



数据安全中心 V3.2.2

用户使用手册

目录

1	系统概述
1.1	部署方式
2	登录数据安全中心
2.1	系统管理员登录
2.2	更改密码
3	首页
4	资产管理
4.1	数据资产
4.2	分类管理
4.3	分级管理
4.4	数据识别规则
5	流转监测
5.1	数据流转测绘
5.2	合规要求
5.3	日志检索
6	风险预警
6.1	功能概述
6.2	操作步骤
7	统计报表
7.1	数据资产梳理报告
7.2	问卷评估报告
7.3	数据出境风险自评估报告
7.4	数据流转统计报表
8	知识库
8.1	IP 地址库
8.2	特征信息库
9	平台管理

9.1 基础设置.....

9.2 账号管理.....

9.3 平台运维.....

9.4 操作审计.....

9.5 角色管理.....

9.6 账号审核.....

9.7 安全配置.....

1 系统概述

1.1 概述

在数字经济发展的今天，数据作为新的关键生产要素，数据不仅仅是企业/组织内部资产，只有实现在更大范围内的流动共享，才能更好地发挥对产业发展、经济增长、社会进步、全球化进程的支撑推动作用。

数据在企业组织内外部流转过程中的安全问题已成为数据安全建设的一个新课题。随着《数据安全法》、《个人信息保护法》、《数据出境安全评估办法（征求意见稿）》等法规相继出台，数据流转监测的需求将会不断增加，本产品着重数据出境相关功能就是流转监测中最新的一个场景。闪捷数据流转监测系统以数据安全产品为锚，利用产品已有能力，采集不同类型的数据流转信息（如数据出入境、内部部门间流转等不同数据流转场景），覆盖结构化、非结构化、半结构化等不同类型数据，统一汇聚至数据安全中心；由安全中心实时监测、统一分析，调度匹配不同安全策略与场景规则，提供数据安全风险告警、安全评估报告等，如数据出境安全自评估、金融数据流转监测或针对不同行业要求的数据安全监测与评估。

1.2 部署方式

数据安全中心产品功能如下：

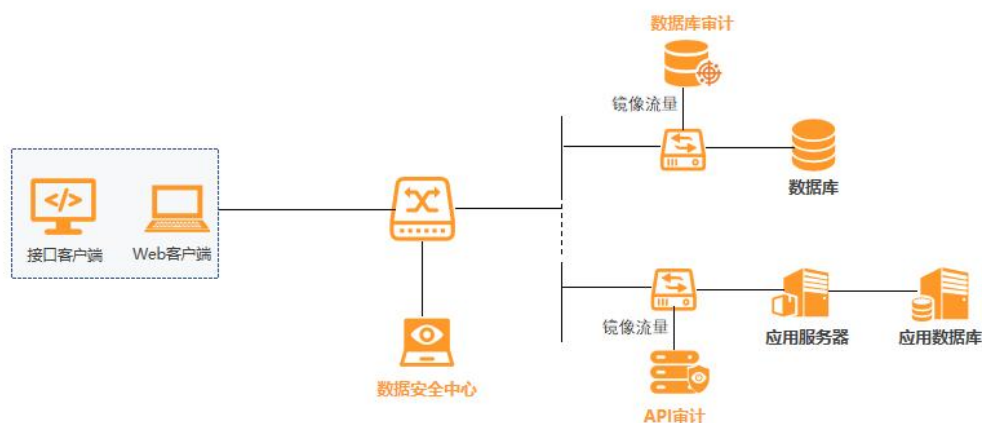


图 1-1 组网图

2 登录数据安全中心

2.1 系统管理员登录

浏览器中输入 URL: https://服务器 IP 地址 (如: https://xxx.xxx.xxx.xxx:9443), 进入数据安全中心登录页面, 输入用户名、密码, 点击“登录”按钮, 进入管理界面, 如图 2.1-1 所示。

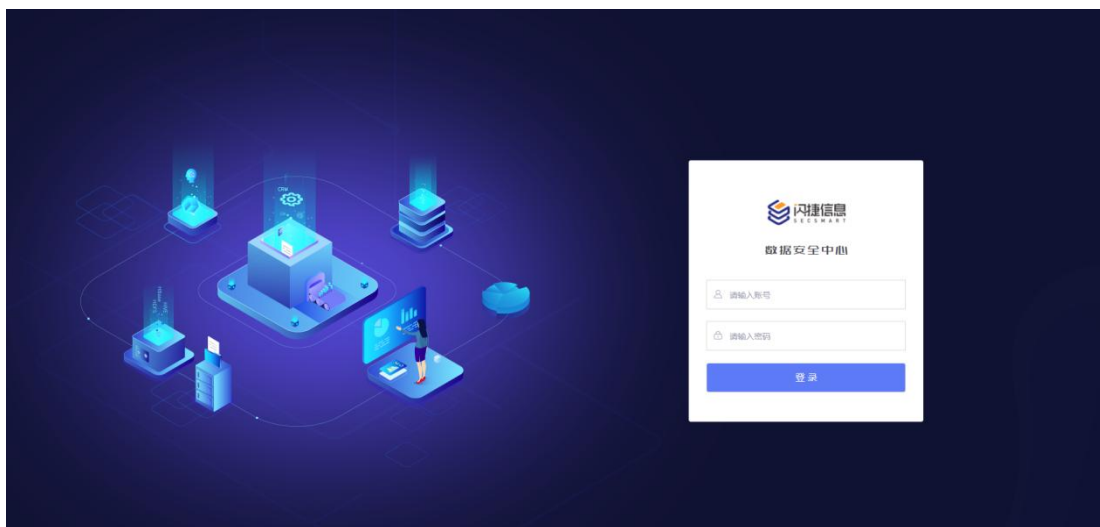


图 2.1-1 登录页面

2.2 更改密码

系统管理员 (sysadmin) 登录数据安全中心, 在主界面右上方点击登录的账户下拉框选择“修改密码”菜单, 如图 2.2-1 所示, 进入更改密码功能界面, 如图 2.2-2 所示。输入原密码、新密码、确认密码, 点击“确定”按钮, 可成功修改密码, 也可点击“取消”按钮, 取消修改操作。

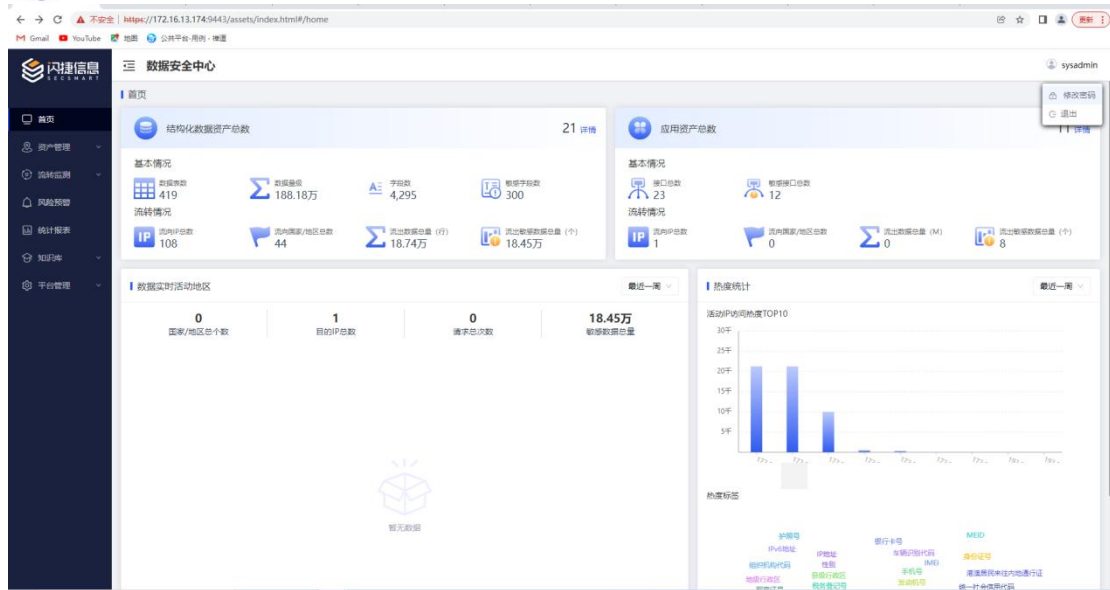


图 2.2-1 下拉框修改密码



图 2.2-2 修改密码界面

3 首页

系统管理员（sysadmin）登录数据安全中心，进入数据安全中心首页，用于查看统计概况，如数据资产的存储情况、流转情况等，查看相应的风险以及数据流转的地区统计等，界面布局如图 3.1-1 和图 3.1-2 所示。



图 3.1-1 数据安全中心首页

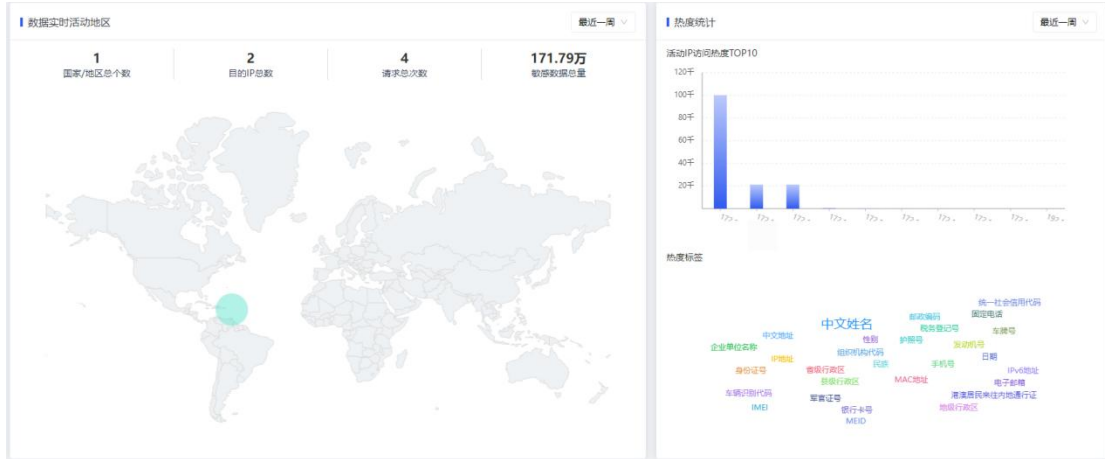


图 3.1-2 数据安全中心首页

功能点说明

数据资产概览

可查看对应数据资产的概况，点击详情可以以列表的形式显示数据库、应用资产全部信息。

基本情况

- a)数据表数：已经扫描到的表总数
- b)数据量级：已经扫描到的表的总行数
- c)字段数：已经扫描到的字段（列）数量
- d)敏感字段数：被已经在敏感数据地图-敏感数据定义中设置为敏感数据的数据识别规则命中的字段（列）数量

e)接口总数：已经扫描到的接口总数

f)敏感接口总数：已经扫描到的敏感接口总数

流转情况

a)流向 IP 总数：统计当前所选数据资产所有数据流向的目的 IP 的总和

b)流向国家/地区总数：统计当前所选数据资产所有数据流向的目的 IP 的所

属国家/地区总和

- c)流出数据总量：统计所有与当前所选资产相关联的，以所选资产的 IP 为
- d)源 IP 的数据总行数：数据库统计行数，应用统计包数。
- e)流出敏感数据总量（条）：统计敏感数据总量。

风险概览

统计当前存在的告警数，并提供快捷入口

数据实时活动地区

（以下统计都是基于数据流转过程）

国家/地区总个数：指定时间内所有目的 IP 的所属国家的总和

目的 IP 总数：指定时间内所有目的 IP 的总和

请求总次数：指定时间内所有目的 IP 的请求次数总和

敏感数据总量：指定时间内所有敏感数据量的总和

热度统计

a)活跃 IP 访问热度 top10

指目的 IP 中请求次数最多的前 10 个

b)热度标签

特征项出现的频率排行

4 资产管理

4.1 数据资产

4.1.1 功能概述

数据出境合规要求中包括存储数据信息，本模块主要针对数据资产的管理，通过同步数据库审计的结构化数据与 API 审计的应用数据，统筹结构化数据与 API 应用存储数据的发现与管理。

4.1.2 应用管理

添加应用

登录数据安全中心，进入【流转监测】-【应用管理】页面，界面布局如图 4.1-1 所示。点击添加应用，弹出添加应用弹窗，如图 4.1-2 所示。这里添加的应用仅为应用数据安全审计系统与数据库审计系统这两个产品，且已进行单点登录功能的适配。



