✅ 6. 赤兔数据资产测绘与管理系统 v1.6 使用手册

文档说明

本文档为赤兔数据资产测绘与管理系统使用手册。适用于赤兔v1.6版本。

1. 产品简介

1.1 产品概述

赤兔数据资产测绘与管理系统（以下简称：赤兔），是一款基于数据分类分级规则，对终端、数据库等进行数据资产扫描、盘点、测绘、安全检查的数据安全产品。

赤兔针对终端数据资产通过内置敏感数据识别算法，智能识别终端敏感数据内容；针对企业内网数据库、大数据平台等数据资产通过智能数据识别引擎，进而实现智能、自动化探测，完成对数据资产进行采集和梳理；通过内置丰富行业策略库以及算法识别模型，在确保识别准确率的前提下，帮助企业数据分类分级建设，规范企业核心数据资产合规合理使用；根据数据分析处理结果，最终形成数据资产清单、绘制数据资产地图，不仅可用于监管单位对下级单位的数据合规检查，亦可助力企业达成对数据资产的盘点和风险自查的目标。

1.2 应用场景

1.2.1 数据安全合规

赤兔数据资产测绘与管理系统能够帮助需要满足数据安全合规的单位和企业，按照标准要求提供对应条例的审计信息，确保企业终端数据安全审计的合规性。

1.2.2 数据资产分析

赤兔数据资产测绘与管理系统内置敏感数据识别算法，智能识别终端敏感数据内容；针对企业内网数据库、大数据平台等数据资产通过智能数据识别引擎，进而实现智能、自动化探测，完成对数据资产进行采集和梳理。

1.3 产品功能

- **风险大盘**

风险大盘会呈现管控终端、资产概况、终端安全事件等数据，将系统当前使用情况可视化，便于管理员掌握系统整体运行状态。

- **数据资产**

数据资产模块将为管理员提供以数据为第一视角的数据资产管理功能，包括分类分级、资产识别、资产地图、流转分析，便于管理员掌握企业内部数据资产整体情况。

- **策略中心**

策略中心可协助管理员对数据泄露风险进行灵活管控，支持告警、截图取证、上传固证、配置水印、白名单、自定义渠道等功能，以实现精准的数据泄露监控或拦截。

- **终端管理**

终端管理帮助管理员对已安装赤兔的终端进行盘点与管理，支持赤兔客户端远程升级及终端相关配置修改。

- **用户管理**

用户管理包含员工列表和系统用户管理，可对企业内部不同组织架构的员工及系统内创建账户进行管理。

- **系统管理**

系统管理为用户提供后台的告警通知、运行监控、权限管理、操作日志等功能。

2. 操作指南

2.1 🆕 风险大盘

风险大盘下的风险总览将实时展示包括CPU利用率、内存使用率等数据在内的**系统性能统计**，管控终端、资产数据、风险数据等**核心指标**，并提供终端安装、创建扫描、创建策略、分类分级等常用功能的**快速入口**，无需跳转多个页面即可掌握系统整体运行状况。

登录赤兔数据资产测绘与管理系统后台，在左侧导航栏中，单击「风险大盘」，再点击「风险总览」，进入风险总览页。风险总览界面提供安全总览信息和相关处理操作，各模块功能说明如下：

2.1.1 快速入口

快速入口中汇集了高频功能的入口，点击按钮可以快速进入对应页面，包括：

- **终端安装**：快速进入终端管理-终端升级-安装包下载页面。
- **创建扫描**：快速进入策略中心-资产发现页面，并打开资产扫描任务创建弹窗。

- **创建策略**：快速进入策略中心-风险防控页面，并打开新增策略弹窗。
- **分类分级**：快速进入数据资产-分类分级页面。
- **风险分析**：快速进入风险分析-风险日志页面。
- **资产地图**：快速进入数据资产-资产地图页面。

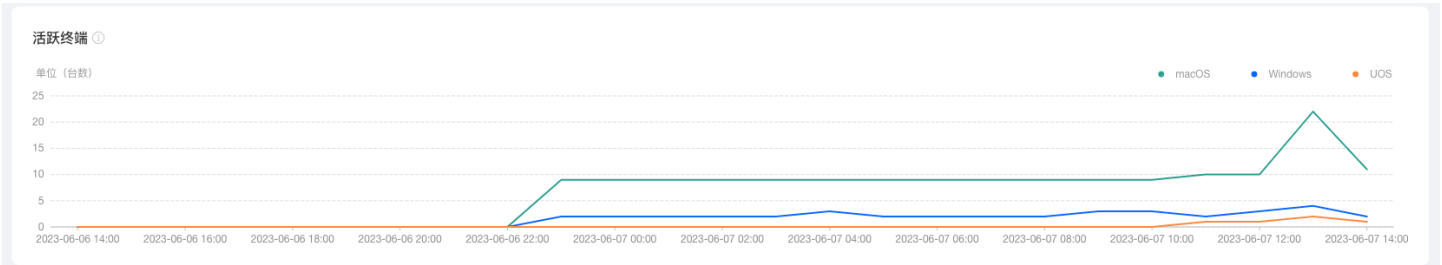
2.1.2 系统性能

在性能指标中，展示了系统性能的重要指标，包括：

- **CPU利用率**：利用率和核心数
- **内存使用率**：使用率和内存大小
- **磁盘占用**：已使用磁盘和磁盘总量
- **入带宽**：入带宽的大小
- **出带宽**：出带宽的大小

2.1.3 活跃终端

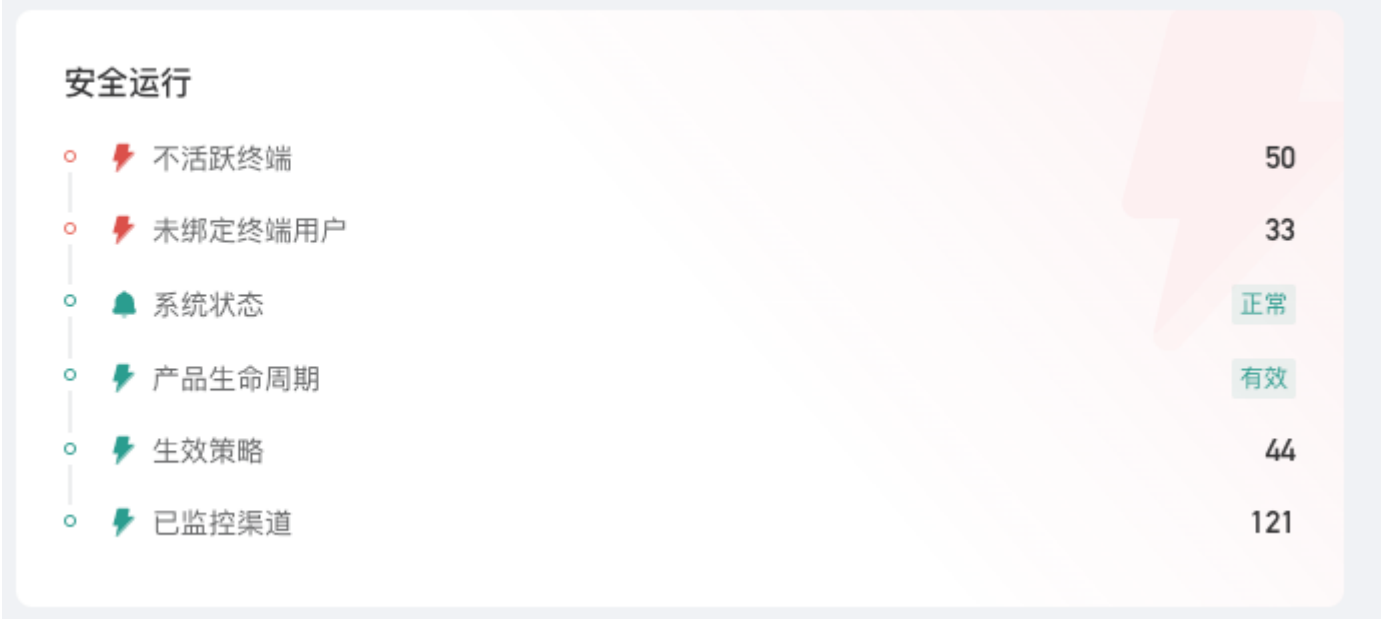
统计近24小时在线状态的终端数量，分别显示不同操作系统的活跃终端数量。



2.1.4 安全运行

安全运行监控将显示赤兔数据资产测绘与管理系统的安全运行告警信息，包括：

- 不活跃终端数
- 未绑定终端用户数
- 系统状态
- 产品生命周期
- 生效策略数
- 已监控渠道数

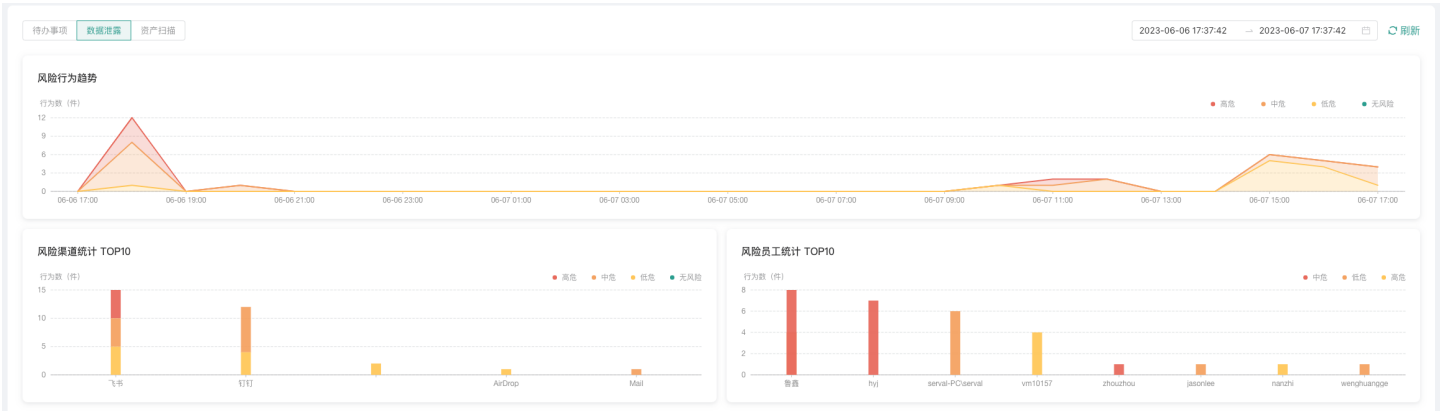


2.1.5 多模块数据

多模块数据将显示待办事项，数据泄露，资产扫描的统计数据：

- 待办事项：风险处理率（包括高危、中危、低危三个等级的风险的处理情况）、任务审批率（包括渠道管控、网络管控、进程管控的审批任务处理情况）

- 数据泄露：风险行为趋势（风险行为事件基于时间维度的数量统计）、风险渠道统计 TOP10（依据风险渠道相关的行为数量产生的排序统计）、风险员工统计 TOP10（依据员工产生的风险行为数量产生的排序统计）



- 资产扫描：资产发现（资产发现任务的完成情况）、命中分类分级 TOP5（不同分类、分级数据的命中情况统计）

2.1.6 面包屑顶部

将实时显示系统状态，点击「查看详情」即可查看系统不同模块的启用/关闭状态。

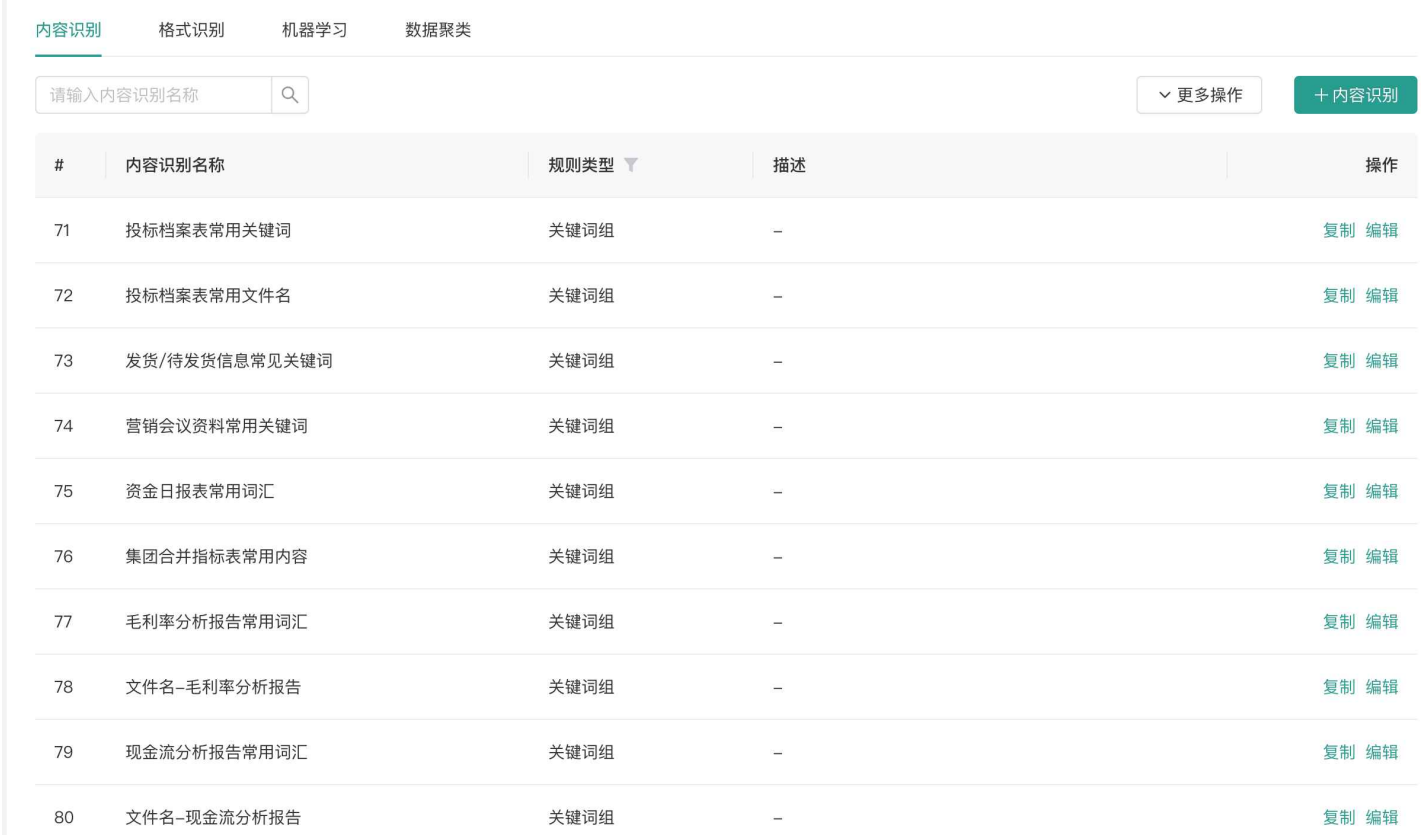
2.2 数据资产

2.2.1 识别管理

识别管理包括内容识别、格式识别、机器学习、数据聚类。其识别条件作为最小原子化能力，基于此，管理员可进一步配置数据分类分级和管控策略，最终将结果下发至终端执行。

2.2.1.1 内容识别

内容识别包含系统内置的300余条常用敏感词条。



除此之外，用户可以自行添加内容识别规则。点击右上角「内容识别」，填写内容识别名称、识别描述，选择合适的规则类型（支持关键词组、正则匹配、关键词对三种类型）即可添加内容识别规则。

关键词组：管理员可输入关键词语，实现对敏感词的规则识别

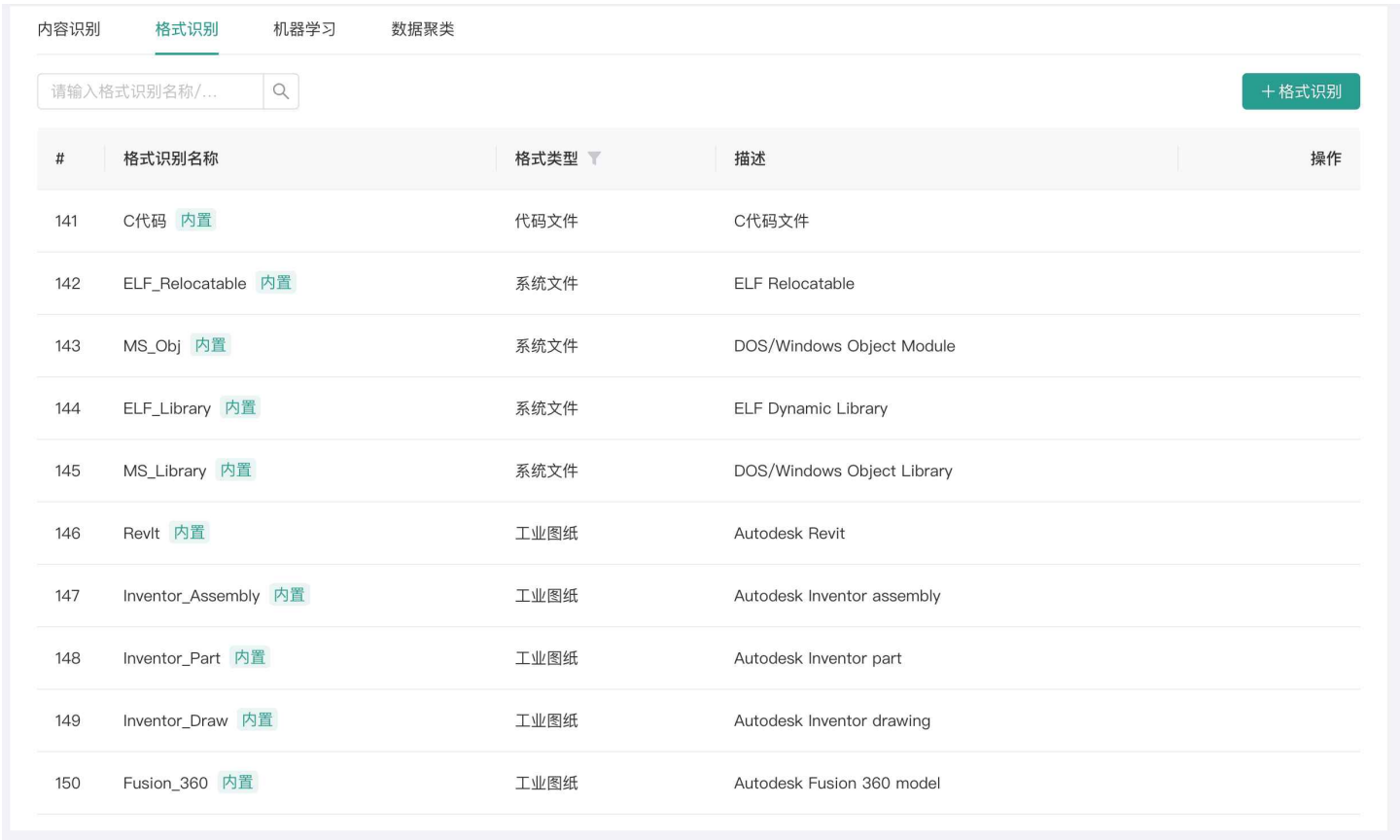
正则匹配：支持管理员输入正则信息，实现对敏感词的规则识别

关键词对：支持输入关键词及间隔信息。如：关键词1:中华 关键词2:国 间隔字符：4 ，则形如中华XXXX国的敏感词将会命中规则

点击「更多操作」，可以导入/导出内容识别规则。请注意，批量导入内容识别规则时，需先选择「导出模板」，按照内容填写完成后上传。

2.2.1.2 格式识别

赤兔具备对数据进行真实文件格式识别的能力，系统内置引擎支持数百种常用文件格式，同时支持管理员自定义添加文件格式。



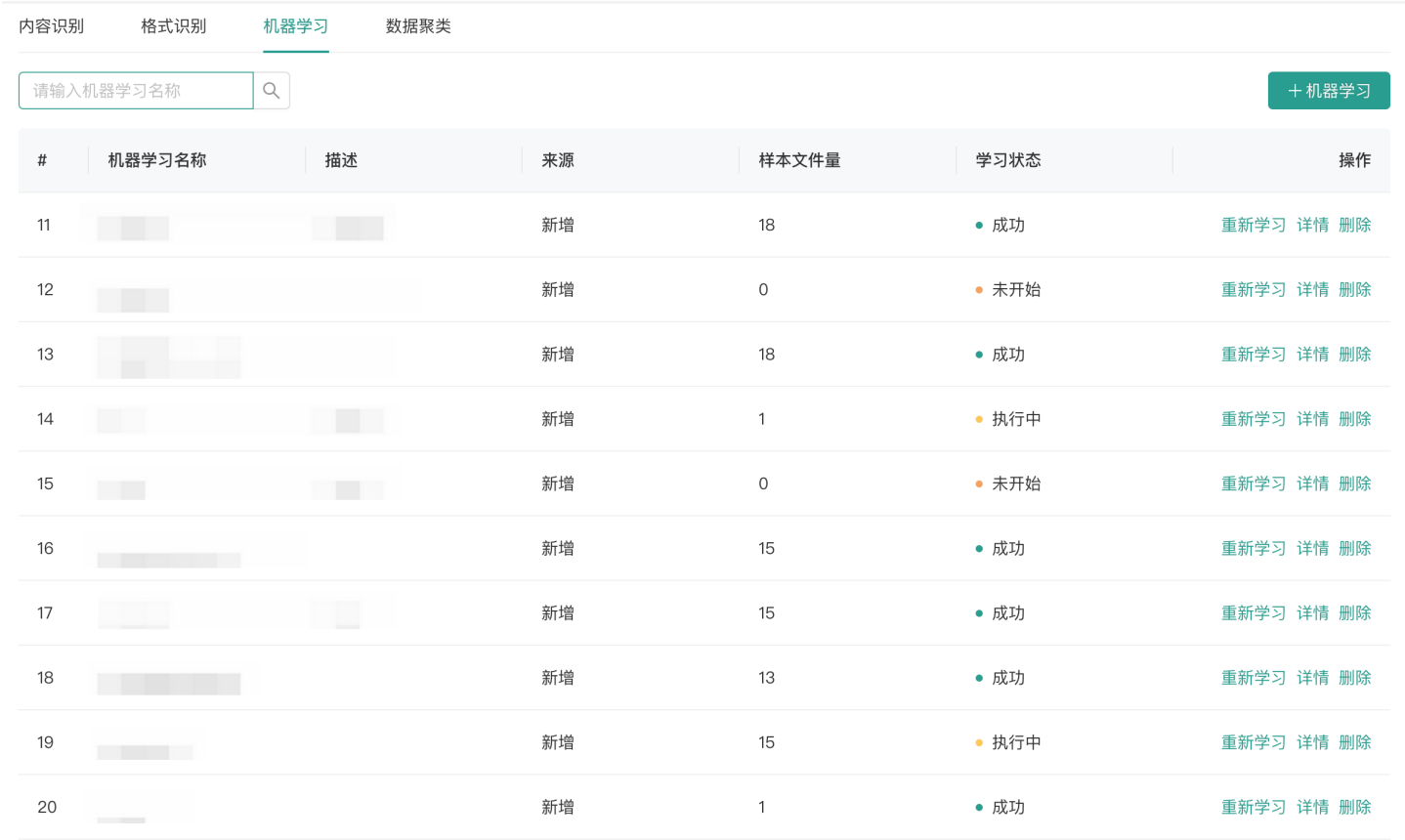
#	格式识别名称	格式类型	描述	操作
141	C代码 内置	代码文件	C代码文件	
142	ELF_Relocatable 内置	系统文件	ELF Relocatable	
143	MS_Obj 内置	系统文件	DOS/Windows Object Module	
144	ELF_Library 内置	系统文件	ELF Dynamic Library	
145	MS_Library 内置	系统文件	DOS/Windows Object Library	
146	Revit 内置	工业图纸	Autodesk Revit	
147	Inventor_Assembly 内置	工业图纸	Autodesk Inventor assembly	
148	Inventor_Part 内置	工业图纸	Autodesk Inventor part	
149	Inventor_Draw 内置	工业图纸	Autodesk Inventor drawing	
150	Fusion_360 内置	工业图纸	Autodesk Fusion 360 model	

- **新增格式识别**

点击右上角「+ 格式识别」，输入格式名称、格式描述、选择格式类型及文件后缀信息后保存。添加完成后，可在数据分类分级中进行查看和引用。

2.2.1.3 🆕 机器学习

赤兔可以通过管理员上传文件样本的方式进行机器学习、计算文件特征，进而帮助管理员提取样本信息，训练生成新的机器学习规则。



- **新建机器学习**

点击右上角「+ 机器学习」，输入基本信息后上传样本文件，保存后即可进行机器学习。需要注意的是：目前已支持doc、docx、xls、xlsx、xlsb、csv、pdf、ppt、pptx、txt、html、htm等文本格式进行机器学习以进行特征提取。

- **详情 & 重新学习**

学习完成后，点击列表中的「详情」按钮，即可查看学习结果的详情，同时也支持重新上传文件再次学习。此外，可根据需要，切换样本文件的内容展示方式，如词云或表格（包含关键词的特征权重）。列表中MD5值右侧的图标支持点击跳转至资产地图，进一步查看此文件的归属信息等内容。

对于未被引用的机器学习，可以直接在列表页中删除；若该机器学习已被引用，需要先删除相应的分类信息，再进行删除。

2.2.1.4 数据聚类

当一批文件的分类和特征未知时，管理员可以使用数据聚类的功能，先对其进行数据聚类，然后再数据归类，并生成相应的识别规则。

1. 首先进行数据聚类设置：上传一批样本文件，根据预期调节文件相似度，操作完成后，点击开始聚类；

2. 左侧栏显示聚类结果的大类信息，此功能会将文件相似度高的文件分成若干个大类，右侧则展示具体分类下的文件，管理员可通过词云/表格按钮进行切换，进而掌握文件中的关键词；

