ALEIYE

让 | 大 | 数 | 据 | 更 | 简 | 单

中国电信 XX 公司

大数据 IT 安全审计平台项目

北京数介科技有限公司

目录

第1章 数介科技简介

北京数介科技有限公司是一家专注于企业大数据分析、挖掘和应用的高新科技企业，国内领先的大数据解决方案解决商。核心理念是为企业在大数据变革中提供技术支撑平台，真正实现企业数据的可见、可用，可挖掘价值。

数介科技依托自主知识产权的 Aleiye 实时大数据分析引擎，形成数据平台+应用服务+行业解决方案的综合大数据产品。可充分应对行业多样化和企业个性化的大数据需求，为企业在 IT 运维、业务运营、系统安全以及合规审计等多方面提供深度服务。

目前，数介科技的大数据服务已深入金融、运营商、广告、政府等多个行业，并协助客户收集并整合海量业务数据，提供多维度的数据分析图表，预测业务发展趋势，为经营决策提供直观、精确、实时的数据支撑。

第2章 Aleiye 技术白皮书

2.1.1 产生背景

根据 IDC 对企业进行的数据调查，当被问及大数据计划对企业来说其重要程度如何时，53%的受访企业回答至关重要或高优先级，另有 34%的受访企业回答为中度优先级，只有 12%的受访企业认为大数据计划尚属低优先级。

被问及针对非机构化数据，受访企业中，认为建设数据管理平台，面临的挑战分别为：

1、组织结构划分细，执行能力下降。

2、业务人员不具备分析能力。

3、职能部门划分，导致业务忙点。

4、新的数据部门会不会带来新的盲点。

5、数据部门紧跟新技术以维护和升级平台。

针对过半的企业对大数据的需求以及，企业在大数据平台建设中所面临的挑战，ALEIYE 数据平台应运而生。

2.1.2 应用场景

- 数据量激增导致现有分析系统无法满足对业务功能上或性能上的支撑的企业。
- 业务类型多样，想从多样的数据中提炼出新的利润增长点的企业。
- 数据流量大，想实时的查看自己设备或是业务发展的企业。
- 使用 ALEIYE 能够快速使企业以业务为驱动快速构建自己的大数

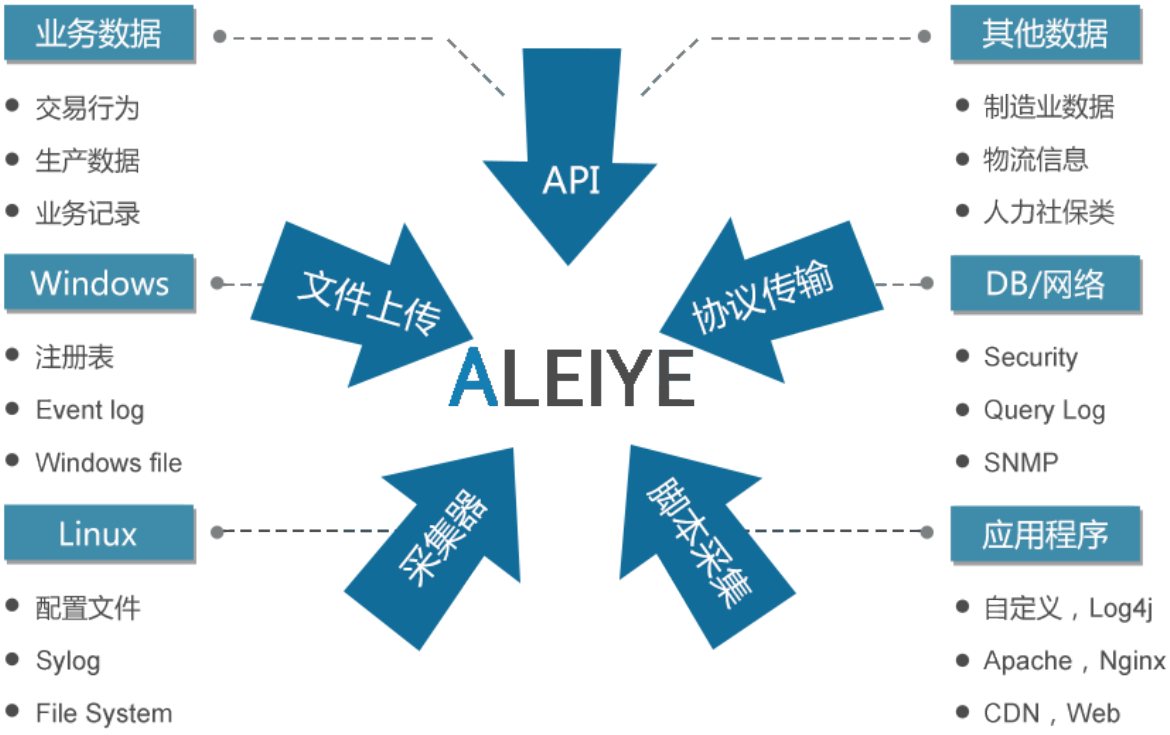
据平台。

- 对于已经意识到大数据是未来的发展方向，且有构建自己的大数据平台挖掘自己数据中的价值的企业，都是 ALEIYE 平台的潜在客户。

2.1.3 产品功能

2.1.3.1 数据整合

企业数据一般都分散存储在不同的业务系统中，企业规模越大业务系统越多，数据类型也就越多越复杂。所以多数据类型的整合是任何企业构企业大数据平台的第一步。ALEIYE 通过如数据采集器、文件上传、协议传输，脚本采集，API 等手段将分散的、异构的数据进行实时的收集、拆解并整合进入平台。企业通过定义的采集规则，通过对数据进行拆解、过滤等手段进行预处理，并保证数据的实效性，完整性及准确性。为数据的关联、分析以及挖掘打下基础。



- 采集器

  数迅自主研发，可直接在服务器中运行，通过 web 控制台，对运行在多台设备上的的采集器进行控制管理。可以支持同时监控多个文件的变化情况，并将变化后的数据实时采集提交到平台。

- 文件上传

  通过 web 界面直接将文件上传至平台。支持格式包含文本文档、csv、rar、zip、7z、tar 和 tar.gz 压缩文件。

- 协议传输

  数据可以通过协议进行传输。支持以下传输协议

  - FTP：支持系统获取固定 FTP 的文件，也可以通过 FTP 协议进行上传。
  - Syslog：通过 syslog 将数据直接发送到平台。

- SNMP：主要针对运维信息，可以通过标准 SNMP 进行采集。

- 脚本采集

平台提供数据上传脚本，可以通过指定的用户名参数，将命令的执行结果发送给系统。

- API

提供入库工具包，可以兼容 java、python、php 等脚本语言。用户可以直接通过编程直接将数据发送给数据平台。

- 其他方式
  - 数据库
    - 支持 mysql、oracle、sqlserver 等常见关系型数据库。
    - 支持历史数据直接导入。
    - 支持增量数据的导入。
  - 自定义
    - 不同业务产生的数据格式各不相同，可通过 API 的方式自定的业务接口进行数据传输。一般扩展周期为 5 个工作日。

2.1.3.2 实时检索

- 实时性

业务系统事件实时查看，达到事件发生可见性，可实时监测应用，可关联分析高速数据流事件，追踪进行中的业务时间和在线的应用活动情况。

- 关键字检索

  类似百度和谷歌的关键字检索，并可以使用布尔代数 AND、OR、NOT 及括号任意组合关键字进行过滤，也可通过正则表达式的方式进行进行检索。

- 标准的 SQL 检索

  可通过 SQL 语句直接进行检索和统计。

- 多数据源同时检索

  所有数据源通过进入平台后可使用检索接口统一进行检索，统一检索结果界面，查看全局数据情况。

- 优化搜寻方式

  在任何时间区间可快速产生结果，内置最近十分钟、昨天、一个月迄今等相对时间访问和指定绝对时间范围的选项，简化用户操作。

- 可视化展示

  根据检索内容，显示符合条件的事件趋势，以图形化的形势展示，并可通过检索直接产生统计和趋势的报表

- 交互式搜索

  利用图表点击放大或缩小时间轴快速显示事件趋势、峰值和异常。在搜索结果中点击信息，可进行下一个维度的分析，实现数据钻取。

2.1.3.3 离线任务

- 历史数据复杂报告定制

对于海量的历史数据，可通过页面设定复杂的离线任务，周期性产生报告。报告也可通过邮件发送或直接导出。

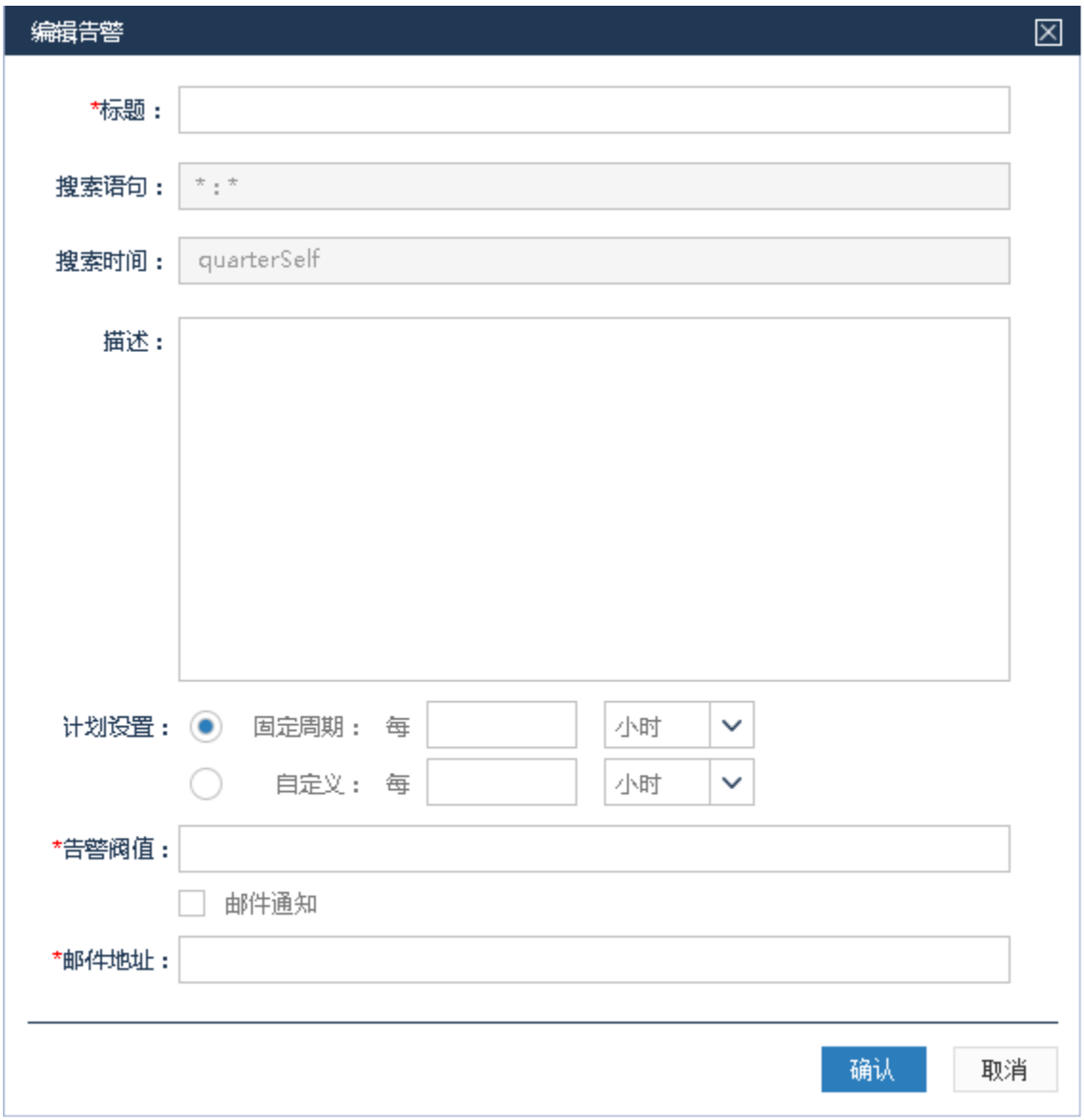
- 历史数据批量迁移

ALEIYE 数据平台提供数据离线导出和导入的接口，因此，任何平台升级、硬件升级或业务系统升级改造都会不影响数据的迁移。

- 历史数据打标

当新业务产生后，有可能需要对历史数据进行新的业务分类。系统提供了历史数据批量打标的功能，满足历史数据添加新标签以知更好的支撑新业务的需要。

2.1.3.4 告警



- 实时告警

  对于时序数据，可根据业务规则定制告警规则，对在数据流动的采集过程中指定时间窗口内发生了满足业务规则的数据流触发告警。

- 任务告警

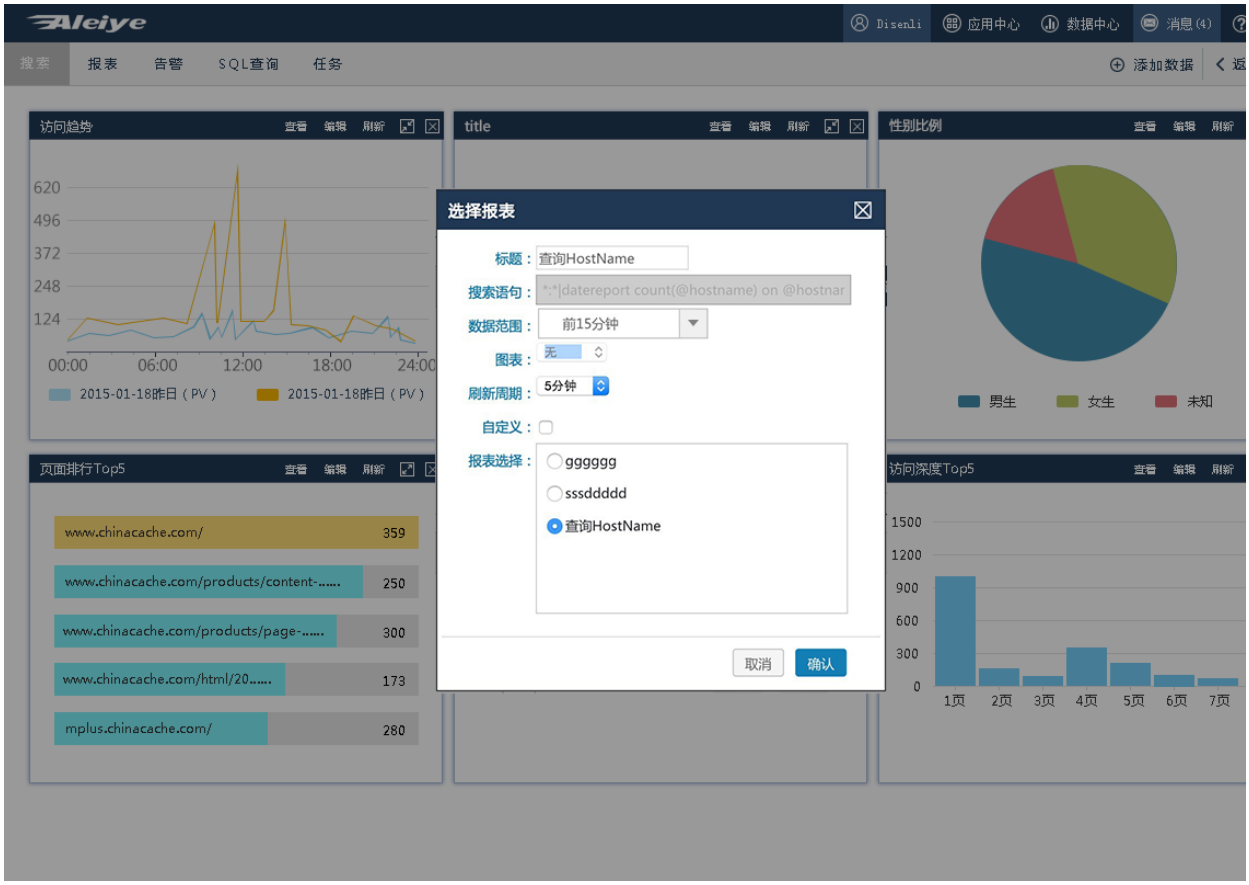
  通过周期性的任务定义告警手段。ALEIYE 平台可以通过关键字或 SQL 语

句对统计的结果判断是否满足告警条件，并按照指定的周期执行。

- 告警动作

告警产生后，可以通过邮件方式发出或对接短信平台直接发送到相关负责人。

2.1.3.5 报表



- 自定义仪表盘

仪表盘是展示业务人员关心指标的实时情况，但是传统的仪表盘只能固定展示某一类指标的情况。ALEIYE 平台提供了自定义仪表盘功能，可以通过各类命令组合，从各种数据源中过滤出业务人员真正关心的业务指标变为一个仪表盘，实时展示。

- 自定义报表

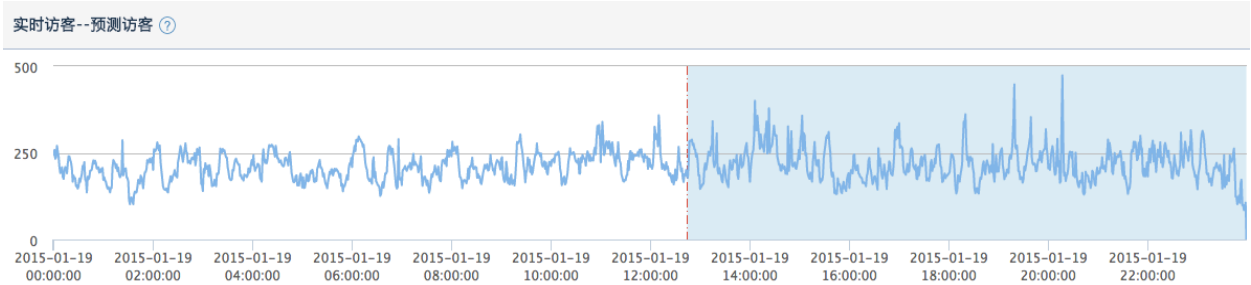
  报表可以将业务最直观展现。传统的数据报表需要编写代码、数据入库、前端展现等多步骤实现，而 ALEIYE 可以直接通过报表命令产生报表，并且组成用户自己报表群支撑日常工作，极大的压缩是时间成本和工作成本。

- 导出为文件

  所有的仪表盘或者报表都可以通过文件导出，作为会议、文档和汇报工作中使用。目前文件格式支持 csv 和 pdf 两种格式。

2.1.4 数据挖掘应用

2.1.4.1 趋势分析



- 预测

  时序数据是具有流动性的，而且一般业务都存在周期性。平台通过对历史数据进行抽象，形成模型。形成的模型结合当前数据的表现，可以预测下一个阶段数据趋势

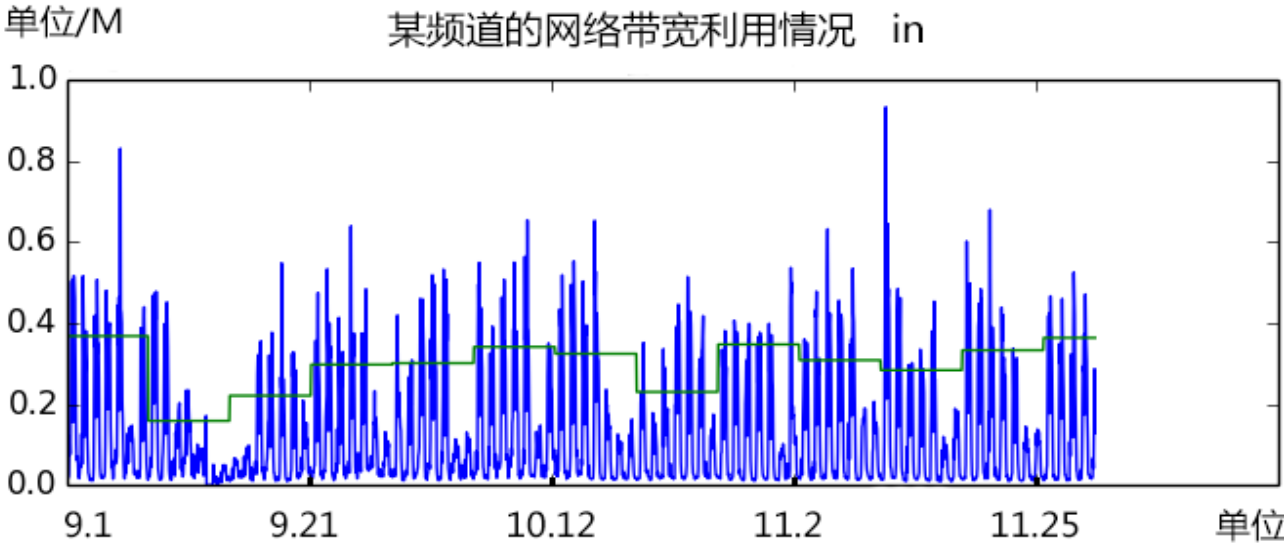
- 预警

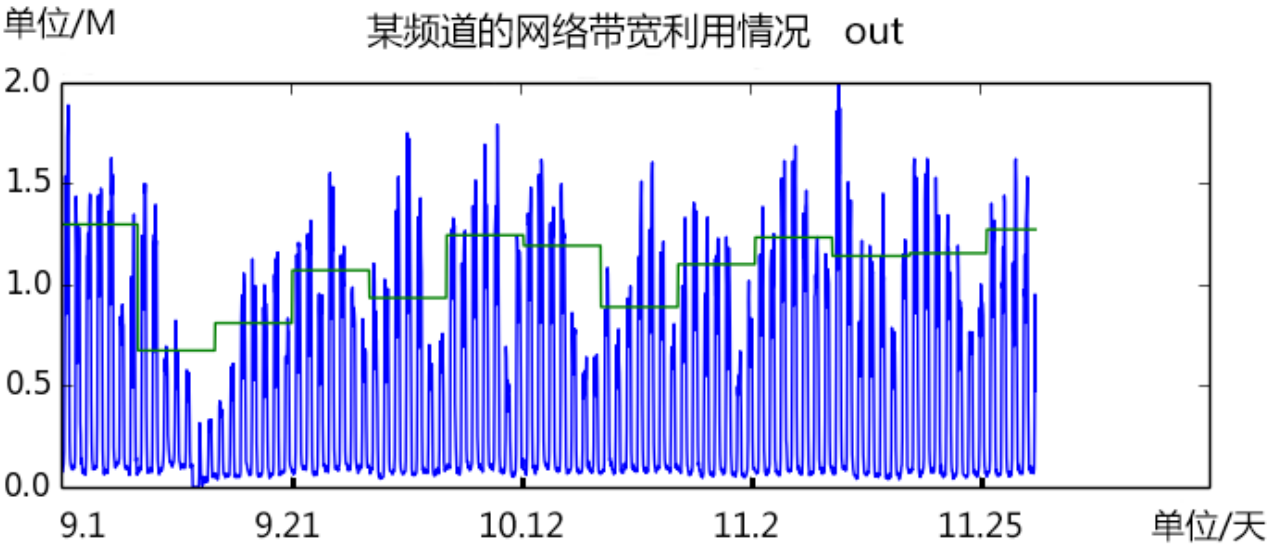
  基于预测结合告警阈值的设置，就可以达到预警的目的，提前发现系统或是业务可能出现的爆发点。

