360数字安全

数 字 安 全 的 领 导 者

360 日志收集与分析系统

操作指南

版权声明

前言

概述

本文档介绍了 360 日志收集与分析系统（以下简称“**LAS 系统**”）的基本概念、基本功能、操作流程和方法，以指导读者了解和使用 LAS 系统。

读者对象

- 实施工程师
- 开发工程师
- 测试工程师
- 售前工程师
- 售后工程师
- 安全主管
- 安全分析/安全运营人员

通用约定

在本文中可能会出现下列文字，它们所代表的含义如下：

符号	说明
	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的后果。
	表示是正文的附加信息，是对正文的强调和补充。

修订记录

文档版本 01 （2024-7-31）

首次发布

目录

1. 快速入门 1
1.1 登录和退出 LAS 系统 1
1.2 系统初始化 3
1.2.1 导入内容包 3
1.2.2 网络环境初始化 4
1.2.2.1 配置内网 IP 4
1.2.2.2 配置网卡 6
1.2.2.3 配置 DNS 6
1.2.3 赋能管理 7
1.2.3.1 配置情报云 7
1.2.3.2 分级部署配置 7
1.2.4 配置服务器时间（NTP） 8
1.3 一键重启 LAS 系统 8
2. 监控态势 9
2.1 工作台 9
2.2 仪表监控 10
2.2.1 维护仪表盘 10
2.2.1.1 维护仪表盘分类目录 10
2.2.1.2 创建仪表盘 11
2.2.1.3 分享仪表盘 14
2.2.1.4 设置常用仪表盘 15
2.2.1.5 切换全屏 16
2.2.1.6 设置筛选条件 16
3. 智能检索 18
3.1 场景化检索模式 18
3.2 综合检索模式 20
3.2.1 表格视图功能 20
3.2.1.1 界面简介 20
3.2.1.2 数据分析 21
3.2.1.3 设置列表字段 22
3.2.1.4 查询日志详情 25
3.2.1.5 字段内容的更多功能 25
3.2.1.6 解码功能 27
3.3 更多关联操作 27
3.3.1 发布查询条件和图表 27
3.3.2 管理历史查询条件 28
3.4 数据分类和关联查询 28
3.4.1 查询 28

3.5 可视化分析 29
3.5.1 配置流程说明 29
3.5.2 配置界面简介 30
4. 资产管理 32
4.1 资产列表 32
4.2 配置资产拓扑图 32
5. 报表中心 34
5.1 报表模板 34
5.2 报告任务 36
5.3 报告列表 38
5.3.1 功能概览 38
5.4 图表管理 39
5.4.1 配置图库分组 39
5.4.2 添加图表 40
5.4.3 管理图表 40
6. 等保助手 42
6.1 等保管理 42
6.2 等保知识库 43
7. 管理知识/案例库 46
7.1 管理知识库 46
7.1.1 配置知识分类 46
7.1.2 配置知识 47
7.2 管理案例库 48
7.2.1 配置案例分类 48
7.2.2 配置案例 49
8. 配置数据接入 52
8.1 数据存储管理 52
8.1.1 创建“KAFKA”类型的数据存储 52
8.1.2 创建“网络转发”类型的数据存储 59
8.1.3 创建“数据转发”类型的数据存储 61
8.1.4 创建“HDFS”类型数据存储 61
8.1.5 更多操作 64
8.2 解析规则管理 64
8.2.1 新建简单模式的解析规则 65
8.2.1.1 简单模式解析规则组成 65
8.2.1.2 基础配置 65
8.2.1.3 解析预览 67
8.2.1.4 数据映射 73
8.2.1.5 预览提交 77

8.2.2 新建高级模式的解析规则 78
8.2.3 解析规则-正则表达式 89
8.2.4 解析规则-键值对 92
8.2.5 解析规则-分隔符 96
8.2.6 解析规则-CEF 101
8.2.7 解析规则-JSON 106
8.2.8 解析规则-不解析 111
8.3 数据接入管理 119
8.3.1 配置前说明 119
8.3.2 配置基本信息 120
8.3.3 采集类型为“本地文件或目录” 122
8.3.4 采集类型为“网络” 123
8.3.5 采集类型为“数据库” 126
8.3.6 采集类型为“KAFKA” 127
8.3.7 采集类型为“HDFS” 131
8.3.8 采集类型为“AWS” 134
8.3.9 采集类型为“SFTP” 136
8.3.10 采集类型为“数据接收” 139
8.3.11 采集类型为“WMI” 139
8.3.12 采集类型为“SNMP” 144
8.3.13 采集类型为“ELASITCSEARCH” 146
8.3.14 更多操作 147
8.4 日志代理 148
8.4.1 Linux 日志代理 149
8.4.2 Windows 日志代理（64 位） 149
8.4.3 Windows 日志代理（32 位） 151
8.5 属性配置 152
8.6 对象配置 156
8.7 数据丰富化 162
8.7.1 二元组丰富化 162
8.7.2 五元组丰富化 163
8.7.3 资产丰富化 164
8.7.4 GEO 丰富化 165
8.7.5 自定义丰富化 166
9. Agent 接入 168
9.1 Agent 管理 168
9.2 Agent 状态日志 170
9.3 Agent 下载 170
9.3.1 Linux 安装 170
9.3.2 Windows agent 安装 171

10. 配置分析管理 173
10.1 维护 SAE 安全分析规则 173
10.1.1 配置前须知 173
10.1.2 配置注意事项 175
10.1.3 SAE 规则-“普通模板” 176
10.1.4 SAE 规则-“普通模板-having count(DISTINCT)” 180
10.1.5 SAE 规则-“普通模板-having count” 182
10.1.6 SAE 规则-“普通模板-having sum” 184
10.1.7 SAE 规则-“普通模板-not_occur” 187
10.1.8 SAE 规则-“关联模板-follow_by” 189
10.1.9 SAE 规则-“关联模板-or_follow_by” 192
10.1.10 SAE 规则-“关联模板-not_follow_by” 196
10.1.11 SAE 规则-“关联模板-Repeat-Until” 198
10.1.12 SAE 规则-“关联模板-any_order” 200
10.1.13 SAE 规则-“关联模板-not_before” 202
10.1.14 非法配置举例 204
10.1.15 导出规则 206
10.1.16 导入规则 206
10.1.17 更多操作 208
10.2 维护安全信息 209
10.2.1 配置信息组分类 209
10.2.2 配置信息组 210
10.2.3 配置信息 212
10.3 管理本地情报 215
10.4 管理全局白名单 217
10.5 管理内容包 218
11. 管理用户 220
11.1 开启数据分权 220
11.2 配置组织机构 220
11.3 配置本地用户 222
11.3.1 配置角色 222
11.3.2 配置本地用户 224
11.4 配置 LDAP 用户 226
11.4.1 连接 LDAP 服务器 226
11.4.2 添加 LDAP 用户 227
11.4.3 LDAP 用户登录方式 229
11.4.4 维护 LDAP 用户 230
12. 基础配置 231
12.1 网络配置 231
12.2 通知管理 232

12.2.1 SMTP 配置与阿里云短信 232
12.2.2 新增通知对象 234
12.2.3 维护通知对象 236
12.3 存储配置 236
12.3.1 配置日志存储 236
12.4 数据备份 237
12.4.1 自定义备份时间 238
12.4.2 数据备份查询 239
12.5 环境信息 239
12.5.1 代理配置 239
12.5.2 设定服务器时间 240
12.5.3 赋能天数显示开关 240
12.6 安全策略 241
12.7 可信主机 243
12.8 上报配置 244
12.9 通知中心 246
12.9.1 通知中心预览 246
12.9.2 配置通知 248
12.9.3 查看推送消息详情 249
12.9.3.1 系统通知 249
12.10 自定义页面元素 250
13. 版本管理 253
13.1 License 管理 253
13.2 升级管理 254
13.3 查看 API key 254
14. 监控系统日志 255
14.1 查看审计日志 255
14.2 查看更新日志 255
15. 系统监控 257
15.1 SNMP 监控 257
15.2 查看系统状态 259
15.3 监控告警说明 260
15.4 设置监控告警 261
15.5 设备管理 261
16. 分布式管理 262
16.1 默认模式 262
16.2 管理节点模式 262
16.3 子节点模式 264
16.4 配置管理 265

附录 267
A.1 HQLite 语法 267
A.1.1 概述 267
A.1.2 全文检索语句 267
A.1.3 运算符的功能和使用 268
B 在搜索分析中的应用 268
C 在 SAE 关联分析规则中的应用 274
D HQL Time Filter 277
D.1 如何开启 WMI 配置 280
D.1.1 配置 Windows 操作系统登录用户 280
D.1.2 在本机测试是否可以连接远程主机 WMI 服务 284
D.1.3 开启远程计算机 WMI 服务 287
D.2 如何开启 SNMP 服务 296
FAQ 298

1. 快速入门

在使用 360 日志收集与分析系统（以下简称“LAS 系统”）之前，您需要先了解 LAS 系统包括哪些功能和服务，以及使用功能向导，便于您快速定位。

1.1 登录和退出 LAS 系统

申请并导入有效 license 后，如何登录 LAS 系统。

背景信息

产品的 license 激活成功后返回登录页面，显示需输入的登录信息。系统管理员的用户名和密码示例为“sysadmin/Q*******c”，此用户拥有 LAS 系统所有管理对象的所有操作权限；安全保密管理员的用户名和密码为“secadmin/Q******c”，此用户拥有用户的管理权限； 审计管理员的用户名和密码为“auditadmin/Q******c”，此用户拥有所有记录的管理权限。

如需获取默认密码，可联系 360 技术支持。

激活 LAS 系统

步骤1. 打开浏览器，访问 URL：https://IP，进入登录页面，界面显示：“**当前产品未导入许可证！您的产品特征码为：XXXXXXX**”。

步骤2. 获取 License 文件。

- （方法一）使用手机扫描二维码获取产品特征码，并提供给 360 技术支持，由 360 技术支持提供 License 文件。

- （方法二）单击二维码下方的“**您的产品特征码**”，显示特征码字符串，提供给 360 技术支持，由 360 技术支持提供 License 文件。

步骤3. 单击“**选择**”，选取 License 文件后单击“**导入**”。

- 若导入成功，随后跳转到正常登录页面，界面显示如下图所示。

- 若导入的 license 无效，则导入失败，界面会显示导入失败的红色提示信息，提示信息可能为“**当前许可证校验失败！**”或“**当前许可证不可用！**”。

登录 LAS 系统

步骤1. 打开浏览器，访问 URL：https://IP，进入登录页面。

步骤2. 输入用户名、密码和验证码，并单击“**登录**”。

入门指引

登录成功后，页面弹出“**入门指引**”，可快捷进入相关页面进行配置 。单击 不再显示，下次登录不会再弹出该向导页。

退出 LAS 系统

单击 LAS 系统页面右上角的 退出。

1.2 系统初始化

首次登录后，需要初始化一系列配置，便于您快速高效的使用 LAS 系统。

1.2.1 导入内容包

通过导入内容包，可以初始化 LAS 系统的内置信息，包括：事件、解析规则、安全信息、知识库和案例库、关联分析、图表、仪表盘、报表模板。

前提条件

您已获取内容包（.zip 包），获取方式请联系 360 技术支持。

操作步骤

步骤1. 单击导航栏右侧，进入“**系统设置**”页面，选择菜单“**分析管理** > **内容包管理**”。

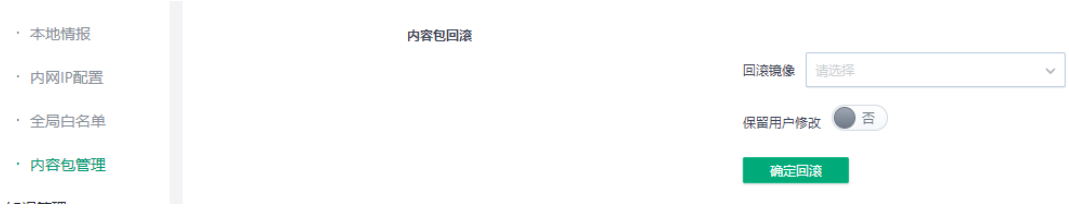
步骤2. 在“**数据文件**”参数下，单击“**上传文件**”，弹出本地文件系统，选择需要导入的文件，单击“**打开**”。

步骤3. 单击“**导入**”。

- 导入成功后，给出提示信息，显示：**导入成功。
- 导入失败后，给出错误提示信息，包括：文件格式错误，文件大小（系统支持最大 20M 的文件导入）错误，文件内容不合法错误。

后续处理

如若内容包在线更新后，发现不适用，可使用回滚功能，将内容包回滚到更新前的版本。在下拉列表中选择待回滚的镜像，根据需要是否打开保留用户修改的开关，单击“**确认回滚**”，即可回滚至导入前的配置。



1.2.2 网络环境初始化

为保证 LAS 系统的网络环境正常，展示内网态势信息，请预先配置内网 IP。

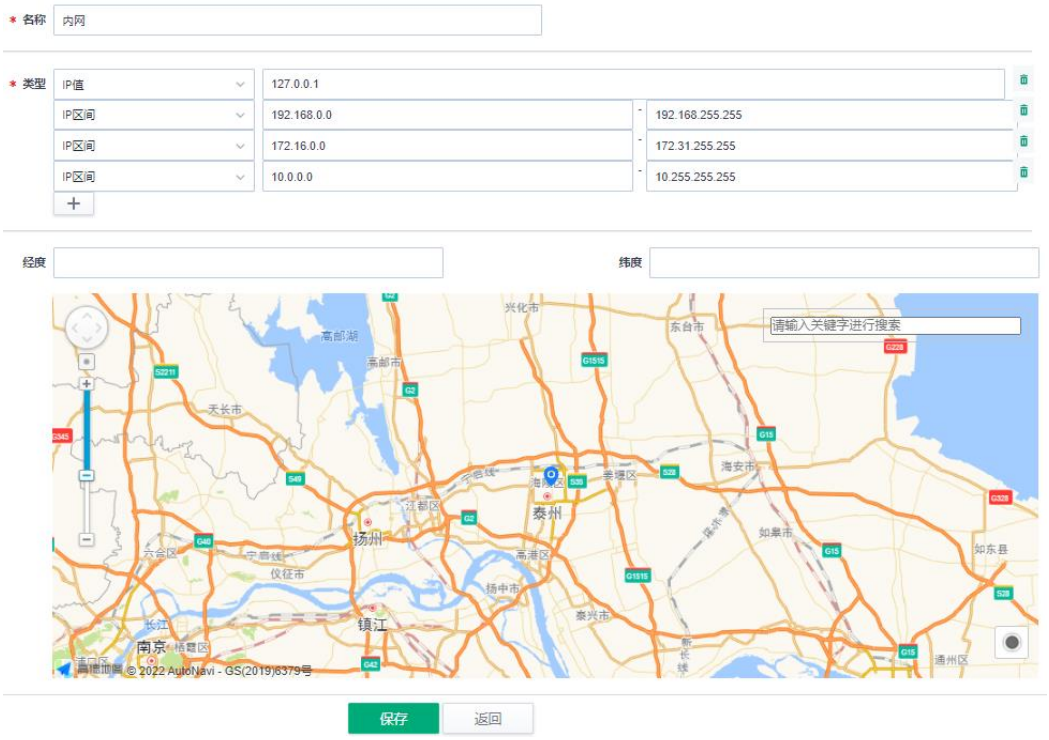
1.2.2.1配置内网 IP

*在使用内网之前，需要先在内网编辑页面，单击“**确认**”，使内网生效。*

操作步骤

步骤1. 单击导航栏右侧，进入“**系统设置**”页面，选择菜单“**分析管理 > 内网 IP 配置**”。

步骤2. 单击“**新增**”，显示内网 IP 新增界面。



步骤3. 配置内网 IP 相关参数。

参数名称	参数说明
名称	配置的内网 IP 的名称。

参数名称	参数说明
类型	通过单击 +，添加内网类型。 • 内网类型包括以下选项： – IP 值：在后面的输入框输入指定的 IP 值。 – IP 区间：在后面的输入框输入指定的 IP 区间。 – 子网掩码：在后面的输入框输入 IP 地址和子网掩码的位数。 – IPV6 值：在后面的输入框输入指定的 IPV6 值 – IPV6 区间：在后面的输入框输入指定的 IPV6 区间。 – IPV6 前缀：在后面的输入框输入 IPV6 地址和子网掩码的位数。 • 内网 IP 支持多种内网类型的添加，单击 +，可弹出新的一行配置。 • 若需删除特定类型的内网类型，单击 。
经纬度	通过输入城市或地址名称，嵌入地图确认经纬度。输入关键字，经纬度信息随之更新。

步骤4. 单击“**确认**”，添加内网成功。

更多操作

操作	说明
修改	您可以通过单击内网 IP 列表后的 ，编辑内网 IP 的参数。
删除	• 方式一：您可以通过单击内网 IP 列表后的 ，删除该条内网 IP 数据。 • 方式二：当内网 IP 列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。

在“智能检索”中的应用

在“**智能检索**”中，需要查询指定内网下产生的日志/告警时，

“**日志查询**”、“**告警查询**”可使用“**IP 类型的属性**”，如属性“**源地址**”属于“**内网**”（即以上配置的内网名称）的条件查询筛选，如：

1.2.2.2配置网卡

LAS 系统开机通电并启动后，将分配给 LAS 系统的网线连接到服务器的 eth0 网口，根据分配的 IP 和网络配置网卡信息。

操作步骤

步骤1. 在“**网络配置**”页面，单击“**网卡配置**”页签。

步骤2. 单击✎，编辑网卡信息。

参数名称	参数说明
IP	分配给服务器的 IP 地址。
子网掩码	当前服务器所在网络环境的子网掩码。
网关	当前服务器所在网络环境的网关。

步骤3. 单击“**保存**”，即可保存网卡配置。

1.2.2.3配置 DNS

操作步骤

步骤1. 在“**网络配置**”页面，单击“**DNS 配置**”页签。

步骤2. 单击“**新建**”，配置 DNS 信息，输入 DNS IP 地址。

步骤3.　单击“**保存**”，即可保存配置。

1.2.3 赋能管理

在“**赋能管理**”下，可以分别配置情报云和分级部署配置。

1.2.3.1配置情报云

申请人收到 **apikey** 和 **salt** 值、情报云用户名后，可在初始化设置中填写注册。

获取“apikey、salt 和 tip 用户名”

这三个参数用于对接情报云云端，从情报云云端拉取情报，获取情报升级的权限。因为数据源在云端，所以授权一定是云端授权。

目前由产线代向情报云团队申请，并通过邮件返回。因此申请人在申请 LAS 系统 license 时，务必勾选选项“**情报云**”，且填写《**申请情报云**》的表单。

操作步骤

步骤1.　在“**系统设置**”下，选择菜单“**版本信息** > **赋能管理**”，显示“**赋能管理**”配置页面。

步骤2.　在“**情报云配置**”区域，配置情报云的 **apikey** 和 **salt** 值和“**情报云用户名**”。

步骤3.　单击“**保存**”，可成功对接 360 情报云。

1.2.3.2分级部署配置

该功能适用于私有云 ES 集群可互通场景下的上下级级联对接。配置后上级可以查看下级的数据信息。

在“**版本信息** > **赋能管理**”下的“**分级部署配置**”区域，通过配置本级的节点名称，上级节点地址，上级节点用户名和上级节点用户密码，完成与上级节点的对接。

1.2.4 配置服务器时间（NTP）

在“**系统设置**”下，选择菜单“**基础配置 > 环境信息**”，“**服务器时间（NTP）设定**”区域支持配置 NTP 参数，保持服务时间的一致性。默认使用系统时间，打开“**使用 NTP 时间**”的开关后，可设置 NTP 的服务地址。

1.3 一键重启 LAS 系统

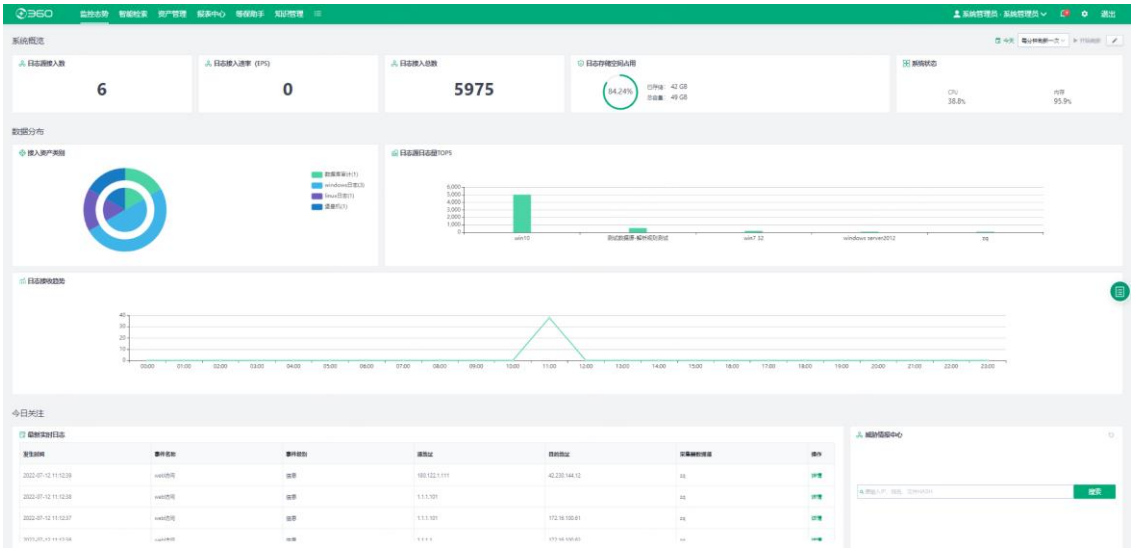
在导航栏单击，选择“**系统监控 > 设备管理**”，LAS 系统进入“**设备管理**”页面，可系统重启、设备关机和恢复出厂设置。

其中：恢复出厂设置指的是恢复到产品刚安装完成的状态。

2. 监控态势

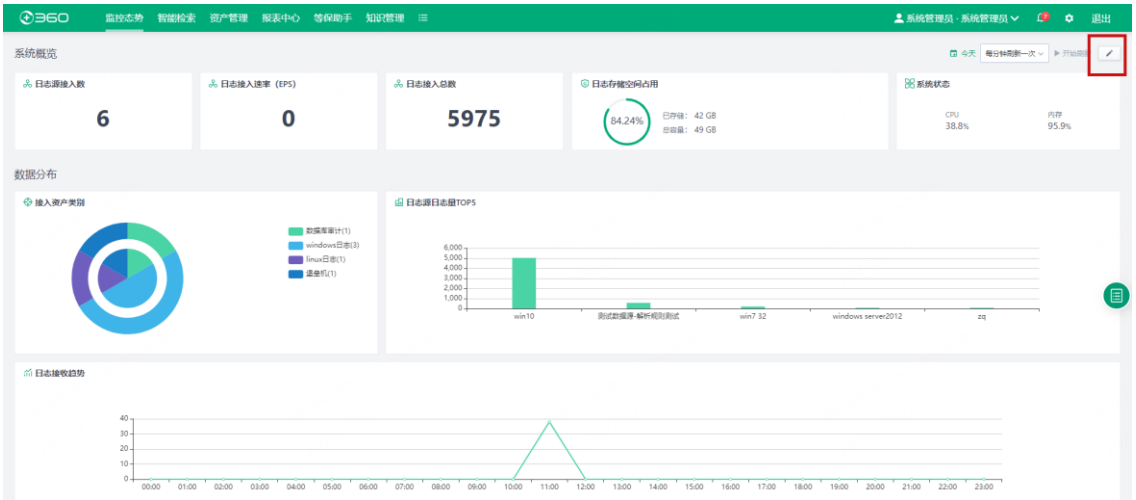
2.1 工作台

工作台是用户登录后进入的系统首页，由大量专项设计的仪表盘构成，用户可清晰浏览系统概况。除了引入各类新设计组件，同样支持自定义仪表盘引用，支持数据下钻。用户可设计个人专属工作台。默认工作台样式如下：



编辑工作台

选择右上角的编辑图标，滑出图库。从图库中选择需要的图表，拖拽到左侧分组中。分组可新增，可调整顺序。



2.2 仪表监控

仪表盘采用组件化设计，各角色用户可根据自己的需求灵活配置个人工作台。通过个人工作台用户可实时监控和统计分析自己负责的日志和告警，并可通过个人工作台直接下钻到日志事件进行安全分析。

2.2.1 维护仪表盘

您可以在创建仪表盘目录后，或者选择已有的目录下，创建所需监控的仪表盘。

通常，您需要通过拖拽“**图库管理**”中的图表创建仪表盘。“**图库管理**”中的图表部分已内置，您亦可自定义图表。

2.2.1.1维护仪表盘分类目录

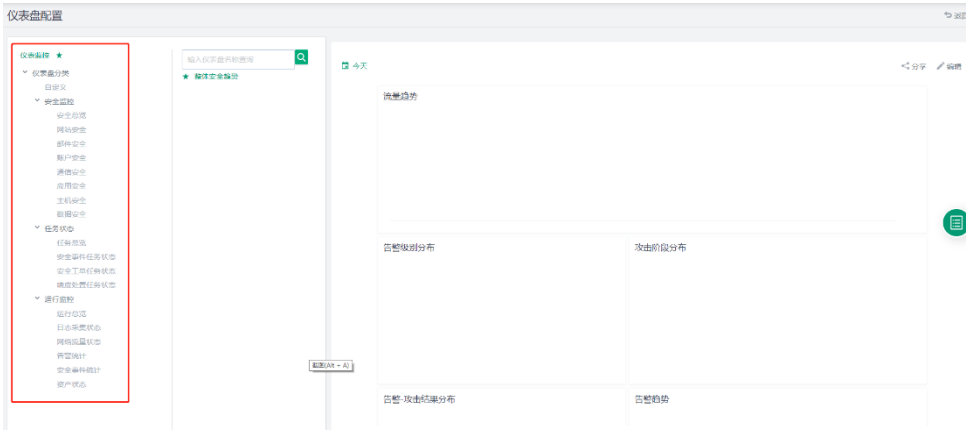
为了更好地维护仪表盘，您可以通过目录管理仪表盘，方便查找与归类。

操作步骤

步骤1. 在导航栏，单击菜单“监控态势 > 仪表监控”，LAS 系统显示“常用仪表监控”界面。

步骤2. 单击当前仪表盘页面右上角“**设置**”，可进入“**仪表盘配置**”页面。

平台仪表盘目录结构，如图所示：



步骤3. 单击“**仪表盘分类目录**”根节点后的 ✚ 按钮，弹出添加仪表盘目录对话框，如图所示。

步骤4. 输入新节点的名称，并单击“**确认**”。

仪表盘分类目录最多设置两级。

更多操作

操作	说明
修改仪表盘分类目录名称	您可以通过单击节点后的编辑图标，修改目录的命名。
删除仪表盘分类目录	您可以通过单击目录后的删除图，删除该条目录。 当删除的目录下有仪表盘，则该仪表盘会归置于上一级目录下。
查询仪表盘	您可以在搜索框内输入仪表盘名称的关键字，按回车键，执行查询，系统自动模糊查询出包含查询关键字的仪表盘。

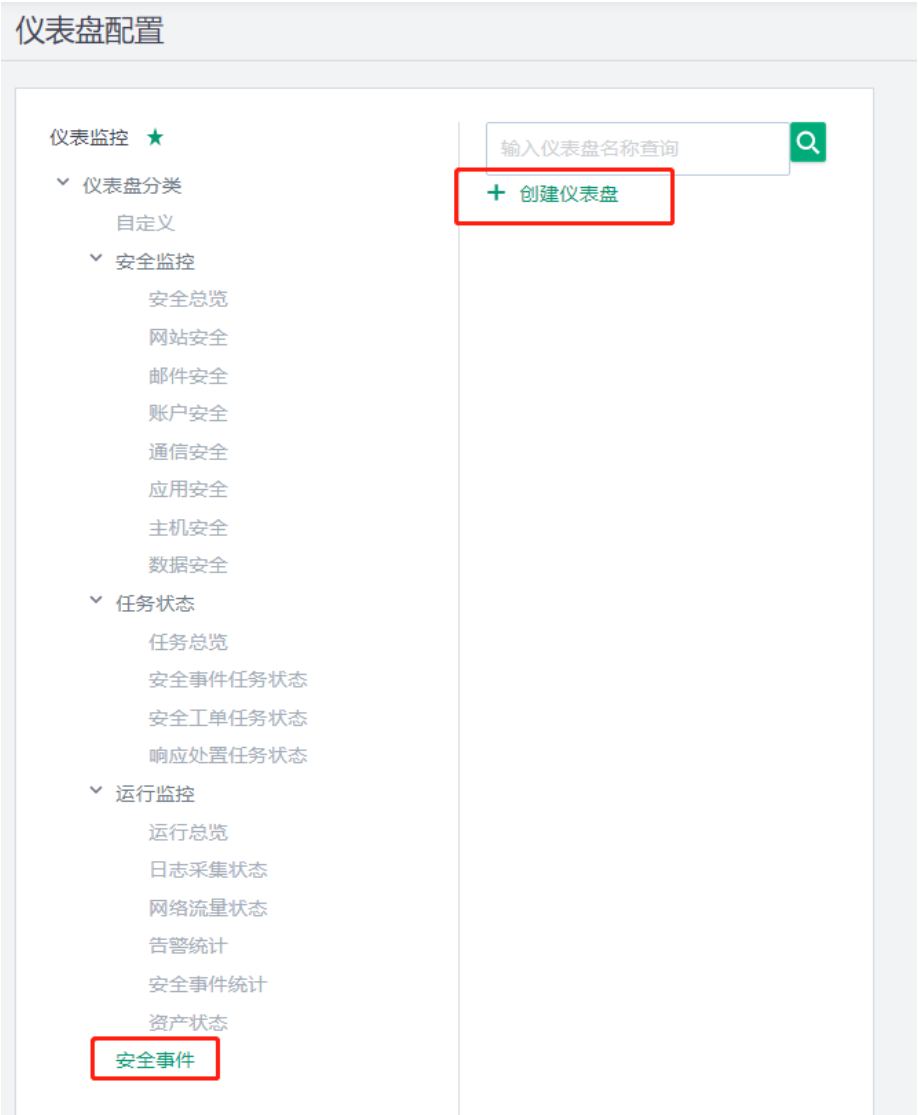
2.2.1.2创建仪表盘

您可以在已创建的仪表盘目录下创建仪表盘。

操作步骤

步骤1. 在“**仪表盘配置**”页面下，单击已创建的目录，如“**安全事件**”，在此目录下创建仪表盘。

步骤2. 单击“**创建仪表盘**”，创建仪表盘任务。



步骤3. 编辑仪表盘基本信息。

1. 单击时间“**今天**”，设置统计时间。

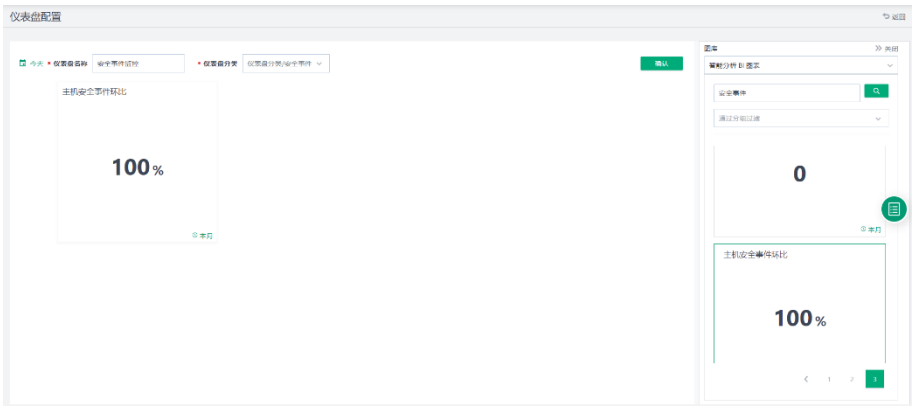
输入“**仪表盘名称**”，如“**安全事件监控**”。

（可选）选择仪表盘分类目录。

步骤4. 单击“**下一步**”，进入仪表盘编辑页面

步骤5. （可选）您可以在“**图库**”区域的输入框内输入标题关键字，模糊搜索所需的图表。

步骤6. 从图库中拖拽所需图表至左侧空白处。当鼠标放置在图表上呈现时，说明图表处于可移动的状态。

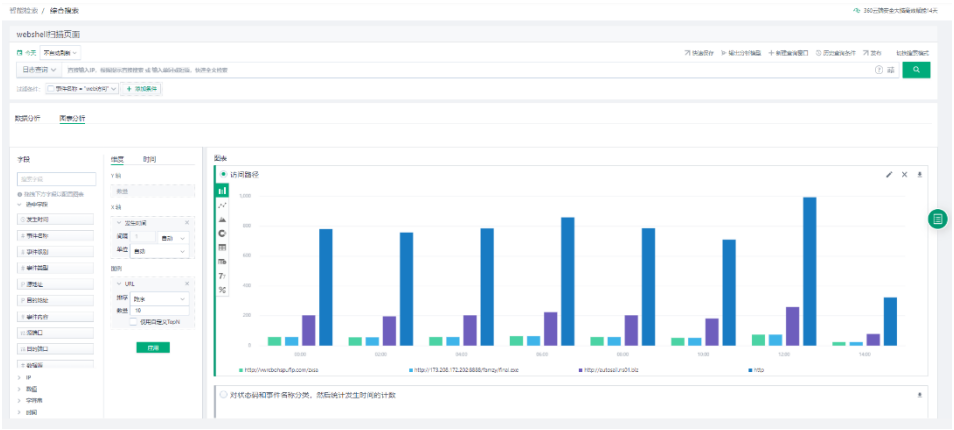


步骤7. 单击“**确认**”，成功创建该仪表盘，返回“**仪表盘配置**”页面

（可选）设置已选图表

将鼠标放置已选择的图表上，出现的操作图标支持以下操作：

- 单击，可设置下钻目标。
- 单击图表框右上角的，可打开一个新的网页，显示在“**智能检索**”下，如“**日志查询**”的图表分析。



- 单击，在此仪表盘编辑页面删除该图表。

仪表盘相关可选操作

- 单击仪表盘名前的 ☆ ，置亮后，可设置其为常用仪表盘，该仪表盘则会出现在菜单“**监控仪表分析**”中，具体可参见 2.2.1.4 设置常用仪表盘。
- 单击时间框可修改仪表盘显示数据的时间范围。
- 单击仪表盘展示区域的“**编辑**”，可打开仪表盘编辑页面，操作方式与创建过程保持一致。
- 单击仪表盘展示区域的“**删除**”，可删除该仪表盘。若该仪表盘设置为常用仪表盘后，则不可以删除。

2.2.1.3分享仪表盘

仪表盘的分享方式包括不分享、公开和指定用户。

注意事项

仪表盘设置为公开分享或者指定用户分享时，被分享用户能看到被分享的仪表盘，若是想要看到仪表盘中的图表，必须对其包含的图表设置可见的分享：被公开分享或者指定用户分享。

操作步骤

步骤1. “**仪表盘配置**”页面，选择一仪表盘，则右侧显示该仪表盘。

步骤2. 单击仪表盘右上方“**分享**”，弹出“**分享仪表盘**”的对话框。

*默认勾选“**分享此仪表盘下的所有图表**”：分享此仪表盘中所使用到的图表图例，图表图例在“**智能报表** > **图表管理**”中维护。*

*如若后续取消勾选，还需要在“**图表管理**”中取消相关图表图例的分享。*

步骤3. 选中“**不分享**”，并单击“**确认**”。

该仪表盘则仅本用户可见，其他用户不可见。

步骤4. 选中“**公开**”，并单击“**确认**”。

该仪表盘则是公开状态，所有用户均可见。

步骤5. 选中“**指定用户**”，弹出“**指定用户**”的对话框。

步骤6. 勾选“**可选列表**”中的用户，并单击添加，添加该用户至“**已选列表**”中。

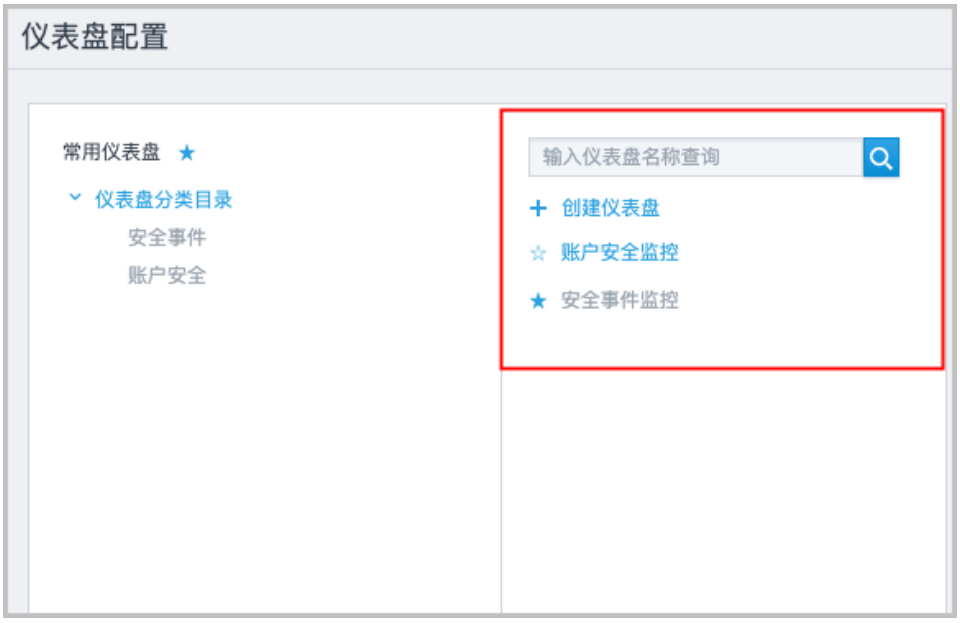
步骤7. 单击“**确认**”，则此仪表盘对以上用户可见。

2.2.1.4设置常用仪表盘

创建仪表盘后，您可以通过设置其为常用仪表盘，创建属于自己的仪表盘工作台。

操作步骤

步骤1. 选择“**仪表盘配置**”，显示“**仪表盘配置**”页面。



- ☆：仪表盘未设置为常用仪表盘。

- ★：仪表盘已设置为常用仪表盘，可在菜单“**常用仪表盘**”中可见。

步骤2. 单击五角星图表，可切换设置仪表盘是否为常用仪表盘。

步骤3. 设置常用仪表盘后，您可以在常用仪表盘下查看。

2.2.1.5切换全屏

您可以根据需要，设置仪表盘显示的形式。

操作步骤

步骤1. 单击仪表盘右上方“**全屏**”，可将仪表盘切换为全屏显示。

步骤2. 按 ESC 键或单击页面顶端区域，可退出全屏状态。

2.2.1.6设置筛选条件

为更好地展示仪表盘数据，您可以通过设置筛选条件，使仪表盘显示您所关注对象的数据。

操作步骤

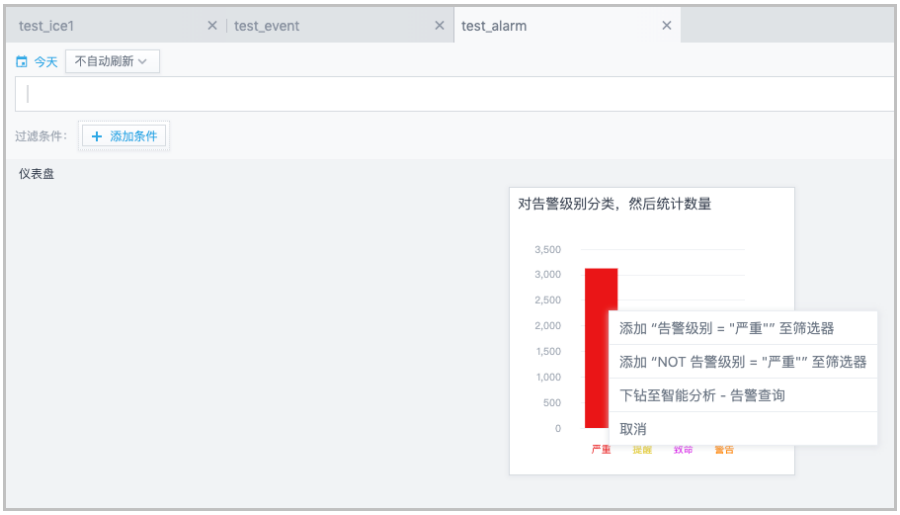
步骤1. 设置左上角的查询时间和刷新频率。

步骤2. 您可以通过 HQLite 过滤仪表盘中的图例数据。

HQLite 的检索能力与“**搜索分析**”保持一致，且支持引用“**安全信息**”中定义的 IP、数字、字符、时间组合对象。

步骤3. 添加图表信息至筛选器。

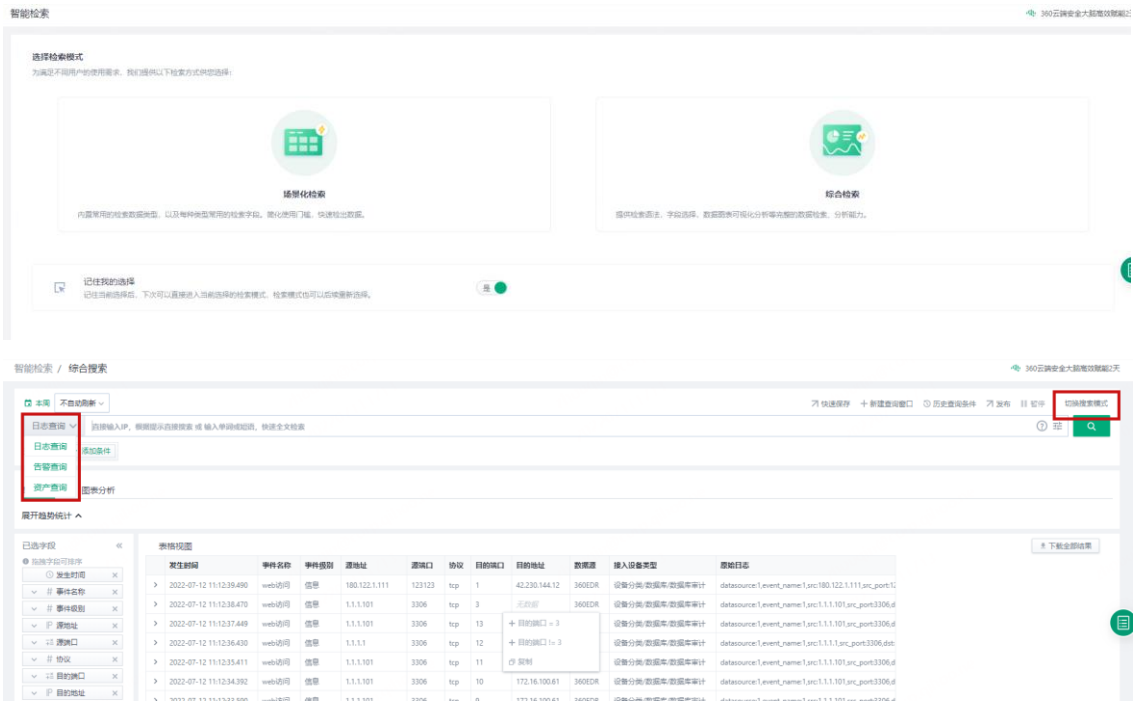
以仪表盘“test_alarm”为例，单击严重区域，弹出以下对话框。



单击“**添加“告警级别=“严重””至筛选器**”，并筛选相应数据显示图表。

3. 智能检索

接入的日志和经过 SAE 规则触发的告警在“**智能检索**”中展示，可以通过日志、告警进行分析溯源。该系统将所有的搜索菜单，以及各种不同的搜索方式（场景化检索、综合检索）统一到一个入口菜单。用户可以选择自己习惯的搜索方式并记住选择，方便以后直接进入。检索模式包括场景化检索和综合检索两种方式，您可以按需选择。记住当前选择，下次可以直接进入当前选择的检索模式，检索模式也可以后续重新选择

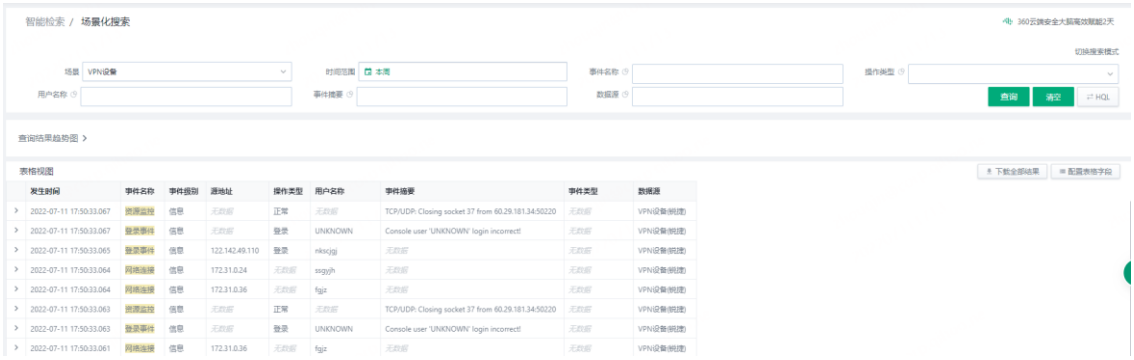


3.1 场景化检索模式

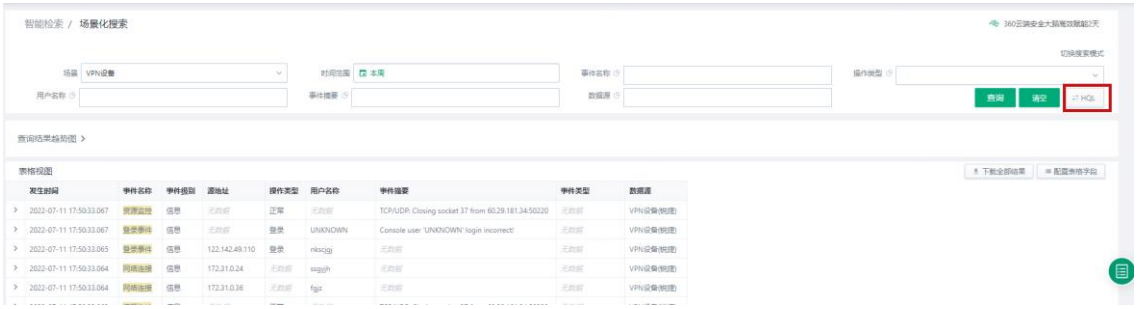
场景化检索方式是根据所选择场景，以及相应的场景化字段，展示相应场景的搜索结果。场景分析中的具体场景及对应的查询字段均已内置。

场景化检索

场景搜索示例如下。以“**VPN 设备**”场景为例，显示以下对应的“**查询字段**”。以此根据选择的场景，配置相应参数来查询告警。



选择“HQL”切换为 HQLite 模式，灵活配置查询参数



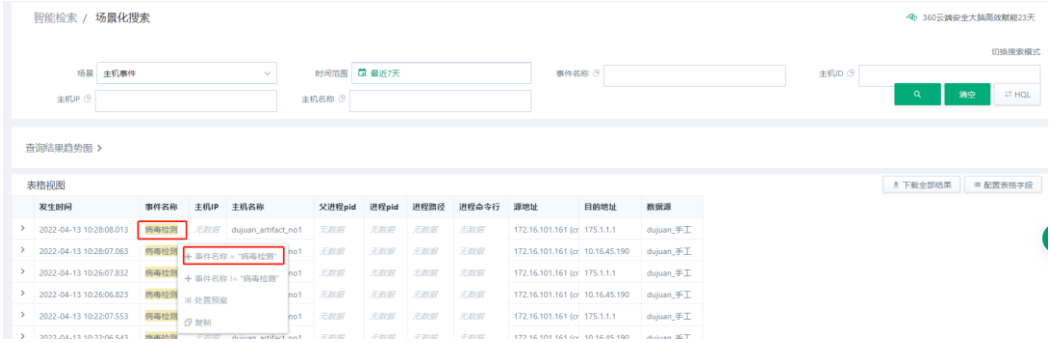
单击“搜索模式”，可切换为 HQLite 模式，灵活配置查询参数。

单击输入框末打开在线帮助进行参考。

添加筛选条件

在查看表格视图下的日志信息时，可直接添加信息内容为筛选条件，以此过滤查看内容。

如操作过程中，想查看事件名称为“病毒检测”的日志。可单击“病毒检测”，在弹出的窗格中单击“**+事件名称 = "病毒检测"**”。



添加“**事件名称 = "病毒检测"**”为筛选条件，显示如下。

3.2 综合检索模式

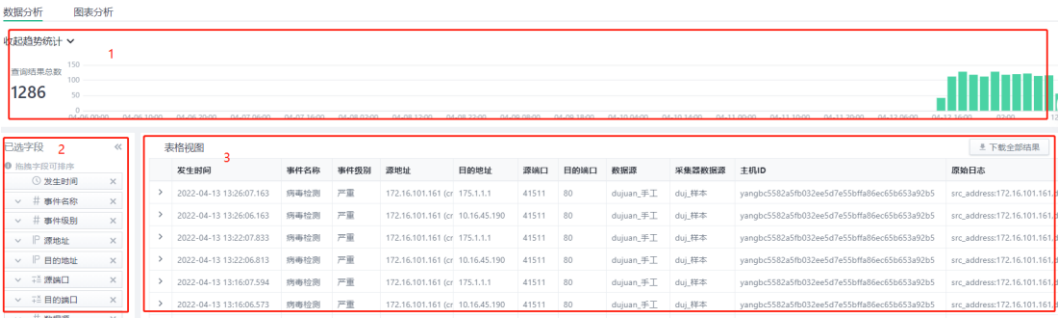
LAS 系统将所有的搜索菜单，日志/告警/资产统一到一个入口查询

3.2.1 表格视图功能

3.2.1.1界面简介

表格视图

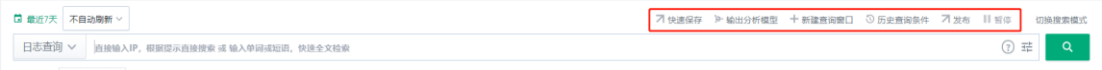
以“**日志查询**”为例，介绍数据分析区的页面。



区域	说明
1	默认是收起状态，单击“**展开趋势统计**”方可展开，展示当前设置条件下的数据总量和趋势柱状图。
2	设置字段属性区域。
3	当前设置条件下，日志事件以列表的形式展示。

通过设置查询时间、过滤条件，对搜索出的日志进行数据分析，主要通过数据总量、趋势图和表格视图展示。

更多功能区



工具栏	说明
快速保存	快速保存功能用于将查询条件和设置的图表快速发布至“**历史查询条件**”中，达到保存结果即视的效果。
新建查询窗口	在已设置查询条件的分析页面上新建一个新的分析页面。
历史查询条件	打开历史保存的查询条件进行日志查询和分析。
发布	将查询条件和设置的图表发布至“**历史查询**”中。
暂停	在“**日志查询**”过程中，可通过单击“**暂停**”，停止搜索。
切换搜索模式	切换场景检索模式或者综合检索模式。

3.2.1.2数据分析

3.2.1.2.1数据分析趋势图

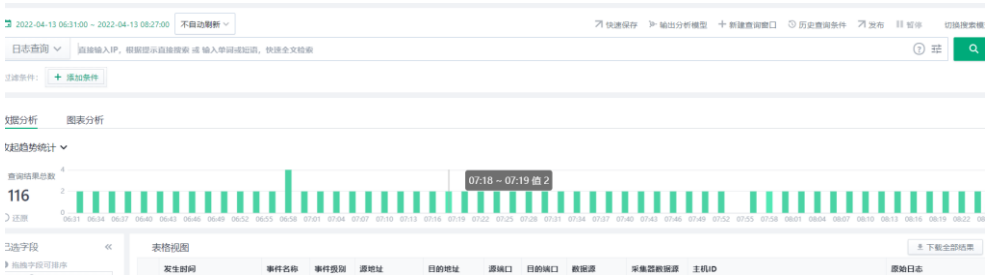
以时间为横轴、发生事件的数量为纵轴，展示符合查询关键字和查询时间窗的事件趋势图。

操作步骤

步骤1. 当鼠标悬停在趋势图上时（鼠标会变为十字箭头），可以对趋势图中的数据按时间段进行过滤。

数据总量下方的 还原 用来还原。

步骤2. 当鼠标悬停在趋势图上存在数据的时间横轴上方时，会出现对应时间下发生的事件数量和对应的统计时间窗。



3.2.1.3设置列表字段

在设置字段区域，您可以选择字段筛选器的排序、右侧列表中显示字段的排序和显示。

字段筛选器的隐藏/展开

- 单击已选字段右侧的，可隐藏字段筛选器。

- 隐藏后，单击“**关键字段筛选**”可恢复字段筛选器的显示。

字段筛选器排序

字段值在所有日志中的占比默认以降序的排序方式显示。可切换为升序的排序方式。

列表字段排序

通过拖拽“**已选字段**”中的字段框，可调整右侧“**表格视图**”中字段显示的顺序。

如，拖拽“**事件名称**”至“**事件级别**”下方，则“**表格视图**”中“**事件级别**”列会出现在“**事件名称**”之前。

选择显示字段

- 通过单击“**已选字段**”后的×，可删除其在“**表格视图**”中的显示。
- 通过单击“**未选字段**”后的+，可添加其在“**表格视图**”中的显示。

查询未选字段

未选字段列可以进行拼音/中文/英文的模糊查询。

锁定列表字段

您可以通过单击表头的字段名，锁定该列。该列成为第一列展示。

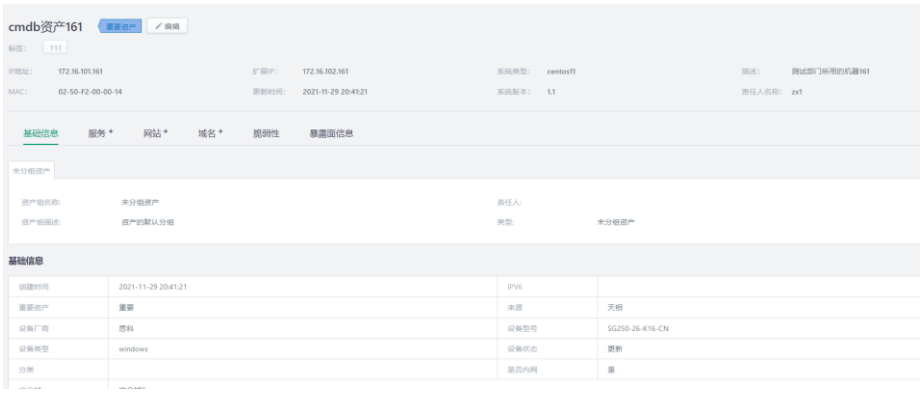
- 支持锁定多个列，依次排序。
- 锁定状态的字段不可拖拽。

3.2.1.4查询日志详情

操作步骤

步骤1. 在“**表格视图**”中，单击某一条日志数据前的 ›，可显示日志的详细信息。

步骤2. 以源地址“172.16.101.161”为例，此为内部资产，单击之，可打开新的页面，显示该资产的风险分析详情页面。



步骤3. “**设备地址**”亦为内部资产，单击之，可打开新的页面，显示该资产的风险分析详情页面。

步骤4. 当“**目的地址**”为外部 IP，单击之，可打开新的页面，显示该 IP 的威胁情报页面。

步骤5. 单击“**域名**”参数值，可打开新的页面，显示该域名的威胁情报页面。

3.2.1.5字段内容的更多功能

复制字段内容

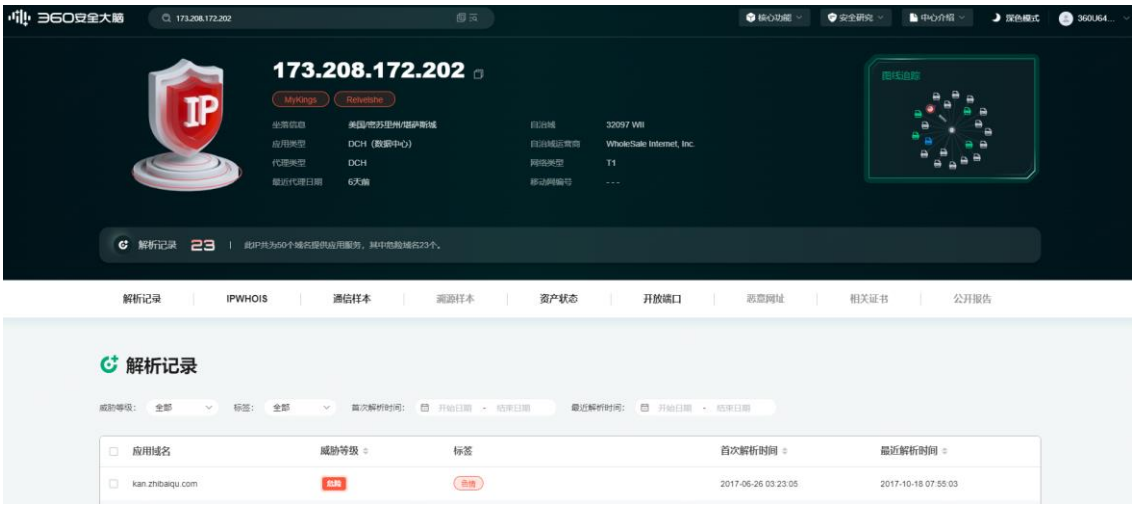
您可以通过复制“**数据分析**”列表中的字段内容。如当您需要将“**原始日志**”复制另存以供分析时，您可执行如下操作。

步骤1. 选择某条日志数据，单击“**原始日志**”列中的内容。弹出提示框。

步骤2.　单击“**复制**”，即可复制原始日志的全部内容。

IP 类字段的跳转

- 若是外网 IP，单击“**打开威胁情报**”，跳转到 360 威胁情报详情页面。



- 若是资产 IP，单击打开“**资产详情**”，则会跳转资产详情页面。

3.2.1.6解码功能

在分析过程中，如遇 BASE64、HEX、URL 或是 JSON 格式的编码，支持在线解码，无需使用其他工具，实现常见编码和解码转换功能，提高分析效率。

3.3 更多关联操作

3.3.1 发布查询条件和图表

发布功能用来保存编辑过的查询条件、列表展示、配置的图表。您可以将查询条件和设置的图表发布至“**历史查询条件**”中。

前提条件

您已使用 HQLite 或过滤条件设置查询条件，并使用图表分析日志。

操作步骤

步骤1. 单击“**发布**”，弹出“**发布**”对话框。

步骤2. 输入“**名称**”、选择“**分组**”，勾选“**历史**”和“**图库**”。

*若未做图表分析，则无法在此处勾选“**图库**”。*

步骤3. 单击“**发布**”，可将该查询条件保存至“**历史查询条件**”中，设置的图表保存至“**报表中心 > 图表管理**”中。

更多操作

编辑已发布过的历史查询，可以选择发布模式：更新/另存为。

3.3.2 管理历史查询条件

您可以通过打开历史保存的查询条件进行日志查询和分析。

操作步

步骤1. 单击查询 HQLite 搜索右上方的“**历史查询**”。

步骤2. 单击条件“**操作**”列的▶，打开该查询条件，数据分析页面显示查询结果。

步骤3. （可选）单击条件“**操作**”列的🗑，可删除该条历史条件。

3.4 数据分类和关联查询

3.4.1 查询

本章节以日志查询为例，介绍基本操作。

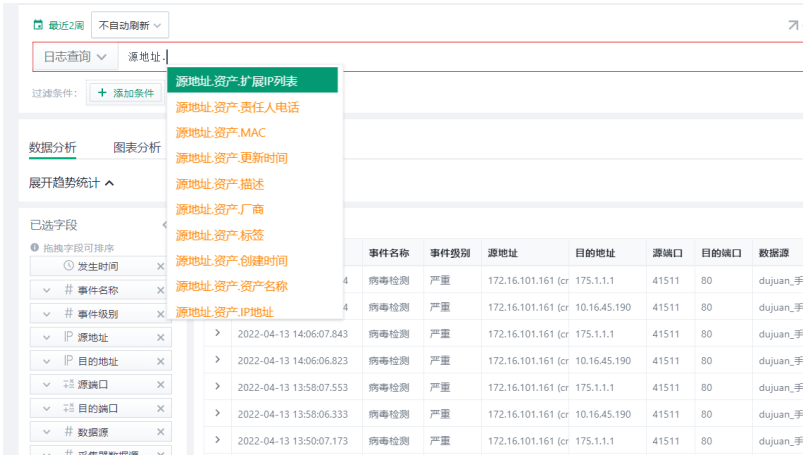
在“**日志查询**”中，您可以编辑 HQLite 查询条件和过滤条件查询相关的日志内容，以供进一步的安全分析。

前提条件

您已接入日志。

背景信息

在日志查询功能里，新增“**关联分析属性**”的字段，使“**源地址**”、“**目的地址**”与**资产、脆弱性**数据相关联，从而查询符合相应条件的日志。以“**源地址**”为例，如图：



3.5 可视化分析

专家模式时支持根据查询条件创建图表，同时满足将查询条件保存并发布与设定周期自动刷新，支持选择查询条件和/或 BI 图例一起保存和发布。

3.5.1 配置流程说明

在专家模式下，根据查询条件和结果来配置图表的流程及说明如下：

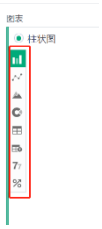
1. **查询数据**：在“**综合分析**”模式下查询日志或者告警等数据生成查询结果。
2. **添加并选择图表类型**：切换至“**图表分析**”，添加图表并选择图表类型，对日志、告警、事件等进行可视化分析。
3. **配置图表**：从左侧列表拖拽字段进入相应维度。

3.5.2 配置界面简介

在“**数据分析**”区域框中完成相应分析后，可单击“**图表分析**”，切换至“**图表分析**”区域框，使用各类图表对日志、告警、事件等进行可视化分析。

选择添加图标

再选择图表样式



再选择应用，即可生成图表

说明如下：

区域	说明
1	字段选择区，可通过拖拽的方式设置维度。

区域	说明
2	设置维度的属性；可切换设置时间属性。 需单击“**应用**”后，方可生效。
3	图表设置区和展示区。 • 初始状态为空，需手动“**添加图表**”，方可出现此区域。 • 可添加多个图表，满足图表丰富化的需求。
3-1	选择设置不同图表的类型。
3-2	•  ：编辑图表的描述。 •  ：删除该图表。 •  ：下载的是图表显示的数据内容。

4. 资产管理

LAS 系统中，资产仅支持一种数据录入方式：日志审计系统页面导入/导出；

4.1 资产列表

在导航栏选择菜单“**资产管理** > **资产列表**”。展示页面如下：

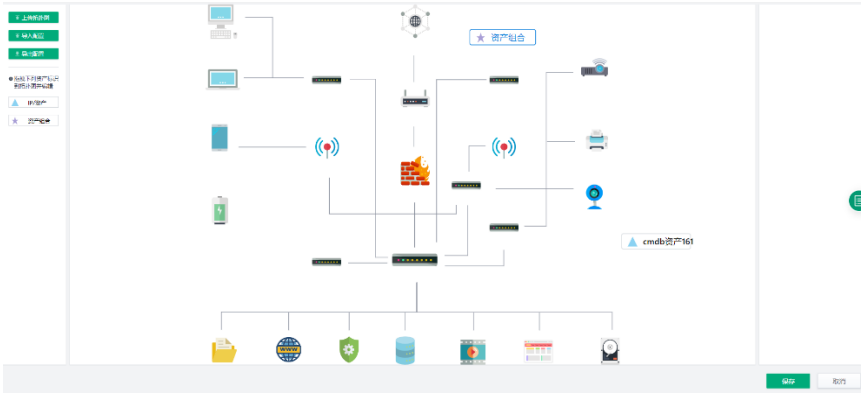
4.2 配置资产拓扑图

操作步骤

步骤1. 在导航栏选择菜单“**资产管理** > **资产拓扑**”。LAS 系统显示“**编辑资产拓扑图**”的页面。

步骤2. 上传资产拓扑图。

1. 单击左侧导航栏“**上传拓扑图**”，可从本地导入拓扑图。

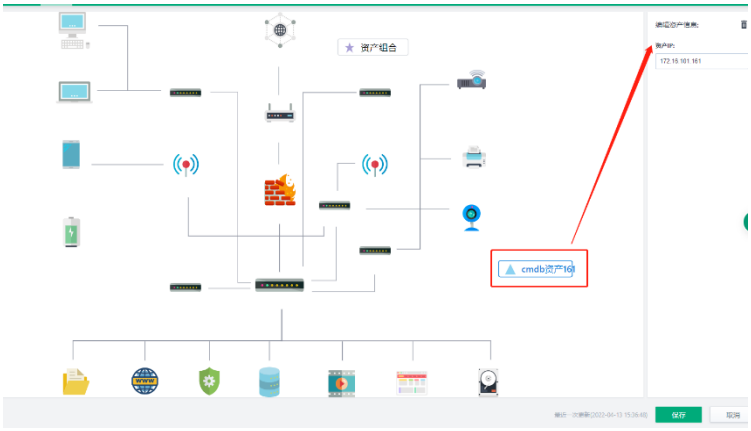


单击“**保存**”。

步骤3. 编辑资产信息。

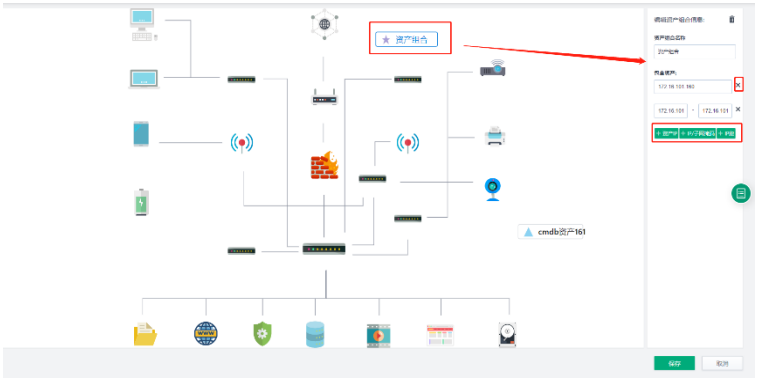
拖拽资产标识（两种类型资产信息）到右侧拓扑图中，并单击该资产图标配置资产信息。

1. 单击资产图标设置资产 IP。



单击资产组合图标，在右侧弹出的信息框中配置多个资产信息。

- 单击“+资产 IP”弹出新的输入框，输入 IP。
- 单击“+IP/子网掩码”弹出新的输入框，输入 IP 及掩码。
- 单击“+IP 段”弹出输入框，输入 IP 地址的网段范围。
- 单击已设置的内容右侧✕，可删除此配置。



