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**天翼云科技有限公司**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

前言

1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 账号管理	介绍标品和涉密版的用户账号管理方法。
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 出厂参数	介绍 LAS 的出厂参数。
B 通信矩阵	介绍 LAS 支持的设备信息和 Agent 支持的操作系统。

2修订记录

日期	修订版本	修改记录
2024-04-25	01	初次发布。

目录

1 设备简介

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。

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。

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。

2.1.1 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。

说明	页面布局中的菜单和工作区会因用户权限的不同而不同，具体情况请以页面展示为准。

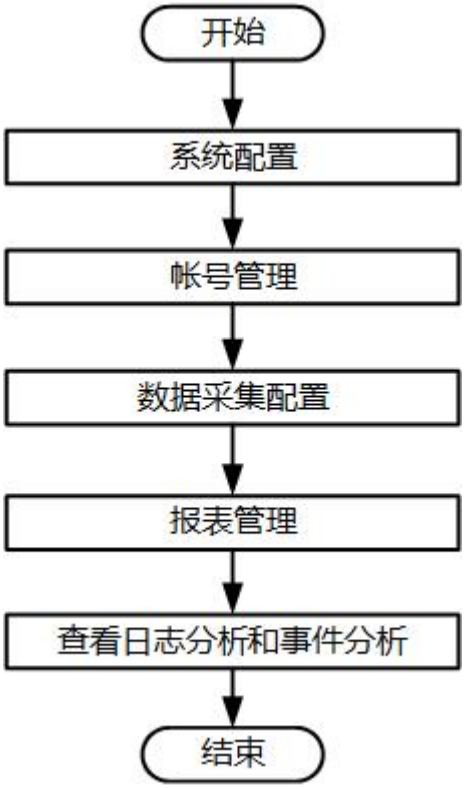
图 2-1 页面布局

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。 •  ：进入总控制台。 •  ：进入消息中心，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。 •  ：包括以下三个功能。 ✓ 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账号信息。对于 admin 用户，还支持对所有账号和角色进行管理。 ✓ 退出系统
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。

2.1.2 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 账号管理

LAS 标品和涉密版的用户账号管理操作略有不同，主要内容如下：

功能	描述
标品	介绍 LAS 标品的用户账号管理方法。

3.1 标品

LAS 标品的账号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。

3.1.1 创建用户账号

LAS 用户账号的创建方法如下：

步骤 1 使用 admin 账号登录 LAS 的 Web 管理页面。

步骤 2 将鼠标悬停在快捷操作栏中的  ，选择【用户中心】，进入 账号管理 > 账号 页面，如图 3-1 所示。

图 3-1 账号列表（LAS 标品）

步骤 3 单击【新建账号】，配置账号参数，如 b.图 3-2 所示。

a. 密码：支持两种设置方式。其中，默认密码为账号名+@123456（例如：账号名为 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 创建用户账号（LAS 标品）

步骤 4 单击【确定】按钮，完成用户账号创建。

----结束

3.1.2 查看用户账号信息

用户账号新建后，查看账号信息的操作方法如下：

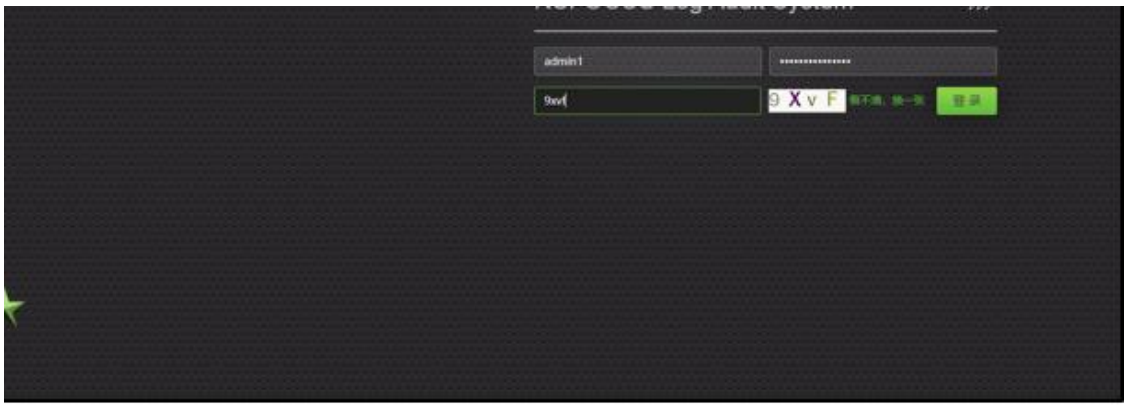
步骤 1 使用新建账号登录 LAS 的 Web 管理页面。

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）

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。

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  ，选择【用户中心】，默认进入 我的账号 页面，如图 3-5 所示。

图 3-5 查看当前登录用户的账号信息（LAS 标品）

----结束

3.1.3 修改用户账号信息

查看用户账号信息 时，支持修改账号信息、登录密码和登录方式。

3修改账号信息

如图 3-6 所示，包括邮箱、手机号码、可登录 IP 范围。

图 3-6 修改用户账号信息（LAS 标品）

4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 修改用户账号登录密码（LAS 标品）

5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 修改用户账号登录方式（LAS 标品）

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

4 系统配置

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	介绍 LAS 邮件通知和短信通知的配置方法。
SFTP/FTP 服务器配置	介绍 SFTP/FTP 服务器的配置方法。

4.1 网络配置

LAS 硬件版、软件版和虚拟化版的网络配置略有不同，下面分别进行介绍。

4.1.1 LAS 虚拟化版网络配置

LAS 虚拟化版的网络配置包括网络接口和网络路由。

4.1.1.1 网络接口配置（LAS 虚拟化版）

网络接口（LAS 虚拟化版）的配置方法如下：

步骤 1 使用 admin 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，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（LAS 虚拟化版）

步骤 3 修改 M 口。

单击网络接口列表操作栏的，编辑 M 口的接口属性（支持 IPv4 和 IPv6）。

步骤 4 打开 DHCP。

在如步骤 2 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。

注意	设置完成后原 IP 不能访问，需前往串口查看新的网络配置信息。

----结束

4.1.1.2 网络路由配置（LAS 虚拟化版）

LAS 虚拟化版的网络路由配置与 LAS 硬件版的基本相同，请参见 **错误！未定义书签。**。

4.2 NTP 配置

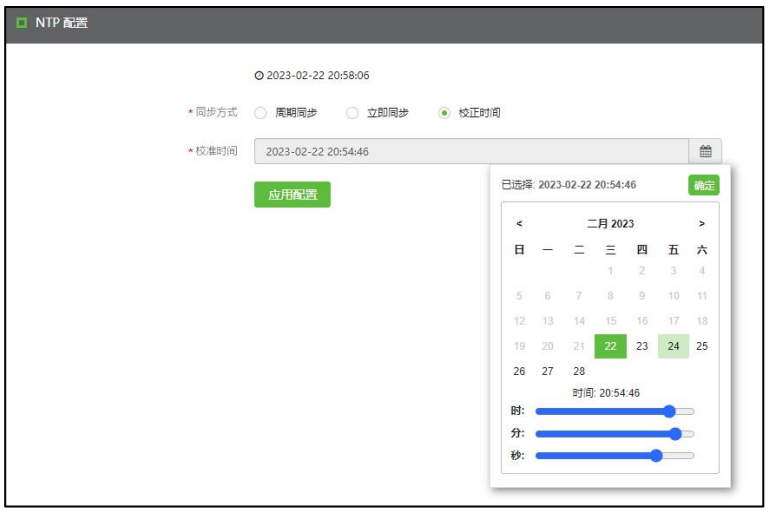
将鼠标悬停在总控制台图标，进入 **系统配置** > **NTP 配置** 页面，LAS 支持三种时间同步方式：

- 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）

图 4-3 NTP 配置（立即同步）

图 4-4 NTP 配置（校正时间）



4.3 通知配置

LAS 支持邮件通知和短信通知。

4.3.1 邮件服务器

6场景

通过邮件通知方式接收事件告警。

7配置思路

- 确认邮件服务器地址、邮件服务器端口、邮件发送地址和邮件发送密码等。
- 准备一个邮件接收地址，用于验证测试邮件配置是否正确。

8配置步骤

若要在 LAS 中触发发送邮件的动作，必须配置 SMTP 相关参数，操作方法如下：

步骤 1 使用 admin 账号登录 LAS 的 Web 管理页面。

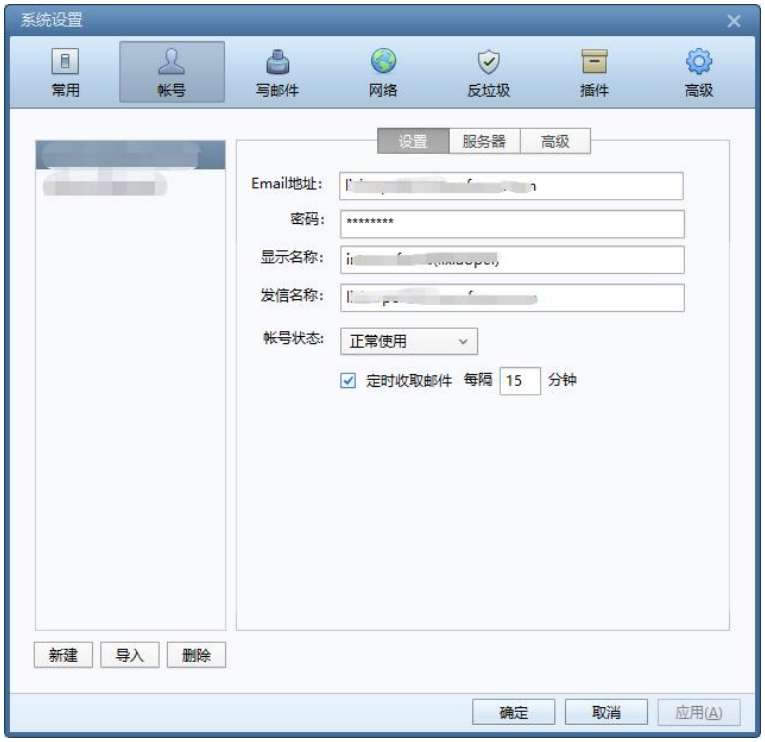
步骤 2 将鼠标悬停在 LAS 总控制台图标，进入 系统配置 > 通知配置 > 邮件服务器 页面，配置邮件服务器参数，如图 4-5 所示。

图 4-5 配置邮件服务器

步骤 3 邮件客户端的账号配置

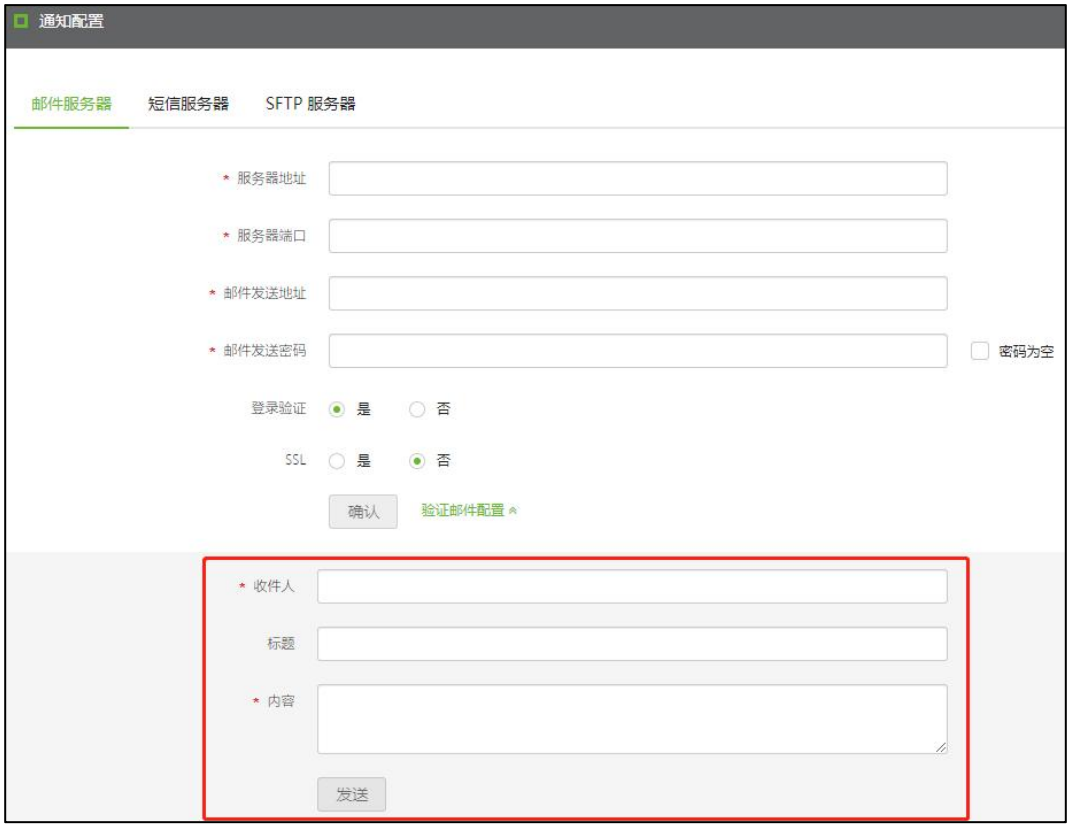
以 Foxmail 为例，进入 **设置** > **账号** 页面，查看邮件服务器相关配置，单击【确定】按钮，保存配置，如图 4-6 所示。

图 4-6 邮件客户端配置（例：Foxmail）



步骤 4 返回如步骤 2 图 4-5 所示的界面，单击【验证邮件配置】 输入收件人、标题、内容，单击【发送】按钮进行验证，如图 4-7 所示。

图 4-7 验证邮件配置



步骤 5 打开收件人邮箱，验证能否正常接收测试邮件。

a. 若能正常接收测试邮件，说明邮件服务器配置正确。

b. 若接收不到测试邮件，说明邮件服务器的配置错误。请执行以上步骤，重新配置。

配置过程中，如果配置有误，可以单击【清空配置】按钮，清除当前已有配置，重新配置邮件服务器参数。

----结束

4.3.2 短信服务器

9场景

通过短信通知方式接收事件告警。

10配置步骤

若要在 LAS 中触发发送短信的动作，必须配置短信服务器，操作方法如下：

步骤 1 使用 admin 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，进入 系统配置 > 通知配置 > 短信服务器 页面，如图 4-8 所示。

图 4-8 配置短信服务器

步骤 3 选择设备类型，配置短信服务器参数（不同设备类型的参数配置也有所不同）。

SMS 设备参数说明如表 4-1 所示，嘉讯 MAS 短信平台参数说明如表 4-2 所示，腾讯云短信平台参数说明如表 4-3 所示。

表 4-1 配置短信服务器（SMS 设备参数）

配置项	描述
设备	选择“SMS”。
用户名	短信服务器的用户名。最多支持 100 个字符。
密码	短信服务器的用户密码。最多支持 100 个字符。
服务器地址	短信服务器的 IP 地址，支持 IPv4 和 IPv6。
数据库名称	短信服务器中用于存储短信通知的数据库名称，最多支持 100 个字符。
表名称	存储短信通知的表名称。最多支持 100 个字符。

表 4-2 配置短信服务器（嘉讯 MAS 短信平台参数）

配置项	描述
设备	选择“嘉讯 MAS 短信平台”。
MAS 服务器 IP 地址	嘉讯 MAS 服务器的 IP 地址。支持 IPv4 和 IPv6。
API 适配监听接口	MAS 上监听客户端的 API 接口号。取值范围为 1~65535。
API 标识	API 接口的编码。

配置项	描述
API 登录密码	API 接口的登录密码。最多支持 100 个字符。
短信扩展码	输入短信扩展码。最多支持 100 个字符。
每分钟最大发送频率	每分钟发送短信的最大频率。取值范围为 1~20。
短信后缀	短信的后缀。最多支持 100 个字符。