2.1.4.2 资源负载分析

平台可以提供专门的资源负载分析，能够整体反应资源的利用情况，如带宽利用率 ，cpu 利用率，内存利用率等。通过不同的关键字也可以做不同业务的真是情况反应。

平台的负载分析功能是结合趋势分析与分段技术，配合流数据而产生的冠以平均值。如下面反映的是某视频网站的某个频道带宽三个月的上行流量使用情况，其中绿色为每周的综合使用情况。





2.1.4.3 关联分析

不同的业务场景，关联分析的内容会有比较大差异。平台提供基于时间和基于业务两种机制。

- 基于时间：

  根据时间进行的关联分析。当某个业务出现异常时，可以帮助用户找到问题之间关系，如先后顺序，影响范围等。

- 基于业务

  结合业务情况，用户选择数据源和需要分析的指标，选择不同的算法定义任务，提交给平台进行分析。

2.1.5 技术说明

2.1.5.1 Hadoop

实现了一个分布式文件系统（Hadoop Distributed File System），简称 HDFS。HDFS 有高容错性的特点，并且设计用来部署在低廉的（low-cost）硬件上；而且它提供高吞吐量（high throughput）来访问应用程序的数据，适合那些有着超大数据集（large data set）的应用程序。HDFS 放宽了（relax）POSIX 的要求，可以以流的形式访问（streaming access）文件系统中的数据。

Hadoop 的框架最核心的设计就是：HDFS 和 Map/Reduce。HDFS 为海量的数据提供了存储，则 Map/Reduce 为海量的数据提供了计算。

ALEIYE 平台在 HDFS 存储的基础上设计开发，保证数据的可靠同时，进行了应用级别的优化。同时使用 Map/Reduce 作为离线任务的底层技术。

2.1.5.2 Spark

Spark 是 UC Berkeley AMP Lab 所开源的类 Map/Reduce 的通用的并行计算框架。Spark，拥有 Map/Reduce 所具有的优点，但不同于 Map/Reduce 的是，Job 中间输出结果可以保存在内存中，从而不再需要读写 HDFS，因此 Spark 能更好地适用于数据挖掘与机器学习等需要迭代的 Map/Reduce 的算法。

ALEIYE 平台使用 spark 作为在实时分析的技术可以用于分析 TB 级的数据实时分析，并将数据流与数据挖掘算法结合，抽象为一个可通过定义即可完成采集，分析，训练的自动化过程。

2.1.6 产品价值

通常企业产生海量数据后，首先从业务的角度出发对数据进行管理，相关部门选择要解决和产生的业务场景。针对需求处理和采取整合这些场景需要的大数据，从而进行分析。其次，直接产生的价值需要与已有的客户关系管理、客户交易等数据进行结合和关联，从而为企业产生总体的关键价值效益。第三，整个企业要建立大数据分析的支持体系、分析的文化、分析数据的人才，彻底形成企业对大数据的综合管理、探索、共识。第四、随着大数据探索范围的扩大，企业要建立大数据的标准。最终，建成企业“统一数据平台”从各类所需的多元的结构化数据源建立整合能力（采集、存储、粗加工）。

ALEIYE 数据平台，帮助企业减少对数据管理步骤，依托于 ALEIYE 数据平台，逆向思维，通过数据推动企业业务，帮助企业在海量数据中找到新的业务需求及业务新的增长点，从而快速带动企业对大数据的分析体系、分析的文化、分

析数据人才的储备的建设。

ALEIYE 数据平台具备处理多源异构数据的能力，可以帮助企业减少多数据源和跨部门数据整合工作，从而顺利的从业务点到整个企业对大数据需求的跨度，减少企业对数据管理建设的周期，降低企业对数据管理平台建设的人力成本。

ALEIYE 数据平台还可以帮助企业建立数据标准，统一的数据格式、采集方法、使用方式等，设定一个共享的愿景和目的，然后按照阶段化的目标去实现。最终，通过新业务和数据，扩展 ALEIYE 数据平台，从而实现数据推动新业务，新业务推动技术的闭环模式，帮助企业建成统一的数据平台，实现“针对正确的人，在正确的时间，正确的方式，提供正确的信息”的目标，形成企业智慧型管理模式。

第3章 Aleiye 使用手册

3.1 功能列表

模块	功能	功能点	功能描述
添加数据	上传方式	文件上传	文件上传格式支持：zip、gz、rar、txt、tar.gz、tar、bzip2、gzip、pack200、xz、z、lzma、7z、sz
		采集器	采集器支持格式：文本文件
		FTP 上传	FTP 上传格式支持：gz、zip、文本文件
		Syslog 上传	Syslog 文件
	数据预览	自定义数据	对于无标准格式的数据进行时间戳和换行格式的交互性配置。并可以在数据配置的过程中，能够实时看到配置后的结果数据。
		表格数据	对于表格数据的标准格式数据，无需填写正则表达式，通过交互实现字段的切分和字段名称的匹配。并可以在数据配置的过程中，能够实时看到配置后的结果数据。
检索	SQL 搜索	告警	支持通过 SQL 语句进行查询功能，对搜索结果可以进行可视化编辑。并保存到告警
		报表	

		仪表盘	及报表，同样可以通过仪表盘，查看实时结果。
	搜索功能	告警	使用 Aleiye 搜索命令，可通过使用关键字、短语、字段、布尔表达式和比较表达式来准确指定您想要从 Aleiye 索引检索到的事件。并保存到告警及报表，同样可以通过仪表盘，查看实时结果。
		报表	
		仪表盘	
数据管理	数据源管理	采集器管理	对通过采集器采集的数据源进行管理，可以对采集器下的路径进行开始/停止和删除的操作
		文件管理	对文件上传的记录进行删除操作。
		FTP 管理	对 FTP 上传的数据进行编辑修改和删除操作。
用户管理	修改密码		可以对已有密码进行修改。

3.2 用户操作说明

3.2.1 鉴权和登陆

Aleiye 是一种 WEB 服务，用户可以通过浏览器打开 Aleiye 登录页面。地址为 www.aleiye.com/de，所有 aleiye 用户需要先通过鉴权后登

陆进入系统。

如图 1-1，获取鉴权信息，用户需输入鉴权码点击提交。

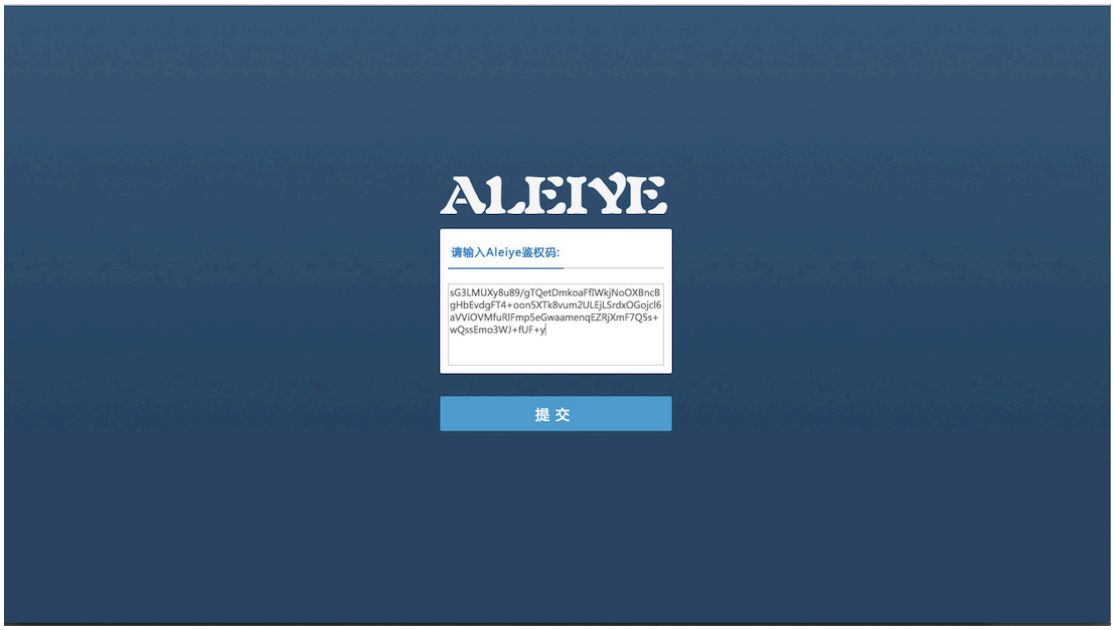


图 1-1

1-1

如图 1-2 用户通过输入用户名和密码进入，如果用户名和密码输入正确可以进入应用，否则无权进入。点击“忘记密码”按钮可重设或找回密码。

图 1-2 用户登录界面

3.2.2 首页

图 2-1

登录成功后，页面跳转至 Aleiye 首页，如图 2-1，在首页界面显示数据摘要、登陆情况、联系信息以及 Aleiye 应用。

如图 2-2，数据摘要界面显示系统应用总事件个数、热点数据保存周期、存储使用量和已开启应用个数。登录情况界面显示用户最后一次登录 IP 和登陆时间，联系我们界面显示 Aleiye 的联系信息。

图 2-2

如图 2-3，应用界面显示 Aleiye 平台所有应用，当应用已开启时，应用界面为高亮效果，未开启时，界面为灰。

在应用框显示应用状态，功能介绍。用户可以点击按钮选择进入应用或者添加数据。

图 2- 3

3.2.3 用户信息

图 3-1

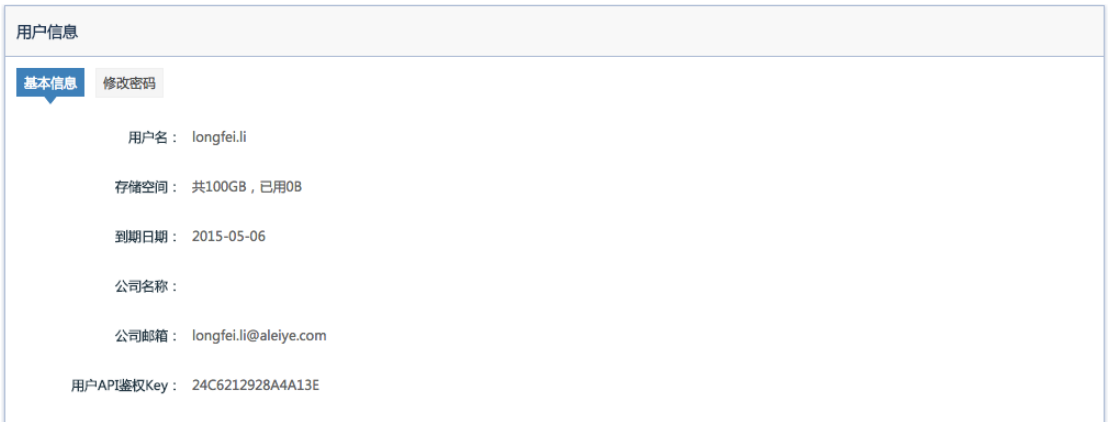


图 3-2

点击导航上方的用户管理（如图 3-1）后，进入用户信息页面，基本信息展示用户基础信息，如：用户名、存储空间、到期日期、公司名称、公司邮箱和用户 API 鉴权 Key（如图 3-2）。

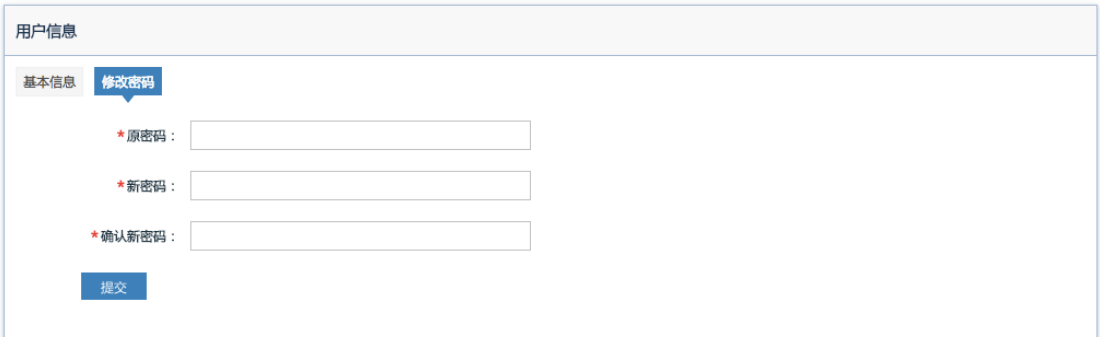


图 3-3

点击修改密码后，可对已有密码进行修改（如图 3-3）。

3.2.4 添加数据

图 4-1

在使用 Aleiye 为您提供的多种应用前，需要您为每个应用上传相关数据。

点击应用下方的“添加数据”（如图 4-1），便可以添加需要 Aleiye 分析的数据了。

Aleiye 为你提供三种上传数据方式：采集端上传、文件上传和 FTP 上传，可以根据您的实际需求，进行选择。（如图 4-2）

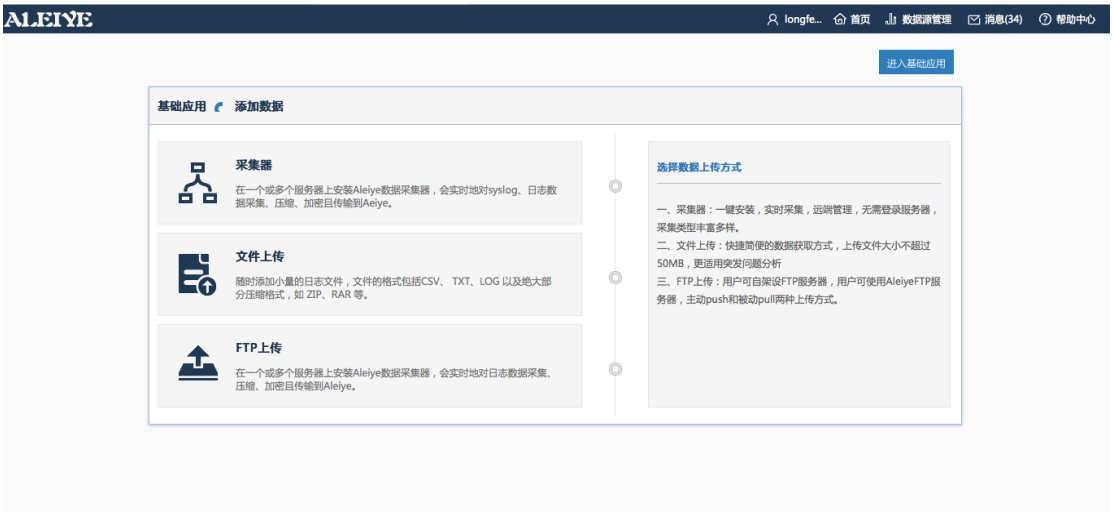


图 4-2

3.2.4.1 采集器

用户可以安装采集器进行远程管理、实时采集数据。采集器上传操作流程如下：

采集器安装

使用数据采集器方式添加据时，需要在数据源服务器上安装 Aleiye 数据采集器以及运行采集器所需的 JDK 环境。步骤如下：

- 下载安装 JDK

Aleiye 要求 JDK 版本最低至少为 java_1.6.0_32。下载完成后进行安装，并且配置 JAVA 的环境变量。（下载 JDK 详见附录一）

- 下载数据采集器（collector），

如图 4.1-1，选好要开启的应用后，点击右下方的添加数据后，选择采集器，点击页面右下方“下载采集器”按钮进行下载；

图 4.1.1-1

采集器下载完成后进行采集器安装。

◆ 安装并启动数据采集器

当服务器操作系统为 Linux 时，安装启动步骤如下：

a、解压下载后的采集器安装包 collector_2.1.zip，命令为:unzip collector_2.1.zip，解压后的文件夹名称为 colletor_2.1;

b、进入解压后的 collector_2.1 目录，启动采集器。命令为：sh startup.sh ;

c、查看采集器是否正常启动。命令为：ps -ef | grep collector。

当服务器操作系统为 Windows 时，安装启动步骤如下：

a、利用如 WinRar 等解压工具进行解压操作;

b、运行 collector_2.1 目录下的 startup.cmd 即可。

采集器采集配置

每个采集器对应一台数据源服务器，对应采集服务状态有三种：正常、未运行以及异常状态。初始状态为异常状态，需要对数据文件进行配置。当安装在数据源服务器上的 Aleiye 数据采集器启

动成功后，便可在配置记录里看到数据采集记录。包括数据采集主机名、IP 地址、拥有者以及日志文件路径个数。（如图 4.1.2-1）

4.1.2-1

Aleiye 可以配置多个类型日志，配置后会在路径个数上进行计数。在数据源服务器上的采集器服务确认正常启动后，需要对日志类型、数据源路径做如下的配置操作：

- 在采集器列表页面中，已配好的采集器，会出现添加数据集按钮，点击添加数据集，进入添加数据配置。（如图 4.1.2-1）
- 当进入添加数据配置页面后，可以选择数据预览模式，也可以跳过数据预览模式，数据预览模式需要上传数据样本，对其进行预览模式下的数据配置（详见数据预览），当点击跳过数据预览并点击确认，进入选择采集方式（如图 4.1.2-2）

图 4.1.2-2

◆ 用户可以选择添加数据集或添加 syslog 方式采集数据。

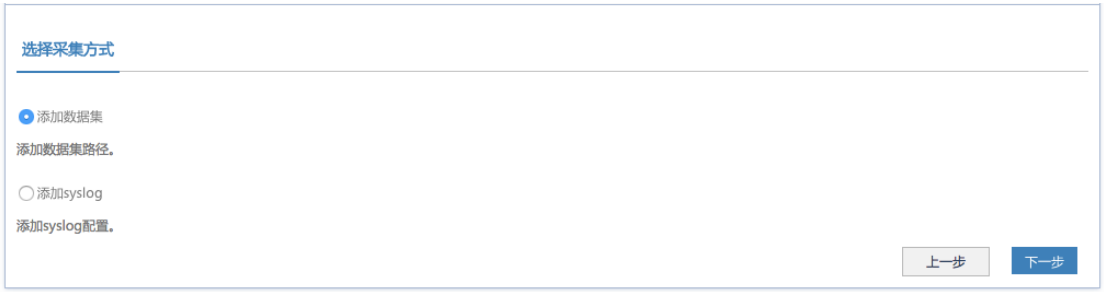


图 4.1.2-3

a、当选择添加数据集时：

在添加数据集页面用户需进行相关配置，详见附录二。

b、当选择添加 syslog 时：

采集方式选择添加 syslog 后，点击下一步进入 syslog 配置页面， 如图 4.1.2-6，syslog 协议可选 UDP 或 TCP，点击确认及完成 syslog 上传配置。

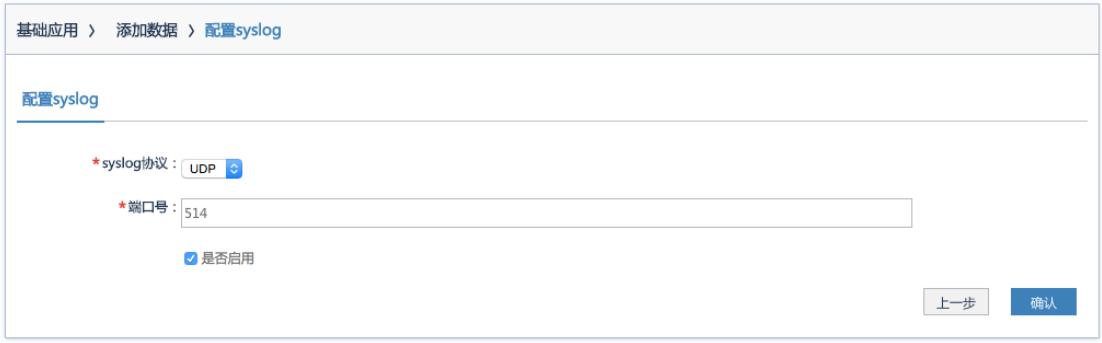


图 4.1.2-4

3.2.4.2 文件上传

Aleiye 可以将数据文件直接上传，文件类型可以有 Apache error logs、Apache Web access logs、Syslog，还可以自定义文件类型。当要上传多个文件时，可压缩成压缩包进行上传，Aleiye 支持绝大多数常用压缩格式，但是在压缩包里 Aleiye 不允许有文件夹。文件上传流程如下：

图 4.2-1

当选择文件上传方式后，点击“选择文件”按钮进行文件选取，文件格式包括 CSV、TXT、LOG 以及如 ZIP、RAR 等绝大部分压缩格式文件，并且文件大小不能超过 50MB，确定选取将要上传的文件，点击下一步。（如图 4.2-1）

用户可选择进入或跳过数据预览。（数据预览内容详见数据预览章节）

当跳过数据预览后，进入文件上传配置页面，定义数据集名称，选择日期格式和所在时区；选择或者自定义日志类型，当日志

类型选择自定义时，正则表达式须手动进行录入；输入部分日志样本，点击“验证”按钮来验证输出内容是否正确，如果显示“正则解析出错”，请检查以上输入内容及格式是否正确；若验证通过，请点击“保存”，待弹出页面提示保存是否成功。（如图 4.2-2）

图 4.2-2

3.2.4.3 FTP 上传

Aleiye 平台可以通过 FTP 协议向 Aleiye 传输数据。点击 FTP 上传方式，用户可使用 Aleiye 的 FTP 服务器，也可使用自架设 FTP 服务器，进行数据上传。