1. 点击右侧「数据归类」，可以在文件聚类结果的基础上，截取关键词信息并将之分类至「新建机器学习」或「归为已有学习」。

2.2.2 分类分级

数据分类分级为企业核心的数据安全运营手段之一。赤兔内置通用的分类分级模板，并支持通过数据分类、数据分级两种视角，切换查看分类分级情况。

2.2.2.1 初始化

初次进入数据分类分级页面，可选择「手动添加」「方案库选择」「导入方案包」三种模式。

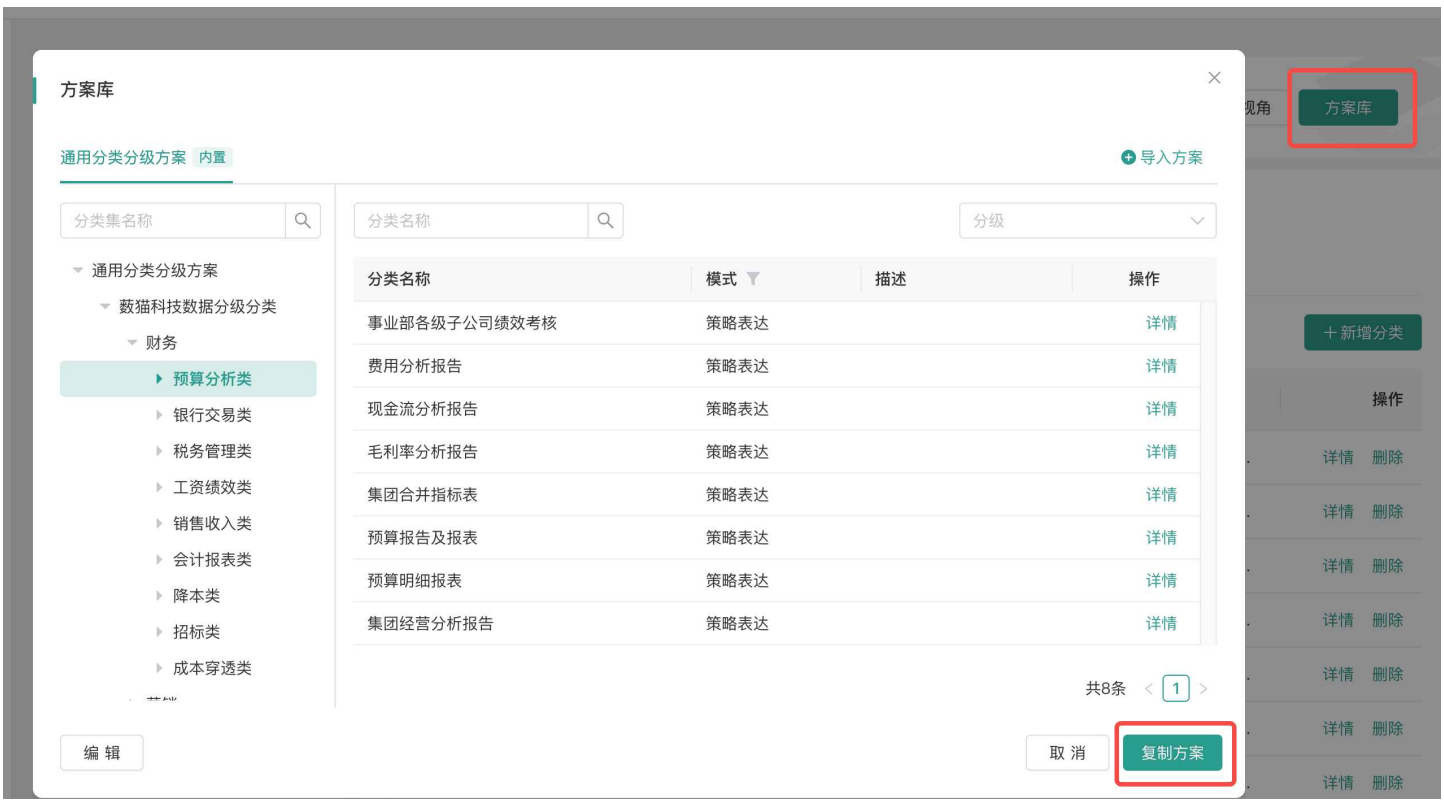
- 手动添加：管理员可通过手动的方式添加分类集、分类等信息。
- 方案库选择：管理员可从方案库中选择相应的方案进行复制，并添加为分类分级。
- 导入方案包：管理员可以将数据分类分级方案包/薮猫科技工程师提供的方案包导入至方案库中。

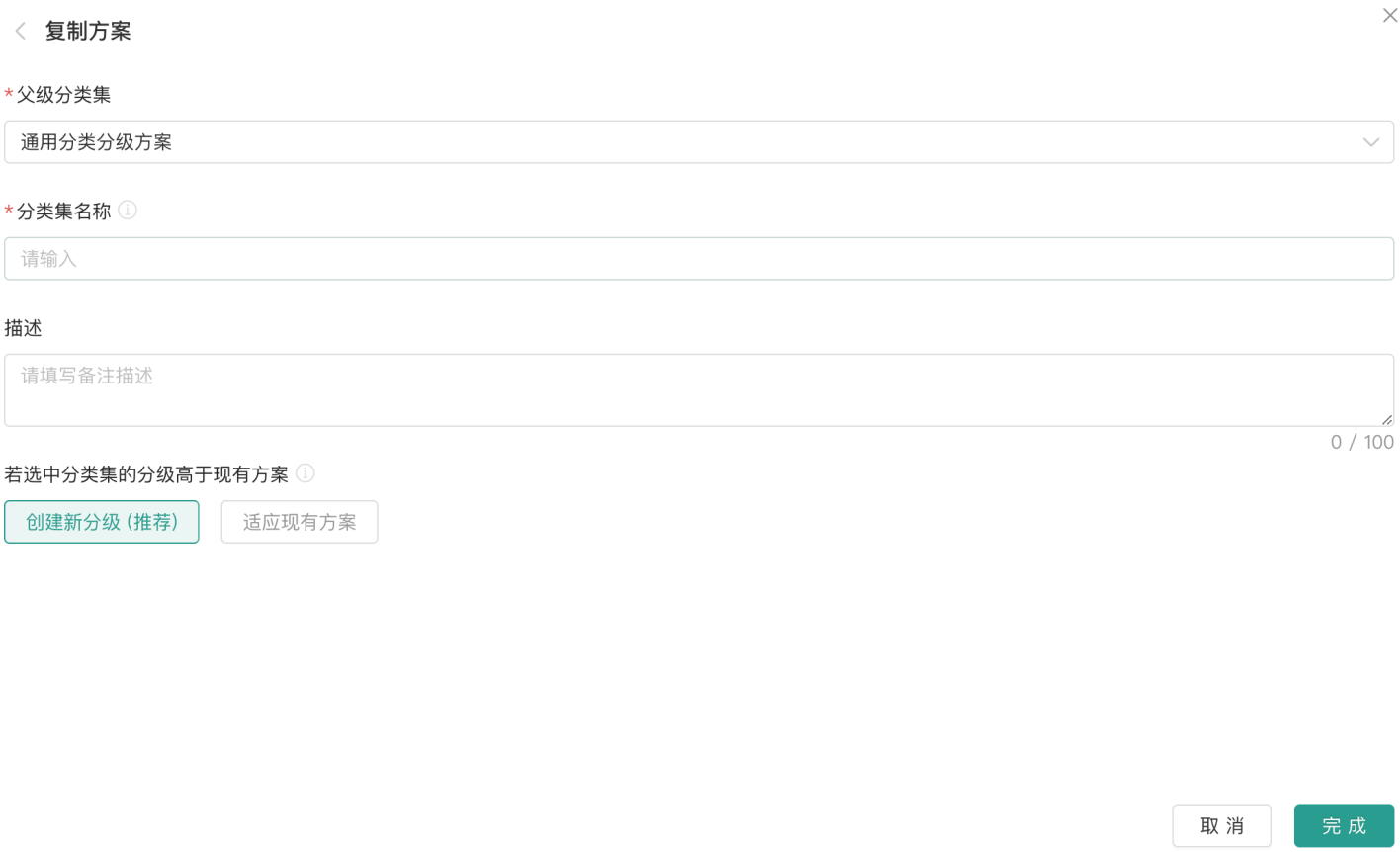
2.2.2.2 方案库

方案库中内置各行各业的分类分级方案，通过快速复制，可帮助管理员高效开展分类分级工作。同时支持管理员自定义方案导入，进一步丰富方案库。

- **复制方案**

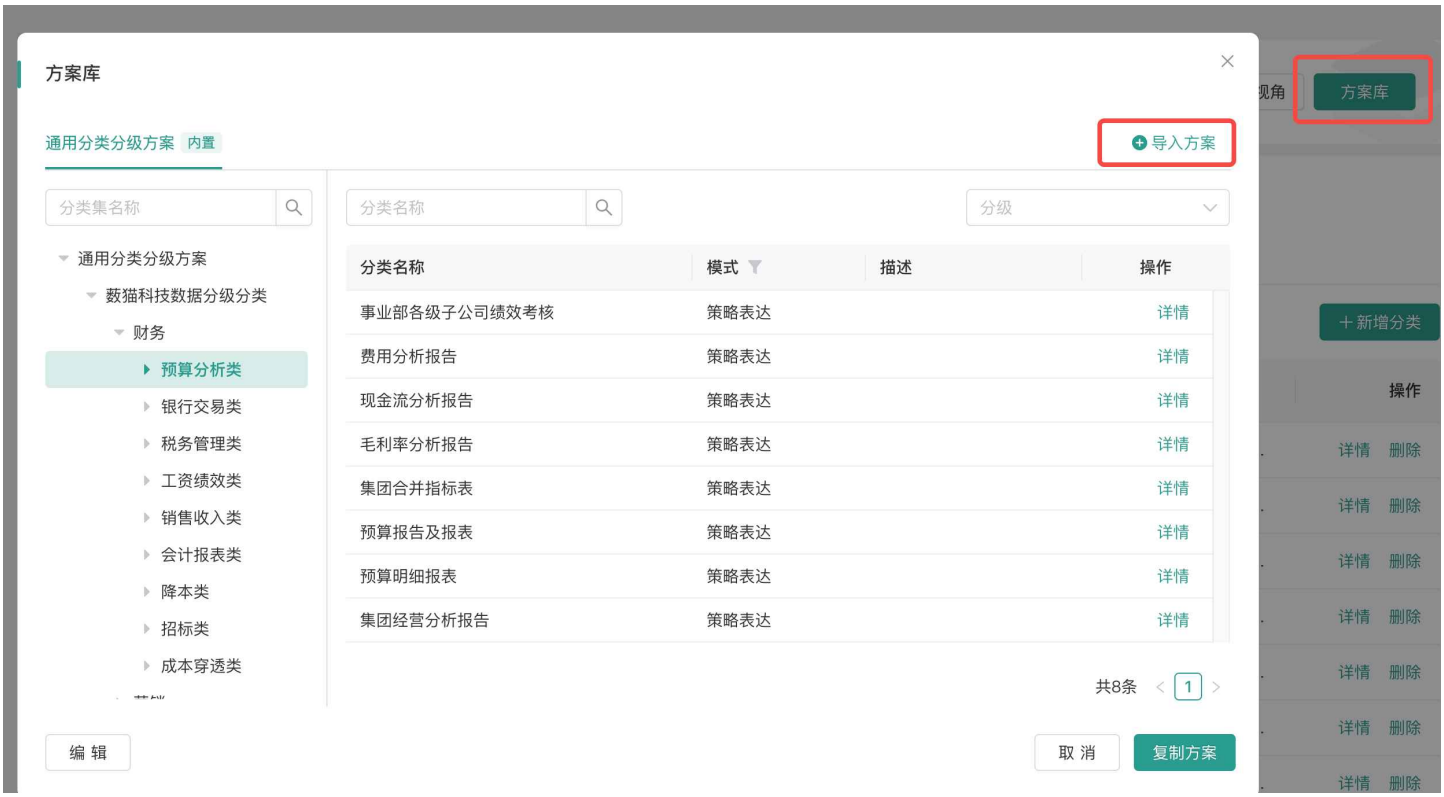
点击「方案库」-「复制方案」，选择需要放置的父级分类集、输入分类集名称以及其它相关配置，点击完成，即可完成方案配置。

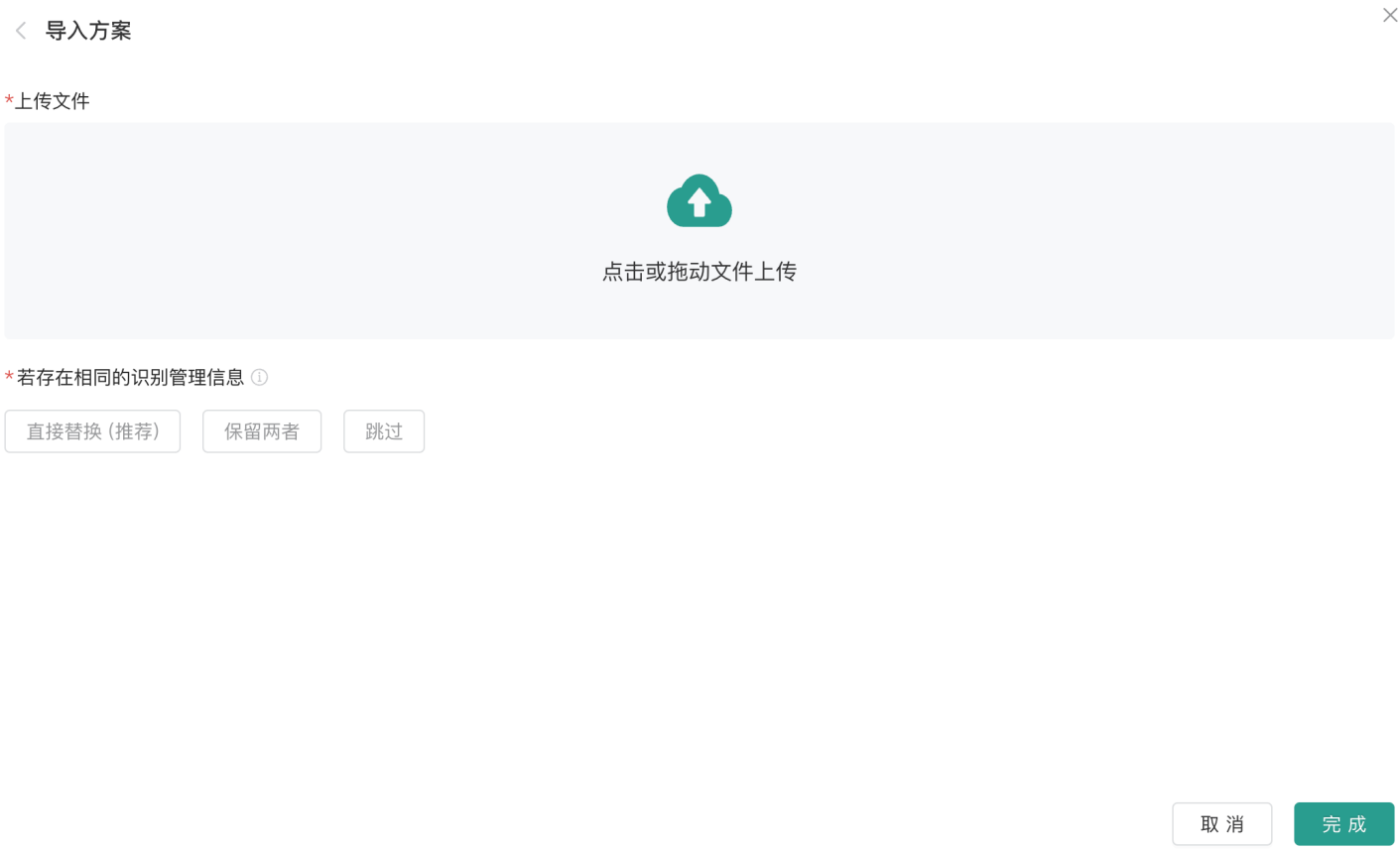




- **导入方案**

点击「方案库」-「导入方案」，导入数据方案包，配置相关信息，点击完成即可新增一种数据分类分级方案。



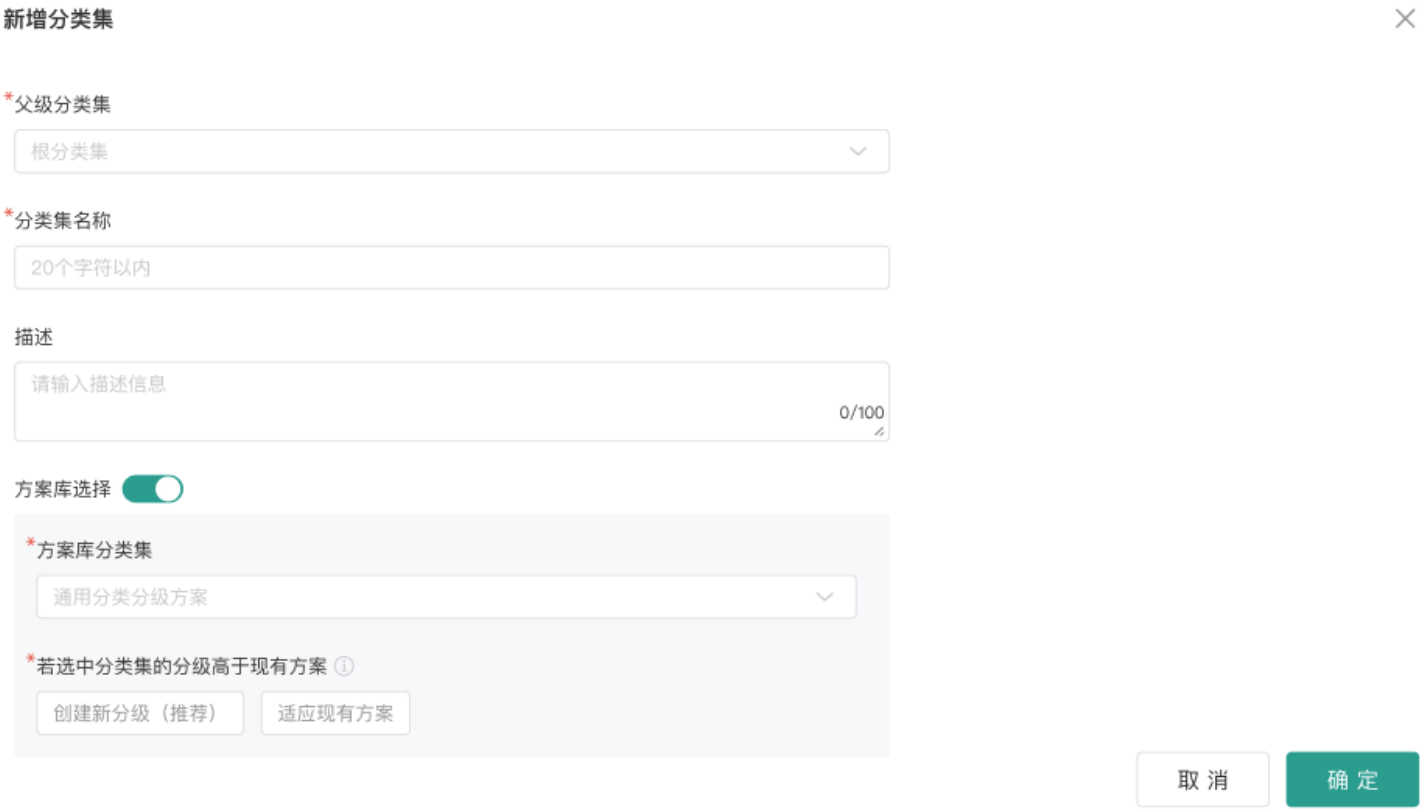


2.2.2.3 数据分类

管理员可在本页面进行新增分类、编辑分类、删除分类、添加分类子集、添加数据分类识别规则等操作。

- **新增分类集**

在分类分级页面，单击「新增分类集」，可在弹窗页面中添加分类集，或直接从方案库中选择分类集。支持创建多层分类集，用于满足不同的数据分类分级设置。



- **数据分类**

1. 点击「新增分类」，即可在新页面中创建新数据分类。管理员可选择自行添加或直接从方案库中进行添加。

2. 在策略配置中可以选择策略表达或智能学习模式，这两种模式分别对应不同数据识别策略。

   - **策略表达**

1）进行扫描位置的选择，可添加多个扫描位置（包括：文件名、首行文字、页眉页脚、文件类型、文件内容）；

2）填写匹配操作符，包括至少命中N次、每项都至少命中N次、至少能够命中M项、至少一项命中N次等多种操作符。

{

语句解析

至少命中N次：即该敏感词条包含的敏感词无论重复至少需要命中x次，：

敏感词一包括（a,b,c,d,e,f,g,）：

每项都至少命中N次：即该敏感词条包含的全部敏感词至少每个都要命中N次；

至少能够命中M项：即该敏感词条在不重复的情况下，至少命中词条中的M项；

至少一项命中N次：即该敏感词条中，至少有一个关键词可以命中N次，才为命中。

举例：

词条A内的敏感词为：（a,b,c,）

A至少命中3次：命中情况为：1)abc ;2)aaa;3)aab;以上类似情况都可以；

A每项都至少命中3次：命中情况为：aaabbbccc；

A至少能够命中3项：命中情况为：abc；

A至少一项命中3次：命中情况为：aaabc；

}

3）填写右变量：可在右变量中选择数据识别名称或数据识别的详情信息，并支持通过高级搜索的方式，快速新增识别规则/关键词。

4）策略配置逻辑关系：可以形成简单的逻辑组合如：A and B/A or B；也可以添加任意的条件组，形成所需的逻辑关系，如：A and（B or（C and D））。

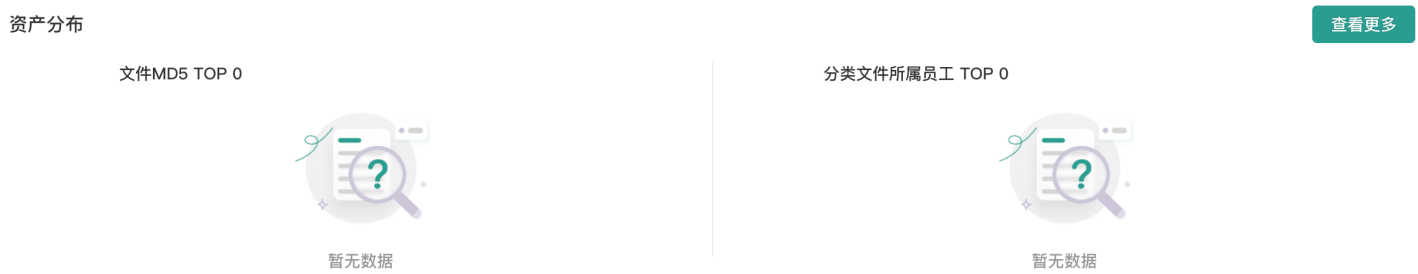
完成以上步骤即可完成数据分类的配置，数据分类可直接在风险策略、资产发现中引用。

- **智能学习**

  点击智能学习，选择文件特征后，对文件相似度（0～100%）进行调节，点击完成即可创建成功。

  需要注意的是：智能学习属于异步识别策略，无法配合风险防控策略中的阻断、警告弹窗等处置动作。

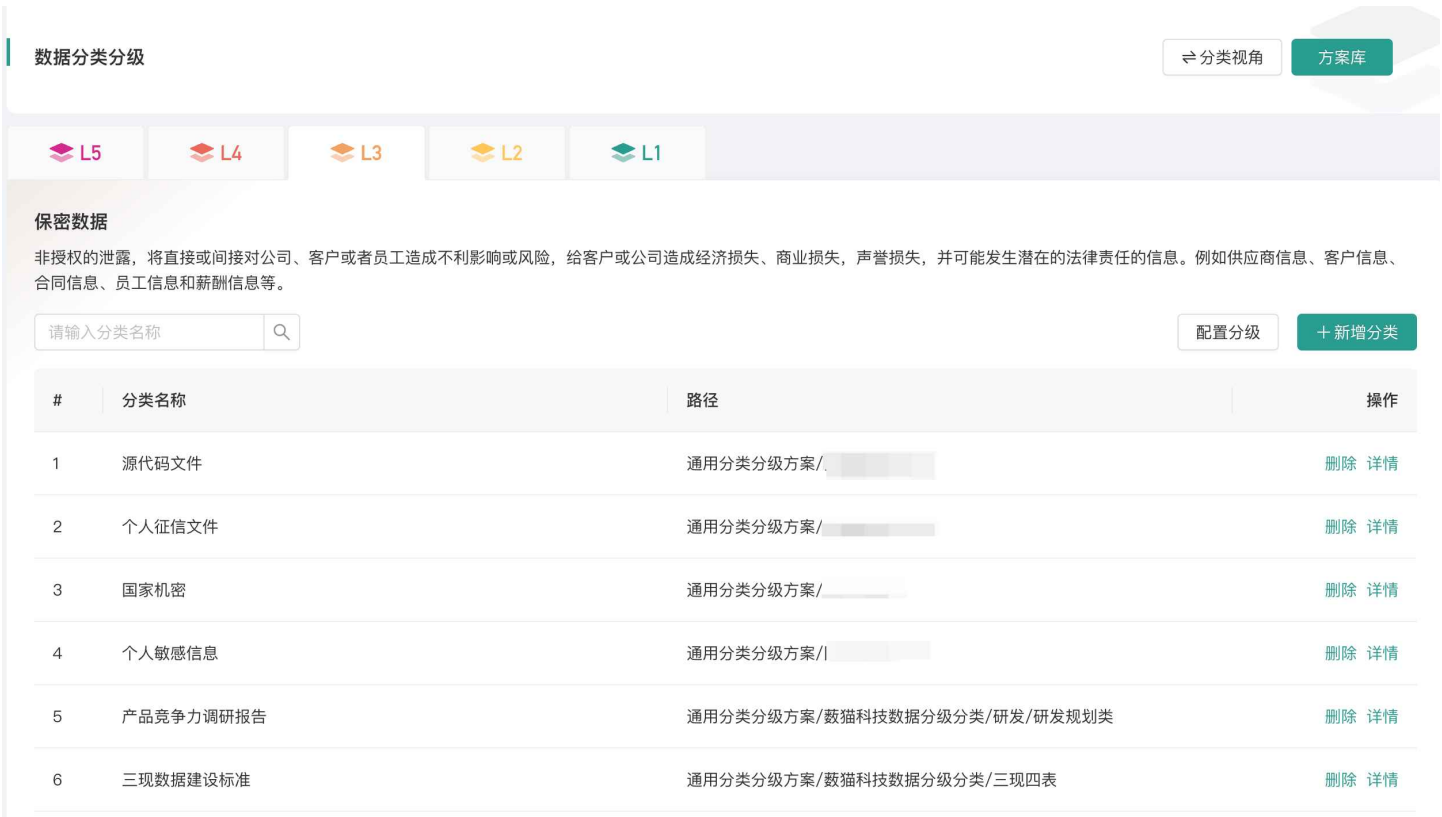
3. 查看分类： 在数据分类的列表页中，点击详情即可查看分类的信息，包括此分类相关的策略配置、血缘信息、资产分布等。