表 4-3 配置短信服务器（腾讯云短信平台参数）

配置项		描述
设备		选择“腾讯云短信平台”。
API 秘钥 ID		API 密钥是构建腾讯云 API 请求的重要凭证，通过腾讯云 API 可以操作用户名下的所有腾讯云资源。
API 秘钥		
短信服务器 URL		接口请求域名。默认为 sms.tencentcloudapi.com
腾讯云应用 ID		短信 SdkAppid 在【短信控制台】添加应用后生成的实际 SdkAppid。
模块与签名	功能模块	LAS 需要使用短信业务的功能模块。目前只有事件告警使用短信业务。
	签名内容	短信签名内容，使用 UTF-8 编码，必须填写已审核通过的签名，签名信息可登录【短信控制台】查看。 说明 国内短信为必填参数。
	短信模板 ID	必须填写已审核通过的模板 ID。模板 ID 可登录【短信控制台】查看，若向境外手机号发送短信，仅支持使用国际/港澳台短信模板。
	模板内容	短信模板内容。
更多配置	短信码号扩展号	短信码号扩展号，默认未开通，如需开通请联系 sms helper。
	手机号码前缀	手机号码的前缀。例如：+86。
	Session 内容	用户的 session 内容，可以携带用户侧 ID 等上下文信息，server 会原样返回。
	发送 ID	国内短信无发送 ID，无需填写该项。 若需开通国际/港澳台短信发送 ID，请联系 sms helper。

步骤 4 短信服务器配置后，单击【验证短信配置】，如图 4-9 所示。

配置验证参数，可以验证短信服务器配置是否正确。

图 4-9 验证短信配置

步骤 5 若能正常接收测试短信，说明短信服务器的配置正确。

----结束

4.4 SFTP/FTP 服务器配置

11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。

12配置步骤

SFTP/FTP 服务器的配置方法如下：

步骤 1 使用 admin 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，进入 系统配置 > 通知配置 > SFTP 服务器 页面，如图 4-10 所示。

图 4-10 SFTP/FTP 列表（初始状态）

步骤 3 单击【新建 SFTP】按钮，在弹出的提示框中单击【已知晓】。

步骤 4 配置 SFTP/FTP 服务器参数，如图 4-11 所示。

图 4-11 配置 SFTP/FTP 服务器

步骤 5 单击【确认】按钮，返回 SFTP/FTP 列表，如图 4-12 所示。

图 4-12 SFTP/FTP 列表（完成配置）

步骤 6 在 SFTP/FTP 列表中，单击操作列的，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 7 SFTP/FTP 服务器的连通性测试成功，完成配置。

----结束

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。

本章主要内容如下：

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。

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，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

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. 在如步骤 2 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

b. 设置端口号并开启配置后，单击操作栏的，如 c.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

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

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

图 5-6 数据源详情（有日志上报）

----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 5.1 步骤 2 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 b.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

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

b. （可选）单击【重新选择】，返回如 5.1 步骤 2 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 b.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

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。

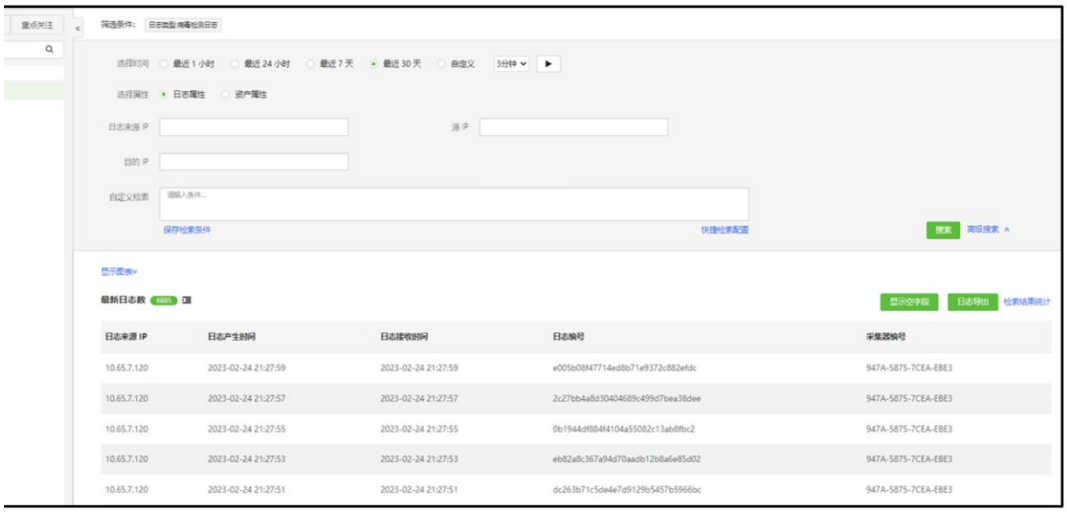
图 5-10 天翼云设备日志已接入

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

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



----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 55.35.3.1 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 55.1 步骤 2 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

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

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

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

----结束

5.3.4 结果验证

第三方安全设备（示例如 55.35.3.1 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，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

----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=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
```

```
<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

图 5-19 配置第三方安全设备的接入方式

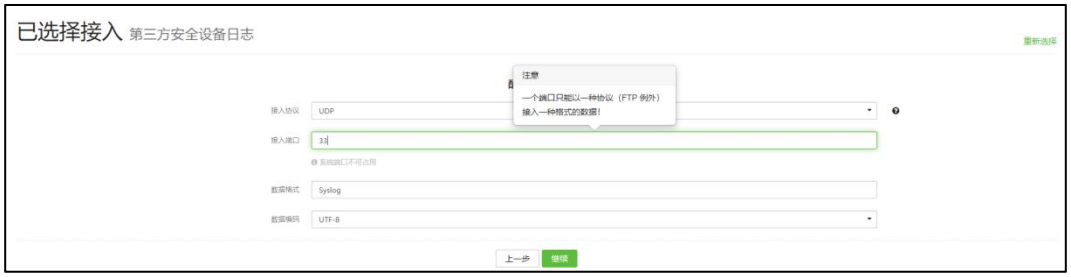


图 5-20 配置第三方安全设备信息

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。

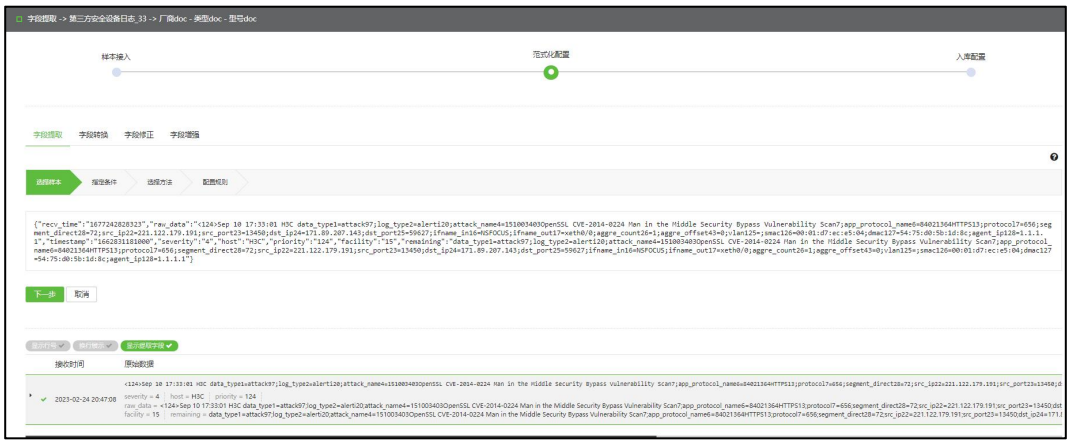
图 5-21 立即提取字段

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

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



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

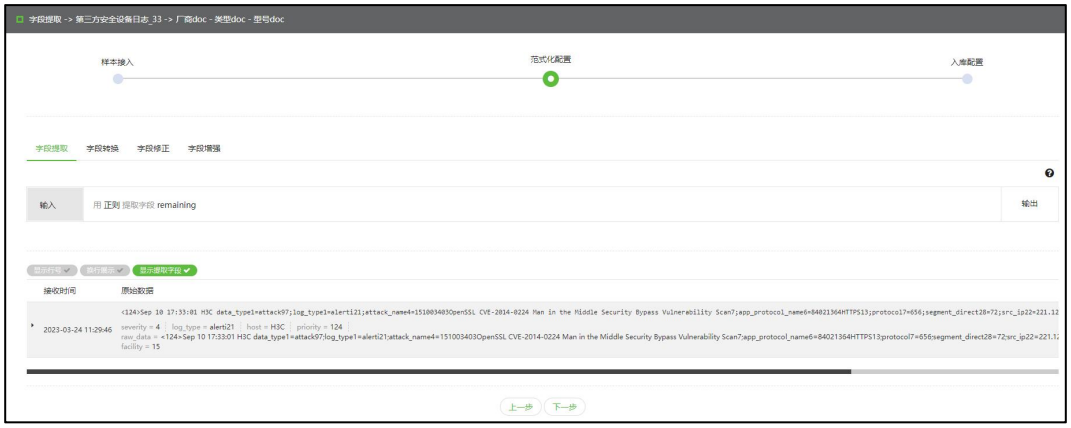
步骤 6 选择方法，此处选择【正则表达式】，如图 5-25 所示。

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

步骤 7 验证，完成规则配置，如图 5-26 所示。

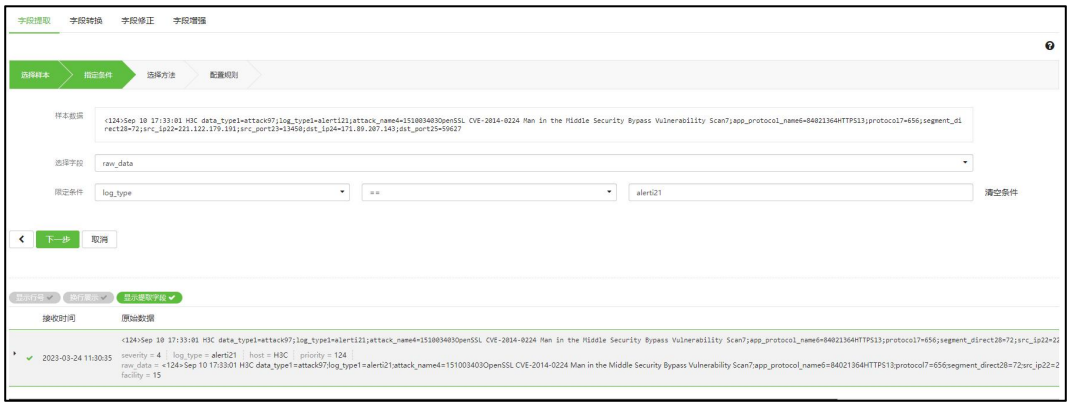
图 5-26 字段提取：验证



步骤 8 创建新规则，如错误！未定义书签。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



步骤 9 选择 Key->Value 方式提取，如错误！未定义书签。和图 5-29 所示。

图 5-28 K->V 方式提取日志（1）

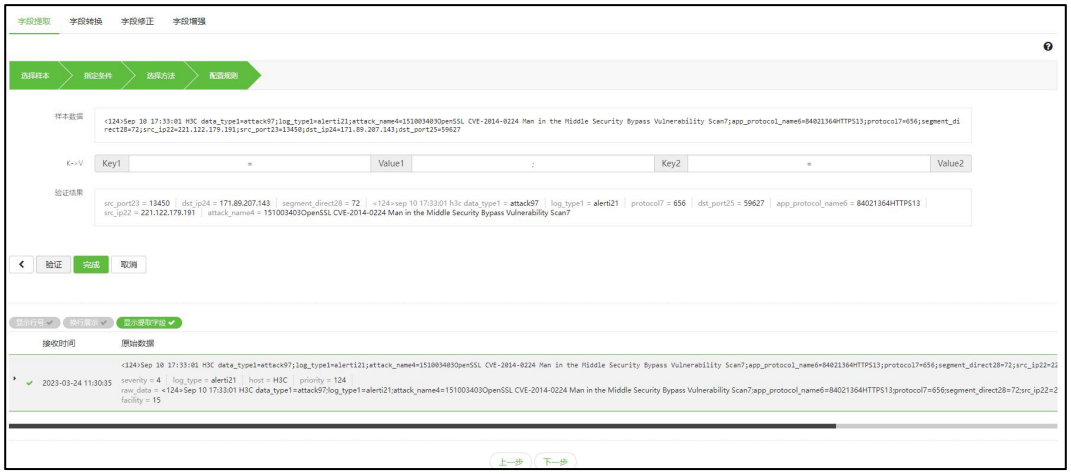
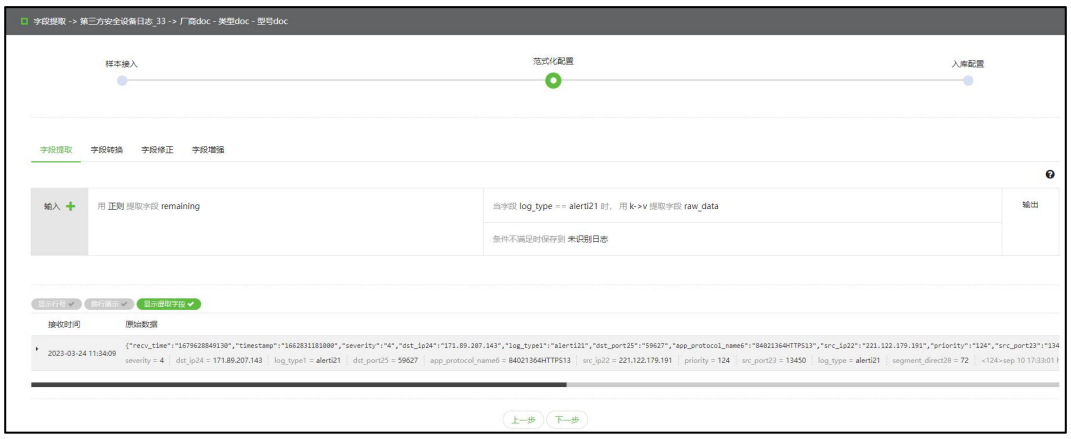
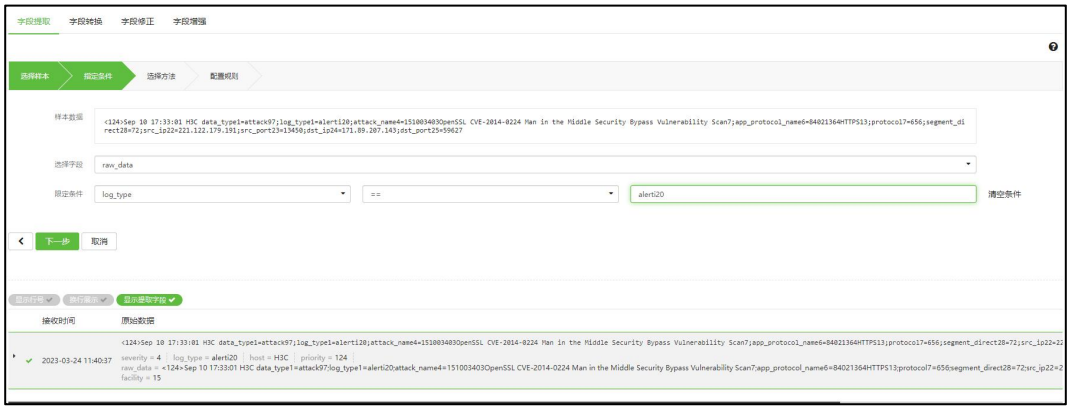


