数据库加密与访问控制网关
V5.0
用户手册

目　录

1. 前言

1.1. 文档目的

本手册主要介绍数据库加密与访问控制网关的配置、使用和管理。通过阅读本文档，用户可以了解数据库加密与访问控制网关的主要功能，并根据实际应用环境配置和使用该系统。

1.2. 读者对象

本用户手册阅读对象产品技术支持人员，实施人员，产品经理，网络管理员，数据库 DBA 及产品运维人员等。

2. 产品概述

2.1. 产品简介

数据库加密与访问控制网关是一款基于透明加密技术、主动防御机制的数据库防泄漏产品，该产品能够实现对数据库中的敏感数据加密存储、访问控制增强、应用访问安全等功能。有效防止明文存储引起的数据泄密、突破边界防护的外部黑客攻击、来自于内部高权限用户的数据窃取，防止绕开合法应用系统直接访问数据库，从根本上解决数据库敏感数据泄漏问题，真正实现了数据高度安全、应用完全透明、密文高效访问等技术特点。

系统支持数据加解密、用户权限管理、密钥管理、资产管理、加密策略管理、数据完整性保护、加密卡管理、多租户管理、HA 高可靠等功能，全方位的保障数据的安全性、机密性和完整性。

通过使用该系统，可以实现如下目标：

- 支持数据库类型 Oracle、MySQL、PostgreSQL、GaussDB、KingbaseES、KADB、AtlasDB、DM7、DM8、DB2、SQL Server。
- 支持丰富的加密算法及类型。
- 达到高效的数据加解密。
- 实现自动实时灵活的动态加密解密。
- 支持细粒度的权限访问控制。
- 支持三级密钥管理。
- 支持数据的完整性保护。

2.2. 系统登录

数据库加密与访问控制网关采用 B/S 模式，打开浏览器（推荐使用 Google Chrome 浏览器），在地址栏输入 https://192.168.1.254（实体机安装完成后系统 IP 地址会默认设置为 192.168.1.254，实际 IP 地址以现场环境为准）访问产品登录界面，如下图所示：

图 2-1 登录页

※注意：进行 web 访问前请确保操作终端与数据库加密与访问控制网关路由可达，且访问链路上放开了 443 端口。

数据库加密与访问控制网关 WEB 端基于三权分立原则设计，内置三个不同权限的管理员，各管理员的功能与职责不同，权限不同，相互监督。系统管理员负责系统的运行设置，安全管理员负责密钥管理和对加密对象进行操作，审计管理员负责查看整体系统的操作日志情况。具体账号信息及权限分配如下表：

账号	角色	缺省密码	功能模块
SysAdmin	系统管理员	Admin@12345	首页、加密卡管理、用户与角色、系统管理、系统信息
SecAdmin	安全管理员	Admin@12345	首页、资产管理、策略管理、密钥管理、用户与角色、系统信息
Auditor	审计管理员	Admin@12345	首页、用户与角色、系统信息

用户首次访问数据库加密与访问控制网关，应首先通过系统管理员登录平台配置或确认相关系统信息，包括但不限于：申请 License 授权、调整管理 IP、确认系统时间、启用加密卡并备份。

2.3. 系统页面布局介绍

系统页面共分为：导航栏、配置区、辅助区、帮助提示区四部分。

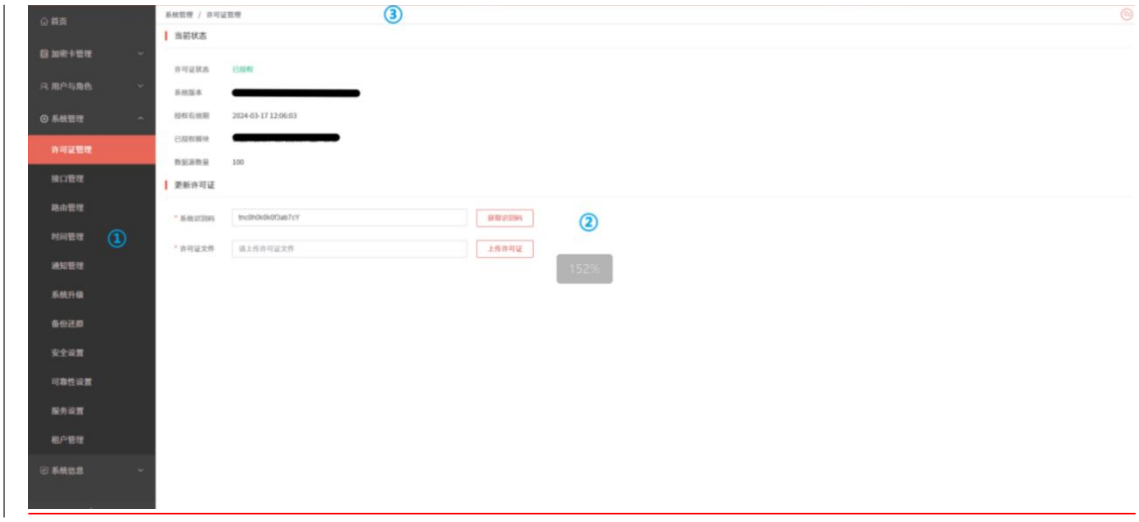

图 2-2 系统页面

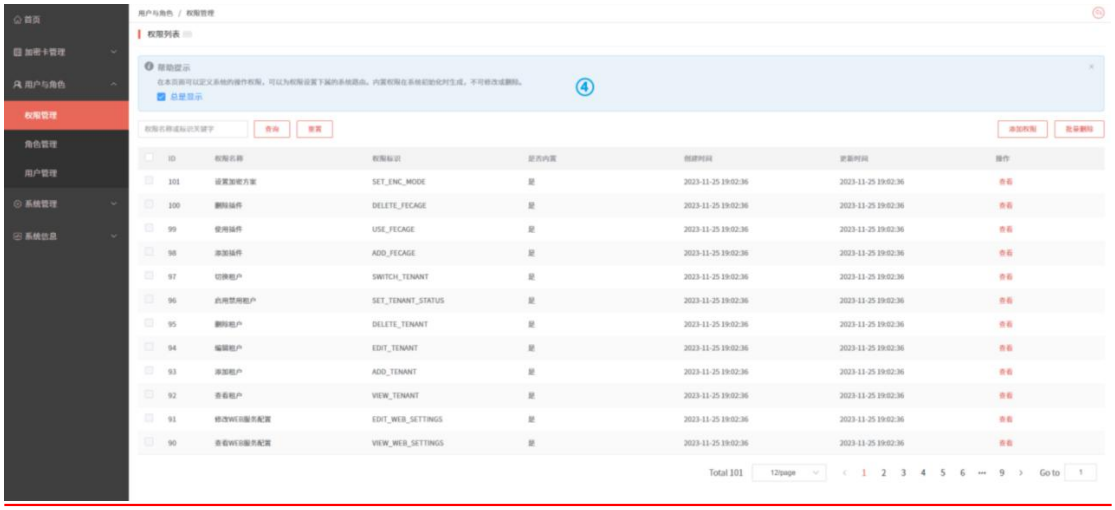

图 2-3 系统页面

①导航栏：以导航树的形式组织设备的功能菜单。用户在导航栏中可以方便的选择模块菜单，选择结果显示在辅助区、配置区中。

②配置区：用户进行配置和查看的区域。

③辅助区：上辅助区显示当前配置区的页面在导航栏中的路径；下辅助区显示当前系统运行状态。

④帮助提示区：为用户操作提供帮助指导。

2.3.1. 帮助提示

通过帮助提示有助于用户便捷了解某功能的使用方法和注意事项。用户登录后，部分页面会显示帮助提示，见下图（以数据源管理页面为例）：

图 2-4 帮助提示

用户在未做设置前，帮助提示默认总是显示，取消<总是显示>，可设置是否在所有页面隐藏帮助提示或仅当前页面隐藏帮助提示。

图 2-5 隐藏帮助提示

用户若希望隐藏的帮助提示再次显示，可点击“ⓘ”，显示帮助提示。

※注意：隐藏帮助提示中的所有页面，指的是系统所有包含“帮助提示”的页面。

2.3.2. 切换语言

系统支持多语言切换，目前支持简体中文和英文两种语言，可通过选择下辅助区的语言选项来切换语言，如下图所示：

图 2-6 切换语言

※注意：①系统初始状态显示的语言类型，由安装时选择的语言类型决定；②安装时已初始化到数据库中的数据只根据安装时指定的语言类型生成，如权限名、角色名、操作日志模板、密钥模板名等。安装成功后，即使在页面切换显示语言，这部分信息也不会切换显示；③用户与用户之间的语言类型相互不影响。

3. 系统管理概述

系统管理需使用系统管理员登录产品进行相关设置，系统管理员是加密系统三大管理员之一，主要负责系统运行维护。可进行加密卡管理、分配权限及角色、新建用户、监控系统性能、配置业务接口、操作系统配置、备份恢复数据。

系统管理包含内容见下表：

主菜单	分类	功能说明
首页	业务基础数据统计	当前备用、在用、历史密钥数量；当前数据源总量、数据源状态异常数量、数据库类型分布
		当前加密表数、未加密表数统计
		最新加密对象信息
	其他数据统计	当前加密卡信息和状态
		当前插件总量、插件状态异常数量
	系统资源统计	CPU、内存的准实时占用率统计；系统接口准实时接收/发送流量统计
加密卡管理	加密卡状态	查看当前加密卡状态、设置加密卡状态
	加密卡备份	备份加密卡信息或下载加密卡备份文件
用户与角色	权限管理	系统权限信息查看及新增权限
	角色管理	添加、查看、编辑角色并赋予其相关权限
	用户管理	用户的创建、授权（系统管理员仅可授权新建用户为系统操作员）、删除
系统管理	许可证管理	导入 license、查看系统状态
	接口管理	查看当前接口使用情况及配置接口
	路由管理	查看 IPv4、IPV6 路由表，静态路由配置

	时间管理	设定系统时间，包括手动和从时间服务器同步
	通知管理	编辑和查看当前的 SYSLOG 通知配置，可选择通知内容
	系统升级	升级系统软件，并查看升级历史、恢复出厂设置
	系统备份	系统配置的手工或自动备份，并可进行异地上传
	安全设置	对系统登录的安全参数进行配置，以提升系统的登录安全性
	可靠性设置	对系统进行 HA 高可靠配置
	服务设置	配置服务端口和 WEB 白名单，与 SNMP 配置和节点信息查看
	租户管理	管理租户共享使用系统的角色和用户
系统信息	系统状态	CPU、内存的近 1 小时占用率统计；数据空间、总储存空间使用情况
	帮助手册	查看系统使用中相关的配置指导手册
个人中心	修改资料	修改个人资料
	修改密码	修改个人密码

3.2. 首页

系统管理员在登录后默认进入首页界面，通过该页面用户可以了解系统的当前业务情况，整体运行状态，首页的监控内容包括业务基础数据统计、其他数据统计、系统资源统计三部分信息。

功能项	说明
业务基础数据统计	当前备用、在用、历史密钥数量；当前数据源总量、数据源状态异常数量、数据源类型分布
	当前加密表数、未加密表数统计
	最新加密对象信息
其他数据统计	当前加密卡信息和状态
	当前插件总量、插件状态异常数量
系统资源统计	CPU、内存的准实时占用率统计；系统接口准实时接收/

