日志审计与分析系统

用户手册

AVCOMM恩创®

日志审计与分析系统

用户手册

关于此用户手册

此用户手册旨在指导专业安装人员安装和配置日志审计与分析系统。包括帮助避免意外发生问题的步骤。

注意:

只有合格且经过培训的人员才能对此产品进行安装、检查和维修。

免责声明

AVCOMM保留随时更改本手册或产品硬件的权利，恕不另行通知。此处提供的信息目的是为了保证其准确可靠。但是可能不会涵盖所有的细节和更改，也并未提供在安装、操作或维护过程中遇到的所有可能的意外情况。如需更多信息，或出现未完全包含在此手册中的特定问题，应将此提交给AVCOMM。用户有责任确定手册是否有任何针对添加的新信息和/或纠正可能的无意造成的技术或印刷错误进行的不定期更新和修订。AVCOMM对其被第三方使用不承担任何责任。

AVCOMM在线技术服务

在AVCOMM，您可以使用在线服务表来请求支持。提交的服务表保存在服务器上，供AVCOMM团队成员分配任务并监控您的服务状态。如遇任何困难，请随时发邮件至sales@n-tron.com.cn

目录

1. 系统概述

本文介绍了恩创日志审计与分析系统的安装维护方法和使用指南。主要包括产品的主要功能介绍、软件安装运行环境要求、软硬件安装配置方法、各菜单功能使用方法、用户管理、系统管理、软件设置和维护注意事项等，还介绍了分布式日志存储计算节点、日志采集探针和日志代理的安装配置方法等。通过阅读本文档, 用户可以了解恩创日志审计与分析系统的基本组成, 并初步掌握配置和使用恩创日志审计与分析系统。

恩创日志审计与分析系统作为一个统一日志监控与审计平台，能够实时不间断地将政企客户中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。如果客户网络中重要网络和业务系统无法产生日志，日志审计与分析系统也能够通过部署硬件探测器的方式主动侦测网络中的协议通讯，并转化为日志，汇集到审计中心。

日志审计与分析系统能够实时地对采集到的不同类型的信息进行标准化处理和实时关联分析，协助安全管理人员从海量日志中迅速准确地识别安全事故，大幅降低了日志分析和管理对安全管理人员的技术能力要求，提高了工作效率。

日志审计与分析系统帮助用户满足安全审计的合规要求，可帮助用户快速出具满足国家法律法规，行业标准的多种合规报表和报告，帮助安全人员对内部管理的合规情况一览无余。

日志审计与分析系统实现了针对海量、高速、异构日志和事件的高吞吐量采集、高效的长期存储和快速实时的数据分析。系统采集和存储事件，支持搜索、检索和报告。系统记录原始日志，支持未修改数据的即席查询，以获取高质量的调查取证数据。

2. 名词解释

日志

日志是 IT 系统产生的数据，它记录着设备、操作系统和应用软件的运行状态，是 IT运维管理人员和安全管理人员日常运维排查故障的重要依据。

范式化

按照一定的规范，将各种不同表达方式的日志或信息数据转换成统一的描述形式，将非结构化数据转化为结构化数据。

告警

由网络管理、系统管理或安全管理对信息进行处理和综合分析后，发现的故障信号或安全问题，以告警的方式进行提示，告警具有严重性等级、分类等信息，在本系统中由关联分析或阈值出发产生。

关联分析

关联分析又称关联挖掘，就是在关系数据或其他信息载体中，查找存在于项目集合或对象集合之间的频繁模式、关联、相关性或因果结构。在日志审计与分析系统中特指从海量的日志和事件中结合相关数据描述一个或多个事件中某些属性同时出现的规律和模式。

管理中心

指日志审计与分析系统的管理中心，又称为分析中心。

日志采集器

用于实现日志采集，并把事件转发给审计或分析中心。采集方式包括主动采集数据库日志、文件日

志、主机日志等，被动接收 Syslog、SNMP Trap 等协议数据包。日志采集器可以安装在被采集设备上，也可以独立部署在另外的服务器上。

日志代理

是指安装在主机上，用来采集主机自身日志，或者是安装在主机上的其他应用系统的日志的代理程序。目前系统提供 Windows 日志代理程序和 Linux 日志采集脚本。

3. 首次使用

3.1 导入许可

系统安装完成，浏览器访问 http://[ip]:16520，进入导入许可页面，如下图：

选择许可文件，导入。若成功，提示：

浏览器重新输入 http://[ip]:16520，即可正常使用系统。

3.2 登录系统

浏览器访问 http://[ip]:16520，进入用户登录页面。

系统基于三权分立原则，内置三个用户：

- operator 安全管理员，负责系统的操作使用和日常运行维护及权限分配。
- admin 系统管理员，管理系统权限，维护用户。
- auditor 审计管理员，对系统操作进行审计分析。

三个内置用户的密码均为Admin@123，请登录后立即修改密码。

使用operator 用户登录系统。

3.3 配置日志源

系统默认启动了 syslog 采集任务，监听 udp 514 端口。 配置要采集日志的主机或设备，将 syslog 日志发送至日志审计服务器。

如需配置更多采集任务，进入节点管理-事件采集器，配置本地事件采集器，添加采集任务。

3.4 分析日志

日志源接入后，在事件分析模块可以看到接收到的事件列表和统计信息。更多系统功能请查看帮助手册的详细功能介绍。

4. 仪表板

仪表板用于将用户感兴趣的内容通过面板的方式，组合在一个页面中，即一个仪表板，便于同一时间关注。

4.1 仪表板菜单

点击菜单上的【仪表板】菜单，将会显示所有当前用户可以查看的仪表板，这些仪表板将会按照创建者来分组展示。直接点击其中的仪表板即可查看此仪表板。

4.2 仪表板的查看

每个用户都可以拥有自己的一套仪表板，这些仪表板只有该用户自己才能够查看。 只有仪表板的创建者将仪表板设置为共享后，则系统内的所有用户都可以查看到仪表板。（可以查看到仪表板并不代表可以查看到仪表板内所有面板的内容，面板内容的可见性还取决于用户是否用户改面板所属模块的权限）。

4.3 仪表板的维护

在【仪表板】菜单中点击【添加】按钮，即可进入仪表板添加（修改）页面。

4.3.1 添加

仪表板的创建需分两步进行：

1、填写仪表板基本信息

- 名称
- 描述

2、面板维护

- 添加/删除面板
- 设置面板的大小/位置

> [提示]
>
> - 第一步完成后，需点击【保存】按钮才能够继续
> - 面板维护的结果即时生效，即对面板进行添加/删除/设置大小/改变位置后，无需点击按钮栏的【保存】按钮

4.3.2 修改

在仪表板查看页面，点击【编辑】按钮，即可以进入仪表板编辑页面，对仪表板的基本信息和面板进行修改。

只有仪表板的创建者才能够修改仪表板。

4.3.3 删除

在查看仪表板页面，点击【删除】按钮，确认后即可删除仪表板。

只有仪表板的创建者才可以删除仪表板。

4.3.4 共享

仪表板缺省为只允许创建者查看，如果想让系统中的其它用户查看，可以在仪表板查看页面点击按钮栏的【共享】复选框按钮，来设置仪表板为共享（或取消仪表板共享）。

当取消仪表板共享后，会自动取消该仪表板的置顶为菜单（如果有）设置。

4.3.5 菜单

有些仪表板仅仅共享给其它用户查看还不够，还希望更快更方便的找到这个仪表板并查看，可以在仪表板查看页面点击按钮栏的【菜单】复选框按钮，来将仪表板置顶为菜单（或取消置顶为菜单）。

通过仪表板查看页面的【菜单】按钮置顶为菜单时，此仪表板将会作为第一个菜单项出现。如果需要调整菜单项位置，则可在【菜单管理】中进行。

置顶为菜单时，会自动将仪表板设置为共享（如果不是）。

4.3.6 全屏

通过点击按钮栏的【全屏】按钮可以将当前仪表板全屏显示。

4.4 仪表板面板

4.4.1 面板的内容

面板的类型包括

- 文本
- 图片
- 页面

4.4.2 面板的添加

在仪表板查看页面，点击按钮栏的【添加面板】按钮，即可弹出添加面板功能区。面板的添加按照添加来源被分为：

- 选择预置面板
- 从其他仪表板中复制
- 创建全新的面板

4.4.2.1 选择预置面板

本产品出厂时，即预置了一定数量的面板，这些面板可以直接添加到你的仪表板中， 并可以在添加后调整大小和位置。

4.4.2.2 从其他仪表板复制

面板还可以来自于已经创建好的仪表板中的面板，仪表板可以是你创建的，也可以是其它用户创建的（已共享）。

通过直接从仪表板中选择相应的面板，即可以添加到你的仪表板中，并在可以在添加后调整大小和位置。

由于系统中已经创建的仪表板数量较多，仪表板中的面板同样数量较多，选择面板页面提供搜索过滤功能，可以在【搜索框】中输入面板名称，来只显示符合过滤条件的面板。

4.4.2.3 创建新的面板

创建新的面板需要输入和选择面板的基本属性，包括：

- 名称，如果不填写名称，则在仪表板查看页面不显示面板标题栏
- 描述
- 面板背景，背景支持
  - 默认
  - 透明
  - 白色

完善基本属性外，还需要选择面板的内容类型，并根据不同的类型，输入和选择扩展属性。

4.4.3 面板的大小

整个仪表板页面被平均分割为 12 列，100 像素高为一行。每个面板的最小宽度为 1列，最小高度为 100 像素；最大宽度为 12 列，最大高度为 6 x 100 像素。

面板的大小，可以在仪表板编辑状态，通过将鼠标置于面板右下角点击后进行调整。

4.4.4 面板的位置

在整个仪表板范围内，只要有足够空间，即可在任意位置放置面板。

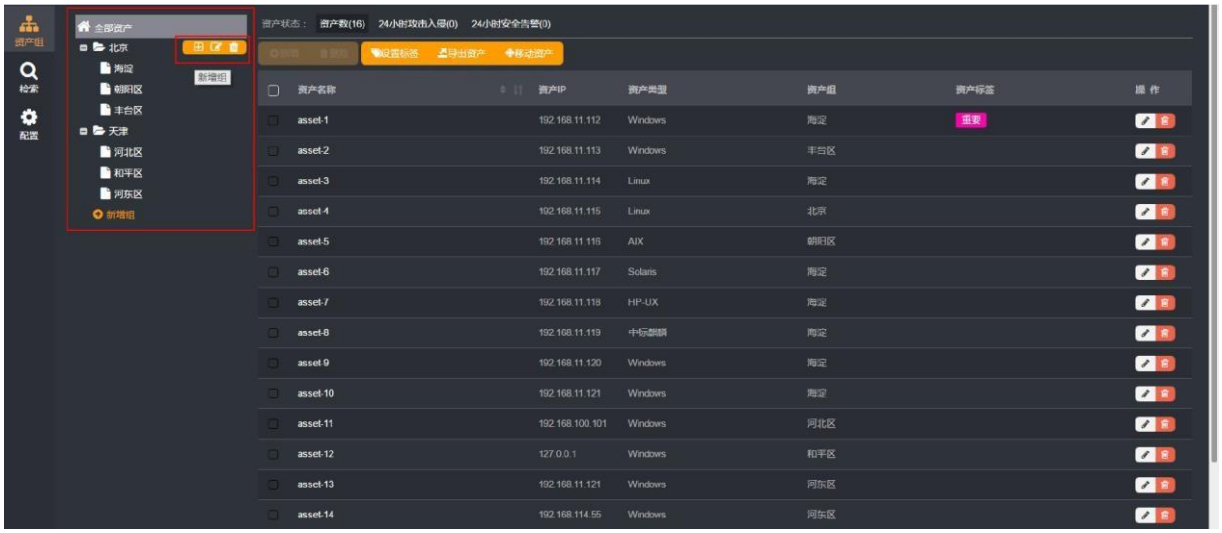
面板的位置，可以在仪表板编辑状态，通过将鼠标置于面板标题位置点击后进行拖放调整。

5. 资产

资产模块实现了对企业或组织中与审计相关的IP 设备的管理。该模块有三个子模块：资产管理、资产检索、资产配置。

5.1 资产组

资产组是指同一环境内有相同的安全保护需求、相互信任、并具有相同的安全访问控制和边界控制策略的网络或系统。每个资产组具有基本相同的安全特性，如安全级别、安全威胁、风险等，依据这些特性，将资产归入不同的资产组中，实施不同的安全保护。资产组管理如下图所示：



5.1.1 添加

资产组的添加可点击新增组按钮或者资产组树上的【新增组按钮】，即可打开新增资产组面板。添加资产组步骤如下：

1、填写资产组信息

- 资产组名称
- 资产组价值
- 等保定级
- 描述[可选]

2、点击【确定】按钮，保存资产组

5.1.2 修改

在资产组页面，点击资产组树上的【编辑组按钮】，即可打开资产组编辑面板，编辑资产组的名称、价值、等保定级和描述信息，点击【确定】修改资产组。

5.1.3 删除

在资产组页面，点击资产组树上的【删除组按钮】，即可打开删除确认状态框，点击【删除】删除该资产组。

[提示]

删除资产组时会删除组下资产，请谨慎操作。

5.1.4查看资产

选择资产组树上节点，可查看该组下资产。

5.2 资产管理

资产以表格展示，可对资产进行新增、修改、删除、设置标签、导出资产和移动资产等操作。

5.2.1 新增资产

新增资产需选中当前登录用户所拥有的资产组，然后点击新增按钮，即可打开新增资产面板。新增资产步骤如下：

1、填写资产基本属性

- 名称
- 类型
- 管理 IP
- MAC 地址
- 序列号
- 生产厂商
- 地理位置
- 设备联系人

2、添加资产标签

- 选择已存在标签或添加新标签

3、选择安全属性

- 机密性
- 资产价值
- 可用性
- 等保定级
- 完整性

4、填写资产接口信息，可填写多个接口

- IP
- MAC

点击【确定】按钮即可保存资产。

5.2.2 修改资产

在资产组页面，点击资产列表中【编辑】按钮，即可打开编辑资产面板，即可对资产的信息进行修改。

5.2.3 删除资产

在资产组页面，点击资产列表中【删除】按钮，确认即可以删除资产。或者选中要删除的资产点击资产列表上的【删除】按钮可删除选中的资产。

5.2.4 设置标签

在资产组页面，选中要设置标签的资产，点击【设置标签】按钮，即可打开选择标签模态框，选择标签点击【确定】按钮后即可为选中资产设置标签。

5.2.5 导出资产

在资产组页面，点击【导出资产】按钮，可导出当前用户权限下所有资产，导出文件格式为 EXCEL 文件。

5.2.6 移动资产

在资产组页面，选中要移动的资产，点击【移动资产】按钮，即可打开选择资产组模态框，选择资产组点击【确定】按钮后即可将勾选的资产移动到指定的资产组中。

5.2.7 资产详情

在资产组页面，点击资产列表中资产名称，即可打开资产详情面板。资产详情包括资产基本信息、攻击入侵、告警、登录事件和配置变更。

5.3 资产检索

资产检索是用来通过关键字、资产类型、资产组、资产标签、资产等级、是否有告警、漏洞、配置等等多种条件组合进行检索资产。

5.3.1 检索条件

资产检索的左侧页面为检索条件，支持的检索条件如下：

1、关键字

- 资产名称
- 资产描述
- 资产 IP
- 操作系统
- 开放端口
- 安装软件列表
- 漏洞编号/名称
- 资产进程
- 应用组件

2、资产组

3、资产类型

4、资产标签

5、等保级别

6、有告警

7、不合规配置

8、资产价值

[提示]

点击对应的具体条件即可检索资产。

5.3.2 资产列表

在资产检索页面，页面右侧表格为资产列表、表格上方为资产操作功能按钮，可以对资产进行导出、设置标签；点击资产名称可以查看资产详情。

5.3.3 导出资产

在资产列表页面，点击【导出资产】按钮，可导出当前检索出来的所有资产，导出文件格式为 EXCEL 文件。

5.3.4 设置标签

在资产表格页面，选中要设置标签的资产，点击【设置标签】按钮，即可打开选择标签模态框，选择标签点击【确定】按钮后即可为选中资产设置标签。

5.3.5 资产详情

在资产表格页面，点击资产列表中资产名称，即可打开资产详情面板。资产详情包括资产基本信息、攻击入侵、告警、登录事件和配置变更。

5.4 预备资产

预备资产以表格展示，可对预备资产进行查询、删除和转为正式资产等操作。

5.4.1 查询

查询条件支持时间范围、资产类型、名称、IP。

5.4.2 邮件预备资产

点击预备资产列表中【删除】按钮，确认即可以删除预备资产。或者选中要删除的预备资产点击列表上的【删除】按钮可删除选中的预备资产。

5.4.3 转为正式资产

点击列表中的【+】按钮，即可打开转正式资产面板

1、填写资产基本属性

- 所属资产组
- 名称
- 类型
- 管理 IP
- MAC 地址
- 序列号
- 生产厂商
- 地理位置
- 设备联系人
- 描述

2、添加资产标签

- 选择已存在标签或添加新标签

3、选择安全属性

- 机密性
- 资产价值
- 可用性
- 等保定级
- 完整性

4、填写资产接口信息，可填写多个接口

- IP
- MAC

点击【转正式】按钮即可转为正式资产。

5.5 资产配置

资产配置主要包括资产标签维护和资产导入这两个功能。

5.5.1 资产标签

资产标签是资产分类的另一个维度，资产标签相当于自定义分类，可以给同一个资产添加一个或多个标签，同一个资产可以有多个标签，不同的资产可以有相同的标签。资产标签组是把类似的资产标签放在一起方便管理。

5.5.1.1 新增资产标签组

资产标签组的添加可点击【新增】按钮，即可打开新增资产标签组面板。添加资产标签组步骤如下：

1、填写资产标签组信息

- 资产标签组名称

2、添加标签[可选]

- 资产标签名称
- 资产标签颜色

点击【确定】按钮，保存资产标签组，并且将新添加的标签保存到标签组。

5.5.1.2 修改资产标签组

在资产标签组页面，点击资产标签组列表的名称，即可打开资产标签组编辑面板，编辑资产标签组的名称和资产标签信息，点击【确定】修改资产标签组。

> [提示]
>
> 资产标签组不能修改默认组。

5.5.1.3 删除资产标签组

在资产标签组页面，点击资产标签组列表中的【删除】按钮，即可打开删除确认框， 点击【确认】按钮删除资产标签组。或者选中要删除的资产标签组点击【删除】按钮，即可打开删除资产标签组确认模态框，点击【删除】删除选中的资产标签组。