图 5-29 K->V 方式提取日志（2）



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



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）

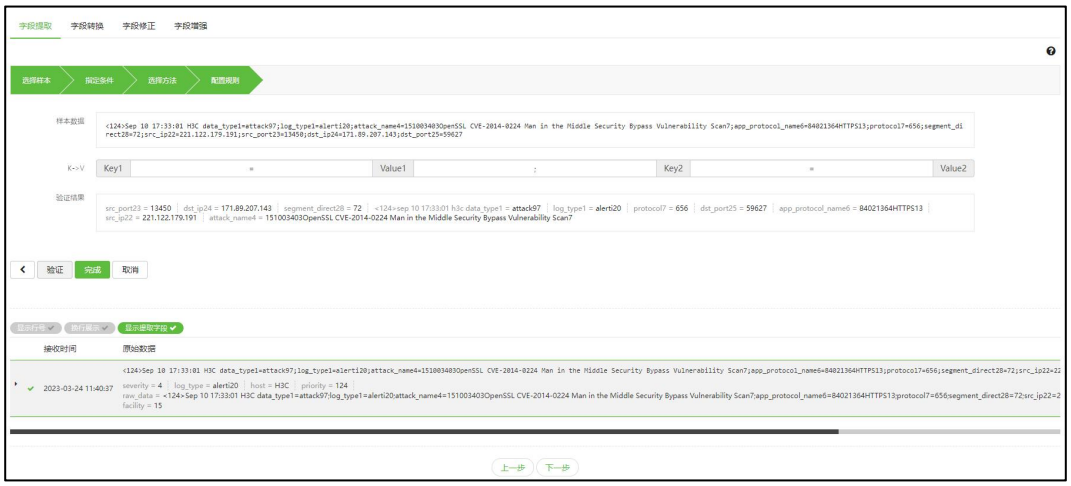


图 5-32 字段提取：Key-value 方式（2）

图 5-33 字段提取：Key-value 方式（3）

图 5-34 字段提取：Key-value 方式（4）

图 5-35 字段提取：存入多张表

步骤 12 完成字段提取，如图 5-36 所示。

图 5-36 完成字段提取

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）

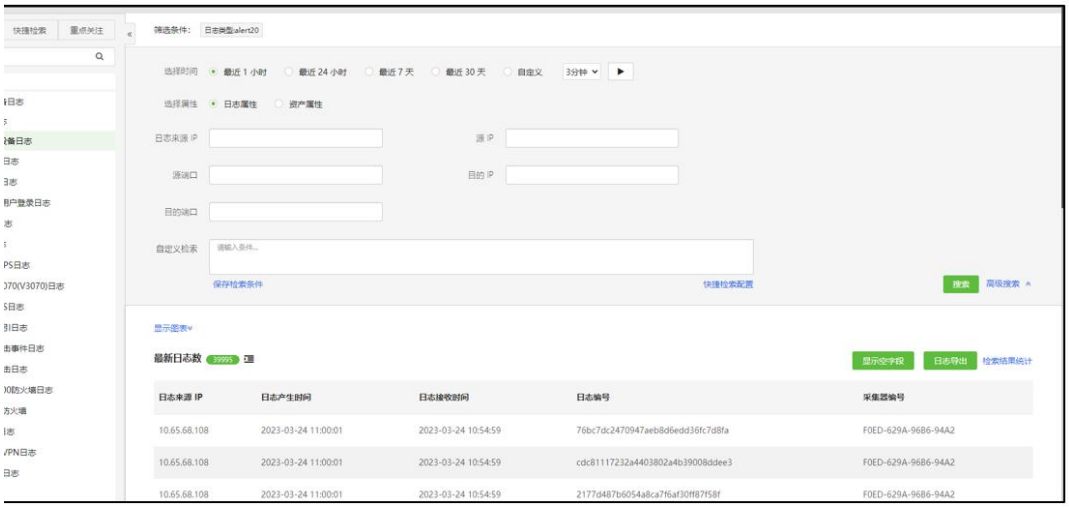
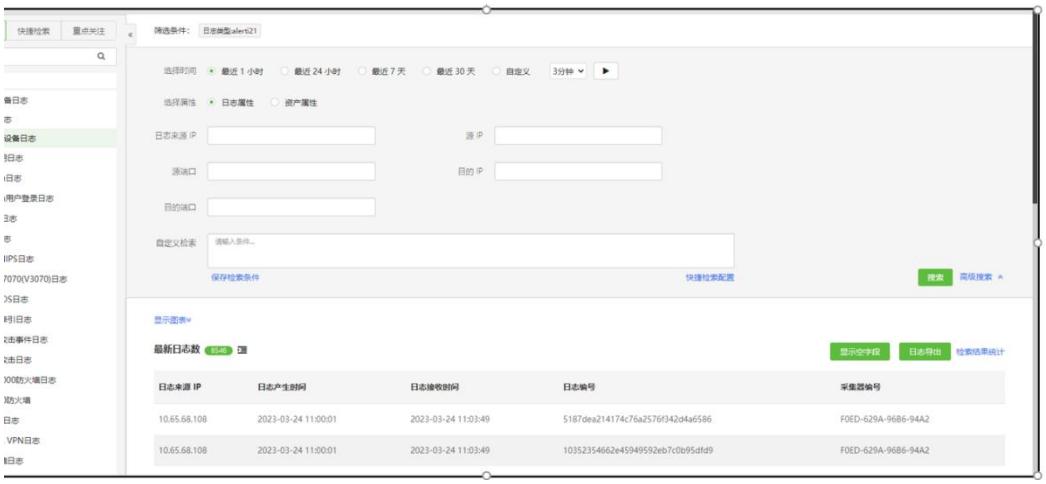


图 5-38 第三方设备的日志检索（2）



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

步骤 16 单击，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

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

图 5-42 字段提取：完成日志提取

----结束

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

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

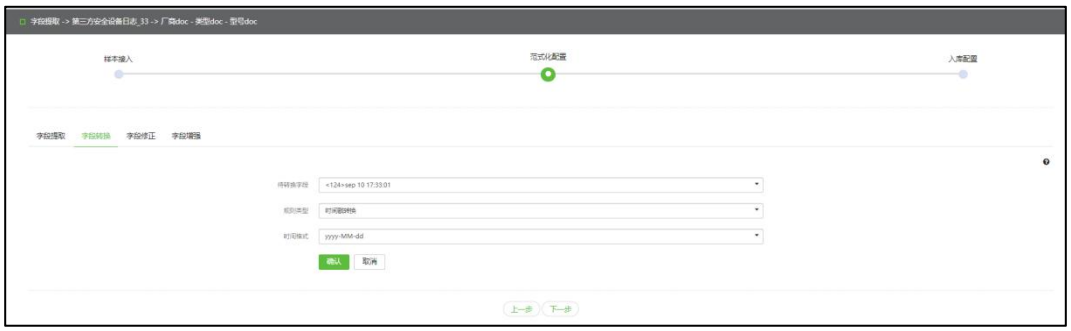
----结束

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

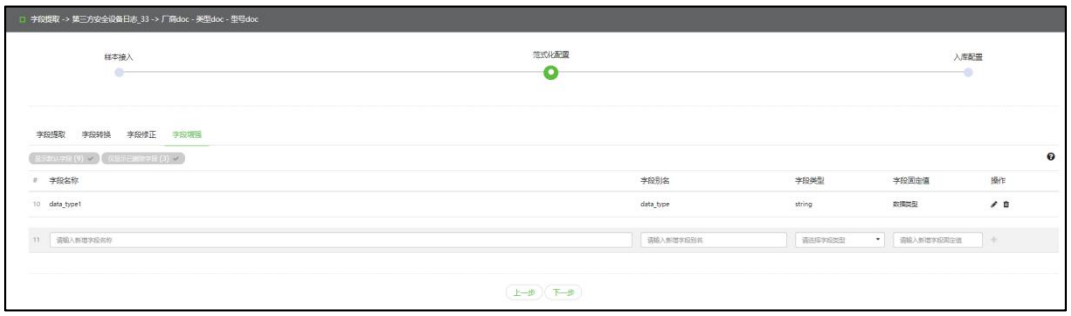


5.3.5.4 字段增强

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



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。

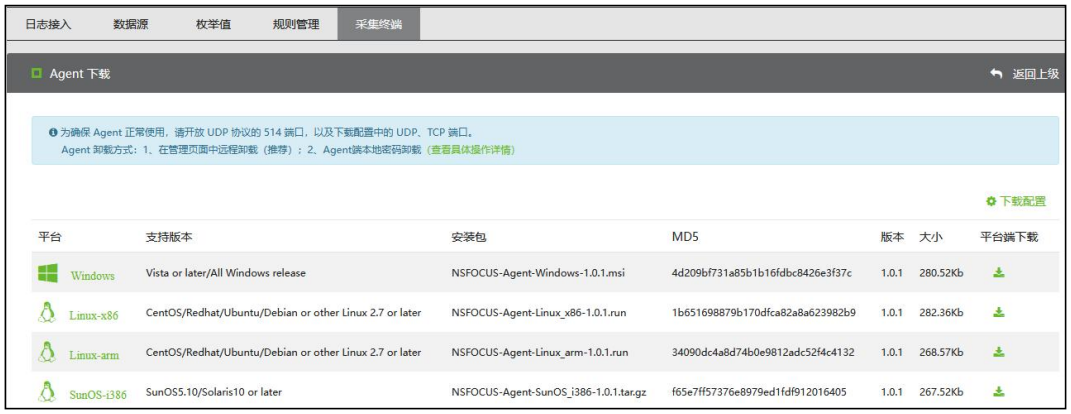
c. 单击【下载 Agent】，进入 Agent 下载页，如−图 5-47 所示。

d. 在 Agent 列表中，单击平台端下载栏的，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



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）

```
[root@localhost ~]# ll
total 23784
-rw-------.  1 root root     1265 Nov  8 17:38 anaconda-ks.cfg
-rw-------.  1 root root  1332424 Jan  5 16:58 nohup.out
-rw-r--r--.  1 root root   298496 Feb 24 14:48 NSFOCUS-Agent-Linux_x86-1.0.1.run
drwxr-xr-x.  6 root root       56 Jan 31 18:46 python36
drwxr-xr-x. 17  501  501     4096 Jan 31 18:45 Python-3.6.4
-rw-r--r--.  1 root root 22710891 Jan 31 18:39 Python-3.6.4.tgz
[root@localhost ~]#
[root@localhost ~]#
```

图 5-49 上传 Agent 安装包（2）

```
[root@localhost ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:eb:31:c3 brd ff:ff:ff:ff:ff:ff
    inet 10.65.68.108/20 brd 10.65.79.255 scope global noprefixroute ens192
       valid_lft forever preferred_lft forever
    inet6 240e:659:120:225:5510:7704:d66b:1b55/64 scope global noprefixroute dynamic
       valid_lft 2591823sec preferred_lft 604623sec
    inet6 fe80::506a:8e7c:76f9:447d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]#
```

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
```

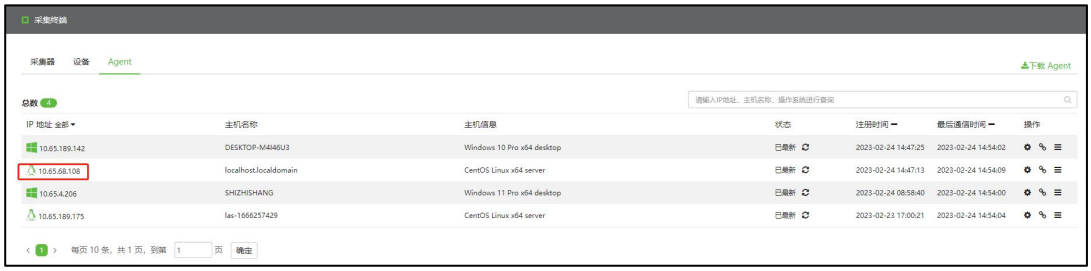
图 5-50 安装 Agent

```
[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。

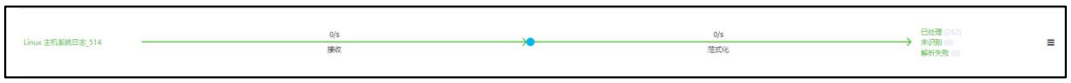
状态为“已最新”，说明 Linux Agent 安装成功。

图 5-51 数据采集 Agent 列表



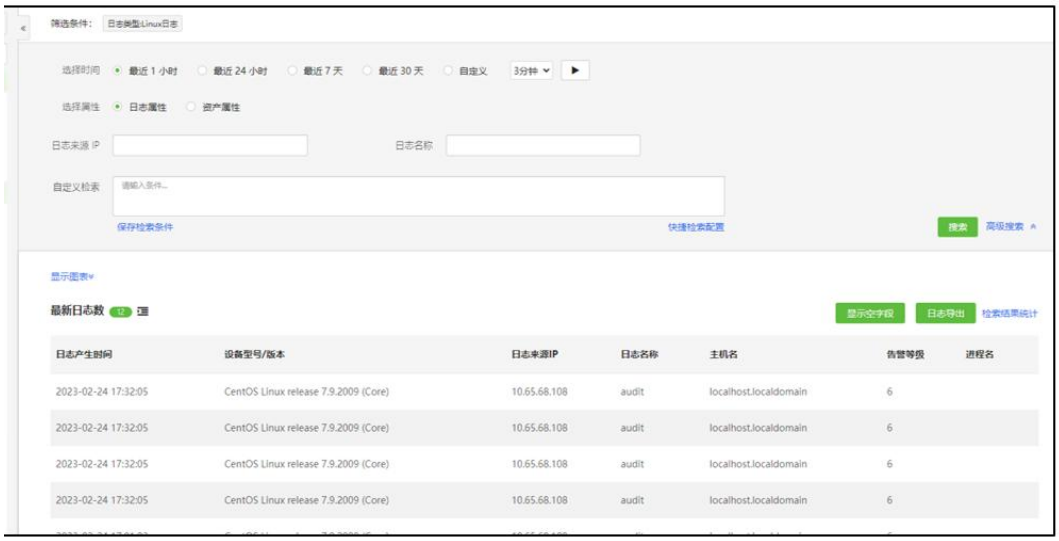
步骤 5 进入 数据采集 > 数据源 页面，可以查看已处理的日志数量，如图 5-52 所示。

图 5-52 数据源（Linux 主机日志）



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）



----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，将对应的 Agent 下载到本地。

步骤 2 鼠标双击 Agent 文件，安装 Windows Agent。

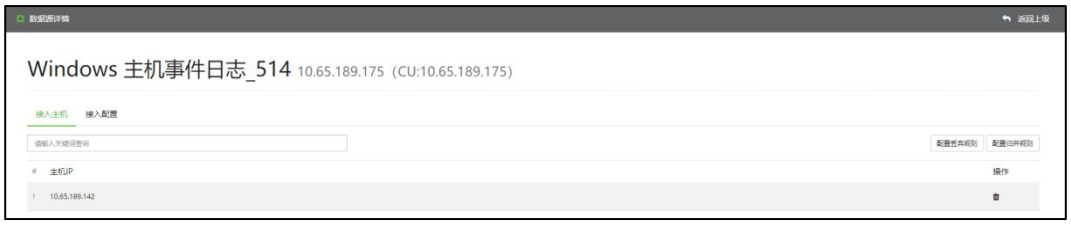
步骤 3 返回 数据采集 > 采集终端 > Agent 页面，查看 Windows 主机是否在线。

Windows 主机已接入，如图 5-54 所示。

图 5-54 数据采集终端列表

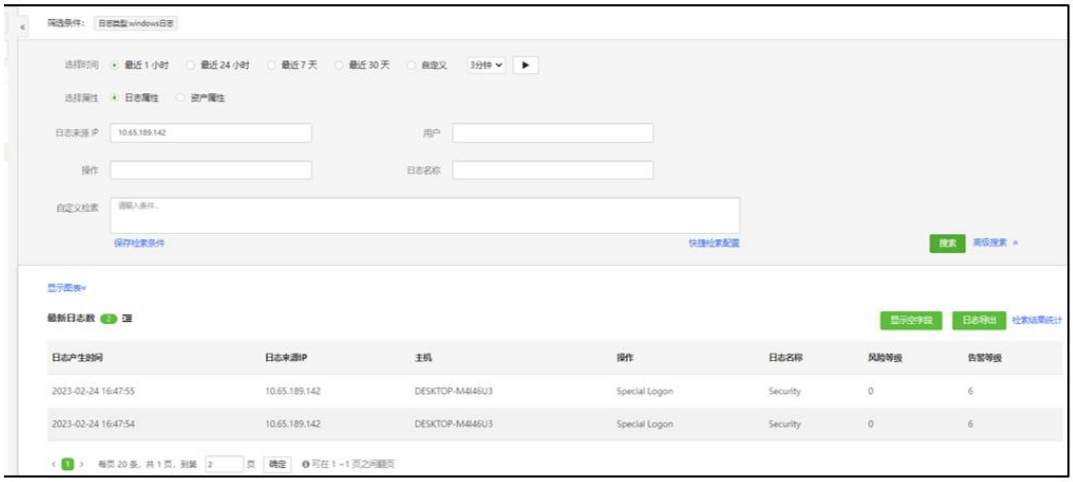
步骤 4 进入 数据采集 > 数据源 页面，单击上一步接入的 Windows 主机，可以查看接入的设备信息，如图 5-55 所示。