（可选）单击编辑右上方的🗑，可删除此资产标识。

单击“**保存**”。

更多操作

- 您可以通过单击“**导出配置**”，将已配置的资产拓扑图导出，以做备份。LAS 系统自动生成拓扑配置文件“topology_config.json”。
- 您可以通过单击“**导入配置**”，将本地的配置文件导入。

5. 报表中心

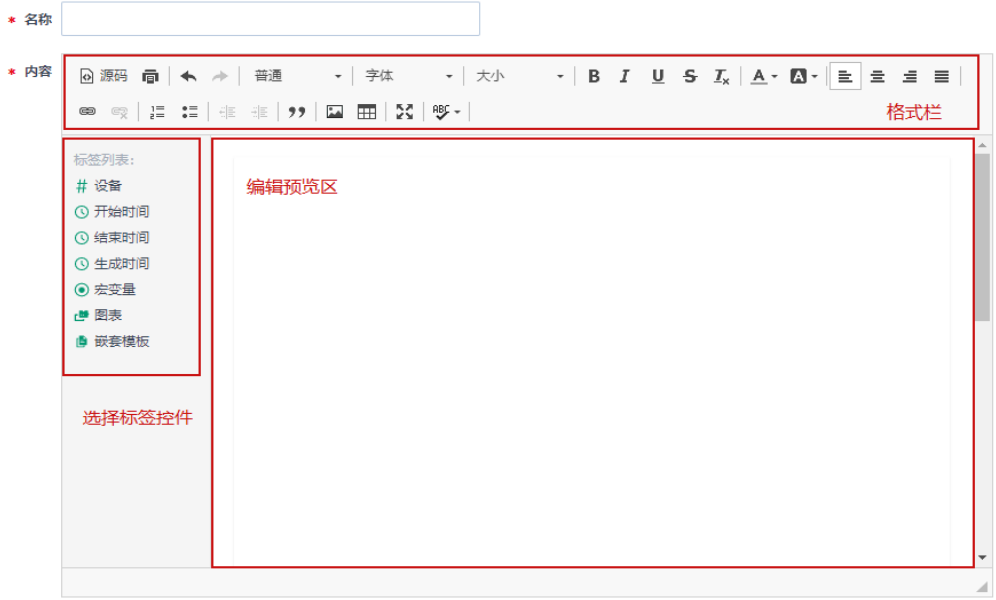
5.1 报表模板

系统当前内置了多个报表模板，包括：PPT 模板和综合报表等，并允许用户自定义报表模板，供定时报表使用。您可以新增、修改、分享或删除报表模板。

操作步骤

步骤1. 选择“**报表中心 > 报告设置 > 模板管理**”，LAS 系统显示“**报表模板**”页面。

步骤2. 单击“**新建**”，LAS 系统显示报表模板编辑页面。

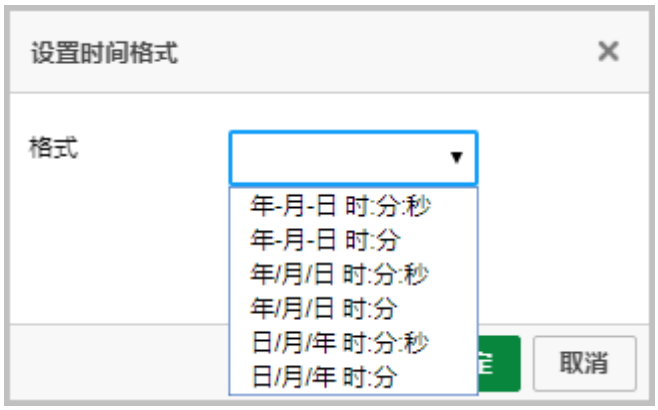


步骤3. 输入报表模板“**名称**”，自定义编辑“**内容**”，可执行以下操作：

- 在格式栏中设置内容的格式，控件自带功能：插入图片、表格，调整一些排版等。
- 标签列表为报表模板的核心内容控件，通过标签的选用和编辑来生成的报表模板内容，标签类型如下：

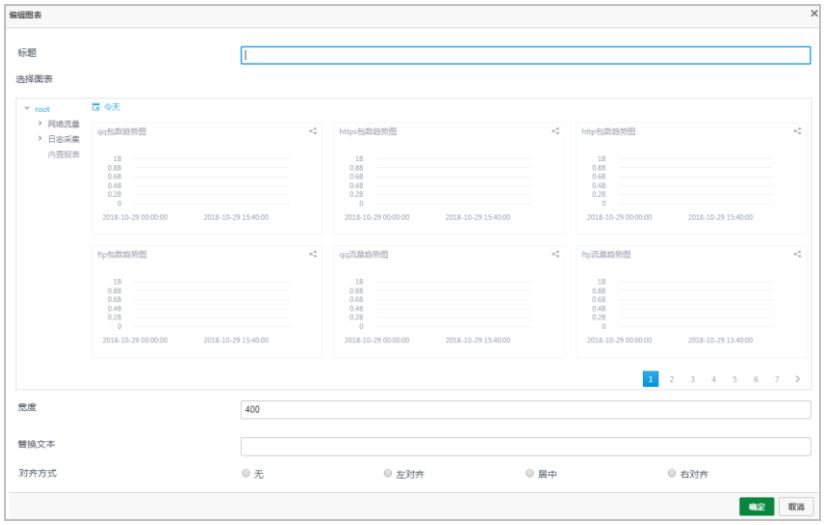
– 设备：显示产生事件和告警的数据源 IP 和采集类型，最多支持显示 5 个数据源。

– 时间：包括“**开始时间**”、“**结束时间**”、“**生成时间**”是同样的时间标签，选择标签的中的时间格式。



- 宏变量：支持宏变量输出统计值，可添加统计、环比类的图表。

- 图表：选择图表库里的任一图表展示在报表里。配置图表的标题、图表展示内容、宽度、替换文本和对齐方式。



- 嵌套模板：选择嵌套模板的类型包括“**告警事件分析**”和“**日志总量分析**”两种。

步骤4. 设置标签内容后，单击“**确定**”，返回报表模板编辑页面，并单击“**保存**”。

该报表模板可在列表中显示。

更多操作

操作	说明
编辑	您可以通过单击报表模板操作列的**编辑**，支持修改“**名称**”和“**内容**”。
删除	• 您可以通过单击报表模板操作列的**删除**，删除该条报表模板。 • 当报表模板中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查看	内置的报表模板只允许查看，操作栏点击**查看**，可查看该报表模板的内容

5.2 报告任务

定时报告任务可以统计即时、一段时间内（前一天、前一周或前一月）的日志事件和告警，可生成 html 文件、word 文件和 ppt 文件，支持用户在线查看，也支持通过邮件的方式发送 word 文件到指定邮箱。系统报表存在定时清理机制，默认每种定时报表只保留最近 50 份。

操作步骤

步骤1. 选择“**报表中心 > 报告设置 > 报告任务**”，LAS 系统显示报告任务的页面。

步骤2. 单击“**新建**”，弹出“**报告任务**”的配置界面。

步骤3. 输入“**报表名称**”，选择“**类型**”。

步骤4. 填写即时报表配置参数。

参数名称	参数说明
报表名称	报表的名称。允许输入 1~64 个字符。

参数名称	参数说明
类型	生成的定时报表反映的时间段。单击可出现下拉框，可以选择即时、日报、周报、月报。 • 即时统计分析范围可为任意时间，用户可根据需求自行配置。 • 日报统计分析范围为设置当天的 00:00 到第二天的 00:00。 • 周报统计分析范围为本周第一天的 00:00 到下周第一天的 00:00。 • 月报统计分析范围为当月第一天的 00:00 到下个月第一天的 00:00。
邮件通知	选择是否将此定时报表的情况通过邮件将 word 报告通知用户。若选择“**是**”，界面此处引用邮件通知对象，可同时配置多个通知对象。
通知对象	当通知选择“**是**”时，需要配置通知对象。 发件人在“**系统管理 > 基础配置 > 通知管理 > SMTP 配置**”中配置，可修改 SMTP 服务器地址、端口、SMTP 用户名（发件人用户名）、密码（发件人密码）。具体请参见 14.2 通知管理。
报表内容	定时报表生成时，引用的通知对象，若配置邮件通知，输出报表内容附件；若配置短信和命令行，输出报表邮件的标题。 此处选择报表模板，默认只包含一个报表模板。
启用	选择是否启用此定时报表。

步骤5. 配置完成后，单击“**确认**”，提示“**报表添加成功**”。

更多操作

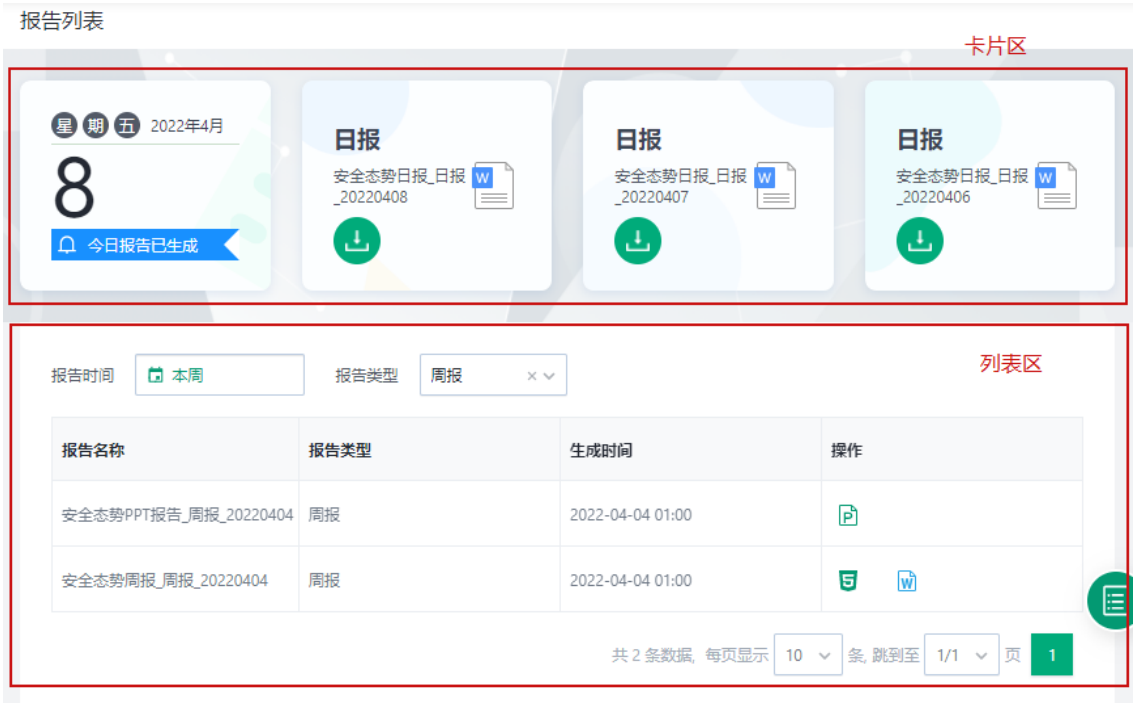
操作	说明
编辑	您可以通过单击报表任务操作列的**编辑**，支持修改报表任务的参数。
删除	• 您可以通过单击报表任务操作列的**删除**，删除该条报表任务。 • 当报表任务中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。（内置任务不允许删除）
执行	您可以通过单击报表任务操作列的**执行**，立即执行以生成报表。

5.3 报告列表

报告列表页面，可以在线查看或下载系统产生的各种报告。

5.3.1 功能概览

单击“**报表中心** > **报告列表**”，进入报告列表页面，页面显示如下。



区域	说明	
卡片区	卡片区	通过 4 张卡片展示系统报告的生成情况。包括： • 第 1 张卡片展示当前日期和今日报告的生成状态。 • 另 3 张卡片展示最近生成的 3 个报告，点击下载按钮可下载报告。
列表区	筛选器	提供两个条件供客户筛选报告：**报告时间**和**报告类型**。缺省设置为：报告时间=“今天”；报告类型=“全部”。

区域	说明	
	报告列表	报告列表区展示系统已产生的各种报告，包含以下信息: • **报告名称**：各报告的实际名称。 • 报告类型：报告所属的类型，包括：即时、日报、周报和月报。 • **生成时间**：该报告产生的具体时间。 • **操作**：点击查看图标，用户可以查看或下载各种格式的报告文件。 ➢ 单击  ，弹出新窗口展示 html 格式的报表。 ➢ 单击  ，可下载以 word 格式生成的报表至本地。 ➢ 单击  ，可下载以 ppt 格式生成的报表至本地。

***PPT 类型的智能报告**，当前选择 PPT 模板才能够产生，其他内置或自定义报告只能生成 html 或 word 格式的报告。*

5.4 图表管理

图表管理功能，用于添加存储“**智能检索**”中使用图表分析设置并发布的图表数据，提供可视化展示结果。您可以对图表库资源进行查看、编辑或删除。同时您可以基于分组查找相应的图表集合。

5.4.1 配置图库分组

图库分组可便于将各图表归类存放。

操作步骤

步骤1. 在导航栏选择菜单“**报表中心 > 图表管理**”，LAS 系统进入“**图表管理**”页面。

步骤2. 单击左侧分组根节点“**root**”后的  ，弹出“**在 root 下添加新的分组**”对话框。

步骤3. 填写相关参数，参数说明如**错误!未找到引用源。**所示。

表5-1 配置图库分类参数

参数名称	参数解释
分组名称	输入分组的名称信息，允许输入 1~64 个字符。
分组描述	输入分组的描述信息，允许输入 1~256 个字符。

步骤4. 单击“**确定**”，完成图库分组的添加。

更多操作

操作	说明
修改	您可以通过单击图库分组节点后的，修改分组的参数。
删除	您可以通过单击图库分组节点后的，删除该分组及对应下的图表。 *不支持删除根节点 root。*

5.4.2 添加图表

单击“添加”，可跳转至“智能检索”下的图表分析界面，在此功能页面下创建图表。

5.4.3 管理图表

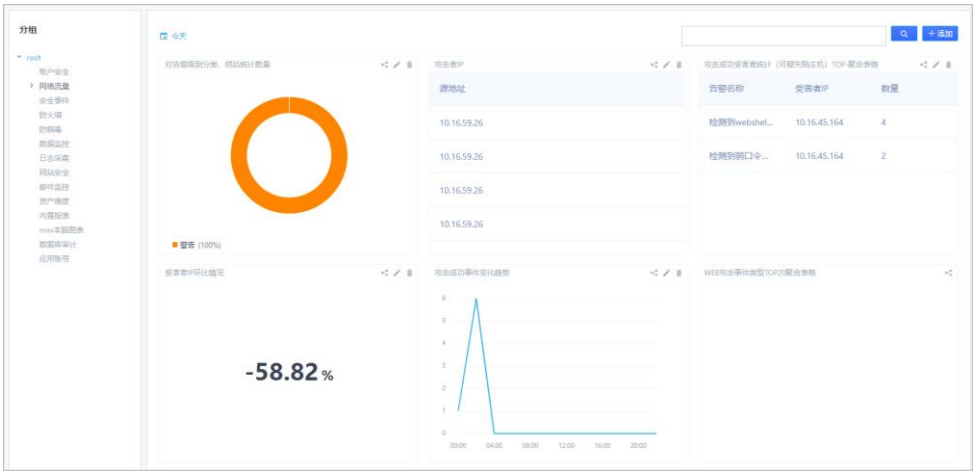
您可以分享、编辑或删除图表。

前提条件

您已经在分析数据时，创建多个类型的 BI 图表并发布至“**图库**”中。

操作步骤

步骤1. 在导航栏选择菜单“**报表中心 > 图表管理**”，LAS 系统进入“**图表管理**”页面。



步骤2. 单击图表右上角的，分享自定义图表。

- 选择“**不分享**”，并单击“**确认**”，则该图表仅自己可见。
- 选择“**公开**”，并单击“**确认**”，则该图表对所有用户可见。
- 选择“**指定用户**”，在“**可选列表**”中的用户添加至“**已选列表**”中，并单击“**确认**”。

步骤3. 单击一图表右上角的，可进入相应的“**搜索分析**”页面，您可以进行编辑修改，更新或另存该图表。

步骤4. 单击一图表右上角的，可删除此图表。

6. 等保助手

等保助手主要包括等保管理和等保知识库两大模块。等保管理主要针对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与报告查询；等保知识库可对内外部法律/部制度等文档进行归档与查看，最大程度发挥安全措施的保护能力。

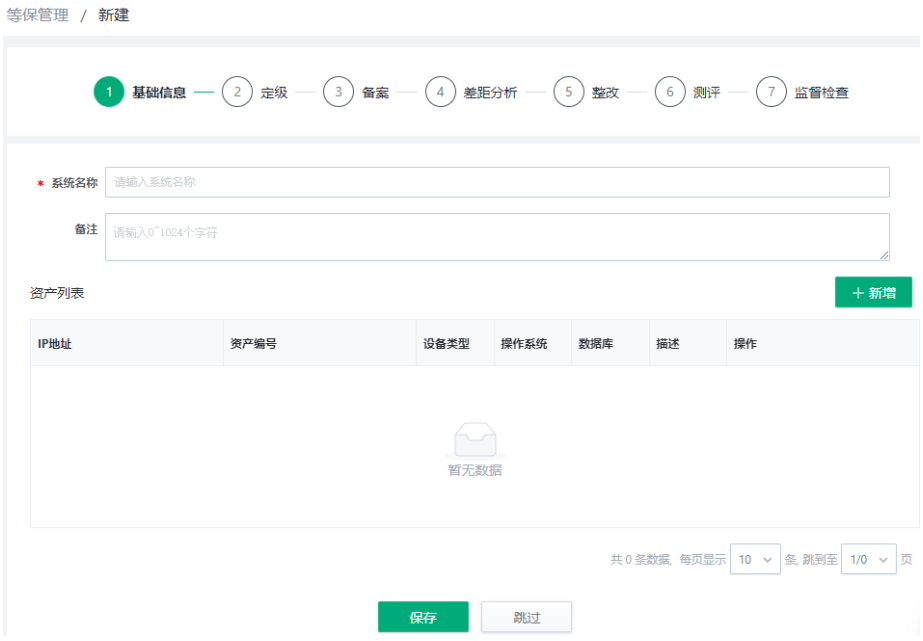
6.1 等保管理

在等保管理页面点击新建，管理员可以创建新的等保信息条目。

操作步骤

步骤1. 选择“**等保助手** > **等保管理**”，进入“**等保管理**”列表页面

步骤2. 单击“**新建**”，打开“**新建等保管理**”页面。



分 7 个阶段创建等保信息，各阶段说明如下：

阶段	说明
基础信息	包括系统名称及对应资产信息
定级	可对系统进行定级、定级报告与专家评审意见的导入

阶段	说明
备案	可进行备案表/备案证明报告的导入
差距分析	可进行高风险项新增、差距分析报告的导入
整改	可进行整改报告的导入
测评	可进行测评结论、分数与高风险项的编辑，测评报告的导入
监督检查	可进行自查报告的导入

步骤1. 输入信息后点击“**保存**”，可回到“**等保管理**”列表页面，可以查看系统中已录入的各等保系统信息。

更多操作

操作	说明
编辑	等保管理列表，单击某个系统操作列的**编辑**，用户可以在弹出的窗口中修改该等保系统各阶段的文档信息。
删除	等保管理列表，单击某个系统操作列的**删除**，删除该等保系统。

6.2 等保知识库

在等保知识库页面，管理员可对内/外部法律，内/外部制度等文档进行归档与查看，主要查看内容包括文档年份、文档类型、文档名称等。

操作步骤

步骤1. 选择“**等保助手** > **等保知识库**”，进入“**等保知识库**”页面

步骤2. 单击“**新建**”，打开“**新建知识库**”页面，进行文档条目的创建与上传，新增页面如下图所示。

参数说明如下。

参数	说明
年份	在下拉列表中选择创建的项目名称。
文档类型	设置该任务的优先级，包括选项：高中低。 责任人接收到任务后，会根据任务的优先级处置。
导入报告	在下拉列表中选择 LAS 系统的内部用户。
备注	设置该任务的到期日，如若内部责任人逾期为处理，则会再次接收到通知中心的实战任务消息推送，外部责任人无法接收。

步骤3. 单击“**保存**”，完成该等保知识库的创建，返回到“**等保知识库**”列表页面，可查看该知识库文档是否已经创建成功。

更多操作

操作	说明
编辑	您可以通过单击报表任务操作列的**编辑**，支持修改报表任务的参数。
删除	• 您可以通过单击报表任务操作列的**删除**，删除该条报表任务。 • 当报表任务中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。（内置任务不允许删除）

7. 管理知识/案例库

7.1 管理知识库

知识库维护当前系统中的知识，支持对知识分类的新增、修改、删除；支持对知识信息的新增、修改、删除，根据标题查询。

7.1.1 配置知识分类

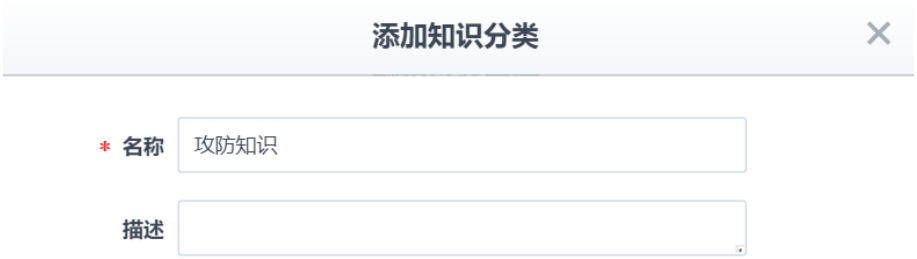
知识分类是对各类知识的分类，在界面左侧显示。默认存在“处置建议”这一知识分类，当需要新增一个知识，原知识分类树中没有其所属分类，则需先创建一个新的知识分类。

操作步骤

步骤1. 选择“**知识管理 > 知识库**”，LAS 系统进入“**知识库**”页面。

步骤2. 单击左侧“**知识分类**”中的“**管理**”，弹出“**编辑过滤条件**”的对话框。

步骤3. 将鼠标悬停在左侧知识分类的一类时，会出现 ，单击之，弹出“**添加知识分类**”对话框。



步骤4. 填写相关参数。

表7-1 配置知识分类参数

参数名称	参数解释
名称	输入知识分类名称信息，允许输入 1~64 个字符。
描述	输入知识分类描述信息，允许输入 1~256 个字符。

步骤5. 单击“**保存**”，完成知识分类添加。

更多操作

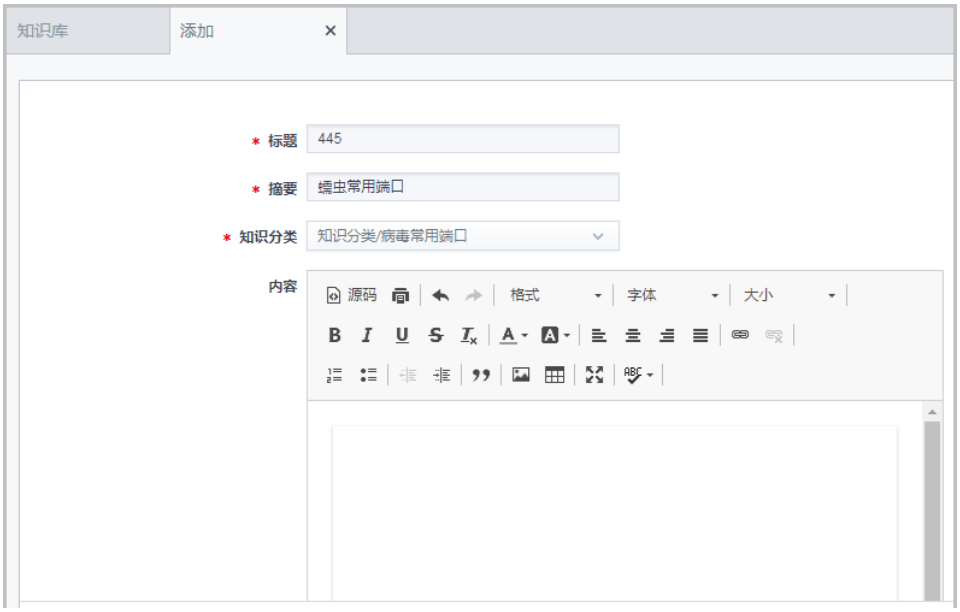
操作	说明
修改	您可以通过单击知识分类树节点后的，修改知识分类的参数。
删除	您可以通过单击知识分类树节点后的，删除该条知识分类树、子树及对应知识信息。 • *不支持修改、删除根节点。* • *删除知识分类时，会弹出提示框，请确认是否删除知识分类下的知识信息，再行删除。*

7.1.2 配置知识

当知识库中的知识内容发生新增、变更，您可以对知识数据进行新增、修改及删除的操作。

操作步骤

步骤1. 单击知识列表页面右侧的“**新建**”，界面展示知识添加页面。



步骤2. 填写相关参数。

表7-2 配置知识参数

参数名称	参数说明
标题	知识标题，允许输入 1~64 个字符。
摘要	知识摘要，允许输入 1~64 个字符。
知识分类	选择当前知识对应的知识分类（知识分类树，仅可单选）。
内容	录入知识具体内容，支持内容格式自定义。
附件	支持附件上传。附件大小不超过 24M。

步骤3. 单击“**确定**”，完成知识新增操作。

更多操作

操作	说明
修改	您可以通过单击知识列表操作列的，支持修改“**标题**”、“**摘要**”、“**内容**”、“**附件**”的修改，不支持修改“**知识分类**”。
删除	• 您可以通过单击知识列表操作列的，删除该条知识数据。 • 当知识列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入知识的“**标题**”，按回车键，执行查询，系统自动模糊查询出知识名称包含查询关键字的知识信息，以列表方式展示。
按创建时间排序	单击创建时间右侧的图标，可切换排序方式。

7.2 管理案例库

案例库维护当前系统中的案例集合，支持对案例分类的新增、修改、删除；案例信息的新增、修改、删除、查询。

7.2.1 配置案例分类

案例分类是对各类案例总结的分类，在界面左侧显示。默认只有案例分类的根目录，可以根据实际案例情况新增、修改、删除案例分类

操作步骤

步骤1. 选择“**知识管理 >案例库**”，LAS 系统进入“**案例库**”页面。

步骤2. 单击左侧“**案例分类**”中的“**管理**”，弹出“**编辑过滤条件**”的对话框。

步骤3. 将鼠标悬停在左侧知识分类的一类时，会出现 ，单击之，弹出“**添加案例分类**”对话框。

步骤4. 填写相关参数。

表7-3 配置案例库分类参数

参数名称	参数解释
名称	输入案例分类名称信息，允许输入 1~64 个字符。
描述	输入案例分类描述信息，允许输入 1~256 个字符。

步骤5. 单击“**保存**”，完成案例分类添加。

更多操作

操作	说明
修改	您可以通过单击案例分类树节点后的 ，修改案例分类的参数，支持修改“**名称**”和“**描述**”信息。
删除	您可以通过单击案例分类树节点后的 ，删除该条案例分类树、子树及对应案例信息。 • *不支持修改、删除根节点。* • *删除案例分类时，会弹出提示框，请确认是否删除案例分类下的案例信息，再行删除。*

7.2.2 配置案例

除了通过安全事件添加的案例，您还可以通过手动新增、变更，对案例信息进行新增、修改及删除案例库中的案例。

操作步骤

步骤1. 单击案例列表页面右侧的“**新建**”，界面显示案例添加对话框如下所示。

步骤2. 填写相关参数。

表7-4 配置案例库参数

参数名称	参数说明
名称	案例名称，允许输入 1~64 个字符。
案例分类	选择案例分类（案例分类树，仅可单选）。
描述	填写案例描述信息，运行 1~255 个字符。
影响范围	录入案例的影响范围。
解决办法	录入案例的解决办法。
附件	支持附件上传。

步骤3. 单击“**确定**”，完成案例新增操作。

更多操作

操作	说明
修改	您可以通过单击案例列表操作列的，支持修改“**名称**”、“**描述**”、“**影响范围**”、“**解决方法**”和“**附件**”的修改，不支持修改“**案例分类**”。
删除	• 您可以通过单击案例列表操作列的，删除该条案例数据。 • 当案例列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入案例的“**名称**”，按回车键，执行查询，系统自动模糊查询出案例名称包含查询关键字的案例信息，以列表方式展示。

8. 配置数据接入

在导入内容包后，初始化了解析规则，用于解析接入的终端日志、流量日志等。

当需要接入第三方传统安全设备时，可以参照此章节接入第三方数据源、以及配置能够解析该类设备日志的解析规则等。

8.1 数据存储管理

除了默认的数据存储，您可以配置其他不同类型数据存储。

默认数据存储为：

- ClickHouse 存储：接收探针日志并持久化至 ClickHouse，供查询、展示和数据分析使用。
- Enterprise-SAE-KAFKA：日志对接，输出到默认的 topic，供关联分析规则使用。

本章节介绍如何创建数据存储类型，数据存储类型包括：KAFKA、网络转发、数据转发和 HDFS 四种类型。

8.1.1 创建“KAFKA”类型的数据存储

操作步骤

步骤1. 配置数据存储的参数：“**TOPIC**”、“**数据缓存**”和“**权限校验**”，参数说明如表 8-1 所示。

表8-1 参数说明（KAFKA）

参数名称	参数说明
TOPIC	KAFKA 的 topic，可以使用“$”引用其他字段的内容。 【示例】 event
数据缓存	数据缓存的条数。 【示例】 1000

参数名称	参数说明
权限校验	通过下拉列表选择权限校验的方式，包括以下选项： • 无：无需权限校验 • PLAIN • KERBEROS • SSL

步骤2. 配置“**权限校验**”：

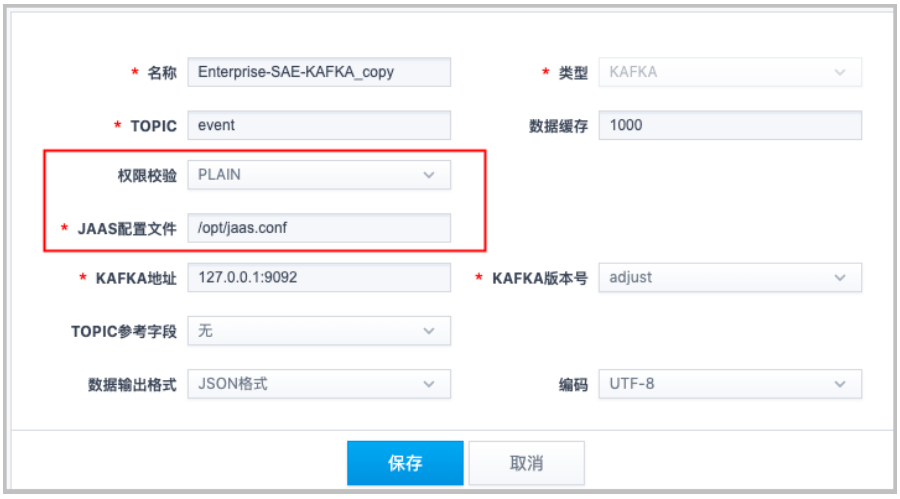
- 当配置“**权限校验**”为“**无**”。

参数说明如表 8-2 所示。

表8-2 参数说明（KAFKA-无）

参数名称	参数说明
KAFKA 地址	输入 KAFKA 的地址，格式为“IP:Port”。
Kafka 版本号	通过下拉列表选择 KAFKA 的版本号。

- 当配置“**权限校验**”为“**PLAIN**”。

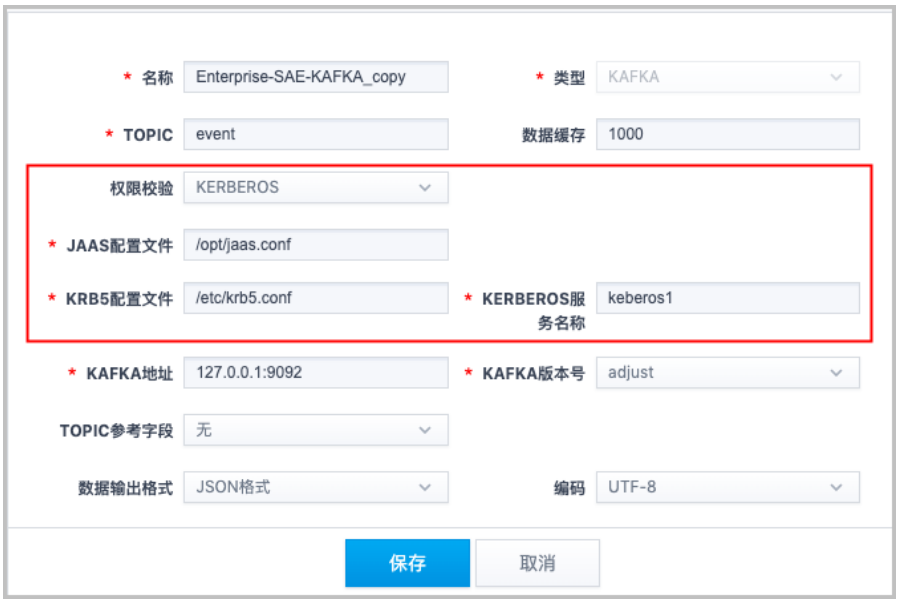


配置参数说明如表 8-3 所示。

表8-3 参数说明（KAFKA-PLAIN）

参数名称	参数说明
JAAS 配置文件	输入 JAAS 配置文件。 【示例】 /opt/jaas.conf *请将 JAAS 配置文件先存放在使用的 DCC worker 所在服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KAFKA 地址	输入 KAFKA 集群的地址，格式为“IP:Port”。
Kafka 版本号	通过下拉列表选择 KAFKA 的版本号。

- 当配置“**权限校验**”为“**KERBEROS**”。



配置参数说明如表 8-4 所示。

表8-4 参数说明（KAFKA-KERBEROS）

参数名称	参数说明
JAAS 配置文件	输入 JAAS 配置文件。 【示例】 /opt/jaas.conf *请将 JAAS 配置文件先存放在使用的 DCC worker 所在服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KRB5 配置文件	输入 KRB5 配置文件。 【示例】 /etc/krb5.conf *请将 KRB5 配置文件先存放在使用的 DCC worker 所在服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KERBEROS 服务器名称	输入 KERBEROS 服务器的名称。
KAFKA 地址	输入 KAFKA 的地址，格式为“IP:Port”。
Kafka 版本号	通过下拉列表选择 KAFKA 的版本号。

- 当配置“**权限校验**”为“**SSL**”。

配置参数说明如表 8-5 所示。

表8-5 参数说明（KAFKA-SSL）

参数名称	参数说明
TRUST 文件	输入 TRUST 文件。 【示例】 /etc/truststore.jks *请将 TRUST 配置文件先存放在使用的 DCC worker 所在服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
TRUST 密码	输入 TRUST 密码。
KEYSTORE 文件	输入 KEYSTORE 文件。 【示例】 /etc/keystore.jks *请将 KEYSTORE 配置文件先存放在使用的 DCC worker 所在服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KEYSTORE 密码	输入 KEYSTORE 密码。

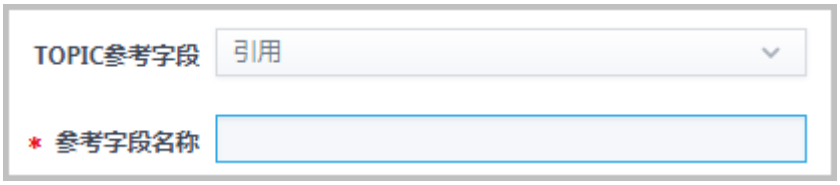
参数名称	参数说明
KEY 密码	输入 KEY 的密码。
KAFKA 地址	输入 KAFKA 的地址，格式为“IP:Port”。
Kafka 版本号	通过下拉列表选择 KAFKA 的版本号。

步骤3. 配置“**TOPIC 参考字段**”，通过下拉列表选择 TOPIC 参考字段的方式。

- 当配置为“**无**”。

  无其他配置参数需另行配置。

- 当配置为“**引用**”时，配置页面如下图所示。



参数说明如下表所示。

参数名称	参数说明
参考字段名称	输入参考字段的名称。

- 当配置为“参考时间字段”时，配置页面如下图所示。

参数说明如下表所示。

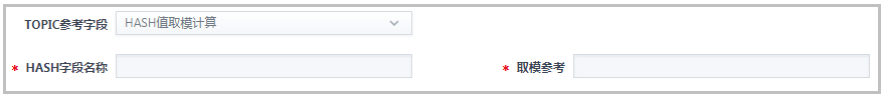
参数名称	参数说明
时间字段名称	输入时间字段的名称。
时间格式化方式	参考 JDK 时间格式化规则，如“yyyyMMdd”。

- 当配置为“截取字段内容”时，配置页面如下图所示。

参数说明如下表所示。

参数名称	参数说明
要截断的字段名称	输入需截取的字段名称。
开始截取位置	通过开关选择开始截取的字段位置。 •  ：此开关表示从头部开始截取字段。 •  ：此开关表示从尾部开始截取字段。
偏移量	开始位置的偏移量。 • 可手动输入 • 通过  递增或递减数值
长度	输入截取字段长度的数值。

- 当配置为“HASH 值取模计算”时，配置页面如下图所示。



参数说明如下表所示。

参数名称	参数说明
HASH 字段名称	输入 HASH 字段的名称。
取模参考	配置为大于 0 的整数即可，根据计算公式得出的余数值会替代索引中的$的值。

步骤4. 配置“**数据输出格式**”，通过下拉列表选择数据输出的格式。

- 当配置为“**JSON 格式**”，则数据输出的格式为 JSON。
- 当配置为“**XML 格式**”，则数据输出的格式为 XML。
- 当配置为“**分隔符格式**”，则配置页面如下图所示。

参数说明如下表所示。

参数名称	参数说明
分隔符	输入分隔符。 • \s：表示空格。 • \n：表示换行。 • \t：表示 tab
字段列表	输入字段列表，用“,”分割，用以规划输出数据字段的数据。

- 当配置为“**键值对格式**”，则配置页面如下图所示。

参数说明如下表所示。

参数名称	参数说明
分隔符	输入分隔符。 • \s：表示空格。 • \n：表示换行。 • \t：表示 tab
键值分隔符	输入键值分隔符。 • \s：表示空格。 • \n：表示换行。 • \t：表示 tab

8.1.2 创建“网络转发”类型的数据存储

操作步骤

步骤1.　配置数据存储参数，新增页面如图 8-1 所示。

图8-1 数据存储（网络转发）

参数说明如表 8-6 所示。

表8-6 参数说明（网络转发）

参数名称	参数说明
名称	区别与其它数据存储的唯一标识。
类型	通过下拉列表选择，包括以下选项： • ELASTICSEARCH • KAFKA • 网络转发 【示例】 网络转发
通信协议	选择通信协议。 【示例】 udp
数据缓存	数据缓存的条数。 • 手动输入 • 通过 递增或递减数值
发送到的地址	输入发送的主机名或 IP 地址。
发送到的端口	发送到的端口号。 • 手动输入 • 通过 递增或递减数值
数据输出格式	数据输出格式的选择与“KAFKA”类型保持一致
编码	在下拉列表中选择文件的格式编码。

8.1.3 创建“数据转发”类型的数据存储

操作步骤

步骤1. 配置数据存储参数，新增页面如图 8-2 所示。

图8-2 数据存储（数据转发）

参数说明如表 8-7 所示。

表8-7 参数说明（数据转发）

参数名称	参数说明
名称	区别与其它数据存储的唯一标识。
类型	通过下拉列表选择，包括以下选项： • ELASTICSEARCH • KAFKA • 网络转发 • 数据转发 【示例】 数据转发
采集器	选择采集器，可选择内部接收和 DCC worker 节点。 【示例】 内部接收
主题	消息队列的名称。用于内部存储采集的数据。

8.1.4 创建“HDFS”类型数据存储

HDFS（Hadoop Distributed File System，分布式文件系统），当需要将采集数据存储于 HDFS 时，需预先创建这类数据存储。

前提条件

为了确保采集器有权限写入，LAS 系统中定义存储生成文件权限有关的 owner 需要和 HDFS 所在的文件夹所有者保持一致。LAS 系统系统默认为 root，以下提供两种修改方法：

1. 方法一，预先在 HDFS 上配置上层文件夹的所有者为 root。
2. 方法二，如若不允许修改 HDFS 服务器，可修改 LAS 系统采集器的默认 owner 值，保持和 HDFS 上的文件夹所有者一致，配置文件路径为：“/opt/qihoo/soc/dataviewer/worker/plugins/dataviewer-plugin-hadoop_2.7.1-2.x_3.x/conf/hdfs.conf”，修改截图中的配置值，修改保存后，并重启 dv-worker。

操作步骤

步骤2. 配置数据存储参数，新增页面如下图所示。

参数说明如表 8-8 所示。

表8-8 参数说明（HDFS）

参数名称	参数说明
名称	区别与其它数据存储的唯一标识。
类型	通过下拉列表选择 【示例】 HDFS
HOST	输入 HDFS 部署的服务器 IP 地址。

参数名称	参数说明
PORT	输入访问 HDFS 服务的端口。
文件路径	存储采集数据的文件路径。 【示例】 /test/event
按文件大小分割文件	设置存储的单个文件最大值。单位：MB
按事件条数分割文件	设置每个文件存储的事件最大条数。单位：条
压缩方式	在下拉列表中选择压缩文件的方式： • 无：不压缩，直接存储 • Gzip • Bzip2 • Snappy 【示例】 无
权限校验	在下拉列表中选择权限校验的方式。 • 无：无需权限校验 • KERBEROS 【示例】 无

步骤3. “**路径参考路径**”的配置请参见 8.1.1 创建“KAFKA”类型的数据存储的步骤 3。

步骤4. **“数据输出格式”**的配置请参见 8.1.1 创建“KAFKA”类型的数据存储的步骤 4。

步骤5. （可选）选择“**编码**”类型，添加描述。

步骤6. 单击“**保存**”，可保存此数据存储数据。

操作结果

采集数据生成的文件名会自动加上后缀：“.[采集 worker 的 ID].[时间戳]”。如图所示。

8.1.5 更多操作

操作	说明
查看	在数据源中已勾选的数据存储不可修改、删除，可通过单击数据存储列表中某条数据操作列 的查看配置内容。
复制	您可以通过单击数据存储列表中某条数据操作列的，复制已有的数据存储，基于原有信息进行编辑以新增数据存储类型。
修改	您可以通过单击数据存储列表中某条数据操作列的，修改该条数据存储的配置信息。 在数据源中已勾选的数据存储不可修改。
删除	• 您可以通过单击数据存储列表中某条数据操作列的，删除该条数据存储数据。 • 当数据存储列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。 在数据源中已勾选的数据存储不可修改。
导出	单击数据存储列表操作栏的，目前列表中存在的数据存储类型以“.json”文件形式自动下载到默认下载位置中。
导入	单击“**导入**”，通过导入数据存储文件以创建数据存储。
查询	您可以通过界面右上角搜索框内输入数据存储名称的关键字，按回车键，执行查询，系统自动模糊查询出包含查询关键字的数据存储，以列表方式展示。 在“**名称**”框中输入“KAF”，并选择“**类型**”为“KAFKA”，单击“**查询**”，可在数据列表中显示包含“KAF 关键字，并类型为“**KAFKA**”数据存储。

8.2 解析规则管理

日志范式化的处理平台可根据样例日志、相应的解析类型产生解析规则。您可以针对不同安全设备、日志的格式，创建/维护解析规则，用于后续数据源的接入，以采集日志数据。目前支持几种解析类型，用于解析不同格式的日志或者脚本：

- **正则表达式**：适用于复杂的其他形式无法解析的日志，采用正则表达式进行解析。
- **Grok 正则**：适用于复杂的其他形式无法解析的日志，采用 GROK 表达式进行解析。
- **分隔符**：以分隔符分开每条日志。
- **键值对**：以字段分隔符、键值分隔符分开每条日志。
- **GEF**：解析 CEF 格式的日志。
- **XML**：适用于解析带有 xml 格式的日志。
- **JSON**：适用于解析带有 JSON 格式的日志。

- **脚本**：适用于解析脚本。
- **不解析**：不对日志进行解析，直接传输。
- **转发透传**：相当于不解析类型，但数据结构存储不同。

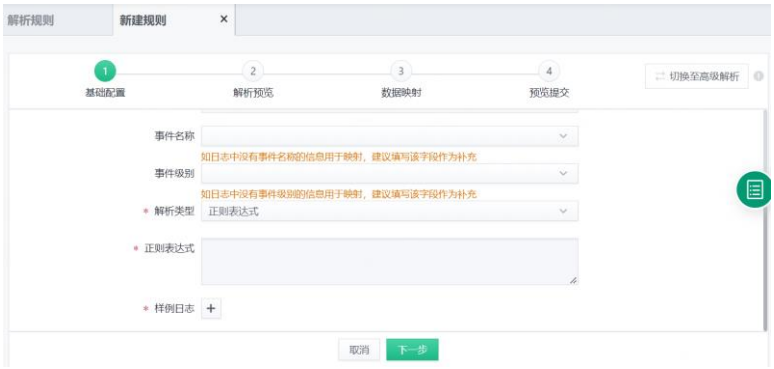
通常初始的解析规则为出厂规则，通过导入内容包生成。若用户具备维护解析规则的权限，也可以根据需要维护解析规则，支持新增、修改、复制、删除、导入、导出的操作。

8.2.1 新建简单模式的解析规则

手动新建简单模式的解析规则的通用步骤如下。而实际场景中，安全分析、运维人员往往从安全设备的类型、日志的格式入手，可参考 8.2.3 解析规则-正则表达式 ~ 8.2.8 解析规则-不解析，参考配置或者维护对应的解析规则。

8.2.1.1简单模式解析规则组成

配置简单模式的解析规则有四大步骤组成，分别为基础配置、解析预览、数据映射、预览提交四个步骤，如图所示：



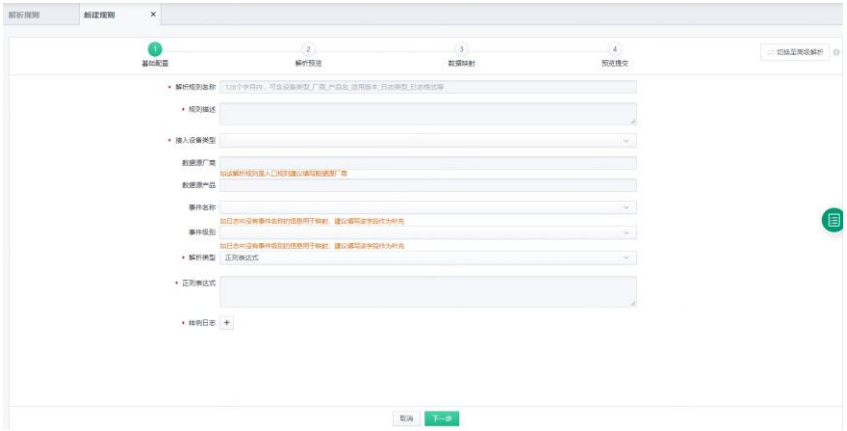
下文按照该四个步骤分别介绍。

8.2.1.2基础配置

操作步骤

步骤1. 单机“**设置** > **数据接入** >**数据解析**”，LAS 系统显示“**解析规则**”页面。

步骤2. 单击“**新建**”，添加解析规则，如下图所示。



步骤3. 填写相关参数，如表所示。

参数名称	参数说明
解析规则名称	输入解析规则的名称信息。 命名规范：设备/应用类型_日志类型_解析类型。 【示例】 Windows_4624_json
规则描述	添加对此解析规则的更多描述。
接入设备类型	在下拉列表，从**设备标准**中选择一个设备分类。
数据源厂商	输入数据源厂商的名称，非必填项。 【示例】 360
数据源产品	输入数据源产品的名称，非必填项。 【示例】 网络神经元
事件名称	从下拉框中选择事件名称。如日志中没有事件名称的信息用于映射，建议填写该字段作为补充。 【示例】 APT 检测
事件级别	从下拉框中选择事件级别。如日志中没有事件级别的信息用于映射，建议填写该字段作为补充。 【示例】 警告
解析类型	根据待解析的日志格式，选择解析类型。 【示例】 正则表达式
样例日志	输入需要解析的样例日志信息。 可以贴一条，或者多条。贴多条日志，则可以将数据多样性完全适配规则，反映出解析规则的健壮性。

8.2.1.3解析预览

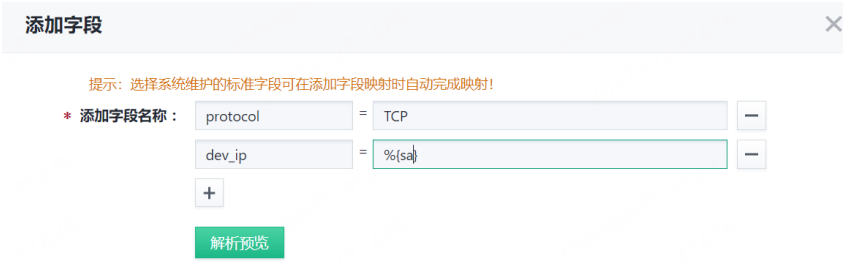
在完成基础配置后，点击“下一步”进入解析预览页面，如下图。

左侧是样例日志，可折叠显示多条。右侧是解析类型对样例日志解析的字段，以及对字段的再操作，包括：添加字段、合并字段、全文再解析、裁剪、解码、再解析、重置。对于添加字段和合并字段，更多下拉选项中还有编辑和删除操作。

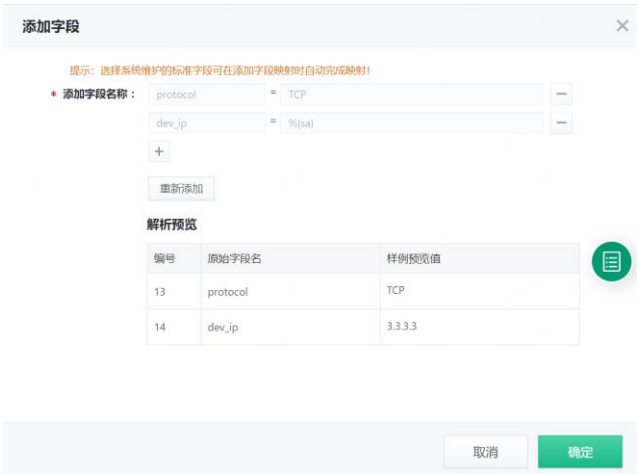
添加字段-示例 1

步骤1. 点击 **“添加字段”**，跳出添加字段的弹框。

步骤2. 分别在输入框中输入**“字段名称”**，如“protocol”，**“字段内容”**为**“TCP”**。**“字段内容”**即字段值，支持固定值和变量。当需填写变量时，可以设置已有字段的值，取值格式为%{待引用的字段名}。



步骤3. 点击“解析预览”，即可查看预览后的添加字段。



步骤4. 点击“确定”，添加字段完成，在列表中可以正确显示。

步骤5. （可选项）如果需要，可以对添加的字段进行编辑和删除。展开添加字段后的“更多”，有编辑和删除按钮。

合并字段

步骤1. 点击“**合并字段**”，跳出合并字段的弹框页。

步骤2. 输入“**合并后的字段名称**”、“**合并链接符**”和“**待合并字段**”。其中，待合并字段可以添加 2 个及以上，并且可以对字段进行上衣、下移，来调整合并后的字段的位置。同事支持对添加的带合并字段进行删除。

表明在解析时，将字段“sa”与“**da**”和并为字段“**sa_da**”。如，“sa”值为“3.3.3.3”，“da”值为“5.5.5.5”，则新字段“sa_da”的值为“3.3.3.5_5.5.5.5”。

步骤3. 点击“解析预览”，即可预览合并后的字段名称以及对应的值。

步骤4. 点击“确定”按钮，合并字段成功。

步骤5. （可选项）如果需要，可以对合并的字段进行编辑和删除。展开合并字段后的“更多”，有编辑和删除按钮。

全文再解析—示例 1

全文再解析的意思是，当指定的字段满足条件时，对 original_log 字段用新的解析规则进行再解析。若不满足匹配条件，则采用默认的解析方式进行再解析。

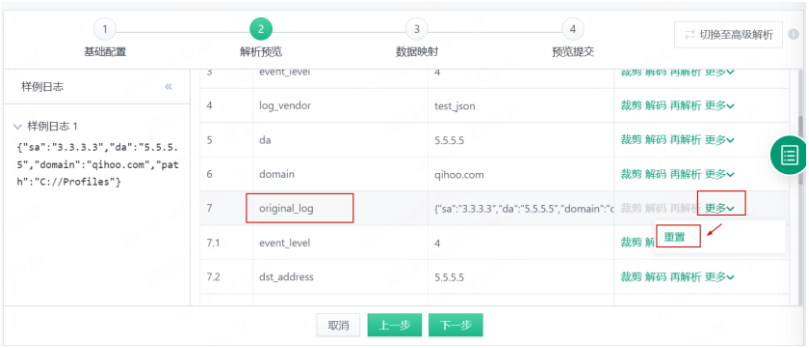
步骤1. 点击“**全文再解析**”，进入全文再解析的弹框。

步骤2. 输入“**字段名称**”，如：“event_name”，“**匹配值**”，如：“网络攻击”，“**解析规则**”，如：“json 类型的解析规则测试”，“**默认条件解析方式**”，选择“无”。

步骤3. 点击“解析预览”，即可预览合并后的字段名称以及对应的值。其中编号以层级形式显示。

步骤4. 点击“确认”按钮，全文再解析成功。

步骤5. （可选项）对于全文再解析的字段，如果想要取消，可以点击“更多”下的“重置”按钮，即可取消全文再解析的字段解析。

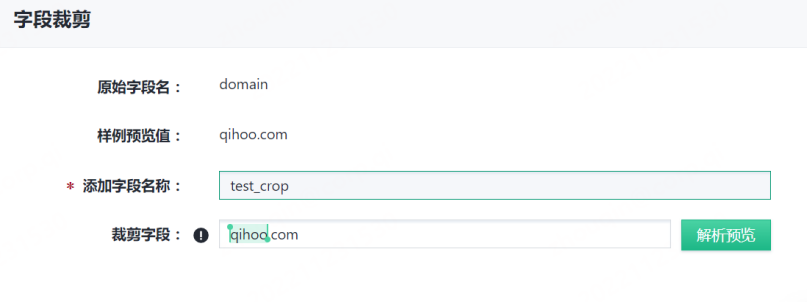


字段裁剪-示例 1

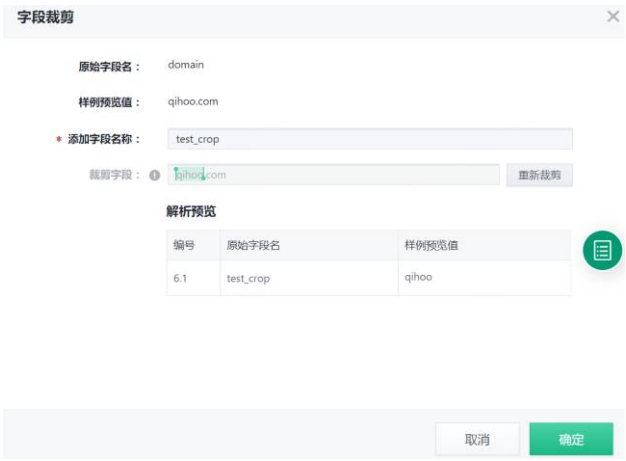
指裁剪要的部分，如下：domian 中.com 前面的值是要的部分，所以截取的起始位置从 1 开始，长度是 5。

步骤1. 选择要裁剪的字段，点击“**裁剪**”。

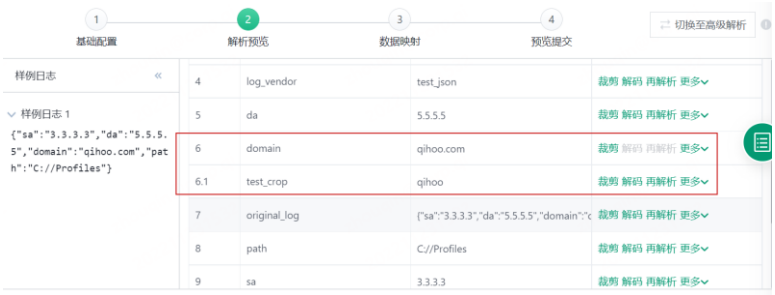
步骤2. 输入剪裁后的字段名称，拖动鼠标选择需要的范围长度字段。若有多个字段，均按该选择的范围长度规则进行裁剪。



步骤3. 点击“解析预览”，即可预览裁剪后的字段名称以及对应的值。



步骤4. 点击“确认”按钮，字段裁剪成功。

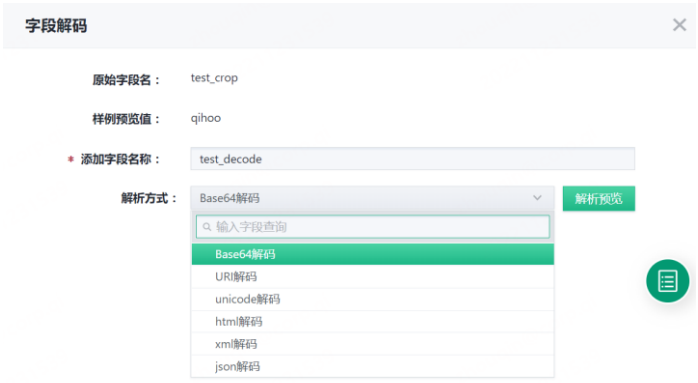


步骤5. （可选项）对于裁剪后的字段，如果想要取消，可以点击被裁减字段的“更多”下的“重置”按钮，即可删除裁剪后的字段。

字段解码

步骤1. 选择要解码的字段，点击“**解码**”，进入字段解码弹窗页。

步骤2. 输入解码后的字段名称，选择解码方式。目前简单模式的解析规则支持的在线解码方式有：Base64 解码、URI 解码、unicode 解码、html 解码、xml 解码和 json 解码。



步骤3. 点击“解析预览”，即可查看解码后的字段名称和样例预览值。

步骤4. 点击“确认”按钮，字段解码成功。

步骤5. （可选项）对于解码的字段，如果想要删除，可以点击被解码字段的“更多”下的“重置”按钮，即可删除解码后的字段。

字段再解析

步骤1. 选择要再解析的字段，点击“**再解析**”，进入字段再解析的弹框页。

步骤2. 选择解析方式，包括：正则表达式、分隔符、键值对、JSON 和子规则。

步骤3. 点击“解析预览”，即可查看再解析的字段名称和样例预览值。

步骤4. 点击“确认”按钮，字段再解析成功。

步骤5. （可选项）对于再解析的字段，如果想要删除，可以点击被再解析字段的“更多”下的“重置”按钮，即可删除再解析后的字段。

8.2.1.4数据映射

在完成基础配置和解析预览配置后，点击“下一步”机内数据映射页面。

该页面主要包括三个部分，分别是系统推荐字段、手动添加字段和未映射字段。下文依次介绍着三部分。

添加字段映射

想要利用数据解析中的解析字段，除了必要的核心字段外，必须将未映射的字段添加映射，才可以映射成系统已存在的属性字段，从而进行业务的分析。

目前系统支持对未映射字段单独添加映射和批量添加映射。入口分别为：

系统推荐字段

系统推荐字段主要是根据基础配置中的“接入设备类型”来推荐的核心字段。原始字段名的下拉框会展示已添加的映射字段，以及样例预览值。

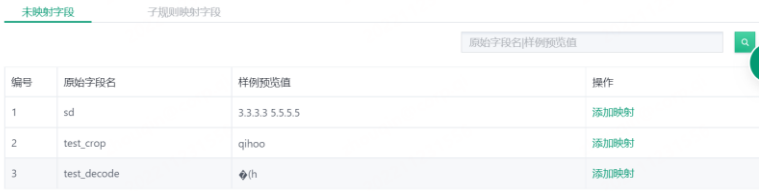
选择对应的原始字段名，与标准字段的类型相同，下一步即可正确解析。

手动添加字段

手动添加字段指将已添加的映射字段映射成系统已存在的属性字段，以便在日志中能够正确解析系统内的业务字段。标准字段类型需要与原始字段样例值的类型保持一致。

未映射字段

顾名思义，就是未被添加映射的字段。



当勾选页面左上角的“保存未映射字段”，系统会将未映射的字段，以原有字段名的形式存储在 ClickHouse 中。

枚举映射

解析规则的数据映射支持对标准字段进行枚举映射，枚举映射方式有：文本、正则、时间和映射列表。

- 文本

- 让“**匹配结果**”变得符合规范，保证与属性数据类型一致、与 SIM 事件名称一致。
- **与属性数据类型一致：**
- LAS 系统有 1000 多个属性，其数据类型除了字符类型还有 IP 类型、整型、时间类型、若在配置时选错数据类型字段界面提示会导致日志解析失败。您能做的是要么重新选择符合类型的属性，要么对“**匹配结果**”进行替换。
- **与 SIM 事件名称一致：**
- WAF 的告警有：SQL 注入、POST Sql Injection、SQL Injection 攻击（insert）、OGNL 表达式攻击、Struts2 漏洞攻击、S2-045 远程代码执行
- IPS 告警：thinkphp varchar sql injection、Java deserialization、ysoserial Remote Code exection 等等
- 我们可以将这一类名称映射符合 SIM 的事件名称，如下：

- 正则
  - 用文本替换显得效率低些，观察文本的规律，用正则替换效率更高。如下：

  - 正则映射示例：

正则	(?i).*Cross_site_scripting.*	XSS 跨站脚本攻击
正则	.*跨站脚本攻击.*	XSS 跨站脚本攻击
正则	.*SQL 注入.*	SQL 注入攻击
正则	(?i).*Sql_Injection.*	SQL 注入攻击
正则	(?i).*Information\sDisclosure.*	信息泄露
正则	(?i).*Overflow.*	溢出攻击
正则	(?i).*Directory_traversal.*	目录遍历攻击
正则	(?i).*Java deserial.*	Java 反序列化攻击
正则	(?i).*CoinMiner.*	挖矿软件
正则	(?i).*Command_Injection.*	命令注入攻击
正则	.*高危端口扫描.*	端口扫描
正则	.*批量 3306 端口扫描.*	端口扫描
正则	(?i).*Spider.*	爬虫攻击
正则	(?i).*Nmap.*	Nmap 扫描

-
- 规范映射事件名称避免了关联规则匹配的问题，所以将多个厂家多个设备的日志统一映射为 SIM 的事件名称，便于后期维护处理。
- **如果原始信息被映射成统一名称，还需要保留原始的内容怎么办？**
- 我们约定俗成了一个属性用于存储日志原始的名称：**威胁信息**

- 时间
  - 按照匹配结果顺序写，预览结果是 13 位的时间戳

  -

  -
  - 时间格式时区问题：
  - 当字段中出现时区时，可以采用 z、Z、X 进行时间格式的映射。
  - 当字段的时间与北京时间相差 8 小时时，可以采用-tz:GMT(+0000)进行时间格式的映射
  - 常见的时区有 UTC、GMT、PST、PDT，CST。
  - 其中 UTC 与 GMT 是相同的，北京时间是 GMT+8(CST);
  - PST(Pacific Standard Time)是太平洋标准时间，与 GMT 相差 8 小时，即 GMT-08:00;
  - PDT(Pacific Daylight Time)是太平洋夏令时，与 GMT 相差 7 小时，即 GMT-07:00;
  -
  - 但也有直接表示的，如-0700(西七区)，+0700(东七区)，如-07:00(西七区)，+07:00(东七区);
  - 在 2018-01-01T12:00:00Z 中，出现了 T 与 Z 代表该时区为 GMT 时区，需要将时间更新为 GMT+8，但是又无法用 z 进行时间映射，可以采用-tz:GMT(+0000)进行时间格式的映射，并使用单引号(')将 T 与 Z 过滤，如 yyyy-MM-dd'T'HH:mm:ss'Z' -tz:GMT(+0000)
  - 在 2018-01-01 12:00:00 GMT 中，GMT 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。
  - 在 2018-01-01 12:00:00 PST 中，PST 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。
  - 在 2018-01-01 12:00:00 Pacific Standard Time 中，Pacific Standard Time 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。
  - 在 2018-01-01 12:00:00 GMT-08:00 中，GMT-08:00 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。

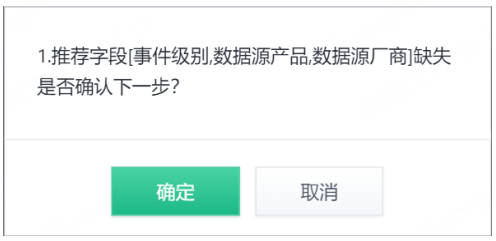
- 在 2018-01-01 12:00:00 PDT 中，PDT 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。
- 在 2018-01-01 12:00:00 Pacific Daylight Time 中，Pacific Daylight Time 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。
- 在 2018-01-01 12:00:00 GMT-07:00 中，GMT-07:00 可以使用 z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss z。
- 在 2018-01-01 12:00:00 -0700 中，-0700 可以使用 Z 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss Z。
- 在 2018-01-01 12:00:00 -07:00 中，-07:00 可以使用 X 进行时间格式的映射，如 yyyy-MM-dd HH:mm:ss X