[提示]

资产标签组不能删除默认组。

5.5.1.4 新增资产标签

在资产标签组页面，点击资产标签组列表中【新增】按钮，可打开新增资产标签面板，添加该组下的标签。

添加资产标签步骤如下：

1、填写资产标签信息

- 名称
- 颜色

点击【确定】按钮，保存资产标签，并且将标签加入到资产标签组。

5.5.1.5 删除资产标签

在资产标签组页面，点击资产标签组列表中标签上的【X】删除按钮，即可删除该资产标签。

5.5.2 资产导入

资产导入可将新的资产批量添加到数据库中，还可以用来恢复以前导出的资产。资产导入步骤如下：

1、下载资产导入模板

2、填写资产信息

- 资产名称
- 资产 IP[可选]
- 资产 MAC[可选]
- 资产类型
- 资产厂商
- 资产设备形态
- 资产机密性
- 资产完整性
- 资产可用性
- 资产价值
- 资产等保定级

3、选择要导入的资产组

4、选择填写好的资产文档

点击【导入】按钮，将文档中资产信息保存到系统中，并在页面显示刚导入的资产列表。

[提示]

导入资产文件必须为 Excel，资产模板文件中红色为必填项。

点击【+】添加按钮可导入多个资产文件

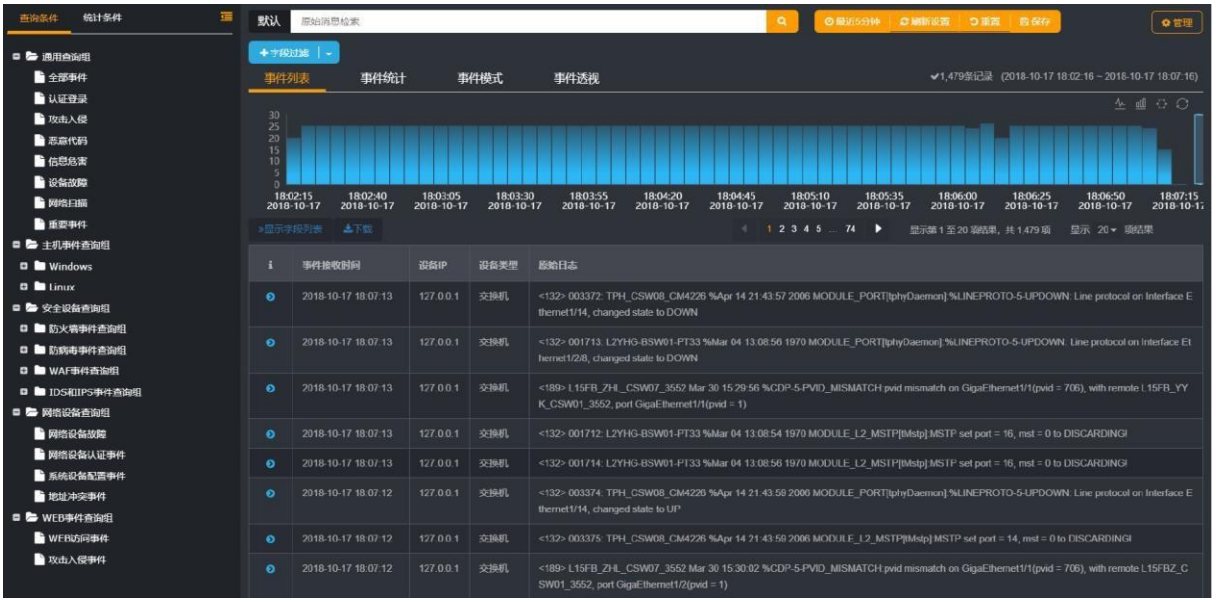
5.5.3 来源设置

通过点击【启/停】按钮控制预备资产的来源。

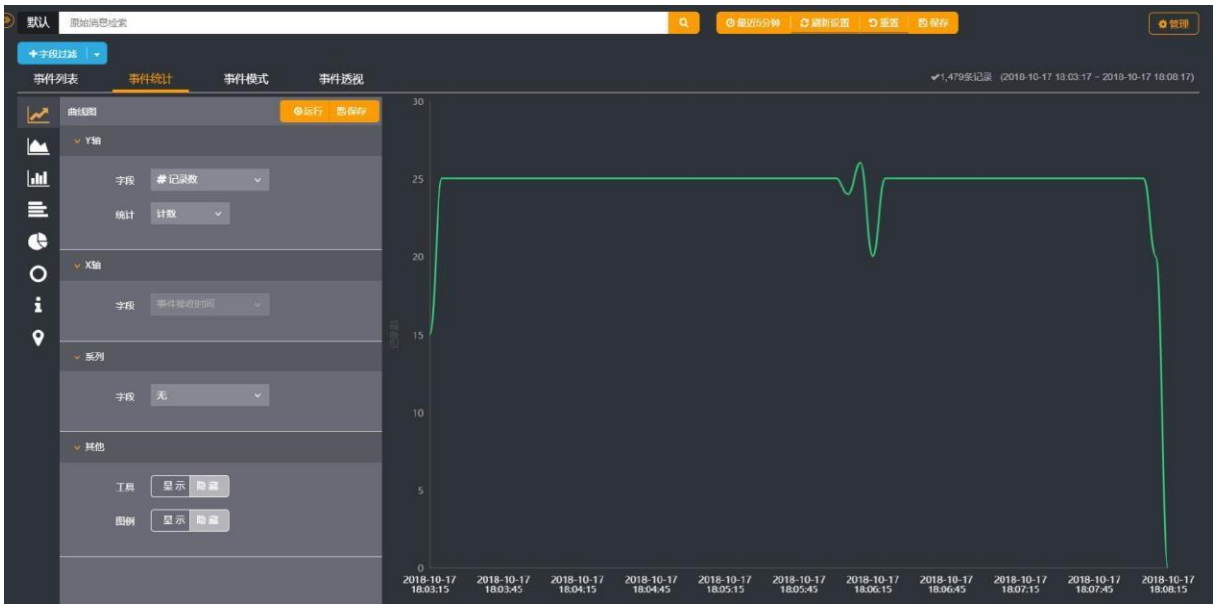
6. 事件分析

6.1 概览

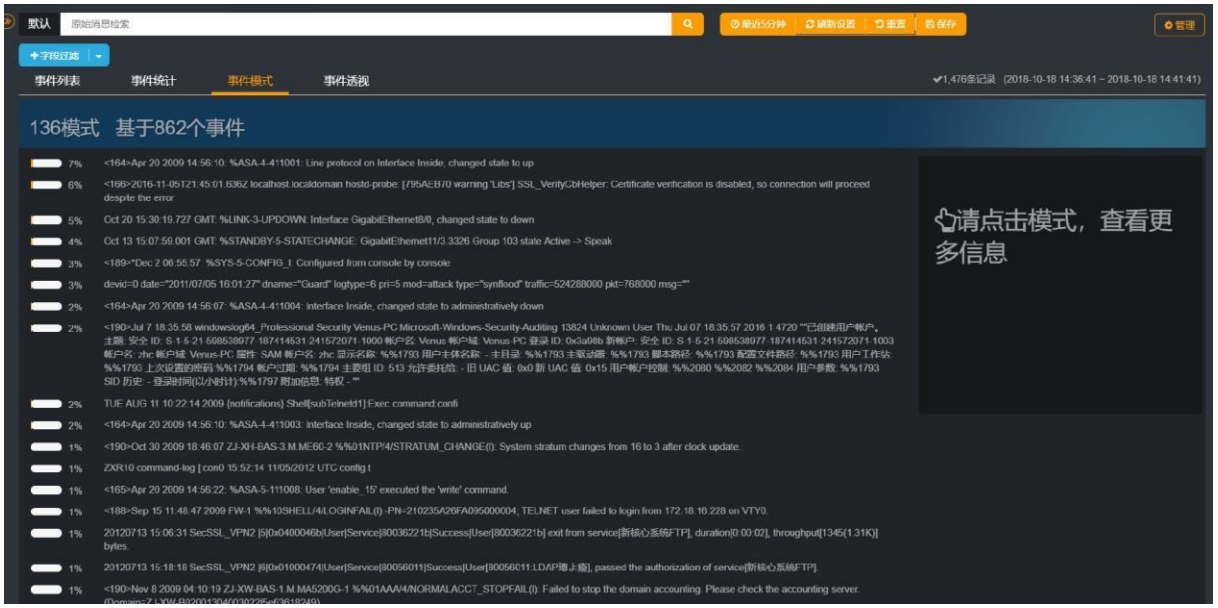
事件分析模块的主要功能是对日志信息进行快速搜索、内容查看、事件统计和模式匹配等功能。点击菜单上的【事件分析】菜单，将会显示事件分析主体页面。该页面显示的是事件分析模块的初始页面，主要包括：搜索条件控制区和搜索结果展示区。如下图所示。



点击【事件统计】会切换到事件统计页面，在事件统计中可通过操作统计图配置面板设置统计属性来进行统计分析。如下图所示。



点击【事件模式】会切换到事件模式页面，事件统计模式主要对当前检索的事件进行相似度比对、匹配等运算，将无规则的日志数据划分为不同的事件模式。如下图所示。



搜索条件控制区包括

- 条件名称
- 原始信息搜索框
- 查询按钮
- 时间范围菜单
- 刷新时间设置菜单
- 条件初始化菜单
- 条件打开菜单
- 条件保存菜单
- 条件管理菜单
- 过滤条件编辑组件

搜索结果展示区包括

- 事件量
- 搜索时间范围
- 事件量时间轴
- 事件列表
  - ➢ 事件字段列表
  - ➢ 事件信息列表
- 事件统计
  - ➢ 统计面板
  - ➢ 统计图
- 事件模式
  - ➢ 事件模式列表
  - ➢ 事件模式信息详情

6.2 设置搜索条件

6.2.1 按原始消息内容搜索

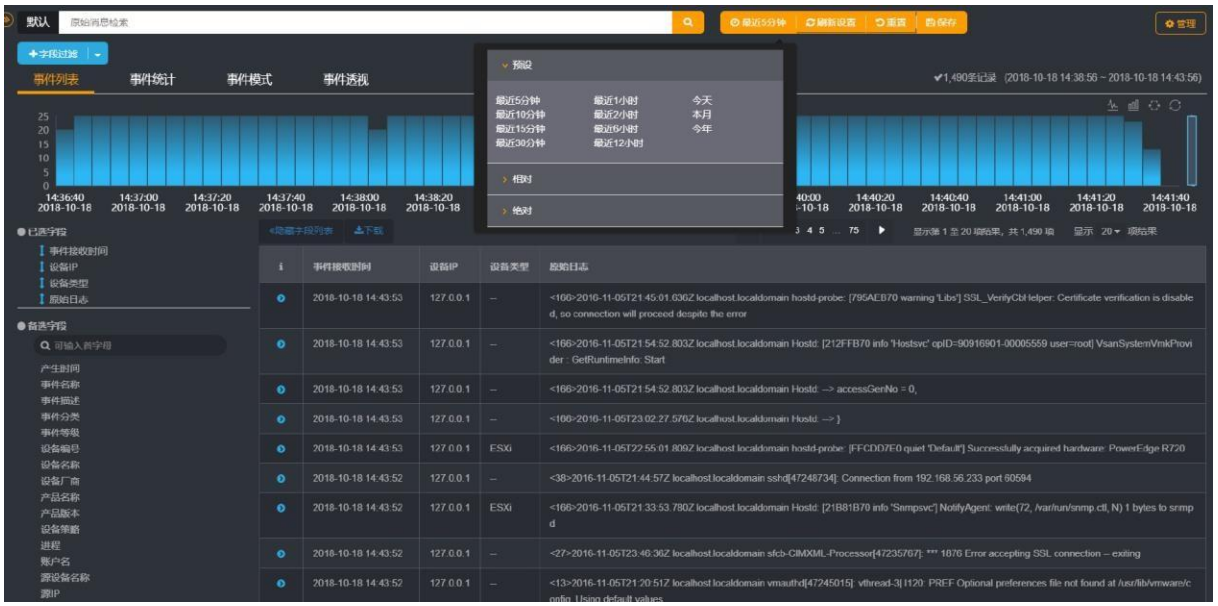
将要搜索的原始日志消息填入原始消息搜索框，敲击【Enter】键(或点击搜索框尾部【搜索】按钮)即可。

> [提示]
>
> 多个关键词按空格分开。

6.2.2 设置时间范围

第一次搜索时，系统会默认检索最近 5 分钟的数据，及搜索时间范围是“最近 5 分钟”。如果需要对搜索的时间范围进行调整。

点击时间范围菜单可以弹出时间范围选择面板。在次面板中可以选择预设的事件范围，可以设置相对时间范围，也可设置绝对时间范围。



6.2.3 设置自动刷新时间

第一次搜索时，系统默认不进行自动刷新，如果需要设置自动刷新菜单，然后选择自动刷新的时间间隔。

6.2.4 设置高级过滤条件

点击【+字段过滤】按钮后的三角在弹出的菜单中点击【高级过滤】按钮，在弹出的条件编辑面板中编辑复杂的过滤条件。

> [提示]
>
> 复杂过滤条件如何编辑请参考过滤器章节。

6.2.5 引用过滤器

点击【+字段过滤】按钮后的三角在弹出的菜单中点击【引用过滤器】按钮，在弹出的过滤器选择面板中选择要引用的过滤器。

6.3 条件的保存、应用、管理

6.3.1 保存为查询条件

点击页面右上方的【保存】按钮即可进入查询条件保存页面。如果当前应用的是已有查询条件则进入的是该查询条件的编辑页面。在编辑页面可以通过是否另存开关，控制另存为新条件还是更新当前条件。

条件信息

- 条件名称
- 条件分组
- 条件描述

6.3.2 保存为统计条件

打开事件统计页面，点击统计面板右上方的【保存】按钮即可进入统计条件保存页面。如果当前应用的是已有的统计条件则进入的是统计条件编辑页面。在编辑页面可以通过是否另存开关，控制另存为新条件还是更新当前条件。

条件信息

- 条件名称
- 条件分组
- 条件描述

6.3.3 打开已有的查询条件

打开左侧面板，点击查询条件名称即可。

6.3.4 打开已有的统计条件

打开左侧面板，切换标签页到统计条件，点击统计条件名称即可。

6.3.5 管理条件组和条件

点击页面右上方的【管理】按钮，在打开的管理页面中可以对条件组进行新增、修改、删除等操作，可以对已保存的条件进行编辑名称、编辑描述、删除条件等操作。

6.4 时间轴

时间轴右上角显示的是当前的事件量、查询时间范围和时间轴的操作按钮。操作按钮依次为

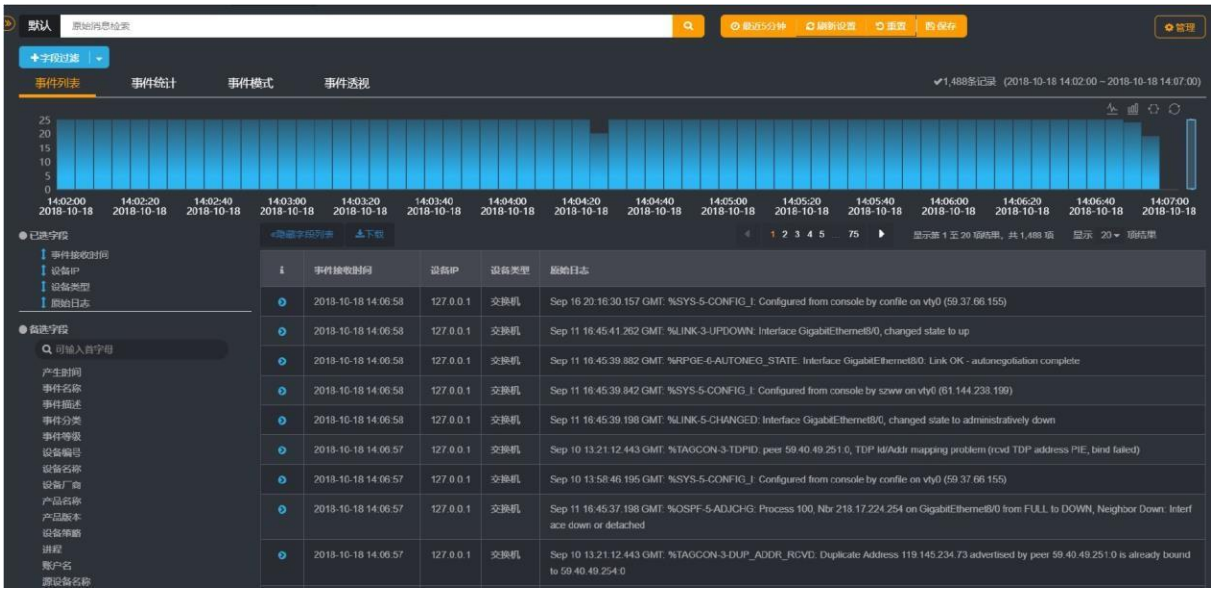
- 切换为折线图按钮
- 切换为柱状图按钮
- 框选按钮
- 返回上一次状态按钮（只有钻取后才显示）
- 刷新按钮

时间轴的操作

点击某个柱子可以将时间范围条件设置为此柱子对应的时间范围，再次点击可取消柱子的选中状态。

点击框选按钮可激活时间轴的框选状态，然后用鼠标框选已选区域查看该区域的事件情况。鼠标悬浮到框选区域按住鼠标左键可以通过左右拖动来改变所选区域。鼠标双击所选区域可以钻取到该时间范围，从而进行进一步的分析。

6.5 事件列表



6.5.1 字段列表

字段列表展示的是所有的事件字段。

6.5.1.1 已选字段

已选字段与事件表中的字段是对应的。

1、如何调整事件表中字段的顺序?

鼠标悬浮到已选字段左端的【✥】按钮，然后按住左键拖动字段，移动到目标位置后松开左键即可完成字段顺序调整。

2、如何从将某字段从已选字段中移除?

鼠标悬浮到目标字段上，点击右端的【】按钮即可完成移除操作

6.5.1.2 备选字段

1、如何将备选字段添加到已选字段中?