点击编辑按钮，可在页面右上角编辑数据分类信息

2.2.2.4 数据分级

1. 点击数据分类分级页面右上角「分级视角」，即可切换至分级视角页面。

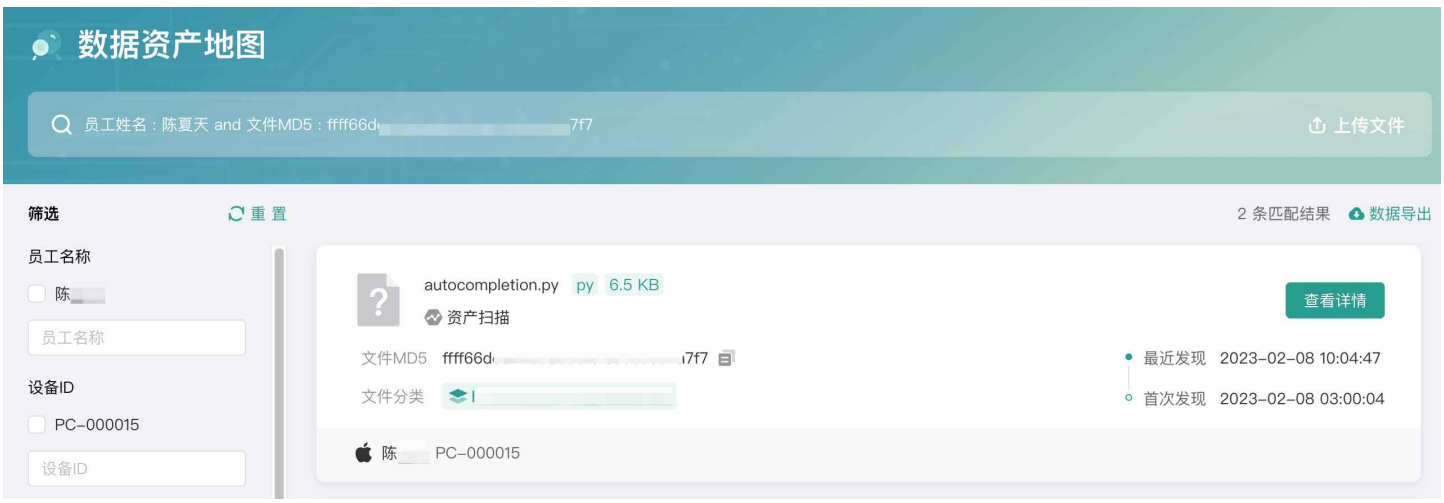


2. 点击「配置分级」按钮，可修改/删除/增加分级信息。产品默认内置4类分级，只能对未被任何分类引用的分级进行删除处理，且只能从高至低删除分级。

2.2.3 资产地图

数据资产地图为管理员展示办公网内的数据资产信息。同时，管理员可通过搜索文件的MD5值/分类名/分类等级/设备ID/员工姓名等内容，找寻相对应的数据资产。

如：查询某一员工设备上的的某一文件信息



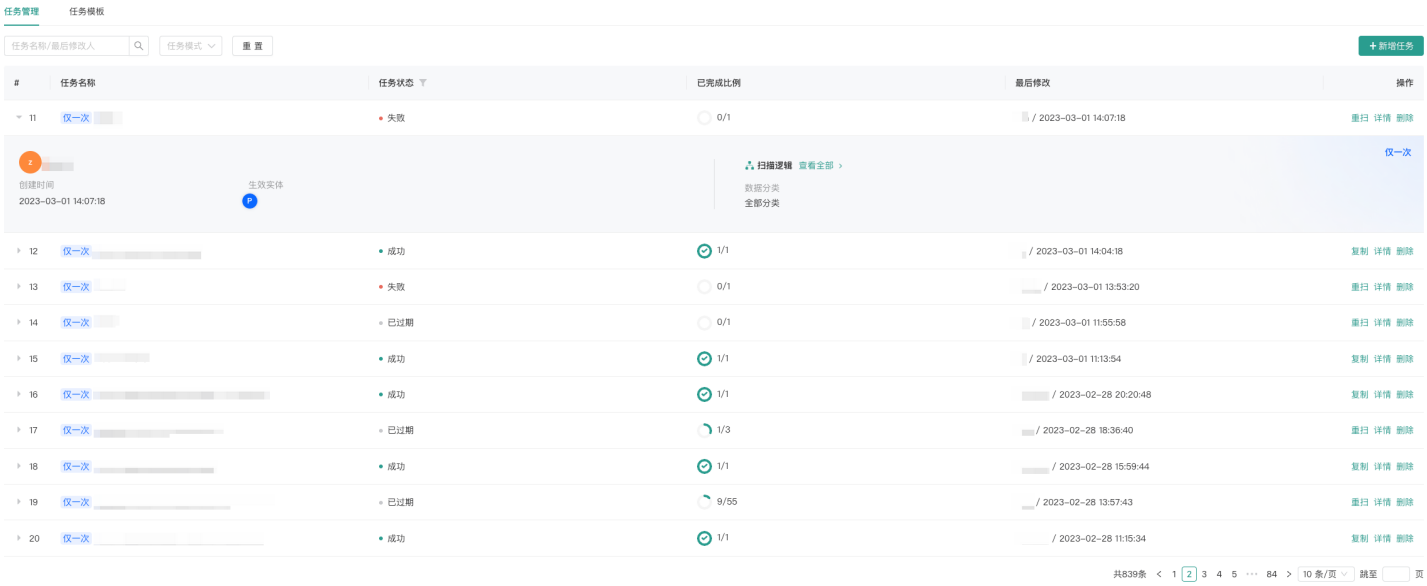
2.3 策略中心

2.3.1 资产发现

资产发现功能有助于帮助管理员摸清办公网终端数据资产的情况，通过扫描任务快速掌握办公终端中存储的数据资产分布情况。功能列表将会展示任务的相关信息、扫描逻辑等。

2.3.1.1 任务管理

1. 在左侧导航栏中，选择「策略中心」-「资产发现」，进入数据资产管理页面，页面布局如图所示。

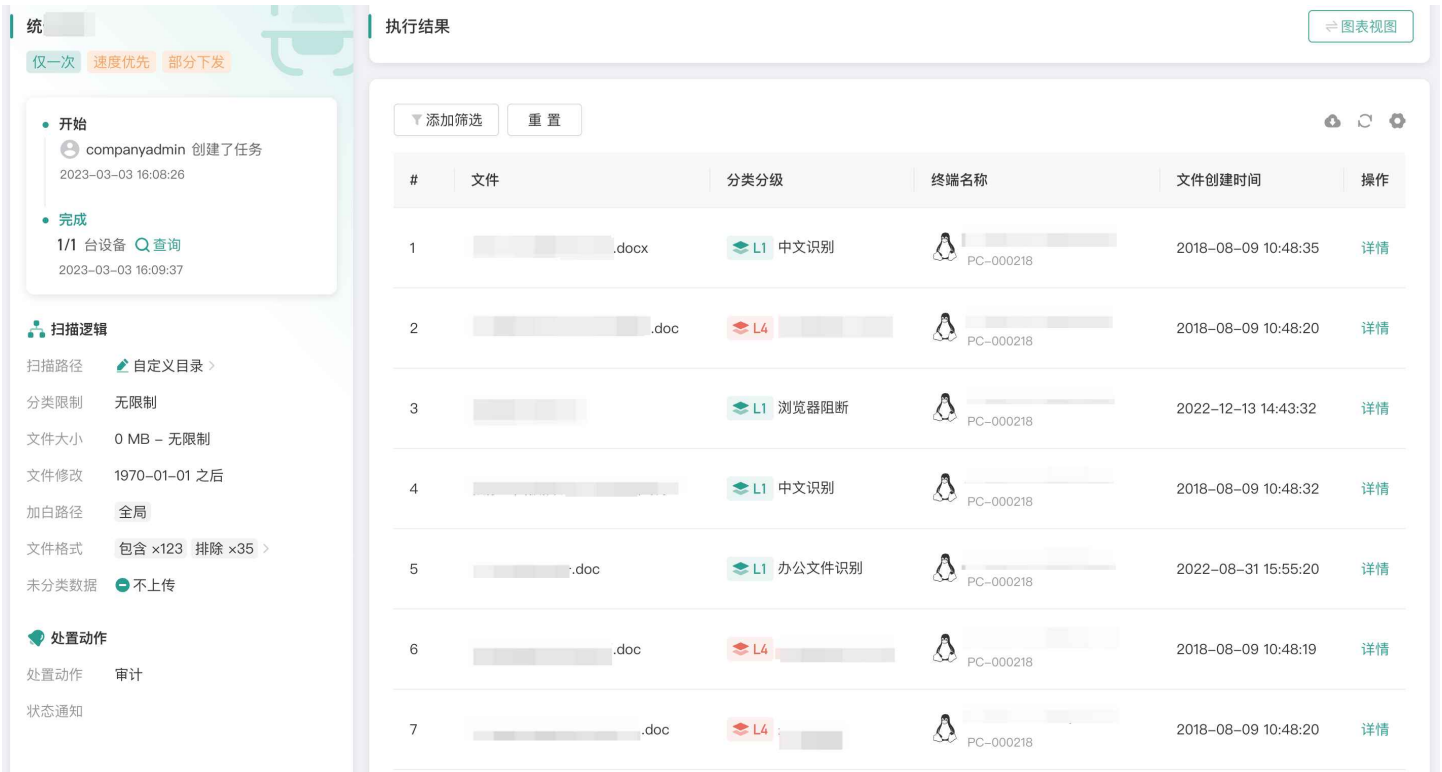


2. 点击右上角「新增任务」，进入到添加终端资产扫描任务界面。用户可以直接从模板添加任务，也可以新建任务。

3. 进入空白任务界面，在页面填写任务基本信息、生效范围（包括生效时间、下发范围）、扫描逻辑（包括扫描路径、分类限制、以及高级选项中文件修改时间、加白路径、排除文件格式、对未分类数据处理信息）、处置动作之后，即可完成任务创建。

4. 对于已经创建完成的任务，用户可直接在资产发现列表中查看。
5. 对于已经完成的任务，用户可以在资产发现列表页面，选择某具体任务，点击「详情」查看该任务信息。

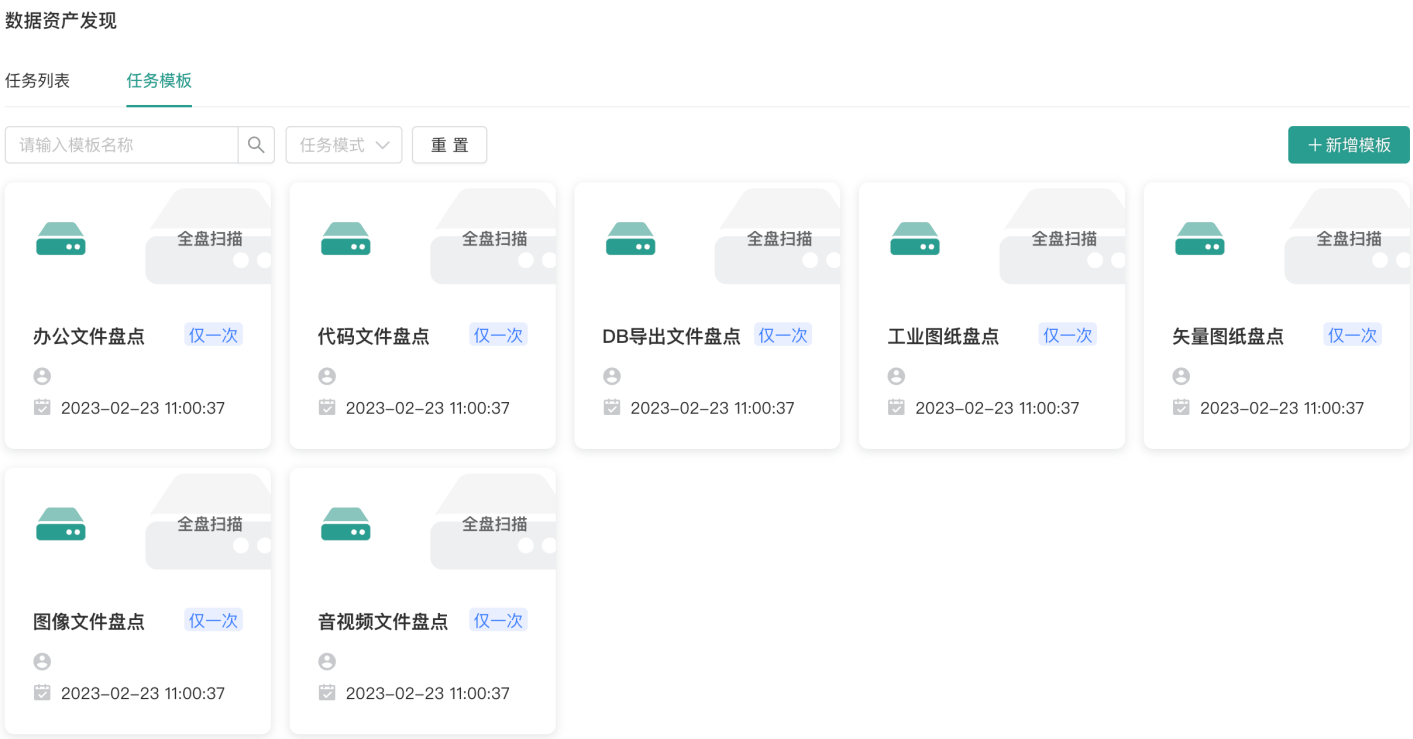
6. 点击页面右上角「列表视图」，可切换至列表展示。



7. 对于执行成功的任务，可以点击「复制」，再次进行任务下发；对于执行失败的任务，可以点击「重扫」，重新进行任务扫描；对于执行中的任务，可以点击「取消」，终止本次扫描任务。
8. 用户可在列表页面，点击操作栏中的「删除」，删除所选任务。

2.3.1.2 任务模板

1. 在左侧导航栏中，选择「策略中心」-「资产发现」，切换至「任务模板」，进入数据资产发现模板页面，页面布局如图所示。



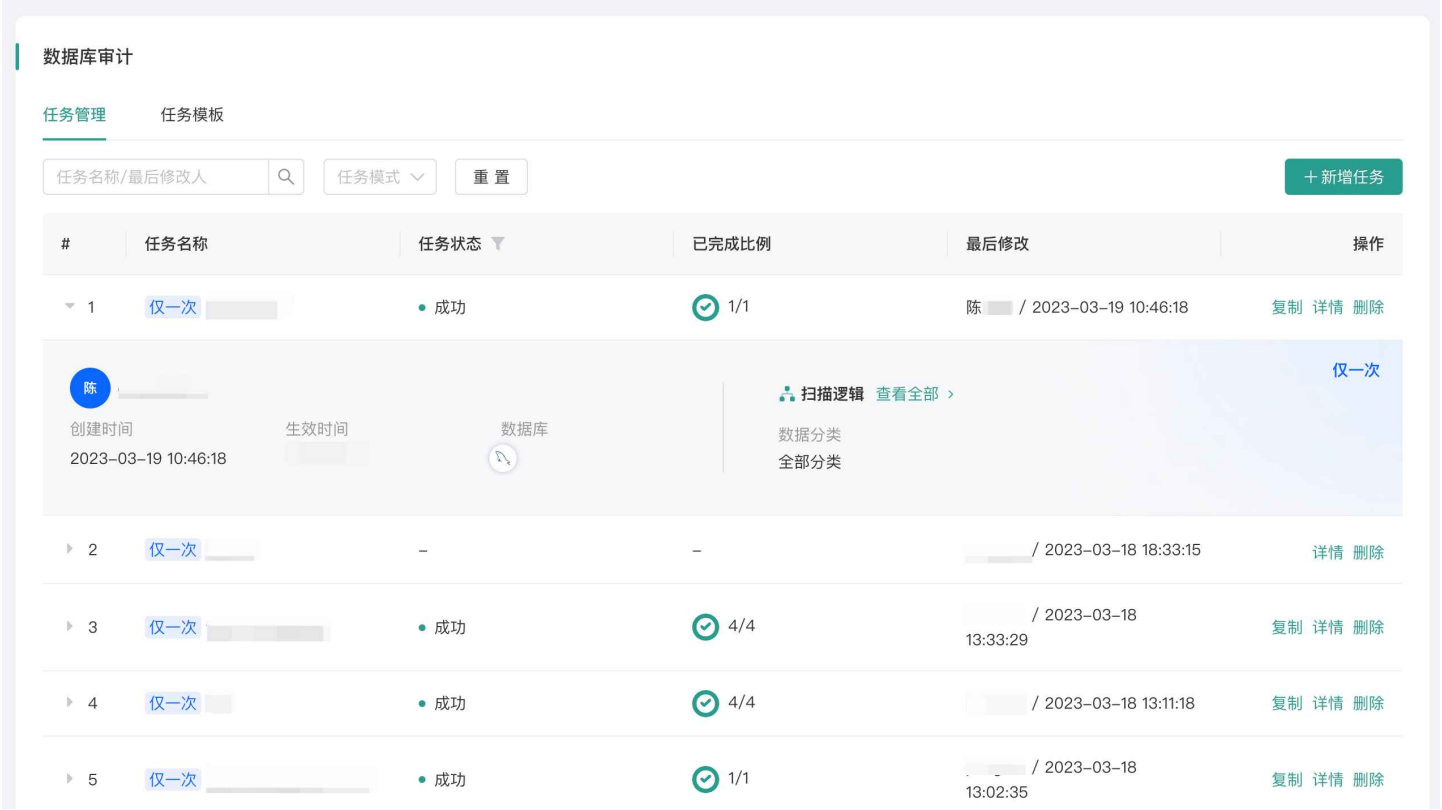
2. 用户可以查看内置模板，或者点击页面右上角「+ 新增模板」，新增资产发现模板。
3. 在弹出的内容页填写相关信息，点击保存即可完成创建。
4. 鼠标移动至模板，可对模板进行“转任务”“编辑”“删除”操作。用户可以根据需要编辑或者删除模板；也可以点击“转任务”直接将模板转为资产发现任务。

2.3.2 数据库审计

数据库审计功能有助于帮助管理员摸清数据库存储内容信息，管理员可以通过新增任务摸排相关内容。数据库审计的任务列表将会展示任务的相关信息、扫描逻辑等信息。

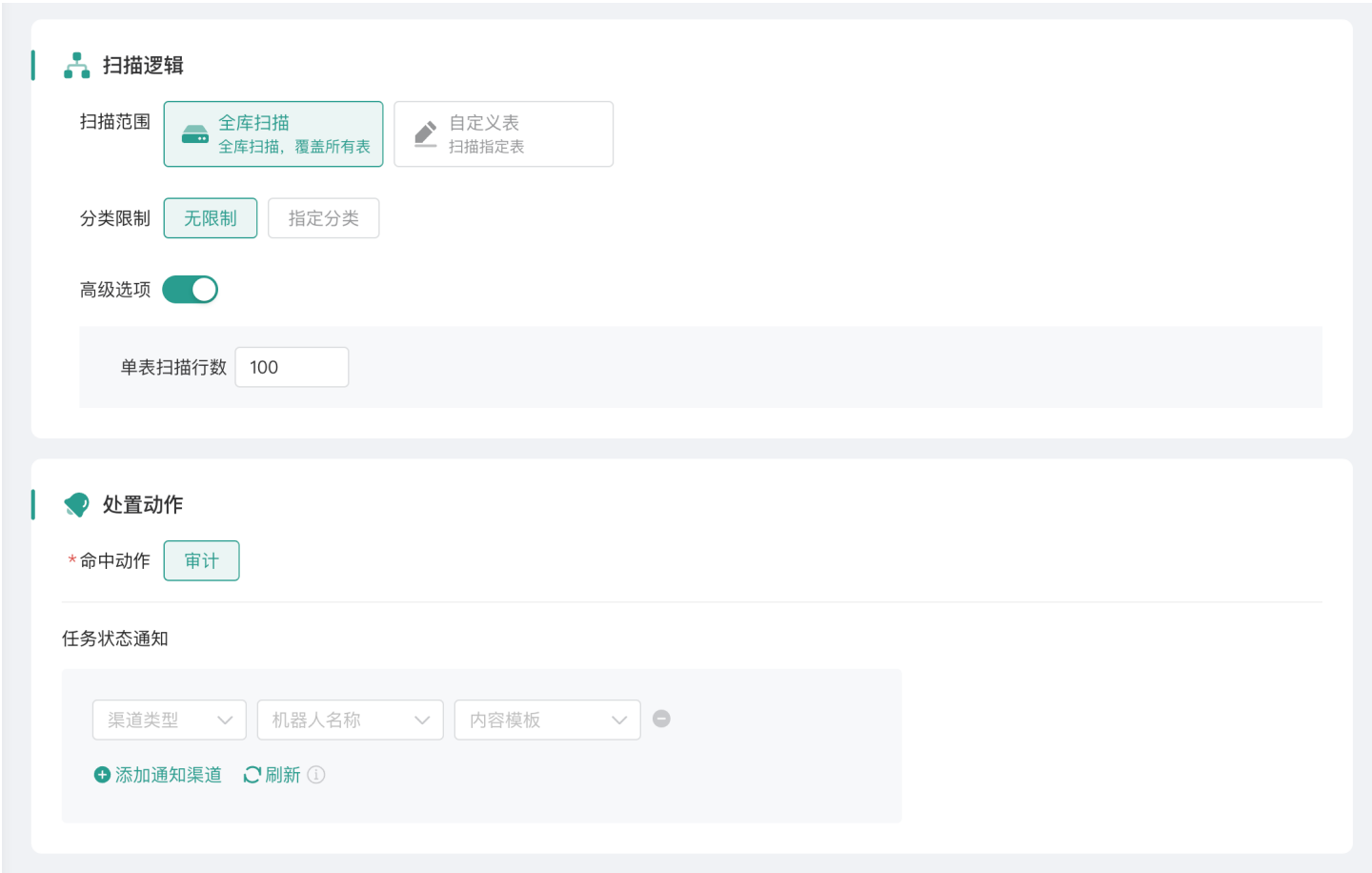
2.3.1.1 新增任务

1. 在左侧导航栏中，选择「策略中心」-「数据库审计」，进入数据库审计页面，页面布局如图所示。



2. 点击右上角「新增任务」，进入到添加终端资产扫描任务界面。用户可以直接从模板添加任务，也可以新增任务。

3. 进入空白任务界面，在页面填写任务基本信息、生效范围（包括生效时间、实体选择）扫描逻辑（包括扫描范围、分类限制、以及高级选项中单表扫描行数）、处置动作之后，即可完成任务创建。



4. 已经创建完成的任务，可直接在列表中查看。

2.3.1.2 查看任务

1. 对于已经完成的任务，用户可以在数据库审计列表页面，选择某具体任务，点击「详情」。即可查看任务信息。

2. 点击页面右上角「列表视图」，可切换至列表展示

3. 对于成功执行的任务，可以点击「复制」按钮，再次进行任务下发；对于执行失败的任务，可以点击「重扫」，重新进行任务扫描；对于执行中的任务，可以点击「取消」，停止本次任务的扫描

2.3.1.3 删除任务

用户可在列表页面，选择要删除的任务信息，点击操作栏中的「删除」按钮，将任务进行删除。

2.3.1.4 新增模板

1. 在左侧导航栏中，选择「策略中心」-「数据库审计」，切换至「任务模板」，进入数据资产发现模板页面。
2. 用户可以查看内置模板，或者点击页面右上角「+ 新增模板」，新增数据库审计模板。

3. 新增模板可以按照页面内容填写相应的信息，点击保存即可完成创建。
4. 鼠标移动至模板，可查看内容有“转任务”、“编辑”、“删除”信息。用户可以根据需要编辑或者删除模板；亦可以点击“转任务”直接将模板转为数据库审计任务。