- 映射列表
  - 对指定属性字段进行映射列表内容的映射，可以在映射表管理页面添加，方便多个样例日志中解析的字段值不同，方便自适应处理。

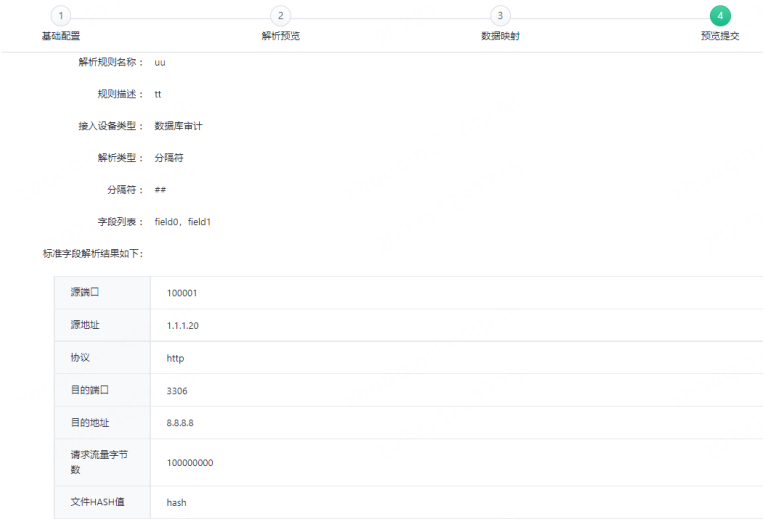
  - 对应的映射列表中包含样例预览值的映射值，如下图：

8.2.1.5预览提交

在完成前三步配置后，点击“下一步”，如果提示推荐字段缺失，可以点击“取消”按钮进行字段的补充，也可以选择“确定”进入预览提交页面。



预览提交页面包含解析规则的基础信息部分和标准字段解析结果两部分。查看各个字段的预览结果，若结果正确，点击保存，解析规则添加成功。



8.2.2 新建高级模式的解析规则

手动新建解析规则的通用步骤如下。而实际场景中，安全分析、运维人员往往从安全设备的类型、日志的格式入手，参考配置或者维护对应的解析规则。

配置基本信息

步骤1. 在导航栏单击，选择“**数据接入** > **数据解析**”，LAS 系统显示“**解析规则**”页面。

步骤2. 单击“**新建**”，添加解析规则，如图 8-3 所示。

图8-3 基本信息

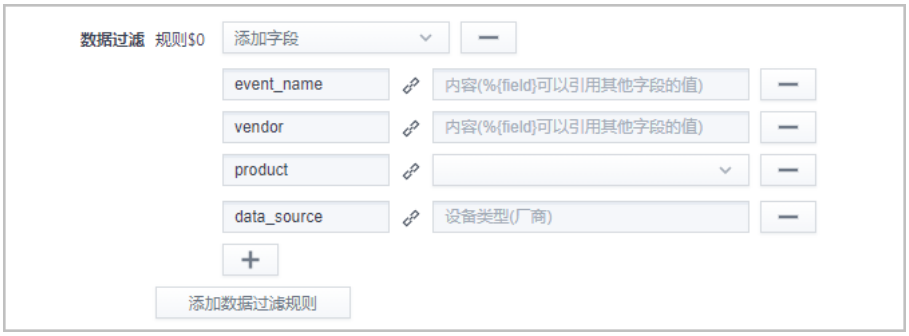
步骤3. 填写相关参数，如表 8-9 所示。

表8-9 参数说明

参数名称	参数说明
解析规则名称	输入解析规则的名称信息。

参数名称	参数说明
是否只作为子规则	设置此规则是否只为子规则，而非入口规则。 默认为“**关**”。如若需要让此规则仅为子规则，则打开开关。
规则描述	添加对此解析规则的更多描述。
设备类型	在下拉列表中选择设备类型。 *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。信息模型与事件分类绑定，选择事件模型后，即确定事件分类。 以下两种场景，建议为空： • 入口规则，一般信息模型为空，以子规则的信息模型确认事件分类。 • 当规则存在多个事件名称，所属不同事件分类时，信息模型可为空，会根据事件名称自动匹配到相应的事件分类。 • *如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。* *通过单击“**信息模型**”，新打开一个 tab 页配置模型，自行丰富信息模型成功后，需等待 30s，解析规则重新刷新模型数据。* • *如若在配置子解析规则时，需要配置信息模型，选择的模型必须是和父规则的模型一致或者是其子模型。* • *如若此解析规则解析出的数据是给 SAE 引擎使用的，请务必选择“**事件类型**”下的模型，其他模型是 context 数据模型（eg: 资产类型、脆弱性类型等）*
解析类型	根据待解析的日志格式，选择解析类型。 【示例】 JSON
样例日志	输入需要解析的样例日志信息。

添加数据过滤规则



建议必配5元组，包括以下字段：

- ***event_name（事件名称）：****有必要参考SIM事件名称做好映射。可使用固定值或者引用变量“%{xxx}”*
- ***event-level（事件级别）：****有必要映射使用固定值或者引用变量“%{xxx}”*
- ***product（产品）：****为综合SAE规则检测需求，固定名称配置涉及10种：防火墙、WAF、IDS、IPS、EDR、NDR、Email安全网关、Web安全网关、EPP、DLP。*
- ***data_source（数据源）：****固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。*
- ***vendor（厂商）***

*如若这些字段不存在，则会影响到后续SAE告警触发，并提示：**“当前解析规则5元组不全请配置齐全或前往入口规则配置”**。*

【使用方法如下】

步骤1. 单击“**添加数据过滤规则**”，在“**规则**”下拉列表中选择数据过滤规则类型。

数据过滤的规则包括以下几种类型：

- **添加字段**：在原有日志字段的基础上添加新的字段。
- **删除字段**：删除无需解析的字段。
- **字段重命名**：更改字段的名字，前面输入原字段名，后面输入新的字段名。
- **合并字段**：合并多个字段为一个。
- **字段裁剪**：对字段的值进行剪裁，前面输入要剪裁的字段名，后面输入开始剪裁的位置，和剪裁的长度。
- **数据匹配再解析**：对字段进行多重设置，当某个字段值为多少时，对该字段进行再次过滤。
- **数据头匹配再解析**：当字段的值为多少时，对字段进行再次过滤，不过可以从前开始匹配。
- **数据尾匹配再解析**：从字段值得后面开始匹配。

- **数据正则匹配再解析**：使用正则匹配个别字段，输入要匹配的字段，匹配的该字段值的规则。
- **数据包含再解析**：与数据匹配再解析类似，数据匹配再解析是全部匹配，包含是包含输入值就可以再做过滤。
- **字段再解析**：对某个字段进行再次解析，且解析规则为其他类型。
- **添加数组字段**：支持添加数组类型的字段。
- **字段拆分成数组**：支持用指定的分割符将字段拆分成数组。
- **格式化为 json 对象**：当待解析字段为 json 值，选择此过滤规则，解析后将字段按键值拆分，分别显示。
- **格式化为 json 数组**：当待解析字段为数组，且数组中的元素为 json 格式。如若需要以原始格式保存至 ES，则需要将此字段添加此条件。

*以上数据过滤规则凡是与数组相关，在解析后，配置“**固定字段**”时，选择的固定字段的**属性类型**必须为**数组**。如若类型不匹配，则会导致解析结果有误。*

步骤2. **添加字段**。

1. 选择“**规则**”为“**添加字段**”。

分别在输入框中输入“**字段名称**”，如“**event_name**”，“**字段内容**”为“**正常访问**”。

即表明添加此字段“**event_name=正常访问**”。

“**字段内容**”即字段值，支持固定值和变量。当需填写变量时，可以设置已有字段的值，取值格式为%{待引用的字段名}。

步骤3. **删除字段**。

1. 选择“**规则**”为“**删除字段**”。

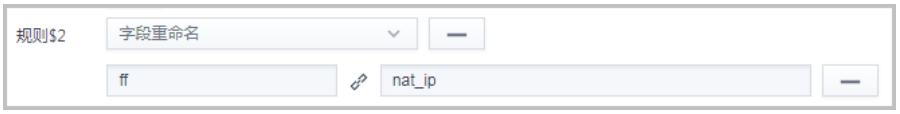
在输入框中输入待删除的字段名，如“**vendor**”。

表明在解析时，删除此字段“**vendor**”。

步骤4. **字段重命名**。

1. 选择“**规则**”为“**字段重命名**”。

在输入框中输入“**日志中的原始字段**”和“**重命名后字段名称**”。

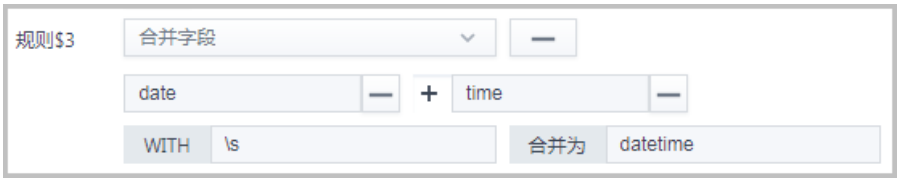


表明在解析时，将字段“**ff**”重命名为“**nat_ip**”。

步骤5. **合并字段**。

1. 选择“**规则**”为“**合并字段**”。

输入要合并的字段名和合并后的字段名。



表明在解析时，将字段“**date**”与“**time**”和并为字段“**datetime**”。如，“**date**”值为“**2018/4/16**”，“**time**”值为“**16:50**”，则新字段“**datetime**”的值为“**2018/4/16*[空格]*16:50**”。

步骤6. **字段裁剪**。

1. 选择“**规则**”为“**字段裁剪**”。

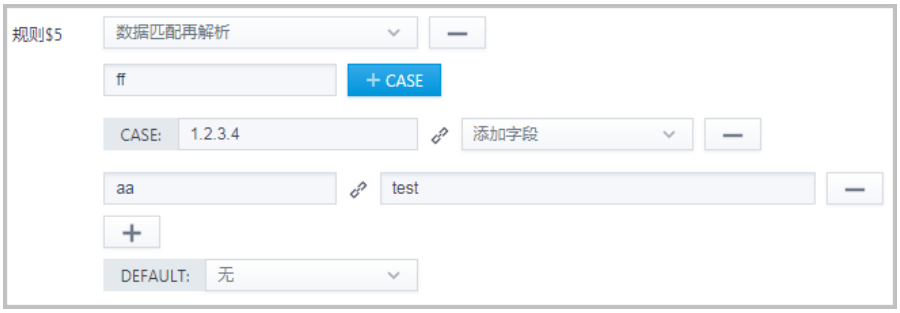
分别输入要剪裁的字段名，开始剪裁的位置，和剪裁的长度。

表明在解析时，将字段“**td**”的值从第 **1** 位开始截取 **20** 个字符。

步骤7. **数据匹配再解析**。

1. 选择“**规则**”为“**数据匹配再解析**”。

输入需要匹配的字段名称，单击“**CASE**”，如下图所示。



表明将字段“**ff**”，匹配值，即 Case 值为“1.2.3.4”，在下拉列表中选择数据过滤规则“**添加字段**”，字段名为“**aa**”，给字段“aa”取值为“**test**”。

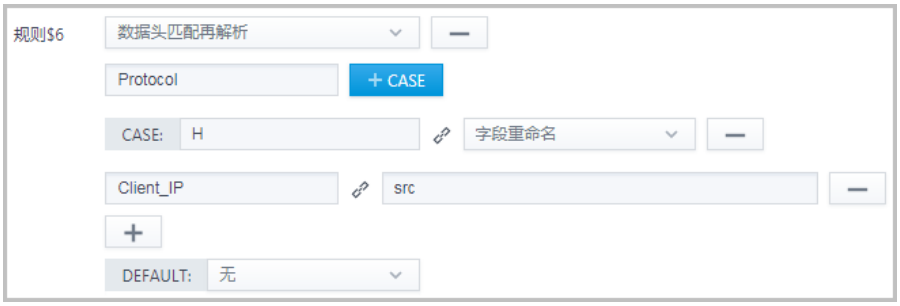
（可选）可配置“DEFAULT”参数。当 CASE 值不生效时，则解析“DEFAULT”中的规则。

- 当“**DEFAULT**”参数设置为“无”时，则对字段不做过滤处理。
- 当“**DEFAULT**”参数设置为其他规则时，则根据规则进行过滤。

步骤8. **数据头匹配再解析**。

1. 选择“**规则**”为“**数据头匹配再解析**”。

输入需要匹配的字段，如“**Protocol**”，匹配值，即 Case 值为“H”，在下拉列表中选择数据过滤条件“**字段重命名**”，原字段名为“**Client_IP**”，重命名为“**src**”。



由于字段 Protocol 有 HTTP，TCP 等，所以当 Protocol 字段的值从头开始解析，为“HTTP”时，则对字段进行再次解析，将“**Client_IP**”字段重命名为“**src**”。

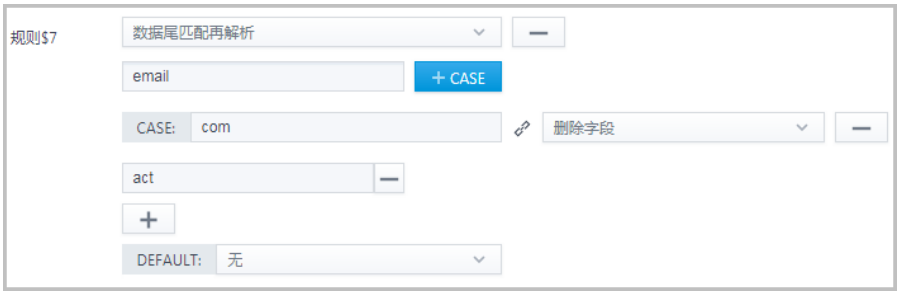
（可选）可配置“**DEFAULT**”参数。当 CASE 值不生效时，则解析“**DEFAULT**”中的规则。

- 当“**DEFAULT**”参数设置为“**无**”时，则对字段不做过滤处理。
- 当“**DEFAULT**”参数设置为其他规则时，则根据规则进行过滤。

步骤9. **数据尾匹配再解析**。

1. 选择“**规则**”为“**数据尾匹配再解析**”。

输入需要匹配的字段，如“email”，匹配值，即 Case 值为“com”，在下拉列表中选择数据过滤条件“**删除字段**”，字段名为“act”。



表明在字段 email 的值为“**gary@xxx.com,henry@xxx.cn**”，即为当 email 字段值为“**xxx.com**”时，对数据从尾部“**com**”进行再次解析，删除字段“**act**”。

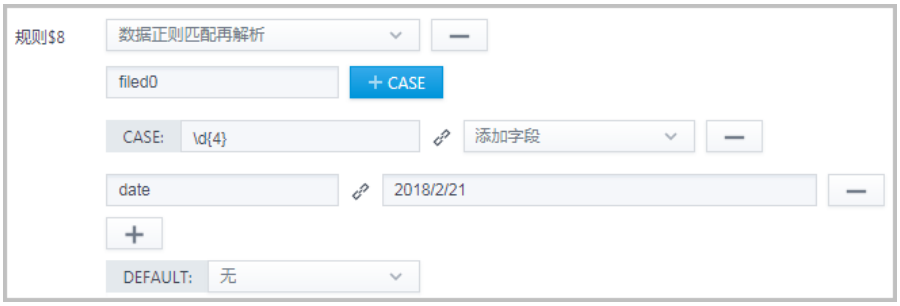
（可选）可配置“**DEFAULT**”参数。当 CASE 值不生效时，则解析“DEFAULT”中的规则。

- 当“**DEFAULT**”参数设置为“**无**”时，则对字段不做过滤处理。
- 当“**DEFAULT**”参数设置为其他规则时，则根据规则进行过滤。

步骤10. **数据正则匹配再解析**。

1. 选择“**规则**”为“**数据正则再解析**”。

输入要匹配的字段名称，如“**filed0**”，匹配值，即 Case 值为“**\d{4}**”，选择“**添加字段**”，字段名称为“**date**”，内容为“**2018/2/21**”。



即当字段“**filed0**”为四个数字时，添加字段“**date**”，取值“**2018/2/21**”。

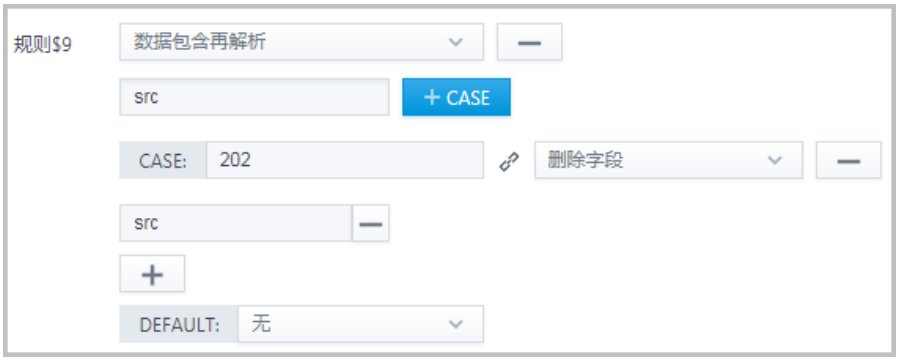
（可选）可配置“**DEFAULT**”参数。当 CASE 值不生效时，则解析“**DEFAULT**”中的规则。

- 当“**DEFAULT**”参数设置为“**无**”时，则对字段不做过滤处理。
- 当“**DEFAULT**”参数设置为其他规则时，则根据规则进行过滤。

步骤11. **数据包含再解析**

1. 选择“**规则**”为“**数据包含再解析**”。

输入要匹配的字段名称，如“**src**”，匹配值，即 Case 值为“**202**”，选择“**删除字段**”，字段名称为“**src**”。



表明即当字段“**src**”中的值包含“**202**”时，就会删除 src 字段。

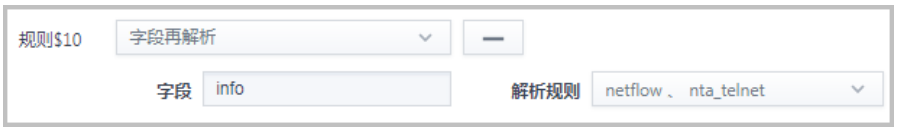
（可选）可配置“**DEFAULT**”参数。当 CASE 值不生效时，则解析“**DEFAULT**”中的规则。

- 当“**DEFAULT**”参数设置为“**无**”时，则对字段不做过滤处理。
- 当“**DEFAULT**”参数设置为其他规则时，则根据规则进行过滤。

步骤12. **字段再解析**

1. 选择“**规则**”为“**字段再解析**”。

输入要匹配的字段名称，如“**info**”，选择已创建成功的解析规则“**net_flow**”。



表明对字段“**info**”进行再次解析，解析规则为“**net_flow**”。

步骤13. **添加数组字段**

1. 选择规则为“**添加数组字段**”。

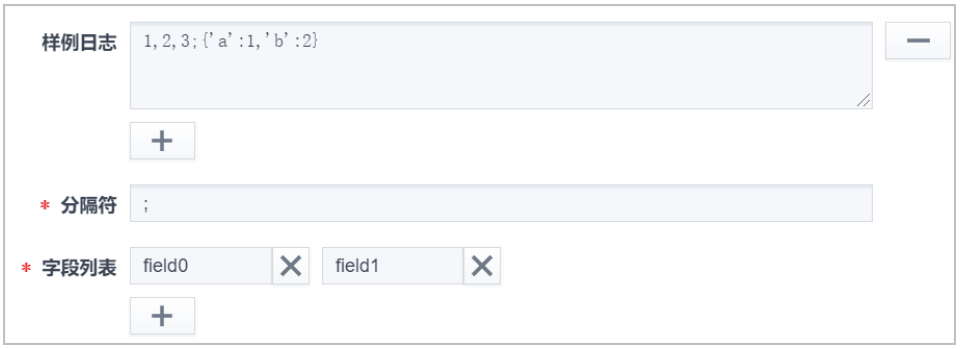
输入需要添加的数组格式的字段，如“**field2**”、“**field3**”，并分别设置其字段值为“**['test1','test2']**”、“**[{'A':1},{'B':2}]**”（这两种均为数组格式）。

步骤14. **字段拆分成数组**

1. 选择规则为“**字段拆分成数组**”。

输入待拆分成数组格式的字段，如“**field0**”，并设置分割的分割符为“，”。

假设样例日志以及分隔结果如下，“**field0**”为“1,2,3”：



添加规则如下：

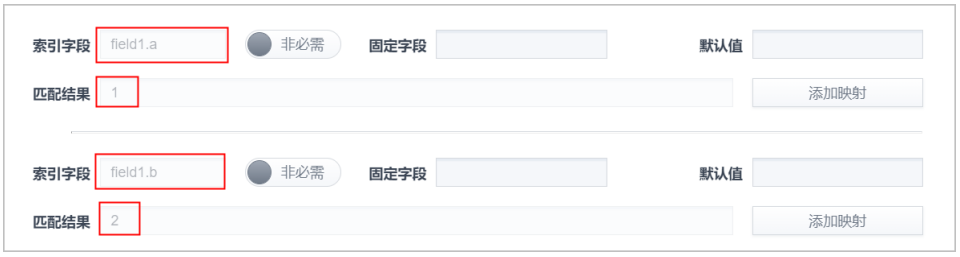
即将字段拆成分数组，将“**field0**”：“1,2,3”拆分为数组“[1,2,3]”

步骤15. **格式化成 json 对象**

1. 选择规则为“**格式化成 json 对象**”。

输入需要格式化为 json 的字段，如“**field1**”。

“**field1**”为“**{'a':1,'b':2}**”，解析后，结果显示为：

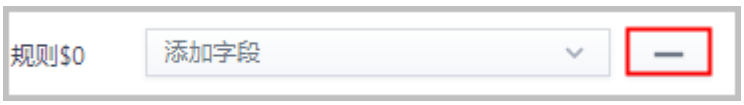


步骤16. **格式化成 json 数组**

1. 选择规则为“**格式化成 json 数组**”。

输入需要格式化为 json 数组的字段，如“**field3**”。“**field3**”为“**[{'A':1},{'B':2}]**”，则“**[{'A':1},{'B':2}]**”以原始格式存储至 ES。如若不选择此规则过滤，则会导致此数组以字符的格式存储。

步骤17. （可选）单击某条规则后的 —，可删除该条规则。



步骤18. 单击“**解析**”，使添加的“**数据过滤规则**”生效。

解析

步骤1. 单击“**解析**”。

- 若解析成功，不给出提示，页面弹出对应解析类型的界面。
- 若解析错误，页面即提示，请修改配置项。

步骤2. 根据已解析的“**索引字段**”，根据显示的“**匹配结果**”以及信息模型提供的参考属性字段，输入“**固定字段**”。

鼠标选中输入框时，按键盘↑、↓会有提示：

- 信息模型中的“**必须属性**”以红色字体提示
- 信息模型中的“**可选属性**”以绿色字体提示
- 其他属性均以灰色字体显示

步骤3. 根据需要，单击“**添加映射**”，并选择“**映射类型**”，输入映射结果。

映射类型包括：

- **文本**
- **正则**
- **时间**
- **Base64 解码**
- **URI 解码**
- **重定义**
- **IP 解码**：选择 IP 类型，包括 IPV4 和 IPV6 选项。
- **映射类别**：映射列表中请根据下载的文件格式写入要映射的参数再上传即可。
- **加密**：支持对字符串类的字段选择加密，在配置用户时选择该用户是否对加密数据可见。
- **unicode 解码**
- **html 解码**
- **xml 解码**
- **json 解码**

1. 若解析出索引字段“**event_name**”，配置属性为“**事件名称**”。

   为了事件名称更加规范化，单击“**添加映射**”，选择“**映射类型**”为“**文本**”，输入“**匹配值**”和“**映射值**”。

即在解析日志时，根据匹配到以下字段名，如“**SQL 注入**”，则会输出相应的映射值“**web 攻击 sql 注入**”。

若解析索引字段“1”，配置属性为“**发生时间**”，单击“**添加映射**”，选择“**映射类型**”为“**时间**”，输入“**时间格式**”，如：**MMM dd HH:mm:ss**，则解析后的“**发生时间**”会根据这个格式显示。

若解析索引字段“**event_name**”，配置属性为“**事件名称**”，匹配结果为一句描述“DNS response resolves to dead IP address”，而实际接入的日志并非固定、一成不变的，此时可以通过“**添加映射**”，使用**正则**的方式，当该句描述以“**DNS reponse**”开头时，多数是“**DNS 响应异常**”。因此配置内容如下。

预览

单击“**预览**”，可预览解析规则的内容。

保存

预览解析规则无误后，可单击“**保存**”。保存成功后，在解析规则列表中查看到此条数据。

更多操作

操作	说明
复制	您可以通过单击解析规则列表中某条解析规则操作列的，复制已有的规则，基于原有信息进行编辑以新增解析规则。
修改	您可以通过单击解析规则列表中某条解析规则操作列的，修改该条规则的信息。
删除	• 您可以通过单击解析规则列表中某条解析规则操作列的，删除该条解析规则的数据。 • 当解析规则列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
导出	单击“**导出**”，目前列表中存在的规则以文件形式自动下载到默认下载位置中。
导入	单击“**导入**”，通过导入解析规则文件以创建解析规则。 *导入解析规则时，如果 ID 已存在或者名称已存在则不导入，只导入 ID 和名称都不存在的规则。*
查询	您可以通过界面右上角搜索框内输入解析规则名称的关键字，按回车键，执行查询，系统自动模糊查询出包含查询关键字的解析规则，以列表方式展示。

8.2.3 解析规则-正则表达式

当接入的日志形式较复杂，且其他形式无法解析，可尝试采用“**正则表达式**”的解析类型进行解析。本章节以某厂商的 WAF 日志为例，介绍这类厂家、日志类型的解析方法。

样例日志

```
<134>Nov 14 10:54:27 localhost fwlog: 日志类型:WAF 应用防护日志, 源 IP:1.119.130.202, 源端口:29000, 目的 IP:10.1.7.108, 目的端口:80, 攻击类型:WEB 登录弱口令防护, 严重级别:中, 系统动作:被记录, URL:hseq.ccccltd.cn/ConserveEnergyTest/waf/loginPost.bo
```

正则表达式

根据样例日志，将其转换成正则表达式的形式，便于后续的解析。

```
((?:Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)\s+\d{1,2}\s+\d{2}:\d{2}:\d{2}).*?日志类型:(.*?),\s+源IP:((?:\d{1,3}\.){3}\d{1,3}),\s+源端口:(\d+),\s+目的IP:((?:\d{1,3}\.){3}\d{1,3}),\s+目的端口:(\d+),\s+攻击类型:(.*?),\s+严重级别:(.*?),\s+系统动作:(.*?),\s+URL:(.*)
```

基本内容说明

参数名称	参数说明
解析规则名称	解析规则名称信息。
是否只作为子规则	设置此规则是否只为子规则，而非入口规则。 默认为“**关**”。如若需要让此规则仅为子规则，则打开开关。
规则描述	解析规则描述。

参数名称	参数说明
设备类型	根据待接入的安全设备的类型选择。  *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 根据设备的作用，日志样例内容的初步审阅，这类日志大概率属于“**网站攻击**”类。 单击“**信息模型**”，可以跳转至“**模型管理**”页签下，自行丰富信息模型。
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。
正则表达式	将样例日志转换为正则表达式的形式，供后续解析各字段。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **vendor（厂商）** • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” 如若这些字段不存在，则会影响到后续 SAE 告警触发。

解析

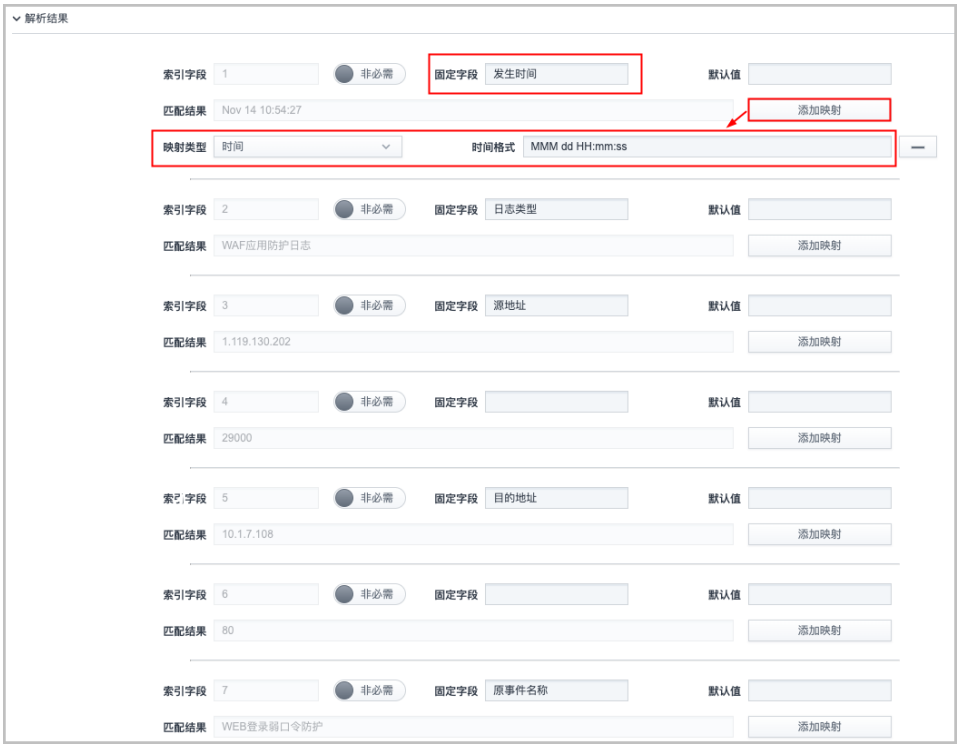
步骤1.　单击“**解析**”后，如若解析成功，显示“**解析结果**”。

步骤2. 将“**索引字段**”抽取，根据显示的“**匹配结果**”以及信息模型提供的参考属性字段，输入“**固定字段**”。

鼠标选中输入框时，按键盘↑、↓会有提示：

- 信息模型中的“**必须属性**”以红色字体提示
- 信息模型中的“**可选属性**”以绿色字体提示
- 其他属性均以灰色字体显示

步骤3. 根据需要，单击“**添加映射**”，并选择“**映射类型**”，输入映射结果。



预览

单击“**预览**”，可预览解析规则的内容。

保存

预览解析规则无误后，可单击“**保存**”，保存成功后，可在解析规则列表中查看到此条数据。

8.2.4 解析规则-键值对

经观察，待接入的厂家设备的日志均是以**字段分隔符、键值分隔符**分开的。可采用“**键值对**”这种解析类型来编辑解析规则。本章节以某厂商安全审计监控日志为例，介绍这类厂家、日志类型的解析方法。

键值对举例

```
a=1 b=2 c=3
a:1,b:2,c:3
```

样例日志

```
account=blank;action name=blank;app cat name=blank;app name=blank;appgname=blank;a
ppname=blank;content=blank;cpu used=blank;create time=blank;disk used=blank;down=b
lank;dst ip=blank;dst port=blank;end time=blank;file name=blank;handle action=blan
k;mem used=blank;msg=blank;pid=blank;session num=blank;src ip=blank;src mac=blank;
temperature=blank;term_device=blank;term_platform=blank;ugname=blank;uip=blank;uma
c=blank;up=blank;url=blank;url_cate_name=blank;url_domain=blank;user_group_name=bl
ank;user_name=blank
```

经观察，这类日志，**“字段分隔符”**为“;”，**“键值分隔符”**为“=”。

具体请根据样例日志配置，当字段以空格分隔，请使用“/s”。

特殊处理办法

当某一类厂家产品的日志，键（key）越多，匹配的日志越多，则需要从大量日志中统计出此款产品日志的所有键名（key）。比如，通过对某网神的下一代防火墙的大批日志进行分类后，得到了 11 类原始日志，都是可以通过键值对来做解析的。处理思路和方法大概如下：

1. 通过仔细观察这些原始日志，可以发现有些键（key）是一样的，但有些键（key）是不一样的，构造一条通用的原始日志，包含所有的键（key）。

   某网神的下一代防火墙的 11 类原始日志如下：（选取其中两个）

```
FW_某网神_NGFW_1

devid="3" dname="SecGateNSG" serial="103b8f2df90639e7f991c40e03927f99a2049272"
type="traffic-end" time="1477461949" module="flow" severity="info" duration="1"
addr src="172.24.230.61" addr dst="180.163.221.210" port src="52310"
port dst="443" proto="TCP" nataddr src="::" nataddr dst="::" natport src="0"
natport dst="0" session id="1777998" session time="1477461948" sess nth="1"
sess dev id="0" interface src="vlan230" interface dst="ge3" zone src="产品演示"
zone dst="To-IT" locale src="" locale dst="上海市" user src="" user dst=""
appname="SSL" action="permit" asset os src="Linux" asset os dst=""
asset name src="" asset name dst="" asset type src="" asset type dst=""
app risk="2" app category="APP NETWORK" focus type="NO" non standard port="NO"
bytes sent="1588" bytes received="1878" pkts sent="8" pkts received="10"
total sess="0" rule="访问公网" profile="" from tunnel="" to tunnel=""

FW 某网神 NGFW 10

devid="3" dname="SecGateNSG" serial="d0ed6f3c69a19f2a5e4054a26079709a9e81da58"
module="flow" severity="info" type="traffic-end" session id="7153768"
time="1509706666" addr_src="fe80::9a30:ff:fe11:1540" addr_dst="ff02::2"
```

```
nataddr_src="::" nataddr_dst="::" natport_src="0" natport_dst="0" proto="ICMPv6"
hit_num="0" focus_type="NO" action="permit" session_time="1509706666"
sess_nth="1" sess_dev_id="0" port_src="1" port_dst="1" user_src="" user_dst=""
locale_src="" locale_dst="" interface_src="s3ge1" interface_dst="" zone_src=""
zone_dst="" appname="ICMP_IPV6" rule="__to_self__" profile=""
non_standard_port="NO" app_category="APP_NETWORK" app_risk="1" asset_os_src=""
asset_os_dst="" asset_name_src="" asset_name_dst="" asset_type_src=""
asset_type_dst="" duration="0" bytes_sent="56" bytes_received="0" pkts_sent="1"
pkts_received="0" total_sess="0" from_tunnel="" to_tunnel=""
```

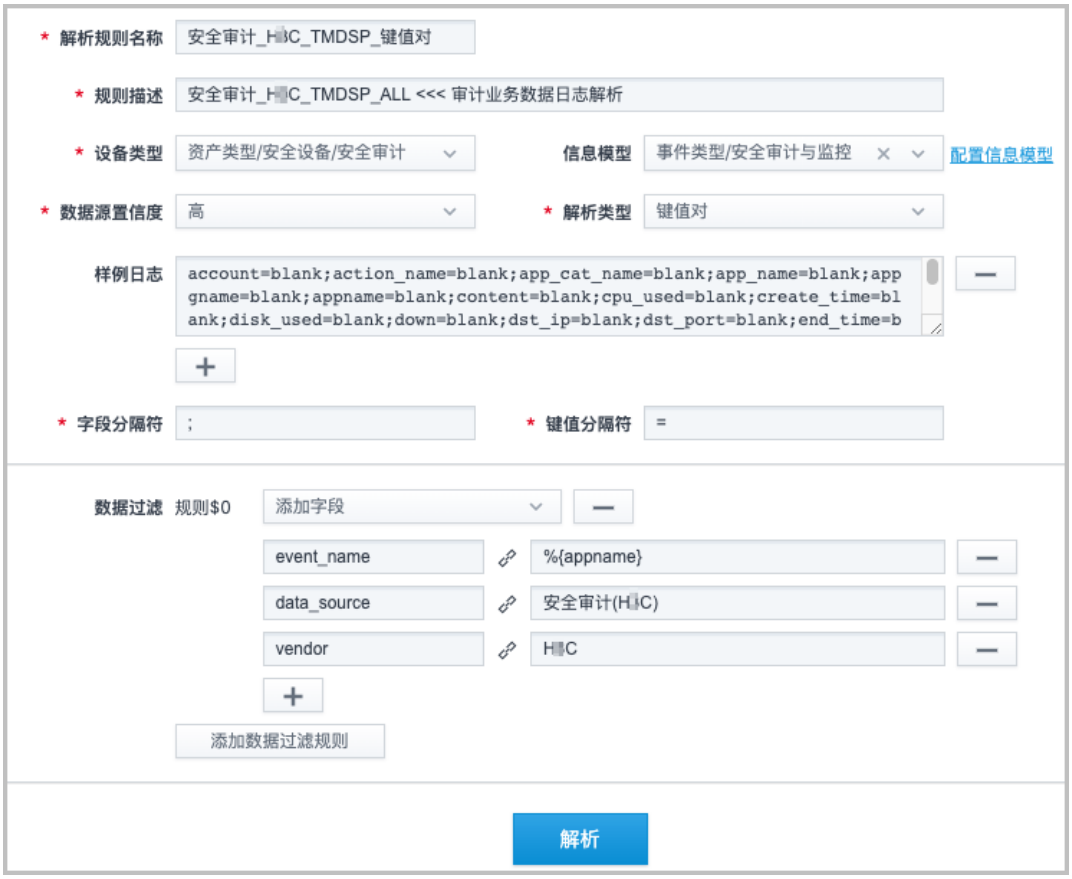
2. 整合原始“**键**”。

   建议：利用 python 脚本，对原始日志进行字符串合并，通过 set()函数对键(key)去重。整合完了，之后就可以适配所有类型的某网神的 NGFW 的日志，如果发现缺少什么键(key)，可以直接增加原始日志的内容。

3. 编辑脚本，输出原始“键”与值的对应关系，根据值理解字段的属性含义。

4. 通过整合出来的构造原始日志的键(key)，并取到与之对应的值(value)，结合 excel 进行处理。

基本内容说明



参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。
设备类型	根据待接入安全设备的类型选择。  *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 根据设备的作用，日志样例内容的初步审阅，这类日志大概率属于“**安全审计与监控**”类。 单击“**信息模型**”，可以跳转至“**模型管理**”页签下，自行丰富信息模型。
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。
字段分隔符	根据样例日志，经观察，输入各个字段之间的分隔符。
键值分隔符	各个 key 值的分隔符号。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 sae 告警触发。

解析

步骤1. 单击“**解析**”后，如解析成功，显示“**解析结果**”。

步骤2. 将“**索引字段**”抽取，根据显示的“**匹配结果**”以及信息模型提供的参考属性字段，输入“**固定字段**”。

鼠标选中输入框时，按键盘↑、↓会有提示：

- 信息模型中的“**必须属性**”以红色字体提示
- 信息模型中的“**可选属性**”以绿色字体提示
- 其他属性均以灰色字体显示

步骤3. 根据需要，单击“**添加映射**”，并选择“**映射类型**”，输入映射结果。

预览

单击“**预览**”，可预览解析规则的内容。

保存

预览解析规则无误后，可单击“**保存**”。保存成功后，在解析规则列表中查看到此条数据。

8.2.5 解析规则-分隔符

经观察，待接入的厂家设备的日志均是以字段分隔符分开的。可采用“**分隔符**”这种解析类型来编辑解析规则。本章节以某厂商防火墙日志为例，介绍这类厂家、日志类型的解析方法。

分隔符举例

```
a,b,c,d,e
a;b;c;d;e
```

样例日志

```
<14>Mar 18 02:08:49 SZDN07FWPA06 1,2019/03/18
02:08:49,013201000909,SYSTEM,general,0,2019/03/18
02:08:49,,general,,0,0,general,informational,"User nbackup logged in via CLI from
10.49.10.20",6504181057246532940,0x8000000000000000,0,0,0,0,,SZDN07FWPA06
```

经观察，这类日志，**“字段分隔符”**为“,”。可以先在线下进行预处理。

处理方法参考

利用 excel 表，

- 把获取的原始字段说明，都按照逗号‘,’回车，变成一列，贴到 excel 第一列；
- 再把原始日志，都按照按照逗号‘,’回车，变成一列，贴到 excel 的第二列。
- 根据原始字段说明，以及与原始日志中的内容，来选择系统内置的属性字段。

示例图

field0	<14>Mar 18 02:08:49 SZDN07FWPA06 1
field1	019/03/18 02:08:49
field2	13201000909
field3	SYSTEM
field4	general

基本内容说明

参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。

参数名称	参数说明
设备类型	根据待接入安全设备的类型选择。  *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 这里是一个入口规则，可选择不配置。更多字段的解析可以走向子规则，提供更多的解析作用。
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。
分隔符	根据样例日志，经观察，输入各个字段之间的分隔符。
字段列表	编辑自定义的字段，与预处理中的一一对应。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 SAE 告警触发。  *示例中，字段“**field14**”（样例日志中是“User nbackup logged in via CLI from 10.49.10.20”）是一段可以进一步解析的日志内容。因此可以通过“**添加字段**”，如“**field121**”，并将其引用为“**field14**”。再对“**field14**”进行“**字段再解析**”，走向该类日志的子规则。利用子规则对此日志进一步解析。*

解析

步骤1. 单击“**解析**”，如若解析成功，显示“**解析结果**”。

步骤2. 将“**索引字段**”抽取，根据显示的“**匹配结果**”以及信息模型提供的参考属性字段，输入“**固定字段**”。

鼠标选中输入框时，按键盘↑、↓会有提示：

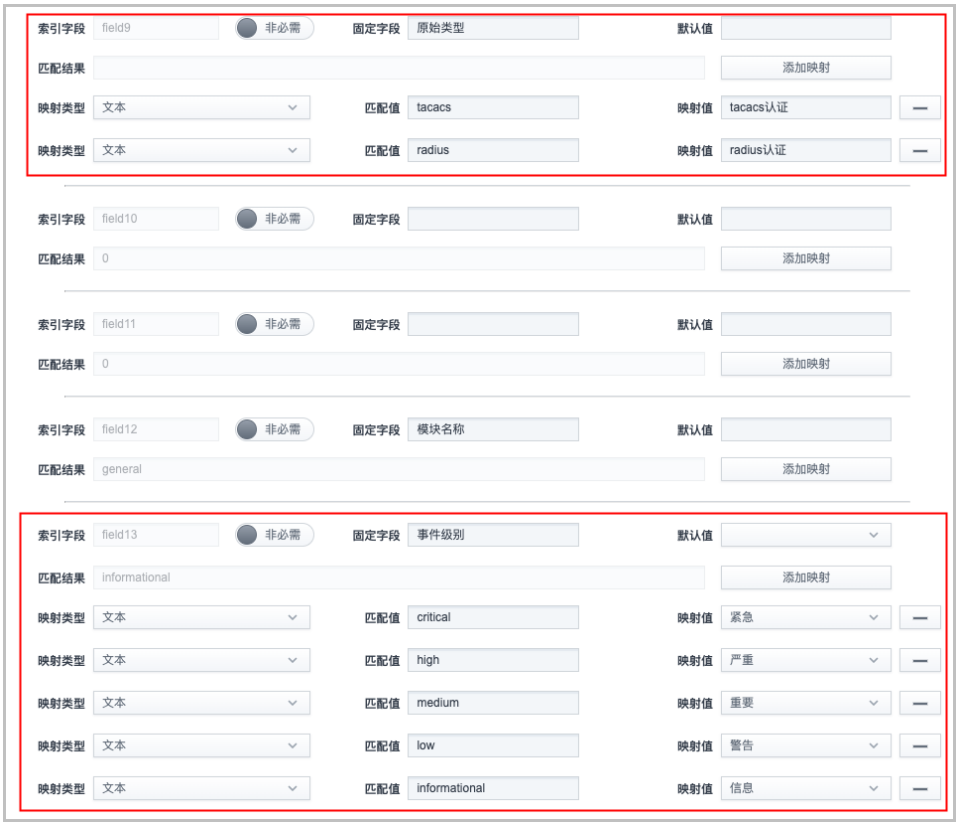
- 信息模型中的“**必须属性**”以红色字体提示
- 信息模型中的“**可选属性**”以绿色字体提示
- 其他属性均以灰色字体显示

步骤3. 根据需要，单击“**添加映射**”，并选择“**映射类型**”，输入映射结果。

比如示例中，索引字段“**field9**”一般会是“tacacs”或者“radius”，这是一个日志事件的“**原始类型**”，因此配置“**固定字段**”为“**原始类型**”。

为了解析结果更加规范，可以将其映射为“**文本**”，当匹配到“**tacacs**”时，解析后就会显示“**tacacs 认证**”。

索引字段“**field13**”同理，不再赘述。



预览

单击“**预览**”，可预览解析规则的内容。

保存

预览解析规则无误后，可单击“**保存**”。保存成功后，在解析规则列表中查看到此条数据。

8.2.6 解析规则-CEF

经观察，待接入的厂家设备的日志均是 CEF 格式。可采用“**CEF**”这种解析类型来编辑解析规则。本章节以某厂商 IDS TDA 的日志为例，介绍这类厂家、日志类型的解析方法。

CEF 格式日志说明

CEF 格式是 ArcSight 开发的一种通用日志格式，用途十分广泛，有通用字段部分，也有自定义的字段部分，且属性字段都描述的比较清楚，不需要像分隔符的日志，需要去额外找字段说明，在日志里就能读懂字段表示的含义，但是也有它的特殊性。

CEF 头部域

```
<150>CEF:0|Asiainfo security|TDA|3.83.1023|38|12 unsuccessful logon attempts - SMB|2|dvc=...
```

CEF 头部 7 个字段通用属性字段如下。其他字段的属性可参见《CEF 字段说明表》。

日志头部 7 个字段	字段参数	属性字段
<150>CEF:0	version	CEF 版本
Asiainfo security|	device_vendor	设备厂商
TDA|	device_product	设备产品
3.83.1023|	device_version	设备版本
38|	signature_id	特征 ID
12 unsuccessful logon attempts - SMB|	name	事件名称
2|	severity	事件级别

样例日志

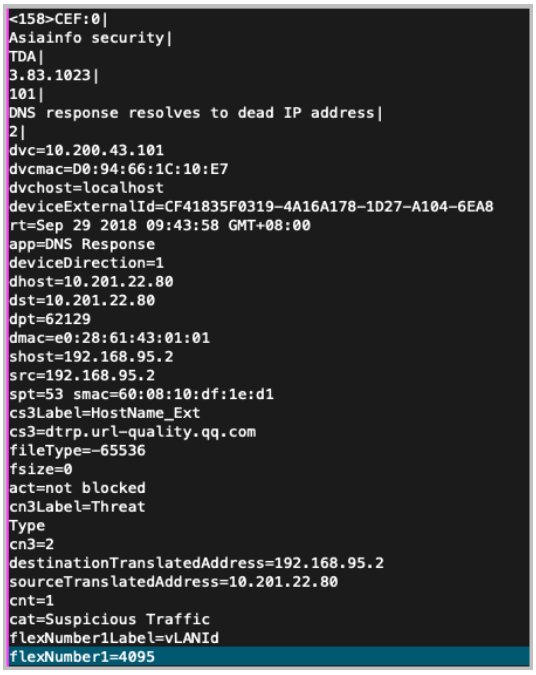
红色字体为除 7 个头部域的日志内容：

```
<158>CEF:0|Asiainfo security|TDA|3.83.1023|101|DNS response resolves to dead IP address|2|dvc=10.200.43.101 dvcmac=D0:94:66:1C:10:E7 dvchost=localhost deviceExternalId=CF41835F0319-4A16A178-1D27-A104-6EA8 rt=Sep 29 2018 09:43:58
```

```
GMT+08:00 app=DNS Response deviceDirection=1 dhost=10.201.22.80 dst=10.201.22.80
dpt=62129 dmac=e0:28:61:43:01:01 shost=192.168.95.2 src=192.168.95.2 spt=53
smac=60:08:10:df:1e:d1 cs3Label=HostName_Ext cs3=dtrp.url-quality.qq.com
fileType=-65536 fsize=0 act=not blocked cn3Label=Threat Type cn3=2
destinationTranslatedAddress=192.168.95.2 sourceTranslatedAddress=10.201.22.80
cnt=1 cat=Suspicious Traffic flexNumber1Label=vLANId flexNumber1=4095
```

处理方法参考

1. 利用文本处理工具将日志的 7 个头部域按照“|”符号换行处理，后面的部分则按照空格回车进行换行处理。



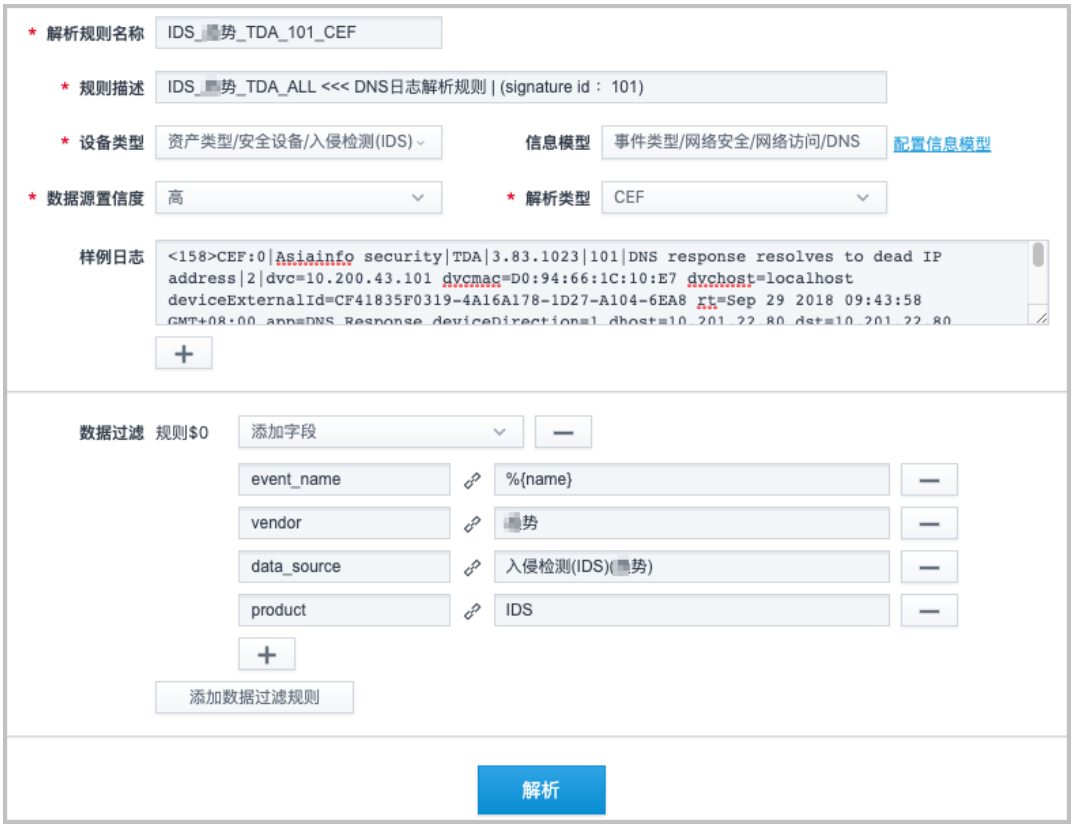
2. 将以上内容拷贝粘贴至 Excel 第一列。

1	<158>CEF:0|
2	Asiainfo security|
3	TDA|
4	3.83.1023|
5	101|
6	DNS response resolves to dead IP address|
7	2|
8	dvc=10.200.43.101
9	dvcmac=D0:94:66:1C:10:E7
10	dvchost=localhost
11	deviceExternalId=CF41835F0319-4A16A178-1D27-A104-6EA8
12	rt=Sep 29 2018 09:43:58 GMT+08:00
13	app=DNS Response
14	deviceDirection=1
15	dhost=10.201.22.80
16	dst=10.201.22.80
17	dpt=62129
18	dmac=e0:28:61:43:01:01
19	shost=192.168.95.2
20	src=192.168.95.2
21	spt=53 smac=60:08:10:df:1e:d1
22	cs3Label=HostName_Ext
23	cs3=dtrp.url-quality.qq.com

3. 除了 7 个头部域，将后面字段的值再处理，剪切至对应的第二列，参考《CEF 字段说明表》进行预处理。

	A	B	C
1	<158>CEF:0|		
2	Asiainfo security|		
3	TDA|		
4	3.83.1023|		
5	101|		
6	DNS response resolves to dead IP address|		
7	2|		
8	dvc	10.200.43.101	设备地址
9	dvcmac	D0:94:66:1C:10:E7	
10	dvchost	localhost	设备名称
11	deviceExternalId	CF41835F0319-4A16A178-1D27-A104-6EA8	
12	rt	Sep 29 2018 09:43:58 GMT+08:00	发生时间
13	app	DNS Response	
14	deviceDirection	1	
15	dhost	10.201.22.80	
16	dst	10.201.22.80	目的地址

基本内容说明



参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。
设备类型	根据待接入安全设备的类型选择。 *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 根据设备的作用，日志样例内容的初步审阅，这类日志大概率属于“**DNS**”类。 单击“**信息模型**”，可以跳转至“**模型管理**”页签下，自行丰富信息模型。

参数名称	参数说明
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 SAE 告警触发。 *示例中，字段“**event_name**”其引用为日志中的字段“**name**”。*

解析

步骤1. 单击“**解析**”，解析成功后，显示“**解析结果**”。

步骤2. 将“**索引字段**”抽取，根据显示的“**匹配结果**”以及信息模型提供的参考属性字段，输入“**固定字段**”。

鼠标选中输入框时，按键盘↑、↓会有提示：

- 信息模型中的“**必须属性**”以红色字体提示
- 信息模型中的“**可选属性**”以绿色字体提示
- 其他属性均以灰色字体显示

步骤3. 根据需要，单击“**添加映射**”，并选择“**映射类型**”，输入映射结果。

比如示例中，索引字段“**event_name**”引用了字段“**name**”，匹配结果为一句描述：“DNS response resolves to dead IP address”，而实际接入的日志该段内容并非固定、一成不变的，此时可以通过“**添加映射**”，使用“**正则**”的方式，

当该句描述以“**DNS reponse**”开头时，多数是“**DNS 响应异常**”。因此配置内容如下。

预览

单击“**预览**”，可预览解析规则的内容。

保存

预览解析规则无误后，可单击“**保存**”。保存成功后，在解析规则列表中查看到此条数据。

8.2.7 解析规则-JSON

经观察，待接入的厂家设备的日志均是 JSON 格式。可采用“**JSON**”这种解析类型来编辑解析规则。本章节以某厂商的 IDS 日志为例，介绍这类厂家、日志类型的解析方法。

JSON 格式

- 标准格式

```
{"ip":"192.168.100.100","port":1038,"mac":"00-50-ba-c1-f8-4e"}
```

- 格式化后

```
{
"ip":"192.168.100.100",
"port":1038,
"mac":"00-50-ba-c1-f8-4e"
}
```

样例日志

- 标准格式

```
{"dt":"VENUS IDS 0600R0700B20120821132212","level":40,"id":"152325010","type"
:"Alert
Log","time":1345873150110,"source":{"ip":"192.168.10.22","port":1038,"mac":"0
0-50-ba-c1-f8-4e"},"destination":{"ip":"192.168.10.30","port":5554,"mac":"00-
50-56-42-b9-eb"},"protocol":"TCP","subject":"TCP 震荡波蠕虫 FTP 后门 缓冲区溢出攻击
","message":"nic=1;"}
```

- 格式化后

```
{
  "dt":"VENUS_IDS_0600R0700B20120821132212",
  "level":40,
  "id":"152325010",
  "type":"Alert Log",
  "time":1345873150110,
  "source":{
     "ip":"192.168.10.22",
     "port":1038,
     "mac":"00-50-ba-c1-f8-4e"
  },
  "destination":{
     "ip":"192.168.10.30",
     "port":5554,
     "mac":"00-50-56-42-b9-eb"
  },
  "protocol":"TCP",
  "subject":"TCP_震荡波蠕虫 FTP 后门_缓冲区溢出攻击",
  "message":"nic=1;"
}
```

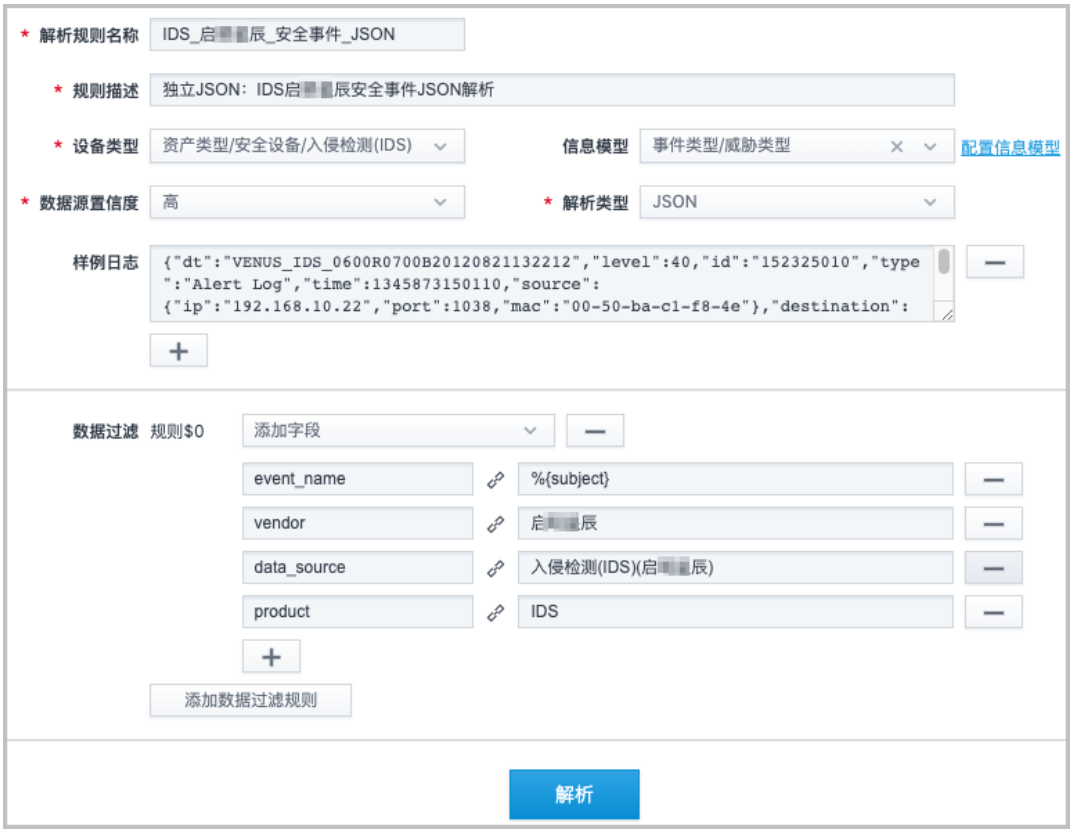
处理方法参考

通过格式化 JSON 格式字符串后，能够比较方便看出键和值之间的对应关系。

利用 Excel 将键和值的关系一一对应，从而做一个初步的预处理。

dt	设备名称	VENUS_IDS_0600R0700B20120821132212
level	事件级别	40
id		152325010
type	日志类型	Alert Log
time	发生时间	1345873150110
source	源地址、源端口、源MAC	"ip":"192.168.10.22","port":1038,"mac":"00-50-ba-c1-f8-4e"
destination	目的地址、目的端口、目的	"ip":"192.168.10.30","port":5554,"mac":"00-50-56-42-b9-eb"
protocol	协议	TCP_
subject	事件名称	TCP_震荡波蠕虫FTP后门_缓冲区溢出攻击
message	事件摘要	nic=1

基本内容说明



参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。

参数名称	参数说明
设备类型	根据待接入安全设备的类型选择。  *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 根据设备的作用，日志样例内容的初步审阅，这类日志大概率属于“**DNS**”类。 单击“**信息模型**”，可以跳转至“**模型管理**”页签下，自行丰富信息模型。
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 SAE 告警触发。  *示例中，字段“**event_name**”其引用为日志中的字段“**subject**”。*

解析

步骤1. 单击“**解析**”，解析成功后，显示“**解析结果**”。

步骤2. 将“**索引字段**”抽取，根据显示的“**匹配结果**”以及信息模型提供的参考属性字段，输入“**固定字段**”。

鼠标选中输入框时，按键盘↑、↓会有提示：

- 信息模型中的“**必须属性**”以红色字体提示
- 信息模型中的“**可选属性**”以绿色字体提示
- 其他属性均以灰色字体显示

步骤3. 根据需要，单击“**添加映射**”，并选择“**映射类型**”，输入映射结果。

比如示例中，索引字段“**event_name**”引用了字段“**subject**”，匹配结果为一句描述：“**TCP_震荡波蠕虫 FTP 后门_缓冲区溢出攻击**”，而实际接入的日志该段内容并非固定、一成不变的，此时可以通过“**添加映射**”，使用“**正则**”的方式，当匹配到相应的匹配值，则会显示对应的映射值。因此配置内容如下。

预览

单击“**预览**”，可预览解析规则的内容。

保存

预览解析规则无误后，可单击“**保存**”。保存成功后，在解析规则列表中查看到此条数据。

8.2.8 解析规则-不解析

“**不解析**”这种解析类型是不对日志进行解析，直接传输的一种过滤方式，一般应用于入口规则，会在字段过滤时走向子规则。

本章节以某网神下一代防火墙的日志为例，介绍这类厂家、日志如何应用此解析规则的。

日志说明

- 常规日志

  这类日志作为常用日志样例，它可能包含威胁的信息；但也可能不包含，就是网络连接、WEB 访问、DNS 查询、邮件收发、内容管理、设备状态类的日志。因此可以将它作为常规日志的样例，在后续数据过滤进行过滤再解析。

```
devid="3" dname="NSG" serial="7861cfc62ef545eedb09bbbc893e18930c2e5e22"
module="flow" severity="info" vsys="root-vsys" type="traffic-end"
session_id="667022" time="1553586639" addr_src="172.16.33.8"
addr_dst="140.205.94.189" nataddr_src="183.238.60.231" nataddr_dst="::"
natport_src="50754" natport_dst="0" proto="ICMP" hit_num="0" last_hit_num="0"
focus type="NO" from="" severity="" direction="" module="" action="permit"
session time="11783" sess nth="0" sess dev id="0" port src="1" port dst="2048"
user_src="" user_dst="" locale_src="内网" locale_dst="浙江省杭州市"
interface_src="s2xg1" interface_dst="s1ge3" zone_src="l3_trust" zone_dst="移动
800M" appname="ICMP" rule="办公内网访问外网-任意出口" profile=""
non standard port="NO" app category="APP NETWORK" app risk="1" asset os src=""
asset os dst="" asset name src="" asset name dst="" asset type src=""
asset type dst="" duration="30" bytes sent="160" bytes received="160"
pkts_sent="4" pkts_received="4" total_sess="0" from_tunnel="" to_tunnel=""
```

- 包含威胁提示的日志

  经过长期观察和经验积累，**type** 字段显示 **threat**，说明该类日志包含了威胁的相关信息，可以进一步解析，从而获取到日志中有用的其他信息，比如威胁类型、威胁的来源等。

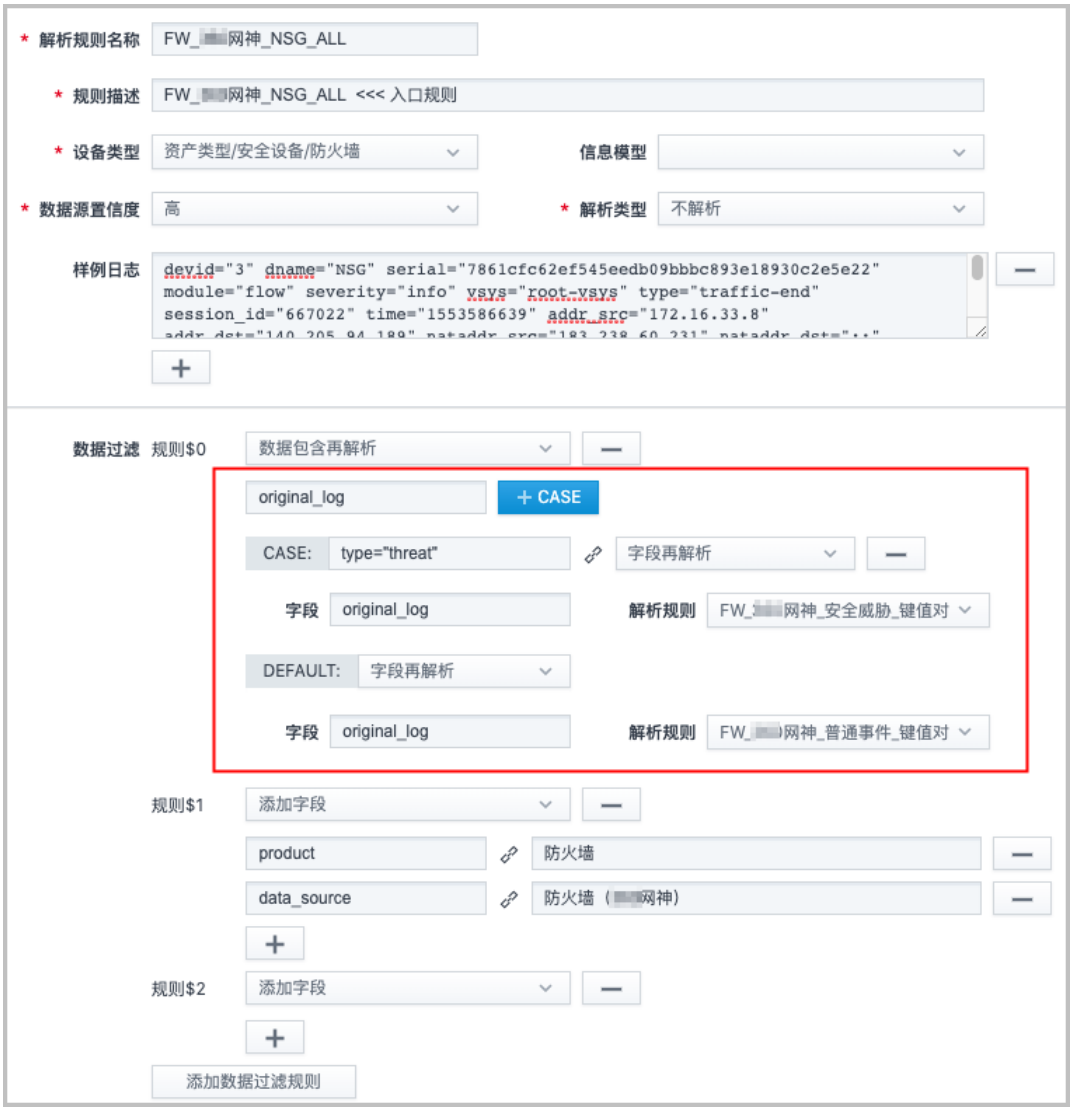
```
devid="3" dname="SecGateNSG"
serial num="103b8f2df90639e7f991c40e03927f99a2049272" type="threat"
time="1477901950" module="black" severity="warning" duration="0"
addr src="172.24.204.244" addr dst="172.24.200.114" port src="52953"
port dst="53" proto="UDP" nataddr src="::" nataddr dst="::" natport src="0"
natport dst="0" session id="0" session time="0" sess nth="0" sess dev id="0"
interface src="" interface dst="" zone src="" zone dst="" locale src="北京市朝
阳区 xx 科技园" locale dst="" user src="" user dst="" appname="APP-NONE"
action="drop" rule="" profile="" asset os src="" asset os dst=""
asset name src="" asset name dst="" asset type src="" asset type dst=""
app risk="5" app category="CATEGORY-NONE" focus type="NO" non standard port="1"
attacker ip="::" attack name="" victim ip="::" victim name="" sample name=""
threat name="Malicious Connection Request" threat id="80043" direction="C2S"
threat class="other" threat type="Addresses black list" threat severity="high"
sample md5="" sample type="" detect method="" malicious type="" file name=""
file_path="172.24.204.244"
```

