WAF 设备型号/版本: V6.0805F01	晟	10 (42 (88)

•	• 内置日志解析规则,不支持删除和导出。
说明	 接入对象为天翼云安全设备日志、数据库数据和 Linux 主机系统日志的规则, 不支持派生功能。

导入规则

单击【规则导入】,单击【点击选择文件】按钮或者将日志文件拖拽到指定区域,单击 【导入】按钮,完成日志规则的导入。

导出规则

单击规则列表上方的4,支持批量导出所选的日志规则。



查看提取规则

在规则列表中,单击操作栏的【查看】,可以查看对应的规则详情。

派生规则

在规则列表中,单击操作栏的【派生】,可以在该规则的基础上稍作修改,生成一条新规则。

删除规则

在规则列表中,单击操作栏的【删除】,可以删除对应的自定义日志解析规则。



10 资产管理

LAS 最多支持管理 10000 个资产,即手动添加资产、手动导入资产和自动发现资产的总数不允许超过 10000 个。若待添加资产数量超过 10000 个,系统将提示用户超过上限。

本章主要内容如下:

功能	描述
资产总览	介绍新建资产、资产导出和资产导入的操作方法。
资产发现	举例介绍资产发现和资产入库的操作方法。

10.1 资产总览

进入 资产管理 > 资产总览 页面,页面左侧可以切换展示不同的属性及属性组,页面 右侧以列表方式展示资产列表,其中,日志接入处接入的设备 IP 将自动添加在资产列表 中,并归属"日志源"标签,如图 10-1 所示。

图 10-1 资产总览

□ 资产总范							م
资产组 🗸	全部						
输入关键字筛选	資产数 15 🔖 🖋 🏛					资产导出	资产导入 新型的产
未分美资产 15	□ 避产	遗产名称	标签		价值 联系人	更新时间	操作
+ 9752	□ ₽ 10.65.148.95 [#69885 ^m]	10.65.148.95	日志潮	更多。	ĩ	2022-09-27 16:02	% ≠ ©
	□ 早10.65.148.234 [本分報22 ²⁴]	10.65.148.234	日志園	ES v	1	2022-09-27 15:55	% ≠ 11
	□ 早10.65.150.134 [未分娩的术]	10.65.150.134	日志源	更多又	۲.	2022-09-27 15:50	% ≠ ±
	□ □ 10.65.144.8 [未分使资产]	10.65.144.8	日志派	ES v	î.	2022-09-27 15:30	% ≠ ±
	□ ₽10.65.148.65 [未分类图产]	10.65.148.65	(日本課)	更多 ×	۲.	2022-09-27 15:21	% ≠ ¤
	□ 10.65.150.133 [未分與资产]	10.65.150.188	日志激	₩S ×	D	2022-09-27 15:19	% / □
	□ [□] 255255255255 [未分类约产]	255.255.255.255	「日本源」	₩S ×	Î)	2022-09-26 16:27	% ≠ ≣
	□ <mark>□ 1.1.1.1</mark> [未分與資产]	1.1.1.1	日志源	ES ×	D	2022-09-26 15:57	% ≠ ±
	□ 早240e659:120:223:00:189:173 [未分类数率]	240e:659:120:223::189:173	目志蒸	更多、	٦ ۲	2022-09-23 18:40	% ≠ =
	□ □ 10.65.189.131 [未分與資产]	10.65.189.131			D	2022-09-23 18:39	% ≠ ₫
	< 1 2 > 每页10条,共2页,到第 2 3	ē 确定					



10.1.1 新建资产

新建资产的详细步骤如下:

步骤 1 单击资产总览页面右侧的【新建资产】按钮,进入新建资产页,如图 10-2 所示。

图 10-2 新建资产

口 新建资产			5 运回上级
幕中信息 主机信息 服务信息 应用	信息	2	2月 靖定
* 1P 18.52			
	批量添加进产		
西产名称			
1815.	80058		
	府 省 市区 日本週		
• 资产组	请输入关键字直线	= /	
地理位置	请输入关键字直线	= /	
业劳养统	请输入关键字直找	≡ ″	
短时来的	请输入关键字直线	≡ /	
经纬度	88		
联张人			
联系人創稿			
联系人事机带			

步骤 2 配置资产的基本信息。

- 步骤 3 (可选)进入 主机信息 页面,配置资产的主机信息。
- 步骤 4 (可选)进入 服务信息 页面,单击【添加服务信息】,配置资产的服务信息。
- 步骤 5 (可选)进入 应用信息 页面,单击【添加应用信息】,配置资产应用信息。
- 步骤 6 单击【确定】按钮,保存配置。
 - ----结束

10.1.2 资产导出

资产导出的操作方法如下:

步骤1 在资产列表中选择需要导出的资产,如图10-3所示。



图 10-3 资产总览

资产总元						
276	~	全部				
输入关键字描选		资产数 💶 (213)76) 🗣 🧨 📋				资产导出 资产导入 新建资产
朱分美资产	6	☑ 资产	资产名称	标签	价值 联系人	更新时间 操作
+ 812		☑ □ 10.65.4.206 (#SHREE**)	10.65.4.206	Eta	Es.	2023-02-24 08:58 % 🖋 🗊
		☑ ↓10.65.7.120 (未分気性产)	10.65.7.120	Baa	BS. 1	2023-02-23 21:18 💊 🖌 🗉
		 (a) (a) (a) (a) (a) (a) (a) (a) (a) (a)	10.11.11.11		ĩ	2023-02-23 20:06 % 🖌 🛙
		☑ □ 10.65.189.142 (未分規肥/*)	10.65.189.142	B&A		2023-02-23 17/00 % 🖋 🛍
		□ 10.65.189.175 (±0.96007*)	10.65.189.175	(188 8)		2023-02-23 17:00 % 🖋 🗓
		☑ ☐ 10.65.68.108 (#-9.95/807*)	10.65.68.108	842	RF (1)	2023-02-23 17:00 % 🖌 🗓
		< 13 > 每页10条,共1页, 到	1 页 确定			

步骤 2 单击【资产导出】按钮,将选定的资产信息导出至本地备份,如图 10-4 所示。

图 10-4 资产导出完成



----结束

10.1.3 资产导入

	批量导入资产时, LAS 允许的最大资产数为1万。
	导入资产的规则如下:
说明	• 若资产列表中已存在相同 IP 的资产,会自动跳过,已有的资产信息及其属性 不受影响。
PG 73	• 若资产/属性不存在,导入后会自动新建资产/属性。
	• 对于未存在于资产文件中但资产列表中已有的资产,不会被删除。

除了手动新增资产,LAS 也支持批量导入资产信息。导入资产信息的操作方法如下:

步骤 1 在资产列表上方,单击【资产导入】按钮,进入资产信息导入页,如图 10-5 所示。

图 10-5 资产信息导入



步骤 2 单击【下载导入模板】,将资产信息模板下载到本地。



- **步骤 3** 在本地打开资产信息模板,按照模板提示录入资产信息,保存为 XLSX 文件,如图 10-6 所示。
 - a. 在本地编辑资产信息时,必须使用 Office 2019、Office 365 或者 WPS 2016 及以上版本。
 - b. 请参考填写说明,填写主机资产、资产信息和字段信息。

图 10-6 录入资产信息

- 步骤 4 返回资产列表,单击【资产导入】按钮,进入资产信息导入页。
- **步骤** 5 单击【点击选择文件】按钮或者将资产信息文件拖拽到指定区域,等待导入完成,如图 10-7 和图 10-8 所示。

图 10-7 资产信息正在导入

口 资产导入	
文件名称	export/set_templates/s
文件大小	0.0348
	<u> 30</u>
	正在分析得人遗产,请等待

图 10-8 资产信息导入完成

口资产导入	n #*9X				
文件名称	esportAsset_template.uks				
文件大小	COME				
	资产导入成功				
	通题 or 继续得入				

- 步骤 6 (可选) 单击【继续导入】, 重复上述步骤导入其他资产文件。
- 步骤 7 单击【返回】按钮,返回资产列表,查看新导入的资产信息,如图 10-9 所示。

图 10-9 资产列表(已完成资产导入)

全部						
资产数 💶 🔖 🖋 🃋					资产导出	资产导入新建资产
资产	资产名称	标签	价值	联系人	更新时间	操作
□ 早22.22.22.22 (未分类如产)	22.22.22.22	日志源			2023-02-24 11:19	% ≠ ±



10.2 资产发现

LAS 支持通过分析上报的日志信息来自动发现资产,无需手动获取资产,大大减轻用户的工作量。

资产发现的规则如下:

- 若正式资产和待入库资产中都没有该资产,对该资产进行发现操作。
- 若正式资产中没有但待入库资产中有该资产,更新待入库资产中该资产的发现时间。
- 若正式资产中有但待入库资产中没有该资产,丢弃该条发现日志。

当 LAS 发现资产时,将资产信息存放在 LAS 的待入库资产列表中;在待入库资产列表中, 按照发现资产时的资产属性,对资产进行归类。资产入库后,该资产才能成为正式资产, 纳入 LAS 管理。

10.2.1 场景

通过 SAS-ICS 设备的病毒检测日志,可以发现资产并进行资产入库。

10.2.2 配置步骤

资产发现的操作方法如下:

步骤 1 请参见 天翼云设备日志接入,在 LAS 平台中接入 SAS-ICS 设备,如图 10-10 所示。

图 10-10 天翼云安全设备列表(已接入 SAS-ICS 设备)

擅入设备				
造输入关键设施设				配置当年成时
≓ i⊋∰ IP	iĝe HASH	设备类型	设备型号/版本	操作
1 10.65.7.120	4920-8904-1863-AC04	SAS-ICS	V6.0R11F00	

步骤 2 进入 资产管理 > 资产发现 页面,单击【配置日志分析】按钮,配置日志分析参数, 如图 10-11 所示。

待发现 IP 范围,支持配置 IP 段。



图 10-11 配置日志分析

II 配置日志分析		
1	▶ 配置给发现 IP 范围	
	10.241.41.154 10.241.41.156	
2	 配置倚灰現日志美型 	8
	病毒检测日志 💌	
3	 • 是否开启 ・ 量 ○ 否 	
	取消 微音	

- 步骤 3 使用回放工具构造流量,等待几分钟。
- **步骤 4** 进入 资产管理 > 资产发现 页面,展示最新发现的资产 IP 和发现时间,如图 10-12 所示。

图 10-12 资产发现

□ 资产发现					
					遗日志分析 []
资产数 🛃 😳 🏛			请输入失健学时【他产】利进行算法		
□ 类型 资产	资P ^{ase} 组	状态	首次发现时间	最近一次发现时间	操作
□ 主称 10.241.41.156	未分詞因严	最新发现	2023-02-23 21:31	2023-02-23 21:31	
□ 主机 10.241.41.154	未分黄资产	最新发现	2023-02-23 21:31	2023-02-23 21:31	8
< 🛐 > 毎页10条,共1页,到第 1 页 執 数	ž.				