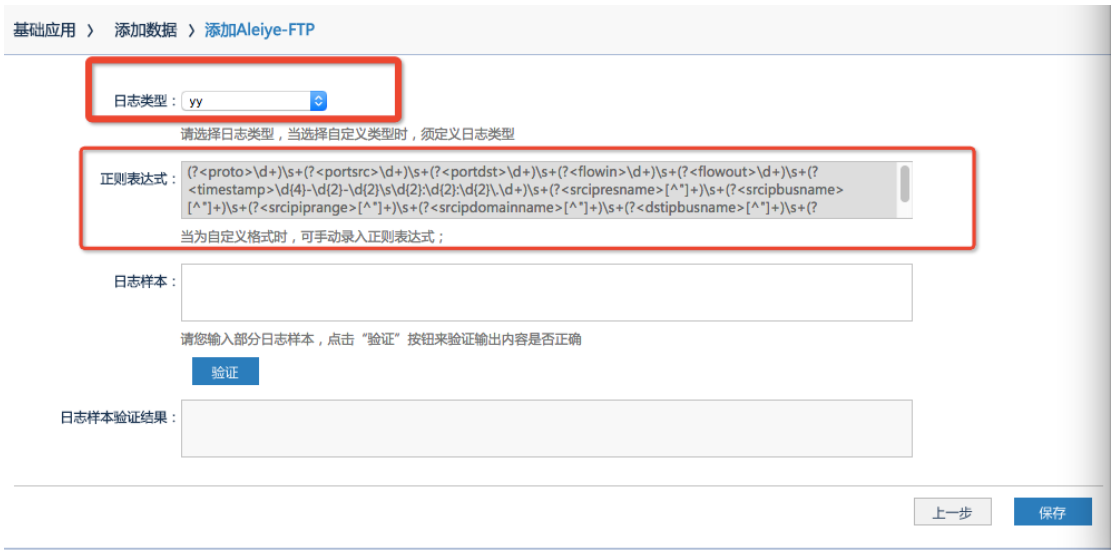
- 选择 Aleiye-FTP 服务器上传数据时：

图 4.3-1

下一步如图 4.3-2，展现 FTP 服务的地址、端口号、用户名和密码。

图 4.3-2

填写数据集名称和 FTP 目录，点击下一步进入对数据类型的配置。（如图 4.3-3）



4.3-3

数据类型配置页面中，选择已有的数据类型或建立新的数据类型，保存，显示保存成功。（如图 4.3-4）

4.3-4

进入基础应用，进入搜索页面。

用户可选择使用任意 FTP 工具，连接到 FTP 服务器（用户可以在数据源管理 ftp 一栏找到配置好的目录）。

FTP 的传输模式设置为“主动模式”，如果是被动模式有可能在连接的时候出现目录读取失败，导致无法登陆 FTP 服务器。

登陆 FTP 后，会在用户名目录下看到刚刚在 FTP 配置过程中填写的目录。（如图 4.3-5）

文件名	文件大小	文件类型	最近修改	权限	所有者/组
..					
kongxp		目录	2015/02/10 1...	drwxr-xr-x	501 501
lilongfei		目录	2015/02/07 0...	drwxr-xr-x	501 501
sdf		目录	2015/02/11 0...	drwxr-xr-x	501 501
ssss		目录	2015/02/10 1...	drwxr-xr-x	501 501
testftp		目录	2015/02/14 1...	drwxr-xr-x	501 501
wer		目录	2015/02/10 0...	drwxr-xr-x	501 501
ywt1		目录	2015/02/10 0...	drwxr-xr-x	501 501
ywt33		目录	2015/02/10 0...	drwxr-xr-x	501 501
yylog		目录	2015/02/09 1...	drwxr-xr-x	501 501
yytable		目录	2015/02/10 1...	drwxr-xr-x	501 501

图 4.3-5

把文件上传到此目录中，会出现文件瞬闪然后消失，表示文件被系统发现并开始入库。

文件上传后可进行验证：

在基础应用搜索界面中数据输入 A_logtype:”yy”（FTP 数据集配置步骤中输入的日志类型），

选择业务时间，如果没有业务时间选择当前时间，出现检索结果。表示 FTP 入库成功。

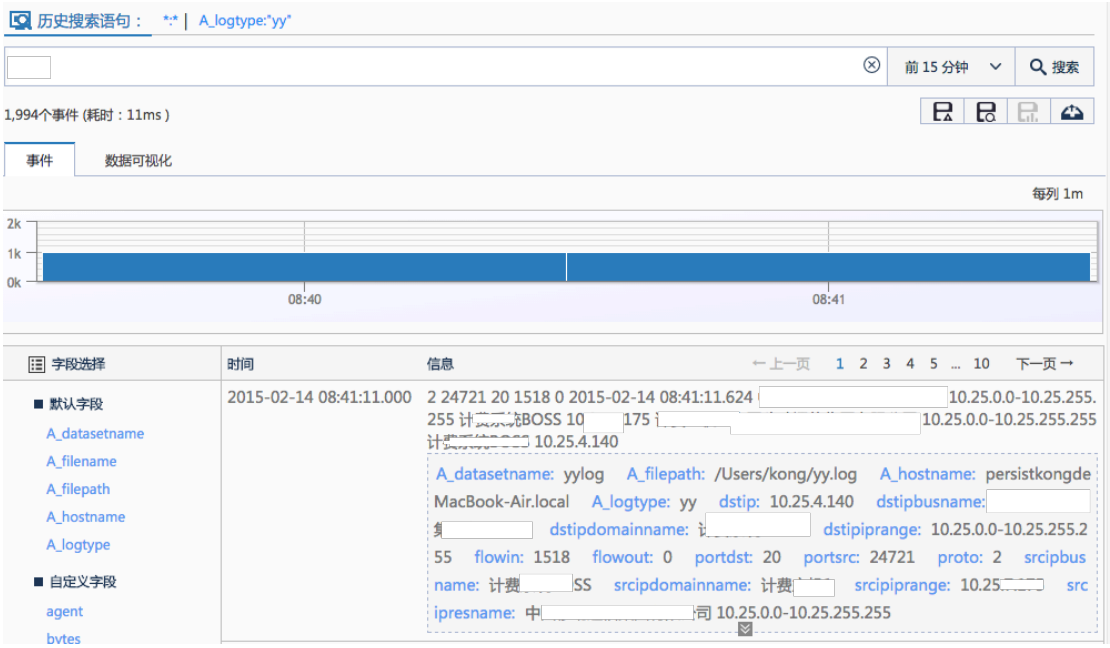


图 4.3-6

以后通过脚本或人工，定时将数据上传至这个 FTP 目录中即可完成数据入库。

◆ 选择自定义 FTP 服务器上传数据时：

选择自定义 FTP 即自己架设 FTP 服务器，通过点击“添加自定义 FTP 服务器”按钮，进入数据预览页面。用户可选择进入或跳过数据预览。（详见数据预览）

如图 4.3-7,点击跳过数据预览页面，用户需填写数据及名称、端口号、用户名及密码、ftp 地址和路径等信息。

图 4.3-7 数据配置

数据配置页面用户需填写数据集名称、端口号、FTP 地址、目录以及用户名和密码等信息，并选择日期格式、所在时区。点击下一步，进入数据配置信息页面。（相关配置方法详见附录二）

3.2.4.4 数据预览

图 5-1

当前版本，Aleiye 数据平台支持三种上传方式，选择任意一种上传方式上传数据时，用户都可以选择数据预览功能，通过数据预览，可以很直观的对数据进行上传配置。

当选择数据预览时，需要用户上传数据样本，样本数据大小为 10MB 以内，以便对数据进行实时配置。

图 5-2

数据上传成功后，点击确认，进入数据预览页面（如图 5-3）。

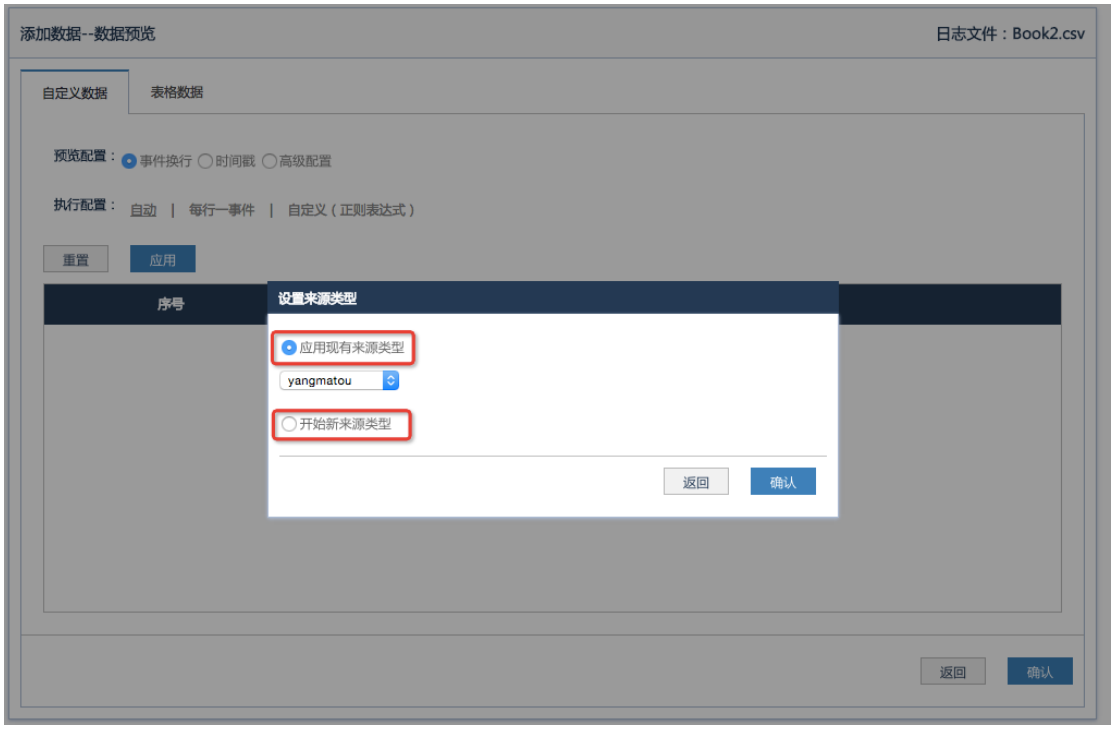


图 5-4

当进入数据预览页面，弹出浮层，提供两种业务选择：应用现有数据类型和开始新数据类型，当选择应用现有来源类型，系统会把已上传的数据，按照之前保存的数据切分类型展示，如果选择开始新来

源类型，会按照系统默认样式对样本数据进行切分。（如图 5-4）

3.2.4.5 自定义数据

自定义数据功能主要针对无标准格式的数据进行时间戳和换行格式的交互性配置。并可以在数据配置的过程中，能够实时看到配置后的结果数据。

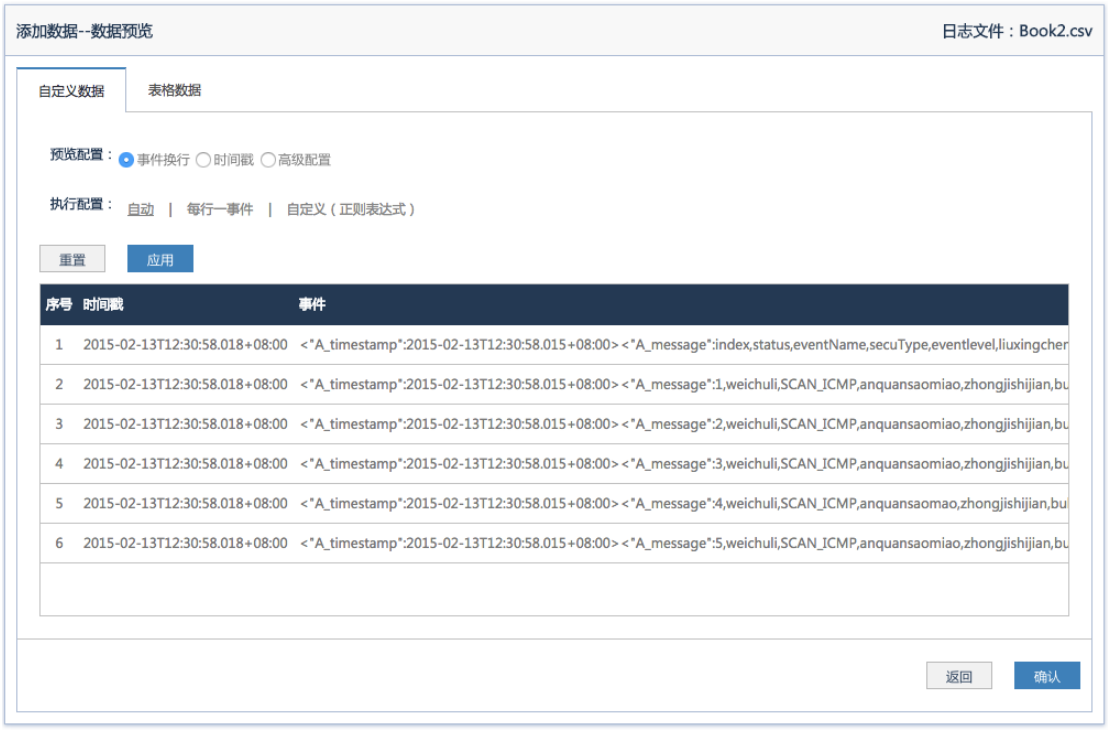


图 5.1-1

事件换行：可以对样本数据中的事件进行定义，Aleiye 数据平台，定义为一行数据为一个事件，所以，用户可以对样本数据进行自定义换行配置。

- 自动：系统默认样本数据中只要有时间戳，即为一行事件。
- 每行一事件：系统默认样本数据中，一行数据既为一个事件。
- 自定义（正则表达式）：如果上述两种不能满足用户对数据换行的

配置，可以通过正则表达式进行数据换行配置。（如图 5.1-2）

图-5.1-2

时间戳：对样本数据中的时间戳进行自定义配置，样本数据中，如果没有时间戳，那么 Aleiye 按照数据入库时间给数据生成时间戳。（如图 5.1-3）

- 自动查找时间戳：如果样本数据中有时间戳，系统会按照数据中的时间戳为准，如果数据中没有时间戳，系统会以数据入库的时间为时间戳。
- 使用当前时间戳：不管数据中是否时间戳，如果选择此选项，系统会以样本数据入库的时间为时间戳。
- 自定义（正则表达式）：时间戳的定义，可以通过正则表达式进行自定义配置。

图-5.1-3

日期格式：时间戳的日期格式，可进行配置，系统会给三种通用

格式，如果不能满足用户需求，可以通过自定义时间格式进行配置。（如图 5.1-4）

图-5.1-4

3.2.4.6 表格数据

表格数据针对标准格式的数据，无需填写正则表达式，通过交互实现字段的切分和字段名称的匹配。并可以在数据配置的过程中，能够实时查看配置后的结果数据。（如图）

图-5.2-1

表格数据中时间戳与自定义数据中的时间戳配置规则一样。

高级配置：对表格数据类型，进行自定义配置，包括字段的切分、拆分和合并等功能。

字段配置：可以根据默认的字符，对表格进行切分，如空格、逗号等，也可以自定义切分符。

图-5.2-2

数据展示：当数据按照切分符进行切分后，在表头上方，可对切分好的字段进行自定义命名（如图 5.2-3）

序号	时间戳	agent	field2	field3	f
1	2015-02-13 14:21:07.120	index	status	eventName	
2	2015-02-13 14:21:07.120	1	weichuli	SCAN_ICMP	anc
3	2015-02-13 14:21:07.120	2	weichuli	SCAN_ICMP	anc
4	2015-02-13 14:21:07.120	3	weichuli	SCAN_ICMP	anc
5	2015-02-13 14:21:07.121	4	weichuli	SCAN_ICMP	an
6	2015-02-13 14:21:07.121	5	weichuli	SCAN_ICMP	anc

图 5.2-3

字段拆分合并：当点击字段后，出现下拉菜单，在下拉菜单中，可选择拆分和合并两个功能，可以对当前选中的字段进行拆分或者是合并功能。

拆分：点击拆分后，可选择拆分规则和字段拆分字符，可对该字段进行自定义拆分（如图 5.2-5），拆分前和拆分后结果对比（如图 5.2-6）。

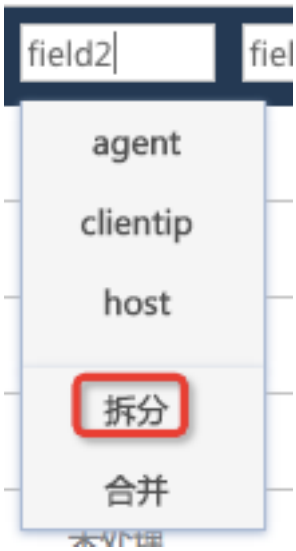
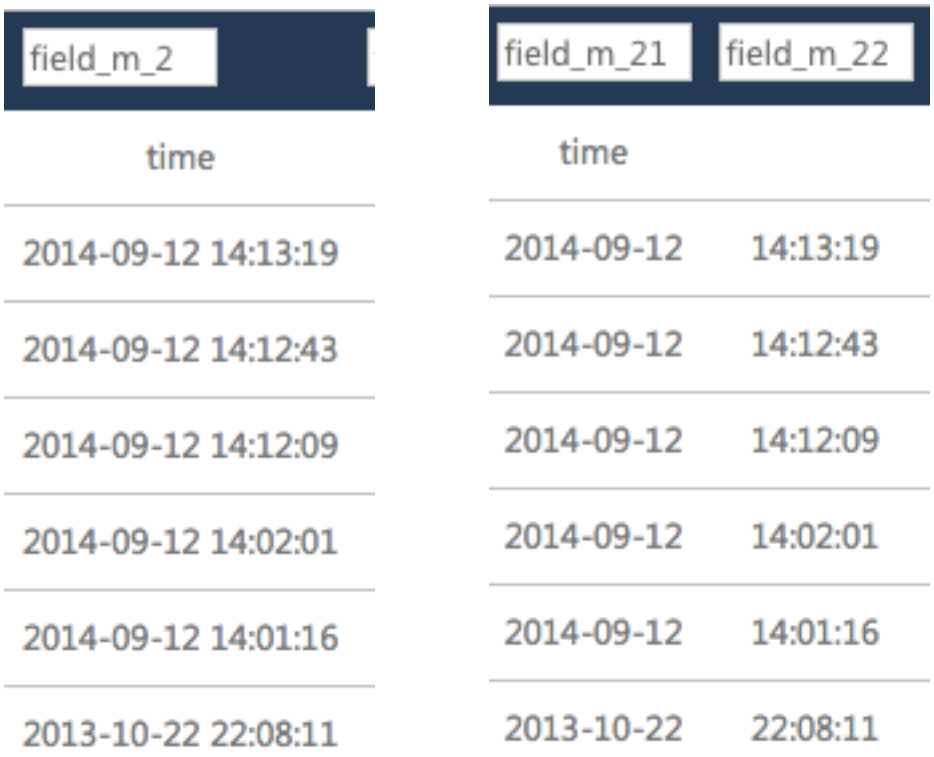

field2
agent
clientip
host
拆分
合并

图 5.2-4


字段拆分设置
拆分规则：
选择规则
字段拆分符：
空格
关闭
确认

图 5.2-5



拆分前　　拆分后

图 5.2-6

合并：当点击字段后，弹出下拉菜单（如图 5.2-7）。

如图 5.2-7

点击合并按钮后，各字段前增加多选框，可对多个字段进行合并，但合并必须为相邻字段（如图 5.2-8）。

如图 5.2-8

选择多个字段后，点击合并，弹出弹层，可选择字段合并符，对字段合并进行相应配置如图 5.2-9：

图 5.2-9

合并结果为图 5.2-10：

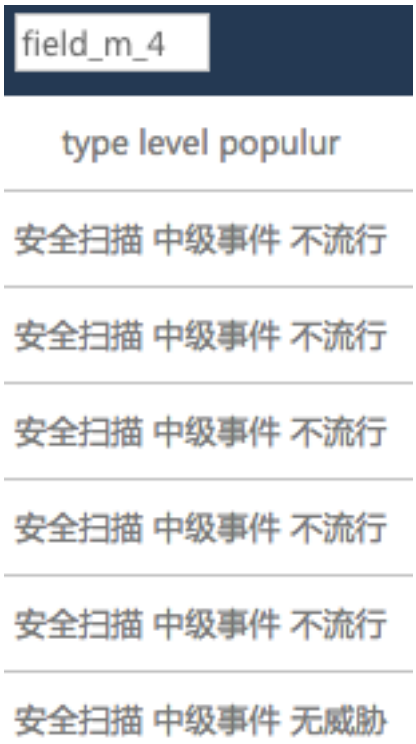


图 5.2-10

配置完毕后，点击确认，保存数据预览中的相应配置，并跳转到数据集配置（数据集配置见附录二添加数据配置信息）。

通过数据预览，对样本数据进行字段提取并对字段名称自定义命名，可以在检索中，快速精准的查询出结果，并可以将该类型进行保存，从而方便下次相同类型的数据进行复用，减少数据上传中的配置操作。

3.2.5 数据源管理

点击首页上方的“数据源管理”图标进入数据源管理页面如图 6-1，数据源管理页面提供采集器、文件上传、FTP 上传文件的详细信息展示和编辑、删除操作；

图 6- 1

数据源管理页面默认显示采集器信息，采集器信息列表中显示已添加采集器的信息，其中包括数据源主机名、数据源 IP 、路径数量、采集状态、采集器状态、应用范围。可点击“停止采集”或删除按钮对采集器进行操作。