- 普通类型的日志

  这类信息就相对普通，整合网络连接、WEB 访问、DNS 查询、邮件收发、内容管理、设备状态等日志，正常按照“**键值对**”的方式去解析即可。

```
sample md5="" dns domain="" dns ttl="" dns host="" behavior proto="" user dst=""
url category="" asset os src="" time="" rule="" filetype="" interface src=""
devid="" natport src="" total sess="" duration="" filename="" threat class=""
threat type="" natport dst="" locale src="" non standard port="" file path=""
addr src="" asset name src="" threat name="" real receiver="" victim name=""
behavior commond="" msg="" threat severity="" malicious type="" serial num=""
dns cname="" victim ip="" profile="" sample name="" sess nth=""
asset type dst="" app risk="" asset name dst="" bytes sent="" attack name=""
attacker ip="" bytes received="" keyword="" asset type src="" zone src=""
mail to="" session id="" action="" module="" user src="" port dst="" msg cn=""
addr dst="" focus type="" type="" pkts sent="" detect method="" port src=""
file name="" from tunnel="" nataddr src="" zone dst="" mail date="" dns type=""
url sub type="" severity="" sample type="" dname="" direction="" mail cc=""
nataddr dst="" proto="" pkts received="" interface dst="" app category="" url=""
serial="" sess dev id="" threat id="" appname="" locale dst="" session time=""
url content type="" mail from="" hit num="" to tunnel="" content type=""
asset_os_dst="" mail_subject=""
```

不解析的入口规则



参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。

参数名称	参数说明
设备类型	根据待接入安全设备的类型选择。 *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 这里是一个入口规则，可选择不配置。更多字段的解析可以走向子规则，提供更多的解析作用。
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。 此处选择不解析
样例日志	输入需要解析的样例日志信息。 输入常规日志样例

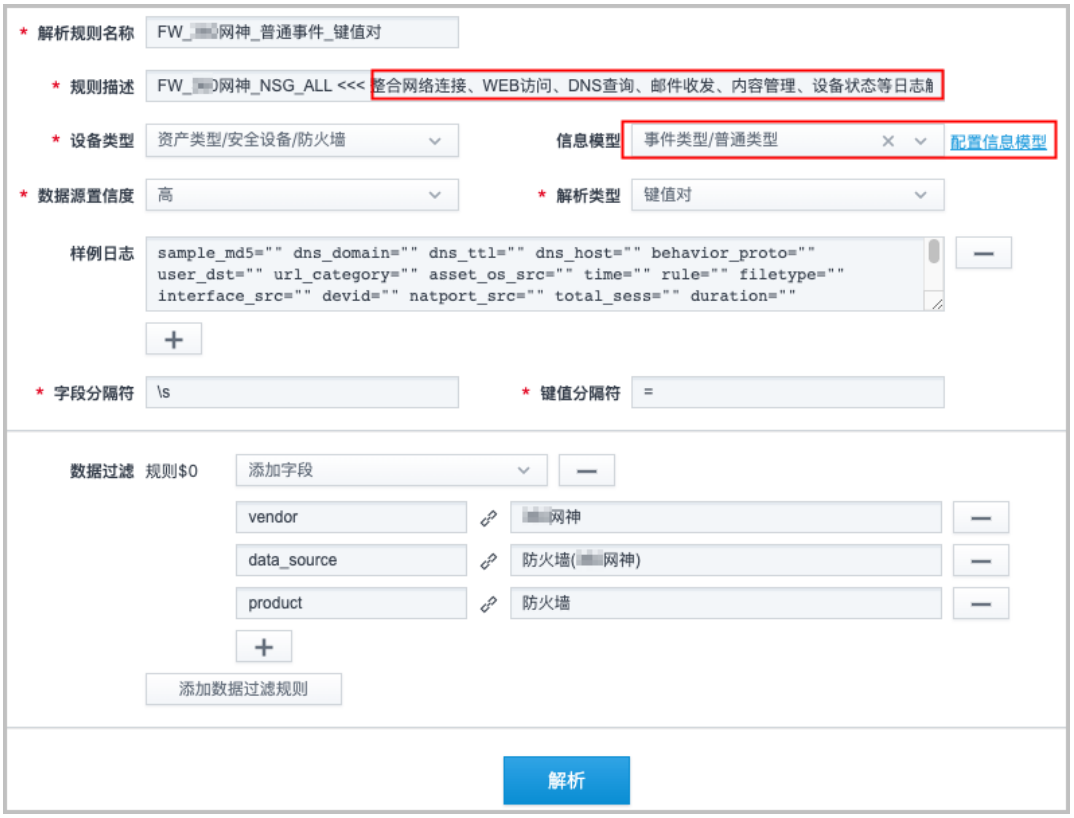
参数名称	参数说明
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 SAE 告警触发。 *示例中，选择“**数据包含再解析**”，新建字段“**original_log**”，谈及添加 CASE。* • *当 CASE 中出现 **type 为 threat**，则进行“**字段再解析**”，接入的日志会走向子规则“**FW_某网神_安全威胁_键值对**”* • *而默认情况是走向子规则“**FW_某网神_普通事件_键值对**”。*

子规则-安全威胁类

参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。
设备类型	根据待接入安全设备的类型选择。 *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 根据日志样例内容的初步审阅，将这类日志配置为“**威胁类型**”类。 单击“**信息模型**”，可以跳转至“**模型管理**”页签下，自行丰富信息模型。

参数名称	参数说明
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。 输入带有 **threat** 的日志样例。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 SAE 告警触发。 *示例中，示例中，字段“**event_name**”其引用为日志中的字段“**threat_name**”。*

子规则-普通事件



参数名称	参数说明
规则名称	解析规则名称信息。
规则描述	解析规则描述。
设备类型	根据待接入安全设备的类型选择。 *为匹配 SAE 规则检测的要求，界面内置了 10 种**设备类型**与**五元组（product 字段）**一一对应。* *比如，“**设备类型**”选择“**防火墙**”后，在“**字段过滤**”下创建字段“**product**”，则可在下拉列表中选择“**防火墙**”，避免自定义为“**firewall**”等，导致 SAE 检测误报。*
信息模型	可选配置参数。如若配置此参数，则解析后的字段会根据模型提供可参考的属性字段以供填写。 根据日志样例内容的初步审阅，将这类日志配置为“**普通类型**”类。 单击“**信息模型**”，可以跳转至“**模型管理**”页签下，自行丰富信息模型。

参数名称	参数说明
数据源置信度	定义对此解析规则的置信度，包括：**高、中、低**三个选项。 当该厂家、设备、日志较稳定，质量较高时，可以选择“**高**”。为后续的安全分析提供判断依据。
解析类型	根据待解析的日志格式，选择解析类型。
样例日志	输入需要解析的样例日志信息。
添加数据过滤规则	建议必配 5 元组，包括以下字段： • **event_name（事件名称）**：有必要参考 SIM 事件名称做好映射。可使用固定值或者引用变量“%{xxx}” • **event-level（事件级别）**：有必要映射使用固定值或者引用变量“%{xxx}” • **product（产品）**：为综合 SAE 规则检测需求，固定名称配置涉及 10 种：防火墙、WAF、IDS、IPS、EDR、NDR、Email 安全网关、Web 安全网关、EPP、DLP。 • **data_source（数据源）**：固定配置值，例如：EDR(360)。**注意**：此处必须为英文格式的括号。 • **vendor（厂商）** 如若这些字段不存在，则会影响到后续 SAE 告警触发。

8.3 数据接入管理

日志通过各类的采集形式（网络、syslog、本地等），经过工作节点将日志发送到报送设备，对应适合的解析规则对采集的日志进行处理。

当配置中需要填写 IP 时，请确保网络之间互通，否则请设置相应的防火墙策略，保证数据正常传递，否则将被拦截。

8.3.1 配置前说明

根据数据源写入的方式不同，采集类型包括以下几种选项：

- 本地服务
  - **网络**：适用于将日志以网络形式传输到采集器上，支持上传 nta 等脚本。
  - **数据库**：适用于将日志保存在数据库中的数据表。
  - **KAFKA**：适用于读取 KAFKA 系统中的数据。

- **HDFS**（Hadoop 分布式文件系统）：适用于将日志以文件的形式保存在 HDFS 系统上。
- **SFTP**（SSH File Transfer Protocol，安全文件传送协议）：适用于将日志以文件的形式保存在 SFTP 服务器上。
- **数据接收**：适用于采集 LAS 系统内部已解析的日志。
- **WMI**（Windows Management Instrumentation，Windows 管理规范）：适用于采集 Windows 服务器的日志。
- **SNMP**（Simple Network Management Protocol，简单网络管理协议）：适用于 walk 方式采集简单网络管理协议提供访问的日志。

- 云服务

  AWS（Amazon Web Services）：适用于将日志以文件的形式保存在 AWS 上。

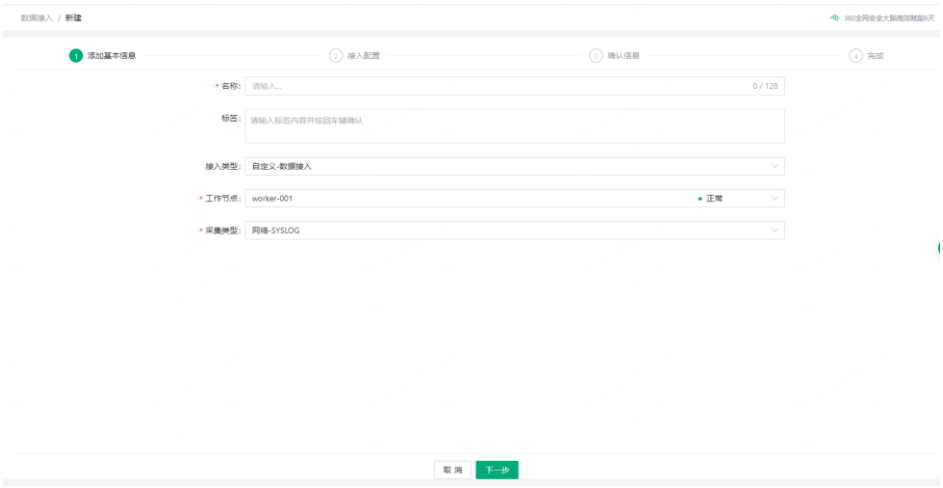
8.3.2 配置基本信息

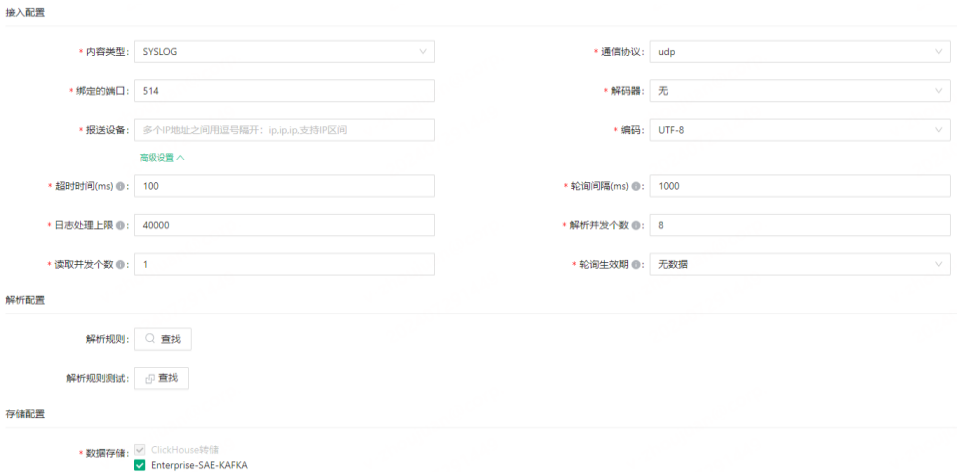
操作步骤

步骤1. 在导航栏单击，选择“**数据接入** > **数据接入**”，LAS 系统默认显示“**数据源**”页面。

步骤2. 单击“**新增**”，显示新增页面如图 8-4 所示。

图8-4 数据源基本信息





参数如表 8-10 所示。

表8-10 参数说明

参数名称	参数说明
名称	数据源名称信息，允许输入 1~64 个字符。
工作节点	在下拉列表中选择数据源工作的节点，默认选择第一个节点。
采集类型	数据源写入的方式，包括以下几种选项： • 本地文件或目录 • 网络 • 数据库 • KAFKA • HDFS • AWS • SFTP • 数据接收 • WMI • SNMP • ELASTICSEARCH
高级设置 *通常保持缺省配置，请根据实际场景需求修改。*	
超时时间（ms）	一次采集的最大等待时长。单位：ms。
轮询间隔（ms）	采集间隔的时间。单位：ms。

参数名称	参数说明
日志处理上限	处理日志的最大值。单位：条。
解析并发个数	为每个读取实例分配的解析实例个数。
读取并发个数	同时读取的实例个数。
轮询生效期	轮询生效期包括以下两个选项： • 无接收数据时：缺省选项。 • 数据源接收时： – 当采集类型为“SNMP”时，请选择该轮询方式。 – 当采集类型为“WMI”且“采集对象”为状态类型的对象时，请选择该轮询方式。
解析规则	显示关联的解析规则，非必选。未选择时默认初始化规则不解析数据。 单击可弹出“**解析规则测试**”窗口，输入“**日志样例**”，单击“**检测**”可模糊匹配出可能适用的解析规则以供选择。
数据存储	数据存储的类别。 请通过勾选选择。

8.3.3 采集类型为“本地文件或目录”

操作步骤

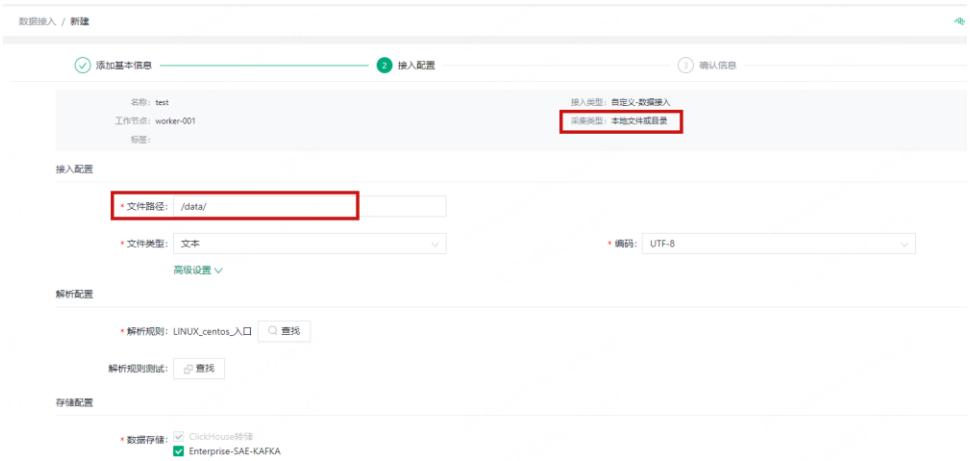
步骤1. 选择“**采集类型**”为“**本地文件或目录**”。

步骤2. 点击“**下一步**”。

步骤3. 填写“**文件路径**”，即输入存放文件的位置，绝对路径，可指定到具体文件，默认为：/data/。

注意：对应的放在服务器的/opt/qihoo/soc/dataviewer/worker/data/目录下。

步骤4. 文件类型默认为“**文本**”，并且支持 zip 和 gzip 打包格式，在下拉列表中选择文件的格式编码，如“**UTF-8**”。



步骤5.　高级设置保持缺省值。

8.3.4 采集类型为“网络”

操作步骤

步骤1.　选择“**采集类型**”为“**网络**”。

步骤2.　选择“**内容类型**”和“**解码器**”，参数说明如下表所示。

参数名称	参数说明
内容类型	在下拉列表中选择采集的方式，包括以下选项： • SYSLOG • SNMP-TRAP • netflow-NETFLOW
解码器	在下拉列表中选择解码器的类型，包括以下选项： • 空 • 单行 • 多行 • 分隔符 • 脚本

- 选择“**解码器**”为“**无**”或“**单行**”，配置页面如下图所示。

参数说明如下图所示。

参数名称	参数说明
报送设备	输入报送设备，即数据源的 IP 地址。
绑定的端口	输入发到采集器上的端口号，即采集器的监听端口号。 • SYSLOG 默认端口：514。 • SNMP-TRAP 默认端口：162。 • netflow-NETFLOW 默认端口：9293。
编码	在下拉列表中选择文件的格式编码。

- 选择“**解码器**”为“**多行**”，配置页面如下图所示。

参数说明如下表所示。

参数名称	参数说明
是否从开头匹配	选择是否从开头匹配开始，包括以下选项： • 是 • 否
正则	输入正则表达式。
报送设备	输入报送设备，即数据源的 IP 地址。
绑定的端口	输入发到采集器上的端口号，即采集器的监听端口号。
编码	在下拉列表中选择文件的格式编码。

- 选择“**解码器**”为“**分隔符**”，配置页面如下图所示。

参数说明如下图所示。

参数名称	参数说明
分隔符	输入分隔符。
报送设备	输入报送设备，即数据源的 IP 地址。
绑定的端口	输入发到采集器上的端口号，即采集器的监听端口号。
编码	在下拉列表中选择文件的格式编码。

- 选择“**解码器**”为“**脚本**”，配置页面如下图所示。

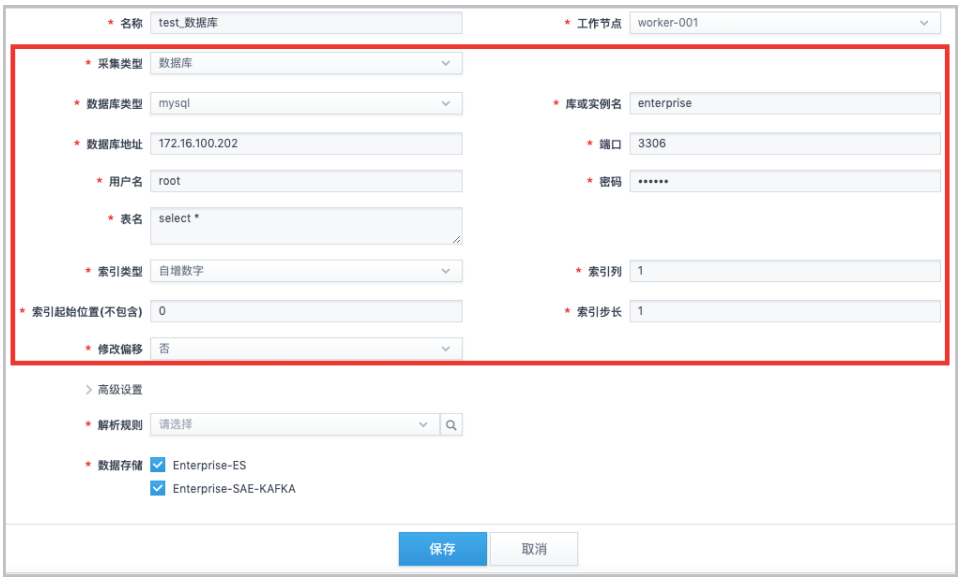
参数说明如下表所示。

参数名称	参数说明
脚本选择	在下拉列表中，选择脚本，包括两种方式： • nta，默认内置脚本。 • 单击“选择脚本”，手动上传脚本文件。
报送设备	输入报送设备，即数据源的 IP 地址。
绑定的端口	输入发到采集器上的端口号，即采集器的监听端口号。
编码	在下拉列表中选择文件的格式编码。

8.3.5 采集类型为“数据库”

操作步骤

步骤1. 选择“**采集类型**”为“**数据库**”，需配置的参数如下图所示。



参数说明如下表所示。

参数名称	参数说明
数据库类型	在下拉列表中选择数据库类型，包括以下选项： • mysql • oracle • sqlserver-default • DB2 • postgresql • sqlsever-域账户认证
库或实例名	输入需要解析的数据库名或实例名。
数据库地址	数据库所在的 IP 地址。
端口	数据库的端口，请与实际数据库的开放端口保持一致。
用户名	用于连接数据库的用户名。
密码	用于连接数据库的密码。
表	需要解析的数据表名。

参数名称	参数说明
索引类型	在下拉列表中选择索引的类型，包括以下选项： • 自增数字 • 时间类型
索引列	当做索引的列名，建议是日期或 id 的字段列。
索引起始位置（不包含）	索引列读取数据的起始位置。 *不包含本身，建议向前写一位。* • 当索引类型为“**自增数字**”时，该值只能设置为数字。 • 当索引类型为“**时间类型**”时，该值格式为“yyyy-MM-dd HH:mm:ss.S”。
索引步长	• 当索引类型为“**自增数字**”时，该值最大为 300000。 • 当索引类型为“**时间类型**”时，该值单位为秒，最大值为 600。
修改偏移	在下拉列表中选择是否偏移。 • 是：从文件开头开始读。 • 否：上次读取到的地方读。

步骤2. 高级设置保持缺省值。

8.3.6 采集类型为“KAFKA”

操作步骤

步骤1. 选择“**采集类型**”为“**KAFKA**”。

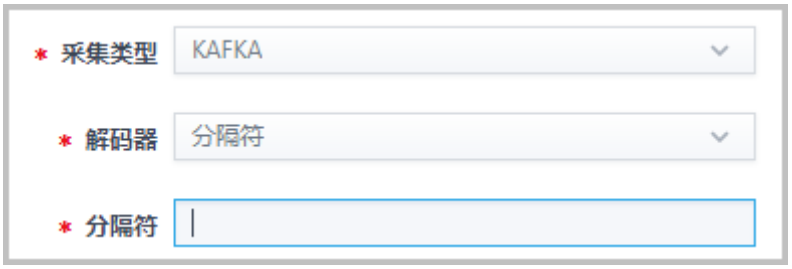
步骤2. 在下拉列表中选择解码器类型。

- 选择“**解码器**”为“**无**”或“**单行**”，请继续执行步骤 3。
- 选择“**解码器**”为“**多行**”，配置参数如下图所示。

参数说明如下表所示。

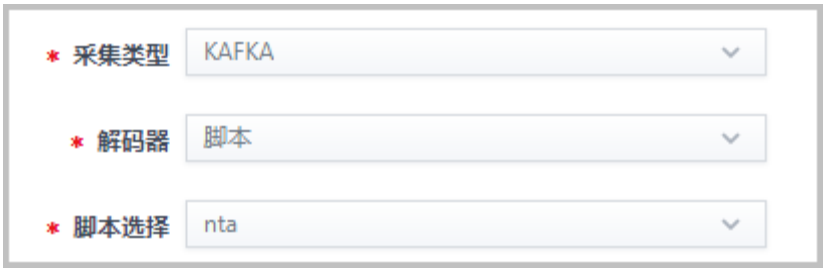
参数名称	参数说明
是否从行首开始	选择是否从行首匹配开始，包括以下选项： • 是 • 否
正则	输入正则表达式。

- 选择“**解码器**”为“**分隔符**”，输入“**分隔符**”参数，配置页面如下图所示。



- 选择“**解码器**”为“**脚本**”，配置页面如下图所示。

  在下拉列表中，选择脚本，包括两种方式：
  - nta，默认内置脚本。
  - 单击“**选择脚本**”，手动上传脚本文件。



步骤3. 配置基本参数，配置页面如下图所示。

参数说明如下表所示。

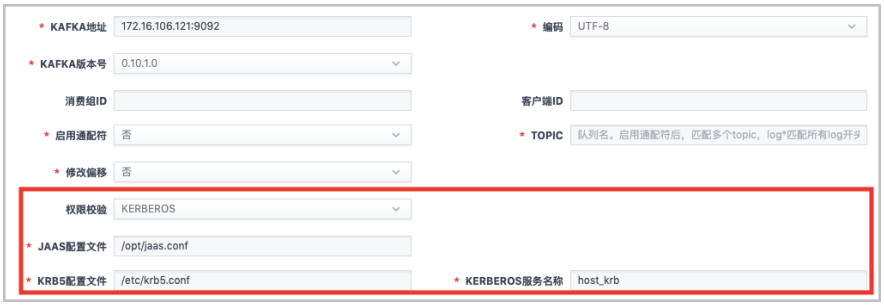
参数名称	参数说明
KAFKA 地址	KAFKA 的地址，格式为“IP:端口”。
编码	在下拉列表中选择文件的格式编码。
kafka 版本号	在下拉列表中选择 KAFKA 的版本号
消费组	输入消费组的 ID。
客户端 ID	输入客户端的 ID。
启用通配符	选择是否启用通配符，包括以下选项： • 是 • 否
TOPIC	对列名。 当启用通配符后，匹配多个 topic。如 log*则匹配所有 log 开头的 topic。
修改偏移	在下拉列表中选择是否偏移。 • 是：从文件开头开始读。 • 否：上次读取到的地方读。
权限校验	在下拉列表中选择权限校验的方式。 • 无：无需权限校验 • PLAIN • KERBEROS • SSL

- 校验类型为“**无**”时，配置页面无新增参数。
- 校验类型为“**PLAIN**”时，配置页面如下图所示。

新增的参数说明如下表所示。

参数名称	参数说明
JAAS 配置文件	输入 JAAS 配置文件 【示例】 /opt/jaas.conf *请将 JAAS 配置文件先存放在使用的 DCC worker 所在的服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*

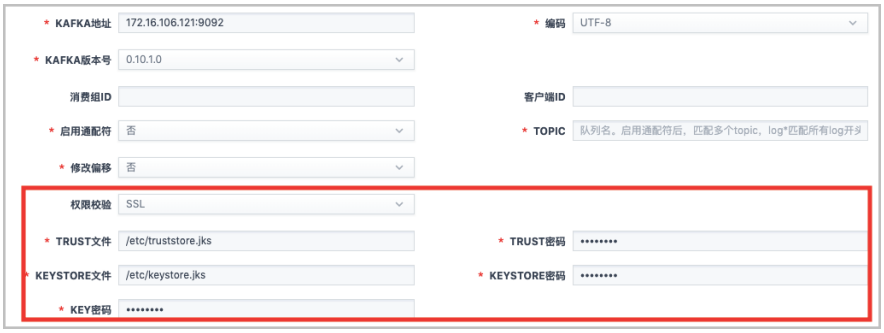
- 校验类型为“**KERBEROS**”时，配置页面如下图所示。



新增的参数说明如下表所示。

参数名称	参数说明
JAAS 配置文件	输入 JAAS 配置文件。 【示例】 /opt/jaas.conf *请将 JAAS 配置文件先存放在使用的 DCC worker 所在的服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KRB5 配置文件	输入 KRB5 配置文件。 【示例】 /etc/krb5.conf *请将 KRB5 配置文件先存放在使用的 DCC worker 所在的服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KERBEROS 服务器名称	输入 KERBEROS 服务器的名称。

- 校验类型为“**SSL**”时，配置页面如下图所示。



新增的参数说明如下表所示。

参数名称	参数说明
TRUST 文件	输入 TRUST 文件。 【示例】 /etc/truststore.jks *请将 TRUST 文件先存放在使用的 DCC worker 所在的服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
TRUST 密码	输入 TRUST 密码。
KEYSTORE 文件	输入 KEYSTORE 文件。 【示例】 /etc/keystore.jks *请将 KEYSTORE 文件先存放在使用的 DCC worker 所在的服务器。此处输入的路径与文件名必须与实际存放的路径和文件名保持一致。*
KEYSTORE 密码	输入 KEYSTORE 密码。
KEY 密码	输入 KEY 的密码。

步骤4.　高级设置保持缺省值。

8.3.7 采集类型为“HDFS”

操作步骤

步骤1.　选择“**采集类型**”为“**HDFS**”。

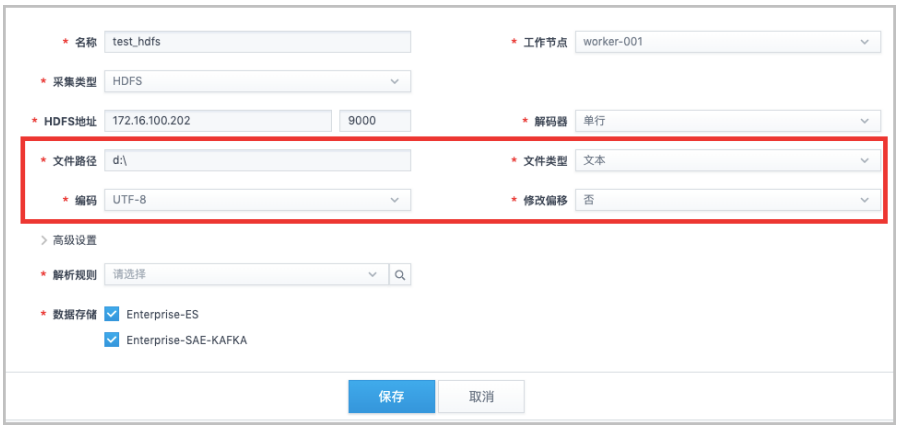
步骤2. 输入“**HDFS 地址**”，在下拉列表中选择“**解码器**”，参数说明如下表所示。

参数名称	参数说明
HDFS 地址	输入 HDFS 的地址和端口号。
解码器	在下拉列表中选择解码器的类型，包括以下选项： • 单行 • 多行 • 分隔符

步骤3. 填写“**HDFS 地址**”的 IP 地址和端口号。

步骤4. 配置解码器。

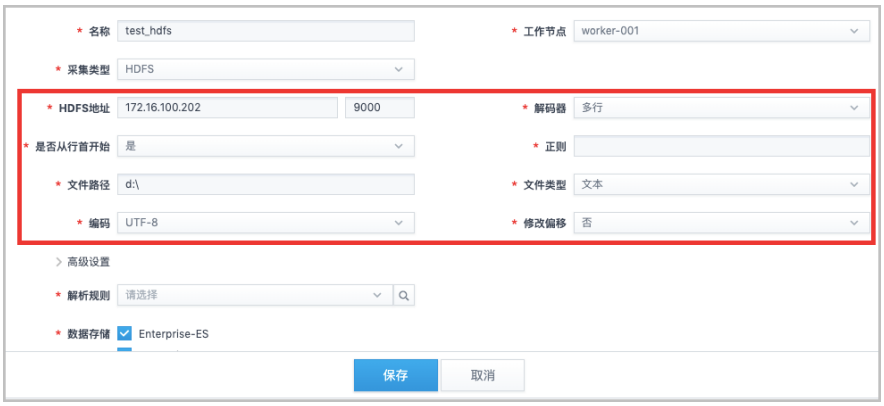
- 选择“**解码器**”为“**单行**”，配置页面如下图所示。



参数说明如下图所示。

参数名称	参数说明
文件路径	输入文件路径的绝对路径。
文本类型	在下拉列表中选择“**文本**”。
编码	在下拉列表中选择文件的格式编码。
修改偏移	在下拉列表中选择是否偏移。 • 是：从文件开头开始读。 • 否：上次读取到的地方读。

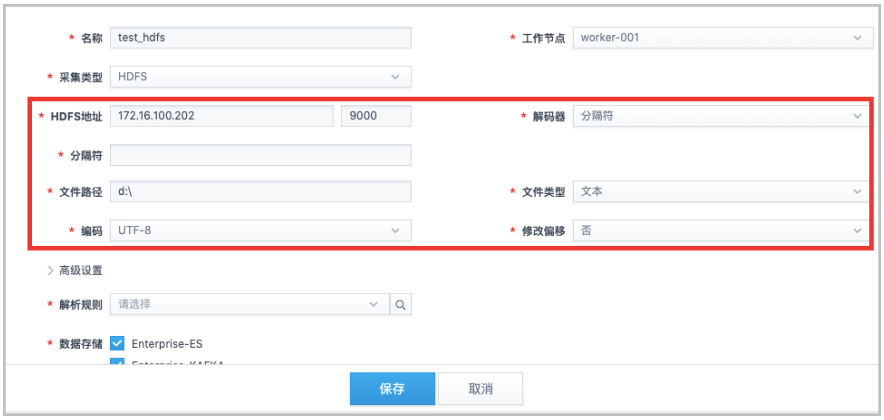
- 选择“**解码器**”为“**多行**”，配置页面如下图所示。



参数说明如下表所示。

参数名称	参数说明
是否从行首开始	选择每条数据是否从行首开始，包括以下选项： • 是 • 否
正则	输入正则表达式。
文件路径	输入文件路径的绝对路径
文件类型	默认为“**文本**”。
编码	在下拉列表中选择文件的格式编码。
修改偏移	在下拉列表中选择是否偏移。 • 是：从文件开头开始读。 • 否：上次读取到的地方读。

- 选择“**解码器**”为“**分隔符**”，配置页面如下图所示。



参数说明如下表所示。

参数名称	参数说明
分隔符	输入分隔符。
文件路径	输入文件路径的绝对路径
文件类型	默认为“**文本**”。
编码	在下拉列表中选择文件的格式编码。
修改偏移	在下拉列表中选择是否偏移。 • 是：从文件开头开始读。 • 否：上次读取到的地方读。

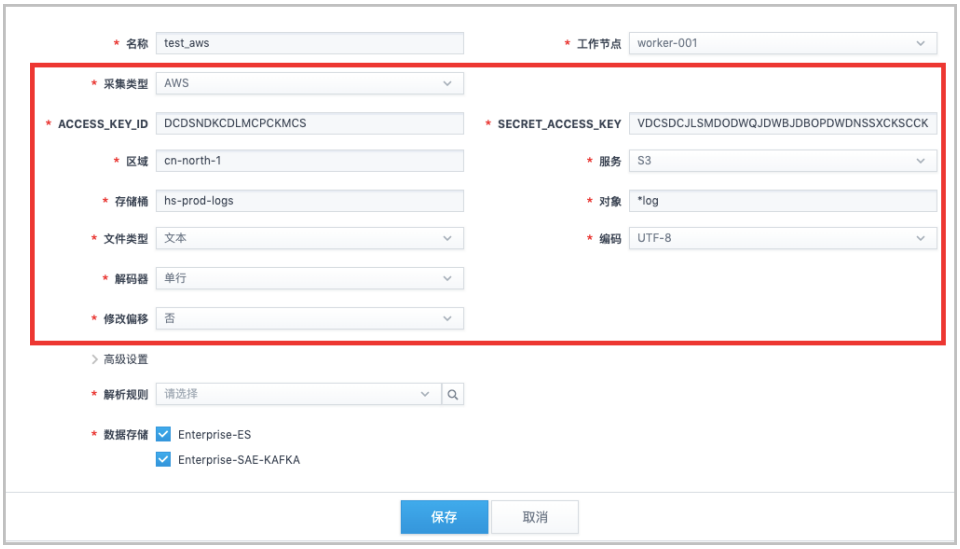
步骤5. 高级设置保持缺省值。

8.3.8 采集类型为“AWS”

操作步骤

步骤1. 选择“**采集类型**”为“**AWS**”。

步骤2. 配置以下连接 AWS 的参数。



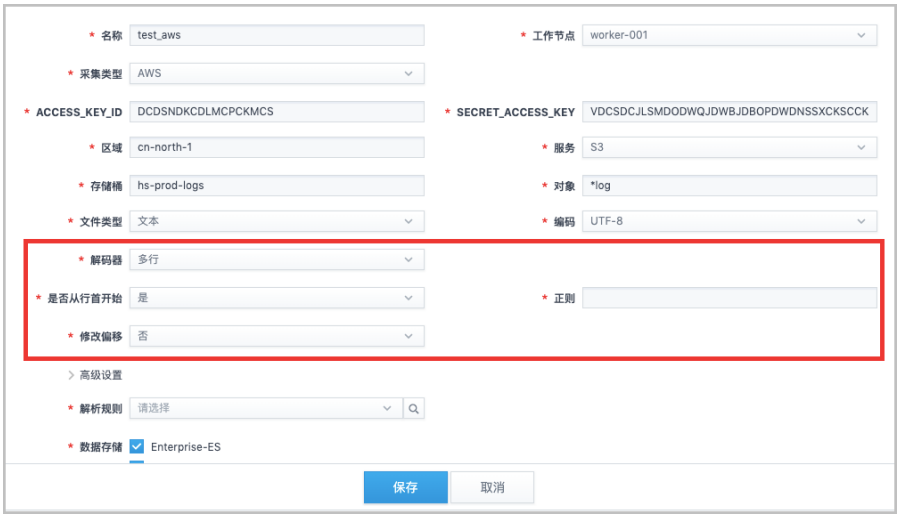
参数说明如下。

参数名称	参数说明
ACCESS_KEY_ID	用于连接 AWS 的 ACCESS_KEY_ID。
SECRET_ACCESS_KEY	用于连接 AWS 的 SECRET_ACCESS_KEY。
区域	用于连接 AWS 的 Location。

参数名称	参数说明
服务	在下拉列表中选择服务“**S3**”。
存储桶	存储在 S3 的 Bucket 名称。
对象	存储在相应 Bucket 中 Object。
文件类型	在下拉列表中选择文本类型，包括： • 文本 • 文本(GZ)
编码	在下拉列表中选择文件的格式编码。
解码器	在下拉列表中选择解码器的类型，包括以下选项： • 单行 • 多行 • 分隔符

步骤3. 配置解码器。

- 选择“**解码器**”为“**单行**”，页面无新增参数。选择是否偏移即可。
- 选择“**解码器**”为“**多行**”，配置页面如下图所示。

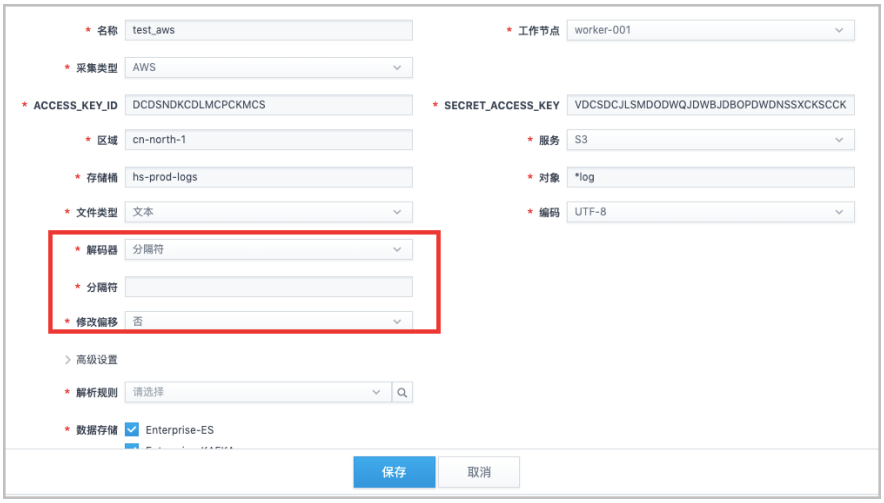


参数说明如下表所示。

参数名称	参数说明
是否从行首开始	选择每条数据是否从行首开始，包括以下选项： • 是 • 否
正则	输入正则表达式。

参数名称	参数说明
修改偏移	在下拉列表中选择是否偏移，包括以下选项： • 是 • 否

- 选择“**解码器**”为“**分隔符**”，配置页面如下图所示。



参数说明如下表所示。

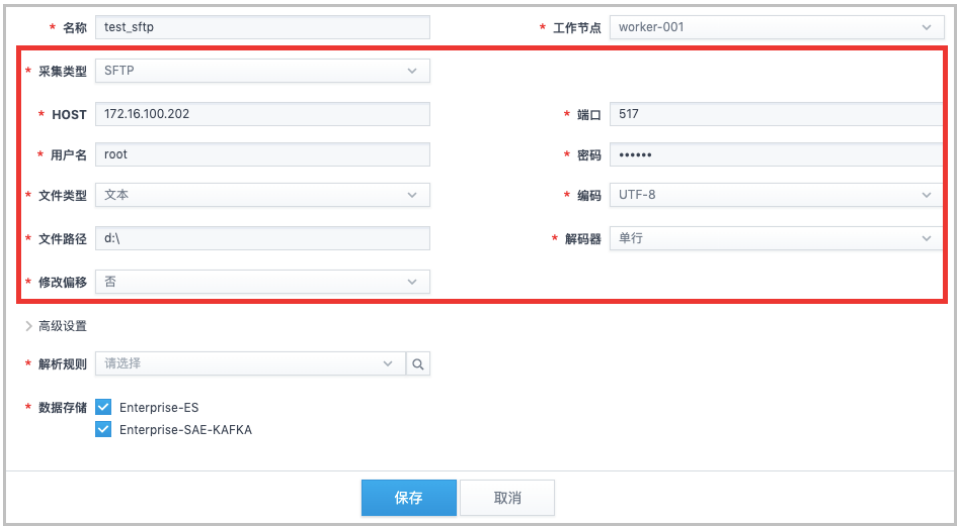
参数名称	参数说明
分隔符	输入分隔符。
是否偏移	在下拉列表中选择是否偏移，包括以下选项： • 是：从文件开头开始读。 • 否：从上一次采集的位置继续采集。

8.3.9 采集类型为“SFTP”

操作步骤

步骤1. 选择“**采集类型**”为“**SFTP**”。

步骤2. 输入 SFTP 服务器的 IP 地址和端口，配置页面如下。



参数说明如下表所示。

参数名称	参数说明
HOST	输入 SFTP 服务器的地址。
端口	输入 SFTP 服务器的端口号。
用户	用于连接 SFTP 服务器的用户名。
密码	用于连接 SFTP 服务器的密码。
文本类型	在下拉列表中选择文本。
编码	在下拉列表中选择文件的格式编码。
文件路径	输入文件路径的绝对路径。
解码器	在下拉列表中选择解码器的类型，包括以下选项： • 单行 • 多行 • 分隔符

步骤3. 配置解码器。

- 选择“**解码器**”为“**单行**”，配置页面如下图所示。

参数说明如下图所示。

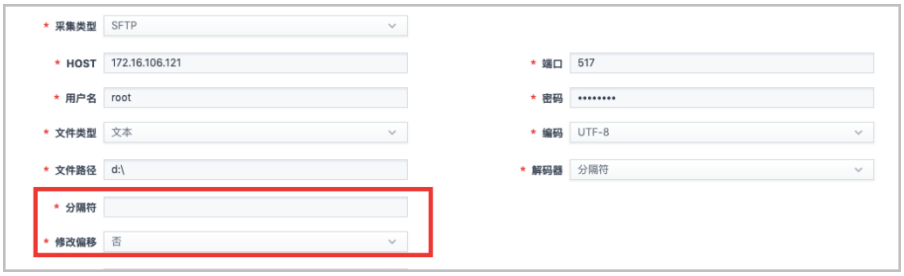
参数名称	参数说明
是否偏移	在下拉列表中选择是否偏移，包括以下选项： • 是：从文件开头开始读。 • 否：从上一次采集的位置继续采集。

- 选择“**解码器**”为“**多行**”，配置页面如下图所示。

参数说明如下表所示。

参数名称	参数说明
是否从行首开始	选择每条数据是否从行首开始，包括以下选项： • 是 • 否
正则	输入正则表达式。
是否偏移	在下拉列表中选择是否偏移，包括以下选项： • 是：从文件开头开始读。 • 否：从上一次采集的位置继续采集。

- 选择“**解码器**”为“**分隔符**”，配置页面如下图所示。



参数说明如下表所示。

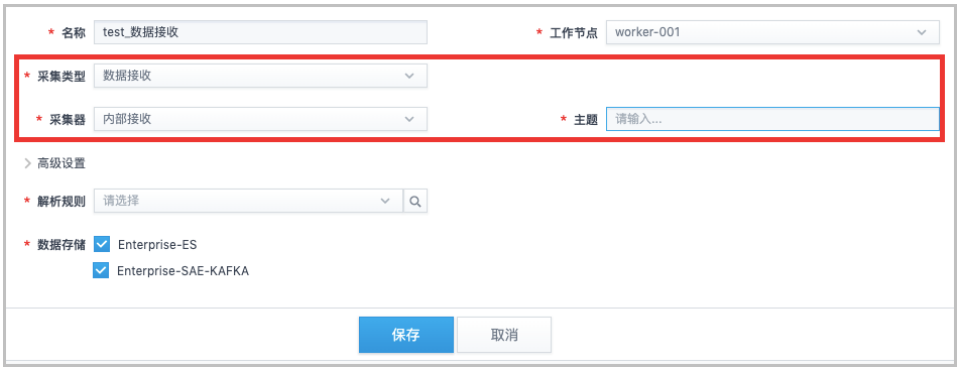
参数名称	参数说明
分隔符	输入分隔符。
是否偏移	在下拉列表中选择是否偏移，包括以下选项： • 是：从文件开头开始读。 • 否：从上一次采集的位置继续采集。

步骤4. 高级设置保持缺省值。

8.3.10 采集类型为“数据接收”

操作步骤

步骤1. 选择“**采集类型**”为“**数据接收**”，配置页面如下。



参数说明如下表所示。

参数名称	参数说明
采集器	选择采集器，包括以下选项： • 内部接收 • DCC worker 节点。
主题	消息队列的名称。即采集该主题下的数据。

步骤2. 高级设置保持缺省值。

8.3.11 采集类型为“WMI”

使用 WMI 采集 Windows 操作系统数据，包括时间类型和状态类型两类采集对象。

时间类型包括 NTLogEvent，状态类型包括：

- Process

- ComputerSystem
- UserAccount
- ShortCutFile

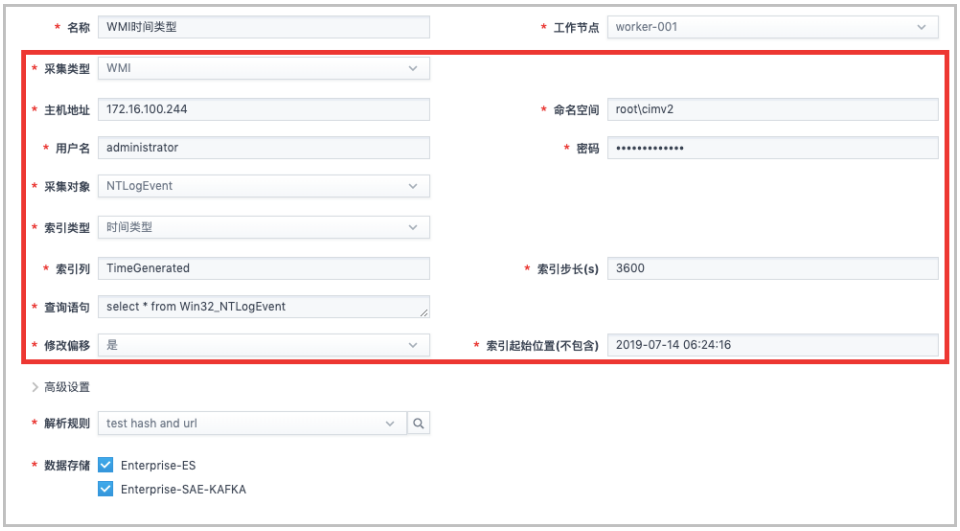
您也可以自定义采集对象，根据实际采集对象，选择索引类型，请根据以下索引类型，配置 WMI 数据源的参数。

前提条件

在配置 WMI 采集类型的数据源前，您需要开启 WMI 配置。

索引类型为“时间类型”的采集对象

步骤1. 选择“**采集类型**”为“**WMI**”，配置页面如下。



配置参数说明如下。

参数名称	参数说明
主机地址	待采集数据的 windows 操作系统远程服务器的 IP。 仅支持采集一台主机，请勿填写多个 IP 地址。
命名空间	与 D.1.2 在本机测试是否可以连接远程主机 WMI 服务的步骤 4 中的缺省命名空间保持一致。 【示例】 root\cimv2
用户名	登录 Windows 系统的用户名。与 D.1.2 在本机测试是否可以连接远程主机 WMI 服务的步骤 4 中“用户名”保持一致。 可使用默认账号 Administrator，亦可使用其他自定义账号。
密码	登录 Windows 系统的用户的密码。

参数名称	参数说明
采集对象	采集对象包括以下选项： • NTLogEvent • 自定义其他时间类型的对象。
索引类型	• 若“**采集对象**”选择“**NTLogEvent**”，索引类型自动关联为“**时间类型**”。 • 若“**采集对象**”选择“**自定义**”，在下拉选项中选择“**时间类型**”。
索引列	• 若“**采集对象**”选择“**NTLogEvent**”，索引的列名，自动关联为“**TimeGenerated**”。 • 若“**采集对象**”选择“**自定义**”，需手动输入索引列，即查询对象的具体时间字段名称。
索引步长	索引步长缺省为 3600，单位为秒。表示 1 小时的每次轮询的查询时间段。
查询语句	• 若“**采集对象**”选择“**NTLogEvent**”，自动关联 select 查询语句，采集对象选择为 NTLogEvent，查询语句自动关联为“select * from Win32_NTLogEvent”。 • 若“**采集对象**”选择“**自定义**”，需手动输入 select 查询语句，查询相应对象。
修改偏移	包括以下选项： • 是：从文件开头开始读。 • 否：从上一次采集的位置继续采集。
索引起始位置（不包含）	当选择为“**是**”，设置索引起始的时间。

步骤2. 打开“**高级设置**”，设置高级参数。

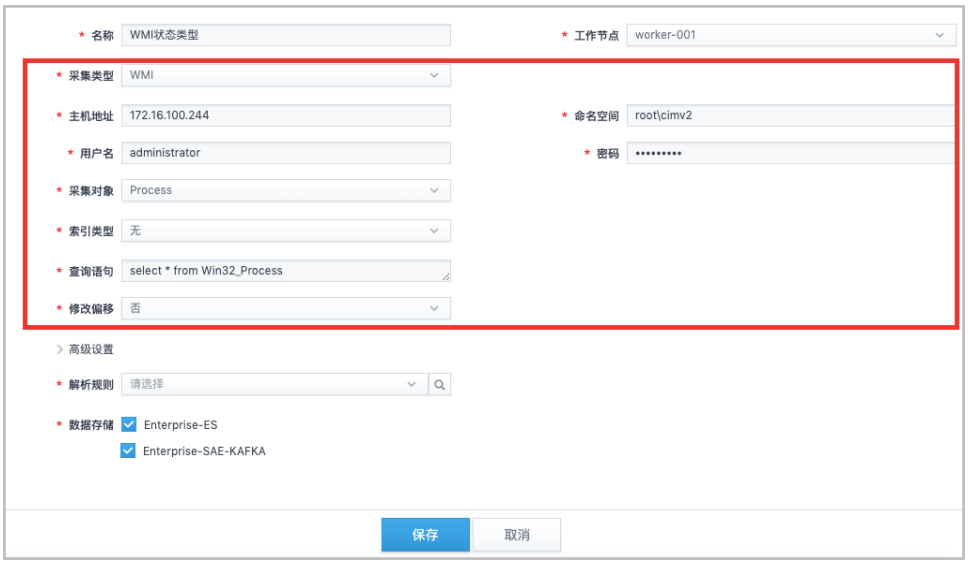
参数说明如下所示。

参数名称	参数说明
超时时间（ms）	一次采集的最大等待时长。单位：ms。
轮询间隔（ms）	采集间隔的时间。单位：ms。

参数名称	参数说明
日志处理上限	处理日志的最大值。单位：条。
解析并发个数	为每个读取实例分配的解析实例个数。
读取并发个数	同时读取的实例个数。
轮询生效期	轮询生效期包括以下两个选项： • 无数据。 • 数据源接收时 当索引类型为“**时间类型**”时，选择“**无数据**”。

索引类型为“状态类型”的采集对象

步骤1. 选择“**采集类型**”为“**WMI**”，配置页面如下。



配置参数说明如下。

参数名称	参数说明
主机地址	待采集数据的 windows 操作系统远程服务器的 IP。 仅支持采集一台主机，请勿填写多个 IP 地址。
命名空间	与 D.1.2 在本机测试是否可以连接远程主机 WMI 服务的步骤 4 中的缺省命名空间保持一致。 【示例】 root\cimv2
用户名	登录 Windows 系统的用户名。与 D.1.2 在本机测试是否可以连接远程主机 WMI 服务的步骤 4 中“用户名”保持一致。 可使用默认账号 Administrator，亦可使用其他自定义账号。

参数名称	参数说明
密码	登录 Windows 系统的用户的密码。
采集对象	采集对象包括以下选项： • Process • ComputerSystem • UserAccount • ShortCutFile • 自定义其他状态类型的对象。 【示例】 Process
索引类型	“**采集对象**”选择“**自定义**”及“**Process**”等其他状态类型的采集对象，索引类型自动关联为“**无**”。
查询语句	• 若“**采集对象**”选择“**Process**”，自动关联 select 查询语句，采集对象选择为 Process，查询语句自动关联为“select * from Win32_ Process”。 • 若“**采集对象**”选择“**自定义**”，需手动输入 select 查询语句，查询相应对象。
修改偏移	包括以下选项： • 是：从文件开头开始读。 • 否：从上一次采集的位置继续采集。 当索引类型为“**无**”时，选择“**否**”。

步骤2. 打开“**高级设置**”，设置高级参数。

参数说明如下所示。

参数名称	参数说明
超时时间（ms）	一次采集的最大等待时长。单位：ms。
轮询间隔（ms）	采集间隔的时间。单位：ms。
日志处理上限	处理日志的最大值。单位：条。
解析并发个数	为每个读取实例分配的解析实例个数。
读取并发个数	同时读取的实例个数。

参数名称	参数说明
轮询生效期	轮询生效期包括以下两个选项： • 无数据。 • 数据源接收时 当索引类型为“**无**”时，选择“**数据源接收时**”。

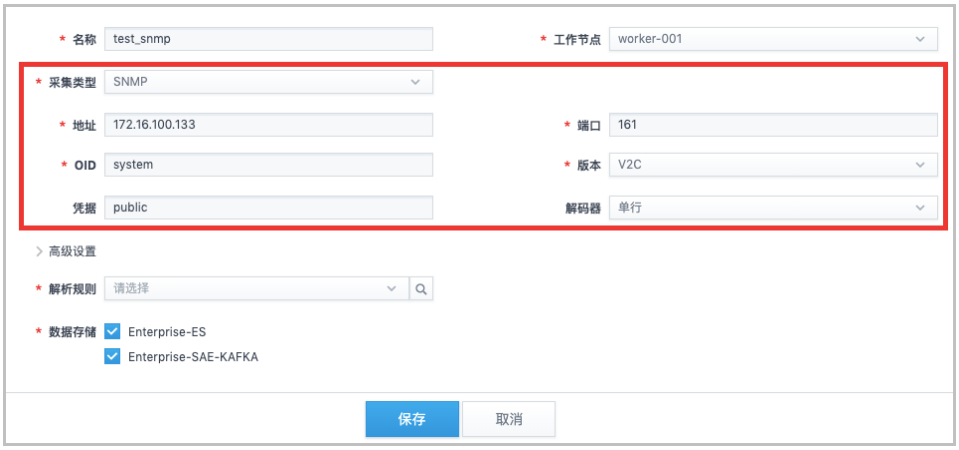
8.3.12 采集类型为“SNMP”

前提条件

在配置 SNMP 采集类型的数据源前，您需要开启 SNMP 服务，具体请参见 D.2 如何开启 SNMP 服务

操作步骤

步骤1. 选择“**采集类型**”为“**SNMP**”，配置页面如下。

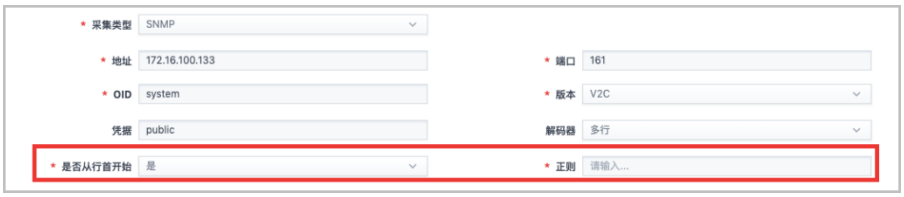


配置参数说明如下。

参数名称	参数说明
地址	目标服务器 IP。
端口	服务访问端口。
OID	SNMP OID 列表，多个逗号分隔。
版本	SNMP 协议版本。
凭据	登录凭据。
解码器	等同其它数据源功能。

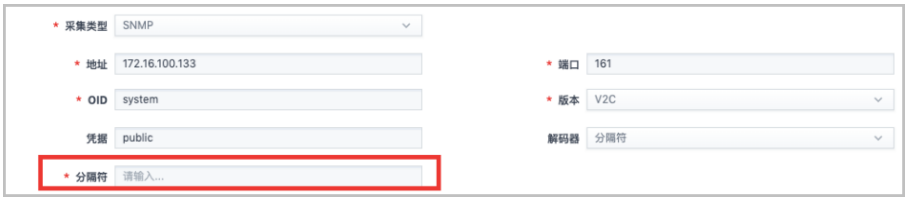
步骤2. 选择“**编码器**”。

- 当设置为“**无**”和“**单行**”时，无新增参数。
- 当设置为“**多行**”时，需配置以下参数。

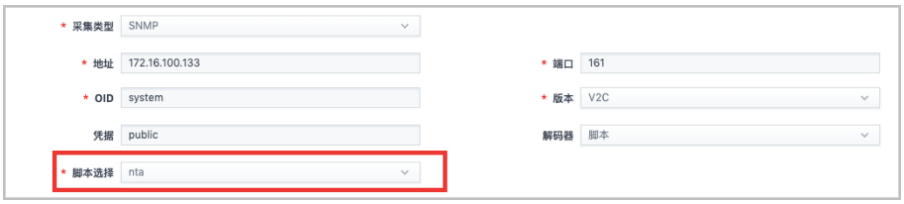


参数名称	参数说明
是否从行首开始	选择每条数据是否从行首开始，包括以下选项： • 是 • 否
正则	输入正则表达式。

- 当设置为“**分隔符**”时，请输入分隔符。



- 当设置为“**脚本**”时，请在“**脚本选择**”后下拉菜单中选择“**nta**”或“**更多脚本上传**”。



- 当设置为“**自定义**”时，请配置以下参数。

参数名称	参数说明
解码名称	自定义插件提供的解码功能，对应配置 worker.codec 下的名称。
解码参数	自定义插件提供的解码功能所需要的参数。

步骤3. 高级设置保持缺省值。确认“**轮询生效期**”为“**数据源接收时**”。

8.3.13 采集类型为“ELASITCSEARCH”

操作步骤

步骤1. 选择“**采集类型**”为“**ELASITCSEARCH**”，配置页面如下。

配置参数说明如下。

参数名称	参数说明
集群名称	部署的 ElasticSearch 集群的名称。

参数名称	参数说明
主机及端口	部署的 ElasticSearch 集群主机的 IP 地址和访问端口。 • 单击 + 可添加多个 ElasticSearch 集群主机的 IP 地址和访问端口。 • 单击 − 可删除已添加的 IP 地址和访问端口。
ES 索引	输入 ES 的索引。 【示例】 event
ES 索引类型	输入 ES 的索引类型。 【示例】 _doc
查询语句	可选项。可以输入 ES 官方查询语句。必须是 Query string 语法格式。
索引列	输入 ES 索引列。 【示例】 occur_time
索引列类型	在下拉列表中选择索引的类型，包括以下选项： • 自增数字 • 时间类型
索引步长	每次采集日志的条数。

步骤2.　高级设置保持缺省值。

8.3.14 更多操作

操作	说明
复制	您可以通过单击数据源列表中某条数据操作列的“**复制**”，复制已有的数据源，基于原有信息进行编辑以新增数据源。
编辑	您可以通过单击数据源列表中某条数据操作列的“**编辑**”，修改该条数据源的配置信息。
删除	• 您可以通过单击数据源列表中某条数据操作列的“**删除**”，删除该条数据源数据。 • 当数据源列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“ 删除 ”，可一次性删除多条数据。
导出	单击数据源列表操作栏的“ 导出 ”，目前列表中存在的数据源类型以“.json”文件形式自动下载到默认下载位置中。

操作	说明
导入	单击“ 导入 ”，通过导入数据源文件以创建数据源。
启动数据源	• 单击“**操作**”列中的“**启动**”，可启动该条数据源。 • 当数据源列表中有多条数据需要启动，可通过勾选需启动的数据，并单击“ 启动 ”，可一次性启动多条数据源。
停止数据源运行	• 单击“**操作**”列中的“**停止**”，可停止该条数据源的运行。 • 当数据源列表中有多条数据需要启动，可通过勾选需启动的数据，并单击“ 停止 ”，可一次性停止多条数据源。
查看	单击数据源列表操作栏的“**查看**”，可查看运行中数据源的配置信息。
日志	单击数据源列表操作栏的“**日志**”，可下载为当前最近的 1000 条日志。
抓包	单击数据源列表操作栏的“**抓包**”，可下载 tcpdump 侦听的所有网卡口的接收报文（接收端口及协议由数据源配置决定）。
查询	您可以通过以下五个字段进行搜索确定数据源范围后，进行批量的启动或停止等操作。 • 采集类型 • 数据源名称 • 工作节点 • 数据连接器|解析规则 • 标签 以上字段均支持模糊搜索，此处以“**数据源名称**”为例，介绍如何查询数据源。 在界面右上角打开“**请选择**”下拉列表，选择“**数据源名称**”，在“**请输入**”的搜索框内输入数据源名称的关键字，按回车键，执行查询，系统自动模糊查询出包含查询关键字的数据源，以列表方式展示。
授权总数	授权总数是 license 签发时，给 LAS 系统的授权点数的限制。与 License 管理页面的授权点数是一致的。 判定授权点数的标准是：报送设备相同的 IP 作为一个授权点数。

8.4 日志代理

日志通过 Windows 代理或者 Linux 代理的方式，将日志经过工作节点发送到报送设备，选择对应的解析规则对采集的日志进行处理。

请确保网络之间互通，否则请设置相应的防火墙策略，保证数据正常传递，否则将被拦截。

8.4.1 Linux 日志代理

操作步骤

步骤1. 在导航栏单击，选择“**数据接入 > 日志代理**”，LAS 系统默认显示“**日志代理**”页面。

步骤2. 点击“Linux”，显示安装建议。

步骤3. 按照操作建议即可采集到 Linux 的日志。

8.4.2 Windows 日志代理（64 位）

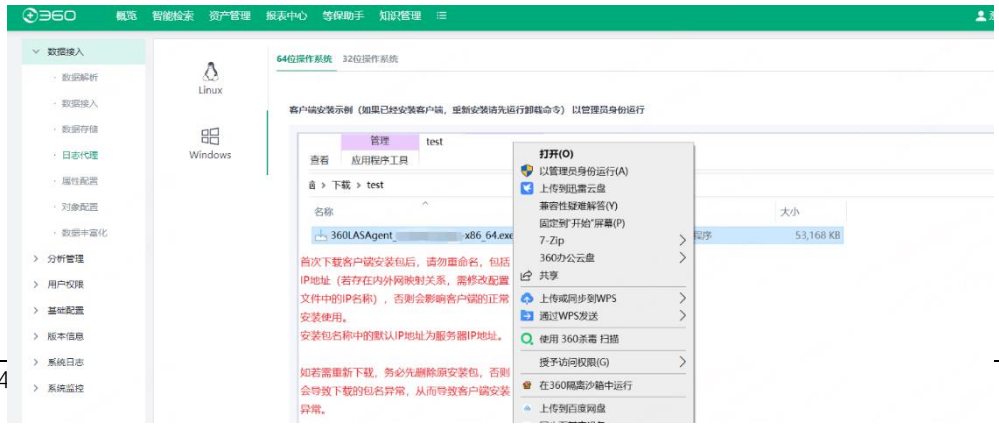
操作步骤

步骤1. 在导航栏单击，选择“**数据接入 > 日志代理**”，LAS 系统默认显示“**日志代理**”页面。

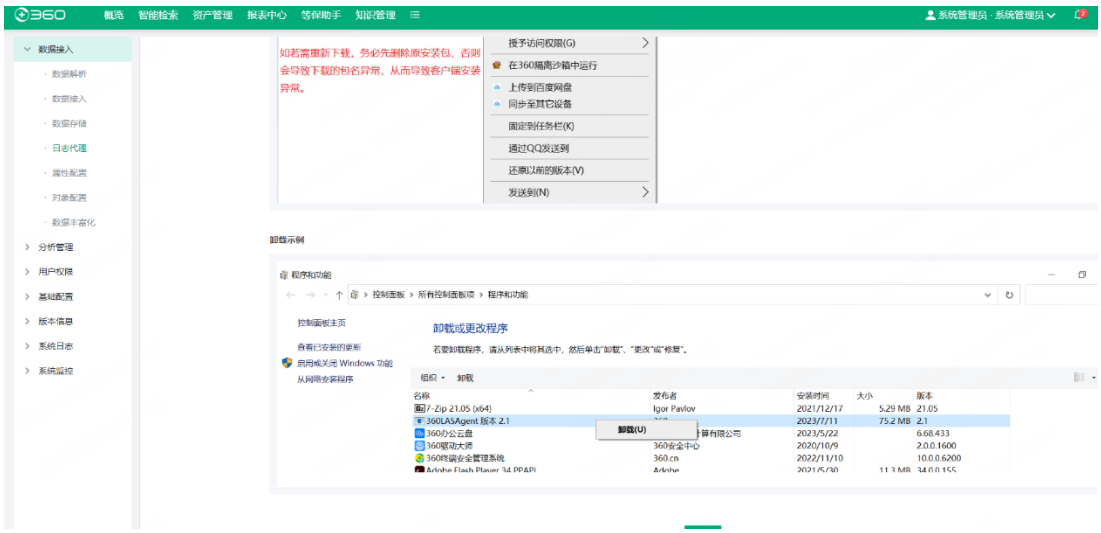
步骤2. 点击“Windows”默认显示 64 位操作系统的日志代理及按照示例；

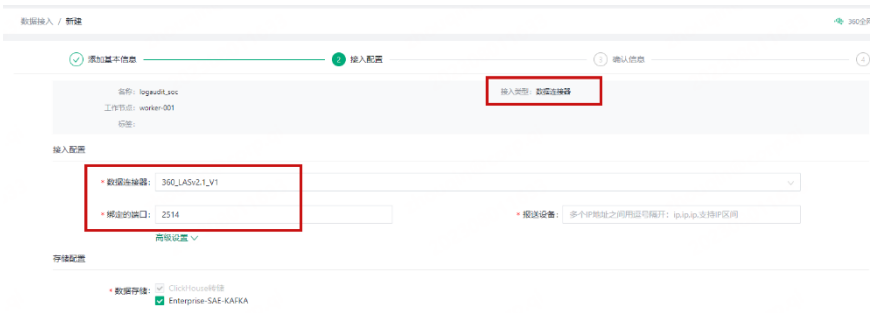
步骤3. 点击页面的“下载”；

步骤4. 将下载的代理客户端传到 Windows 机器上，按照示例说明进行安装和卸载；



步骤5. 在数据接入页面，新增网络--**syslog** 数据源，端口为：**2514**，通信协议为：**tcp**，解析规则为：“360LSA 日志代理_入口”，选择数据存储，保存并启动；
或者在数据接入页面，选择采集类型为：数据连接器，数据连接器选择“360LASv2.1_v1”，通信协议为：**tcp**，配置并保存。