步骤5(可选)资产入库。

勾选需要入库的资产,单击列表左上方的④,将所选资产入库。



11 _{日志分析}

本章主要内容如下:

功能	描述			
日志检索	介绍日志的检索方法,包括查看日志详情、高级检索、快捷检索、保存检索 条件、历史日志检索、重点关注日志查看、日志列表配置和日志导出的方法。			
主机审计分析	介绍主机审计日志的分析方法和分析结果的查看方法。			
Web 服务器日志分析	介绍 Web 服务器日志的分析方法和分析结果的查看方法。			
自定义仪表盘	介绍仪表盘的自定义方法。			

11.1 日志检索

进入 **日志分析 > 日志检索** 页面,默认展示最近 1 小时接收的全部日志情况,如图 11-1 所示,日志检索页面布局说明如表 11-1 所示。

图 11-1 日志检索

日志英型 快速检索 重点关注	e 福祉保存: 日元成款金利日石
OVERNIEW I	
全部日志	1845日1月 ● 載江21 小村5 載江24 小村5 第254
+ 绿盟安全设备日志 + 绿盟终强日志	治済同注 ● 日表開注 ○ 波戸開注
+ 第三方安全设备日志	日志未遂 P
+ 网络设备日志	1970 June 1970 J 2014
+ Windows 王初都件日志	一日之间 龙山 化合金属
+ Unux 土机制計口心	· · · · · · · · · · · · · · · · · · ·
+ 网络设备流量	
+ 其它日志	
	0
	11.7503日
	♀ 自定文检索中、您可以没再查询日志:
	1.金文检索。例3DEA: 200, error, quick brown,
	2. 附近学科全文检索。例ZIEA): dcartsystem。
	3. Faihan 2020年3月11日前海道2003年99),学校国家A. author? John Smith*, 4. Faihan 2020年3月11日(1997年3月11日)(1997年3月11日)(1997年3月11日)(1997年3月11日)))
	* a statustication is production into (*, *, *, *, *, *, *, *) by balance visition 2000, control (*, *) cont
	6.分验需指导、受出使用运导() 对唐州最终地行分验需用,每回输入: status200 AND (port80 OR port443), title(quick OR brown),
	7.通晓符通讯,支持区题"任于个字明,?"(她个字明, 参加第 人:statuses"。
	8. 全文位面特种学符(如1. /) 要要原如(U) 转义。例如面入:G1/1、转义面为G1/U1。



表 11-1 日志检索页面布局说明

区域	描述		
日志搜索方式	 页面左侧支持切换页面,通过以下三种方式进行日志检索: 日志类型:默认展示全部日志,也可以按照日志类型进行搜索。支持日志类型名称的模糊查询。 快捷检索:支持使用常用的检索条件,快速搜索满足条件的日志。请参见快捷检索日志。 重点关注:支持设置重点关注的日志类型,快速搜索满足条件的日志。请参见重点关注日志。 单击图标《可以将日志搜索方式区域隐藏起来,再次单击可恢复显示。 		
日志捜索条件	页面右侧的日志搜索条件区域默认显示高级搜索条件,单击【高级搜索】 可以切换基本搜索模式和高级搜索模式。请参见日志基本/高级搜索。 日志检索后,单击【保存检索条件】可将当前的搜索条件保存为模板,以 便于快捷检索。请参见保存检索条件。		
日志统计图/日志列 表	日志检索后,展示日志统计图和日志列表。 日志统计图:默认不显示。单击【显示图表】,展示符合条件的日志数量趋势图,将鼠标悬停在图中可显示具体时间及其对应的日志数量;单击【隐藏图表】可以将日志统计图隐藏起来。单击统计图右侧的图标支持以下操作。 ✓		
日志检索帮助说明	进行日志检索之前,页面右侧底部展示自定义检索的帮助说明。		

11.1.1 日志基本/高级搜索

日志搜索支持基本搜索方式和高级搜索方式,单击【搜索】按钮,页面默认以列表形式 展示搜索结果。查询条件说明如表 11-2 所示。

表 11-2 日志查询条件

查询项		描述
	时间范围	选择产生日志的时间范围,支持最近1小时、最近24小时、最近7天、最近30天和自定义起止时间。
基本 搜索	刷新频率	自动刷新功能默认关闭,使用 F5 快捷键可以手动刷新页面信息。 若需开启自动刷新,需要先选择刷新频率(可选项有 3 分钟、5 分钟、10 分钟、30 分钟),然后单击 b按钮;自动刷新开启后,按钮变为 ; 再 次单击可关闭自动刷新功能。
高级	选择属性	• 日志属性:查询指定日志类型的日志。日志类型所在的大类不同,需要



查询项		描述
搜索		设置的查询条件略有不同,查询条件说明如表 11-3 所示。 • 资产属性:查询指定资产或指定资产标签的日志。
次立口		选择属性为"资产属性"时,可以指定资产 IP 进行查询。支持资产 IP 的模 糊查询。
页	页) IF	可以通过下拉列表进行选择,也可以通过单击 呈 进行选择。单击
	标签	选择属性为"资产属性"时,可以指定资产标签进行查询。支持多选。
	自定义检索	若要进一步细化查询结果,单击文本框,支持参照弹出的帮助说明输入自定 义检索条件。

表 11-3 日志属性查询条件

查询只	Д	描述		
全部日志	日志来源 IP	日志源设备的 IP 地址。		
工翌二它人识々口士	日志来源 IP	日志源设备的 IP 地址。		
入異乙女王反奋口心	源/目的 IP	日志中的源/目的 IP 地址。		
天翼云终端日志	日志来源 IP	日志源设备的 IP 地址。		
	日志来源 IP	日志源设备的 IP 地址。		
第三方安全设备日志	源/目的 IP	日志中的源/目的 IP 地址。		
	源/目的端口	日志中的源/目的端口号。		
	日志来源 IP	日志源设备的 IP 地址。		
网络设备日志	源/目的 IP	日志中的源/目的 IP 地址。		
	源/目的端口	日志中的源/目的端口号。		
数据库数据	日志来源 IP	日志源设备的 IP 地址。		
	日志来源 IP	日志源设备的 IP 地址。		
Mindaus 计扣审供日士	用户	日志中的用户名称。		
Windows 主机事件口芯	操作	日志中的对主机进行的操作。		
	日志名称	日志的名称。		
山山山之中	日志来源 IP	日志源设备的 IP 地址。		
Linux 主机东统口芯	日志名称	日志的名称。		
	日志来源 IP	日志源设备的 IP 地址。		
Web 服务器日志	客户端 IP	日志中记录的客户端 IP 地址。		
	协议版本	日志中的协议版本信息。		



查询巧	Д	描述
	请求方法	向 WEB 服务器发起请求的方法。
	状态码	WEB 服务器响应请求的状态码。
虚拟化平台日志	日志来源 IP	日志源设备的 IP 地址。
	日志来源 IP	日志源设备的 IP 地址。
网络设备流量	源/目的 IP	日志中的源/目的 IP 地址。
	源/目的端口	日志中的源/目的端口号。
其它日志	日志来源 IP	日志源设备的 IP 地址。

11.1.2 快捷检索配置

日志快捷检索的配置方法如下:

- 步骤1 进入日志检索配置页。支持以下两种方式:
 - a. 在如图 11-1 所示的日志检索页,单击页面右侧的【快捷检索配置】,进入日志监控配置页。
 - b. 在页面左侧的快捷检索页,单击*,进入日志监控配置页。
- 步骤 2 添加分组。
 - a. 单击分组列表的 , 弹出新建分组对话框。
 - b. 配置分组名称(最多支持 30 个字符;不允许包含特殊字符;名称不允许相同)。
 - c. 单击【确定】按钮。
- 步骤3(可选)根据需要,添加子组。
 - a. 在分组列表中选择一个分组。
 - b. 单击右侧子组列表中的 ,弹出添加子组对话框。
 - c. 配置子组名称(最多支持 30 个字符;不允许包含特殊字符;名称不允许相同)。
 - d. 单击【确定】按钮。
- 步骤4 添加检索条件。

选择一个分组/子组,将保存检索条件保存的未分类分组拖拽至该分组中。



单击某个检索条件的名称,将跳转至如图 11-1 所示页面,可以重新配置检索条件。

步骤 5 单击【确定】按钮。



11.1.3 保存检索条件

LAS 支持手动保存 日志基本/高级搜索 使用的搜索条件,以便用户对满足该条件的日志 进行多次搜索。

手动保存日志检索条件的操作方法如下:

- 步骤1 在如图 11-1 所示的日志检索页, 配置日志检索条件。
- 步骤 2 单击【保存检索条件】,弹出检索另存为对话框。
- 步骤 3 配置当前检索条件的名称(最多支持 30 个字符)。
- 步骤 4 保存检索条件。

单击【保存】或【保存并分组】按钮,将检索条件保存至 快捷检索配置 的未分类分组 中。

步骤 5 日志检索条件保存后,可以进行快捷检索。后续操作方法请参见 快捷检索日志。

----结束

11.1.4 历史日志检索

当 LAS 系统的日志接收已满 6 个月,或者系统接入的日志量超过阈值时,超限部分的日 志会按照时间顺序进行压缩后离线。

系统日志离线阈值

系统的内存大小不同,离线阈值也有所不同,具体说明如表 11-4 所示。

内存	阈值描述
内存<48GB	LAS 离线阈值为 30 亿,最多支持重载 2 亿条日志。
48GB≤内存<80GB	LAS 离线阈值为 40 亿,最多支持重载 3 亿条日志。
80GB≤内存<144GB	LAS 离线阈值为 50 亿,最多支持重载 4 亿条日志。
144GB≤内存<272GB	LAS 离线阈值为 77.5 亿,最多支持重载 5 亿条日志。