图 4.1-1 应用管理页面

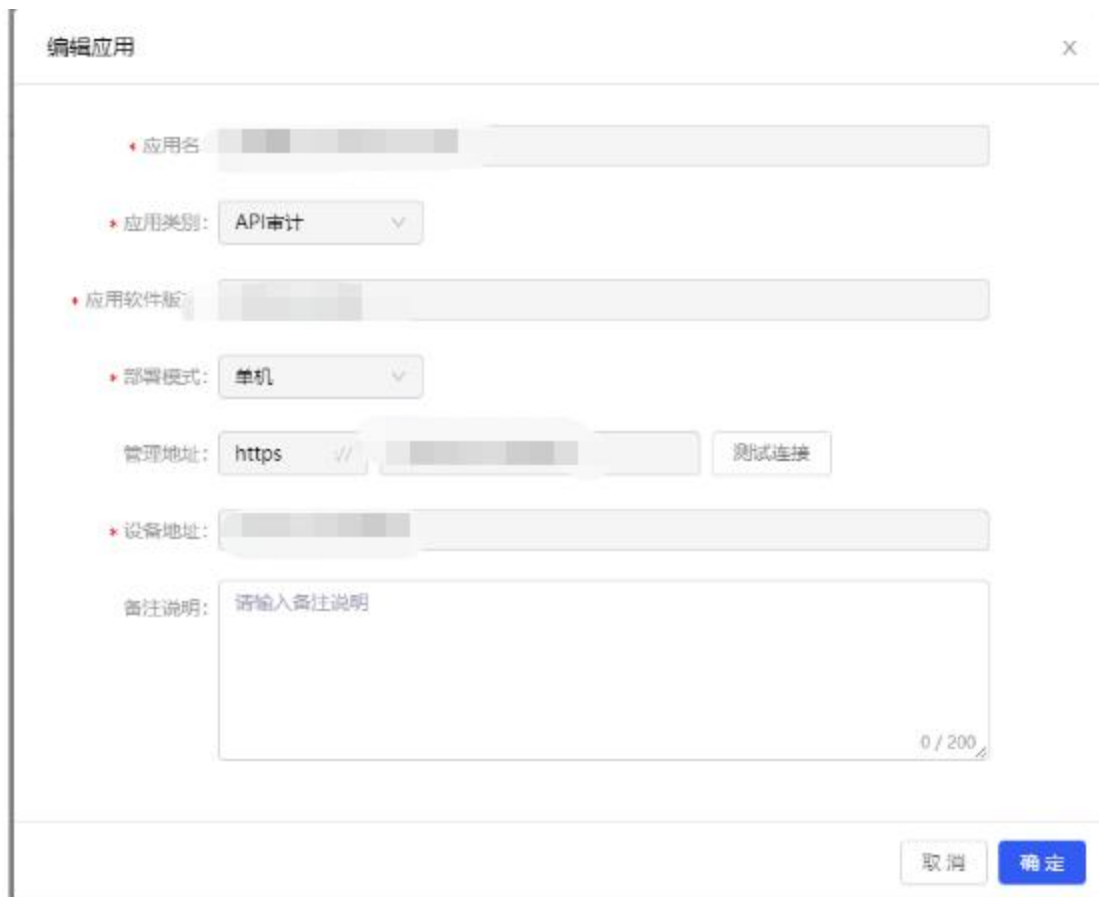


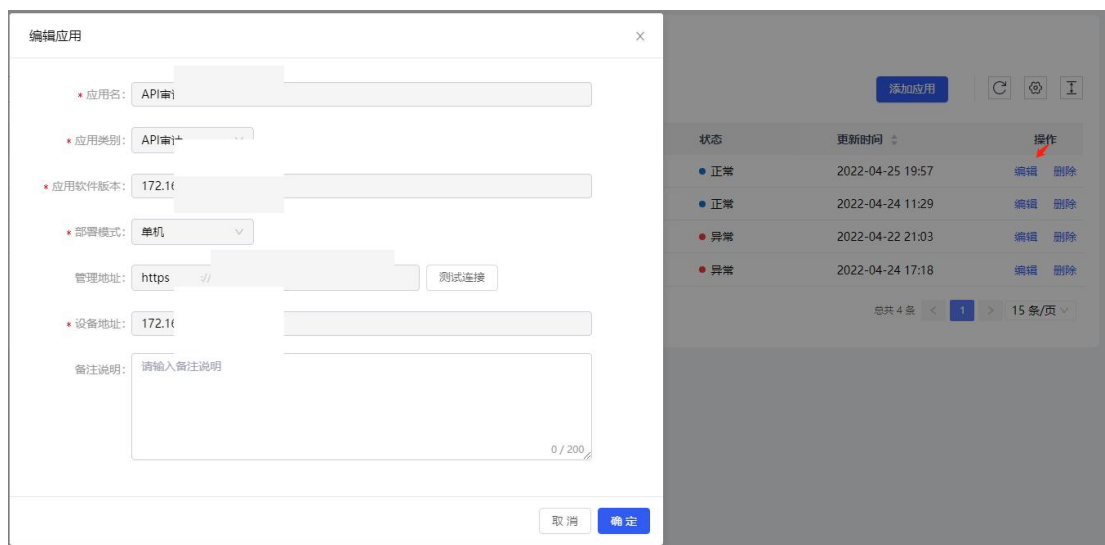
图 4.1-2 添加应用弹窗

- 1) 应用名：自定义应用名称
- 2) 应用类别：对应应用的类别可选项，所添加应用的类别：数据库审计、API 审计
- 3) 应用软件版本：应用对应的版本号
- 4) 部署模式：应用的部署模式，可选择单机、双机、集群三种模式
- 5) 管理地址：应用访问地址，ip+端口
- 6) 设备地址：设备的 ip 地址，输入时应加上对应端口号，如部署模式为双机或集群，应用英文逗号隔开
- 7) 备注说明：应用的备注

数据安全设备列表中，设备状态为：正常时，点击应用名称即可单点登录至对应的平台,账号权限取决于平台登录的账号对应的平台账号。当数据库审计环境出现问题或者资产管理配置有误，设备状态显示异常。

编辑应用

应用添加完成后会显示在页面中，点击需要修改的应用对应的编辑按钮，即可进入应用编辑页面，如图 4.1-3 所示，编辑完成后，点击“确定”完成编辑，点击“取消”则取消编辑。


图 4.1-3 应用编辑页面

删除应用

应用添加完成后会显示在页面中，选择需要删除的应用，点击删除按钮，即进入删除页面，如图 4.1-4 所示，点击“确定”，若所添加应用产品已添加资产，需要将审计产品资产全部删除才可以删除该条应用，点击“取消”则取消删除此应用。

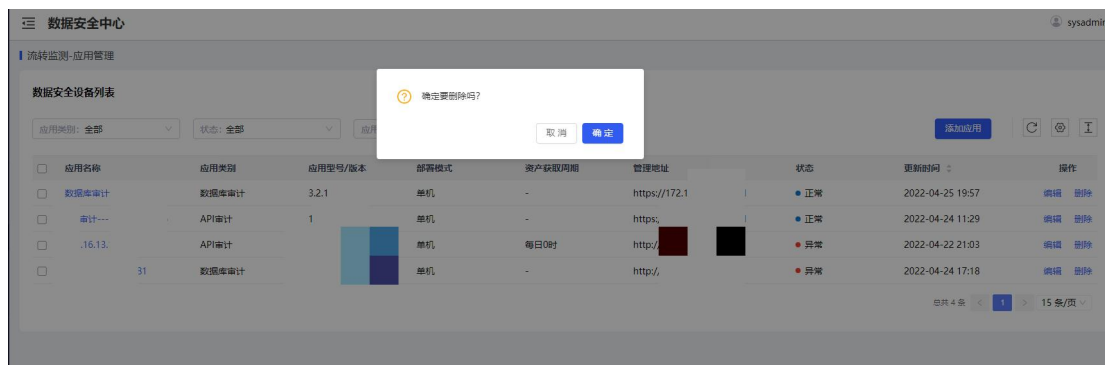


图 4.1-4 应用删除页面 1



图 4.1-5 应用删除页面 2

4.1.3 资产同步

以数据库审计资产为例：打开【流转监测】-【应用管理】页面，数据安全设备列表中，通过单点登录的方式进入数据库审计平台。如图 4.1-6



图 4.1-6 通过单点登录进入数审界面

在数据库审计平台添加数据库资产（数据库审计操作可查看数据库审计应用手册），返回数据安全中心【资产管理】-【数据资产】页面，默认进入结构化数据页面，点击“资产获取”得到如图 4.1-7 弹出框，选择资产获取的地址与方式。

★资产获取地址：数据库审计设备地址

★资产获取方式：1.立即获取 2.周期获取(每日 0 时)

若资产获取的方式为：立即获取，则在结构化数据资产列表中可以显示数据库审计系统中所添加的资产且同步状态显示：同步中，如图 4.1-8。若数据库审计环境出现异常或资产管理配置有误，同步状态显示：失去同步。

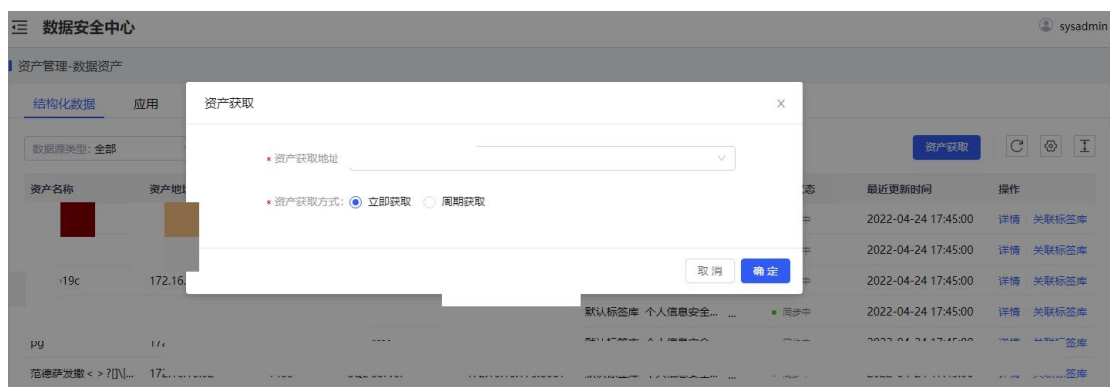
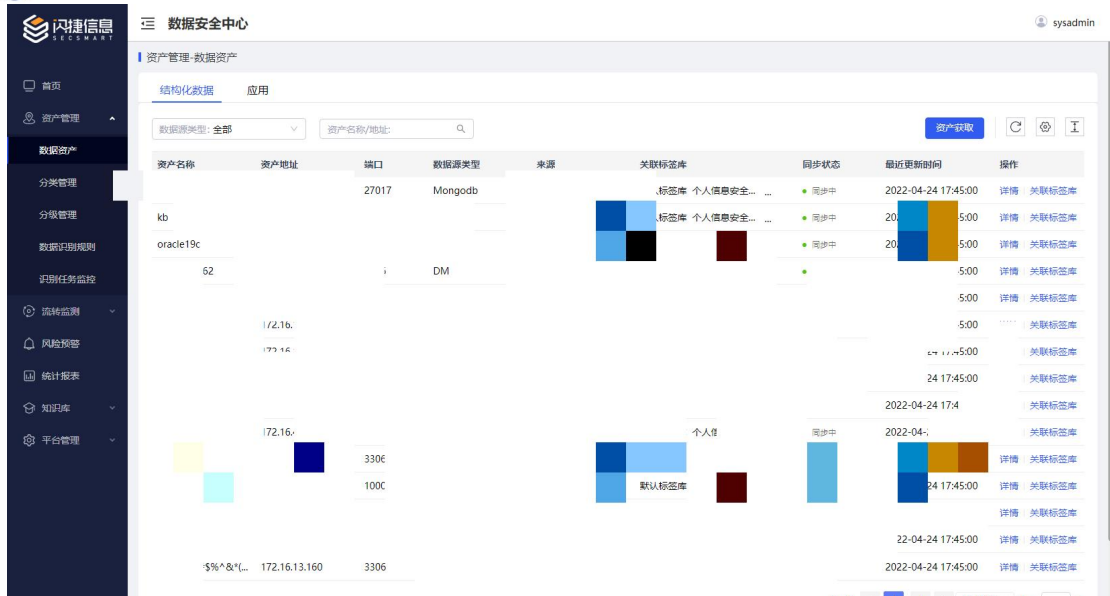


图 4.1-7 获取数据库审计资产信息



资产名称	资产地址	端口	数据源类型	来源	关联标签库	同步状态	最近更新时间	操作
kb		27017	Mongodb		标签库 个人信息安全...	同步中	2022-04-24 17:45:00	详情 关联标签库
oracle19c					标签库 个人信息安全...	同步中	2022-04-24 17:45:00	详情 关联标签库
	62	i	DM			同步中	2022-04-24 17:45:00	详情 关联标签库
	172.16.13.160					同步中	2022-04-24 17:45:00	详情 关联标签库
	172.16.13.160					同步中	2022-04-24 17:45:00	详情 关联标签库

图 4.1-8 结构化数据资产列表

结构化-数据库表详情页面查看

点击详情可以查看数据库中表信息，包括表名称、数据量级、数据分类、数据分级，最近更新时间，如图 4.1-9 结构化数据资产列表详细信息。

详情页面查看

表详情里点击操作列下的“详情”图标，进入详情页面，如图 4.1-10 所示。页面显示数据库表的字段信息，包括字段名称、数据类型、数据长度、字段注释、数据分类和数据分级。

表名称	数据层级	数据分类	数据分级	最近更新时间	操作
columns_priv	0	未分类		2022-04-22 21:10	详情
db	0	未分类		2022-04-22 21:10	详情
event	0	未分类		2022-04-22 21:10	详情
func	0	未分类		2022-04-22 21:10	详情
general_log	0	未分类		2022-04-22 21:10	详情
help_category	47	未分类		2022-04-22 21:10	详情
help_keyword	825	未分类		2022-04-22 21:10	详情
help_relation	1660	未分类		2022-04-22 21:10	详情
help_topic	603	未分类		2022-04-22 21:10	详情
innodb_index_stats	0	未分类		2022-04-22 21:10	详情
innodb_table_stats	0	未分类		2022-04-22 21:10	详情
ndb_binlog_index	0	未分类		2022-04-22 21:10	详情
new	6	个人电话号码 IP地址0		2022-04-22 21:10	详情
plugin	0	未分类		2022-04-22 21:10	详情
proc	0	未分类		2022-04-22 21:10	详情

图 4.1-9 结构化数据资产列表详细信息

字段名称	数据类型	数据长度	字段注释	数据分类
home	tinytext	255		未分类
name	text	65535	111	未分类
phone	varchar	255	个人电话号码0	未分类
ip	varchar	255	IP地址0	未分类
id	varchar	255	11111111111111111111...	未分类

图 4.1-10 数据库表详细信息

切换至数据样例页面，命中分类标签和分级标签的字段显示前 5 行数据，如图 4.1-11 所示

详情 ×

🔍

字段名	样例数据1	样例数据2	样例数据3	样例数据4	样例数据5
home	z**ng	be**ng	sha****hai	zhe*****ang	sha*****ong
name	s*n	l*u	z**ng	s*n	w*
phone	177*****287	188*****767	198*****176	198*****163	188*****392
ip	192*****3.1	176*****0.1	172*****1.1	192*****2.1	192*****1.1
id	1	2	3	4	5

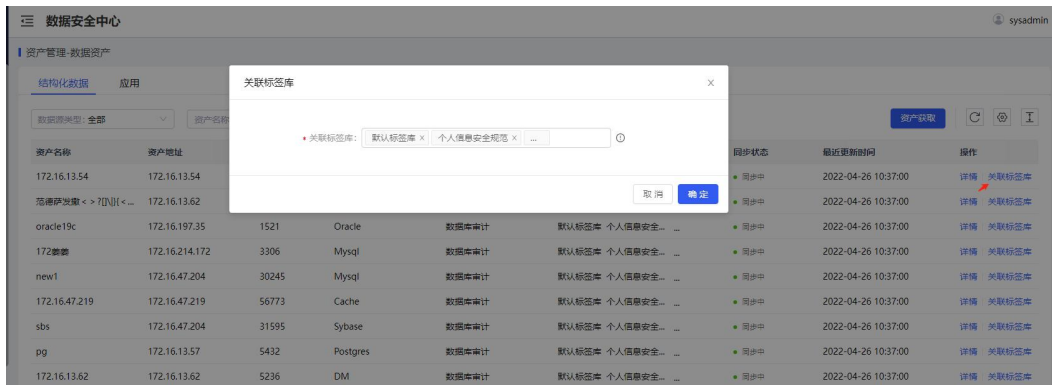
总共 5 条 < 1 > 10 条/页

图 4.1-11 详情-数据样例页面

切换至建表语句页面，读取数据表的创建语句。切换至变更历史页面，记录数据库字段新增和删除情况。

关联标签库

若存储数据为结构化数据，则可以通过关联标签库的方式对数据库审计中存储的敏感数据资产打上标签。从数据库审计系统同步过来的资产默认关联全部标签库。这里的标签库可以通过【资产管理】-【分类管理】分类标签列表进行更新，更新方法详见 4.2 节分类管理。



资产名称	资产地址	资产类型	同步状态	最近更新时间	操作
172.16.13.54	172.16.13.54	数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
范德萨发童 < > 7[D][[< ...	172.16.13.62	数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
oracle19c	172.16.197.35	1521 Oracle 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
172数据库	172.16.214.172	3306 Mysql 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
new1	172.16.47.204	30245 Mysql 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
172.16.47.219	172.16.47.219	56773 Cache 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
sbs	172.16.47.204	31595 Sybase 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
pg	172.16.13.57	5432 Postgres 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库
172.16.13.62	172.16.13.62	5236 DM 数据库审计	同步中	2022-04-26 10:37:00	详情 关联标签库

4.2 分类管理

4.2.1 功能概述

分类管理页面可以进行分类标签库和分类标签的管理，添加后的分类标签

可用于数据识别规则设置，通过分类实现对数据的不同标识。分类标签库和分类标签均支持添加、编辑、删除及导入操作。

4.2.2 操作步骤

创建

进入分类管理页面，如图 4.2-1 所示。点击添加分类标签库按钮，进入创建标签库页面填写标签库名称、标签说明，点击“确定”即可创建标签库。

- 1) ★标签库名称：必填项，自定义标签库的名称
- 2) 关联数据源：非必选项，选择关联的数据源。默认关联全部
- 3) ★顺序：必填项，0-99。标签库显示的优先顺序，顺序小的显示在前面。
- 4) 状态：启用和停止。