图 5-55 接入的主机信息（Windows 主机日志）



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）



----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，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）

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

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

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

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 b.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

图 5-62 Web 服务器日志完成接入

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 b.图 5-63 所示。

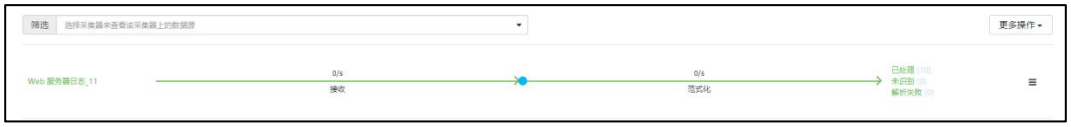
b. 配置主机采集参数和应用服务日志参数，其中应用服务日志参数包括服务名、日志采集路径、日志文件名全路径和端口号（即步骤 4 接入的端口），如图 5-64 所示。

图 5-63 数据采集终端列表（Web 服务器日志接入）

图 5-64 数据采集终端配置（Web 服务器日志接入）

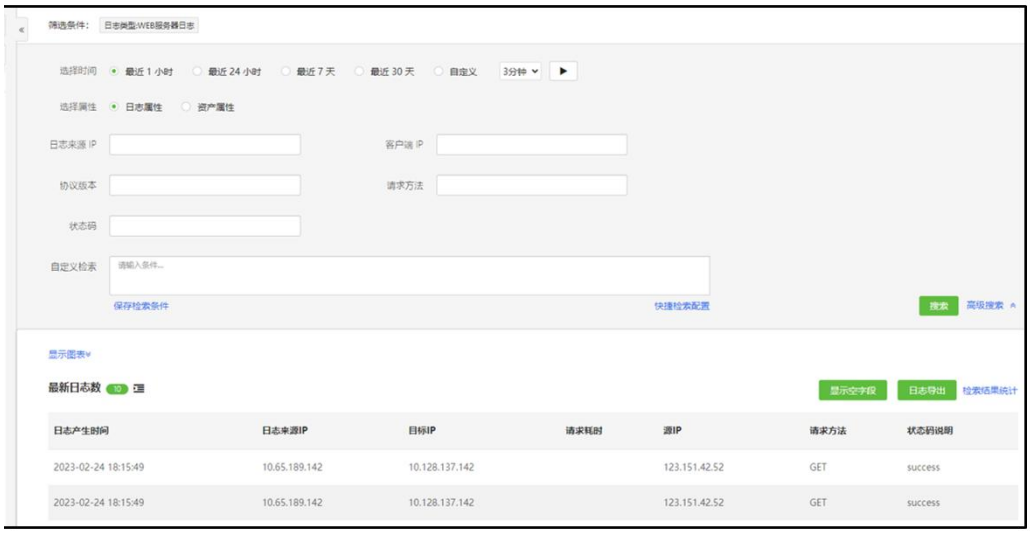
步骤 8 进入 数据采集 > 数据源 页面，当有日志上报时，可以查看已处理的日志条数，如图 5-65 所示。

图 5-65 已接入日志的 Web 服务器



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）



----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）

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

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 c.图 5-69 所示。

b. 配置数据库接入参数，如 c.图 5-70 所示，主要参数说明如 c.图 5-70 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、连接账号和连接密码是否正确。

图 5-69 添加要接入数据的数据库

图 5-70 配置数据库接入参数

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

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 b.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

图 5-73 数据库数据完成接入

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

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）

注意	数据表主键属于 other 类型，不是常规的 string、int、时间戳等，所以不支持接入。

----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，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）

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

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

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 b.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

图 5-80 虚拟化平台日志完成接入

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 c.图 5-81 所示。

b. 搜索键：Syslog.global.logHost，结果如 c.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

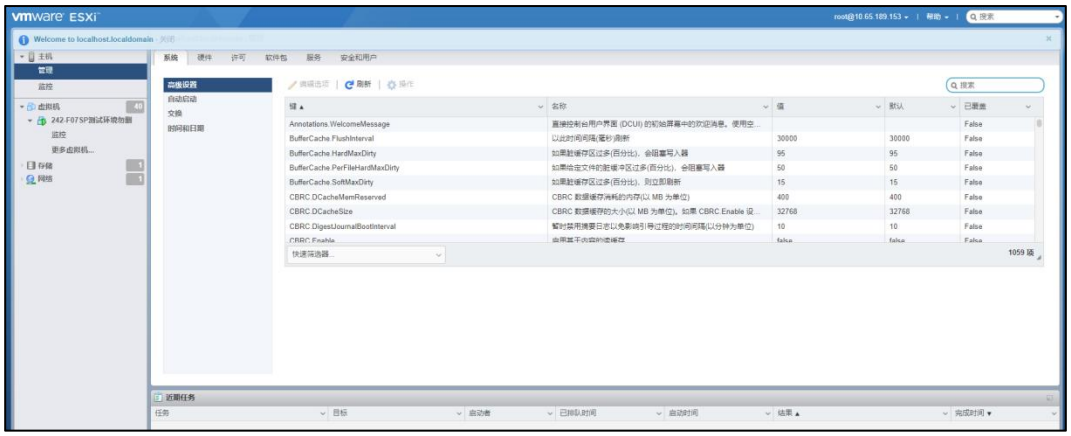
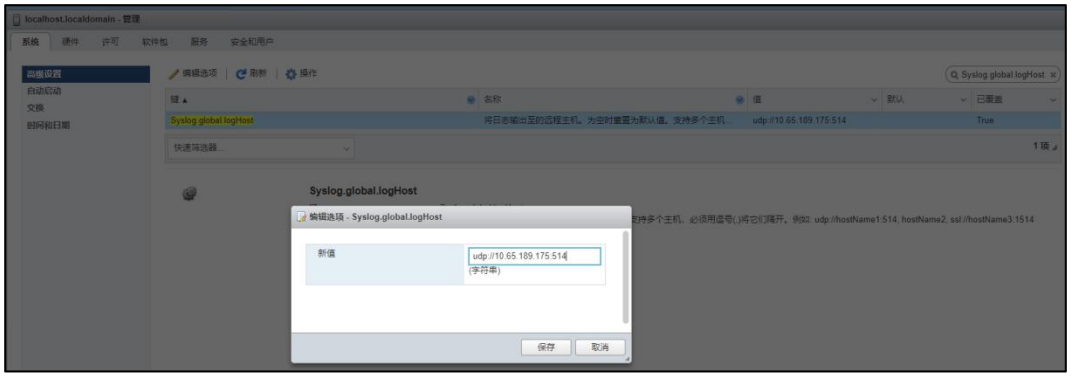


图 5-82 系统高级配置

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	向其转发 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。可以包括协议和端口，例如 ssl://hostName1:1514。支持 UDP（仅在端口 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

图 5-84 编辑选项

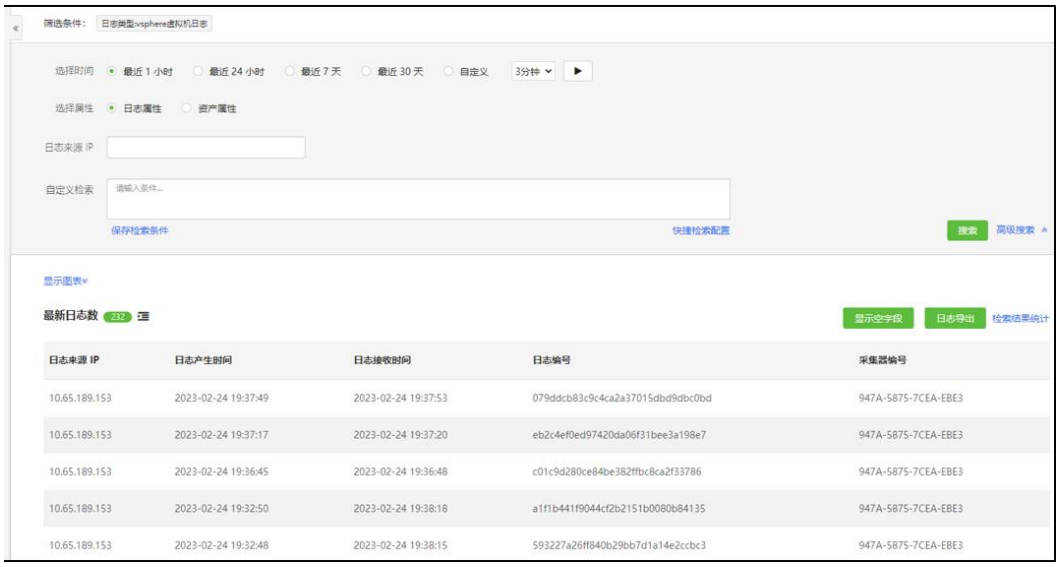


步骤 7 进入 数据采集 > 数据源 页面，可以查看已处理的日志条数，如图 5-85 所示。

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）



----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，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）

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

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 b.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

步骤 5 添加接入流量的网络设备，如 b.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

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）

----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，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

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

步骤 5 添加接入的文件日志来源设备，如 b.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

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。

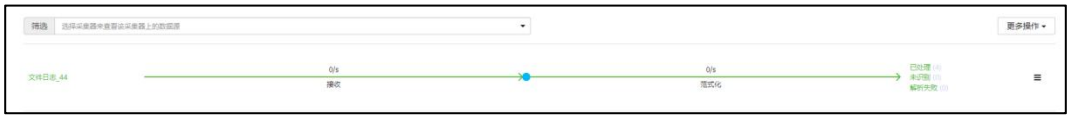
b. 单击文件日志来源设备列表操作栏的，弹出上传日志文件对话框，如 c.图 5-96 所示。

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

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



----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。

说明	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，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）

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

步骤 4 配置其他日志的接入方式，如 b.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

步骤 5 配置其它日志的来源设备。

a. 配置 KAFKA 设备 IP，如 c.图 5-101 所示。

b. 配置 KAFKA 接入参数，如 c.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

图 5-102 配置 KAFKA 接入参数

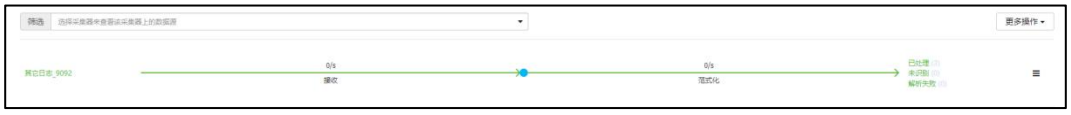
图 5-103 添加其它日志的主题

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

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



----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：

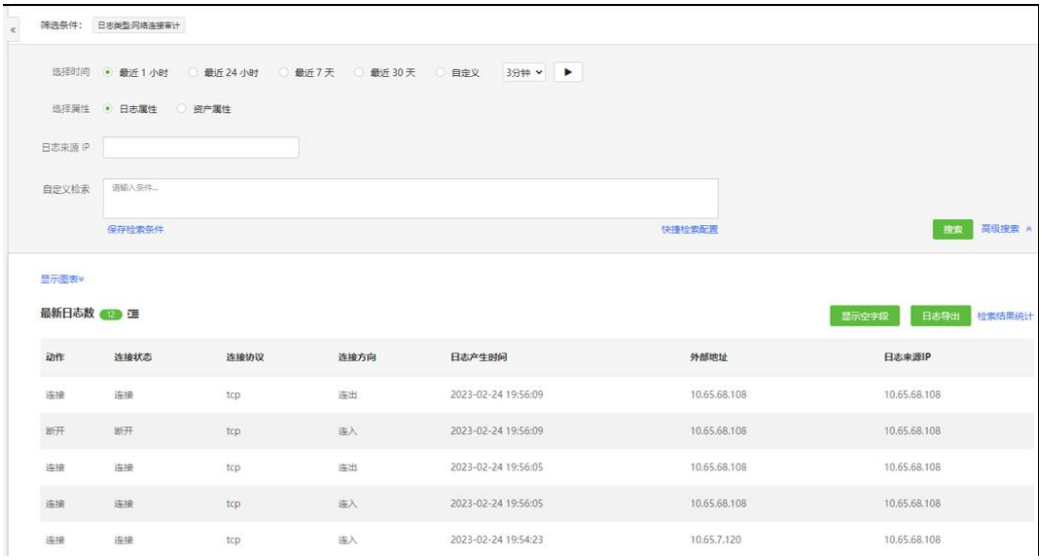
步骤 1 请参见 Linux 主机日志接入，接入 Linux 主机日志。

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

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）



----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 3 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

步骤 4 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

说明	NAT 配置接入方式不可修改。接入 LAS 前进行了 NAT 转换的数据设备中，只有满足以下条件之一的数据源设备可以配置 NAT： • 使用 UDP 协议。 • 与数据源端口保持一致。 • 数据格式为 Syslog。

步骤 5 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。
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 6 单击 完成数据源设备添加。

步骤 7 单击【完成接入】按钮，保存数据源设备 NAT 配置。

----结束

6 数据源

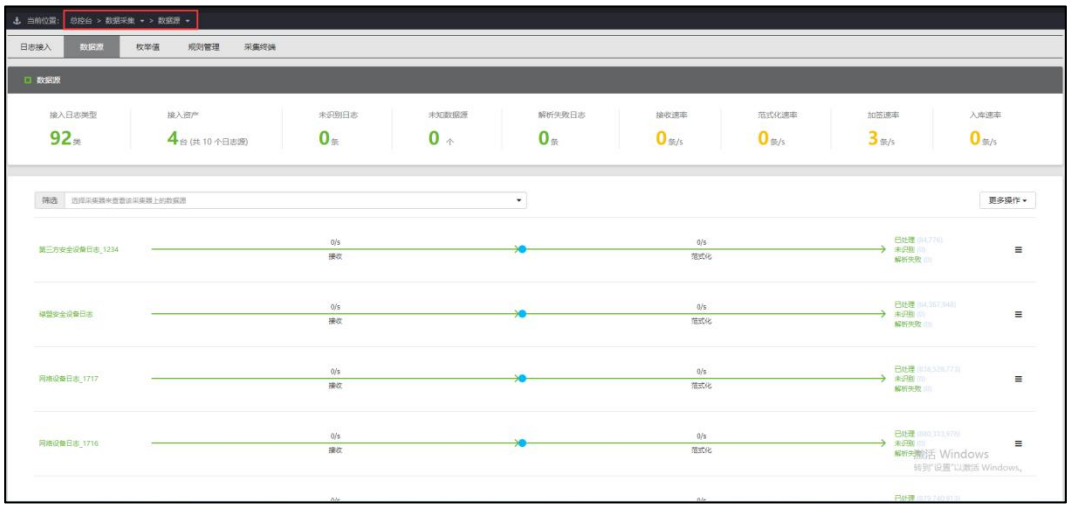
对于 日志接入 的日志对象，LAS 采集器会根据相应的字段提取规则来对其输出的日志进行提取。完成提取后，在数据源下可以对所有日志数据的各个环节进行集中管理和配置。

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，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