	发送流量统计

图 3-1 主页

3.2.1. 业务基础数据统计

展示业务运行基础数据，包括密钥相关信息、数据源相关信息、数据源类型分布、加密相关信息四部分。

- 密钥相关信息：当前备用密钥数量、在用密钥数量、历史密钥数量，来提醒用户当前密钥的使用情况，若备用密钥数量不足可及时补充。

图 3-2 密钥信息

- 数据源相关信息：当前数据源总量和数据源状态异常数量，来提醒用户是否有连接异常的数据源及时定位。

图 3-3 数据源信息

- 数据源类型分布：方便查看当前系统资产情况，及不同数据库类型的占比情况。

图 3-4 数据源类型分布

- 加密相关信息：当前加密对象的加密情况和最近 5 条加密对象信息，方便用户直观查看最新加密情况。

图 3-5 最新加密表

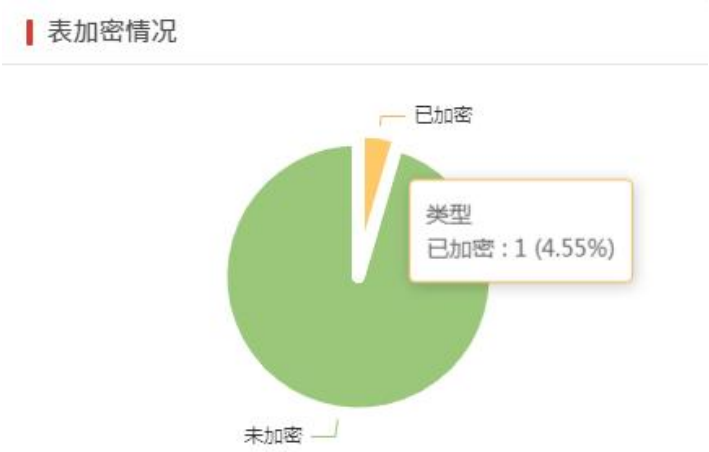

图 3- 6 表加密情况

3.2.2. 其他数据统计

其他数据统计，包括加密卡信息、插件信息两部分。

- 加密卡信息：当前加密卡信息和状态，用户可以直观看到加密卡的型号及当前加密卡状态，若加密卡状态异常时方便及时调整。

图 3- 7 加密卡状态

- 插件信息：当前插件总量、插件状态异常数量，来提醒用户有连接异常的数据源可及时定位。

图 3- 8 插件信息

3.2.3. 系统信息

系统资源使用率包括 CPU、内存和网速（上行/下行）三部分，通过趋势图（数据更新周期为每 5 秒一次）帮助用户判断当前系统性能压力。同时展示当前

使用软件版本，及系统时间。

图 3-9 系统信息

3.3. 加密卡管理

一台数据库加密与访问控制网关硬件设备中内置一张加密卡。

加密卡管理主要包括加密卡信息和加密卡备份两部分内容，可以查看到加密卡当前的状态信息、设置加密卡的状态、备份加密卡。

3.3.1. 加密卡用户角色

在数据库加密与访问控制网关中，一张加密卡的内置用户角色有 2 种，分别为操作员和管理员。一张加密卡拥有 1 个操作员和 3 个管理员，每一个用户都有一个专属的 UKey。在设置加密卡状态时，需要插入对应角色的 UKey，并输入对应的密码才能进行下一步操作。

3.3.2. 加密卡信息

系统管理员登录系统后，点击“加密卡管理”->“加密卡信息”进入该页面，可以查看加密卡信息，包括：型号、硬件唯一标识、状态。

图 3-10 加密卡信息

3.3.3. 加密卡状态

3.3.3.1. 加密卡状态

加密卡的状态是未插卡、未初始化、已禁用、已启用（常规模式）、已启用（管理模式）五种内置状态，分别定义如下：

- 未插卡：系统未检测到加密卡；
- 未初始化：系统检测到加密卡，但未初始化；
- 已禁用：加密卡已初始化，但未启用；
- 已启用（常规模式）：加密卡已启用，处于常规模式；
- 已启用（管理模式）：加密卡已启用，处于管理模式；

不同的状态下，系统可操作的功能不同。某些密钥相关操作和加解密操作只能在特定模式下才可完成，具体区别见下表：

状态	功能
已启用（常规模式）	创建主密钥、生成备用密钥（数据加密密钥）、加密数据、解密数据
已启用（管理模式）	加密数据、解密数据、备份加密卡数据

※注意：系统启动后，加密卡的状态默认为“已禁用”，在使用过程中按需求设置加密卡状态即可。若系统提示“未初始化”、“未插卡”或“加密卡状态错误”等报错信息，请联系厂家处理。

3.3.3.2. 设置状态

系统管理员登录系统后，点击“加密卡管理”->“加密卡信息”进入该页面，点击<设置状态>可以设置加密卡的目标状态和工作模式， 点击<下一步>，需要按操作提示插入 UKey 并输入 UKey 密码和当前系统登录账号的密码，点击<提交>完成状态设置，系统会提示“操作成功”，加密卡状态改变。

图 3-11 设置加密卡状态

图 3-12 设置加密卡状态

用户可以在已禁用、已启用（常规模式）和已启用（管理模式）三个状态间互相切换，一共有 6 种切换场景。

- 已禁用状态切换为已启用（常规模式）状态，需要插入操作员 UKey 并输入 UKey 密码和当前系统登录账号的密码。
- 已禁用状态切换为已启用（管理模式）状态，需要依次插入任意 2 位管理员 UKey 并输入 UKey 密码和当前系统登录账号的密码。
- 已启用（常规模式）状态切换为已禁用状态，需要输入当前系统登录账号的密码。
- 已启用（常规模式）状态切换为已启用（管理模式）状态，需要依次插入任意 2 位管理员 UKey 并输入 UKey 密码和当前系统登录账号的密码。
- 已启用（管理模式）状态切换为已启用（常规模式）状态，需要插入操作员 UKey 并输入 UKey 密码和当前系统登录账号的密码。
- 已启用（管理模式）状态切换为已禁用状态，需要输入当前系统登录账号的密码。

切换为已启用（管理模式）状态时，登录第一个管理员后，需在 5 分钟内登录第二个管理员，超过 5 分钟将自动恢复为设置前状态。若意外关闭弹框，可选择<继续>登录第二个管理员，或者<放弃>设置状态，恢复为设置前状态。

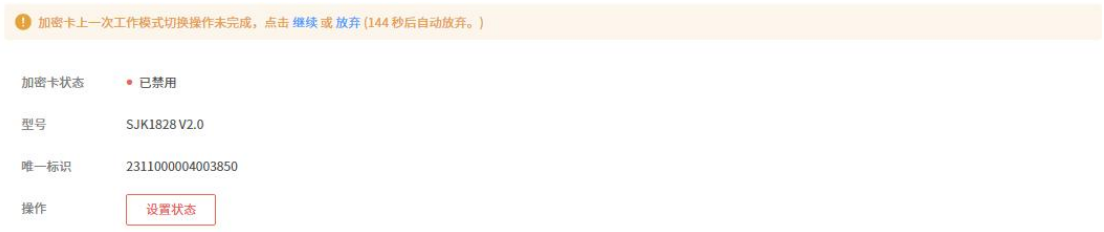

图 3-13 设置加密卡状态

※注意：①加密卡未进行备份操作时，不允许切换为“常规模式”②需妥善保管 Ukey，在有数据已加密情况下，UKEY 丢失，可能会导致数据无法解密，进而影响业务的正常运行，同时加密设备需返厂处理。

3.3.3.3. UKey 锁定

在加密卡的使用过程中，系统会记录 UKey 的连续错误次数，若用户在输入错误 UKey 密码连续累计 8 次后，UKey 将被永久锁定。UKey 被锁定时，禁止所有 UKey 的登录操作，但可以登出 UKey。即 UKey 被锁定时，当前状态为“管理模式”，且操作员已处于登录状态，仍可切换状态为“常规模式”。

UKey 被锁定后，不涉及 UKey 登录操作的其他功能仍可使用。即 UKey 被锁定时，当前状态为“常规模式”，系统仍可正常加解密，创建数据加密密钥。

UKey 被锁定后，很大程度上影响业务的正常运行，同时加密设备需返厂处理。

※注意：除上述情况外，单个 UKey 密码连续累计输入错误超过 10 次，会导致单个 UKey 被锁定，UKey 被锁定后，加密设备需返厂处理。

3.3.4. 加密卡备份

为了保证加密数据的安全，当加密卡出现故障时能够及时恢复，应及时备份加密卡数据。这些数据包括加密卡中存储的用户（管理员和操作员）信息、密钥加密密钥（密文）。

系统管理员登录系统后，点击“加密卡管理”->“加密卡备份”可以进入到加密卡备份页面。页面展示了历史备份信息，包括文件名、文件大小、来源、备注、创建时间等。

图 3-14 历史备份文件

3.3.4.1. 备份加密卡

点击<备份>按钮，显示当前要备份的加密卡信息，可对备份文件做备注标记，点击<提交>按钮，备份当前加密卡信息。

图 3- 15 备份加密卡

※注意：加密卡备份需将加密卡状态设置为“已启用（管理模式）”才可操作。

3.3.4.2. 编辑文件备注

点击<编辑>按钮，可以对文件的备注进行修改，点击<提交>按钮保存设置。

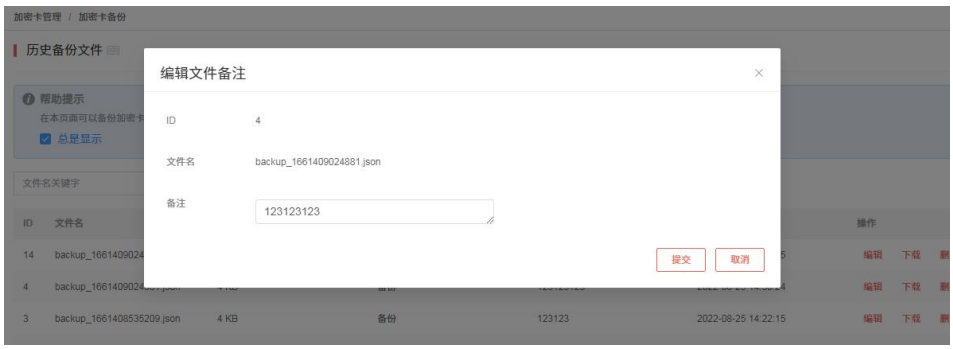

图 3- 16 编辑文件备注

3.3.4.3. 下载备份文件

点击<下载>按钮，可以下载历史备份文件，点击<保存>选择指定位置保存。

图 3-17 下载备份文件

3.3.4.4. 删除备份文件

点击<删除>按钮，可以删除历史备份文件，点击<确定>按钮删除。

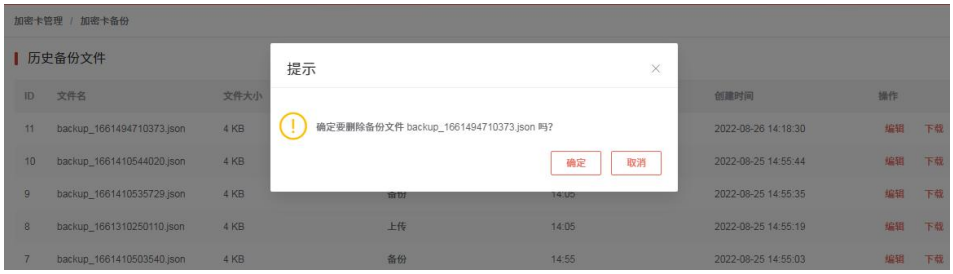

图 3- 18 删除备份文件

3.3.4.5. 恢复加密卡

系统支持将历史备份的数据恢复到相同型号的加密卡中，若有此需求，请联系我司售后技术支持人员。

3.4. 用户与角色

通过系统为角色分配权限，并将“角色”赋予用户，从而建立用户与权限之间的关联关系，实现针对用户的权限控制。系统中的权限、角色、用户设置满足“等保”测评标准中的“三权分立”要求。

3.4.1. 权限管理

系统管理员登录系统后，点击“用户与角色”->“权限管理”进入到权限列表页面。用户可以在此查看系统权限信息，包括权限名称、权限标识、是否内置、创建时间、更新时间等，见下图：