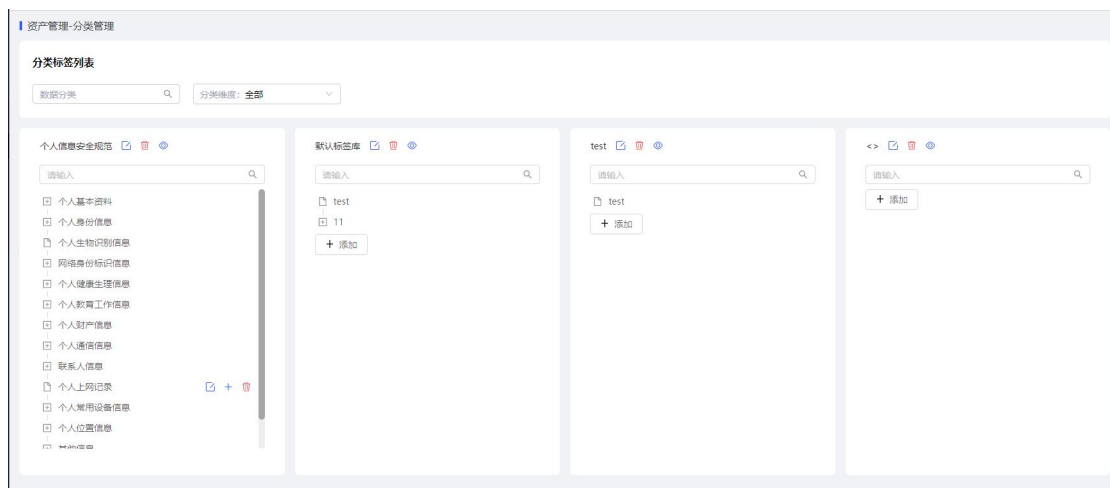


图 4.2-1 分类管理页面

点击标签库下的添加按钮，进入创建分类标签页面，填写标签库名称、标签说明，点击“确定”即可创建标签。将鼠标移动到标签库中的分类标签上，点击后方的“+”添加子级标签。最多允许添加三级分类标签，三级标签后不再显示图标“+”。

- 1) ★标签名称：必填项，自定义标签的名称
- 2) ★建议安全级别：选填项，该分类标签推荐的分级级别名称

标签库详情

点击已添加标签库右上角的详情图标，弹窗显示标签库详情页面。详情页面从左到右依次显示 1 级到 3 级的分类标签名称，数据分级则显示最低一级分类标签的数据分级。

编辑

支持标签库和标签信息修改。分类标签的数据分级和标签库的关联数据源修改后，相关的打标标签重新扫描后更新。

删除

可通过删除按钮，删除标签库和标签。存在标签的标签库和存在子标签的标签不允许删除。

导入

点击导入分类标签库按钮，进入导入分类标签页面，下载维度标签模板后，严格按照模板填写标签库信息。填写完成后，点击“选择文件”按钮并选择对应的文件，点击“确定导入”按钮，完成导入。

4.3 分级管理

4.3.1 功能概述

分级管理页面可进行分级标签的编辑操作，分级标签可用于数据扫描规则设置。实现不同等级的数据标记不同的分级标识。

编辑分级标签

进入分级标签页面，如图 5.2-1 所示。点击“编辑”按钮，进入创建分级标签页面。填写规则名称、选择规则定义、标签颜色、规则权重值、填写规则说明，点击“确定”即可创建分级标签。

- 1) ★分级名称：必填项，自定义分级的名称

- 2) 规则定义：非必选项，选择数据识别规则到分级规则名称后，该数据识别规则的分级即为该等级
- 3) ★规则权重：必填项，设置规则的权重值。当字段或表有两个不同的分级标签时，最终分级标签为权重高的分级标签。
- 4) ★标签颜色：必填项，设置规则的标签颜色
- 5) 建议管控策略：非必填项，输入建议的管控策略
- 6) 分级说明：非必填项，分级的补充说明信息



图 4.3-1 创建分级标签页面

编辑分级标签时可以修改全部内容。分级标签的规则定义、规则权重、标签颜色修改后，相关的打标标签重新扫描后更新。

4.4 数据识别规则

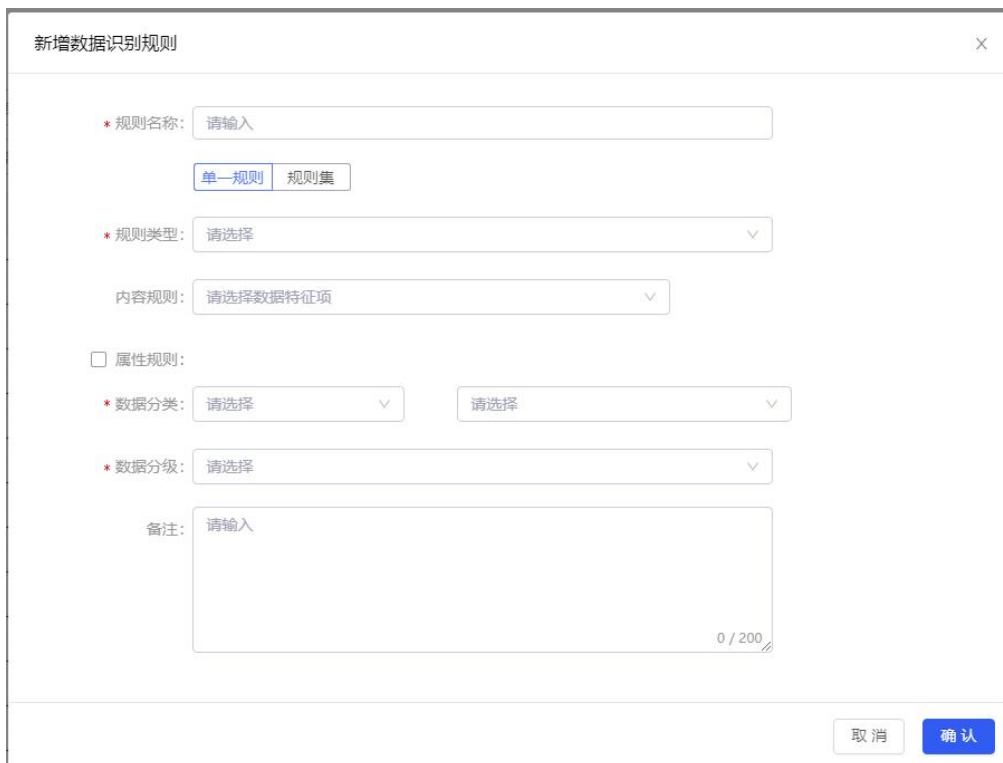
4.4.1 功能概述

数据识别规则页面可创建、修改、删除、复制数据识别规则。通过设置数据规则，可对存在的数据源资产中的特征信息进行识别。识别结果可在数据地图-资产检索页面查看。

4.4.2 操作步骤

添加

系统管理员进入【分级分类】-【数据识别】规则页面，点击“添加”按钮进入新增数据识别规则页面。选择规则类型为结构化数据，页面如图 4.4-1 所示，其中单一规则对表中的字段进行打标，而规则集可以通过多个条件对表进行打标。



新增数据识别规则

* 规则名称: 请输入

单一规则 规则集

* 规则类型: 请选择

内容规则: 请选择数据特征项

属性规则:

* 数据分类: 请选择

* 数据分级: 请选择

备注: 请输入 (0 / 200)

图 4.4-1 新增数据识别规则（单一规则）

- 1) ★规则名称：必填项，自定义规则名称
- 2) 单一规则/规则集：单选项，规则模式

- 3) ★规则类型：必填项，选择结构化数据
- 4) ★内容规则：非必填项，选择内容规则（即特征项）。特征项必须包含在特征信息类别中才能被选择
- 5) ★命中率：必填项，仅选择结构化数据类时显示。数据库中某一列的特征数据条数大于等于表行数*命中率，该列为命中状态
- 6) 测试：输入测试内容验证能否被内容规则命中。可用于检查内容规则的准确性。仅结构化数据类型支持
- 7) 属性规则：非必填项（勾选后为必填项，仅结构化数据类支持）。支持设置表名称、表注释、数据源（名称和 IP）、表字段的属性规则。设置后数据识别规则仅对满足属性规则的表进行识别。如果添加多个属性规则则需要同时满足
- 8) ★数据分类：必选项，选择分类管理中的标签库和分类标签
- 9) ★数据分级：必选项，选择分级管理的分级标签
- 10) 备注：非必填项，备注说明

字段分类分级

通过【数据资产】-【结构化资产】，可以发现数据库表中的敏感数据根据数据识别规则打上了字段标签，如图 4.4-2，分级显示所有敏感数据中级别最高的分级。



数据源	数据分类	数据分级	最后更新时间	操作
0	未分类		2022-04-25 20:07	详情
0	未分类		2022-04-25 20:07	详情
0	未分类		2022-04-25 20:07	详情
0	未分类		2022-04-25 20:07	详情
general_log			2022-04-25 20:07	详情
help_category	帮助		2022-04-25 20:07	详情
help_keyword	帮助		2022-04-25 20:07	详情
help_relation	帮助		2022-04-25 20:07	详情
help_topic	帮助	1	2022-04-25 20:07	详情
innodb_index_stats	帮助	1	2022-04-25 20:07	详情
innodb_table_stats	帮助	1	2022-04-25 20:07	详情
syslog	帮助	0	2022-04-25 20:07	详情
syslog	帮助	6	2022-04-25 20:07	详情

图 4.4-2 数据资产打上字段标签

新增数据识别规则页面点击规则集，切换至规则集模式，如图 4.4-3 所示。通过点击规则编辑器上的属性规则、内容规则添加条件，默认前置条件为 AND。前置条件可选择 AND 或 OR。选中规则后可以删除、增加条件和拆分条件

操作。



新增数据识别规则

单一规则 规则集

规则编辑器

属性规则 内容规则 删除 增加条件 拆分条件

* 数据分类: 请选择

* 数据分级: 请选择

备注: 请输入

0 / 200

取消 确认

图 4.4-3 新增数据识别规则（规则集）

添加成功的数据识别规则默认为开启状态。关闭后扫描时将不执行对应的数据识别规则。开启或关闭识别规则，均在重新扫描时生效。

表分类分级

通过【数据资产】-【结构化资产】，可以发现数据库表中的敏感数据根据数据识别规则打上了表标签，如图 4.4-4。

资产管理-结构化资产-详情

返回

结构化资产列表

表名称:

● 表标签 (生日00)
● 字段标签 未分类

表名称	数据层级	数据分类	数据分级	最近更新时间
priv		生日00	S3	2022-04-26 19:59
db		生日00	S3	2022-04-26 19:59
ent		生日00		2022-04-26 19:59
rc		00		2022-04-26 19:59
neral_log	0			2022-04-26 19:59
lp_category	47			2022-04-26 19:59
...word	000			2022-04-26 19:59
tion				2022-04-26 19:59
c				2022-04-26 19:59
index_stats				2022-04-26 19:59
line	ats	0	00 个人	2022-04-26 19:59
nd	ex	0	00	2022-04-26 19:59
new	6		300 IP地址00	2022-04-26 19:59
plugin	0	生日00	S3	2022-04-26 19:59

图 4.4-4 数据资产打上表标签

删除

通过删除按钮，可以删除数据识别规则。删除识别规则并重新扫描后，字段和表的打标标签不再显示。

编辑

数据识别规则仅支持规则名称和备注修改，且支持对结构化数据类的内容规则进行测试。规则名称修改后，相关的打标标签重新扫描后更新。

拷贝

点击拷贝图标，进入添加数据识别规则页面，页面内容与被复制的数据识别规则一致，且全部信息都可以编辑，可实现快速添加数据识别规则。

4.4.3 识别任务监控

识别任务监控可以查看各个数据源的扫描类型和扫描状态，支持手动添加扫描任务，手动停止执行中的任务。

操作步骤

系统管理员进入【分级分类】-【识别任务监控页面】。

手动扫描

点击手动扫描按钮，进入手动扫描页面，如图 4.4-5 所示。选择单个或多个数据源后，点击“立即执行”按钮，即可添加任务。



图 4.4-5 手动扫描页面

5 流转监测

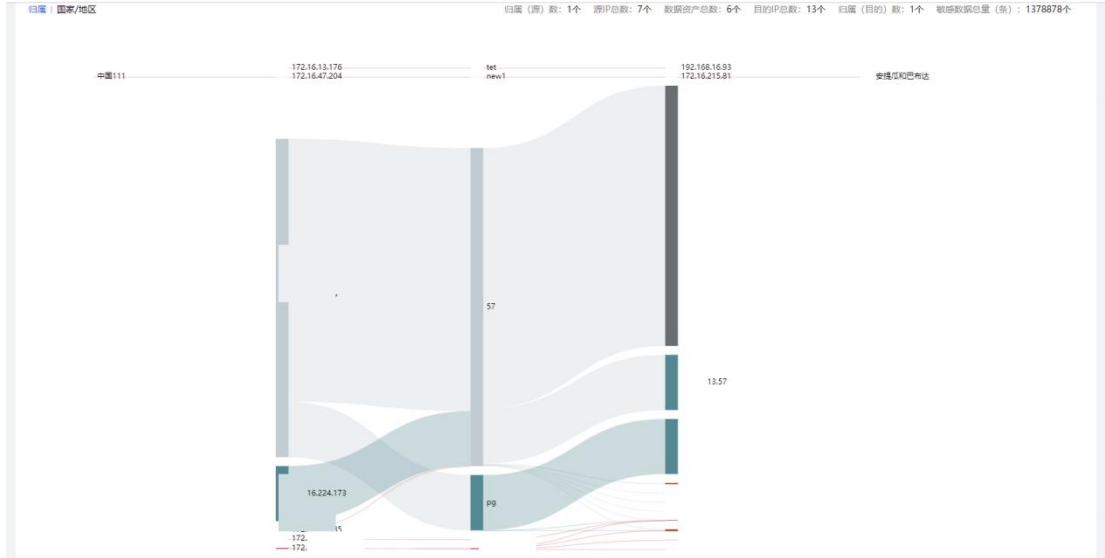
系统管理员（sysadmin）登录数据安全中心，可以进入流转监测界面。流转监测菜单下包括数据流转测绘、合规要求、应用管理、日志检索、评估任务。数据流转测绘支持对数据流转进行测绘，可视化展现数据的流动情况；合规要求支持合规要求的统一管理；应用管理支持应用的统一管理，支持子系统的单点登录；日志检索：对于数据库审计收集监测到的数据库访问行为日志，可查看数据库访问的操作语句、应答内容等信息，对于 API 审计收集监测到的接口调用日志，可查看数据库访问的接口类型、响应体等信息；评估任务：问卷任务的统一管理。

5.1 数据流转测绘

系统管理员进入数据流转测绘页面，页面包含流转测绘查询与结果展示。可以根据需求选择可视化展示（桑基图）或列表展示,如图 5.1-1 流转测绘查询、5.1-2、5.1-3 流转测绘查询结果展示。



5.1-1 流转测绘查询



5.1-2 流转测绘查询结果展示

源IP	源国家/地区	源归属	目的IP	目的国家/地区	目的归属	关联资产	流转方式	流量数(条)	敏感数据量(条)
172.16.13.176			192.16.215.81			tet	API	3	12
57			172.16.215.81			57	数据库	13	130
57	中国	内网	172.16.215.81			57	数据库	926	7408
57			172.16.215.81			57	数据库	381	3429
			172.16.215.81			57	数据库	329	6
			172.16.215.81			172.16.215.81	数据库	31	72
			172.16.215.81			57	数据库	2	0
			172.16.215.81			57	数据库	573	2963
164			172.16.215.81			wdporacle	数据库	28	0
172	204	中国	172.16.215.81	安提瓜和巴布达		new1	数据库	83	0
172	204	中国	172.16.215.81	安提瓜和巴布达		new1	数据库	4	12

5.1-3 流转测绘查询结果列表展示

数据流转测绘展示

1) 可视化展示:

默认为可视化展示，鼠标移动到相应区域上展示相应的统计信息。分为归属和国家/地区为两个统计维度，点击可切换展示维度，但当筛选条件为国家/地区或归属时，不可进行切换。

2) 列表展示:

★第一层列表统计

指定条件下**相同源 IP→相同目的 IP**，且资产为同一个的数据流转情况。展示内容包括源 IP、源国家/地区、源归属、目的 IP、目的国家/地区、目的归属、关联资产、流转方式、流量数（条）、敏感数据量（条），其中除了源国家/地区、源归属、目的国家/地区、目的归属需要进入【知识库】-【IP 地址库】进行手动配置才能展示，配置方法详见第 8.1 节 IP 地址库，其余信息均通过调用数据库资产或 API 资产后自动显示。如图 5.1-3 流转测绘查询列表展示。

注：

- 1、**关联资产**：数据流转行为所关联的资产名称，如 select 的哪一个数据库、或者接口 get 的是哪个应用等
- 2、**流转方式**：关联资产为数据库的，方式即数据库；关联资产为应用的，方式即 API；关联资产为服务器的，方式即 FTP/JDBC 等

★第二层列表展示第一层信息的详情内容，日志展示数量等于流量条数。

如图 5.6-4 流转测绘查询列表详情展示，展示内容包括：

服务端 IP：所调用数据库审计或 API 审计系统资产 IP

客户端 IP：向数据库审计或 API 审计系统资产发起请求的 IP

账号：数据库审计或 API 审计系统资产账号

源IP	源国家/地区	源归属	目的国家/地区	目的归属	关联资产	流转方式	流量数 (条)	敏感数据量 (条)
					tet	API	3	12
							13	130
							2	0
							403	1453
								0
								12

服务端IP	客户端IP	账号	数据分类	数据分型	敏感数据量 (条)	开始时间	操作	
		root			0	2022-04-24 15:46:48	详情	
					8		详情	
					0	2022-04-24 15:46:48	详情	
116.19.77.207	116.19.6.101		116.19.6.101	IP地址	S2	11	2022-04-24 15:46:48	详情

图 5.1-4 流转测绘查询列表展示

数据分类分级

★**数据分类**：调用数据库审计或 API 审计系统资产过程中，流通的敏感数据在【知识库】-【特征信息库】进行关联分类分级后被打上标签，特征信息库的配置详见第 8.2 节特征信息库。

★**数据分级**：同数据分类

★**敏感数据量（条）**：第二层列表的敏感数据量之和。

★**开始时间**：调用数据库审计或 API 审计系统资产的时间。

源IP	源国家/地区	源归属	目的IP	目的国家/地区	目的归属	关联资产	流转方式	流量数 (条)	敏感数据量 (条)
172.16.1			1'			tet	API	3	12

服务端IP	客户端IP	账号	数据分类	数据分级	敏感数据量 (条)	开始时间	操作	
	19:	6.93	aabb1	个人姓名,个人电话号码...	S3	4	2022-04-24 16:09:06	详情
					4	2022-04-24 10:32:30	详情	
1			码...	S3	4	2022-04-24 10:32:24	详情	

总共 3 条 < 1 > 15 条/页

服务端IP	客户端IP	账号	数据分类	数据分级	敏感数据量 (条)	开始时间	操作
		root			0	2022-04-24 15:44:45	详情
		root			1	2022-04-24 15:44:45	详情
		t			0	2022-04-24 15:44:45	详情
				S2	11	2022-04-24 15:44:45	详情
	17	root		S2	11	2022-04-24 15:40:21	详情

总共 5 条 < 1 > 15 条/页

图 5.1-5 流转测绘查询列表详情展示

点击详情按钮展示同日志检索中的详情。其中数据库审计详情应答内容仅展示部分样例数据。

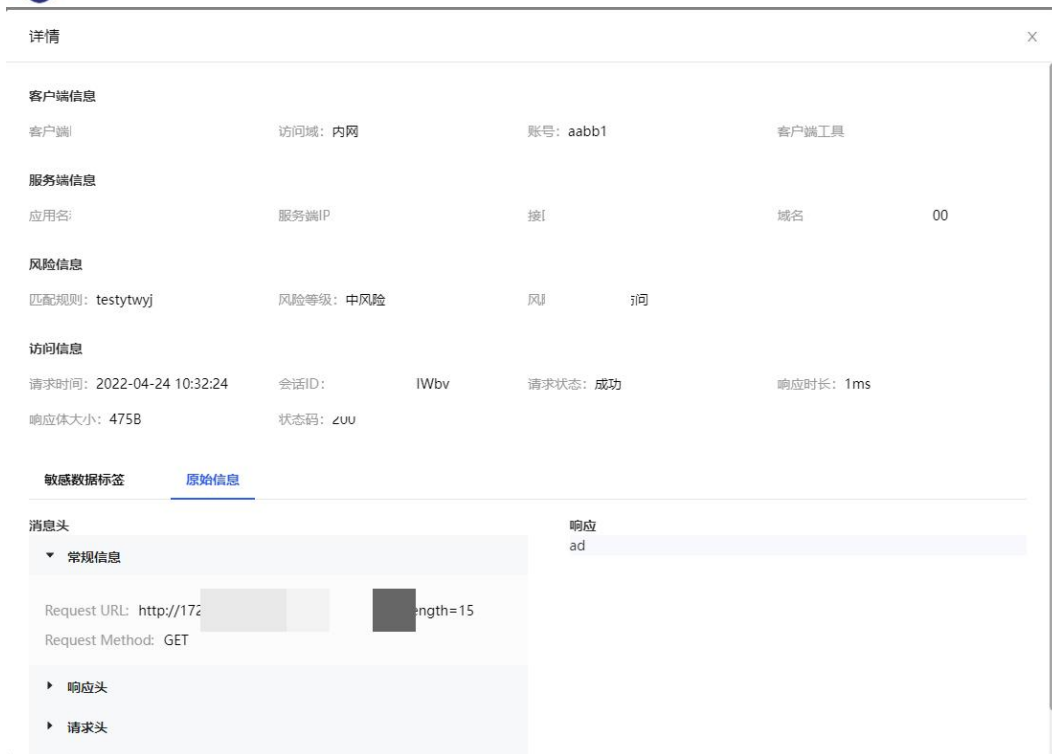


图 5.1-6 API 审计日志详情



图 5.1-7 数据库审计日志详情

导出

【数据流转测绘】页面以列表形式展示，点击“导出”按钮，自动下载当前数据流转详情表文档，查看文档显示正常。

5.2 合规要求

5.2.1 功能概述

随着《数据安全法》、《个人信息保护法》、《数据出境安全评估办法（征求意见稿）》等法规相继出台，数据流转监测的需求将会不断增加，针对数据出境相关要求在流转监测-合规要求中内置了六条出境管理要求，根据要求设置，对违反管理要求的行为进行告警：提醒与违规，并在风险预警-告警列表进行显示。

5.2.2 操作步骤

页面展示

系统管理员进入【流转监测】-【合规要求】页面，合规要求列表显示内置与新建合规要求，包括合规要求名称、依据法律标准、数据类型、告警级别、要求类型、要求说明、最后操作时间、状态，如图 5.2-1



合规要求名称	依据法律标准	数据类型	告警级别	要求类型	要求说明	最后操作时间	状态	操作
<input type="checkbox"/> 等等兜	222	存储数据	违规	人工		2022-04-24 17:56:16	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 一般数据处理者-存储个人...	数据出境安全评估办法...	存储数据	提醒	内置	处理个人信息达到一百...	2022-04-24 17:51:59	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 一般数据处理者-出境个人...	数据出境安全评估办法...	流转数据	违规	内置	累计向境外提供超过十...	2022-04-24 17:51:59	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 一般数据处理者-出境数据...	数据出境安全评估办法...	流转数据	违规	内置	累计向境外提供超过一...	2022-04-24 17:51:59	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 所有数据处理者-出境重要...	数据出境安全评估办法...	流转数据	违规	内置	出境数据中包含重要数据	2022-04-24 17:51:59	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 关键基础设施运营者-出境...	数据出境安全评估办法...	存储数据	提醒	内置	关键信息基础设施的运...	2022-04-24 17:51:59	<input type="checkbox"/>	编辑 删除
<input type="checkbox"/> 关键基础设施运营者-出境...	数据出境安全评估办法...	存储数据	提醒	内置	关键信息基础设施的运...	2022-04-24 17:51:59	<input type="checkbox"/>	编辑 删除

图 5.2-1 合规要求列表

添加合规要求

点击新建，弹出新建要求弹出框，依次填入以下内容，如图 5.2-2

★合规要求名称

★依据法律标准

★数据类型： 选择“存储数据”或“流转数据”

存储数据：指数据库审计与 API 审计资产中存储的数据，即【资产管理】-【数据资产】中的数据

流转数据：指调用数据库审计与 API 审计资产所流转的数据，在【流转监测】【数据流转测绘】与【日志检索】中的数据

★告警级别：选择违规或提醒

★过滤条件：选择 IP，过滤所选 IP

★告警条件：选择数据分类或数据分级，如选择分类，属于个人姓名，数据量超过 10 个，保存规则即可生效，即刻统计流转数据中个人姓名数据量，若累计超过 10 个，则产生风险预警产生告警。

注：

若选择流转数据，还会弹出是否只统计出境数据，则需要数据流向为中国→国外才会被记录，即在【IP 地址库】将添加源 IP 的国家为中国，目的 IP 的国家为除中国外其它国家。

编辑要求
✕

* 合规要求名称:

* 依据法律标准:

* 数据类型: 存储数据 流转数据

* 是否只统计出境数据: 是 否

* 告警名称:

* 告警级别:

要求说明: 5 / 200

过滤条件

* **告警条件**

图 5.2-2 添加合规要求

触发告警后，进入【首页】，页面上方提示：当前共存在*处告警，如图 5.2-3。点击“前往处理”，可跳转至风险预警页面，图 5.2-4（或直接点击目录栏【风险预警】）风险预警模块处理详见第六章风险预警模块。



图 5.2-3 首页告警展示

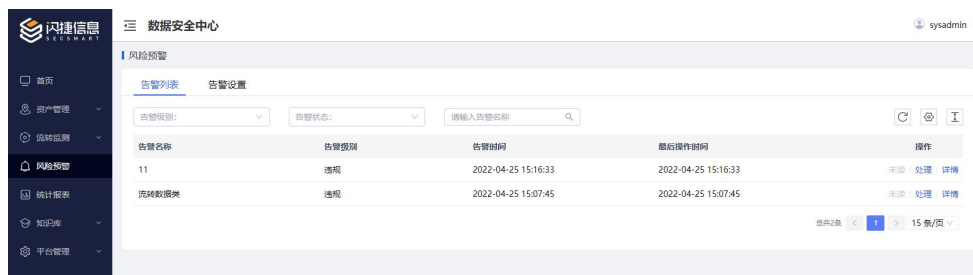


图 5.2-4 风险预警—告警列表

5.3 日志检索

通过调用【应用管理】中的数据库审计与 API 审计系统的应用，产生的日志可以在【流转监测】-【日志检索】的数据库审计与 API 审计页面实时展示。页面包含流转日志查询与结果展示。

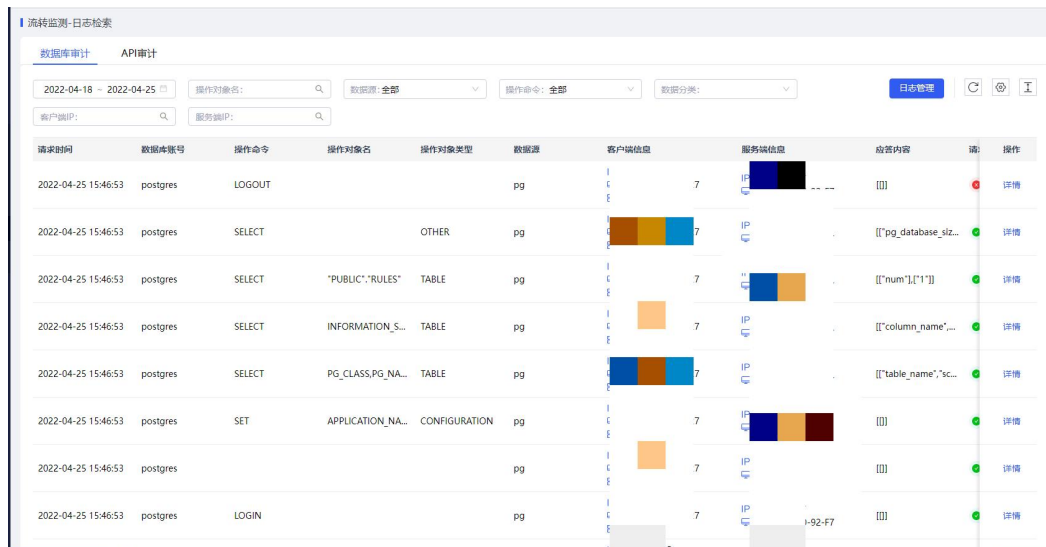
查询与展示

数据库审计查询条件：

- 1) 请求时间
- 2) 操作对象名：数据库审计中进行操作的表名称
- 3) 数据源：数据库审计中数据库资产名称
- 4) 操作命令：SELECT、UPDATE、INSERT、DELETE
- 5) 数据分类：对敏感数据打标结果
- 6) 客户端 IP
- 7) 服务端 IP

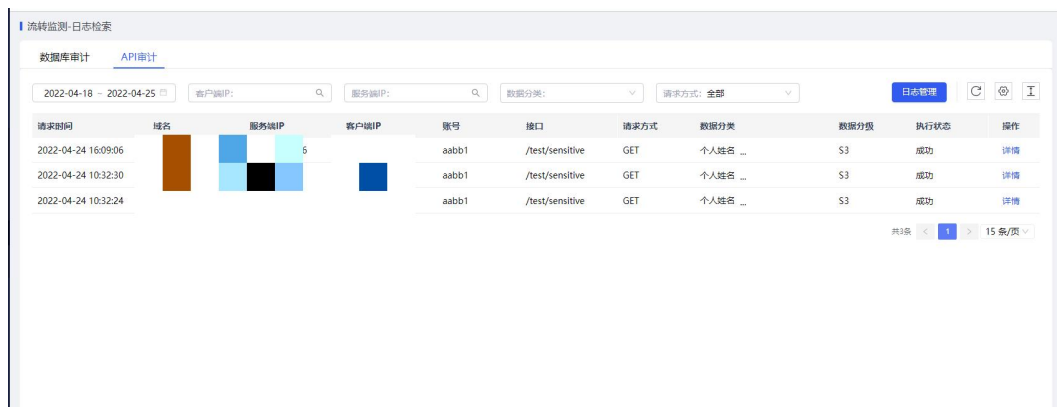
API 审计查询条件：

- 1) 请求时间
- 2) 客户端 IP
- 3) 服务端 IP
- 4) 数据分类：对敏感数据打标结果
- 5) 请求方式：接口发送请求方式，包含：GET、POST、DELETE、PUT、OPTIONS、HEADE、TRACE、CONNECT



请求时间	数据库账号	操作命令	操作对象名	操作对象类型	数据库	客户端信息	服务端信息	应答内容	确	操作
2022-04-25 15:46:53	postgres	LOGOUT			pg		7			详情
2022-04-25 15:46:53	postgres	SELECT		OTHER	pg		7	[[pg_database_siz...		详情
2022-04-25 15:46:53	postgres	SELECT	"PUBLIC";"RULES"	TABLE	pg		7	[[num"],["1"]]		详情
2022-04-25 15:46:53	postgres	SELECT	INFORMATION_S...	TABLE	pg		7	[[column_name",...		详情
2022-04-25 15:46:53	postgres	SELECT	PG_CLASS,PG_NA...	TABLE	pg		7	[[table_name";sc...		详情
2022-04-25 15:46:53	postgres	SET	APPLICATION_NA...	CONFIGURATION	pg		7			详情
2022-04-25 15:46:53	postgres				pg		7			详情
2022-04-25 15:46:53	postgres	LOGIN			pg		7			详情