2.3.3 远程取证

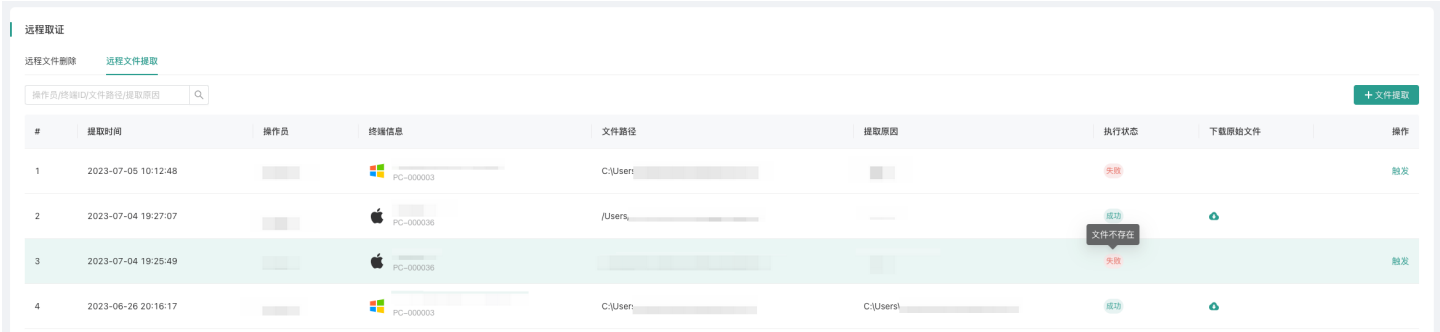
支持管理员远程对用户终端存在的敏感文件进行删除或提取。

2.3.3.1 🆕 远程文件删除

远程文件删除页面布局如图所示。用户可在本页面创建远程文件删除任务，并支持任务信息搜索。

在执行状态中展示当前任务的执行状态，鼠标悬浮在失败状态上时将展示失败原因。

点击触发按钮，云端将重新向终端下发任务；超级管理员可以删除任务列表中的任务。



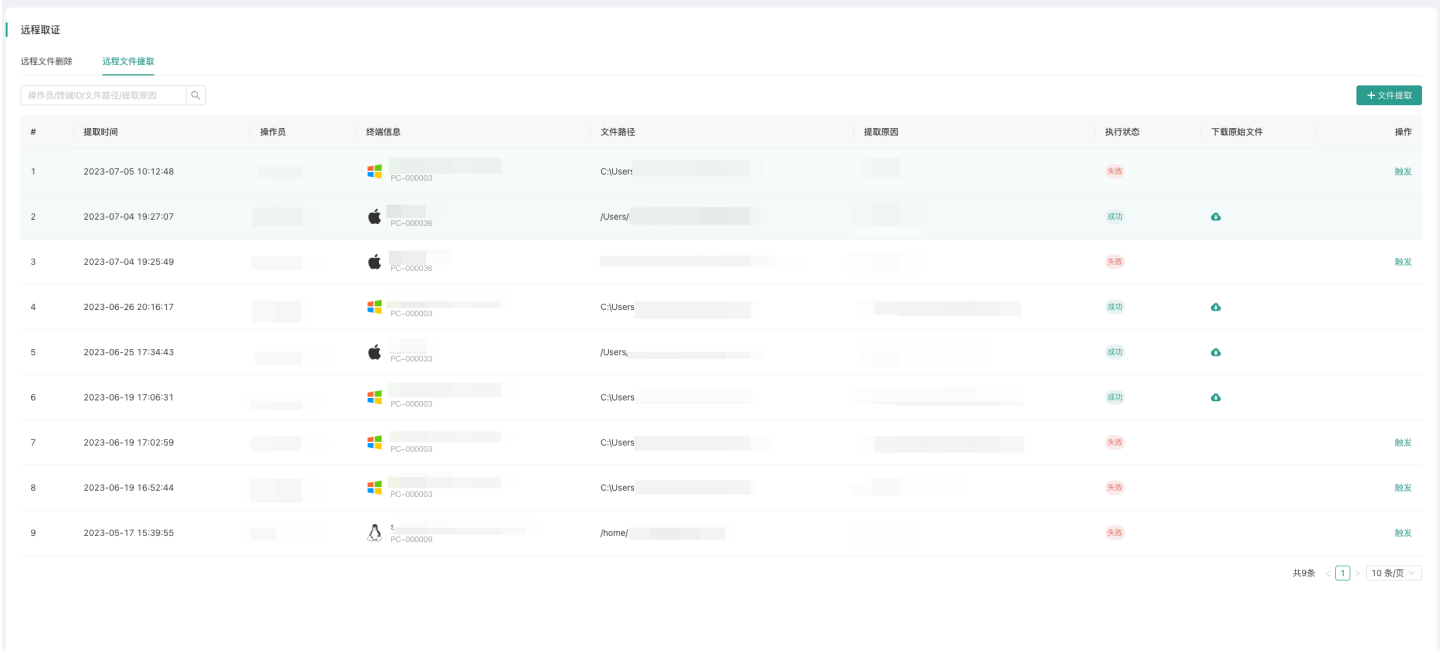
点击页面右侧「+文件删除」，填写相应信息，保存后即可新增远程删除任务。

2.3.3.2 🆕 远程文件提取

远程文件提取页面布局如图所示。用户可在本页面创建远程文件提取任务，并支持任务信息搜索。

在执行状态中展示当前任务的执行状态，鼠标悬浮在失败状态上时将展示失败原因。

点击触发按钮，云端将重新向终端下发任务；超级管理员可以删除任务列表中的任务。



点击页面右侧「+文件提取」按钮，在弹窗页新增提取任务

2.3.4 白名单管理

2.3.4.1 目录白名单

当某些终端部分目录下的文件不希望进行资产扫描时，可以通过添加目录白名单的方式来实现。

在目录白名单的页面，点击右上角「新增名单」，在弹窗中填写操作系统分类，目录地址等信息，即可完成目录白名单的新增。

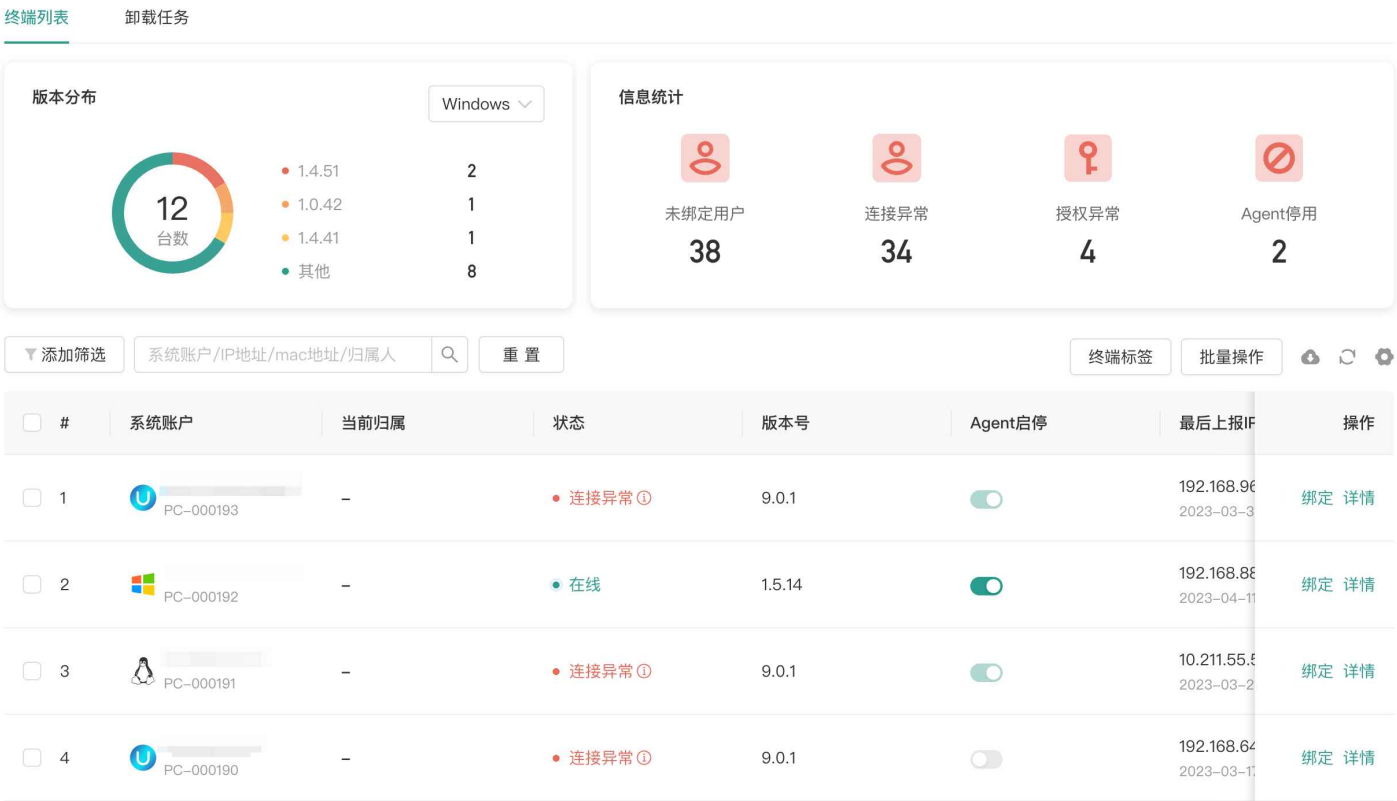
如有需要，可以点击每个操作系统右侧的清空列表，清除之前新增的白名单目录地址。

2.4 终端管理

2.4.1 终端列表

2.4.1.1 终端信息

赤兔提供设备管理能力，为管理员展示终端的各类情况：终端列表主要包含不同版本的数据统计、异常状态的信息统计，同时以列表形式展示当前已安装Agent的终端信息情况，点击详情将可显示设备自身信息。



- **系统账户**

产品采集终端软硬件信息后将生成mashID，依据每个唯一的mashID将会对应出现设备ID以便在系统内使用；同时会采集相应的操作系统及账户信息，组合为系统账户在设备列表页面展示。

- **终端状态说明**

1. 终端状态包括，在线、离线、异常（包括连接异常、授权异常）、已卸载；终端设备有正常心跳时为在线状态，超过一定时间无心跳则将变为离线状态；
2. 终端设备卸载Agent后，列表中的终端状态将变为已卸载。已卸载状态的设备不会在列表上显示，可通过搜索设备ID找到该设备；
3. 当终端超过10天无心跳时，终端列表将显示“连接异常”。此时管理员需要线下排查该终端的情况，查看连接异常原因；
4. 当终端卸载时，将显示“卸载中”状态。若通过在线卸载进行卸载，卸载完成后状态将变为注销；若通过离线卸载进行卸载，管理员需手动点击“完成卸载”按键；
5. 若macOS的终端未完全授权设备权限，会提示健康异常。

- **Agent启停说明**

当管理员需要关停某台设备上Agent运行时，可以通过设备的Agent启停来控制，点击开关状态即可进行Agent的启停。此项功能建议在终端设备上因Agent的运行出现问题时使用，停用可能会造成再次段时间内发生数据安全事件。

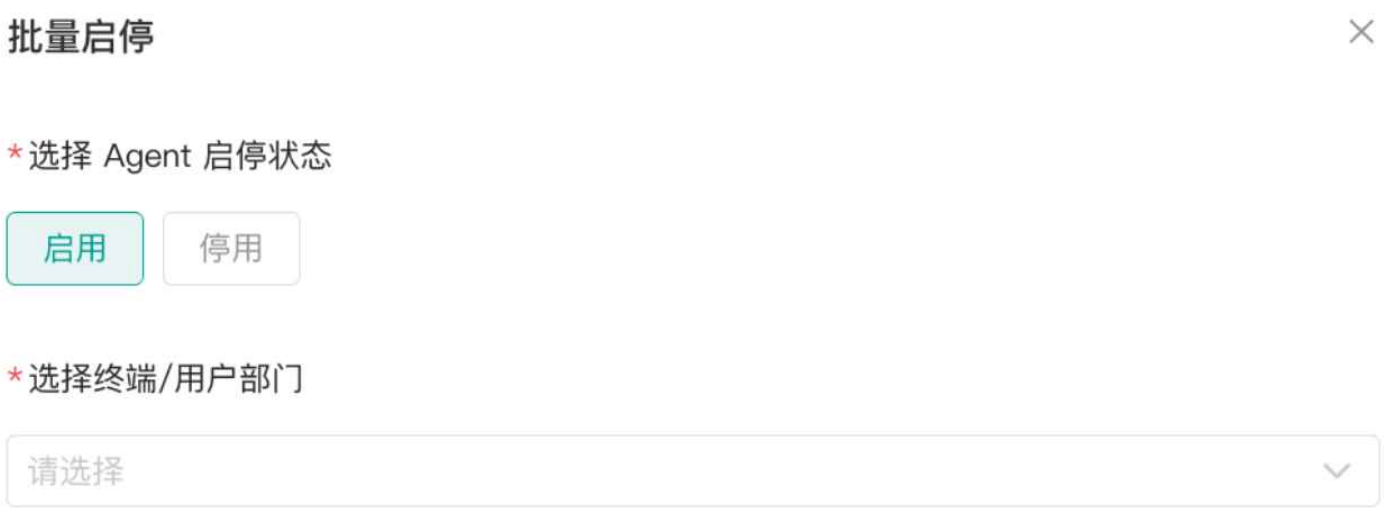
- **终端标签**

点击标签栏，可以为终端配置标签，便于管理员对设备进行快速分组、筛选、下发策略等操作。

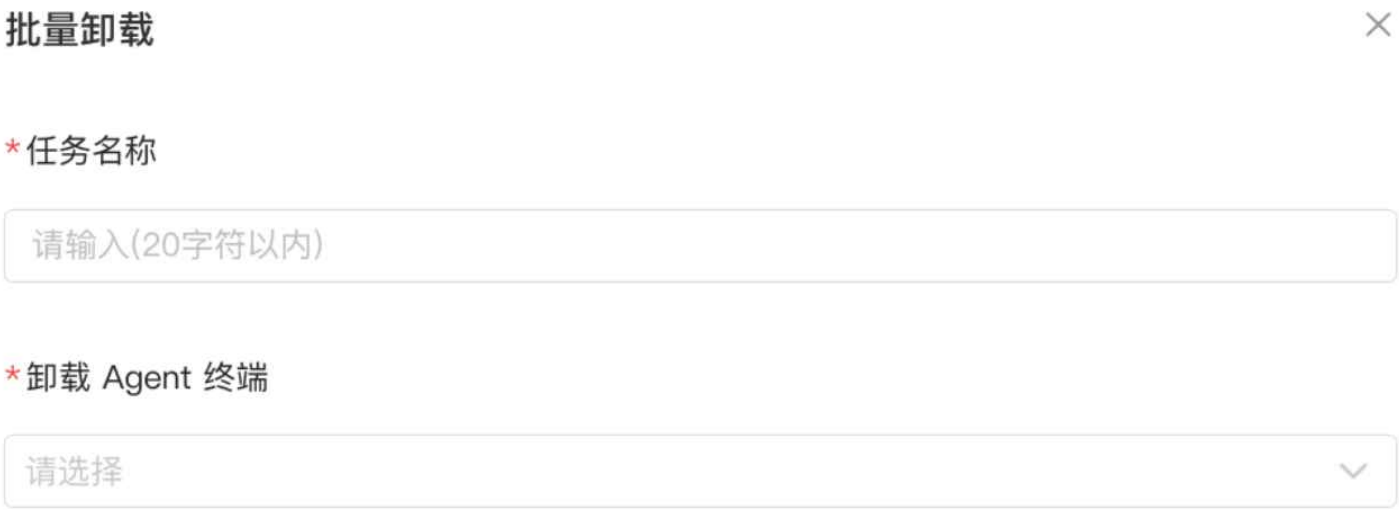
- 批量操作

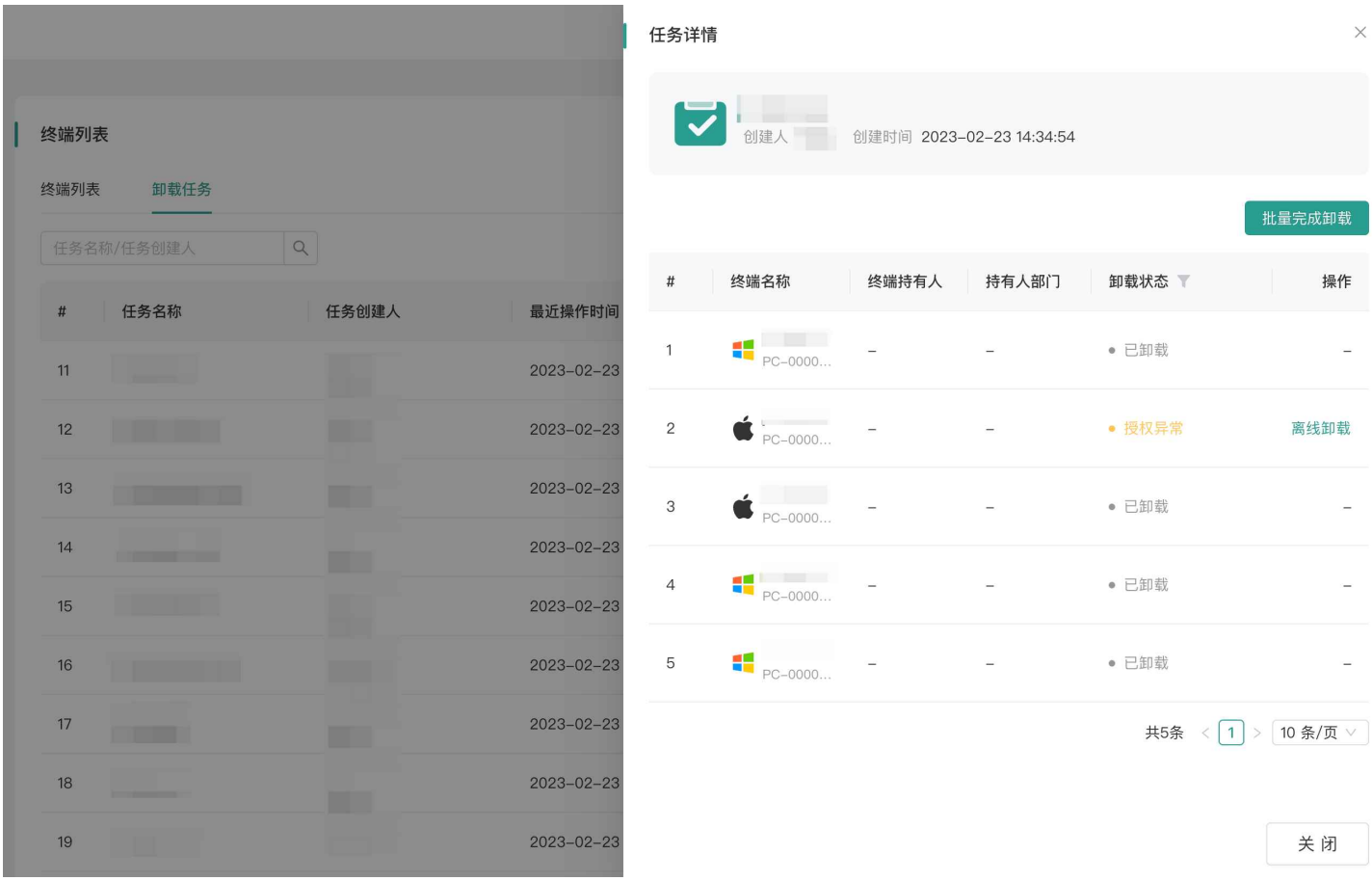
点击页面右上角「批量操作」，可以选择对终端进行批量启停/批量卸载任务。

- **创建启停任务：**选择「创建启停任务」，管理员可一键勾选需要启用/停用Agent的设备。



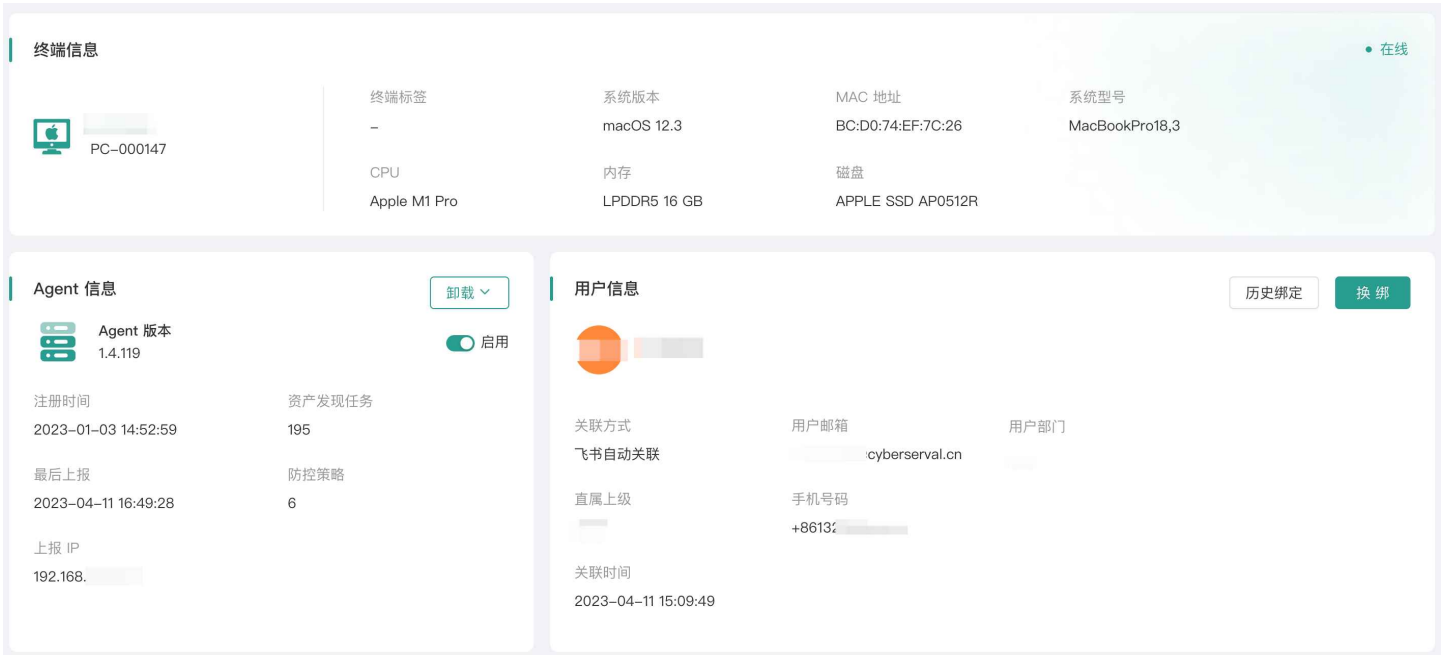
- **创建卸载任务：**新建卸载任务，选择卸载Agent终端，下发任务即可进行Agent卸载。对于卸载异常或已经离线的设备，可以点击离线卸载，在相应终端输入卸载码卸载。





2.4.1.2 设备详情

设备详情页为管理员提供了详细的设备信息，包括该设备的基础信息、硬件信息、终端数据资产、进程信息、终端性能信息等。



风险行为信息

风险行为信息将以日历盘的形式显示设备命中策略的信息，点击不同日期将带条件筛选至风险日志信息

关联防控策略

关联防控策略将显示该设备的相关策略信息。

终端数据资产

终端数据资产显示当前终端上的数据资产以及数据分类及分类分布结果。点击「详情」可跳转至数据资产地图页面，查看本设备拥有的数据文件信息。

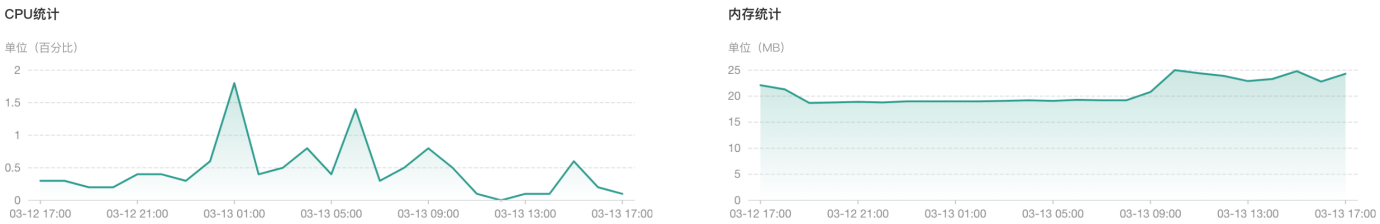
进程信息

进程信息显示当前终端上运行的进程，并支持实时刷新获取最新进程。

#	进程名称	PID	运行用户	CPU	内存	进程路径	启用时间	签名姓名	父进程	父进程ID
1		73312		0	–	/Applicatio	1678439944		launchd	1
2	S	1190		0	–	/Library	1678358634		launchd	1
3	co con	73316		0	–	/Librar	1678439954		launchd	1
4	cc ind.	419		0	–	/Librar	1678358571		launchd	1
5	L er)	95605		0	–	/App	1678528552		Feishu	95590