表 11-4 系统日志离线阈值

重载离线日志

若要查看因超限而离线的日志信息,可以通过重载离线日志对历史日志进行查询/查看。 重载离线日志时,LAS 系统会将压缩的日志信息进行解压。

- **步骤 1** 进入 日志分析 > 日志检索 页面,日志接收已满 6 个月或者系统接入的日志量超过阈 值,页面出现提示信息。
- 步骤 2 单击提示信息中的【重载离线日志】,进入历史日志检索页,如图 11-2 所示。



- a. 页面左侧展示全部日志类型,日志类型后显示的数字表示 LAS 对该类日志进行过离线 缓存,存在离线索引,数字代表离线索引的数量。
- b. 页面右侧以日历方式展示对应类型的日志 1~6 月或 7~12 月的离线缓存情况。当前月份 属于上半年,页面右侧展示 1~6 月的离线缓存情况;当前月份属于下半年,页面右侧展 示 7~12 月的离线缓存情况。

单击某类日志,页面右侧展示该类日志的离线索引情况:

- 灰色气泡表示未重载的离线索引,灰色气泡的数量表示未重载离线索引的数量。
- 绿色气泡表示已重载的离线索引,绿色气泡的数量表示已重载离线索引的数量。
- 灰色气泡和绿色气泡的位置表示离线缓存的时间。

图 11-2 历史日志检索

□ 窩线日志							▲ 法间上级
単位 2020-07-38 元帝的日安已建築時時年 日元: 611日の日来6 5 月、 61年前時入日の早期は 30 亿、東京会村成日 高坂日市共 464,972,996 条	證分的日志高校: 最多可以	夏義 2 亿余日志					
協入地路?	④ 所有日志美型, 最多 2020	可重報 100 天的日志数据 七月	八月	九月	十月	+-月	● 已里致 ◎ 水亜鉱 十二月
業級防护日本 信言日本 皮用管理日本	(7-12)						
TAC告誓日志 VPN日志 防火衛日志							
0.正日志 ■P流星日志							
較振卒审计日志 時後調整12日本							

步骤 3 选择离线索引。

单击页面右侧某个灰色气泡, 气泡颜色由灰色变为绿色, 表示选择该离线索引进行重载。 步骤 4 单击【保存并重载】按钮, 重载选定的离线索引中离线的日志数据, 供用户查询。

----结束

11.1.5 快捷检索日志

LAS 支持使用常用的检索条件,快速搜索满足条件的日志。具体操作方法如下:

- 步骤 1 在如图 11-1 所示的日志检索页,单击页面左侧的【快捷检索】进入快捷检索页。
- **步骤 2** 展开日志类型并选择某个日志类型子组,在页面右侧设置日志搜索条件后,展示符合条件的日志详情。
- **步骤 3** 单击☆即可在重点关注日志中添加该条日志检索信息,该类日志的图标变为★。 若要取消日志类型的重点关注,单击★即可将其从重点关注日志中移除。
- **步骤 4** 日志类型被重点关注后,可以进入重点关注页进行快捷检索。后续操作方法请参见 重点关注日志。





快捷检索必须为三级子组标题,一级和二级子组标题不支持检索。

11.1.6 重点关注日志

LAS 支持设置重点关注的日志类型,快速搜索满足条件的日志。

在如图 11-1 所示的日志检索页,单击页面左侧的【重点关注】进入重点关注日志页,可以直接查询重点关注的日志。同时支持以下操作:

- 单击某条重点关注日志,然后单击★,可从重点关注日志中移除该条日志检索信息。
- 单击某条重点关注日志,然后单击对应的
 并进行拖拽,可在重点关注日志中移动该
 日志的排序。

11.1.7 日志管理操作

日志检索后,页面右侧展示符合条件的日志列表,支持对日志进行查看详情和管理操作。

查看日志详情

在日志列表中,单击某条日志,即可展开查看该日志的详细内容。同时支持以下操作:

- 单击 / 可以配置该日志的字段提取规则。
- 单击 2 可以配置事件规则,增加未解析日志的过滤条件。
- 单击,可以对其它日志-签名信息日志进行验签,验签通过后,显示对应的日志原文。

日志字段配置

单击 **三**可以通过选择字段来控制日志列表的展示内容(最多支持显示 7 列)。支持日志 字段的显示排序。

显示/隐藏空字段

单击【显示空字段】按钮,日志列表会将检索出的日志空字段显示出来,按钮变为【隐 藏空字段】。再次单击此按钮,日志列表会将日志空字段隐藏起来。

日志导出

单击【日志导出】按钮,配置日志导出条件,可以导出当前日志列表中的全部日志。日 志导出条件说明如表 11-5 所示。



表 11-5 日志导出条件

配置项	描述	
设置密码	导出日志的解压缩密码。若不设置,为默认密码 las123456。	
导出形式	每日生成一个文件:日志每个日志类型每日生成一个文件。共生成一个文件:每个日志类型只生成一个文件。	
导出字段	选择导出的日志字段。支持多选。	

	 为了保证日志导出的效率,单次最多支持导出100万条日志,若选择的数据 超过100万条时,只导出最近的100万条日志。
说明	• 若需导出更多日志,建议分批多次进行导出。

检索结果统计

单击【检索结果统计】,可以配置日志检索结果的统计规则。

11.2 主机审计分析

LAS 支持主机日志在线分析,分析结果包括登录概览审计、核心文件/文件夹监控、核心服务监控审计、敏感操作执行审计、异常网络外联审计和帐号密码变更。

使用本功能之前,需前往 Agent 数据采集配置页,添加日志采集策略并获取待分析的主机日志,请参见 Agent。

进入 **日志分析 > 主机审计分析** 页面,选择时间范围(支持过去1天、过去7天或过 去30天),单击【开始分析】按钮,等待日志分析完成;完成后单击【我知道了】按钮, 页面展示指定时间范围的主机审计日志分析结果,如图11-3所示,主机审计分析结果 说明如表11-6所示。



图 11-3 主机审计日志分析

过去1天 过去7天 过去30天 开始分析 2022-09-09 00:00 至 2022-10-06 23:59 日志分析编集 ◎ Agent 取取采集 »	
登录概念审计	*
核心文件/文件央监控	*
核心服务监控审计	*
敏感操作执行审计	*
异宋网络外联审计	*
网络外银行方约主机分布	
199107. 1970-3 1770-3 1005-199209	
ショニが中立用きが設行力が立ち対象がも、利益の発信生化会や在いたりが用かり得知りた成果、な単単的に見当れ、対点が知識が属子弁知る果、最い中立の法行力、再発き一分から、	
账号索码变更	۶

表 11-6 主机审计分析结果

	展示项	描述
	登录失败 IP 分布 TOP10	针对主机日志,展示指定时间范围登录系统失败次数 TOP 10 的 IP 地址及次数,用于辅助检测是否存在疑似暴力破解密码的攻击 行为。 当某个 IP 出现大量登录失败的场景时,疑似为暴力破解攻击场 景。
登录概览	注销登录 IP 分布 TOP10	针对主机日志,展示指定时间范围注销登录次数 TOP 10 的 IP 地址及次数。以可视化的方式分析当前存在异常登录注销的行为。
QΠ	登录成功 IP 分布 TOP10	针对主机日志,展示指定时间范围登录系统成功次数 TOP 10 的 IP 地址及次数。以可视化方式分析登录成功操作涉及的 IP 分布情况。
	登录成功帐户分布 TOP10	针对主机日志,展示指定时间范围登录系统成功次数 TOP10 的帐号及次数。以可视化方式分析登录成功操作涉及的帐号分布情况。
核心文件/ 文件夹监 控	Linux 主机开机自 启动文件监控	开机自启动文件/etc/rc.d/rc.local 是主机的敏感核心文件,系统开机时会自动执行文件中记录的相关命令。 针对主机日志,展示指定时间范围最近 10 次开机自启文件的详细变更记录。
	Linux 主机用户信 息文件监控	主机用户信息文件/etc/shadow 是主机的敏感核心文件,记录主 机用户的相关信息。 针对主机日志,展示指定时间范围最近 10 次主机用户信息文件 的详细变更记录。
核心服务 监控审计	注册表审核监控	注册表属于主机的核心服务配置,用于服务的启停控制与核心权限。 展示指定时间范围最近 10 次注册表的详细变更记录。



展示项		描述
	Linux crontab 监控	crontab 文件属于主机的核心服务配置,用于周期执行 crontab 文件中的命令。 展示指定时间范围最近 10 次 crontab 文件的详细变更记录。
敏感操作 执行审计	su 或 sudo 特权命 令执行的用户分布	su和 sudo命令为主机特权命令,用于非 root 用户提权使用。 以可视化方式展示指定时间范围 su/sudo 特权命令执行的用户分 布,用于辅助查看对应用户是否存在滥用执行命令的情况。
	chmod/chown 敏感 操作执行的 IP 分布	chmod 和 chown 命令用于对文件或者文件夹的访问权限与所有 者进行变更修改,属于敏感操作。 展示指定时间范围执行 chmod 和 chown 命令的 IP 分布。
异常网络 外联审计	网络外联行为的主 机分布	网络外联,是指主机会存在访问外网 IP 的特殊访问场景,如果当前主机属于内网系统,该外联请求属于异常场景,疑似存在攻击行为,需要进一步分析。 展示指定时间范围连接外网次数 TOP 10 的主机及连接次数。
帐号密码 变更	帐号变更	针对主机日志,展示指定时间范围最近 10 次帐号变更的详细记录。
	密码变更	针对主机日志,展示指定时间范围最近 10 次用户密码变更的详细记录。

11.3 Web 服务器日志分析

LAS 支持 Web 服务器日志在线分析,分析结果包括总体概览分析、访客分析、请求关键 点、安全审计分析和响应结果分析。

使用本功能之前,请确保 LAS 已接入 Web 服务器日志。请参见 Web 服务器日志接入。

进入 日志分析 > Web 服务器日志分析 页面,选择时间范围(支持过去1天、过去7 天或过去30天),单击【开始分析】按钮,等待日志分析完成;完成后单击【我知道了】 按钮,页面展示指定时间范围的 Web 服务器日志分析结果,如图 11-4 所示,Web 服务 器日志分析结果说明如表 11-7 所示。



图 11-4 Web 服务器日志分析

急体概览分析							*
Veb访问日志趋势							
100000隆		2					
80000振							
60000条							
40000號							
20000泉		/					
0%	2021-05-07 203	1-05-10 2021-05-13	2021-05-16 2021	-05-19 2021-05-22	2021-05-25 20	21-05-28 2021-05-31	
	開內的Web访问请求的整体趋势变	٤.					