图 5.3-1 采集数据库审计日志查询与展示



请求时间	域名	服务端IP	客户端IP	账号	接口	请求方式	数据分类	数据分级	执行状态	操作
2022-04-24 16:09:06				aabb1	/test/sensitive	GET	个人姓名...	S3	成功	详情
2022-04-24 10:32:30				aabb1	/test/sensitive	GET	个人姓名...	S3	成功	详情
2022-04-24 10:32:24				aabb1	/test/sensitive	GET	个人姓名...	S3	成功	详情

图 5.3-2 采集 API 审计应用日志查询与展示

支持日志管理，可选择日志备份的时间，默认永久



日志管理 ✕

* 日志保存天数: 半年 一年 永久

取消
确定

评估任务

评估任务负责问卷任务的统一管理，支持任务的添加、编辑、删除；可根

据相应的问卷模板进行问卷评估列表功能并生成评估报告。

添加评估任务

点击新建，弹出添加任务弹出框，依次填入：评估任务名称、问卷模板、评估时间，然后保存。若所填评估时间包含此刻，则评估任务列表状态显示为：进行中，若所填评估时间不包含此刻，则评估任务列表状态显示为：待进行。如图 5.3-4。



添加任务

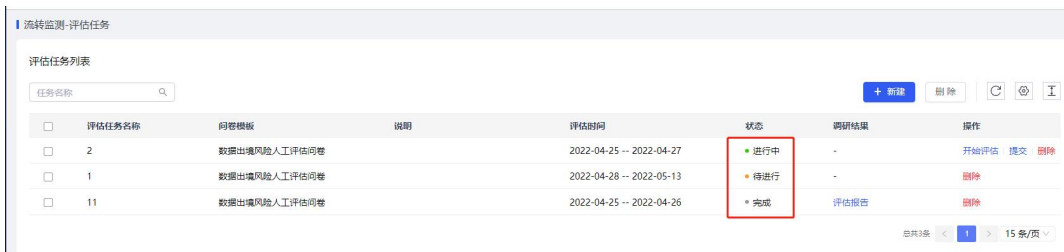
* 评估任务名称:

* 问卷模板:

说明: 0 / 200

* 评估时间: ~

图 5.3-3 添加评估任务



流转监测-评估任务

评估任务列表

任务名称

<input type="checkbox"/>	评估任务名称	问卷模板	说明	评估时间	状态	调研结果	操作
<input type="checkbox"/>	2	数据出境风险人工评估问卷		2022-04-25 -- 2022-04-27	进行中	-	开始评估 提交 删除
<input type="checkbox"/>	1	数据出境风险人工评估问卷		2022-04-28 -- 2022-05-13	待进行	-	删除
<input type="checkbox"/>	11	数据出境风险人工评估问卷		2022-04-25 -- 2022-04-26	完成	评估报告	删除

总共3条 < 1 > 15条/页

图 5.3-4 评估任务列表

评估

评估任务列表选择状态为：进行中的评估任务，点击“开始评估”，跳转至“数

据处境风险人工评估问卷”页面，进行问卷作答，作答过程中除了勾选答案还可以上传符合性证据进行辅助，文件格式可以为 doc、docx、xls、xlsx、pdf、jpg、png、.gif、ppt、pptx，文件大小限制 100M。点击提交后，跳转至统计报表（或点击【统计报表】目录下问卷评估报告）即可查看评估报告。如图 5.3-5、5.3-6 查看评估报告报表，可以对报表进行：在线预览、导出、查看导出记录等操作。

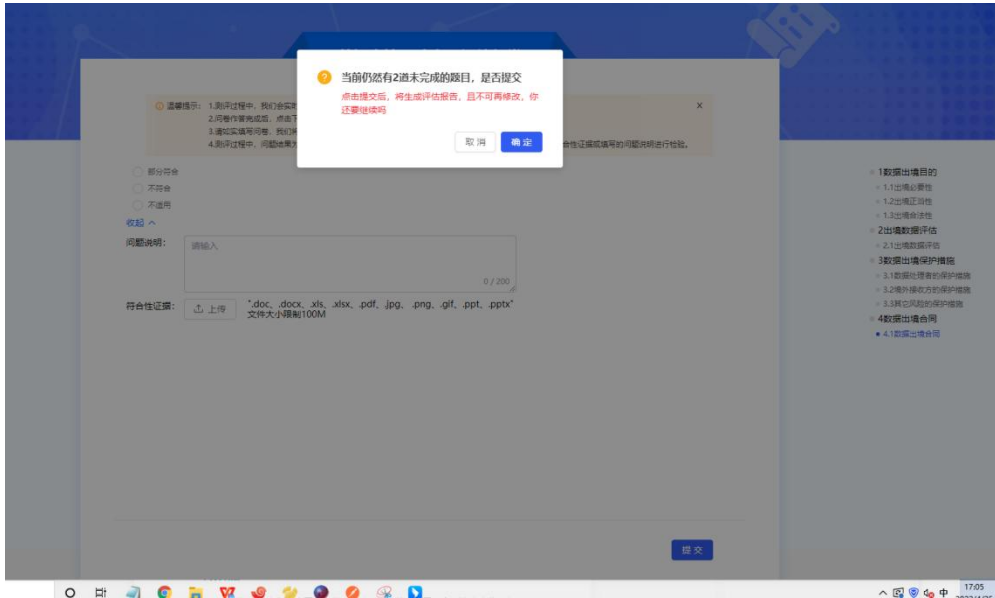


图 5.3-5 提交评估报告



图 5.3-6 查看评估报告报表

6 风险预警

6.1 功能概述

风险预警模块用来统计触发合规要求的告警，并对告警进行对应的处置操

作。调用数据库审计或 API 审计资产，触发一条或多条合规要求，产生告警。打开【风险预警】页面，默认进入告警列表，显示告警名称、告警级别、告警时间、最后操作时间、操作。



图 6.1-1 风险预警页面

处理

选择未处理状态的告警，点击“处理”按钮，弹出页面如图 6.1-2 所示，查看告警信息。处理方式处，勾选“我已手工处理”，点击“确定”按钮，告警事件处理成功，列表图标变化（忽略显示绿色、其他显示灰色），且无法再次点击，如图 6.1-3 所示。点击“取消”按钮，取消处理告警事件。

- 1) 告警名称：显示告警名称
- 2) 告警级别：提醒或违规
- 3) 告警详情：产生告警的原因
- 4) 处理方式：勾选项，我已手工处理



图 6.1-2 告警事件处理页面

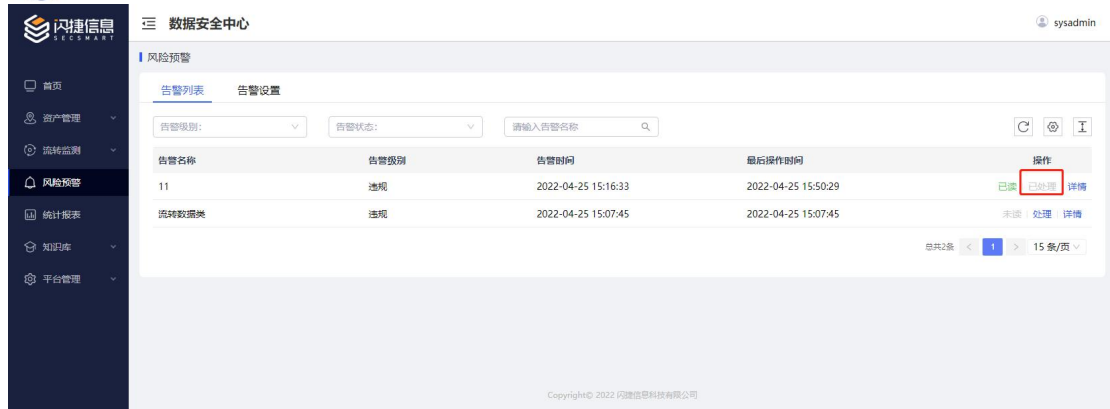


图 6.1-3 处理情况

6.2 操作步骤

报警邮件配置

报警邮件用于发送告警列表中告警信息，报警邮件配置页面如下图 7.2-1 所示，分别填入邮件服务器地址、邮箱账号、密码，通过邮件配置测试可以验证服务器地址是否正确、账号密码是否匹配。



图 7.2-1 报警邮件配置

7 统计报表

7.1 数据资产梳理报告

进入【统计报表】-【数据资产梳理报告】，如图 7.1-1 所示，报表预览可以选择数据库审计所有资产，选择任一资产后，点击“在线预览”，即可展示资产梳理报告，报告内容包含 7 个部分，分别为：01 概要、02 数据资产概览、03 数据资产分布、04 数据分级概览、05 数据分类概览、06 敏感数据概览、07

敏感数据分布。还可以对报表进行导出、查看导出记录等操作。

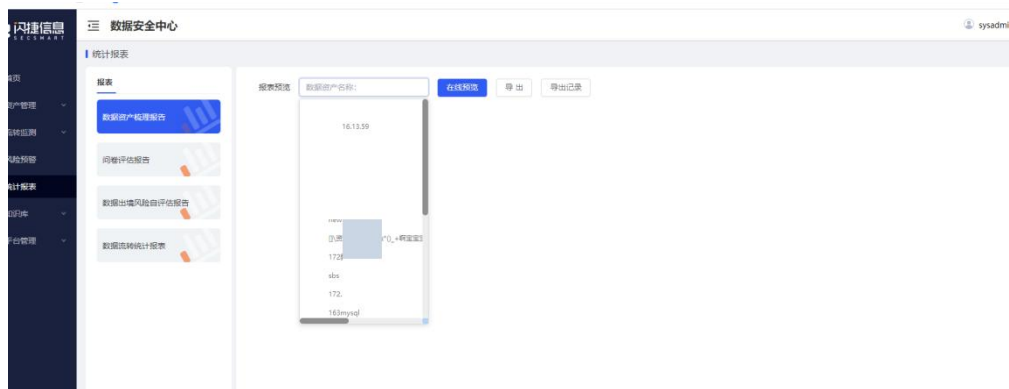


图 7.1-1 数据资产梳理报告



图 7.1-2 数据资产梳理报告预览

7.2 问卷评估报告

进入【统计报表】-【问卷评估报告】页面，如图 7.2-1 所示，报表预览可以选择评估任务中的所有任务，选择任一评估任务后，点击“在线预览”，即可展示问卷评估报告，报告中评估结论包含控制域、控制项、制度要求、检查项、评估结论、符合性证据，问题说明，除了可以对以上内容查询，还可以下载符合性证据中的文档进行查看。以及对报表进行导出、查看导出记录等操作。



图 7.2-1 问卷评估报告预览

7.3 数据出境风险自评估报告

进入【统计报表】-【数据资产自评估报告】页面，如图 7.2-1 所示，需要选择报表预览的时间段、数据库审计资产任一资产，并且选择评估任务。点击“在线预览”，即可展示数据资产自评估报告，报告内容包含 4 个部分，分别为：01 概述、02 出境数据评估、03 人工评估、04 合规评估。还可以对报表进行导出、查看导出记录等操作。



图 7.3-1 数据资产梳理报告预览

7.4 数据流转统计报表

进入【统计报表】-【数据流转统计报表】页面，如图 7.4-1 所示，需要选择报表预览的时间段、数据库审计资产或 API 审计资产中任一资产。点击“在线预览”，即可展示数据资产自评估报告，报告内容包含 5 个部分，分别为：01 概述、02 资产流转统计、03 敏感数据流转统计、04 数据流出情况统计、05 数据流入情况统计。还可以对报表进行导出、查看导出记录等操作。

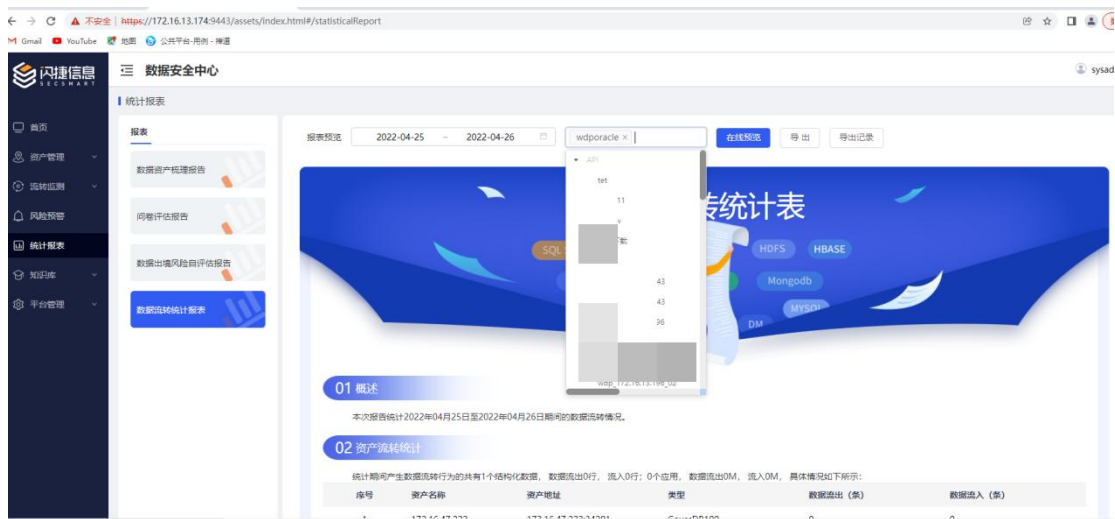


图 7.4-1 数据流转统计报告预览

8 知识库

知识库管理包括 IP 地址库、特征信息库和问卷模板模块，分别管理了 IP 地址信息域特征项信息和对问卷模板的下载与查看。

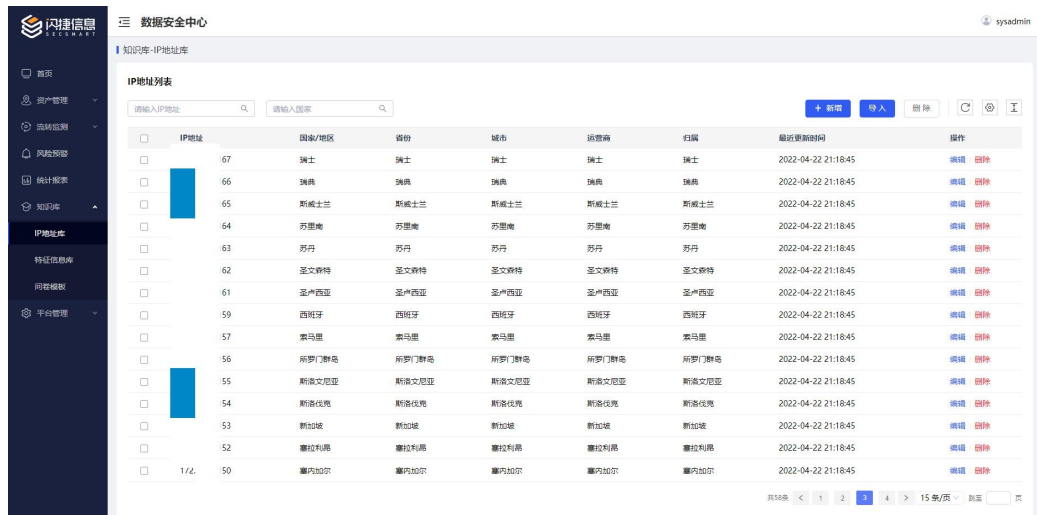
8.1 IP 地址库

8.1.1 功能概述

系统内置默认 IP 地址库，可自动匹配数据流转过程中对应 IP 的所属地区/国家，同时也支持人工添加 IP 地址库，支持编辑、删除、导入操作。

8.1.2 操作步骤

进入【知识库】-【IP 地址库】界面，如图 8-1-1 所示，可管理自定义的 IP 地址。各类服务端 IP、客户端 IP 识别都将基于此自定义 IP 库和内置的 IP 库。



