# AiThink 用户与实体行为分析系统

# 用户操作手册

# 目录：

# 1 用户总体风险

通过本页面，您可以洞察用户总体风险情况，通过用户风险排行及风险类型分布等功能，快速排查您最需要关注的用户及相应风险。

## 1.1 解决方案视角

通过切换解决方案视角，用户可以查看在不同解决方案（主机安全、数据库安全、账号安全及通用解决方案）下的用户总体风险情况。切换解决方案视角后，下方数据皆会随视角改变： 【通用解决方案】展示系统当前接入数据的所有用户风险排名。 【主机安全解决方案】以主机为视角分析用户对主机的操作及主机间通信行为，展示主机相关的风险排名。【数据库安全解决方案】展示系统当前所接入数据中数据库账号及数据库相关的风险排名。【账号安全解决方案】以用户账号为视角分析用户异常行为，包括邮件账号、VPN 账号、OA 账号、AD 账号、零信任账号等，展示用户账号相关的风险排名。 点击解决方案视角右侧图表，即可跳转至相应解决方案大屏界面，使得用户能够通过画像信息快速的掌握当前风险态势。如图 1。


图 1 解决方案视角

## 1.2 排行类内容详情

### 1.2.1 用户信息展示

在用户风险排行中，默认展示用户基本信息（帐号类型、组织架构、角色、上次活跃时间等）、风险分数及排名。

### 1.2.2 用户分值及排名

每个用户会在其信息后方展示出该用户的当前的分数值，并且分值会展示出与上次计算分值的变化情况：↑表示当前分值较上次计算分值为上升、—表示当前分值较上次计算分值不变、↓表示当前分值较上次计算分值为下降。

排名顺序以当前分值高低进行排序，可对排行榜进行下拉浏览，并且最多下拉到 100 名。同分值的用户系统默认排名显示为一样。

将鼠标移动到用户后方的分值上，可以查看该用户最近一周历史风险趋势图，将鼠标移动到展开的历史风险趋势图中，还可以查看到具体日期时间节点的用户风险分值。

### 1.2.3 关注用户及离职用户

在页面右侧用户排行中，展示关注用户和离职用户的风险排行榜，两个类型可以随意切换。

关注用户：为该系统在用户管理模块中对指定用户进行重点关注的用户。

离职用户：已经离职的用户。

### 1.2.4 用户行为画像入口

在用户排行功能区域，可以点击相关用户信息区域，点击有页面跳转进入到该用户的行为画像页面。

## 1.3 图表类内容详情

### 1.3.1 最近一周趋势图

该趋势图主要展示日高风险用户数和日活跃用户数两个指标，显示近七天的数据，并且点击图表右上方图例可以对图中的曲线进行选择性展示。

鼠标移动到相应的曲线的具体日期节点上，此时会弹出相应的数据详情，具体显示内容为：日期、日高风险用户数、日活跃用户数、查看当日数据。如图 2 所示：

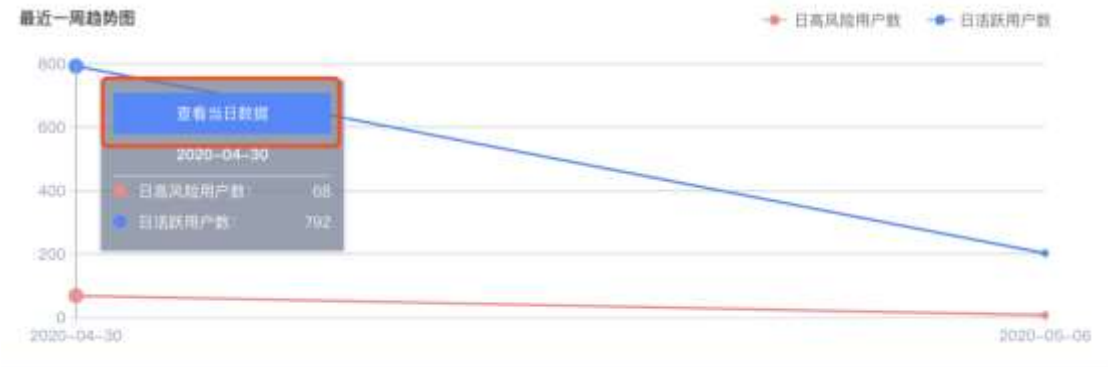



图 2 具体日期时间节点详情

点击“查看当日数据”按键后，页面中的最近一周趋势图，用户风险分布图，风险类型分布，这三张图表内容会进行联动展示，只展示选择日期的数据。如图 3 所示：


图 3 图表联动展示

### 1.3.2 用户风险分布图

该图表主要展示在某天的时间节点上用户风险值的分布情况，并且可以对四个等级的风险用户进行筛选显示。图 4 所示：

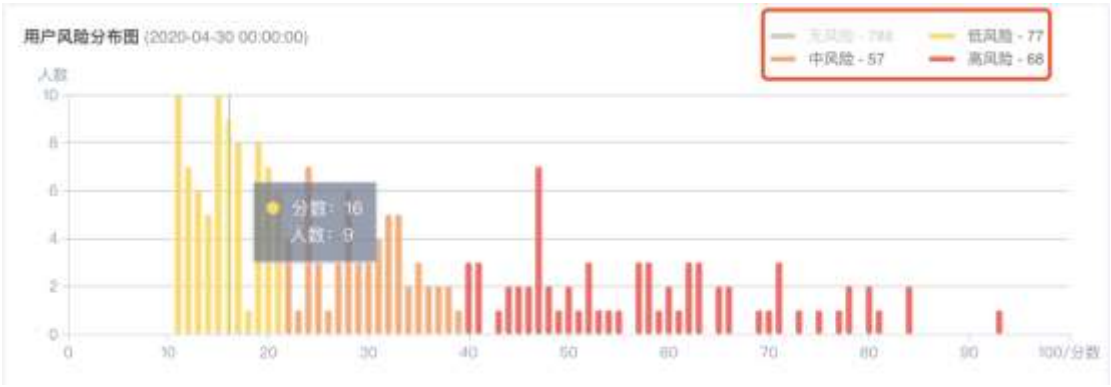


图 4 用户风险分布图

### 1.3.3 风险类型分布图

该图表主要反映含有风险用户的风险类型，从高到低排序，并且每种风险类型显示出其中风险值最高的 5 个用户（top5），如图 5 所示。并且可以点击该用户主键名称，跳转到该用户的行为画像页面。


图 5 风险类型分布图

## 1.4 页面数据跳转及筛选功能

### 1.4.1 风险阈值调整

风险阈值调整功能可以根据用户的实际情况，自由更改风险等级的分值阈值区间，改动后立即生效。并且对整个用户总体风险都有效果。点击页面中的“风险阈值调整”按键后弹出相应的操作弹窗。图 6 所示：


图 6 风险阈值调整

在风险阈值调整窗口中，含有四个风险等级：

无风险：最小值为 0，最大值为 97，页面颜色为：绿色；

低风险：最小值为 1，最大值为 98，页面颜色为：黄色；

中风险：最小值为 2，最大值为 99，页面颜色为：橙色；

高风险：最小值为 3，最大值为 100，页面颜色为：红色；

默认阈值：

无风险：0——10

低风险：11——30

中风险：31——70

高风险：71——100

点击“重置默认阈值”按键后，四种风险等级阈值范围恢复到默认阈值。

### 1.4.2 刷新周期调整

刷新周期调整功能，主要用于调整用户总体风险页面数据刷新周期，可选择时间范围有：1 分钟、5 分钟、10 分钟、30 分钟、1 小时。选择不同的刷新周期，页面会根据所选刷新周期重新计算所有数据。

同时用户也可以选择统计计算分数的数据时间区间，有最近一周、最近一个月、最近三个月、最近六个月四种时间跨度可供选择。用户可根据自己的实际情况随心将刷新周期和数据时间进行组合，更加符合实际场景需求。

系统默认刷新时间为 10 分钟，数据获取时间周期为最近一周。如图 7 所示：


图 7 刷新周期调整

### 1.4.3 数据类型选择

用户可以直接点击页面右上角数据筛选类型下拉框，可以下拉选择【已录入的用户/数据中发现的所有用户】。默认为数据中自动发现的所有用户。该选择相当于一个过滤条件，会作用于整个页面的所有图表。选择后立即刷新。

# 2 用户行为画像

通过本页面，您可以针对特定用户进行全方位的用户行为画像分析，用户行为画像解决方案视角默认与用户总体风险、特征管理内视角一致，默认显示信息包括该用户姓名、关注权重、工作状态、VPN 账号和风险评分等信息，提供风险详情模式和全局画像模式这两种模式。

全局画像模式：提供包括该用户的风险趋势图、风险事件分布图、数据源视角和风险类型视角的多种可视化图表信息，支持自适应排序或固定排序。

风险详情模式：提供包括该用户的风险趋势图、风险事件分布图、风险详情（描述、详情、处置建议和相关可视化图表），其中风险详情支持以风险或以时间轴排序。

## 2.1 全局画像模式

从左侧功能菜单栏或者点击指定用户进入到用户风险画像页面，具体展示如图 1 所示：

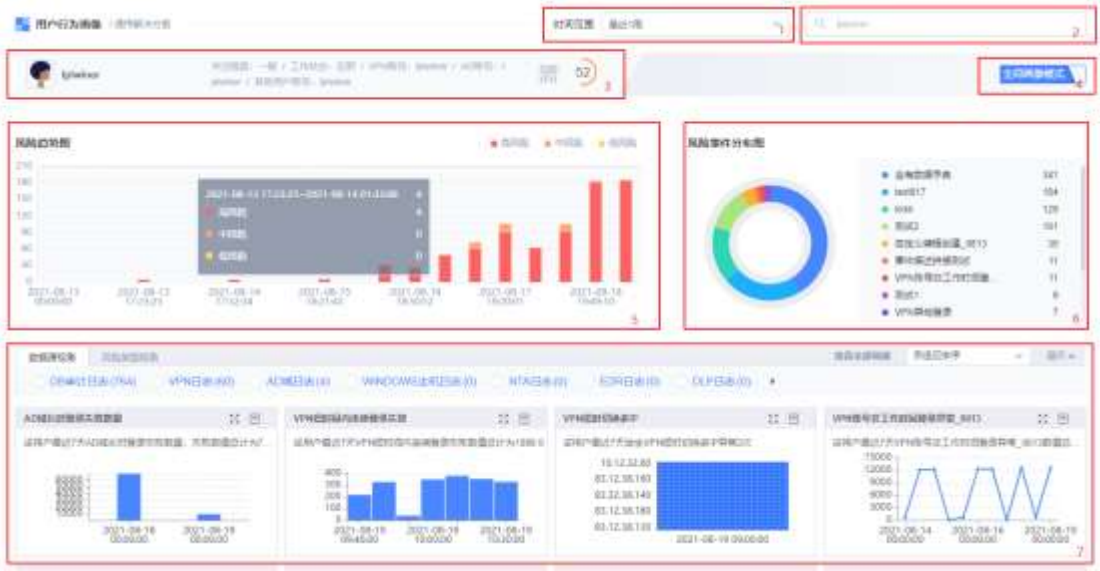


图1　用户行为画像

用户行为画像-全局画像模式主要分为以下功能模块，见表 1 所示：

| 序号 | 名称 | 说明 |
| --- | --- | --- |
| 1 | 时间范围 | 默认显示最近一周，可以选择时间范围：最近一周、最近1个月、最近3个月、最近6个月，选择后用户行为画像页面立即执行离线模型，等待计算结果返回、显示数据。 |
| 2 | 查询功能 | 默认查询框中显示为当前用户名，在输入框中输入用户名后回车可直接查询到输入用户的用户行为画像。 |
| 3 | 用户信息 | 该区域主要展示该用户的基本信息，包括所有用户在用户管理中录入的用户信息，当信息内容超过显示范围时，会以“……”形式代替，鼠标放到其上方可以查看全部信息；若此用户是非录入用户，则可能没有用户基本信息显示。 |

| | | |
|---|---|---|
| 4 | 模式切换 | 该功能用于切换用户全局画像模式和风险详情模式。 |
| 5 | 风险趋势图 | 风险趋势图主要展示该用户在最近一周时间内的风险分值变化情况，其图例有筛选功能，会联动风险趋势图、风险事件分布图和下方的全局画像。 |
| 6 | 风险事件分布图 | 风险事件分布图展示最近7天当前用户风险事件的分布情况。点击右侧图例，图表对应选中，可联动风险趋势图、下方的全局画像。 |
| 7 | 全局画像区域 | 全局画像区域主要分为两个视角：数据源视角和风险类型视角。不同的视角中含有的特征的类型不同，具体特征见特征管理模块。相关操作见下文详解。 |

表1　用户行为画像-全局画像模式功能模块详情

### 2.1.1 风险趋势图详解

风险趋势图主要展示用户最近一段时间内的风险分值变化，将鼠标移动到具体的柱状图上时，可以查看到具体时间范围和各风险等级对应风险事件数量，并且可以对高中低风险等级事件进行筛选显示，联动风险趋势图、风险事件分布图以及风险详情。如图 2 所示：


图2　风险趋势图详情

### 2.1.2 风险事件分布图详解

风险事件分布图主要展示用户最近一段时间内的风险事件分布图，将鼠标移动到具体的环形图上时，可以查看到该风险事件总数量和各风险等级对应数量。点击图例，会默认选中对应图表部分，联动风险趋势图、风险详情以及数据源/风险类型视角，如图 2 所示：


图3　风险事件分布图详情

### 2.1.3 全局画像详解

全局画像内共展示两种视角内容：数据源视角、风险类型视角，默认显示数据源视角，特征类型可以展开查看，每个特征图可以将鼠标移动到其上方查看数据详情，并且可以点击查看日志按键去查看更多相关的原始日志。

特征图存在排序功能，可以选择【自适应排序/固定排序】，默认为自适应排序。自适应排序会根据每个特征图内在的实时风险评分贡献度进行排序，方便用户快速排查最重要的信息。固定排序适合培养用户的固定排查习惯，形成排查记忆。也可以直接点击页面右上角“查看全部画像”按键，显示全部特征画像。如**错误!未找到引用源。**所示：

图4 全局画像

全局画像可展开，如图 5 所示：

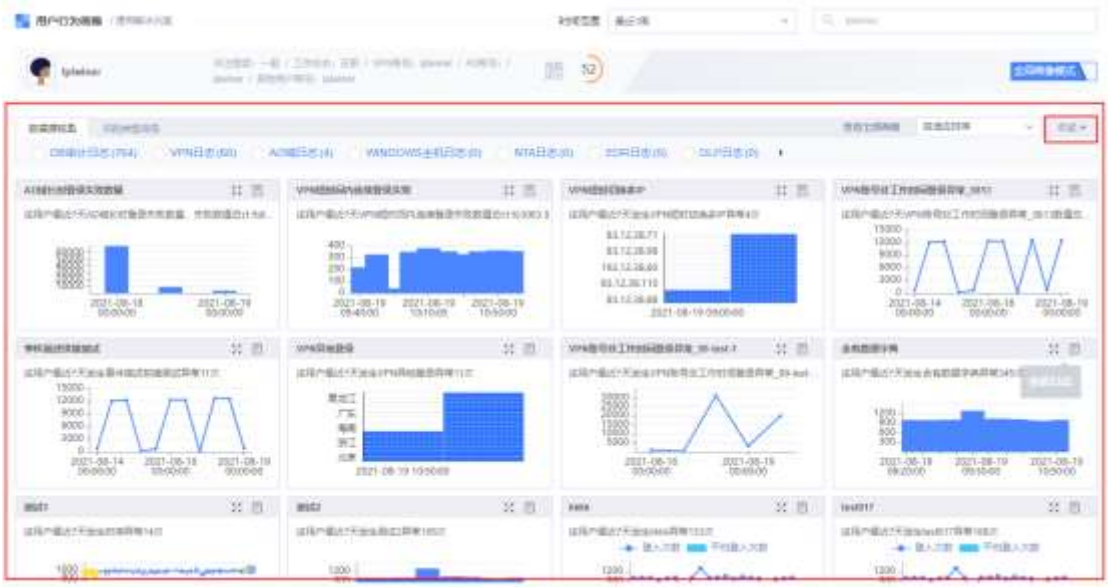


图5 全局画像展开状态

## 2.2 风险详情模式

风险详情模式主要展示以下内容：用户信息、风险趋势图、风险事件分布图以及风险事件详情，具体展示情况如**错误!未找到引用源。**所示：

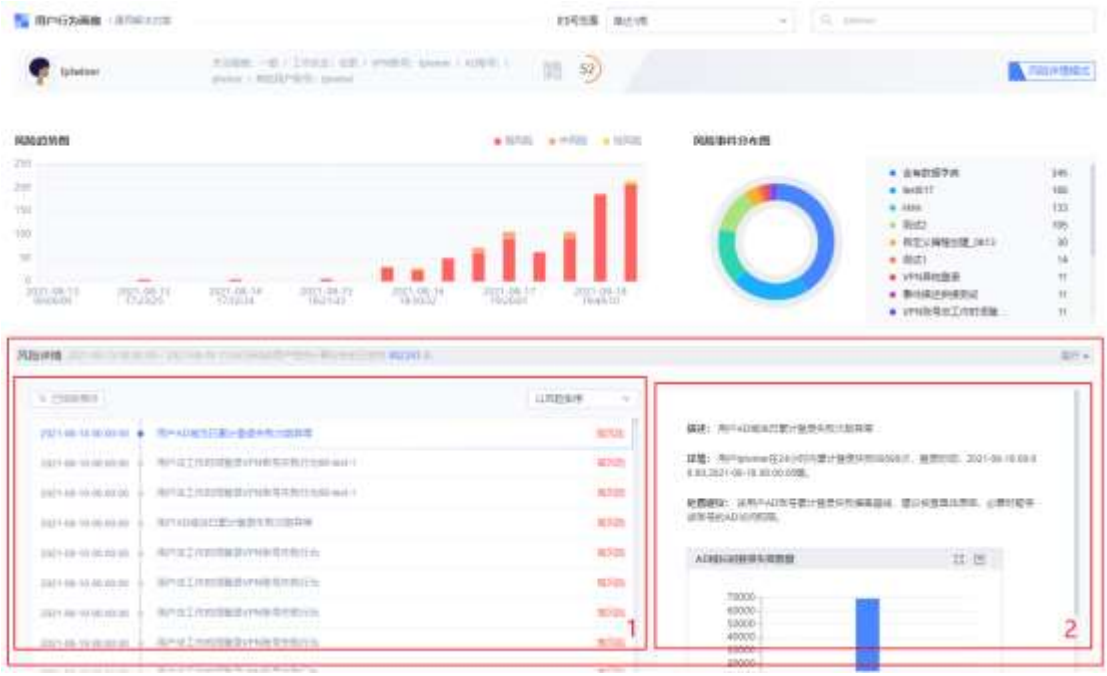


图6 风险详情模式

风险详情模式与全局画像模式有所不同，具体展示在如下 0 中：

| 序号 | 名称 | 说明 |
| --- | --- | --- |
| 1 | 风险详情 | 风险详情主要展示在一定时间范围内，和该用户相关的日志总数及异常信息列表，具体详情2.2.1。 |
| 2 | 风险事件 | 展示具体相关风险事件详情、特征图及处置意见。 |

表2 相关全局画像内容说明

### 2.2.1 风险详情及风险事件详解

风险详情主要展示在一定时间范围内，和该用户相关计算的日志总数及异常信息列表，并且可以对异常信息列表进行排序查看，点击风险详情模块右上角下拉框，可以对下方列表按照不同方式排序。如**错误!未找到引用源。**所示：

图7 风险事件排序

风险详情列表中，可以对已存在的风险进行剔除和过滤操作，方便用户更细化的排查某些指定的特征和行为异常，使得可以更快速定位危险异常内容，如图所示：


风险详情列表内，可以对特征进行白名单过滤处理，在添加白名单后，系统将不再对添加至白名单的该风险对象的风险特征进行计算，如图所示：


在点击新增白名单后，会弹出添加白名单窗口，窗口内会显示白名单条件，用户可以选择编辑策略名称及策略描述，同时可以选择是否删除最近 7 天的风险事件，若选择删除，则会删除最近 7 天当前风险对象该特征的风险事件，如图所示：


添加成功后的白名单可在白名单模块中查看，详情可参考 17.3 白名单。

风险详情部分可展开/收起，如图 8 所示：

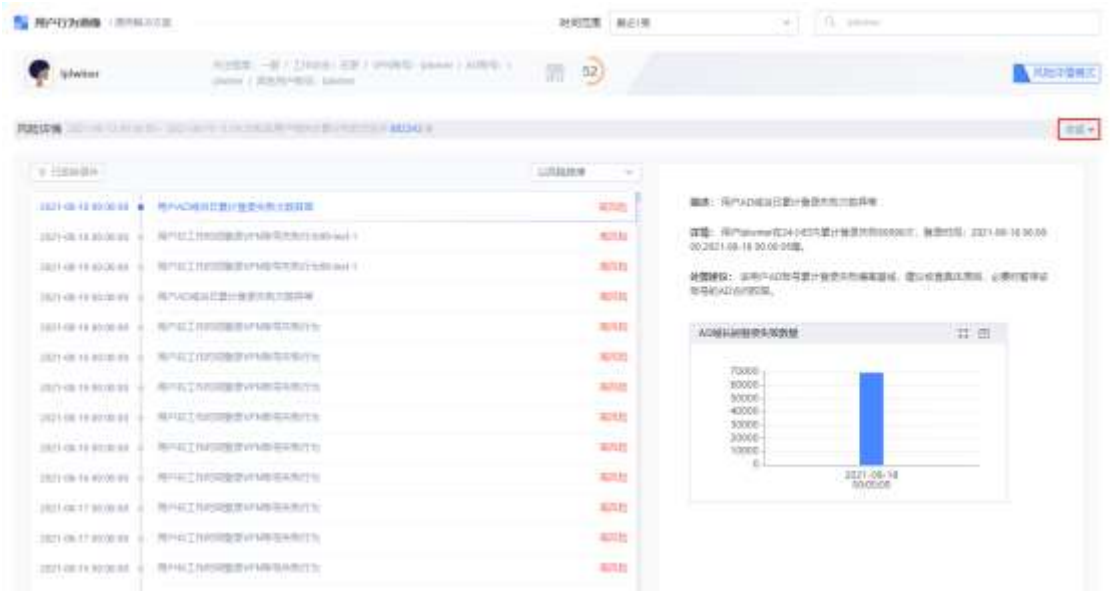


图8 风险详情展开状态

点击左侧风险列表中某风险事件的信息，页面右侧会展示出该异常信息的详情事件、处置意见及相关的风险画像图表，点击风险画像图表右上角按键，可对图表进行放大并展示更多数据，鼠标放置图中的数据可以查看具体详情。若需对改风险事件进行原始日志溯源，可以点击查看风险画像图表右上角中的查看日志图标。放大效果如**错误!未找到引用源。**所示：

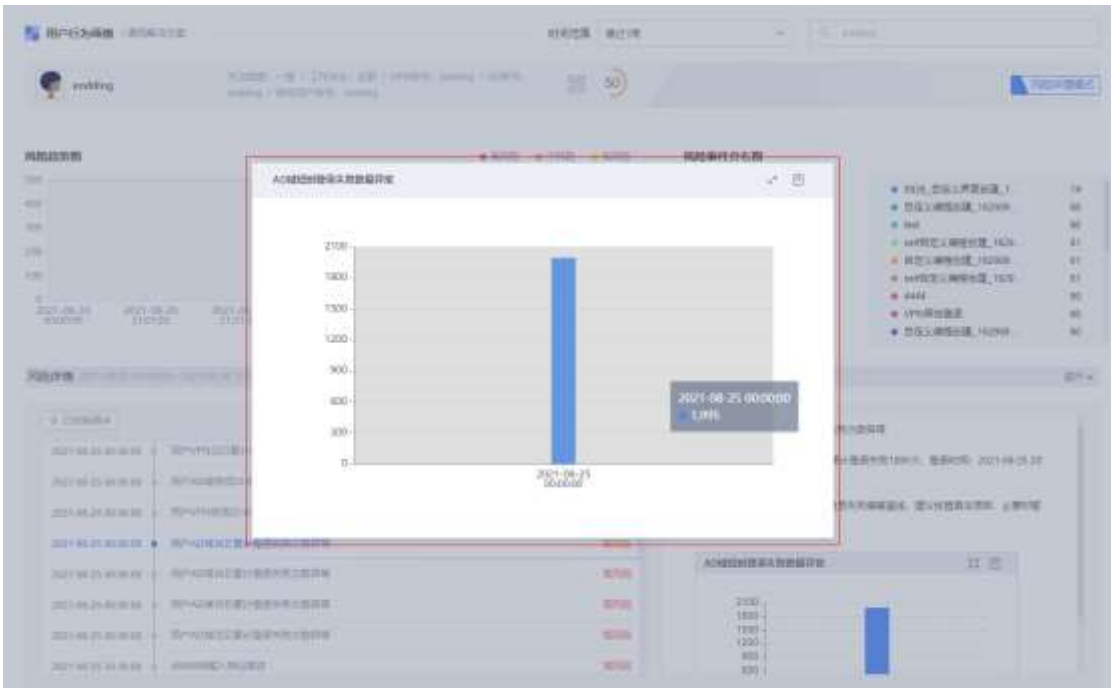


图9 风险事件详情

# 3 用户信息管理

通过本页面，您可以进行用户的相关信息查看、批量导入用户、添加、编辑和删除用户等操作。并且可以设置主动，设置关联其他账号信息。

## 3.1 设置主键

AiThink 用户与实体行为分析系统默认出厂设置以 vpn 账号为主键，用户可以根据自己需求更改主键字段。

当用户管理中不存在任何用户时，可以在系统中更改用户主键，如图 1 所示：

图1　重新设置主键

点击“重新设置主键”按键后，页面直接跳转到用户主键设置页面，该页面中用户可以选择如下主键（主键唯一，不可多选），选定主键并创建用户后，无法再次修改主键字段，如果需要重新修改主键，那么需要删除所有用户才能重新设置主键。如图 2 所示：