8.4.3 Windows 日志代理（32 位）

操作步骤

步骤1. 在导航栏单击，选择“**数据接入 > 日志代理**”，LAS 系统默认显示“**日志代理**”页面。

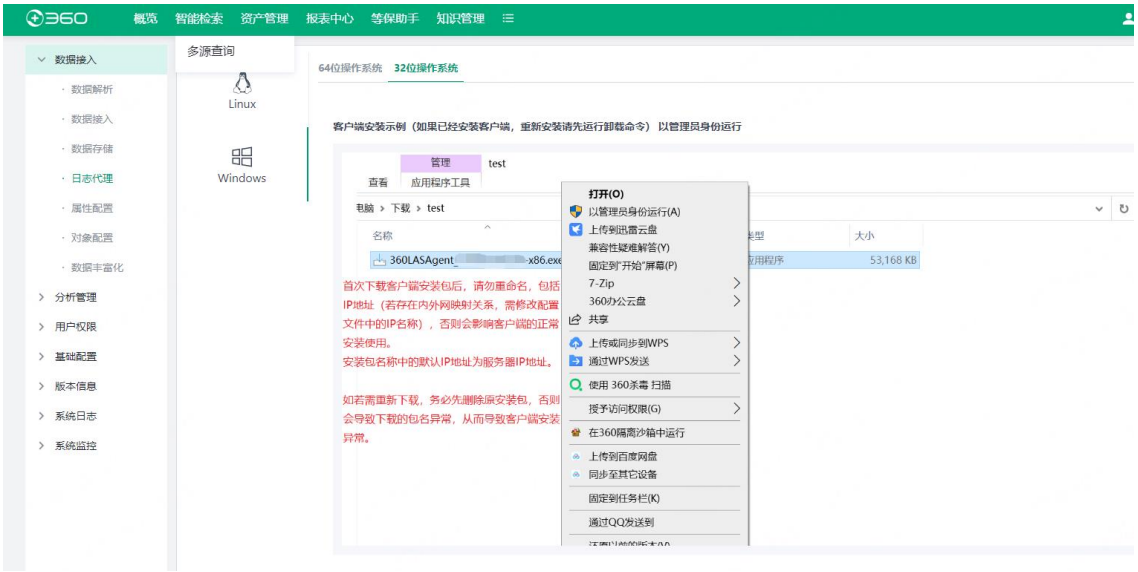
步骤2. 点击“Windows”，切换到“32 位操作系统”；

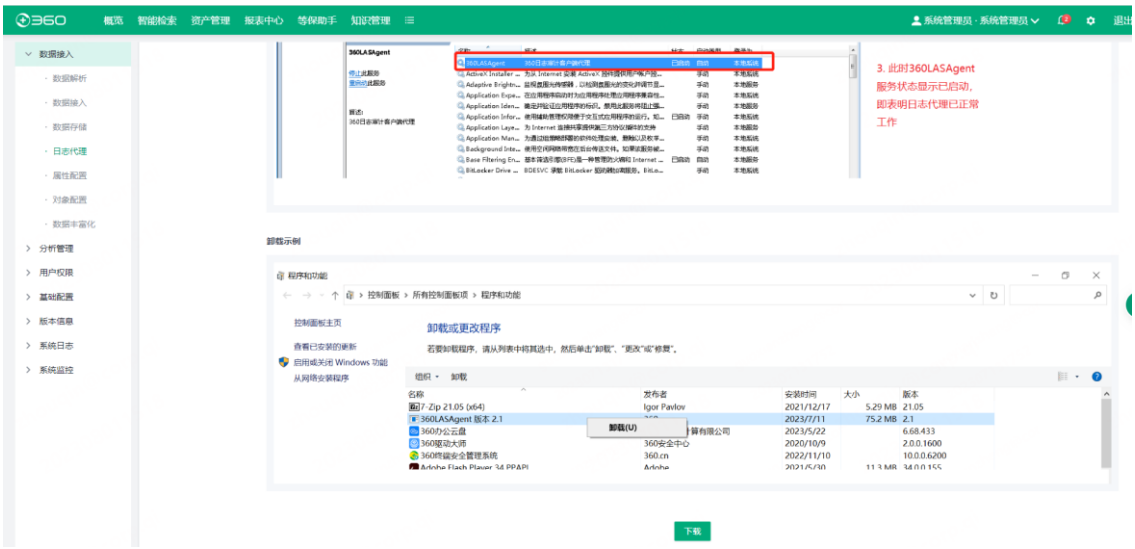
步骤3. 点击页面的“下载”；

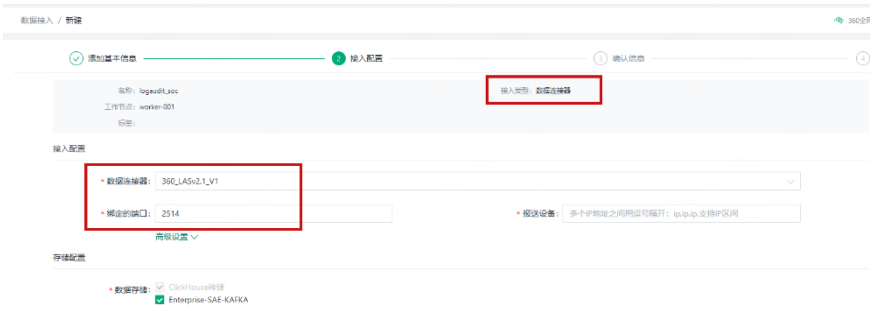
步骤4. 将下载的代理客户端传到 Windows 机器上，按照示例说明进行安装和卸载；

步骤5. 在数据接入页面，新增网络--**syslog** 数据源，端口为：**2514**，通信协议为：**tcp**，解析规则为：“360LSA 日志代理_入口”，选择数据存储，保存并启动；

或者在数据接入页面，选择采集类型为：数据连接器，数据连接器选择“360LASv2.1_v1”，配置并保存。







8.5 属性配置

属性配置里包含字段名称、属性名称、属性类型、描述、属性类别等信息

在导航栏单击，选择“数据接入 > 属性配置”，LAS 系统默认显示“属性配置”页面。

字段介绍

选中某个字段，单击，即可查看并编辑字段的详细内容：

字段的参数信息说明：

参数	说明
属性名称	字段的中文名称。如果属性名称中包含英文，请使用大写。
字段名称	字段的英文名称。 字段名称遵循以下命名规范： ①只支持字母开头，可以包含数字下划线和点； ②字段名称建议使用小写； ③字段名称按照“**关系_对象_字段含义**”的方式进行命名。以“**p_proc_path**”为例，其中“p”，表示父亲关系，“**proc**”是“**process**”对象的缩写，“**path**”是字段含义“**路径**”，拼接起来 p_proc_path 就是“**父进程路径**”的含义；再以“**http_method**”为例,该字段中没有关系，http 表示“**HTTP 协议对象**”，method 表示“**请求方法**”，拼接起来就是“**HTTP 请求方法**”。
属性类型	字段的数据类型，包括 IP 类型、整型类型、长整型类型、浮点型类型、时间类型、字符类型、枚举类型。
是否数组	数组类型。
描述	关于字段的描述信息。

除了上述参数，字段还有一个特殊的参数——**属性类别**，属性类别由 LAS 系统分配，无法被编辑。

属性类别标识了字段的功能，包含以下类别：

- **基础属性**：安全团队或用户定义的字段，可以被 SAE、解析使用，可以被修改；
- **业务属性**：LAS 系统定义的字段，可以被解析、SAE 使用，但是安全团队不能更改的字段；
- **关联分析属性**：LAS 系统定义的字段，用于 SAE，不可以被解析使用；
- **系统属性**：LAS 系统定义的字段，用于告警、安全事件等模块，不可以被解析使用；

- **高级业务属性**：LAS 系统定义的字段，用于资产、脆弱性、情报模块，不可以被 SAE、解析使用；

用户只能新增或修改基础属性，无法修改其他类别的属性。

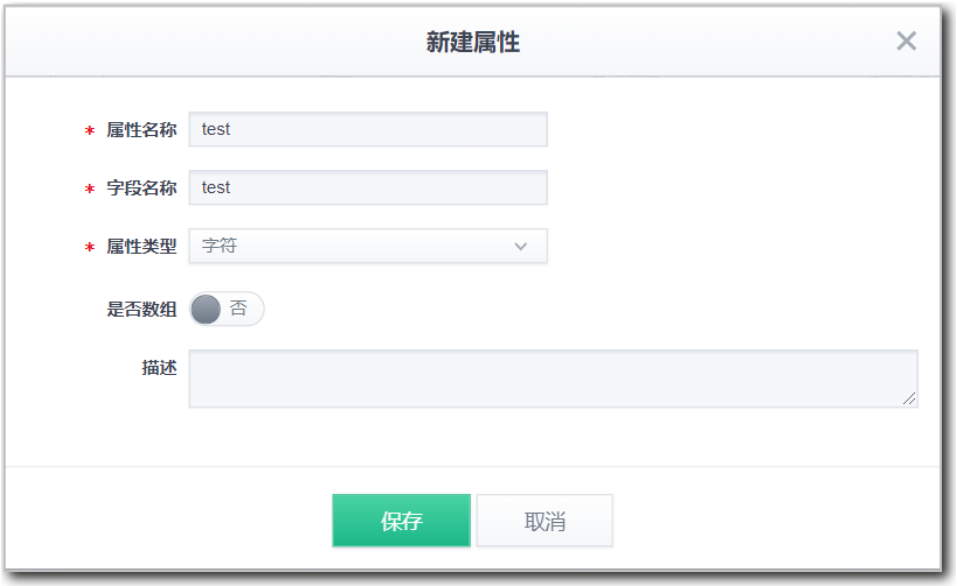
新建字段

LAS 系统内置了 1000 多个字段，用户可以使用的有 800 多个字段。如果现有字段不满足用户需求，用户可以新增字段。

【操作步骤】

步骤1. 在导航栏单击，选择“**数据接入 > 属性配置**”，LAS 系统显示“**属性**”页面。

步骤2. 单击“**新建**”，输入字段内容并保存。



参数名称	参数说明
属性名称	属性名称信息，允许输入 1~64 个字符。
字段名称	输入字段的名称，允许输入 1~64 个字符。
属性类型	在下拉列表中选择属性的类型，包括以下选项： • IP 型 • 整型 • 长整型 • 浮点型 • 时间 • 字符 • 枚举
是否数组	选择此字段是否为数组类型。

参数名称	参数说明
描述	输入对属性的描述。

字段添加保存后，字段名称将无法修改！

*用户新增字段，LAS 系统会默认在字段名称上添加"**c_**"前缀（表示 custom 含义）。如下图所示，用户新建"**test**"字段，保存时默认变成"**c_test**"字段：*

字段编辑

选中某个字段，单击，即可编辑字段，如“**字段详情**”章节所述。

对于用户自定义字段，用户可以编辑除“**字段名称**”外的所有参数；

对于 LAS 系统内置字段，用户只能编辑枚举字段的枚举值，其他参数均无法编辑；

更多操作

操作	说明
修改	单击属性列表操作栏的，弹出属性编辑界面，显示原有信息， • 内置属性仅支持修改“**属性名称**”和“**描述**”。 • 自定义属性除修改“**属性名称**”和“**描述**”，还可以修改所属数据源。
导入	单击“**导入**”，通过导入已编辑的 excel 文件上传属性数据。
导出	勾选一个或多个属性，并单击界面左上方“**导出**”，可将属性的数据以“.xlsx”的格式导出至本地。
查询	您可以通过界面右上角搜索框内输入属性名称，如“**地址**”，并按回车键，查询出属性名称中包含地址的属性，以列表方式展示。 您可以通过以下四个字段进行搜索关联分析规则。 • 属性名称 • 字段名称 • 属性类型 • 属性类别 以上“**属性名称**”和“**字段名称**”均支持模糊搜索，“**属性类型**”和“**属性类别**”则在对应的下拉列表中选择。 并可以通过勾选“**数组**”，筛选出数组类型的属性。

8.6 对象配置

对象是对字段的组织管理。

单击“设置> **数据接入**> **对象配置**”，显示“**对象配置**”页面。

对象介绍

按照对象的功能划分，将对象分为了基础对象和业务对象：

- **基础对象**：是从日志中提取出的行为主体，用户可以使用的字段都被划分都某个基础对象里。基础对象又被细分为“**日志对象**”、“**计算机对象**”、“**安全设备**”、“**协议**”四类。
- **业务对象**：LAS 系统资产、脆弱性、情报、安全事件等功能模块使用的字段，都被划分到业务对象里。

*业务对象是 LAS 系统基础功能模块使用的，除“**日志**”对象外，所有业务对象均不应该可被用户使用。*

*“日志”对象是描述“**第三方日志**”信息的对象，包括日志来源的设备、IP、厂商等信息，这些信息需要用户手动填入。*

LAS 系统所有内置对象如下：

对象种类	对象类型	对象名称
基础对象	日志对象	威胁
		事件
	计算机对象	设备
		流量
		主机
		服务端
		文件
		进程
		线程
		堆栈
		模块
		补丁
		驱动
		计划任务
		脚本
		容器

对象种类	对象类型	对象名称
		服务
		注册表
		网络共享
		会话
		登录
		管道
		存储设备
		窗口
		WMI 对象
		UAC
		用户
		用户组
		环境变量
		配置
		证书
		组织
		漏洞
		认证
		应用
		备份
		对象
		域
		位置
		计算机资源
		属性
	安全设备	APT
		防火墙
		威胁情报
		沙箱
		邮件

对象种类	对象类型	对象名称
		数据库
		蜜罐
		恶意程序
	协议	tcp 协议
		smb 协议
		dhcp 协议
		arp 协议
		icmp 协议
		ftp 协议
		dns 协议
		http 协议
		tls 协议
		ja3 协议
		ldap 协议
		pop3 协议
		nfs 协议
		telnet 协议
		oicq 协议
		ssh 协议
		rdp 协议
		ospf 协议
		kerberos 协议
		rpc 协议
业务对象		日志
		告警
		服务资产
		安全事件类型
		脆弱性类型
		资产打分类型
		用户类型

对象种类	对象类型	对象名称
		预案编排类型
		情报类型
		主机资产
		应用资产
		网站资产
		域名资产

*LAS 系统中存在一个“**设备**”对象，该对象与“**设备标准**”里“**设备**”的含义是完全不同的。“**设备标准**”里的“**设备**”表示向 LAS 系统发送日志的设备；而“**设备**”对象里的“**设备**”是日志内容里的设备。例如，无线路由器向 LAS 系统发送了一条手机连接 wifi 的日志，“**无线路由器**”就是“**设备标准**”里的设备，“**手机**”就是“**设备**”对象里的设备。*

对象与字段

前文介绍字段时，都是从日志角度出发，字段是日志中值的标识；如果从对象角度出发，字段又有了新的定义：

字段：对象的属性被称作字段。

一个字段可以属于多个对象，在不同对象里，字段的含义不发生变化。

以“**用户名称**”为例，该字段即属于“**用户**”对象，又属于“**ftp 协议**”对象；在使用时，只有一个“**用户名称**”字段，而不会区分“‘**用户**’的‘**用户名称**’”和“‘**ftp 协议**’的‘**用户名称**’”。

根据属性的重要程度，又将对象里的字段分为**核心字段**和**扩展字段**(又叫非核心字段)。用户在使用对象时，LAS 系统将主动推荐核心字段。

新建对象

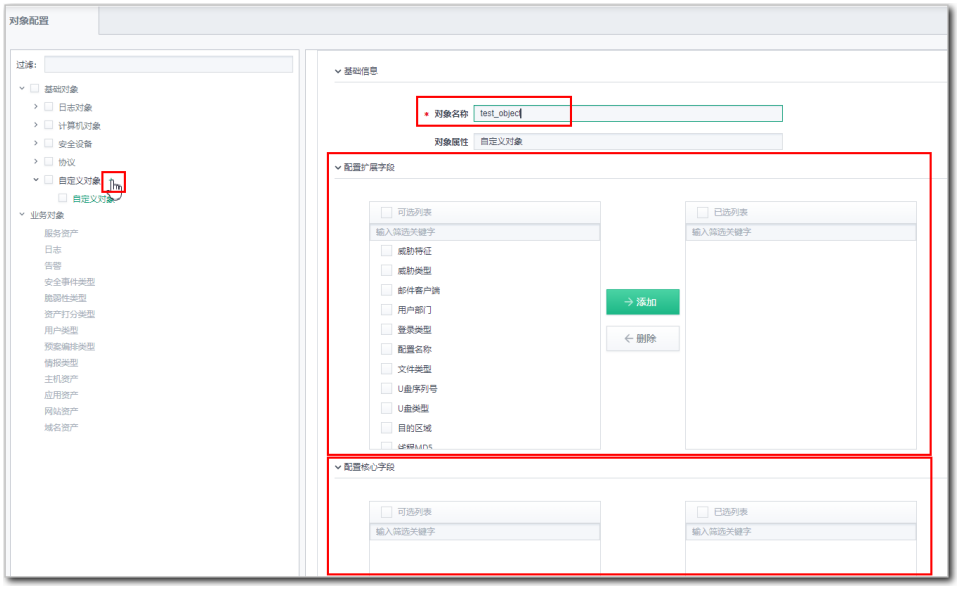
LAS 系统内置了 80 多个对象，用户可以使用的有 70 多个对象。如果这些对象不满足用户需求，用户可以新增对象，新增对象默认属于“**基础对象 > 自定义对象**”。

【操作步骤】

步骤1. 单击“设置 > **数据接入 > 对象配置**”，LAS 系统显示“**对象配置**”页面；

步骤2. 单击“**自定义对象**”后的加号，即进入新建对象页面；

步骤3. 根据页面提示，填写“**对象名称**”，选择“**扩展字段**”和“**核心字段**”：



将某个字段添加进对象的核心字段时，需先其添加进扩展字段；再从扩展字段列表中选择，添加进核心字段。

对象编辑

用户无法编辑 LAS 系统内置的对象，只能编辑自定义对象。

步骤4. 单击“**设置** > **数据接入** > **对象配置** > **自定义对象**”；

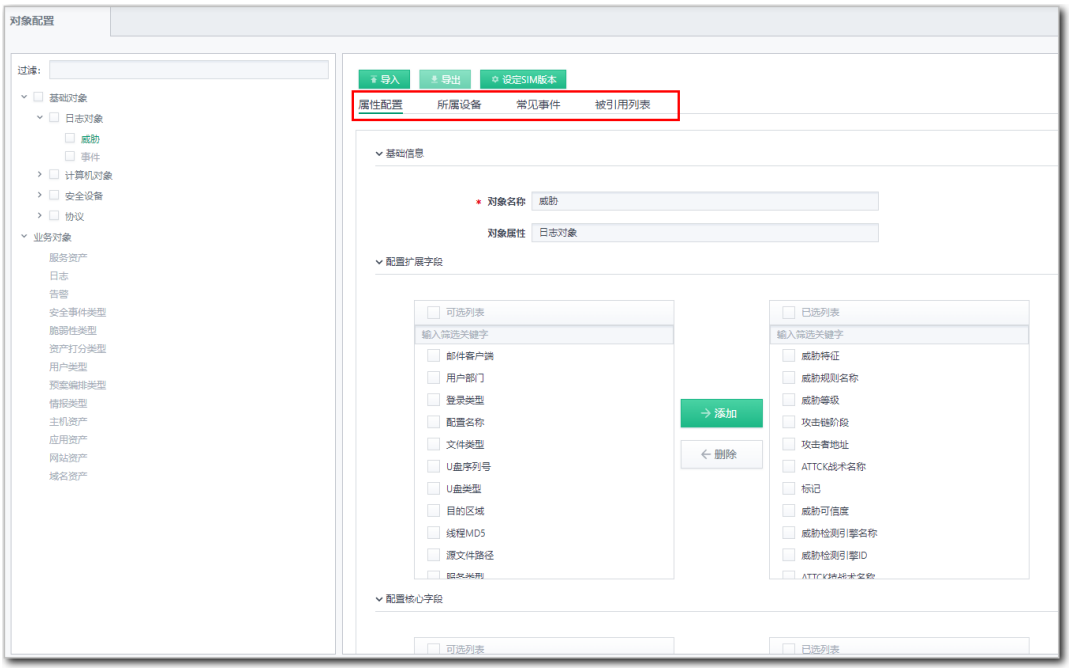
步骤5. 选择要编辑的对象，开始编辑；

在进行对象编辑时，用户只能编辑对象名称、配置扩展字段和配置核心字段，无法进行其他操作。

注意事项

对象页面中有 4 个 Tab 页面：属性配置、所属设备、常见事件、被引用列表。在进行对象编辑时，只能编辑属性配置页面。

- **属性配置**：配置对象的字段；
- **所属设备**：展示设备与对象的关系，需要在“**设备配置**”页面配置该关系；
- **常见事件**：展示事件名称与对象的关系，需要在“**事件配置**”页面配置该关系；
- **被引用列表**：展示该对象被哪些解析规则引用；



8.7 数据丰富化

本脑支持对日志中的原始字段进行信息的丰富化，提供更为全面的安全日志以供分析和统计。数据的丰富化包括多类信息：资产信息、地理位置信息、网段信息以及自定义信息等。数据丰富化有效地帮助用户自定义日志、告警内容，从而提升安全分析的效率，提高安全运营的效果。

系统默认补全二元组、五元组。其他需要手动添加。

8.7.1 二元组丰富化

开启方式

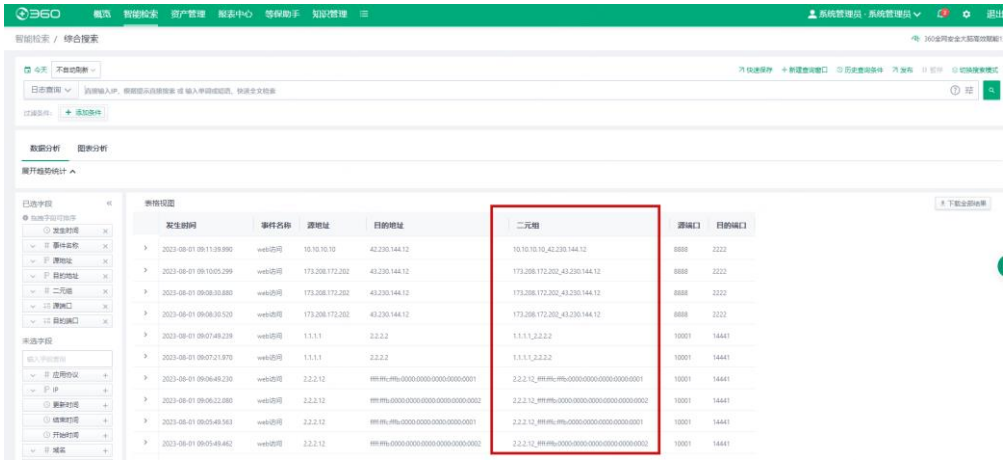
系统默认开启二元组补全。

二元组丰富化的含义

二元组丰富化指的是将日志中的源地址、目的地址字段进行拼接，生成丰富化目标字段：二元组，并添加到日志中。

示例：

丰富化目标：二元组，值为：源地址_目的地址。



8.7.2 五元组丰富化

开启方式

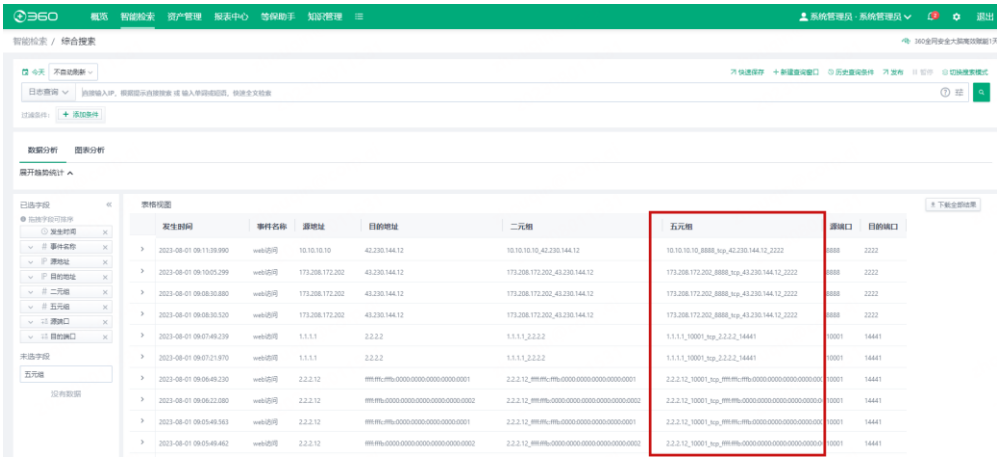
系统默认开启五元组补全。

五元组丰富化的含义

五元组丰富化指的是将日志中的源地址、源端口、协议、目的地址、目的端口字段进行拼接，生成丰富化目标字段：五元组，并添加到日志中。

示例：

丰富化目标字段“五元组”，字段值为：源地址_源端口_协议_目的地址_目的端口。



8.7.3 资产丰富化

开启方式

需要手工开启。

资产丰富化的含义

资产丰富化是指利用系统中的资产信息，将日志或者告警中原始字段进行资产信息的丰富化，并生成丰富化目标字段，添加到日志或者告警中。

可以进行资产丰富化的原始字段主要有：源地址、目的地址、主机 IP、日志来源地址。

丰富化目标字段名称为：丰富化原始字段_丰富化目标字段，并将对应的属性添加到属性管理中。

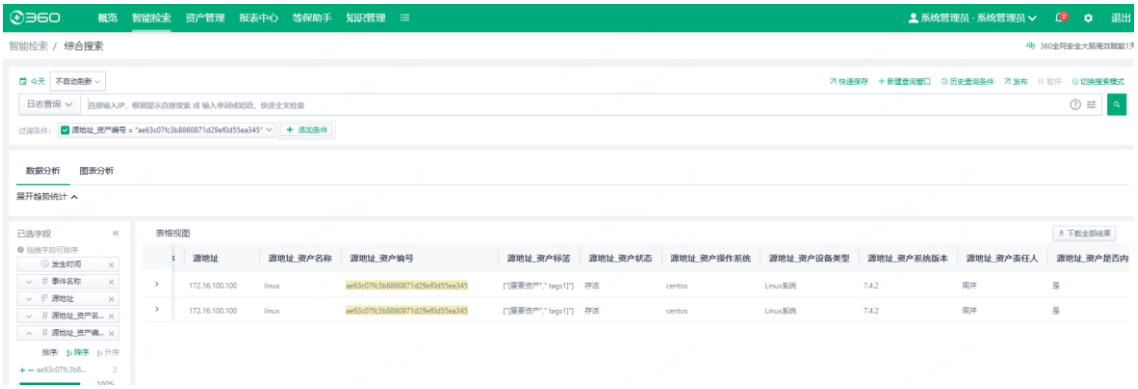
示例：

以源地址的资产丰富化为例，介绍如何新增资产补全的操作。

步骤1. 点击“**设置** > **数据接入** > **数据丰富化**”，系统进入丰富化规则列表页面；

步骤2. 点击“**新建**”按钮，选择**丰富化类型**为“**资产**”，选择**丰富化原始字段**为“**源地址**”，根据需求选择丰富化字段，并勾选**丰富化目标**“**日志**”，选择开启状态，点击“**确认**”。

步骤3. 点击“**智能检索**”，查看原始日志信息，将源地址的资产丰富化的信息添加到已选字段，查看对应的丰富化信息。



8.7.4 GEO 丰富化

开启方式

日志的 GEO 丰富化需要手工开启，告警的 GEO 丰富化默认自动开启。

GEO 丰富化的含义

GEO 丰富化是指利用系统中的 GEO 信息，将日志或告警中的原始字段进行 GEO 信息的丰富化，并生成丰富化目标字段，添加到日志或者告警中。

可以进行 GEO 丰富化的原始字段主要有：源地址、目的地址、日志来源地址。

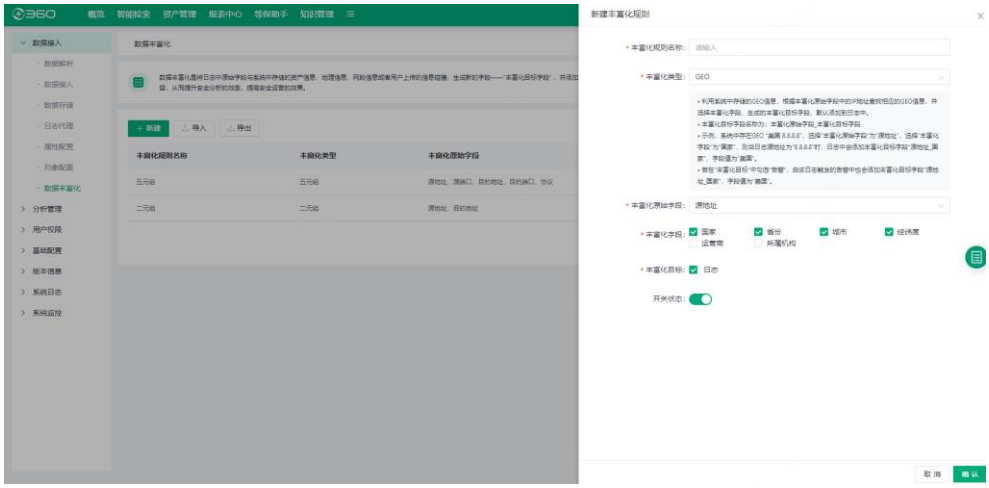
丰富化目标字段名称为：丰富化原始字段_丰富化目标字段，并将对应的属性添加到属性管理中。

示例：

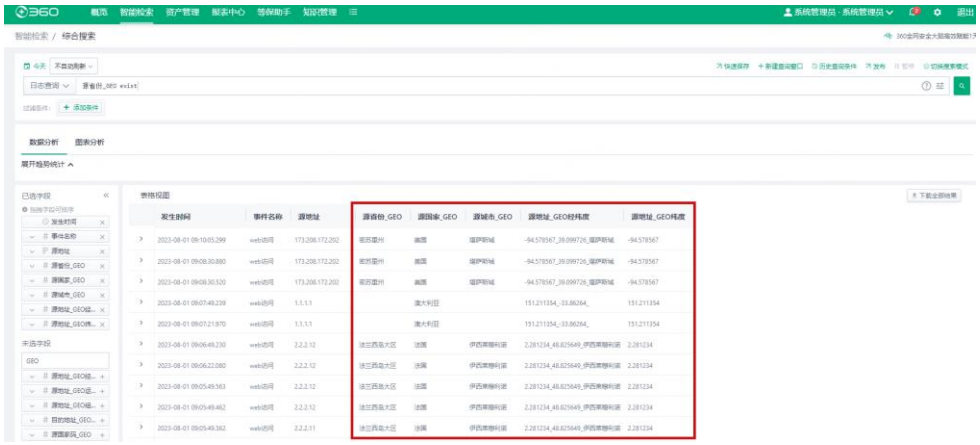
以源地址的 GEO 丰富化为例，介绍如何新增 GEO 补全的操作。

步骤1. 点击“**设置** > **数据接入** > **数据丰富化**”，系统进入丰富化规则列表页面；

步骤2. 点击“**新建**”按钮，选择**丰富化类型**为“**GEO**”，选择**丰富化原始字段**为“**源地址**”，根据需求选择丰富化字段，并勾选**丰富化目标**“**日志**”，选择开启状态，点击“**确认**”。



步骤3. 点击“**智能检索**”，查看原始日志查询，将源地址的 GEO 丰富化的信息添加到已选字段，查看对应的丰富化信息。



8.7.5 自定义丰富化

开启方式

需要手工开启。

自定义丰富化的含义

自定义丰富化是指选择日志中的任一字段作为丰富化的原始字段，在丰富化映射表中自定义编辑丰富化字段，并构建原始字段和丰富化字段的映射关系，生成丰富化目标字段，并添加到日志或者告警中。

可以进行自定义丰富化的原始字段是除了数组之外的其他任何字段。

丰富化目标字段名称为：丰富化_丰富化原始字段_丰富化目标字段，并将对应的属性添加到属性管理中。

示例：

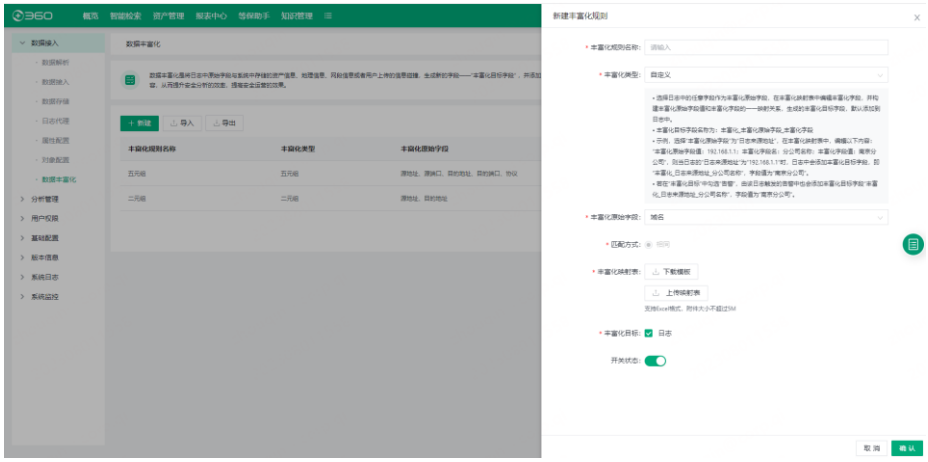
以源地址的自定义丰富化为例，介绍如何新增自定义丰富化补全的操作。

步骤1. 点击“**设置** > **数据接入** > **数据丰富化**”，系统进入丰富化规则列表页面；

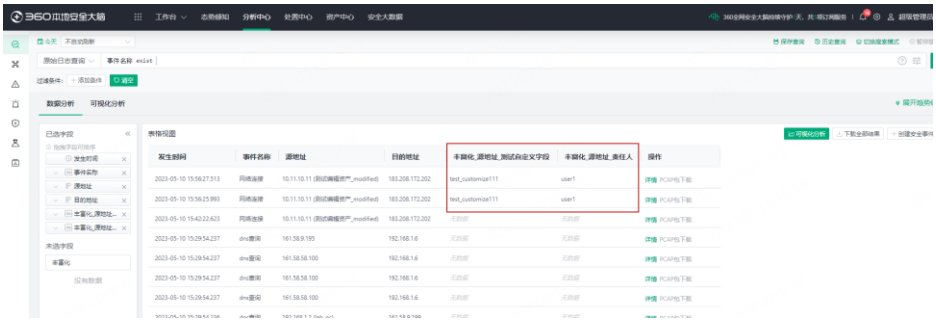
步骤2. 击“**新建**”按钮，选择**丰富化类型**为“**自定义**”，选择**丰富化原始字段**为“**源地址**”，下载模板，并在模板中构建映射关系。

A	B	C	D
待富化的字段的内容	对条件字段富化的目标字段名称	富化的目标字段的内容	
条件字段值*	富化字段名*	富化字段值*	
10.11.10.11	责任人	user1	
10.11.10.11	测试自定义字段	test_customize111	

步骤3. 点击“**新建**”按钮，选择**丰富化类型**为“**自定义**”，选择**丰富化原始字段**为“**源地址**”，上传映射表，并勾选**丰富化目标**“**日志**”，选择开启状态，点击“**确认**”。



步骤4. 点击“**智能检索**”，查看原始日志查询，将源地址的自定义丰富化的信息添加到已选字段，查看对应的丰富化信息。



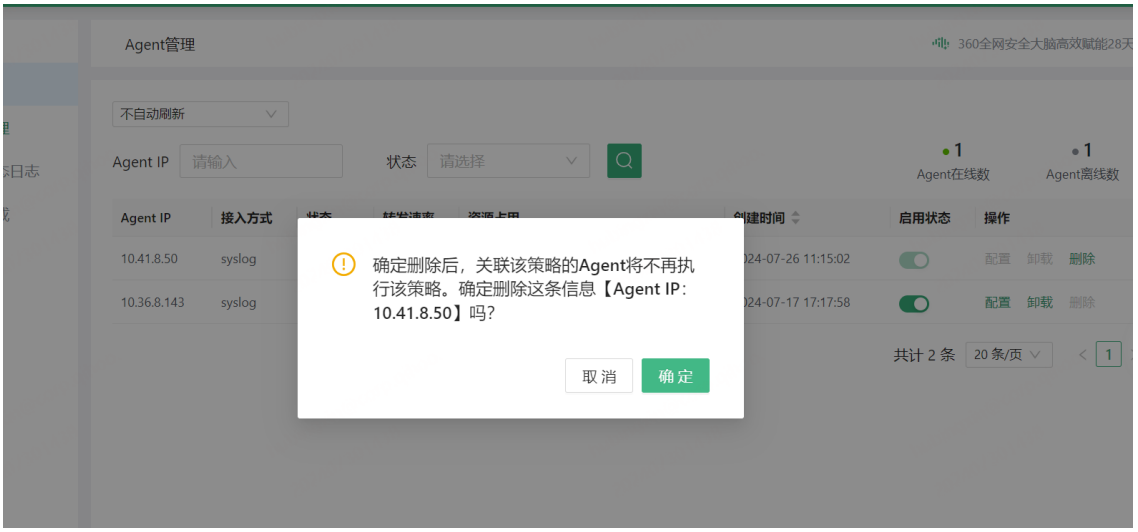
9. Agent 接入

9.1 Agent 管理

Agent 部署并接入后，在 agent 管理页面可查看到所有接入的 agent 客户端，包含 IP、状态、eps、资源占用等信息，如图

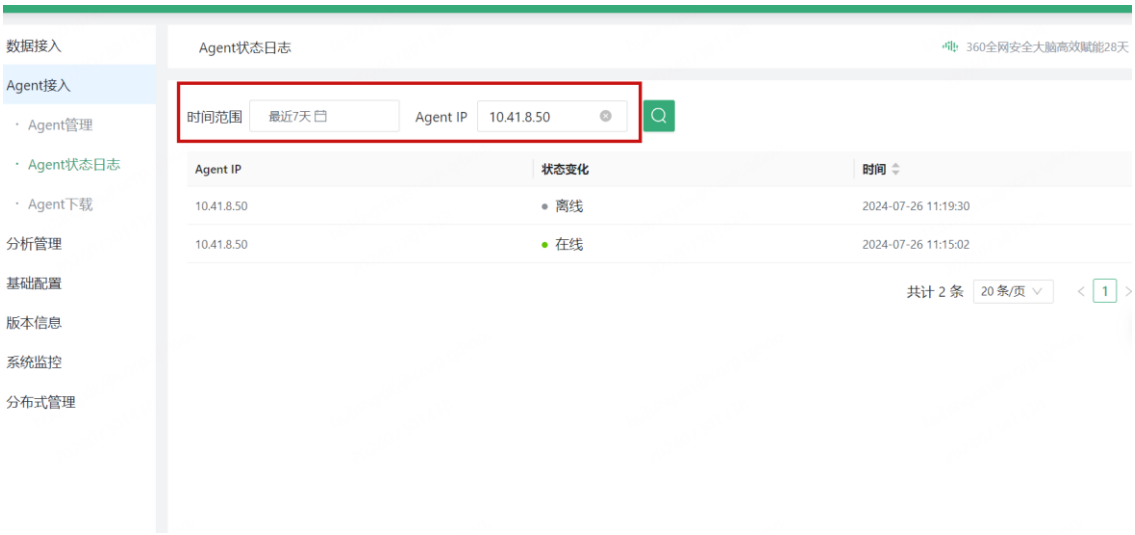
在线 agent 可配置或卸载操作，如图

离线 agent 只可进行删除操作，如图



9.2 Agent 状态日志

查看 agent 在线状态，输入 agent IP 后点击查询



9.3 Agent 下载

9.3.1 Linux 安装

linux 操作系统日志代理采集，推荐使用 rsyslog 标准工具包，且兼容市面上主流的 linux 操作系统发行商，包括：centos，rhel，suse，ubuntu，debian 等。

1. 首先检查环境上是否已安装了 rsyslog 工具包，执行：rsyslogd -v 查看。

2. 若步骤 1 命令执行失败，则需要先安装 rsyslog，以 centos 为例，执行：yum install rsyslog。

3. 配置系统日志转发规则，使用自己喜欢的文本编辑器，以 vi 为例，执行：vi /etc/rsyslog.conf，在文本最后追加*.* @服务器 ip:514，此时将以 udp 方式转发

4. 将 rsyslog 注册为开机启动并重启，执行：systemctl enable rsyslog && systemctl restart rsyslog。

5. 在日志审计系统界面上新增 syslog udp 接收数据源，选择合适的解析规则对上报数据进行解析。例如 centos

基本信息

名称	linux-agent185	工作节点	Cluster Select/worker-001(127.0.0.1:正常)
采集类型	网络-SYSLOG		
内容类型	SYSLOG	通信协议	udp
绑定的端口	511	解码器	无
报送设备	11.43.177.185	编码	UTF-8

高级设置

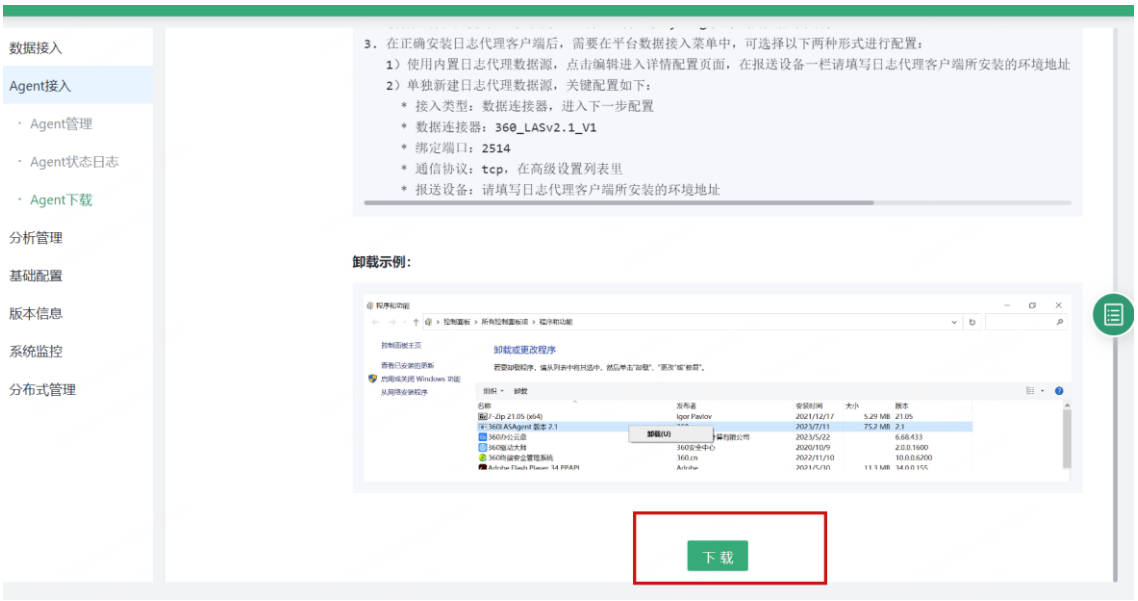
解析规则	LINUX_centos_入口
数据存储	ClickHouse转储， Enterprise-SAE-KAFKA
标签	

6. 跳转到智能检索界面，等待 1 分钟后，点击查询，即可查到最新上报的 linux 系统日志。

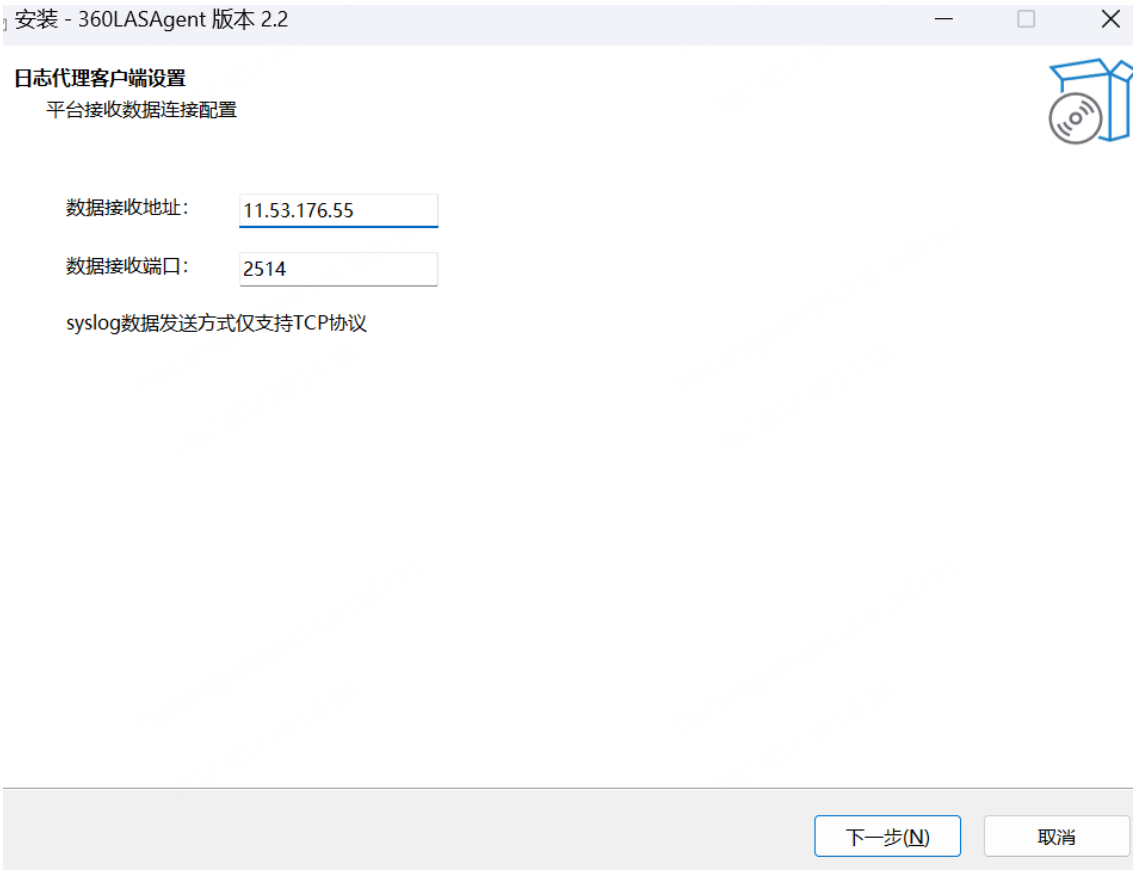
9.3.2 Windows agent 安装

64 位操作系统

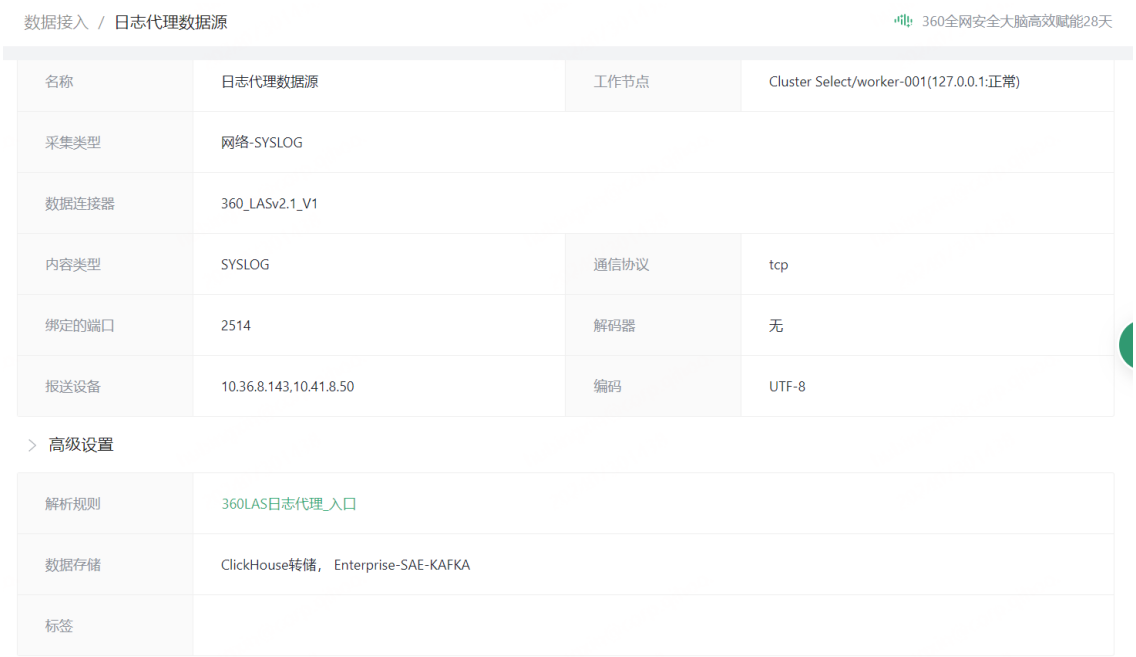
1、 安装包下载，进入高级设置-agent 接入-agent 下载，选择 windows-64 位操作系统后，下拉页面到最后，可看到下载按钮。



2、 下载安装包并检查安装包名称中不包含空格，以管理员身份运行并安装，默认使用 TCP 协议 2514 端口，请不要修改，如图



3、 安装后在数据接入新建日志代理数据源，数据连接器 360_LASv2.1_V1，绑定端口 2514，协议 tcp，如图



32 位操作系统，参考 64 位系统，操作步骤相同。

10. 配置分析管理

10.1 维护 SAE 安全分析规则

SAE 规则即关联分析规则，通过对关联分析的配置，将日志事件生成告警以供安全运维人员分析会审。您可以手动创建或上传符合要求的规则文件。

10.1.1 配置前须知

事件源说明

可以配置事件源为全局事件或具体事件名称，全局事件需配置过滤条件。事件说明如下：

事件	说明
普通事件	dv 解析后生成的普通事件。
内部事件	类似告警，由 SAE 生成，可供其他规则使用。
威胁情报 IP 匹配事件	提取 dv 解析后的事件中的源地址和源端口，目的地址和目的端口，分别与当前环境中的威胁情报信息做比较，如果匹配，则生成该事件。
威胁情报 Domain 匹配事件	提取 dv 解析后的事件中的域名，与当前环境中的威胁情报信息做比较，如果匹配，则生成该事件。
威胁情报 URL 匹配事件	提取 dv 解析后的事件中的网址，与当前环境中的威胁情报信息做比较，如果匹配，则生成该事件。
全局事件	包含以上任意事件。

SAE 规则模板

流式分析类型的 SAE 主要基于以下十种模板，通过一定的组合逻辑设置告警规则。

表10-1 流式关联分析规则模板

模板名称	模板描述	事件源配置
普通模板	基于单个属性的事件名称触发，一对一告警。	有且只有一个事件源
普通模板-having count(DISTINCT)	在一段时间内，多个事件中某属性值不同的次数满足条件即触发告警，统计类告警，分组字段非必须。	
普通模板-having count	在一段时间内，某事件发生的次数满足条件即触	

模板名称	模板描述	事件源配置
	发告警，统计类告警，分组字段非必须。	
普通模板-having sum	在一段时间内，多个事件中某属性值的和满足条件即触发告警，统计类告警，分组字段非必须。	
关联模板-follow_by	某事件 A 发生之后的一段时间内发生了事件 B，关联类告警，关联条件非必须。	至少两个事件源
关联模板-any_order	一段时间内发生多个事件，发生时间无顺序要求，关联类告警。 不允许配置关联条件，可配置分组条件。 当前只支持两个事件，多个事件暂不支持。	
关联模板-not_follow_by	某事件 A 发生之后的一段时间内一定不发生事件 B，关联类告警，关联条件非必须。	有且只有两个事件源
关联模板-or_follow_by	在一段时间内，事件 A 和事件 B 均发生，但对发生时间无先后顺序要求，关联类告警，关联条件非必须。	
关联模板-Repeat-Until	至少 M 次事件 A 发生之后的一段时间内发生了事件 B，关联类告警，关联条件非必须。	
关联模板-not_before	事件 B 发生之前的一段时间内没有发生事件 A，关联类告警。关联条件非必须，如配置， 要求关联条件只支持多个与逻辑运算，且 A 和 B 的关联字段数量必须一致。	

威胁情报丰富化属性说明

当前系统内置的威胁情报丰富化属性字段说明如下：

属性字段	属性名称
type	情报类型. 分类
malcious_family	情报类型. 恶意家族
ioc	情报类型. 威胁情报_ioc
ioc_detail_host	情报类型. 威胁情报_ioc 主机
ioc_detail_path	情报类型. 威胁情报_ioc 路径
alert	情报类型. 是否告警
risk	情报类型. 威胁情报_风险等级
confidence	情报类型. 威胁情报_可信性
malicious_type	情报类型. 威胁情报_恶意类型
campaign	情报类型. 攻击团伙

属性字段	属性名称
control_type	情报类型. 威胁情报_远控类型
hot	情报类型. 威胁情报_是否热点
status	情报类型. 状态
protocol	情报类型. 协议
tags	情报类型. 标签
ioc_detail_port	情报类型. 威胁情报_ioc 端口
first_seen	情报类型. 首次发现时间
last_seen	情报类型. 最近发现时间

10.1.2 配置注意事项

模板选择

不同模板用途是不一样的，处理逻辑和性能也是不同的，在选择时注意其应用场景，选择合适的模板。

部分模板存在一些已知问题，选取时需注意：

- 统计类规则，输出字段值取最后一个事件的字段值。
- not_before 模板规则，第一个告警可能会生成不了，存在告警漏报问题。
- Repeat_until 模板规则，因 AB 时间差不满足条件，存在告警漏报问题。
- or-follow-by 模板可能会有重复告警。

事件源配置

- 全局事件需配置过滤条件。
- 如果确定了该规则的事件名称，应指定事件源的**事件名称**，而不要采用**全局事件**。
- 对于威胁情报相关的规则，事件源名称应配置为“**威胁情报 IP 匹配事件**”、“**威胁情报 Domain 匹配事件**”或者“**威胁情报 URL 匹配事件**”。如果事件源配置为全局事件，需要在过滤条件中使用 match 操作符过滤具体的匹配字段。

过滤条件配置

目前，**应用协议(app_protocol)、网络协议(net_protocol)、协议(protocol)、情报类型.协议(protocol)**这四个字段对过滤条件的右值尽量配置为大写。

时间窗口配置

时间窗口的定义：从第一笔满足条件的事件进入引擎开始，最大允许的时间范围。在该范围内只要数据满足条件，即可触发告警，并将状态清零。

输出属性与内部事件

- 内部事件类似于告警，它的属性只有生成该内部事件的规则所配置的所有输出字段，生成时注意输出字段选取。当前我们规则中有些内部事件的输出字段不完整，导致引用该内部事件做再次匹配的规则因字段缺失而无效。
- 内部事件的事件名称建议有统一格式。
- 普通模板规则不建议生成内部事件。

其他注意点

- **“规则名称”、“告警内容”、“告警处置”**建议支持采用**“$”**引用输出字段。
- 标记属性字段，相当于给告警打了一个标记，不允许与输出属性重复。
- **普通模板规则 data_source、client_host_sign 默认输出**，无需在输出属性中配置。
- **安全信息**：当前系统中内置安全信息分为 IP、数字、字符、时间四种类型，在配置时注意尽量精简信息组内容的数量，保证处理性能。

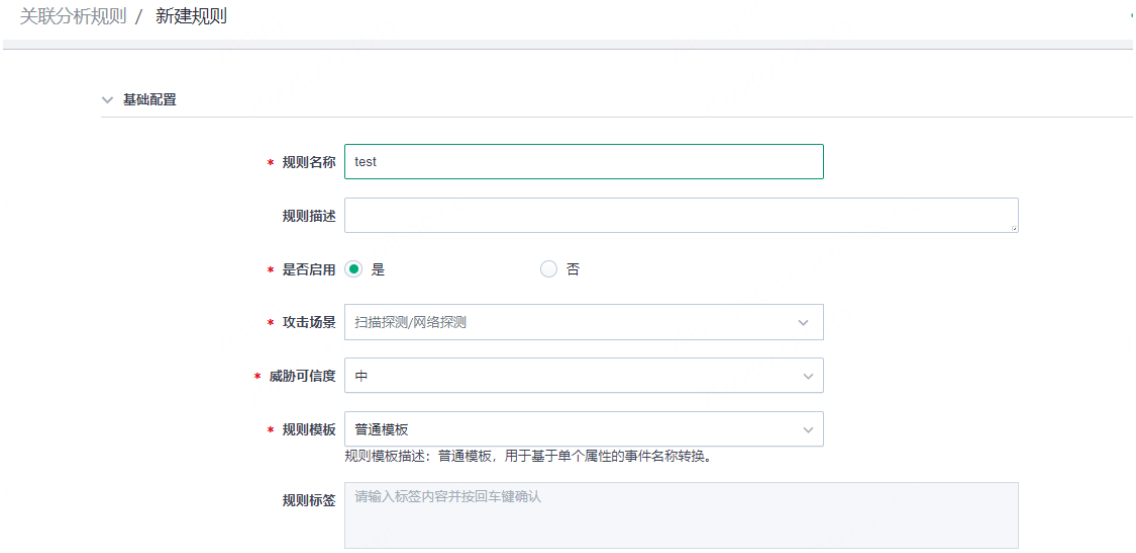
10.1.3 SAE 规则-“普通模板”

场景举例

此模板对单个属性的事件名称转换，如：针对账户在非工作时间异常登录系统的告警。

配置基础信息

步骤1. 单击**“新建”**，弹出配置规则的界面。
步骤2. 配置规则基本信息。



参数名称	参数说明
规则名称	用户自定义规则名称。允许输入 1~64 个字符。规则名称不能重名。
规则描述	用户自定义描述信息。
是否启用	规则添加完成后是否立即生效，默认值“**是**”。 • “**是**”表示立即生效。 • “**否**”表示不生效。
攻击场景	内置告警规则内容。
规则模板	不同模板用途是不一样的，处理逻辑和性能也是不同的，在选择时注意其应用场景，选择合适的模板。 在模板列表中选择一个，规则界面根据规则模板动态更新，根据此处选择的模板后面的配置内容不同，选择后弹出新内容。 模板说明如表 10-1 所示。 选择“**普通模板**”。
全局关联分析使能	选择是否使用全局关联分析，默认值“**否**”。 只有 SAE 分布式达到百万 EPS，且注册多级时，方有此选项。 根据用户实际情况，修改 SAE 规则，打开使能聚合，选择“**是**”。
是否允许下发	当 LAS 系统多级部署时方有此选项。 选择“**是**”，则会将父级的规则下发至子节点（如果有孙节点，亦会下发）。 最末端节点无此选项。
规则标签	支持自定义规则的个性标签。

配置事件源参数

步骤1. 从下拉框中选择相应的“**事件名称**”。

该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

*当配置“**全局事件**”时，必须配置过滤条件。*

步骤2. 单击“**过滤条件** > **编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。

过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

配置输出结果

参数名称	参数说明
输出属性	根据所选的信息模型输出以上输出属性。
添加标记属性	添加的标记属性，主要是日志属性，相当添加一个固定字段，并手动设置该字段的值。 若与日志中的值冲突，以该标记值为准。
内部事件	如果启用内部事件，需添加内部事件的名称。 内部事件的意思是，该条规则的告警数据会转换成一条新的事件重新进入引擎，并可以被引擎中的规则进行分析处理。例如在此例子中，事件的告警会变成 InnerEvent 事件，该事件除了包含规则配置的输出属性，还包括 **event_name=“InnerEvent”** 属性。

配置告警配置的参数

参数名称	参数说明
启用	• 勾选“**是**”后，下面的内容才能进行配置，代表着符合条件的事件发生后会触发告警。 • 勾选“**否**”，不产生告警。
告警阶段	单击下拉框，可以从**侦查**、**投放**、**利用**、**安装**、**控制**、**攻击**六个阶段中选择。
告警级别	单击下拉框，可以从**提醒**、**警告**、**严重**、**致命**中选择。
ATT&CK ID	在下拉列表中勾选适合的 ATT&CK 攻击技术。
告警内容	手动输入告警的内容，并支持**$**引用输出的属性字段。

参数名称	参数说明
告警处置建议	手动输入对告警处置的建议，并支持$引用输出的属性字段。

保存

配置完成后，单击“**保存**”即可新建该条关联分析规则。

10.1.4 SAE 规则-“普通模板-having count(DISTINCT)”

场景举例

此模板是连续多次事件中某个属性出现不同的次数。示例是针对“外部大量主机针对网站发起爬虫攻击”的告警。

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。

步骤3. 根据模板配置规则参数

1. 配置事件源参数，从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

单击“**过滤条件** > **编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。

过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

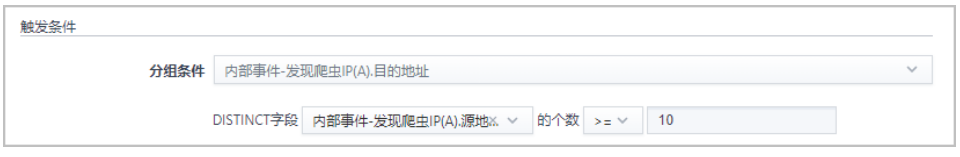
配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

以下设置表示“在 2 分钟以内发现爬虫”。

参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

配置触发条件。

以下设置即：当爬虫的源地址大于等于 10 次时会触发。



步骤4.　配置输出结果。

步骤5. 配置告警配置的参数。

步骤6. 单击“**保存**”即可新建该条关联分析规则。

10.1.5 SAE 规则-“普通模板-having count”

场景举例

此模板是某个事件发生的次数配置告警。示例为针对“内网主机对外部网站发起 web 攻击”的告警。

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。

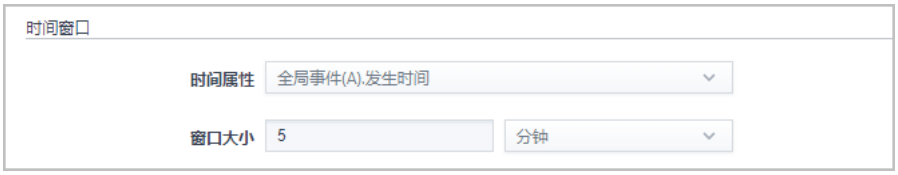
步骤3. 根据模板配置规则参数

1. 配置事件源参数，从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

以下设置表示：事件的发生时间在 5 分钟内。



配置触发条件。

以下设置说明当事件发生的源地址和目的地址多于 5 次时会触发。可添加 DISTINC 字段并设置其条件。在此条件下，当事件发生的源地址和目的地址多于 5 次时会触发。

步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。

步骤6. 配置完成后，单击“**保存**”即可新建该条关联分析规则。

10.1.6 SAE 规则-“普通模板-having sum”

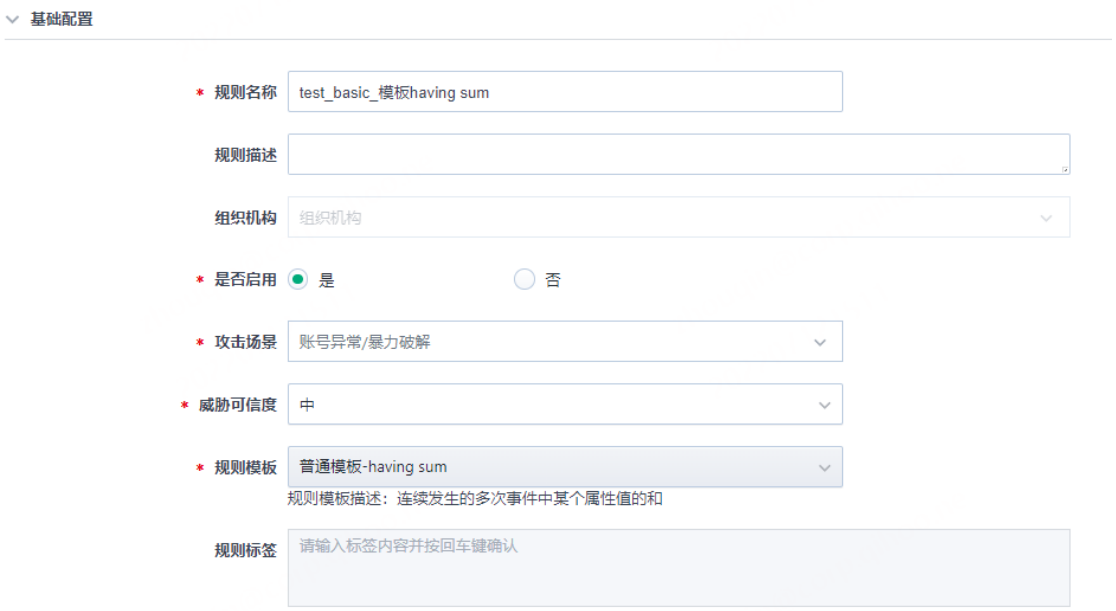
场景举例

此模板是连续多次事件中，某个事件属性的和配置告警。示例为“暴力破解”的告警。

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。



步骤3. 根据模板配置规则参数。

1. 配置事件源参数，从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

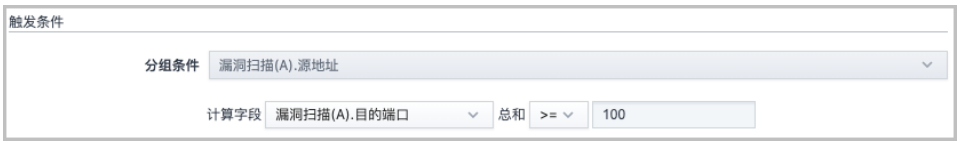
配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