IP地址	国家/地区	省份	城市	运营商	归属	最近更新时间	操作
67	瑞士	瑞士	瑞士	瑞士	瑞士	2022-04-22 21:18:45	编辑 删除
66	瑞典	瑞典	瑞典	瑞典	瑞典	2022-04-22 21:18:45	编辑 删除
65	新加坡	新加坡	新加坡	新加坡	新加坡	2022-04-22 21:18:45	编辑 删除
64	芬兰	芬兰	芬兰	芬兰	芬兰	2022-04-22 21:18:45	编辑 删除
63	苏丹	苏丹	苏丹	苏丹	苏丹	2022-04-22 21:18:45	编辑 删除
62	圣文森特	圣文森特	圣文森特	圣文森特	圣文森特	2022-04-22 21:18:45	编辑 删除
61	圣卢西亚	圣卢西亚	圣卢西亚	圣卢西亚	圣卢西亚	2022-04-22 21:18:45	编辑 删除
59	西班牙	西班牙	西班牙	西班牙	西班牙	2022-04-22 21:18:45	编辑 删除
57	索马里	索马里	索马里	索马里	索马里	2022-04-22 21:18:45	编辑 删除
56	所罗门群岛	所罗门群岛	所罗门群岛	所罗门群岛	所罗门群岛	2022-04-22 21:18:45	编辑 删除
55	斯洛文尼亚	斯洛文尼亚	斯洛文尼亚	斯洛文尼亚	斯洛文尼亚	2022-04-22 21:18:45	编辑 删除
54	斯洛伐克	斯洛伐克	斯洛伐克	斯洛伐克	斯洛伐克	2022-04-22 21:18:45	编辑 删除
53	新加坡	新加坡	新加坡	新加坡	新加坡	2022-04-22 21:18:45	编辑 删除
52	塞拉利昂	塞拉利昂	塞拉利昂	塞拉利昂	塞拉利昂	2022-04-22 21:18:45	编辑 删除
50	塞内加尔	塞内加尔	塞内加尔	塞内加尔	塞内加尔	2022-04-22 21:18:45	编辑 删除

图 8.1-1 IP 地址列表

- 添加 IP 地址：点击<添加>按钮，弹出如图 8.1-2 窗口，填写相应字段，可新增一条新的 IP 地址。
- 删除 IP 地址：选择 IP 地址，点击<删除>按钮，可删除一条 IP 地址。勾选多条 IP 地址，点击<批量操作>中的<批量删除>，可删除多条 IP 地址。
- IP 地址查询：默认查询条件有 IP 地址、国家。

新增
✕

* IP地址:

* 国家/地区:

省份:

城市:

运营商:

归属:

图 8.1-2 添加 IP 地址

- 导入 IP 地址：点击<导入>，弹出如图 8.1-3 的窗口，点击<导入 IP 地址模板>即可下载导入模板。按要求填写表格后，点击<上传文件>，上传文件后，最后点击<确认导入>进行添加。

导入文件
✕

下载文件模板



点击或将文件拖拽到这里上传

支持xls、xlsx格式

请严格按照模板说明填写，请勿随意修改，否则可能导致失败

图 8.1-3 导入文件

8.2 特征信息库

8.2.1 功能概述

特征信息库页面可进行特征信息库和特征项的添加、编辑、删除。特征信息库由特征信息类别和特征项组成。特征项设置完成后可用于数据识别规则的内容规则，实现对数据库中的某类数据进行分类。

8.2.2 操作步骤

系统管理员登录数据安全中心，进入知识库管理/特征信息库页面。

添加特征项

点击“添加”按钮，即可进入特征项页面，点击添加后，如图 8.2-1 所示，输入相应特征项名称、规则类型、规则定义后点击“下一步”按钮，如图 8.2-2 所示，输入规则定义，点击“完成配置”，成功添加特征信息，同时可以在特征项页面进行查看，点击“取消”按钮，则取消添加特征信息。

- 1) ★特征项名称：必填项，特征项的名称
- 2) ★规则类别：必选项，选择规则类别（结构化数据类和非结构化数据类）
- 3) 特征信息类别：非必选项，选择特征信息库创建的特征信息类别
- 4) 规则说明：非必填项，规则的说明
- 5) ★规则定义：必填项，根据规则类型定义规则
- 6) 测试内容：非必填项，选择部分特征项（正则表达式）后显示

图 8.2-1 创建特征项页面-1

图 8.2-2 创建特征项页面-2

特征项编辑

特征项创建完成后会显示在页面中，点击需要修改的特征项对应的编辑按钮，即可进入特征策略编辑页面，如图 8.2-3 所示，编辑完成后，点击“完成配置”完成编辑，点击“取消”则取消编辑。

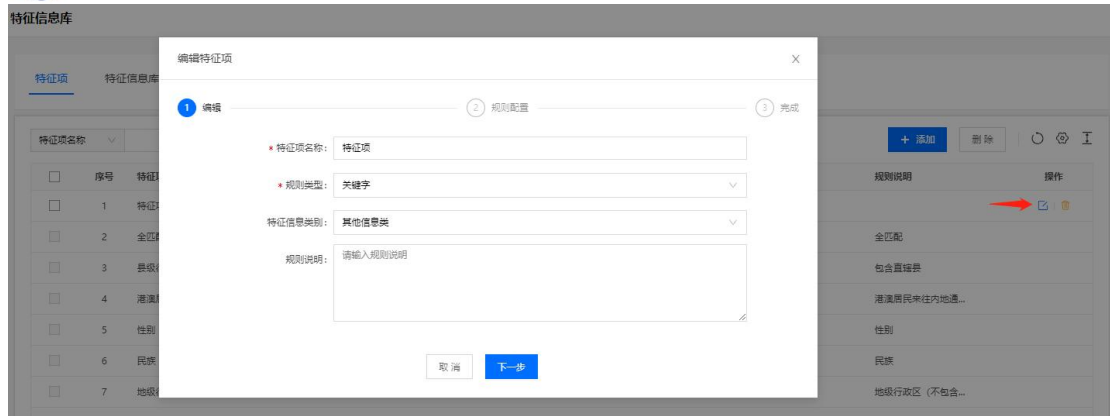


图 8.2-3 特征项编辑页面

特征项删除

特征项创建完成后会显示在页面中，选择需要删除的特征项，点击删除按钮，即进入删除页面，如图 8.2-4 所示，点击“确定”即可删除相应特征项，点击“取消”则取消删除特征项。

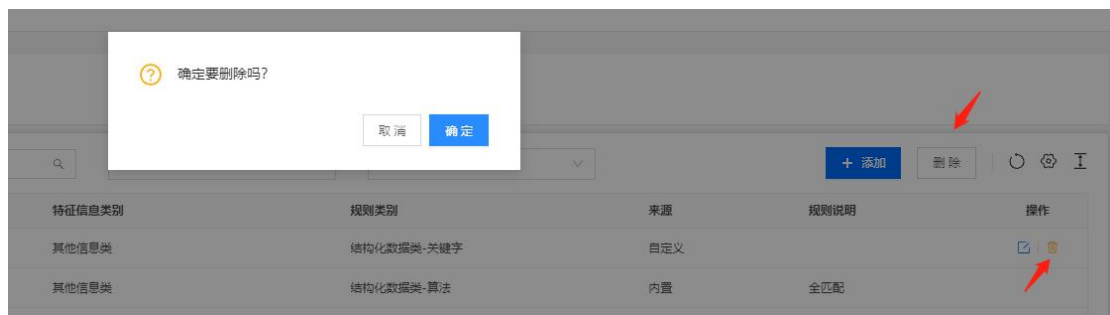


图 8.2-4 删除特征项页面

关联分类分级

特征项创建完成后，可关联流转数据分类分级，如图 8.2-5，关联分类分级后，会在特征项信息中显示对应的分类分级，如图 8.2-6。同时数据库审计与 API 审计数据流转过程中也会根据关联的分类分级参数进行打标。具体体现在【流转监测】-【数据流转测绘】列表展示的日志中，如图 8.2-7，以及【流转监测】-【日志检索】中，如图 8.2-8。



图 8.2-5 关联分类分级

特征项 特征信息库

特征项名称: [搜索框] 规则类别: [下拉] 来源: 全部 [下拉] + 关联分类分级 + 添加 删除 [刷新] [重置] [帮助]

特征项名称	特征信息类别	规则类别	来源	数据分类	数据分级	规则说明	操作
22	车辆信息类	结构化数据类-正则表达式	自定义				编辑 删除
县级行政区	其他信息类	结构化数据类-算法	内置	住址	S4	包含直辖市	
港澳居民来往内地通行证	其他信息类	结构化数据类-正则表达式	内置	出入证	S3	港澳居民来往内地通行证	
性别	其他信息类	结构化数据类-正则表达式	内置	性别	S2	性别	
民族	其他信息类	结构化数据类-正则表达式	内置	民族	S2	民族	
地级行政区	其他信息类	结构化数据类-算法	内置			地级行政区 (不包含台湾地区)	
省级行政区	其他信息类	结构化数据类-算法	内置			省份 (中国内地)	
统一社会信用代码	其他信息类	结构化数据类-算法	内置			统一社会信用代码	
港澳通行证	其他信息类	结构化数据类-正则表达式	内置	出入证	S3	港澳通行证 (包含新版和旧版)	
组织机构代码	其他信息类	结构化数据类-算法	内置			组织机构代码	
IP地址	其他信息类	结构化数据类-正则表达式	内置	IP地址	S1	IP地址	
IPv6地址	其他信息类	结构化数据类-正则表达式	内置			IPv6地址	
JDBC连接串	其他信息类	结构化数据类-正则表达式	内置			JDBC连接串	
MAC地址	其他信息类	结构化数据类-正则表达式	内置	MAC地址	S1	MAC地址	
IMEI	其他信息类	结构化数据类-正则表达式	内置			IMEI	

共38条 < 1 2 3 > 15条/页 刷新 页

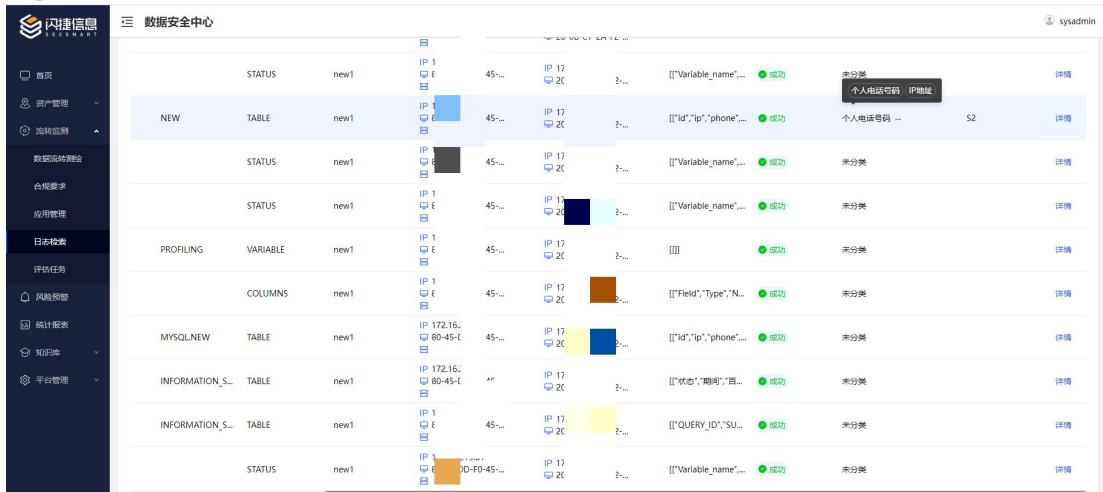
图 8.2-6 关联后显示分类分级

数据安全中心 sysadmin

服务IP	客户端IP	账号	数据库	数据分类	数据分级	敏感数据量 (条)	开始时间	操作
172.17.0.1	172.17.0.1	root	数据库			381	2022-04-24 15:46:48	详情
172.17.0.2	172.17.0.2	root	数据库			329	2022-04-24 15:46:48	详情
172.17.0.3	172.17.0.3	root	数据库			31	2022-04-24 15:46:48	详情
172.17.0.4	172.17.0.4	root	数据库			2	2022-04-24 15:46:48	详情
172.17.0.5	172.17.0.5	root	数据库			573	2022-04-24 15:46:48	详情
172.17.0.6	172.17.0.6	root	数据库			28	2022-04-24 15:46:48	详情
172.17.0.7	172.17.0.7	root	数据库			83	2022-04-24 15:46:48	详情
172.17.0.8	172.17.0.8	root	数据库			4	2022-04-24 15:46:48	详情
172.17.0.9	172.17.0.9	root	数据库	数据库	S2	11	2022-04-24 15:46:48	详情
172.17.0.10	172.17.0.10	root	数据库			23	2022-04-24 15:46:48	详情
172.17.0.11	172.17.0.11	root	数据库			21336	2022-04-24 15:46:48	详情
172.17.0.12	172.17.0.12	root	数据库			28	2022-04-24 15:46:48	详情
172.17.0.13	172.17.0.13	root	数据库			80	2022-04-24 15:46:48	详情

总共 4 条 < 1 2 3 > 15条/页 刷新 页

图 8.2-7 流转数据的分类分级 1




Item Name	Type	Status	Source	Destination	Rule	Result	Classification	Action
STATUS	new1	IP 1	45...	IP 17	[[Variable_name],...	成功	未分类	详情
NEW	TABLE	new1	IP 1	IP 17	[[id,"ip","phone",...	成功	未分类	详情
STATUS	new1	IP 1	45...	IP 17	[[Variable_name],...	成功	未分类	详情
STATUS	new1	IP 1	45...	IP 17	[[Variable_name],...	成功	未分类	详情
PROFILING	VARIABLE	new1	IP 1	IP 17	[[id,"ip","phone",...	成功	未分类	详情
COLUMNS	new1	IP 1	45...	IP 17	[[Field,"Type";"N...	成功	未分类	详情
MYSQLNEW	TABLE	new1	IP 172.16.80-45-f	IP 17	[[id,"ip","phone",...	成功	未分类	详情
INFORMATION_S...	TABLE	new1	IP 172.16.80-45-f	IP 17	[[状态","期初","百...	成功	未分类	详情
INFORMATION_S...	TABLE	new1	IP 1	IP 17	[[QUERY_ID";SU...	成功	未分类	详情
STATUS	new1	IP 1	45...	IP 17	[[Variable_name],...	成功	未分类	详情

图 8.2-8 流转数据的分类分级 2

添加特征信息库

切换至特征信息库页面，点击添加按钮，进入创建特征类别页面，如图 8.2-8 所示，输入相应的类别名称和类别说明，点击“确定”按钮，成功创建特征类别，点击“取消”则取消创建特征类别。只有关联到特征信息类别中的特征项可以被数据识别规则使用。

- 1) ★类别名称：必填项，特征类别的名称
- 2) 特征项：非必选项，选择未被关联到特征信息类别中的特征项
- 3) 类别说明：非必填项，特征类别的说明



创建特征类别
✕

* 类别名称:

特征项:

类别说明:

取消
确定

图 8.2-8 创建特征类别页面

特征信息库编辑

特征信息添加完成后，系统管理员可通过页面编辑按钮分别对特征类别进行编辑，选择对应特征类别，点击编辑按钮，即可进入特征类别编辑页面，如图 8.2-9 所示。进入相应编辑页面后，编辑相应信息。点击“确定”则编辑成功，点击“取消”则取消编辑。