终端性能信息

终端性能信息显示终端当前的CPU统计和内存统计信息。

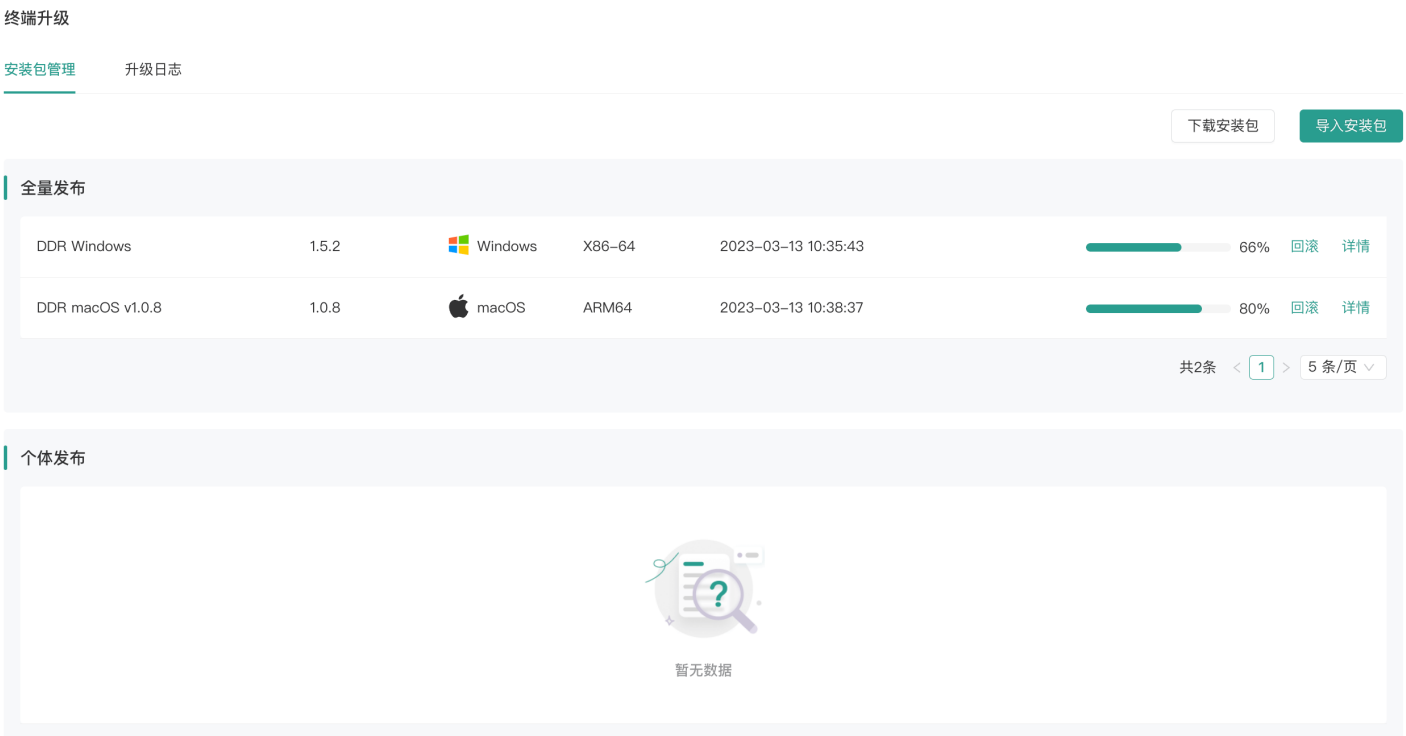


异常一键诊断

对于异常终端，可以在此处进行一键终端检测，同时可将检测结果压缩打包后，发送给薮猫科技工程师进行进一步排查。

2.4.2 终端升级

1. 在左侧导航栏中，点击【终端管理】，再点击【终端升级】进入终端升级页面。页面布局如下图所示。



2. 点击页面右上角「下载安装包」按钮，选择对应系统类型下载，点击【下载安装包】按钮进行下载。（安装包需先导入之后，选择全量发布，方可进行下载）。

导入安装包获取，请咨询薮猫科技工程师。

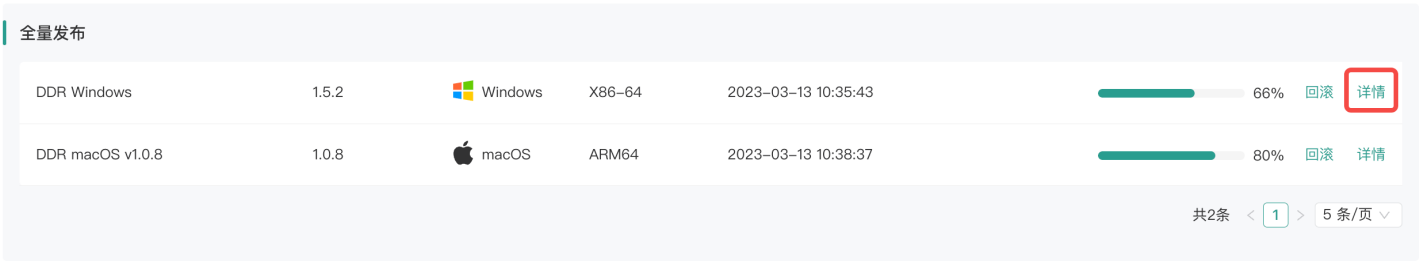
2.4.2.1 全量发布

全量发布代表着全员安装包推送，且每个操作系统的安装包仅有一个能处于可全量发布的状态。只有处于全量发布状态下的安装包可下载。

全量发布将向所有设备推送新的安装包，如针对特殊设备需要特殊版本的安装包，需指定设备进行个体发布。

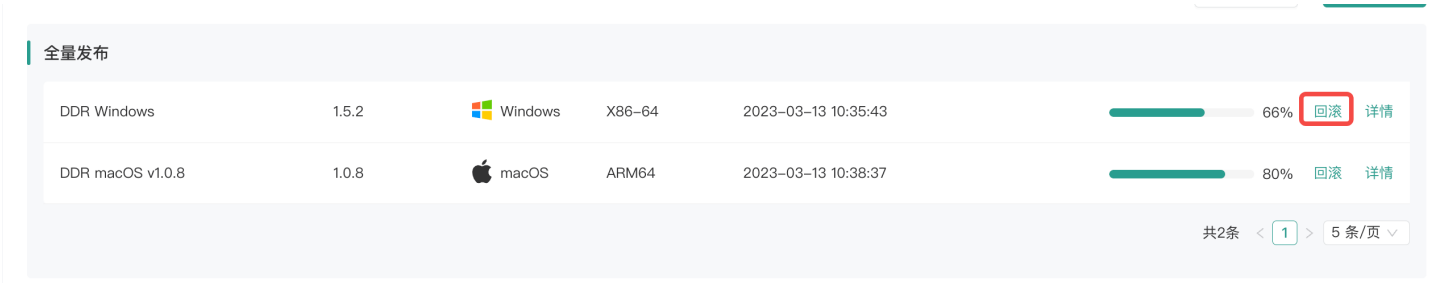
2.4.2.2查看发布详情

点击发布记录中的详情，可查看发布情况。



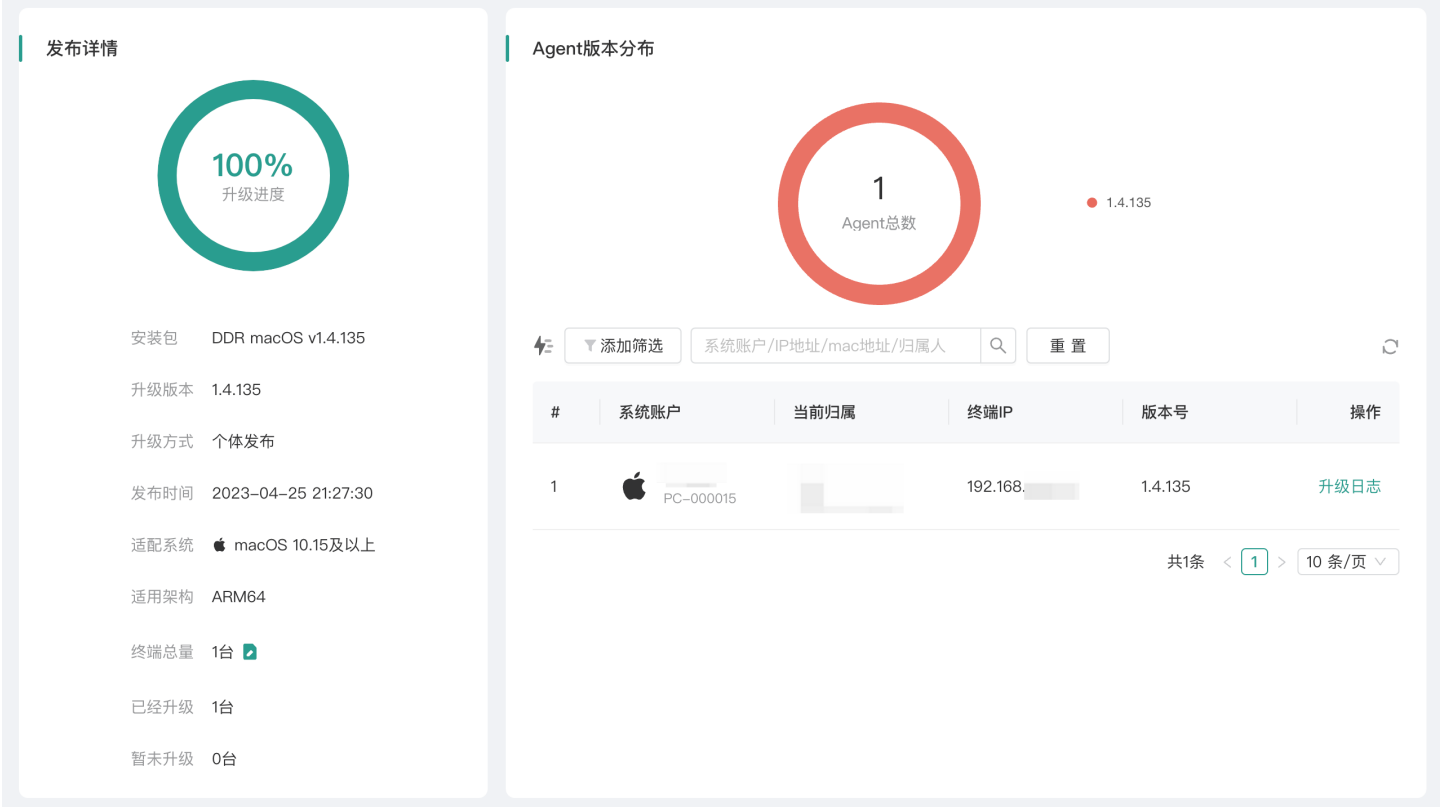
2.4.2.3 回滚发布

点击发布记录中的回滚，可回滚本次发布。



2.4.2.4 个体发布

在终端升级页面，点击个体发布，进入个体发布配置页面，选择设备后，点击发布即可完成。点击详情可以查看当前升级进度，升级成功的设备将有升级日志信息。



2.4.2.5 升级日志

点击升级日志界面，即可查看终端升级的相关信息。

2.4.3 终端配置

为保障终端的统一可用，且不影响员工正常工作。赤兔为终端提供了丰富的终端配置项：包括终端运行资源、云端通信配置、macOS授权配置、安全防护。

2.4.3.1 运行资源配置

管理员可在本页面对Agent在终端运行时的CPU、存储、网络进行资源配置，配置项为资源运行上限信息，建议配置数据适当宽松。

2.4.3.2 云端通信配置

为保障终端云端通信，管理员可以添加多台服务端的网络配置信息，并设置通信连接。终端会根据管理员设置的优先级依次尝试连接，直至成功为止。

为确保心跳及策略同步信息、Agent状态信息的判定，管理员可在本页面进行通信连接的配置。

2.4.3.3 macOS授权配置

因macOS系统的特殊性，在macOS上想要使用赤兔的全功能，需要员工在终端上为赤兔进行一系列授权。授权内容主要包括：完全磁盘访问权限。授权配置内容为：

- 授权提醒的弹窗频率：若员工不愿意为赤兔授权，赤兔将频繁弹窗提醒员工进行授权；
- 累计后台提醒告警：当累计多次弹窗员工仍不授权时，系统将会通知管理员协调处理；
- 通知告警设置：可通过邮件、IM机器人等多种方式对拒不授权的事件进行通知告警。

2.4.3.4 安全防护

用户可在此处配置资产扫描、数据库审计相关配置，以及浏览器强管控等相关内容。

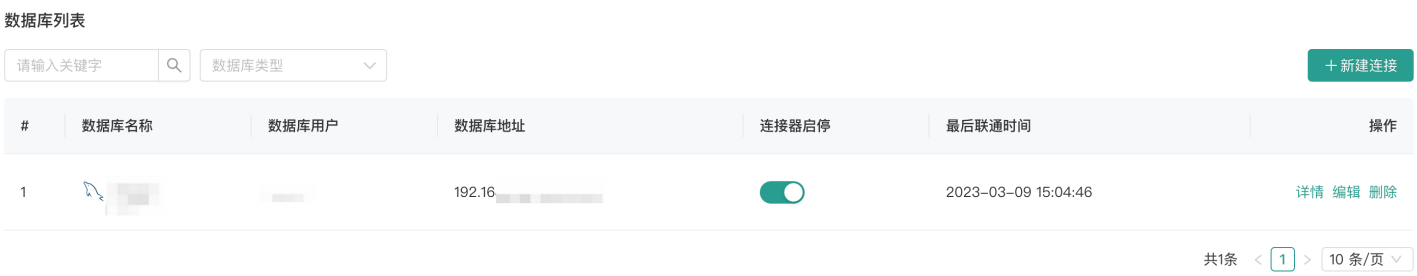
2.4.4 数据库列表

管理员可在本页面对数据库进行管理，查看详情、编辑信息等，也可以在本页面新建数据库连接。

2.4.4.1 新建数据库连接

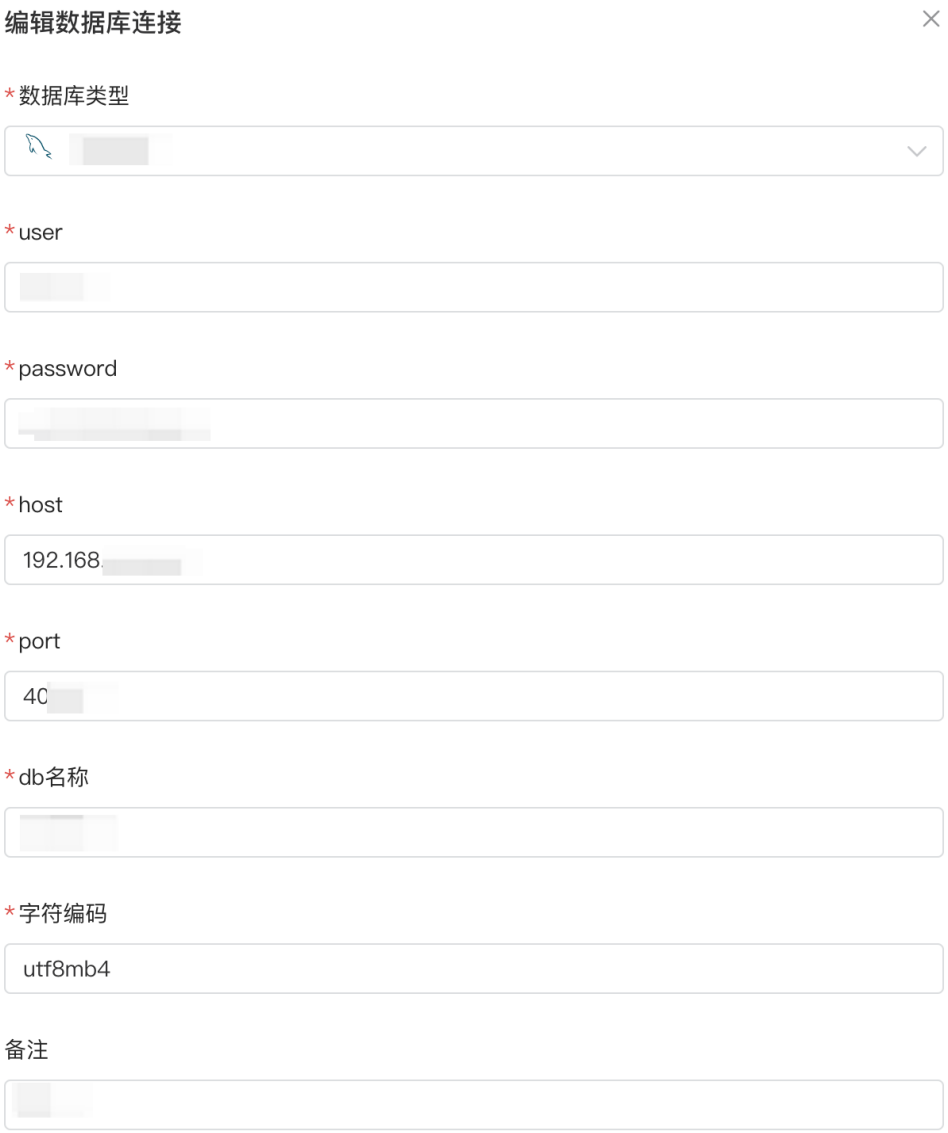
点击「终端管理」-「数据库列表」，进入数据库列表界面。点击页面右上角「+新增连接」，填入相关信息，即可新建数据库连接。

通过连接测试并且添加成功的数据库信息，会在本页以列表的形式展示。



2.4.4.2 编辑数据库连接信息

用户可在列表页面，编辑相应的数据库信息，点击操作栏中的「编辑」按钮，可编辑数据库中的详情信息。



2.4.4.3 查看详情信息

用户可在列表页面，查看相应的数据库信息，点击操作栏中的「详情」按钮，可查看数据库中的详情信息。

2.4.4.4 删除数据库信息

用户可在列表页面，选择要删除的数据库信息，点击操作栏中的「删除」按钮，将数据库信息进行删除。

2.5 用户管理

2.5.1 企业员工

赤兔坚持以人为中心，管控、运营、分析都应围绕人来进行，故赤兔具备齐全的员工管理功能。包括与企业现有的组织架构进行对接、根据企业现有部门及部门特性设置安全策略、以人的维度进行安全分析。

赤兔支持选择一个第三方系统进行用户同步，且第三方同步的信息不支持管理员进行编辑。也支持直接通过手动方式，在系统中创建用户，在系统内创建的用户有“手动”的标记，支持在系统内编辑和

信息修改。

2.5.1.1 员工列表

点击侧边栏「用户管理」，点击二级菜单「企业员工」，即可进入员工用户管理页面。页面左侧为企业组织架构信息，右侧为员工列表。员工管理页面可以显示员工所持设备，为员工赋予横向部门标签。员工管理页面包含系统创建和第三方系统导入的用户。

2.5.1.2 员工详情

点击列表页右上方的手动操作，选择添加用户，在侧边栏选择批量导入多个用户/新增单个添加用户

2.5.1.3 手工创建员工

点击列表页右上方的手动操作，选择添加用户，在侧边栏选择批量导入多个用户/新增单个添加用户。

- **批量导入**

切记批量导入需要先导出模版，并要根据模版填写相关信息。导入时需要管理员选择是否覆盖系统内已有用户，选择覆盖，将会覆盖系统内同样的用户。

- **单个添加**

当无需批量添加用户时，可以选择单个添加用户进行快速添加。输入相应的用户信息后完成创建。

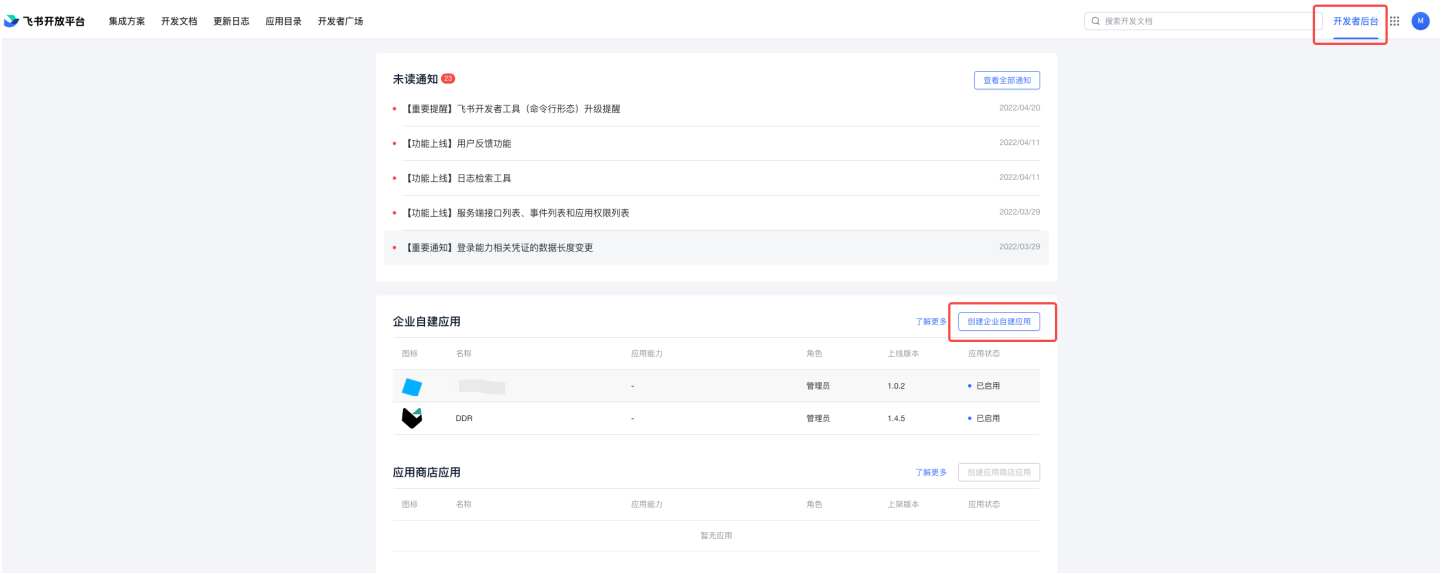
2.5.1.4 飞书同步员工

配置飞书同步，赤兔需要获取以下参数（所有的参数信息需在飞书开放后台中创建一个内部应用）

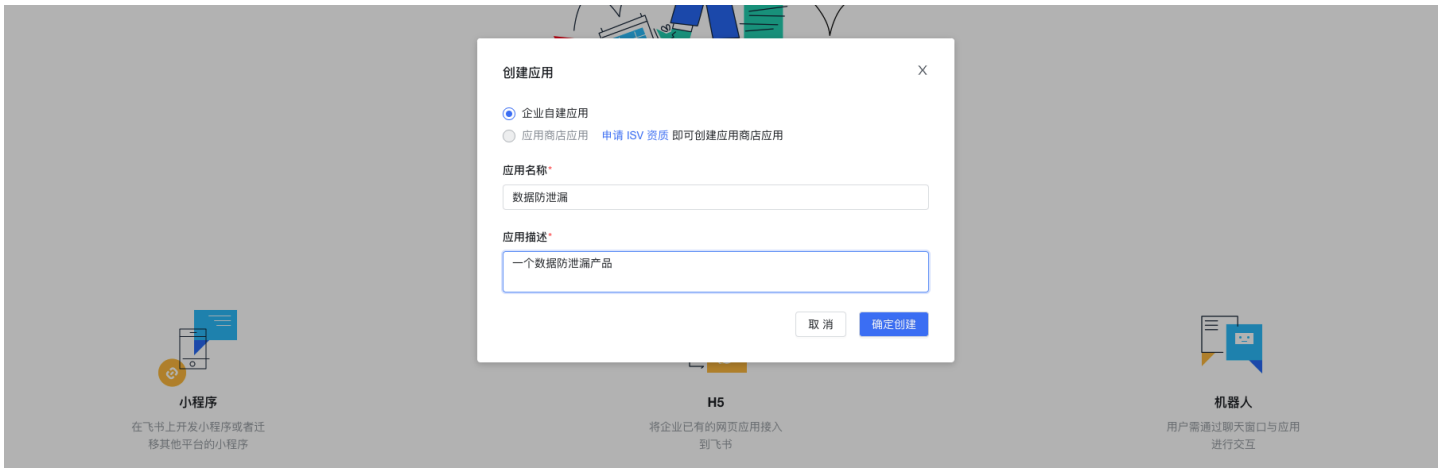
- App ID：飞书应用的 App ID
- App Secret：飞书应用的 Secret

2.5.1.4.1 步骤一：登录飞书开放平台，创建应用并获取相应参数信息

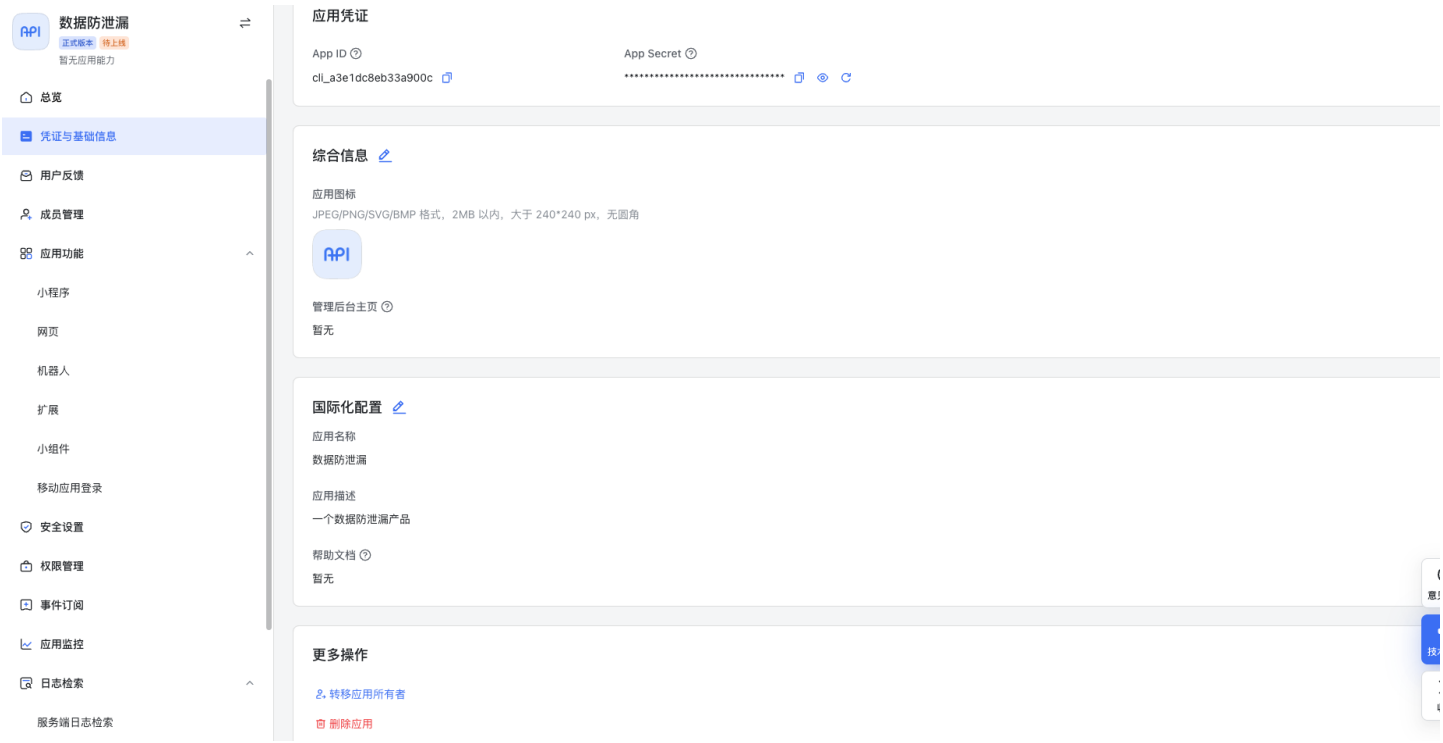
1. 登录飞书后台地址： https://open.feishu.cn/app ，使用具有飞书企业管理员权限的账户进行登录。
2. 进入飞书开放平台「首页」，点击「企业自建应用」。



3. 点击创建应用，填写相应的信息。（选择企业自建应用）

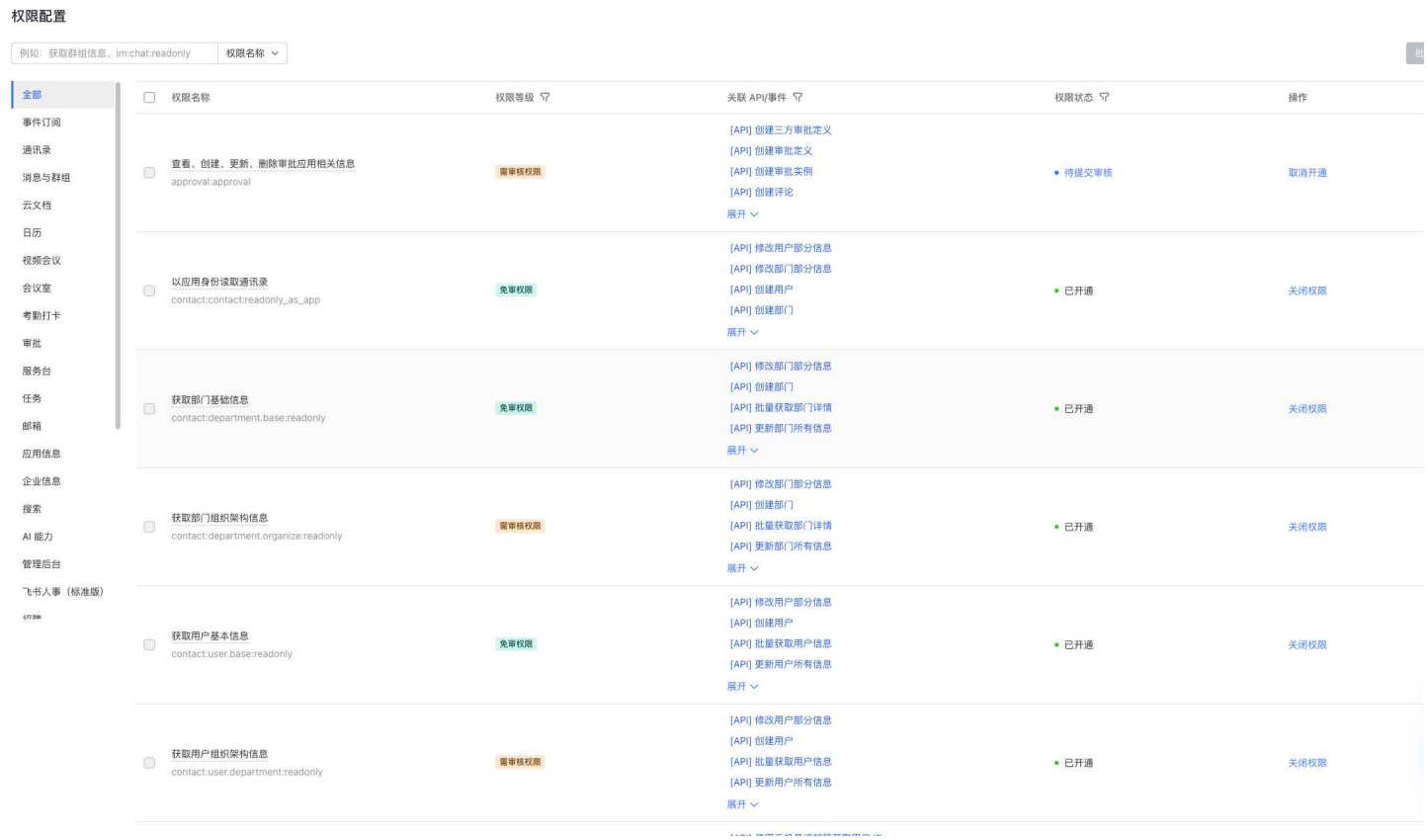


4. 进入应用列表页面，选择对应的企业自建应用。点击进入，并在右侧边栏选择「凭证与基础信息」，即可查询App ID 和 App Secret；



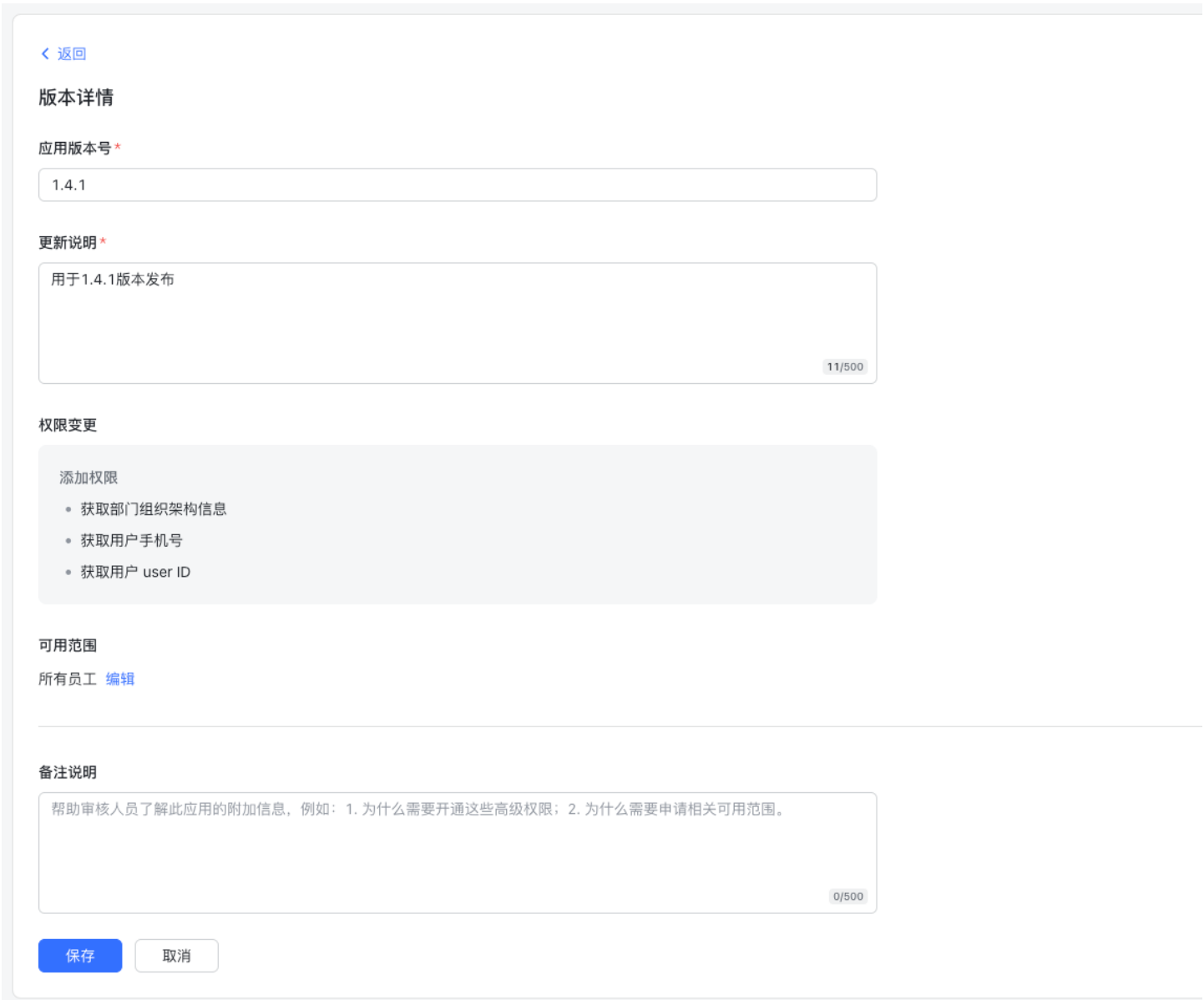
5. 点击权限管理，通讯录权限。

- 配置权限范围：全部成员
- 为 赤兔 开通“应用身份读取通讯录、获取部门基础信息、获取部门组织架构信息、获取用户基本信息、获取用户User ID、获取用户手机号”等权限。