以下设置表示在 1 分钟内漏洞扫描。

参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

配置触发条件。

以下设置说明当扫描端口超过 100 次时会触发。



步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。

步骤6. 单击“**保存**”即可新建该条关联分析规则。

10.1.7 SAE 规则-“普通模板-not_occur”

场景举例

此模板是一段时间内某事件没有发生，则会触发生成告警。

示例：10 秒内没有 webshell 上传事件发生，且以不同的目的地址区分，即会触发生成告警。

前提条件

此模板在日志持续接入的情况下根据模板规则正常生成告警，若无日志接入不会触发告警。

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息，规则模板选择“普通模板-not_occur”。

步骤3. 根据模板配置规则参数。

1. 配置事件源参数，从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

以下设置表示在 10 秒内发生 webshell 上传。

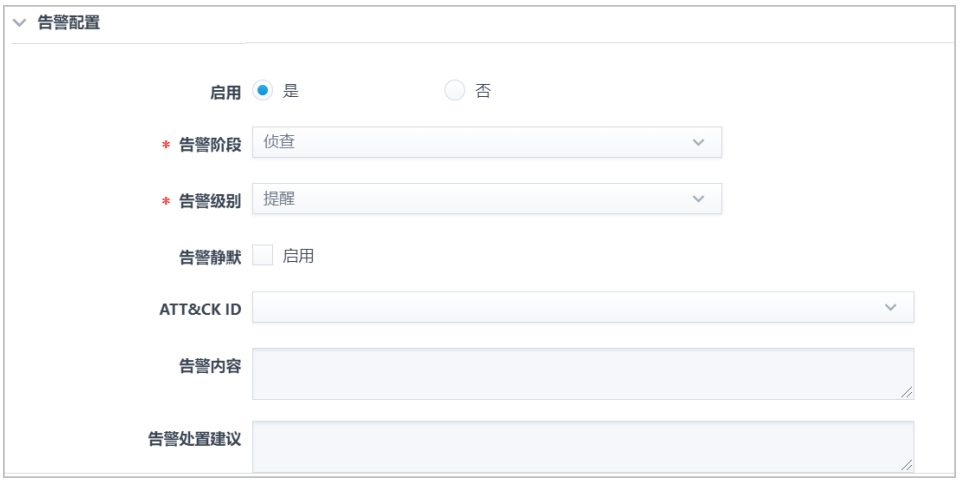
参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

配置触发条件。

以下设置表示以 webshell 上传的目的地址区分。

步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。



步骤6. 单击“**保存**”即可新建该条关联分析规则。

10.1.8 SAE 规则-“关联模板-follow_by”

场景举例

此模板是事件 A 之后，发生了事件 B、C 等。示例中，事件 A：外网主机发起 web 扫描后，发生了事件 B：针对网站发起大量 web 攻击。针对此类事件触发告警。

*如果 followby 的 A 事件是**内部事件**，那么应该把内部事件的**开始时间重命名为开始时间**;*
*如果 followby 的 B 事件是**内部事件**，那么应该把 **B 的结束时间配置为结束时间**。*

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。

步骤3. 根据模板配置规则参数

1. 配置事件源参数。根据选择的模板，至少添加两个事件。从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

（可选）设置事件的过滤条件。单击“**过滤条件 > 编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

（可选）设置关联条件。

如事件 A 的源地址与事件 B 的源地址相同。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

以下设置表示在 10 分钟内外网主机发起 web 扫描。

参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。

步骤6. 单击“**保存**”即可新建该条关联分析规则。

10.1.9 SAE 规则-“关联模板-or_follow_by”

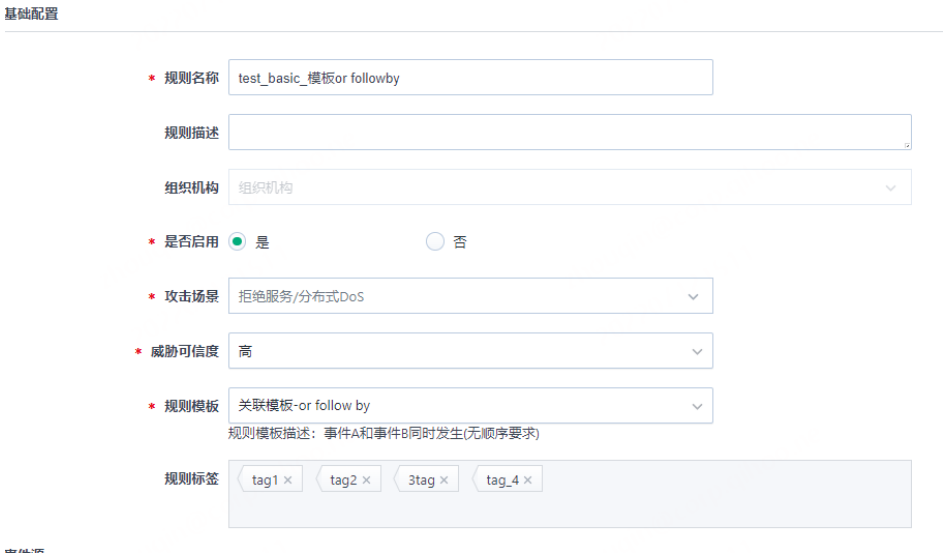
场景举例

同时发生了“事件 A：更改注册表”和“事件 B：创建 Windows 进程”。针对此类情况触发告警。

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。



步骤3. 根据模板配置规则参数。

1. 配置事件源参数，根据选择的模板，显示两个**事件名称**的设置项。从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

（可选）设置事件的过滤条件。单击“**过滤条件** > **编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

如事件 A 的过滤条件，设置注册表的地址。

（可选）设置关联条件。

如事件 A 的“**客户端标识**”、“**进程 ID**”与事件 B 的“**客户端标识**”、“**父进程 ID**”分别相同。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

以下设置表示在 2 分钟内更改注册表。

参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

步骤4.　配置输出结果。

步骤5. （可选）配置预案触发条件。

步骤6. 配置告警配置的参数。

步骤7.　配置完成后，单击“**保存**”即可新建该条关联分析规则。

10.1.10 SAE 规则-“关联模板-not_follow_by”

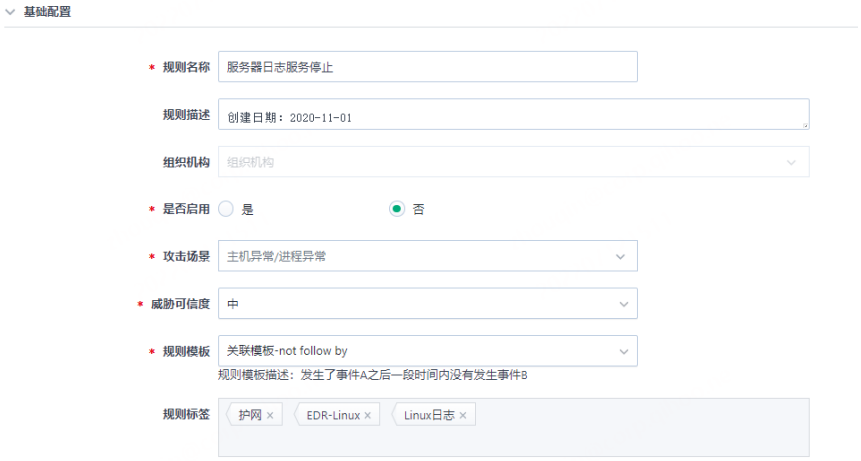
场景举例

发生了“事件 A”后，没有发生“事件 B”。针对此类情况触发告警。

操作步骤

步骤1.　单击“**新建**”，弹出配置规则的界面。

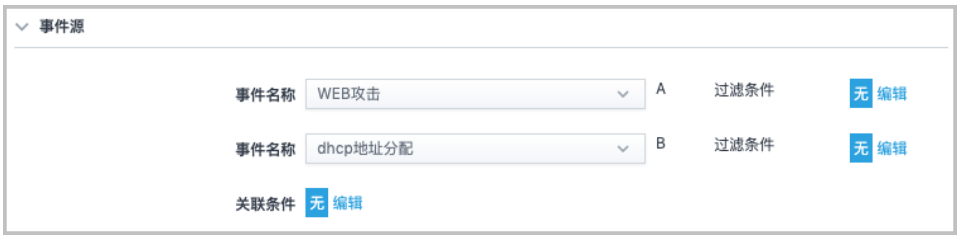
步骤2.　配置规则基本信息。



步骤3.　根据模板配置规则参数。

1. 配置事件源参数。根据选择的模板，显示两个**事件名称**的设置项。从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。



（可选）设置事件的过滤条件。单击“**过滤条件 > 编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

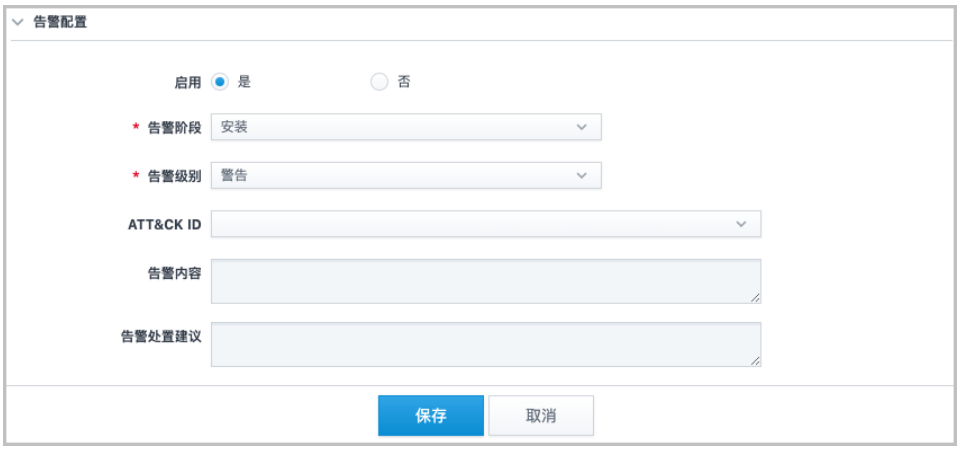
（可选）设置关联条件。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。



步骤6. 配置完成后，单击“**保存**”即可新建该条关联分析规则。

10.1.11 SAE 规则-“关联模板-Repeat-Until”

场景举例

发生 N 次“事件 A：web 攻击”后发生了“事件 B：漏洞扫描”。

操作步骤

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。

步骤3. 根据模板配置规则参数。

1. 配置事件源。根据选择的模板，设置重复下限的次数及两个**事件名称**。从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

（可选）设置事件的过滤条件。单击“**过滤条件** > **编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

（可选）设置“**关联条件**”。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

参数名称	参数说明
时间属性	在下拉列表中选择事件属性的字段。
窗口大小	填写窗口的时间及单位。

步骤4. 配置输出结果。

步骤5. （可选）配置预案触发条件。

步骤6. 配置告警配置的参数。

步骤7.　配置完成后，单击“**保存**”即可新建该条关联分析规则。

10.1.12 SAE 规则-“关联模板-any_order”

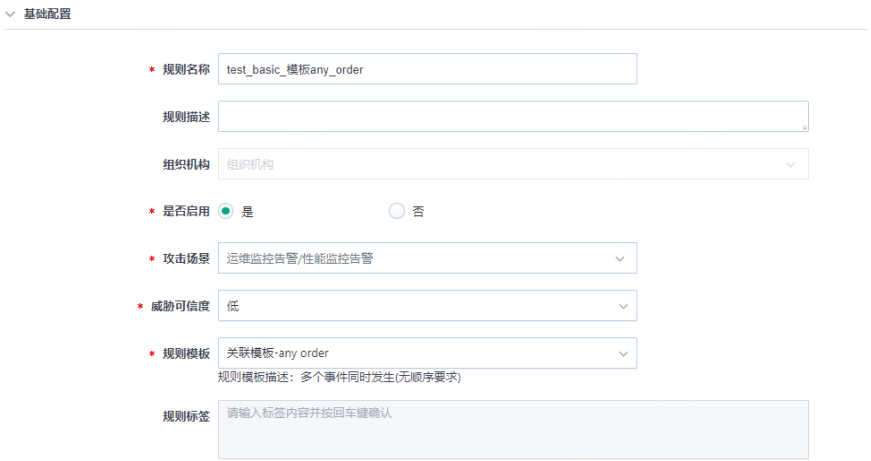
场景举例

发生多个事件，且无顺序要求。当前仅支持两个事件。

操作步骤

步骤1.　单击“**新建**”，弹出配置规则的界面。

步骤2.　配置规则基本信息。



步骤3.　根据模板配置规则参数。

1. 配置事件源。根据选择的模板，可设置多个**事件名称**。从下拉框中选择相应的“**事件名称**”。

该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

（可选）设置事件的过滤条件。单击“**过滤条件 > 编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。

步骤6. 配置完成后，单击“**保存**”即可新建该条关联分析规则。

10.1.13 SAE 规则-“关联模板-not_before”

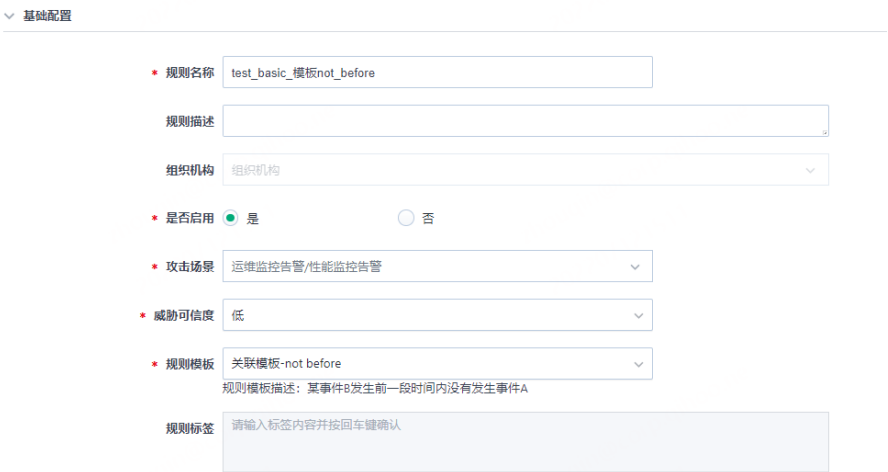
场景举例

发生事件 B 之前，没有发生事件 A。

配置基础信息

步骤1. 单击“**新建**”，弹出配置规则的界面。

步骤2. 配置规则基本信息。



步骤3. 根据模板配置规则参数。

1. 配置事件源。根据选择的模板，可设置两个**事件名称**。从下拉框中选择相应的“**事件名称**”。

   该**事件名称**表示事件解析后的事件名称，与事件分类中的事件名称保持一致。

（可选）设置事件的过滤条件。单击“**过滤条件** > **编辑**”，打开“**过滤条件**”的对话框，使用条件编辑器。过滤条件的使用方式请参见 C 在 SAE 关联分析规则中的应用。

配置“**时间窗口**”参数，即在时间内符合条件的会触发告警。

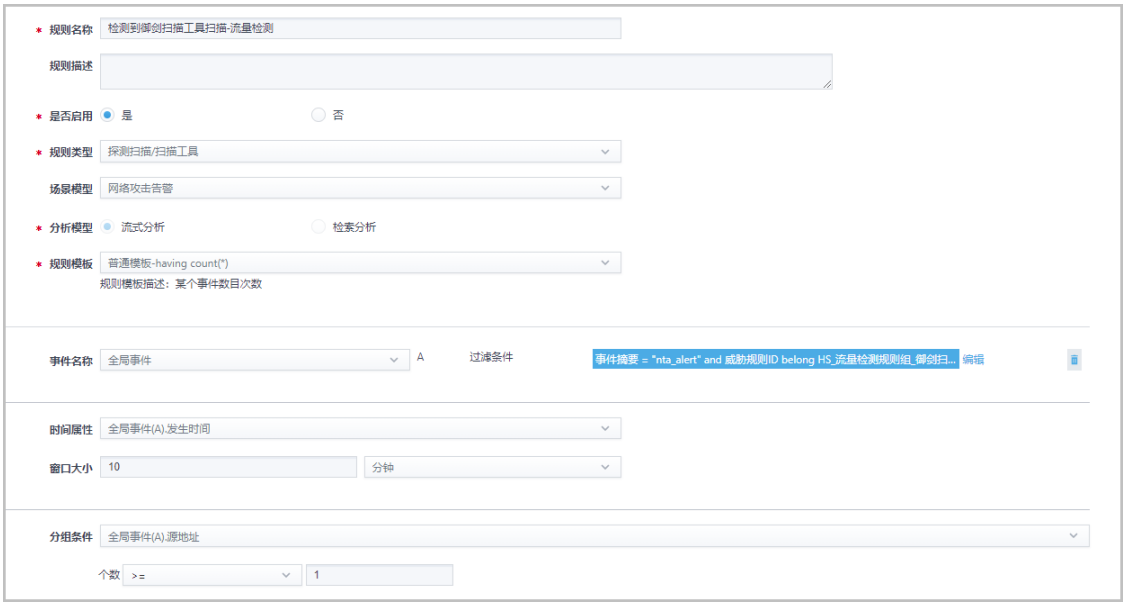
步骤4. 配置输出结果。

步骤5. 配置告警配置的参数。

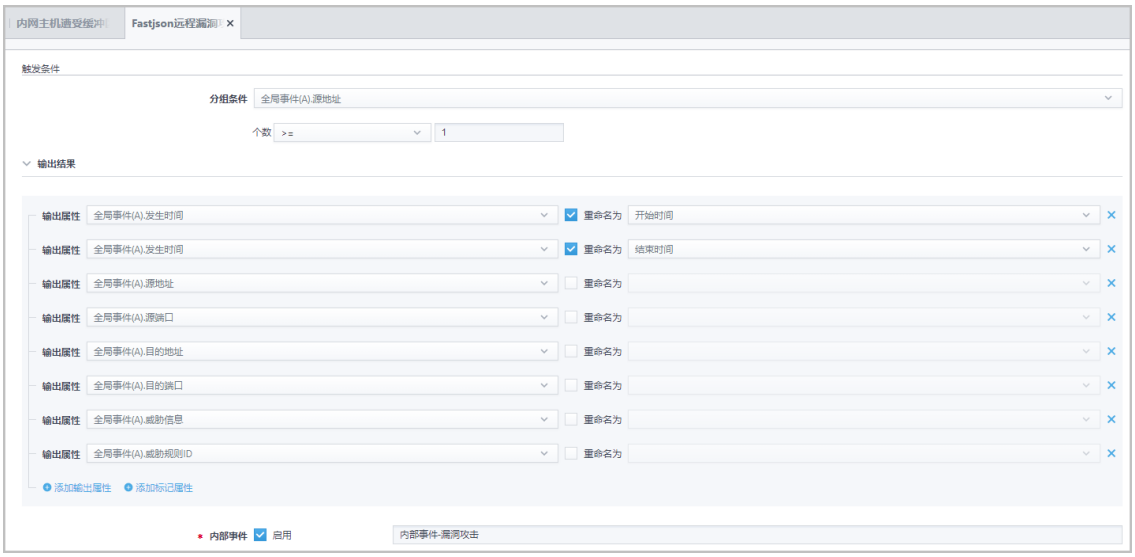
步骤6.　配置完成后，单击“**保存**”即可新建该条关联分析规则。

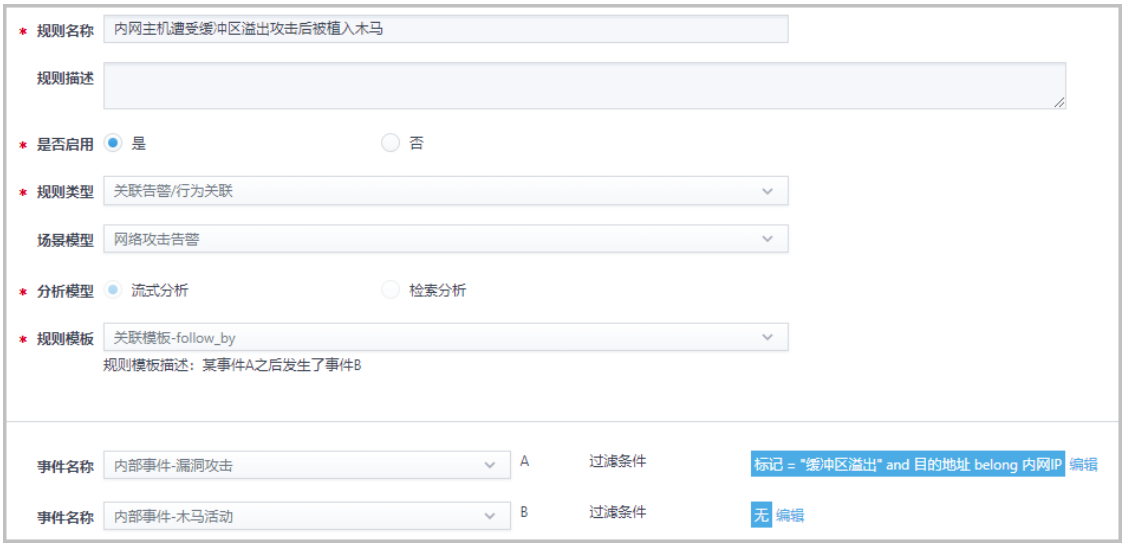
10.1.14 非法配置举例

模板选择错误，统计类规则，触发条件>=1



内部事件没有输出相关属性，导致引用内部事件的规则无效





过滤条件、关联条件理解错误，在关联条件中配置某一事件的过滤条件

未启用告警及内部事件，导致规则无效

10.1.15 导出规则

- 勾选需导出的规则，单击“ ⋮ > **导出**”，勾选的规则以文件形式自动下载到默认下载位置中。
- 若不勾选，导出所有关联分析规则。

10.1.16 导入规则

前提条件

单击“ ⋮ > **导出**”，目前列表中存在的规则以文件形式自动下载到默认下载位置中。您可以在此基础上编辑新的规则。

背景信息

规则在逻辑上分为系统规则和用户自定义规则。

- 出厂自带的规则都属于系统规则。
- 用户在该规则上有过修改的动作或者新增的规则都属于自定义规则。

注意事项

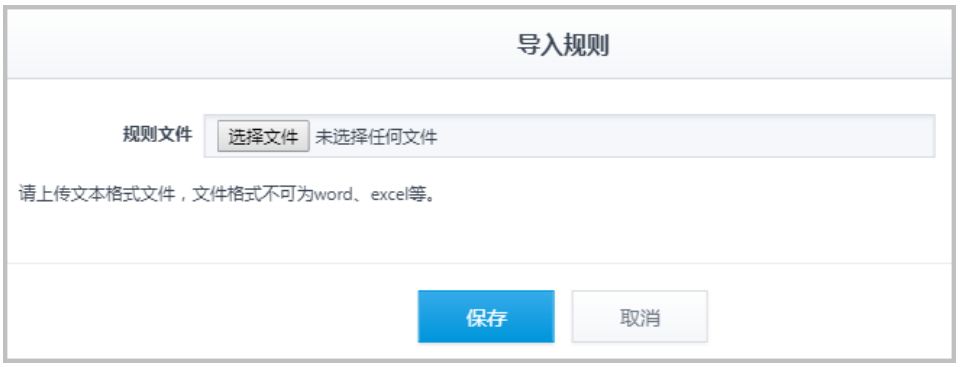
检查导入的规则是否与 SAE 中已有的规则有重名并给出提示。

- 系统内置规则指 LAS 系统安装好之后就有的且没有经过编辑的规则。如果导入的规则与系统内置规则有重名，则直接覆盖，且页面不会弹出提示。
- 用户自定义规则指系统安装好之后用户自己添加的规则，或者在内置的规则上进行过修改保存的规则。重名的三种策略处理的效果分别如下：

- 覆盖：更新原有的规则为最新。
- 重名：在原有的规则名后面加数字作为新的名称导入。
- 跳过：重名的规则不导入。

操作步骤

步骤1. 单击“ ⋮ > **导入**”，弹出如下提示框：



步骤2. 单击“**选择文件**”，弹出文件选择器，选择符合要求的文件。

步骤3. 单击“**保存**”，确认导入。

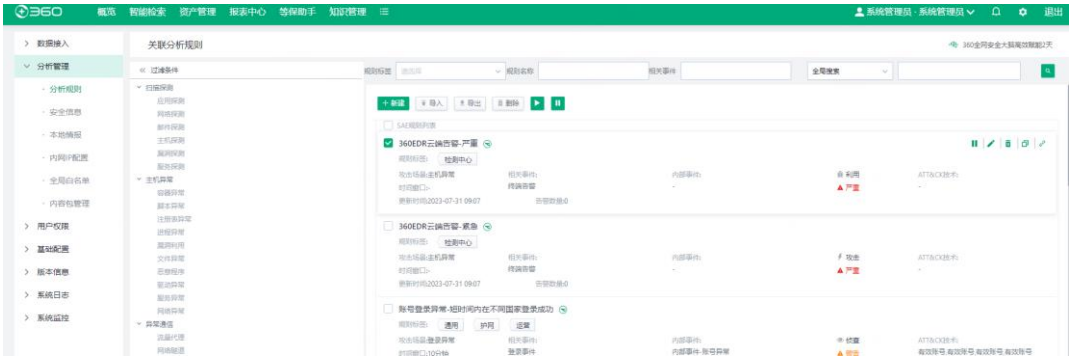
- 若选择的文件类型不符合要求，提示：“**导入的文件非法！导入失败！**”
- 若选择的文件类型且规范符合要求，且存在同名或者同模板的情况，跳出相应提示。
  - 选择“**取消**”，放弃导入；
  - 选择“**重命名**”：在原有的规则名后面加数字作为新的名称导入；
  - 选择“**覆盖**”：更新原有的规则为最新；
  - 选择“**跳过**”，重名的规则不导入。

- *如果检查结果没有重名的则直接导入不会出现提示。*
- *导入的规则默认情况下不启动。*
- *如果导入规则时用户选择了指定的分类，则导入之后的规则属于该分类下；如果没有指定分类，则导入的规则属于原来的分类。若原来的分类不存在，则属于根分类。*

导入成功后，导入成功的规则出现在列表中；若有导入失败的情况发生，会出现提示框说明导入的情况。

10.1.17 更多操作

选中一条规则后，方可显示对该条规则更多的操作。



操作	说明
复制	单击，即复制出一条与此规则配置相同的第二条规则（命名不同），基于原有信息进行编辑以新增关联分析规则。
修改	单击，修改该条规则的信息。
停止	规则创建完成后，若符合要求，则自动启动。若需要停止该规则的运行，您可以执行以下操作。 • 单击，停止该条规则运行。 • 当规则列表中有多条数据需要停止，可通过勾选需停止的数据，单击列表上方的，可批量停止多条数据。
启动	若关联分析规则被停止运行。若需要恢复该规则的运行，您可以执行以下操作。 • 单击，恢复该条规则运行。 • 当规则列表中有多条数据需要恢复运行，可通过勾选需恢复的数据，单击列表上方的，可批量启动多条数据。
查询	您可以通过以下四个字段进行搜索关联分析规则。 • 规则标签 • 规则名称 • 相关事件 • 更多搜索维度：默认为**全局搜索**。通过下拉选择**内部事件**、**规则模板**、**分析模型**、**信息组**和**动态信息组**。 以上字段均支持模糊搜索，此处以“**规则名称**”为例，介绍如何查询关联分析规则。 在“**规则名称**”的输入框中输入规则名称的关键字，按回车键，执行查询，系统自动模糊查询出包含查询关键字的规则，以列表方式展示。

操作	说明
删除	• 单击 ，删除该条规则的数据。 • 当规则列表中有多条数据需要删除，可通过勾选需删除的数据，选择并单击“ > **删除**”，可批量删除多条数据。

10.2 维护安全信息

安全信息管理展示有价值的内部信息，在关联分析时，对于 IP 类型、数字类型或字符类型的字段可以添加过滤条件属于信息，便于进行分析。初始化时通过导入内容包，LAS 系统中已内置一些安全信息数据：

10.2.1 配置信息组分类

为了更好的展示信息组及所属类别，在左侧过滤条件区展示信息组分类。

背景信息

系统默认所有信息分类为“**IP 类信息**”、“**数字类信息**”、“**字符类信息**”和“**时间类信息**”，可以在这四类信息类型下新建更多的信息组分类。

操作步骤

步骤1. 在导航栏单击，选择“**分析管理** > **安全信息**”，LAS 系统默认显示“**安全信息**”页面。

步骤2. 单击左侧“**信息管理**”分类中的“**管理**”，弹出“**编辑过滤条件**”的管理对话框。

步骤3. 将鼠标悬停在左侧信息组一类信息时，会出现 ，单击之，弹出“**添加分类**”对话框。

步骤4. 输入自定义的分类名称。

步骤5.　单击“**确定**”，完成添加。

更多操作

操作	说明
修改	您可以通过单击信息组节点后的，修改信息组的名称，不支持修改“**信息类型**”。
删除	您可以通过单击信息组节点后的×，删除自定义的信息分类。 • 不支持删除内置的信息分类。 • 若在此信息分类下存在信息数据，则不允许删除，并弹出提示。 *不支持修改、删除根节点。*

10.2.2 配置信息组

当需要新增一个内部信息，原信息分组中没有其所属组别，则需先创建一个新的信息组。

背景信息

配置的信息主要用于关联分析规则的过滤条件，适用于 belong 操作符，如：

操作步骤

步骤1. 在“**安全信息**”页面，单击左侧“**信息分类**”中选择一分类，以“**数字类信息**”下的“**网络端口**”为例。

步骤2. 在信息组列表区，单击“**新增**”，弹出“**添加信息组**”的对话框。

步骤3. 填写信息组相关参数。

参数名称	参数说明
信息组分类	已选择的信息组分类。
信息组名称	信息组的名称。允许输入 1~64 个字符，不能重名。
信息类型	不同的信息分类对应的信息类型分别如下： • IP 类：IP • 数字类：端口 • 字符类： – 正则部分匹配 – 字符串比较 – 正则全匹配 • 时间类： – 相对时间 – 绝对时间

步骤4. 单击“**确定**”，完成添加。

更多操作

不支持修改、删除 LAS 系统内置的信息组。

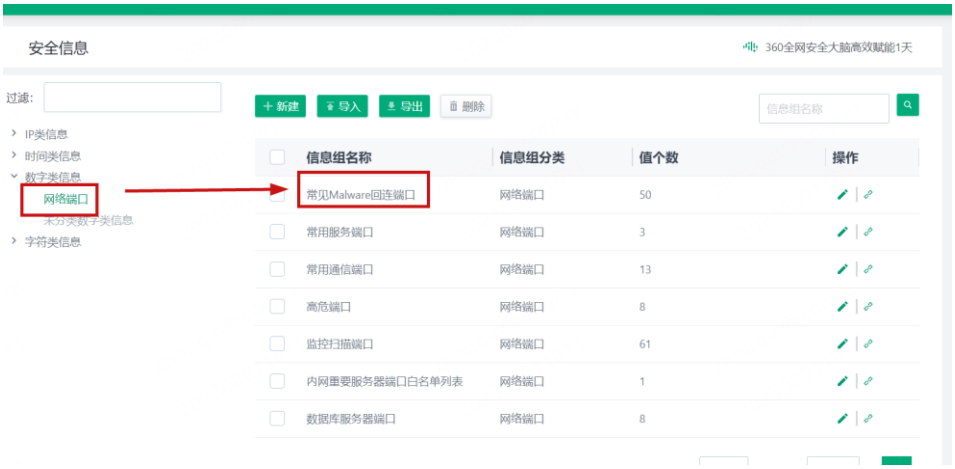
操作	说明
修改	您可以通过单击信息组操作列的，仅支持修改自定义的信息组的信息组名称。
导出	如需导入 LAS 系统中已有的全部或者部分信息组，可单击“**导出**”，导出信息组文件
导入	如有批量导入信息组的 excel 文件，您可以通过单击“**导入**”，打开本地目录，添加上传。
删除	选中待删除的一条或多条信息组数据，单击 “**删除**”，删除自定义的信息组。
查看引用的 SAE 规则	单击一信息组操作列的，可跳转至“**关联分析规则**”下，显示引用此信息组的 SAE 规则。

10.2.3 配置信息

您可以配置信息，对信息行新增、修改及删除的操作。

操作步骤

步骤1. 在“**安全信息组**”列表页面单击一安全信息组，如下图所示。



步骤2. 单击信息组，进入此信息组的信息列表页面。

步骤3. 单击“**新建**”，弹出添加信息界面。

步骤4. 配置信息相关参数。

表10-2 IP 类信息组

参数名称	参数说明
所属信息组	已选择的信息组。
内容类型	单击弹出下拉框，IP 类信息中内容类型有值、区间、子网掩码三种。

参数名称	参数说明
信息内容	输入该信息的内容。 • “**内容类型**”选择值时，需要输入一个格式正确的精确的 IP 地址。 • “**内容类型**”选择区间时，需要输入区间两端的 IP 地址。 • “**内容类型**”选择子网掩码时，需要输入 IP 地址和掩码位数。

表10-3 数字类信息组

参数名称	参数说明
信息类型	信息类型为数字类信息。
内容类型	单击弹出下拉框，数字类信息中内容类型包括精确值和区间。
信息内容	输入该信息的内容。 • “**内容类型**”选择精确值时，需要输入一个格式正确的精确的端口号。 • “**内容类型**”选择区间时，需要输入区间两端点的端口号。

表10-4 字符类信息组

参数名称	参数说明
信息类型	信息类型为字符类信息。
内容类型	内容类型只能选择精确值。
信息内容	输入字符形式的信息内容。

表10-5 时间类信息组（相对时间）

参数名称	参数说明
信息类型	信息类型为时间类信息。
内容类型	内容类型只能选择值。
每周时间	勾选每周的信息时间的复选框。
时间段	需要输入一个精确的时间段。

表10-6 时间类信息组（绝对时间）

参数名称	参数说明
信息类型	信息类型为时间类信息。
内容类型	内容类型只能选择值。
时间段	需要输入一个精确的时间段。

步骤5. 配置完成后，单击“**确认**”，信息添加成功，弹出提示。

*首次新增信息数据后，“**导出**”呈现可用状态。您可单击导出信息文件“**intellgence.xlsx**”，excel 文件中包含已配置的信息数据，在文件中新增信息数据后，再在 LAS 系统系统中导入。*

更多操作

在信息列表页面还支持以下操作：

操作	说明
导出	首次新增信息的数据后，“**导出**”控件呈现可用状态。您可单击导出信息文件“intellgence.xlsx”，excel 文件中包含已配置的信息数据，在 excel 文件中新增信息数据后，再在 LAS 系统系统中导入。
导入	您可以通过单击“**导入**”，打开本地目录，添加 excel 格式的文件。
修改	您可以通过单击信息列表操作列的，修改信息内容。不支持修改“**信息类型**”和“**内容类型**”参数。
删除	• 方式一：您可以通过单击信息列表操作列的，删除该条信息数据。 • 方式二：当信息列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入信息内容的关键字，按回车键，执行查询，系统自动模糊查询出信息内容包含查询关键字的信息数据，以列表方式展示。

10.3 管理本地情报

情报白名单管理用于展示和管理威胁情报的白名单和黑名单信息。在分析威胁情报时，对于 IP 类型 Domain 类型的字段可以添加过滤条件，使其属于情报白名单，便于进行分析。情报白名单类型包括：IP 和 Domain 类型。也可以在页面添加或者导入情报黑名单，当日志中的

数据匹配上黑名单后，就会生成对应的威胁情报告警，便于安全分析。您可以在配置页面新增、导入、修改、删除和查询情报白名单内容。

背景信息

目前支持新增的情报白名单类型包括：IP 和 Domain 类型，其中 IP 类型包含 IPV4 值、IPV4 区间、IPV4 子网掩码、IPV6 值、IPV6 区间、IPV6 前缀，共 6 种。本章节以新增 Domain 类型的情报白名单为例，介绍如何维护情报白名单。

操作步骤

步骤1. 在导航栏单击，选择“**分析管理** > **本地情报**”，在 LAS 系统显示“**本地情报**”管理页面。

步骤2. 单击“**新建**”，显示新增页面，如下图所示。

步骤3. 在下拉框选项中，选择“**情报类型**”为“**DOMAIN**”，选择情报的黑白属性，输入“**DOMAIN**”值，并单击“**保存**”。

更多操作

操作	说明
导出	首次新增情报数据后，“**导出**”控件呈现可用状态。您可单击导出情报文件“whitelist.xlsx”，excel 文件中包含已配置的情报数据，您可在 excel 文件中新增情报数据后，再在 LAS 系统中导入本地情报。
导入	您可以通过单击“**导入**”，打开本地目录，选择已编辑的文件。
修改	您可以通过单击情报列表操作列的，修改情报的信息。

操作	说明
删除	• 方式一：您可以通过单击情报列表操作列的，删除该条情报数据。 • 方式二：当情报列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入情报的“**情报内容**”，按回车键，执行查询，系统自动模糊查询出情报内容包含查询关键字的情报白名单信息，以列表方式展示。

10.4 管理全局白名单

白名单管理用于展示和管理全局的白名单信息。当发送的日志中包含全局白名单（IP、Domain、URL 和 ACCOUNT）时，就不会触发 SAE 规则产生告警。您可以在配置页面新增、导入、修改、删除和查询全局白名单内容。

背景信息

目前支持新增的全局白名单类型包括：IP、Domain、URL 和 ACCOUNT 类型。本章节以新增 Domain 类型的全局白名单为例，介绍如何维护全局白名单。

操作步骤

步骤1. 在导航栏单击，选择“**分析管理** > **忽略白名单**”，在 LAS 系统显示“**忽略白名单**”管理页面。

步骤2. 单击“**新建**”，显示新增页面，如下图所示。

步骤3. 在下拉框选项中，分别选择“**白名单类型**”和“**内容类型**”为“**IP**”和“**值**”，输入白名单内容，并单击“**保存**”。

更多操作

操作	说明
导出	首次新增忽略白名单数据后，“**导出**”控件呈现可用状态。您可单击导出白名单文件“global_whitelist.xlsx”，excel 文件中包含已配置的白名单数据，您可在 excel 文件中新增白名单数据后，再在 LAS 系统中导入白名单。
导入	您可以通过单击“**导入**”，打开本地目录，选择已编辑的文件。
修改	您可以通过单击白名单列表操作列的，修改白名单的信息。
删除	• 方式一：您可以通过单击白名单列表操作列的，删除该条白名单数据。 • 方式二：当白名单列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入白名单的“**白名单内容**”，按回车键，执行查询，系统自动模糊查询出内容包含查询关键字的白名单信息，以列表方式展示。

10.5 管理内容包

资源初始化后，您还可以更新、导出内容包，回滚至导入前的状态。

前提条件

您已获取所需的内容包（.zip 包），获取方式请联系 360 技术支持。

导入内容包

步骤1. 在导航栏单击，选择“**分析管理** > **内容包管理**”，在 LAS 系统显示“**内容包管理**”页面。

步骤2. 在导入区域，可以单击“**上传文件**”，弹出本地文件系统，选择需要导入的文件，单击“**打开**”。

步骤3. 单击“**导入**”。

- 导入成功后，给出提示信息，显示：**导入成功。
- 导入失败后，给出错误提示信息，包括：文件格式错误，文件大小（系统支持最大 20M 的文件导入）错误，文件内容不合法错误。

内容包回滚

在下拉列表中选择待回滚的镜像，根据需要是否打开保留用户修改的开关，单击“**确认回滚**”，即可回滚至导入前的配置。

导出内容包

勾选需要导出的模块，单击“**导出**”，会以“.zip”的文件格式存储在本地文件系统。

*导出文件的依赖关系。其中：**事件**、**安全信息**、**知识库**和**案例库**、**图表**、**安全事件规则**、**应用联动**是可以单独导出的模块，不需要依赖其他的模块。*

*但是**解析规则**、**关联分析**、**仪表盘**、**报表模板**、**预案**、**自动化脚本**的导出都是有模块依赖关系的，即系统会自动勾选依赖的模块一起导出。*

11. 管理用户

用户权限管理提供了一个对系统组织机构、角色及用户进行展示和维护的平台。您可以创建、维护系统本地用户，也可以通过 LDAP 添加、维护用户。

11.1 开启数据分权

本地用户、LDAP 用户均会配置所属组织机构，以便于用户的维护和管理。

在“**本地用户**”和“**LDAP 用户**”页面下，通过左侧的树形控件可以查看维护系统本地用户和 LDAP 用户的组织机构。单击左侧树形控件中某组织机构，右侧列表展示该组织机构及下级组织机构下的所有用户。

以“**本地用户**”为例，介绍如何创建组织机构。

操作步骤

步骤1. 在导航栏单击，选择“**用户权限 > 本地用户**”，LAS 系统进入“**本地用户**”页面。

步骤2. 开启/关闭“组织机构数据分权条件启用”开关，决定是否启用数据分权功能。

11.2 配置组织机构

本地用户、LDAP 用户均会配置所属组织机构，以便于用户的维护和管理。

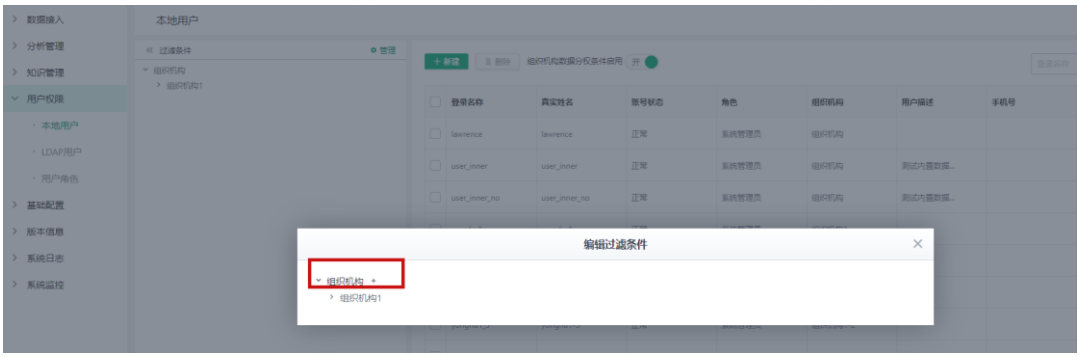
在“**本地用户**”和“**LDAP 用户**”页面下，通过左侧的树形控件可以查看维护系统本地用户和 LDAP 用户的组织机构。单击左侧树形控件中某组织机构，右侧列表展示该组织机构及下级组织机构下的所有用户。

以“**本地用户**”为例，介绍如何创建组织机构。

操作步骤

步骤1. 在导航栏单击，选择“**用户权限** > **本地用户**”，LAS 系统进入“**本地用户**”页面。

步骤2. 单击页面左侧“**过滤条件**”中的“**管理**”，弹出“**编辑过滤条件**”对话框。



步骤3. 单击组织机构根节点后的添加按钮，弹出“**添加组织机构**”对话框，如图所示。

步骤4. 配置组织机构相关参数。

参数名称	参数说明
名称	输入组织机构名称信息，允许输入 1~64 个字符。
描述	输入组织机构描述，允许输入 1~255 个字符。
数据分权	若开启数据分权，该项可编辑，后续该组织机构下的用户将根据此条件进行数据分权。 若未开启数据分权，该项不可编辑。

步骤5. 单击“**确定**”，完成组织机构添加。

更多操作

操作	说明
修改	在“**编辑过滤条件**”对话框中，您可以通过单击组织结构树节点后的，修改组织结构的参数。

操作	说明
删除	在“**编辑过滤条件**”对话框中，您可以通过单击组织结构树节点后的×，删除该条组织结构。

- *不支持修改、删除根节点。*
- *删除某一组织机构时，下级组织机构以及用户信息都将被删除，请谨慎操作。*

11.3 配置本地用户

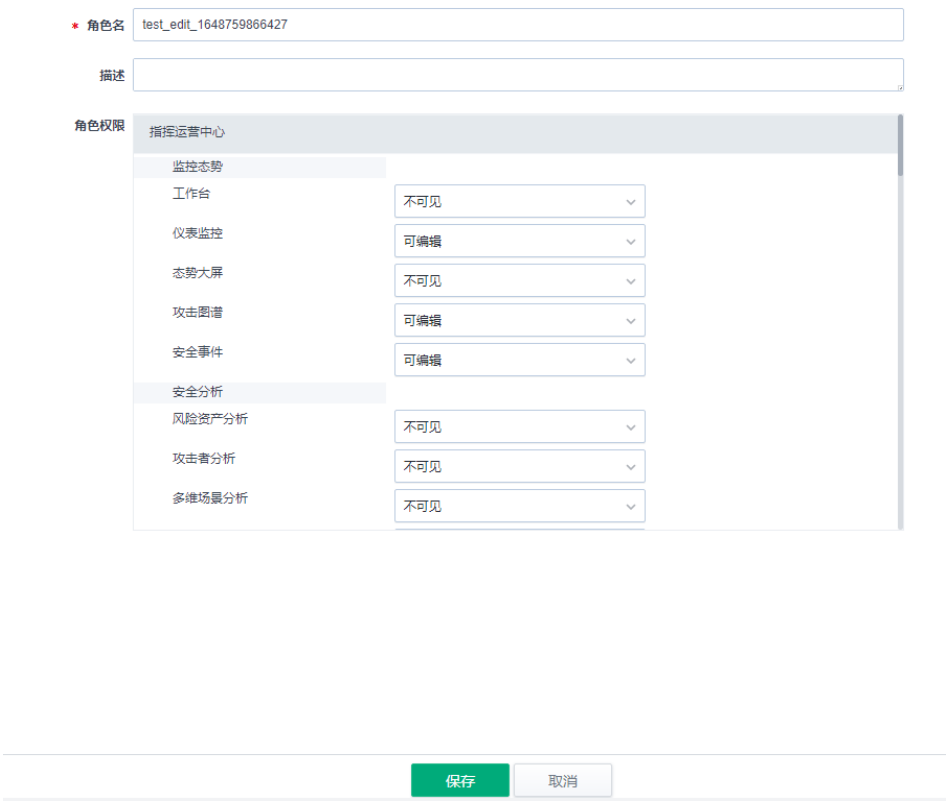
11.3.1 配置角色

在创建本地用户时需要为其选择角色，您可以通过创建不同的角色赋予其相应的角色权限。每个角色对菜单有不同的权限。系统内置“**安全保密管理员**”、“**安全审计员**”和“**系统管理员**”三种角色。

操作步骤

步骤1. 选择菜单“**用户权限** > **用户角色**”，LAS 系统进入“**用户角色**”管理界面。

步骤2. 在角色列表展示界面，单击“**新建**”，弹出角色新增界面。



步骤3. 填写角色相关参数。

表11-1 配置角色参数

参数名称	参数说明
角色名	角色名称。可输入 1~64 个字符。
描述	对该角色的描述。
角色权限	设置添加角色对于各个菜单的权限，权限有三种： • 不可见：默认为不可见。当设置菜单项为不可见，则配置该角色的用户登录后无法看到该菜单项。 • 只读：当设置菜单项为只读，则配置该角色的用户登录后对该菜单项显示的所有内容只有只读权限。 • 可编辑：当设置菜单项为可编辑，则配置该角色的用户登录后对该菜单项显示的所有内容拥有读写权限。 *在配置角色时，不能设置所有菜单权限均为“**不可见**”。*

步骤4. 单击“**确认**”，完成角色的新增。

- 若输入的角色名称与已存在的角色重复，会弹出相应提示框。
- 角色新增成功后，弹出如图所示提示框。

更多操作

操作	说明
修改	您可以通过单击角色列表操作列的 ，可修改“**角色名称**”、“**描述**”和“**角色权限**”。
删除	• 您可以通过单击角色列表操作列的 ，删除该角色。 • 当角色列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。

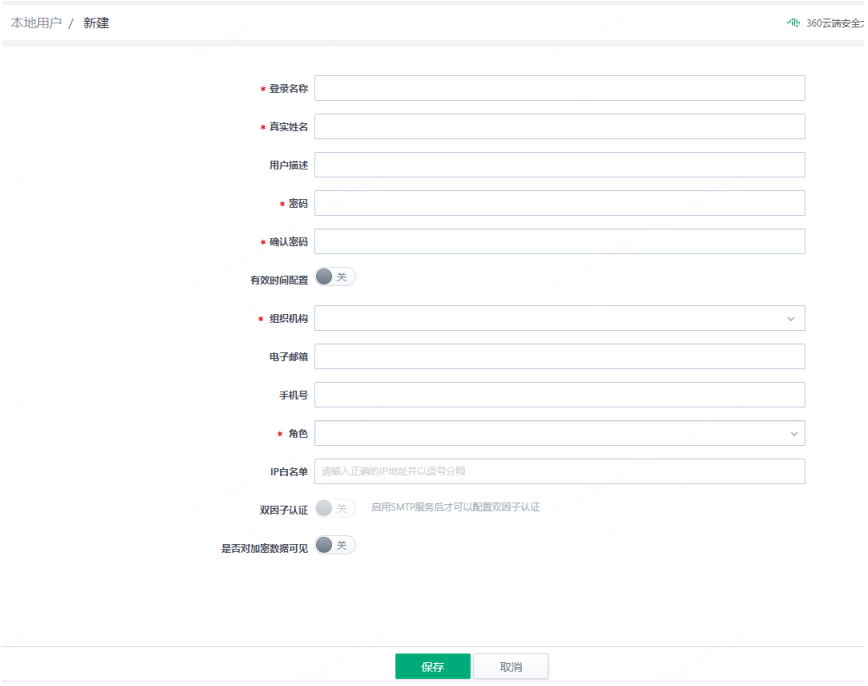
11.3.2 配置本地用户

用户以列表的方式展示，默认内置 3 个用户，分别是：系统管理员 sysadmin、安全保密管理员 secadmin 和安全审计员 auditadmin。您可以对本地用户进行新增、修改、删除等操作。

操作步骤

步骤1. 选择菜单“**用户权限** > **本地用户**”，LAS 系统进入“**本地用户**”管理界面。

步骤2. 单击“**新建**”，弹出用户新增界面。



步骤3. 配置本地用户相关参数。

表11-2 配置本地用户参数

参数名称	参数说明
登录名称	登录的用户名称，该名称为用户的唯一标识，不同用户的登录名称不可相同。可输入 1~64 个字符。
真实姓名	用户的真实姓名，可输入 1~64 个字符。
用户描述	输入对该用户的描述，方便了解、管理用户。
密码	用户登录的密码，密码要求 8 位以上，必须包含字母、数字、特殊字符。
确认密码	确认用户的密码，输入内容应与密码相同，密码要求 8 位以上，必须包含字母、数字、特殊字符。
有效时间配置	打开此开关，弹出“**有效到期时间**”配置参数，配置该用户的有效期。
有效到期时间	单击配置框，弹出时间管理器，选择该用户有效期的到期时间。如设置的是“**2020 年 5 月 31 日**”，则从 2020 年 6 月 1 日 0 点起，该用户到期失效，无法登录 LAS 系统。
组织机构	选择用户所属的组织机构。
电子邮件	输入用户的邮箱。 *配置用户 A 的邮箱后，当某条安全事件的责任人设置为用户 A 时。如若在“**本地用户**”处配了用户 A 的邮箱，则系统会自动发邮件通知用户 A。*
手机号	用户的手机号。
角色	设置添加用户的角色，勾选表示为用户配置该角色，可以为用户配置多个角色。用户对菜单项的权限为所有角色权限的合集。
IP 白名单	输入与用户绑定的 IP 地址，用户的 IP 只有属于白名单 IP 才可以登录 LAS 系统。 支持多个 IP，请使用英文逗号隔开。
双因子认证	打开此开关后，登录 LAS 系统时，该用户需要输入邮箱发送的验证码，输入正确的验证码后，该用户方可成功登录。 **前提条件** *您已经配置 SMTP，方可接收邮箱发送的消息。*
是否对加密数据可见	打开此开关后，该用户在“**指挥中心**”的“**智能分析 > 日志查询**”和“**安全事件**”的关联事件中能够查看到已加密的数据； 若关闭此开关，则无法查看已加密的数据。

步骤4. 单击“**保存**”，完成用户的新增。

- 若输入的登录名称与已存在的用户重复，会弹出相应提示。
- 用户新增成功后，弹出相应提示，新增用户则会在列表中显示。

更多操作

操作	说明
修改	您可以通过单击本地用户列表操作列的 ，可修改用户信息。
删除	• 您可以通过单击本地用户列表操作列的 ，删除该用户。 • 当本地用户列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入“**登录名称**”，如“admin”，并按回车键，查询出登录名中含有 admin 关键字的用户，以列表方式展示。
锁定/解锁	使用 admin 用户单击被锁定用户列表操作栏的 ，对该用户进行解锁/锁定。 用户被锁定后不允许登录系统，如果需要登录系统，需要手动解锁用户。

11.4 配置 LDAP 用户

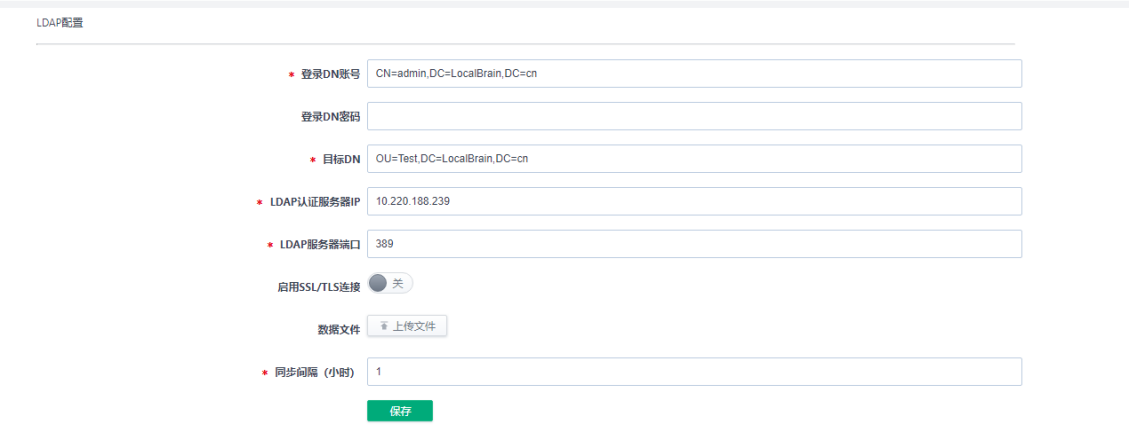
11.4.1 连接 LDAP 服务器

当在 LAS 系统中配置企业域账号，需要集成 LDAP 用户，则请先连接 LDAP 服务器。

操作步骤

步骤1. 在导航栏单击 ，选择“**基础配置** > **环境信息**”，LAS 系统进入“**环境信息**”页面。

“**LDAP 配置**”区域如下所示。



步骤2. 配置相关参数。

参数名称	参数说明
登录 DN 账号	根据实际情况，配置为用户域服务器的 AD 账号。 示例： CN=gitlab,OU=NJ,OU=qihoo,DC=qihoo,DC=com
登录 DN 密码	根据实际情况，配置为用户域服务器的 AD 账号密码。
目标 DN	根据实际情况，配置为用户域服务器的目标 DN。 OU=qihoo,DC=qihoo,DC=com
LDAP 认证服务器 IP	根据实际情况，配置为用户方 LDAP 认证服务器 IP 地址。
LDAP 认证服务器端口	根据实际情况，配置为用户方 LDAP 认证服务器端口号。 示例： 389 或 636
是否启用 SSL/TLS 连接	根据需求，选择是否需要配置加密链接： • 启用 SSL/TLS 连接：加密连接 • 关闭 SSL/TLS 连接：不加密连接
数据文件	启用 SSL/TLS 连接后，需要导入数据文件，即用户域服务器的数字证书。该数据文件需维护域服务器的管理员提供。
同步时间间隔（小时）	配置系统同步域的时间间隔，只能配置为自然数。

步骤3. 单击“**保存**”，配置集成 LDAP 用户完毕。

11.4.2 添加 LDAP 用户

您可以对 LDAP 用户进行新增、修改、删除等操作。

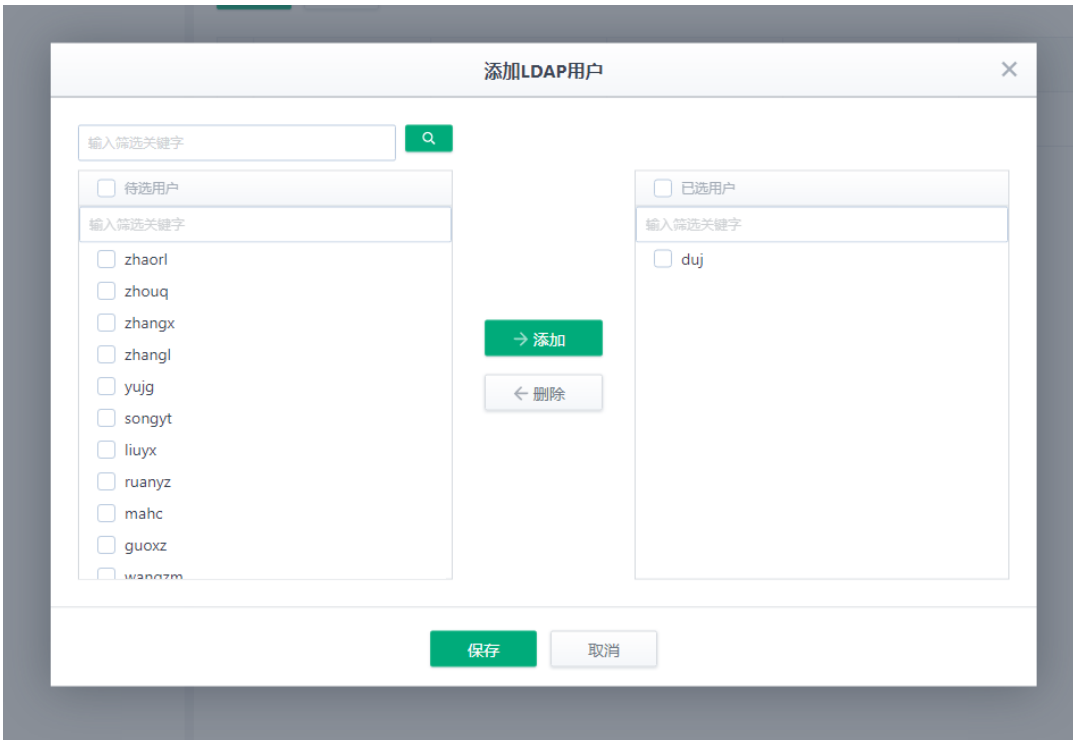
背景信息

- 只有安全审计员角色的用户可以执行新增、修改、删除的操作。
- 系统管理员角色的用户仅可执行查看、查询的操作。

操作步骤

步骤1. 选择菜单“**用户权限** > **LDAP 用户**”，LAS 系统进入“**LDAP 用户管理**”界面。

步骤2. 单击“**新建**”，弹出添加 LDAP 用户界面。



步骤3. 在“**待选用户**”中选择待添加的 LDAP 用户，支持选中多条同时导入。

步骤4. 单击“**添加**”，导入域用户，该用户在列表中显示，并提示编辑“**角色**”和“**组织机构**”。

步骤5. 单击“**编辑**”，弹出用户信息编辑页面。

参数名称	参数说明
组织机构	选择用户所属的组织机构。
角色	设置添加用户的角色，勾选表示为用户配置该角色，可以为用户配置多个角色。用户对菜单项的权限为所有角色权限的合集。
数据角色	设置添加用户的数据角色，勾选表示为用户配置该数据角色，可以为用户配置多个数据角色。数据角色决定用户可看到的数据。
双因子认证	打开此开关后，登录 LAS 系统时，该用户需要输入邮箱发送的验证码，输入正确的验证码后，该用户方可成功登录。 **前提条件：** • *您已经配置 SMTP，具体请参见**错误!未找到引用源。错误!未找到引用源。**，方可接收邮箱发送的消息。* • *导入的 LDAP 用户中包含了其邮箱信息。*
是否对加密数据可见	打开此开关后，该用户在“**大数据中心**”的“**智能分析 > 日志查询**”和“**安全事件**”的关联事件中无法查看到已加密的数据。

步骤6.　单击“**保存**”，完成 LDAP 用户的新增。

11.4.3 LDAP 用户登录方式

如 LDAP 用户是“xxx”，企业域为“yyy”，那么该 LDAP 用户有两种登录方式：使用用户名“xxx@yyy.com”或者“yyy\xxx”，密码为 LDAP 服务器管理员提供。

11.4.4 维护 LDAP 用户

操作	说明
修改	您可以通过单击 LDAP 用户列表操作列的  ，可修改用户信息。
删除	• 您可以通过单击 LDAP 用户列表操作列的  ，删除该用户。 • 当 LDAP 用户列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入“**登录名称**”，如“**admin**”，并按回车键，查询出登录名中含有 admin 关键字的用户，以列表方式展示。
锁定/解锁	使用 admin 用户单击被锁定用户列表操作栏的  ，对该用户进行解锁/锁定。 用户被锁定后不允许登录系统，如果需要登录系统，需要手动解锁用户。
同步用户	• 同步时间 有用户登录系统时，或者根据集成 LDAP 用户配置页面配置的同步时间，同步一次 LDAP 用户信息。 • 同步内容 不存在的用户从 LDAP 用户列表清除，存在的 LDAP 用户，同步真实名称、电子邮件、手机号信息。

12. 基础配置

12.1 网络配置

网络配置包括网卡配置、静态路由和 DNS 配置。

本节介绍网络工具箱的功能

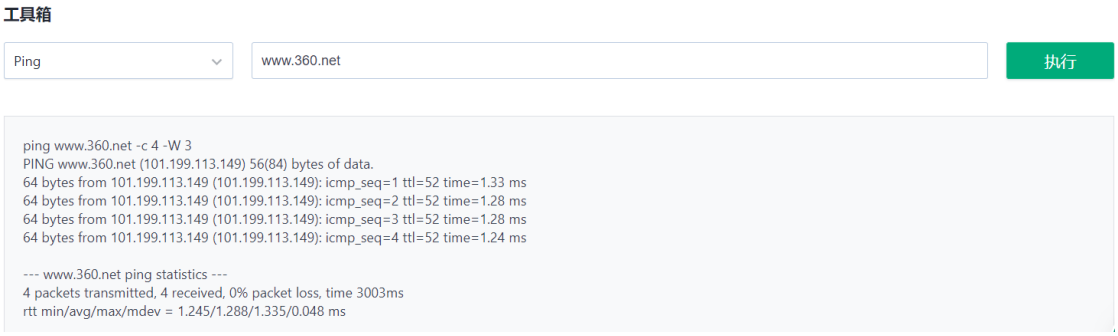
操作步骤

步骤1. 在导航栏单击，选择“**基础配置** > **网络配置**”，LAS 系统进入“**网络配置**”页面。页面下方是工具箱部分：

配置默认路由时，不要选择网卡，若选择网卡会导致下一跳地址设置为 0.0.0.0，如

图

步骤2. 工具箱中提供了 Ping/Tcpdump/Netstat 和 Telnet 四个命令工具，管理员选择相应的命令，填入参数后点击执行，下方会返回相应的命令结果。管理员根据结果，可以了解 LAS 系统设备的网络状况。



12.2 通知管理

在报告任务、系统监控等配置中可以添加邮件/短信类的通知对象，系统根据配置的通知对象发送消息给责任人。

12.2.1 SMTP 配置与阿里云短信

通知对象的方式包括邮件、短信方式。当选择发送邮件通知时，需要配置 SMTP 服务器参数。

操作步骤

步骤1. 在导航栏单击，选择“**基础配置 > 通知管理**”，LAS 系统进入“**通知管理**”页面。根据下图配置 **SMTP 配置**，单击保存完成配置。

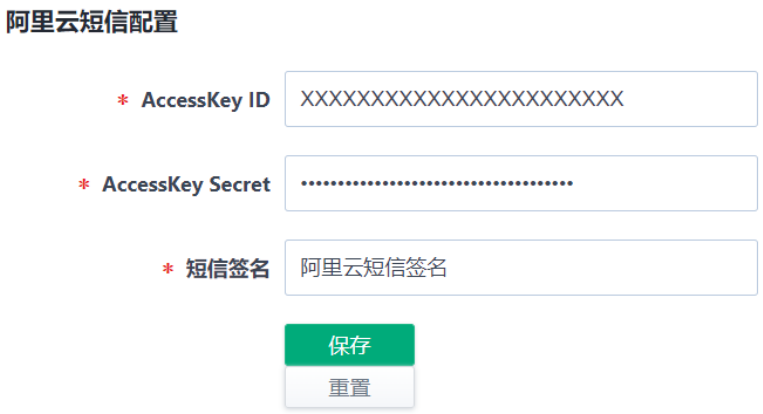
配置 SMTP 参数说明如下。

参数名称	参数说明
SMTP 服务器地址	发件人服务器的 SMTP 的服务器地址。 如：smtp.163.com、smtp.126.com 等
SMTP 服务器端口	默认值是 25。
SMTP 用户名	发件人的邮箱用户名，需要与 SMTP 服务器地址类型保持一致，即选择邮箱的类型。
密码	发件人邮箱对应的**密码或授权码（根据服务商设置）**。
是否启用 SMTP 服务	通过开关设置是否启用 SMTP 服务。

步骤2. 如需启用短信通知，用户需首先开通阿里云短信服务，申请获取相应的短信签名和模板（阿里云短信服务网址：https://dysmsnext.console.aliyun.com/quickstart）。申请短信模板时请参考下图配置模板内容：

参数名称	参数说明
host_ip	告警主机
moduleName	告警模块的名称
alert	告警内容

步骤3. 阿里云短信服务已经开通后，请参考下图完成阿里云短信配置：



参数名称	参数说明
AccessKey ID	阿里云账号的 AccessKey ID，与 Secret 一起用于通过认证后访问阿里云服务
AccessKey Secret	阿里云账号的 AccessKey Secret
短信签名	发件人的邮箱用户名，

12.2.2 新增通知对象

您可以配置通知对象，及其获取通知的方式。

操作步骤

步骤1. 在导航栏单击，选择“**基础配置** > **通知管理**”，LAS 系统进入“**通知管理**”页面。

步骤2. 在通知对象列表展示界面，单击“**新建**”，显示通知对象新增界面。新增邮件和短信对象的界面分别如下。

步骤3. 配置通知相关参数。

参数名称	参数解释
名称	通知对象的名称，该名称为用户的唯一标识，不同通知对象的名称不可相同。

参数名称	参数解释	
通知方式	邮件	勾选邮件通知方式，输入收件人和抄送人的邮箱地址，支持一个或多个邮箱。发件人邮箱在 SMTP 中配置，具体请参见 **SMTP 配置与阿里云短信**章节。
	短信	勾选短信通知方式，输入手机号，支持一个或多个手机号。通知对象的短信依赖于阿里云短信服务。 模板 ID 为阿里云短信服务中申请的短信模板 ID，请参见 **SMTP 配置与阿里云短信**章节。