图 8.2-9 特征类别编辑页面

特征信息库删除

选择已存在的特征类别和特征项，通过删除按钮即可删除相应的特征类别和特征信息。删除按钮如图 8.2-9 所示



图 8.2-9 删除按钮

特征信息库支持特征信息类别、特征项查询。列表右侧同样支持刷新、列展示和调整列高度功能。

8.3 问卷模板

支持问卷的管理，可手动添加和导入添加，内置数据出境评估问卷模板。

系统管理员登录数据安全中心，进入【知识库】-【问卷模板】页面。问卷模板列表内置数据出境风险人工评估问卷。可以对内置问卷进行下载与预览操作。如图 8.3-1。



图 8.3-1 问卷模板列表

8.3.1 添加问卷模板

点击“新建模板”按钮，即可进入创建模板页面，选择列表层数：二层列表或三层列表、点击确认后，如图 8.3-1 所示，输入相应问卷模板名称、三层标签名称、问题描述即答案选项，如图 8.3-2 所示，最后点击“保存”，成功添加问卷模板，同时可以在问卷模板列表页面进行查看。如图 8.3-3，进一步，通过【流转监控】-【评估任务】进行添加评估任务时，问卷模板选项也同步更新。如图 8.3-4。



图 8.3-1 创建问卷模板页面-1

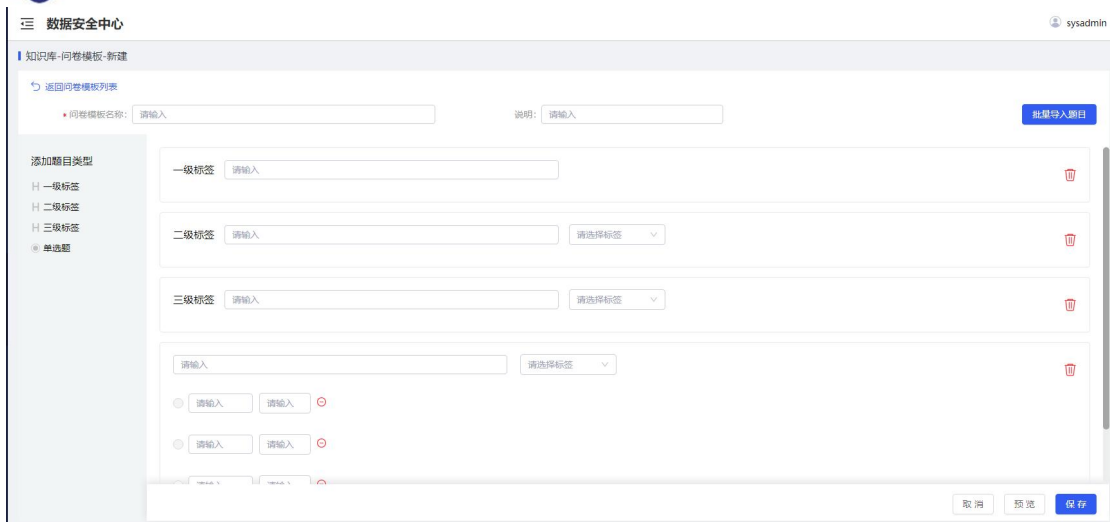


图 8.3-2 创建问卷模板页面-2



图 8.3-3 问卷模板创建成功

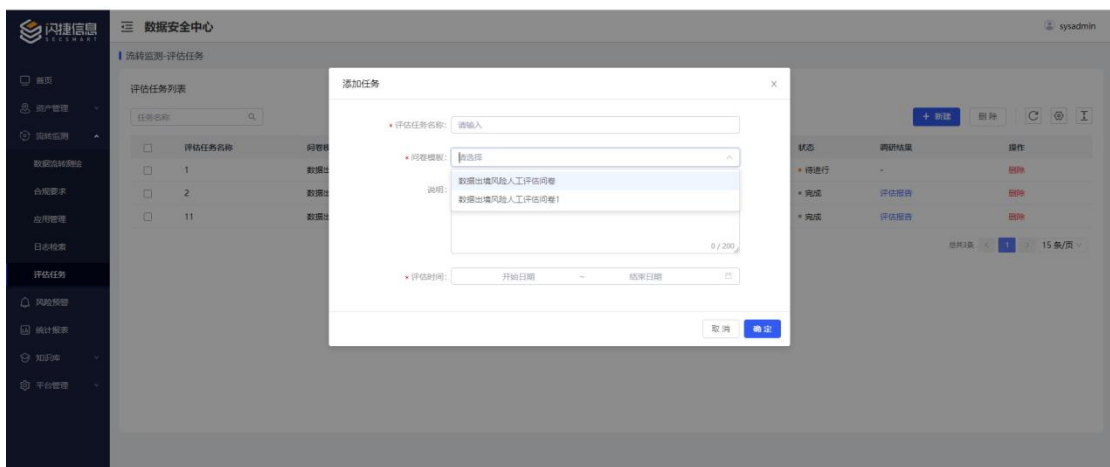


图 8.3-4 问卷模板

8.3.2 问卷模板编辑

问卷模板创建完成后会显示在页面中，点击需要修改的问卷模板对应的编辑按钮，即可进入特征策略编辑页面，如图 8.3-5 所示，编辑完成后，点击“完

成配置”完成编辑，点击“取消”则取消编辑。

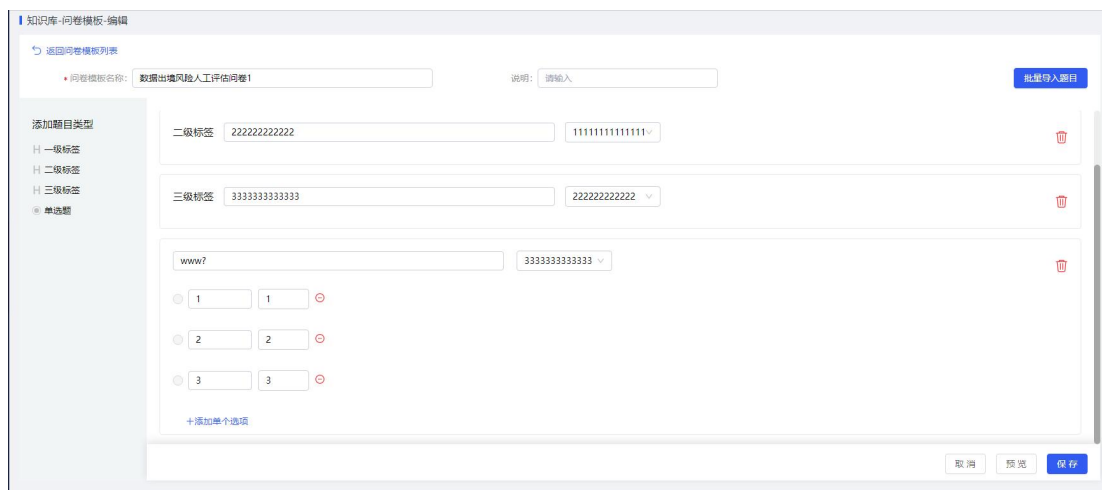


图 8.3-5 特征项编辑页面

8.3.3 特征项删除

问卷模板创建完成后会显示在页面中，选择需要删除的特征项，点击删除按钮，即进入删除页面，如图 8.3-2 所示，点击“确定”即可删除相应问卷模板，点击“取消”则取消删除特征项。

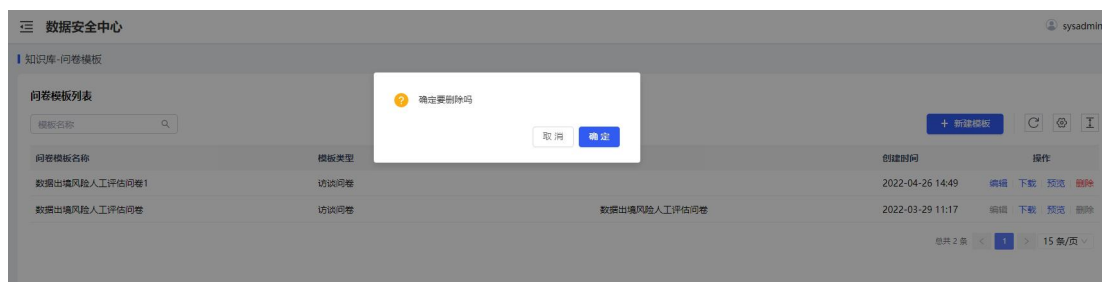


图 8.3-6 删除问卷模板页面

可以设置允许登录 IP 地址和网络权限配置(禁止 ICMP 探测),如图 12.6-3 所示。

9 平台管理

平台管理主要用于授权、查看平台及服务器信息、修改网络配置和系统安全配置、账号管理等。包括基础设置、账号管理、平台运维、操作审计、角色管理、账号审核、安全配置等子菜单。

9.1 基础设置

9.1.1 功能概述

基础设置包括平台信息和网络设置两部分。平台信息支持平台信息的查看和个性化设置。网络设置支持修改网卡信息的配置。

9.1.2 操作步骤

平台信息

系统管理员进入【平台管理】-【基础设置】-【平台信息】页面，可以查看平台信息并进行授权、个性化设置、修改系统时间等操作。点击授权期限后的授权图标，可对系统进行授权操作。下载机器码后将机器码通过授权系统进行授权，再导入授权文件，点击授权即可。

个性化设置

个性化设置功能需要在授权管理系统勾选相应的功能后可用，默认不支持个性化设置。授权后，系统管理员进入【平台管理】-【基础设置】-【平台信息】页面，点击产品名称后的编辑按钮，出现如图 9.1-1 所示页面。支持外页 Logo、内页 Logo、内页折叠 logo、外页产品名称、内页产品名称、标签页图标和责任人电话设置。Logo 支持 JPG（JPG、JPEG）、PNG、GIF 格式且大小不超过 500KB 的图片。

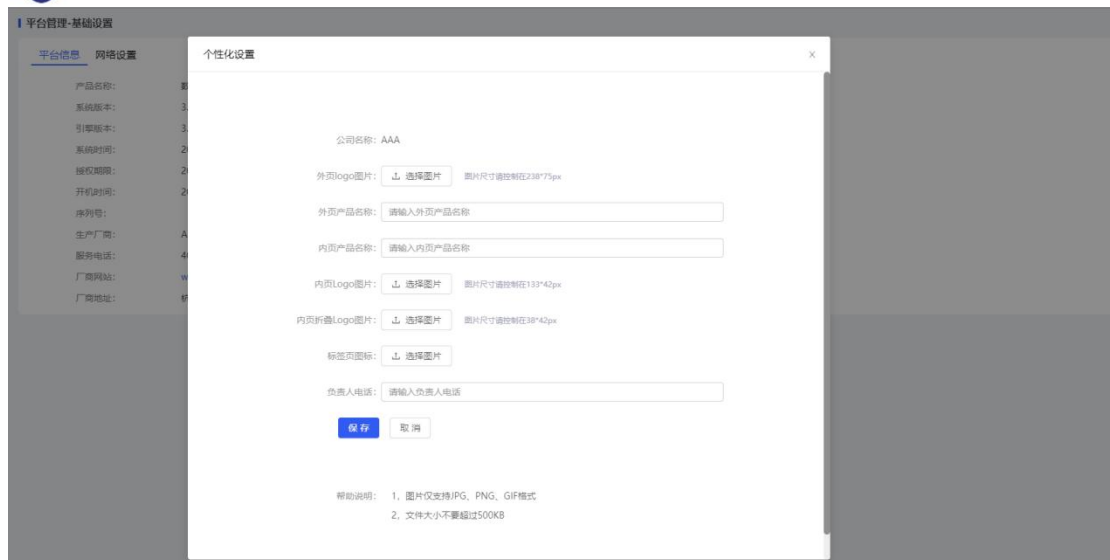


图 9.1-1 个性化设置页面

网络设置

系统管理员进入【平台管理】-【基础设置】-【网络设置】页面，出现如图 9.1-2 所示页面。该页面展示所有网卡状态和列表，支持修改网口名称、类型、IP 地址、网关、子网掩码、DNS 等信息。

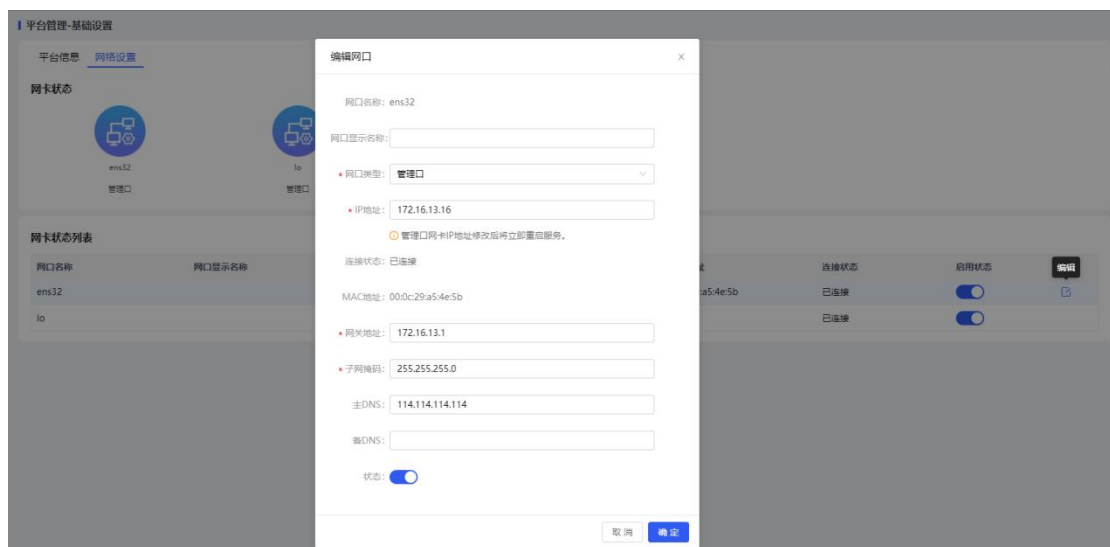


图 9.1-2 网络设置页面

9.2 账号管理

9.2.1 功能概述

系统管理员在账号管理模块中，创建新的账号。新建的账号必须审核通过

之后才能使用。账号管理页面支持对账号进行创建、编辑、删除、导入、初始化密码操作。

9.2.2 操作步骤

创建账号

系统管理员进入【平台管理】-【账号管理】页面，点击“创建账号”按钮，弹出创建账号。

- 1) 账号：必填项，自定义账号的名称，同时也是登录名
- 2) 密码：必填项，登录密码，自定义账号密码
- 3) 密码确认：必填项，与密码保持一致
- 4) 使用人：必填项，自定义账号姓名
- 5) 角色：必选项，账号所属角色（角色与权限相关，务必确认清楚）
- 6) 组织架构：非必选项，账号所属组织架构
- 7) 电话：非必填项，账号所属人的电话
- 8) 邮箱：非必填项，账号所属人的邮箱
- 9) 使用期限：必选项，默认永久
- 10) 时间期限：必填项（使用期限勾选定义期限时），达到设置的时间后，账号将不可用。
- 11) 备注说明：非必填项，对账号的补充说明信息

导入

点击“导入”，在导入账号信息页面下载导入账号模板，按照账号模板的格式要求输入账号名称、密码等信息。选择填写后的账号模板，点击“确认导入”即可。导入前可通过导入测试检查文件内容正确性。

初始化密码

选择需要初始化的账号记录，点击“初始化密码”按钮，提示弹窗点击“确定”。初始化成功后，账号密码设置为 Admin@123

编辑账号

编辑账号时不能修改账号密码，其他字段与创建账号时一致且都能修改。

删除账号

支持删除单个或多个账号，账号删除后不能恢复，请仔细确认。

9.3 平台运维

9.3.1 功能概述

平台运维包含设备状态、升级恢复、系统日志、系统诊断、服务器配置等。可以直观展示设备的 CPU、内存、网卡吞吐量、硬盘等信息，并进行系统日志、告警外发配置。同时支持 web 界面升级、重启服务、重启设备、关闭设备等操作。