图2　用户数据主键设置

## 3.2 批量导入用户

该用户管理模块支持批量导入用户功能，点击页面右上角“批量导入”按键，点击后弹出批量导入操作窗口，用户可以根据窗口中的提示语进行操作，并且支持模板下载。如图 3 所示：


图3　批量导入用户窗口

点击模板下载按键后系统自动下载相应模板，模板中存在相应的字段填写样例，其中主键为必填项。如图 4 所示：

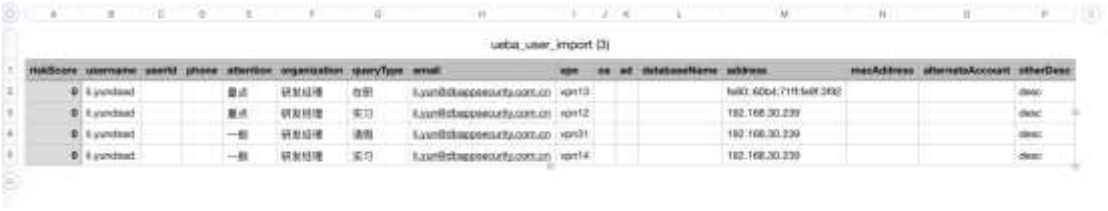



图4　模板内容详情

选择模板进行导入，导入后会覆盖原数据表内容。（请谨慎操作）

## 3.3 添加用户

点击用户管理页面右上角“添加用户”按键，点击后跳转到添加用户页面，其中分别存在 17 个字段需要填写，必填项为主键字段，前方有红色“*”提示，不同的字段还有不同的字符限制。如图 5 所示：

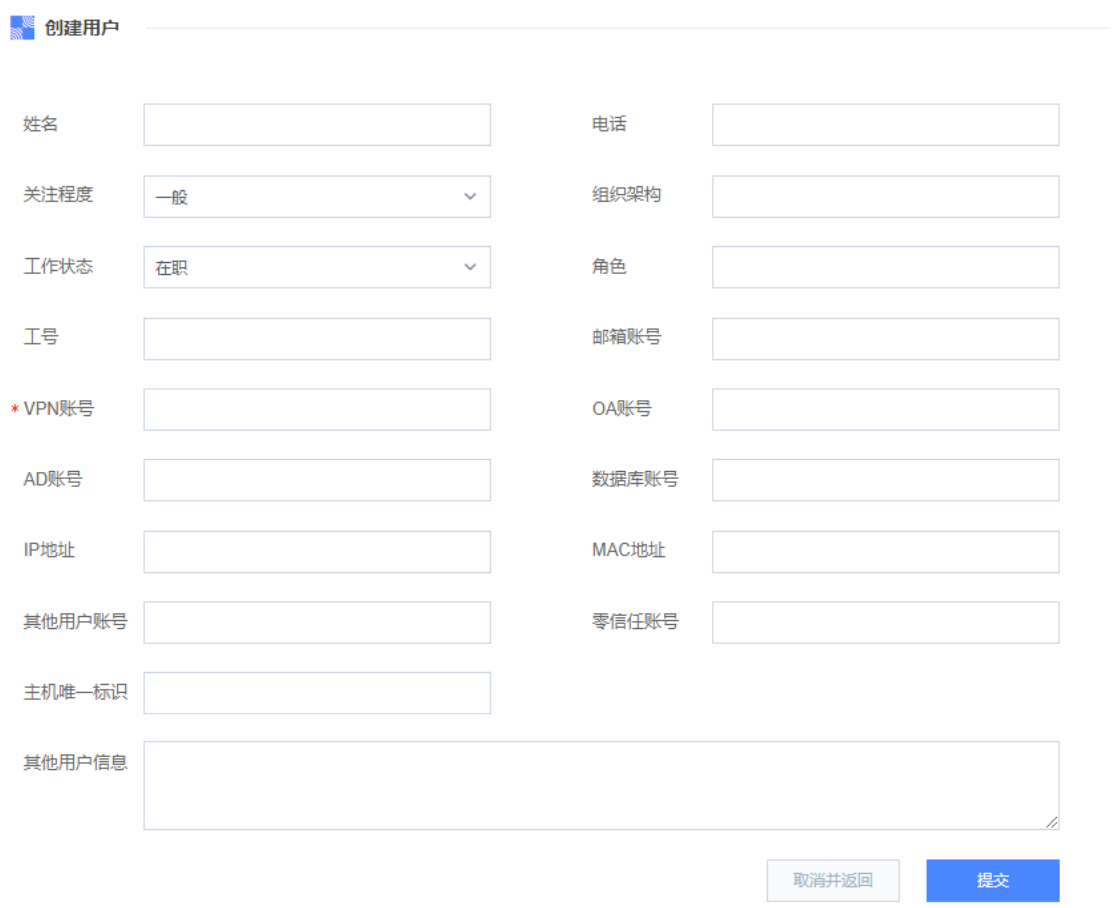



图5　添加用户

## 3.4 全文搜索

用户管理模块支持全文搜索功能，并且支持模糊查询，可以在输入框中输入任何内容，当符合相关搜索条件时，下方用户列表则显示出查询结果。

## 3.5 用户列表

用户列表中包含如下字段：VPN 账号、分数、姓名、电话、组织架构、工作状态、角色、工号、邮箱账号、OA 账号、AD 账号、数据库账号、IP 地址、MAC 地址、其他用户账号、零信任账号、主机唯一标识、其他用户信息，主键始终显示在列表最前面。

每一列字段都支持排序功能，因字段内容过多，显示器显示不下，用户列表可以左右拖动显示，并且支持多功能翻页组件功能。

## 3.6 修改用户

每个用户都可以单独进行编辑修改，点击列表内操作栏下最后的编辑按键，跳转到该用户的用户信息页面，在该页面中，各个输入框中含有该用户原本保存的信息内容，并且所有内容都可以被修改（主键唯一，不可重复，不可为空）。

当修改的内容包含主键时，修改成功后，计算该用户的风险分值会重新以新的主键内容进行计算。

## 3.7 删除用户

用户管理模块支持用户单个及批量删除功能，选择一个或者多个用户，点击页面左下角“删除”按键，点击后页面弹出删除二次确认窗口，点击其中的确定，则删除选择用户。

## 3.8 关注用户

创建用户及修改用户中，可以选择对该用户的关注程度。如图 6 所示：


图6　用户的关注程度

后期可以在用户列表中对用户进行关注和取消关注操作。如图 7 所示：

图7　关注用户

## 3.9 离职用户

创建用户及修改用户中，可以选择该用户的工作状态。如图 8 所示：


图8　用户的工作状态

## 3.10 账号自动发现

账号自动发现功能，默认为开启状态，开启后自动发现接入数据中的其他数据类型，并且会将发现的数据类型关联到已设置的主键中，并会将发现的用户自动录入。相关用户会在用户列表中进行显示，并且用户来源为自动发现。

该功能可以自动发现除主键外其他数据源的分析对象，并进行自动关联，从而提供跨数据源的安全分析及关联能力。如图 9 所示：

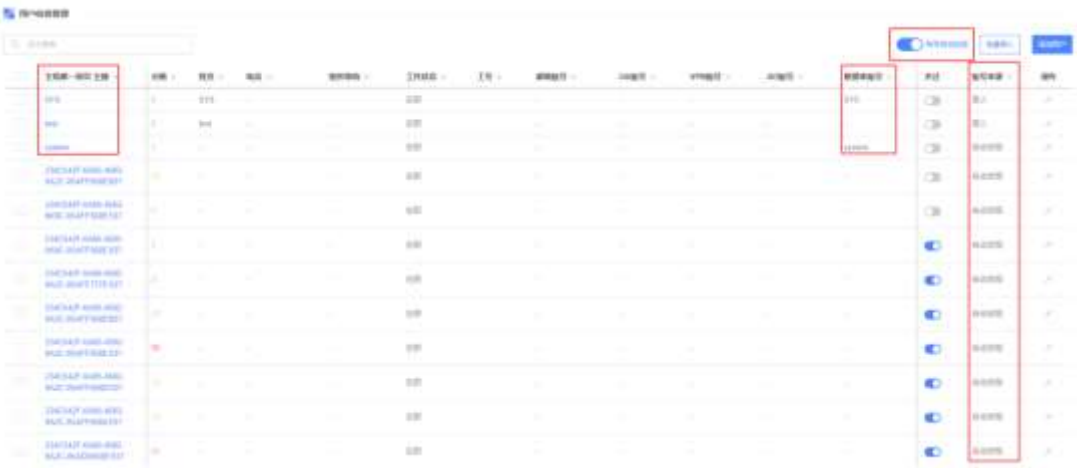


图9　账号自动发现

# 4 用户特征管理

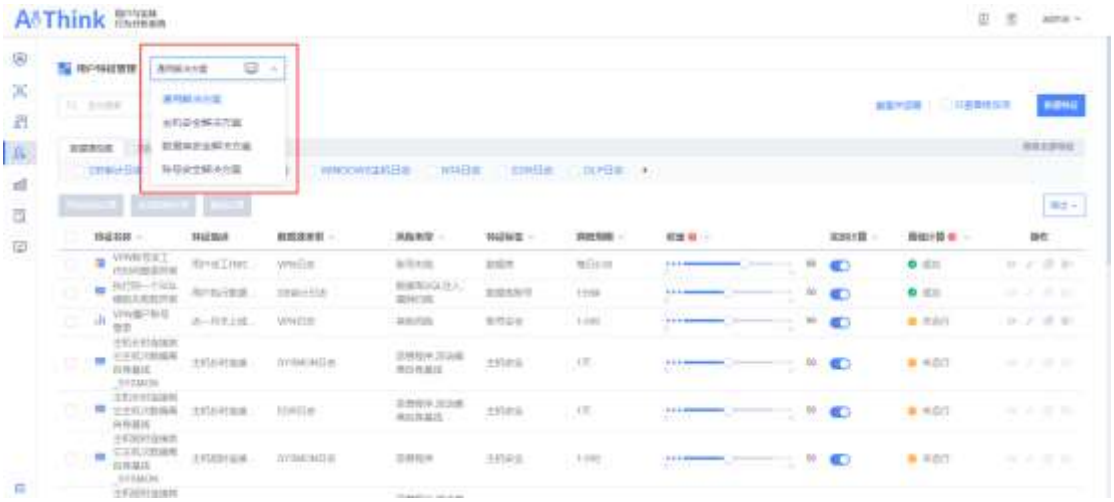
通过本页面，您可以搜索、查看、编辑、克隆和删除用户特征，对特征名称、特征描述、数据源类型、风险类型、调度周期和权重等进行调整。

页面提供自定义编程创建和自定义时序创建两种新建特征方式，同时内置了 100+个 UEBA 用户通用特征场景，开箱即用。

## 4.1 解决方案视角

解决方案视角可以更好地展现本产品在不同问题方面的特征，针对不同方案展现不同视角。

解决方案视角分为：通用解决方案、账号解决方案、数据库安全解决方案、主机安全解决方案；不同的解决方案视角展示不同的特征，切换解决方案视角将影响全文搜索、重置并部署、只查看修改项、数据源视角、风险类型视角、查看全部特征，即切换解决方案视角后该些功能只展示当前方案下的特征。如图:



解决方案视角

通用解决方案（默认视角）展示系统内所有特征。点击视角内大屏按键可以跳转至用户行为风险态势大屏。

账号安全解决方案展示特征标签为账号安全的特征。点击视角内大屏按键可以跳转至账号安全态势感知大屏。

数据库安全解决方案展示特征标签为数据库或数据库账号的特征。点击视角内大屏可以跳转至数据库安全态势感知大屏。

主机安全解决方案展示特征标签为主机安全的特征。点击视角内大屏可以跳转至主机安全态势感知大屏。

## 4.2 特征视角

特征视角分数据源和风险类型两类，数据源视角下可选择 DPI，DB 审计，VPN 等数据源进行筛选，风险类型视角下可选择数据泄露，账号被盗，远程办公效率分析等风险类型进

行过滤。无特征激活匹配的选项自动被置灰并且下拉收起默认不展示。点击查看全部特征按钮，返回查看所有特征。如图 1 所示：

图 1 特征视角

## 4.3 特征列表

特征列表含有如下字段，不同字段含有相关的意义。相关字段的详情含义见下表 1 所示：

| 名称 | 说明 |
| --- | --- |
| 特征名称 | 根据新增特征或者修改特征时填写的内容为准，在用户行为画像模块会有相关区域展示。鼠标移动到图标上方，显示对应特征类型。 |
| 特征描述 | 该区域主要用于展示相关特征的解释，可以在创建特征和修改特征时对其进行改动。 |
| 数据源类型 | 该类目主要展示该条特征所属的数据源分类。 |
| 风险类型 | 该区域主要介绍该特征所属风险类型。 |
| 特征标签 | 该区域展示不同的特征属于不同的类型主题。 |
| 调度周期 | 该区域中的值主要介绍该特征的调度计算周期，方便用户根据实际时间需求更改权重设置。 |
| 权重 | 该区域主要用于改变指定特征对整个计算分值系统的影响，并且默认出厂设置为 50，详情信息见下文。 |
| 实时计算 | 该功能可以让用户自定义决定指定特征的开关，当关闭时此特征不进行实时计算。 |
| 离线计算 | 该区域展示特征的离线计算状态，有未运行、成功、运行中、失败，四种状态，鼠标移动到状态上方，有相关的状态详情信息展示。 |
| 操作 | 该处主要为多个操作的集成模块，包括查看、修改、克隆、删除。具体操作详情见下文。 |

表 1 特征列表字段详情

## 4.4 权重

### 4.4.1 权重调整

特征权重，主要功能在于决定相关用户风险分值的重要程度，默认权重出厂设置为 50，可以对其进行修改调整，调整范围在【0，∞】之间，其中“0”代表对整体影响为 0，类似于关闭该特征，“∞”代表将该特征的权重重要性无限放大，类似于只关注该特征。如图 2 所示：

图 2 特征权重

对相关特征的权重进行调整后，页面右上角会出现“部署最新权重”按键，此按键在没有对特征权重做出改动时默认隐藏，仅在修改特征权重后，该按键才会出现。如图所示。

### 4.4.2 重置权重

点击特征管理页面右上角中的“重置权重并部署”按键，可以对当前视角所有内置特征的权重进行重置并生效，生效后默认特征的新权重都为 50。

点击“重置权重并部署”按键后会弹出二次确认窗口，如图 1 所示：点击确定后方可重置权重成功。


图 1 重置权重二次确认窗口

### 4.4.3 查看修改项

特征管理页面中支持只查看修改项的功能，该功能方便用户对修改的特征的进行查看筛选，点击页面右上角“只查看修改项”勾选框后直接生效。

## 4.5 实时计算

用户可以根据实际使用场景，决定特征是否开启实时计算功能，当关闭特征的实时计算，则该特征不进行未来时间的特征计算和得分计算。如图 4 所示：

图 4 实时计算

## 4.6 离线计算

离线计算主要功能可以帮助用户因为业务原因需要溯源过去时间的特征计算结果。

离线计算可以选择一个或者多个特征进行数据时间范围可配的离线任务，并且可以根据实际使用情况进行选择是否覆盖已计算结果。

特征离线任务状态有未运行、成功、运行中、失败等四种状态，默认特征为未运行状态。当特征进行离线任务计算，则该特征会靠前排序显示。离线计算页面如图 5 所示：

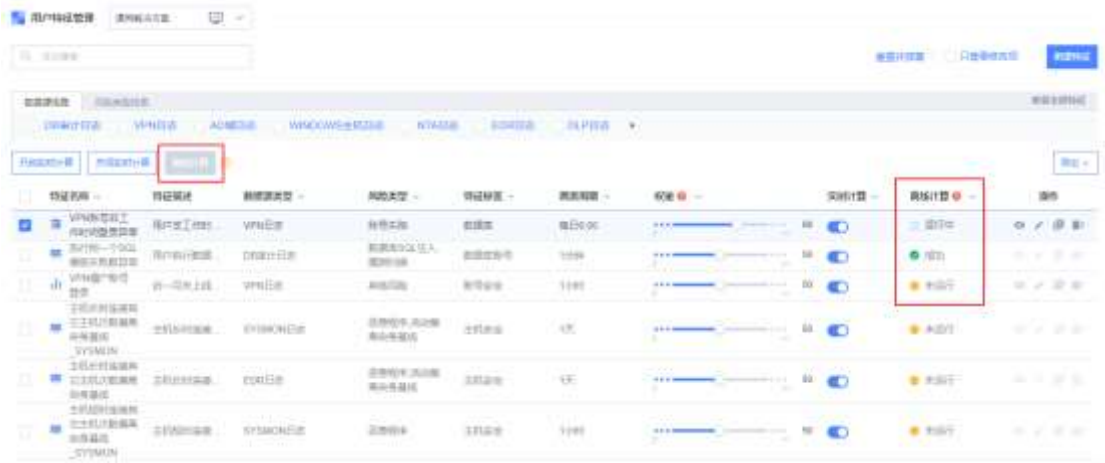


图 5 离线计算

离线计算可以自由选择计算时间和是否覆盖计算结果。如图 6 所示：


图 6 离线计算时间及覆盖对话框

## 4.7 操作

### 4.7.1 查看特征

对于非内置的特征，点击特征操作栏中的第一个查看特征详情按键，点击后页面跳转进入到相关特征的详情页面，如图 7 所示：

图 7 查看特征详情

在该页面中，主要展示被选择查看特征的相关创建流程，并且可以查看每个创建步骤的详细信息。

### 4.7.2 编辑特征

在特征管理模块中，允许用户编辑特征信息，但是只能编辑自建特征信息，无法编辑出厂设置中自带的特征。点击特征操作栏中的第二个编辑按键，页面弹出编辑特征窗口，其中可以编辑内容包括：特征名称、特征描述、数据源类型、风险类型、调度周期。创建特征编辑界面如图 8 所示：


图 8 编辑特征

特征名称选项为必填项，并且名称须唯一。数据源类型、风险类型、调度周期三个选项后方都有相关的提示信息标记，用户可点击了解这三处参数的作用，方便操作。

### 4.7.3 克隆特征

在特征管理模块中，允许用户对所有特征进行克隆操作，方便用户创建类似的特征，减少操作难度及步骤。

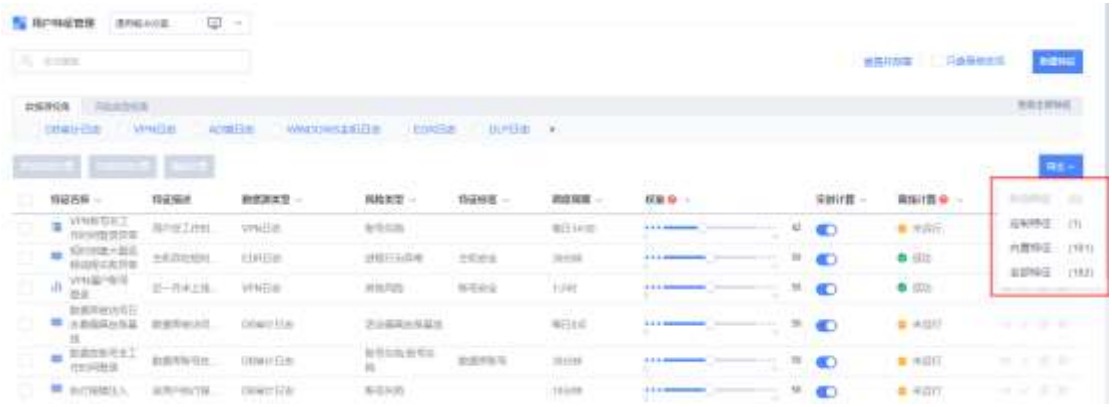
用户可以点击特征操作栏中的克隆按键，点击后页面会跳转到相关创建特征页面。此页面中含有被选择克隆特征的所有信息，用户可以自己对有需要改变的信息进行修改操作。

### 4.7.4 删除特征

可以根据相关需要，对相关的特征进行删除操作，点击指定特征后方操作栏中的第四个删除按键，点击后页面弹出二次确认窗口，只有在点击确定后才能对指定特征进行删除。

## 4.8 导出

点击导出，显示四种特征（所选特征、定制特征、内置特征、全部特征）及对应条数。如图：

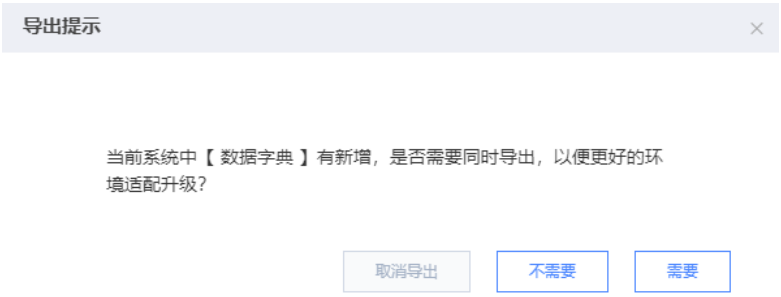


### 4.8.1 所选特征

勾选特征，点击导出，所选特征的条数对应勾选条数。

点击所选特征，判断特征元数据没有更新时，直接导出所选特征的升级包，如图：

特征元数据（数据字典、特征库表）有新增时，弹出提示如图：“当前系统中【】有新增，是否需要同时导出，以便更好的环境适配升级？”，【】内容显示对应新增项。




用户可以按需要选择是否导出特征元数据。点击需要，导出特征和特征元数据；点击不需要，只导出特征；点击取消导出，不导出特征升级包。

### 4.8.2 定制特征

点击定制特征，导出所有定制特征的升级包，特征元数据判断同 4.8.1。

aithink_v3.0.2_feature_custom_1629345585547.zip

### 4.8.3 内置特征

点击内置特征，导出所有内置特征的升级包，特征元数据判断同 4.8.1。

aithink_v3.0.2_feature_builtIn_1629345630311.zip

### 4.8.4 全部特征

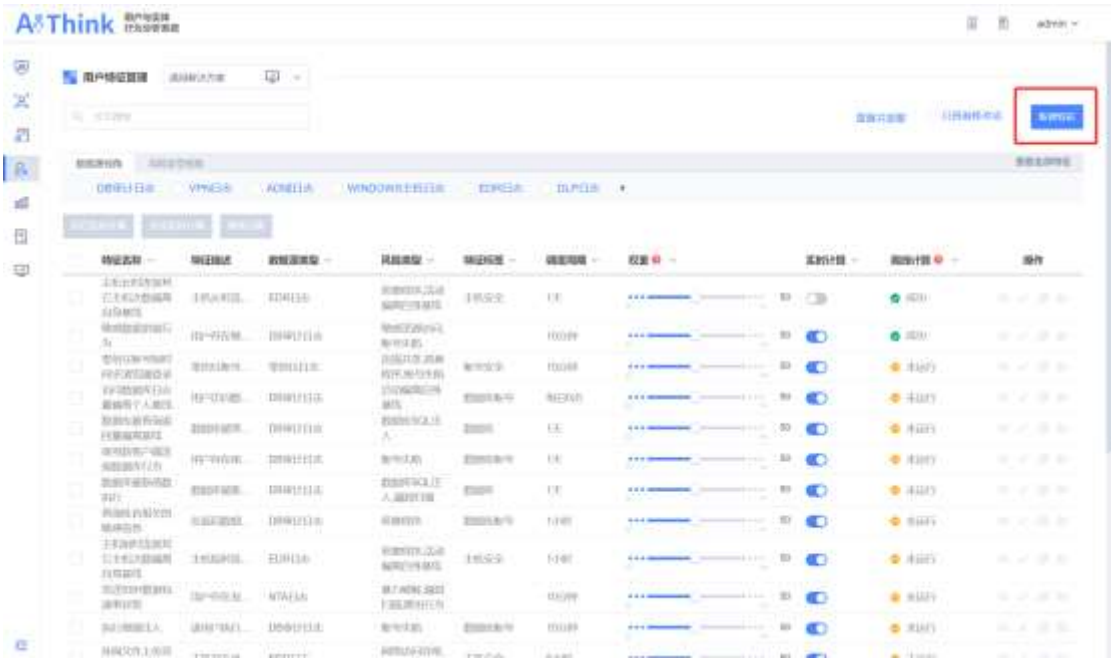
点击全部特征，导出所有特征的升级包，特征元数据判断同 4.8.1。

aithink_v3.0.2_feature_all_1629345687009.zip

# 5 新建特征

创建 UEBA 特征的方式共三种：自定义时序创建、自定义编程创建、自定义编程创建。

点击用户特征管理界面右上角新建特征按键，即可选择创建特征方式。如图：



## 5.1 自定义时序创建

自定义时序创建特征支持直接在界面上点击选择，通过引入时序分析模块的模型进行用户特征的创建。

在选择创建方式为自定义时序创建后，进入自定义时序创建页面。自动生成默认特征名称，格式为“自定义界面创建_XXX”的格式。所有自定义时序创建的数据流向固定，包含 5 个固定节点，从左到右有依赖地按顺序依次配置及运行。如图 2 所示。