鼠标悬浮到目标字段上，点击右端的【】按钮即可完成添加操作。

6.5.1.3 字段微观分析

点击某个字段触发字段微观分析，分析完毕后会显示微观分析页面，在微观分析页面中显示了该字段的分类 Top10。

如果想将微观分析的结果添加到字段过滤条件中则可以点击末端的【】按钮，即可将该字段值添加到字段过滤条件中。

[提示]

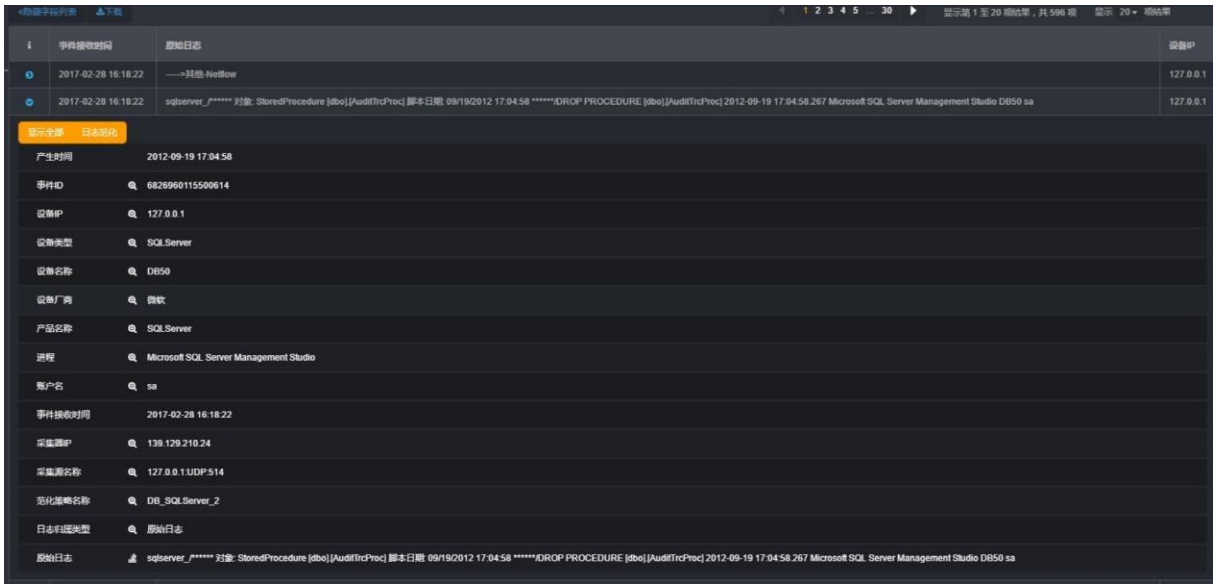
时间类型字段和原始消息不支持微观分析。

6.5.2 事件列表

事件列表中展示了事件的的字段信息。

6.5.2.1 查看事件详情

点击目标事件左端的【】按钮即可打开事件详情页面。



默认只显示有值的字段，如果想要查看全部字段可以点击【显示全部】按钮查看所有字段。

1、如何查看目标日志的范化信息?

点击【日志范化】按钮即可显示日志范化页面。如果该事件已经未匹配任何的范化策略，则显示的是新增范化策略页面。如果该事件已经匹配到了范化策略，则显示的是

范化策略编辑页面。

[提示]

复杂过滤条件如何编辑请参考范化策略。

2、如何将字段值添加到字段过滤条件中?

点击目标字段对应的【🔍】即可将目标字段值添加到字段过滤条件中。

[提示]

时间类型字段不支持添加到搜索条件操作。

原始日志字段只支持查看日志范化操作。

6.5.2.2 下载当前事件

1、点击事件表格上方的【下载】按钮，即可弹出下载字段选择窗口。

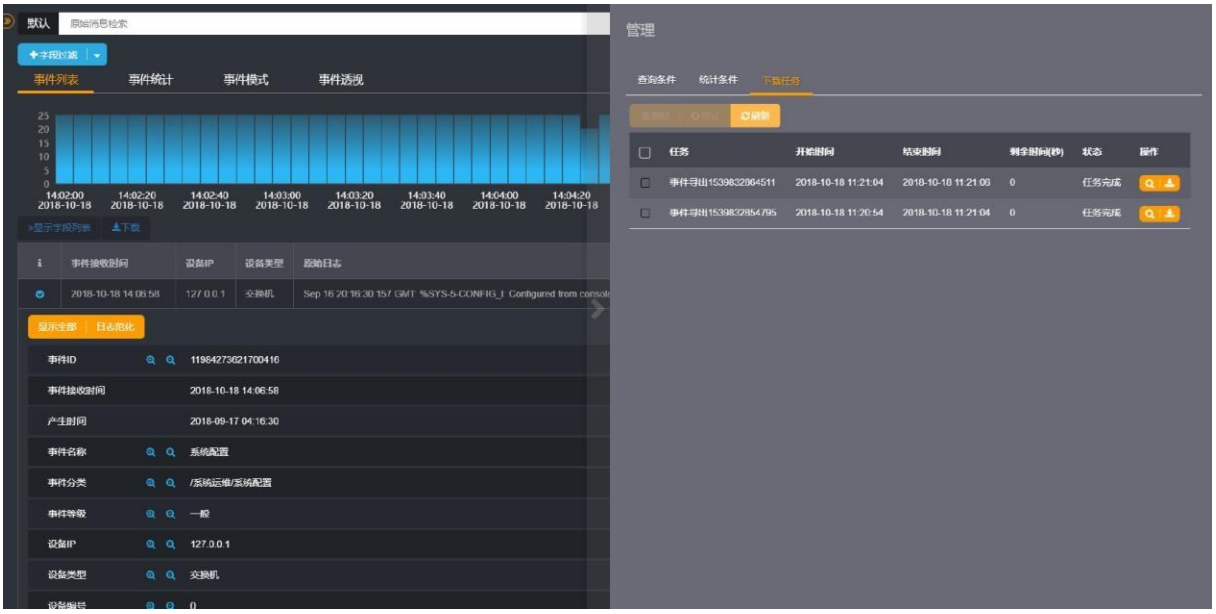
2、选择要下载的事件字段。

3、点击【确定】按钮即可执行下载操作。

[提示]

如果下载的事件量不大，则直接将文件下载到本地。

如果下载得事件量太大，则会创建下载任务，需点击页面右上方的【管理】中查看下载任务。



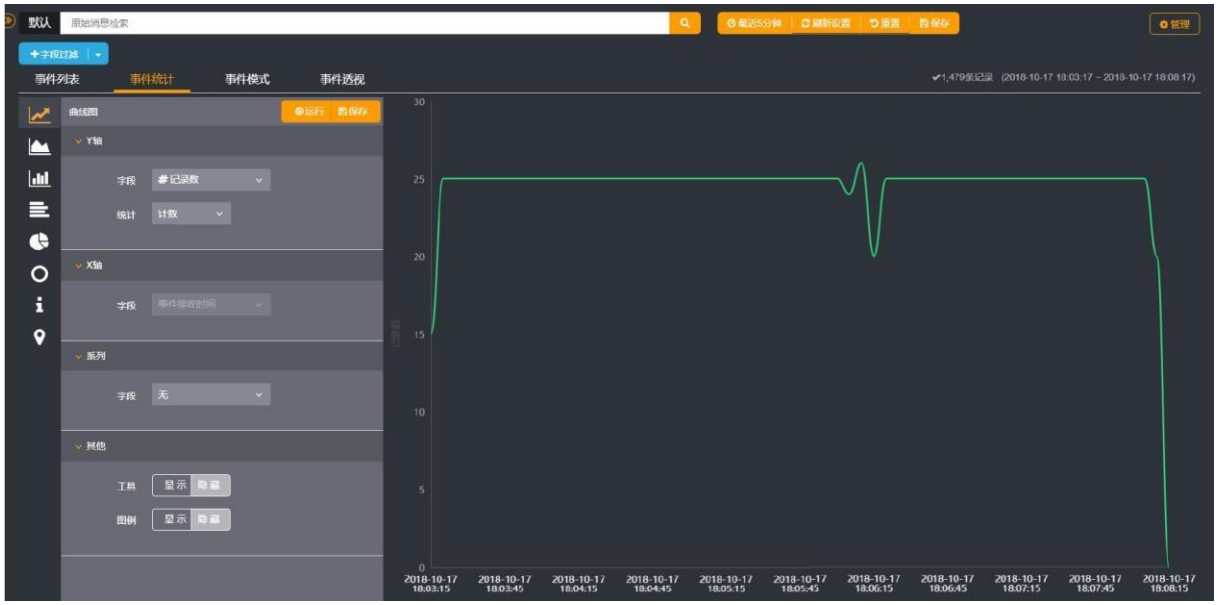
6.6 事件统计

进入事件分析模块后，点击【事件统计】标签页即可进入事件统计页面

6.6.1 创建统计图

1、点击左侧统计图类型图标，选择需要的统计图类型。

2、在操作面板中设置统计信息



统计面板包括：

- 统计图类型
- 【运行】按钮
- 【保存】按钮
- Y 轴配置菜单（曲线图、面积图、柱状图特有）
- X 轴配置菜单（曲线图、面积图、柱状图特有）
- 系列配置菜单（曲线图、面积图、柱状图特有）
- 统计值（饼状图、环状图特有）

- 分组项（饼状图、环状图特有）
- 其他配置菜单（是否显示图表工具，是否显示图例等）

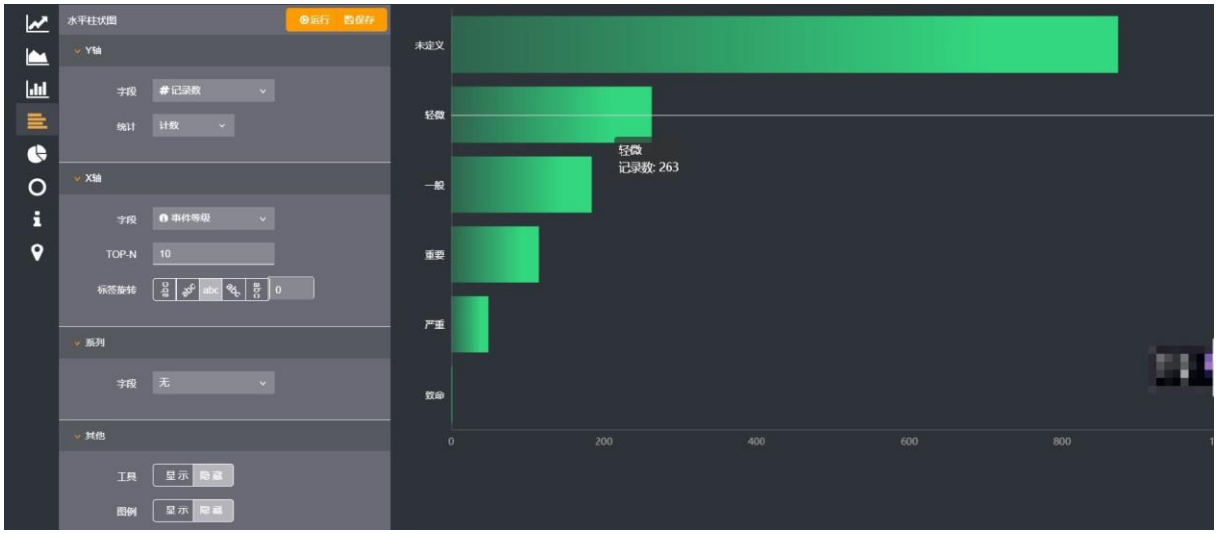
3、点击【运行】按钮即可生成统计图

4、样例：按照事件分类字段统计事件量 Top10 柱状图

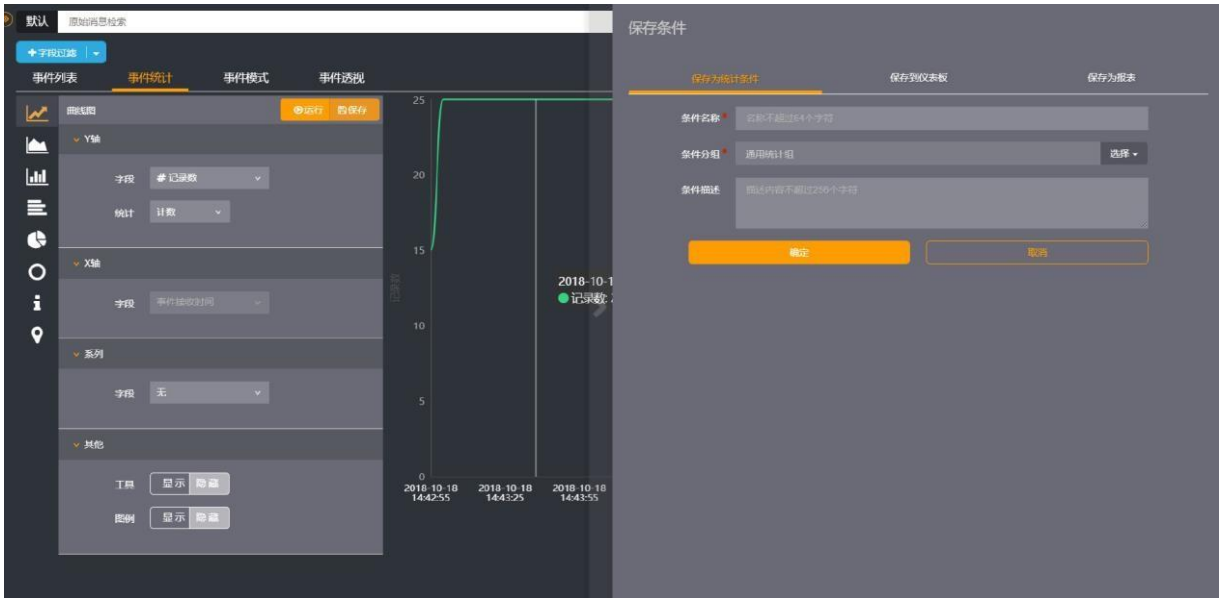
a.点击柱状图图标切换到柱状图编辑面板

b.设置X 轴的字段为 “事件分类”

c.设置X 轴 TOP-N 为10



将统计图保存为统计条件



1、 配置好统计图后，点击统计面板右上方的【保存】按钮，在弹出的条件保存页面中点击【保存为统计条件】标签页即可进入事件统计条件保存页面。

2、 填写表单信息后，点击【确定】按钮完成事件统计条件的保存操作。

- 输入条件名称

- 选择条件分组
- 输入条件描述

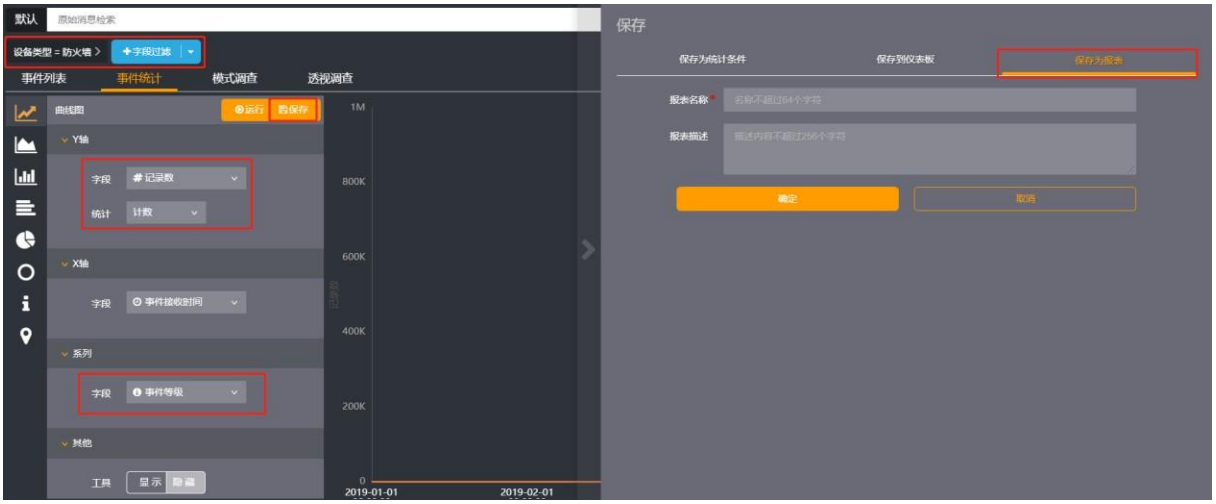
6.6.2 将统计图保存到仪表板

1、配置好统计图后，点击统计面板右上方的【保存】按钮，在弹出的条件保存页面中点击【保存到仪表板】标签页即可进入保存到仪表板页面。

2、填写表单信息后，点击【确定】按钮即可将统计图保存到仪表板中。

- 选择目标仪表板
- 输入面板名称
- 输入面板描述
- 设置面板背景

6.6.3 将统计图保存为报表



1、进入事件分析模块，选择条件进行事件统计

- 选择过滤字段[可选]
- 选择图表类型
- 选择图表参数

2、点击保存按钮，填写报表基本信息

- 选择保存为报表
- 报表名称
- 报表描述

6.7 模式调查

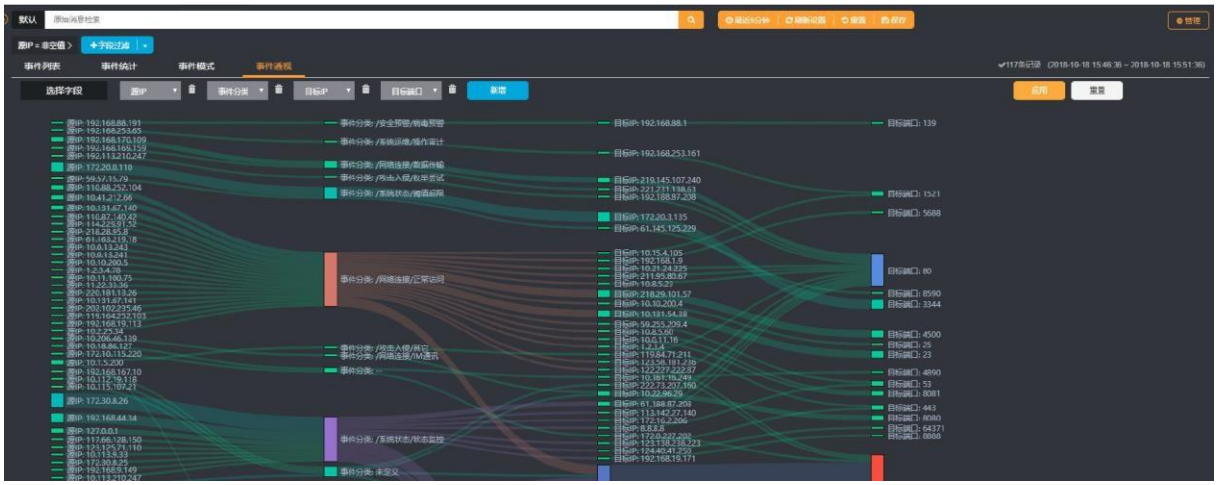
为了将大量的事件进行分类，以便于对大量的事件进行分析、整理，事件模式会对当前条件下的事件按照原始日志信息进行匹配整合。经过一系列的运算、比较后，将繁杂的事件进行分类，最终以模式的形式展现出来。