6.2 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。

13查看接入日志类型

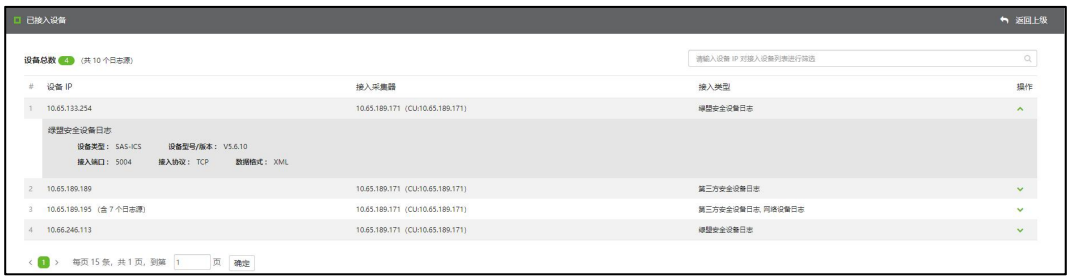
进入已接入日志类型详情页，页面左侧展示所有已经接入 LAS 的日志类型，将鼠标悬停在日志类型上，可以在页面右侧查看该日志类型包含的子日志类型，如图 6-2 所示。

图 6-2 已接入日志类型

14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



15查看未识别日志

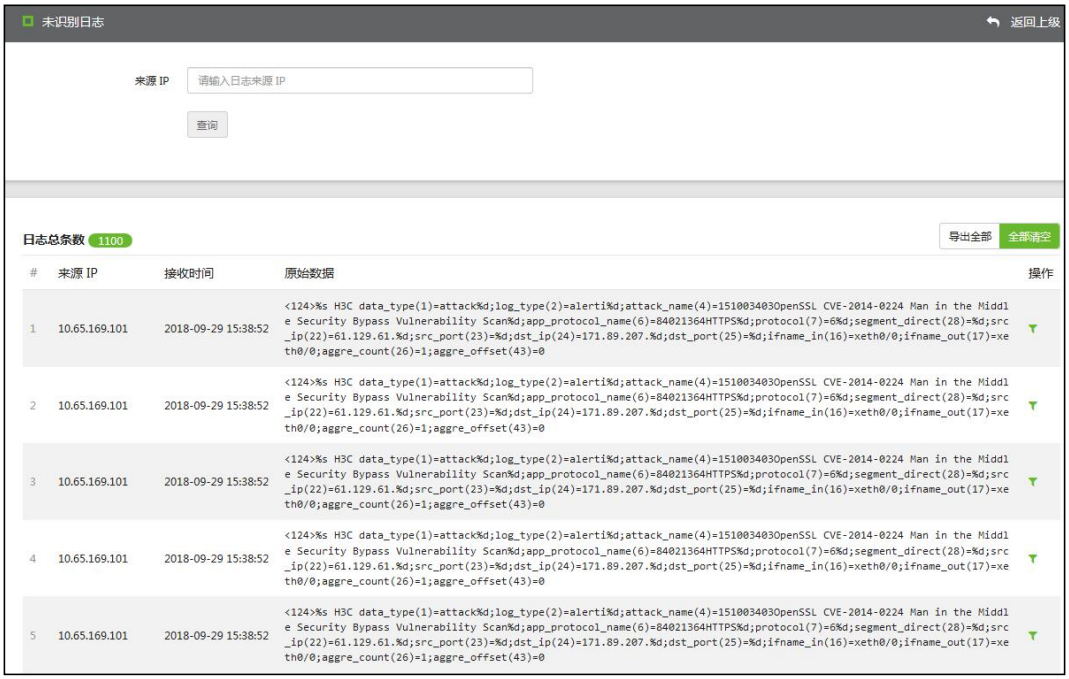
进入未识别日志页面，可以查看与现有规则不匹配及尚未配置字段提取规则的日志信息，仅展示最新的 1000 条数据，如图 6-4 所示。

单击操作栏的，执行 **错误！未定义书签。**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



16查看未知数据源

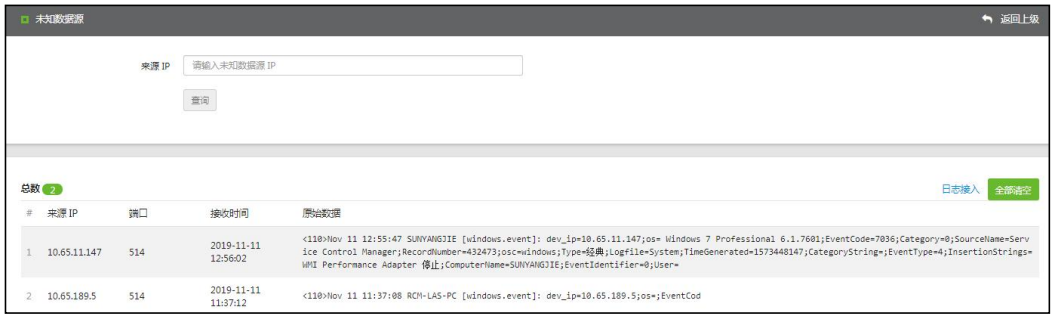
若有未进行过日志接入配置的设备 IP 向 LAS 发送日志数据，该设备会被 LAS 归类为未知数据源。

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



17查看解析失败日志

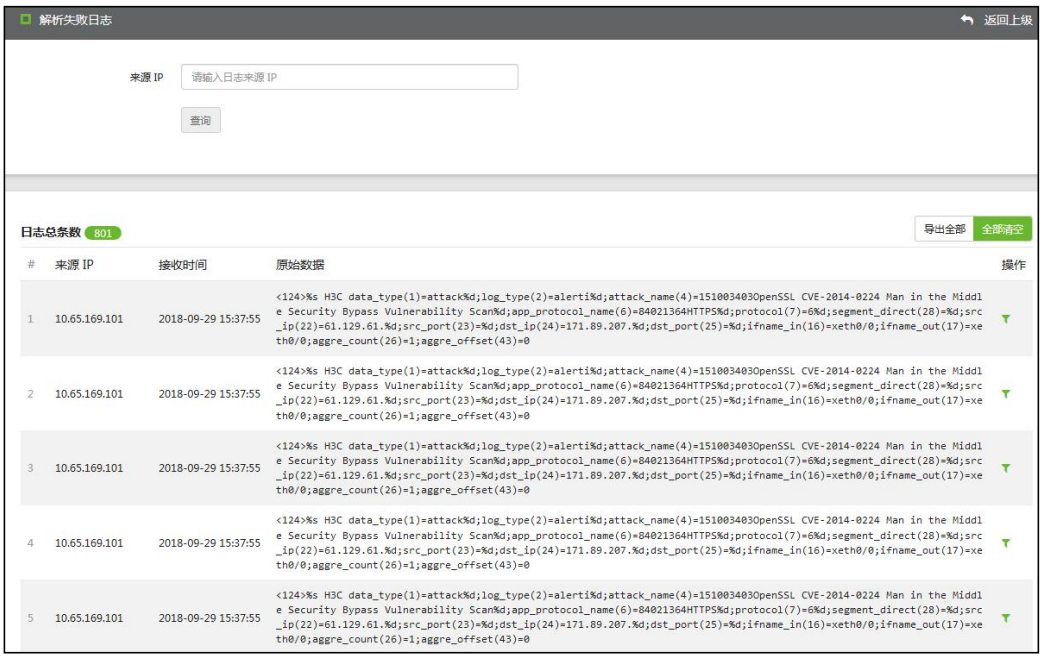
进入解析失败日志页面，可以查看与现有字段提取规则匹配但解析失败的日志信息，如图 6-6 所示。

查看解析失败日志，主要是用来验证已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



18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

6.3 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

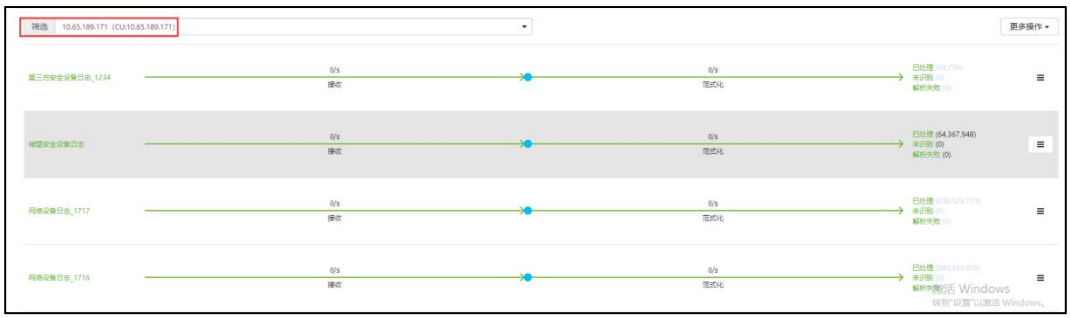
6.4 数据源管理操作

在如 6.2 图 6-8 所示的区域中，用户可以对数据源进行以下操作：

6.4.1 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。

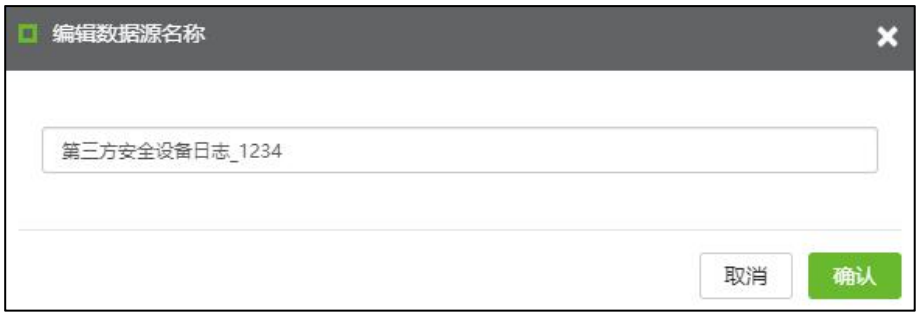
图 6-9 查询数据源



6.4.2 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

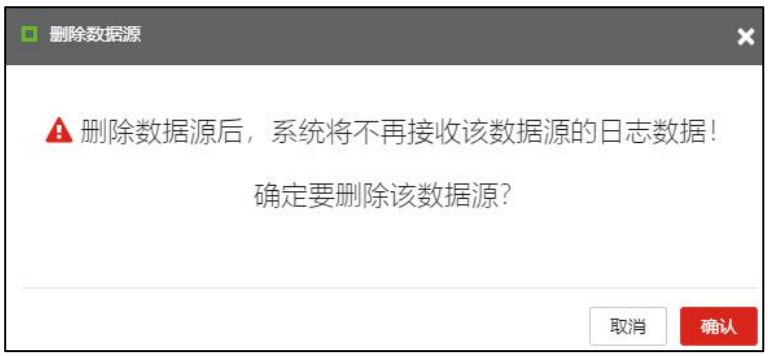


6.4.3 删除数据源

单击☰，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



6.4.4 启用/停用数据源

单击☰，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。

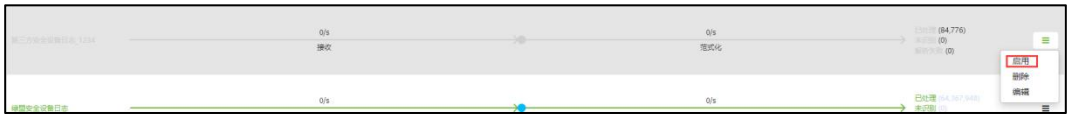
图 6-13 停用数据源

2. 数据源停用后，数据源置灰，如图 6-14 所示。

图 6-14 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。

6.5 配置数据源

在如 6.2 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

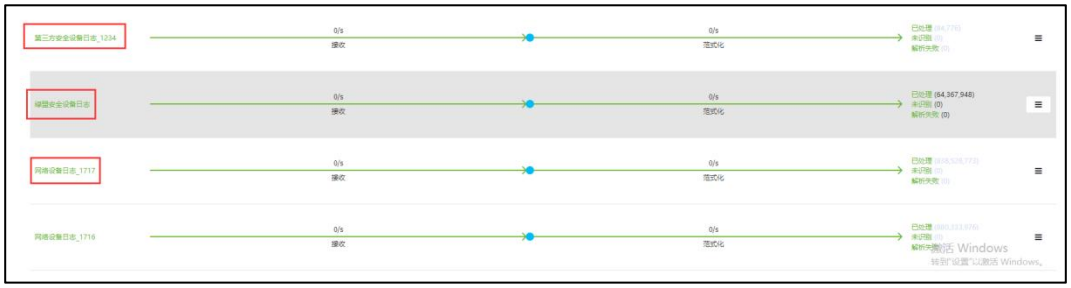


图 6-17 数据源详情

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》。

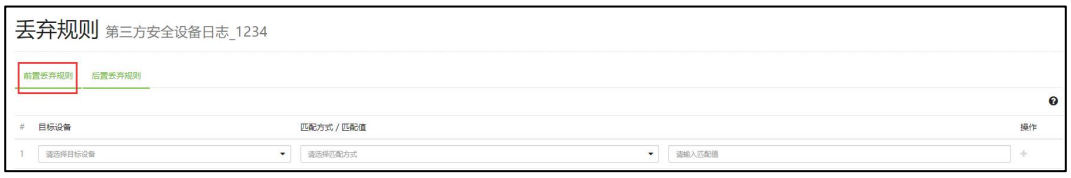
通过配置丢弃规则，可以丢弃某些不需要的字段，分为两种：

- 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 2 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）



步骤 3 选择目标设备、匹配方式及其匹配值，单击操作栏的➕，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图 6-19 表 6-1 所示。

图 6-19 前置丢弃规则（2）

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 4 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。

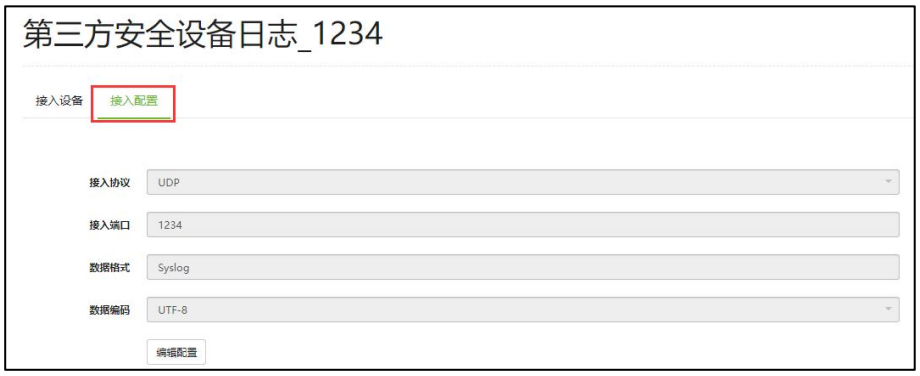
----结束

19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。

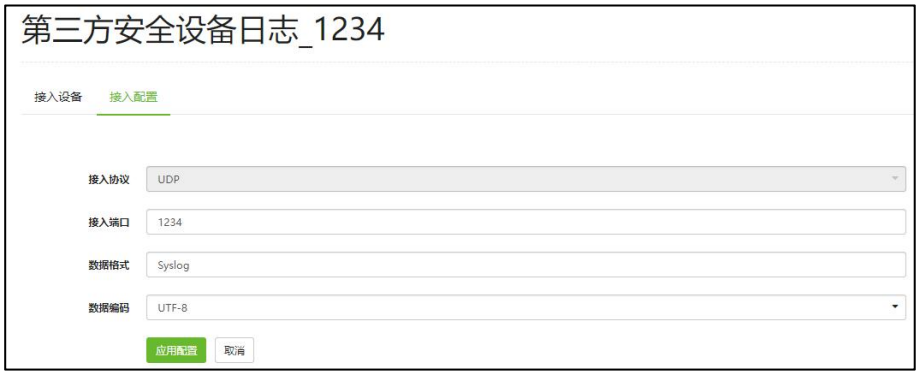
图 6-20 数据源的接入配置页



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



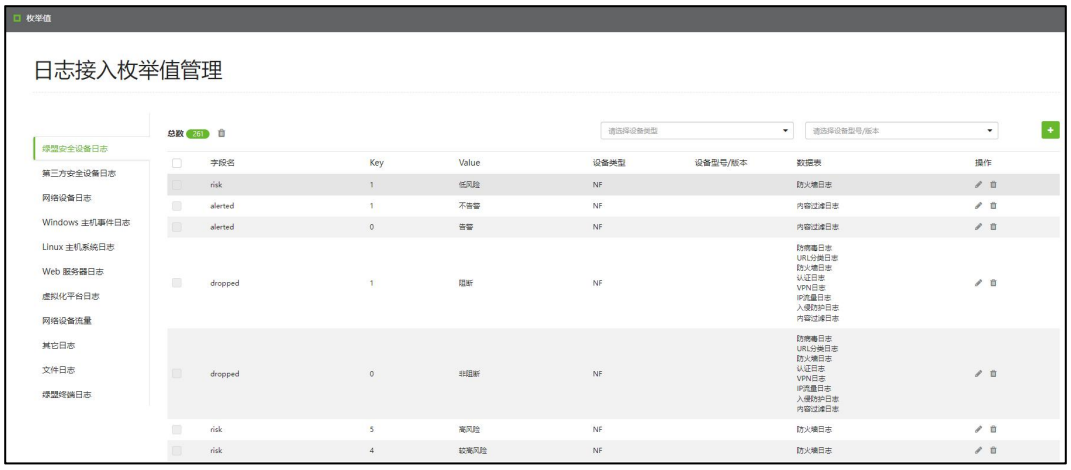
----结束

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，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**