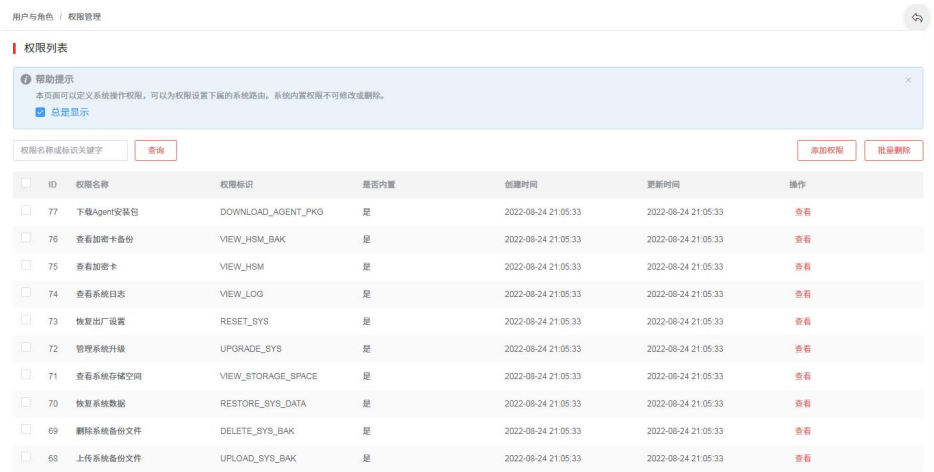

图 3- 19 权限列表

在操作区通过点击<查看>按钮，可以查看所有权限的详细信息，包括：权限

名称、权限标识、是否内置、下属路由、创建时间、更新时间。

在操作区通过点击<编辑>按钮，可以编辑自定义权限的权限名称、权限标识、下属路由。

在操作区通过点击<删除><批量删除>按钮，可以删除单个或多个自定义权限。

在操作区输入框内填写权限名称或标识关键字，点击<查询>按钮，可以对筛选查找权限。

※注意：内置权限和路由不支持编辑和删除。此功能只在系统管理员下可查看。安全管理员和安全操作员默认拥有所有的自定义权限。

3.4.2. 角色管理

系统内置 7 个角色，包括安全管理员、系统管理员、审计管理员、安全操作员、系统操作员、审计操作员、默认用户，它们的权限划分如下：

- 安全管理员拥有所有与加密管理业务相关的权限，以及对特定用户进行授权、编辑资料或重置密码等权限；
- 系统管理员拥有所有与系统配置管理操作相关的权限，以及加密卡管理、权限管理、角色管理、用户管理等权限；
- 审计管理员拥有管理系统操作日志的权限，以及对特定用户进行授权、编辑资料或重置密钥等权限；
- 安全操作员拥有所有与加密管理业务相关的权限；
- 系统操作员拥有所有与系统配置管理操作相关的权限，以及加密卡管理权限；
- 审计操作员拥有管理系统操作日志的权限；
- 默认用户拥有最低权限，仅能查看系统运行状态和统计信息；

系统管理员登录系统后，点击“用户与角色”->“角色管理”进入到角色列表页面。用户可以在此查看角色信息，包括角色名称、是否内置、创建时间、更新时间等，见下图：

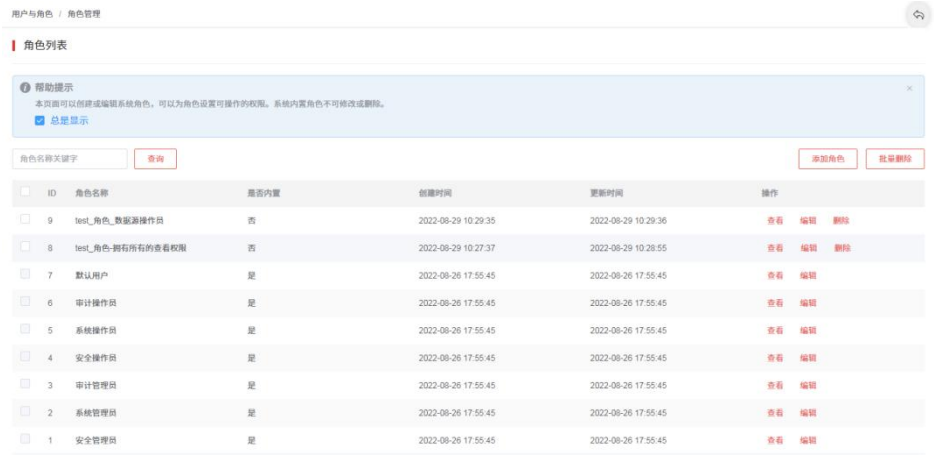

图 3-20 角色列表

在操作区通过点击<添加角色>按钮，添加新角色，相关配置内容如下表：

配置项	是否必填	说明
角色名称	是	填写角色名称，不能重复
选择权限	是	默认添加基本权限，可再另外添加权限

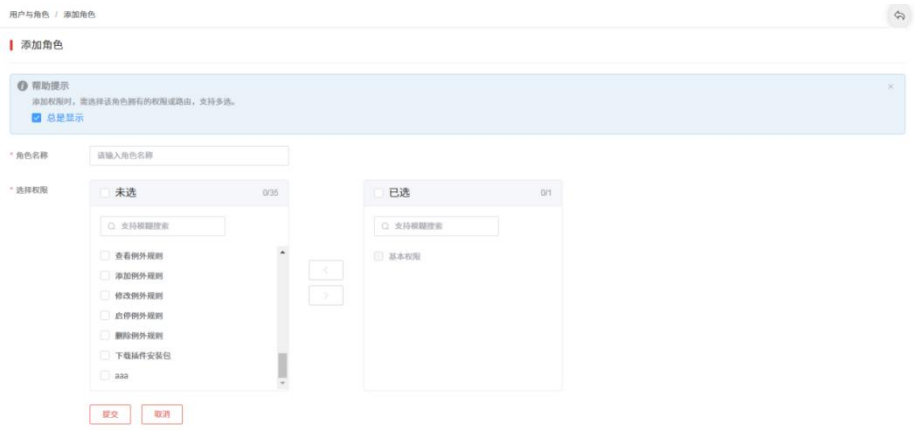

图 3-21 添加角色

在操作区通过点击<查看>按钮，可以查看所有角色的详细信息，包括：角色名称、是否内置、拥有权限、创建时间、更新时间。

在操作区通过点击<编辑>按钮，可以编辑自定义角色的角色名称、拥有权限。

在操作区通过点击<删除><批量删除>按钮，可以删除单个或多个自定义角色。

在操作区输入框内填写角色名称关键字，点击<查询>按钮，可以筛选查找相关角色。

※注意：①内置角色不支持编辑和删除。②自定义角色的权限范围不得超过安全操作员。③修改自定义角色的权限时，若该角色已绑定用户，将断开这些用户的会话，强制其重新登录。④删除自定义角色时，若该角色已绑定用户，不允许删除。⑤此功能只在系统管理员下可查看。

3.4.3. 用户管理

系统用户分为内置用户和自定义用户两类，内置用户包括 SecAdmin、SysAdmin、Auditor，分别属于安全管理员、系统管理员、审计管理员三个角色，内置用户支持查看。

3.4.3.1. 添加用户

系统管理员登录系统后，点击“用户与角色”->“用户管理”进入到用户列

表页面。用户可以在此查看用户信息，包括用户名、所属角色、是否内置、状态（正常/禁用）、UKEY（已绑定/未绑定）、最近登录时间、创建时间等，见下图：

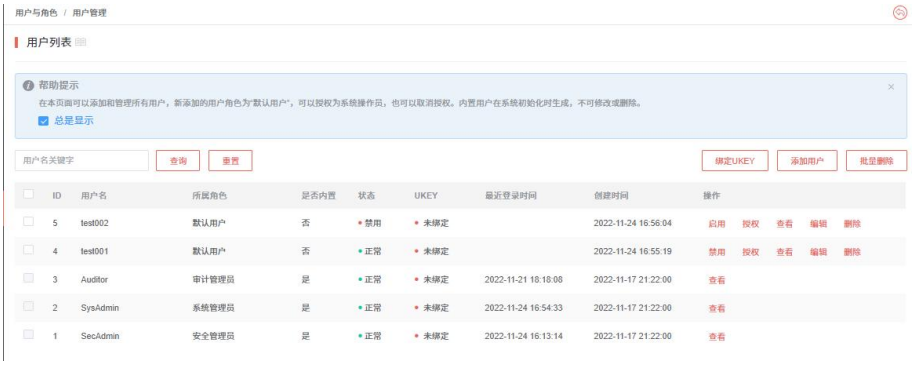

图 3- 22 用户列表

在操作区通过点击<添加用户>按钮，添加新用户，相关配置内容如下表：

配置项	是否必填	说明
用户名	是	填写用户名，长度 6-30 个字符，应具备唯一性，区分大小写，且只能由以下字符组成：英文字母、数字、下划线；
密码	是	填写密码，长度要求 10-20 个字符；至少包含大写字母、小写字母、数字、特殊字符（`~!@#$%^&*()-_=+|[{}];:'",<.>/? 和空格）中的三种；不能与用户名相同；
确认密码	是	与密码相同
真实姓名	否	填写姓名
手机号	否	填写手机号，长度 11 个字符。且应 13、14、15、18 开头，14 开头的第三位只能是 5、7，15 和 18 开头第三位不能是 4
电子邮箱	否	填写电子邮箱
状态	否	默认为启用，可选择禁用

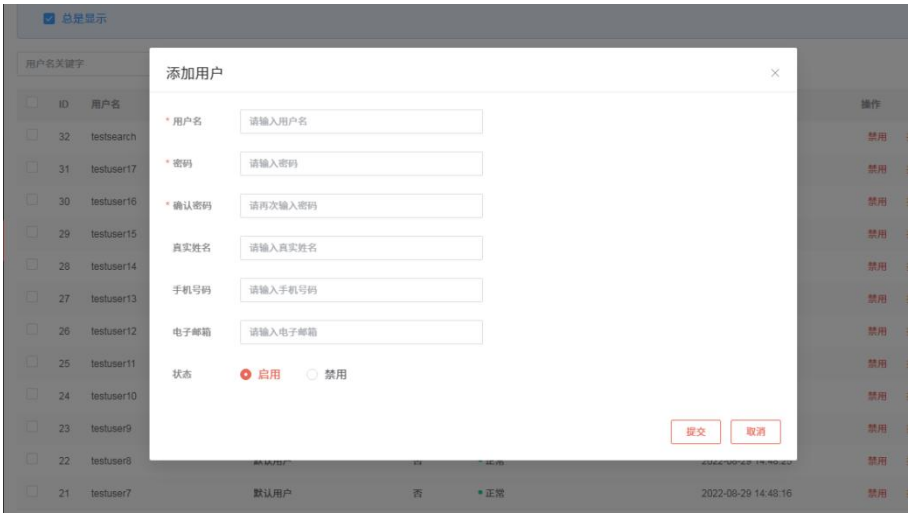

图 3- 23 添加用户

※注意：非内置用户首次登录时，需要重新设置密码。

3.4.3.2. 切换用户状态

新增用户默认为启用状态，在操作区通过点击<禁用>按钮，禁用状态下用户不可登录。

若状态为禁用状态，在操作区通过点击<启用>按钮，用户可正常登录并操作相应功能。

3.4.3.3. 授权用户

在操作区通过点击<授权>按钮，用户可查看当前用户角色，选择切换角色（只可在默认用户与系统操作员中选择），并选择是否重置密码。点击<提交>保存设置，若当前用户正在登录中，系统会主动注销该用户的会话，该用户需重新登录。

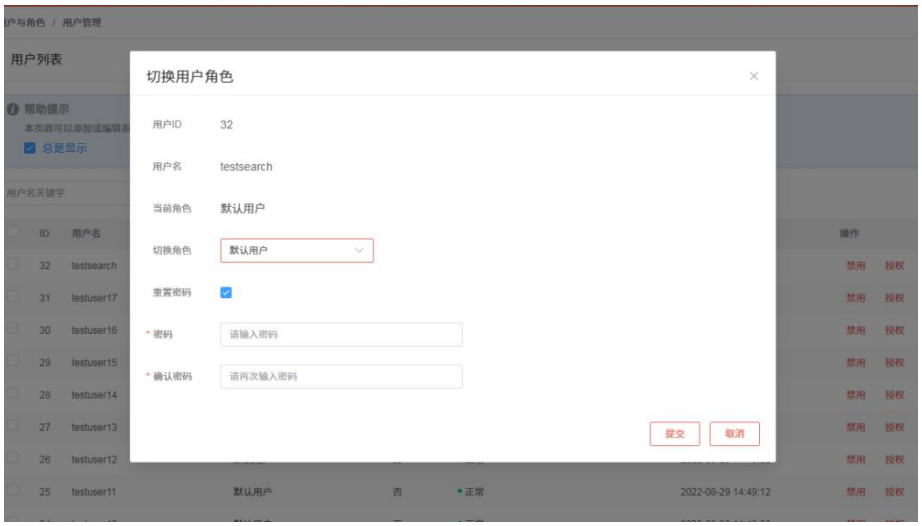

图 3- 24 切换用户角色

3.4.3.4. 查看用户

在操作区通过点击<查看>按钮，可以查看用户信息，包括：用户名、所属角色、真实姓名、手机号码、电子邮箱、状态、UKEY、是否内置、登录次数、最近登录 IP、最近登录时间、创建时间、更新时间，如下图：