其中：

路径个数：采集器已添加的路径个数；

采集状态：采集状态分为两种，对采集器添加路径后，当采集器正常采集数据时显示“采集中”否则，显示未采集；

采集器状态：采集器状态是指采集器的运行状态，分为正常、未运行、异常状态；

如图 6-2，点击采集器行首图标打开采集器路径列表，采集器列表显示数据的应用范围，也在列表中可以编辑和删除路径信息。

图 6-2

如图 6-3，点击“编辑”按钮弹出编辑弹窗，用户可编辑数据集或 syslog 信息。

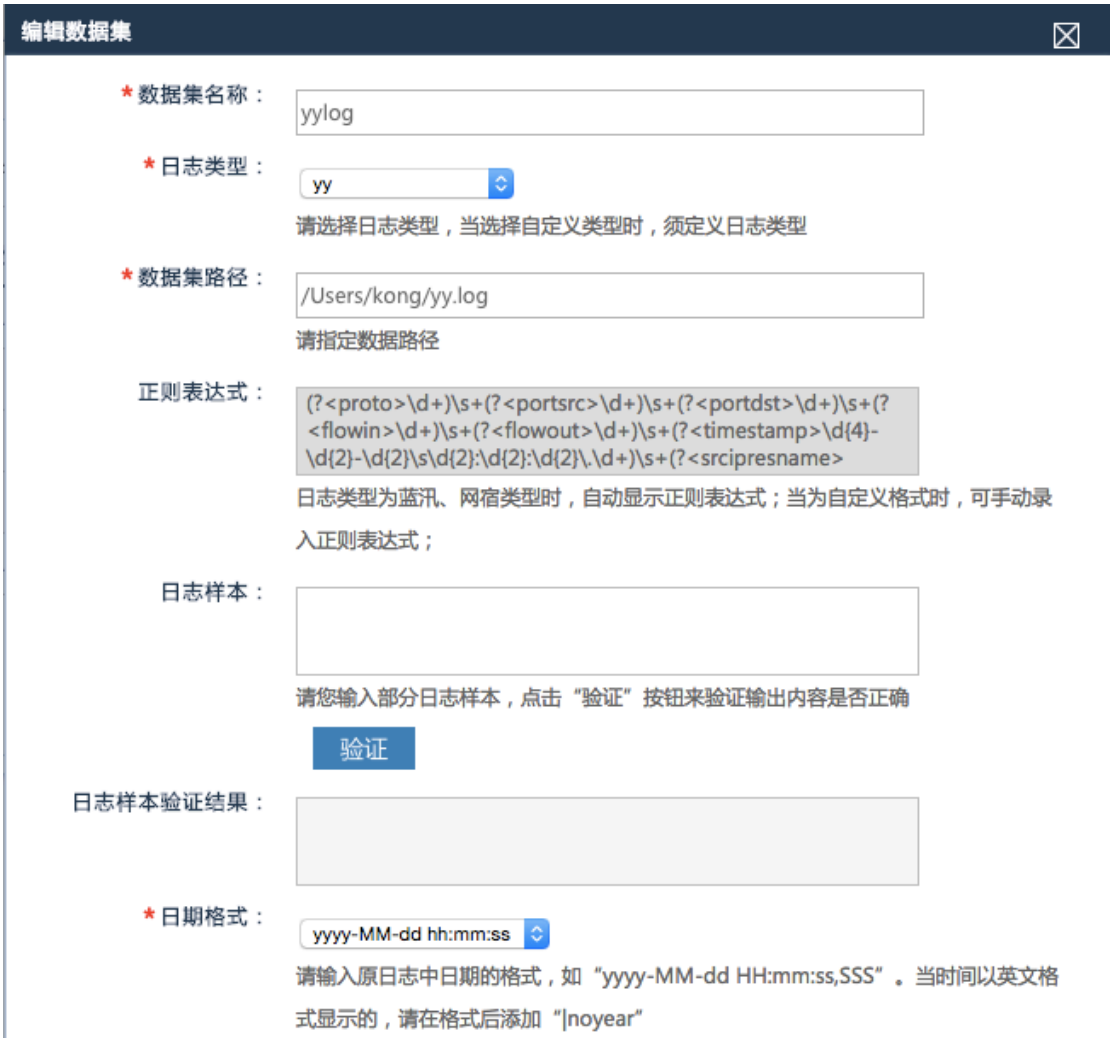


图 6-3

点击页面上方的数据上传方式图标可切换页面信息，如图 6-4，文件上传界面显示数据集名称、日志类型、文件名称、文件大小、上传时间、应用范围等信息。在操作栏中点击“删除”按钮可以删除本条信息。

图 6-4

如图 6-5，自定义 FTP 上传界面显示数据名称、类型、用户名、FTP 路径、应用范围等信息，点击“编辑”按钮可编辑自定义- FTP 服务器，点击“删除”可删除数据信息。

图 6-6

点击功能图标页面切换至 Aleiye- FTP 服务器界面，如图 6-6，Aleiye- FTP 服务器界面显示服务器信息，点击操作按钮可编辑或删除信息。

图 6-7

点击“刷新”按钮，可以页面刷新 。

3.2.6 基础应用

Aleiye 基础应用支持多种数据检索方式，使用户更高效、便捷的

获取信息，并以可视化的方式展现出来。

在应用中心界面点击基础应用框或“进入应用”按钮进入基础应用，基础应用分为搜索、报表、告警、SQL 搜索四个模块，点击页面上方的功能图标可以切换页面。

3.2.6.1 搜索功能

Aleiye 的搜索功能可以将 Aleiye 整合的不同源、不同类型的数据进行检索，以图表或报告的形式展示给用户。检索是通过输入关键字结合时间范围的方式，以满足不同业务对数据检索的需求。检索结果可以导出为 PDF、CSV 格式。

如图 7.1-1 所示搜索页面，按 Aleiye 的搜索语言，在搜索栏中输入搜索信息（搜索命令详见本标书<Aleiye 产品检索命令手册>），按回车键或点击搜索栏右端的搜索图标启动搜索。点击搜索栏右侧按钮打开下拉菜单，可选择预设或者自定义时间范围进行搜索（注：数据文件如果有时间戳，时间范围以时间戳为准，否则以入库时间为准）。Aleiye 默认搜索范围为“前 15 分钟”。点击上方的“添加数据”图标可以为该应用添加数据，点击“返回应用中心”可 返回至首页界面。

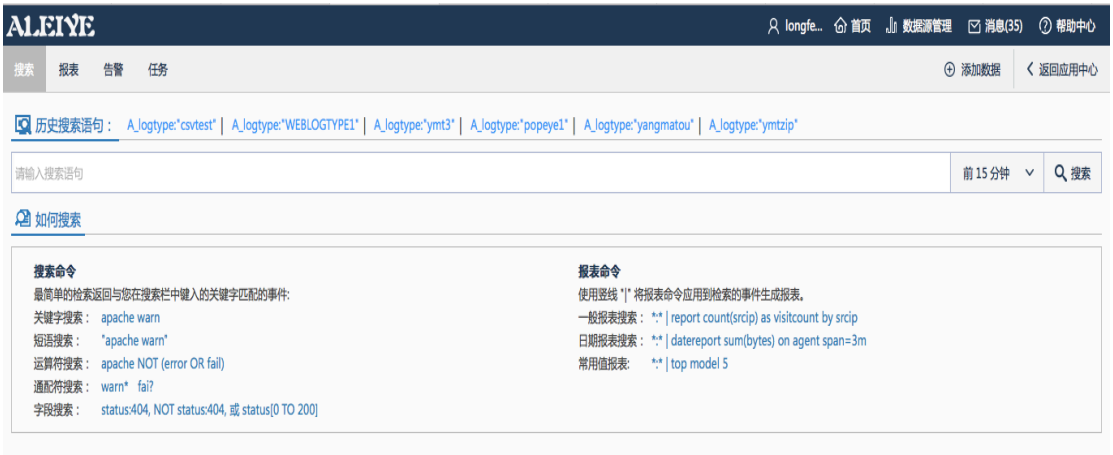


图 7.1-1

如图 7.1-2，点击搜索栏打开辅助搜索界面，辅助搜索提供日志类型、搜索历史、保存的搜索条件、保存的报表，可帮助用户快速搜索。其中，

日志类型：用户可选择一个或多个日志类型，帮助用户精准的查询到想要的数据。

搜索历史：系统可纪录用户近几次的搜索语句，最多保存五条搜索纪录。

保存的搜索条件：显示用户已保存的搜索命令。

保存的报表：显示通过搜索结果保存的报表，点击报表可重现报表结果。

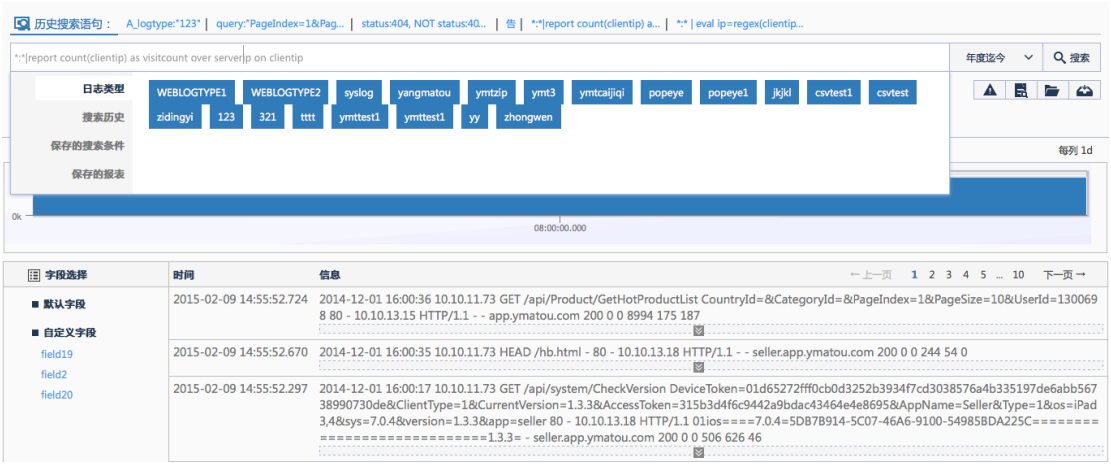


图 7.1-2

输入命令后点击“搜索”，如图 7.1-3，跳转至事件页面，此页面将显示搜索到的事件的统计视图和事件信息表，事件信息表中，字段选择列分为默认字段和自定义字段。

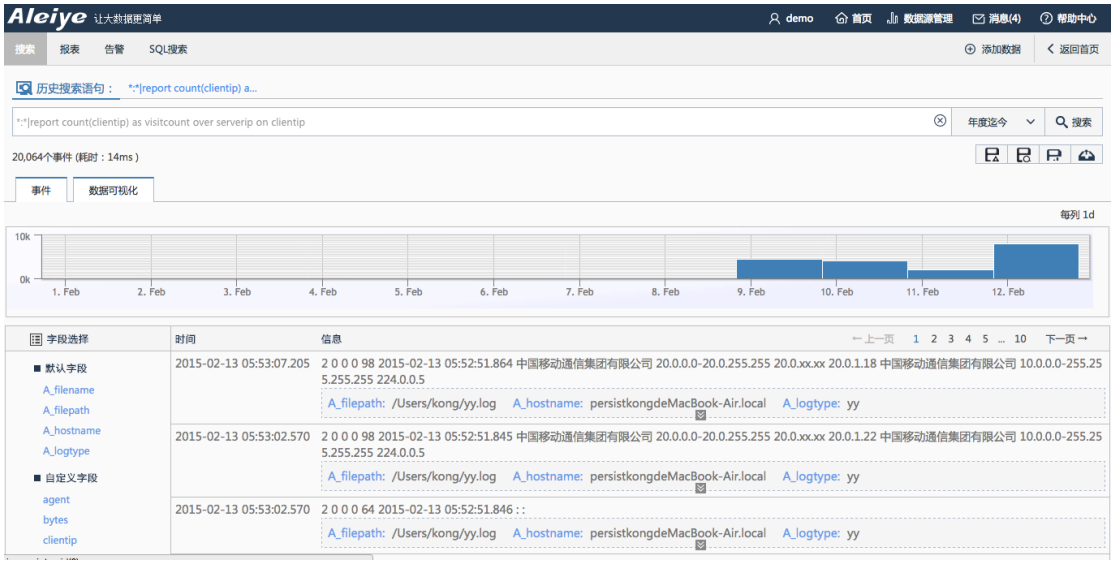


图 7.1-3

如图 7.1-4 所示，点击字段选择图标可选择字段进行展示，在页面中点击选中字段，可多选或者点击全部选中图标批量操作。其中“A_”字段为 Aleiye 默认字段，其余为用户上传数据自定义的字段。

其中，各字段解释如下：

A_filepath ： 采集路径 通过采集端采集文件有值对应 例如：/usr/aaa/bbb.log

A_filename ： 上传文件此字段有值 例如：my.log

A_logtype ： 日志类型

A_hostname ： 只有启用采集端 此字段有意义

A_datasetname： 数据集名称

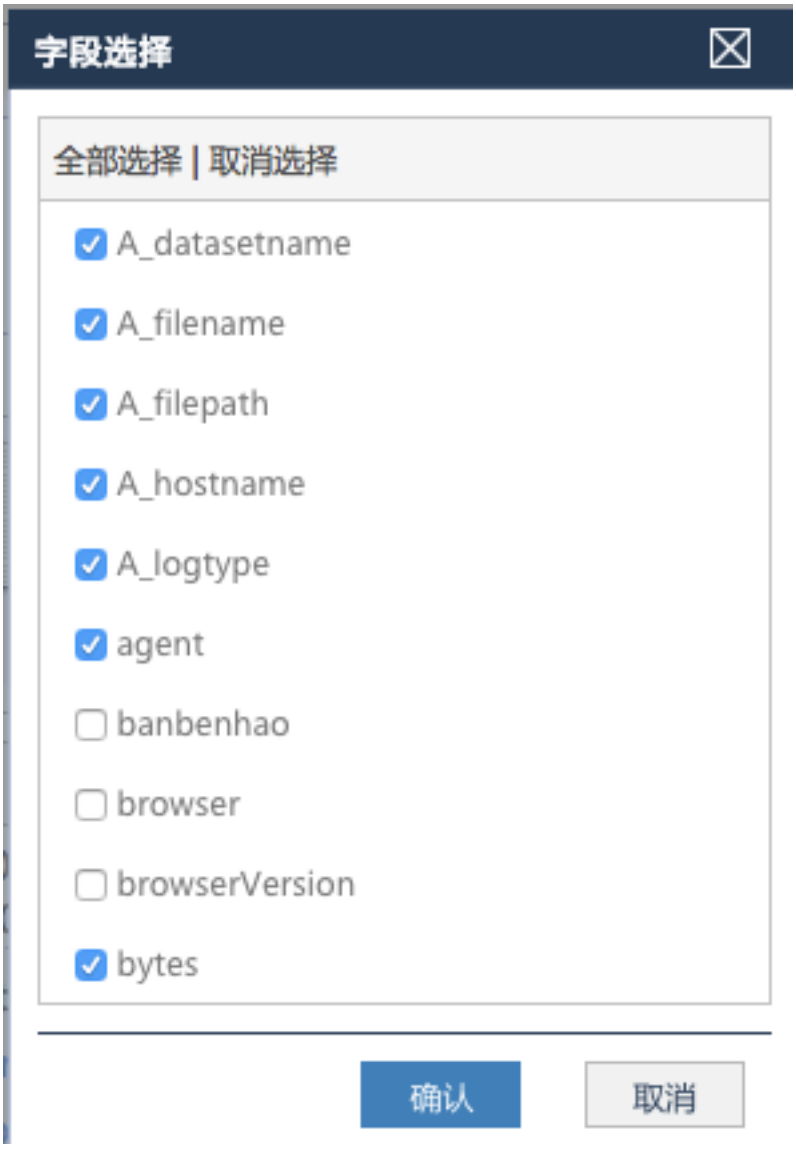


图 7.1- 4

点击字段名可弹出字段统计页面，如图 7.1-5 所示，在此页面显示字段 Top 值统计信息，“计数”为该字段下数据的个数，“%”为该条数据占该字段总数的比率。

图 7.1-5

如图 7.1-6 在事件列表中，点击信息栏下方的下拉图标显示事件信息详情。在事件信息列表中点击字段名，Aleiye 可根据字段名过滤事件信息。

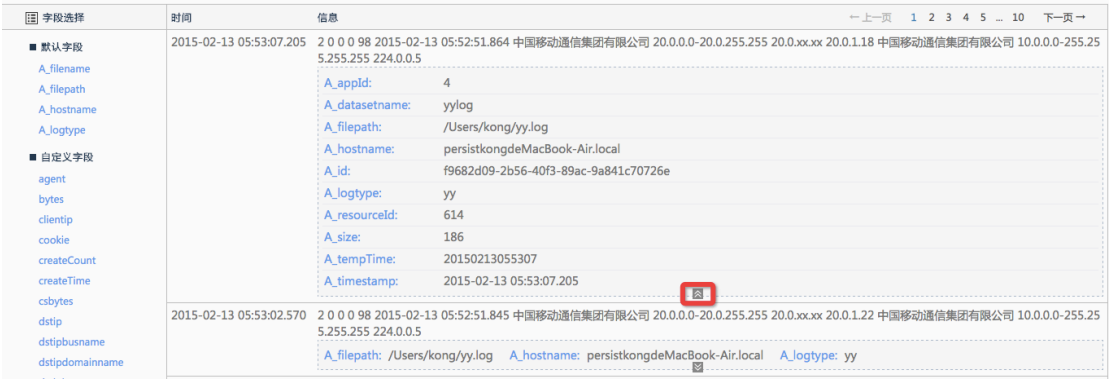
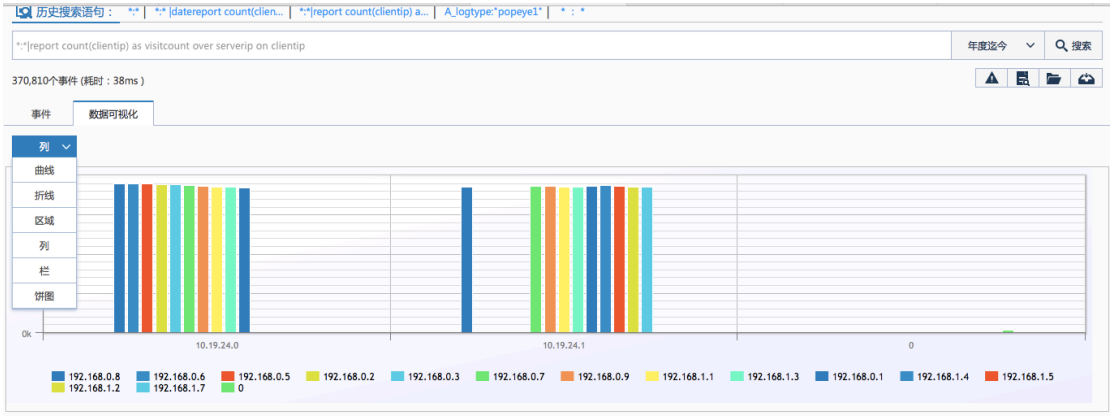


图 7.1-6

点击“数据可视化”图标可切换至数据可视化页面，将数据的各个属性值以多维数据的形式展示，如图 7.1-7，点击下拉菜单可选择不同的图形展示形式。



bb_serverip	bb_clientip	ss_count_visitcount
10.19.24.0	192.168.0.8	9484
10.19.24.0	192.168.0.6	9475
10.19.24.0	192.168.0.5	9461
10.19.24.0	192.168.0.2	9408
10.19.24.0	192.168.0.3	9406

图 7.1-7

如图 7.1-8，Aleiye 对搜索结果提供告警、保存搜索、保存报表、导出报告或数据等操作。

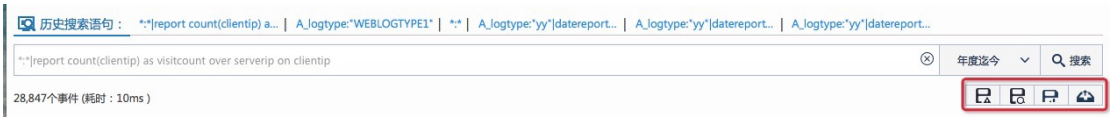


图 7.1-8

其中，

告警：点击告警图标，输入查询语句，设置周期和告警阀值等信息可保存至告警；

保存报表：将本次搜索保存为报表，可在报表页面查看或编辑已保存的报表；

保存搜索：常用的搜索语句和条件可以通过辅助搜索功能进行存储，方便用户快速搜索；

导出：搜索结果可以导出 PDF 和 CSV 格式的文件；

3.2.6.2 SQL 搜索功能

SQL 搜索功能模块支持标准的 SQL 语句，并将搜索结果以可视化的形式展现出来。点击切换至 SQL 搜索界面，如图 7.2-1

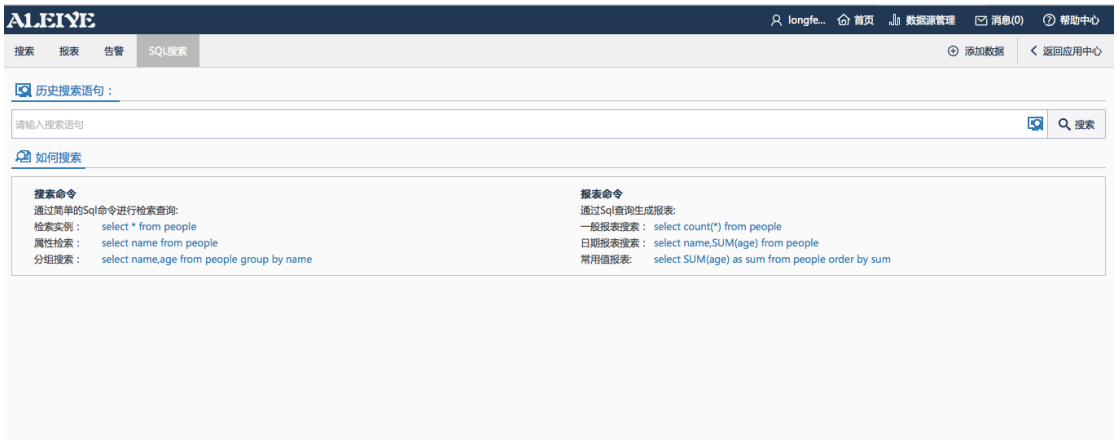
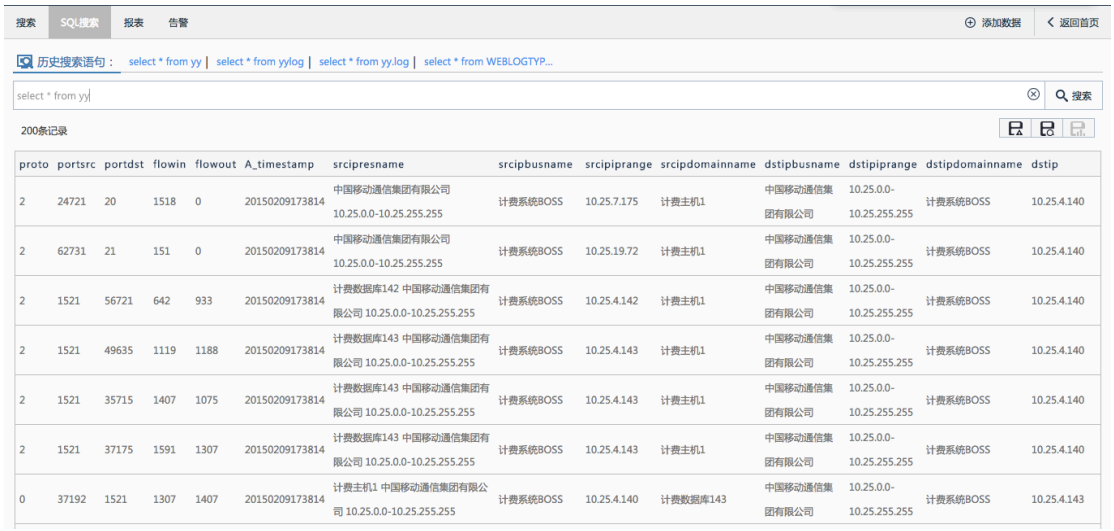


图 7.2-1

页面下方“如何搜索”栏列举用户常用搜索命令和报表命令。点击搜索栏，在弹出窗口可查看搜索历史、保存的搜索条件、保存的报表。

在搜索框中输入 SQL 语句可进行数据检索(SQL 语句参考《Aieiye 产品 V2.1 检索命令手册》)，如图 7.2-2，检索结果为表格后，可对表格进行可视化编辑。



proto	portsrc	portdst	flowin	flowout	A_timestamp	srcipresname	srcipbusname	srcipiprange	srcipdomainname	dstipbusname	dstipiprange	dstipdomainname	dstip
2	24721	20	1518	0	20150209173814	中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.7.175	计费主机1	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140
2	62731	21	151	0	20150209173814	中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.19.72	计费主机1	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140
2	1521	56721	642	933	20150209173814	计费数据库142 中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.142	计费主机1	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140
2	1521	49635	1119	1188	20150209173814	计费数据库143 中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.143	计费主机1	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140
2	1521	35715	1407	1075	20150209173814	计费数据库143 中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.143	计费主机1	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140
2	1521	37175	1591	1307	20150209173814	计费数据库143 中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.143	计费主机1	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140
0	37192	1521	1307	1407	20150209173814	计费主机1 中国移动通信集团有限公司 10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.140	计费数据库143	中国移动通信集团有限公司	10.25.0.0-10.25.255.255	计费系统BOSS	10.25.4.143