表 11-7 Web 服务器日志分析结果

展示项		描述	
总体 概览 分析	Web 访问日志趋势	展示指定时间范围 Web 访问请求数量的整体变化趋势。	
	请求访问结果分布 TOP10	展示指定时间范围 web 访问请求结果次数 TOP 10 的结果类型及次数,用于分析当前接入的 Web 服务器的运行状况。	
访客 分析	访客请求 IP 分布	展示指定时间范围 Web 访问请求次数 TOP 10 的 IP 地址及次数,用于 分析当前接入的 Web 站点最频繁访问的访客列表。	
	热门资源URL TOP10	展示指定时间范围 Web 访问请求次数 TOP 10 的热门资源及被请求次数,用于分析当前接入的 Web 站点的热点资源。	
请 关 键 点	请求浏览器类型分 布 TOP10	求浏览器类型分 展示指定时间范围 Web 访问请求发起次数 TOP 10 的浏览器类型 数,用于分析当前接入的 Web 站点的客户端类型分布情况。	
	Web 访问请求的 Referer 分布	Referer 是 HTTP 请求头中描述请求来源的字段,可根据该字段对当前 接入的 Web 站点的用户来源进行分析。	
		展示指定时间范围 Web 访问请求中 Referer 字段内容的分布情况。	
	Web 访问请求的转 发地址分布	Web 访问请求中的响应码为 3XX 状态码,一般具有请求重定向的作用, 根据该特点可分析出当前系统中请求重定向的转发地址分布。	
		展示指定时间范围 Web 访问请求中请求响应码为 3XX 请求的转发地址 分布。	
安全 审计 分析	请求状态 404 访客	Web 访问请求中,如果存在某访客 IP 出现大量 404 的访问请求,该访 客 IP 为疑似恶意扫描 IP。	
	u divîtî	展示指定时间范围请求结果为 404 次数 TOP 10 的 IP 及次数。	
	疑似恶意扫描 IP (****)访问涉及面 分布	当 Web 访问中存在某访客 IP 出现大量 404 的访问请求场景,并超过设定的保护阈值,会对疑似恶意扫描 IP (****)访问涉及面进行分析。展示指定时间范围涉及疑似恶意扫描 IP 的 URL。	
响应	请求字节数大于 5KB的 URL 请求分	Web 访问请求中,请求字节数一般会低于 5KB,当大于 5KB 时需要关	



展示项		描述				
结果	布	注分析,是否存在疑似 DDoS 行为。				
分析		展示指定时间范围请求字节数大于 5KB 的 URL 及请求次数。				
	请求成功但响应字 节数为 0 的 URL 请 求分布	Web 访问请求中,如果存在请求成功但响应字节数为0的情况,需要 关注分析是否正常。 展示指定时间范围请求成功但响应字节数为0的URL及请求次数。				

11.4 自定义仪表盘

仪表盘,是指通过将统计项加入分组,并为每种统计项配置统计时间范围的方式配置仪 表盘,通过仪表盘查看日志。LAS 支持通过仪表盘展示重点关注的日志分析信息。

除了系统默认分组之外,为了方便用户分类查看重点关注日志的分析信息,LAS 最多支持自定义 20 个仪表盘。自定义仪表盘的操作方法如下:

- 步骤 1 进入 日志分析 > 自定义仪表盘 页面,初始状态下只有一个默认分组。
- 步骤 2 默认进入默认分组页,单击页面右侧的+,填写分组名称。
 - a. 分组名称最多支持 10 个字符。
 - b. 最多支持创建 20 个分组。
- 步骤 3 单击【确定】按钮,分组创建成功。
- 步骤 4 进入配置图表页, 配置仪表盘图表展示内容。
 - a. 选择统计项。

从左侧的列表中选择统计项(支持多选,支持模糊查询),选中的统计项展示在右侧列 表中。

- b. 配置统计时间。
 - 单击【下一步】按钮,进入配置统计时间页。
 - 分别为已选的统计项配置统计时间范围,可选项有最近3天、最近5天、最近1
 周、最近1个月。支持批量操作。
 - 单击【完成】按钮,保存配置。
- 步骤 5 仪表盘新建后,将鼠标悬停在分组中,出现操作图标支持以下操作:
 - a. 单击夺可以配置对应仪表盘的刷新频率(单位: 秒)。
 - 0表示不自动刷新。
 - 取值范围为 0~180 秒。
 - b. 单击器可以全屏展示对应的仪表盘。
- 步骤 6 (可选)单击页面右侧的➡可以上下拖动调整分组的排序。


12 日志源管理

本章主要内容如下:

功能	描述
日志源监控	从采集器和资产两个维度介绍日志源监控信息的查看方法。
采集资产监控	介绍日志源资产的监控和分析方法。
日志源拓扑	介绍日志源拓扑图的绘制方法。

12.1 日志源监控

LAS 支持从采集器和资产两个维度进行日志源监控。

12.1.1 采集器维度日志源监控信息

LAS 支持选择采集器,并查看指定采集器的监控数据。

进入 **日志源管理 > 日志源监控**页面,默认展示采集器的日志源监控信息,页面顶部 支持采集器监控信息的切换,如图 12-1 所示。采集器维度的日志源监控信息说明如表 12-1 所示。



图 12-1 日志源监控信息(采集器维度)

CU:10.65.189.167	×			127	1999 B 1	
328,465,979	102, +BBM	330,508 (##\$/###(#)	12 ^{接入日志进个数}		1816 (来位图率(研/d)	1814 新时语图中(美小3)
CPU	■2(%) 150 40 40 70 8 142/06 156006 1	5168 153068	與存 (MB) 391 163 SWAPとTHE SWAP	183 23784 32084 Pole ni7-2118 ni7-08	평효 (G8)	296 3689 ambulika: ambulika
Battelise tors • *Pearet e etc. • Recaret • ector 313,468 20	entanate •vindows⊒e cationate	日日次開始 NorfelativeRX2日か 日本Note日日 NoteStateので 同じ Apatite	Be858 195.52775 140,796,133 7,946,983 1,099,716 1,209,130	Helistati 2109 1.000 1.000 600 600 200 1.0000 1.0000 2000000	22000 0000 2200 3400 #872E + 872E + 100	0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-
监控集警			查查更多	重点关注资产		
音響名称	普響內容		音響时间	P		速率(多/s) 解析速率(多/s) 入库速率(多/s)
CPU 2498日至	E.809(10.65.189.167)(PUB)	190%	2022-09-28 17:07:04	172.16.1.1	1 109.383 0	0 0

表 12-1 采集器维度日志源监控信息

展示项	描述		
已处理采集数据总量	展示当前采集器已处理的日志总量(单位:条)。		
今日己处理采集数据量	展示当前采集器今日已处理的日志总量(单位:条)。		
接入日志源个数	展示当前采集器接入的日志源个数。		
接收速率	展示当前采集器的接收速率(单位:条/s)。		
解析速率	展示当前采集器的总范式化速率(单位:条/s)。		
CPU	展示当前采集器的 CPU 占用情况(单位:%),包括 CPU 占用百分比和 近 1 小时的 CPU 占用情况趋势图。		
内存	展示当前采集器的内存占用情况(单位: MB),包括内存占用百分比、 SWAP 占用数、SWAP 总数、内存占用数和内存总数。		
磁盘	展示当前采集器的磁盘占用情况(单位: GB),包括磁盘占用百分比、 磁盘占用数和磁盘总数。		
日志类型分布 TOP5	展示当前采集器的日志量前 5 名的日志类型,包括日志类型分布图和日 志类型数量列表。 单击图例可以取消/显示对应类别在图中的统计,将鼠标悬停在图中可以 查看具体的统计数据。		
采集日志趋势	以面积图方式展示当前采集器的日志采集趋势,单击图例可以切换显示 以下内容: 接收速率:最近 24 小时的日志接收速率变化趋势。 解析速率:最近 24 小时日志的解析速率变化趋势。 日志总量:最近 30 天的日志总量变化趋势。 将鼠标悬停在图中可以查看具体的统计数据。		
监控告警	以列表方式展示当前采集器最新采集的5条监控告警,包括风险等级+		



展示项	描述				
	告警名称、告警内容和告警时间。				
	单击【查看更多】,跳转至消息中心页,后续操作方法请参见 消息中心。				
重点关注资产	在资产维度的日志源监控信息页中已关注的资产信息,会被置顶展示在 这里,包括资产 IP、日志源个数、日志总数(单位:条)、接入速率(单 位:条/s)、解析速率(单位:条/s)和入库速率(单位:条/s)。 单击资产 IP,进入资产维度的日志源监控信息页,后续操作方法请参见 资产维度日志源监控信息。				

12.1.2 资产维度日志源监控信息

在如图 12-1 所示页面的重点关注资产列表中,单击资产 IP,进入对应资产的日志源监控信息页,页面顶部支持资产监控信息的切换,并查看对应资产的监控数据,如图 12-2 所示。资产维度的日志源监控信息说明如表 12-2 所示。