6. 选择侧边栏「总览」，点击第四步—「应用发布」。

7. 点击右上角「创建版本」，输入内容信息，点击「保存」。在保存完成后的返回页面，点击右上角「申请线上发布」，联系飞书管理员（若登录账户为管理员权限可使用当前账号审核通过）通过权限及应用发布审核。



至此，应用创建成功！

2.5.1.4.2 步骤二：登录产品后台，进行同步配置

1. 选择 自动同步- 飞书同步
2. 填写配置信息

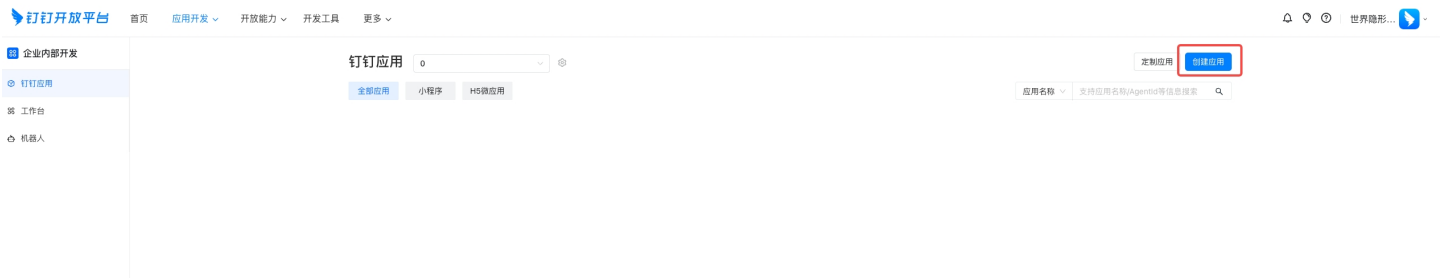
- App ID： 输入步骤一获取的应用参数App ID
- Secret： 输入步骤一获取的应用参数Secret
- 选择是否周期同步（建议开启）：周期同步开启后每日0:00自动全量同步飞书数据
- 飞书审批：请查阅本文档中处置模版-飞书审批部分

2.5.1.5 钉钉同步员工

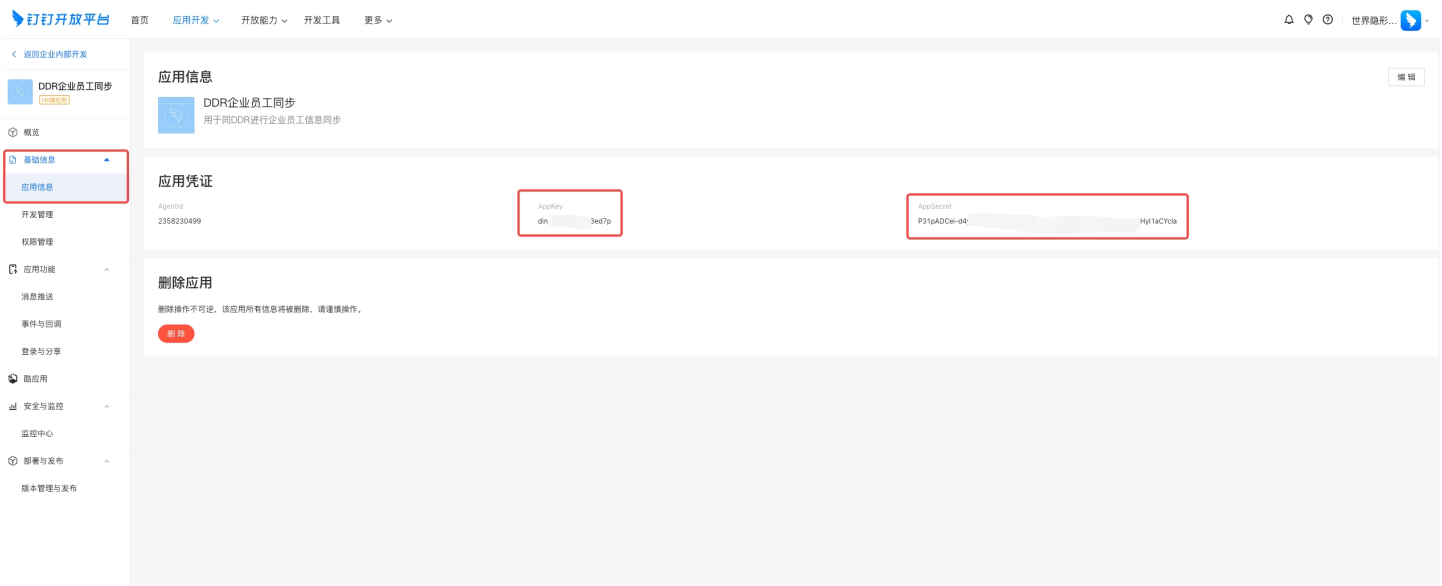
2.5.1.5.1 步骤一：登录钉钉开放平台，创建应用并获取相应参数信息

1. 登录钉钉后台地址：https://open.dingtalk.com/，使用具有钉钉企业管理员权限的账户进行登录。
2. 进入钉钉开放平台「首页」，点击「应用开发-企业内部开发」。

3. 点击创建应用，填写相应的信息。

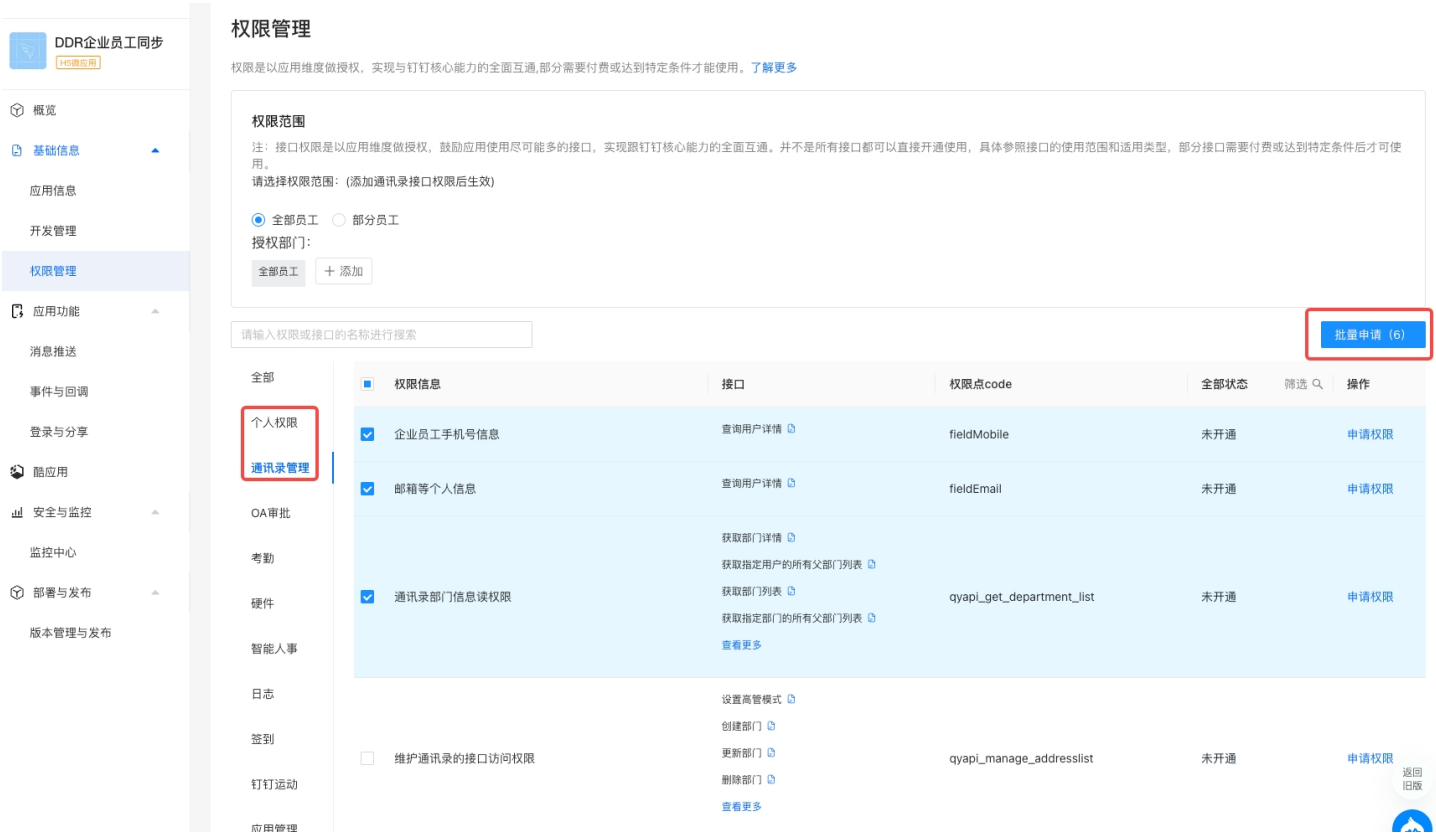


4. 进入应用详情页面，在右侧边栏选择「基础信息-应用信息」，即可查询AppKey和AppSecret；



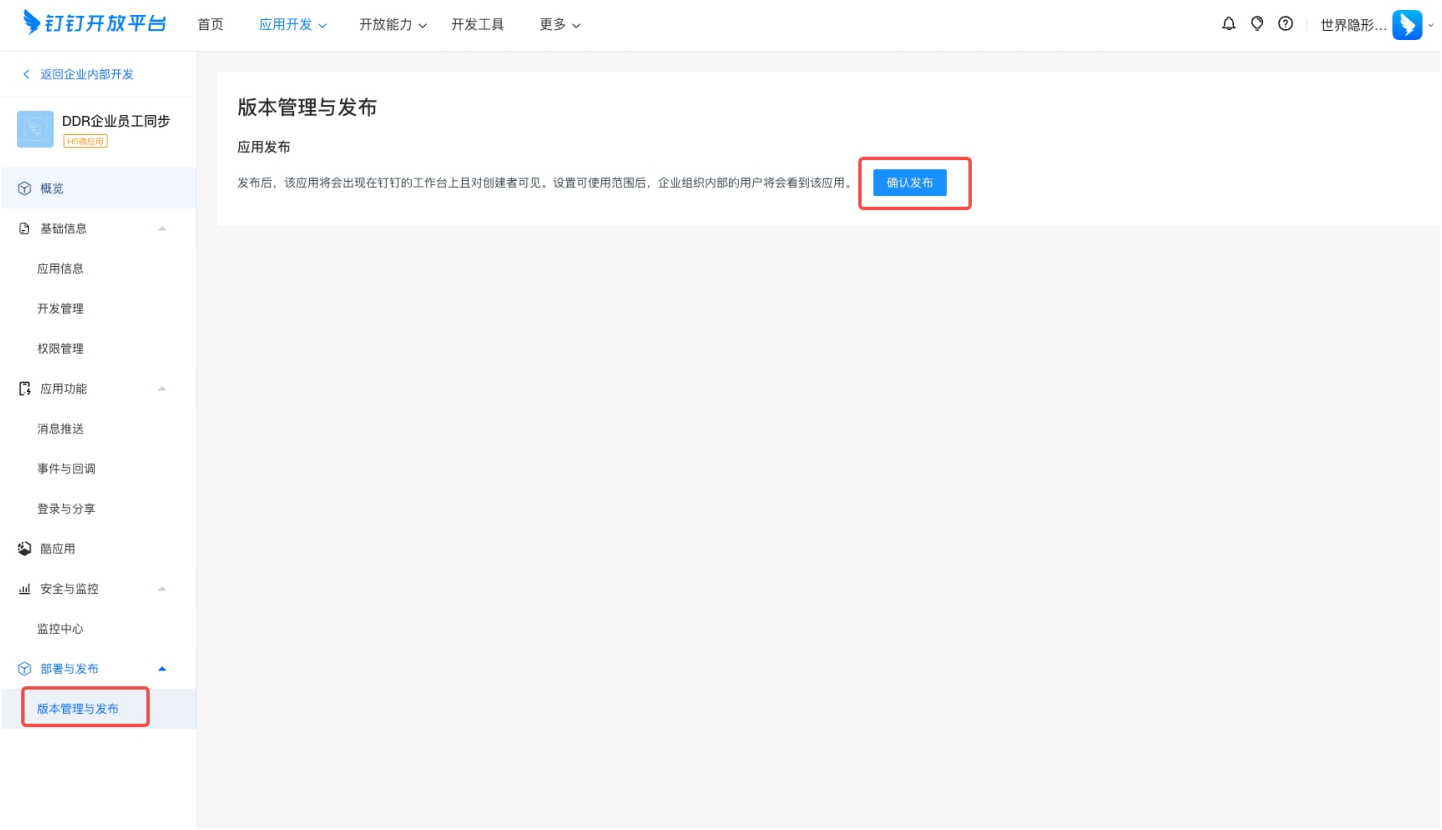
5. 点击权限管理，通讯录权限。

- 配置权限范围：全部成员
- 为 赤兔 开通“个人权限-通讯录个人信息读权限”、“通讯录管理-通讯录部门信息读权限 ”、“通讯录管理-成员信息读权限”、“通讯录管理-通讯录部门成员读权限”、“通讯录管理-企业员工手机号信息 ”、“通讯录管理-邮箱等个人信息”权限。
- 若后续需要使用钉钉审批，需开通“企业调用接口执行审批操作的权限”、“审批流数据管理权限”、“工作流实例写权限”、“工作流模板写权限”、“工作流模板读权限”、“工作流实例读权限”

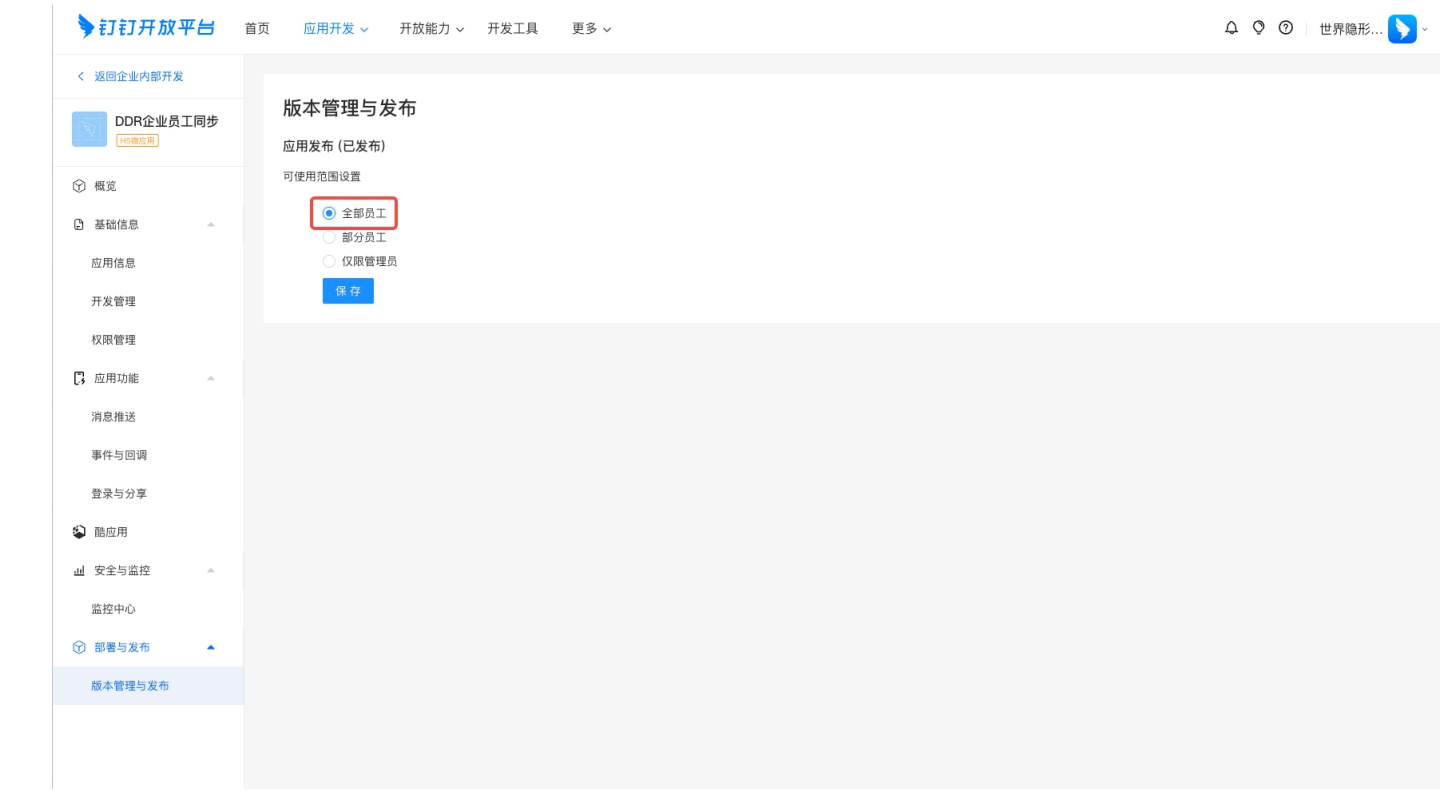


- 点击右上角「批量申请」

6. 选择侧边栏「部署与发布-版本管理与发布」，点击「确认发布」。



7. 配置使用范围：全部员工



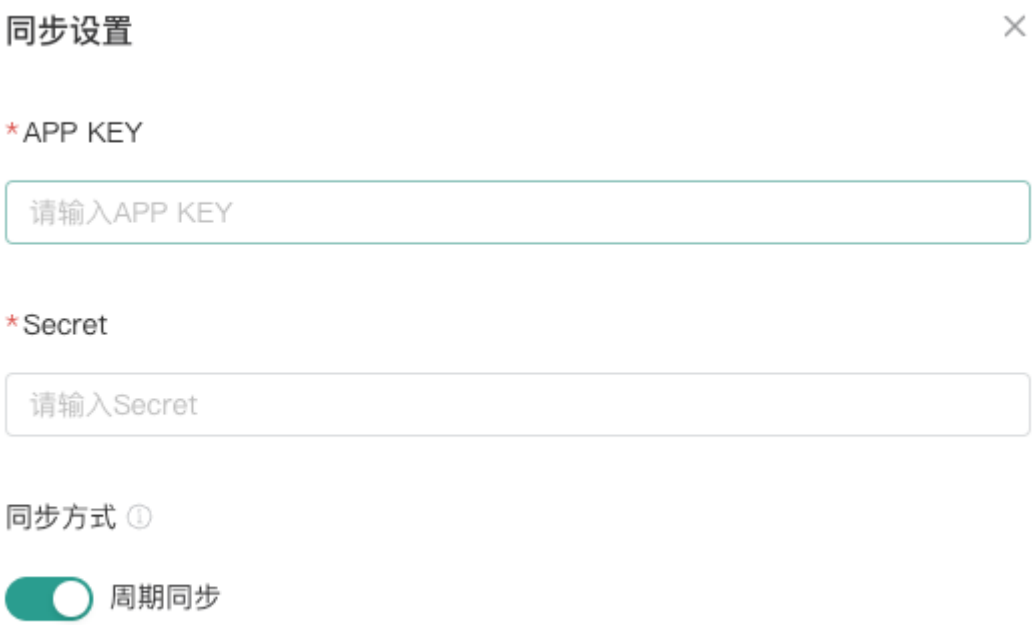
至此，应用创建成功！

2.5.1.5.2 步骤二：登录产品后台，进行同步配置

1. 选择 自动同步- 钉钉同步
2. 填写配置信息

- AppKey：输入步骤一获取的应用参数AppKey

- Secret： 输入步骤一获取的应用参数AppSecret
- 选择是否周期同步（建议开启）： 周期同步开启后每日0:00自动全量同步飞书数据



2.5.1.6 LDAP/AD同步员工

赤兔为管理员提供了LDAP和AD同步用户及组织架构的功能，管理员可通过选择LDAP和AD同步，并填写相应的信息后快速同步LDAP和AD上的企业员工信息及组织架构信息。

1. 选择LDAP或AD域同步后，进入同步列表页。LDAP和AD域都支持多组织分别挂载，故可以设置多个LDAP/AD的同步设置。（因LDAP和AD的同步类似，此处将以LDAP举例，不再单独举例AD）。
2. 点击右上角的LDAP同步设置，填写相应的同步内容。

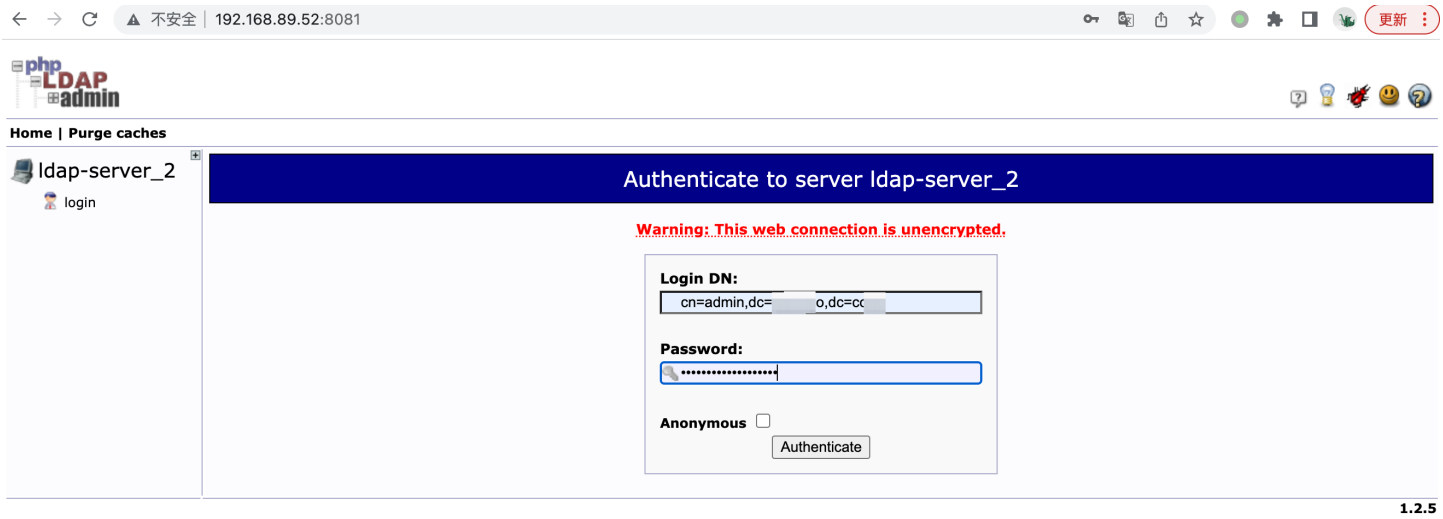
- 填写完连接接信息后，可以进行下连接接测试；
- 管理员可根据需要进行用户、组织架构的过滤；
- 用户OU及根域名节点切记勿填错，其他用户字段可根据实际情况调整。

3. 创建完同步设置后，管理员亦可根据需要查看同步历史，把握每次同步的状况。每次同步后，将会有同步历史的显示，管理员可即时查看每次的同步情况。包括新增员工、更新员工、注销员工及是否有同步失败的情况；同步的组织部门、更新的组织部门，注销的组织部门，是否有同步失败的情况。