图 2 自定义时序创建界面

### 5.1.1 数据关联节点

此处数据关联节点与自定义编程的数据关联节点一致，详情请参考自定义编程创建章节。

### 5.1.2 时序特征节点

此处为每个特征的专属节点，不共用，可以被编辑、查看。该节点是从数据关联结果表中通过界面创建时序特征，用于后续的 AI 异常检测。点击时序特征节点的“编辑”按键，在弹窗下拉框内可以选择符合要求的特征（数据表为数据关联结果表，对象分组为主键的特征才符合要求）。如图 3 所示。


图 3 特征选择

如果没有符合要求的特征或者想要新的特征，可以点击“新增”按键，跳转到创建特征界面，用户可在此创建自己想要的特征。如图 4 所示。该部分的详细信息会在后文的特征列表章节进行介绍。

图 4 特征创建

### 5.1.3 AI 异常检测节点

这是每个特征的专属节点，不共用，可以被编辑、查看。该节点基于时序特征，使用 AI 异常检测算法检测相关异常，作为 UEBA 特征，用于后续风险得分计算。

点击“编辑”按键，在弹窗下拉框可以选择符合要求的 AI 异常检测模型（使用时序特征节点所选特征创建的模型，才符合要求）。如果没有符合要求的模型或者想要新的模型，可以点击“新增”按键，跳转到创建模型界面，选择特征固定为符合要求的特征，创建完之后再选择符合要求的 AI 异常检测模型。

详细描述：可以下拉选择已有模板，如果觉得已有模板不合适，可以对其中非参数的文字进行修改，修改之后的详细描述不会保存在现有模板中。模板如“用户账号一天之内产生访问日志量共计${#3}条，所有用户均值为${#2}条,该用户已经偏离整体基线${#1}%”。

处置建议：可以下拉选择已有模板，如果觉得已有模板不合适，可以对其中非参数的文字进行修改，修改之后的详细描述不保存在现有模板中。模板如“该用户账号有${#1}的风

险，建议结合该用户登录之后的访问行为进一步核查，若情况属实需立即停止该账号的访问权限”。如图 5 所示。


图 5 AI 模型配置

### 5.1.4 特征得分与映射节点

此处节点与自定义编程特征得分与映射节点一致，详情请参考 6.4。

### 5.1.5 风险总得分节点

此处节点与自定义编程的风险总得分节点一致，详情请参考 6.5。

### 5.1.6 画图节点

在 AI 异常检测节点与特征得分与映射节点之间的数据流连线中可以添加画图节点，最多只能添加一个画图节点。如图 6 所示。

图表类型，固定为时序图，不可选择。图内描述，可以下拉选择已有模板，如果觉得已有模板不合适，可以对其中非参数的文字进行修改，修改之后的详细描述不保存在现有模板中。模板如“该用户最近 7 天发生${#1}异常${#2}次”。

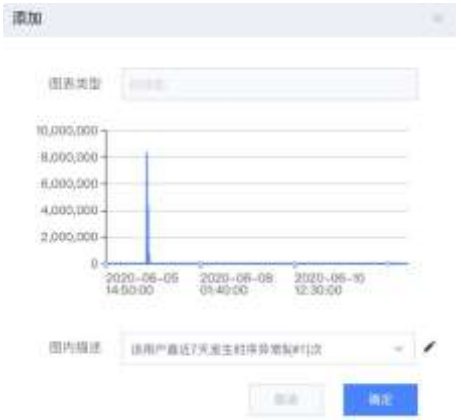



图 6 画图节点

### 5.1.7 验证特征按键及创建特征按键

此处节点与自定义编程的验证特征按键以及创建特征按键功能一致，详情请参考 6.7。

## 5.2 自定义编程创建

自定义编程创建特征使用 Python 语言实现特征的创建，模块收录大部分常用 Python 第三方库，包含多种机器学习及深度学习框架，支持 SQL 预处理数据以提升模型运行效率，同时内置多种情形下的模板以供参考。

在选择创建方式为自定义编程创建后，进入自定义编程创建页面。所有自定义编程创建特征的数据流向固定，包含 5 个固定节点，从左到右有依赖地按顺序依次配置及运行。如图 7 所示。

图 7 自定义编程创建特征

### 5.2.1 数据关联节点

数据关联节点是所有特征共用的一个节点，该节点无法被编辑，只能查看该节点的数据关联结果表。点击数据关联节点右下角查看按键，右侧会弹出弹窗，展示最近 7 天日志重点字段的饼图信息及相关原始日志，饼图展示默认为精简模式，如图 8 所示。

图 8 数据关联节点弹窗展示

同时，点击弹窗右上角的“完整模式”即查看日志所有字段的饼图信息，如图 9 所示。


图 9 完整模式

### 5.2.2 数据过滤节点

数据过滤节点的作用为针对性过滤出构建特征所需的日志，是每个特征的专属节点，不共用。点击“编辑”按键，右侧弹出窗口进行过滤条件的配置，如图 10 所示。

图 10 数据过滤节点编辑窗口

点击“添加过滤条件”，展开条件筛选栏，可在此添加条件、条件组进行过滤。添加的条件字段分为字符型、数值型、时间型，相应的可选择候选值或输入数值。添加条件默认为 AND 关系，添加组默认为 OR 关系。如图 11 所示。


图 11 过滤条件

过滤条件下方为输出数据过滤，可以多选字段输出到数据过滤结果表。固定必选 startTime、userKey 及 primaryKey ，如图 12 所示。输出数据过滤下方为调试时间范围，可以下拉进行选择。如图 13 所示。

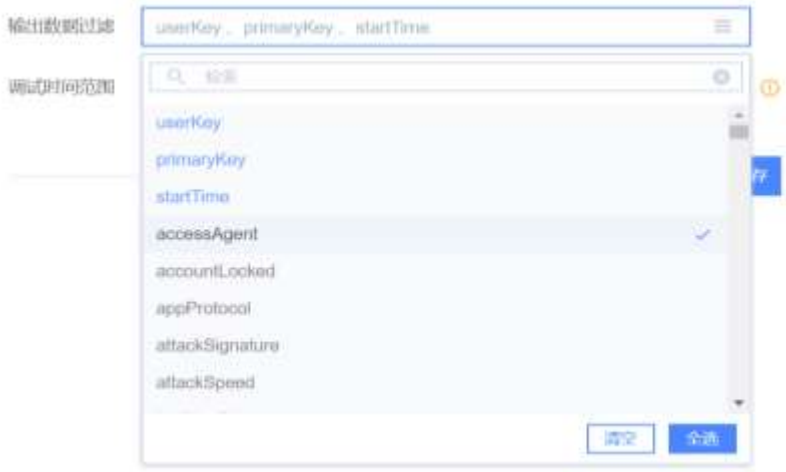



图 12 输出数据过滤

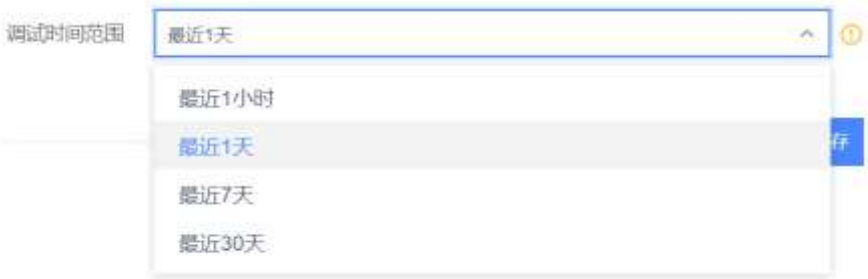



图 13 调试时间范围

在配置完数据过滤条件后，点击数据过滤节点的“执行”按键，开始执行数据过滤，执行过程中会有动画提示，执行成功或失败也会有相应提示。如图 14 所示。


图 14 数据过滤节点执行

待数据过滤节点执行成功后，可以点击查看按键，点击后右侧弹出数据过滤执行结果窗口，可查看数据执行过滤结果。如图 15 所示。

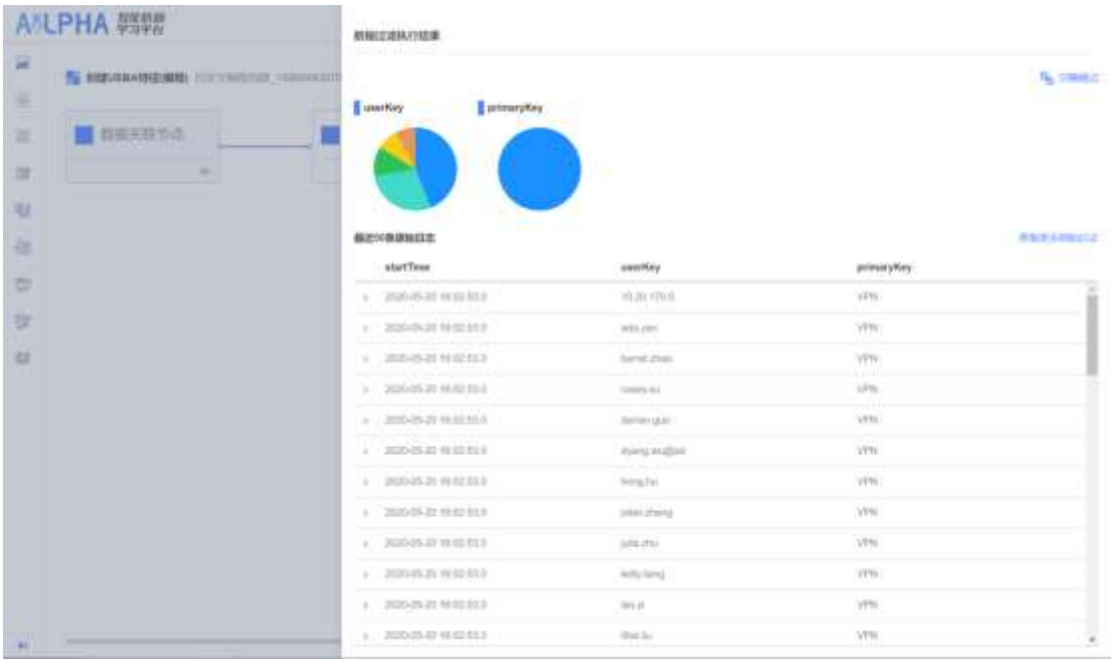



图 15 数据过滤节点执行结果

### 5.2.3 特征计算与事件评级节点

该节点基于上个节点的结果，运行特征计算与事件高中低风险评级的代码及逻辑，将结果写入特征结果表。点击该节点的“编辑”按键，右侧弹出节点配置窗口，可以编辑特征计算及事件评级的相关选项及代码，如图 16 所示。

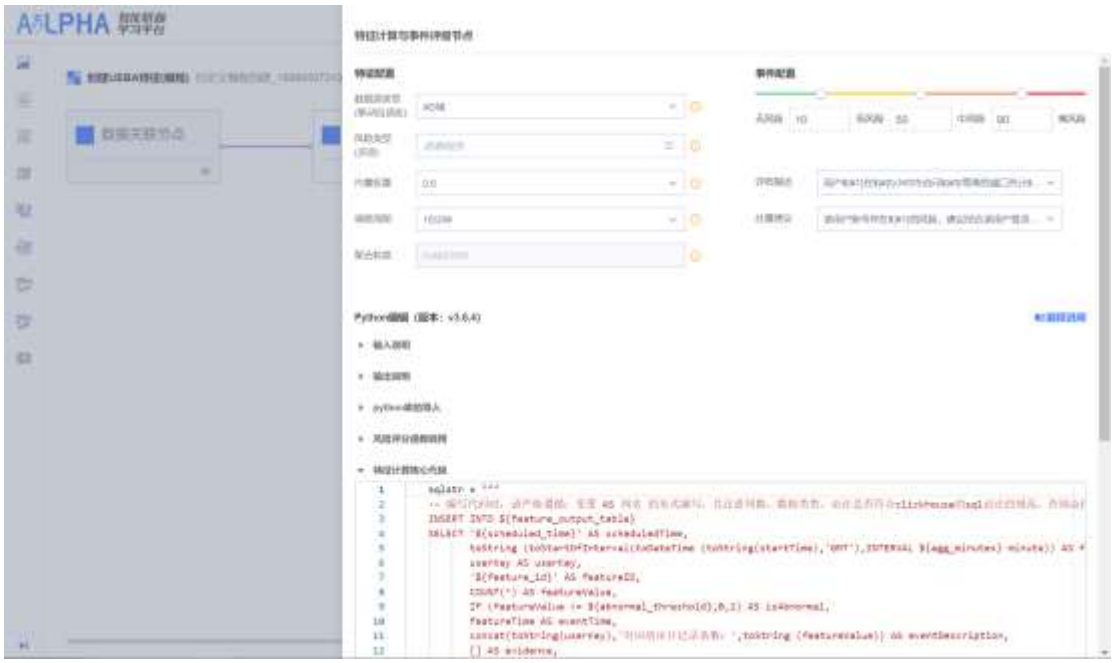


图 16 特征计算与事件评级节点配置窗口

数据源类型：可以选择一种数据源类型，是计算该特征所依赖的主要数据源。选择数据源不正确的情况下，可能因数据问题导致分析结果有所差异。如图 17 所示。


图 17 数据源类型

风险类型：可以选择多个，为该特征所属的风险类型。 点击风险类型下拉框，支持模糊搜索、全选字段、清空字段，如图 18 所示。


图 18 风险类型

内置权重：默认为 0.5，当特征较为重要且聚合粒度较小时，可尝试将内置权重适当调小；当特征较为重要且聚合粒度较大时，可尝试将内置权重适当调大。如图 19 所示。

图 19 内置权重

调度周期，更改调度周期则影响特征的调度时间，默认调度周期为 10 分钟。如图 20 所示。

聚合粒度：该版本的聚合粒度同调度周期一致，其中调度周期每小时 0 分实际聚合粒度为 1 小时，每日 0 点实际聚合粒度为 1 天，每周周一 0 点实际聚合粒度为 7 天。如图 20 所示。

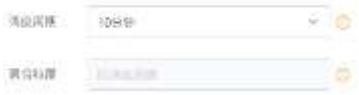


图 20 调度周期和聚合粒度

事件风险阈值：表明“配置事件评级所需的阈值，生成无风险事件，低风险事件，中风险事件，高风险事件”。如图 21 所示。10 分

详细描述：是对特征风险事件的详细描述，可以下拉选择已有模板，如果觉得已有模板不合适，可以对其中非参数的文字进行修改，修改之后的详细描述不保存在现有模板中。如图 21 所示。

处置建议：是对特征风险事假的处置建议，可以下拉选择已有模板，如果觉得已有模板不合适，可以对其中非参数的文字进行修改，修改之后的详细描述不保存在现有模板中。如图 21 所示。


图 21 事件配置

Python 编辑框：用户可在此自己修改编写代码，来改变特征。Python 编辑框内支持语法高亮，Tab 键所占的位置也支持特殊显示，方便用户查看 Python 代码的缩进对齐，减少用户运行 Python 代码的出错概率。其中 Python 编辑框内，输入说明、输出说明、python 库的导入、风险评分函数调用相关代码默认不展开，且不可修改。特征计算核心代码默认展开，可以被编辑。如图 22 所示。


图 22 Python 编辑框

点击“编程说明”按键，弹出参考代码展示窗口，方便用户参考代码，编程说明内的代码可以复制但不能编辑。如图 23 所示。

图 23 编程说明参考代码

在全部编辑完特征计算与事件评级节点的配置后，可以进行执行操作。点击执行后，从数据过滤结果表中拉取数据，运行特征计算与事件评级的代码及逻辑，写入特征结果表（字段固定）；同时弹窗显示执行的相关信息（成功提示或者失败信息）。如图 24 所示。

图 24 执行成功

当执行成功后，可以再点击“查看”按键，查看执行结果。查看功能与数据关联节点内查看功能一致。如图 25 所示。

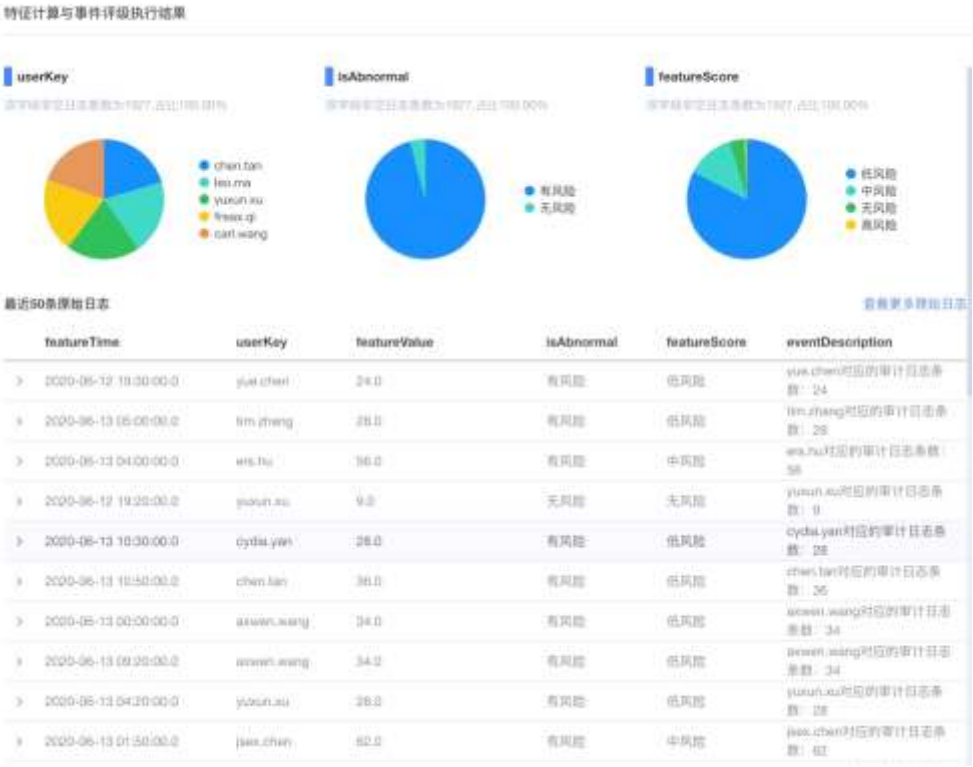



图 25 特征计算与事件评级执行结果

### 5.2.4 特征得分与映射节点

该节点是每个特征的专属节点，不共用。目前该版本不可进行交互，即不可被编辑、执行、查看。该节点会根据特征结果表中最近 7 天的特征数据，使用内置算法完成特征归一化得分计算及映射。

### 5.2.5 风险总得分计算节点

该节点是所有特征共用的一个节点，该版本不可进行交互，即不可被编辑、执行、查看。该节点会根据用户所有的特征得分，使用内置的自适应算法计算用户风险评分。

### 5.2.6 画图节点

在特征计算与事件评级节点与特征得分与映射节点之间的可以添加画图节点，用于形式化展示特征计算与事件评级的结果。如图 26 所示。点击“执行”按键后，图表会根据前一节点的配置而去执行，然后展示结果。点击保存“保存”按键，图表得到保存。

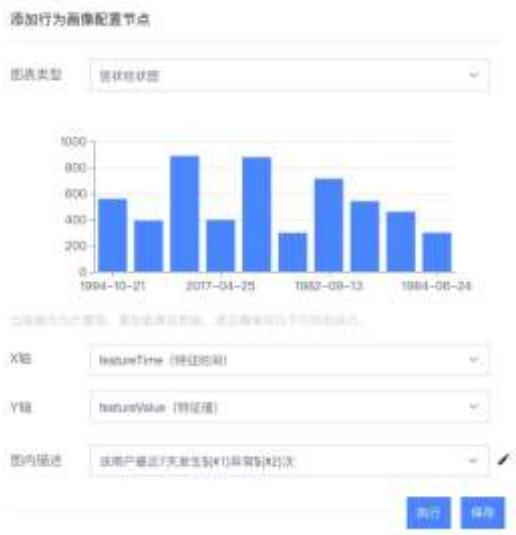



图 26 画图节点配置

### 5.2.7 验证特征按键及创建特征按键

点击“验证特征”按键后，会验证当前页面配置的特征。验证出错时，右侧会弹窗显示相关出错信息以及修改建议。验证通过后，“创建特征”按键生效，如图 27 所示。

图 27 验证特征成功

点击“创建特征”按键，会弹窗显示特征的信息，用户可确认与修改，如图 28 所示。


图 28 创建特征弹窗

特征名称最多可以输入 40 个字符，且不可现有的特征名称重复。模型描述最多可输入 1000 个字符。数据源类型、风险类型、调度周期都特征计算与事件评级节点相关类型一致。权重默认设置为 50，用户可以自由调节，调整为 0 代表关闭特征，调整为∞代表只看该特征而忽略其他特征，1~100 数值越大代表特征的权重越大。点击确定即可完成特征创建。

## 5.3 自定义模板创建

自定义模板创建，为方便用户创建，降低创建特征的难度，系统内置了 7 个模板供用户选择，用户可根据模板按需创建特征，每个模板特征模板不一致，创建流程一致。如图 1 为 7 个特征模板：

图 1 自定义模板特征选择模板界面

以下以第一个模板为例，简述创建流程。

### 5.3.1 数据过滤节点

模板样例简述当前模板风险事件样例。 在数据过滤节点内，用户可以添加条件，针对性的过滤出构建特征所需要的行为日志。 账号类型内的组织架构与角色都为系统内录入数据。用户可在用户信息管理中自行配置，可根据账号特定的组织架构以及角色进行群体行为分析建模。 不同的模板，在行为配置内会默认含有不同的过滤条件、输出数据过滤、调试时间范围，过滤条件、输出数据过滤、调试时间范围等操作方式皆与自定义编程创建方式一致。如图 2。

图 2 数据过滤节点

在添加完条件后，点击“执行”按键，开始执行数据筛选，完成后系统会相应的提示。执行成功后，用户可以点击“预览”按键，查看数据过滤执行结果，如图 3。

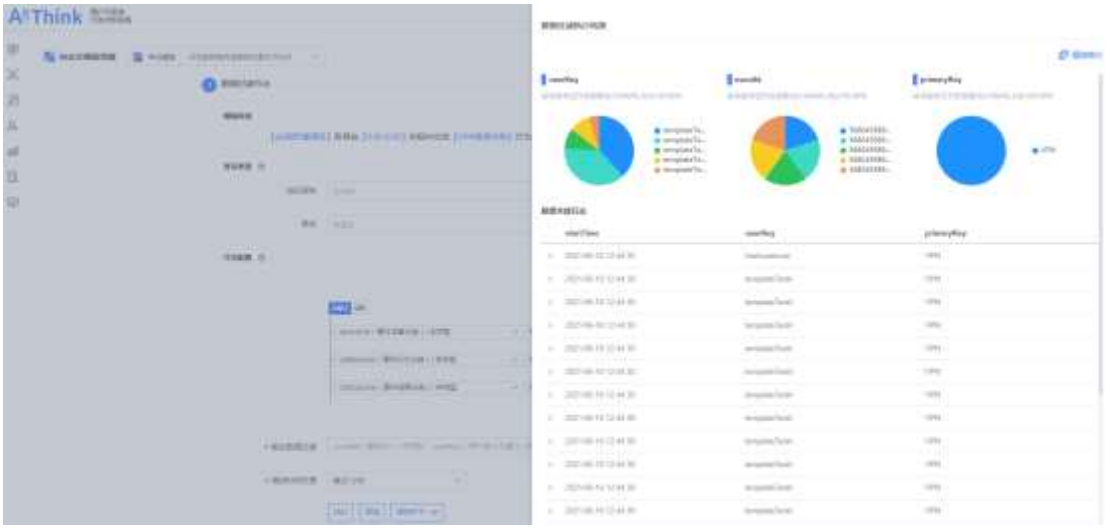


图 3 数据过滤执行结果

### 5.3.2 特征计算与事件评级节点

该节点主要用于特征的计算与事件的评级，该节点数据源即上一数据过滤节点的输出内容，用户可参考样例，并配置自己的特征逻辑。如图 4。

图 4 特征计算与事件评级节点

在配置完条件后，点击“执行”按键，节点开始计算，计算完成后，系统会有相应的提示。执行成功后，用户可以点击“预览”按键查看执行结果。如图 5。

图 5 特征计算与事件评级节点结果

### 5.3.3 行为画像节点

行为画像节点用于配置特征图表，用户可以选择不同的图表及描述，从而更好地提升风险事件的可解释性。点击“预览”按键，图表会根据上一节点调试的结果展示详情，如图 6。

图 6 行为画像节点

### 5.3.4 验证特征及创建特征

此处节点与自定义编程的验证特征按键以及创建特征按键功能一致，详情请参考 6.7。

# 6 时序分析

## 6.1 特征列表

本页面是时序分析环节中的 Step1 创建查看特征环节。通过 Step1 创建特征，Step2 针对所选特征创建 AI 模型，Step3 通过单时序异常探索或综合异常探索进行最终 UEBA 场景的构建、调试和选定。

通过本页面，您可以针对数据表中任意字段进行特征创建，并支持查看、搜索、修改、克隆和删除等操作，以及 Backfill 补全未计算时间段数据，根据选定特征进行 Step2 创建 AI 模型。同时可以查看特征计算任务。

从左侧菜单功能栏进入到特征列表模块页面。特征列表中包括如下字段：特征名称、特征分组、特征描述、SQL、数据表、创建人、创建时间、状态、最近运行、操作。其中除了特征描述、SQL 和操作栏以外全部可以进行排序。默认排序规则：按照创建时间由近到远进行排序。

### 6.1.1 全文搜索

本模块支持全文搜索，并且支持模糊查询，在本模块内所有字段内容都可以通过全文搜索框进行查询，全文搜索输入框中支持对查询内容的一键删除操作，方便用户修改查询内容。

### 6.1.2 创建特征

点击特征列表页面右上角的“创建特征”按键，页面跳转进入到创建特征页面，其中默认选择数据表为 ailpha_securitylog，特征字段为空，特征值为 count 日志计数、对象分组为空、时序字段为 startTime（起始时间）| 时间型，聚合粒度为 10 分钟，过滤条件为空。