在模式列表中点击某个模式后，在右侧会显示出该模式的相关信息。

点击右下角【🔍】按钮可将当前模式的日志内容作为搜索条件添加到字段过滤条件中。

6.8 事件透视

为了将大量的事件进行分类，以便于对大量的事件进行分析、整理，事件模式会对当前条件下的事件按照原始日志信息进行匹配整合。 经过一系列的运算、比较后，将繁杂的事件进行分类，最终以模式的形式展现出来。



7. 智能分析

7.1关联规则

关联规则配置了如何对接收的事件进行关联分析和处理，以检测可能的攻击和威胁。如果事件触发了设定的关联规则，系统将生成告警，并执行相应的告警动作。

7.2 关联规则组

过滤器采用树型分组结构进行管理。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

7.3 关联规则

关联规则是对事件进行关联分析和处理的配置，其属性包括规则名称、规则描述、关联条件、计数条件、告警配置、告警动作配置等。

一个关联规则的示例如下：

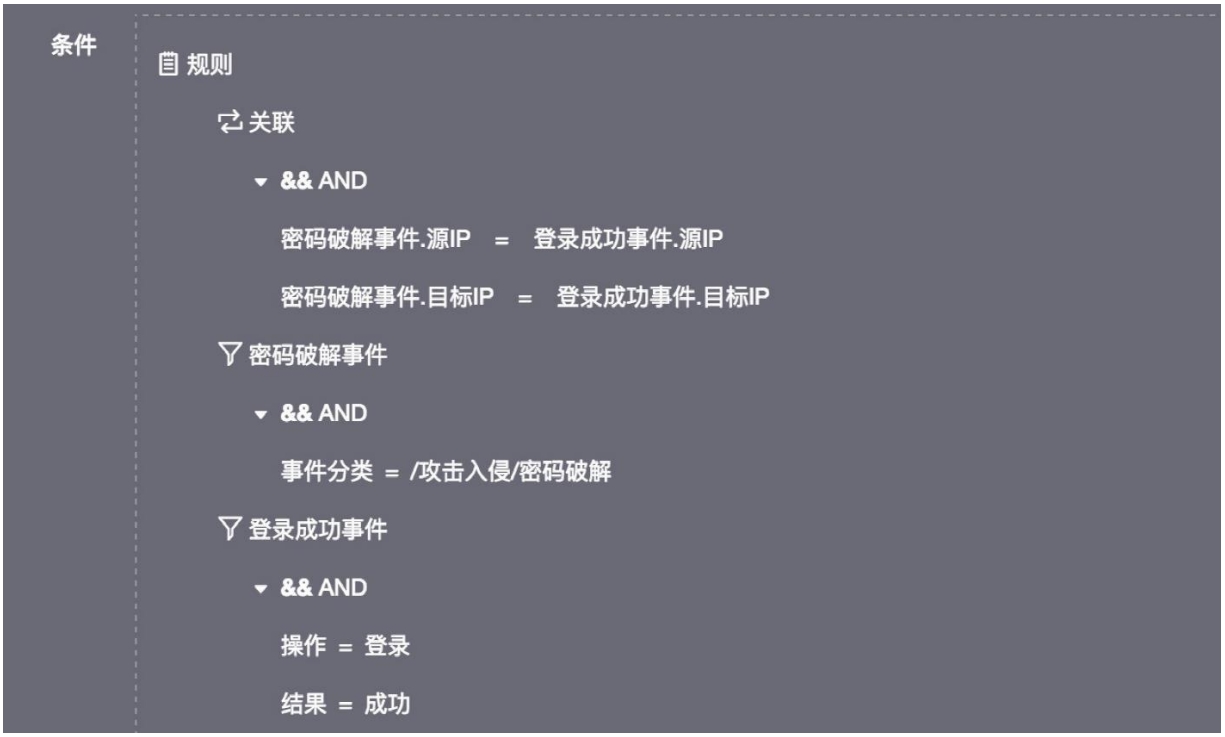
7.4 规则条件

简单的规则条件配置与过滤器配置相同。支持简单的事件字段条件，也支持复杂的与或非逻辑条件。

关联规则还可以支持多事件关联。

7.5 多事件关联

多事件关联可以设置不同类型事件的关联条件，如事件 A 的目标 IP 与事件 B 的源 IP相同。示例如下：



鼠标移动到规则上方时，显示【+】添加事件按钮，可以添加多个事件

鼠标移动到关联上方时，显示【+】添加关联条件按钮，可以添加事件关联条件，事件关联条件也支持与、或、非逻辑运算。

7.6 计数条件

计数条件对事件发生次数进行设置：

- 设置在指定时间范围内事件发生次数达到设定值时触发规则
- 设置在指定的时间范围内不重复触发规则

7.7 关联事件重定义

重新设置内部关联事件的属性值，可以引用事件属性。

关联事件是关联规则匹配成功后，由关联引擎产生的事件，为内部事件。

7.8 告警重定义

重新设置告警事件的属性值，可以引用事件属性。

7.9 告警动作

告警生成后，可以执行一系列的告警动作，并可设置触发告警动作时间间隔。

- 发送邮件
  邮件发送告警内容。
  需要设置邮箱服务器，参看【系统>常用设置>邮箱配置】
- 执行命令行
  执行服务器本地命令，支持引用事件属性。
- 设备协同
  在远程设备上远程执行命令，支持使用 SSH 协议和Telnet 协议。
- 发送**syslog**
  向目标设备发送 syslog 消息。
- 发送**snmptrap**
- 向目标设备发送 snmptrap 消息

7.10 引用事件属性

在关联事件和告警重定义、设置告警动作时，可以在文本中引用事件属性，引用的格式为"#{属性名}"。

例如在邮件的主题中输入："#{lrecepttime};#{cdevip};告警等级:#{ieventlevel}",用户收到的告警邮件主题形式如："2011-08-01 星期一 12:00:00;12.50.10.1:告警等级:警告"。

引用事件属性的情况包括：

- 关联事件重定义
- 告警重定义
- 发送邮件：主题、内容
- 发送 SNMPTrap：内容
- 执行命令

8. 告警

告警模块展示系统产生的各种告警事件，支持告警数据统计和告警追踪分析。

8.1 告警来源

产生告警事件的来源包括：

- 事件关联分析（系统接收的事件触发了关联规则）
- 系统自身监控（系统运行指标达到告警阈值）

8.2 告警属性

告警基本属性包括告警发生时间、名称、详情、来源、严重程度、状态、告警设备IP、告警设备类型等。

- 告警状态包括未确认、待处理、处理中、已关闭四种状态，可以根据告警的处理情况手动修改。
- 告警严重程度分为高、中、低三级。

8.3 告警合并

为了避免短时间内产生大量重复告警，可以设置对一个时间范围内某些属性重复的告警进行合并。

例如，1 小时内产生的告警名称和设备地址均相同的告警合并为 1 条告警。

8.4 告警数据保存周期

为了防止告警数据占用过多存储空间，可以设置告警最长保存时间和最大保存条数。在[系统>常用配置>告警数据维护]中进行设置。

默认的配置为：

- 最长保存时间 90 天
- 最大保存条数 1000000 条

9. 报表

报表用于将事件按照一定的统计方式展示给用户，它提供了广泛的报表选项，包括众多报表参数和图表类型。报表目前支持的格式为PDF/HTML/PNG/DOCX/RTF/XLSX/XLS。

9.1 说明

创建报表需使用数据源，创建智能报告则需要使用报表，故需要创建报表或智能报告需安照【数据源->报表->智能报告】的先后顺序创建。

9.2 数据源

数据源是按照一定的时间间隔、指定的统计条件（分组、汇总）和过滤条件等，持续不断地对原始数据表进行汇总统计，并保存统计结果。数据源可为报表提供数据，并支持对过滤。

9.2.1 统计条件

统计条件首先是报表针对中间表统计时分组的依据，同时也是最终报表展现时列表中的统计项以外的字段，列表中除统计项字段外，只有统计条件字段。

9.2.2 统计项

统计项是指最终用来计算的字段。计算的方式包括求和、平均、计数、最大和最小值等。

9.2.3 导入

通过导入数据源文件创建数据源，避免创建过多数据源生成中间表影响系统性能。进入【报表->数据源】界面，添加数据源如下图：

导入数据源步骤如下：

1、 生成数据源文件，可使用数据源生成工具生成数据源

```
<cn.cybertron.brick.report.entity.ReportCache>
<id>0</id>
<uuid>eventcount</uuid>
<model>数据源类型（event）</model>
<title>数据源名称</title>
<description>数据源描述</description>
<type>cache</type>
<statiitems>
  <cn.cybertron.brick.report.data.cache.ZReportItem>
    <aggregate>count</aggregate>
    <index>false</index>
    <field>
      <name>lid</name>
      <dataType>LONG</dataType>
      <alias>事件ID</alias>
      <model>event</model>
      <dictId></dictId>
      <oprType>0</oprType>
      <length>20</length>
      <sequence>51</sequence>
    </field>
  </cn.cybertron.brick.report.data.cache.ZReportItem>
</statiitems>
<groupitems>
  <cn.cybertron.brick.report.data.cache.ZReportItem>
    <index>false</index>
    <field>
      <name>cdevip</name>
      <dataType>IP</dataType>
      <alias>设备IP</alias>
      <model>event</model>
      <dictId></dictId>
      <oprType>0</oprType>
      <length>255</length>
```

```
        <sequence>7</sequence>
      </field>
    </cn.cybertron.brick.report.data.cache.ZReportItem>
  </groupitems>
  <expression></expression>
  <intervalTime>15</intervalTime>
  <storageTime>90</storageTime>
  <system>true</system>
```

- model 数据类型，事件数据或流量数据等
- title 数据源名称
- description 数据源描述
- type 数据源类型，source：可供终端用户使用的中间表，cache：只限其他中间表使用的中间表
- state items 统计字段，不可为空
- group items 分组字段，不可为空
- expression 统计条件
- interval Time 数据源统计时间间隔，单位：分钟
- storage Time 数据源中数据保存时间范围，单位：天

2、 点击上传按钮，导入数据源

- 导出成功后系统自动创建中间表，系统内置数据源将生产三张中间表
- 中间表默认初始化 1 小时数据

[提示]

数据源只支持导入，避免创建过多数据源影响系统性能。

9.2.4 导出

在数据源查看页面选中数据源，点击【导出】按钮可导出数据源文件。

9.2.5 是否启用数据源

数据源支持启用和停用，启用时系统定时统计数据保存至数据源对应中间表，停用时数据源将不进行定时统计并且不可用来创建报表。

9.2.6 修改

数据源可修改标题、描述、数据存放时间、统计时间间隔和过滤条件，修改数据源如下图：

数据源还可以清空中间表和检查中间表是否损坏，并对损坏的中间表进行修复。

[提示]

数据源不可修改统计字段和分组字段，数据源对应中间表创建后表结构不可修改

9.2.7 删除

在数据源查看页面，点击列表中【删除】按钮，确认即可以删除数据源，删除数据源时将删除数据源对应中间表。

[提示]

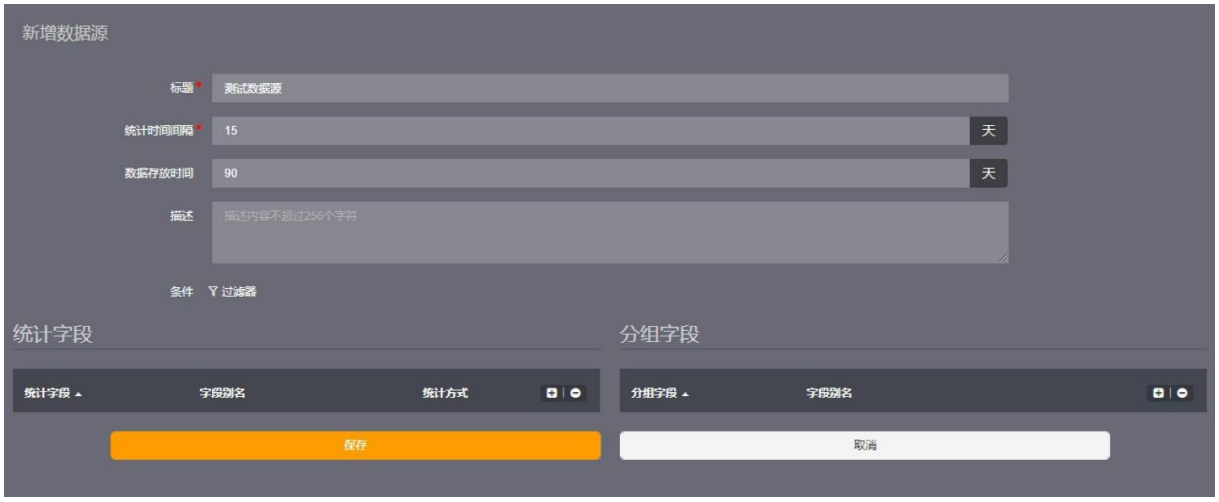
报表创建依赖数据源，删除数据源将导致对应报表不可用，请谨慎操作！！

9.2.8 数据源生成工具

数据源生成工具可在页面配置生成数据源文件，并将生成的数据源文件保存为可导入的xml 文件。

1、下载数据源生成工具，并将下载工具上传至服务器 cbt/server/webapps/[laa]目录。

2、登录系统,访问 http://ip:port/[laa]/cache.jsp，点击添加按钮，页面如下图所示：



1、填写资产基本属性

- 数据源名称
- 数据源统计时间间隔，单位：分钟
- 数据源中数据保存时间范围，单位：天
- 数据源描述

2、配置统计条件

- 统计条件

3、选择统计字段和分组字段

- 统计字段，不可为空
- 分组字段，不可为空

4、点击【保存】按钮生成数据源文件，使用 SCP 工具登录服务器 cbt/server/temp 目录找到最新生成 report_cache_xxxx.xml 下载到本地

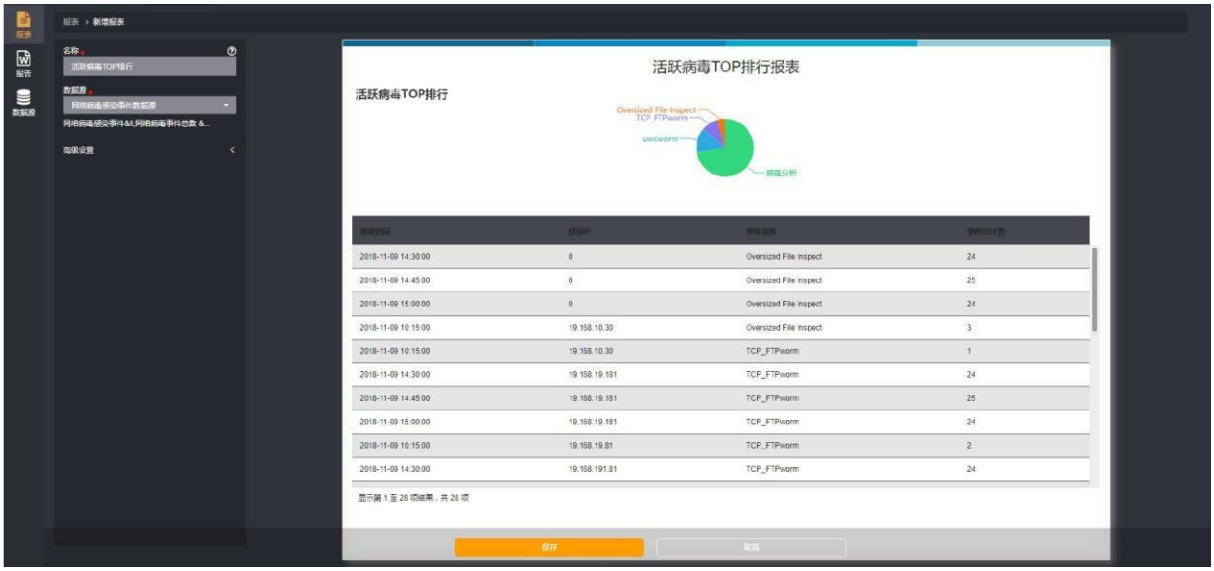
5、可修改数据源文件，将数据源文件压缩后可导入系统中

9.3 报表

报表用于将事件按照一定的统计方式展示给用户，它提供了广泛的报表选项，包括众多报表参数和图表类型。报表目前支持的格式为PDF/HTML/PNG/DOCX/RTF/XLSX/XLS。

9.3.1 添加

进入报表界面，选择唯一报表组，在此报表组下创建报表。报表创建如下图：



创建报表步骤如下：

1、输入报表名称

2、选择数据源

- 选择报表使用数据源，可不选择数据源创建空报表

3、高级设置

- 设置导出文件页眉页脚[可选] 4、输入报表标题

5、添加报表组件

- 添加小标题
- 添加文本，文本支持${id_count}占位符添加统计值。
- 添加统计图，图形支持折线图、面积图、柱图、饼图、堆积面积图、堆积柱图、水平柱图、水平堆积柱图，统计图支持过滤条件。添加统计图如下图：