步骤4. 单击“**确认**”，完成用户的新增。

12.2.3 维护通知对象

操作	说明
修改	您可以通过单击通知对象列表操作列的**编辑**，可修改通知对象的“**名称**”和“**通知方式**”。
删除	您可以通过单击通知对象列表操作列的**删除**，删除该条通知对象。当通知对象列表中有多条数据需要删除，可通过勾选需删除的数据，并单击“**删除**”，可一次性删除多条数据。
查询	您可以通过界面右上角搜索框内输入“**通知名称**”，并按回车键，查询出通知名称中包含关键字的通知对象，以列表方式展示。

12.3 存储配置

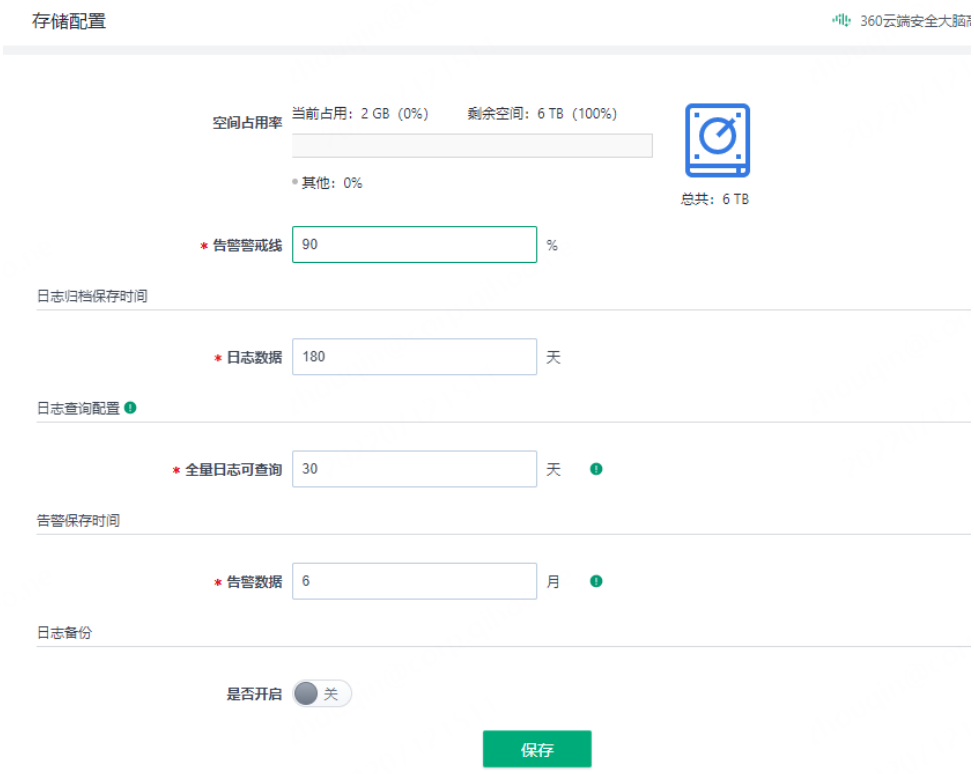
请根据实际需求配置以下环境参数，以满足日常系统管理运维的需要及确保 LAS 系统的正常运行。

12.3.1 配置日志存储

当需要修改日志存储策略时，可在系统配置中修改相关参数。

操作步骤

步骤1. 在导航栏单击，选择“**基础配置** > **存储配置**”页面，打开“**存储配置**”页面。



参数名称	参数说明
告警警戒线（%）	当磁盘存储空间超过了该设置值，系统就会提示用户注意磁盘空间大小，默认值为“90”。
日志归档保存时间	日志文件在磁盘中最长的保留天数，默认值为“180”。
全量日志可查询	可配置全量日志可查询的天数，默认值为“30”天。
告警保存时间	告警数据保留的月数，默认值为“6”个月
日志备份	可以选择本地备份、FTP 备份和 SFTP 备份。如果开启，每日凌晨 1 点会自动备份前一天的 event 日志到客户设置的服务器路径，本地备份的路径是：/archive 目录。客户需配置正确的 ftp 或者 sftp 的**存放路径、账号和密码。**

步骤2.　单击“**保存**”，刷新日志存储的策略。

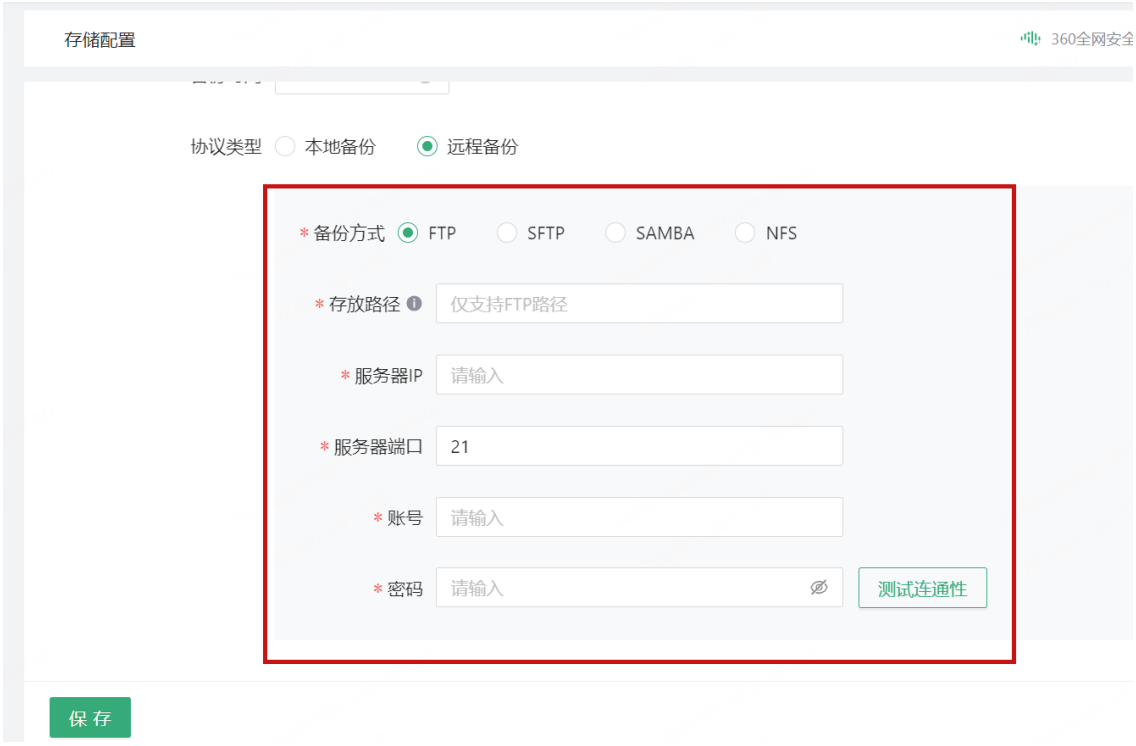
12.4 数据备份

新增数据备份，数据恢复操作，自定义备份时间

12.4.1 自定义备份时间

高级设置->基础配置->存储配置，日志备份，可设置是否备份、备份时间和本地备份或远程备份。

远程备份支持 ftp、sftp、samba 和 nfs



12.4.2 数据备份查询

日志备份开启后，到设置时间后自动备份，在数据备份页面可查看空间占用及备份记录

备份数据状态包含在线、归档和离线，离线状态数据可进行恢复操作，勾选备份数据可进行导出或删除操作。

12.5 环境信息

请根据实际需求配置以下环境参数，以满足日常系统管理运维的需要及确保 LAS 系统的正常运行。

12.5.1 代理配置

若已成功安装代理服务器，请根据实际情况配置代理。

操作步骤

步骤1. 在“**环境信息**”页面，配置“**代理地址**”和“**代理端口**”。

步骤2. 单击“**保存**”，完成代理服务器的配置。

步骤3. （可选）若不需要配置代理，可单击“**重置**”。

12.5.2 设定服务器时间

“**环境信息**”页面下，在“**服务器时间（NTP）设定**”区域，可以设置系统时间，或者通过启用 NTP 服务，并设置 NTP 服务的地址。

12.5.3 赋能天数显示开关

“**环境信息**”页面下，在“**赋能天数设置**”区域，可以通过打开/关闭“**是否显示赋能天数**”，并单击“**保存**”，切换是否在系统的右上角显示 360 云端安全大脑高效赋能的天数。

12.6 安全策略

您可以根据实际情况灵活设置该账号的安全策略。

操作步骤

步骤1. 在导航栏单击，选择“**基础配置** > **安全策略**”，LAS 系统进入“**安全策略**”页面。

步骤2. 配置相关参数。

参数名称	参数说明
密码最小长度	账号密码的最小长度，该值不得小于 8。 以下四个选项至少选择三项： • 密码口令包含大写英文字母 • 密码口令包含小写英文字母 • 密码口令包含数字 • 密码口令包含特殊字符
尝试登录失败后锁定时间配置	选择是否打开登录失败后锁定账号的开关。
尝试登录次数	打开登录失败后锁定开关后，需配置允许登录失败的次数，该值不得小于 1，默认值为“5”。
自动解锁时间（分钟）	打开登录失败后锁定开关后，需配置用户被锁定后的自动解锁时间，该值不得小于 1，默认值为“15”。
超时认证配置	选择是否打开用户超时认证的开关。
TOKEN 失效时间（分钟）	打开用户超时认证开关后，需要配置超时时间，该值不得小于 1，默认值为“30”。
管理员口令更换周期限制	选择是否打开管理员口令更换周期限制的开关。
更换周期（天）	打开管理员口令更换周期限制开关后，需要配置更换周期，该值不得小于 1，默认值为“90”。
用户登录源 IP 限制	选择是否打开用户登录源 IP 限制开关。
IP 白名单	打开开用户登陆源 IP 限制开关后，需要配置具体的 IP 白名单，每个 IP 之间以逗号分隔。

步骤3. 单击“**保存**”，账号安全策略配置完毕，并且配置立即生效。

其中，密码复杂度的相关配置，只针对新增用户和用户修改密码有效。

后续处理

单击“**更新**”，可更新“**最后刷新时间**”及“**系统监控**”的最新数据。

相关操作

当用户超过 90 天未修改密码，当再次登录 LAS 系统，会提示修改密码，修改密码后方可登录 LAS 系统。

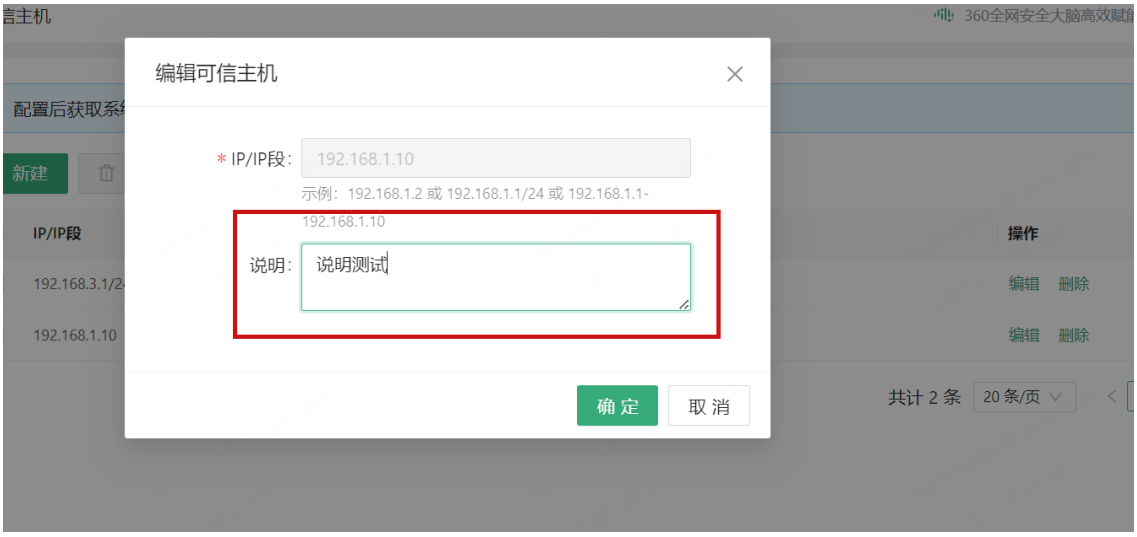
12.7 可信主机

支持界面配置系统后台的主机 SSH 访问限制策略，提升设备部署安全性，未添加可信主机不能通过 ssh 方式连接服务器。

1、新增可信主机

支持 IP 或 IP 段配置，如图

2、编辑主机，编辑只可更改说明，无法修改主机 IP



3、删除可信主机，支持单条删除和批量删除

12.8 上报配置

态势感知可以上报 snmp 和 syslog 用于监控和数据转发

操作步骤

步骤1. 在导航栏单击，选择“**基础配置** > **上报配置**”，LAS 系统进入“上报配置”页面。

步骤2. 配置 SNMP 相关参数。

参数名称	参数说明
启/停	选择是否开启 SNMP。
端口	用于给监控设备使用的 SNMP 端口。
版本	用于 SNMP 的版本，有 v1 和 v2c 可以选择。
团体名	SNMP 的弱密码。
保存	保存 SNMP 的配置。
重置	清空 SNMP 配置。

参数名称	参数说明
帮助	可以查看 SNMP 监控可用 OID 的用法

步骤3. 单击“**保存**”，SNMP 上报配置完毕，并且配置立即生效。

步骤4. 配置 syslog 相关参数。

参数名称	参数说明
状态	选择是否开启 Syslog。
协议	选择使用 tcp/udp 协议发送 syslog。
服务器	配置接收 syslog 的服务器的 ip 和 port。
数据源	可以选择通过 syslog 转发态势感知系统接收到的日志或者产生的告警。
排除字段	排除字段用于发送 Syslog 时排除不需要的字段，可以不填、可以单个、也可以多个。
保存	保存 Syslog 的配置。
重置	清空 Syslog 的配置

步骤5. 单击“**保存**”，Syslog 上报配置完毕，并且配置立即生效。

12.9 通知中心

对于 LAS 系统用户来说，一旦有系统消息通知、预警通知或是被分配的待处置任务，包括安全事件、预案动作、HW 任务，通知中心会及时通知相关用户关注和处置，更加方便及时。

12.9.1 通知中心预览

在使用通知中心之前，您可以先了解通知中心的窗格、配置和消息列表页面。

通知窗格

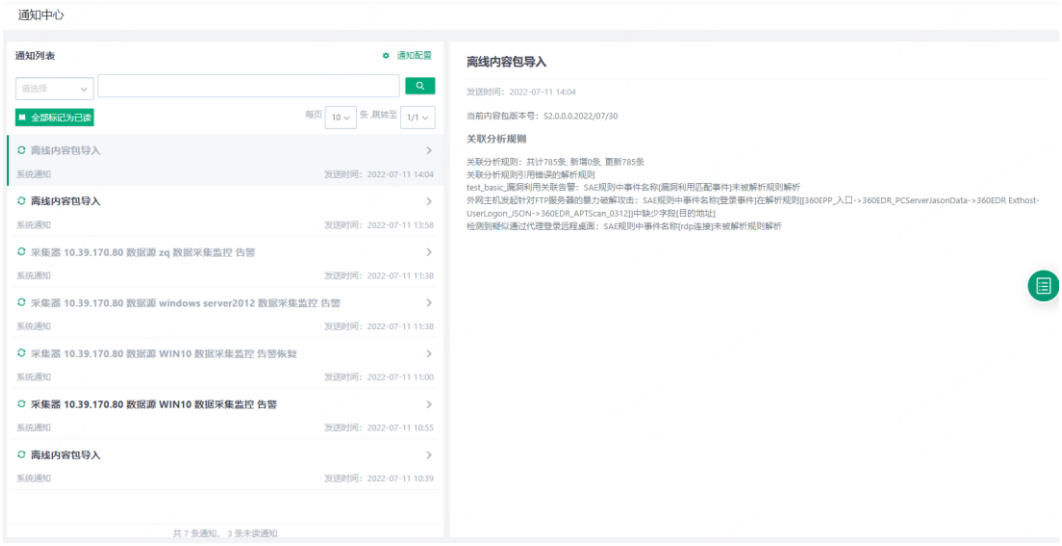
当接收到推送的系统消息、待处置的任务时，通知图标会显示汇聚的未读消息总数。单击之，会展开“**通知**”窗格。如下图所示。

通知窗格中展示的消息类型

- 按时间倒序显示通知消息
- 通过×号可以关闭指定的未读消息。
- 单击具体的消息可以查看消息的详情。
- 超过 10 条消息时，在窗格底部可单击“**更多**”展开查看。

通知中心列表

单击窗格右上角列表按钮，可以展开“**通知中心**”页面，如下图所示。



区域	说明
通知列表	通知列表页包含了一些基础功能，包括： • 列表中展示所有推送过的消息。置灰则说明已读。 • 提供搜索功能：根据推送的消息类型，支持通知消息标题的模糊搜索。 • 通过一键“**全部标记为已读**”，快速标记消息。 • 单击“**通知配置**”，可打开“**配置通知**”的提示框。 • 单击待处置任务，可查看消息详情。
右侧信息框	默认展示当前页第一条有详情的系统通知详情，如“**离线内容包导入**”的详细信息。

通知配置

LAS 系统提供两个入口打开“通知配置”提示框。

4. 在“**通知窗格**”右侧单击⚙。
5. 在“**通知中心**”的“**通知列表**”区域，单击“**通知配置**”。

如下图所示。在“**通知配置**”页面，您可以选择通知消息类型，是否提示音播放及提示音的类型。

12.9.2 配置通知

用户可以通过配置，选择接收推送的通知消息类型，是否提示音播放及提示音的类型。

操作步骤

步骤1. 在 LAS 系统页面上方导航栏右侧，单击，弹出“**通知**”窗格。

步骤2. 单击，打开“**通知配置**”信息框。

参数名称	参数说明
推送配置	推送配置的任务类型包括了： • 系统通知：离线内容包。
播放提示音	选择是否需要设置消息提示音。
提示音效	在下拉列表中选择提示音效。

步骤3. 单击“**保存**”，保存消息通知中心的设置。通知中心会按照您的选择推送消息，以及播放提示音。

12.9.3 查看推送消息详情

12.9.3.1系统通知

通知中心推送的系统通知，主要是“**离线内容包更新**”。离线内容包更新指的是从初始化页面导入。

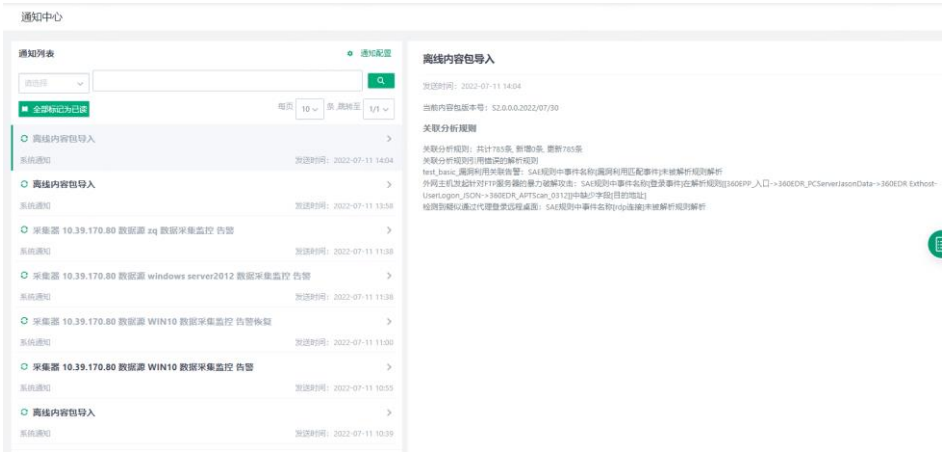
对于内容包中的模块，会触发通知的有：**解析规则**、**安全信息**、**系统属性**、**关联分析规则**、**基础事件**。

操作步骤

步骤1. 通知图标显示有新消息，单击之，弹出“**通知**”窗格，提示“**系统通知：离线内容包导入**”。

步骤2. 单击窗格右上角，展开“**通知中心**”页面。

通知列表中展示系统通知的信息和其他未读的待处置任务，右侧信息框区域则展示该条“**离线内容包导入**”的详细信息。

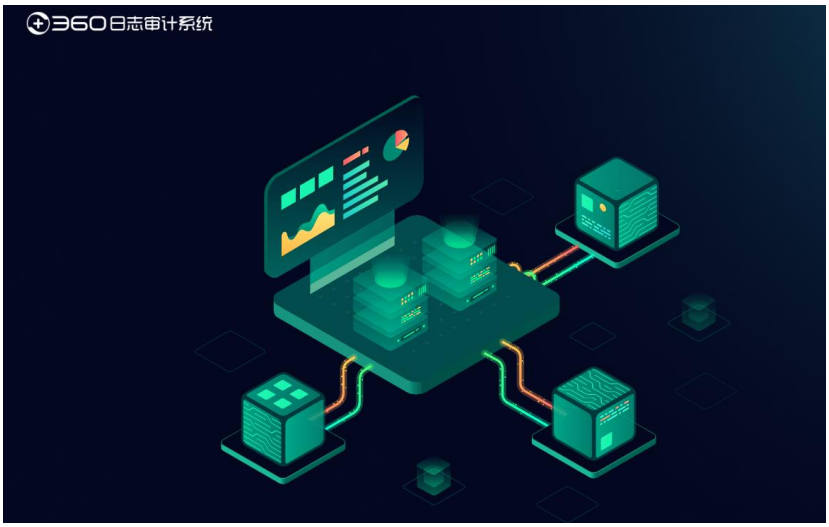
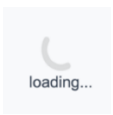


12.10 自定义页面元素

出于方便项目定制，实施运维工程师可通过在 LAS 系统系统管理中替换页面中的 logo 元素和文字。

背景信息

您可以修改的页面元素一一对应关系如下。

界面参数	替换位置
登录页面配置	即登录页面的底图。 
大屏页面配置	
顶部栏配置	
浏览器标签配置	
loading 配置	

界面参数	替换位置
通知报告配置	该图是通过邮件发送报告的信息。 

注意事项

- 务必上传符合界面要求大小、格式的图片。
- 一般场景下以上元素均会全量修改，因此只有全量上传后方可保存成功。
- 单击右上角“**恢复至默认设置**”，则会全量恢复为具备 360 元素的 logo 和文字。

操作步骤

步骤1. 在导航栏单击，选择“**基础配置 > 自定义元素**”，LAS 系统进入“**自定义元素**”页面。

步骤2. 选择“**页面元素配置**”，显示页面元素配置页面。

步骤3. 修改“**登录页面配置**”。

1. 单击“**上传文件**”，打开本地文件选择器。

选择符合尺寸、文件名的图片，并单击“**确定**”。

单击“**预览**”，可查看上传的图片。

步骤4. 依次修改以下元素。

步骤5. 单击“**保存**”，并刷新浏览器，即可完成修改。

13. 版本管理

13.1 License 管理

在版本管理中可查看使用的 LAS 系统的版本号、build 号、序列号、机器码、授权点数等一系列信息。并可按需更新 license 文件。

操作步骤

步骤1. 在导航栏单击，选择“**版本信息 > License 管理**”，LAS 系统进入“**License 管理**”页面。

可查看 LAS 系统的版本号、build 号、授权点数，License 的状态、类型、失效时间等信息。使用手机扫描二维码也获取产品特征码。

步骤2. 单击“**序列号**”后的，序列号呈可见模式。

步骤3. （按需执行）若要更新 license 文件，可单击“**上传文件**”，上传新的 license 文件即可更新。

版本号规范说明：

例如：V2.0D6R22M00P000B18424

参数名称	参数说明
V2.0	代表系统的大版本号，也就是软著中的版本。
D6	代表日审编号。
R22	代表主线版本号。
M00	M00 为空，则代表是标准版本，没有定制。
P0000	P000 为空，则代表是标准版本首次发布。
B18424	Build 版本号，系统打包自动生成

13.2 升级管理

操作步骤

步骤1. 在导航栏单击，选择“**版本信息** > **“升级管理”**，LAS 系统进入“**升级管理**”页面。

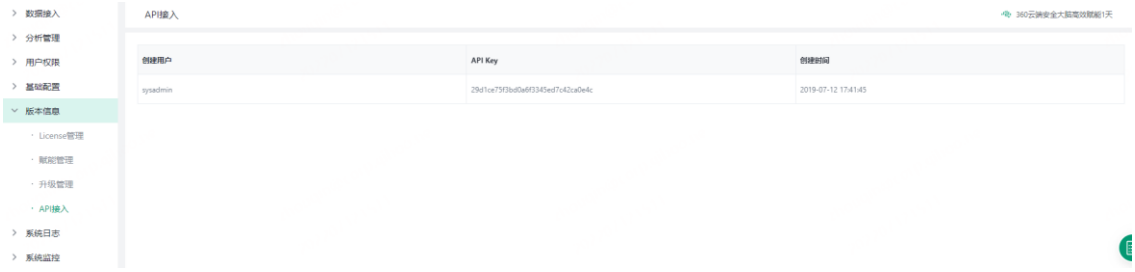
步骤2. 单击“导入升级包”，选择上传文件上传，即可完成一键升级。

13.3 查看 API key

您可以在前端页面查看 API key，提供给第三方，向 LAS 系统注册。

操作步骤

步骤1. 在导航栏单击，选择“**版本信息** > **API 管理**”，LAS 系统进入“**API 管理**”页面。即可获取 APIKey 值。



14. 监控系统日志

系统日志包括审计日志和更新日志。您可以通过 LAS 系统查看各日志的详细信息。

14.1 查看审计日志

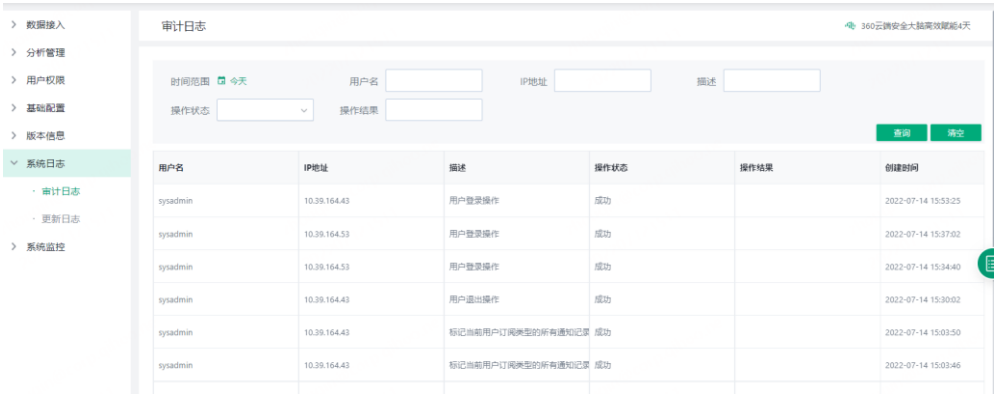
审计日志是用来记录用户所有的系统操作信息和状态，具体展示内容包括：用户名、IP 地址、描述、操作状态、操作结果、创建时间。

审计日志不支持删除。

操作步骤

步骤1. 在导航栏单击，选择“**系统日志 > 审计日志**”，LAS 系统进入“**审计日志**”页面。

步骤2. 默认查看当天 24 小时内的审计日志。



步骤3. （可选）设置查询时间，可查询指定时间内的审计日志。

步骤4. 设置用户名、IP 地址、描述、操作状态、操作结果，可以查询符合条件的审计日志。

14.2 查看更新日志

更新日志是用来记录 LAS 系统资源更新的信息，具体展示内容包括：集成的资源类名、具体描述、操作状态和创建时间。

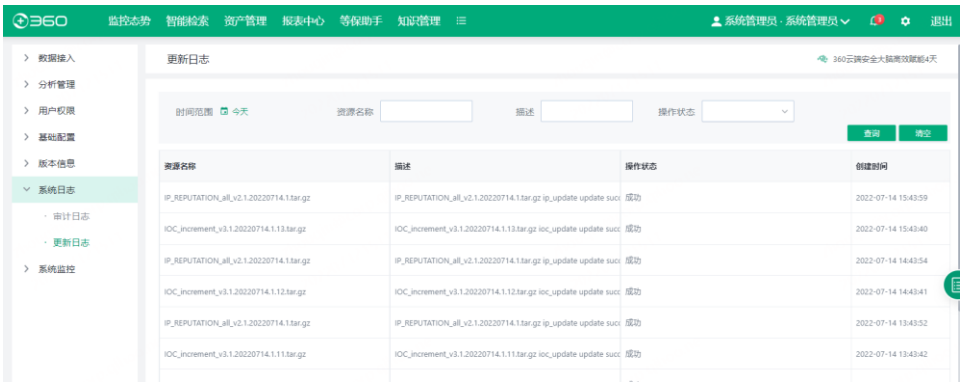
操作步骤

步骤1. 在“**系统日志**”菜单下切换“**更新日志**”，LAS 系统显示“**更新日志**”的页面。

步骤2. 选择“**更新日志**”的页签，LAS 系统进入“**更新日志**”界面。

步骤3. 查看系统的更新日志信息。

步骤4. （可选）设置查询时间，可查询指定时间内的更新日志，包括资源类名、描述、操作状态和创建时间。



步骤5. 设置用户名、IP 地址、描述、操作状态、操作结果，可以查询符合条件的审计日志。

15. 系统监控

LAS 系统提供系统监控入口，可监控当前搜索分析功能、各节点功能及数据总线的状态是否正常。同时，提供监控告警开关，通过添加通知对象；当有状态异常时，则发送告警通知至通知对象。

15.1 SNMP 监控

态势感知可以通过添加 SNMP 监控，来监控其它适配的资源使用情况。

操作步骤

步骤1. 在导航栏单击，选择“**系统监控 > SNMP 监控**”，态势感知进入“SNMP 监控”页面。

步骤2. 新增 SNMP 监控。

新增 SNMP 监控相关配置：

查看内容	内容说明
监控名称	用于区别被监控设备的名称
设备 IP	配置设备的 IP 和 PORT
采集帧	选择采集 SNMP 信息的频率： • 60s（默认） • 300s • 30s • 10s
状态	是否开启监控。
版本	被监控设备的 SNMP 版本： • v1 • v2c • v3
团体名	SNMP 的弱密码 注：版本 v1、v2c 必填，v3 非必填
用户名	用于 SNMP v3 版本的认证鉴权。
鉴权方式	用户 SNMP v3 版本的鉴权方式 • 认证 认证方式：MD5、SHA1 认证密码 • 加密 加密方式：DES、AES128、AES192、AES256 认证密码
OID 配置	用于监控的项目： 设备名称 OID CPU 使用率 OID 内存使用率 OID 网络上行流量 OID 网络下行流量 OID
保存/取消	保存 SNMP 监控配置 取消 SNMP 监控配置

步骤3. 单击“**保存**”，SNMP 上报配置完毕，并且配置立即生效。

步骤4. 查看 SNMP 监控列表

15.2 查看系统状态

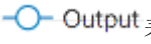
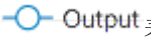
通过系统监控，您可以了解到当前搜索分析功能、各节点功能及数据总线的状态是否正常。

操作步骤

步骤1. 在导航栏单击，选择“**系统监控** > **服务监控**”，LAS 系统进入“**服务监控**”页面。

您可以查看以下内容：

查看内容	内容说明
总体状态	• 主机运行的总体状态是否正常。 • 系统已运行的时长。
CPU 使用率	您可以查看最近 5 分钟，CPU 的使用率。 以时间为横坐标、CPU 使用率值为列坐标展示。 您可以通过将鼠标悬浮在曲线上查看某一时间点 CPU 的使用率。
内存使用率	您可以查看最近 5 分钟，内存的使用率。 以时间为横坐标、内存使用率值为列坐标展示。 您可以通过将鼠标悬浮在曲线上查看某一时间点内存的使用率。

查看内容	内容说明
网络 I/O	您可以查看最近 5 分钟，网络 Input 和 Output 的数据传输率。 以时间为横坐标、数据传输率为列坐标展示。 其中， •  表示 Input 的曲线 •  表示 Output 的曲线 您可以通过将鼠标悬浮在曲线上查看某一时间点网络 Input 和 Output 的数据传输率。
磁盘 I/O	您可以查看最近 5 分钟，磁盘 Input 和 Output 的数据传输率。 以时间为横坐标、数据传输率为列坐标展示。 其中， •  表示 Input 的曲线 •  表示 Output 的曲线 您可以通过将鼠标悬浮在曲线上查看某一时间点磁盘 Input 和 Output 的数据传输率。
各模块状态	您可以通过此列表查看 LAS 系统各模块是否运行正常:

更多操作

操作	说明
重启	您可以通过单击“ ”，重启指定模块。
全部重启	您可以通过单击“ ”，重启全部模块。
下载日志信息	您可以通过单击 “ ”，可以下载各模块的后台运行日志。

15.3 监控告警说明

监控告警规则

目前监控告警规则均是内置的。

告警通知

发送告警通知的时间周期：

针对每个告警规则，从第一次监测到异常，直到系统恢复正常期间，只会发送一次告警通知；如果正常运行一段时间后，再次被监测到异常，又会重新发送告警通知。

15.4 设置监控告警

您可以通过打开监控告警开关，并添加通知对象。当有状态异常时，则发送告警通知至通知对象。

操作步骤

步骤1. 单击“**系统监控** > **服务监控**”页面右上方的“**通知配置**”，弹出“**告警通知**”对话框。

步骤2. 设置“**通知**”开关。

- 当设置状态为“**开**”，则打开告警通知的功能，并执行步骤 3，配置通知对象。
- 当设置状态为“**关**”，则关闭告警通知的功能。

步骤3. 在下拉列表中勾选已创建的“**通知对象**”。

步骤4. （可选）单击“**添加新对象**”，则跳转至“**基础配置** > **通知对象**”页面。

步骤5. 单击“**确定**”，可保存设置。

15.5 设备管理

操作步骤

步骤1. 在导航栏单击，选择“**系统监控** > **设备管理**”，LAS 系统进入“**设备管理**”页面。点击相应的按钮，可以执行**系统重启、设备关机和恢复出厂设置**等设备管理操作。

16. 分布式管理

支持硬件级别的分布式部署方式，一级节点支持二级节点采集配置下发和状态管理

16.1 默认模式

默认模式是设备作为单机运行，系统安装后默认单机运行。

操作步骤

步骤1. 在导航栏单击，选择“**分布式管理**”，LAS 系统进入“**分布式管理**”页面。

步骤2. 系统默认单机模式。

16.2 管理节点模式

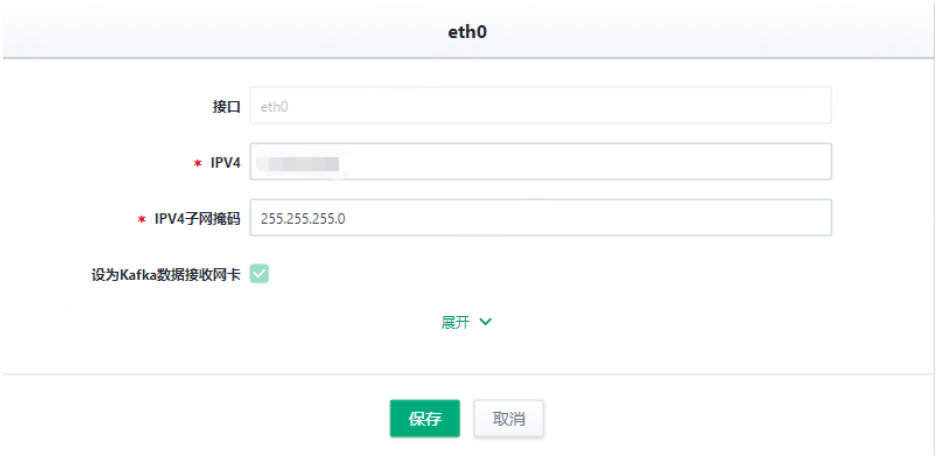
管理节点可以维护子节点信息，包括：IP 地址、外部页面访问 IP、责任人及责任人电话。管理节点可以采集和存储子节点的日志，展示子节点的状态，CPU，内存，磁盘数据，日志数据及数据源接入情况。

操作步骤

步骤1. 首先设置网卡为 kafka 数据接收网卡。

1、 在“**基础设置**”菜单下切换“**网络设置**”，选择设备的网口，单击“**编辑**”。

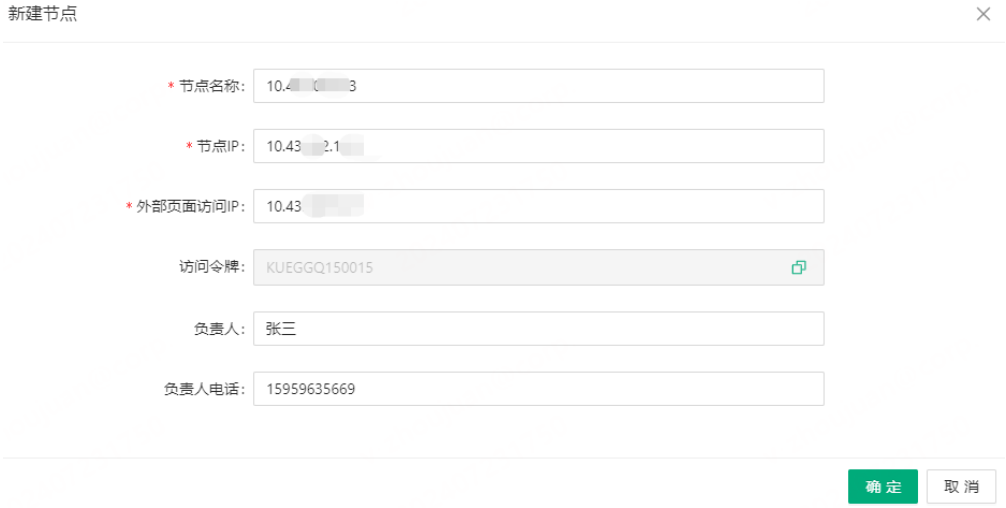
2、 勾选“**设为 kafka 数据接收网卡**”，单击“**保存**”。



步骤2. 选择“**分布式管理**”，进入“**分布式管理**”页面。

步骤3. 切换管理节点模式，单击管理节点“**切换**”按钮，进入“**分布式管理模式-管理节点**”页面。

步骤4. 创建子节点，单击“**新建**”，系统显示“**新建节点**”编辑页面。系统自动生成子节点的访问令牌，输入子节点名称，IP、外部页面访问 IP、负责人信息。



步骤5. 单击“**确定**”，系统新增子节点记录。在子节点未接入到管理节点前，子节点是离线状态，且设备状态展示异常。

16.3 子节点模式

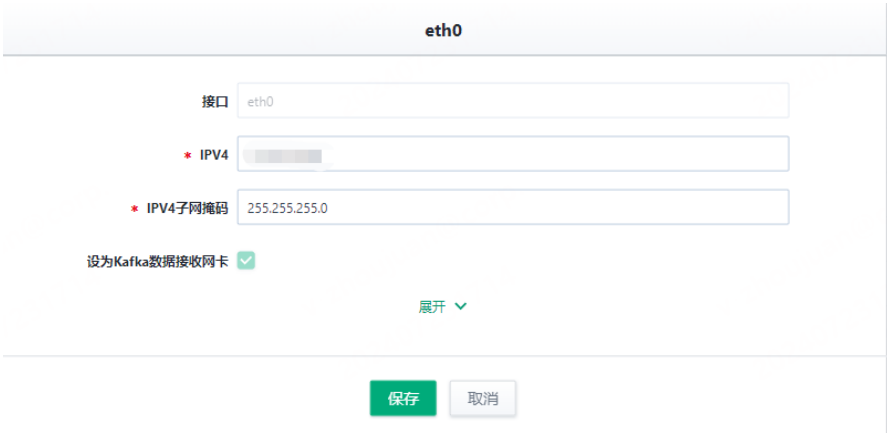
子节点可以将原始日志数量和详情数据、资产数量、告警数量上报到管理节点。管理节点页面可以查看子节点上报的数据及数据源接入情况。

操作步骤

步骤1. 首先设置网卡为 kafka 数据接收网卡。

1、 在“**基础设置**”菜单下切换“**网络设置**”，选择设备的网口，单击“**编辑**”。

2、 勾选“**设为 kafka 数据接收网卡**”，单击“**保存**”。



步骤2. 选择“**分布式管理**”，进入“**分布式管理**”页面。切换子节点模式，单击子节点下的“**切换**”按钮，进入“**分布式管理模式-子节点** ”页面。

步骤3. 输入管理中心 IP（即管理节点）、令牌（即上文中自动生成的访问令牌），勾选要上报的数据，单击“**保存**”。

步骤4. 页面提示保存成功后，打开“**分布式管理/管理节点**”，子节点的在线状态更新为“**在线**”，设备状态更新为“**正常**”，同时显示子节点的 CPU 利用率、内存利用率。

参数名称	参数说明
在线状态	• 离线：子节点没有接入到管理节点。 • 在线：子节点接入到管理节点。
设备状态	• 异常：子节点服务模块运行异常。 • 正常：子节点服务模块运行正常。
CPU 使用率	设备状态正常时，显示子节点设备的 CPU 使用率。
内存使用率	设备状态正常时，显示子节点设备的内存利用率。
嵌入日志(EPS)	显示子节点设备日志接收的速率，每分钟更新。

更多操作

操作	说明
管理	您可以通过单击子节点操作列的“**管理**”，跳转到子节点的配置管理页面。
登录	您可以通过单击子节点操作列的的“**登录**”，跳转到子节点系统页面。
编辑	您可以通过单击子节点操作列的的“**编辑**”，支持修改子节点的参数。
删除	您可以通过单击子节点操作列的“**删除**”，删除该子节点。

16.4 配置管理

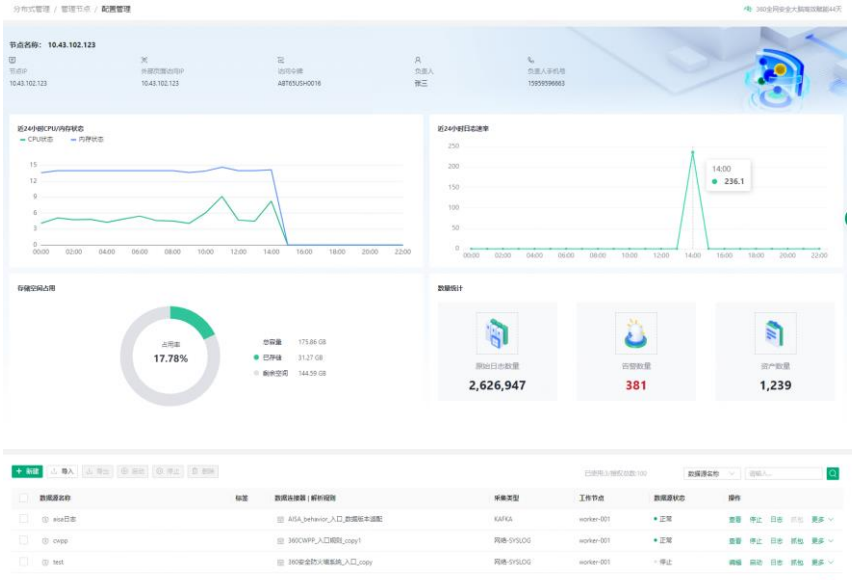
配置管理页展示节点的基本信息、近 24 小时 CPU/内存趋势图、近 24 小时日志速率、存储空间占用、原始日志数量，告警数量，资产数量。同时也展示子节点接入的数据源数据，并可以对数据源进行基本操作，如：新建、导入、导出、停止、启动、下载日志、抓包等操作。

操作步骤

步骤1. 选择“**分布式管理**”，进入“**分布式管理**”页面。单击管理节点“**已选择**”，进入“**分布式管理模式-管理节点**”页面。

步骤2. 选择接入的子节点，单击“**管理**”，进入“**配置管理**”页。

步骤3. 系统展示子节点基本信息及近 24 小时 CPU/内存、近 24 小时日志接收速率、存储空间占用、日志数量、告警数量、资产数量、子节点的数据源接入情况，并可以进行一些基本操作，具体操作参考：数据接入管理



附录

A.1 HQLite 语法

A.1.1 概述

功能描述

- 支持任意字段关键字自定义查询，支持关键字高亮、时间窗口自定义查询、过滤条件查询；
- 查询条件支持 and、or、not 等多重逻辑操作组合；
- 查询条件支持 **等于、不等于、大于、小于、存在、不存在、属于（内置安全信息）、网段包含、字符串匹配、正则表达式匹配**等多种操作符；
- 支持命令行交互检索查询（类 SQL 语言）方式对目标数据进行查询操作。

适用范围

- 搜索分析：日志查询、告警查询。
- SAE 关联分析规则中配置事件源时编辑过滤条件。
- 仪表盘

A.1.2 全文检索语句

对原始日志的过滤，支持全文检索，无需使用字段名、运算符。

全文检索语句的语法说明

全文检索语句包含以下两种语法：

- 整个语句是一个由引号包裹的完整且合法的字符串。
  - 正确示例：`"helloworld"`
  - 正确示例：`"访问用户北京"`
  - 错误示例：`"你好` -> 缺少后引号
  - 错误示例：`"你说你的"朋友"` -> 字符串内部引号需要使用转义符
  - 正确示例：`"你说你的\"朋友"`

- 整个语句只包含中文汉字、英文字母、数字。
  - 正确示例：访问端口 -> 等价于 "访问端口"
  - 正确示例：helloworld
  - 错误示例：www.360.cn -> 需要使用引号 "www.360.cn"

目前全文检索只对日志查询页面的原始日志字段生效，由于原始日志字段一般内容较多，为了查询的效率，我们对原始日志字段进行了分词处理，因此全文检索只能搜索分词之后的字符串。

举例：原始日志为 a=1,b=C:\Windows\system32\mmsys.cpl,c=www.360.cn

- 正确检索到该日志：a 1 Windows ystem3 "mmsys.cpl" "www.360.cn"
- 无法检索到该日志："a=1" "C:\\Windows" "Windows\\system32"

A.1.3 运算符的功能和使用

HQLite 是针对客户提供命令行式检索语言，包括支持以下操作符。

B 在搜索分析中的应用

以“**日志查询**”为例，介绍如何使用操作符的使用方法。

操作符“=”

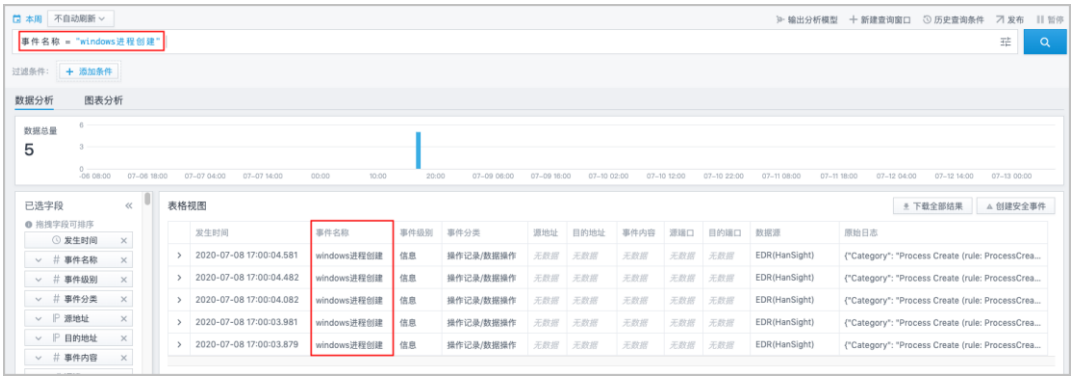
【描述】

运算符“=”用于筛选字段与查询条件相等的记录。

【示例】

在输入框中输入“**事件名称 =“windows 进程创建”**”，并单击  。

“**表格视图**”区域显示所有“**windows 进程创建**”的日志。



操作符“!=”

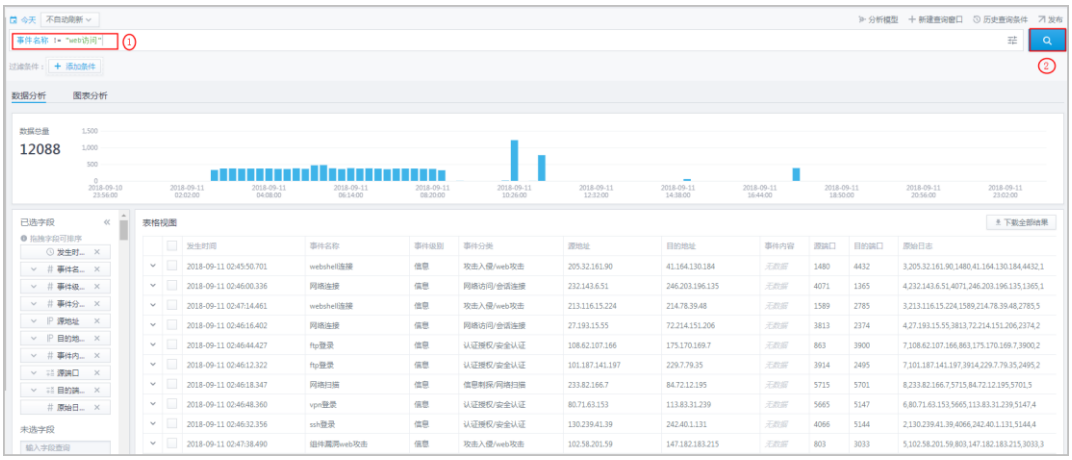
【描述】

运算符“!=”用于筛选字段与查询条件不相等的记录。

【示例】

在输入框中输入“**事件名称 != "web 访问"**”，并单击。

“**表格视图**”区域显示除“**web 访问**”的日志。



操作符“>”、“<”、“>=”和“<=”

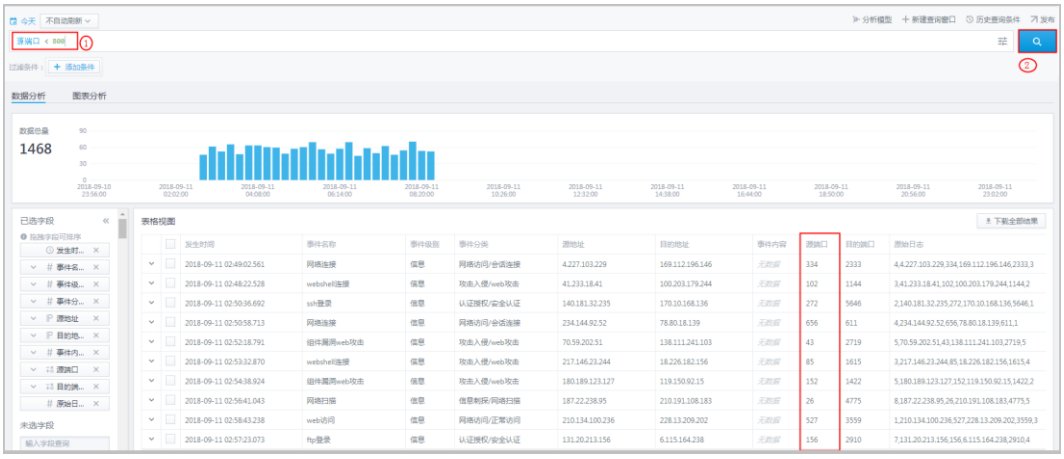
【描述】

操作符“>”、“<”、“>=”和“<=”，均用于数值大小的比较。

【示例】

以“<”为例，如在输入框中输入“**源端口 < 800**”，并单击。

“**表格视图**”区域显示源端口小于“800”的日志。



操作符“exist”

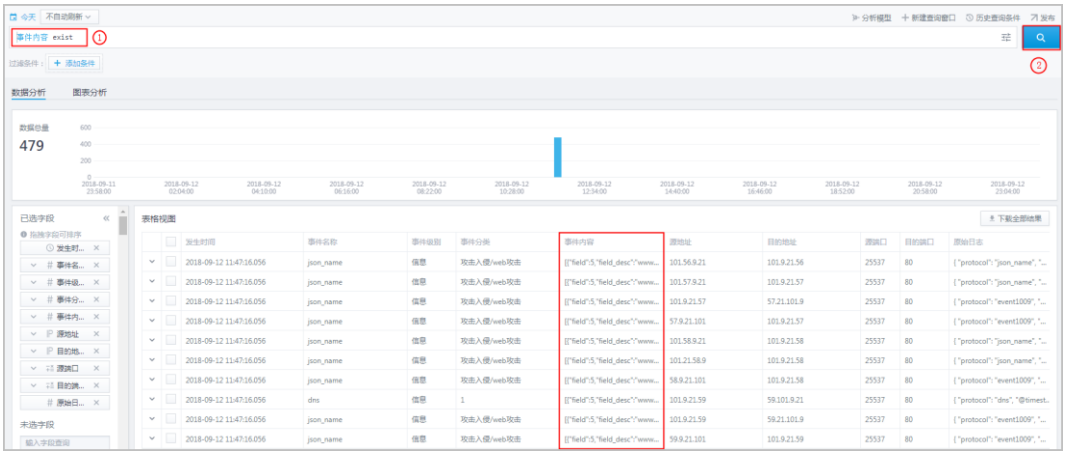
【描述】

操作符“**exist**”用于筛选字段“有内容”的日志。

【示例】

在输入框中输入“**事件内容 exist**”，并单击。

“**表格视图**”区域显示“**事件内容**”字段有内容的所有日志。



操作符“not_exist”

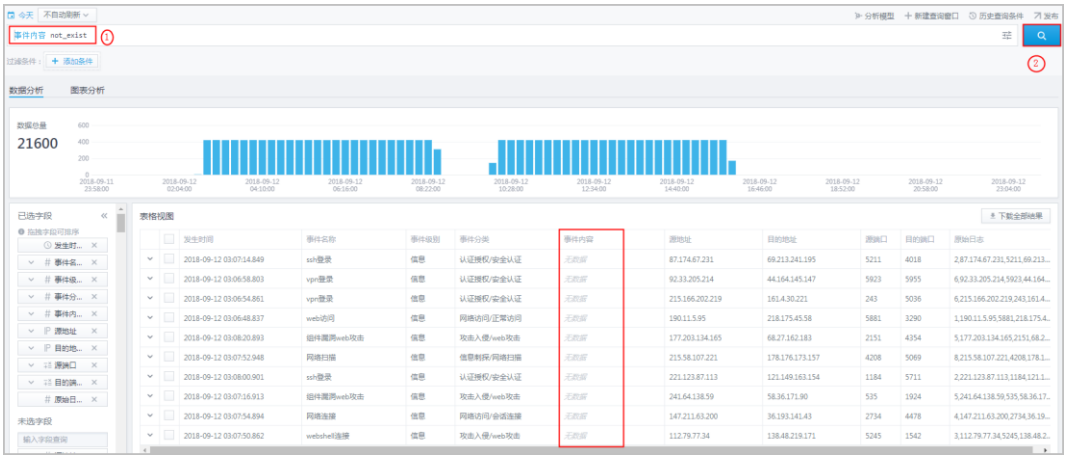
【描述】

操作符“not_exist”用于筛选字段“无内容”的日志。

【示例】

在输入框中输入“**事件内容 not_exist**”，并单击。

“**表格视图**”区域显示“**事件内容**”字段无内容的所有日志。



操作符“belong”

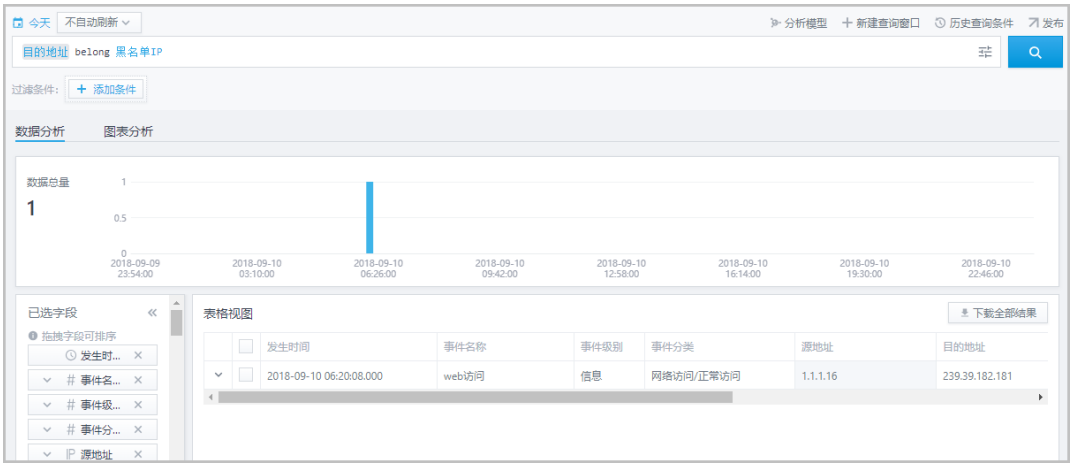
【描述】

操作符“belong”用于设置字段之间关联属于的关系。值（VALUE）只能使用安全信息的字段。

【示例】

如在输入框中输入“**目的地址 belong 黑名单 IP**”，并单击。

“**表格视图**”区域显示“**目的地址**”为“**黑名单 IP**”的所有日志。



操作符“like”

【描述】

操作符“**like**”为字符串匹配，大小写敏感。

【示例】

日志的字段为访问路径，值为 C:\Windows\system32\mmsys.cpl，以下输入都能匹配到该字段：

- 访问路径 like "C:\\Windows\\system32\\mmsys.cpl"
- 访问路径 like "Windows"
- 访问路径 like "dows\\syst"
- 访问路径 like "mmsys.cpl"

操作符“rlike”

【描述】

操作符“rlike”用于使用正则表达式匹配相关字段，大小写敏感。

【示例】

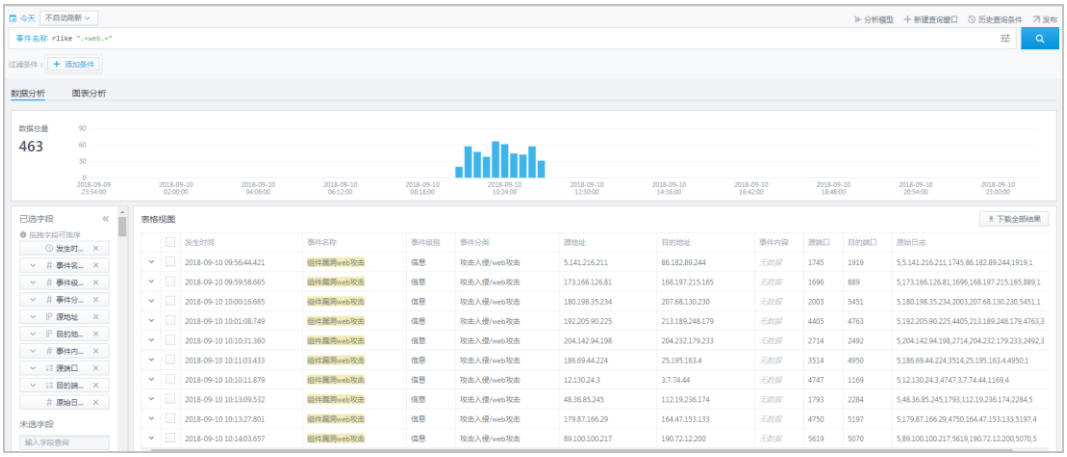
日志的字段为访问路径，值为 C:\Windows\system32\mmsys.cpl，以下输入都能匹配到该字段：

- 访问路径 rlike ".*C:\\Windows\\system32\\mmsys\.cpl.*"
- 访问路径 rlike ".*dows\\syst.*"
- 访问路径 rlike ".*mmsys\.cpl.*"
- 访问路径 rlike ".*Windows.*mmsys.*"
- 访问路径 rlike ".*Windows.*mmsys\.cpl.*"

【示例 2】

在输入框中输入“事件名称 rlike ".+web.+"”，并单击 。

“**表格视图**”区域显示“**事件名称**”字段中“**web**”前后均有内容的所有日志。



Like/rlike 注意事项

- 为了方便告警规则的配置，“**SAE 规则**”配置里的 **like** 或 **rlike** 操作符对所有字段都**不区分大小写**。
- 只有“**日志查询**”页面会有原始日志字段，其他搜索分析页面与 SAE 规则都没有原始日志字段。
- 由于“**原始日志**”字段一般内容较多，为了查询的效率，对“**原始日志**”字段进行了分词处理，分词器会根据中文字典、标点符号、空格等对字段进行分词并转换为小写，对“**原始日志**”字段使用 **like** 或 **rlike** 操作符进行匹配时，只能匹配分词之后的结果，并且不区分大小写。

【示例】

原始日志为 a=1,b=C:\Windows\system32\mmsys.cpl,c=Google Chrome,d=www.360.cn

- 以下语法可以搜索到该日志
  - 原始日志 like "windows"

  - 原始日志 like "Chrome"
  - 原始日志 like "www.360.cn"
  - 原始日志 like "mmsys.cpl"
  - 原始日志 rlike ".*mmsys\.cpl.*"
  - 原始日志 rlike ".*360.*"
- 以下语法无法搜索到该日志
  - 原始日志 like "a=1" -> =会被分词
  - 原始日志 like "Windows\\system32" -> \会被分词
  - 原始日志 rlike ".*Google Chrome.*" -> 空格会被分词

操作符“in”

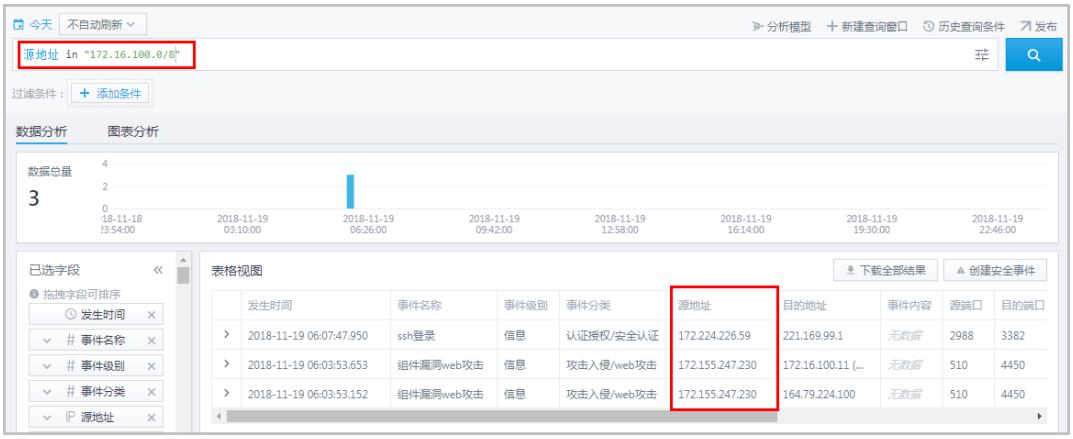
操作符“in”用于设置网段的包含。IP 类字段支持的格式：

- IP 字段 in “xxx-xxx”，如“源地址 in “1.1.1.1-200.1.1.1”” 。
- IP 字段 in “xxx,xxxx”，如“源地址 in “7.7.7.7,9.9.9.9,142.93.138.122,27.155.88.191”” 。
- IP 字段 in “xxx/xx”，如“源地址 in “142.1.1.1/8”” 。

【示例】

如在输入框中输入“**源地址 in 172.16.100.0/8**”，并单击 。

“**表格视图**”区域显示“**源地址**”属于网段“172.16.100.0/8”的所有日志。



操作符“contain”和“match”

操作符“contain”和“match”用于配置 SAE 规则，此处不适用，具体请参见 C 在 SAE 关联分析规则中的应用。

C 在 SAE 关联分析规则中的应用

配置流式关联分析规则时，会使用过滤条件，可以在对应过滤事件中提取出符合过滤条件的事件，以便设置触发告警的规则。使用说明如下。

- HQLite 区域可编辑，编辑结果在条件筛选框中同步显示。
- 添加多个条件和条件组的使用方法请参考**错误!未找到引用源。错误!未找到引用源。**。
- **1**：在下拉框列表中选择查询字段名，也可在输入框中输入字段名。
- **3**：包括以下两个选项
  - **V**：使用录入数据，即手动输入内容。
  - **F**：使用关联字段，即选择字段。
- **4**：
  - 当 3 框中选择 **V** 时，您需要手动输入查询字段的内容。
  - 当 3 框中选择 **F** 时，您需在下拉框列表中选择相应的字段。
- **2**：在下拉列表中选择操作符，使用规则如下：

关系操作符

=、!=、>、>=、<、<=：均为关系操作符，支持任意类型属性。

exist/not_exist

存在/不存在，无右操作数，支持任意类型属性。

like

字符串包含，**忽略大小写**，支持字符类型属性和字符串数组类型属性，对于字符串数组类型，只要数组的任意元素包含该字符串即可匹配。

使用方式与在搜索分析中保持一致，此处不再赘述。

rlike

正则全匹配，**忽略大小写，“.”支持匹配换行符**，仅支持字符类型属性，特殊字符需转义。

使用方式与在搜索分析中保持一致，此处不再赘述。

in

属于网段，仅支持 IP 类型属性，右操作数可配置为单个 IP，IP 区间(-)，子网掩码格式，逗号连接的多个 IP。

网段的包含。包含以下两种使用方法：

belong

属于特征，支持任意类型属性，右操作数仅支持 F，用于匹配系统内置安全信息。

在“**安全信息**”中，配置时“**字符类信息**”细分为“**字符串比较、正则全匹配、正则部分匹配**”三种子类型，

- **字符串比较**是用事件的字段值与该信息组的内容做比较，只要该事件的字段值与该信息组的任一内容相等即可(**大小写敏感**)；
- **正则全匹配**类型是用事件的字段值与该信息组的内容做正则模式全匹配，只要该事件的字段值能够完全匹配该信息组的任一正则表达式即可(**忽略大小写**)；
- **正则部分匹配**类型是用事件的字段值与该信息组的内容做正则模式部分匹配，只要该事件的字段值能够部分匹配该信息组的任一正则表达式即可(**忽略大小写**)。

正则类安全信息，不支持匹配换行符。

下面给出 belong 操作符样例：

contain

包含，仅支持数组类型，数组元素可为任意类型，数组任意元素内容与输入值相同即可匹配，**字符类属性大小写敏感。**

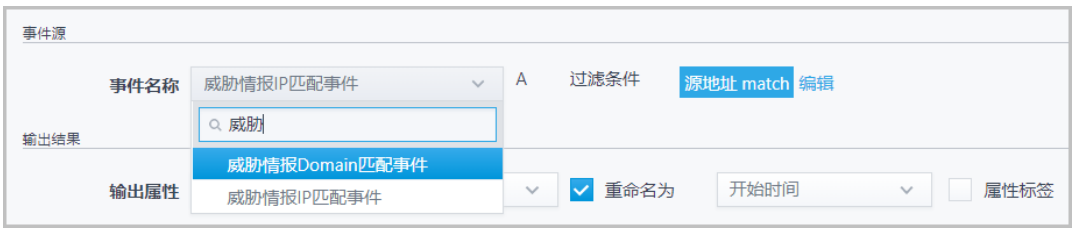
关联包含，针对 list 和数组类型，当前仅有威胁情报的个别属性支持 contain 操作符。支持的属性如下：