如果当前资产包含多个日志类型,页面顶部显示【更多采集信息】,将鼠标悬停在此可以展示更多采集来源信息。

10.65.109.167	•					 第四
3,130,4	144	998,476	1		22	20
千夫政治の量(名)		今日已处现天景教探索(案)	设备数量日志得数(个)		後以逐漸(系/4)	柳行道率(長/s)
CPU			内存 (MB)		避盛 (G8)	
	96% 96% 95%	N) 23 154023 155528 161023 162528	50%	23644 3208 NRT NRT	34 3%	595 7482 ಡುಕ್ರಾಂಗತ: ಡುಕ್ರಂತ:
统产情意			***	采集日志趋势		
资产名称	10.65.189.167	创建时间 2022-	09-27 04:15:21	15	part and a second	2
联系人	-	肥系电话		12 0-3		
操作系统	NeoKylin Desktop	操作系统版本		9		
等保级制	\$1A1G1	设备类型		6		
1987 R		必需型号		3		
资产错述	-			0	17.00 22.00 23.00 03.00 01.00 02.00 03.00 04.00 05.00 06.00 0	1700 0800 0900 1000 1100 1200 1300 1400 1500 162
					· Mart · Svirt · Hard	
5(3N+HE)3				采集翻流 0	最近开展和1间: 2022-09-29 09:30:49 最近告望时间:	2022-09-28 17:07:04
事件名称	IFIP	目的IP 产生时间	告留代本	告望名称	告璧内容	告留时间
				CPU 运转货管	田田時(10.65.189.167)CPU設計90%	2022-09-28 17.07.04

图 12-2 日志源监控信息(资产维度)

表 12-2 资产维度日志源监控信息

展示项	描述
采集数据总量	展示当前资产的日志总量(单位:条)。
今日已处理采集数据量	展示当前资产的今日已处理采集数据量(单位:条)。
设备数量日志源数	展示当前资产接入的日志源个数。
接收速率	展示当前资产的总接收速率(单位:条/s)。
解析速率	展示当前资产的总范式化速率(单位:条/s)。



展示项	描述
CPU	展示当前资产的 CPU 占用情况(单位:%),包括 CPU 占用百分比和近 1 小时的 CPU 占用情况趋势图。
内存	展示当前资产的内存占用情况(单位: MB),包括内存占用百分比、内存占用数和内存总数。
磁盘	展示当前资产的磁盘占用情况(单位: GB),包括磁盘占用百分比、磁 盘占用数和磁盘总数。
资产信息	展示当前资产的基本信息。 单击【关注】按钮,可将该资产设置为重点关注资产,置顶展示在采集 器维度日志源监控信息的重点关注资产区域。关注后,按钮变为【已关 注】。
采集日志趋势	以面积图方式展示当前资产的日志采集趋势,单击图例可以切换显示以下内容: 接收速率:最近24小时的日志接收速率变化趋势。 解析速率:最近24小时日志的解析速率变化趋势。 日志总量:最近30天的日志总量变化趋势。 将鼠标悬停在图中可以查看具体的统计数据。
事件概览	以列表方式展示最新产生的 5 个事件概览,包括事件名称、源/目的 IP、 产生时间和告警状态。
采集概览	展示最近采集时间、最近告警时间和当前资产最新的5个告警信息,单 击【查看更多】,跳转至消息中心页,后续操作方法请参见消息中心。 单击,可以配置该资产的采集监控参数,参数说明如表 12-3 所示。
近一周关联事件分布 TOP10	展示近一周与当前资产的日志源关联的事件分布 TOP10 及攻击分布图。

表 12-3 采集监控参数

配置项		描述
告警等级		可选项有低、中、高。
CPU 告警阈值/持续时间		 CPU 告警阈值: CPU 的使用率达到设定值, 触发告警。取值 范围为 10%~95%。 持续时间: CPU 告警持续的时间。取值范围为 10~60 分钟。
资源 监控	内存告警阈值/持续时间	 内存告警阈值:内存的使用率达到设定值,触发告警。取值范围为 10%~95%。 持续时间:内存告警持续的时间。取值范围为 10~60 分钟。
	磁盘告警阈值	磁盘的使用率达到设定值,触发告警。取值范围为 10%~95%。
采集	采集空闲告警	开启后,在设定时长内未接收到日志数据,LAS 平台产生告警信息(单位:分钟)。
监控	采集激增告警	开启后,5分钟内采集的日志数据量增幅超过设定值,LAS平台产生告警信息(单位:条)。



	配置项	描述
	采集骤降告警	开启后,5分钟内采集的日志数据量降幅超过设定值,LAS平台 产生告警信息(单位:条)。
采集限速	采集限速	开启后,需要配置资产接入速率的最大值(单位: eps)。 2011 若当前资产存在多个日志源,配置的采集限速会均分给支持 采集限速的所有日志源。

12.2 采集资产监控

LAS 不仅支持对日志进行全生命周期的管控,还支持对日志接入的日志源资产进行实时 持续的监控和分析,及时发现网络中的安全事件及异常资产。

进入 **日志源管理 > 采集资产监控**页面,默认展示所有采集资产的监控数据;单击页面顶部的采集资产类型,展示对应的资产接入列表,如图 12-3 所示,页面展示内容说明如表 12-4 所示。

图 12-3 采集资产监控

6 交主设备	2 Misiga	1 政策本報	ESE 2	nips	0 Web 服务器	4 никое
接入资产					请他人 IP 对很入资产进行描述	
IP	日志源数重(个) -	日志总数(条) -	'	解析速率(祭/s) -	入库速率(禁/s) -	最近采集时间 -
10.65 189 101	2	26,291,276	294	297	291	2022-03-22 15:12:44
10.66 240 122	1	113,796	1	1	1	2022-03-22 15:12:44
10.65.189.181	6 T	26,978,196	0	0	291	2022-03-22 15:12:44
10.3.3.3	1	0	0	0	0	2022-03-21 17:00:13
10666	1	0	0	0	0	2022-03-21 18:40:21
255.255.255.255	1	0	0	0	0	2022-03-21 14:30:05
10 65 189 138	1.1	1,044,000	0	0	0	2022-03-22 15:12:05
1.1.1.1	1	0	0	0	0	2022-03-21 15:30:07

表 12-4 采集资产监控页内容

展示项	描述
采集资产类型监控	LAS 支持对安全设备、网络设备、数据库服务器、主机设备、Web 服务器和 其他设备进行监控和分析。
	页面顶部展示以上几类采集资产的接入数量。单击数字,以列表方式展示对 应类型的资产接入信息。
采集资产接入列表	采集资产接入信息包括资产 IP、日志源个数、日志总数(单位:条)、接入 速率(单位:条/s)、解析速率(单位:条/s)、入库速率(单位:条/s)和



展示项	描述
	最近采集时间。支持以下操作:
	· 单击表头旁边的图标,可以按照对应字段进行升序/降序排列。
	• 通过资产 IP 进行接入资产的筛选。
	 将鼠标悬停在日志源数量上,显示资产信息和已接入的日志源信息。
	 单击资产 IP,进入资产维度的日志源监控信息页,后续操作方法请参见资产维度日志源监控信息。
	 当一个资产属于多个采集器时,单击资产 IP,选择一个采集器,进入采集器维度的日志源监控信息页,后续操作方法请参见采集器维度日志源监控信息。

12.3 日志源拓扑

LAS 支持配置日志源拓扑图,用户可以根据实际的日志源网络分布情况进行拓扑图的绘制及管理,保存后在首页大屏中展示。

- 步骤1 进入 日志源管理 > 日志源拓扑 页面。
 - a. 若尚未配置日志源拓扑图,页面为空,单击【配置拓扑】进入步骤 2。
 - b. 若己有日志源拓扑,展示已保存的日志源拓扑图,单击 进入步骤2。
- 步骤 2 进入日志源拓扑图绘制页,如图 12-4 所示。

页面左侧展示已接入 LAS 平台的安全设备、主机设备、网络设备、数据库服务器、Web 服务器和自定义节点,页面右侧是拓扑图的绘制区域。

图 12-4 日志源拓扑图绘制页

图 保存配置		<i>诺加油</i> 线 活用和希望	@ 预览
◎ 拖搬添加分组			
✔ 安全设备			
10.65 189 101	10 65 189 101		
	3		
10.65.189.101	255.255.255.255		
▲ 主机设备			
▲ 网络设备			
へ 其他设备			
▲ 自定义节点			
			<u>è</u>
			٩
			Q

步骤 3 编辑拓扑图。

こ 美天 む

- a. 在页面左侧拖动【拖拽添加分组】到绘制区域,鼠标右键单击支持对该组进行以下操作: 重命名、文字位置、列数调整、宽度调整、高度调整、删除分组。
- b. 在页面左侧单击展开设备列表,拖动设备图标至右侧的绘制区域。
 - 鼠标右键单击设备支持以下操作: 文字位置、移除节点。
 - 鼠标右键单击自定义节点支持以下操作: 重命名、文字位置、移除节点。
- c. 添加设备之间的连线。
 - 单击【添加连线】按钮,按钮出现√,进入连线状态。
 - 鼠标左键单击需要连线的设备图标1。
 - 将鼠标移动至设备图标 2,并单击鼠标左键。
 - 完成设备图标1与设备图标2的连线。
 - 鼠标右键单击连线支持以下操作:连线方式、删除连线。
 - 再次单击【添加连线】按钮,按钮的√消失,退出连线状态。
- d. 单击【活跃度配置】按钮,配置设备活跃度数值。
 当天设备接入日志量达到设定值时,LAS认为此设备为活跃状态。
- e. 在页面左侧展开设备列表,图标右上角出现、的设备,表示已经在拓扑图中。
- 步骤4 (可选) 拓扑图的其他操作。
 - a. 单击 , 居中展示拓扑图。
 - b. 单击 Q, A, 放大/缩小展示拓扑图。
- 步骤 5 单击页面左侧的【保存配置】按钮,保存当前拓扑图,同时支持首页拓扑效果调整配置。
 - a. 进行分组调整、连线添加的操作。
 - b. 设置首页拓扑图,可选项有系统内置拓扑、自定义拓扑。
 - c. 单击【确定】按钮,保存首页拓扑图。
- 步骤 6 (可选)单击【预览】按钮,在线预览当前拓扑图。

----结束



13 事件告警

通过配置事件规则和告警规则,LAS可以产生事件和告警。本章以查看华为抗 DDoS 设备的防护日志为例,具体操作方法如下:

- 步骤 1 使用 admin 帐号登录 LAS 的 Web 管理页面。
- 步骤 2 请参见 第三方安全设备/网络设备接入,接入第三方安全设备日志。

第三方安全设备信息如下:

- 厂商: 华为
- 类型: AntiDDoS
- 型号/版本: 8030
- **步骤 3** 将鼠标悬停在总控制台图标 → ,进入 数据采集 > 数据源 页面,单击上一步接入的数据源名称,确认数据源详情,如图 13-1 所示。

图 13-1 数据源详情页

第三方安全设备日志_225 10.65.189.236 (CU:10.65.189.236)					
接入设备 接入配置					
请输入关键词查询				配置丢弃规则	配置旧并规则
# @&P	厂商	英型	型号/版本		操作
1 10.65.189.101	华为	AntiDDoS	8030		τa

- **步骤 4** 进入 **事件告警 > 事件规则**页面,单击【创建规则】按钮,按照页面提示设置必填项, 如图 13-2 所示。
 - a. 规则模式: 单源过滤模式。
 - b. 攻击阶段/事件类型/风险等级:选择默认值,也可以根据实际需求进行填写。
 - c. 事件源:选择步骤 2 接入的华为抗 DDoS 防护日志。
 - d. 单击【确定】按钮,创建事件规则。



图 13-2 创建事件规则

● 基础设置		
*规则名称	测试事件规则	
"规则模式	 単源过達模式 ● 多源矢联模式 ● 多源対界模式 	
"政击阶段	(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	
*事件类型	网络其他攻击	
"风险等级	(ERE ~	
攻击手段	\$2(#448)四	
攻击方法	本對意思	
规则描述		
2 ,规则设置		
"事件源	华为统DDos额护日志×	
A 华为抗DDoS防护日志 过滤条件	(2里	
设为内部事件	○ 是 ④ 否	
3 • 输出结果		

步骤 5 上一步创建的规则展示在事件规则列表的第一条,默认为启用状态,如图 13-3 所示。

□ 事件規則										则成功	
+ 网络政击		全部									
+ 攻击危害 + 拒绝服务攻击事件	,	現刻数 🖅 🔳 📋 🤞	(建议用用的规则条数不大于 50	条、已已用 11 条规则]					0 检查规则	导入规则(*.dat)	+ OKRAUM
+ 系统入侵事件 + 扫描窃听事件		规则名称	规则描述	事件源	风险等级	事件类型	规则模式	攻击链阶段	内置规则	創建时间	損作
+ 信息破坏事件		創 試事件规则		华为抗DDoS	\star 低风脸	网络攻击/网络其他攻击	单源过油模式	位赛	a a	2023-02-21 16:37:08	. / 0
+ 有害程序事件	0	木马后门通信	特洛伊木马	入侵防护日志	★ 應风脸	系统入侵事件/后门攻击	多源关联模式	命令控制	<u>#</u>	2019-10-28 00:00:00	. / 0
+ 内容安全事件		Spring11396	Springtan	入侵防护日本	* 憲风险	系统入侵事件/应用履词	多源关联模式	攻击渗透		2019-10-28 00:00:00	I / 0
+ 网络钓鱼事件		水恆之證風	永恒之盟 (E	入侵防护日志	* 海风脸	系统入侵事件/应用局词	多源关联模式	命令控制		2019+10+28 00:00:00	. / 0
+ 其它事件		Webshell	webshell是	入侵防护日志	★ 庵风脸	系统入侵事件/系统入侵	多源关键模式	安装工具	-	2019-10-28 00:00:00	. / 0
+ WEB入侵衛件		Web很乐器	Web證房醫	WAF攻击日志	★ 憲风給	系统入侵事件/应用局间	多源关联模式	攻击渗透		2019-10-28 00:00:00	. / 0
+ Windowsamsemite		主机把矿行为	主机得在门	入侵防护日志	★ 憲风险	有害程序事件/有害程序	多源关联模式	恶意活动	是	2019-10-28 00:00:00	. / 0
T CHURCHERE WITH		tomcat漏洞	Tomcat服务	入侵防护日志	* 中风脸	系统入侵事件/应用局间	多源关联模式	攻击渗透	-	2019-10-28 00:00:00	. / 0
		Redis未接权	因为其他受	入侵防护日志	* 中风脸	系统入侵事件/应用尾闾	多源关联模式	攻击渗透	*	2019-10-28 00:00:00	. / 0
		MicrosoftIIS	IIS互联网信	入侵防护日本	* 中国陰	系统入侵事件/应用履词	多源关联模式	攻击渗透	*	2019-10-28 00:00:00	. / 0
		weblogic属	WebLogic	入侵防护日志	* 中风脸	系统入侵事件/应用属词	多源关联模式	攻击渗透		2019-10-28 00:00:00	. / 0
	0	DNS REQUE		總盟ADS攻	★ 夜风险	拒绝服务攻击事件/DNS REQUEST Flood	多遵关默模式	位変	-	2020-04-15 13:44:03	. / 0

图 13-3 事件规则列表

- **步骤 6** 进入 事件告警 > 告警规则 页面,单击【创建规则】按钮,按照页面提示设置必填项, 如图 13-4 所示。
 - a. 规则设置:选择默认值,也可以根据实际需求进行填写。
 - b. 告警方式: 至少选择一种,本示例选择默认的"滚动通知"。
 - c. 告警抑制:选择默认值。
 - d. 单击【确定】按钮,创建告警规则。



图 13-4 创建告警规则

□ 创建告警规则	
Vallademe. / Lowdebb, Roomdelly,	
基本设置	
* 舌鬟名称	测试告偿
告题本级	④ 在● ○ 中● ○ 高●
福述	
1	l. It
規则设置	
* 事件类型	· □ 2
#1938.01 (F1382.01	全部 -
1160 P	• V
27. P	= v
舉注因將者86	= v
告誓方式	
	0 清至少远终一种告爱方式
用5个子 3回5口	O.£ ⊛ 8
地市湖田	0 8 8 5
家动造地	● # ○ 8
产音道印	○ 문 : ● 8
告輩抑制	
室口以菜	5 60 00 01 01 00 00 00 00 00 00 00 00 00 00
2004/state	30
and representations	 NURSEW, WERSHMICH, (5 - 50 (99)) . WHINESAMEDICERYM. (0 - 30 (X) . NEEDEW
	TOHE OLIN

步骤 7 上一步创建的规则展示在告警规则列表的第一条,默认为启用状态,如图 13-5 所示。

图 13-5 告警规则列表

яянях 🚯 û		告警等级: 📕 低 🚦	• • • #	+ CHERCARDAN
音響在称	抑制策略	更新时间 ↓	规则状态 全部 🕶	操作
■ 数式王等	審□长宮:5分钟 抑制資質:0次	2023-02-21 16:42:33	•	/ 0
< 1 > 每页10条, 共1页				

步骤 8 事件规则和告警规则创建完成后,向步骤 2 创建的数据源发送华为抗 DDoS 防护日志。

- 步骤 9 进入 事件告警 > 事件分析 页面, 查看事件告警信息。
 - a. 当前面创建的事件规则已经识别到上传的日志,产生大量事件,事件的告警状态为"待处理",如图 13-6 所示。
 - b. 当前面配置的告警规则识别到系统的待处理事件之后,会按照前面配置的告警方式在页面顶部循环滚动告警信息(包含告警名称、告警发生时间和告警发生次数),同时告警状态变为"已告警",如图13-7所示。



图 13-6 事件分析

事件分析									۹ -
事件类型 请选择 査询 3		时间 2023-02-14	16:47 ~ 2023-02-21 16:47	1	源P 是多可输入10个。多个ip用,分割	•	⊟£3IP	最多可输入10个,多个ip用,分割	•
高风脸 1528	规则命中 TOP5		攻击源 TOP	25		攻击目的 TOF	25		
中风脸 263	0		-8.01 1:591 1:591 1:591 1:591	69.1 68.10.234 68.10.240 68.10.174		192.168 192.168 10.0.02 192.168	1.57.128 1.10.33 1.10.50		
低风脸 27	● 木马斯门通证 ● MicrosoftilS應用的双击渗进 ● web ● 附近即件规则	logic擁國攻击 🛑 tomcat擁國攻	± 0	.126.136 200 张	400 张 600 张	0	1.10.23 50 会	100 张	150 张
事件数 (1818)									
事件名称	事件类型	风险等级	源	日的	攻击阶段	告警状态 标	86	产生时间	操作
测试事件规则	同議攻击/网議其他攻击	* 低风脸	13.216.203.34	11.1.1.18	结察	待处理		2023-02-21 16:46:22	R 👁
測试事件規则	网络攻击/网络翼他攻击	* 任风险	13.63.75.155	11.145.189.2	侦察	待处理		2023-02-21 16:46:20	N (10)

图 13-7 事件分析 (显示告警信息)



----结束



14 _{报表管理}

本章主要内容如下:

功能	描述
我的报表	介绍 LAS 已经成功创建的所有报表的查看方法。
报表任务	介绍报表任务的新建方法和管理方法。
模板管理	介绍报表模板的新建方法和管理方法。

14.1 我的报表

进入 报表管理 > 我的报表 页面,默认展示 LAS 已经成功创建的所有报表,如图 14-1 所示。

图 14-1 我的报表

日报	表文件					٥
Bł	日 日日 日	全部				
报表费	牧 💿 🖸					
	名称	横板名称	分类	文件格式	创建时间	操作
	12345	Web服务器日志报表	应用服务器	e 🖪 🖻	2018-09-07 09:39:48	Ą
	6	Windows主机日志报表	主机报表	e 🗅 🖬	2018-09-06 16:41:47	¢
	12345	Web服务器曰志报表	应用服务器	e 🖪 🖬	2018-09-06 11:53:47	4
	123	Linux主机日志报表	主机报表	e 🖪 🕅	2018-09-06 11:30:24	Ą
	123	Windows主机日志报表	主机报表	e 🗅 🖬	2018-09-06 11:18:20	Д
< 🚺) 每页10条,共1页,	到第 1 页 确定				