- 添加数据列表，可选择显示字段和显示记录条数

6、点击【保存】按钮即可保存报表。

9.3.2 修改

在报表查看页面，点击列表中【编辑】按钮，即可以进入报表编辑页面，对报表进行修改，修改报表操作同上。

> [提示]
>
> 报表只能修改名称和描述信息。

9.3.3 删除

在报表查看页面，点击列表中【删除】按钮，确认即可以删除报表。或者选中要删除的报表点击【删除】按钮可删除选中的报表。

9.3.4 预览

用户可自定义时间预览报表，并可下载指定格式报表。步骤如下：

1、预览

- 点击列表中【预览】按钮
- 选择时间范围
- 点击确定预览

2、下载

- 选择选择报表格式下载报表

9.3.5 调度

报表调度用于定时将报表按照用户自定义的时间范围和文件格式生成报表，并可以下载生成的报表或者发送到用户邮箱。

9.3.6 查看调度

在报表查看页面，点击列表中【调度】按钮，即可以查看报表的调度信息，报表调度页面如下图：

9.3.7 添加调度

在报表调度页面，点击【新增】按钮进入添加调度页面，添加报表调度步骤如下：

1、选择策略

- 执行一次需选择时间范围

2、选择生成报表格式和生成报表时间

3、发送附件，填写发送邮件信息

- 接收人，多个用‘，’隔开
- 邮件主题
- 邮件正文

[提示]

报表调度执行一次绝对时间范围为报表创建时间至当前时间。

9.3.8 删除调度

在报表调度页面，点击列表中【删除】按钮，确认即可以删除报表。或者选中要删除的调度，点击表格上删除按钮删除选中调度信息。

9.3.9 下载报表

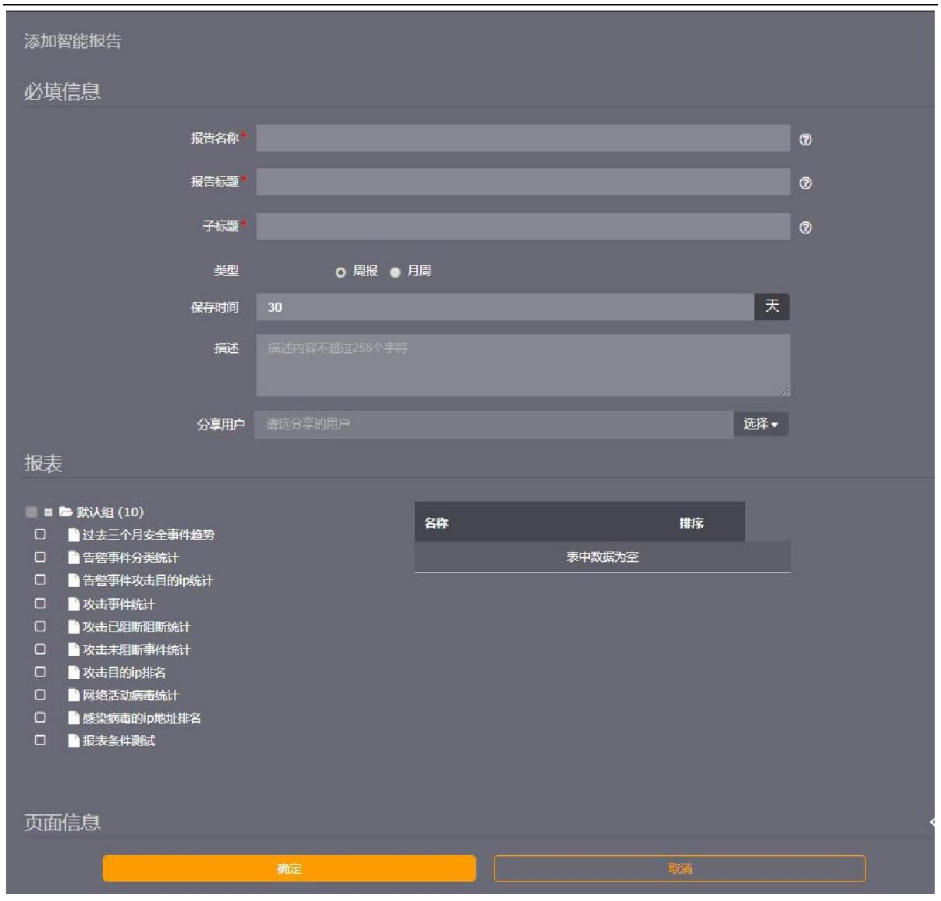
在报表调度页面，点击列表中【下载】按钮，选择下载条件可下载调度生成的报表。

[提示]

报表调度生成报表文件会定期删除，文件个数可能会少于预期。

9.4 报告

报告按照应用场景，以一定目录结构将多个报表的汇总，并以树目录方式显示的报告。报告支持文件格式为 PDF/HTML/DOCX。



9.4.1 添加

使用已创建报表生成智能报告。进入智能报告界面，添加智能报告如下图：

创建智能报告步骤如下：

1、点击【新增】按钮，填写报告基本信息

- 报告名称
- 报告标题
- 报告子标题
- 报告类型
- 报告保存时间
- 报告描述[可选]
- 分享用户[可选]

2、选择报表，并以一定目录结构对报表进行排序

3、设置报告页面信息

4、点击【确定】按钮保存报告

[提示]

创建智能报告中报表为同级目录

9.4.2 导入

在智能报告查看页面，点击【导入】按钮，可导入智能报告文件。导入智能报告步骤如下：

1、生成智能报告文件

```
<Reports>
<id>0</id>
<name>安全运维智能报告</name>
<title>安全运维智能报告</title>
<scheduletype>WEEKLY</scheduletype>
<created>1515723574629</created>
<modified>1517457761716</modified>
<creatorid>10</creatorid>
<filelifetime>30</filelifetime>
<page>
  <size>A4</size>
  <orientation>LANDSCAPE</orientation>
</page>
<description>安全运维智能报告</description>
```

```
<summary>
  <cn.cybertron.brick.report.entity.ReportSummary>
    <name>1 综述</name>
    <tag>h1</tag>
    <chkDisabled>true</chkDisabled>
    <checked>true</checked>
    <reportid>1</reportid>
  </cn.cybertron.brick.report.entity.ReportSummary>
  <cn.cybertron.brick.report.entity.ReportSummary>
    <name>2 告警事件统计</name>
    <tag>h1</tag>
    <chkDisabled>true</chkDisabled>
    <checked>true</checked>
    <children>
      <cn.cybertron.brick.report.entity.ReportSummary>
        <name>2.1 告警事件分类统计</name>
        <tag>h2</tag>
        <chkDisabled>true</chkDisabled>
        <checked>true</checked>
        <reportid>3</reportid>
      </cn.cybertron.brick.report.entity.ReportSummary>
    </children>
  </cn.cybertron.brick.report.entity.ReportSummary>
</summary>
<system>true</system>
<subreportids>1,3</subreportids>
</Reports>
```

- summary 目录
- children 子目录

2、 点击上传按钮，导入报告

[提示]

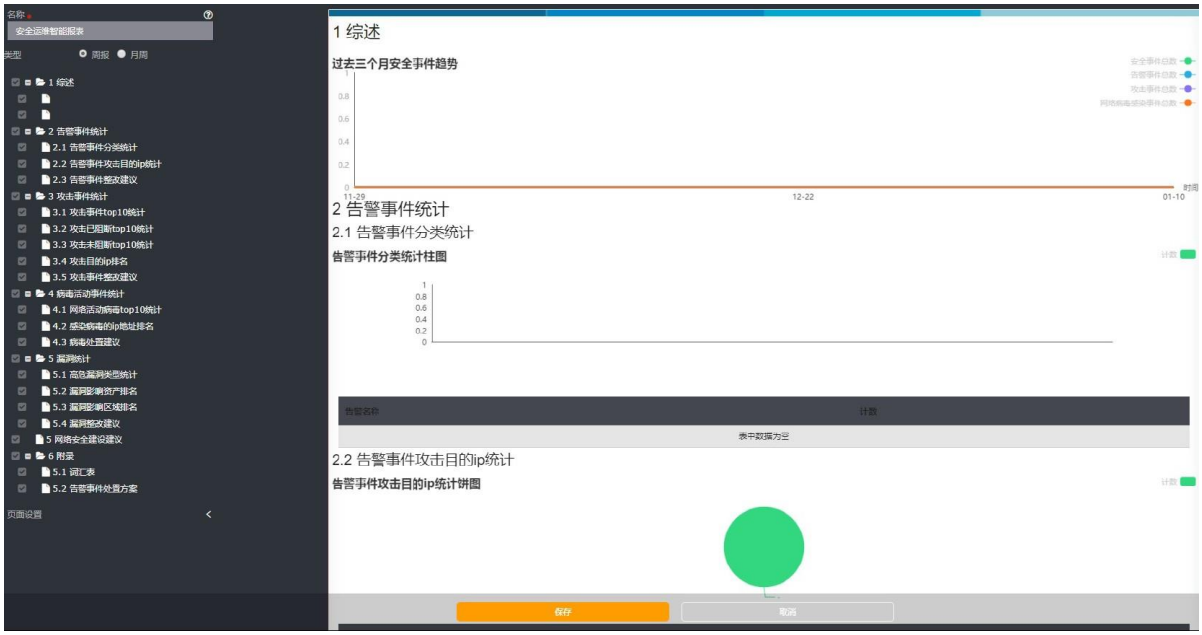
上传智能报告文件为 zip 包，可上传多个智能报告。

9.4.3 导出

在智能报告查看页面，点击【编辑】按钮可导出智能报告文件。

9.4.4 修改

在智能报告查看页面，点击列表中名称或【编辑】按钮，即可以进入智能报告编辑页面，对智能报告进行修改。修改智能报告如下图：



[提示]

报告中报表不可修改。

9.4.5 删除

在报表查看页面，点击列表中【删除】按钮，确认即可以删除报表。或者选中要删除的报表点【删除】按钮可删除选中的报表。

9.4.6 预览

用户可自定义时间预览报表，并可下载指定格式报表。步骤如下：

1、预览

- 点击列表中【预览】按钮
- 选择时间范围
- 点击确定预览

2、下载

- 选择选择报表格式下载报表

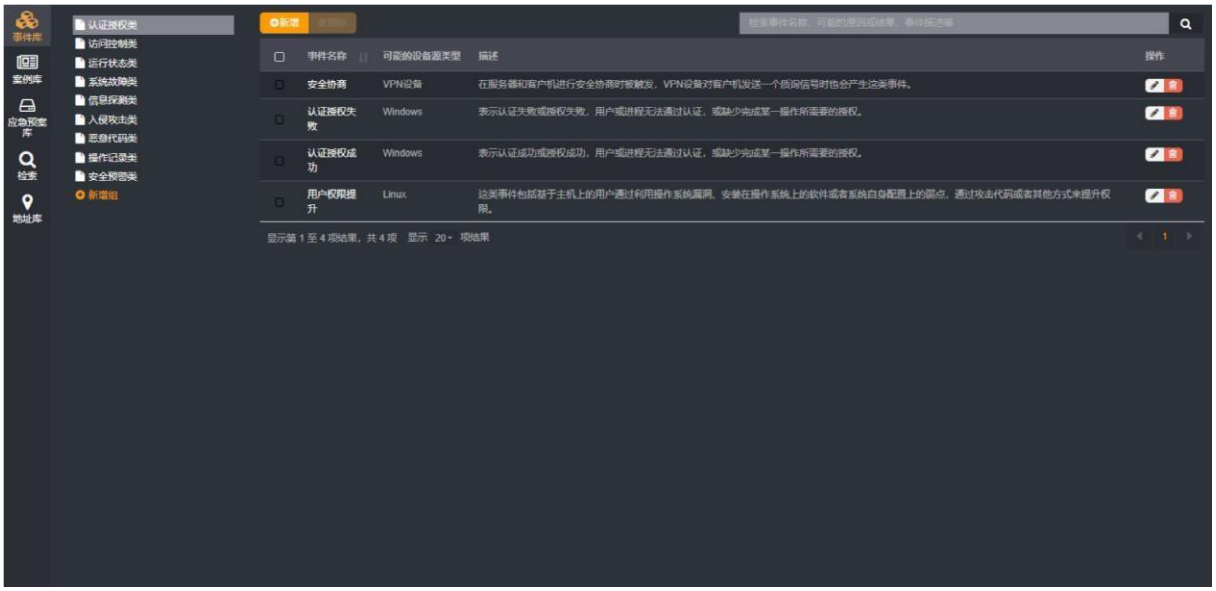
10. 知识库

知识库包含事件库、案例库、应急预案库、检索及地址库 5 个模块。事件库、案例库、应急预案库和地址库中存储器不同类型的知识数据，检索模块提供关键字全文检索知识库内容

- 事件库
- 案例库
- 应急预案库
- 检索
- 地址库

10.1 事件库

事件库是知识库的首页。事件库页面左侧展示事件库组树形图，右侧展示当前选中事件库组对应的所有事件的列表。如图：



10.1.1 事件库组

事件库是知识库的首页。事件库页面左侧展示事件库组树形图，右侧展示当前选中事件库组对应的所有事件的列表。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

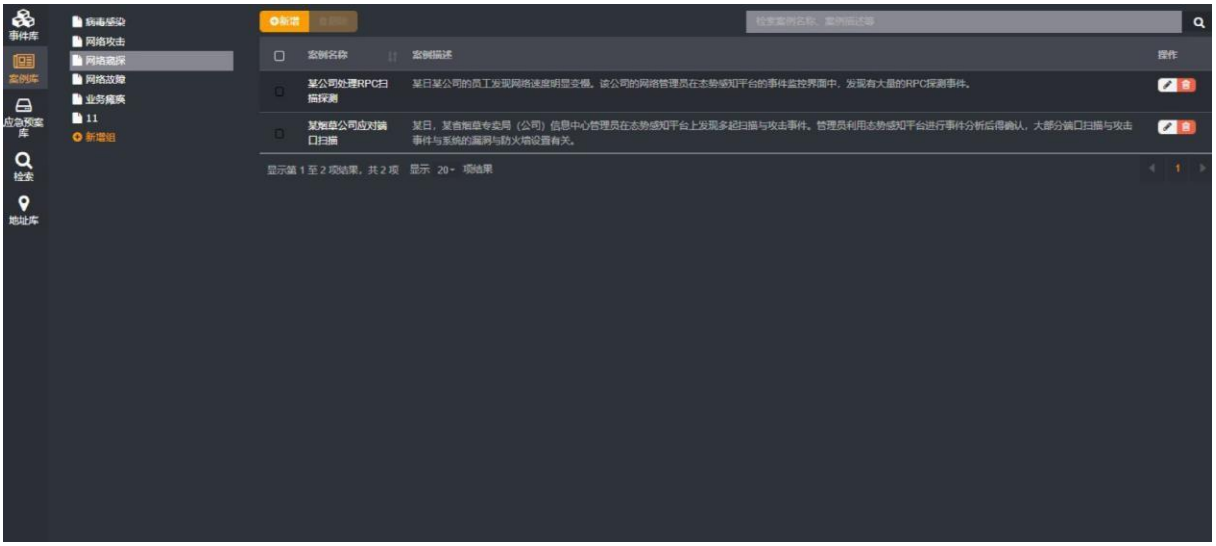
10.1.2 新增事件

新增字段：填写属性值：

- 事件名称（必填，不可重复）
- 事件描述（可选）
- 可能得设备源类型（可选，支持多选）
- 可能得原因或结果 点击 [保存]，即添加成功。如图：

点击编辑、删除按钮对事件进行编辑、删除操作，也可选择多条事件进行批量删除。

10.2 案例库



10.2.1 案例库组

根据案例类型分为不同的案例库组，以树形图展示在左侧列表。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

10.2.2 新增案例

新增字段：填写属性值：

- 案例名称（必填，不可重复）
- 案例描述（可选）
- 解决办法（可选）
- 影响范围（可选）

附件（可选）点击【保存】，即添加成功。如图:

点击编辑、删除按钮对案例进行编辑、删除操作，也可选择多条案例进行批量删除。

10.3 应急预案库

10.3.1 预案库组

根据预案类型分为不同的预案库组，以树形图展示在左侧列表，系统预置了默认的预案库组，用户可以自行添加。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

10.3.2 新增应急预案

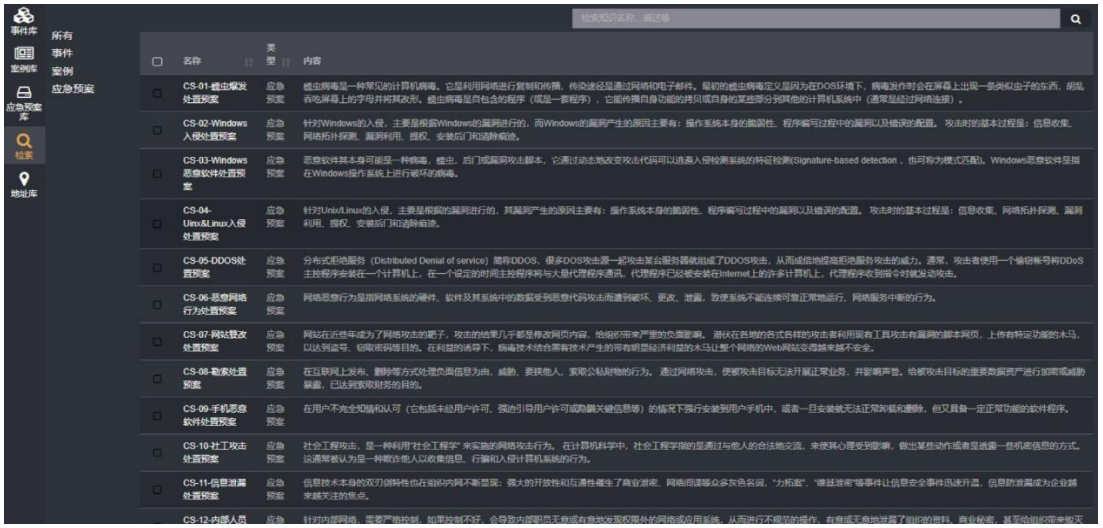
新增字段：填写属性值：

- 应急预案名称（必填，不可重复）
- 摘要（可选）
- 附件（可选）点击【保存】，即添加成功。如图：

点击编辑、删除按钮对预案进行编辑、删除操作，也可选择多条应急预案进行批量删除。

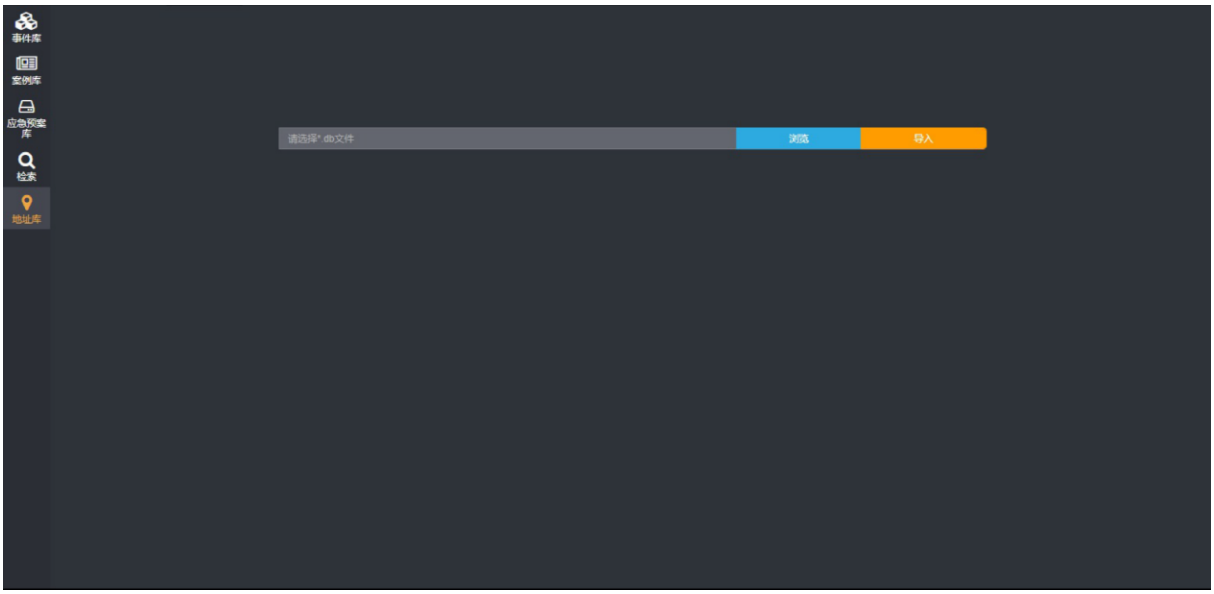
10.4 检索

提供了知识快速检索方式，可按照名称或描述查询所有知识库或者指定库知识，检索后结果如图：



10.5 地址库

地址库中系统预置了内部地址库，可通过导入.db 文件更新对应的地址库信息。如图：



11. 节点管理

对平台各种节点进行管理，可以添加、删除、配置节点，监控节点状态。

11.1 注册/修改节点

注册/修改节点需要配置如下信息：

- 节点类型
- 描述
- 主机（节点访问地址）
- 端口（节点访问端口）
- 协议（可选择 http、https）
- 访问帐号（单点登录节点帐号）
- 访问密码（单点登录节点密码）
- 反向访问主机（如果从节点反向访问管理中心需要地址转换，需要填写）
- 反向访问端口