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 2 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 3 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 b.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**

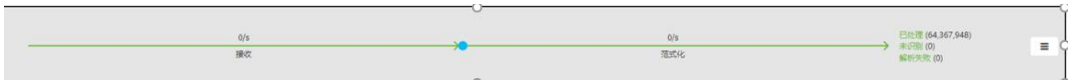


图 7-3 天翼云设备信息

步骤 4 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）

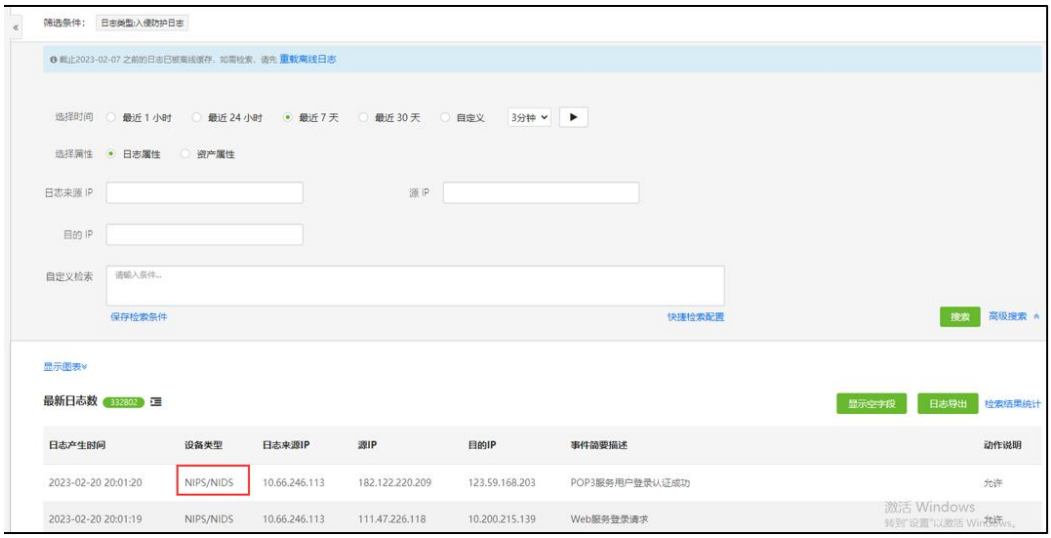
步骤 5 以 gr_type 字段为例，介绍日志详情的查看方法。

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）

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）



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）

----结束

8 采集终端

本章主要内容如下：

功能	描述
设备列表	介绍天翼云设备的接入方法。
Agent	介绍 Agent 的各类操作方法。

8.1 设备列表

设备是指天翼云科技的安全设备（例如：NIPS、NIDS）。只有当设备接入 LAS 后，才能向采集器上报日志/数据。

将鼠标悬停在总控制台图标，进入 **数据采集** > **采集终端** > **设备** 页面，如图 8-1 所示。

图 8-1 天翼云设备列表

不同版本的天翼云科技安全设备，在设备端接入 LAS 的方法略有不同，如表 8-1 所示。

表 8-1 天翼云设备接入方法

设备版本状态	设备及版本	通过设备端注册
新设备	NF V6.0R01F05	在设备端的 Web 管理页面进行配置，具体配置请参见 通过新设备端注册。
	NF V6.0R03F00	
	NF V6.0.1	
	NIDS/NIPS V5.6R10F00	

设备版本状态	设备及版本	通过设备端注册
	NIDS/NIPS V5.6R10F01	
	NIDS/NIPS V5.6R10F02	
	NIDS/NIPS V5.6R11F00	
	TAC V2.0R01F00	
	TAC V2.0R01F01	
	TAC V2.0R02F00	
	TAC V2.0R02F01	
	SAS V5.6R10F00	
	WAF V6.0R06F00	
	WAF V6.0R06F01	
	WAF V6.0R07F00	
	WAF V6.0R07F01	
	SAS-H V5.6R10F00	
老设备	NIDS V5.6.7~ V5.6.9	在设备端的 Web 管理页面进行配置，具体配置请参见 通过老设备端注册。
	NIPS V5.6.7~ V5.6.9	
	SAS V5.6.7~ V5.6.8	
	WAF V6.0R05F01	

注意	对于不同版本的不同设备，对设备管理各功能支持的情况不同，具体的支持情况请以页面展示为准。本节仅介绍在 LAS 上如何管理设备。

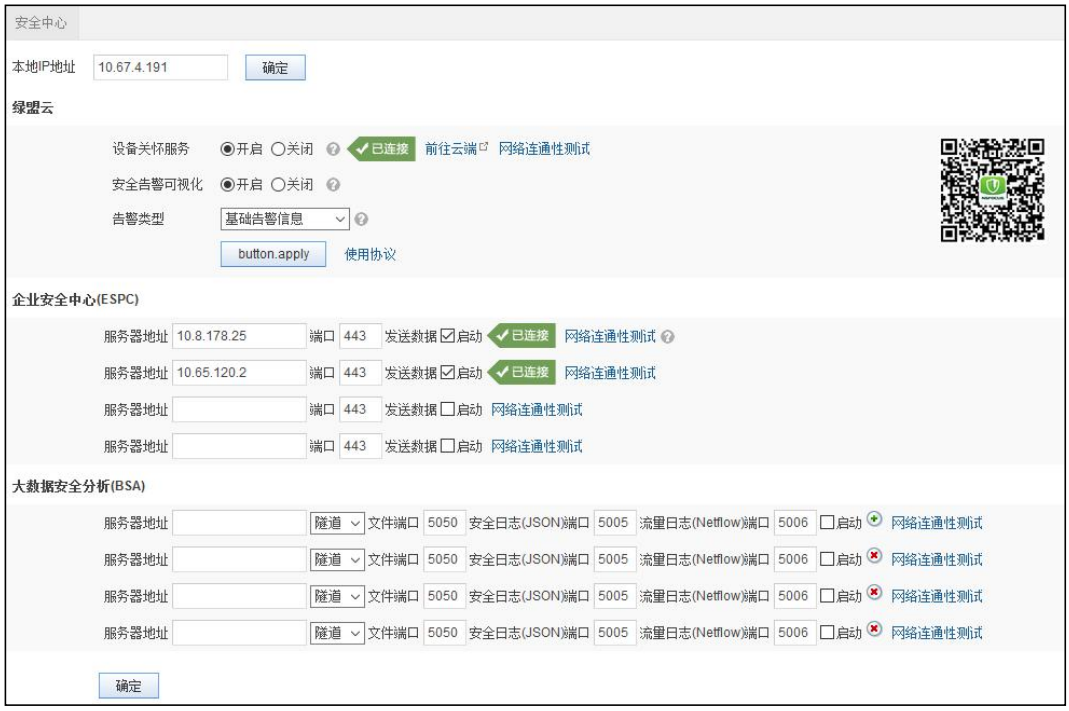
8.1.2 通过新设备端注册

以 NIPS V5.6R10F00 为例，介绍新版本的安全设备上如何配置，来实现设备端接入 LAS。

步骤 1 登录 NIPS。

步骤 2 进入 系统 > 安全中心 页面，如图 8-2 所示。

图 8-2 新设备的安全中心配置页面



步骤 3 配置连接参数，参数说明如表 8-2 所示。

表 8-2 连接参数

配置项		描述
本地 IP 地址		用于管理 NIPS 的 IP 地址。
企业安全中心（ESPC）	服务器地址	采集器的 IP 地址。支持连接至多台 LAS。
	端口	与 LAS 通信的端口号，目前仅支持 443。

步骤 4 勾选“启动”。

步骤 5 单击【确定】按钮。

连接成功后，状态会显示为“已连接”。

----结束

8.1.3 通过老设备端注册

以连接 NIPS V5.6.9 版本的安全设备为例，介绍老版本的安全设备上如何配置，来实现设备端接入 LAS。

步骤 1 登录 NIPS。

步骤 2 进入 系统 > 安全中心 页面，如图 8-3 所示。

图 8-3 老设备的安全中心配置页面

步骤 3 配置基本配置参数，参数说明如表 8-3 所示。

表 8-3 基本配置参数

配置项	描述
本地 IP 地址	用于管理 NIPS 的 IP 地址。
天翼云企业安全中心地址 1/2/3/4	采集器的 IP 地址。 • 对于同一 LAS，配置天翼云企业安全中心 1/2/3/4 中的任意一个即可。 • 支持连接至多台 LAS。

步骤 4 勾选“启动”。

步骤 5 单击【确定】按钮。

步骤 6 在弹出的对话框中，单击【确定】按钮。

步骤 7 重启引擎。

a. 进入 系统 > 系统控制 页面。

b. 单击【重启引擎】按钮。

----结束

8.2 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。

8.2.1 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 8-4 Agent 列表

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

图 8-5 Agent 下载页面

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 下载参数说明如图 8-6 表 8-4 所示。

图 8-6 平台端 Agent 下载配置

表 8-4 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，将对应的 Agent 下载到本地（请根据安装平台选择 Agent）。

----结束

8.2.2 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。

20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。

21在 Linux 系统中安装

步骤 1 登录 Linux 主机，切换为 root 权限。

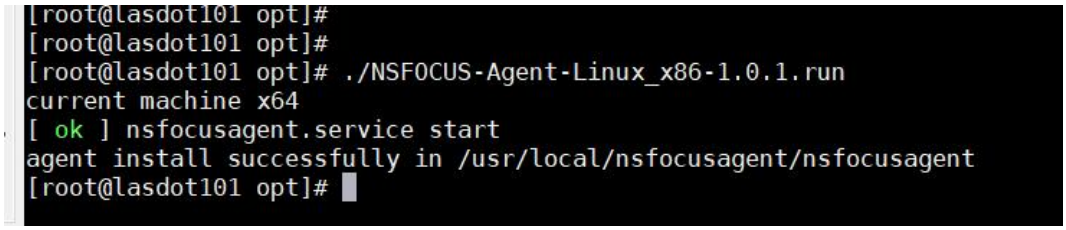
步骤 2 执行命令“chmod 755 CTYUN-Agent-Linux_x86-1.0.1.run”赋予 Linux 系统 755 权限，如图 8-7 所示。