图 3- 25 查看用户

在操作区输入框内填写用户名关键字，点击<查询>按钮，可以筛选查找相关用户。

3.4.3.5. 编辑用户

在操作区通过点击<编辑用户>按钮，编辑用户信息，相关配置内容如下表：

配置项	是否必填	说明
密码	否	填写密码，长度要求 10-20 个字符；至少包含大写字母、小写字母、数字、特殊字符（`~!@#$%^&*()-_=+|[{}];:'",<.>/? 和空格）中的三种；不能与用户名相同；留空表示不修改密码
确认密码	否	与密码相同
真实姓名	否	填写姓名
手机号	否	填写手机号，长度 11 个字符。且应 13、

		14、15、18 开头，14 开头的第三位只能是 5、7，15 和 18 开头第三位不能是 4
电子邮箱	否	填写电子邮箱

点击<提交>按钮保存设置；或者点击<取消>按钮取消编辑。

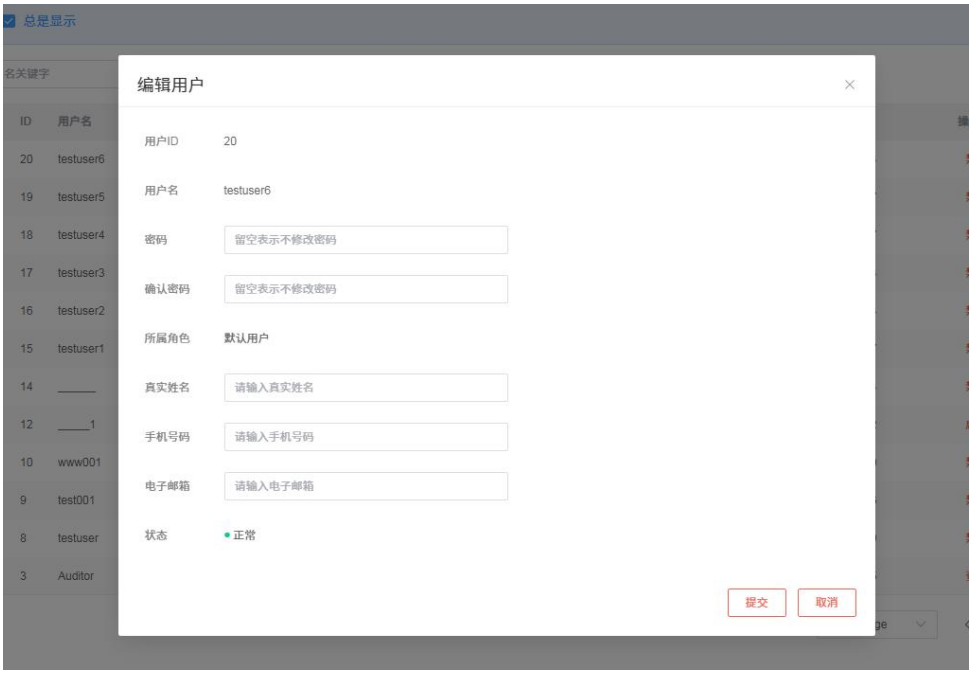

图 3- 26 编辑用户

3.4.3.6. 删除用户

在操作区通过点击<删除><批量删除>按钮，可以删除单个或多个自定义用户。

3.4.3.7. 绑定 UKey

在操作区通过点击<绑定 UKEY>按钮，将 UKey 插在设备上的 USB 接口，系统自动识别 UKey 序列号、UKey 对应的用户名。点击<绑定>即可将 UKey 与用户绑定，当 SecAdmin、SysAdmin、Auditor 三个用户都绑定 UKey 成功后，才可以开启双因子认证（见 3.5.8 章节）。

※注意：安装智能密码 UKEY 程序后，才能自动识别 UKey 信息。通过程序页面可查询 UKey 证书，修改 UKey 口令（默认密码 11111111）。若有其他问题，可寻求厂家技术支持人员帮助。

3.5. 系统管理

系统管理主要包括授权管理、接口管理、路由管理、时间管理、通知管理、系统升级、系统备份、安全设置、可靠性设置、服务设置、租户管理等功能模块，通过系统配置提供的能力完成系的安全设置基础管理工作。

3.5.1. 许可证管理

数据库加密与访问控制网关现有三个授权模块，分别为：数据库加密、访问控制、租户管理。用户可根据实际应用需要，给系统授权不同的授权模块。只有当授权相应模块后，对应功能才可正常使用，使用过程中可对授权模块做调整。不同授权模块对应的功能如下表：

授权模块	覆盖功能
数据库加密	数据源管理、插件管理、密钥管理、加密配置
访问控制	数据源管理、插件管理、访问控制
租户管理	租户管理

系统管理员登录系统后，点击“系统管理”，系统默认进入该页面，许可证管理用于对产品的授权信息进行校验，上传与当前硬件匹配且正确的许可证文件，校验通过后系统方可正常使用。通过授权界面，还可查看系统当前的软件版本、系统状态、授权到期时间、已授权的功能模块、数据源数量等信息，见下图：

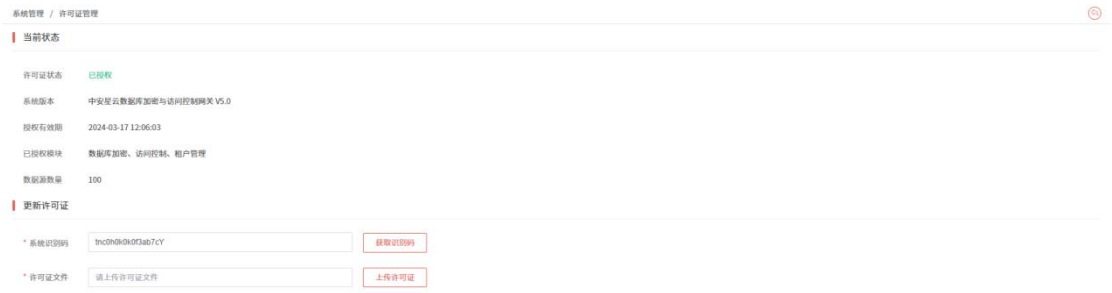

图 3- 27 授权管理

在操作区通过点击<获取识别码>按钮，用户可下载系统的授权申请文件。将该文件发送至厂家进行授权。

在操作区通过点击<上传许可证>按钮，上传已经完成授权的授权文件进行系统的激活。

在进行完授权文件激活且系统校验成功后，系统处于激活状态，各项已授权的业务方可正常使用。

※注意：在系统使用前应对授权状态给予确认。系统未授权或授权到期时，会禁用数据源管理、插件管理、密钥管理、加密配置管理、访问控制管理功能。另外，系统用户需关注授权到期时间，以免由于授权过期导致业务障碍。（在授权到期后，以下功能能够继续使用：针对已配置的加密对象，数据库写操作时的加密处理；对已配置的加密对象，数据库读操作时的解密处理；已配置并生效的读保护规则、已配置并生效的访问控制规则。）

3.5.2. 接口管理

系统管理员登录系统后，点击“系统管理”->“接口管理”进入该页面，用户可以在此查看接口的连接状态和配置接口。

此页面展示了网卡的链接状态及网卡对应的接口信息，接口信息以列表的方式进行，展示的字段包括：名称、IPv4 地址、IPv6 地址、MAC 地址、Mask（子网掩码）、状态（正常/断开）等。点击操作区的其他网卡可查看对应网卡下的接口信息。

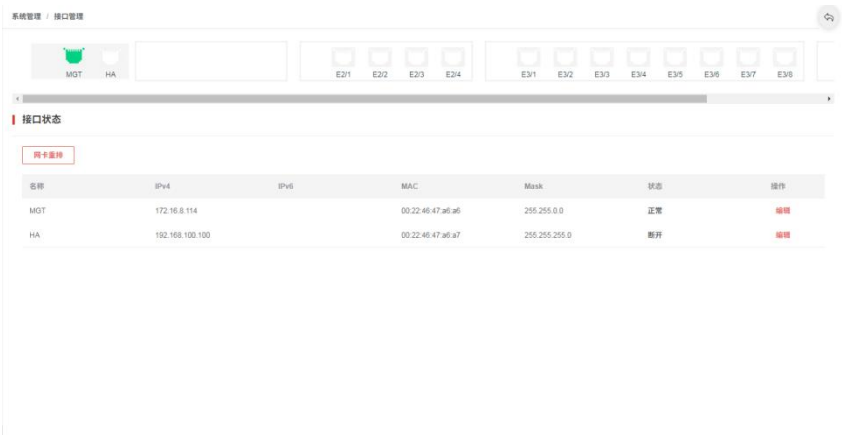

图 3- 28 接口管理

指定接口旁点击<编辑>，可以配置其接口的 IPv4 地址、IPv4 子网掩码、网关信息，编辑完成后点击<提交>即可完成添加。

图 3- 29 编辑接口

硬件设备自带扩展卡或新增扩展卡的情况，可能网卡接口显示不准确或接口编号混乱，此时要对网卡进行重新设置，点击<网卡重排>二次确认，对设备的所有网络接口进行重新排序。

图 3-30 网卡重排

※注意：操作网卡重排，设备会执行重启，需先确认是否有正在进行的加密或解密操作，以防影响业务流程。

3.5.3. 路由管理

系统管理员登录系统后，点击“系统管理”-> “路由管理”按钮进入该模块，用户可通过路由设置模块对当前系统中的静态路由进行管理，支持对系统 IPv4/ IPv6 路由信息进行查看，对静态路由进行配置。

点击静态路由表区域的<添加>按钮对路由进行配置，相关配置信息如下表所示：

配置项	是否必填	说明
选择接口	是	选择需要添加静态路由的接口名
目的 IP	是	填写目标网络地址信息，支持 IPv4
子网掩码	是	填写子网掩码，支持 IPv4
网关	是	填写网关 IP
优先级	否	填写路由的优先级

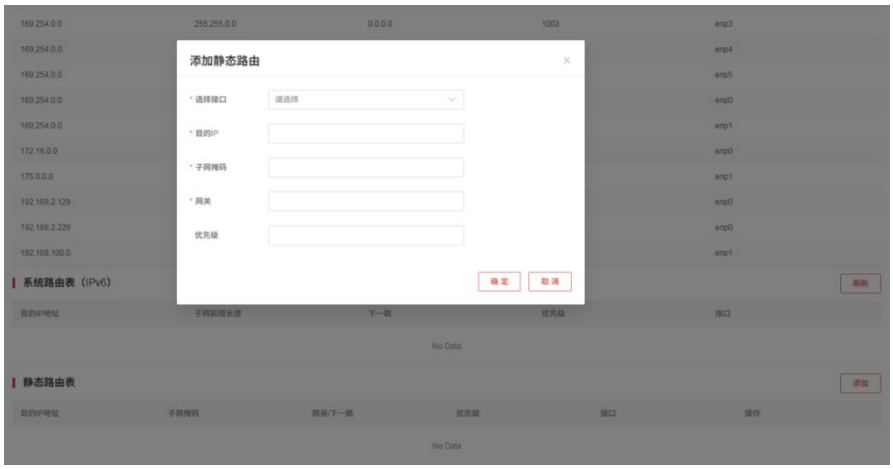

图 3-31 添加静态路由

3.5.4. 时间管理

系统管理员登录系统后，点击“系统管理”->“时间管理”进入该页面，通过系统时间配置模块使用可以对系统时间进行设置。

“服务与时间配置”的配置说明，如下表所示：

配置项	说明
时间配置	手工设置系统时间
	从时间服务器方式同步系统时间

3.5.4.1. 手动设置

在时间设置区域，可通过手工方式修改系统时间。单击“设置时间” 的配置框，将弹出日历对话框。用户可通过选择日历中的年、月、日、时、分、秒来对系统时间进行设置，然后点击<OK>按钮，实现自定义时间设置。