11.2 节点卡片列表

点击【配置】-【节点管理】菜单，即可进入节点列表页面。事件节点列表中每个卡片中显示了节点的

- 名称
- 地址
- 端口
- 访问路径
- 状态（绿色表示正常，红色表示日志采集器出现故障）

- CPU 利用率及内存利用率
- 在卡片右下角按钮可以点击查看该采集器的详细监控信息，包括：
- 当前 CPU 利用率及最近 1 小时 CPU 利用率趋势
- 当前内存利用率及最近 1 小时内存利用率趋势
- 当前磁盘使用情况
- 当前系统负载情况及最近 1 小时系统负载趋势
- 最近 1 小时网卡流量趋势

在卡片右上角可以对该节点进行操作，对于分布式节点可以进行配置、修改、删除操作，对于本地节点可以进行配置操作。对于不同的节点需要进行对应的配置。

11.3 事件采集器

11.3.1 注册/修改日志采集器

注册/修改日志采集器需要配置如下信息：

- 节点类型
- 描述
- 主机（日志采集器访问地址）
- 端口（日志采集器访问端口）
- 协议（可选择 http、https）
- 访问帐号（单点登录日志采集器帐号）
- 访问密码（单点登录日志采集器密码）
- 反向访问主机（如果从日志采集器反向访问管理中心需要地址转换，需要填写）
- 反向访问端口

11.3.2 配置日志采集器

可以对采集任务、转发及接收参数、过滤策略、日志代理进行配置。详细见采集管理章节。

11.3.3 事件采集器卡片列表

点击【配置】-【节点管理】菜单，即可进入事件采集器列表页面。事件采集器列表中每个卡片中显示了事件采集器的

- 名称
- 地址
- 端口
- 访问路径
- 状态（绿色表示正常，红色表示日志采集器出现故障）
- CPU 利用率及内存利用率

在卡片右上角可以对该该采集器进行操作，对于分布式采集器可以进行配置、修改、删除操作，对于本地事件采集器可以进行配置操作。

在卡片右下角按钮可以点击查看该采集器的详细监控信息，包括：

- 当前 CPU 利用率及最近 1 小时 CPU 利用率趋势
- 当前内存利用率及最近 1 小时内存利用率趋势

- 当前磁盘使用情况
- 当前系统负载情况及最近 1 小时系统负载趋势
- 最近 1 小时网卡流量趋势

12. 范化

12.1 范化策略

范化策略是配置各种类型日志的解析规则，系统已经内置了常用的日志范化策略，能够识别、解析常见的日志格式。对于一些内置范化策略不支持的日志格式，用户可以自定义自己的范化策略。

从导航栏点击【配置】-【范化】，进入范化策略主界面。

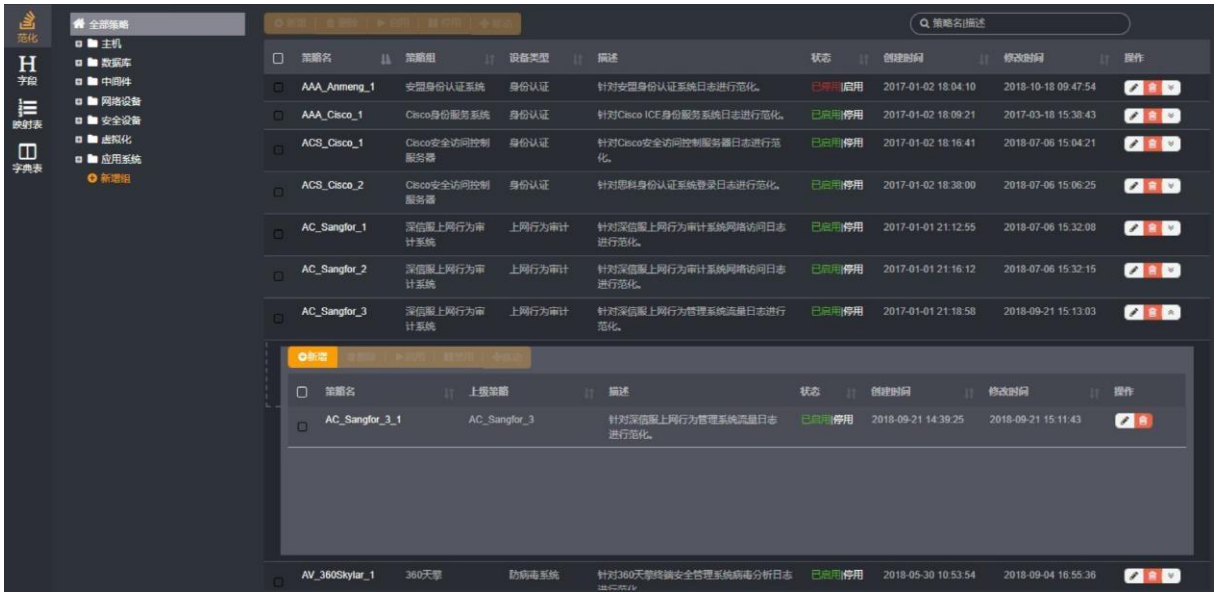
12.1.1 范化策略组

范化策略组采用树型分组结构进行管理。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

12.1.2 范化策略

系统支持二级范化，可对已范化的内容进行详细范化，最终的泛化结果为一级二级范化后合并的结果。当多条日志共性较大差异性较少时，可通过添加一级范化策略，对差异部分添加对应二级范化策略进行处理，或者日志复杂直接编写策略难度较大，可在一级范化进行粗略提取，在二级进行更详细的提取等，二级范化的目的是减少范化策略的编写难度，减轻工作量，并且对未知格式日志提供最大程度的支持。如图：



范化策略相关说明：

索引（#1）：#1 表示正则表达式针对当前日志样本提取出来的第一个索引值，#后面数字不能大于当前正则表达式提取出字段值的个数。

字段名：选择当前索引值对应的字段名称。

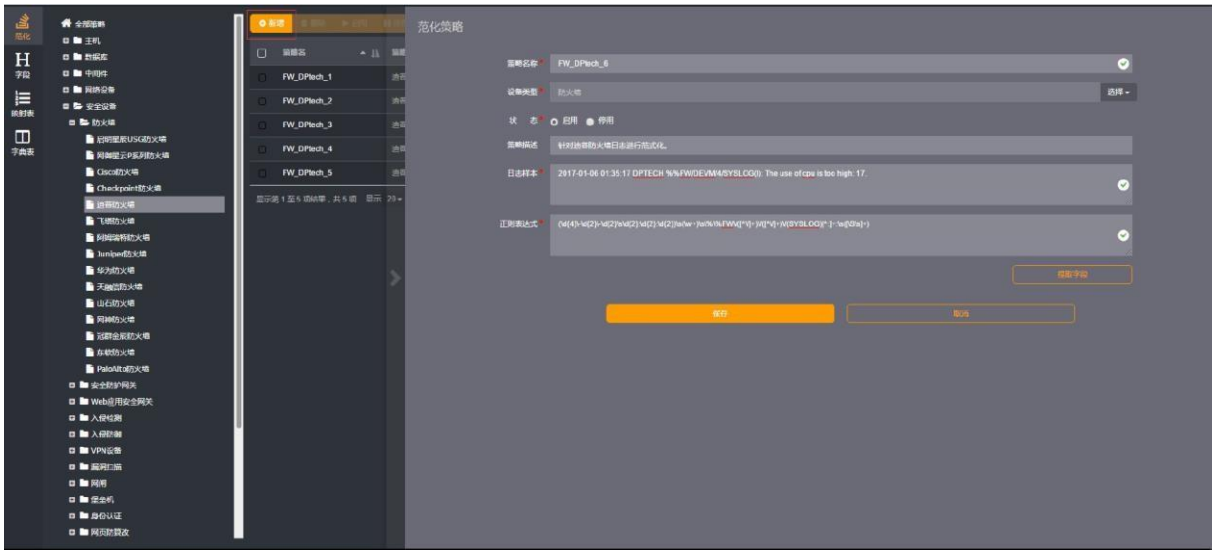
赋值：目前可支持映射表、时间格式化、解析函数、直接赋值、正则匹配方式。

- 若当前索引值需要通过映射表映射（是否有映射关系，请查看映射表模块），则需要选择对应的映射关系；
- 若当前索引值是一个时间值，则需要选择对应的时间格式转换为统一默认格式（年-月-日 时:分:秒）；
- 若当前索引值是一些特殊的有意义字符串，需要选择对应的解析函数转换为更直观的表示；

- 若当前索引值只有部分符合使用要求，可选择正则匹配，添加一个或多个正则表达式（或的关系）对索引值进行详细提取，且多个正则表达式按照从高到低优先级进行排列，可通过右侧排序微调按钮进行设置。

添加字段：针对此范化策略添加一个字段，不依赖正则表达式提取的字段，假设用户确定此类日志属于某种设备的日志，而从日志样本又获取不到对应的字段，则可以使用【添加字段】功能来添加已经可以确定的字段。

新增一个范化策略，选择要添加的范化策略组，点击右侧【新增】按钮，补充必填字段，如图：



点击下方【提取字段】按钮，即可验证正则表达式是否正确，如果正则有问题，会提示给出错误提示，如果正确，如下图所示：

其中[提取值]和[字段赋值]列出正则表达式当前能提取出的字段，接下来用户就可以自行选择每个提取值所对应的字段名称、时间格式以及映射关系。如果提取值需要多次使用，或者多个提取值需要拼接使用，请点击上图中 1 号位置的【+】按钮，此操作会在当前[字段赋值]列表最下方新增一行，用户需要手动输入索引值，如#3 或者#3#4（多个

索引值拼接时，系统默认在两个索引值中间加个空格处理），确定之后即可选择字段名称，映射关系等……

如果用户需要自行添加字段，请点击上图中 2 号位置的【+】按钮，此操作会在[添加字段]列表中新增一行，接下来用户可以操作选择[字段名]和[赋值]，如下图：

上图中

- 1 号位置列是选择索引值对应的字段名称
- 2 号位置列是选择映射关系和时间格式等
- 3 号位置是新增一行带索引值的字段
- 4 号位置为新增一行自定义字段。

每配置一个字段，此页面最下方会有数据验证列表显示，用户可根据验证列表显示数据，判断配置是否正确，验证之后点击【保存】按钮，完成策略新增。

12.1.3 范化策略状态

点击范化策略列表[状态]栏【启用】或【停用】按钮进行单条范化策略状态操作，选择多条范化策略，点击列表上方【启用】或【停用】按钮进行范化策略状态批量操作。

12.1.4 范化策略移动

选择一条或多条范化策略，点击列表上方【移动】按钮，选择要移动到的范化策略组名称，并选择对应策略组中的位置，点击【确定】按钮，完成范化策略移动操作。移动一级范化策略时将同步移动关联的二级范化策略。

12.1.5 范化策略优先级调整

选择一条或多条范化策略，点击列表上方【优先级】按钮，选择要参照的泛化策略及策略的目标位置，点击【确定】按钮，完成范化优先级移动操作。注意优先级调整只在范化策略组子节点同级调整时生效。

12.2 字段

字段作为事件的属性，主要作用于描述一个事件，系统已经内置了常用的字段，对于一些内置字段不满足用户需求的，用户可以自定义自己的字段。

从导航栏点击【配置-范化-字段】，进入字段主界面。

12.2.1 字段组

系统内置了两个字段组，分别为[所有字段]，[未知设备]：

- 所有字段：组包含了一个事件目前所需要的所有字段。
- 未知设备：组的字段是[所有字段]组中的部分字段，作用于当前范化策略无法解析的事件。

12.2.2 新增字段

选择[所有字段]或[未知设备]组，点击右侧【新增】按钮，选择 添加方式 ： 从已有字段添加：选择要添加的字段，点击【保存】，即添加成功。

新增字段：填写属性值：

- 名称（字段名称，必填，不可重复）
- 别名（字段别名，必填，不可重复）
- 描述（可选）
- 类型（字段类型，必填）
- 映射函数（可选）
- 字段长度（必填，0-255）
- 操作符集（必填）
- 取值范围（可选，此属性作用于关联字典表） 点击 [保存] ，即添加成功。