图 8-7 在 Linux 系统中安装 Agent：赋权

```
[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 8-8 在 Linux 系统中安装 Agent：执行安装



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

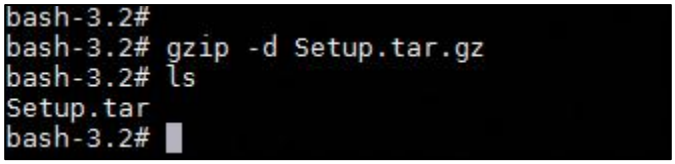
----结束

22在 Unix 系统中安装

步骤 1 登录 Solaris 10 主机。

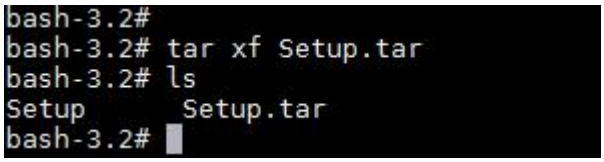
步骤 2 执行命令“gzip -d Setup.tar.gz”解压 Setup.tar.gz，得到 Setup.tar 压缩包，如图 8-9 所示。

图 8-9 在 Unix 系统中安装 Agent：获得压缩包



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 8-10 在 Unix 系统中安装 Agent：获得 setup 文件夹



步骤 4 执行命令“cd Setup”，进入 Setup 文件夹。

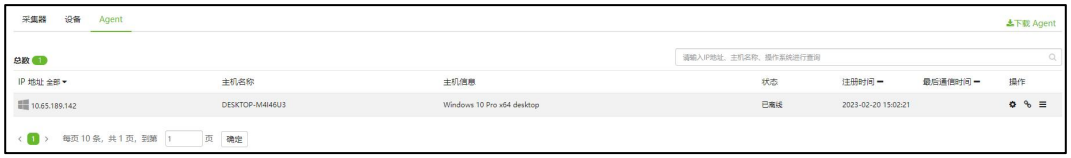
步骤 5 执行命令“./install.sh”，进行安装 agent，直至安装完成。

----结束

8.2.3 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 8-11 Agent 列表



8.2.4 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 8-12 Agent 数据采集配置

步骤 2 配置主机采集参数，参数说明如表 8-5 所示。

表 8-5 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。

配置项	描述
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。

表 8-6 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。 除了以上内置服务，支持填写服务名自定义应用服务。格式建议使用“应用类型”或“日志类型”。例如：apache.access 是指 apache 访问日志。
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 8-7 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 8-8 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、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，支持多选。

步骤 7 单击【确定】按钮，保存配置。

----结束

23Agent 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，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。

8.2.5 启用/禁用 Agent

在 Agent 列表中，单击操作栏的，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 8-13 启用/禁用 Agent

8.2.6 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，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 8-14 离线 Agent 不支持升级

8.2.7 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，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 8-9 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。
已更新	表示已经更新到 Agent 最新版本。

8.2.8 卸载 Agent

对于离线状态的 Agent，不支持卸载功能。

24卸载在线 Agent

在 Agent 列表中，单击操作栏的，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”。

注意	• Agent 卸载后不可恢复，请谨慎操作。 • 卸载 Windows/Linux 系统中的在线 Agent 的操作方法基本一致。

25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”。

----结束

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：

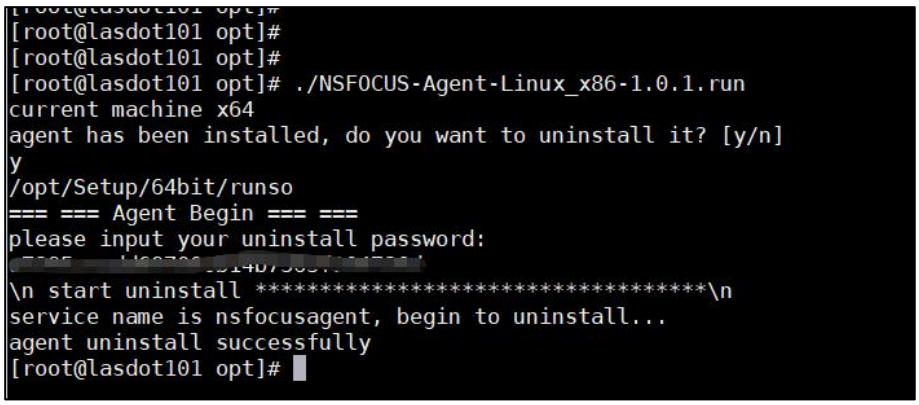
步骤 5 登录 Linux 主机。

步骤 6 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 8-15 执行卸载



步骤 7 显示“agent uninstall successfully”，卸载成功。

----结束

8.2.9 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。

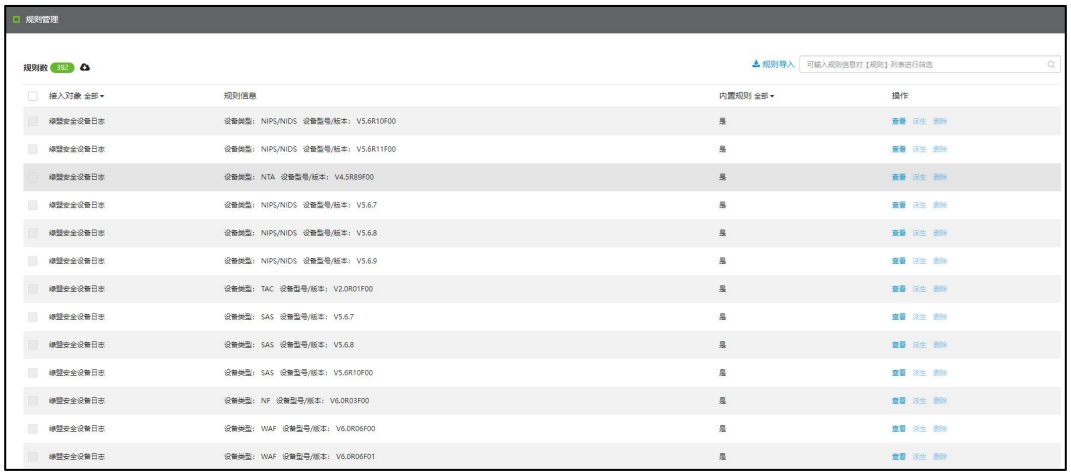
注意	• 在线状态的 Agent 删除后，若进行刷新操作，Agent 会重新出现在 Agent 列表中。 • 只有离线状态的 Agent 可以被彻底删除，删除后不可恢复，请谨慎删除离线状态的 Agent。

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，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



说明	• 内置日志解析规则，不支持删除和导出。 • 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。

26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。

27导出规则

单击规则列表上方的，支持批量导出所选的日志规则。

28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。

29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。

30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。

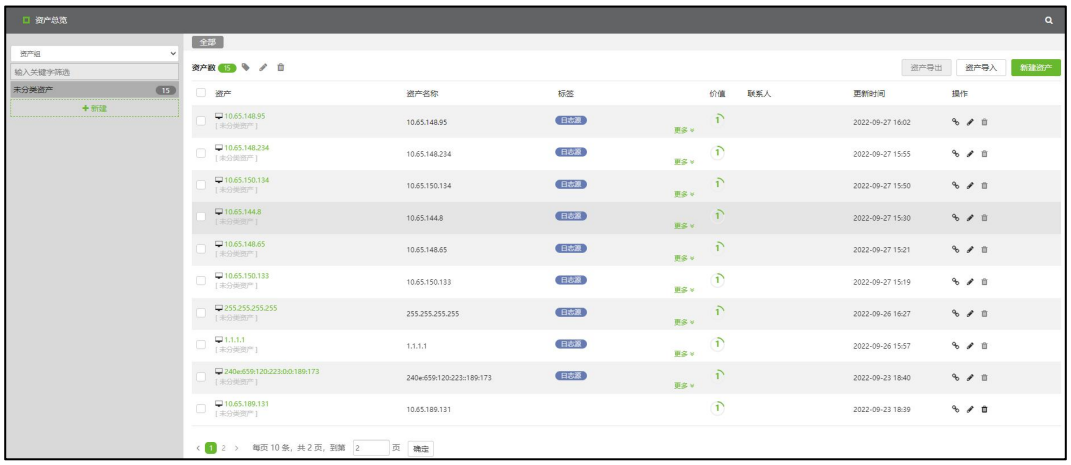
本章主要内容如下：

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

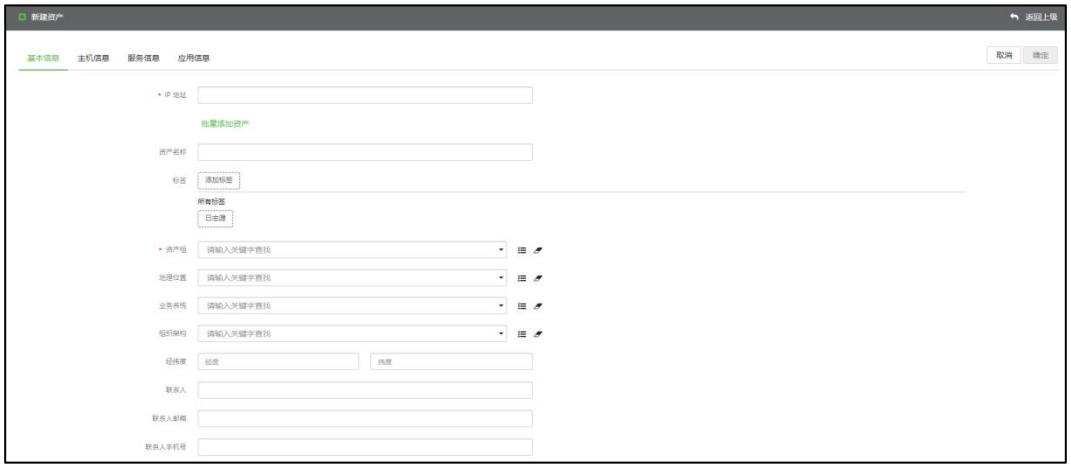


10.1.2 新建资产

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



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。

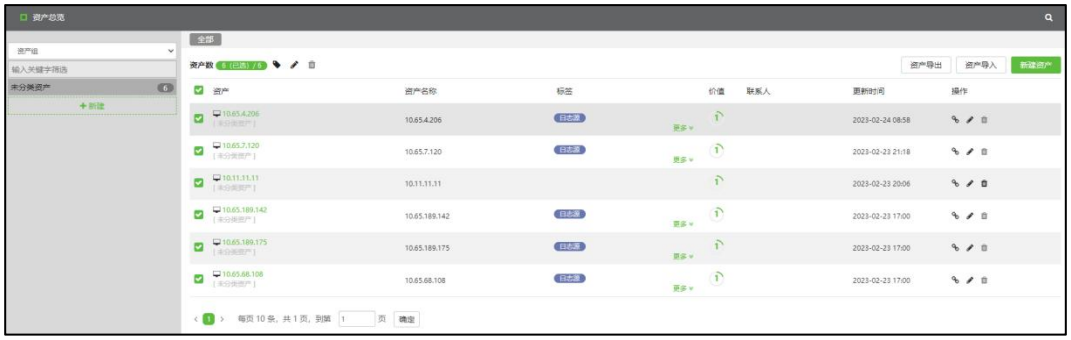
----结束

10.1.3 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



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

10.1.4 资产导入

说明	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： • 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。 • 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

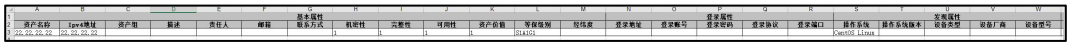
步骤 2 单击【下载导入模板】，将资产信息模板下载到本地。

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 b.图 10-6 所示。

b. 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。

c. 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

图 10-8 资产信息导入完成

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）

----结束

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）

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

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

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，将所选资产入库。

----结束

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图 11-1 表 11-1 所示。

图 11-1 日志检索

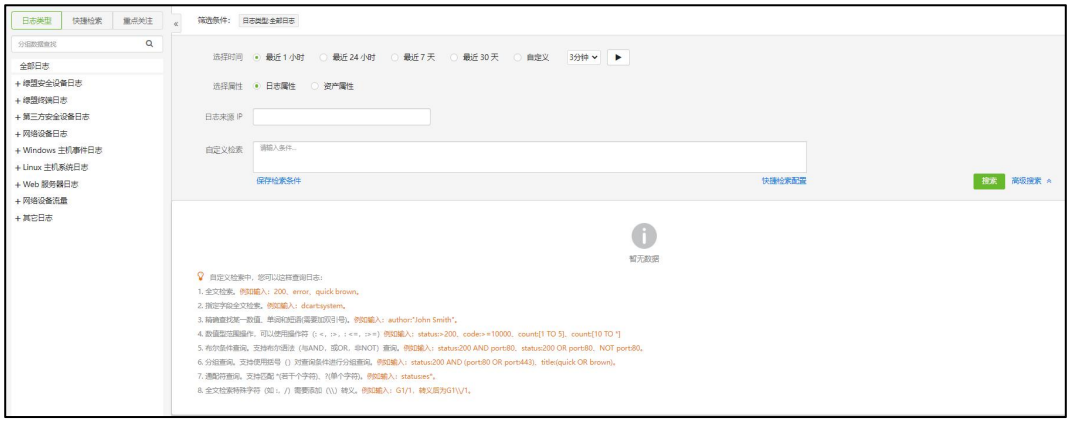


表 11-1 日志检索页面布局说明

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。
日志搜索条件	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。 ✓  ：切换为柱状图。 ✓  ：切换为折线图。 ✓  ：将当前的日志统计图保存为 PNG 文件。 • 以列表方式展示符合搜索条件的日志详情，同时支持日志的管理操作。请参见 日志管理操作。
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。

11.1.2 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
基本搜索	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。
	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▶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。
	资产 IP	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。 可以通过下拉列表进行选择，也可以通过单击进行选择。单击清除所选。
	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

查询项		描述
全部日志	日志来源 IP	日志源设备的 IP 地址。
天翼云安全设备日志	日志来源 IP	日志源设备的 IP 地址。
	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。
第三方安全设备日志	日志来源 IP	日志源设备的 IP 地址。
	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。
网络设备日志	日志来源 IP	日志源设备的 IP 地址。
	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。
Windows 主机事件日志	日志来源 IP	日志源设备的 IP 地址。
	用户	日志中的用户名称。
	操作	日志中的对主机进行的操作。
	日志名称	日志的名称。
Linux 主机系统日志	日志来源 IP	日志源设备的 IP 地址。
	日志名称	日志的名称。
Web 服务器日志	日志来源 IP	日志源设备的 IP 地址。
	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。

查询项		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。
网络设备流量	日志来源 IP	日志源设备的 IP 地址。
	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。

11.1.3 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 1111.1 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。

说明	单击某个检索条件的名称，将跳转至如 1111.1 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。

----结束

11.1.4 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 1111.1 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

11.1.5 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。

31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。

表 11-4 系统日志离线阈值

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。

32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

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

11.1.6 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 1111.1 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。

----结束

说明	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。

11.1.7 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 1111.1 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。

11.1.8 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。

33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。

34日志字段配置

单击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。

35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。

36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。

配置项	描述
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。

说明	• 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。 • 若需导出更多日志，建议分批多次进行导出。

37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账号密码变更。

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

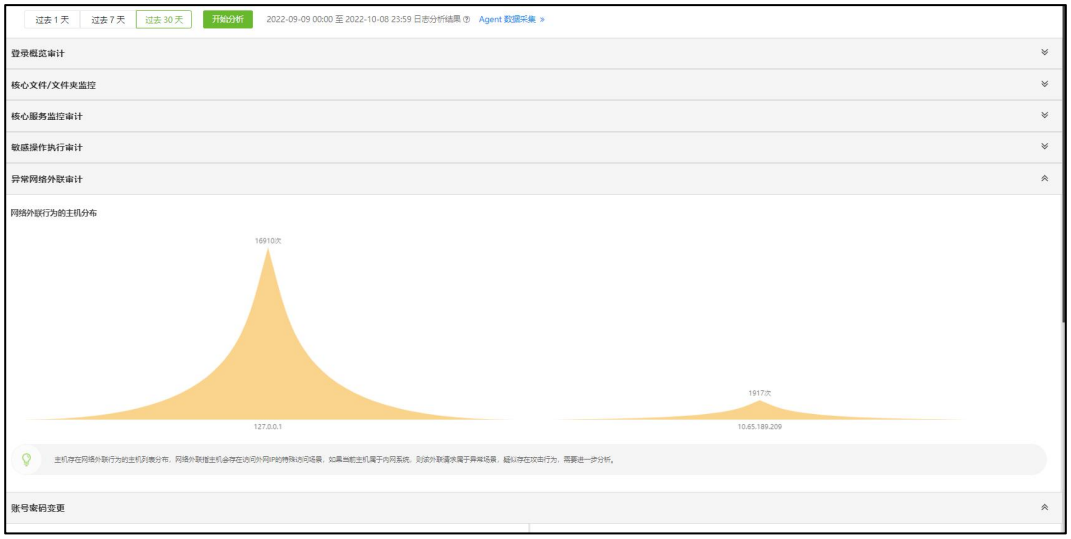


表 11-6 主机审计分析结果

展示项		描述
登录概览设计	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。
	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。
	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 的账号及次数。以可视化方式分析登录成功操作涉及的账号分布情况。
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。
账号密码变更	账号变更	针对主机日志，展示指定时间范围最近 10 次账号变更的详细记录。