查看不同执行周期的报表

单击页面顶部的【日报/周报/月报/季报】,可以查看已经生成的日报、周报、月报或季 报的报表列表。



查看所有报表

单击页面顶部的【全部】,可以查看已经生成的所有报表,包含立即执行、定时执行和 周期执行生成的报表。

下载报表

在报表列表中,勾选需要下载的报表,单击列表左上方的**⊙**,即可将所选的报表文件下 载到本地。

查看在线报表

在报表列表中,单击文件格式栏的 €/ 上/ , 可以在线预览 HTML/PDF/Word 格式的报表。

手动通知/推送报表

在报表列表中,单击操作栏的♀,即可按照如所示的参数配置通知/推送报表。



14.2 报表任务

用户可以根据需要,通过报表任务生成指定内容的报表。报表任务建成后根据执行情况 不同而处于不同的状态,报表状态说明如表 14-1 所示。

表 14-1 报表状态

报表状态	描述
M	调度中
28%	运行中
~	运行成功
×	运行失败
	己停止

14.2.1 新建报表任务

新建报表任务的具体操作如下:



步骤 1 进入 报表管理 > 报表任务 页面。

步骤 2 单击【创建任务】按钮,进入新建报表任务页面。

步骤 3 配置报表任务的任务调度和报表设置参数,参数说明如表 14-2 所示。

配置项	描述
立即执行	创建任务后,立即执行报表任务,生成报表。 起止时间:对该时间段内的数据生成统计报表。
定时执行	创建任务后,在指定时间执行报表任务,生成报表。 • 执行时间:执行报表任务的时间。 • 起止时间:对该时间段内的数据生成统计报表。

• 执行时间:执行报表任务的频度和时间。

• 起止时间:对该时间段内的数据生成统计报表。

生成的报表中包含的内容。支持报表模板的模糊查询。

配置后, 仅对该 IP 或该段 IP 内的数据生成统计报表。

创建任务后,在指定时间周期性的执行报表任务,生成报表。

生成日志来源的 IP 地址或 IP 段。支持 IPv4 和 IPv6,多个 IP 之间用英文逗号分隔。

表 14-2 任务调度和报表设置参数

步骤 4	配置执行设置参数,	参数说明如表 14-3 所示。

配置项	描述	
任务名称	报表任务的名称,取值范围 1~30 个字符。 不能和己有报表任务重名,且不能使用非法字符(以界面展示为准)。	
任务描述	对报表任务的说明,取值范围 1~250 个字符。	
报表类型	支持生成 HTML、WORD、PDF 三种类型报表,默认生成 HTML 类型报表,用户可以 自行选择是否同时生成 PDF、WORD 类型报表。	
	• 8: 生成 HTML 格式的报表。	
	• D. 生成 PDF 格式的报表。	
	• 🐨 : 生成 Word 格式的报表。	

表 14-3 执行设置参数

周期执行

报表模板

日志来源 IP

步骤 5 配置报表通知/推送参数,参数说明如表 14-4 所示。



表 14-4 报表通知/推送参数

配置项	描述	
SETD 推送	是否将报表发送至 SFTP 服务器。启用前,需要配置 SFTP 服务器,配置方法请参见通知配置(FTP/SFTP 配置)。	
3FTF 1庄人	 SFTP 地址: 勾选需要接收报表的 SFTP 服务器。 文件格式: 发送的报表类型。 	



步骤 6 单击【创建任务】按钮,完成新建报表任务的操作。

----结束

14.2.2 管理报表任务

报表任务新建后,进入 报表管理 > 报表任务 页面,可以对列表中的报表任务进行管理。

查看任务

单击报表任务所在行,展示对应的报表任务详情。

删除任务

状态为"调度中"和"运行中"以及周期执行的报表任务,不允许删除。其他状态的报表任务,支持以下两种删除方式:

- 单个删除:单击操作栏的意,可以删除对于的报表任务。
- 批量删除:勾选需要删除的报表任务,单击列表左上方的,可将所选的报表任务删除。

停止任务

单击操作栏的■,可以停止进度小于 100%或调度中的报表任务。

重新执行

单击操作栏的♥,可以重新执行对应已完成或已停止的报表任务。

手动通知/推送

单击操作栏的^①,可以在现有报表任务的基础上增加通知/推送的内容,参数说明如表 14-4 所示。通知/推送仅限当次有效,即不保存本次通知配置。



14.3 模板管理

LAS 默认提供多个内置报表模板供用户使用,不允许编辑、下载和删除。

用户可以根据需要,复制模板或自定义报表模板,方便用户在新建报表任务时直接引用。

14.3.1 新建报表模板

新建报表模板的操作方法如下:

- 步骤 1 进入 报表管理 > 模板管理 页面。
- 步骤 2 单击【新建模板】按钮,进入新建报表模板页面。
- **步骤 3** 单击【为报表模板设置描述】,在展开的文本框中配置报表模板的描述信息,最多支持 250 个字符。
- 步骤 4 配置报表模板的名称。

单击"新建报表模板"旁边的≥,在文本框内填写报表模板的名称(最多支持 30 个字符,不能与已有报表模板重名),单击≤2。

步骤5(可选)添加报表目录。

最多支持配置深度为3的子标题。

- a. 单击【添加目录】,添加新的一级标题。
- b. 将鼠标移至该一级标题上,单击+,可以添加对应的二级标题。
- c. 参考上述操作,继续添加对应的的三级标题或新的目录。
- 步骤 6 配置报表模板内容。

将鼠标悬停在目录区域的某一标题上,显示可以执行的操作图标,操作说明如表 14-5 所示。

《 I+-J] [[[[]]] 合 i L 且	表 14-5	报表模板内容配置
--------------------------------	--------	----------

操作图标	描述	
	配置各级别标题的名称。	
0	配置各级别标题对应区域将展示内容的描述信息。	
11	选择各级别标题对应区域将展示图表的样式。 • 一级标题不支持设置统计项。 • 单击【如需新增统计项,前往统计管理】,跳转至统计项配置页,可以配置 新的统计项。每个报表模板最多支持配置 100 个统计项。	
×	删除不需要的报表目录以及目录下的统计项。	
+	添加子标题。详见步骤 5。	

步骤 7(可选)单击²,可以在右侧区域在线预览报表目录。



步骤 8 保存报表模板。

- a. 单击【保存】按钮,保存报表模板至报表模板列表。
- b. 单击【保存并创建任务】按钮,保存报表模板至报表模板列表,同时进入新建报表任务 页,可以使用该报表模板创建报表任务。后续操作方法请参见新建报表任务。

----结束

14.3.2 管理报表模板

进入 报表管理 > 模板管理 页面,可以对列表中的报表模板进行管理。

查看报表模板

单击操作栏的 ,可以查看对应的报表模板详情。

单击报表模板名称,可以查看该报表模板引用的统计项。

创建报表任务

单击操作栏的[●],进入新建报表任务页,可以使用该报表模板创建报表任务。后续操作 方法请参见 新建报表任务。

编辑报表模板

单击操作栏的,然后单击【编辑模板】,可以编辑对应的报表模板。

删除报表模板

支持以下两种报表模板的删除方法:

- 单个删除:单击操作栏的三,然后单击【删除模板】,可以删除对应的报表模板。
- 批量删除:勾选需要删除的报表模板,单击列表左上方的¹,可将所选的报表模板删除。

复制模板

单击操作栏的**三**,然后单击【复制模板】,进入复制报表模板页面,可以复制对应的报 表模板,在该模板基础上进行编辑,从而生成新的报表模板。

下载模板

不允许下载内置报表模板。对于自定义报表模板,支持以下三种下载方式:

- 单个下载:单击操作栏的,然后单击【下载模板】,可以下载对应的自定义报表模板。
- 批量下载:勾选需要下载的报表模板,单击列表左上方的,然后单击【批量下载】,可以下载所选的自定义报表模板。
- 全部下载:单击列表左上方的♥,然后单击【全部下载】,可以下载所有的自定义报表 模板。



导入模板

单击【导入模板】按钮,可将已经下载的报表模板重新导入 LAS。

查看执行结果

在执行结果栏中单击,弹出历史报表文件对话框,可以执行以下操作:

- 查看使用该模板的报表任务的执行时间和执行结果。
- 单击执行结果栏的图标,可以在线预览对应格式的报表文件。
- 勾选报表任务,单击左上角的⁽¹⁾,可将所选的报表文件下载至本地(包含所有的生成格式)



15 数据管理/备份恢复

本章主要内容如下:

功能	描述
备份恢复	介绍各类接入日志、数据文件的备份方法和恢复方法。
磁盘扩展	介绍 LAS 虚拟化版的磁盘扩展方法。
NFS 配置	介绍 NFS 服务器的配置方法。
超限管理	介绍系统磁盘超限管理策略的配置方法。

15.1 备份恢复

LAS 支持日志备份、日志恢复、文件备份和文件恢复。

15.1.1 日志备份

将鼠标悬停在总控制台图标³,进入 **数据管理 > 备份恢复 > 日志备份**页面,显示临时仓库剩余空间(单位: GB),并支持手动备份和自动备份。

无论是手动备份还是自动备份,LAS 会自动将日志文件存储在"本地临时仓库路径"设置的位置,再将日志文件上传至指定的 SFTP 服务器。其中,SFTP 服务器的配置方法请参见通知配置(FTP/SFTP 配置)

手动备份日志

0

配置手动备份日志参数,单击【开始备份】按钮,开始备份日志;备份完成后,显示成 功备份时间和已备份日志的日期。手动备份日志参数说明如表 15-1 所示。



表 15-1 手动备份日志参数

配置项	描述	
备份日期	选择待备份日志的时间范围,支持快捷选择过去3天、过去5天和过去7天。	
日志类型	选择待备份日志的类型,支持多选/全选。	
目的 SFTP 服务器	选择备份日志的目的 SFTP 服务器,选择后自动检测并显示连接状态。 29 当前 LAS 设备与目的 SFTP 服务器网卡 MTU (最大传输单元) 应至少有 一方为 1500,才能保证 SFTP 功能正常使用。	
本地临时仓库路径	本地临时仓库的路径,用于临时保存备份日志。不支持修改。	

自动备份日志

配置自动备份日志参数,单击【确定】按钮,即可按照最新的配置结果自动备份日志。 自动备份日志参数说明如表 15-2 所示。

配置项	描述	
备份周期	选择待备份日志的备份周期,支持每天一次、每周一次、每月一次,并设置对应的备份时间。	
日志类型	选择待备份日志的类型,支持多选/全选。	
目的 SFTP 服务器	选择备份日志的目的 SFTP 服务器,选择后自动检测并显示连接状态。 29 当前 LAS 设备与目的 SFTP 服务器网卡 MTU (最大传输单元)应至少有 一方为 1500,才能保证 SFTP 功能正常使用。	
本地临时仓库路径	本地临时仓库的路径,用于临时保存备份日志。不支持修改。	
是否启用自动备份	是否开启自动备份功能。	