默认不选择对象分组时，默认分组操作栏置灰，无法进行操作；相关的数据源时序图分为上下两张，分别根据筛选条件的不同而展示不同情况下的数据值。

支持对展示数据的时间范围进行自由调整（无法选择未来时间），并且支持对时序图进行缩放、拖拽等操作。

#### 6.1.2.1 特征字段与特征值

点击特征字段下拉框，可以选已存在的字段内容，如图 1 所示：


图1　特征字段内容

根据特征字段不同下拉选择的特征算子不同。特征值有默认值不能为空。如图 2 所示：


图2　特征值内容展示

#### 6.1.2.2 对象分组与默认分组

根据所选数据表，下拉的内容为该数据表的除时间型以及所选特征字段之外的所有字段。

当选择对象分组后，点击刷新，时序图发生改变，默认分组会从灰色变为白色，并且可以对其进行操作，如图 3 所示：

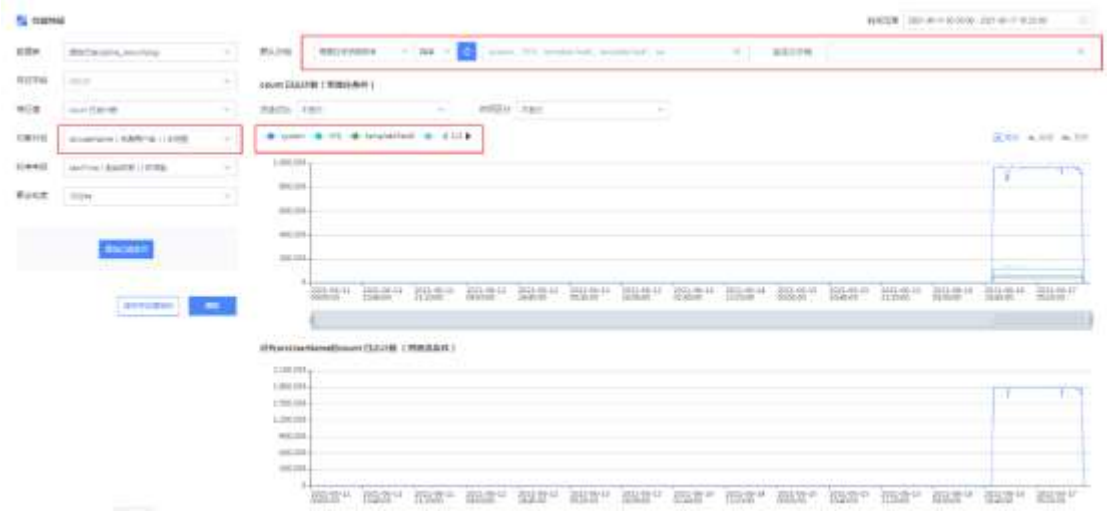


图3　对象分组

默认分组可以对已筛选的数据进行选择排序方式，可以选择根据日志总数排序、根据周密度排序、根据最大特征值排序，并且支持降序和升序两种排序模式，如图 4 所示：


图4　默认分组排序功能

选择排序方式后，点击排序刷新按键，页面立即进行排序，切换到柱状图，默认展示 25 个对象实体，并且可以选择展示对象数量，有 10、25、50 可供选择。

点击柱状图中的具体对象可以跳转到该对象的特征时序图。并且点击柱状图右上角的“返回”按键可以返回到特征时序图页面。

默认分组（对象实体 top10）在曲线时序图中默认显示 top5 的对象实体，可以通过全选或者清空按键对实体进行全选和取消选取。每当多勾选一个对象时，曲线时序图中就会立即展示一条新的实体特征时序。如图 5 所示：

也可以通过各自需求不同，进行自定义分组，在自定义分组中可以选择不存在与 top10 中的对象实体，让其在特征时序图中进行展示，默认最多展示 10 条。

在默认分组和自定义分组中，点击对象实体后方的＋符号，可以对在列表中的对象，进行钻取操作，使其加入到过滤条件中。从而根据特征条件进行数据细化筛选的操作。

图5　默认分组 top10

#### 6.1.2.3 时序字段与聚合粒度

根据所选数据表，下拉的内容为所有时间型字段。默认： startTime（起始时间）|时间型，如图 6 所示：

图6　时序字段内容

聚合粒度主要用于特征在该时间粒度范围内做一次数据的特征聚合显示

下拉选择【1 分钟，5 分钟，10 分钟，30 分钟，1 小时，6 小时，1 天】。默认为 10 分钟。如图 7 所示：

图7　聚合粒度内容

#### 6.1.2.4 添加过滤条件

在创建特征页面点击页面左下角的“添加过滤条件”按键，点击后页面弹出过滤条件添加控件。

支持添加条件，添加组等功能。用不同背景颜色区分层级。添加条件，添加组和原来的条件默认是 AND 关系；添加组，组内默认是 OR 关系。

根据所选数据表，字段选择的下拉内容仅为该数据表的字符型和数值型字段。

如图 8 所示：

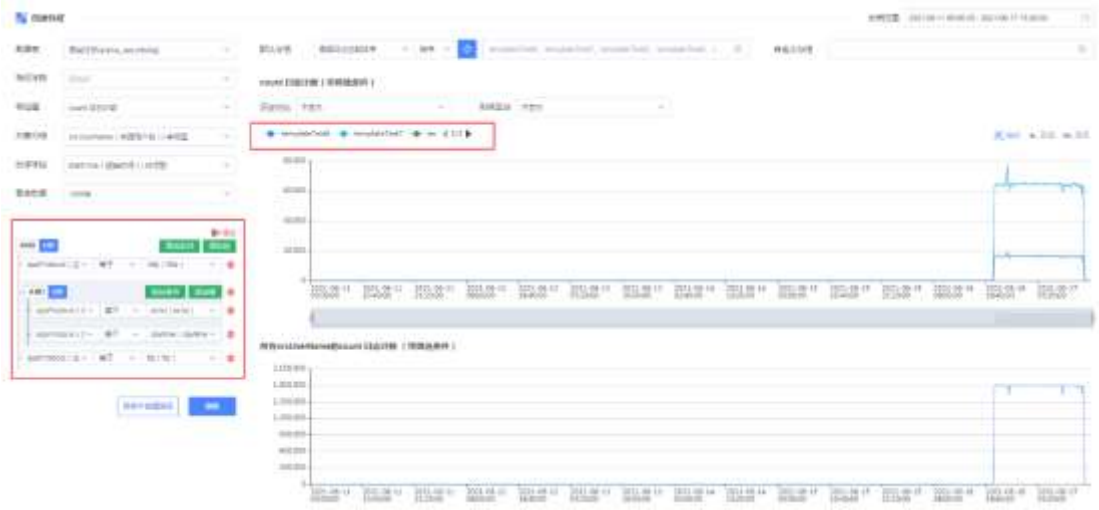


图8　添加过滤条件

#### 6.1.2.5 时间范围控件

在创建特征时，可以对时序图的时间范围进行随意调整并浏览，点击页面右上角时间控件，展开成如图 9 所示：

图9　时间范围组件

本组件可以具体选择到秒为单位的时间节点，点击组件中的“选择时间”按键，并且时间和日期之间可以来回切换操作。本组件支持快速选择时间范围，更改时间后，点击确定并刷新按钮直接生效。

#### 6.1.2.6 历史对比与时间区分

在创建特征时序图上方可以选择历史对比，该功能主要用于将当前时间数据与过去时间的数据进行直观上的数据比较，如图 10 所示：

图10　历史对比

在创建特征时序图上方可以选择时间区分，该功能主要用于区分在展示的时间范围内特定时间日期，并且历史对比和时间区分可以同时显示，如图 11 所示：

图11 时间区分

#### 6.1.2.7 时序图

如图 12 所示，页面主要展示相关时序图所有内容，时序图主要由上下时序图和时间轴组成，将鼠标移动到时序图曲线上，会展示出该时间节点，图中曲线的具体数据数值。并且上下图会进行联动显示。

图12 时序图

相关具体组件功能详情信息见下表 1 所示：

| 序号 | 名称 | 说明 |
| --- | --- | --- |
| 1 | 曲线标注 | 此区域主要用于解释曲线时序图中的曲线分别代表的含义，并且点击此处的注释可以直接对该注释的对象进行筛选，曲线时序图中只显示该对象。 |
| 2 | 时序图操作栏 | 此区域主要用作于对时序图的操作，可以对时序图进行缩放、回退和重置的操作。 |

| | | |
|---|---|---|
| 3 | 上时序图及信息详情 | 将鼠标移动到时序图上方时，会在鼠标位置展示出该时间节点，在时序图中展示的对象的数值，并且上下时序图联动。上时序图主要显示的内容为默认分组和自定义分组中的对象的数据值。 |
| 4 | 时间轴 | 时间轴主要用于展示此时时序图的时间范围，并且其中的样式类似于实际上时序图的样子。 |
| 5 | 下时序图 | 下时序图主要显示的内容和上时序图存在差异，互为补充，具体参考不同情况下的不同图名 |

表1

#### 6.1.2.8 总体概览

在创建特征页面或者特征详情页面中，点击时序图中的特征点，点击后页面右侧会弹出相应的原始日志信息窗口——总体概览。

在窗口中主要显示该特征点相关的数据，可以对该创建页面进行模式的切换，分为精简模式和完整模式两种。

当鼠标移动到饼图上方时，系统展示出鼠标所在饼图区域的详情信息，并且带有“将字段及取值加入筛选条件”的按键，点击该按键后，系统自动将该处的对象实体加入到过滤条件中，如图 13 所示：


图13 饼图详情及对象加入筛选条件

直接在饼图中点击或者在完整模式下点击饼图右侧的注释信息，则系统自动将该字段进行钻取操作，并且多次钻取以 AND 的形式进行过滤，并且可以对已经钻取的条件进行单个删除或者全部删除操作。如图 14 所示：


图14 饼图钻取功能

页面下方展示为最近 50 条原始日志信息，默认显示为精简模式，只显示 7 个字段，如图 15 所示。对相关的原始日志进行点击，则会展开显示该条原始日志的详情信息。该处详

细信息为该条日志数据的所有不为空的字段信息。并且默认只能展开一条日志信息，如果展开其他日志信息，则自动收起上一条日志信息。展开日志信息后，默认自动将饼图从精简模式切换到完整模式。

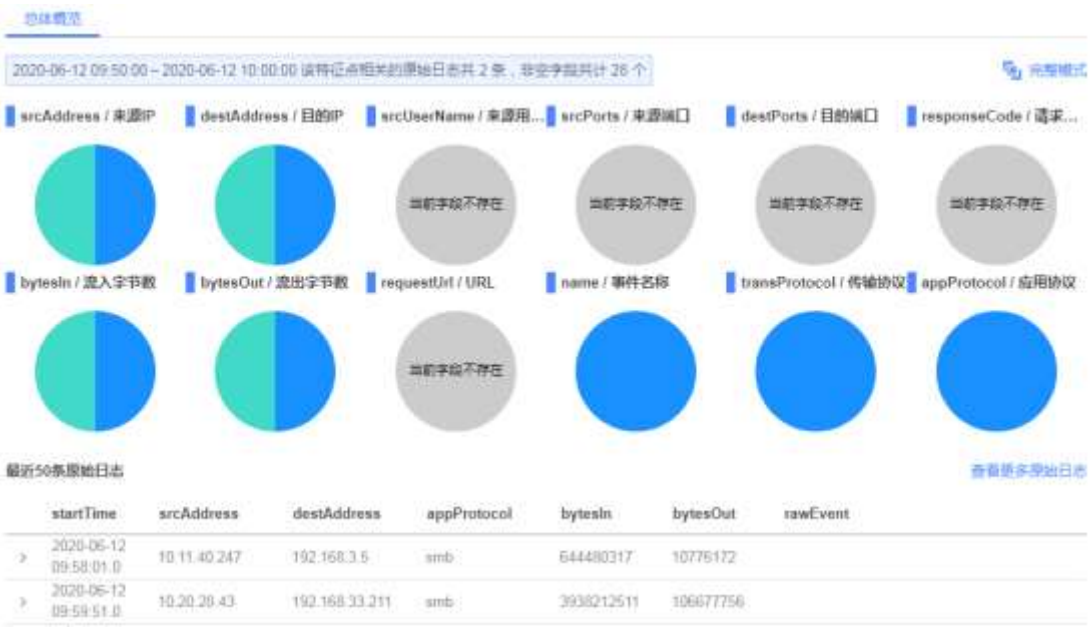



图15原始日志列表

#### 6.1.2.9 刷新及保存指标

每次对创建特征中的数据条件进行更改时，刷新按键都会进行实时动态显示，提醒用户刷新后才能对更改内容生效。

点击“保存并创建指标”后，创建特征窗口。如图 16 所示：


图16 刷新及保持特征指标

在保存特征窗口中，含有特征名称、特征分组、特征计算时间范围、特征描述四个输入项，特征名称为必填且唯一。点击确定后，成功创建相关特征，并且在特征列表中显示。

### 6.1.3 特征计算任务及特征状态

点击特征列表页面右上角“特征计算任务”按键，点击后页面跳转进入所有特征的计算任务页面，在该页面中，主要展示特征在每个粒度时间节点上的计算情况，状态包括成功、失败和执行中。此页面主要用于观察，并且可以对其进行全文搜索，功能同上文中的全文搜索。该界面主要是查看，无其他任何操作的功能。

系统也支持在单个特征中进入特征计算任务，只查看该特征的计算任务。

在特征列表页面中，系统只会对开关状态为开的特征进行计算，当开关为关时，则不进行特征计算，如图 17 所示：

图17 特征状态

## 6.2 特征操作栏

### 6.2.1 查看特征详情

在特征列表中点击特征操作栏中的查看特征按键，页面直接跳转到该特征的详情页面，只能对该特在的时序图进行查看操作，不能对原有条件进行更改。

### 6.2.2 Backfill

Backfill 功能可以对指定特征进行回填计算，该回填针对于过去未计算的时间范围，并且不能早于数据接入时间。

点击特征后方操作栏中的 backfill 按键后，弹出 backfill 对话框，在对话框中可以对需要回填的时间范围进行选择，开始 backfill 后，系统会对选定的时间范围作出新的计算任务。如图 18 所示：


图18 Backfill

### 6.2.3 创建 AI 模型

点击特征列表中指定特征后方操作栏中的“创建 AI 模型”按键，点击后页面直接跳转到创建 AI 模型页面，并且选择的特征为刚选定的特征。

### 6.2.4 修改、克隆和删除

在特征操作栏中，可以对特征进行修改、克隆和删除操作，相关功能和上文中所提到的修改克隆和删除一致。其中无法删除已经被运用到 AI 模型中的特征，需要提前删除模型才能删除此特征。

## 6.3 AI模型列表

本页面是时序分析环节中的 Step2 创建查看 AI 模型环节。通过 Step1 创建特征，Step2 针所选特征创建 AI 模型，Step3 通过单时序异常探索或综合异常探索进行最终 UEBA 场景的构建、调试和选定。

通过本页面，您可以进行 AI 模型创建、查看、搜索、修改、克隆和删除等操作，针对已创建的特征进行 Step2 创建 AI 模型操作，以及针对特定 AI 模型进行 Step3 单时序异常探索或综合异常探索。同时可以查看模型计算任务。

### 6.3.1 AI 模型列表

整体 AI 模型列表中的功能和特征列表功能类似，请参考特征中所述。包括全文搜索、列表内容、展示信息及模型任务，如图 29 所示：

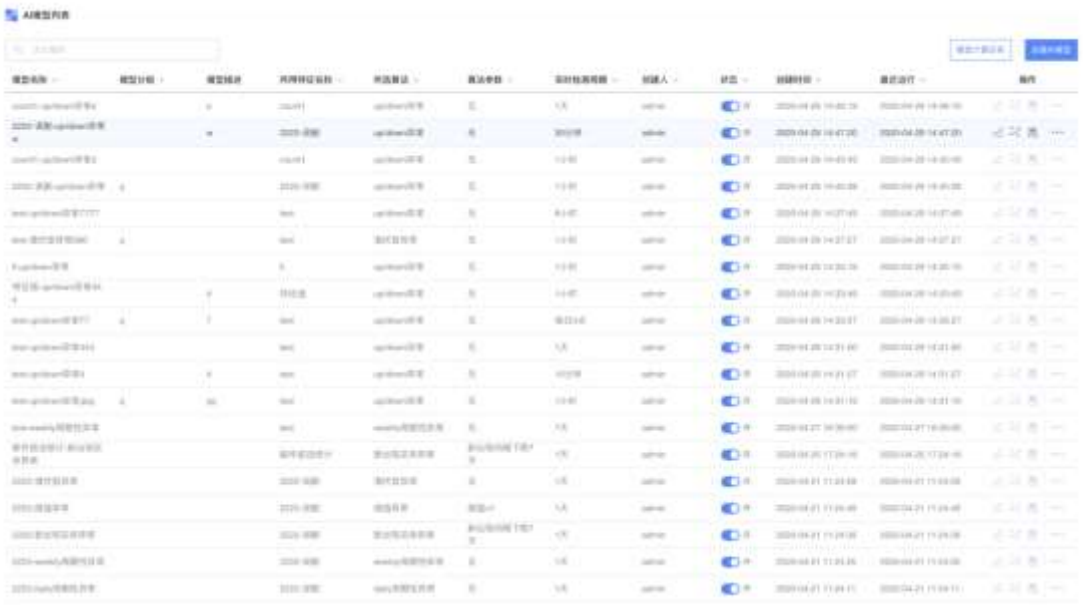


图 29 AI 模型列表

### 6.3.2 创建 AI 模型

#### 6.3.2.1 创建 AI 模型内容介绍

点击 AI 模型列表右上角“创建 AI 模型”按键，点击后页面跳转进入到创建 AI 模型页面，在该页面中，默认特征选择为最新创建的一个特征，选择特征下拉框支持手动输入并且支持查询功能。

算法选择框，展开显示共有 6 种算法：up/down 异常、daily 周期性异常、weekly 周期性异常、新出现实体异常、阈值异常和潜伏型异常。选择算法下拉框默认算法为：up/down 异常。

算法参数，不同的算法有不同的参数，现阶段只对阈值异常和新出现实体异常开放参数。选择其他算法，显示“算法参数 无参数”。

实时检测周期主要作用于模型的计算周期，该周期与特征的聚合粒度可以不同，但是存在一定规则，模型的实时检测周期一定大于或等于特征的聚合粒度。

当选择的特征含有对象分组时，在 AI 模型创建页面才能对默认分组进行操作，否则显示置灰无法操作。

时序图中的操作规则同特征时序图。以上内容，如图 30 所示：

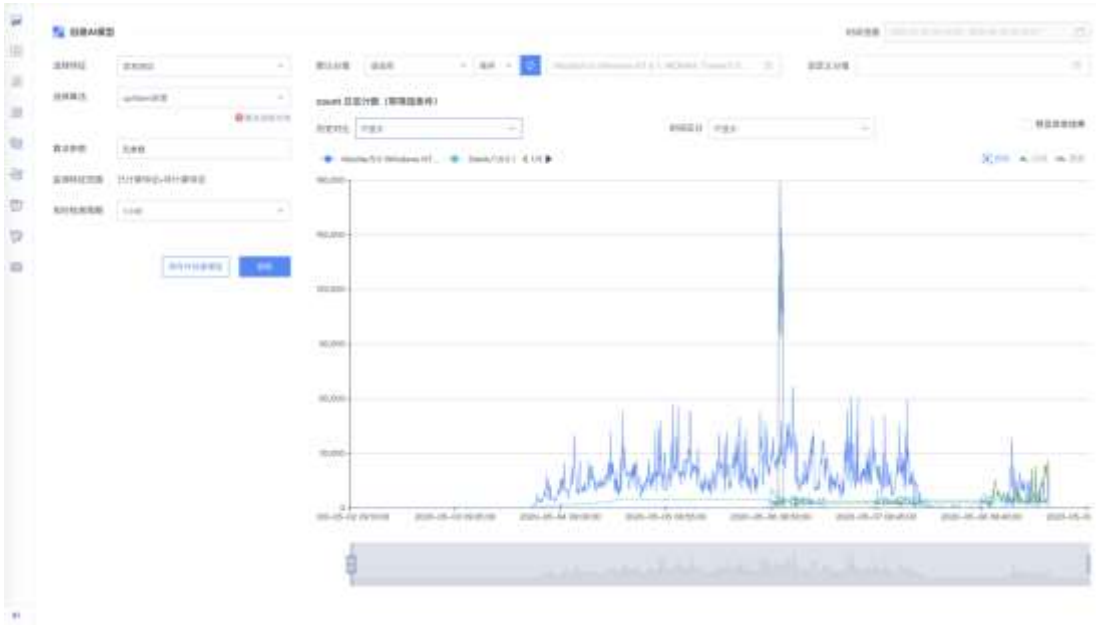


图 30 创建 AI 模型

时序图中有特征时序图有所不同的地方在于，模型时序图中，可以勾选“预览异常单”功能，勾选后时序图会展示出异常点，不同严重等级的异常显示为不同颜色，比较直观，如图 31 所示：

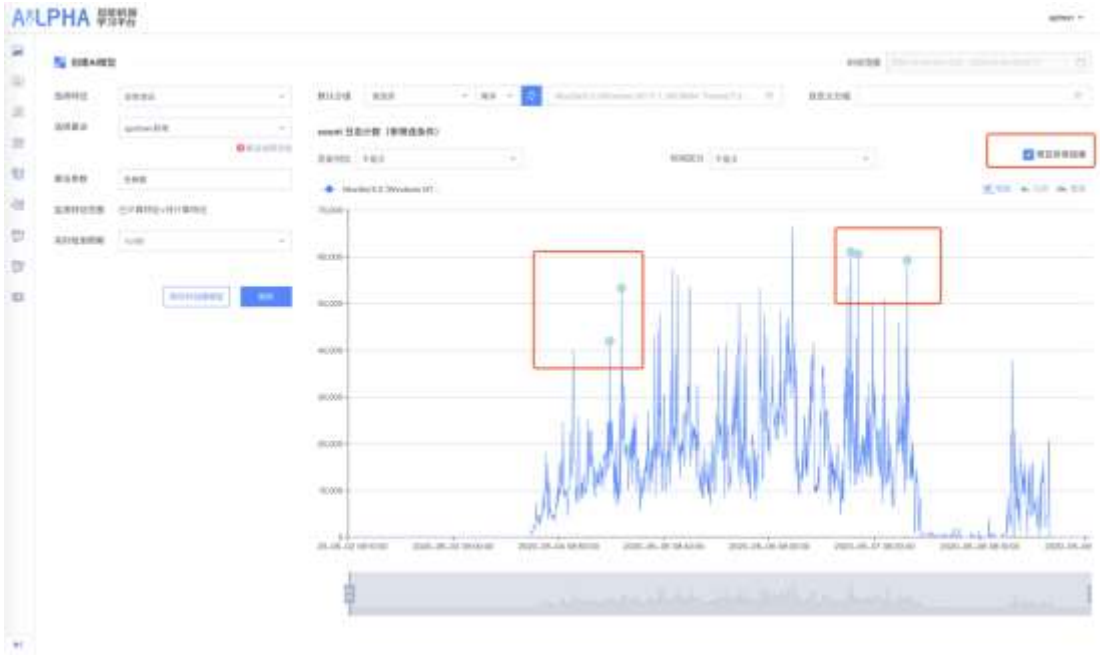


图 31 预览异常结果

### 6.3.3 刷新与保存并创建模型

在创建 AI 模型页面中修改部分参数后，刷新按键会动态显示，用户提示用户刷新并浏览。

点击“保存并创建模型”后，页面弹出保存窗口，其中需要输入的内容有：模型名称、模型分组、模型描述，其中模型名称是唯一的，为必填项。如图 320 所示：


图 32 保存并创建模型

### 6.3.4 模型操作栏

#### 6.3.4.1 单时序异常探索和综合异常探索入口

在 AI 模型列表中，点击模型后方操作栏中的单时序异常探索和综合异常探索按键，点击后跳转到相应的模块，并且默认模型为该模型。

#### 6.3.4.2 修改、克隆、删除

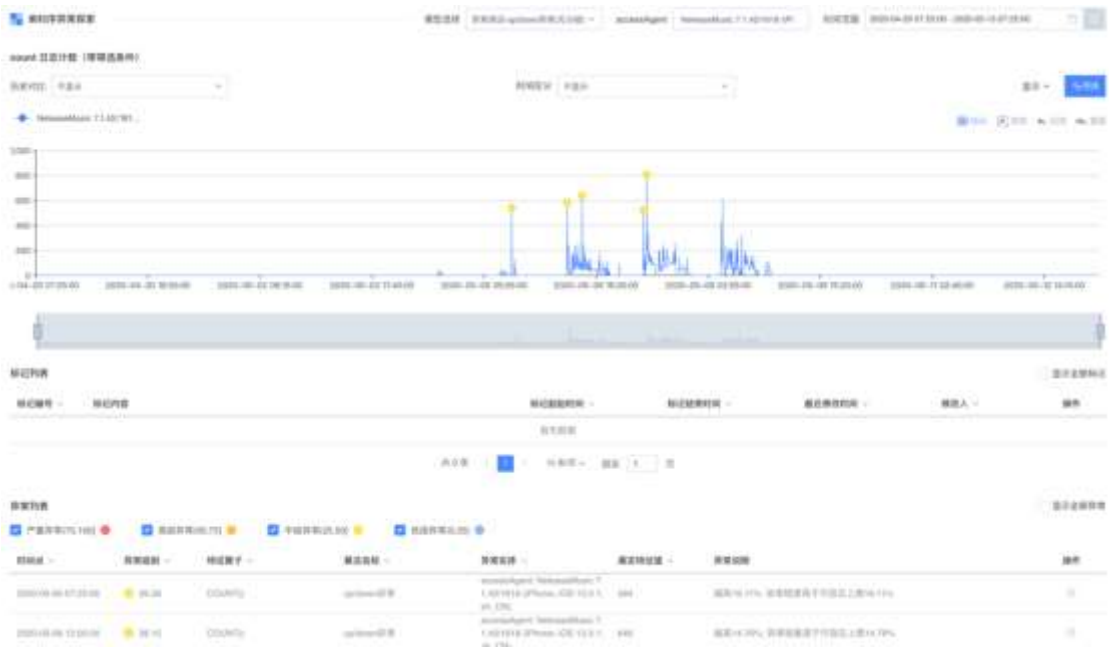
在特征操作栏中，点击操作栏中的 按键可以对特征进行修改、克隆和删除操作，相关功能和上文中所提到的修改克隆和删除一致。如图 33 所示：