12.2.3 字段顺序调整

选择要调整顺序的字段，点击【移动】按钮，选择要移动到的位置，点击确定，即完成移动操作。

12.3 映射表

映射表是提供范化策略做数据关系映射使用，系统已经内置了常用的映射表，对于一些内置映射表满足不了的范化策略，用户可以自定义自己的映射表。

从导航栏点击【配置-范化-映射表】，进入映射表主界面。

12.3.1 映射表组

映射表组采用树型分组结构进行管理。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

12.3.2 映射分类

新增一个映射表分类，选择要添加的映射表组，点击右侧【新增】按钮，补充必填字段，包括映射

表名称、字段名称（选择字段名称用于配置范化策略时的映射关系），如下图：

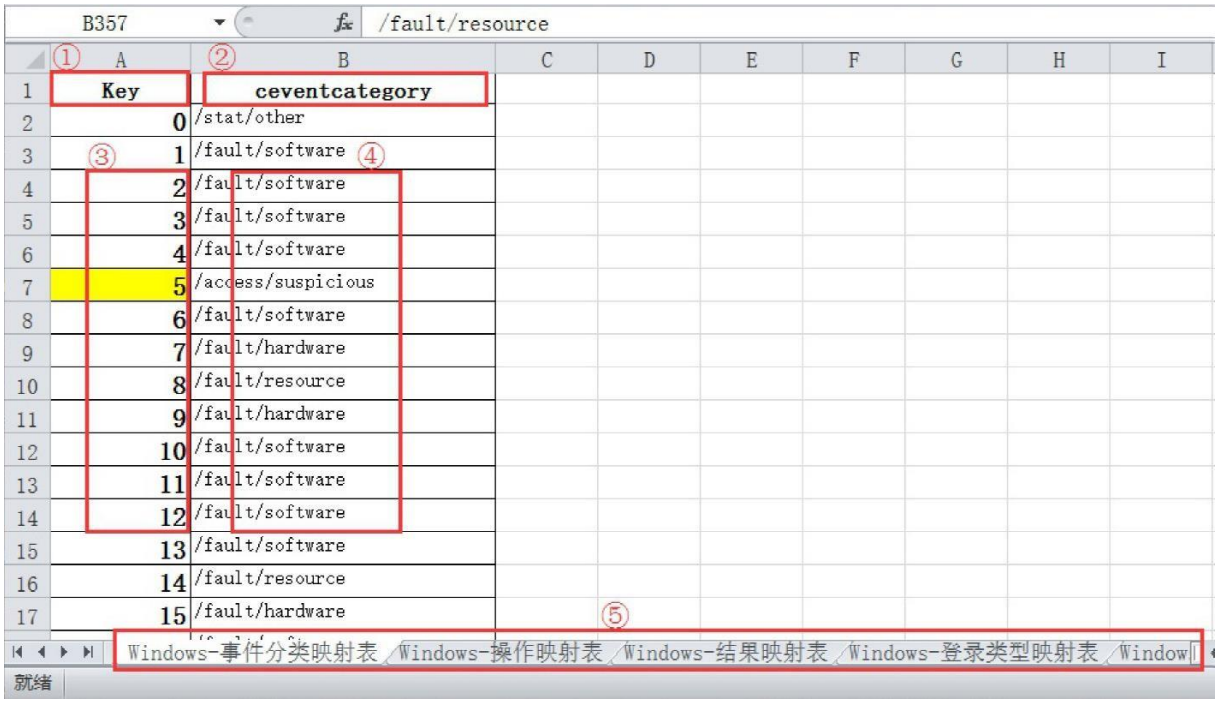
12.3.3 映射取值表

添加完映射表分类之后才可以添加映射取值表，点击【新增】按钮，补充映射原始值和映射后取值，点击【 ✔ 】按钮，即可添加成功。

12.3.4 映射表导入

映射表导入会覆盖当前映射表组下的所有映射表，请谨慎操作

选择要导入的映射表组，点击右侧【导入】按钮，选择要导入的映射表文件（*.xlsx），点击【导入】按钮，即可导入映射表，导入文件格式如下图：



上图中

- 1 号位置为固定格式
- 2 号位置为字段名称（字段名称请参照字段模块）
- 3 号位置为映射原始值
- 4 号位置为映射后取值

- 5 号位置为此类设备针对不同字段的映射表，同一类设备不同字段的映射表应该在同一个*.xlsx 文件中的不同 sheet 里。

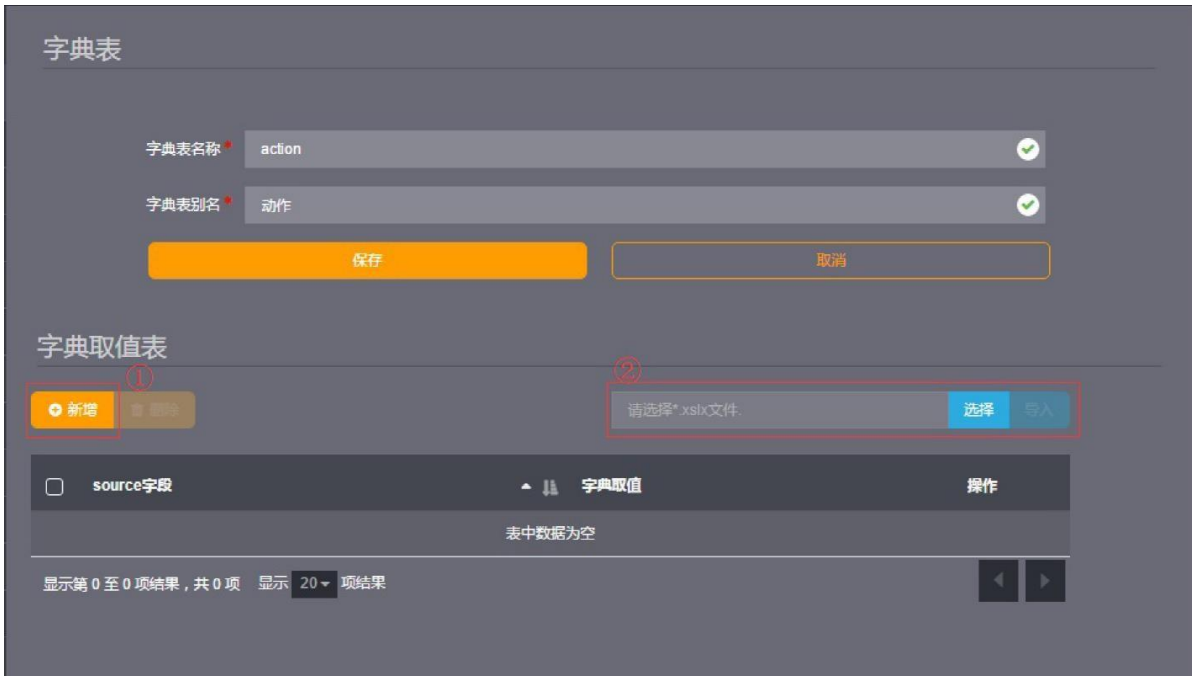
12.4 字典表

字典表是全局的翻译工具，系统已经内置了常用的字典表，对于一些内置字典表不满足用户需求的，用户可以自定义自己的字典表。

从导航栏点击【配置-范化-字典表】，进入字典表主界面。

12.4.1 新增字典表

新增一个字典表，点击【新增】按钮，补充必填字段，包括字典表名称、字典表别名，点击【保存】按钮，即可添加成功，如下图：



12.4.2 字典取值表

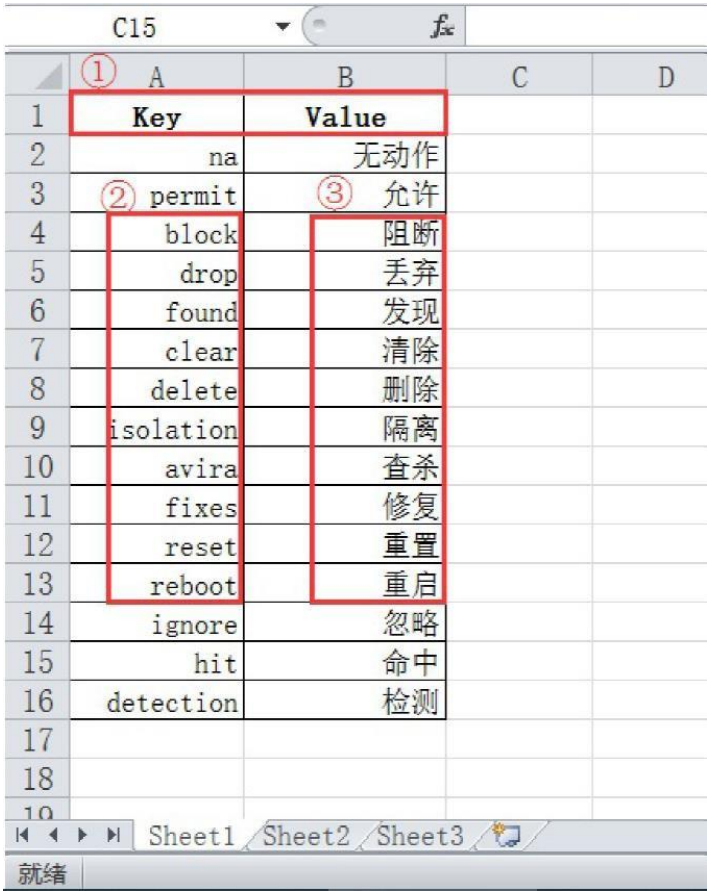
添加完字典表之后才可以添加字典取值，点击上图中1号位置【新增】按钮，补充source 字段和字典取值，点击【 ✔ 】按钮，即可添加成功。

12.4.3 字典取值表导入

字典取值表导入会覆盖当前字典取值下的所有数据，请谨慎操作。

点击上图中 2 号位置【选择】按钮，选择要导入的字典取值表文件（*.xlsx），点击【导入]按钮，即可导入

字典取值表，导入文件格式如下图：



	A	B	C	D
1	Key	Value		
2	na	无动作		
3	permit	允许		
4	block	阻断		
5	drop	丢弃		
6	found	发现		
7	clear	清除		
8	delete	删除		
9	isolation	隔离		
10	avira	查杀		
11	fixes	修复		
12	reset	重置		
13	reboot	重启		
14	ignore	忽略		
15	hit	命中		
16	detection	检测		
17				
18				

上图中，

- 1 号位置为固定格式
- 2 号位置 source 字段
- 3 号位置为字典取值

字典取值表导入目前只支持单 sheet 导入。

13. 日志源

日志源是记录系统采集器所能采集到全部日志的设备列表，当采集器采集到新的设备类型的日志时，系统会将该设备地址以及设备类型等内容添加到此列表。

从导航栏点击【配置-日志源】，进入日志源主界面。

13.1 日志源新增

新增一个日志源，点击【新增】按钮，补充必填字段：

- 设备地址（设备 IPV4 地址活 IPV6 地址，必填）
- 设备类型（必填）
- 采集器（采集器 IP 地址，必选）
- 编码（该设备类型编码格式，必选）
- 分隔符（选填）
- 告警时间（该字段表示 告警时间 内没有接收到此设备类型的日志，将产生告警）

点击【保存】按钮，完成日志源新增。

13.2 日志源编辑

日志源编辑功能只能修改编码、分隔符和告警时间。

13.3 白名单

白名单是配置系统只接收固定设备的日志。

从导航栏点击【配置-日志源-白名单】，进入白名单主界面。白名单配置分为三种：

- 单个 IP 地址，如有多个地址请用逗号分隔：例如:192.168.1.11,192.168.1.12
- IP 地址范围，例如：192.168.1.100-192.168.1.200
- 子网地址，例如：192.168.1.100/24

14. 采集管理

点击【配置】-【节点管理】菜单，进入事件采集器列表页面，点击某个采集器卡片右上角【配置】按钮，即可对该采集器的采集任务、转发与接收、过滤、日志代理进行配置。

14.1 采集任务

点击采集任务菜单，可以对该采集器的采集任务进行管理，系统支持多种采集方式，针对每种采集方式都可以进行新增、修改、删除、启用及停用采集任务，查看采集任务信息及查看采集任务列表操作。

目前支持的采集任务包括以下几种采集方式：

- syslog
- 文件及目录
- snmp trap
- jdbc

针对不同的采集方式，需要配置不同的采集任务信息。

14.1.1 syslog

syslog 采集任务需要配置的信息有：

- 任务名称
- 协议（可选择 UDP、TCP，默认 TCP）
- 端口
- 状态（可选择启用，禁用，默认启用）

syslog 为常用的采集方式，因此系统默认一个采集任务，端口为 514，协议为 UDP，该采集任务可以修改端口、启用及停用，不可删除。

14.1.2 文件及目录

文件及目录自动识别文件及目录，针对文件的存放位置，分四种采集方式：

- 本地（存放在采集器所在主机的日志）
- 远程共享（远程主机上共享的日志）
- 远程 FTP 方式（远程主机上可以通过 FTP 访问的日志）
- 远程 SFTP 方式（远程主机上可以通过 SFTP 访问的日志） 文件及目录采集需要配置的信息有：
- 名称
- 采集方式（可选择本机日志、共享方式、FTP 方式）
- 文件或目录（可填写文件或路径，支持*通配符。当为目录时，可以采集该目录及子目录（最多三级子目录）符合条件的文件）
- 原始编码（可选择 UTF-8、UTF-16、GBK、ISO-8859-1 等，默认 UTF-8）
- 任务间隔（单位为秒）
- 状态（可选择启用，禁用，默认启用）

除以上通用信息外，还需要针对采集方式配置特有信息。

14.1.2.1 本地

本机日志配置以上通用信息即可。

14.1.2.2 远程共享

需要额外配置以下信息：

- 服务器 IP
- 用户名
- 密码

14.1.2.3 远程FTP

需要额外配置以下信息：

- 服务器 IP
- 服务器端口
- 用户名
- 密码
- 传输模式（主动、被动）
- 是否包含子目录（选择是，最多采集三级子目录）
- 服务器字符集（可选择 UTF-8、GBK）

14.1.2.4 远程 SFTP

需要额外配置以下信息：

- 服务器 IP
- 服务器端口
- 用户名
- 密码
- 是否包含子目录（选择是，最多采集三级子目录）

14.1.2.5 SNMP trap

snmp 采集任务需要配置的信息有：

- 名称
- SNMP 版本（可选择 SNMPV1/V2、SNMPV3）

- 端口
- 团体字符串
- 状态（可选择启用，禁用，默认启用） 当选择 SNMP 版本为 SNMPV3 时，还需要配置：
- 环境引擎 ID
- 环境名称
- 是否需要身份验证（如果选择身份验证，需要配置用户名及密码）
- 是否加密（如果选择加密，需要配置加密密码、加密协议）

14.1.2.6 jdbc

jdbc 采集任务需要配置的信息有：

- 名称
- 数据库类型（可选择 oracle、sqlserver、mysql、db2、sybase、postgresql、informix、teradata）
- 服务器 IP
- 服务器端口
- 用户名
- 密码
- 实例/数据库名
- sql 语句(如：id=0#select * from tableName where id>?,如果使用 group by,#号前的列名，必须在 select 中包含，且名称一致)
- 原始编码（可选择 UTF-8、UTF-16、GBK、ISO-8859-1，默认 UTF-8）
- 状态（可选择启用，禁用，默认启用）

14.2 转发与接收

接收与转发的应用场景包括：

- 分布式采集器上报数据给管理中心或分布式数据节点。
- 平台或分布式采集器将数据转发给第三方平台。
- 管理中心接收分布式采集器上报的数据需要配置接收信息。

14.2.1 采集器数据接收

配置采集器上报数据的接收端口，该参数只有管理中心本地采集器才可以调整。默认9514。

14.2.2 数据上传

- 上传目标（显示上传的目标及状态。默认上传到本地，配置了数据节点后，上传目标为数据节点的 ip 及状态）
- 上传协议（UDP/TCP）
- 上传压缩加密（默认不压缩加密）
- 是否上传（默认上传

14.2.3 转发数据

- 转发目标服务（格式为 IP:端口，多个以逗号分隔）
- 转发协议（可选择 UDP、TCP，默认 UDP）
- 转发压缩加密（默认不压缩加密）
- 是否转发（默认转发）

14.3 过滤

用于管理中心对数据进行过滤，将不需要进行分析及存储等处理的数据进行丢弃。可以配置多条过滤策略，只要命中即丢弃。过滤功能包括新增、修改、删除、启用、禁用、查看详细及查看过滤策略列表功能。

过滤策略新增或修改后，仅对新接收的日志有效。

14.3.1 新增/修改过滤策略

新增过滤策略需要填写如下信息：

- 名称
- 描述
- 选择过滤器
- 状态（可选择启用、禁用，默认启用）

14.3.2 删除过滤策略

选择需要删除的过滤策略，点击【删除】按钮，系统会弹出删除确认，确认后系统删除选中的过滤策略。

14.3.3 启用/禁用过滤策略

已启用状态下的过滤策略可点击【禁用】按钮，已禁用状态下的过滤策略可点击【启用】按钮。

14.4 日志代理

显示注册到本平台的 Windows 日志代理的连接状态等信息。当 Windows 日志代理注册到平台时，日志代理列表中会自动增加该日志代理的信息。当日志代代理不再往平台发送事件时，可以在列表中，手动删除该日志代理。从日志代理列表中，可以看到如下信息：

- 设备名称
- 设备地址
- 注册时间
- 连接状态（无法连通、正常）

15. 过滤器

过滤器是根据事件属性创建的组合过滤条件，它可以是单个事件属性条件，也开始是使用与、或、非组合的复杂条件。

过滤器是系统中经常使用的基础组件，可用于事件采集、事件检索、事件统计、关联分析、报表等多个场景。

从导航栏点击【配置-过滤器】，进入过滤器主界面，如下图：

15.1 过滤器组

过滤器采用树型分组结构进行管理。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

15.2 过滤器

一个过滤器的示例如下：

点击过滤器列表上方的【新增】按钮，打开新增过滤器面板，输入名称、描述、过滤器条件，可添加新的过滤器。

过滤器条件支持逻辑条件、字段条件、引用过滤器。

15.3 逻辑条件

支持与、或、非逻辑运算，支持嵌套的逻辑条件。

15.4 字段条件

字段条件支持对各个事件属性设置判定条件，字段条件由事件字段、操作符、右值三部分组成。

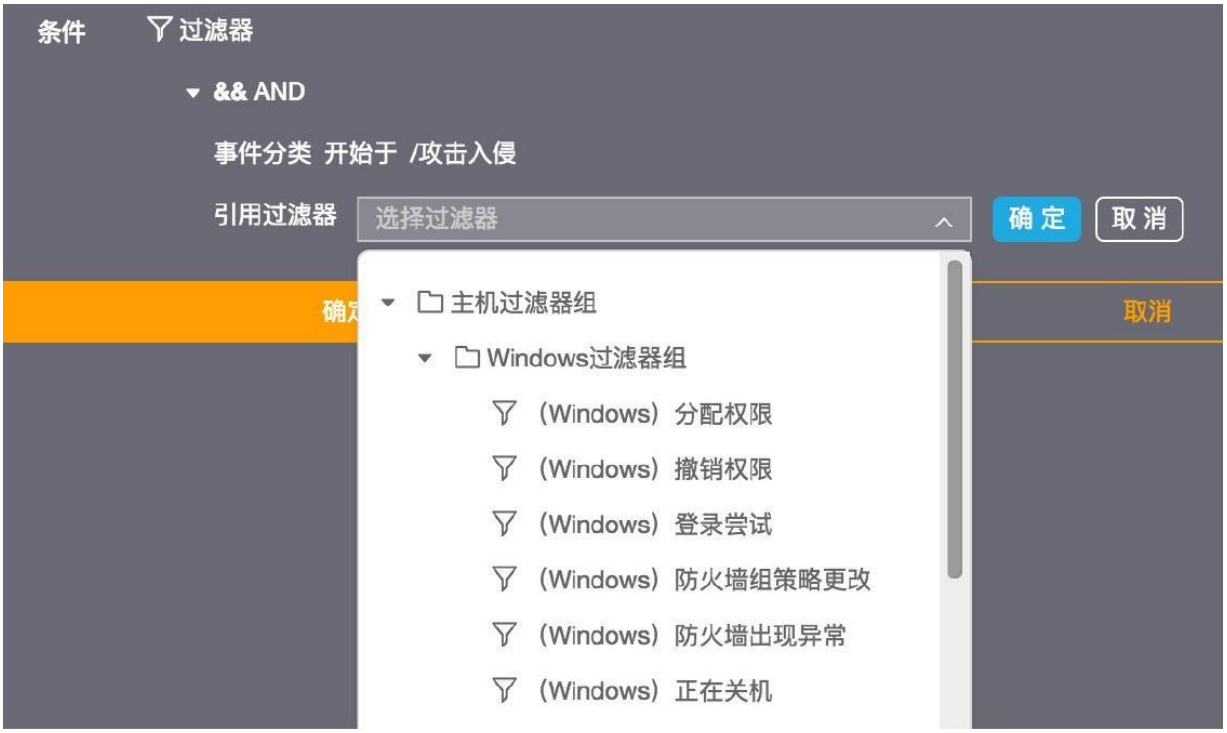
支持的操作符包括

- 等于
- 不等于
- 大于
- 大于等于
- 小于
- 小于等于
- 在两者之间
- 开始于
- 结束于
- 包含
- 属于
- 是否为空
- 通配符匹配
- 正则匹配
- 引用资源