表 15-2 自动备份日志参数

15.1.2 日志恢复

日志恢复的操作方法如下:

- **步骤 1** 将鼠标悬停在总控制台图标 → 进入 数据管理 > 备份恢复 > 日志恢复 页面,选择目的 SFTP 服务器。
- 步骤 2 显示连接状态正常后,单击【开始恢复】按钮,开始日志恢复。
- **步骤 3** 全部日志恢复完成后,使用具有"系统组件"管理权限的帐号登录 LAS,进入 系统组件 > 系统服务 页面,单击【重启系统】按钮,重启索引存储服务,使数据生效。



----结束

15.1.3 文件备份

将鼠标悬停在总控制台图标³³³,进入 数据管理 > 备份恢复 > 文件备份 页面,勾选备 份对象(支持多选),单击【开始备份】按钮,直至完成文件备份。

15.1.4 文件恢复

文件恢复的操作方法如下:

- **步骤 1** 将鼠标悬停在总控制台图标 → ,进入 数据管理 > 备份恢复 > 文件恢复 页面。
- **步骤 2** 单击【选择文件(*.dat)】按钮,从本地选择通过 文件备份 下载的配置文件,开始自动恢复。
- 步骤 3 (可选) 若导入的配置文件包含数据源或事件规则, 需要手动重新开启, 以使配置生效。
 - a. 重启索引存储服务:使用具有"系统组件"管理权限的帐号登录 LAS,进入 系统组件 > 系统服务 页面,单击【重启系统】按钮,重启索引存储服务,使数据生效。
 - b. 手动启用数据源:请参见 数据源管理。
- 步骤 4 文件恢复后, 会覆盖当前系统的相关配置文件。

----结束

15.2 磁盘扩展

本功能仅支持 LAS 虚拟化版。

当 LAS 系统空间不足时,可通过磁盘扩展功能扩展系统空间容量。每次操作仅支持挂载 1 个磁盘,通过多次操作可以加载多个磁盘。

下面介绍挂载、卸载磁盘的操作方法:

步骤 1 将鼠标悬停在总控制台图标 →, 进入 数据管理 > 磁盘扩展 页面, LAS 将自动检测是 否有可加载的磁盘, 当检测到有可挂载的磁盘时, 展示磁盘信息, 如图 15-1 所示。

图 15-2 可挂载磁盘信息

⑦系統磁盘空间不足时,可通过磁盘扩展,增加系统磁盘全部挂载/卸载完成后,请前往【系统组件】,	存储容量;单次操作,仅支持挂载一个磁盘,可分多次挂载。 重启 索引存储服务 ,使配置生效。
磁盘名称:/dev/sdc	
磁盘大小: 10GB	
磁盘技載	

步骤 2 单击【磁盘挂载】,弹出确认框。



步骤 3 单击【确定】按钮,等待出现页面提示"磁盘挂载成功"。

- **步骤 4** 将鼠标悬停在总控制台图标 → 进入 系统组件 > 系统服务 页面,重启索引存储服务, 使挂载的磁盘生效。
- 步骤 5 (可选) 重复以上步骤, 挂载多个磁盘。
- 步骤6(可选)卸载磁盘。
 - a. 挂载的磁盘可以卸载,单击已挂载磁盘下的【磁盘卸载】,确认后即可卸载相应磁盘。
 - b. 磁盘卸载后,进入 系统组件 > 系统服务 页面,重启索引存储服务,使磁盘卸载生效。

----结束

15.3 NFS 配置

LAS 支持 NFS (Network File System,网络文件系统),当系统存储空间不足时,可以将日 志数据存储到网络文件系统中,达到扩展存储空间的目的。



配置准备

配置 NFS 服务器之前,请确认服务器已安装 NFS 服务,并已对当前 LAS 开放权限。服务器的详细配置步骤如下:

- 步骤 1 新建共享存储目录,并确保拥有读写权限(chmod go+w)。
- **步骤 2** 在/etc/exports 文件中配置客户端权限为 rw,sync,no_root_squash 格式如下: 挂载路径 客户端 ip(权限)

示例: /data 10.65.1.1(rw,sync,no_root_squash)

步骤 3 重新加载 nfs 配置,执行命令 exportfs -rv

----结束

配置方法

将鼠标悬停在总控制台图标题,进入 数据管理 > NFS 配置 页面,配置 NFS 服务器 IP 地址和存储路径;单击【保存配置】按钮,保存配置。

NFS 服务器配置完成后,单击》可以编辑服务器参数。





若服务器共享目录磁盘空间不足,消息中心将会出现告警信息,同时停止数据转 移。

15.4 超限管理

通过超限管理,可以设置系统磁盘的超限管理策略,包括磁盘占用率超限和磁盘数据保 存时间超期。

将鼠标悬停在总控制台图标[™],进入 **数据管理 > 超限管理**页面,配置超限管理策略参数,单击对应的【应用配置】按钮,完成策略配置。超限管理策略参数说明如表 15-3 所示。

表 15-3 超限管理策略参数

配置项		描述	
超限删除	设 置 删 除限度	当系统磁盘的占用率达到设定值时,将触发告警。 取值范围为 50%~90%,默认值 90%。	
	设 置 删 除天数	当系统磁盘占用率达到"设置删除限度",将一次清除指定天数内的日志 信息,或者自动重复多次删除动作,直到磁盘可用空间降至超限阈值之下。 取值范围为 1~7天。	
超期删除 (日志)	设 置 删 除状态	默认为禁用。	
	设 置 时 间期限	启用后,当日志存储时间超过设定值,系统自动删除超出天数的日志。 取值范围为 180~1000 天,默认为 180 天。	
超期删除 (审计日志)	设 置 删 除状态	默认为禁用。	
	设 置 时 间期限	启用后,当审计日志存储时间超过设定值,系统自动删除超出天数的审计 日志。	
		取值范围为 180~1000 大, 默认为 180 天。	



16 _{消息中心}

LAS 提供消息中心提醒功能,当有需要通知用户的消息产生时消息中心会进行提示。以下情况会触发消息中心提醒功能:

- 设备注册、设备状态变化、删除设备。
- 证书过期及过期前提醒。
- 运维监控告警。
- FTP、邮件发送失败。
- 需要发送邮件,但是未在事件通知中配置服务器信息。
- 级联联动状态异常告警:系统进行级联上下节点的双向存活检测、软件版本和时间一致 性检测,异常时消息中心告警提醒。

若触发消息提醒,在页面右上角快捷工具栏的消息中心中会出现提示信息条数 单击图标,进入未读消息页面,如表 16-1 所示。

图 16-1 消息中心

□ 消息中心		
		◆ 消息通知 未透消息 已透消息
消息标题	消息内容	发生时间 类型(全部) 🗸
● 中 系统证书即将过期	平台证书将在30天后过期,请注意更换证书。	2022-03-15 10:44:03 证书美
< 1 > 每页 20 条, 共 1 页		

删除消息/设置消息状态

在消息列表中,勾选指定的消息,单击图标【**具**/**面**】,可以设置该消息为已读消息/删除该消息。

查看消息

单击【已读消息】/【未读消息】按钮,进入已读消息/未读消息页面,查看已读消息/ 未读消息。



配置消息通知

单击【消息通知】, 配置消息通知策略参数, 参数说明如表 16-1 所示。

配置项		描述
基本设置	消息类型	产生消息通知的消息类型,可选项有系统类、采集类、证书类,支 持多选。
	消息等级	产生消息通知的消息安全等级,可选项有高、中、低。
系统类/采集 类通知抑制	/采集 抑制时间 抑制 抑制时间 消息类型为"系统类"或"采集类"时,需要配置此项。 系统对系统类/采集类的同一消息内容消息进行合并提醒,在设定时间间隔内,有相同的事件时系统将不再重复提示,避免出现系消息风暴。 取值范围为 5~60 分钟。	
证 书 类 通 知 抑制	通知频次	消息类型为"证书类"时,需要配置此项。 系统对证书类的内容消息进行合并提醒,在设定的时间间隔内,有 相同的事件时系统将不再重复提示,避免出现系统消息风暴。 设定时间间隔,可选项有:三天内、一周内、一个月内。

表 16-1 消息通知策略参数





A.1 Agent 支持的操作系统

系统分类		版本信息
		Windows XP
		Windows server 2003
		Windows server 2008
		Windows server 2012
		说明
Windows		Standard 和 Datacenter 版均支持。
		Windows server 2016
		Windows server 2019
		Windows 7
		Windows 8
		Windows 10
Linux X86		CentOS 6.5
	X86	CentOS 6.6
		CentOS 6.7
		CentOS 6.9
		CentOS 7.0/7.1/7.4/7.5/7.7/7.8/7.9
		CentOS 7.2
		CentOS 7.3
		CentOS 7.6
		Debian 6.0.6
		Debian 8.7



系统分类		版本信息
		Debian 9.11
		Debian 10.2/10.7/10.9
		Red Hat 5.4
		Red Hat 5.9
		Red Hat 6.4
		Red Hat 6.5
		Red Hat 6.7
		Red Hat 7.3
		Red Hat 7.4
		Red Hat 7.2/7.5/7.6/7.7
		SUSE 11 sp4、SUSE 11 sp2
		SUSE 11 SP3/SP5
		SUSE 12 SP3/SP5
		凝思
		凝思 6.0.60
		红旗 Asianux Server 7.6
	arm	银河麒麟 4.0
		银河麒麟 V10 Kylin Linux Advanced Server
		NeoKylin Linux Advanced Server release V7Update6 (Chromium)(中标麒麟)
		Uniontech OS Server 20 Eterprise Linux oa-sms01 4.19.0-arm64-server
Unix		Solaris 10 (SunOS 5.10)
Ubuntu		Ubuntu16/16.04
		Ubuntu14.04
		Ubuntu18.04
		Ubuntu20.04
		Ubuntu12
BC-Linux		7.1/7.4/7.5/7.6/7.7
		8.1/8.2
OpenSUSE		42.3
		15.2