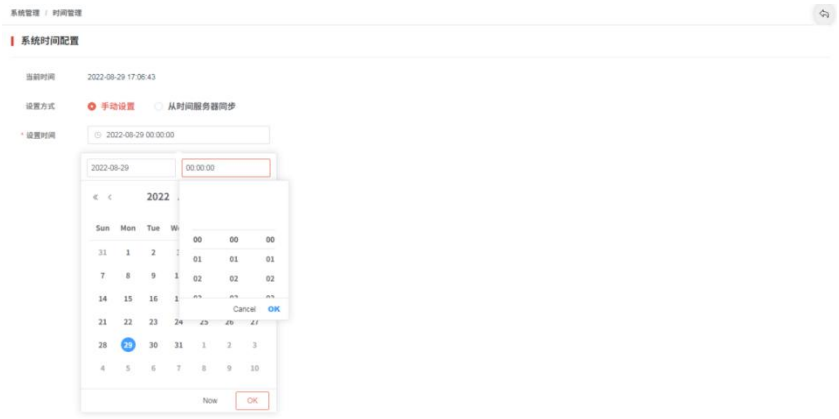

图 3-32 手动设置时间

※注意：在进行系统时间设置时应避免出现错误，以免对加密作溯源造成干扰。

3.5.4.2. 时间服务器

在时间服务器配置区域，通过设置时间服务器的 IP 地址（IPv4）及服务端口（默认端口 123）实现从时间服务器获取系统时间。系统支持配置 3 个时间服务器，若需要配置多个时间服务器，可依次选择“时间服务器 1”、“时间服务器 2”、“时间服务器 3”分别进行配置。点击<测试>按钮，系统会检测与时间服务器的连通性，点击<保存>后可完成时间服务器的定时（默认 30 分钟）同步。

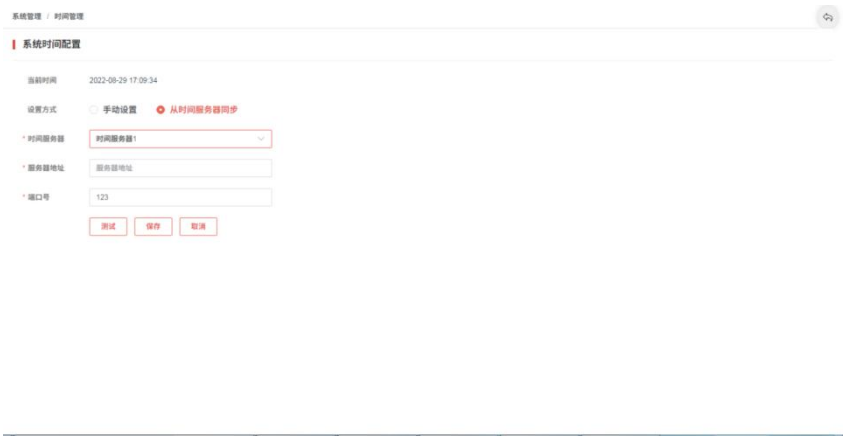

图 3- 33 从服务器同步时间

3.5.5. 通知管理

系统管理员登录系统后，点击“系统管理”->“通知管理”进入该页面管理 SYSLOG 通知配置，SYSLOG 通知默认为关闭状态，点击<编辑>可对 SYSLOG 通知进行编辑。

可以对开启状态、编码格式、远程服务址、远程服务端口、通知内容进行设置，可点击<测试>测试目标服务器的连通性，点击<保存>完成配置设置。

配置项	是否必填	说明
状态	开启或关闭二选一	默认关闭状态，可开启
编码格式	UTF-8 或 GBK 二选一	默认 UTF-8，可选择
目的服务器 IP	是	默认为 127.0.0.1，可填写 IPv4 格式
端口	是	默认 514 端口，可调整
通知内容	是	可选择系统运行日志或系统操作日志

SYSLOG 通知开启的情况下，系统会实时把已选的通知内容自动发送到到配置的远程服务地址上。

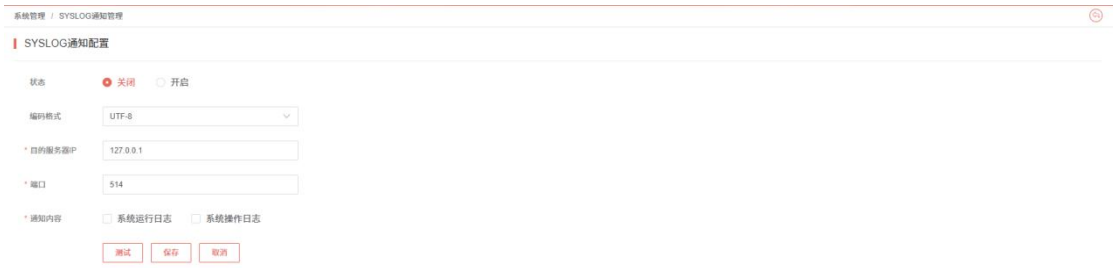

图 3- 34 SYSLOG 配置

3.5.6. 系统升级

3.5.6.1. 系统升级

系统管理员登录系统后，点击“系统管理”->“系统升级”进入该页面，通过系统升级功能，用户可对系统进行软件版本更新。点击“请上传升级文件”输入框，选择在终端内已放置好的升级文件（升级文件为.tar.gz 格式），上传文件系统会提示“操作成功”。在升级文件上传成功后点击操作区域右侧的<升级>按钮对升级进行系统。升级前系统会判断升级文件的版本信息是否正确，如果版本信息异常则不会执行升级动作。

升级列表可对系统的升级历史进行记录和查看，查看的内容包括系统升级版本、版本描述、升级时间、升级结果。

图 3-35 系统升级

※注意：升级者回退版本需要清空浏览器缓存，防止浏览器缓存机制导致操作失败。

3.5.6.2. 恢复出厂设置

系统管理员登录系统后，点击“系统管理”->“系统升级”进入该页面，点击<恢复出厂>按钮，可以恢复出厂设置.

※注意：此操作将清除所有业务数据，并将系统配置恢复至出厂状态，请慎用！双机状态下，禁止恢复出厂！

3.5.7. 系统备份

通过备份模块用户可以对系统的操作日志、配置文件等数据进行本地备份并异地上传，以提升安全性和减少系统存储压力，并可通过便捷的日志恢复功能对备份的数据进行恢复。

系统管理员登录系统后，点击“系统管理”->“系统备份”进入该页面，页面展示了存储空间的使用情况，及备份情况的记录。备份记录以列表形式展示，包括：备份时间、文件名、系统版本、文件大小、备份方式（人工备份/自动备份）、备份状态（备份成功/备份失败）、上传状态（未上传/上传成功/上传失败）等。

3.5.7.1. 人工备份

点击<备份>按钮，再点击<确定>按钮二次确认要对系统进行备份，系统提示

“操作成功”，备份记录中随即生成一条备份记录。用户可以下载或者删除备份文件，支持按关键字搜索备份文件。

图 3-36 系统备份

3.5.7.2. 自动备份

点击自动备份操作栏中的<配置>，查看当前自动备份的配置信息，包括：启用状态、备份频率、是否自动上传、本地清理等内容，见下图：

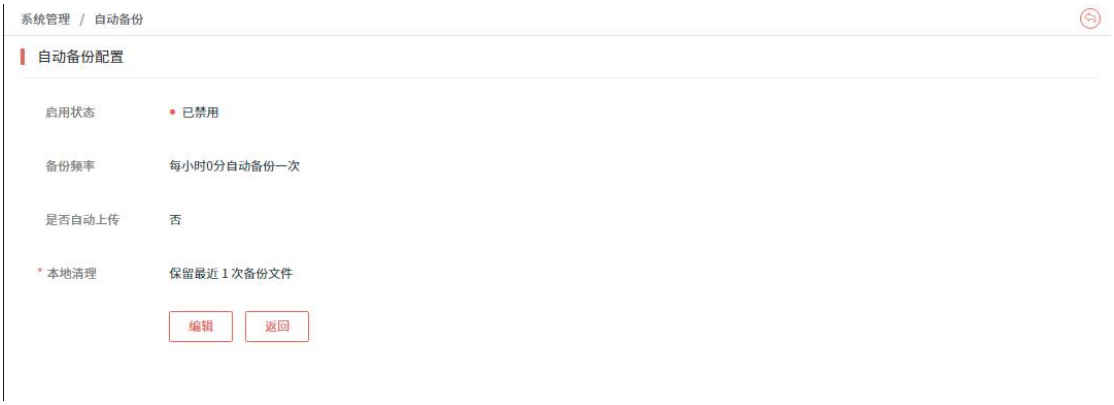

图 3-37 自动备份配置信息

点击<编辑>按钮，用户可在页面进行自动备份相关配置，相关配置内容如下表：

配置项	是否必填	说明
启用状态	启用或禁用二选一	默认为禁用，启用后，自动备份配置即时生效
备份频率	是	可按每小时几分、每天几时、每周几几时发起自动备份
是否自动上传	是或否二选一	默认为否，若选择自动上传需填写相关的上传路径信息
本地清理	是	填写 1~10 的正整数，默认为 1，本地的自动备份文件超出设置数量，将自动清理

上传方式	FTP 或 SFTP 二选一	若选择自动上传需填写，默认为 FTP，FTP 目标服务端需支持被动传输模式，否则请使用 SFTP 方式上传
编码格式	UTF-8 或 GBK 二选一	若选择自动上传需填写，默认为 UTF-8，可选择
目标服务器 IP	是	若选择自动上传需填写，仅支持编写 IPv4 格式
目标服务器端口	是	若选择自动上传需填写，填写 1~65535 的整数
登录账户	是	若选择自动上传需填写，填写有相关上传权限的账户
登录密码	是	若选择自动上传需填写，填写登录账号密码，可选择为空密码
上传目录	否	若选择自动上传需填写，上传目录是相对应服务器根目录的绝对路径，比如 ftp/data、data、data/等，若路径为空时，默认上传到服务器的根目录
失败重传次数	否	若选择自动上传需填写，可选择 0-5 次

点击<检测>，可检测目标服务器及账户是否能正常登录。点击<提交>按钮，完成自动备份设置，若目标服务器无法连通，则无法保存自动备份配置。

图 3-38 自动备份配置

3.5.7.3. 系统恢复

系统支持将历史备份的数据恢复到相同版本的系统中，若有此需求，请联系我司售后技术支持人员。

3.5.8. 安全设置

系统管理员登录系统后，点击“系统管理”->“安全设置”进入该页面，点击<编辑>可以设置登录安全参数和密码参数，以提升系统的登录安全性。

安全设置包括：登录安全参数、登录会话超时、密码长度参数、密码过期参数、双因子身份验证、文件下载密码验证六部分内容。双因子认证开启后，用户需插入已绑定的 UKey 才可登录系统。文件下载密码验证开启后，在系统内下载文件需输入正确密码才可下载。