图 33 修改、克隆、删除

## 6.4 单时序异常探索

单时序异常探索模块主要用于分析单个模型在指定范围时间内的异常情况。主要含有以下功能单元：模型选择、时序图、标记列表、异常列表。

该模块如**错误!未找到引用源。**所示：



### 6.4.1 模型选择

当从模型列表中选择模型直接跳转到单时序异常探索页面的情况时，模型为模型列表中选择的模型。

当从系统左侧功能菜单栏进入时，模型默认显示为最新的模型。

当选择的模型的特征含有对象分组时，单时序异常探索页面才会显示对象分组属选择框，否则该选择框隐藏。如图 34 所示：


图 34 模型选择及对象分组 appProtocol

### 6.4.2 时序图操作

#### 6.4.2.1 历史对比、时间区分、时序图操作

历史对比和时间区分同《特征列表》指南中所示，请参考 8.2.6。

时序图可以有如下操作功能：缩放、回退、重置、标记。

在时序图上方可以对时序图展示的内容进行筛选，包括：上下界、标记、预测，如图 35 所示：

图 35 历史对比、时间区分、时序图操作

#### 6.4.2.2 预测功能

单时序异常探索模块支持对 up/down、daily、weekly、阈值模型曲线预测。点击时序图右上角的预测按键，弹出预测窗口，在预测窗口中选择学习区间、预测起始时间、预测时长，预测算法学习历史数据进行未来曲线模拟。在预测期间，无法进行其他操作。预测结果如图 36 所示：

图 36 预测功能

#### 6.4.2.3 原始日志窗口

点击单时序异常探索时序图中的异常点，页面右侧会弹出原始日志窗口，其中有四个 tab，分别为：总体概览、同时段异常、同实体异常、其他设备告警。

总体概览展示当前异常点风险概览情况。同时段异常展示同一时段下所有已创建模型的异常情况。同实体异常展示当前实体在其他模型计算的异常情况。其他设备警告展示当前实体在其他设备下的告警情况。

相关展示页面如图 37 所述：

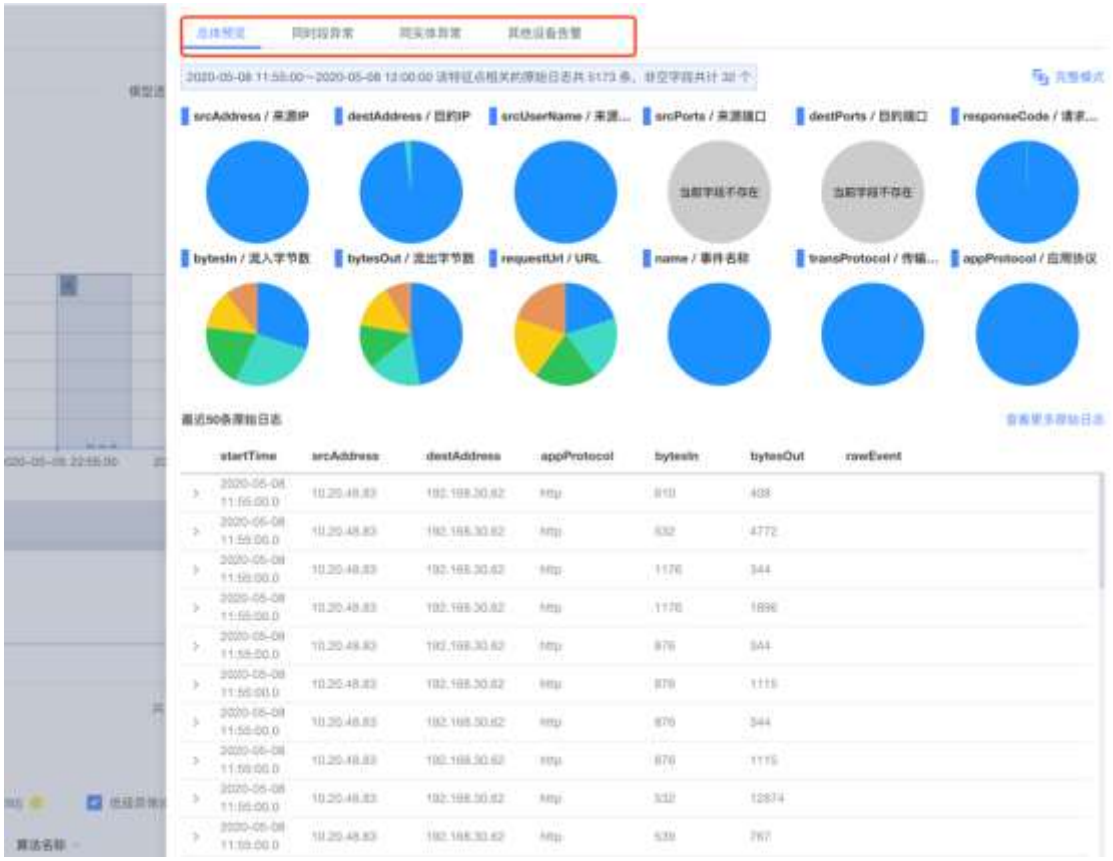



图 37 原始日志窗口

### 6.4.3 标记列表

在单时序异常探索时序图中，可以对曲线进行标记操作，点击时序图上方“标记”按键后，鼠标可以对时序图进行时间范围的选择，随之会弹出创建标记对话框，输入标记编号与标记内容创建标记。如图 38 所示：


图 38 标记窗口

创建成功的标记，会在页面中部的编辑列表中显示，一个模型最多可以创建的标记为 26 个，可对已存在的标记进行修改和删除。

### 6.4.4 异常列表

单时序异常探索页面底部是异常列表模块，该模块显示了所选模型的所有异常内容，用户可以对其通过异常严重等级继续筛选，分别为：低级异常、中级异常、高级异常、严重异常，以蓝、黄、橙、红四色表示。如图 39 所示：

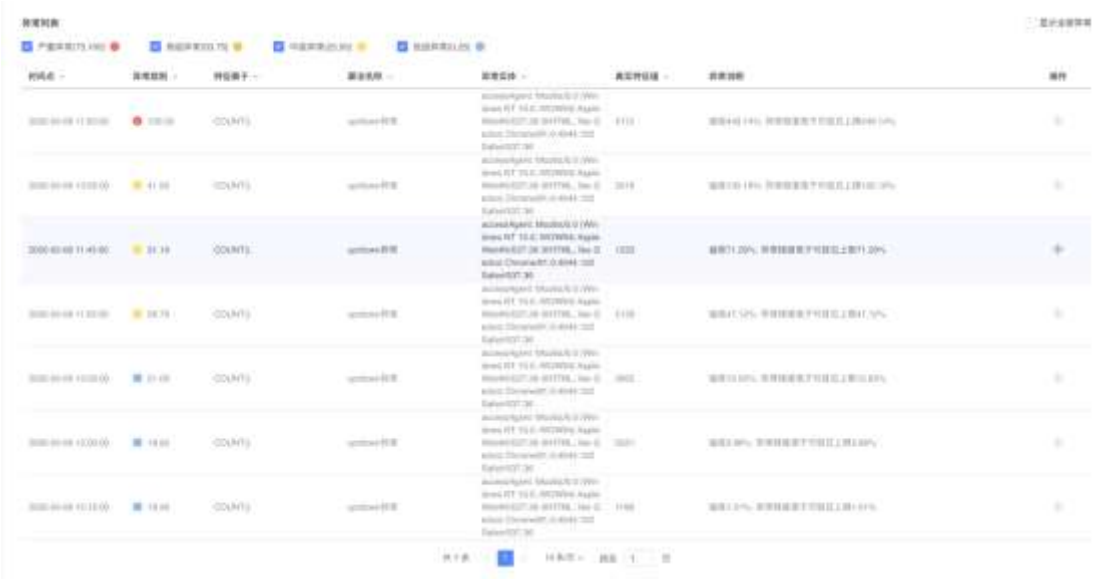


图 39 异常列表

点击异常列表中异常后方的“高亮并溯源分析”，页面中的时序图将高亮异常点，并在页面右侧弹出原始日志窗口，方便对异常时序点进行溯源分析。如图 40 所示：

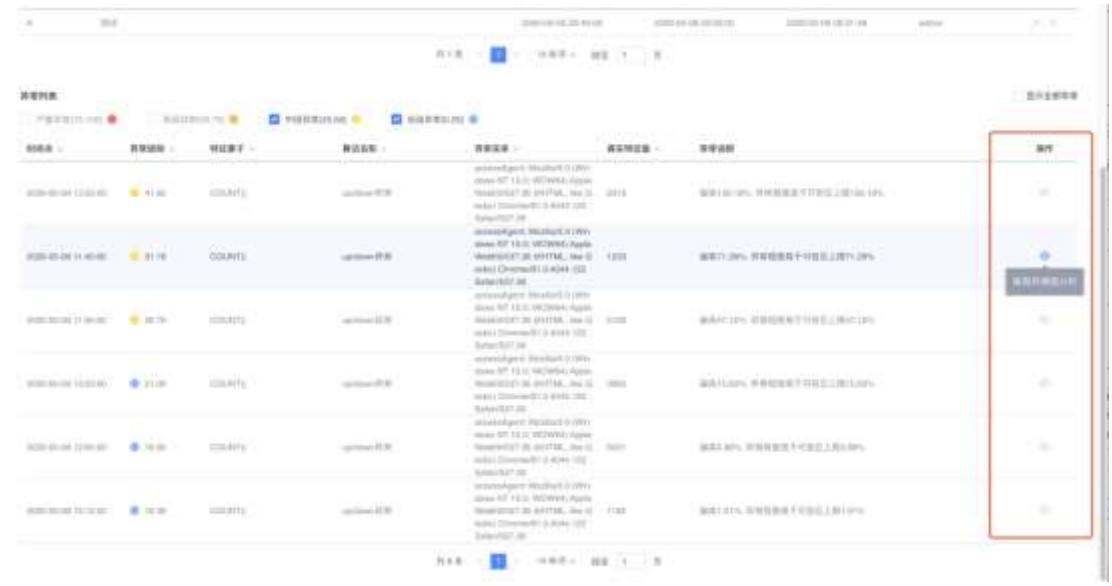


图 40 高亮并溯源分析

## 6.5 综合异常探索

通过本页面，您可以选择您关心的模型，进行综合的异常探索。该界面支持以总体概览，模型，实体等视角进行异常探索，并且支持交集/并集等高级功能。您可以随心所欲地过滤、钻取、跳转，从而快速地进行异常排查。

### 6.5.1 模型选择

综合异常探索首次进入时，默认模型选择为最新的模型，用户可以根据自己需要对模型进行选择，在模型选择框中，没有模型数量限制，可以支持全选和清空。并且已选择的模型默认会高亮并置顶。

用户第二次及以后进入则默认为上一次选择的模型。

模型选择支持搜索查询功能，方便用户快速定位模型。

注：当选择模型后，如果不点击右上角的“刷新”按键，则没有生效，必须点击刷新后才能生效。

### 6.5.2 添加过滤条件

综合异常探索中，支持添加过滤条件，该过滤条件的添加方式同时序分析_特征列表同理，请参考 8.2.4。当添加完过滤条件，必须刷新之后才能对数据生效。如图 41 所示：


图 41 添加过滤条件

### 6.5.3 快捷标签

综合异常探索模块支持将筛选条件保存为标签的功能，方便用户后期对同一情况下的模型异常情况进行查询对比。

操作流程：对模型选择、时间范围、实体过滤、所选模型异常点的并集/交集进行选择填写后，点击“刷新”按键，让其生效，此时再点击页面中的“保存为快捷标签”按键。点击按键后，页面弹出保存标签窗口，其中需要填写标签名称字段（该字段唯一且必填）。如图 42 所示：


图 42 保存标签窗口

系统默认标签数量上限为 100 个，可以对标签栏进行展开和收起操作。并且在标签栏中点击编辑按键可以对已存在的标签进行修改和删除操作。如图 43 所示：


图 43 标签列表及修改删除

点击已存在的标签后，页面立即刷新为该标签的筛选条件。

### 6.5.4 异常时间线

异常时间线主要分为两个模块，总体概览和各个模型泳道图。

总体概览中，主要展示所有模型经过交集/并集算法逻辑处理后的异常集合，方便用户观察整体情况，各个模型的泳道图，相互独立，不存在相互影响，可以清楚观察到每个模型的异常情况。

异常等级划分如下：蓝色→低级异常；黄色→中级异常；橙色→高级异常；红色→严重异常；无色→无异常。

将鼠标移动到相应的泳道图上方时，页面会展现出相关模块的时间范围、最大异常分值、异常等级。

使用鼠标点击异常时间线中的小方块，此方块高亮，其他区域置灰，并且系统会默认以该方块中的内容作为过滤条件，对整个页面中的信息进行过滤操作，并立即生效。当再次点击该方块时，则取消过滤条件；当点击其他方块时，则切换过滤条件。如图 44 所示：

图 44 异常时间线

下方泳道图查看方式可以以不同模型或以对象分组进行显示，点击后页面立即生效，并且可以设置数量限制，如图 45 所示：

图 45 查看方式及数量

### 6.5.5 异常排名

异常排名位于综合异常探索页面左边，主要显示模型的对象分组中各个实体的异常值，并且有两种排序方法：最大异常分数降序排序、总和异常分数降序排序。

当含有多个模型，且每个模型都有对象分组时，那么异常排名就会有多个，默认只展开第一个，下方所有排名都默认收起，可以手动展开。如图 46 所示：


图 46 异常排名

在异常排名列表中，可以对实体进行钻取操作，操作流程：选择需要钻取的实体，点击其后方的“+”号表示在原有的过滤条件下以 AND 的方式加入【该字段=该字段值】新的过滤条件，点击其后方“-”号，表示在原有的过滤条件下以 AND 的方式加入【该字段！=该字段值】的过滤条件。并且可以同时添加多个过滤条件。如图 47 所示：

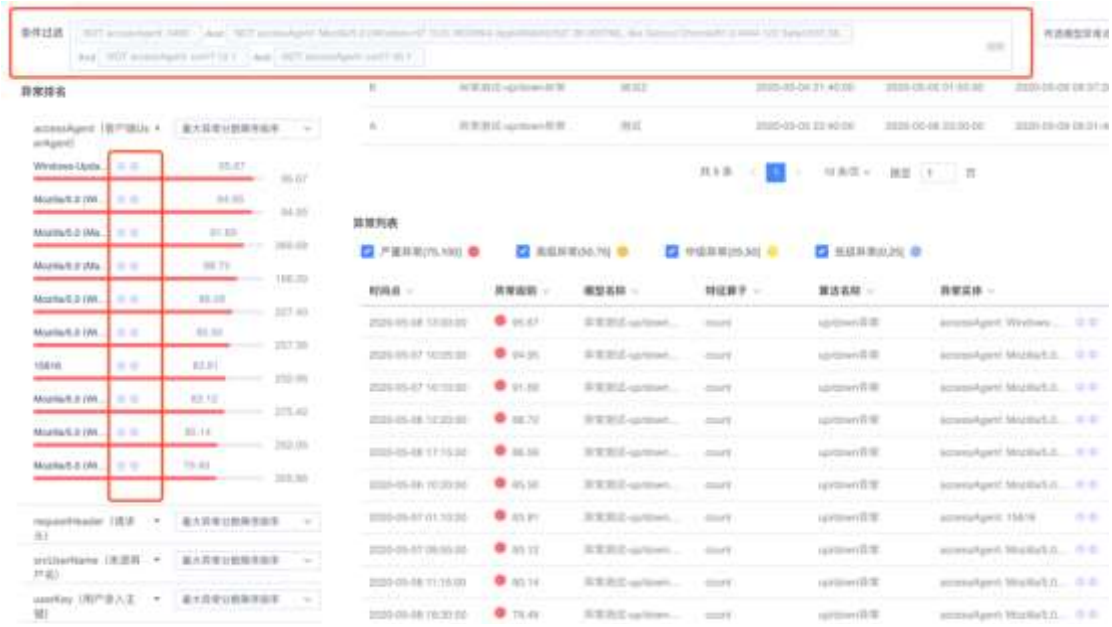


图 47 钻取

### 6.5.6 标记列表

综合异常探索中的标记列表主要来源于模型在单时序异常探索中的标记，并且两边互相关联。

综合异常探索模块无法对模型添加标记，但是可以对模型进行修改和删除，修改和删除同步影响该模型在单时序异常探索中的标记显示。如图 48 所示：

图 48 标记列表

### 6.5.7 异常列表

综合异常探索中的异常列表，和单时序中的异常列表功能一致，请参考相关信息。

综合异常探索中的异常列表还有额外功能，异常钻取和异常跳转单时序异常探索。

异常钻取操作上面的异常排名一样，请参考相关信息。

选择异常列表中的异常，点击其操作栏中的“单时序异常探索”按键，点击后页面跳转进入到该条异常所在模型的单时序异常探索页面中。如图 49 所示：

图 49 异常列表

# 7 日志查询

日志查询页面提供所有接入日志的查询和可视化功能，并支持结果的保存和导出。

## 7.1 搜索

在界面右方选择查询日志类型，其中：原始日志表示所有接入的原始日志数据，数据关联日志表示符合所选主键数据源及用户信息管理中所录入/自动发现用户的关联日志，风险事件日志表示已存在的风险事件及详情日志。如图所示。

图 50 数据源

选择数据源后，在搜索栏输入字段过滤条件并选择时间范围进行日志搜索。搜索栏支持字段提醒，如搜索逻辑较复杂，点击搜索栏左侧按钮，可添加组合搜索条件。如图 51 所示。

图 51 搜索栏

搜索栏下方的柱状图展示搜索结果在时间轴上的数量分布。

界面左侧可选择查询日志结果的默认展示字段。日志查询结果以时间倒序排列，点击某一条日志左侧箭头，可展开显示日志详细信息，详细信息包含所有内容不为空的字段。如图 52 所示。

图 52 日志查询结果

## 7.2 导出和保存

导出按钮支持以 csv 格式保存查询结果至本地电脑。

保存按钮支持保存搜索条件，点击已存搜索按钮即可查看并使用保存的搜索条件，方便查询结果重复使用。如图 53 所示。

图 53 搜索条件保存

## 7.3 可视化

可视化功能支持用图表展示日志查询结果，可选择柱状图、折线图、面积图、列表、大字报、饼状图六种图表类型。

数据栏配置坐标轴对应展示字段，样式栏配置坐标轴单位信息。如图 54 所示。

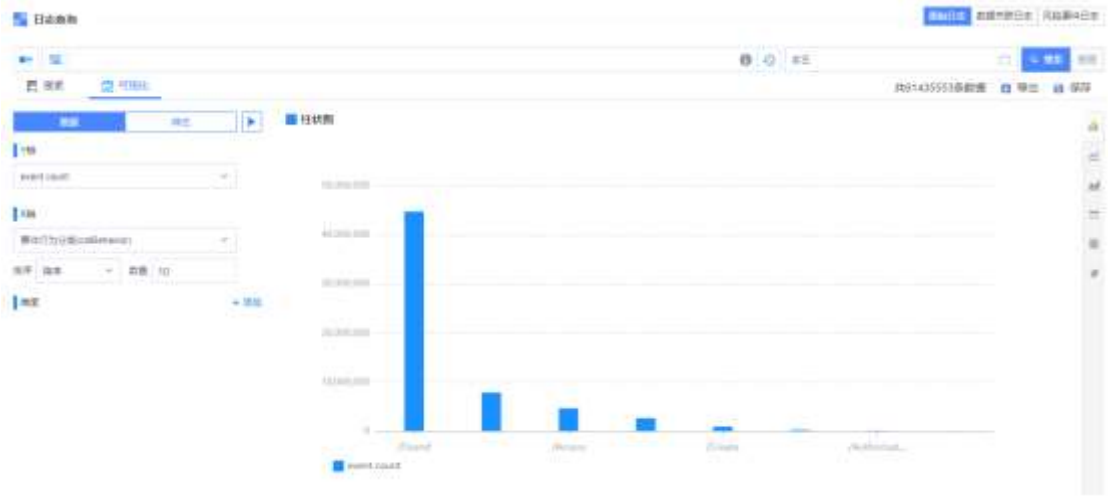


图 54 日志可视化

## 7.4 操作

风险事件日志，点击操作，显示三种操作：日志查询、新增白名单、关闭特征。如图：

点击日志查询，跳转新页面至日志查询，溯源到事件数据关联日志。

点击新增白名单，会弹出添加白名单窗口，窗口内会显示白名单条件，用户可以选择编辑策略名称及策略描述，同时可以选择是否删除最近 7 天的风险事件，若选择删除，则会删除最近 7 天当前风险对象该特征的风险事件，如图所示：

点击关闭特征，跳转新页面至用户特征管理，通用解决方案下全文搜索框检索该特征名称，如图所示：

# 8 数据字典

## 8.1 页面介绍

点击页面上方导航栏数据字典按键进入到数据字典功能模块，在该模块用户可以新增及查看数据字典字段。具体功能介绍见下图及表。

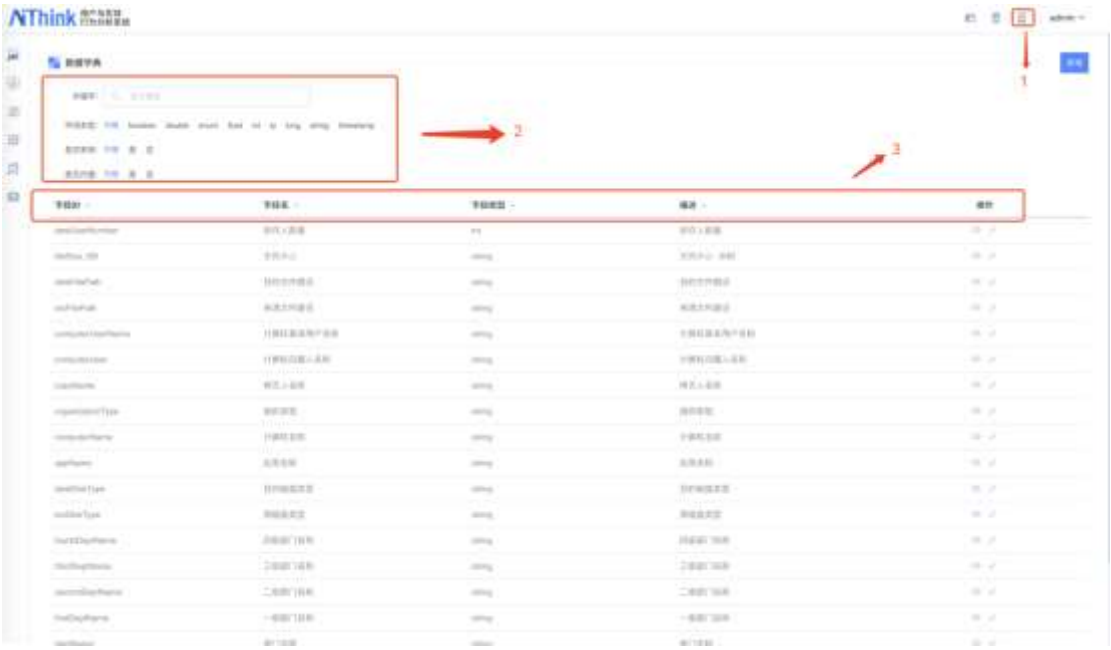


图 1 页面图

| 序号 | 名称 | 说明 |
| --- | --- | --- |
| 1 | 入口 | 数据字典功能模块入口 |
| 2 | 查询搜索功能栏 | 主要用于对已存在的字段进行条件查询 |
| 3 | 字段列表 | 展示已存在的字段区域，默认新添加的字段会显示在最前面，并且只有初始化字段无法进行修改操作。 |