引用资源 资源包括地址资源、端口资源、时间资源，在【配置-资源】中定义。

15.5 引用过滤器

在过滤条件中，可以引入已定义的过滤器使用。



15.6 应用场景

过滤器的应用场景包括：

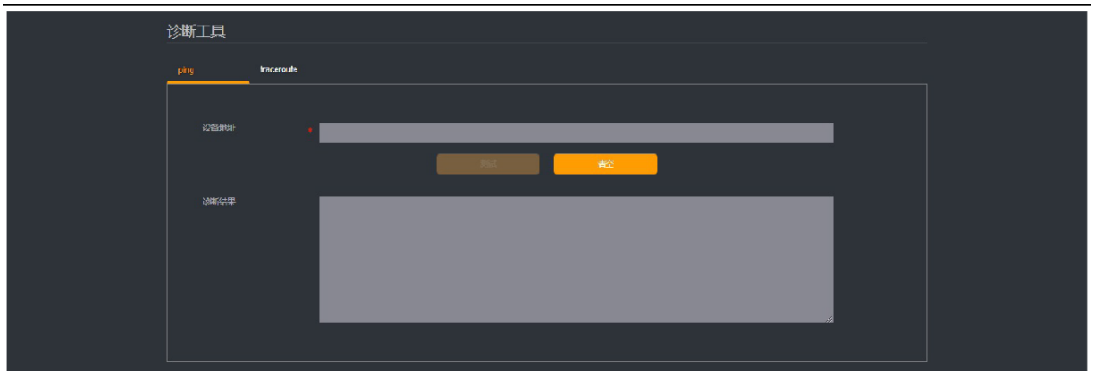
- 事件查询
- 事件统计
- 关联分析

16. 网络诊断

诊断工具是为了方便管理员对设备进行常用命令网络诊断，简化操作及入手的难度。目前支持的命令有 ping、traceroute(tracert)。

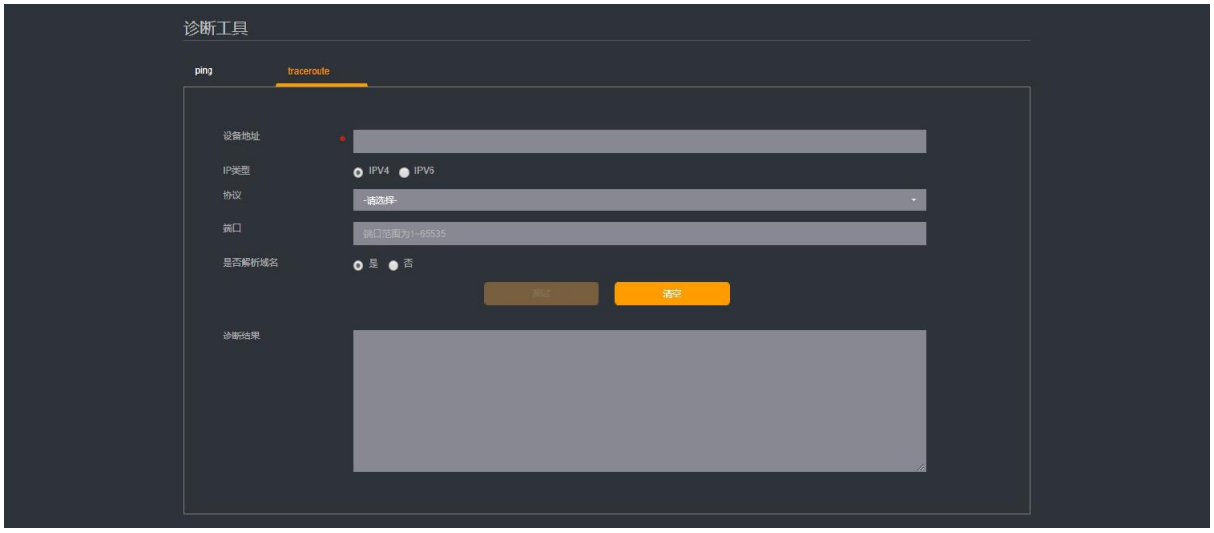
16.1 Ping 操作

直接输入目标设备 IP，点击测试即可。



16.2 traceroute (tracert) 操作

输入目标设备的 IP、IP 的类型、协议、目标端口、是否解析域名，点击诊断即可。



17. 系统

- 菜单维护
- 常用配置
- 诊断日志
- 在线用户

17.1 菜单维护

只有具有所有模块权限的系统管理员才能够进行菜单维护，菜单维护入口只有在满足此条件时才会显示。通过点击菜单栏最右侧的【】下拉列表中的【菜单管理】即可。菜单维护是全局性的，即对整个系统中的所有用户而言，只有一个菜单设置，每个用户能够看到的菜单项只是由于权限的不同而不同。因此请谨慎进行菜单维护操作。

所有的预置菜单项和已共享的仪表板都可以放置到菜单中显示，也可以从菜单中移除不再显示。所有放入菜单的项目都可以通过拖拽的方式调整顺序。

17.1.1 菜单组

可以将多个菜单项组合到一起，合并为一个菜单组放入菜单中显示。在菜单维护对话框的[新建菜单组]中:

- 选择菜单组图标
- 填写菜单组名称

点击【+】按钮后即可添加一个菜单组。

添加菜单组后，通过鼠标将菜单项拖拽到组中，即可进行菜单组的配置。

菜单组不允许修改，只能删除。菜单组删除后，组中的所有菜单项并不会被移除，而是被追加到菜单的最后位置。

17.1.2 移除

需注意的是，如果从菜单中移除，意味着：

- 移除预置菜单项，只是将此菜单项隐藏，并不会删除，仍然可以在菜单维护对话框的[隐藏的菜单项]中看到。
- 移除已共享的仪表板，会修改仪表板的置顶菜单设置，但并不会直接删除仪表板，也不会修改仪表板的共享设置。
- 移除菜单组，则会直接删除菜单组，无法恢复；但并不会删除组中的菜单项。

17.1.3 恢复出厂设置

如果菜单出现混乱或希望进行重新维护，则可以通过在菜单维护对话框中，点击【恢复出厂设置】按钮来使得菜单恢复到第一次运行时的状态。

17.2 常用配置

17.2.1 许可管理

许可管理功能可显示当前授权状况，包括设备序列号，用户名称，授权状态和授权剩余时间。同时，升级的授权许可文件亦可通过此功能导入。

17.2.2 服务器地址

系统运行过程中，可能需要与事件采集器等其他节点通讯，因此需要服务器具备确定的设备地址。

如果由于各种原因本系统所在的服务器配置了多个IP 地址，就有可能造成通讯失败。为避免此类问题，请在此指定一个专供系统使用的 IP 地址。

17.2.3 时间设置

用于修改系统当前时间和设置时间自动同步。

时间自动同步功能需要您指定一个时钟服务器地址（需网络可达）。

请注意:如果您使用的是本系统的软件版本，启用时间自动同步功能将会关闭操作系统原有的时间同步功能，请您在启用此功能前做好相关评估。

17.2.4 登录认证配置

登录认证配置可用于减少系统遭受非法访问的可能。

- 登录重试次数：即登录失败的最大次数，默认为 3 次，同一用户登录失败超过此阈值，将会导致账户锁定。
- 锁定时间：超过登录重试次数后，系统将被锁定的时间，默认 5 分钟。
- 密码有效时长：用户需要修改密码的最长时限（天）。默认为 0（表示密码永久有效）。
- 同一用户登录的会话数：默认为 0（表示不限制）。
- 会话超时时间：当会话无操作时默认的超时时间，默认 60 分钟。

17.2.5 邮件配置

系统默认的邮件发送的 SMTP 配置，请向您的网络管理员咨询相关参数。

- 邮件服务器地址（IP 地址或域名）
- 邮件发送服务端口
- 是否需要认证或 SSL 加密
- 邮件帐号

- 邮件密码（在系统中，邮件密码会被加密存储，请您放心使用）
- 发件人邮件地址（与您的邮件帐号相关）

配置完成后，可以通过“发送测试邮件”功能向您指定的邮箱中发送测试邮件，以验证配置。

请注意:第三方邮件系统为了保证安全性可能会做出一些调整，当您无法成功发送邮件时请详细阅读其配置说明（例如：网易邮箱的邮件密码与 Web 登录密码并不相同，需要您单独设置）。

17.2.6 自身监控阈值配置

用于监控系统自身性能阈值。

- CPU 告警阈值，默认 80%
- 内存告警阈值，默认 80%
- 磁盘使用告警阈值，默认 80%

17.2.7 告警数据维护

用于维护告警数据存储时限及数量。

- 最长保存时间，默认 90 天。
- 告警最大容量,默认 100 万条，超出后将删除最旧的告警。以上两条维护规则同时生效，互不干扰。

17.3 事件管理

用于事件数据的备份与恢复。

17.3.1 备份配置

- 事件数据备份目录
- 在线保存时间，默认 30 天。超出在线保存时间的数据将转为离线保存状态。
- 离线保存时间，默认 180 天。超出离线保存时间的数据将被清除。

17.3.2 手工备份与恢复

用于手工备份和恢复在线数据。

17.4 诊断日志

- 本功能用于从集群各节点中下载运行日志（包括系统调试日志、Web 服务器运行日志等）用于研发分析调试。
- 可以根据需要选择需要下载日志的节点，如无特殊情况建议选择全部节点。

17.5 在线用户

显示当前登录系统的用户，用户类型，终端地址以及在线时间。

17.6 当前用户

17.6.1 查看/编辑用户信息

点击界面右上角的用户头像，在下拉框中点击用户名即可打开用户信息状态框。 若要修改用户信息，只需按格式要求修改用户信息后，点击【确定】按钮即可完成用户自身信息的修改。

17.6.2 修改用户密码

点击界面右上角的用户头像，在下拉框中点击【修改密码】即可打开用户密码修改模态框。

按照要求填写正确的“当前登录密码”、“新的登录密码”及“确认密码“后，点击【确定】按钮即可完成用户密码修改。

密码修改成功后会自动跳转到登录页面。

18. 数据

- 配置管理
- 策略包
- 事件管理

18.1 配置管理

配置管理用于以下功能：

- 设定系统配置备份的路径和周期；
- 手工备份和还原配置
- 清理系统操作日志及事件数据
- 查看配置备份还原历史

18.1.1 备份配置

此处配置指系统当前所应用的各配置参数，包括您在系统中设定的大部分内容，例如系统中常用配置，过滤器，规则，映射表，资源，泛化配置等；不包括各种数据（例如日志数据，FLOW 数据，告警，资产等)。

配置备份可以设定为手动或自动的周期性进行，用于对配置周期性存档，避免误操作带来的损失。

您也可以通过配置备份/还原操作快速部署新的节点。

18.1.2 配置备份与还原

- 手工备份系统配置。
- 手工还原系统配置。

18.1.3 数据清理

用于系统试运行结束后的测试日志和数据清理。

- 清理系统操作日志。
- 清理事件数据。

请注意：此操作不可恢复，请谨慎使用。

18.1.4 配置备份还原历史

- 记录备份/还原操作历史，操作者以及操作状态。
- 对已备份的配置提供下载。

18.2 策略包

策略包功能可以将系统中一系列相关配置导出并平移至目标系统；可用于项目成果快速共享。

策略包可以包含以下内容：

- 仪表板

- 规则
- 分析
- 泛化
- 报表

18.2.1 策略包导出

请注意：同时选择左侧模块与对应右侧树后，策略包导出按钮才变为可用状态。

18.2.2 策略包导入

选择策略包文件，点击“导入”按钮，即可将策略包导入。

18.2.3 策略包操作历史

- 记录备份/还原操作历史，操作者以及操作状态。
- 对已备份的策略包提供下载。

19. 资源

用户维护系统使用中引用的各种资源，包括：

- IP 资源
- 端口资源
- 时间资源

19.1 IP 地址资源

用于维护 IP 地址资源合法的 IP 资源格式：

- 单个 IP 地址，如有多个地址请用逗号分隔: 例如:192.168.1.11,192.168.1.12
- IP 地址范围，例如:192.168.1.100-192.168.1.200
- 子网地址，例如:192.168.1.100/24

19.2 端口资源

用于维护端口资源

合法的的端口资源格式:

- 单个端口，如有多个端口请用逗号分隔: 例如:80,8080
- 端口范围，例如 80:90

19.3 时间资源

用于维护时间资源

可添加的时间资源:

- 时间段，指定起始时间和结束时间
- 月周期，指定每月的起始时间到结束时间
- 周周期，指定每周的起始时间到结束时间

20. 权限

系统权限基于三权分立原则设计，内置三个用户：

- operator 安全管理员，负责系统的操作使用和日常运行维护及权限分配。
- admin 系统管理员，管理系统权限，维护用户。
- auditor 审计管理员，对系统操作进行审计分析。

20.1 用户管理

20.1.1 用户组

用户组采用树型分组结构进行管理。

点击组节点右侧的操作按钮可以进行新增子组、编辑当前组、删除当前组的操作。点击最下方的【新增组】按钮可以新增顶层组节点。

20.1.2 用户卡片列表

点击【权限】-【用户】菜单，即可进入用户管理页面。角色列表中显示了用户的

- 头像
- 用户名
- 真实姓名
- 该用户的角色
- 操作按钮
  - [编辑用户]
  - [修改密码]

20.1.3 新增/编辑用户

点击表格上的按钮栏中的【新增】按钮即可进入用户新增页面。点击用户卡片中的【头像】或【编辑用户】即可进入用户的详情和编辑页面。在弹出的新增/编辑用户面板中，填写用户的基本信息后点击确定按钮即可完成新增/编辑。

点击用户卡片中的【修改密码】即可进入用户的密码信息编辑页面。在弹出的密码修改面板中，填写用户的密码信息后点击确定按钮即可完成用户密码的修改。

20.1.4 基本信息

基本信息包括：

- 用户名：新用户的登录名称，必填，(用户名由 2-64 个字母、数字或"组成,且不能以"开头和结尾)
- 真实姓名：新用户的真实名称，必填
- 角色
- 联系电话
- 手机
- 电子邮箱
- 描述

20.1.5 密码信息

- 登录密码：用户的密码，必填
- 确认密码：再次确认用户的密码，必填

20.1.6 删除用户

点击用户卡片上的复选框选中目标用户，然后点击上方的按钮栏中的【删除】按钮，删除选中的用户。系统内置的用户不允许删除。

20.1.7 快速搜索

在上方工具栏中的快速搜索框内可根据用户的用户名或真实姓名进行快速检索。

20.1.8 排序

点击上方工具栏中的【排序】按钮，在下拉菜单中选择排序方式，可对用户卡片列表进行排序。

20.2 角色管理

20.2.1 角色列表

点击【权限】-【角色】菜单，即可进入角色列表页面。角色列表中显示了角色的

- 名称
- 描述
- 用户该角色的所有用户

20.2.2 新增/编辑角色

点击表格上的按钮栏中的【创建】按钮即可进入创建角色页面。点击角色的【名称】即可进入角色的详情和编辑页面。

在弹出的创建/编辑角色面板中，填写角色的基本信息、用户分配和授权信息后，即可完成创建/编辑。

20.2.3 基本信息

基本信息包括：

- 名称
- 描述
- 角色类型，基于三权分立原则，角色类型包括
  - 系统管理
  - 审计管理
  - 权限管理

角色类型只能在创建时指定，编辑角色时不能够修改角色类型。

20.2.4 用户分配信息

角色可以被授予多个用户。但可被分配的用户列表还受角色类型的限制。根据角色基本信息中的角色类型，用户列表中只会显示：

- 尚未被分配任何角色的用户
- 已被分配角色，但已分配角色的角色类型与当前选择角色类型相同

20.2.5 授权信息

角色的授权信息是角色的核心属性，包括功能授权和数据授权。

- 功能授权

功能授权以功能模块划分，每个模块支持读和写两种授权。写授权依赖于读授权，即选择写授权后，读授权会被自动选择。

功能模块会跟随角色类型的不同而变化，不同的角色类型包含不同的功能模块。 数据授权数据授权通过选择授权树中的节点完成授权。只有被勾选的节点的数据，才能被拥有该角色的用户访问。

- 数据授权

数据授权树的节点选择原则为：勾选父节点，则所有当前子节点（如果有）被勾选并被禁用，即拥有该父节点和节点下的所有当前子节点和未来创建的子节点权限勾选所有子节点，父节点不会被自动勾选，即只拥有父节点下当前子节点的权限

20.2.6 删除角色

点击角色行最后的【删除】按钮可以删除单个角色；通过勾选角色行最前的复选框，并点击表格上的按钮栏中的【删除】按钮，可以删除多个角色。

系统内置的角色不允许删除。

20.2.7 用户与角色关联

一个角色可以被授予多个用户；一个用户可以拥有多个角色，但多个角色只能是同一角色类型。一个尚未被授予任何角色的用户，可以被授予任意角色类型的角色。

21. 命令行配置详解

平台管理命令为 cbtcmd，使用 cbtadmin 账号即可使用此命令。

21.1 显示帮助提示

```
cbtcmd -h
```

说明：无参数 cbtcmd 命令后添加任何无效的参数都将显示帮助提示。

21.2 系统管理

21.2.1 应用启停

启动服务：

```
cbtcmd --start
```

停止服务：

```
cbtcmd --stop
```

重启服务：

```
cbtcmd --restart
```

```
cbtcmd --status
```

显示服务状态：

21.2.1 修改 cbtadmin 用户密码

```
cbtcmd -P
或cbtcmd --passwd
```

21.2.3 修改主机名

```
cbtcmd -N
或cbtcmd --name
```

参数 hostname，将主机名修改为参数 hostname 给出的名字。此参数缺省时，显示当前主机名。

21.3 软件系统管理

21.3.1 获取序列号

```
cbtcmd --sn
```

21.3.2 软件升级

```
cbtcmd -U <filename>
或cbtcmd --update <filename>
```

参数：filename，升级文件的绝对路径。 使用举例 cbtcmd –U update_20190328.tar.gz
使用升级命令前，需通过 ssh 的方式上传升级包至服务器cbtadmin 用户的主目录中。

21.3.3 软件升级，不重启应用

```
cbtcmd -UNR <filename>
cbtcmd --update_without_restart <filename>
```

参数：filename，升级文件的绝对路径。
使用举例 cbtcmd -UNR update_20190328.tar.gz
使用升级命令前，需通过 ssh 的方式上传升级包至服务器cbtadmin 用户的主目录中。

21.3.4 显示软件版本信息

```
cbtcmd -sv
cbtcmd --swversion
```

21.3.5 显示安装路径

```
cbtcmd --path
```

21.3.6 启用/停用HTTPS

```
cbtcmd --https on/off
```

参数：on 启用https，off 停用https，开启http 端口号为16520，开启https 端口为16525。

21.3.7 导出系统日志

```
cbtcmd -E 或者cbtcmd --export_log
```

无参数，导出日志数据库及 webserver 日志，导出文件放置在 ftp 根目录（即 cbtadmin用户主目录）