2.5.1.6.1 步骤一：获取LDAP配置信息

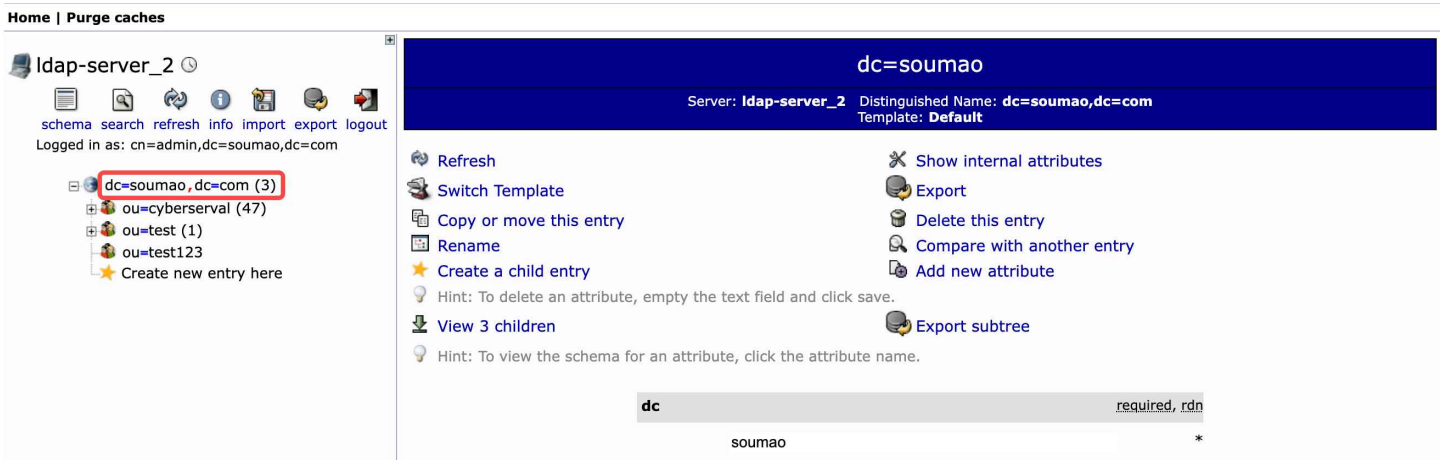
1. 获取LDAP配置信息

咨询 LDAP 的管理员，获取 LDAP 服务器地址、端口号、加密方式、管理员账号及密码，并登录 LDAP 服务器平台。



2. 查看BaseDN (根域名/根目录）节点。

咨询 LDAP 的管理员，获取BaseDN信息。BaseDN信息代表赤兔系统将从输入的BaseDN目录开始搜索，如：dc=soumao,dc=com

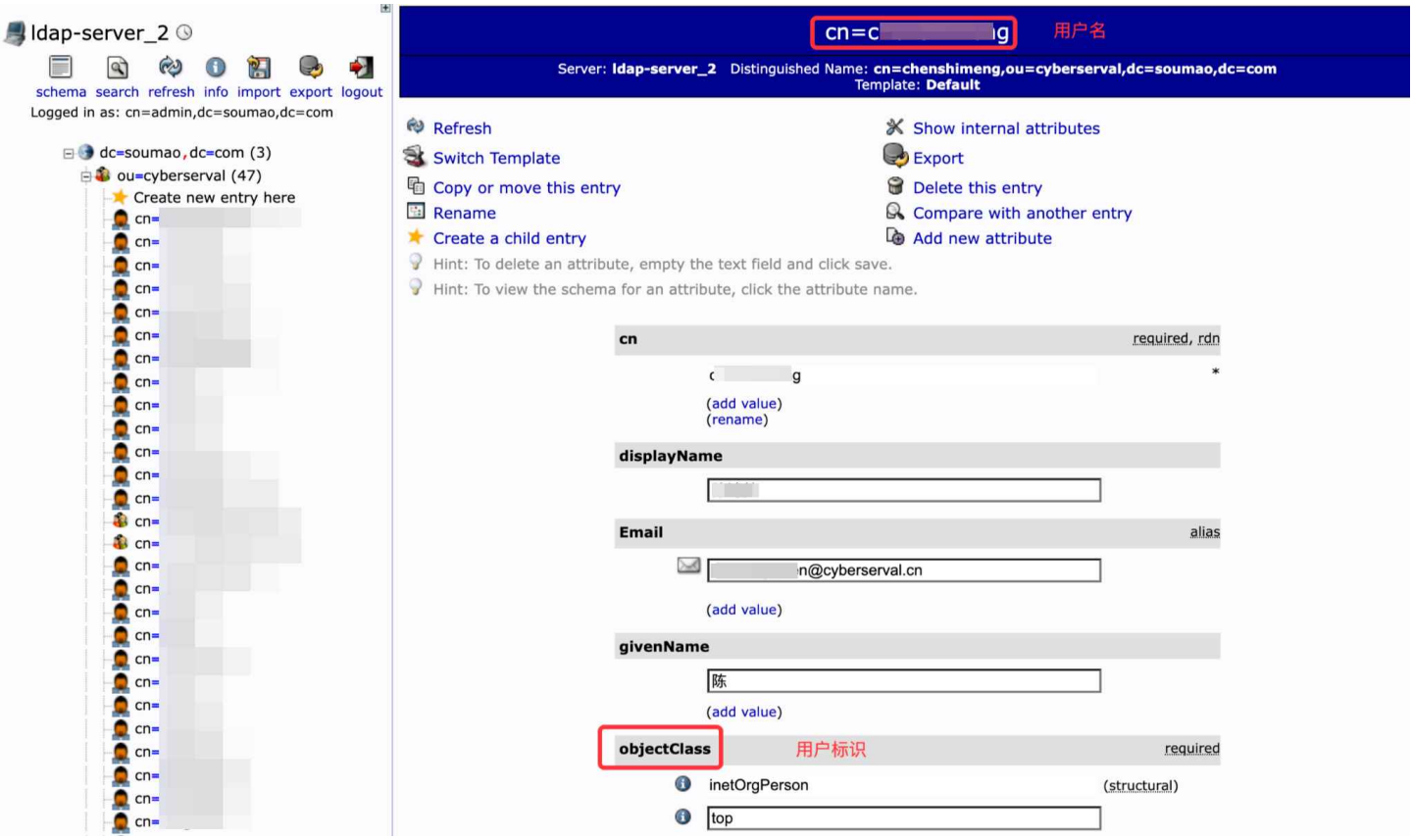


3. 点击部门，记录部门标识的属性名称。

说明：

部门标识：objectClass=organizationalUnit；类型为所有organizationalUnit的对象。在赤兔用户过滤中将查询结果中objectClass = organizationalUnit 的对象作为LDAP 中的部门信息。

4. 点击具体员工，记录用户标识的属性名称。



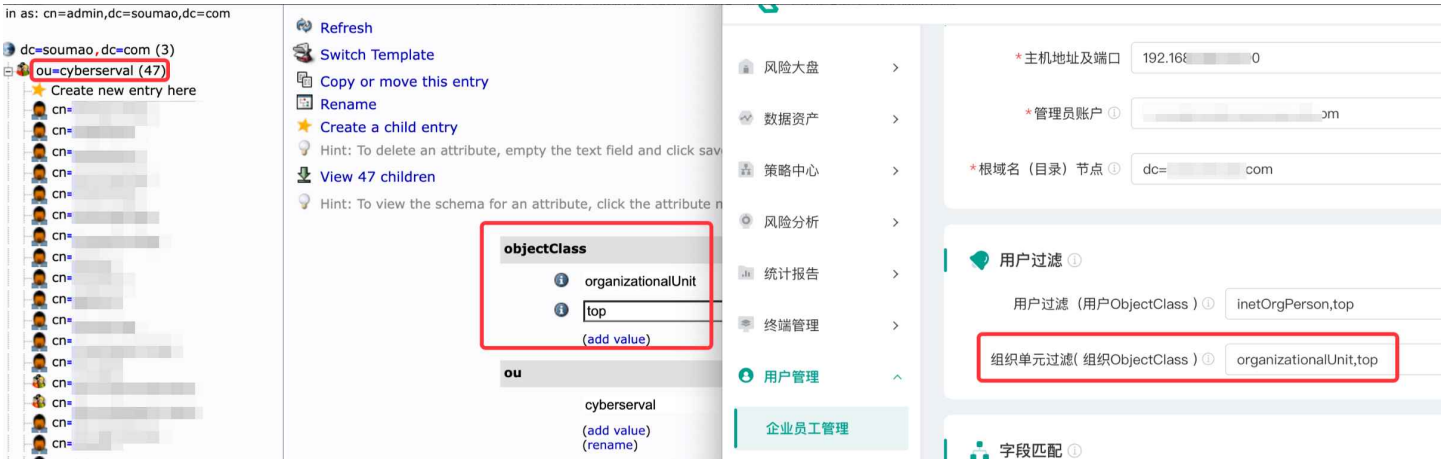
说明：

用户标识：objectClass=top；类型为所有 top 的对象。在赤兔用户过滤中将查询结果中 objectClass = top 的对象作为LDAP 中的用户信息。

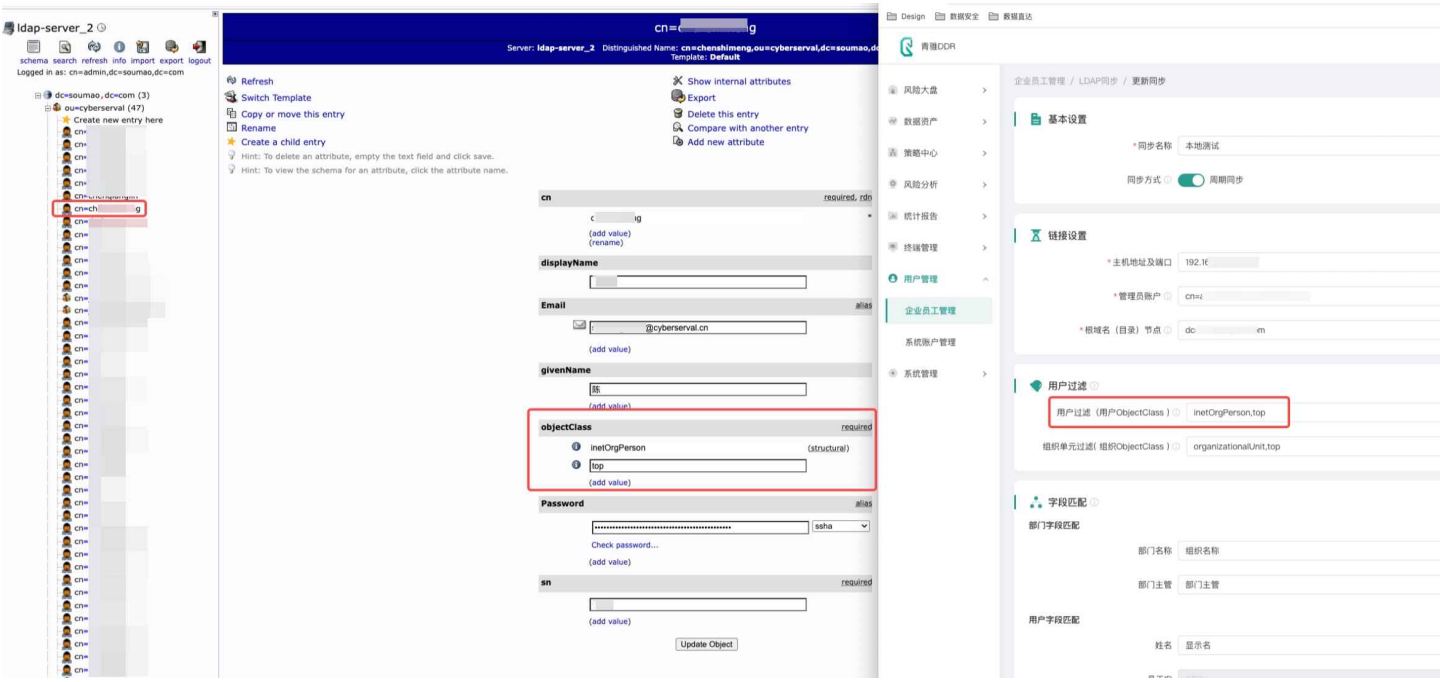
2.5.1.6.2 步骤二：登录产品后台，进行同步配置

1. 选择 自动同步- LDAP同步/AD同步
2. 填写配置信息

- 同步名称：本同步配置的名称
- 用户OU：LDAP信息导入至产品后台的组织架构位置（推荐选择根部门）。
- 链接设置：输入在步骤一中获取 LDAP服务器地址、端口号、加密方式、管理员账号及密码、BaseDN(根域名/根目录节点)信息。
  - 若不确定配置是否正确，可点击测试链接进行配置验证。
- 用户过滤：输入在步骤一中获取 LDAP中的部门及用户属性标识。



组织单元过滤



用户过滤

- 字段匹配：默认即可。

3. 点击「触发同步」，进行信息同步。

2.5.1.7 切换同步

企业若因经营调整需要需要更换同步员工信息及组织架构的同步方式，可以在第三方同步设置的页面选择切换同步方式，点击「切换同步方式」，选择需要切换的同步方式即可。

需要注意的是：切换同步方式，将会丢失之前保存的同步用户信息以及用户与设备的绑定信息，用户将需要重新绑定其所持设备。（通过系统自行创建的用户不会丢失。）

2.5.1.8 自动关联设备

赤兔具备先进的自动将用户与设备关联的能力。当前支持飞书、钉钉导入用户和LDAP/AD账户。企业员工及组织架构信息同步完成后：员工只需要在安装了飞书Agent的设备上登录飞书应用，或通过域账户登录终端设备，赤兔将能把员工与终端设备完成自动绑定。需要注意的绑定方式与同步方式是相对应的。通过LDAP和AD导入仅可通过域账户绑定，通过飞书、钉钉导入，需要员工在设备上登录飞书、钉钉后方可绑定。

2.5.1.9 手动关联设备

若用户希望手动批量关联设备，可以点击页面右上角「绑定设置」并选择关联设备方式。管理员可以选择通过IP地址关联或通过硬件MAC地址关联，并一定要按照导出的模版进行填写。填写完成后，系统将根据导入的信息进行关联。

2.5.2 NEW 系统账户

系统管理员用于管理所有账号，可以通过列表查看所有账号信息，包括用户名、角色、创建时间、最近登录时间。

2.5.2.1 账户管理

- **添加账户**

如需增加账户，点击右上角「+ 新增账户」，并填写相应信息，您可以从您已经创建的角色及系统内置角色中选择。

新增账户

*账户名称

30个字符以内 0 / 30

*角色

操作员

*管理范围

全局 部分

*设置密码

请输入密码 自动生成

密码长度8-20位，且需包含大小写字母、特殊字符、数字中的2种

所属部门

请输入使用该账户的员工所属部门

*邮箱

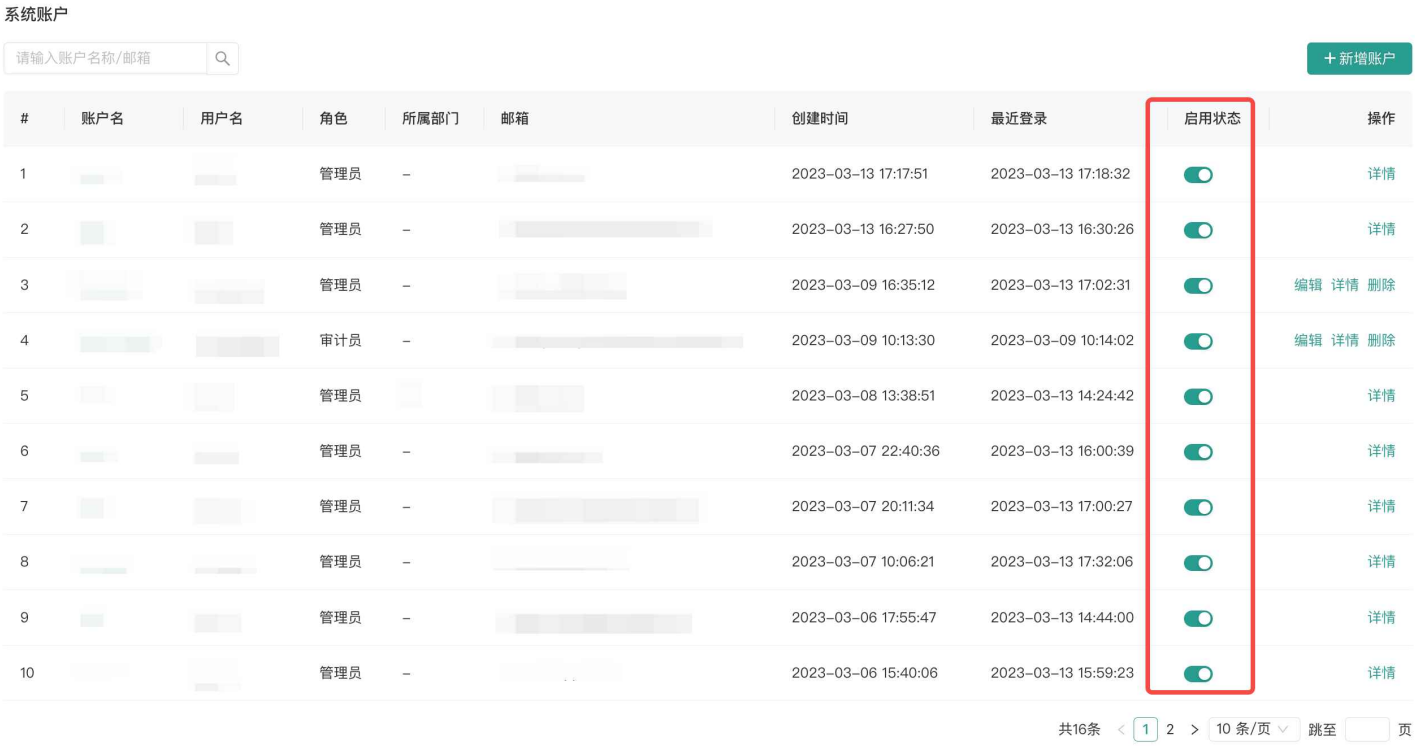
请输入邮箱

用户名

请输入用户名

- **修改、禁用、删除账号**

如需对账号进行修改或删除，可在相应账号操作列单击进行调整。也可点击开关按钮，对账户启用/禁用状态进行设置。



2.5.2.1.1 管理员

系统的管理员包括超级管理员和管理员，超级管理员为系统最高权限的管理者，具备所有权限，但超级管理员账户唯一。管理员也具备系统的所有管理权限，可以有多个管理员的账户，但其不可创建同级别的账户，仅可通过超级管理员创建。

2.5.2.1.2 审计员

审计员为系统内审计风险事件的角色，可以有多个。

2.5.2.1.3 操作员

操作员为系统的前置运营人员，可以同步用户、为不同的员工下发策略、统计企业内的数据资产、下发任务、建立数据的分类分级等。

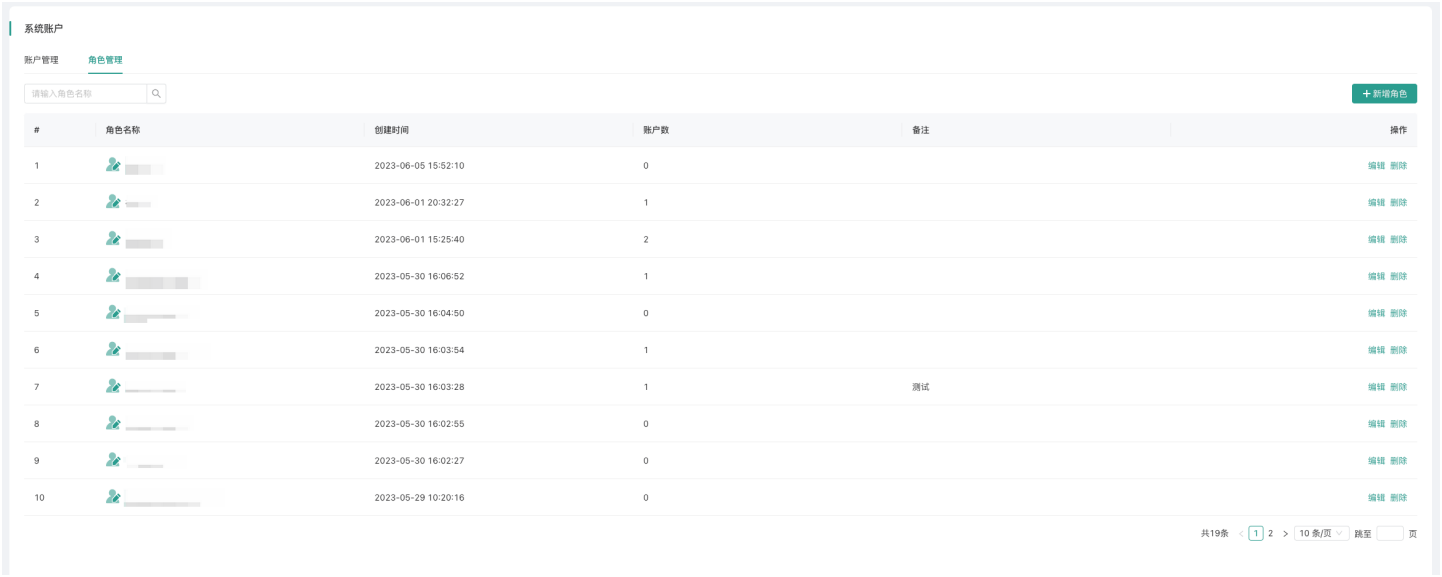
2.5.2.1.4 自创建角色

在角色管理中可以创建角色，自由分配其权限。

2.5.2.2 角色管理

2.5.2.2.1 角色列表

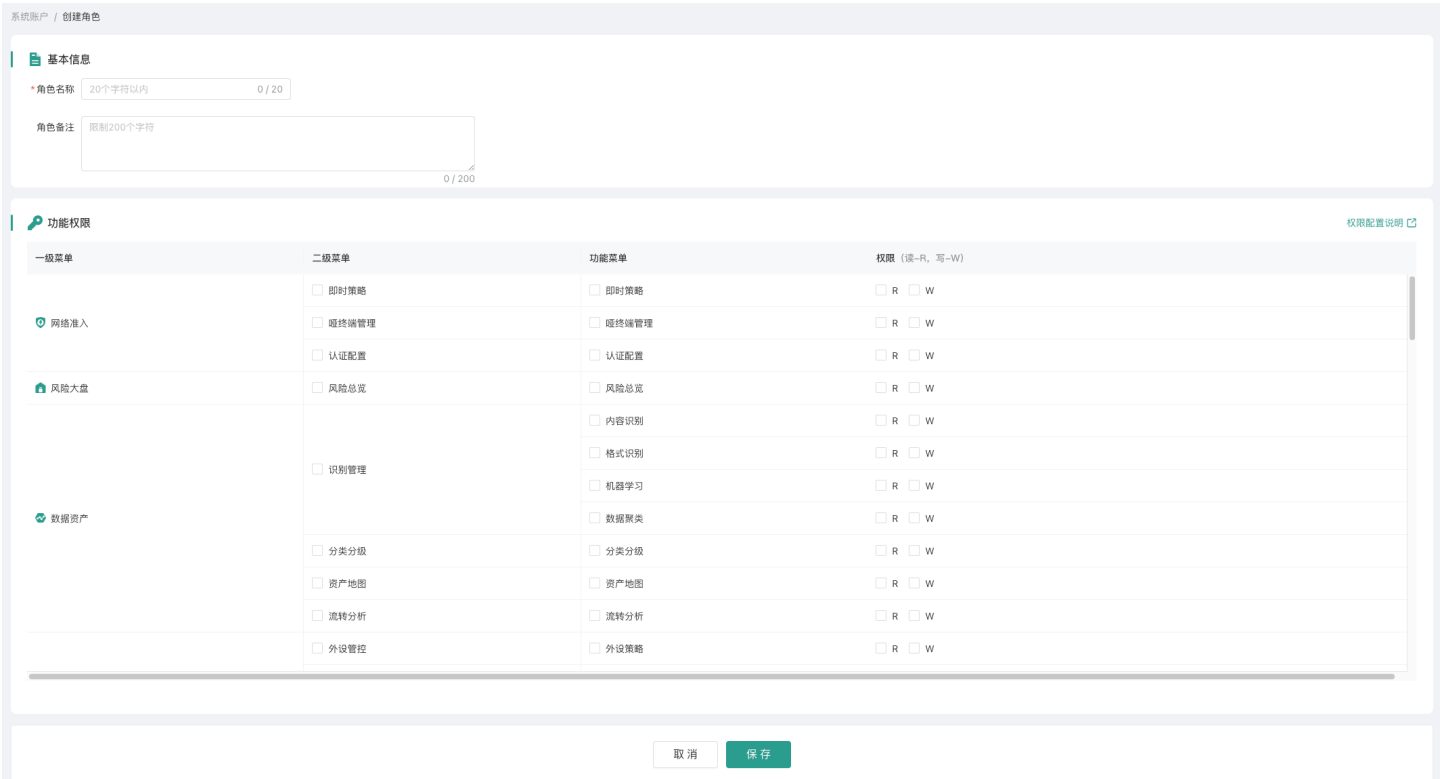
角色列表显示了您已经创建的所有角色，以及角色分别被赋予的账户数。



2.5.2.2.2 新增与编辑角色

新建角色需填写角色的基本信息，包括角色名称和角色备注。

需要为角色分配功能权限，包括对于不同菜单的读、写权限。

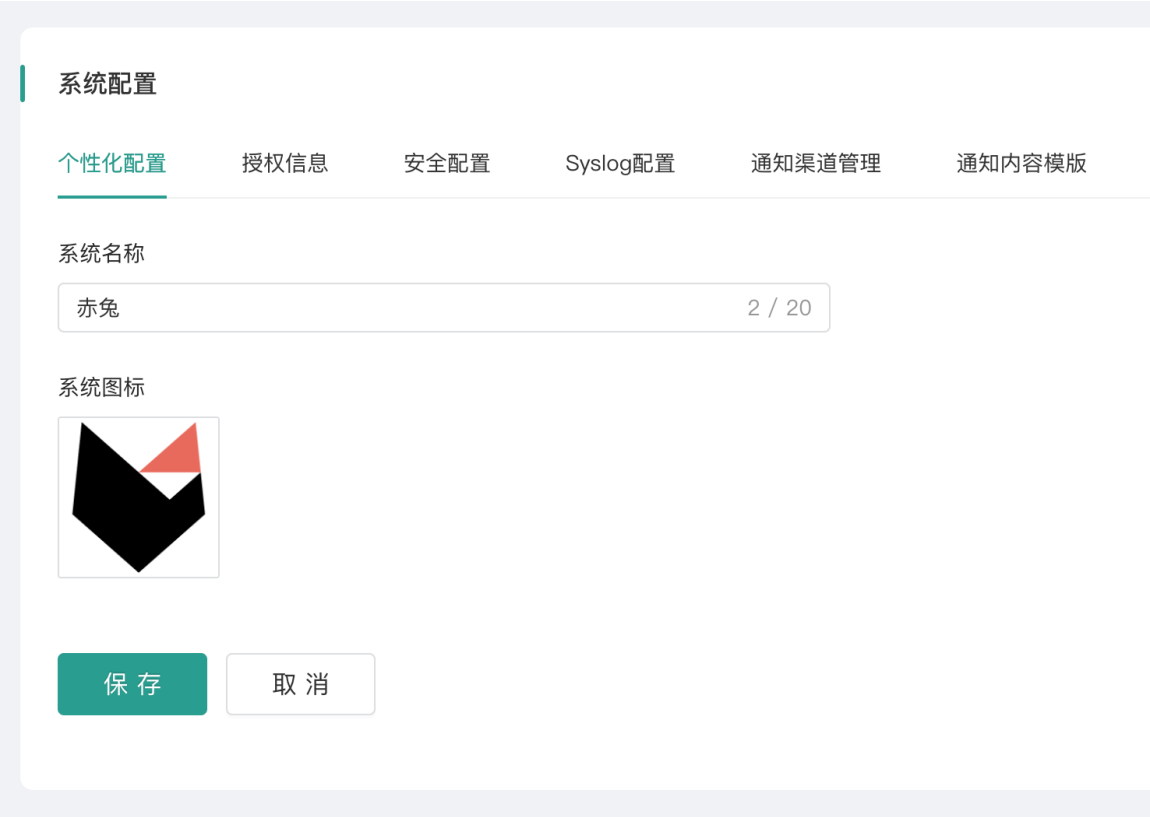


2.6 系统管理

2.6.1 系统配置

2.6.1.1 个性化配置

个性化配置可修改系统名称和和系统图标，包括主界面右上角名称、系统登录界面登录框名称等。



2.6.1.2 🆕 授权信息

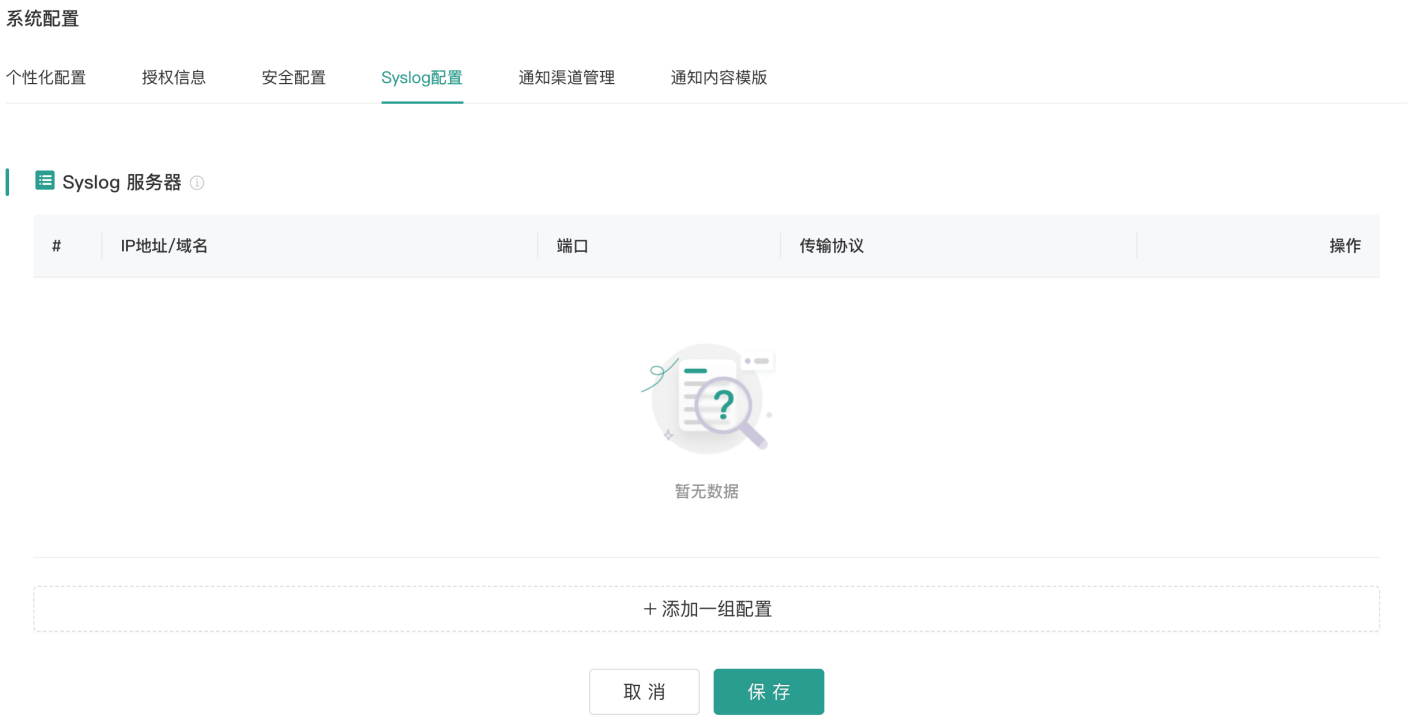
授权信息为杭州薮猫科技为产品制作 License 信息，当 License 过期或者需要续约时，可点击重新上传。复制/下载授权码文件后，将授权码文件递交给售后服务人员，获取最新的 License 文件，再次提交后即可更新授权信息。