图 7.2-2

如图 7.2-3 所示点击“可视化编辑”按钮可弹出可视化编辑页面，用户可设置 x 轴 y 轴并选择图形的展现形式。

设置 x 轴：用户可定义 x 轴、编辑名称并选择图形策略，策略分为分组、线性、和时间三种形式。

设置 y 轴：用户可定义多个 y 轴，点击策略下拉菜单可选择图形展示策略。

图 7.2-3

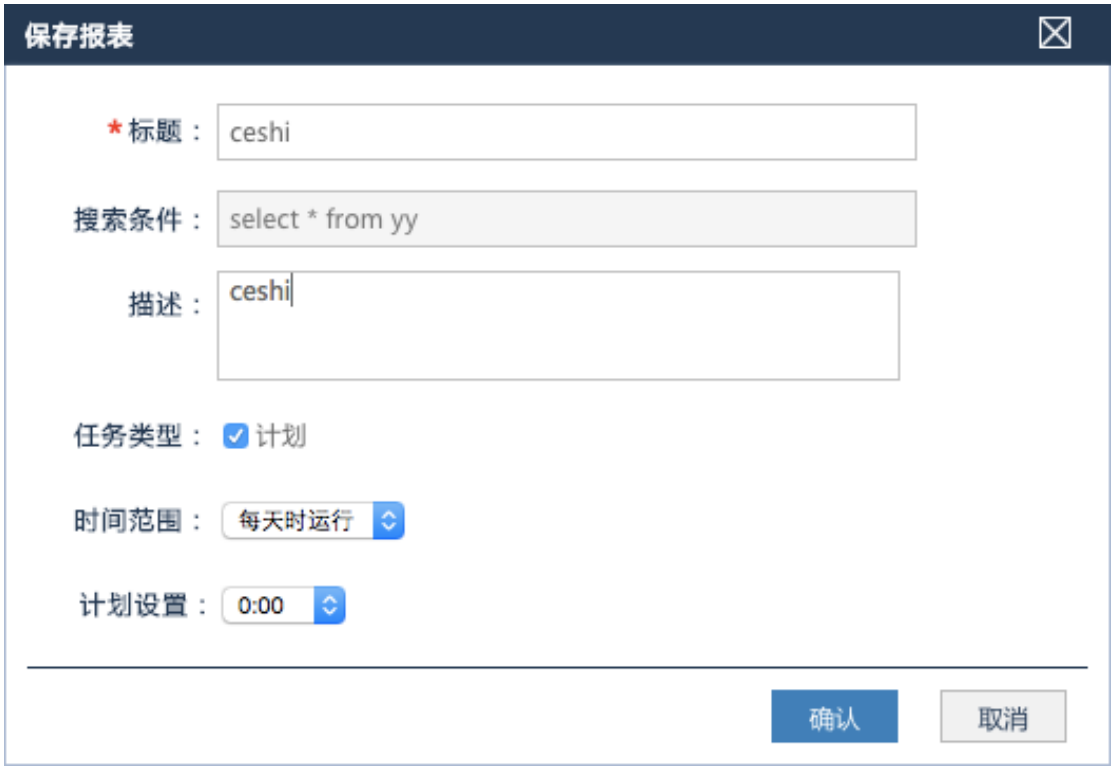


图 7.2-4

如图点击 7.2-4，SQL 搜索可以吧结果保存到报表中，点击“保存报表”图标可弹出保存报表弹窗，需定义报表标题、描述。点击选中计划框可开启计划任务,可选择时间范围如：每天运行、没周运行等，定期执行该搜索语句，从而实现计划性报表。

3.2.6.3 报表功能

报表功能模块显示以保存的报表，报表类型共分为两类报表，一类为 SQL 报表，一类为原语报表

SQL 报表：通过 SQL 语句检索出来的结果保存的报表为 SQL 报表，SQL。

原语报表：基于 Aleiye 自身的语言检索出来的结果保存的报表为

原语报表。

点击页面上方的功能图标切换至报表页面如图 7.3-1，报表页面显示报表标题、描述、报表类型、最后检索时间并提供在搜索中打开、编辑和删除等操作，可以在报表列表行首选中报表，也可多选或者点击上方的“全选/全不选”按钮批量删除。在页面上方搜索栏中输入报表名进行搜索。