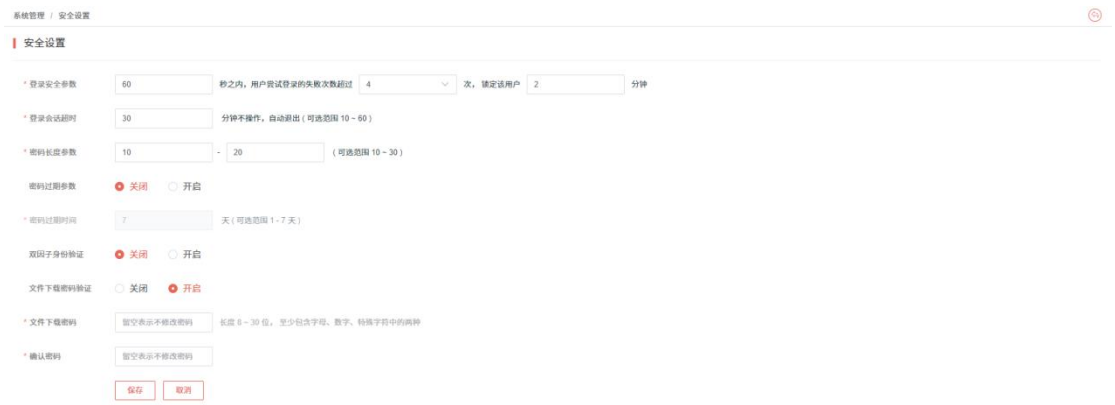

图 3-39 安全设置

3.5.9. 可靠性设置

对设备进行可靠性设置，目的是保障业务连续性的有效方案。此系统支持双机主备工作模式，若将两台设备进行 HA 主备设置，那双机间配置能实时同步，当一台设备出现问题时，另一台设备可立即接管，保证用户的业务不间断，把故障对业务的影响降到最小。

HA 部署方式下，要求两个系统硬件型号、内存容量、CPU 型号、硬盘容量均相同；软件版本、许可证授权模块、系统语言一致；加密卡已初始化、型号相同且 KEK 已经同步，且模式为常规模式。另外，为确保重要数据不丢失，备机需清空绑定插件，且各数据源无选择加密方案。

系统管理员登录系统后，点击“系统管理”->“可靠性设置”进入该页面。HA 管理分为两部分，包括：HA 设置和 HA 运行日志。

3.5.9.1. HA 设置

在“HA 设置”标签页中，用户可以查看双机信息和配置 HA。

1）双机信息

当未做 HA 设置时，双机信息只能显示本机 SN 码，运行模式为单机模式，如下图：

图 3-40 HA 管理-未做配置

当完成主备 HA 设置并且连接成功时，双机信息显示本机和对端的 SN 码、运行模式、HA 接口 IP 和 HA 启动时间，如下图：

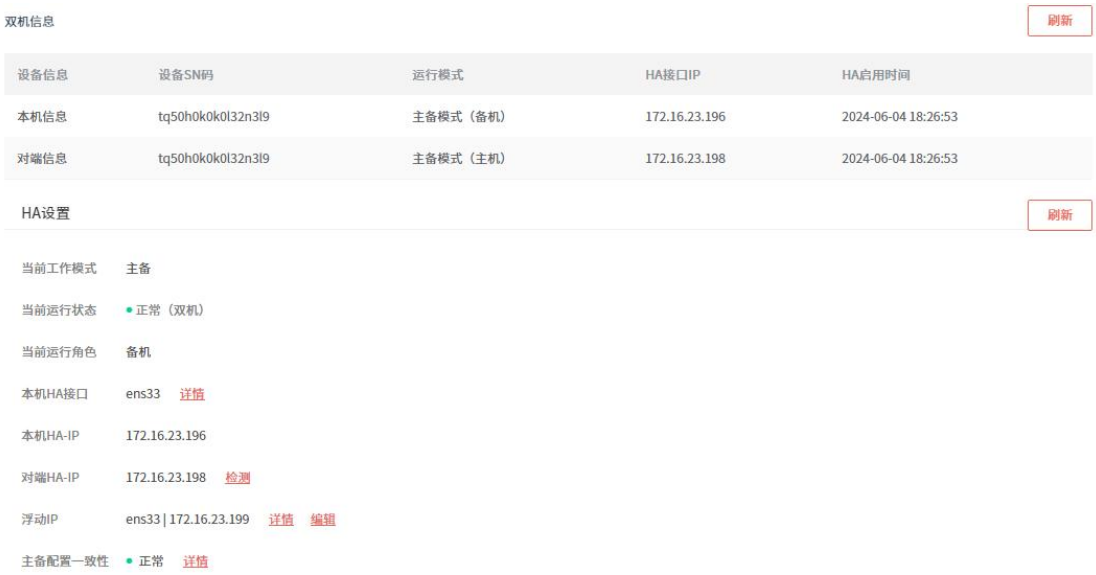

图 3-41 HA 管理-已做配置

2）切换为双机模式

建立 HA 前需满足以下条件：系统初始版本号、升级记录一致；授权状态、授权模块、授权数据源数量一致；安装时的 OEM 参数、设备类型参数、默认语言参数一致；系统时区、系统时间、web 服务端口、SNMP 状态、SYSLOG 状态一致；加密卡型号、状态、KEK 一致；未被数据安全平台纳管。

当前运行模式为单机模式时，只显示当前运行模式信息，可将模式设置为双机模式，点击<切换为双机模式>按钮，用户可在 HA 设置弹窗中进行相关配置，相关配置内容如下表：

配置项	是否必填	说明
工作模式	否	显示目标工作模式，当前应为“主备模式”
本机运行角色	主机和备机二选一	在主机和备机中二选一，默认为主机
本机 HA 接口	是	在现有接口中选择，推荐选择 HA 接口
HA-IP 地址	是	若接口已经配置了 IP 和子网掩码，自动匹配 IP。若无配置或需要修改，可点击<去设置>快速跳转“接口管理”页面进行设置，本机端口号需与对端一致
子网掩码	是	若接口已经配置了 IP 和子网掩码，自动匹配子网掩码。若无配置或需要修改，可点击<去设置>快速跳转“接口管理”页面进行设置
对端 HA-IP	是	仅支持填写 IPv4 格式，对端端口号需与本机一致
浮动 IP 接口	是	在现有接口中选择，不建议共用 MGT 接口
浮动 IP	是	仅支持填写 IPv4 格式，不可与本机/对端 HA-IP 一致，一对主备机的浮动 IP 应相同
子网掩码	是	填写格式如：255.0.0.0

点击<检测>，可检测对端 HA 接口及 IP 连通性。点击<提交>按钮，完成 HA 设置。

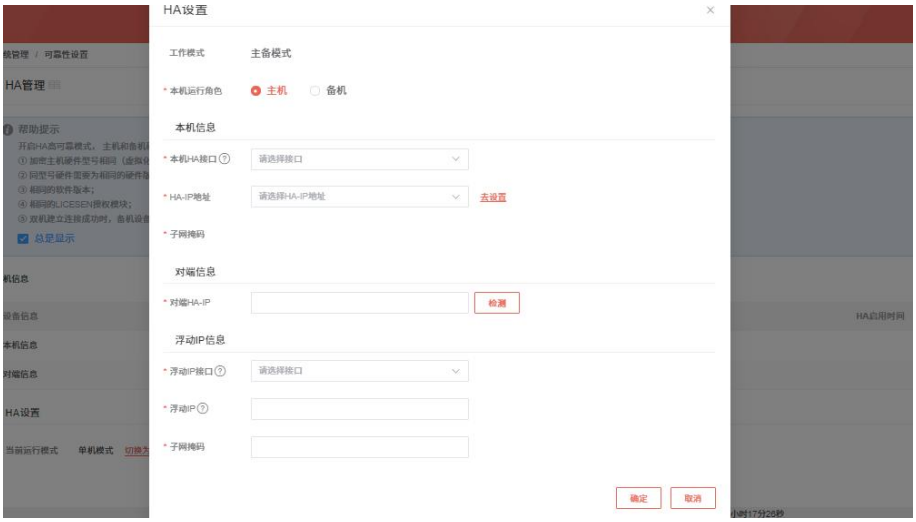

图 3-42HA 设置

主备机任意一角色均可先行配置，配置完成后，进入到“待启用”模式，等待与对端建立连接，“待启用”状态的有效时间为 10 分钟，到期后若未能与对端建立连接，状态变回“单机”。

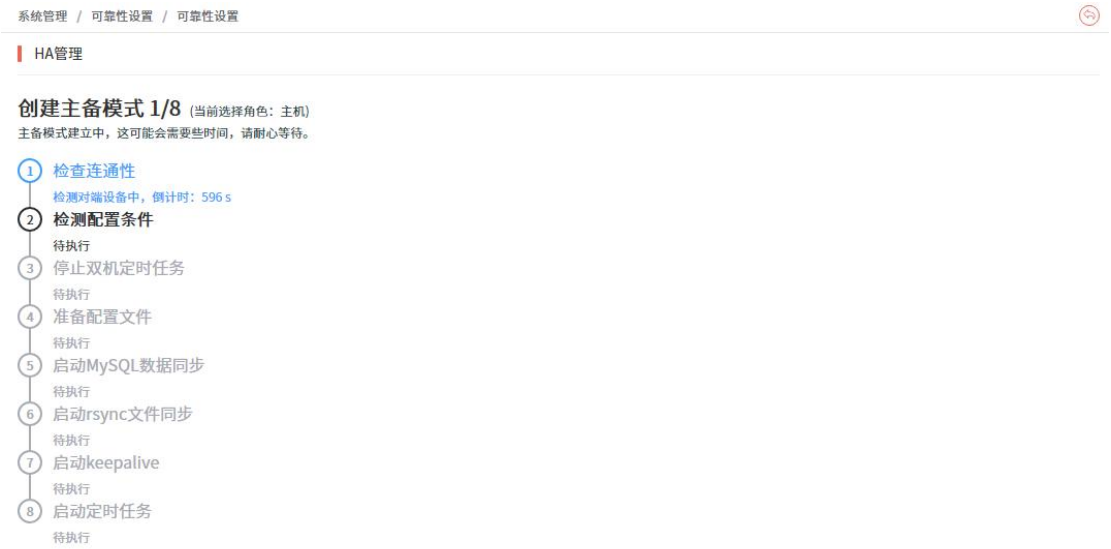

图 3-43 创建主备模式进度

若创建主备模式失败，页面将显示失败原因，可根据提示进行修改再重新配置。

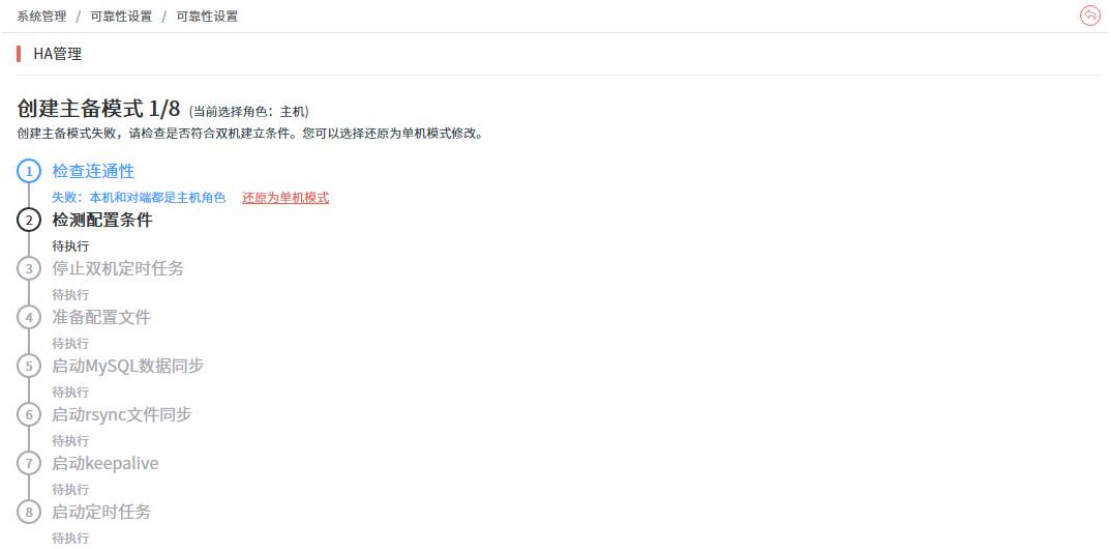

图 3-44 创建主备模式失败原因

※注意：①主备模式建立成功后，备机设备上的信息会被初始化（除加密卡信息）。②双机状态为“待启用”“启用中”“启用失败”时，备机将会限制数据源、插件、加密配置、访问控制和加密卡等功能的操作。③双机模式下不允许对设备进行以下操作：安装补丁包、升级软件版本、进行系统重装操作、恢复系统出厂设置、修改接口 IP（页面或后台）。如需进行这类操作，需要先将双机状态切换成单机状态。④主备模式建立成功后，被数据安全平台纳管时，须使用浮动 IP 进行纳管