9.3.2 操作步骤

设备状态

设备状态页面包括当前时间、系统已运行时长，重启服务、重启设备、关闭设备等操作按钮，以及 CPU、内存、网卡吞吐量、硬盘等图表信息。

系统管理员进入【平台管理】【平台运维】【设备状态】页面，如图 9.3-1 所示。

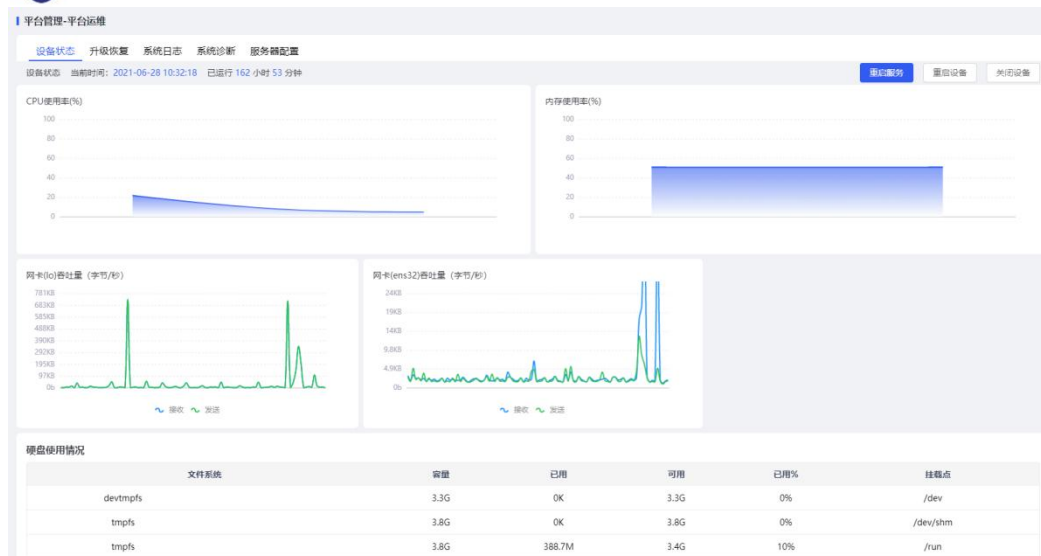


图 9.3-1 平台运维页面

进行重启服务、重启设备、关闭设备等操作时会有弹窗提示，确认后进行对应操作，取消则退出操作。成功进行重启设备操作，大约两分钟后，重启操作完成。重启过程中系统不能访问，请谨慎操作。

升级恢复

升级恢复页面支持 jar 包升级操作。系统管理员进入【平台管理】-【平台运维】-【升级恢复】页面，如图 9.3-2 所示。点击右侧“升级”按钮，在升级弹窗点击“上传文件”，可选择升级包（jar 包）。升级包上传后，需要重启服务使升级包生效。升级列表显示序号、版本号（补丁号）、升级内容（升级说明）、配置说明和升级时间。



图 9.3-2 升级恢复页面

系统日志

系统日志页面可以进行日志自动清除和日志备份操作。系统管理员账户进入【平台管理】-【平台运维】-【系统日志】页面，如图 9.3-3 所示。支持开启

自动清除或自动备份。

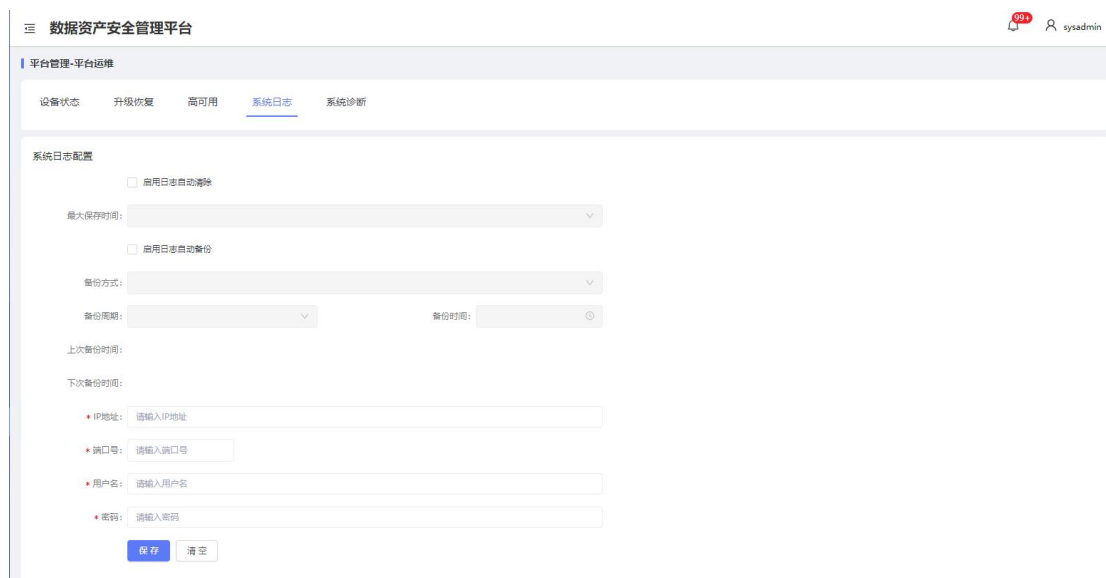


图 9.3-3 系统日志页面

1) 自动清除：非必选项，勾选“启用日志自动清除”后，系统将在每天凌晨自动清除超过最大保存时间的操作审计日志。

2) 最大保存时间：必填项（启用日志自动清除后），可设置一周，15 天，1 个月，3 个月，6 个月和一年

3) 启用日志自动备份：非必选项，勾选“启用日志自动备份”

以下字段，启用日志自动备份后必填：

- 4) 备份方式：必填项，支持 FTP 或 SFTP
- 5) 备份周期：必填项，可设置每天、每周或每月
- 6) 备份时间：必填项，设置备份的时间（时分）
- 7) IP 地址：必填项，FTP 或 SFTP 服务器的 IP 地址
- 8) 端口号：必填项，FTP 或 SFTP 服务器的端口号
- 9) 用户名：必填项，FTP 或 SFTP 服务器的用户名
- 10) 密码：必填项，FTP 或 SFTP 服务器的密码

系统诊断

系统管理员进入【平台管理】-【平台运】-【系统诊断】页面，如图 9.3-4 所示。可以对内核、cpu&mem、磁盘、网卡、磁盘 IO 等进行实时诊断。点击调试日志下载，可以下载系统的运行日志。

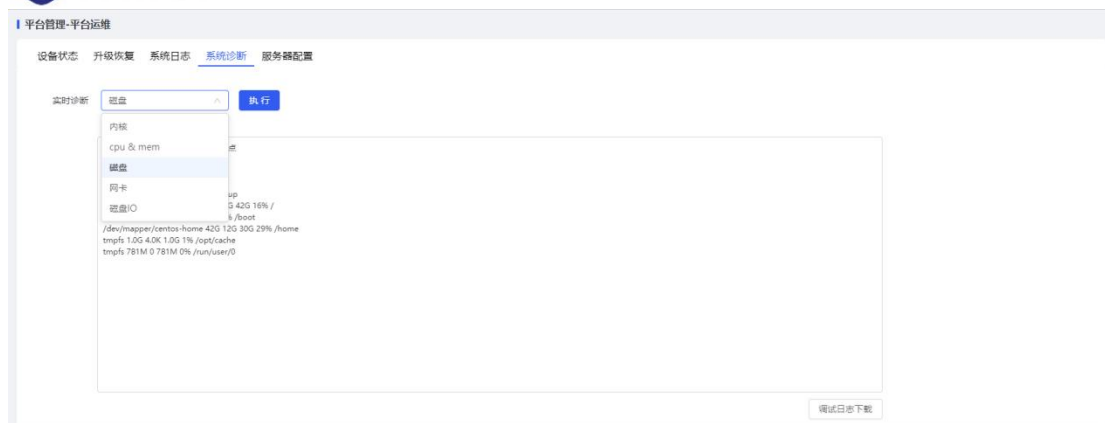


图 9.3-4 系统诊断页面

服务器配置

系统管理员进入【平台管理】-【平台运维】-【服务器配置】页面，如图 9.3-5 所示。配置 SYSLOG 服务器和 SNMP 服务器后，可将告警事件、设备状态、系统操作日志等发送到对应的服务器。

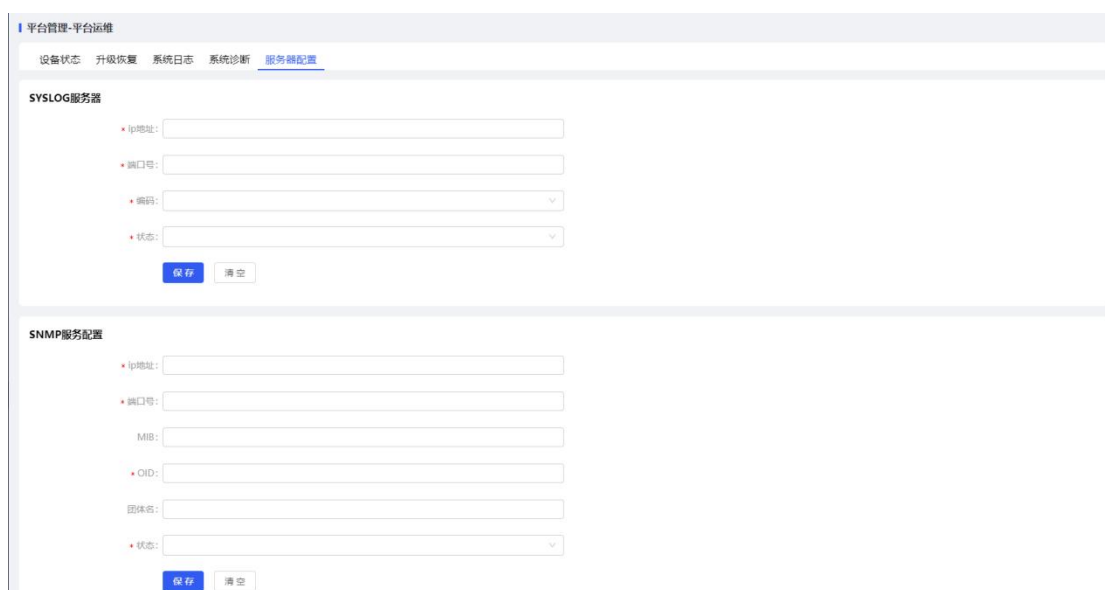


图 9.3-5 服务器配置页面

9.4 操作审计

操作审计中可以查看系统所有的操作日志。

9.4.1 操作审计

功能概述

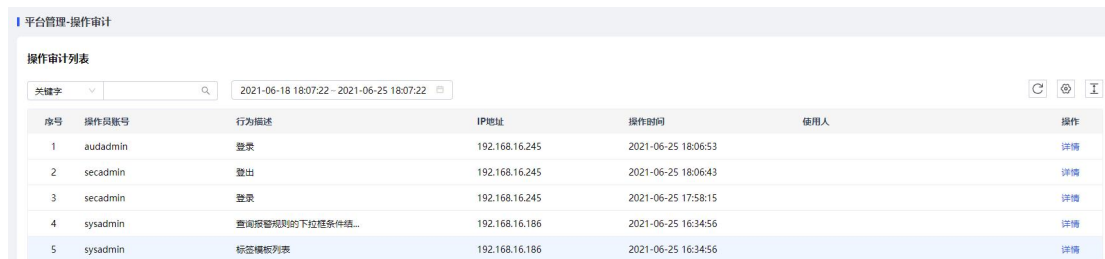
操作审计中可以查看系统所有的操作日志。

操作审计支持操作员账号、使用人、IP 地址、关键字、时间检索。

通过点击详情按钮，支持查看单条操作审计记录的详细信息。

操作步骤

系统管理员进入操作审计界面，界面布局如图 9.4-1 所示。



序号	操作员账号	行为描述	IP地址	操作时间	使用人	操作
1	audadmin	登录	192.168.16.245	2021-06-25 18:06:53		详情
2	secadmin	登出	192.168.16.245	2021-06-25 18:06:43		详情
3	secadmin	登录	192.168.16.245	2021-06-25 17:58:15		详情
4	sysadmin	查阅报警规则的下拉框条件框...	192.168.16.186	2021-06-25 16:34:56		详情
5	sysadmin	标签模板列表	192.168.16.186	2021-06-25 16:34:56		详情

图 9.4-1 操作审计页面

9.5 角色管理

9.5.1 功能概述

安全管理员（secadmin）通过角色管理功能，可以新建、删除、修改、角色以及角色的权限。系统内置角色审计管理员和安全管理员不支持编辑和删除。

9.5.2 操作步骤

创建角色

安全管理员进入【平台管理】-【角色管理】页面，如图 9.5-1 所示。点击“创建角色”。输入角色名称、角色描述，选择角色类别，角色权限，点击“确定”，成功创建角色。



图 9.5-1 角色管理页面

删除角色

支持单个或多个角色的删除。已被账号关联的角色不允许删除。

9.6 账号审核

9.6.1 功能概述

手动审核创建的账号信息，可以通过或拒绝。也可以授权自动审核，授权的账户可以自动审核通过自身创建的账号，即创建的账号默认为正常状态。操作步骤

手动审核

安全管理员登录数据资产安全管理平台，进入【平台管理】-【账号审核】-【手动审核】页面，如图 9.6-1 所示。审核通过后账号可登录管理平台，审核拒绝的账号不能登录平台。审核拒绝的账号需要再次审核的，可以删除后重新添加正确的账号信息，进行重新审核。



图 9.6-1 手动审核页面

授权自动审核

安全管理员进入【平台管理】-【账号审核】-【自动审核】界面，选中相

应账号，点击“授权自动审核”，可授权自动审核。

撤销自动审核

选中已授权自动审核的账号，点击“撤销自动审核”，可撤销自动审核。

9.7 安全配置

9.7.1 功能概述

安全管理员可在该页面进行平台登录安全、账号密码安全以及网络访问安全设置。

9.7.2 操作步骤

平台登录安全设置

安全管理员进入【平台管理】-【安全配置界面】，如图 9.7-1 所示。可以设置平台安全管理方式，上传 https 证书。设置登录动态验证码，空闲超时登出时间，登录安全策略、短信验证码等。



图 9.7-1 安全配置页面

账号密码安全设置

账号密码安全设置可以选择是否启用初次登录强制更改密码，密码长度和密码复杂度要求，如图 9.7-2 所示。

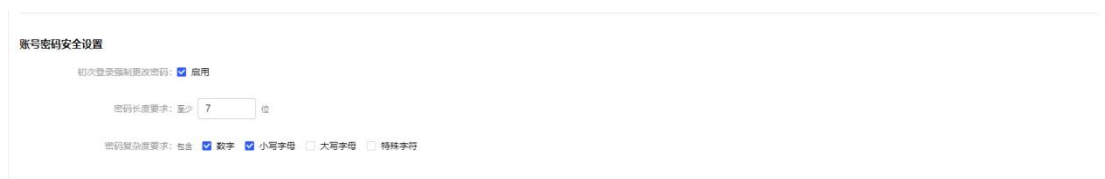


图 9.7-2 账号密码安全设置页面

网络访问安全设置

可以设置允许登录 IP 地址和网络权限配置（禁止 ICMP 探测），如图 9.8-3 所示。

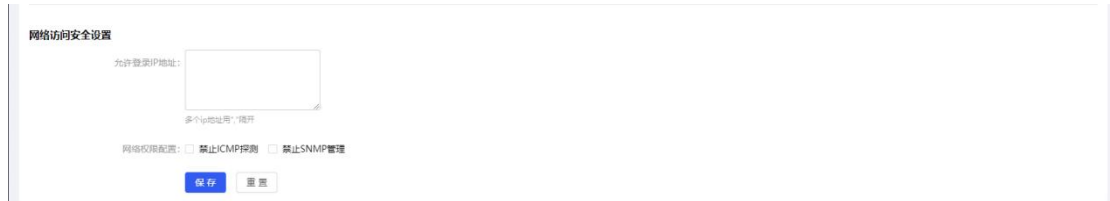


图 9.7-3 网络访问安全设置页面