点击报表标题或“在搜索中打开”按钮可跳转至搜索页面并自动添加至搜索栏进行搜索。

图 7.3-1

如图 7.3-2，点击“编辑”按钮弹出编辑对话框，可编辑标题和描述，查看搜索条件和时间范围。

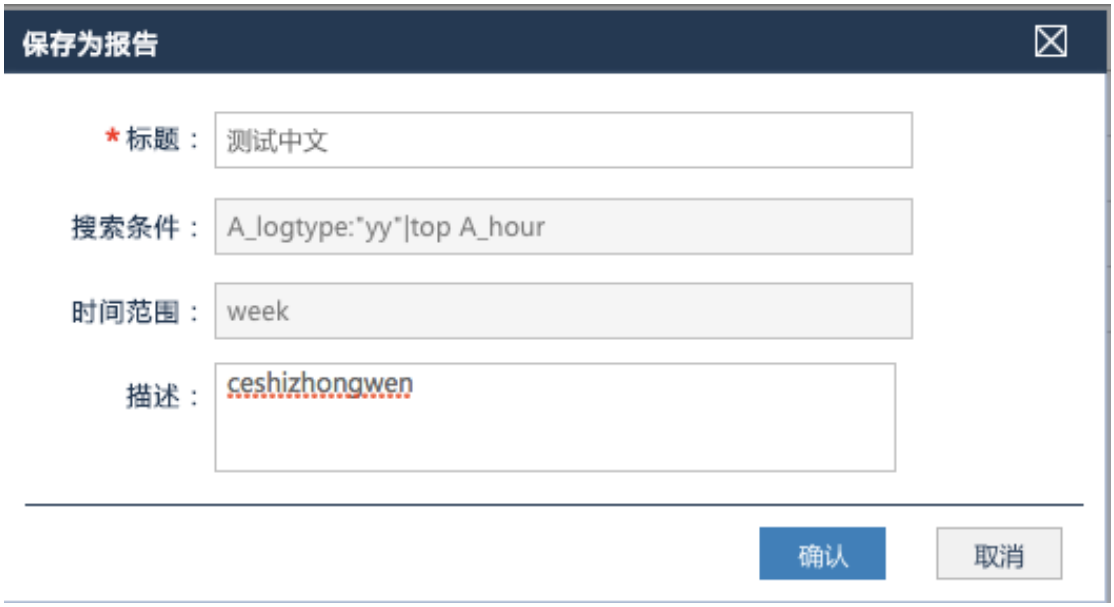


图 7.3-2

3.2.6.4 告警功能

告警功能模块显示已添加的告警信息，切换至告警页面如图 7.4-1，显示告警标题、周期、阀值等信息并提供添加、删除告警等操作。

图 7.4-1

点击信息列表前端选择框可进行单选或者多选，点击表头上方的“全选 / 全不选”图标可进行批量操作。点击操作栏可在搜索中打开、编辑或者打开告警记录等操作。

点击“添加告警”按钮跳转至告警配置页面，（如图 7.4-2）。

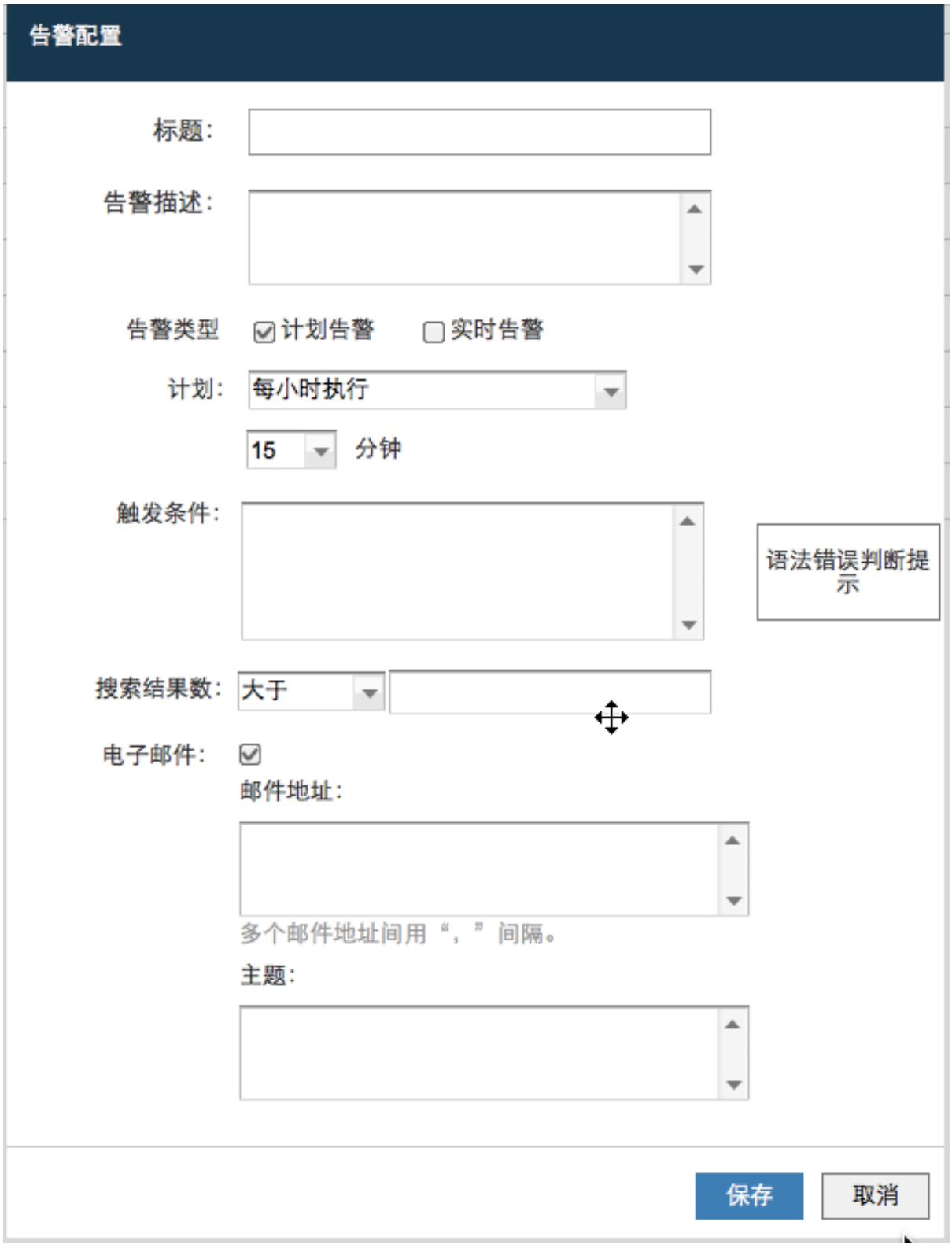


图 7.4-2

用户需要填写告警标题和告警描述，选择要添加的告警类型，告警类型分为计划告警和实时告警。(计划告警和实时告警分别在 7.4.1、

7.4.2 中作详细介绍，这里就不在赘述。）

如图 7.4-3 所示，点击编辑按钮可转到编辑告警页面，在此页面可编辑标题、描述、计划设置、告警阀值和邮件地址等信息。搜索语句和时间为不可编辑框。

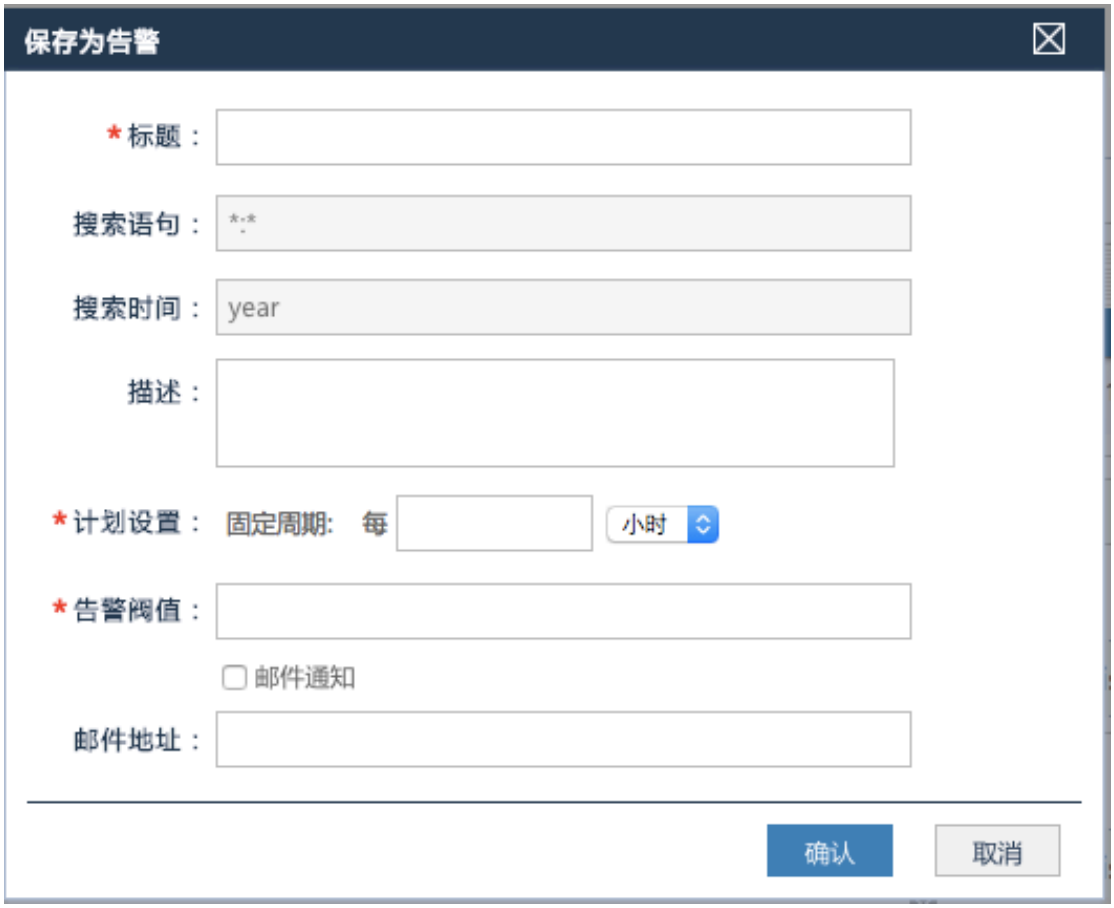


图 7.4-3

其中，

阀值：启动告警的临界值；

计划设置：启动搜索的频率，可设置为每小时、每天或者每月固定次数按搜索语句启动搜索。

用户也可设置邮件提醒，当用户选中电子邮件选择框时弹出邮件地址和主题框，邮件地址框可支持多个邮箱。多个邮箱间需用“,”间

隔。（如图 7.4- 4）

图 7.4-4

计划告警

计划告警可定期执行告警命令，用户点击选择计划告警框时，需要配置计划、触发条件、搜索结果数信息。（如图 7.4.1-1）

其中，

计划：告警执行周期，分别为每小时执行、每天执行、每周执行、每月执行和 cron 执行，cron 执行为用户自定义执行周期。

触发条件：通过输入命令来触发告警，用户在输入命令时需要有语法错误判断提示。

搜索结果数：对搜索结果数进行设置来启动告警，例如设置搜索结果数大于 100 时可启动告警。

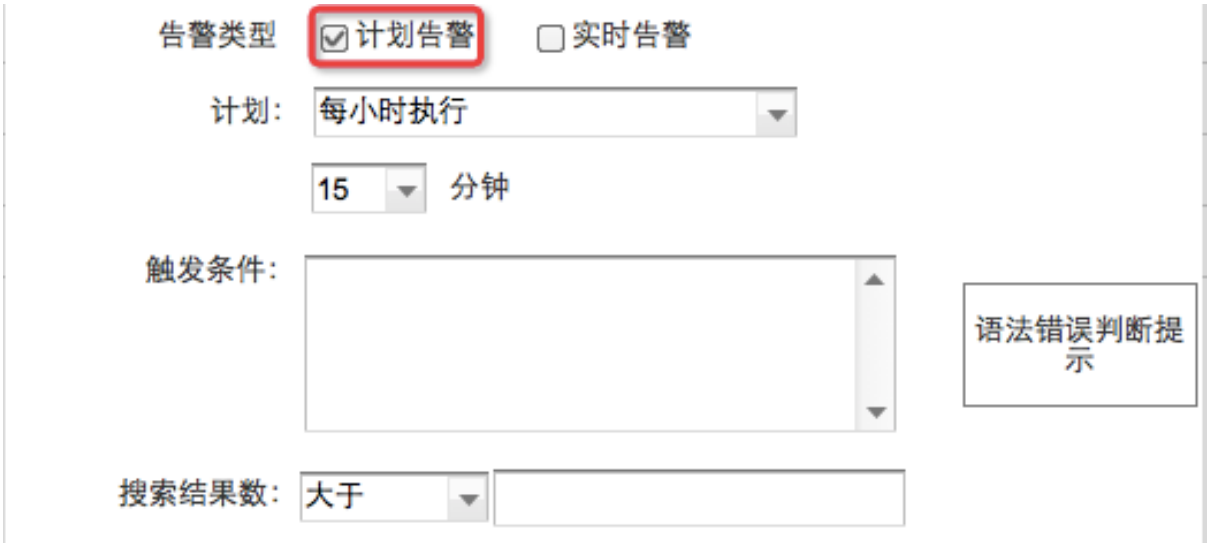


图 7.4.1-1

实时告警

用户可添加实时告警任务，当点击实时告警选择框时弹出实时告警配置页面，用户需配置时间窗口、数据类型、过滤条件、触发条件等信息。（如图 7.4.2-1）

其中，

时间窗口：

数据类型：用户在上传数据时为其定义的数据的类型。（可参考名词解释［数据类型］）

过滤条件：过滤条件分为“或”、“且”和“自定义”，用户可设置多个过滤条件。

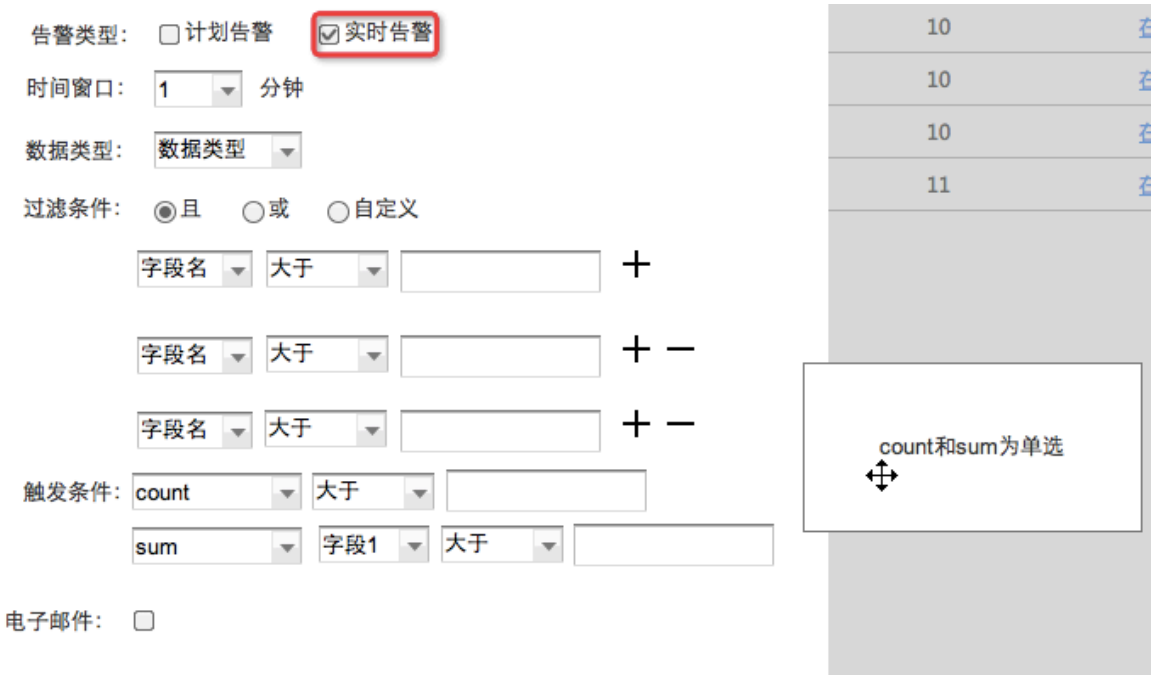


图 7.4.2-1

触发条件：用户设置触发条件来启动实时告警，触发条件分别为 count 和 sum，（注：count 和 sum 均为单选）

如图 7.4.2-2 所示，当用户选择自定义过滤条件时，需定义字段值和过滤条件表达式。

图 7.4.2-2

所有配置完毕后，点击保存，会弹出页面提示。

3.2.7 仪表盘

仪表盘应用可以将多个仪表、图表、报表等内容整合在一个页面上进行实时展示。

打开仪表盘应用，如图 8-1，仪表盘可显示多个报表。

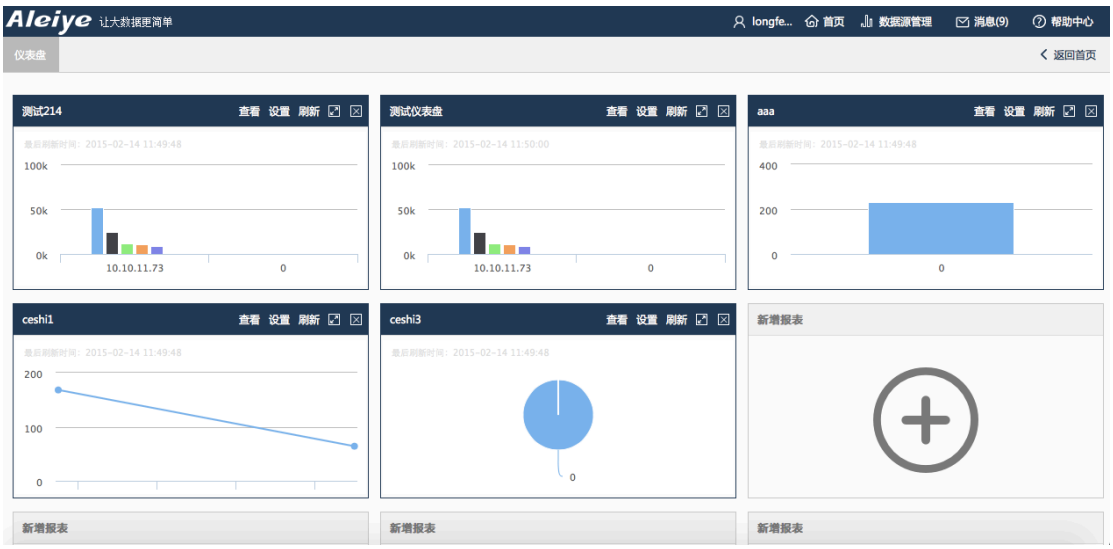


图 8-1

如图 8-2，点击“新增报表”框可添加报表，用户可选择以保存报表或自定义新报表。

选择以保存报表时，用户需定义标题名称、设置报表刷新周期。

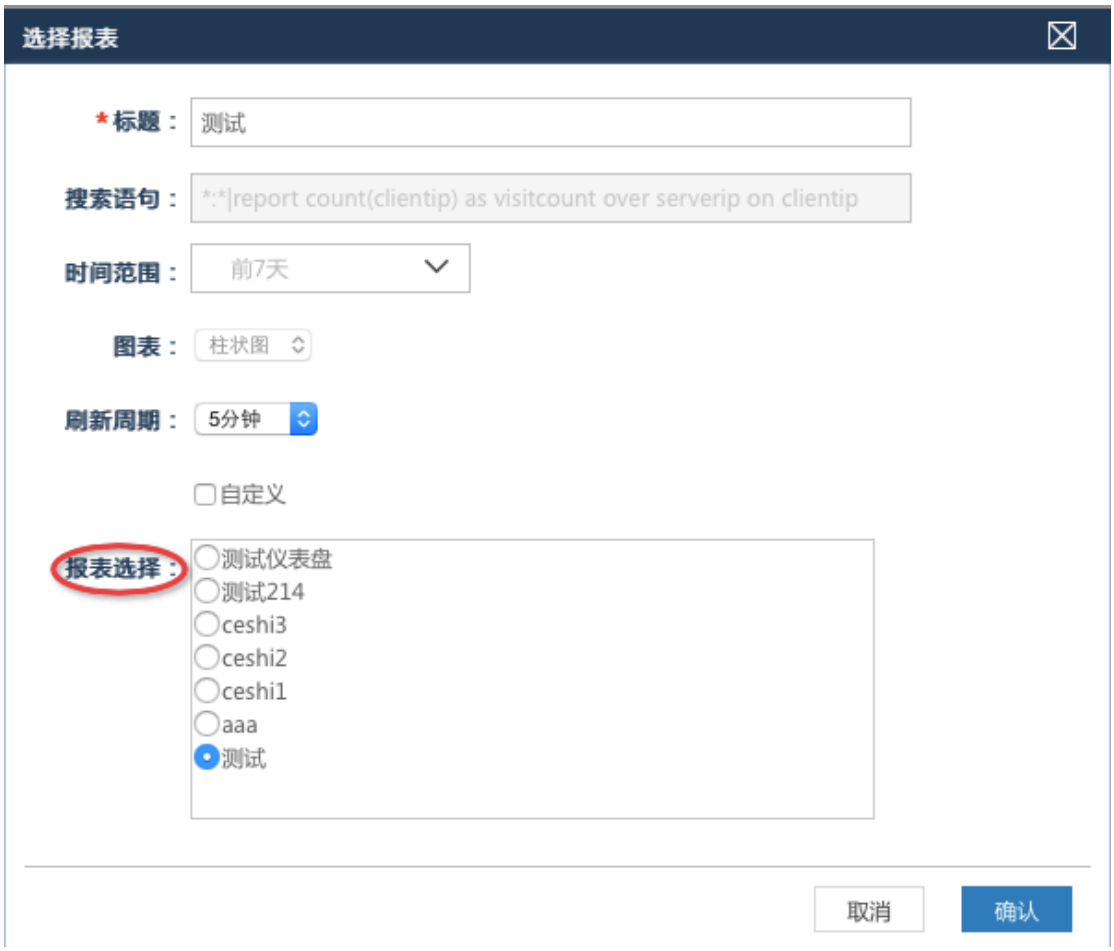


图 8-2

如图 8-3，点击选择“自定义”，可输入报表命令、设置时间范围新增报表。

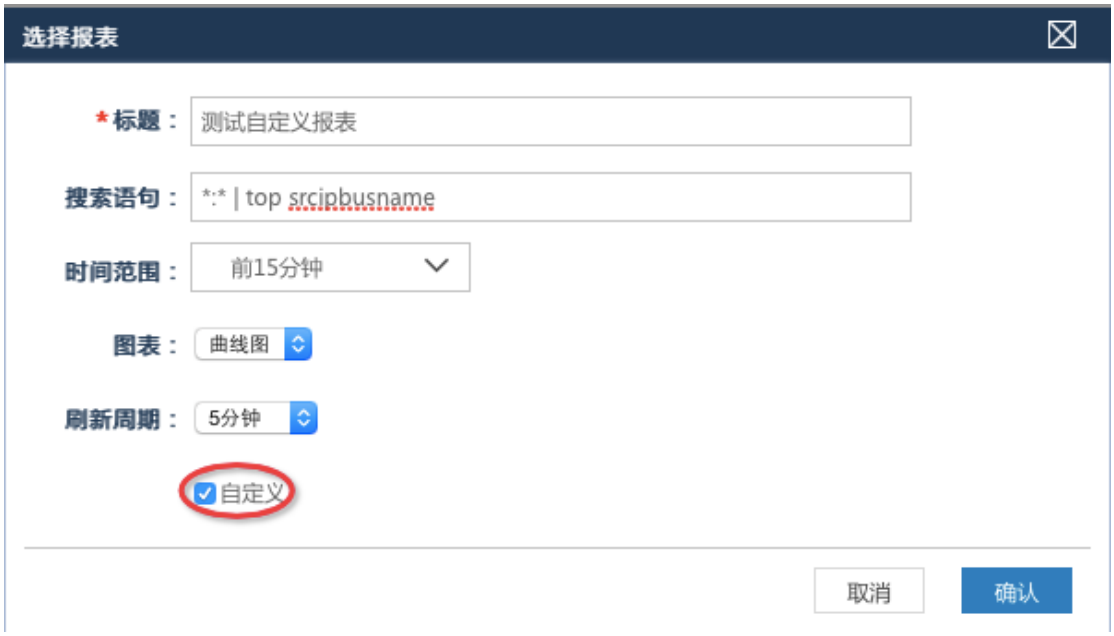


图 8-4

如图 8-5，点击报表界面的“查看”按钮可在搜索界面打开报表；点击“设置”会弹出选择报表窗口，在选择报表窗口可以编辑标题、刷新时间。

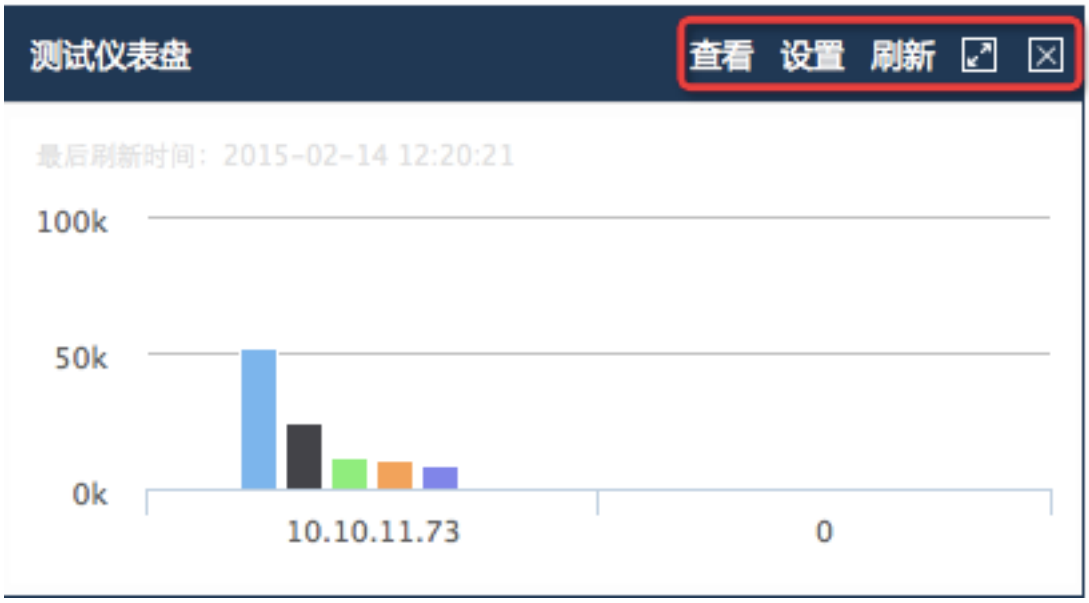


图 8-5

3.2.8 消息

点击“消息”图标可打开消息列表，如图 9-1，点击消息列表右端的删除图标可删除本条消息，点击“清空”按钮可清空消息列表。

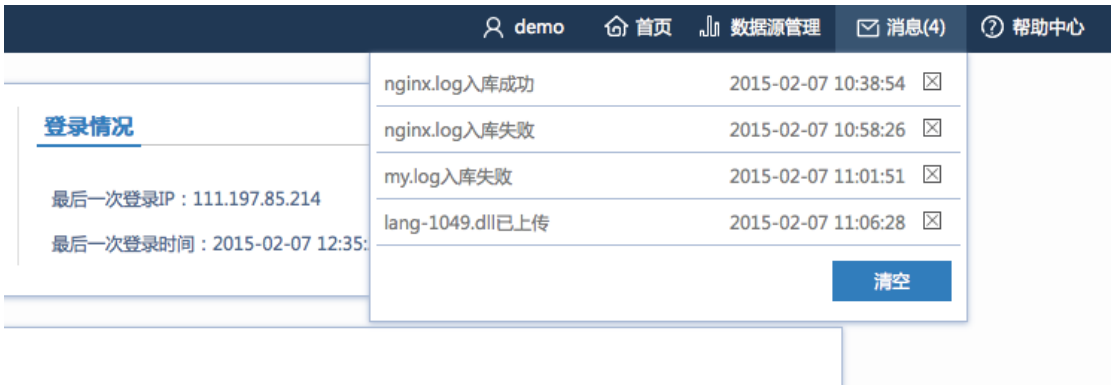


图 9-1

3.3 技术支持信息

公司提供本系统的维护和升级，在使用中如何遇到任何问题，可以及时与公司联系，具体的联系方式如下：

电话：010-82053991

E-mail：service@aleiye.com

Web 网址：www.aleiye.com

3.4 附录

3.4.1 附录一：下载 JDK

登录 ORACLE 官网网站下载 JDK,链接地址为：http://www.oracle.com/technetwork/java/javase/downloads/index.html。

3.4.2 附录二：添加数据配置信息

如图 2-1 进入添加数据集页面，用户需要定义数据集名称、填写指定数据路径，同时要对日期格式和所在时区进行配置。

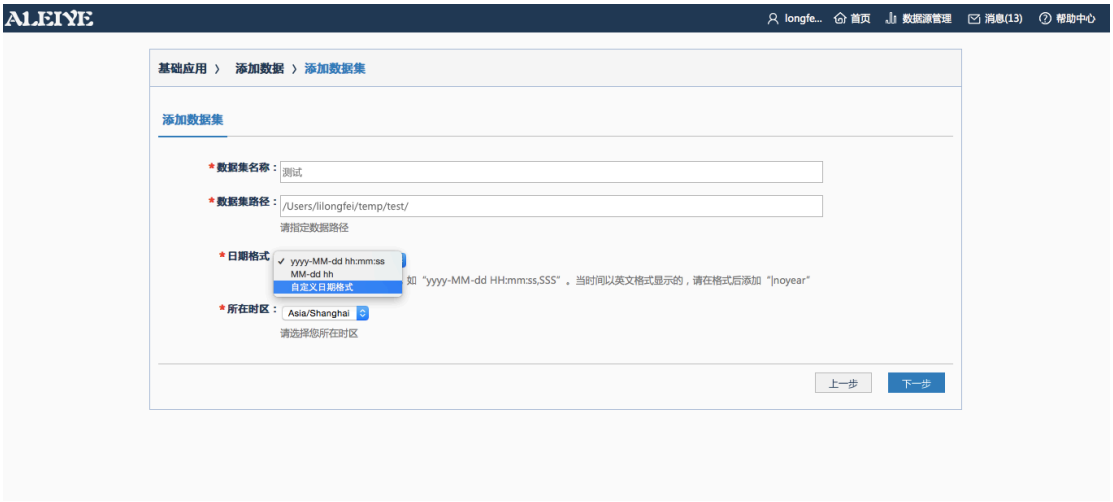


图 2-1

如图 2-2，点击下拉菜单选择或者自定义日志类型，当用户选择自定义格式时须手动录入正则表达式，用户可以输入部分样本日志对其验证，若显示"正则解析出错"，请检查正则表达式是否正确，若验证通过，可点击"保存"，系统返回页面提示是否保存成功；

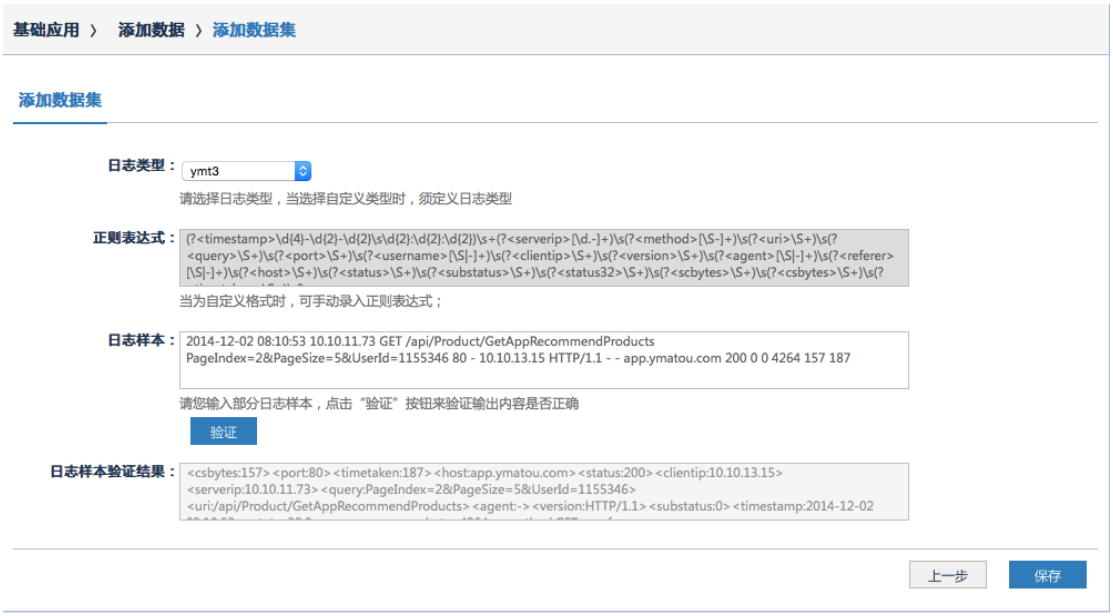


图 2-2

例：将关于样本数据的正则表达式录入到输入框内：

(?<timestamp>\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2})\s+(?<serverip>[\d.-]+)\s(?<method>[\S-]+)\s(?<uri>\S+)\s(?<query>\S+)\s(?<port>\S+)\s(?<username>[\S|-]+)\s(?<clientip>\S+)\s(?<version>\S+)\s(?<agent>[\S|-]+)\s(?<referer>[\S|-]+)\s(?<host>\S+)\s(?<status>\S+)\s(?<substatus>\S+)\s(?<status32>\S+)\s(?<scbytes>\S+)\s(?<csbytes>\S+)\s(?<timetaken>\S+)\r?

在将日志样本黏贴到输入框内：

2014-12-01 16:00:00 10.10.11.73 GET /api/Product/GetHotCountryGroupList - 80 - 10.10.13.15 HTTP/1.1 - - app.ymatou.com 200 0 0 987 118 93

点击验证，系统会基于正则表达式对样本数据切分，并把切分结果进行展示：

<csbytes:118><port:80><timetaken:93><host:app.ymatou.com><status:200><clientip:10.10.13.15><serverip:10.10.11.73><query:-><uri:/api/Product/GetHotCountryGroupList><agent:-><version:HTTP/1.1><substatus:0><timestamp:2014-12-01 16:00:00><status32:0><username:-><scbytes:987><method:GET><ref

erer:->

对数据集配置完毕后，点击下一步，保存数据，如图 2-3。

图 2-3

数据保存后，可进行多个步骤的操作，可进入数据源管理、继续添加数据和返回首页。

第4章 Aleiye 产品检索命令手册

4.1 Aleiye 检索概述

ALEIYE 使用类数据库系统提供了一套完整的查询搜索语言，包括关键字搜索、短语搜索、通配符搜索、字段搜索。

Aleiye 可以进行实时的交互式搜索。利用放大或缩小时间轴快速显示事件趋势、峰值和异常。在搜索结果中点击信息，可快速滤除无用信息，在巨量的数据中找到想要的结果。实时搜索意味着事件和攻击发生的可见性，可实时监测应用，可关联分析高速数据流事件，追踪进行中的交易和在线的应用活动情况。

4.2 Aleiye 检索命令

Aleiye 命令由三个部分组成,每部分由竖线间隔。语法:

基础搜索|自定义字段|报表命令

如： *:* |eval alias=parserLong(field) |top alias

其组成规则如下:

- 所有命令必须以基础搜索开始;
- 自定义报表字段可以有任意个，也可以没有;
- 报表命令可以没有，但是如果存在报表命令，语句必须以报

表命令结束并且报表命令只能由一个。没有报表只有自定义报表，自定义字段部分没有价值；

4.2.1 基础搜索部分

通过数据关键字、短语、逻辑关系进行数据检索。

4.2.1.1 关键字检索

普通关键字检索：多个关键字之间使用空格间隔，那么多个关键字将是与的概念。

如：hello aleiye 检索原文信息中包含 hello 并且包含 aleiye 的。

短语检索：使用“(注意是英文的双引号)包裹需要搜索的关键字，那么检索将双引号的内容视为一个关键字。

如“hello aleiye”，那么将检索原文中包含“hello 空格 aleiye”的数据。

4.2.1.2 字段检索

数据根据配置，可将数据且分为多个字段，可以根据字段名和值进行检索。

语法为；字段名:”字段值”。

如: title:"we are best!" ，那么检索结果将是 title 值为“we are best!“的数据。

4.2.1.3 模糊检索

Aleiye 可使用通配符进行检索。匹配单一字符使用符号“?”，匹配多个字符使用符号“*”。

- “?”：通配符将查找所有满足通过一个字符替换后符合条件的文档。

  如：搜索“test”和“text”你可以使用：te?t

- “*”：通配符将查询 0 个或者多个字符替换后符合条件的。

  如：查询 test，tests 或者 tester，你可以使用一下字符串来搜索： test* ， 也可以将“*”放在字符的中间。 te*t

  如：搜索客户端 ip 为 117.22.66 段的数据是:

  clientip:117.22.66.*

- 注意：Aleiye 不允许将“*”和“?”放在第一个字符来查询同样不能用模糊匹配的方式检索数字类型的数据。

4.2.1.4 范围检索

范围检索，如果字段为时间或者数字型的字段。

检索语法为：字段名：[开始 TO 结束]。注意，中括号是英文，并且 TO 为大写。

- 包含关系： date:[20020101 TO 20030101]
- 不包含关系： date:{20020101 TO 20030101}
- 其中，[]{} 也可以混合使用 如[}。

例如：需要检索网站响应时间在三秒以内的数据。

responseTime:[0 TO 3000];

4.2.1.5 逻辑检索

- OR

  或操作符，检索条件之间使用 OR 链接 那么检索结果将是符合两个条件的并集。

  如："hello aleiye" OR aleiye

- AND

  与操作符，规定必须所有的检索条件都出现才能满足查询条件。如果我们要搜索一个文档中同时含有“hello aleiye”和“bye aleiye”，我们可以使用如下语法：

  如：" hello aleiye " AND " bye aleiye "

- NOT

  非操作符，规定查询的文档必须不包含 NOT 之后的检索条件。当我们要搜索数据中必须含有“hello aleiye”同时不能含有“bye aleiye”时，我们可以使用如下查询；

  如："hello aleiye" NOT "bye aleiye"

- +、-

  加号表示与，减号表示非

  title:(+sucess -"aleiye is good")

- 正则表达式检索

TODO

- 特殊字符

+ - && | | ! ( ) { } [ ] ^ " ~ * ? : \

需要检索特殊符号的时候使用 \进行转义。 如搜索\ 应该使用\\.