	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图 11-4 表 11-7 所示。

图 11-4 Web 服务器日志分析

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。
请求关键点	请求浏览器类型分布 TOP10	展示指定时间范围 Web 访问请求发起次数 TOP 10 的浏览器类型及次数，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 IP 分布	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。 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
结果分析	布	注分析，是否存在疑似 DDoS 行为。 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。

----结束

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）

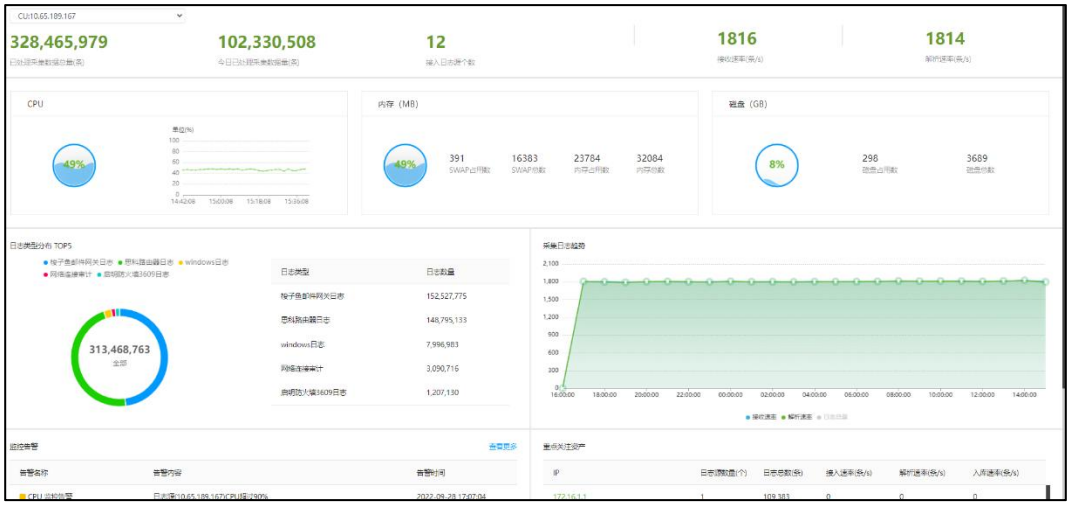


表 12-1 采集器维度日志源监控信息

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）。
今日已处理采集数据量	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。

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。
资源监控	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。
	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%。
采集监控	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）。
	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）。 说明 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图 12-3 表 12-4 所示。

图 12-3 采集资产监控

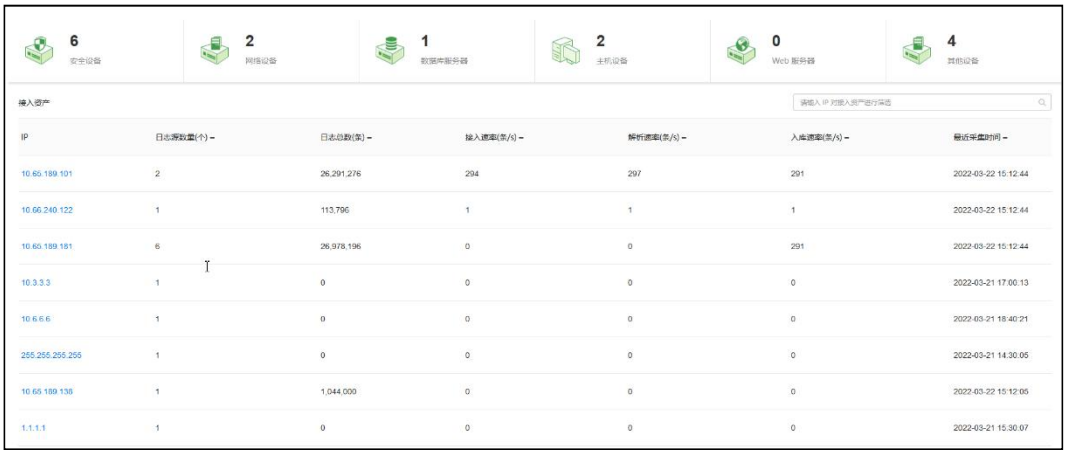


表 12-4 采集资产监控页内容

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。

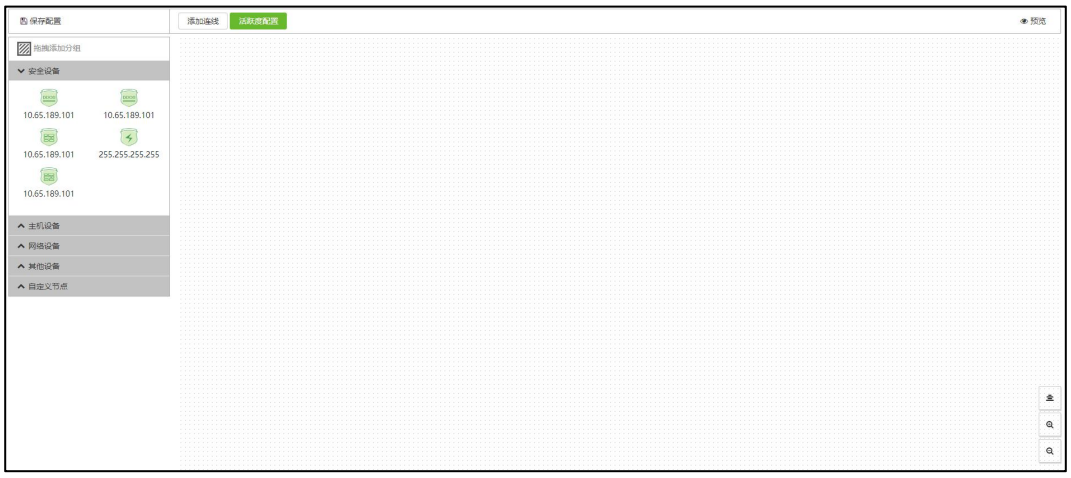
a. 若尚未配置日志源拓扑图，页面为空，单击【配置拓扑】进入步骤 2。

b. 若已有日志源拓扑，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



步骤 3 编辑拓扑图。

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  /  ，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 账号登录 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

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d.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。

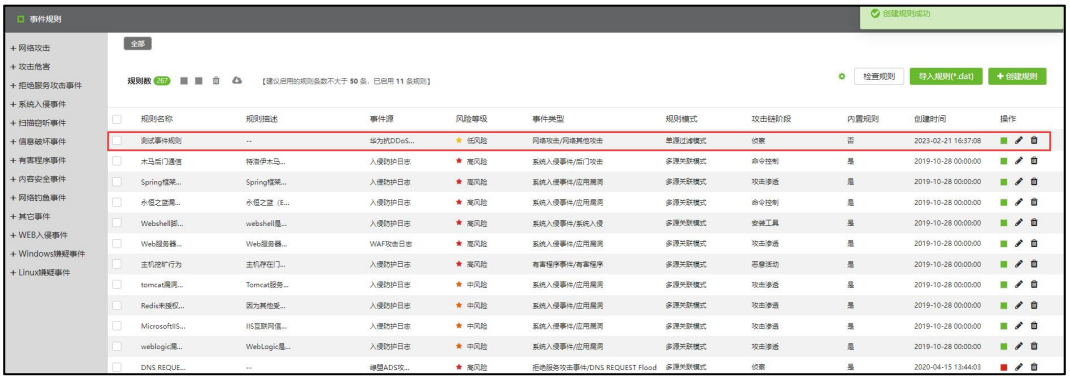
c. 事件源：选择步骤 2 接入的华为抗 DDoS 防护日志。

d. 单击【确定】按钮，创建事件规则。

图 13-2 创建事件规则

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。

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d.图 13-4 所示。

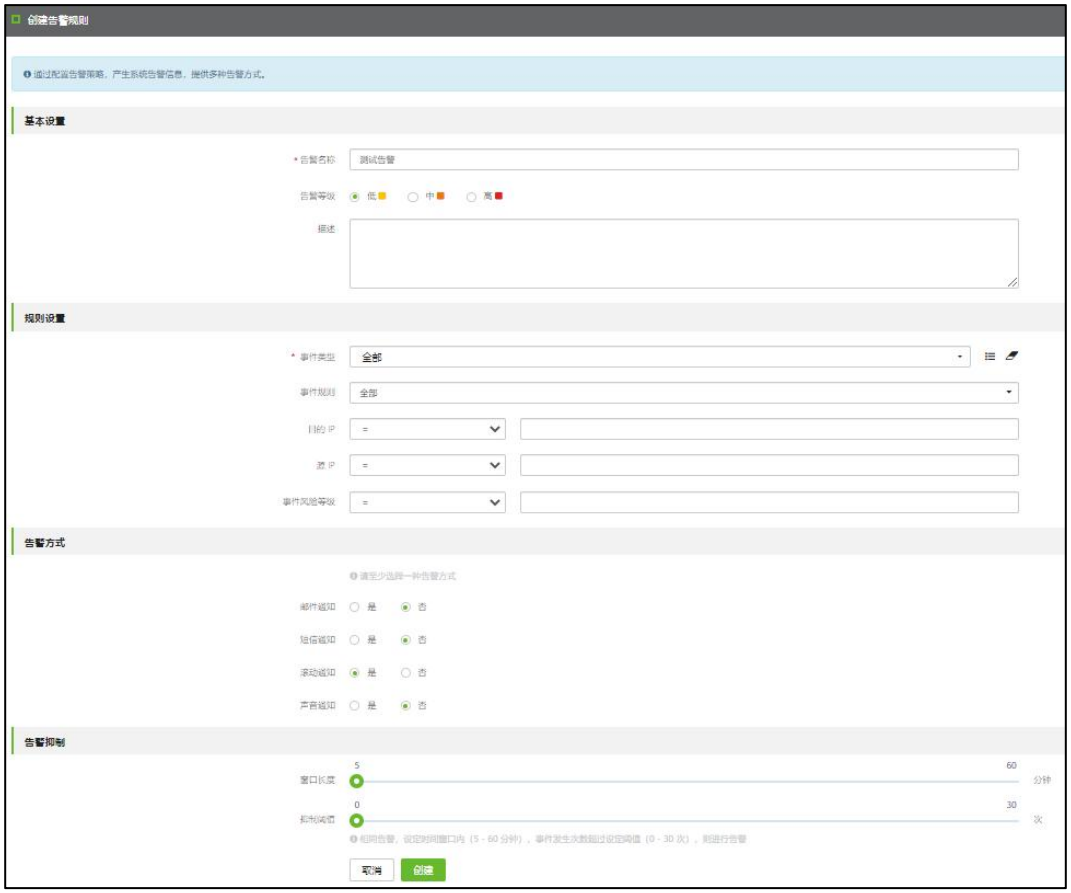
a. 规则设置：选择默认值，也可以根据实际需求进行填写。

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。

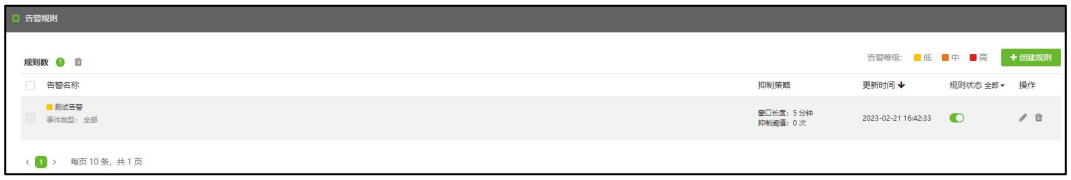
d. 单击【确定】按钮，创建告警规则。

图 13-4 创建告警规则



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



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 b.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

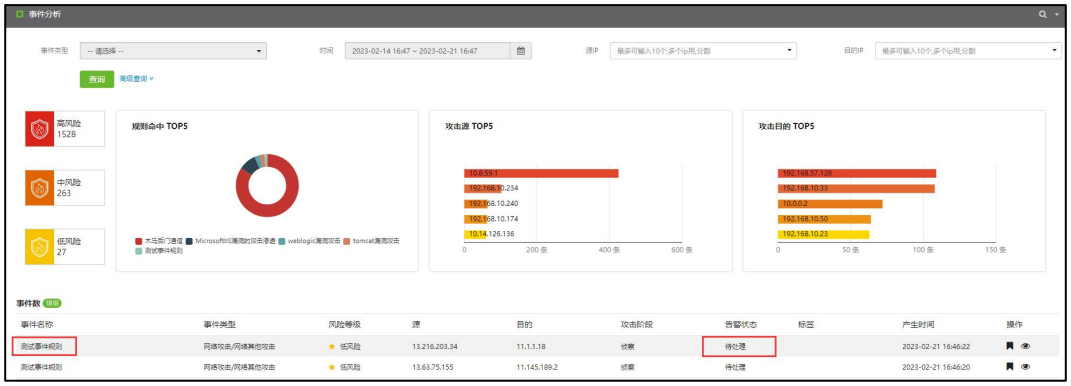
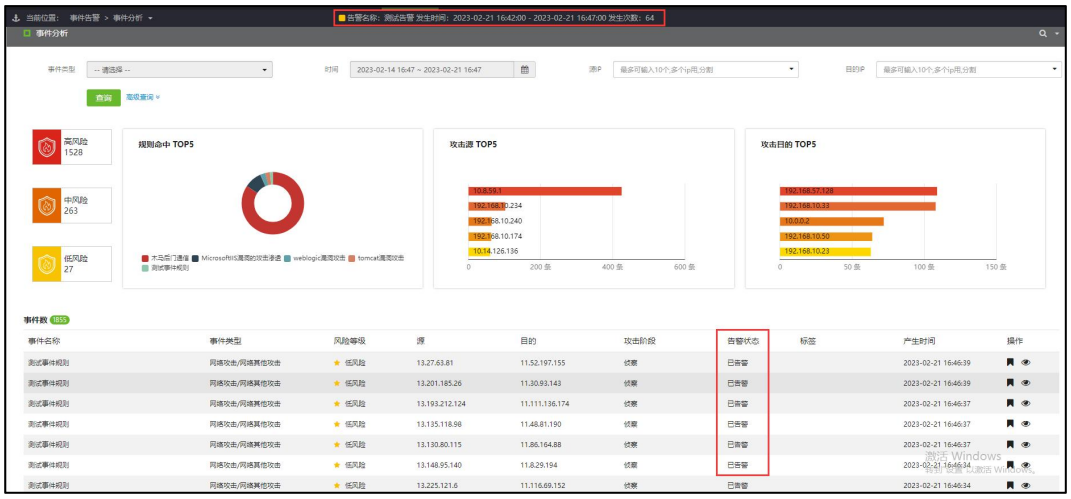


图 13-7 事件分析（显示告警信息）



----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

38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。

39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。

40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。

41查看在线报表

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

42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。

说明	• 手动通知/推送报表仅限当次有效，即不保存本次配置。 • 仅支持对现有报表进行通知/推送。

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
	调度中
28%	运行中
	运行成功
	运行失败
	已停止

14.2.2 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。

表 14-2 任务调度和报表设置参数

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。
周期执行	创建任务后，在指定时间周期性的执行报表任务，生成报表。 • 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。
报表模板	生成的报表中包含的内容。支持报表模板的模糊查询。
日志来源 IP	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。 配置后，仅对该 IP 或该段 IP 内的数据生成统计报表。

步骤 4 配置执行设置参数，参数说明如表 14-3 所示。

表 14-3 执行设置参数

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。 不能和已有报表任务重名，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。 •  ：生成 HTML 格式的报表。 •  ：生成 PDF 格式的报表。 •  ：生成 Word 格式的报表。

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
邮件通知	是否将报表发送至电子邮箱。启用前，需要配置邮件服务器，配置方法请参见 邮件服务器。

配置项	描述
	• 邮件地址：填写接收报表的电子邮箱。 • 选择附件：选择邮件附件中报表的类型。若不选择，仅发送通知，不发送附件。
SFTP 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 SFTP/FTP 服务器配置。 • 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。

说明	通知/推送报表的格式依赖于“报表类型”的选择，不能超出“报表类型”的范围。

步骤 6 单击【创建任务】按钮，完成新建报表任务的操作。

----结束

14.2.3 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。

43查看任务

单击报表任务所在行，展示对应的报表任务详情。

44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，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。

45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。

46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。

47手动通知/推送

单击操作栏的，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 步骤 5 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。

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。

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。
	配置各级别标题对应区域将展示内容的描述信息。
	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，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。

48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。

49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。

50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。

51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，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，可将所选的报表模板删除。

52复制模板

单击操作栏的，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。

53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。

54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。

55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，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，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 SFTP/FTP 服务器配置。

56手动备份日志

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。

配置项	描述
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。 说明 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。

57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。

表 15-2 自动备份日志参数

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。 说明 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。

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”管理权限的账号登录 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，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”管理权限的账号登录 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 15-2 所示。

图 15-2 可挂载磁盘信息

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。

注意	• NFS 不支持 IPv6。 • 集群部署下，不支持 NFS 配置。 • LAS 的软件版和硬件版支持 NFS 配置，虚拟化版不支持 NFS 配置。

58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

59配置方法

将鼠标悬停在总控制台图标，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。

说明	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 天，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

60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【  】，可以设置该消息为已读消息/删除该消息。

61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。

62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。

表 16-1 消息通知策略参数

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。
通知方式（至少选择一种通知方式）	邮件通知/邮件地址	是否开启消息邮件通知。开启后，需要配置接收邮件通知的邮箱地址。 开启邮件通知需要先进行 邮件服务器。
	短信通知/手机号码	是否开启消息短信通知。开启后，需要配置接收短信通知的手机号码。 开启短信通知需要先进行 短信服务器。
系统类/采集类通知抑制	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。 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。

A 出厂参数

本节介绍设备的出厂参数。

A.1 串口通讯参数

波特率	传输位数
115200	8

B 通信矩阵

B.1 支持的设备信息

本章介绍 LAS 支持接入的设备信息，接入方法请参见对应的操作指南。

支持设备	设备引擎版本
NF	V6.0.1 V6.0R01F05 V6.0R03F00
NIDS	V5.6.7 V5.6.8 V5.6.9 V5.6R10F00 V5.6R10F01 V5.6R10F02 V5.6R11F00
NIPS	V5.6.7 V5.6.8 V5.6.9 V5.6R10F00 V5.6R10F01 V5.6R10F02 V5.6R11F00
NTA	V4.5R89F00SP04 及以上版本
SAS	V5.6.7 V5.6.8 V5.6R10F00
SAS-ICS	V5.6.10
SAS-H	V5.6R10F00
TAC	V2.0R01F00 V2.0R01F01 V2.0R02F00

支持设备	设备引擎版本
	V2.0R02F01
OSMS	V5.6R10F00
FWCX	V6.0R70F30
WAF	V6.0R05F01 V6.0R06F00 V6.0R06F01 V6.0R07F00 V6.0R07F01

B.2 Agent 支持的操作系统

系统分类		版本信息
Windows		Windows XP
		Windows server 2003
		Windows server 2008
		Windows server 2012 说明 Standard 和 Datacenter 版均支持。
		Windows server 2016
		Windows server 2019
		Windows 7
		Windows 8
		Windows 10
Linux	X86	CentOS 6.5
		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

系统分类		版本信息
		Debian 6.0.6
		Debian 8.7
		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

系统分类	版本信息
	15.2