表 1 页面图

## 8.2 新增字段

在页面中可以点击“新增”按键进行数据字典的添加操作，点击后出现如果所示页面：


图 55 添加字段页面

在该页面中，可以添加字段 ID、字段名、字段类型、是否常用、字段描述，根据需要添加不同类型的字段内容。点击提交之后整个系统中都会相关联的运用到已添加的字段信息。

添加不同的字段页面会展示不同的添加方法，例如 enum 类型的字段，需要继续新增字段值，并且输入相应的字段值 ID 和字段值名，如图所示：

图 56 enum 类型

# 9 用户与实体态势

## 9.1 用户行为风险态势大屏

用户行为风险态势大屏整体界面如图：


### 9.1.1 最近一周风险分布

最近一周风险分布展示最近一周内各风险用户人数情况。如图 1。

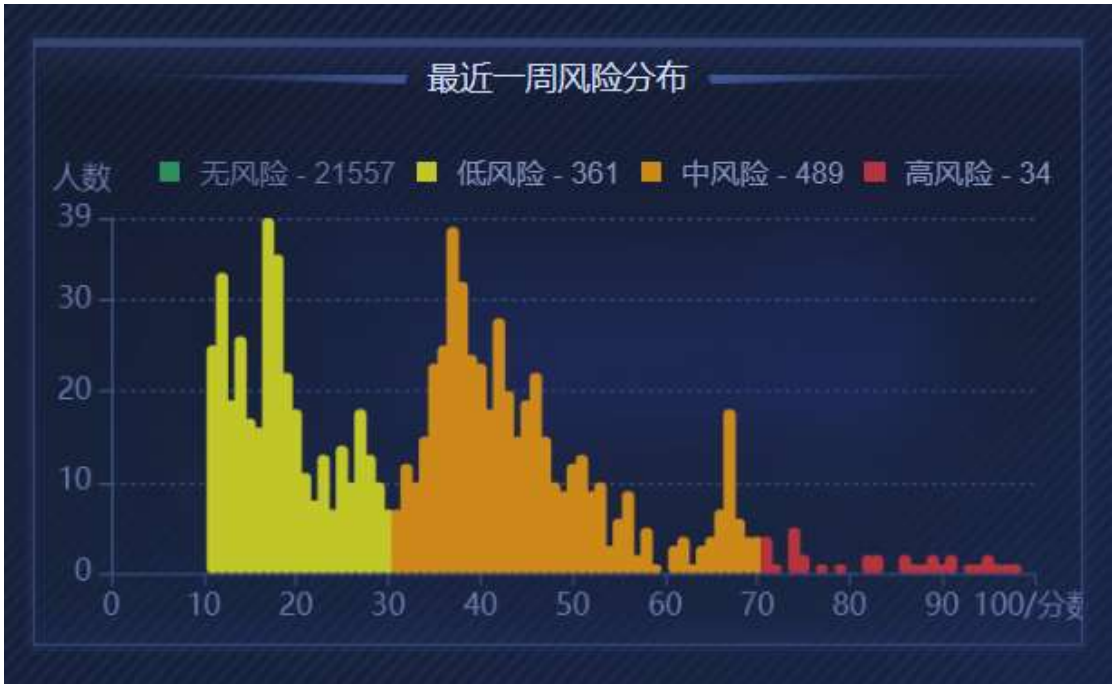



图 1 最近一周风险分布

### 9.1.2 最近一周趋势

最近一周趋势会展示最近一周内的日高风险用户数。如图 2。

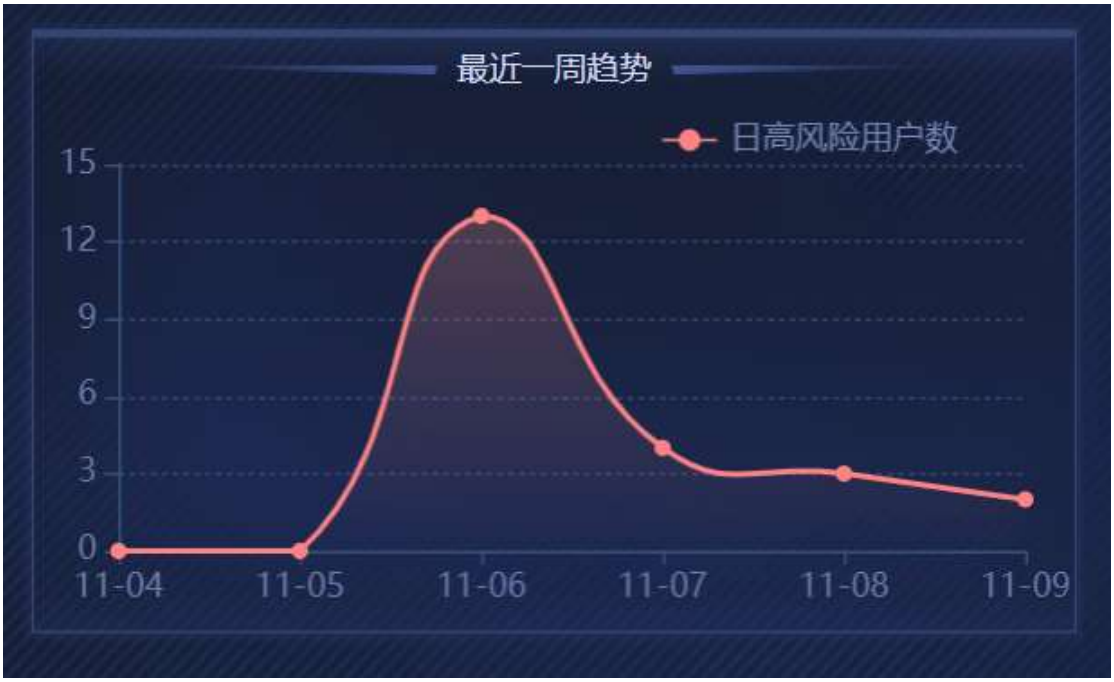



图 2 最近一周趋势

### 9.1.3 风险类型文字云

风险类型文字云展示最近一周内所有用户发生的风险类型，风险类型所占用户数越多文字越大。如图 3。


图 3 风险类型文字云

### 9.1.4 轮播事件栏

轮播事件栏会轮播展示最新的风险事件。如图 4。


图 4 轮播事件栏

### 9.1.5 活跃用户总数及高风险用户数

活跃用户总数会展示最近一周内活跃用户的总数量，对比昨日的总数会计算增减比显示在总数旁边，如图 5。

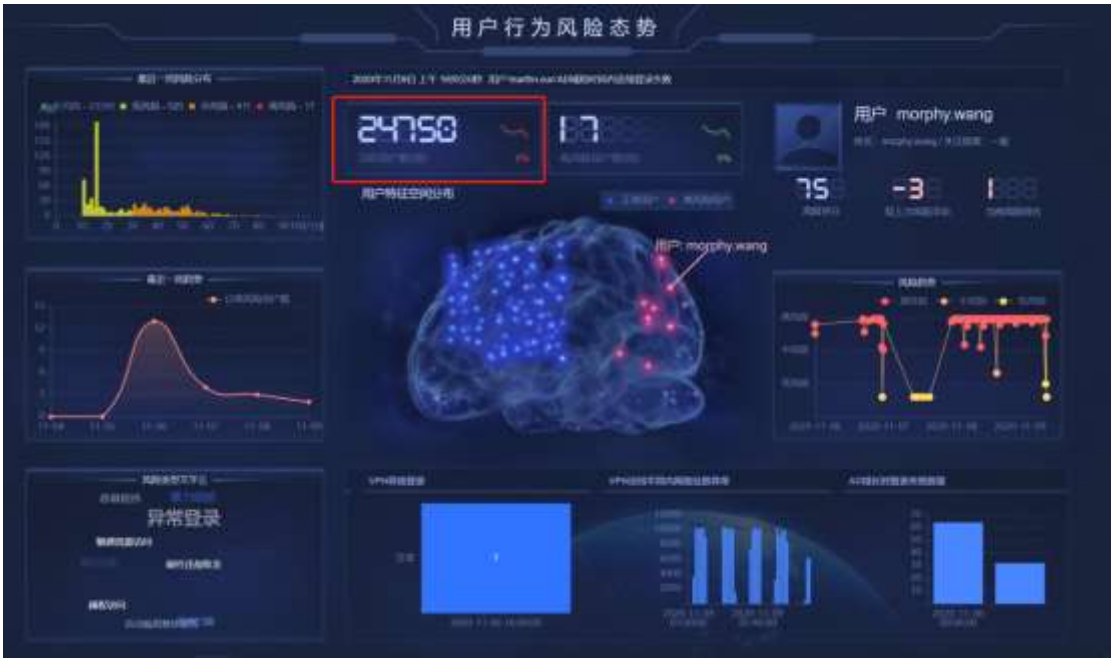



图 5 活跃用户总数

高风险用户数会展示最近一周内的高风险用户总数，对比昨日的总数会计算增减比显示 总数旁边，如图 6。


图 6 高风险用户数

### 9.1.6 用户特征空间分布

用户特征分布展示高风险用户数及活跃用户的整体情况。红色圆点代表风险排名前 10 的高风险用户，蓝色圆点代表其他活跃用户。点击红色圆点可以联动右侧用户信息展示区域及下方图表区域。如图 7。


图 7 高风险用户联动

### 9.1.7 用户其他属性信息

用户其他属性信息会轮播展示风险排名前 10 的用户属性信息、风险排名、较上次风险浮动、风险评分、风险趋势。如图 8。


图 8 用户其他属性信息

### 9.1.8 用户特征图

用户特征图展示风险分数排名前 10 的用户的特征图。共展示 6 张特征图，每屏 3 个，左右轮播展示。如图 9。


图 9 用户特征图

## 9.2 数据库安全解决方案大屏

### 9.2.1 数据库安全态势感知

大屏整体布局如图 1 所示。大屏默认五分钟会进行一次刷新。


图 1 数据库安全态势感知大屏

#### 9.2.1.1 数据概览

数据概览内会展示系统内数据库及数据库账号的概要信息。数据库个数表示系统内数据库个数总和。数据库类型表示所有数据库的类型个数。数据库账号个数表示系统内数据库账号的个数。访问 IP 地址个数表示所有数据库账号访问 IP 地址的总和。SQL 模板个数表示系统内 SQL 模板的个数总和。SQL 语句平均执行时长表示数据库账号及数据库执行 SQL 语句的平均时长。SQL 查询平均影响行数表示每条 SQL 语句查询后影响行数的平均值。平

均返回结果集大小表示数据库账号及数据库返回结果集的平均值。总访问量表示数据库账号及数据库的访问量总和。总返回结果大小表示数据库账号及数据库的返回集总和。如图 2。

图 2 数据概览

#### 9.2.1.2 访问量趋势

访问量趋势展示的是当前所选时间范围内，所有数据库账号及数据库的访问量趋势。所选时间范围改变，访问量趋势的 X 轴根据时间范围做自适应改变，如图 3。

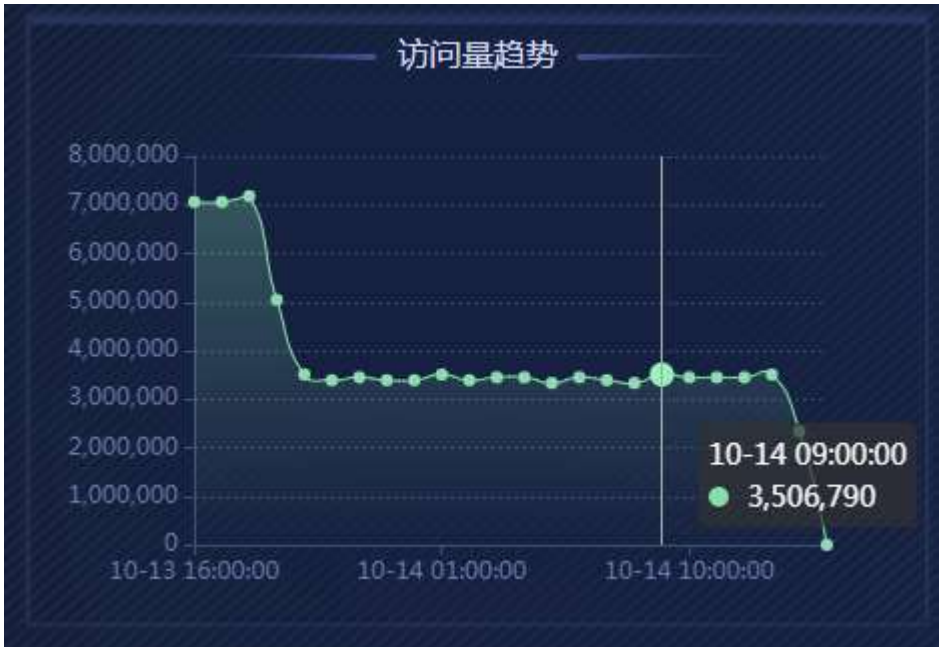



图 3 访问量趋势

#### 9.2.1.3 数据库账号风险排名 top10

数据库账号风险排名 top10 会展示系统内所有数据库账号风险分值最高的前 10 名用户，该处数据库账号分数与用户总体风险内账号分数评定方式不一致，同一账号分数可能存在不同；鼠标在用户悬浮后可查看数据库账号详细信息，详细信息包含数据库账号组、客户端用户数、访问量、UEBA 风险数、数据库审计告警数。点击数据库账号图标后，可以跳转至相应的账号风险画像中。如图 4。


图 4 数据库账号风险排名 top10

#### 9.2.1.4 数据库风险排名 top10

数据库风险排名 top10 会展示系统内所有数据库风险分值最高的前 10 个数据库，鼠标悬浮后可查看数据库详细信息，详细包含数据库所属资产、资产 IP、被访问量、UEBA 风险数、数据库审计告警数。点击数据库图标后，可以跳转至相应的数据库风险画像中。如图 5。


图 5 数据库风险排名 top10

#### 9.2.1.5 返回结果集大小趋势

返回结果集大小趋势展示的是所选时间范围内所有数据库账号及数据库的返回结果集。所选时间范围改变，返回结果集大小趋势的 X 轴会根据时间范围做自适应改变。如图 6。


图 6 返回结果集大小趋势

#### 9.2.1.6 数据库访问信息排名

该处可查看数据库、数据库账号、IP 地址、客户端工具的访问排名信息。可以分别从访问量、返回结果集两个视角进行查看，可选择查看前五名或最后五名的信息。如图 7。


图 7 数据库访问量信息排名

#### 9.2.1.7 风险事件

该处主要展示数据库及数据库账号发生的风险事件信息。风险对象可以选择数据库或者数据库账号，风险等级分为高、中、低三种，只能进行单选；在选择完毕后，异常风险行为数量会展示所选条件的事件数量总和，而风险列表内只会展示 100 条数据，翻滚至底部，可以点击“查看更多”按键，跳转至日志查询界面后查看更多日志，如图 8。


图 8 各选项及查看更多按键

点击列表内时间旁边的箭头可对风险事件进行排序操作（升序、降序）；点击风险对象可以跳转至相应的大屏子页面（数据库账号风险画像或数据库风险画像）；鼠标悬浮在风险详情图标上会显示具体的风险事件详情，点击原始日志，可以跳转至日志查询界面。如图 9。


图 9 风险详情

### 9.2.1.8 风险类型文字云

该处显示已发生风险事件所属的风险类型，事件数量越多，文字越大；鼠标悬浮在文字云上会显示具体事件数量；点击文字云后，会联动左侧风险事件列表，风险事件列表内显示相应类型的事件，如图 10。


图 10 文字云联动风险事件

#### 9.2.1.9 时间范围

时间范围可以筛选整个大屏的数据时间范围，时间范围可选择范围有：最近 24 小时、最近 7 天、本日、本周、本月、半年，如图 5。默认时间范围为最近 24 小时。调整时间范围后，页面内各模块会根据时间范围进行刷新，获取新的数据。如图 11。


图 14 -11 时间范围

### 9.2.2 数据库账号风险画像

数据库账号风险画像大屏整体布局如图 12 所示。大屏默认五分钟会进行一次刷新。


图 12 数据库账号风险画像

#### 9.2.2.1 账号搜索

数据库账号风险画像支持账号搜索功能，在搜索框内输入数据库账号，搜索后大屏会展示该数据库账号信息，如图 13。


图 13 账号搜索

#### 9.2.2.2 数据库账号信息及概要信息

在此处会显示数据库账号信息，信息包含：数据库账号、风险排名、风险分值、数据库账号组、活跃时间、客户端信息。客户端信息会优先展示登录主机名、若登录主机名为空则显示主机 IP 信息。右侧显示当前数据库账号的概要信息：使用 IP 地址个数、总访问量、总返回结果集大小、SQL 模板个数、SQL 语句平均执行时长、SQL 查询平均影响行数、平均返回结果集大小。

#### 9.2.2.3 访问量趋势

访问量趋势展示的是当前所选时间范围内，当前数据库账号的访问量趋势。所选时间范围改变，访问量趋势的 X 轴根据时间范围做自适应改变。

#### 9.2.2.4 数据库账号访问拓扑

数据库访问拓扑主要展示对应数据库账号至数据库之间的访问路径及访问关系。从内至外依次为数据库账号节点、访问路径节点、访问数据库节点。如图 14。

数据库账号节点内展示数据库账号名称、访问数据库个数。访问路径节点展示访问中使用的 IP 地址或者访问者的主机登录名。访问数据库节点内展示数据库名称、数据库风险分数、数据库所属资产信息。

图 14 数据库账号访问拓扑

鼠标悬浮在访问数据库节点及周边区域后，会展示对该数据库访问路径的聚合信息：登录主机名、客户端工具、执行操作类型、执行语句成功率、触发数据库审计告警数。点击访问数据库节点可以跳转至相应的数据库风险画像。如图 15。


图 15 聚合信息展示

#### 9.2.2.5 返回结果集大小趋势

返回结果集大小趋势展示的是所选时间范围内当前数据库账号的返回结果集。所选时间范围改变，返回结果集大小趋势的 X 轴会根据时间范围做自适应改变。

#### 9.2.2.6 数据库账号访问信息排名

该处可查看数据库访问量、客户端 IP 地址访问量、客户端工具访问量、操作类型访问量、数据库信息探测行为访问量。可以分别从访问量、返回结果集两个视角进行查看，可选择查看前五名或最后五名的信息。如图 16。


图 16 数据库账号访问信息排名

#### 9.2.2.7 风险事件

该处主要展示当前数据库账号在当前选择时间范围内发生的风险事件。用户可以更改风险等级来查看不同风险等级的事件，风险等级分为高、中、低三种，只可进行单选。选择完毕后，异常风险行为数量会展示所有事件的数量，而风险列表内只会展示 100 条风险事件，翻滚至页面底部，可以点击“查看更多”按键，跳转至日志查询界面查看更多日志。鼠标悬浮在风险详情上可以展示具体风险详情信息。如图 17。


图 17 风险事件

点击风险事件后，可以联动上方数据库账号访问拓扑，显示相应的数据库访问节点。点击时间旁边的排序按键可以对风险事件进行排序（升序或降序）；点击风险事件内的原始日志，可以跳转至日志查询界面查看该风险的日志详情。如图 18。


图 18 风险事件联动拓扑

#### 9.2.2.8 数据安全风险行为路径

数据安全风险行为路径展示当前数据库账号的风险行为路径。各个风险类型后面是该类型事件的计数个数。点击风险类型，可以联动左侧风险事件，显示相应的风险类型。如图 19。

图 19 数据安全风险行为路径联动风险事件

#### 9.2.2.9 时间范围

时间范围可以筛选整个大屏的数据时间范围，时间范围可以选择范围有：最近 24 小时、最近 7 天、本日、本周、本月、半年，如图 20。默认时间范围为最近 24 小时。调整时间范围后，页面内各模块会根据时间范围进行刷新，获取新的数据。


图 20 时间范围

### 9.2.3 数据库风险画像

数据库风险画像整体布局如图 21 所示。大屏默认五分钟会进行一次刷新。


图 21 数据库风险画像

#### 9.2.3.1 账号搜索

数据库风险画像支持账号搜索功能，在搜索框内输入数据库名称，搜索后大屏会展示该数据库信息，如图 22。


图 22 账号搜索

#### 9.2.3.2 数据库信息及概要信息

在此处会显示数据库信息，信息包含：数据库名称、风险排名、风险分值、数据库所属资产、活跃时间、访问客户端信息。访问客户端信息会优先展示登录主机名、若登录主机名为空则显示主机 IP 信息。右侧显示当前数据库的概要信息：访问 IP 地址个数、总访问条数、总返回结果集大小、SQL 模板个数、SQL 语句平均执行时长、SQL 查询平均影响行数、平均返回结果集大小。

#### 9.2.3.3 访问量趋势

访问量趋势展示的是当前所选时间范围内，当前数据库的访问量趋势。所选时间范围改变，访问量趋势的 X 轴根据时间范围做自适应改变。

#### 9.2.3.4 数据库访问拓扑

数据库访问拓扑主要展示对应数据库账号至数据库之间的访问路径及访问关系。从内至外依次为数据库节点、访问路径节点、访问数据库账号节点。

数据库节点内展示数据库名称、来访账号个数。访问路径节点展示访问中使用的 IP 地址或者访问者的主机登录名。访问数据库账号节点内展示数据库账号名称、数据库账号风险分数、数据库账号组信息。


图 23 数据库访问拓扑

鼠标悬浮在访问数据库账号节点及周边区域后，会展示对该数据库访问路径的聚合信息：登录主机名 TOP3、客户端工具 TOP3、执行操作类型 TOP3、执行语句成功率、触发数据库审计告警数。点击访问数据库节点可以跳转至相应的数据库风险画像。如图 23。


图 23 聚合信息展示

#### 9.2.3.5 返回结果集大小趋势

返回结果集大小趋势展示的是所选时间范围内当前数据库的返回结果集。所选时间范围改变，返回结果集大小趋势的 X 轴会根据时间范围做自适应改变。

#### 9.2.3.6 数据库账号访问信息排名

该处可查看数据库账号访问量、客户端 IP 地址访问量、客户端工具访问量、操作类型访问量、数据库信息探测行为访问量。可以分别从访问量、返回结果集两个视角进行查看，可选择查看前五名或最后五名的信息。如图 24。

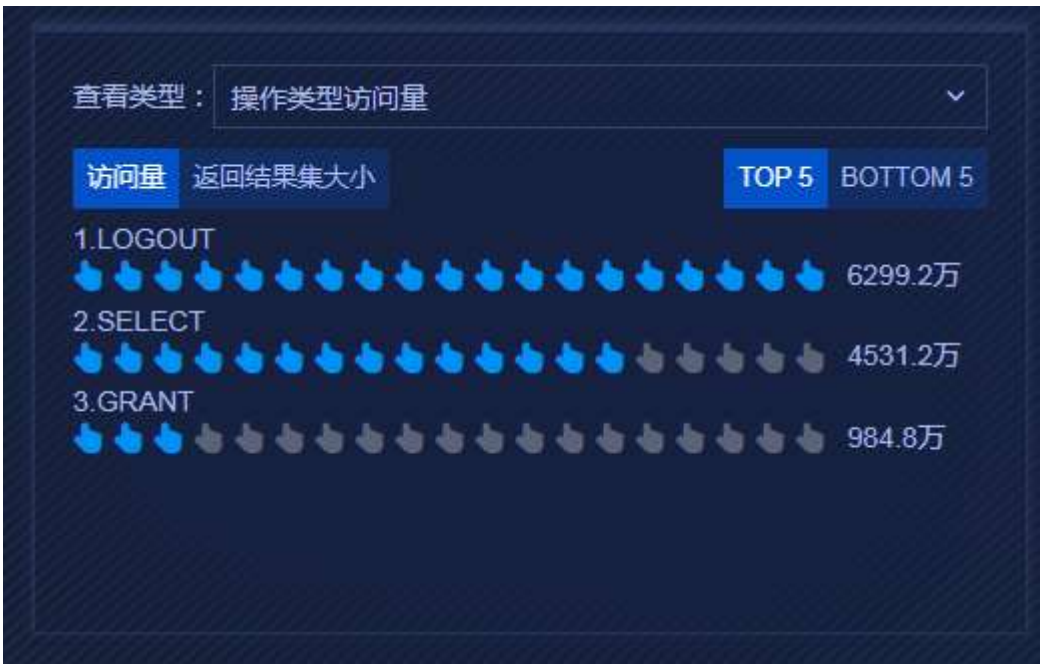



图 24 数据库账号访问信息排名

#### 9.2.3.7 风险事件

该处主要展示当前数据库在当前选择时间范围内发生的风险事件。用户可以更改风险等级来查看不同风险等级的事件，风险等级分为高、中、低三种，只可进行单选。选择完毕后，异常风险行为数量会展示所有事件的数量，而风险列表内只会展示 100 条风险事件，翻滚至页面底部，可以点击“查看更多”按键，跳转至日志查询界面查看更多日志。鼠标悬浮在风险详情上可以展示具体风险详情信息。如图 25。


图 25 风险事件

如图 26。点击风险事件后，可以联动上方数据库访问拓扑，显示相应的数据库账号访问节点。点击时间旁边的排序按键可以对风险事件进行排序（升序或降序）；点击风险事件内的原始日志，可以跳转至日志查询界面查看该风险的日志详情。


图 26 风险事件联动拓扑

#### 9.2.3.8 数据安全风险行为路径

数据安全风险行为路径展示当前数据库的风险行为路径。各个风险类型后面是该类型事件的计数个数。点击风险类型，可以与左侧风险事件联动，显示相应的风险类型。如图 27。


图 27 数据安全风险行为路径联动风险事件

#### 9.2.3.9 时间范围

时间范围可以筛选整个大屏的数据时间范围，时间范围可以选择范围有：最近 24 小时、最近 7 天、本日、本周、本月、半年，如图 28。默认时间范围为最近 24 小时。调整时间范围后，页面内各模块会根据时间范围进行刷新，获取新的数据。


图 28 时间范围

## 9.3 账号安全解决方案大屏

### 9.3.1 账号安全态势感知大屏

账号安全态势感知大屏整体布局如图所示。大屏默认五分钟会进行一次刷新。


图 1 账号安全态势感知大屏

#### 9.3.1.1 分析视角及分析时间范围

分析视角，切换分析视角可以影响整个大屏，下方数据会随视角改变，视角包含：整体关联视角、VPN 日志、AD 域日志、上网行为审计日志、堡垒机日志、邮件审计日志、零信任日志，默认选项为整体关联视角，如图 2。