4.2.2 报表命令

通过在搜索中添加报表命令将数据生成报表或者图表，以及汇总数据结果。报表命令需要放到搜索命令或者统计命令之后，用管道符号“|”来分割

主要报表命令包括:

report :此命令用来制作图表，可通过不同维度展示数据，图表中维度用X轴来展现。

语法：report stats-function [over field] on field

应用场景：统计各访问ip的访问流量平均量和总流量

使用命令： *:* |report avg(csbytes),count(csbytes) over clientip

datereport: 此命令用来制作以时间为X轴的时间趋势图表。

语法：datereport [stats-function]+ [on field] [span=n] 时间粒度单位：[h|m|s|d|y|M|w]

应用场景：使用 Web 访问数据向您显示访客在每个工作日的总数

使用命令：*:* |datereport count(clientip) on clientip span=1d

top：此命令用来对信息进行统计数量的图表。

语法：top (num[default 10])? field

应用场景：统计访问ip前10情况

使用命令：*:* |top clientip

stats:此命令可将数据以树状图的形式进行展现。

语法：stats (stats-function(field) [as field])+ [on field-list]

4.2.3 自定义字段

自定义字段是eval关键字的一种重新定义的字段操作命令，如现有aleiye平台中的数据不能够满足统计的需求 ，可通过eval自定义字段进行统计分析。

语法：eval <field>=<function>

field：是自定义的变量，field的名称是由字母组成的字段名。字段有两个来源一个是数据本身的字段，另外一个是由其他eval生成的字段

function：函数列表

函数类型	函数名称	功能说明
类型转换	parserLong	将字段数据转换为长整型
	parserDouble	将类型转换为浮点类型
	parserStr	讲类型转化为字符串类型
字符串操作	regex	通过正则拆解字段
	substr	截取字段的字串
	concat	连接两个字段值
	trim	字符串去空格
	upper	字符串字母全部转为大写
	lower	字符串字母全部转为小写
	split	字符串按照字符拆分
逻辑运算	case	逻辑判断
四则运算	+-*/（）	数字四则运算

parserLong

说明：将指定字段的数据类型转换为长整型Long

语法：parserLong(field)

参数说明：filed:字段

应用场景：统计各小时访问IP的总数

检索语句：*:*|eval ip=substr(clientip,0,2) | eval ip2=parserLong(ip)|datereport count(clientip) on clientip span=1h

parserDouble

说明：将指定字段的数据类型转换为字符型Double

语法：parserDouble(field)

参数说明：filed:字段

应用场景：统计访问流量加基数100后的排名

检索语句：*:* | eval s=parserDouble(csbytes)+100|top s

parserStr

说明：数据类型转换为String类型

语法：parserStr(field)

应用场景：统计各类服务器访问码排名情况

检索语句：*:* | eval s=parserStr(status)|eval su=substr(s,0,1)|top su

regex

说明：将字段按正则表达式进行匹配

语法：regex(field,"rex",num)

参数说明：field：字段； rex:正则表达式； num:第N个

应用场景：统计各网段服务器访问排名

检索语句：

:|eval ip=regex(clientip,"(\d+\.\d+\.\d+)",1)|top ip

substr

说明：对字符串进行截取，

语法：substr(field,int,length)

参数说明：field:字段； int：起止位数，可为负数； length:长度

应用场景：统计各网段服务器访问排名

检索语句：*:*|eval ipcate=substr(serverip,0,8)|top ipcate

concat:

说明：对多个字段数据进行拼接

语法：concat(field1, field2)

参数说明：field1、field2:字段；也可为字符串

应用场景：统计所有网站全频道访问排名

检索语句：*:* | eval url=concat(host,uri)|top url

trim

说明：对字段数据首尾进行去空格或制表符，或只去左侧、右侧空格

语法：rtrim(field)、ltrim(field)、trim(field)

参数说明：field:字段

应用场景：对url字段前后进行去空格操作

检索语句：*:*|eval uri=trim(uri)|top uri

upper

说明：将字段类数据转换为大写显示

语法：upper(field)

参数说明：field:字段

应用场景：将uri字段进行大写显示

使用命令：*:* | eval uri=upper(uri)|top s

lower

说明：将字段类数据转换为小写显示

语法：lower(field)

参数说明：field:字段

应用场景：将version信息统一为小写

使用命令：*:* |eval version=lower(version)|top s

split()

说明：将字符串类型数据按给定的正则表达式来切分数据，并指写切分后的第几个数据

语法：split(field,char)[i]

参数说明：field:字段; char:切分字符；i：自0开始计算

应用场景：将IP按“.”符号切分后取第2位切分内容

检索语句:

:|eval ip=split(clientip,"\.")[1]|datereport count(clientip) on ip2 span=1h

case

说明: 可根据不同条件将数据显示为不同信息

语法: case(booleanfun,value(,booleanfun,value)[,else ,vaule])

参数说明: booleanfun:判断函数; value:显示值; else: 表示除此之外的情况

应用场景:根据不同流量大小统计大、中、小三种级别客户

使用命令: *:* |eval xx=parserLong(csbytes)|eval a=case(xx<=100,"small",xx>100 and xx<200,"middle",else,"big")|report sum(xx) over a

4.3 sql 检索命令

Sql 搜索支持 SQL92 标准，支持 70%左右的 Sql 语句检索。可分为以下几类:

4.3.1 简单查询

简单的 Transact-SQL 查询只包括选择列表、FROM 子句和 WHERE 子句。它们分别说明所查询列、查询的表以及搜索条件等。

例如：下面的语句查询 people 表中姓名为“张三”的 name 字段和 age 字段：

```
select name, age from people where name='张三'
```

4.3.1.1 指定查询字段

选择列表指出所查询字段，它可以是一组字段组，星号、简单表达式、变量等构成；

1) 选择所有字段

举例：下面语句显示 people 表中所有字段的数据：

```
select * from people
```

2) 选择部分列并指定它们的显示次序

查询结果集合中数据的排列顺序与选择列表中所指定的列名排列顺序相同

如：select name,age from people

3) 更改字段别名

在选择列表中，可重新指定字段标题，定义格式为：

字段名 as 别名

如果指定的别名不是标准的标识符格式时，应使用引号定界符，例如，下列语句也可以使用汉字来显示列标题。

如：select name as a, age as b from people

select name as 姓名, age as 年龄 from people

4) 删除重复行

SELECT 语句中使用 ALL 或 DISTINCT 选项来显示表中符合条件的所有行或删除其中重复的数据行，默认为 ALL。使用 DISTINCT 选项时，对于所有重复的数据行在 SELECT 返回的结果集合中只保留一行。

5) 限制返回的行数

在 SQL 语句中添加 LIMIT 进行返回行数的限制：

如：select name, age from people limit 5

4.3.1.2 子查询

FROM 子句指定 SELECT 语句查询及与查询相关的表。在 FROM 子句中可指定多个表，它们之间用逗号分隔。

在 FROM 子句同时指定多个表时，如果选择列表中存在同名列，这时应使用对象名限定这些列所属的表。例如在 people 和 development 表中同时存在 name 列，在查询两个表中的 name 时应使用下面语句格式加以限定：

如：select people.name,age from people,development where

people.name=development.name

在 FROM 子句中可用以下两种格式为表或视图指定别名：

表名 as 别名

如：上面语句可用表的别名格式表示为：

select p.name,p.age,d.dev from people p,development d where p.name=d.name

SELECT 不仅能从表中检索数据，它还能够从其它查询语句所返回的结果集合中查询数据

select d.name,d.dev from development d,(select name from people where age > 25) as p where d.name=p.name

此例中，将 select 返回的结果集合给矛一别名 p，然后再从中检索数据。

4.3.1.3 设置查询条件

where 子句设置查询条件，过滤掉不需要的数据行。例如下面语句查询年龄大于 20 的数据：

select * from people where age > 20

where 子句可包括各种条件运算符：

- 比较运算符（大小比较）：>、>=、=、<、<=、<>、!>、!<
- 范围运算符(表达式值是否在指定的范围)：

BETWEEN...AND...、NOT BETWEEN...AND...

- 列表运算符(判断表达式是否为列表中的指定项)：IN (项 1,项 2.....)
- 列表运算符例： NOT IN (项 1,项 2.....)
- 模式匹配符(判断值是否与指定的字符通配格式相符):LIKE、NOT LIKE
- 空值判断符(判断表达式是否为空)：IS NULL、NOT IS NULL
- 逻辑运算符(用于多条件的逻辑连接)：NOT、AND、OR
  - 范围运算符例：age BETWEEN 10 AND 30 相当于 age>=10 AND age<=30
  - 列表去处符：age IN (25,26)
  - 模式匹配符例：常用于模糊查找，它判断列值是否与指定的字符串格式相匹配。可用于 char、varchar、text、ntext、datetime 和 smalldatetime 等类型查询。

可使用以下通配字符：

- 百分号%：可匹配任意类型和长度的字符，如果是中文，请使用两个百分号即%%。
- 下划线_：匹配单个任意字符，它常用来限制表达式的字符长度。
- 方括号[ ]：指定一个字符、字符串或范围，要求所匹配对

象为它们中的任一个。[^]：其取值也[]相同，但它要求所匹配对象为指定字符以外的任一个字符。

例如：

- 限制以 Publishing 结尾，使用 LIKE '%Publishing'
- 限制以 A 开头：LIKE '[A]%'
- 限制以 A 开头外：LIKE '[^A]%'
- 空值判断符，如：WHERE age IS NULL
- 逻辑运算符：优先级为 NOT、AND、OR

4.3.1.4 查询结果排序

使用 ORDER BY 子句对查询返回的结果按一列或多列排序。ORDER BY 子句的语法格式为：

ORDER BY {column_name [ASC|DESC]} [,...n]

其中 ASC 表示升序，为默认值，DESC 为降序。ORDER BY 不能按 ntext、text 和 image 数据类型进行排序。

如：select * from people order by age desc

4.3.2 统计查询

计算查询是指通过系统提供的特定函数(聚合函数)在语句中的直接使用而获得某些只有经过计算才能得到的结果。常用的函数有：

- COUNT(*)　　计算元组的个数

- COUNT(字段名) 对某一列中的值计算个数
- SUM(字段名) 求某一列值的总和(此列值是数值型)
- AVG(字段名) 求某一列值的平均值(此列值是数值型)
- MAX(字段名) 求某一列值中的最大值
- MIN(字段名) 求某一列值中的最小值

例如：统计总人数和平均年龄

```
select count(*), AVG(age) from people
```

4.3.3 连接查询

通过连接运算符可以实现多个表查询。连接是关系数据库模型的主要特点，也是它区别于其它类型数据库管理系统的一个标志。

在关系数据库管理系统中，表建立时各数据之间的关系不必确定，常把一个实体的所有信息存放在一个表中。当检索数据时，通过连接操作查询出存放在多个表中的不同实体的信息。连接操作给用户带来很大的灵活性，他们可以在任何时候增加新的数据类型。为不同实体创建新的表，尔后通过连接进行查询。

连接可以在 SELECT 语句的 FROM 子句或 WHERE 子句中建立，似是而非在 FROM 子句中指出连接时有助于将连接操作与 WHERE 子句中的搜索条件区分开来。所以，在 Transact-SQL 中推荐使用这种方法。

SQL-92 标准所定义的 FROM 子句的连接语法格式为：

FROM join_table join_type join_table

[ON (join_condition)]

其中 join_table 指出参与连接操作的表名，连接可以对同一个表操作，也可以对多表操作，对同一个表操作的连接又称做自连接。

join_type 指出连接类型，可分为三种：内连接、外连接和交叉连接。内连接(INNER JOIN)使用比较运算符进行表间某(些)列数据的比较操作，并列出这些表中与连接条件相匹配的数据行。根据所使用的比较方式不同，内连接又分为等值连接、自然连接和不等连接三种。外连接分为左外连接(LEFT OUTER JOIN 或 LEFT JOIN)、右外连接(RIGHT OUTER JOIN 或 RIGHT JOIN)和全外连接(FULL OUTER JOIN 或 FULL JOIN)三种。与内连接不同的是，外连接不只列出与连接条件相匹配的行，而是列出左表(左外连接时)、右表(右外连接时)或两个表(全外连接时)中所有符合搜索条件的数据行。

交叉连接(CROSS JOIN)没有 WHERE 子句，它返回连接表中所有数据行的笛卡尔积，其结果集合中的数据行数等于第一个表中符合查询条件的数据行数乘以第二个表中符合查询条件的数据行数。

连接操作中的 ON (join_condition) 子句指出连接条件，它由被连接表中的列和比较运算符、逻辑运算符等构成。

无论哪种连接都不能对 text、ntext 和 image 数据类型列进行直接连接，但可以对这三种列进行间接连接。例如：

select p.name,p.age,d.dev from people as p INNER JOIN devlopment as d on p.name=d.name

4.3.3.1 内连接

内连接查询操作列出与连接条件匹配的数据行，它使用比较运算符比较被连接列的列值。内连接分三种：

- 等值连接：在连接条件中使用等于号(=)运算符比较被连接列的列值，其查询结果中列出被连接表中的所有列，包括其中的重复列。
- 不等连接： 在连接条件使用除等于运算符以外的其它比较运算符比较被连接的列的列值。这些运算符包括>、>=、<=、<、!>、!<和<>。
- 自然连接：在连接条件中使用等于(=)运算符比较被连接列的列值，但它使用选择列表指出查询结果集合中所包括的列，并删除连接表中的重复列。

下面使用等值连接列出 authors 和 publishers 表中位于同一城市的作者和出版社：

select * from people as p inner join develop d as p on p.name=d.name

4.3.3.2 外连接

内连接时，返回查询结果集合中的仅是符合查询条件(WHERE

搜索条件或 HAVING 条件)和连接条件的行。而采用外连接时，它返回到查询结果集合中的不仅包含符合连接条件的行，而且还包括左表(左外连接时)、右表(右外连接时)或两个边接表(全外连接)中的所有数据行。如下面使用左外连接将论坛内容和作者信息连接起来：

```
SELECT p.*,d.* FROM people as p LEFT JOIN develop as b
ON p.name=d.name
```

下面使用全外连接将 city 表中的所有作者以及 user 表中的所有作者，以及他们所在的城市：

```
SELECT p.*, d.* from people as p full outer join devlopment as d
on p.name=d.name
```

4.3.3.3 交叉连接

交叉连接不带 WHERE 子句，它返回被连接的两个表所有数据行的笛卡尔积，返回到结果集合中的数据行数等于第一个表中符合查询条件的数据行数乘以第二个表中符合查询条件的数据行数。例，people 表中有 10 条记录，而有 development 表中有 10 个部门，则下列交叉连接检索到的记录数将等于 10*10=100 行。

```
SELECT name,dev  from people cross join development order by dev
```

4.4 附录

4.4.1 sql 检索的结果 json 解释

```
select   *   from people

结果：表

{

      "head": [   //表头

           "name",

           "age"

     ],

     "data": [//数据

           [

                "陈”,”23"

           ],

           [

                "田** “,”14"

           ]

     ],


}
```

4.4.2 aleiye 搜索 stats 统计结果 json 解释

:|stats sum(字段 1) on 字段 2

可以同时多级分组统计多个字段

```
{
    "bulketsName": "root",  //根目录
    "children": [
        {
            "bulketsName": "bb_字段 2 值", //bb 开始的都是字段分组
            "children": [
                {
                    "doc_count": "552",  //出现的 count 值，结果集按照这个数值倒序排列
                    "key": "字段 1 的值",//字段值
                    "children": [
                        {
                            "bulketsName": "ss_sum_字段 1",//ss 开头的都是统计函数的值
                            "value": "706560.0"//统计值
                        }
                    ]
                }
            ]
```

```
            }
        ]
}
```

第5章 技术方案

5.1 项目背景

[介绍本项目的背景，一般来自于招标方的技术文件，也可以在互联网上搜索相关背景做介绍，便于方案阅读者了解项目的背景知识，便于理解方案的后面章节。]

随着互联网业务和应用的迅猛发展以及移动互联网的爆炸式增长，电信运营商客户行为数据、网络运维数据等海量数据的存储与分析日益成为电信运营商的重要挑战，大数据技术的出现与发展为电信运营商深挖数据提供了新的技术手段，同时也为其更好地服务客户提供了新的机遇。

同时随着电信运营商全业务的开展，电信行业的竞争已经从传统的用户资源、资费方式的竞争，上升到以客户为核心的服务竞争。因此从运营角度出发，由于竞争加剧导致总体收益的下降，运营商当前迫切需要寻找新的业务增长点。从自身角度出发，在提供安全可靠的网络线路、各类增值服务的同时，必须解决由于网络攻击、病毒爆发等安全事件的影响，对用户服务质量的降低。

在运营商内部，部署了大量的防火墙、入侵监测系统、虚拟专用网和防病毒软件等网络安全设备，从而保证网络的可用性和网络信息的机密性、完整性，防止来自外部或内部的攻击行为。这些工具和设备都已日志形式记录着大量的安全问题，这些信息成为网络安全工作中防御、监测和响应的重要基础依据。

- 如何面对多源异构的数据

原始日志是安全管理过程中获取的重要内容，如：Syslog 数据、SNMP 数据、

数据库等;由于不同数据种类存在在不同设备和不同系统中，做为数据预处理、关联分析和告警响应的重要信息来源，需要对上述的异构数据进行有效实时的采集，是运营商面临的第一个挑战。

- 如何对异构数据进行统一管理

在对数据源统一管理的过程中，由于原始日志存在采集来源的不同，导致其数据格式存在差异，例如通过 Syslog 和 SNMP 采集的同一类型的事件，但由于采集方式的不同，导致其数据格式不统一;数据源中，还会存在大量的重复信息、不可信信息和不重要信息，这些问题将会导致最终的数据统计分析结果的准确性降低，是运营商面临的第二个挑战。

- 如何对安全事件进行深入分析

基于传统告警方式，对固定指标设定固定阀值的方式，无法更全面的重构安全事件攻击场景，如何利用不同设备、不同系统间的数据进行关联分析，实现真正的安全告警，从而降低误报率，帮助安全监控人员分析出网络中潜在的安全隐患，也是运营商面临的第三个挑战。

5.2 建设目标

[一般来自于客户招标文件，明确系统建设的目标。]

5.3 建设原则

总的原则：遵循标准、立足需求、以运营为目的、总体规划、分步实施。

5.3.1 标准性原则

数介科技提供的系统解决方案及相关软硬件系统完全满足相关国内标准;国内没有标准的则参照相应国际标准。对当前正在制定和即将制定的国内标准，数介科技承诺在标准出台后能够平稳接轨。

5.3.2 可扩展原则

数介科技所提供的系统可以在保证初期业务的前提下，留有充分的扩展空间，保证将来各种新业务的开展。数介科技所建议采用的单机设备在后期扩展方面拥有极大的优势，运营商可以在业务需要的时候方便的添加设备。不仅可以添加系统设备，而且可以添加符合标准的增值业务设备。

5.3.3 可升级原则

随着技术的飞速进步，现有的设备和系统肯定在不同时期需要进行升级和不同程度的更新，数介科技本次的组网建议能够实现可预见的平滑升级，确保在系统不作大的变更前提下，平滑升级到更高的层次。在升级过程中，能够确保业务不间断，同时保证原设备能正常使用，在未来尽可能的保护原有投资，减少二次投资。

5.3.4 全开放性原则

数介科技本次组网方案采用开放式设计，保证系统与其它各大厂商设备、系统的良好集成性能，能够确保对符合相关标准的第三方厂家设备进行兼容，以便

于第三方设备能公平地进入已经部分搭建完毕的系统。

5.3.5 安全性原则

数介科技本次提供的设备系统均按照电信级运营平台标准建设，系统能够有效地杜绝、限制黑客非法进入系统，以确保系统安全；并且可以根据需要加入系统级备份，可以根据需要选择对系统进行冷备份和热备份。

5.3.6 稳定性原则

数介科技研发的系统能保证单个设备的长期稳定运行，从而保证整个平台的稳定与安全。在某个模块出现问题的时候，也可以很方便的进行更换和维修，因而最大限度的缩小了波及的范围。

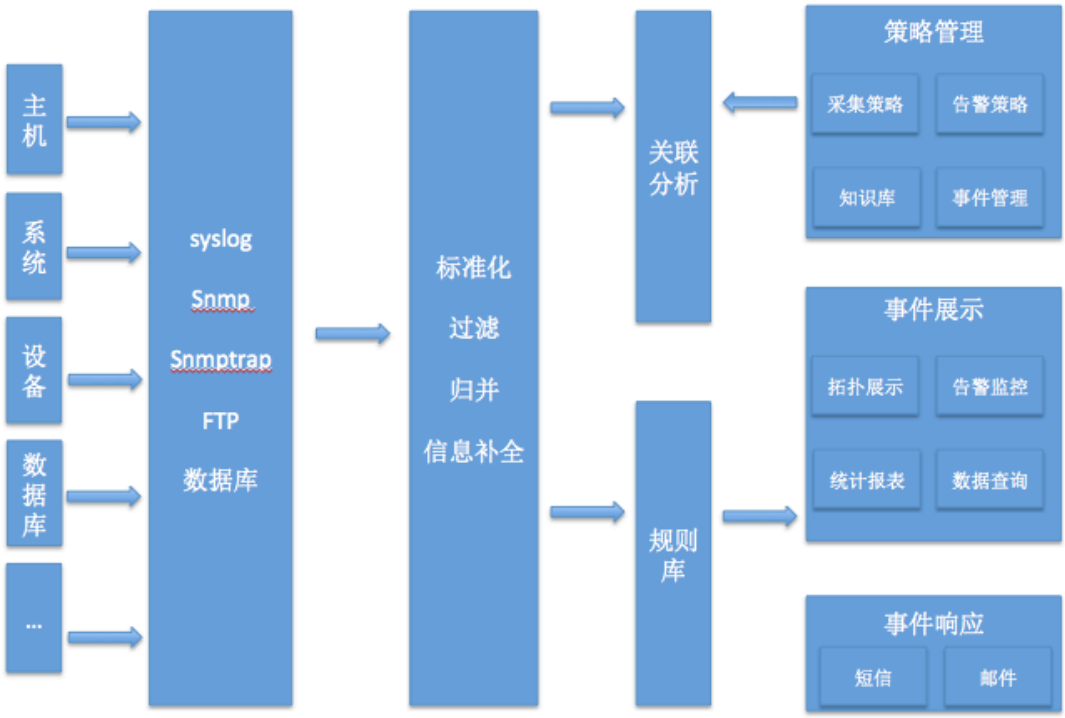
5.3.7 可管理性原则

数介科技本次提供的系统具有完善、健全的网络管理接口，可通过网管的统一控制对设备进行实时全面的监测和控制；可对业务、用户进行方便快捷的查询和管理。并且根据软件系统的重要程度，数介科技提供了不同级别的访问权限设置。

5.3.8 实用性原则

数介科技的系统设计、设备选型均符合中国国情，充分考虑到了国内电信运营商的需要和市场情况，性能价格比极佳，并通过合理科学的设备选型和网络搭建最大可能的降低买方的长期成本。

5.4 Aleiye 方案设计



5.4.1 数据采集

5.4.1.1 采集方式

数据采集层，主要是针对不同的业务系统和不同的安全设备中的日志进行采集，作为后续的数据处理和关联关系的信息来源，其采集方式重要包括 syslog、SNMP、SNMP Trap、FTP、代理采集和数据库等几种方式。

- Syslog 方式：支持 syslog 内容解码。
- SNMP 方式：支持 SNMP V1、V2、V3，内容解码。
- FTP 方式：支持 FTP 协议方式进行日志文件获取。
- 数据库方式：支持当前主流数据库并从中获取日志，其中包括：Oralce、Sybase、DB2、Informix、MySQL、Postgresql 等
- 代理采集：系统须具备在通过安装代理软件实现原始日志的采集功能。

5.4.1.2 采集管理

在分布式采集或单点采集的状况下，Aleiye 数据平台提供采集节点集中管理，实现对采集状态、采集规则和采集起始进行统一管理。

- 批量操作：在分布式采集的状况下，可以对各采集节点进行统一管理，如批量关闭、批量启动、批量暂停、批量下发操作。

- 策略复制：在分布式采集的状况下，可以将单采集节点中的采集策略复制到其他采集节点。
- 采集状态监控：可实时监控不同采集节点的采集状态，在数据传输过程中出现异常，系统会给与采集异常提示。

5.4.2 数据预处理

原始日志采集之后，需要进行数据预处理的过程，通过标准化配置，对数据源进行明确的数据类型划分，将日志格式进行统一转化和分类，根据划分好的数据类型进行过滤、归并、补全等规则操作，为后续的关联分析提供信息。最终输出明确的事件类型和各字段属性及补全后的安全对象信息等内容的标准事件