3）切换为单机模式

当前运行模式为主备模式时，主机用户可将模式设置为单机模式，点击<切换为单机模式>按钮，可切换为单机模式。此操作需双机运行状态为“正常”情况下才可操作，否则不允许切换为单机。

※注意：当双机建立成功后，只能从主机上切换为单机模式，切换后原备机自动切换为单机模式，且数据被清空。

4）查看 HA 设置

进行完主备模式设置提交成功后，双机信息下会显示对端的角色和 HA 接口 IP。HA 设置下会显示配置信息，用户可查看当前运行模式、当前运行状态、当前运行角色、本机 HA 接口、本机 HA-IP、对端 HA-IP、浮动 IP、主备配置一致性。

点击本机 HA 接口的<详情>按钮，可查看本机 HA 接口状态，接口、IPv4、MAC、子网掩码、状态等信息。

点击浮动 IP 的<详情>按钮，可查看浮动 IP 的接口状态、IPv4、MAC、子网掩码、状态等信息。

若当前运行状态异常，可根据提示，查看异常原因。

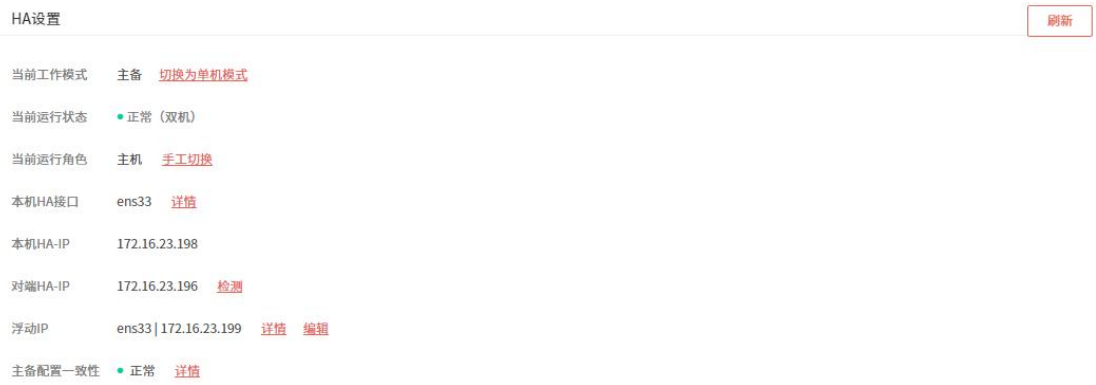

图 3-45 主备模式下 HA 详情

5）手工切换

当模式为主备模式，运行状态为正常时，可在主机上强制进行主备机切换，即主备机角色互换。切换详情可在“HA 运行日志”中查看。

※注意：当手工切换进行中时，禁止其他操作。

6）修改双机模式

若需修改浮动 IP，可以点击<编辑>，对浮动 IP 的接口、IP、子网掩码进行修改。

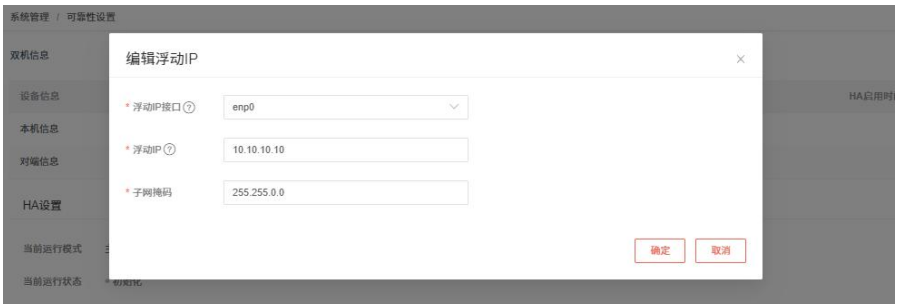

图 3- 46 修改浮动 IP

若需修改本机或对端 IP 信息、角色信息，需先将主备机的工作模式均切换为单机模式，再重新进行 HA 配置。

7）主备配置一致性

操作区可查看主备配置一致性的状态，点击一侧的<详情>按钮，可查看检测详情。在弹框内点击<检测>可发起再一次检测，若检测结果为“不通过”，可根据提示查看不通过原因。

图 3-47 主备配置一致性

※注意：禁止主备机同时点击主备配置一致性的<检测>按钮。

3.5.9.2. HA 运行日志

在操作区通过点击“HA 运行日志”标签进入到 HA 运行日志列表，用户可以在此查看日志信息，包括日志描述、操作类型、操作结果、操作人、操作客户端 IP、更新时间等，见下图：

图 3-48 HA 运行日志

在操作区输入框内填写日志 ID 或内容关键字，点击<查询>按钮，通过简单查询可以筛选查找相关日志信息。

在操作区通过点击<高级搜索>按钮，可以进行高级搜索查询，筛选内容包括：关键字、操作客户端 IP、状态、更新时间范围。点击<查询>按钮，可以根据配置的条件进行查询。点击<重置>按钮，可以清空筛选条件和取消列表按条件展示。

3.5.10. 服务设置

系统管理员登录系统后，点击“系统管理”->“服务设置”进入该页面。服务设置分为两部分，包括：WEB 服务配置和 SNMP 服务配置。

3.5.10.1. WEB 服务配置

在 WEB 配置中，可设置对本系统的 WEB 页面访问进行控制。可设置 IP 白名单的状态，是开启或者关闭。

配置项	是否必填	说明
端口	是	系统 WEB 服务的默认端口号为 443，禁止使用下列端口：1~1024（443 除外）、2222、3306、6379、8080、8086、50024、50025、50032
IP 白名单	关闭或开启二选一	关闭即不设置 web 访问策略，所有地址均可访问系统 web 服务；开启即只有在白名单内的 IP 地址才能访问系统 WEB 页面。支持输入单个或多个 IP、IP/子网（表示 IP 范围），使用逗号（,）分隔。如：172.16.1.100（单个 IP）,172.16.10.0/24（IP/子网）

图 3- 49 WEB 服务配置

3.5.10.2. SNMP 服务配置

简单网络管理协议（SNMP），由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资源对象。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。

通过 SNMP 配置可以对 SNMP 服务进行设置，查看常用节点信息列表，包括：OID、名称、描述。在 SNMP 服务开启状态下，可查看常用节点具体信息。

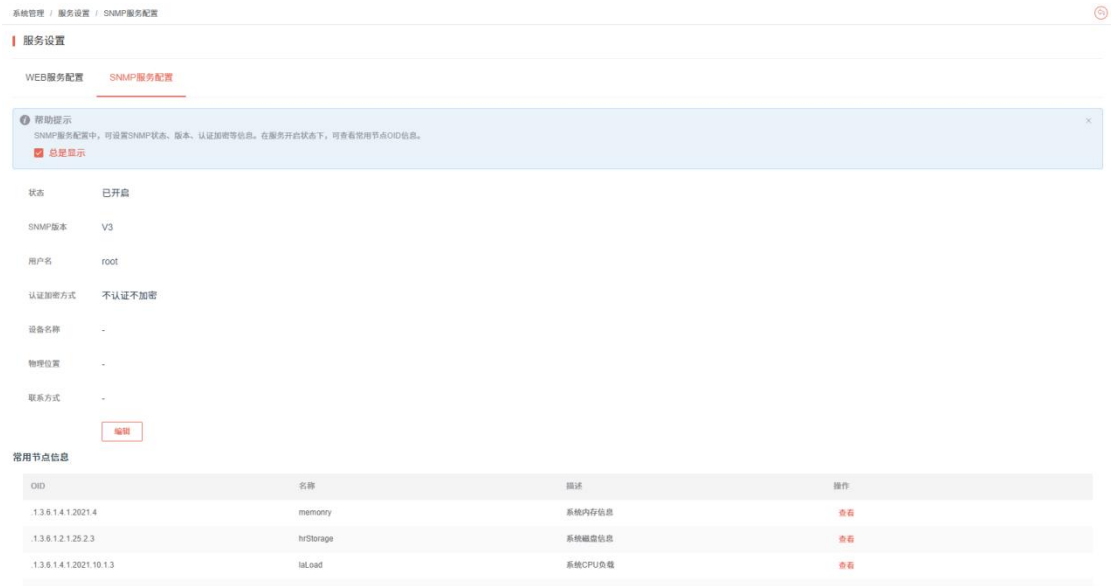

图 3- 50 SNMP 配置

配置项	是否必填	说明
状态	关闭或开启 二选一	默认为关闭状态，可开启
SNMP 版本	V1&V2 或 V3 二选一	默认为 V1&V2 版本，可选择

团体名	是	仅选择 V1&V2 版本时需要填写，默认为 public，可修改
设备名称	否	填写设备名称，长度 1~30 位
物理位置	否	填写设备的物理位置，长度 1~30 位
联系方式	否	填写设备的联系人方式
认证加密方式	不认证不加密或认证加密或仅认证，三选一	仅选择 V3 版本时需要选择认证加密方式
认证方式	SHA 或 MD5 二选一	当选择认证时需选择，SHA 和 MD5 为认证方式的算法
认证密码	否	长度 8~30 位， 至少包含字母、数字、特殊字符中的两种，留空表示不修改密码
加密方式	DES 或 AES 二选一	当选择加密时需选择，DES 和 AES 为认证方式的算法
加密密码	否	长度 8~30 位， 至少包含字母、数字、特殊字符中的两种，留空表示不修改密码

图 3-51SNMP-V1&V2

图 3-52SNMP-V3 不认证不加密

图 3-53SNMP-V3 认证及加密

图 3- 54SNMP-V3 仅认证

3.5.11. 租户管理

系统支持多租户管理，能够实现多个租户共享系统的程序和功能模块，各租户之间数据和配置相互隔离。隔离后，租户内的用户只能操作租户内被允许的操作，只能访问租户内被允许访问的数据，对租户内的用户来说，他访问的是一个相对独立的系统。

租户之间可共享系统的一些配置功能，且互不干扰，这些功能包括：

- 角色管理
- 用户管理
- 数据源管理
- 插件管理
- 密钥管理
- 密钥模板管理
- 加密策略管理
- 访问控制管理
- 日志管理
- 系统信息

系统运行环境所依赖的公共配置是租户共享的，为避免配置冲突，其对应的配置功能禁止在租户内使用，具体包括：

- 加密卡状态切换
- 加密卡备份
- 系统权限管理
- 授权管理
- 接口管理
- 路由管理
- 时间管理
- SYSLOG 通知配置
- 系统升级与还原
- 安全设置
- 可靠性设置
- 服务设置
- 租户管理

租户间形成配置及数据隔离，但是系统内置管理员（SysAdmin、SecAdmin、Auditor）可以查看并操作租户所创建的数据，在租户内操作新产生的数据也限制在该租户内使用。

3.5.11.1. 添加租户

系统管理员登录后，点击 “系统管理”->“租户管理”进入该页面。用户可以在此查看系统的租户信息，包括租户名称，以及其三位管理员的账号信息（安全管理员、系统管理员、审计管理员），当前状态（正常/禁用）和创建时间等，见下图：

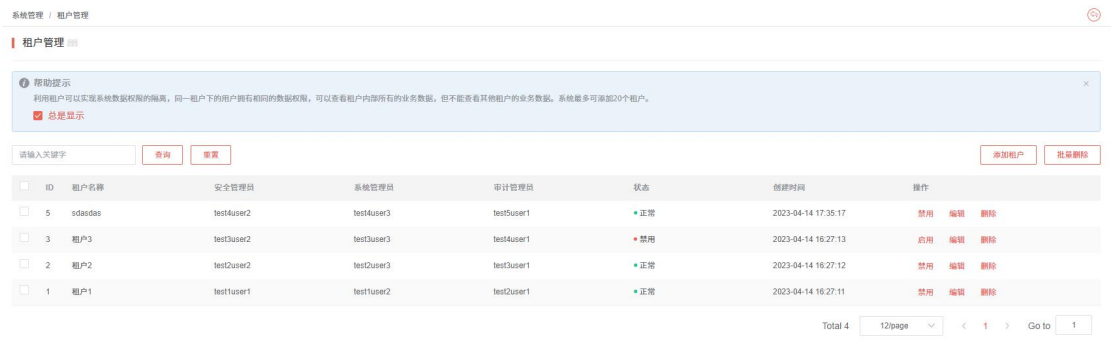

图 3-55 租户管理

在操作区通过点击<添加租户>按钮，添加新租户，相关配置内容如下表：

配置项	是否必填	说明
租户名称	是	填写租户名称，不能重复
安全管理员	是	只可选择角色为“默认用户”且状态为启用

		的用户，同一租户内的管理员账号不能重复
系统管理员	是	只可选择角色为“默认用户”且状态为启用的用户
审计管理员	是	只可选择角色为“默认用户”且状态为启用的用户
状态	启用或禁用二选一	默认为启用状态，可禁用
备注	否	填写该租户的备注信息，长度不超过 100 个字符