图 2 分析视角

分析时间范围，切换时间范围可以影响整个大屏，大屏的时间随之改变，时间范围包含：最近 24 小时、最近 7 天、本日、本周、本月、半年，默认选项为最近 7 天，如图 3 所示。


图 3 分析时间范围

#### 9.3.1.2 账号日志概览

账号日志概览显示当前所选时间范围和分析视角下的日志数量及账号数量。

日志量表示原始日志数量，告警量表示异常结果日志数量，活跃账号数表示有效登录或访问的账号数量，高风险账号数表示风险评级为高的账号数量。如图 4。


图 4 账号日志概览

#### 9.3.1.3 账号地理位置分布图

账号地理位置分布图展示在所选时间范围和分析视角下所有账号在地图上的位置。点击左上角图标，可以在世界地图与中国地图之间切换。在地图上会有亮点显示，表示该处有

账号登录或访问，账号数量的多少会决定各地区的颜色深浅。鼠标放置于亮点上，会显示当前地理位置、账号数量、出现频率 top3 的账号，点击任意账号可以跳转至账号安全风险画像大屏下的该用户画像。如图 5。

图 5 账号亮点显示

在分布图左下角为局域网模块，展示 10、172、192 三个网段的账号数，鼠标放置任一网段后，显示该网段出现频率 top3 的账号及登录次数。点击任意账号可以跳转至账号安全风险画像大屏下的该用户画像。如图 6。

图 6 局域网模块

#### 9.3.1.4 账号风险排名 top5 及账号登录失败 top5

账号风险排名 top5，展示在所选时间范围及分析视角下风险得分排名前 5 的账号及其分数，鼠标放置在账号上，会悬浮展示该账号的部门、日志量、最近登录时间、最常用来源 IP、最常用目的 IP、告警 top3 等信息。点击任意的账号可以跳转至账号安全风险画像大屏下的该用户画像。如图 7。


图 7 账号风险排名 top5

账号登录失败 top5，展示所选时间范围及分析视角下登录失败数量前 5 的账号及其失败次数。鼠标放置在账号上，悬浮显示该账号的部门、日志量、最近登录时间、最常用来源 IP、最常用目的 IP、告警信息等。点击任意账号可以跳转至账号安全风险画像大屏下的该用户画像。如图 8。


图 8 登录失败 top5

#### 9.3.1.5 日志量情况轮播

该处区域会轮播日志量的相关图表，一共四张图表：日志量趋势、24 时账号数量分布、部门日志量 top5、账号日志量 top5。

日志量趋势，展示日志总量趋势及平均值，如图 9。

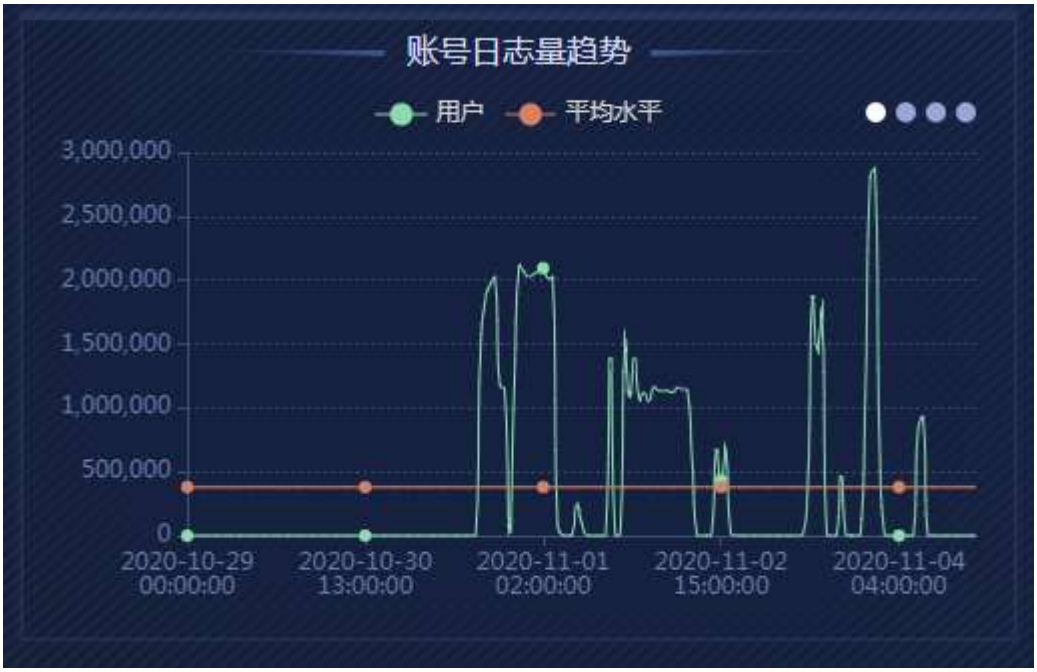



图 9 日志量趋势

24 时账号数量分布，展示当天 0 至 24 时每个小时段的在线账号数量和平均值，如图 10。


图 10 24 时账号数量分布

部门日志 top5，展示日志量排名前 5 的部门和日志数量，如图 11。


图 11 部门日志量 top5

日志量 top5，展示日志量前 5 的账号和日志数量。鼠标放置在账号上，悬浮显示该账号的部门、日志量、最近登录时间、最常用来源 IP、最常用目的 IP、告警 top3 等信息。点击任意账号可以至账号安全风险画像大屏下的该用户画像。如图 12。


图 12 账号日志量 top5

#### 9.3.1.6 风险事件

风险事件主要展示所选时间范围及分析视角下账号发生的风险事件信息。风险等级分为高、中、低三种，只能进行单选；在选择完毕后，异常风险行为数量会展示所选条件的事件数量总和，而风险列表内只会展示 100 条数据，翻滚至底部，可以点击“查看更多”按键，跳转至日志查询界面后查看更多日志。如图 13。


图 13 风险事件

点击列表内时间旁边的箭头可对风险事件进行排序操作（升序、降序）；点击风险对象可以跳转至相应的大屏子页面（账号安全风险画像）；鼠标悬浮在风险详情图标上会显示具体的风险事件详情，点击原始日志，可以跳转至日志查询界面。

#### 9.3.1.7 风险类型文字云

风险类型文字云，显示已发生风险事件所属的风险类型，事件数量越多，文字越大；鼠标悬浮在文字云上会显示具体事件数量；点击文字云后，会联动左侧风险事件列表，风险事件列表内显示相应类型的事件，如图 14。


图 14 风险类型文字云

### 9.3.2 账号安全风险画像

账号安全风险画像整体布局如图所示。大屏默认五分钟会进行一次刷新。


图 15 账号安全风险画像

#### 9.3.2.1 账号搜索

账号搜索，用户可以在此处搜索想要呈现的账号，大屏数据随之改变。


16 账号搜索

#### 9.3.2.2 账号分析视角及时间范围

分析视角，切换分析视角可以影响整个大屏，下方数据会随视角改变，视角包含：整体关联视角、VPN 日志、AD 域日志、上网行为审计日志、堡垒机日志、邮件审计日志、零信任日志，默认选项为整体关联视角，如图 17。


图 17 分析视角

分析时间范围，切换时间范围可以影响整个大屏，大屏的时间随之改变，时间范围包含：最近 24 小时、最近 7 天、本日、本周、本月、半年，默认选项为最近 7 天，如图 18 所示。


图 18 时间范围

#### 9.3.2.3 账号信息

账号信息展示账号的基本信息（姓名、关注程度、组织架构、工作状态、），风险评分、较昨日风险浮动、当前风险排名。点击账号可以跳转至该用户的用户行为画像界面。如图 19。


图 19 账号信息

#### 9.3.2.4 账号概览

账号概览展示所选时间范围及分析视角下的账号的日志数、触发模型数量、登录成功次数、登录失败次数。点击日志数量、触发特征数量、登录成功次数、登录失败次数可以跳转至相应的日志查询界面。如图 20。


图 20 账号概览

#### 9.3.2.5 账号地理位置分布图

账号地理位置分布图展示所选时间范围及分析视角下账号在地图上的位置信息。点击左上角图标，可以在世界地图与中国地图之间切换。在地图上会有亮点显示，表示该处有账号登录或访问，账号数量的多少会决定各地区的颜色深浅。鼠标放置于亮点上，会显示当前地理位置、账号登录次数、出现频率 top3 的 IP 及其登录次数。如图 21。


图 21 账号地理位置分布图

在分布图右下角为局域网模块，展示 10、172、192 三个网段的账号数，鼠标放置任一网段后，显示该网段出现频率 top3 的账号及登录次数。如图 22。


图 22 局域网模块

#### 9.3.2.6 访问量趋势

访问量趋势展示所选时间范围及分析视角下当前账号和所有账号的平均日志数量趋势。如图 23。

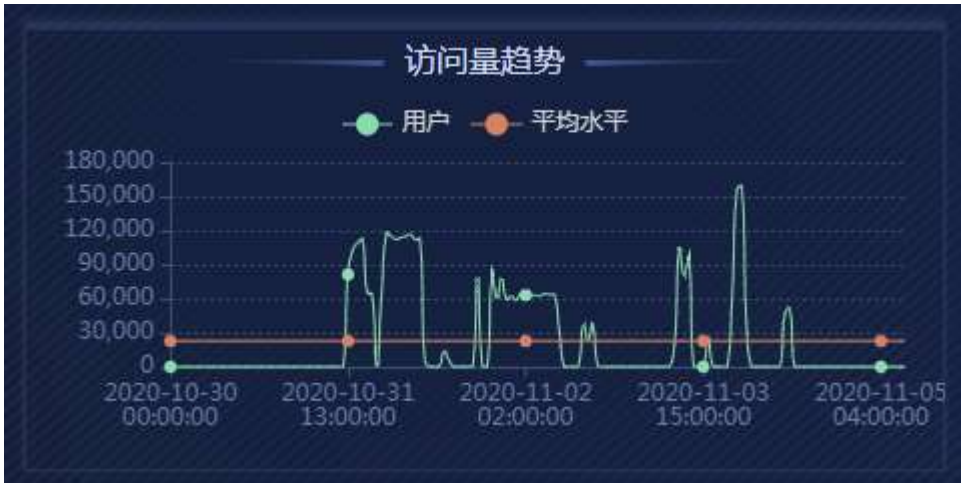



图 23 访问量趋势

#### 9.3.2.7 24 时段在线频次

24 时段在线频次展示所选时间范围和分析视角下账号 0 至 24 时每个小时段的日志量和所有账号的平均日志数量。如图 24。


图 24 24 时段在线频次

#### 9.3.2.8 风险画像

该处会展示所选时间范围及分析视角下，账号异常排名前三的特征的风险画像。如图 25。


图 25 风险画像

#### 9.3.2.9 风险事件

风险事件主要展示所选时间范围及分析视角下当前账号发生的风险事件信息。风险等级分为高、中、低三种，只能进行单选；在选择完毕后，异常风险行为数量会展示所选条件的事件数量总和，而风险列表内只会展示 100 条数据，翻滚至底部，可以点击“查看更多”按键，跳转至日志查询界面后查看更多日志。如图 26。


图 26 风险事件

点击列表内时间旁边的箭头可对风险事件进行排序操作（升序、降序）；鼠标悬浮在风险详情图标上会显示具体的风险事件详情，点击原始日志，可以跳转至日志查询界面。

#### 9.3.2.10 风险类型文字云

风险类型文字云，显示已发生风险事件所属的风险类型，事件数量越多，文字越大；鼠标悬浮在文字云上会显示具体事件数量；点击文字云后，会联动左侧风险事件列表，风险事件列表内显示相应类型的事件，如图 27。

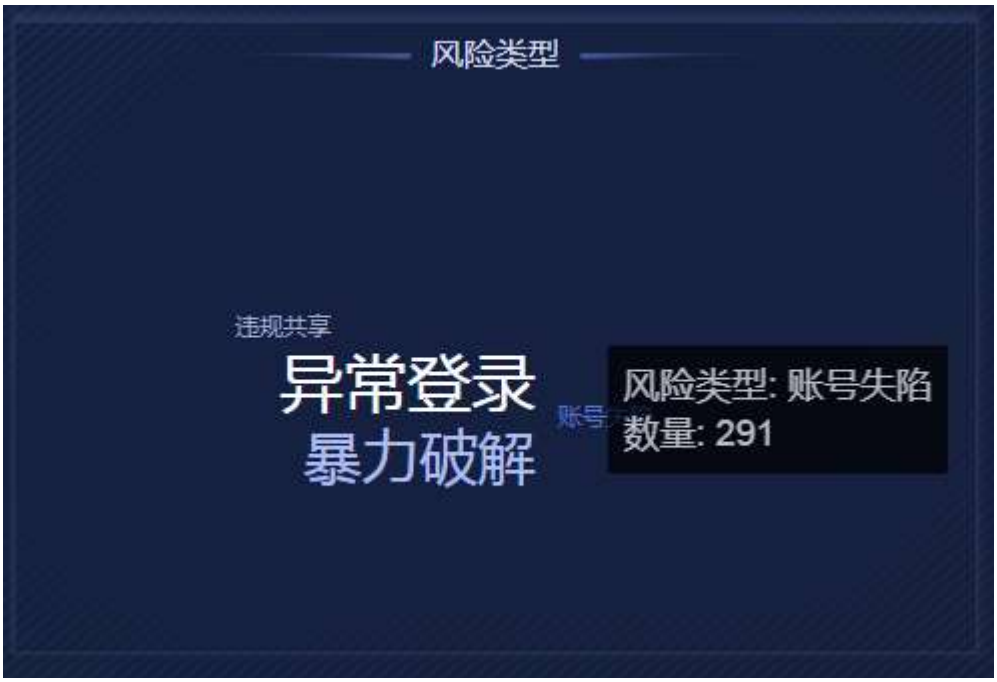



图 27 风险类型文字云

## 9.4 主机安全大屏

### 9.4.1 主机安全态势感知

大屏整体布局如图 1 所示。大屏默认五分钟会进行一次刷新。


图 1 主机安全态势感知大屏

#### 9.4.1.1 主机概览

主机概览主要展示系统内主机的概要信息。展示字段包含：Windows 主机个数、Linux 主机个数、MAC 主机个数、主机账号个数、登录 IP 个数、主机连接数、总日志量、总告警量、高风险主机个数。如图 2。

Windows 主机个数表示所选时间范围内 Windows 主机的个数。

Linux 主机个数表示所选时间范围内 Linux 主机的个数。

MAC 主机个数表示所选时间范围内 MAC 主机的个数。

主机账号个数表示所选时间范围内登录每台主机的所有账号总和。

登录 IP 个数表示所选时间范围内所有 IP 地址的总和。

主机连接数表示所选时间范围内每台主机连接数的总和。

总日志量表示所选时间范围内原始日志的数量。

总告警量表示所选时间范围内特征触发的告警数量。

高风险主机个数表示所选时间范围内风险评级为高的最新的高风险主机个数。

图 2 主机概览

#### 9.4.1.2 高风险主机趋势

高风险主机趋势展示所选时间范围内风险评级为高的主机数量趋势。鼠标悬浮某个时刻可以展示该时刻的高风险主机个数、高风险主机 top3。如图 3。

点击高风险主机 top3 内的 IP 地址可以跳转至相应的主机风险画像。

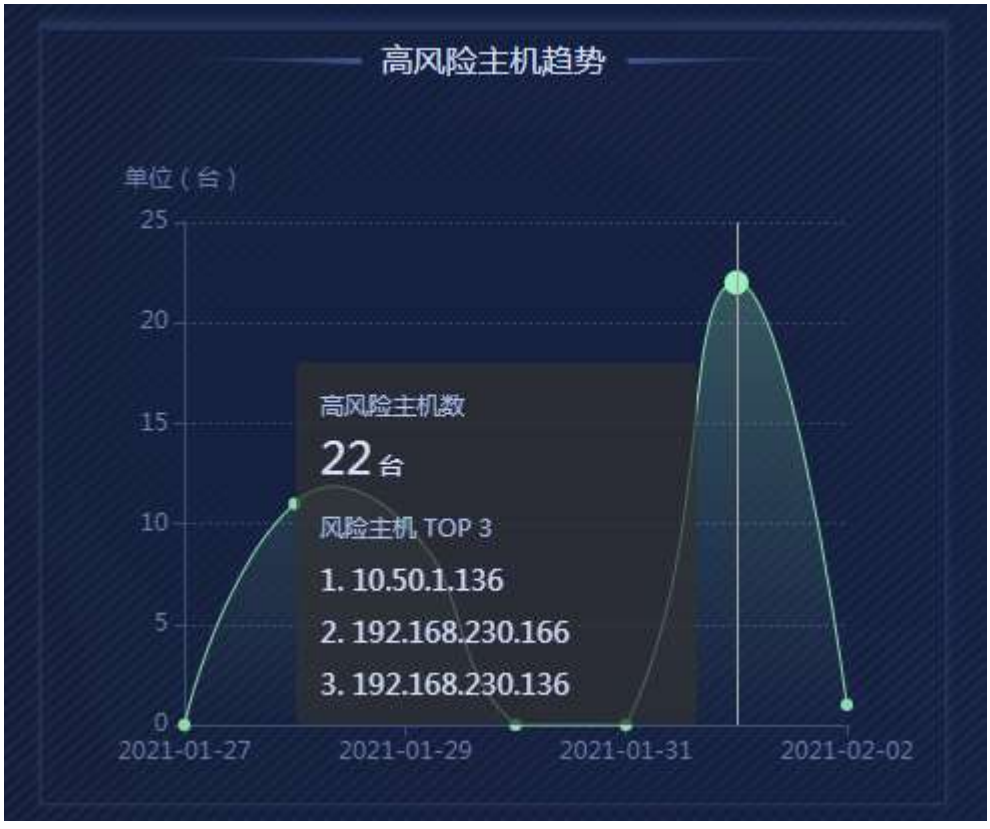



图 3 高风险主机趋势

#### 9.4.1.3 风险主机连接拓扑及主机风险排名 top10

风险主机连接拓扑及主机风险排名 top10 轮播展示所选时间范围内风险排名前 10 的主机。如图 4。


图 4 风险主机连接拓扑及主机风险排名 top10

如图 5。风险主机连接拓扑展示主机的连接关系，默认展示与该主机有连接关系的风险评分前 8 的风险主机。鼠标放置在主机上可以展示主机的风险评分、主机部门、日志数量、主机唯一标识、告警 top3。点击主机唯一标识可以跳转至相应的主机风险画像。


图 5 悬浮窗口展示

主机风险排名 top10 展示风险排名前 10 的主机 IP 及风险评分。点击排名中的 IP 地址，可以联动左侧风险主机连接拓扑，会显示相应的主机。且当鼠标移入主机风险排名 top10，会停止轮播，鼠标移出后继续轮播。如图 6。

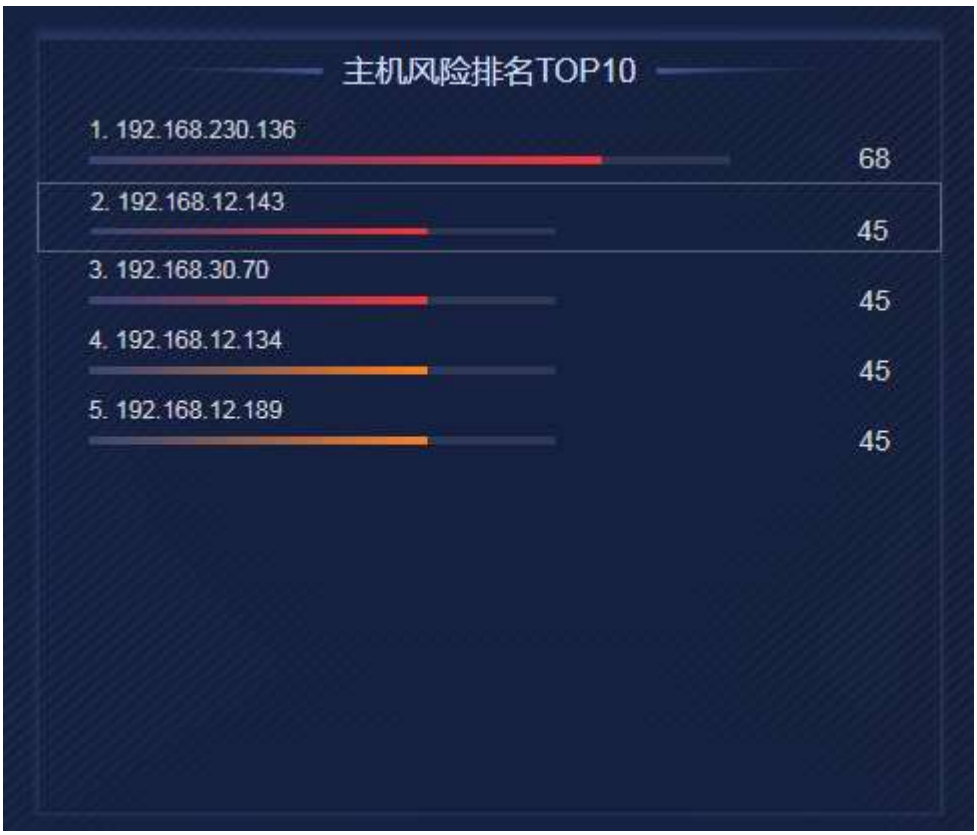



图 6 主机风险排名 top10

#### 9.4.1.4 风险部门主机概览及部门风险排名 top10

风险部门主机概览及部门风险排名 top10 轮播展示所选时间范围内风险排名前 10 的部门。如图 7。

图 7 风险部门主机概览及部门风险排名 top10

当系统内没有部门消息时，风险部门主机概览置灰，鼠标移至该处会提示“当前数据源中无部门消息，可在添加部门相关信息后查看。”

风险部门主机概览会展示部门的风险主机信息，默认展示风险主机数最多的部门。鼠标放置在主机上可以展示主机的风险评分、主机部门、日志数量、主机唯一标识、告警 top3。如图 8。点击主机唯一标识可以跳转至相应的主机风险画像。


图 8 悬浮窗口展示

部门风险排名 top10 展示风险排名前 10 的部门及风险评分。点击排名中的部门，可以联动左侧风险部门主机概览，会显示相应的部门。且当鼠标移入部门风险排名 top10，会停止轮播，鼠标移出后继续轮播。如图 9。


图 9 部门风险排名 top10

#### 9.4.1.5 五图轮播区域

该处是分别是主机访问量趋势、主机账号日志量 top5、24 时活跃主机分布、主机发送连接数 top5、主机接收连接数 top5 五张图进行轮播展示。

主机访问量趋势展示所选时间范围内的日志总量趋势和访问的平均值。鼠标悬浮某个时刻，展示该时刻的时间、日志数、平均水平。如图 10。


图 10 主机访问量趋势

主机账号日志量 top5 展示所选时间范围内总日志量排名前五的主机账号和日志量数。点击任一主机账号可跳转至相应的主机风险画像。如图 11。


图 11 主机账号日志量 top5

24 时活跃主机分布展示所选时间范围内 0 至 24 时每个时段的活跃主机分布。鼠标悬浮在某一时刻，展示该时刻的时间、主机数、平均水平。如图 12。


图 12 时活跃主机分布

主机发送连接数 top5 展示所选时间范围内发送连接数排名前五的主机和连接数，主机用登录名和主机 IP 地址展示。点击主机可以跳转至相应的主机风险画像。如图 13。

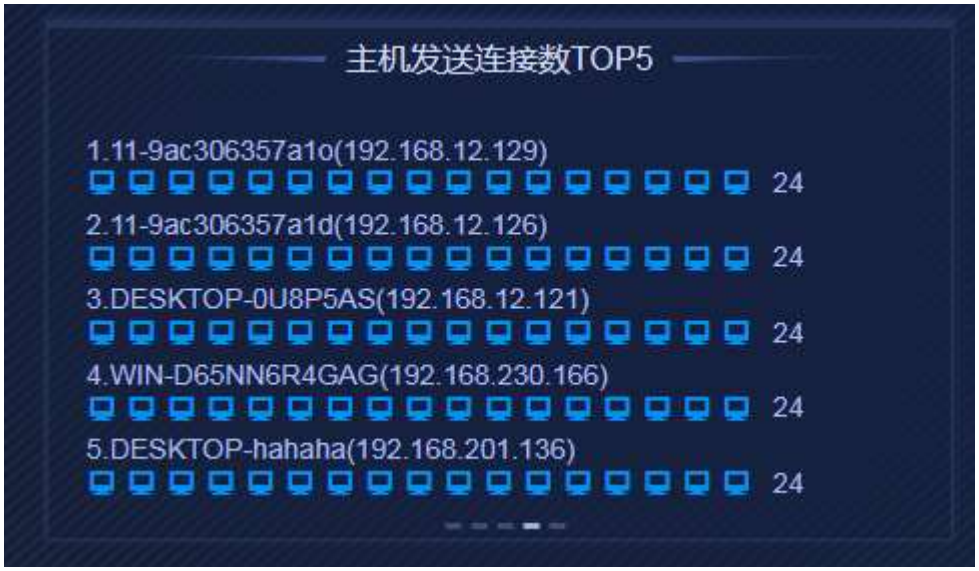



图 13 主机发送连接数 top5

主机接收连接数 top5 展示所选时间范围内接收连接数排名前五的主机和连接数，主机用登录名和主机 IP 地址展示。点击主机可以跳转至相应的主机风险画像。如图 14。