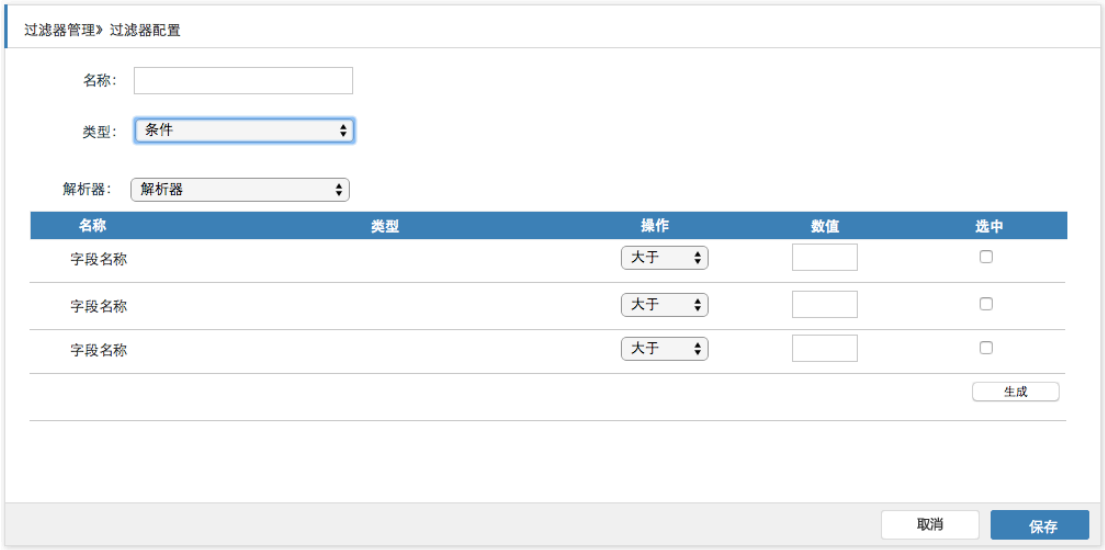
5.4.2.1 数据标准化

根据数据源的内容和格式，对应相应的事件类型进行字段提取、命名等操作，最终形成结构化数据。

5.4.2.2 事件过滤

事件过滤功能通过自定义设置，可对不影响后续分析的安全事件进行过滤，

减少不可信、不重要的事件，过滤策略可根据字段间的条件进行有效过滤，字段件条件包括：大于、小于、等于、大于等于、小于等于、等于、不等于；还可以通过关键字和 IP 段进行过滤规则的配置。



5.4.2.3 事件归并

对于重复发生、大部分属性相同的疑似安全事件，在不影响后续事件分析的前提下，应对个体进行合并，减少事件个体数量，并可以对合并后的数据进行新事件的创建。

5.4.2.4 信息补全

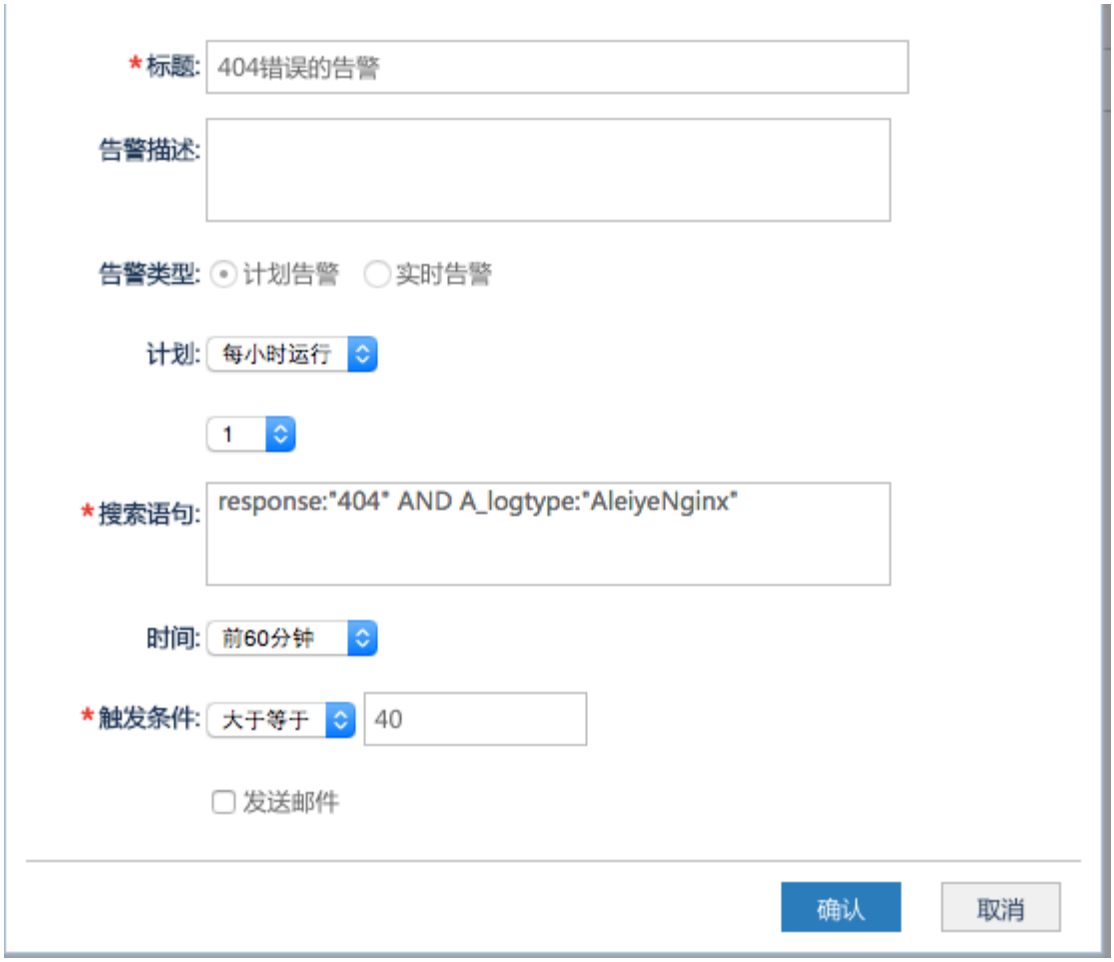
对于未直接体现在原始日志中的必要信息，事件管理模块应具备补全功能，主要为与事件相关的安全对象信息。

5.4.3 安全告警关联分析

安全告警关联分析是指安全告警的分析方法，以事件触发为基础，对实际业务情况进行深度挖掘，从而实现高可信度的安全告警信息。安全告警关联分析基于统计关联、模式关联两种方式进行组合，分析安全告警、挖掘安全隐患、判断安全事件的严重程度和实质影响。从而重构整个攻击场景，降低误报率，帮助安全监控人员分析出网络中潜在的安全隐患。

5.4.3.1 统计关联

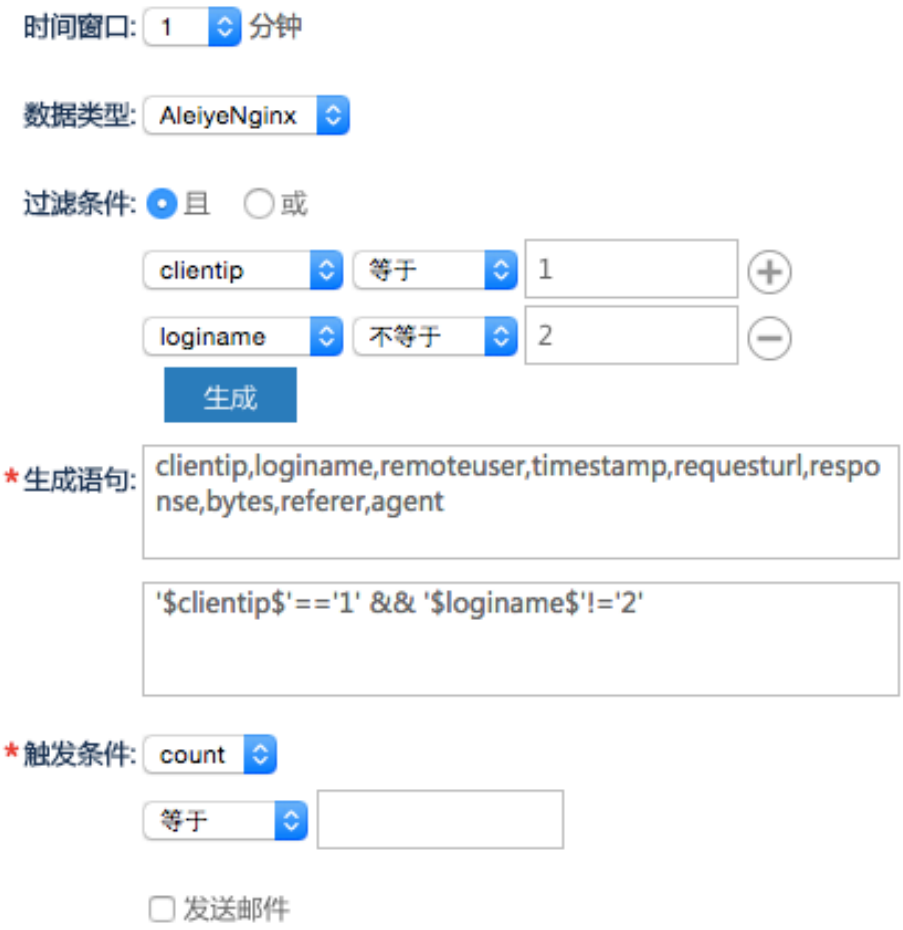
使用计数器来统计某类事件发生的次数，并设定可以接受的数值范围，一旦在统计过程中发现事件超出了正常设定的阈值，就认为系统出现了异常，而生成告警。基于统计关联的方法适应于检查统计量发生次数有明确限制情况



5.4.3.2 模式关联

基于模式的关联分析是指将可疑的安全活动场景（例如某潜在安全攻击行为的一系列安全事件序列）加以预先定义，对收集到的安全事件进行检查，确定该事件是否和特定的模式匹配。

其中，条件为安全事件中某些属性的限制条件，具有检测事实存在与否、比较事实、根据标志检验事实等功能。条件可以由单个检测属性组成，也可以由多个检测属性组成，且各属性用逻辑符号 OR、AND、NOT 来表示多属性的逻辑关系。结果是新安全告警的输出，同时指定此安全告警的严重程度。



5.5 测试性能

5.6 原型展示

5.7 方案价值

Aleiye 数据平台可以整合各个安全设备数据，统一设备输出的事件，帮助安全管理人员从全局角度保证整体安全态势。

第6章 项目管理

6.1 项目管理体系

为了规范工程项目行为管理，提高项目施工质量，数介科技制定了详细的项目管理体系制度，包含以下几方面的内容：

一、项目参与人员岗位责任制

数介科技企业内部具有清晰的组织结构，自 CEO 向下层层负责。公司拥有 30 多人的创新型研发团队和高素质售后服务团队，针对本次项目数介科技成立了专门的项目组，项目组内部包括项目经理、技术总监、售后技术经理等项目组成员。组内成员实行岗位责任制，责任分工清晰、明确，各岗位衔接紧密，无遗漏。以下是项目小组成员：

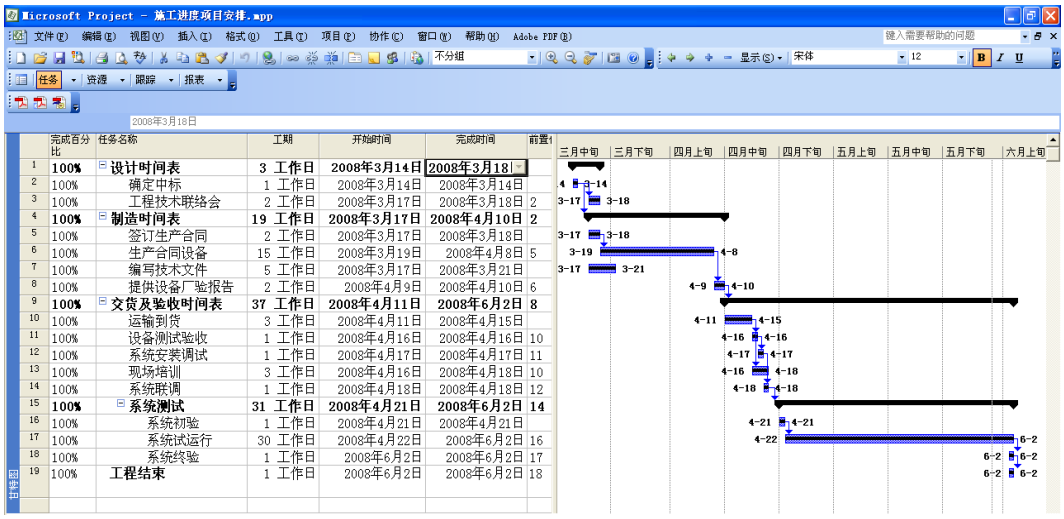
序号	姓名	专业	职称	本项目中的职责	项目经历	参与本项目的到位情况
1	张晓宇		项目经理	项目经理负责项目的沟通与协调		正常

2	温承华	机械	总工程师	技术方案总负责		正常
3	周元龙		售后工程师	方案实施总负责		正常

二、 项目计划、统计、进度管理

1、签定项目合同后，数介科技将由项目小组负责具体联络，根据招标方需求合理安排工期和项目流程。

2、项目责任人组织人员制定施工计划、分解进度目标，以分解后的进度目标为各施工人员设定施工节点计划，确保总进度目标实现。以下是数介科技工程实施进度管理模板：



3、项目进行期间，数介科技将做好各阶段文档编制及提交工作，包括施工日记、测试记录、自检记录、隐蔽记录、进度记录等按期向工程部提交。

4、因项目需求或物理环境变化等客观原因影响工程进度的，数介科技将及

时与招标方沟通，并提出有针对性的解决方案。

5、工程计划执行过程，如发现未能按期完成工程计划，数介科技及时检查分析原因，立即调整计划和采取补救措施，以保证工程施工总进度计划的实现。

三、项目质量、安全管理

1、数介科技将严格按照国家及地区规范、施工图纸及合同进行施工；明确项目组成员的岗位责任制，把各处的质量责任落实到各个责任人。

2、数介科技将在项目进行前分析项目的重点、难点，为本次项目制定针对性强的具体施工方案。

3、数介科技将在项目中做好的“检、复检、交接检”工作，不缺省中间环节。

6.2 实施进度计划

同时数介科技作为专业的技术、系统、产品与服务一体化供应商，为此次项目提供如下工程实施方案。

项目	内容	数介科技工作
第一项	确定中标	数介科技接到中标通知，将优先为本次项目调度生产、测试等资源，根据投标技术文件确定的产品数量和配置，进行相应的组织。
第二项	工程技术设计联络会	合同签订后数介科技和运营商在招标方要求的前提下举行一次工程技术设计联络会，以解决合同中的具体技术实施问题。

第三项	生产合同系统，提供厂验报告	根据最终双方确定的产品配置，优先为本次系统组织系统生产。所有系统生产结束后，按照 ISO9001:2000 质量体系标准要求，进入测试及系统出厂检验，并提供出厂测试项目、测试指标、测试方法和测试结果。
第四项	运输到货及验收	设备按照双方签订的合同要求的时间运抵指定地点后，将由数介科技、招标方共同组成验收小组，货到指定地点后出具双方签字的《到货验收报告》。验收过程中如经双方确认发现设备有缺陷、破损，数介科技将按采购人要求补发、更换。
第五项	设备安装、调试	数介科技负责设备安装、调试，并对招标方人员提供现场技术指导，以确保正确地安装、调试和使用。
第六项	系统初验	设备安装结束后，经双方确认后可进入系统初验。系统调测由数介科技负责，招标人派工程技术人员参加。测试前数介科技提出完整的调试计划（包括测试的内容、项目、指标、方法和进度），并提供相应的仪器和工具，经招标人确认后，方可实施。在系统调测期间，数介科技按技术规范的

		要求对设备进行全面的技术指标测试的诊断，在调测期间如发生故障和障碍，作详细记录，查明原因并写出相应的分析报告。系统调试结束后，数介科技将测试诊断记录整理后交给招标人，招标人认可后工程进入验收测试阶段。
第七项	系统终验	初验通过后，达到合同规定的要求后，由招标人召集数介科技对系统进行最终验收。系统验收由数介科技负责，招标方派相应技术人员参加。详细验收标准及验收方案由数介科技与招标方共同商讨完成。 在系统验收期间，数介科技将在本技术规范书基础之上与招标方进一步明确测试内容，遵循国际标准或经双方认可的通用测试方法，对系统进行全面细致的测试。 在终验期间如发生故障和障碍，数介科技做详细记录，查明原因并写出相应的分析报告。认定指标全部达到要求时，双方签署终验报告。然后进入质保期。并出具双方签字的《正式验收报告》。

注：以上项目管理及实施进度计划以最终合同签订为准。

第7章 售后服务承诺

针对本次项目，数介科技将提供完善周到的售后服务保障，其主要内容如下：

质量保证体系

安装督导

质保期内服务

质保期后服务

热线支持服务

技术培训

技术文件

升级扩展服务

7.1 质量保证体系

数介科技所投产品严格按照质量管理体系的规定和要求进行产品的研发、生产、销售和服务。根据实际需要，用户可在双方商定的时间内与数介科技接触，以了解数介科技质量体系并及时提出新的建议或要求。用户亦可进行现场考察，以就目前状况、具体事宜、进度等与数介科技达成协议。

签订合同后，数介科技可向用户提供项目相关文件，包括质量和生产检验指标以及合同规定的其他技术文件，以这些文件作为依据来确保质量执行过程与合同规定的质量计划一致。

7.2 安装督导

数介科技向用户方提供产品的安装、培训和维护服务等全部内容的服务，并完成整个系统的网络联调工作。

数介科技拥有强大的工程队伍和丰富的工程经验，在数介科技承接的所有平台搭建工程项目中，均提前并合格的完成了工程任务。

数介科技将优先为本次项目调动工程实施人员，积极与用户配合，进行工程设备的安装调测，保证整个工程进行的顺利快捷。

在产品到达安装现场后，数介科技将负责派有经验的技术人员到现场处理货物质量和数量短缺等问题，并对系统的调测进行指导。

在系统现场安装调试期间，如果出现不正常情况（如损坏、故障），数介科技免费在不延误工期的情况下从速替换或修复。

7.3 质保期内服务

数介科技提供自整个系统验收合格并投入正常运行之日起 12 个月的免费保修服务。在质保期内，所有出现故障的软件和硬件设备（人为原因或不可抗拒的自然灾害等造成的设备损坏除外），数介科技将迅速修复或更换，数介科技由此所发生的全部费用自行承担。

在免费质保期内，所有出现故障的硬件和软件，数介科技提供 24 小时的热线支持。在接到系统故障通知后，数介科技公司将快速响应。如果需要到现场解决，数介科技承诺在尽快安排到达现场排除故障。如果系统故障在检修后仍无法

排除，数介科技将提供不低于故障系统或设备规格型号档次的备用系统或设备给用户使用，直至系统故障彻底排除。

7.4 质保期后服务

质保期后，数介科技对其提供的系统提供技术支持。

系统故障排查以及维修等所发生的费用中，数介科技免收人工费，只收成本费。

7.5 热线支持服务

数介科技的公司总部设立在北京，在南京成立了办事处并长期驻扎专门的技术支持人员能够及时、快速的响应用户的需求。数介科技提供 7×24 小时的技术热线支持服务。

热线联系方式：

技术支持热线：010-82053991

项目联系人：张晓宇　　电话：18611665193

技术支持号码：xxxxx　　联系人：温承华

传　真：010-82053992

E-mail 地址：service@aleiye.com

热线支持的范围：

数介科技公司提供的所有产品（包括所集成的产品）。

7.6技术培训

为了保证数介科技所提供的产品在运行中更好的工作，将为用户培训一批合格的系统维护人员和工程技术人员。

培训总则

提供满足用户要求的培训服务；

向用户提供高水平的培训，所提供的培训计划随投标文件一起提交；

向用户派的培训教员具有丰富的理论知识和相应实践经验；

所有的培训教员用中文授课，所有的培训资料用中文书写；

可根据实际需要提供用户切实所需的相关培训，具体细节双方可另行协商；

为所有被培训人员提供有关培训的实验环境、文字资料和讲义等相关用品；

培训目标

通过培训，系统维护人员能够理解并掌握数介科技产品的使用及其如何与其他相关系统配合，能够熟练地掌握产品相关软硬件的维护工作，并能及时排除大多数的系统软件和硬件故障。最终具备独立完成系统各项应用和维护系统安全稳定运行的能力，以及阅读系统清单、分析系统故障等工作的能力。

培训内容

类别	培训内容
基本理论培训	➢ 大数据的常用技术 ➢ Aleiye 平台的大数据技术
本次工程	➢ 本次工程系统的构架、原理和产品配置

专项培训	➢ 产品的工作原理、技术特性和功能
	➢ 产品的安装、测试
	➢ 产品的操作方法、参数设置
	➢ 产品的日常维护、简单故障检测与排除
	➢ 整个系统的日常管理和维护
	➢ 系统运行和业务开展所需的其它相关培训
	➢ 被培训人员根据要求完成指定的操作和实践
	➢ 根据运营需要进行操作考核

培训相关事宜

培训类型	地点	时间	人数	备注
现场培训	双方商定	1-3 天	人数不限	/

7.7 技术文件

数介科技的所有技术资料文件均按照相关要求书写，使用国际电信联盟（ITU-T），国际电工委员会（IEC）所推荐的标准符号和术语，并向用户提供本次项目所需的完整的技术文件，具体包括：

⑴ 系统总体说明书；

⑵ 产品的使用手册，包括详细配置、技术性能、功能、工作原理、使用操作及维护方法；

⑶ 产品安装调试说明；

⑷ 产品测试验收手册与规范建议，包括测试方法、操作程序等；

⑸ 根据实际情况和需要，向用户开放的协议和接口标准等；

⑹ 用户在本次项目中所要求的其它资料和文档。

7.8 升级扩展服务

数介科技提供的设备和系统完全符合各种相关标准，对于目前尚无标准可循的、将来标准有更改或标准有提高的部分，数介科技承诺在相关标准出台后，按用户的要求在一定时间内（具体时间与数介科技商定）免费为本次系统进行升级，使之符合新标准。

将来系统业务扩展时，数介科技将为用户提供扩展服务，并以优惠的条件向用户提供相关的产品和服务，具体细节双方另行协商确定。

注：以上售后服务承诺与培训计划中的条款以合同最终签订为准。

（此页以下无正文）

ALEIYE

让 | 大 | 数 | 据 | 更 | 简 | 单

公司地址：北京市西城区新街口外大街28号普天德胜大厦A座405

邮　　编：100088

联系电话：010-82053991

电子邮箱：service@ALEIYE.cn