2.6.1.3 安全配置

为保障系统安全，为管理账户添加了相应的安全配置。

2.6.1.4 Syslog配置

Syslog 配置页面，单击【添加一组配置】，在页面填写相应的配置信息后，保存即可完成一组 Syslog 配置。



2.6.1.5 通知渠道管理

通知渠道帮助管理员最快地获取系统内的安全告警。此处为通用设置，管理员可根据需要添加多个邮箱、IM机器人。

2.6.1.1 邮件通知

1. 选择「系统管理-系统配置-通知渠道管理」，点击「新增渠道」
2. 输入名称，选择类型为「邮件通知」
3. 填写信息

- 发送邮箱：发送通知的邮箱信息
- 用户名：发送通知的邮箱用户名（一般情况下发送邮箱和用户名信息可以保持一致）
- 密码：发送通知的邮箱密码
- 发送服务器：
  - 如果是内部邮件服务器，请联系内部人员获取配置信息
  - 飞书：smtp.feishu.cn 端口：465

    - QQ：smtp.qq.com 端口：465
    - 企业微信：smtp.exmail.qq.com 端口：465 参考文档：https://work.weixin.qq.com/help?doc_id=431&helpType=exmail
    - 钉钉企业邮箱：http://mailhelp.mxhichina.com/smartmail/detail.vm?knoId=5871700
- 端口：填入端口
- 加密：进行加密方式选择

4. 发送测试：输入一个接受邮件的地址进行测试配置的正确性
5. 保存

2.6.1.2 飞书通知

1. 选择「系统管理-系统配置-通知渠道管理」，点击「新增渠道」
2. 输入名称，选择类型为「飞书机器人」
3. 填写信息

- 参考文档：https://open.feishu.cn/document/ukTMukTMukTM/ucTM5YjL3ETO24yNxkjN
- 获取方式：确认消息推送群聊，在群聊中选择新增自定义机器人，配置完成后，复制webhook地址即可。

- webhook：填入webhook信息
- 加签：填入加签信息

4. 保存

2.6.1.3 钉钉通知

1. 选择「系统管理-系统配置-通知渠道管理」，点击「新增渠道」
2. 输入名称，选择类型为「钉钉通知」
3. 填写信息

- 参考文档：https://open.dingtalk.com/document/group/custom-robot-access
- 获取方式：确认消息推送群聊，在群聊中选择智能群助手，下拉选择新增自定义机器人，勾选加签，配置完成后，复制webhook地址即可。
- webhook：填入webhook信息

- 加签：填入加签信息

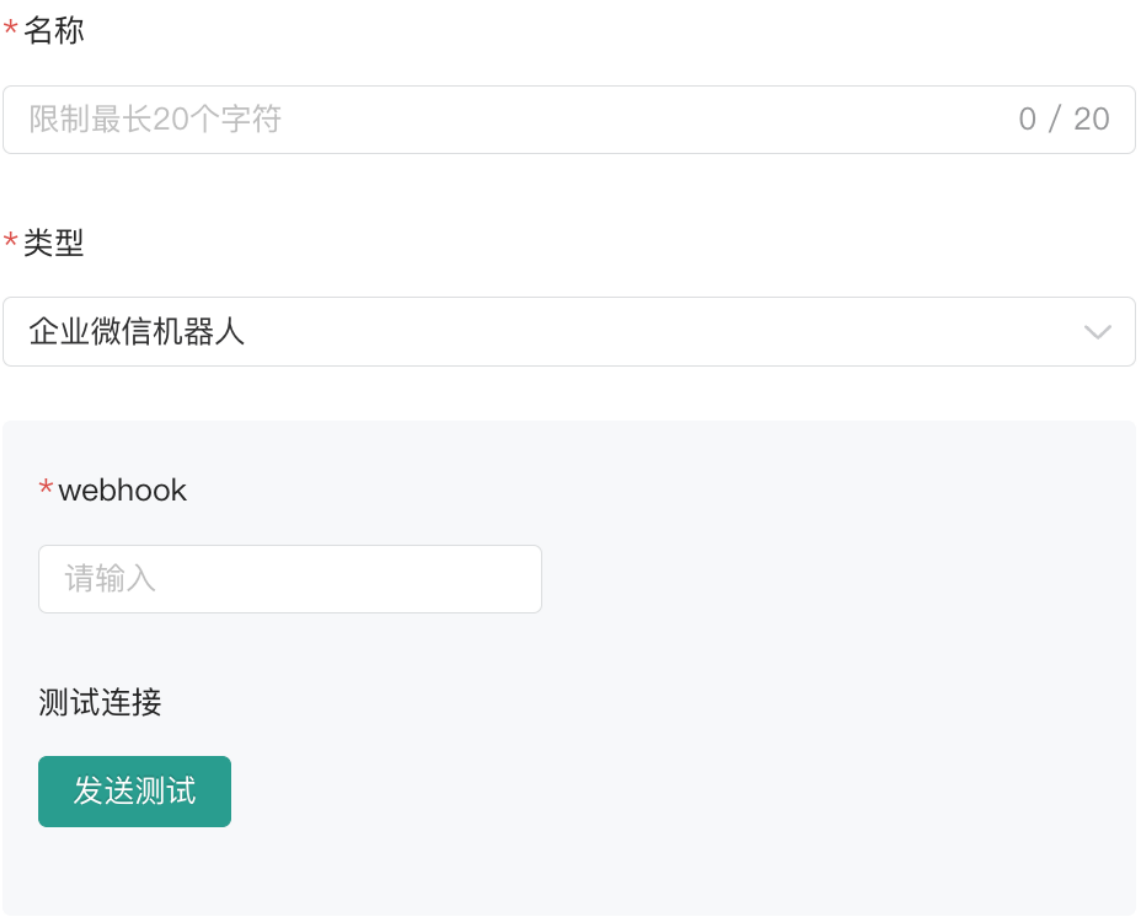
4. 保存

2.6.1.4 企业微信通知

1. 选择「系统管理-系统配置-通知渠道管理」，点击「新增渠道」
2. 输入名称，选择类型为「企业微信通知」
3. 填写信息

- 参考文档：https://developer.work.weixin.qq.com/document/path/91770
- 获取方式：确认消息推送群聊（内部群），点击右上角图标进入到群聊设置 — 进入群机器人页面，添加群机器人，设置群机器人昵称并点击添加，机器人添加完成后，复制webhook地址即可。
- webhook：填入webhook信息
- 加签：填入加签信息

4. 保存



2.6.1.6 通知内容模版

管理员可在本页面对通知内容进行模版配置。通知模板将会根据告警内容的不同，进行变量更换，实现精准告警。

新增模版

管理员填写模版名称，选择该模版对应的模块。发送内容将会根据模块选择展现不同的提示，管理员可以根据需要进行自定义。切记在自定义时，需要插入“变量”，否则告警信息将会无法有针对性的提示管理员告警的严重性。

2.6.2 系统日志

2.6.2.1 管理员操作日志

任何管理员的操作均在此处进行日志记录，以便于后续追溯审计。

请选择管理员

#	创建时间	管理员	角色	IP	行为
1	2023-03-13 16:27:50		超级管理员	192.168.88.146	用户管理-系
2	2023-03-13 16:21:21		管理员	192.168.89.53	策略中心-资扫2_16786956
3	2023-03-13 16:11:26		管理员	192.168.88.45	策略中心-资试_167866626
4	2023-03-13 16:11:04		管理员	192.168.88.45	策略中心-资试_167866626
5	2023-03-13 16:10:53		管理员	192.168.88.45	数据资产-分
6	2023-03-13 16:10:36		管理员	192.168.88.45	数据资产-识
7	2023-03-13 16:08:44		管理员	192.168.88.139	策略中心-资机号正则回归)
8	2023-03-13 16:08:31		管理员	192.168.88.139	策略中心-资归01_6786652
9	2023-03-13 16:08:22		管理员	192.168.88.51	策略中心-自(fa1eb1cd-bc5
10	2023-03-13 16:08:11		管理员	192.168.88.51	策略中心-自(a5463668-02

共2125条 < 1 2 3 4 5 ••• 213 > 10 条/页 跳至 页

2.6.2.2 系统登录日志

任何角色的管理员在登录系统时，均在此处进行日志记录。

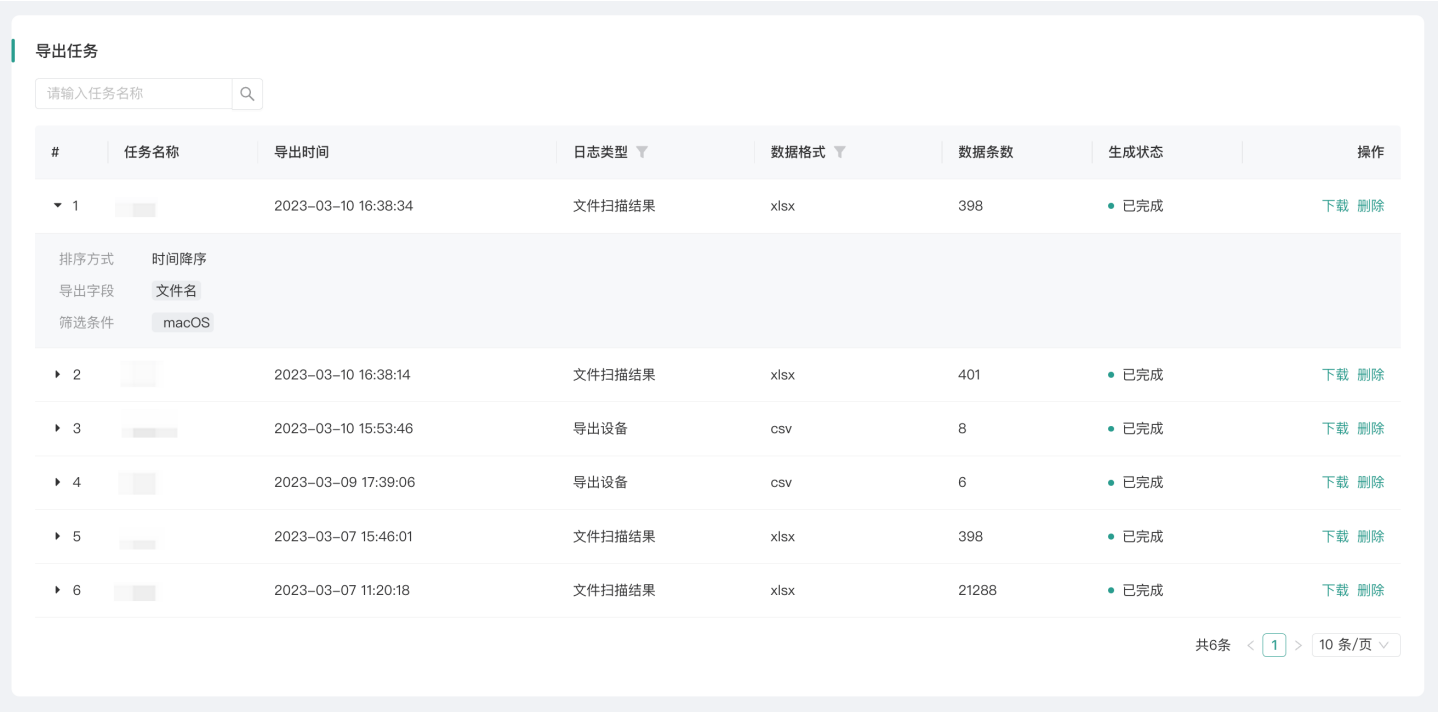
请选择管理员

#	创建时间	管理员	角色	IP	行为
1	2023-03-13 16:30:26		管理员	192.168.89.30	--登录
2	2023-03-13 16:29:56		管理员	192.168.89.30	--登录
3	2023-03-13 16:27:05		超级管理员	192.168.88.146	--登录
4	2023-03-13 16:26:59		管理员	192.168.88.146	用户管理-系统账户-登出
5	2023-03-13 16:00:40		管理员	192.168.89.30	策略中心-资产发现---登录
6	2023-03-13 15:59:23		管理员	192.168.88.251	--登录
7	2023-03-13 15:43:47		管理员	192.168.89.53	数据资产-识别管理-内容识别-登录
8	2023-03-13 15:43:42		超级管理员	192.168.89.53	数据资产-识别管理-内容识别-登出
9	2023-03-13 15:43:39		超级管理员	192.168.89.53	--登录
10	2023-03-13 15:42:23		管理员	192.168.89.53	数据资产-资产地图-登出

共621条 < 1 2 3 4 5 ••• 63 > 10 条/页 跳至 页

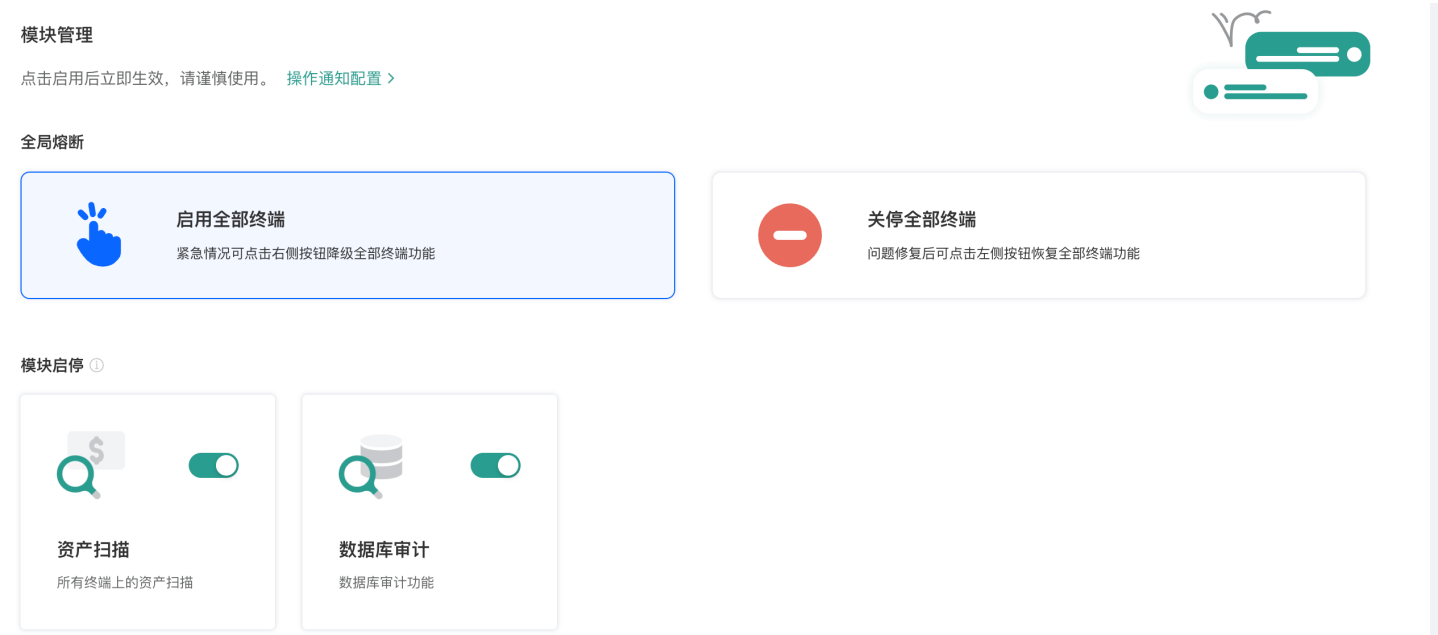
2.6.3 导出任务

系统为管理员提供了相应的数据导出功能，管理员可进入风险行为日志/行为日志分析/资产发现结果页面，根据需要将数据进行配置导出，显示内容支持管理员自定义。

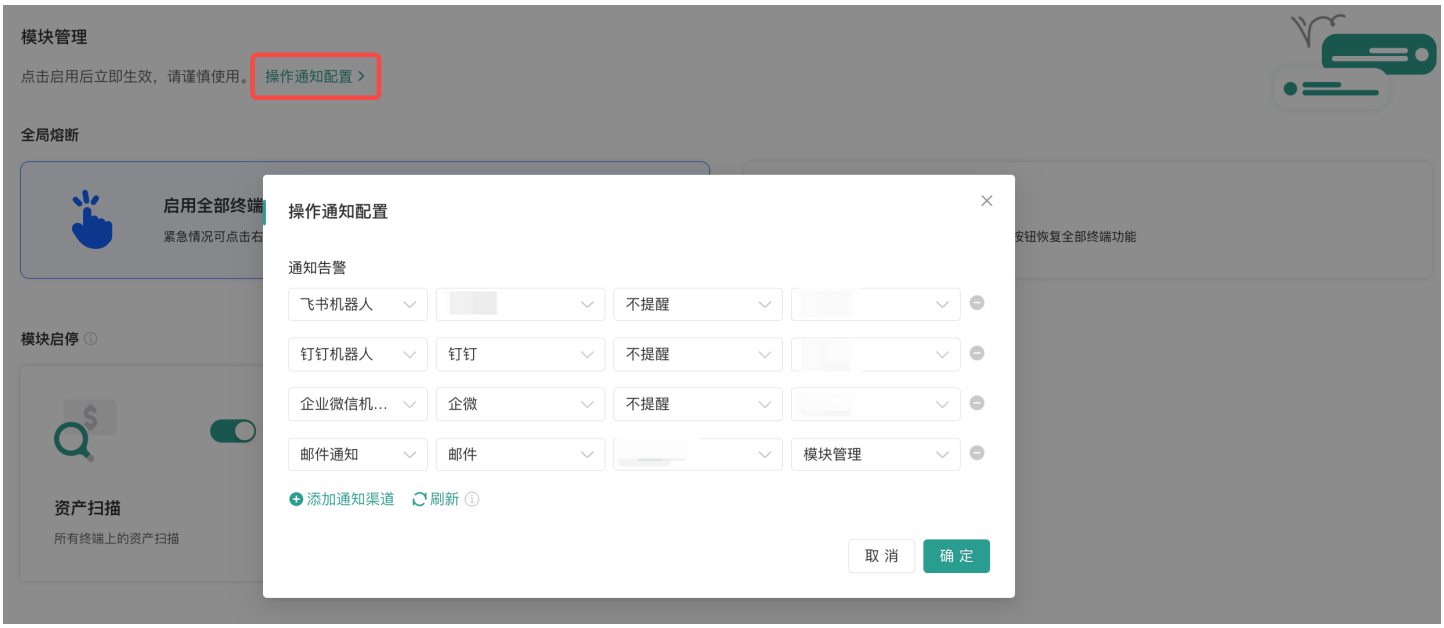


2.6.4 模块管理

当遇到特殊极端情况时，管理员可通过稳定性开关一键启停Agent。也可以针对部分模块功能进行启停。



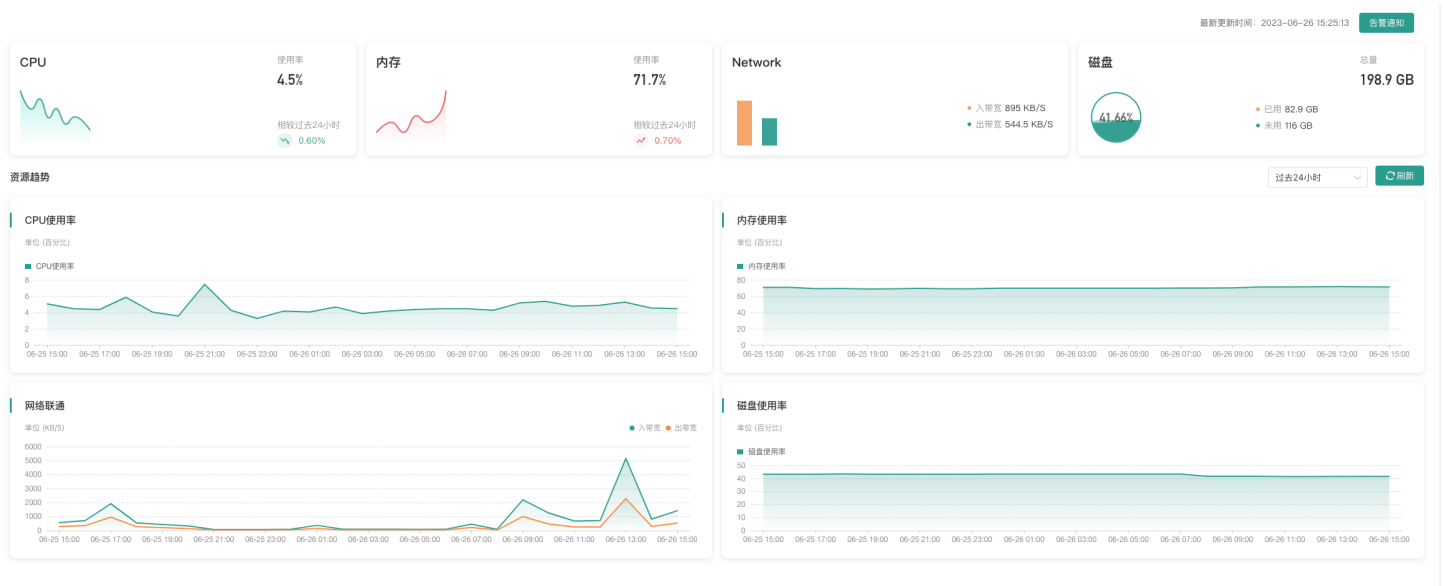
管理员可点击「操作通知配置」，配置开关的开启/停用通知信息，实时跟踪模块启停情况。



2.6.5 NEW 运行监控

2.6.5.1 系统监控

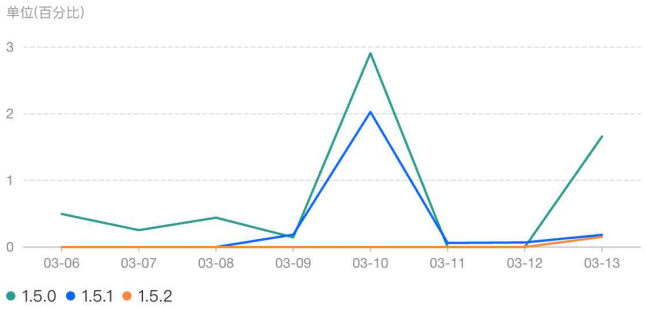
为防止服务端运行资源过载，系统为管理员提供了系统运行监控界面，支持其自定义告警通知。当系统运行过载时，系统将第一时间通知管理员进行排查。



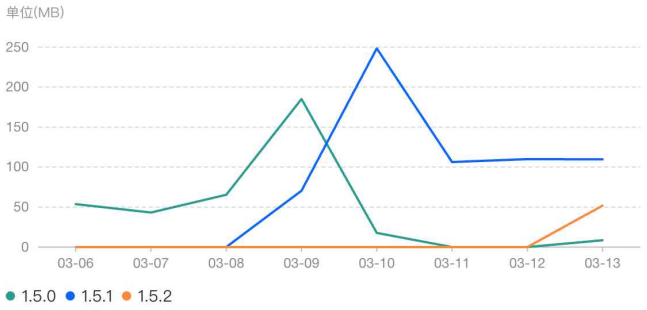
2.6.5.2 终端监控

终端运行监控，将分别统计 Windows、macOS、Linux 等操作系统上Agent分别占用的 CPU、内存的平均值。

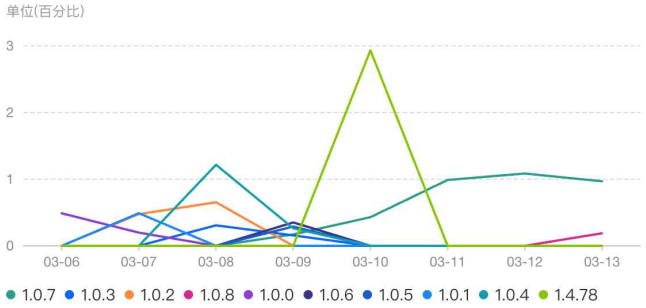
Windows 分版本平均CPU统计



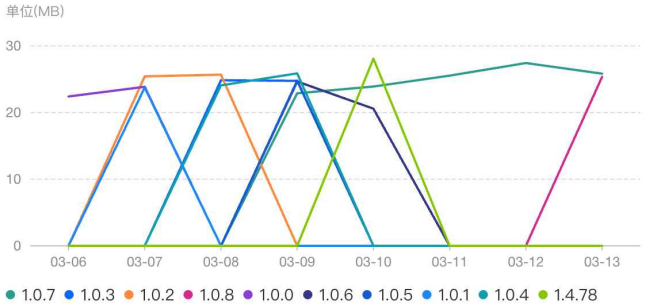
Windows 分版本平均内存统计



macOS 分版本平均CPU统计

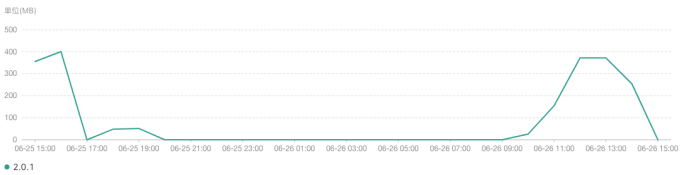


macOS 分版本平均内存统计

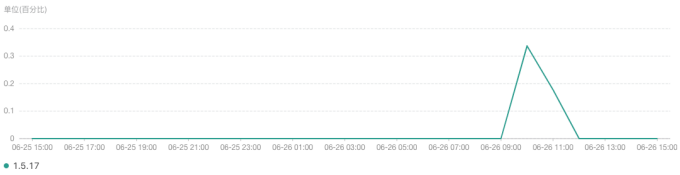


Linux 分版本平均CPU统计

Linux 分版本平均内存统计



UOS 分版本平均CPU统计



UOS 分版本平均内存统计

Kylin 分版本平均CPU统计

Kylin 分版本平均内存统计