以“**情报标签**”为例，样例如下：

match

匹配情报，无右操作数，当前仅针对源地址/目的地址/域名三个字段有效。在配置威胁情报相关的规则时注意“**事件名称**”更新为“**威胁情报 IP 匹配事件**”或“**威胁情报 Domain 匹配事件**”。

样例如下：



示例

字符串及正则匹配，待匹配字符串：C:\Windows\system32\mmsys.cpl

- like/rlike 操作符

  进程命令行 rlike "C:\\Windows\\system32\\mmsys\.cpl" and 进程命令行 like "C:\\Windows\\system32\\mmsys.cpl"

- 字符串信息组:

  正则：C:\\Windows\\system32\\mmsys\.cpl

  字符串比较：C:\Windows\system32\mmsys.cpl

D HQL Time Filter

HQL Time Filter 是 HQL Filter （即 HQLite） 的子集，其模板为 发生时间 > ? AND 发生时间 < ?，

- 发生时间 是数据源指定的 defaultTimeField 字段的名称。
- > 和 < 为运算符，还可以是 >= 或 <=。
- ? 代表的是时间值。

时间值的分类

- 时间字符串，比如，"2018-10-11 12:00:00"，这种字符串必须由引号包裹。
- 时间戳，比如 1527657723667，不能有引号包裹，必须满足整数格式。
- 时间表达式，不能有引号包裹，示例如下：
  - now ：现在，此刻。
  - now/y：今年开始那一刻
  - now/mon：本月开始那一刻
  - now/w：本周开始的那一刻
  - now/d：今天开始那一刻
  - now/h：最近一小时开始那一刻

- now/m：最近一分钟开始那一刻
- now/s：最近一秒钟开始那一刻。
- now - 3m：此刻的 3 分钟之前；now + 1y 此刻的一年之后。
- now/d - 2d ：两天前的开始那一刻；
- now/mon - 2d ：这个月开始那一刻的两天之前。

应用

在事件分析和仪表盘中，返回给后端的查询时间范围，统一用 HQL Time Filter。常见示例如下：

- 发生时间 >= 1527657723667 AND 发生时间 <= 1527657723667 指定明确时间戳范围。
- 发生时间 >= '2018-03-01' AND 发生时间 < '2018-10-11' 指定明确日期时间范围。
- 发生时间 >= now/d - 1d AND 发生时间 < now/d 指定相对时间范围：昨天
- 发生时间 >= now/d 指定相对时间范围：今天到现在为止。
- 发生时间 >= now/w - 1w AND 发生时间 < now/w 上周
- 发生时间 >= now/d - 2d AND 发生时间 < now/d - 1d 前天
- 发生时间 >= now/y - 1y AND 发生时间 < now/y 去年
- 发生时间 >= now/y 今年到现在
- 发生时间 >= now/mon - 1mon + 1w AND 发生时间 < now/mon - 1mon + 2w 上个月的第二周

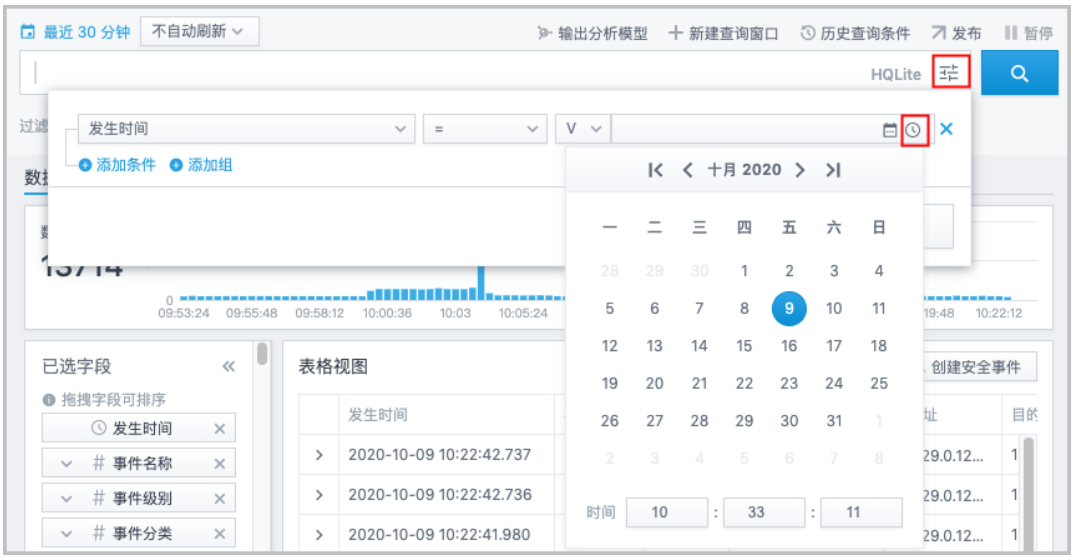
使用方法

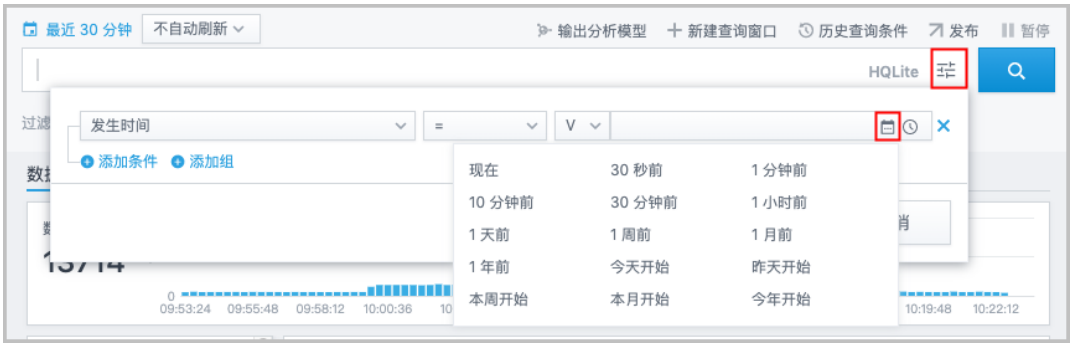
【方法一】

在 HQLite 输入框内输入时间参数，如“**发生时间**”，空格键后显示运算符及更多快捷选择时间。

【方法二】

在条件检索窗口打开快捷选择时间。





D.1 如何开启 WMI 配置

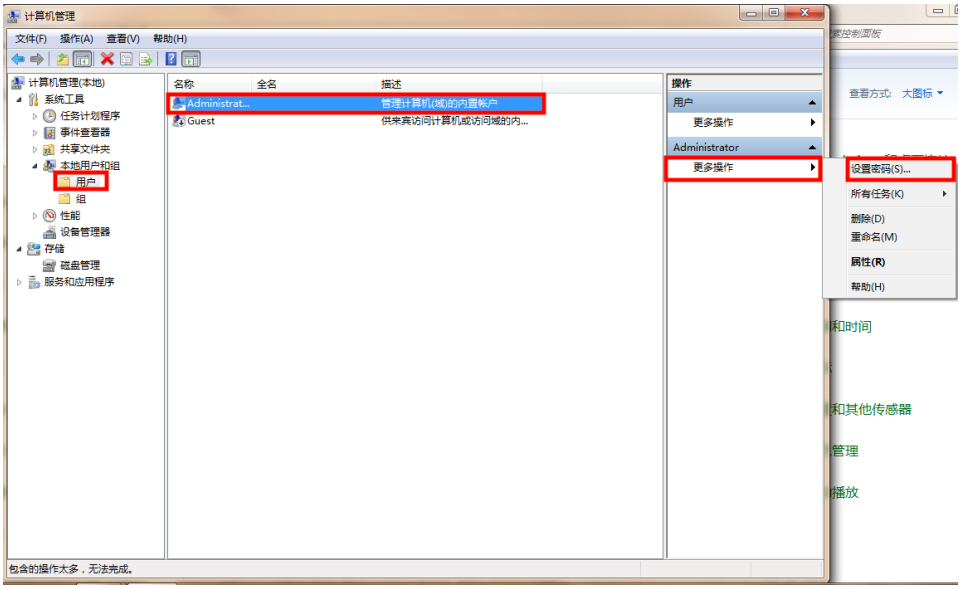
通过远程的方式连接 WMI 获取计算机信息时，可能会出现远程主机拒绝访问。以 Win10 为例介绍如何开启当前计算机的 WMI 服务，连接远程服务。

D.1.1 配置 Windows 操作系统登录用户

操作步骤

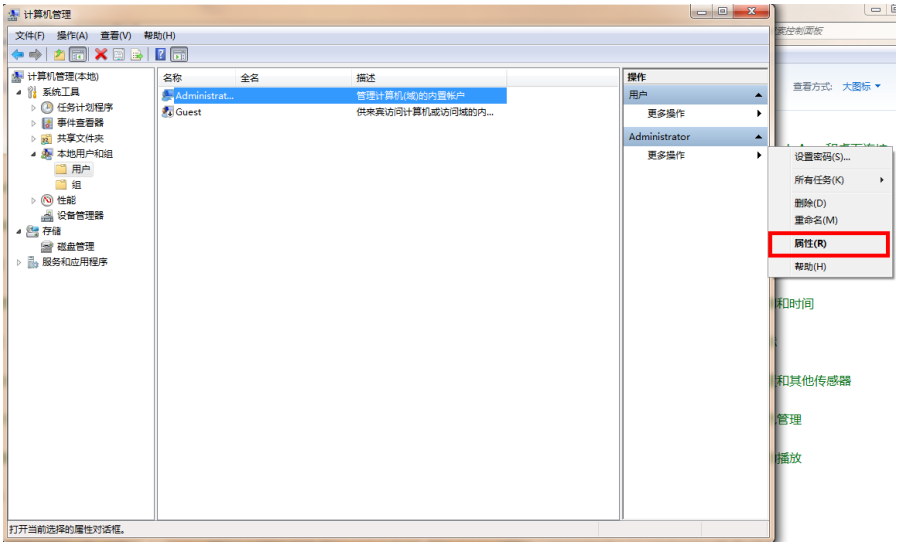
步骤1. （可选）若登录用户已设置密码，则请跳过此步骤；若登录用户未设置密码，可通过以下步骤设置。

依次选择“**控制面板** > **管理工具** > **计算机管理**”，在“**计算机管理**”页面依次选择“**本地用户和组** > **用户**”，单击选中“**Administrator**”，在右侧该用户下的“**更多操作**”下拉菜单中单击“**设置密码**”，在弹出的对话框中输入设置密码。

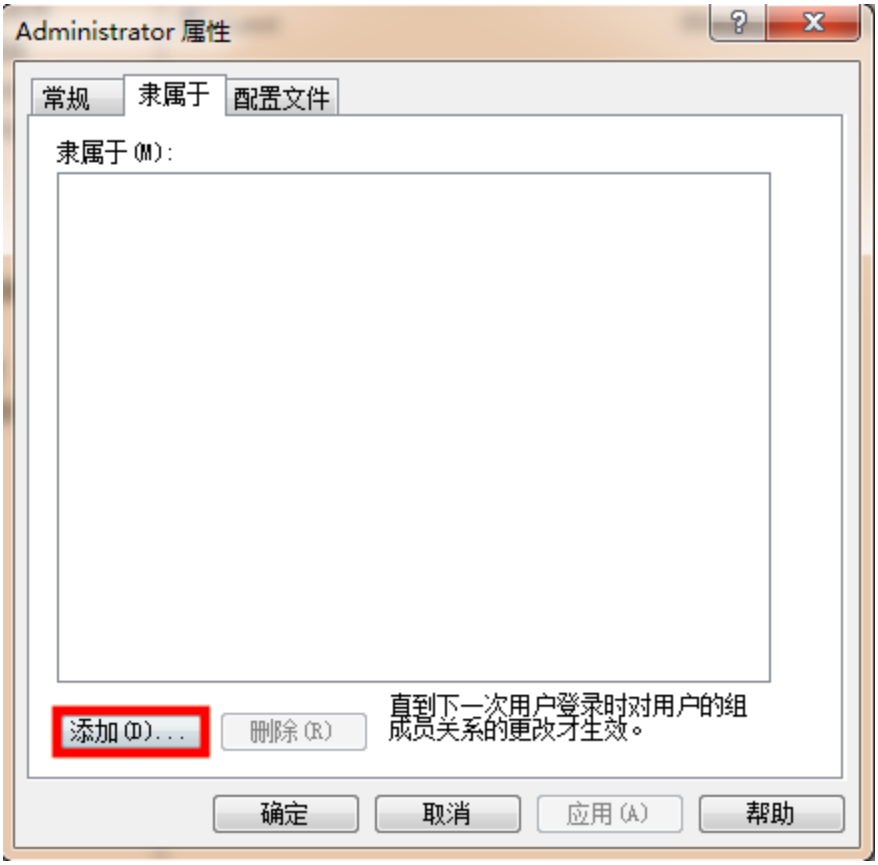


步骤2. 将登录用户添加到用户组“**Administrators**”和“**Distributed COM Users**”中。只有添加到这个组中才具有使用此计算机上的分布式 COM 对象的功能。

1. 在右侧该用户下的“更多操作”下拉菜单中单击“属性”，弹出“Administrator 属性”对话框。

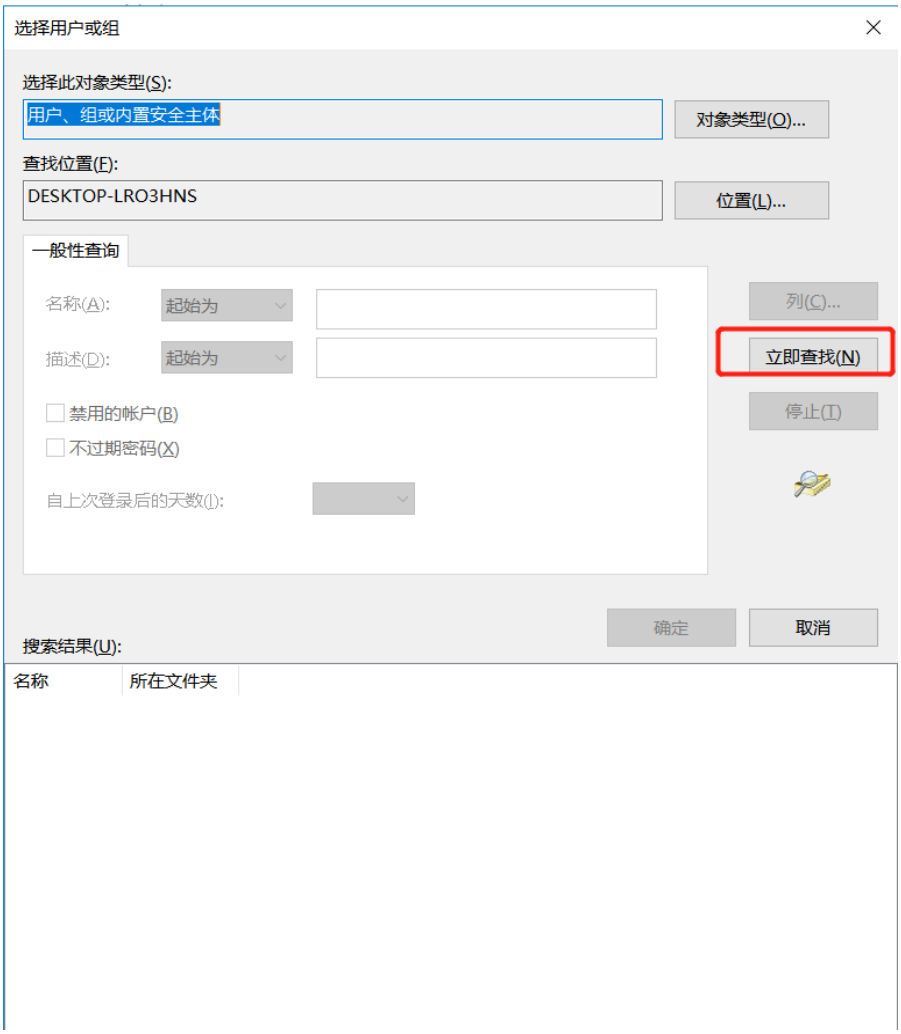


在“**Administrator 属性**”对话框中，选中页签“**隶属于**”。

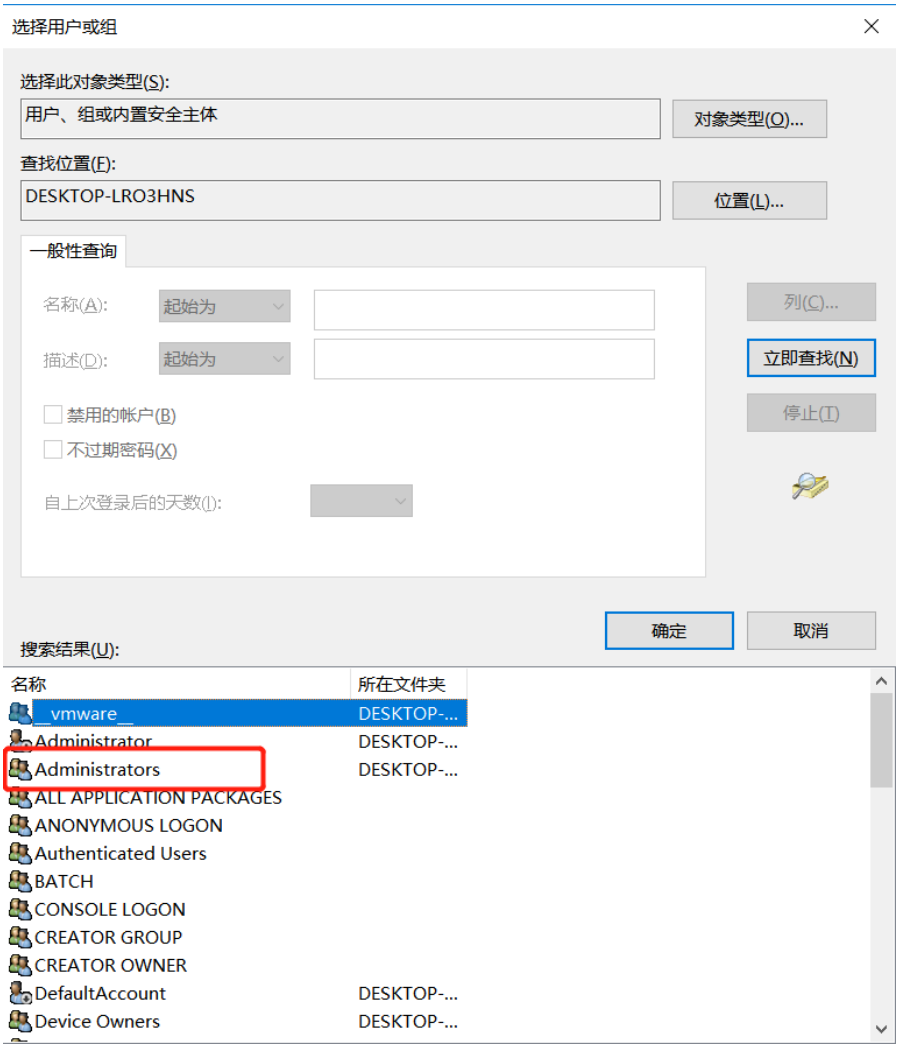


单击“**添加**”，弹出“**选择用户或组**”的对话框。

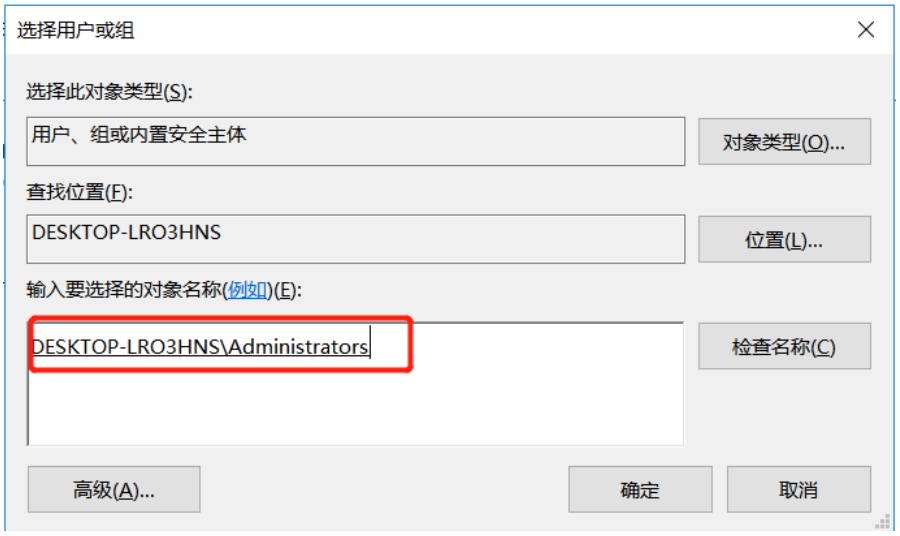
单击“**高级**”，弹出“**一般查询**”信息框。



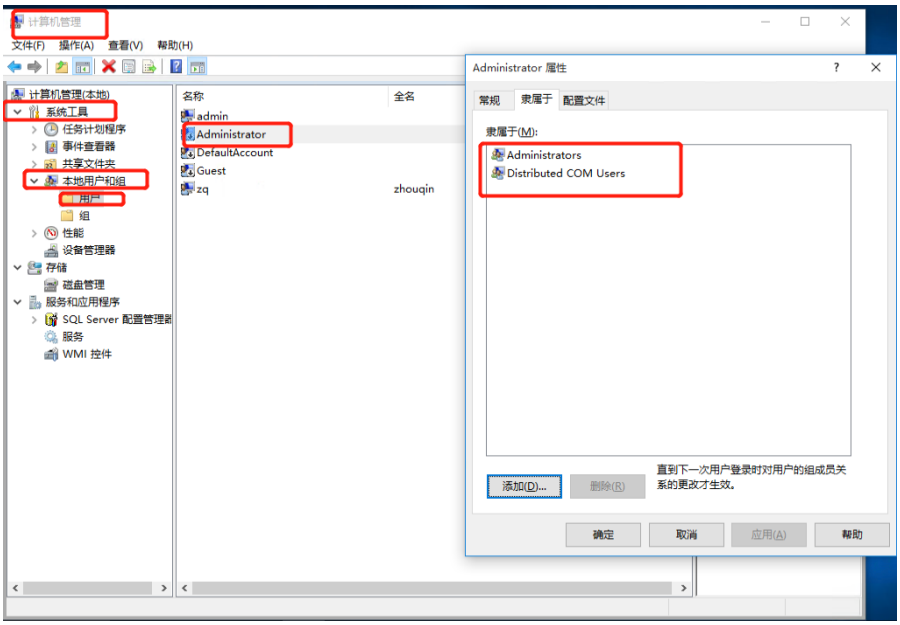
单击“**立即查找**”，显示搜索结果，分别选中“**Administrators**”和“**Distributed COM Users**”，并单击“**确定**”。



单击“**确定**”，设置用户组为“**DESKTOP-LRO3HNS\Administrators**”和“**DESKTOP-LRO3HNS\ Distributed COM Users**”。



单击“**确定**”，返回“**Administrator 属性**”对话框。



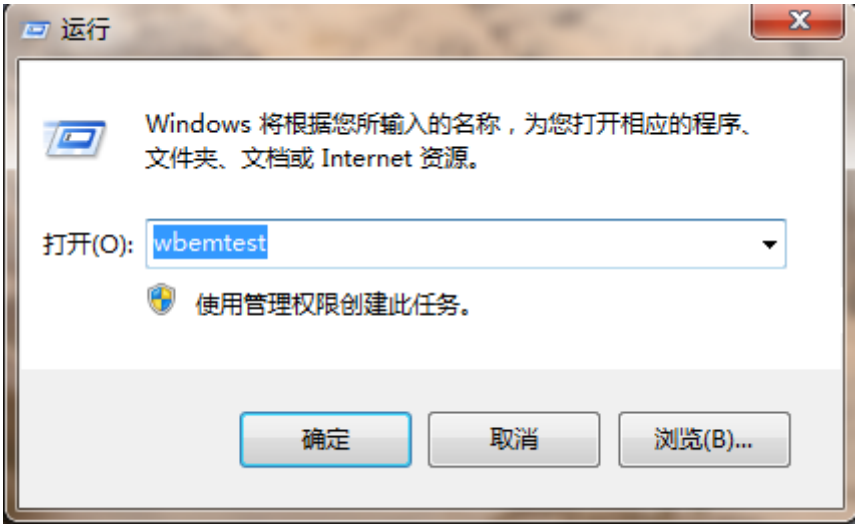
单击“**确定**”，完成用户组的设置。

D.1.2 在本机测试是否可以连接远程主机 WMI 服务

操作步骤

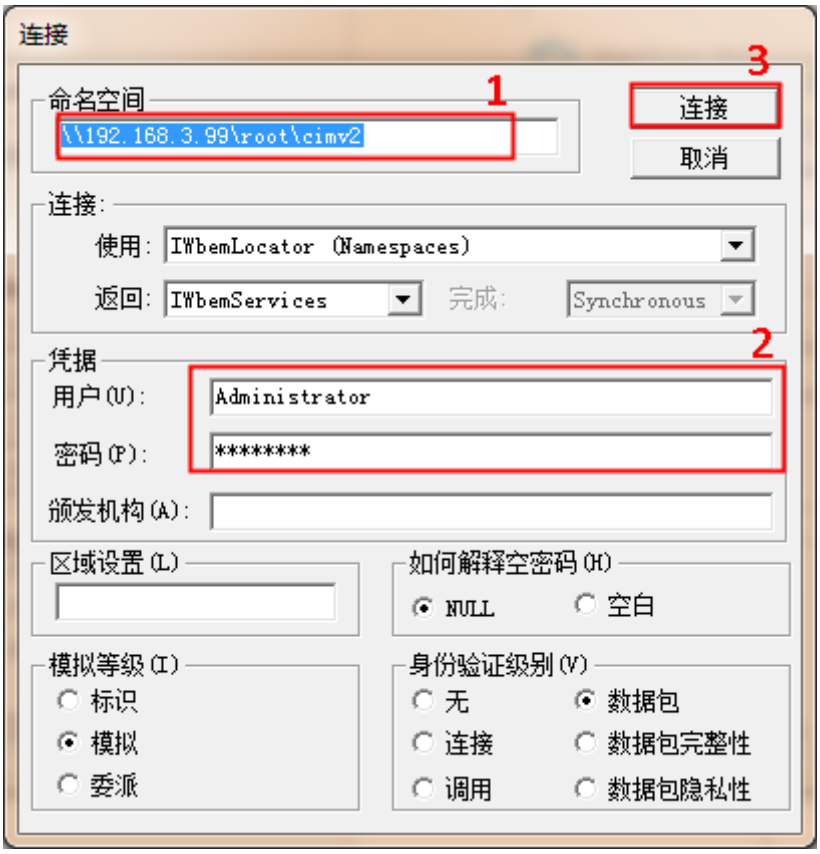
步骤1. 按下 **Windows+R** 组合键，调用系统运行窗口。

步骤2. 输入“**wbemtest**”命令。



步骤3. 打开 WMI 测试器。

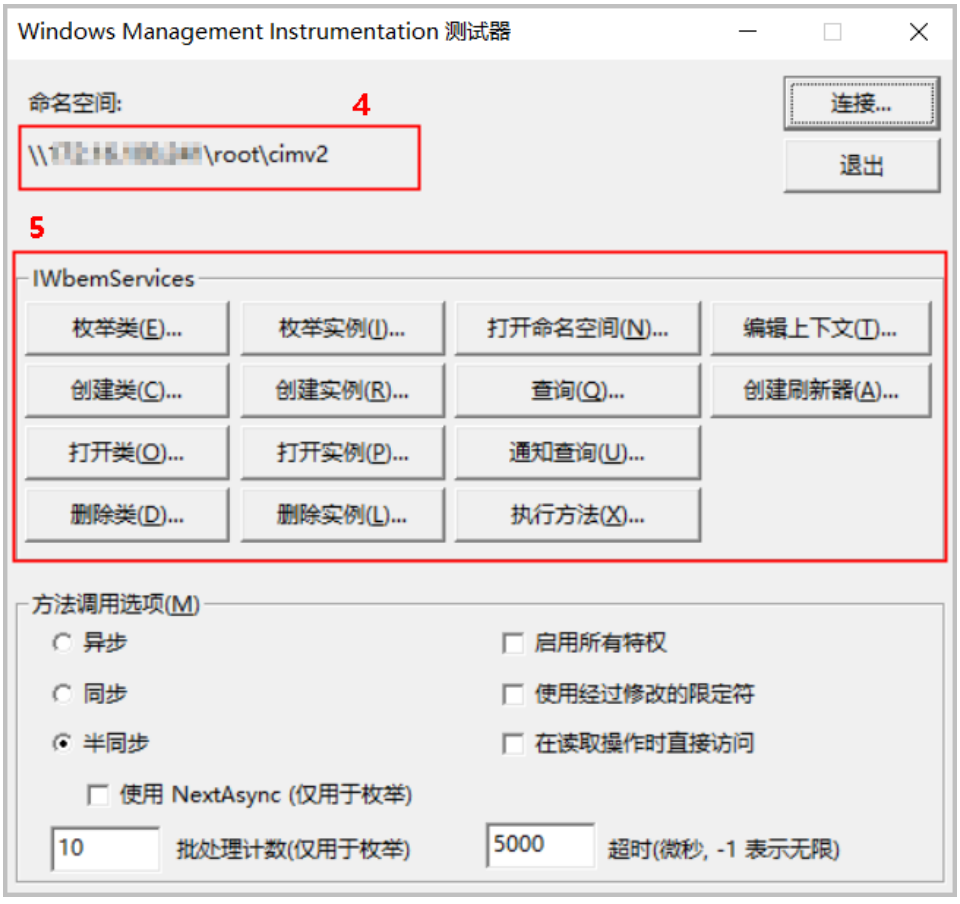
步骤4. 单击“**连接**”，配置连接远程 WMI 服务的参数。



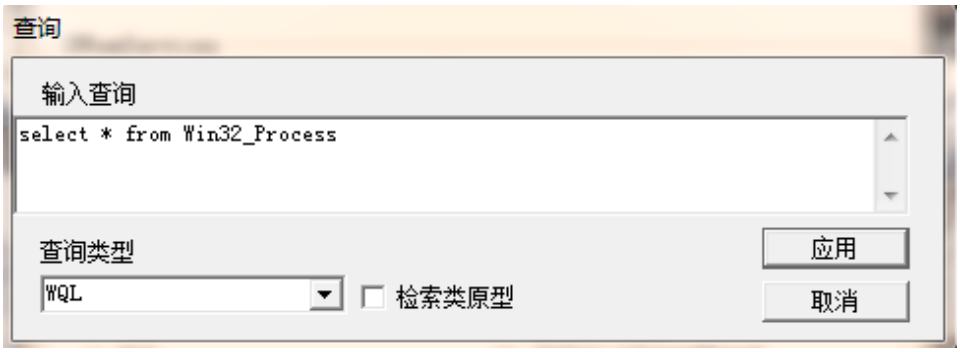
配置参数如下所示。

参数名称	参数说明
命名空间	缺省值为“root\cimv2”。 在缺省值前添加待采集数据的 windows 操作系统远程服务器的 IP。如“192.168.3.99”。 【示例】 \\192.168.3.99\root\cimv2
凭据	
用户	登录 Windows 系统的用户名。 可使用默认账号 Administrator，亦可使用其他自定义账号。
密码	登录 Windows 系统的用户的密码。

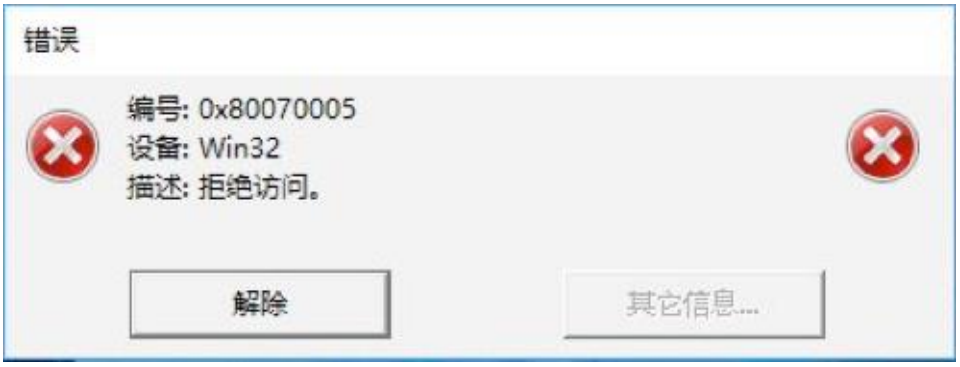
步骤5. 单击“**连接**”，返回以下页面。



步骤6. 在“**IWbemServices**”区域框中，单击“**查询**”，在弹出的对话框中输入 select 查询语句。



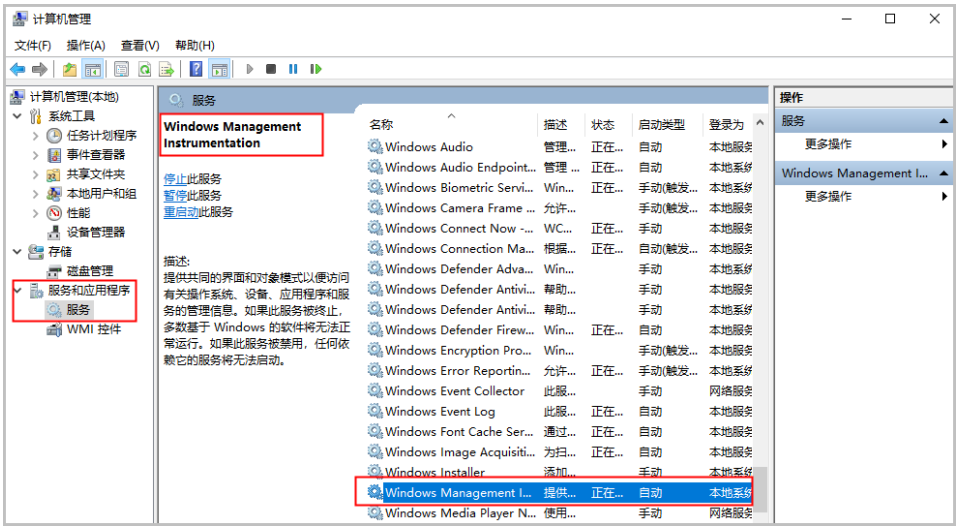
步骤7. 单击“**应用**”，若可查看相关 Windows 信息，则说明连接成功；否则失败，当弹出如下失败提示，请参考以下步骤解决。



D.1.3 开启远程计算机 WMI 服务

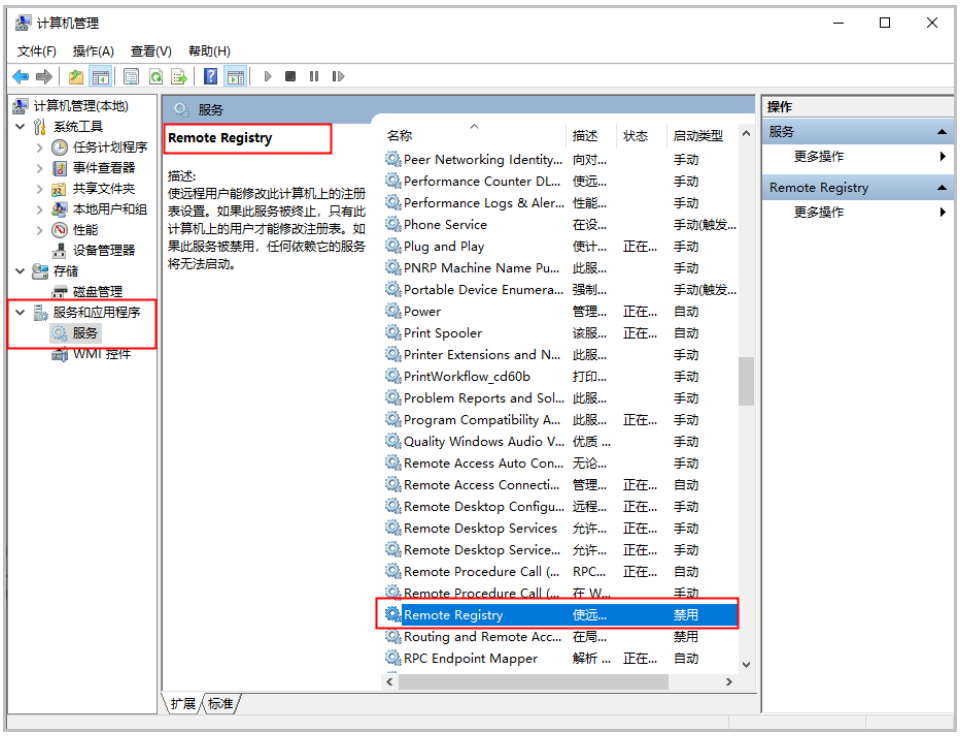
操作步骤

步骤1. 依次选择“**计算机管理 > 服务和应用程序 > 服务 > Windows Management Instrumentation**”，在“**更多操作**”列表中单击“**启动**”。



步骤2. 查看是否启用远程 Remote Registry 服务

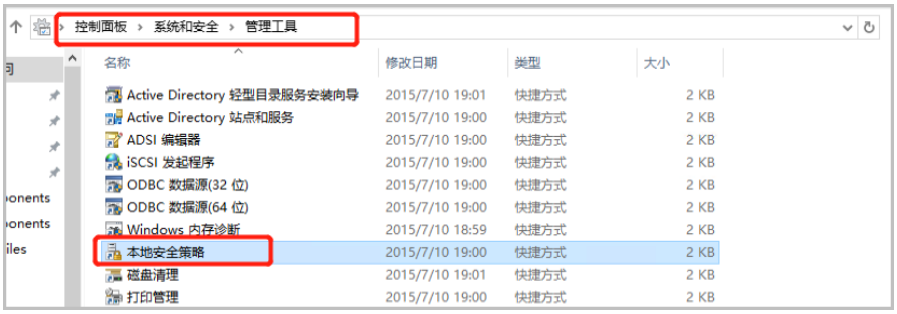
依次选择“**计算机管理 > 服务和应用程序 > 服务 > Remote Registry**”，在“**更多操作**”列表中单击“**启动**”。



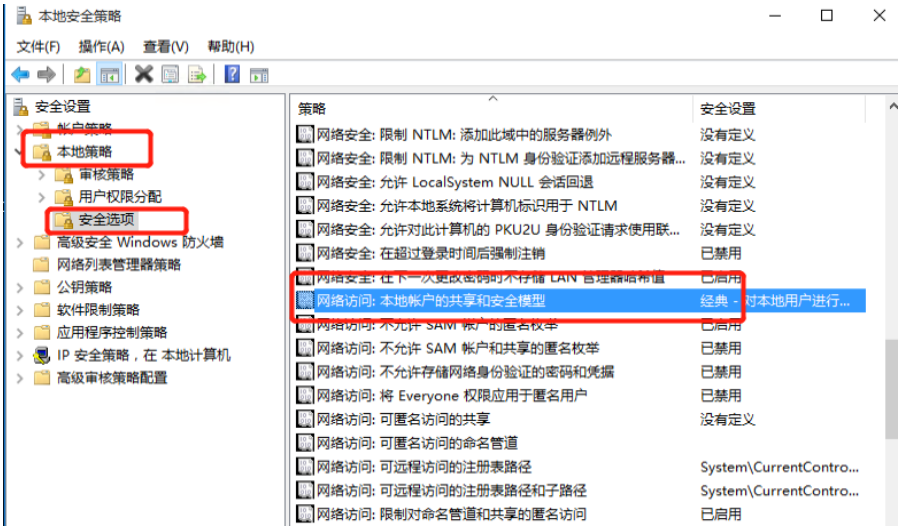
步骤3. 修改安全策略。

1. 依次选择“**控制面板 > 系统和安全 > 管理工具 > 本地安全策略**”。

在“本地安全策略”中选择“本地策略 > 安全选项”。

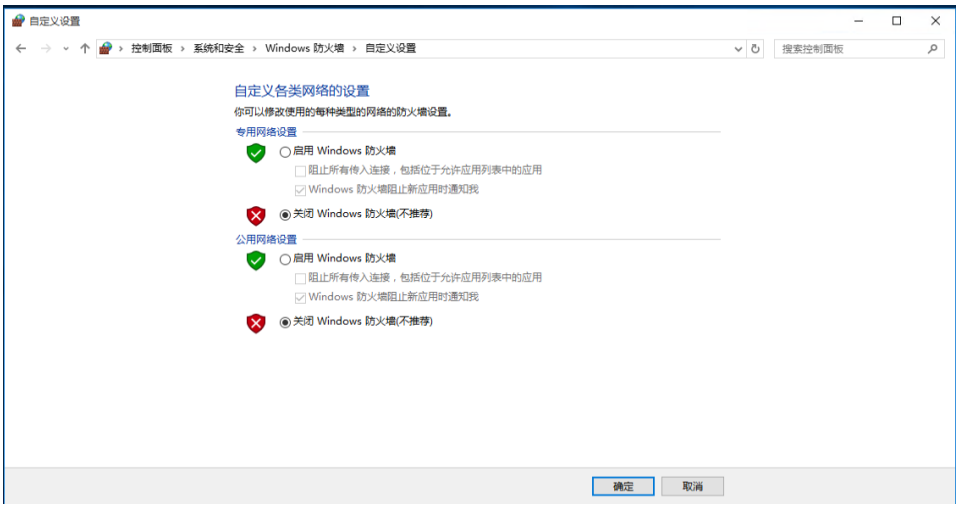


设置策略“**网络访问：本地账户的共享和安全模型**”，修改为“**经典**”。



步骤4. 关闭防火墙。

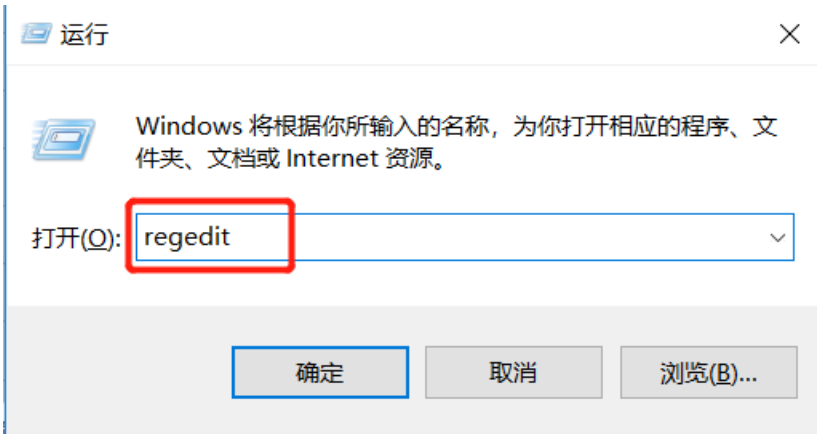
依次选择“**控制面板 > 系统和安全 > Windows 防火墙 > 自定义设置**”，关闭防火墙。



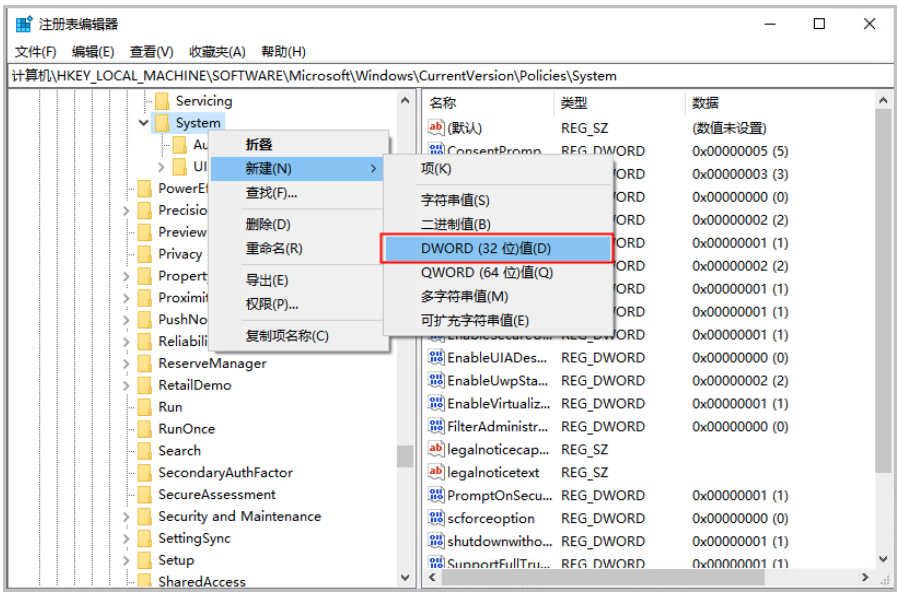
步骤5. 修改注册表。

1. 按下 Windows+R 组合键，调用系统运行窗口。

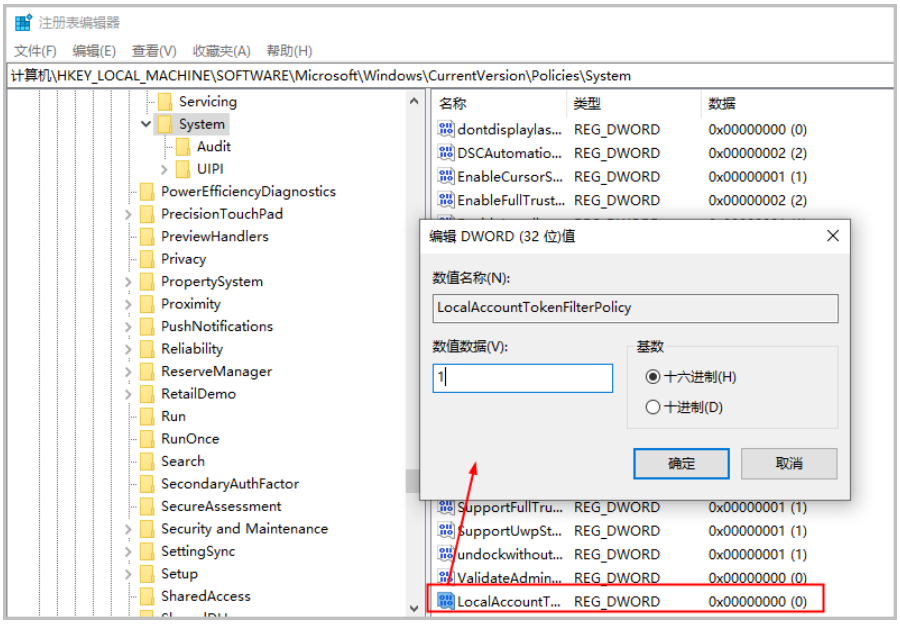
输入 regedit 命令。



修改“regedit”中“HKEY_LOCAL_MACHINE\SOFTWARE\Micrisoft\Windows\CurrentVersion\Policies\System\”，添加“LocalAccountTokenFilterPolicy”。



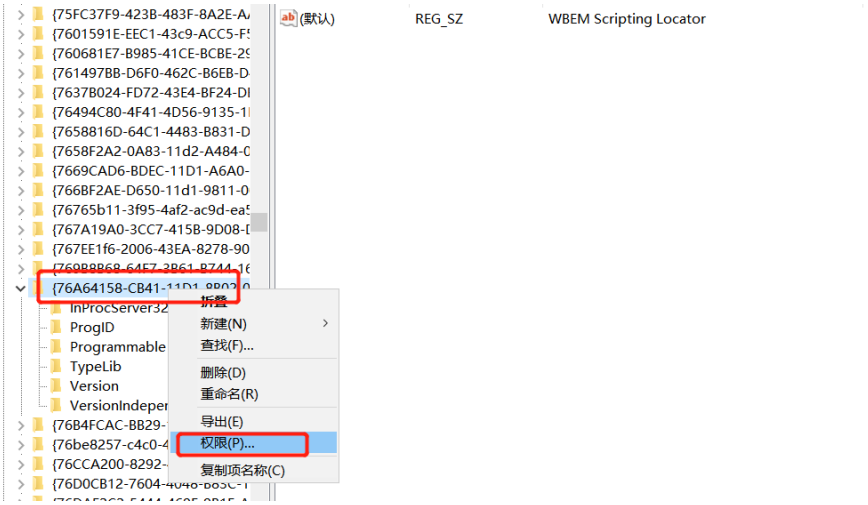
设置数值为“1”。



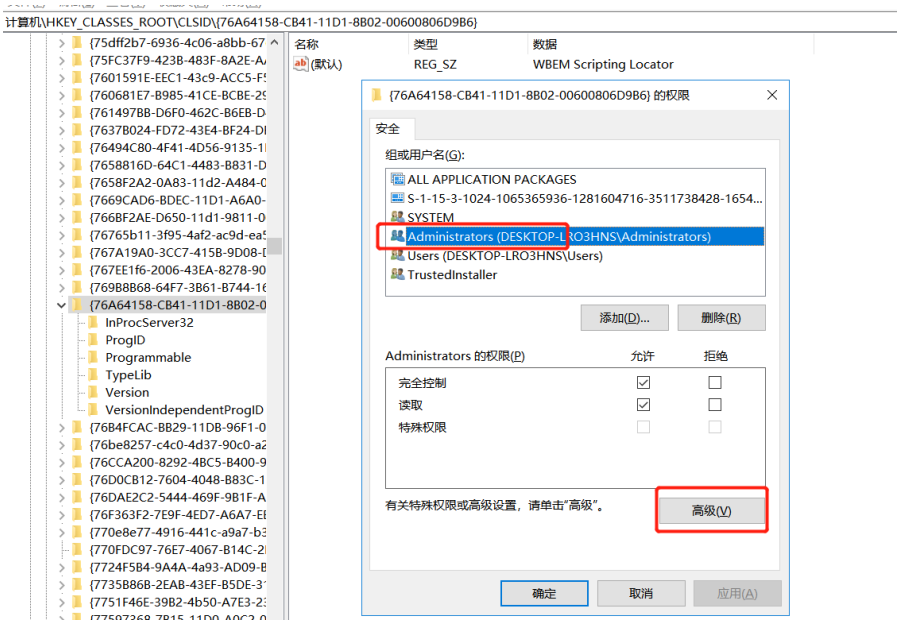
步骤6. 修改注册表。

修改“regedit”中“HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}”的权限，windows2008 不再给 Administrators 完全控制权。

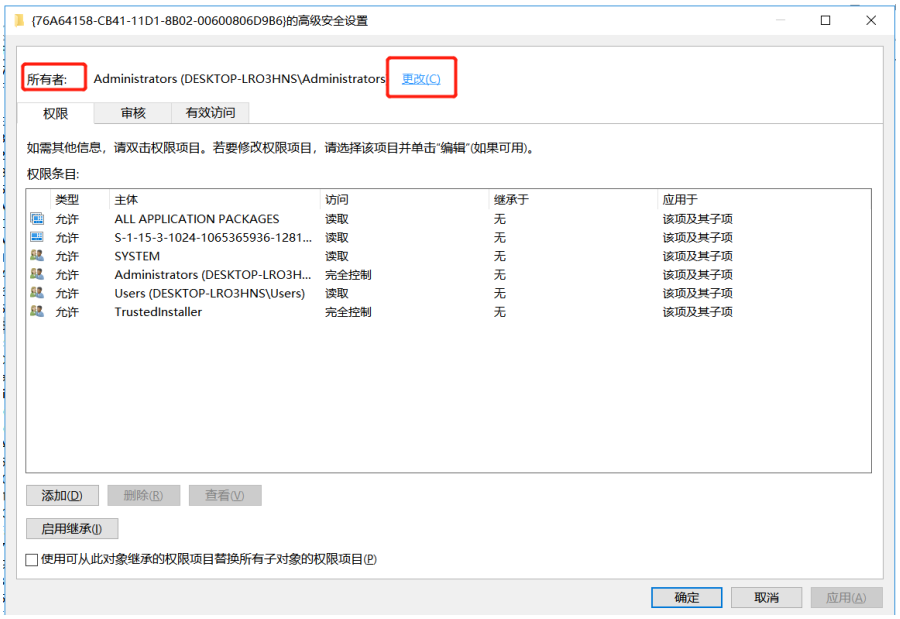
1. 根据路径定位“{76A64158-CB41-11D1-8B02-00600806D9B6}”，并选中右击。



单击“**权限**”，弹出该权限的对话框，选择“**组或用户名**”为“**Administrator（DESKTOP-LRO3HNS\Administrators）**”。

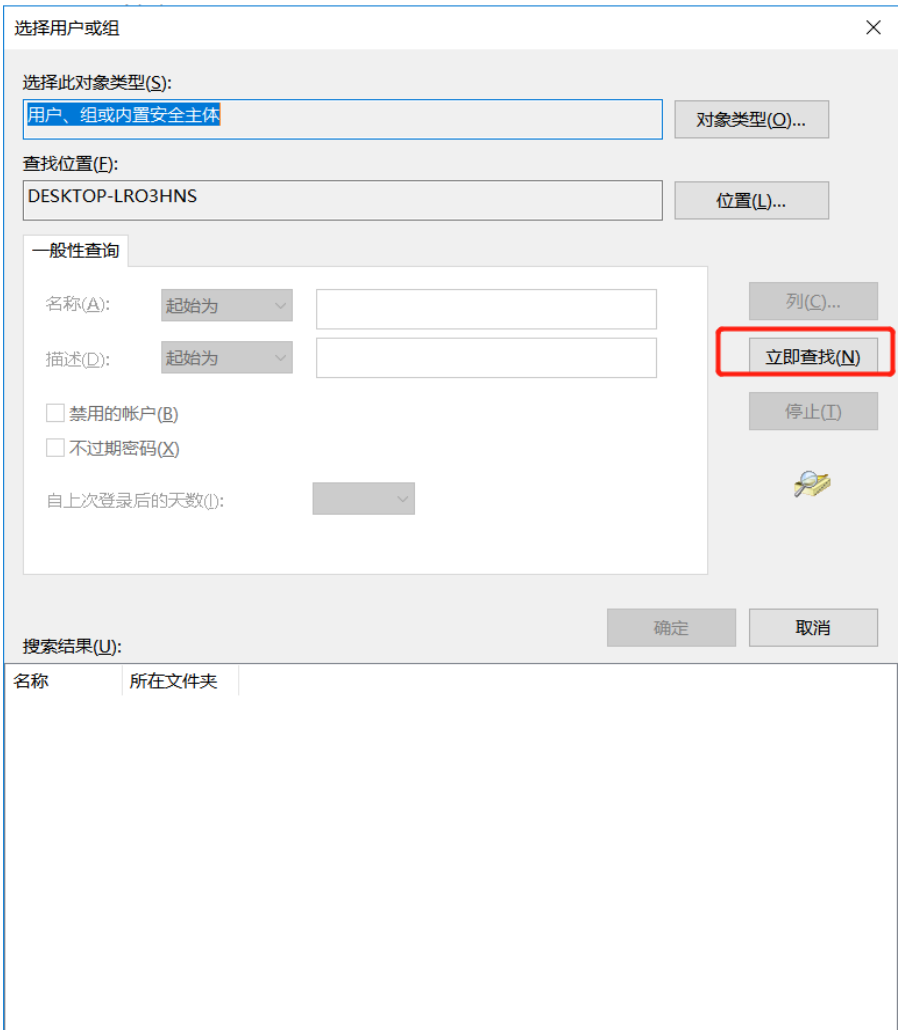


单击“**高级**”，弹出“**高级安全设置**”的对话框。



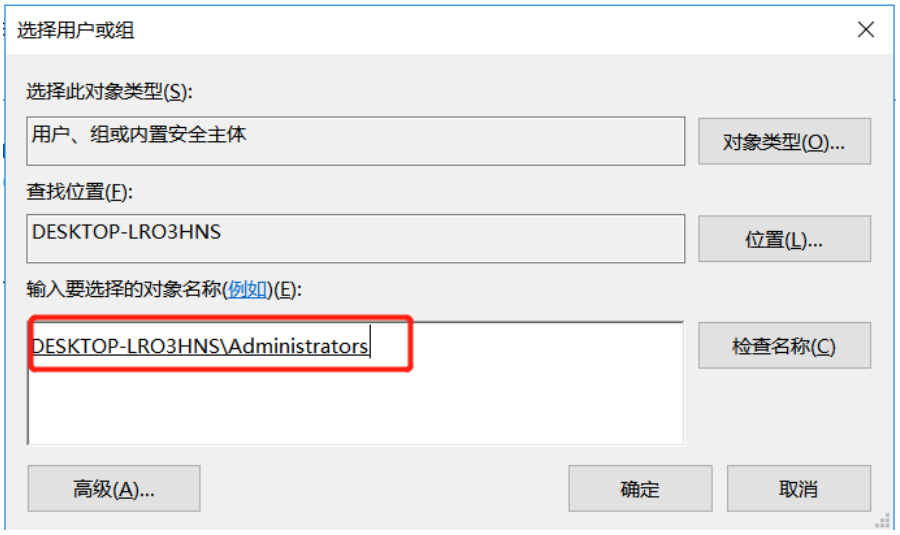
单击“**更改**”，弹出“**选择用户或组**”的对话框。

单击“**高级**”，弹出“**一般查询**”信息框。



单击“**立即查找**”，显示搜索结果，选中“**Administrators**”，并单击“**确定**”。

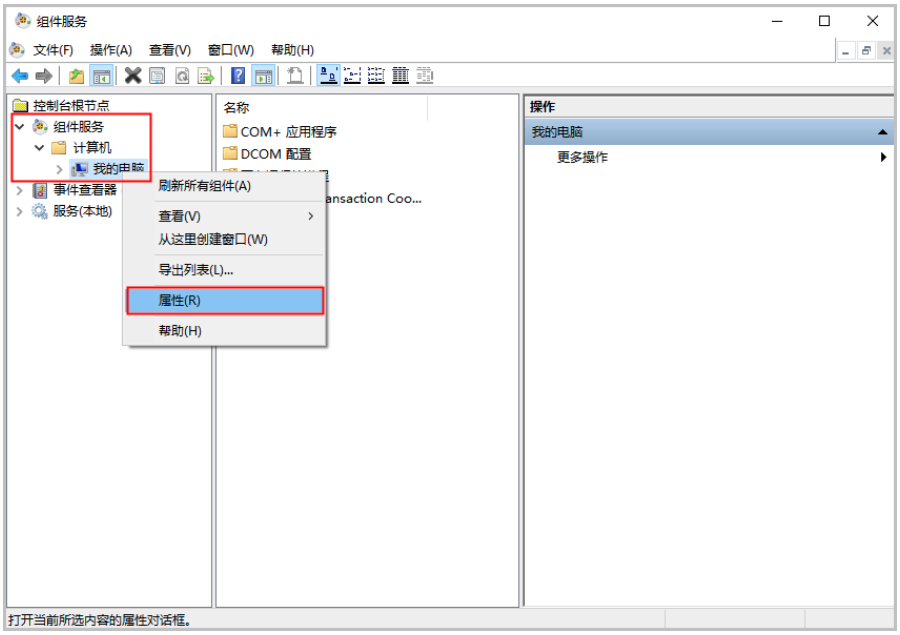
单击“**确定**”，设置用户组为“**DESKTOP-LRO3HNS\Administrators**”。



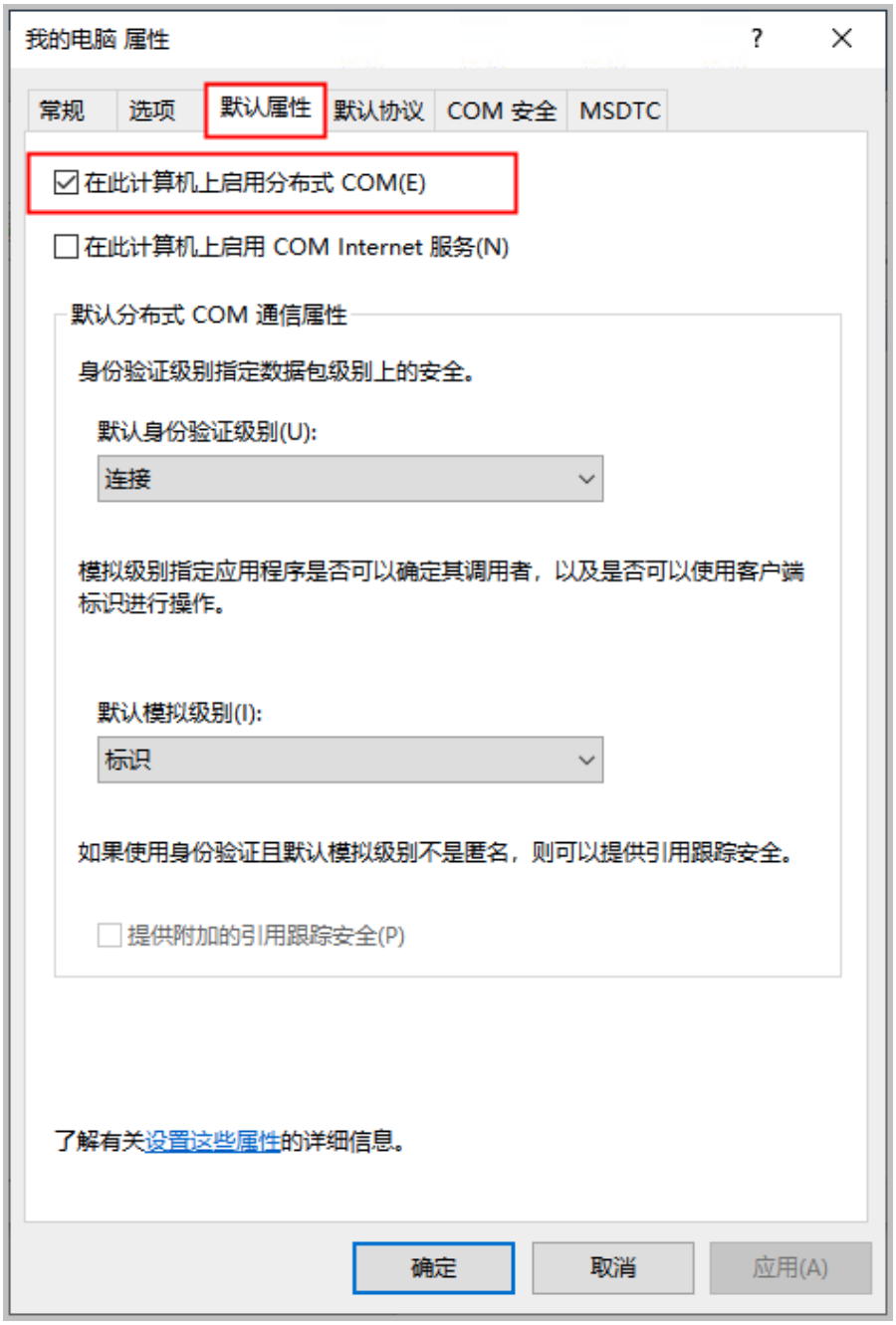
步骤7. 确认当前计算机是否已启用分布式的 COM 对象，只有开启才能够使用远程的 WMI 服务。具体查看方法如下：

1. 在计算机“**运行**”中输入“**dcomcnfg**”。

依次选择“**组件服务** > **计算机** > **我的电脑**”，右击之，并在弹出的菜单中单击“属性”。



在“**默认属性**”中查看是否勾选“**在此计算机上启用分布式 COM（E）**”，勾选即可。



D.2 如何开启 SNMP 服务

请被采集服务器中开启 SNMP 服务，否则会导致采集日志失败。本文以 Centos 服务器为例，介绍如何开启 SNMP 服务。其他类型的网络设备，如交换机、负载均衡等，请参见对应厂商的手册。

操作步骤

步骤1. 安装软件。

 # yum -y install net-snmp

步骤2. 修改配置文件。

 # vim /etc/snmp/snmpd.conf

请保证以下配置一致。

```
40 #       sec.name  source          community
41 com2sec notConfigUser  default       public
42
43 ####
44 # Second, map the security name into a group name:
45
46 #       groupName      securityModel securityName
47 group   notConfigGroup v1           notConfigUser
48 group   notConfigGroup v2c           notConfigUser
49
50 ####
51 # Third, create a view for us to let the group have rights to:
52
53 # Make at least  snmpwalk -v 1 localhost -c public system fast again.
54 #       name           incl/excl     subtree         mask(optional)
55 #view    systemview    included   .1.3.6.1.2.1.1
56 #view    systemview    included   .1.3.6.1.2.1.25.1.1
57 view    systemview    included   .1
58
59 ####
60 # Finally, grant the group read-only access to the systemview view.
61
62 #       group          context sec.model sec.level prefix read   write  notif
63 access  notConfigGroup ""      any       noauth    exact  systemview none none
64
65 # -------------------------------------------------------------------------
```

步骤3. 执行以下命令，重启 SNMP 服务。

 # service snmpd restart

步骤4. 执行以下命令，设置 snmpd 每次开机时自动启动。

 # chkconfig snmpd on

步骤5. 执行以下命令，检查 snmpd 服务是否已在运行：

 # netstat -nlup | grep ":161"

```
udp 0 0 0.0.0.0:161 0.0.0.0:* 16986/snmpd
```

该命令检查本地是否已在监听 UDP 端口 161，如果返回类似以上结果，表明 snmpd 服务启动成功。

FAQ

关联分析规则导入失效

问题描述

LAS 系统 1 的环境中，在“**系统管理 > 基础配置 > 内网 IP**”配置中添加内网子网，如：xx 云；在一条关联分析规则“**rule1**”中添加过滤条件，如：源地址 belong xx 云，配置其他必填项，规则生效。

将该规则“**rule1**”导入 LAS 系统 2 环境中后，该规则失效。

解决方法

在 LAS 系统 2，“**系统管理 > 基础配置 > 内网 IP**”配置中添加相同的内网子网后，并在关联分析规则“**rule1**”中重新编辑此过滤条件：源地址 belong xx 云。此关联分析规则才会生效。

更多提示

当 LAS 系统 1 中的关联规则的过滤条件包括信息组的过滤，导入 LAS 系统 2 中失效了，说明此信息组为自定义的。因此需要在 LAS 系统 2 中添加此信息组，并重新编辑一下过滤条件。