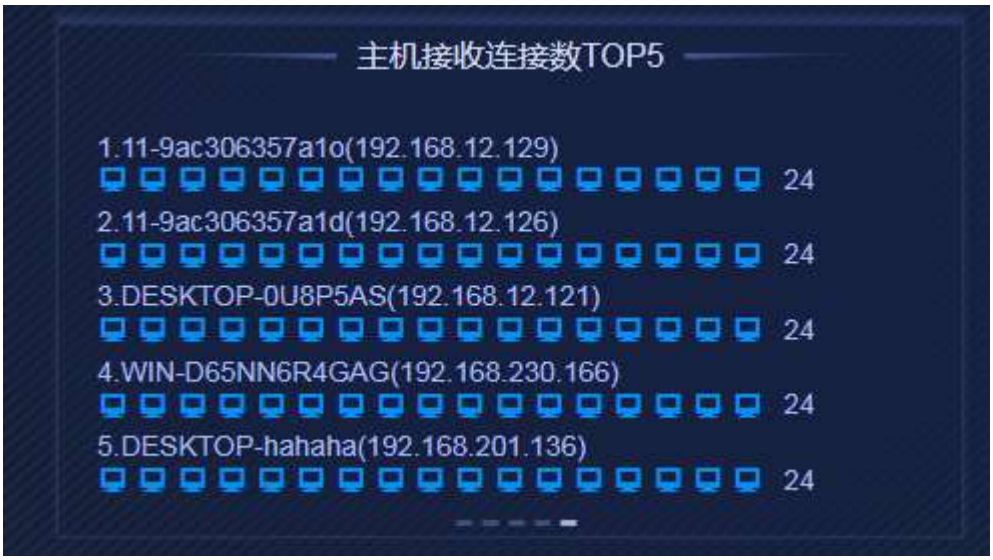



图 14 主机接收连接数 top5

#### 9.4.1.6 风险事件

风险事件主要展示主机相关的风险事件信息。展示字段包含异常风险行为数量、风险等级、时间、风险对象、风险描述、风险类型、风险详情、溯源操作。

风险等级分为高、中、低三种，只能进行单选；在选择完毕后，异常风险行为数量会展示所选条件的事件数量总和，而风险列表内只会展示 100 条数据，翻滚至底部，可以点击“查看更多”按键，跳转至日志查询界面后查看更多日志，如图 15。


图 15 各选项及查看更多按键

点击列表内时间旁边的箭头可对风险事件进行排序操作（升序、降序）；点击风险对象可以跳转至相应的主机风险画像；鼠标悬浮在风险详情图标上会显示具体的风险事件详情，点击原始日志，可以跳转至日志查询界面。如图 16。

图 16 风险详情

#### 9.4.1.7 风险类型

风险类型展示 10 种风险类型：异常登录、数据泄露、文件访问异常、恶意程序、敏感资源访问、活动偏离自身基线、网络访问异常、注册表操作异常、进程行为异常、其他风险。鼠标放置在风险类型上会显示该风险类型在所选时间范围内触发的次数，点击风险类型可以联动左侧风险事件，风险事件内会显示该风险类型的事件。如图 17。

图 17 风险类型联动风险事件

#### 9.4.1.8 时间范围

时间范围可以筛选整个大屏的数据时间范围，时间范围可选择范围有：最近 24 小时、最近 7 天、本日、本周、本月、半年，如图 18。默认时间范围为最近 7 天。调整时间范围后，页面内各模块会根据时间范围进行刷新，获取新的数据。


图 16 -18 时间范围

### 9.4.2 主机风险画像

主机风险画像大屏整体布局如图 19 所示。大屏默认五分钟会进行一次刷新。


图 19 主机风险画像

#### 9.4.2.1 主机搜索

主机风险画像支持搜索功能，在搜索框内输入主机唯一标识或者主机 IP 地址，搜索后大屏会展示该主机信息，如图 20。


图 20 主机搜索

#### 9.4.2.2 主机信息

主机信息展示当前主机的基本信息、风险评分、较昨日风险浮动、当前风险排名。基本信息展示字段包含主机名、主机 IP 地址、操作系统、主机唯一标识。如图 21。点击主机唯一标识可跳转至相应的用户行为画像下的全局画像模式。


图 21 主机信息

#### 9.4.2.3 风险趋势

风险趋势展示所选时间范围内该主机风险评级为高中低的趋势，鼠标悬浮某个时刻会展示该时刻的时间及风险评分。如图 22。


图 22 风险趋势

#### 9.4.2.4 主机总体连接

主机总体连接主要展示当前主机整体的连接情况，展示当前主机以及与该主机有连接关系的前 10 的主机。不同风险程度的主机会用不同颜色进行标识。主机之间的连接线上不同的流向代表了主机的发送接收关系。点击任意主机 IP 可以跳转至相应的主机风险画像。如图 23。


图 23 主机总体连接

鼠标悬浮在某一主机，会展示风险评分、主机部门、日志数量、主机唯一标识、告警 top3，如图 24。


图 24 悬浮窗口展示

#### 9.4.2.5 主机发送连接

主机发送连接主要展示当前主机整体的连接情况，展示当前主机以及与该主机有发送关系的前 10 的主机。不同风险程度的主机会用不同颜色进行标识。点击任意主机 IP 可以跳转至相应的主机风险画像。鼠标悬浮在某一主机，会展示风险评分、主机部门、日志数量、主机唯一标识、告警 top3。如图 25。


图 25 主机发送连接

#### 9.4.2.6 主机接收连接

主机发送连接主要展示当前主机整体的连接情况，展示当前主机以及与该主机有发送关系的前 10 的主机。不同风险程度的主机会用不同颜色进行标识。点击任意主机 IP 可以跳转至相应的主机风险画像。鼠标悬浮在某一主机，会展示风险评分、主机部门、日志数量、主机唯一标识、告警 top3。如图 26。


图 26 主机接收连接

#### 9.4.2.7 主机概览

主机概览展示所选时间范围内当前主机的日志数、主机账号数、触发特征数、总连接数。如图 27。


图 27 主机概览

#### 9.4.2.8 主机 24 时活跃分布

主机 24 时活跃分布展示在所选时间范围内 0-24 时当前主机的日志量分时统计趋势。鼠标悬浮在某一时刻展示该时刻的时间、主机、平均水平。如图 28。


图 28 主机 24 时活跃分布

#### 9.4.2.9 趋势图轮播区域

趋势图轮播区域轮播展示主机日志量趋势、主机发送连接数趋势、主机接收连接数趋势。

主机日志量趋势展示所选时间范围内当前主机日志总量趋势和所展示时间范围的平均值。鼠标悬浮在某一时刻展示该时刻的时间、日志数、平均水平。如图 29。


图 29 主机日志量趋势

主机发送连接趋势展示所选时间范围内当前主机发送连接数趋势，鼠标悬浮在某一时刻会展示该时刻的时间、连接数。如图 30。

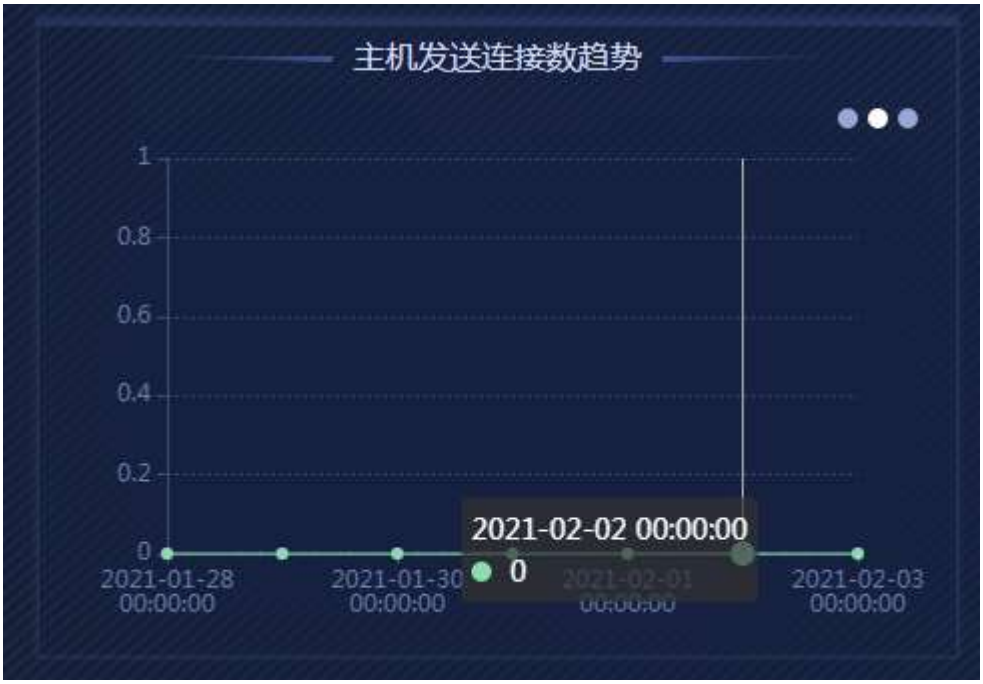



图 30 主机发送连接数趋势

主机接收连接趋势展示所选时间范围内当前主机接收连接数趋势，鼠标悬浮在某一时刻会展示该时刻的时间、连接数。如图 31。

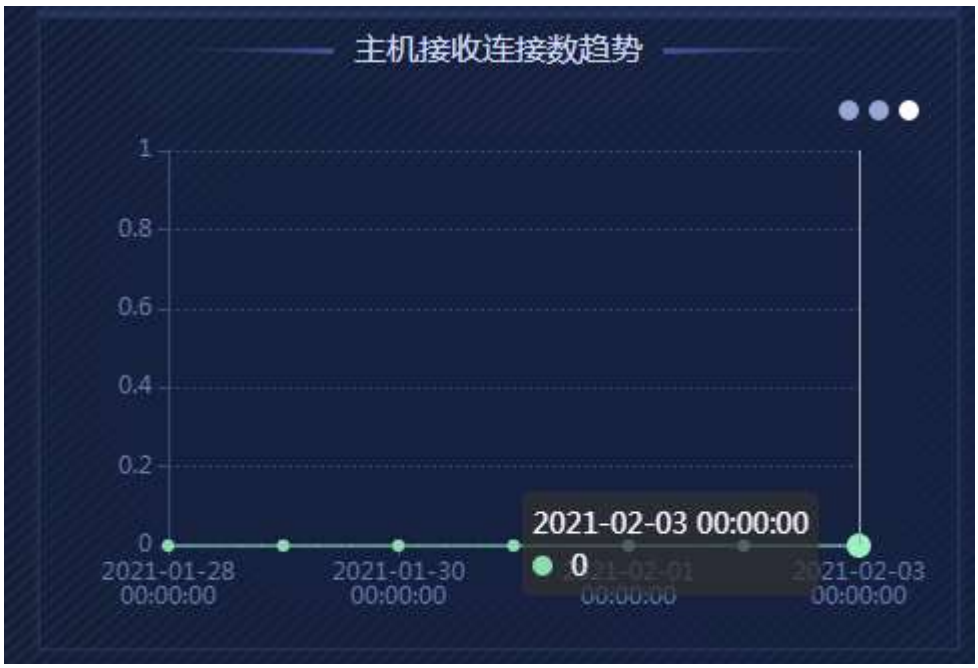



图 31 主机接收连接数趋势

#### 9.4.2.10 风险事件

风险事件主要展示当前主机的风险事件信息。展示字段包含异常风险行为数量、风险等级、时间、风险描述、风险类型、风险详情、溯源操作。

风险等级分为高、中、低三种，只能进行单选；在选择完毕后，异常风险行为数量会展示所选条件的事件数量总和，而风险列表内只会展示 100 条数据，翻滚至底部，可以点击“查看更多”按键，跳转至日志查询界面后查看更多日志，如图 32。


图 32 各选项及查看更多按键

点击列表内时间旁边的箭头可对风险事件进行排序操作（升序、降序）；鼠标悬浮在风险详情图标上会显示具体的风险事件详情，点击原始日志，可以跳转至日志查询界面。如图 33。


图 33 风险详情

#### 9.4.2.11 风险类型

风险类型展示当前主机的 10 种风险类型：异常登录、数据泄露、文件访问异常、恶意程序、敏感资源访问、活动偏离自身基线、网络访问异常、注册表操作异常、进程行为异常、其他风险。鼠标放置在风险类型上会显示该风险类型在所选时间范围内触发的次数，点击风险类型可以联动左侧风险事件，风险事件内会显示该风险类型的事件。如图 34。

图 34 风险类型联动风险事件

#### 9.4.2.12 时间范围

时间范围可以筛选整个大屏的数据时间范围，时间范围可选择范围有：最近 24 小时、最近 7 天、本日、本周、本月、半年，如图 35。默认时间范围为最近 7 天。调整时间范围后，页面内各模块会根据时间范围进行刷新，获取新的数据。


图 35 时间范围

# 10 系统配置

## 10.1 升级管理

点击系统页面右上角，展开功能框，点击“升级管理”，页面跳转进入到相关页面，在该页面中，支持升级管理功能，能够通过升级包的形式对平台功能及 UEBA 特征进行快速的升级优化，如下图表所示：


图 57 升级页面

| 序号 | 名称 | 说明 |
| --- | --- | --- |
| 1 | 版本说明 | 对当前的版本进行一个简单的介绍 |
| 2 | 上传功能 | 可以将相关的升级包进行上传升级（会对包进行名称校验等） |
| 3 | 说明 | 对在升级过程中，会遇到的一些情况及时间进行说明描述，方便用户知晓 |
| 4 | 升级历史 | 该区域可以展示出历史中已经升级过的记录，备注列显示具体升级情况 |
| 5 | 特征升级 | 可以对系统原有的特征进行平滑升级 |

表 1 升级功能

点击上传特征升级包，全部特征包/内置特征包，上传后直接覆盖升级；

上传所选特征包/定制特征包，上传后判断导入环境是否已有特征，弹出对应提示：【xx1、xx2…】特征已存在共 n 个，是否确定覆盖升级？


点击确定，覆盖已有特征；点击取消，跳过已有特征升级。

## 10.2 外发配置（告警外发）

### 10.2.1 Kafka 外发告警

点击系统页面右上角，展开功能框，点击“外发配置”，页面跳转进入到相关页面

外发配置功能，该功能可以将系统内的风险事件详情发送至指定的 KAFKA 服务器内，如图:

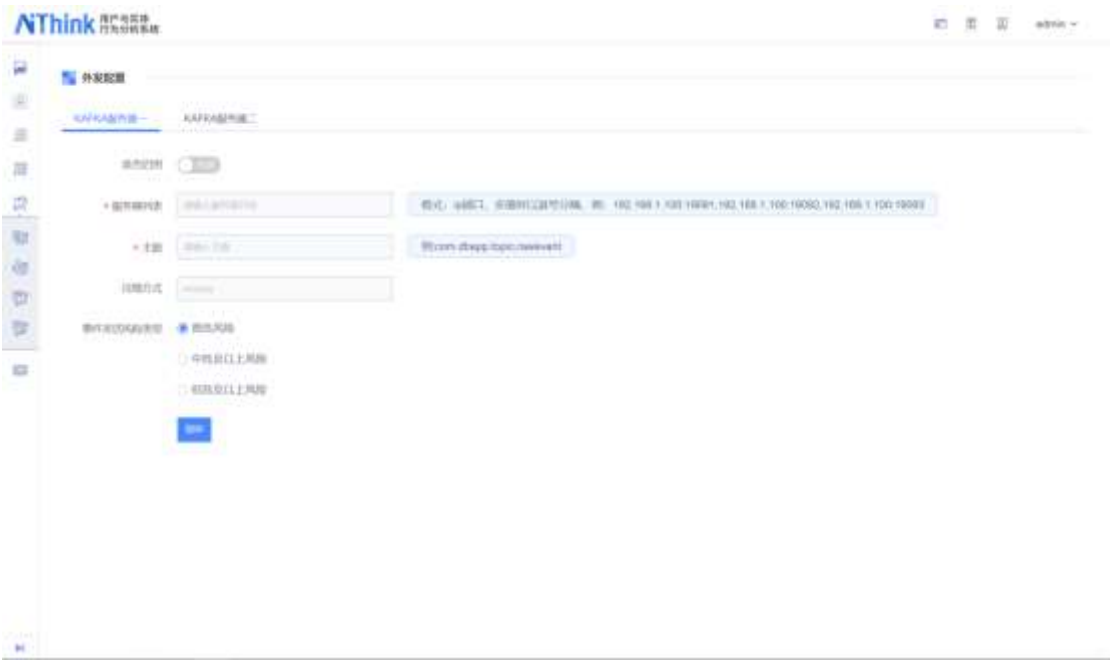



图 58 外发配置页面

服务器列表:此处填写 KAFKA 服务器的地址及其端口号，格式为 IP 地址端口号，当存在多个 KAFKA 节点时以逗号进行分隔，例如：192.168.30.190:19091,192.168.30.190:19092,192.168.30.190:19093。

主题:此处填写 KAFKA 服务器内的具体主题（topic）名称。

压缩方式默认为 snappy，不可修改。

事件发送风险类型，有三种选项，分别为高危风险、中危及以上风险、低危及以上风险。事件风险级别为高中低三种，该级别与用户总体风险内风险阈值调整无关，与用户行为画像内风险级别一致。

在配置完 KAFKA 服务器列表及主题，选择事件发送风险类型后，可进行连通性测试，若是可以连接成功，会有连接成功的提示。

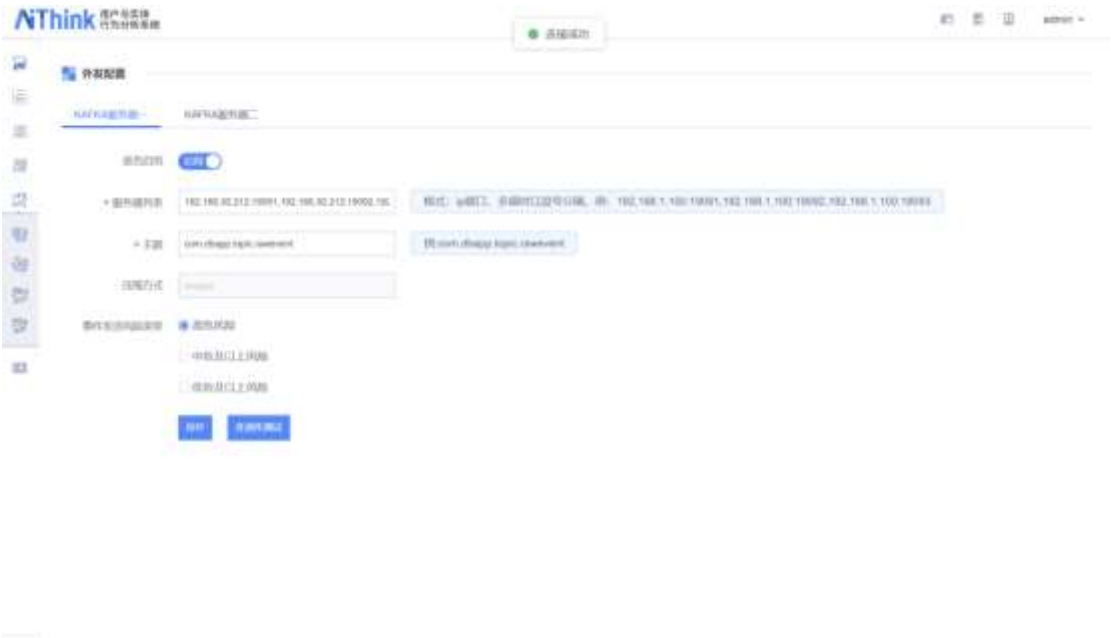


图 59 连接成功

外发配置可同时配置两个 KAFKA 服务器，按照用户需求可分别发往不同 KAFKA 服务器，以及选择不同事件发送风险类型。

### 10.2.2 Syslog 转发功能

Syslog 转发功能，该功能可以将系统内风险事件详情发送至指定的服务器中，如图 4：

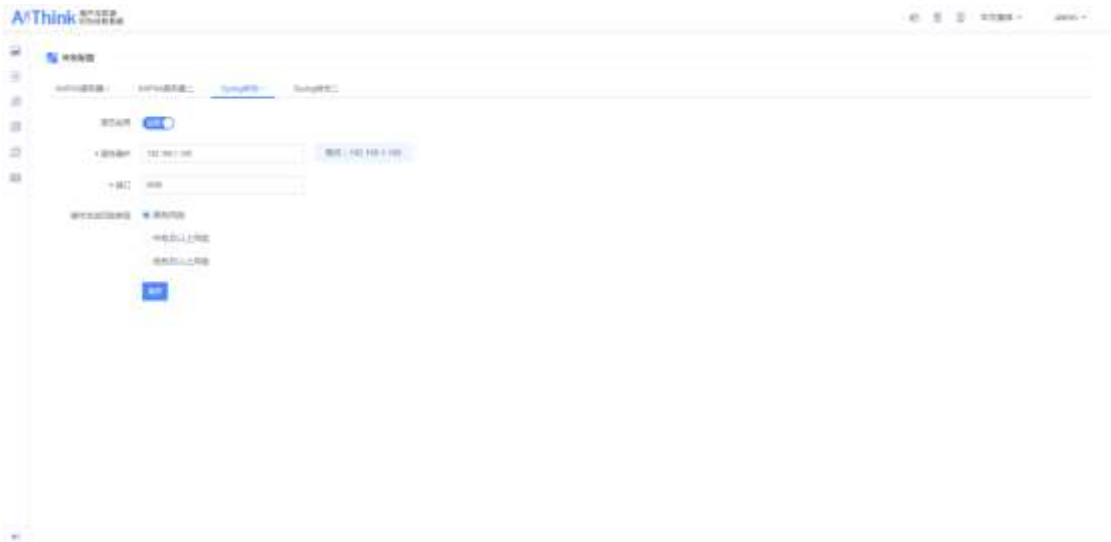


图 4 Syslog 转发功能

服务器 IP：此处填写需要发往数据的服务器地址，格式为 IP 地址，例如 192.168.1.100。

端口：此处填写服务器的端口号。

事件发送风险类型，有三种选项，分别为高危风险、中危及以上风险、低危及以上风险。事件风险级别为高中低三种，该级别与用户总体风险内风险阈值调整无关，与用户行为画像内风险级别一致。

Syslog 转发可同时配置两个服务器，按照用户需求可分别发往不同服务器，以及选择不同事件发送风险类型。

## 10.3 白名单

点击系统页面右上角，展开功能框，点击“白名单”，页面跳转进入到相关页面。

白名单配置页面，主要用于对系统内白名单进行配置。用户可在该页面新增、编辑、查找、删除白名单。如图 5：


图 5 白名单配置页面

点击新增白名单按键，弹出添加白名单窗口，配置相关白名单的条件、策略名称、策略描述、历史风险。白名单条件为风险特征名称以及用户录入主键，策略名称及策略描述可随意填写，历史风险勾选后则会删除当前用户录入主键该特征最近 7 天的风险事件（用户行为画像内风险事件、日志查询内风险事件），单次勾选有效，如图 6：


图 6 添加白名单

白名单添加完成后，系统内不再对白名单内的风险对象的该特征进行计算。

启用、禁用：在设置白名单后，默认为开启状态，用户可以选择禁用白名单，禁用后白名单不再生效。

全文搜索框：用户可以通过全文搜索框输入白名单名称或白名单条件等查找白名单。

## 10.4 许可证

点击系统页面右上角，展开功能框，点击“许可证”，页面跳转进入到相关页面。该页面中可以导出许可证申请文件用户许可证申请，可以带入相关的许可证（如果许可证不正确将提示错误信息）。

并且在许可证页面中会有先关系统及许可在的相关信息。居然如下图 7 所示：


图 7 许可证

## 10.5 修改密码

点击系统页面右上角，展开功能框，点击“修改密码”，页面跳转进入到相关页面。该页面可以对本系统的密码进行重置操作，重置成功后默认会退出系统，需要重新登录。


图 8 修改密码

## 10.6 关于

点击系统页面右上角，展开功能框，点击“关于”，页面跳转进入到相关页面。

该页面中主要展示本系统版本信息，包括系统名称、软件版本、所属公司。如图 9 所示：

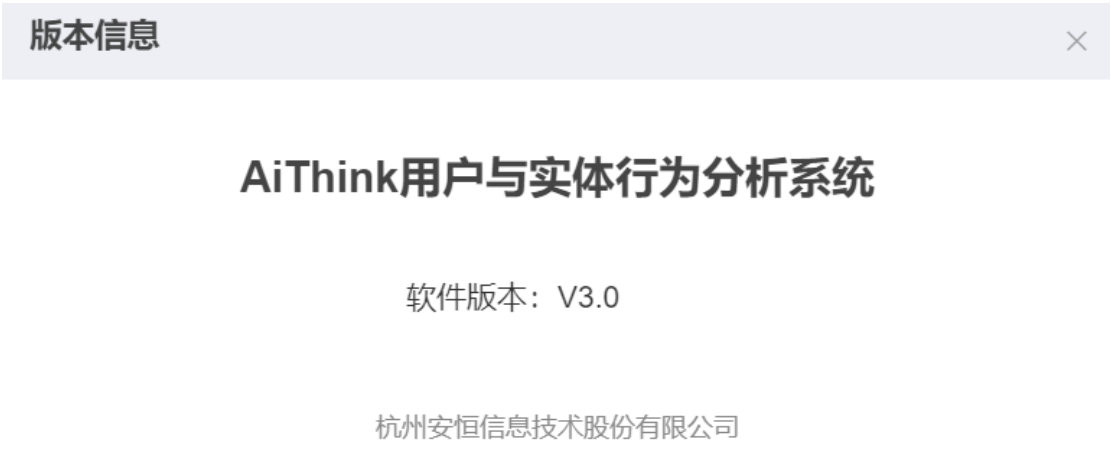



图 9 关于