图 3-56 添加租户

点击<提交>按钮保存设置；或者点击<取消>按钮取消编辑。

租户添加成功后，不可修改内置的管理员。

在操作区输入框内填写用户名关键字，点击<查询>按钮，可以筛选查找相关用户。

3.5.11.2. 编辑租户

在操作区通过点击<编辑>按钮，编辑租户信息，相关配置内容如下表：

配置项	是否必填	说明
租户名称	是	填写租户名称，不能重复
备注	否	填写该租户的备注信息，长度不超过 100 个

		字符

点击<提交>按钮保存设置；或者点击<取消>按钮取消编辑。

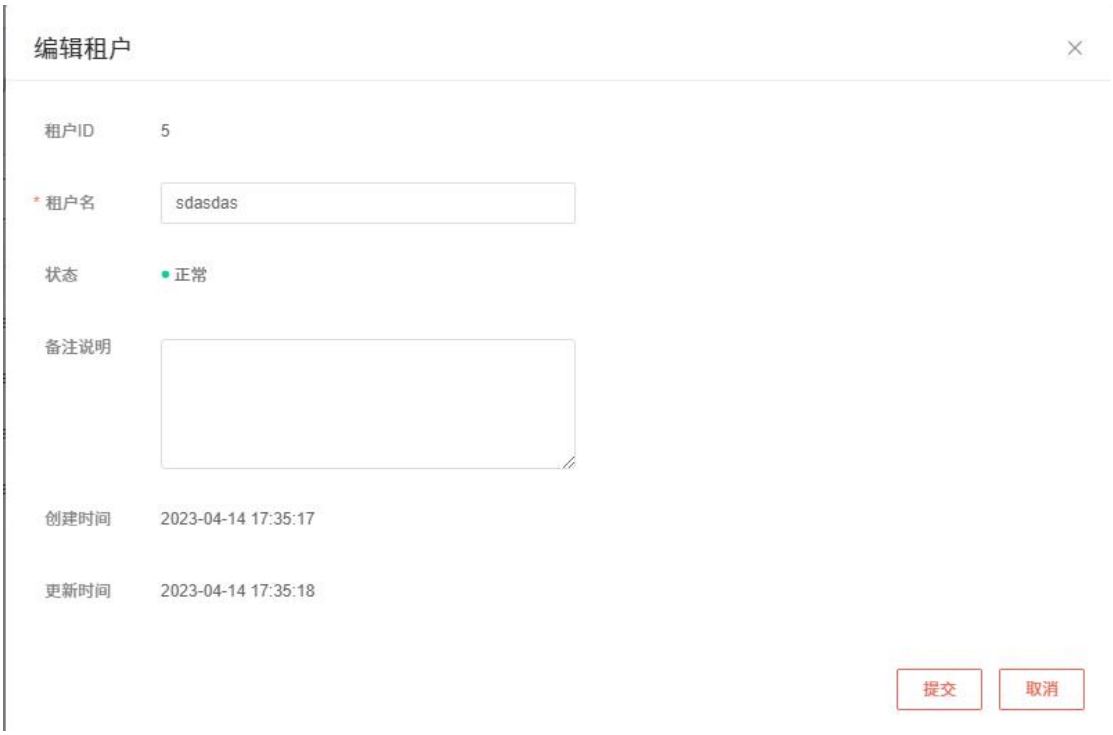

图 3-57 编辑租户

3.5.11.3. 禁用租户

在操作区通过点击<禁用>按钮，用户可禁用当前租户。点击<确认>保存设置，若当前租户内用户正在登录中，系统会主动注销该用户的会话。禁用后，该租户下的所有用户禁止登录和使用系统，但系统内置管理员（SysAdmin、SecAdmin、Auditor）仍可查看和管理该租户下的配置。

图 3-58 禁用租户

3.5.11.4. 启用租户

在操作区通过点击<启用>按钮，用户可启用当前租户。点击<确认>保存设置，启用后，该租户下的所有用户可正常登录和使用系统，

图 3-59 启用租户

3.5.11.5. 删除租户

在操作区通过点击<删除><批量删除>按钮，二次确认输入登录密码可以删除单个或多个租户。

※注意：租户下存在数据源时禁止删除租户；删除租户后，会同时删除该租户下所有除内置管理员之外的其他用户，并将租户的内置管理员还原成系统“默认用户”。

3.5.11.6. 切换租户

当系统授权租户管理模块后，系统上方导航栏会显示当前所在租户，默认为全局。

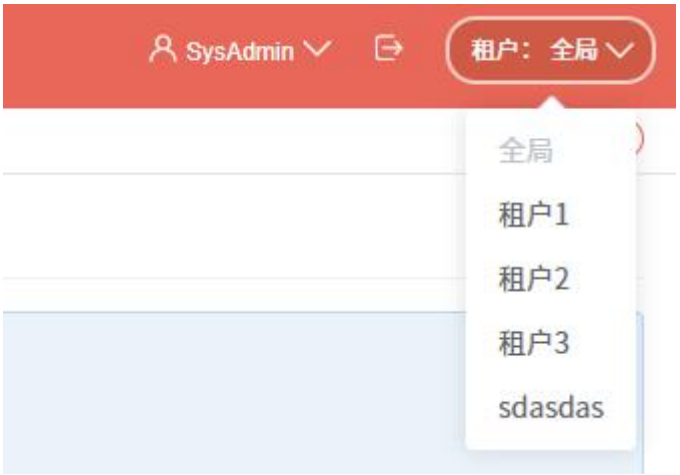

图 3-60 切换租户

※注意：租户登录时，不会显示该按钮。

3.6. 系统信息

3.6.1. 系统状态

系统管理员登录后，点击 “系统信息”->“系统状态”进入该页面。系统状态是对系统设备运行环境状态的实时监控，包括 CPU 使用率、内存使用率、数据空间使用情况和硬盘容量使用情况，帮助用户判断当前系统性能压力。

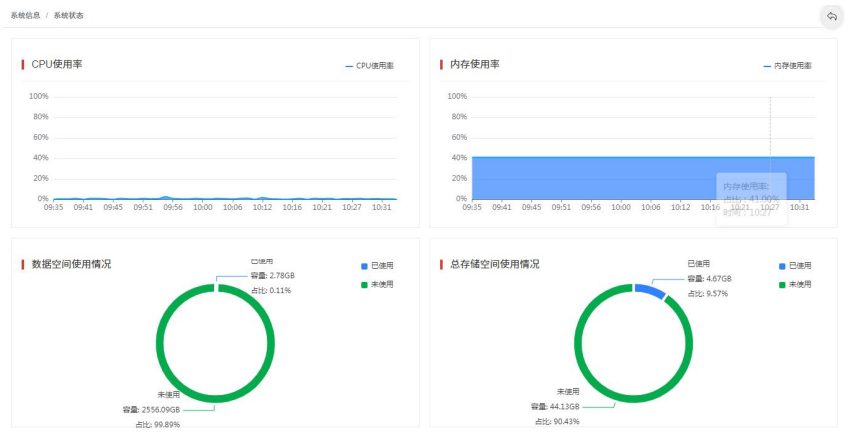

图 3-61 系统状态

3.6.2. 帮助手册

帮助手册是系统所有配置文档及规格文档的汇总，包括加密插件的下载与安装、启用和配置 Oracle 数据库 NTE 功能的方法、MySQL v8.0.4 及以上版本配置加密目录的方法、各数据库的加密方案及算法支持规格、MySQL 数据库安装 SM4 算法插件的方法、SQL Server 数据库安装 SM4 算法插件的方法等。

系统管理员登录后，点击 “系统信息”->“帮助手册”进入该页面，见下图：

图 3-62 帮助手册

3.7. 个人中心

系统管理员登录系统后，点击右上角“SysAdmin”，用户可以修改系统管理员的资料或者密码。

图 3-63 个人中心

3.7.1. 修改密码

系统管理员登录系统后，点击右上角“SysAdmin”->“修改密码”，用户需输入旧密码和新密码，点击<提交>保存密码设置，系统管理员自动登出系统。

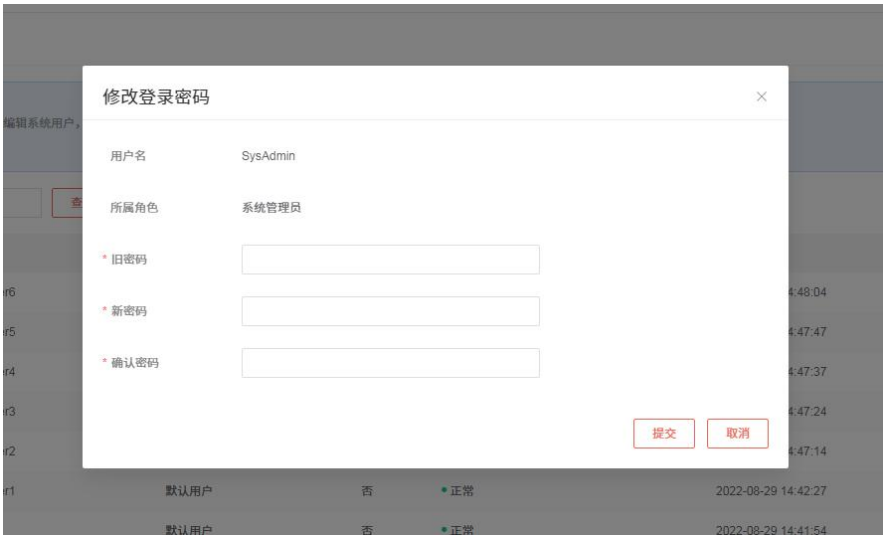

图 3- 64 修改登录密码

3.7.2. **修改资料**

系统管理员登录系统后，点击右上角“SysAdmin”->“修改资料”，用户可以修改真实姓名、手机号和电子邮箱，点击<提交>保存修改设置。

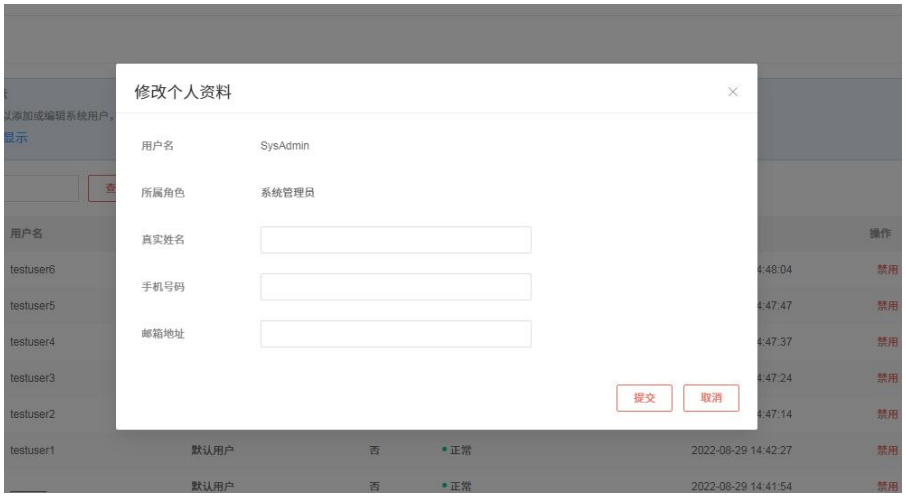

图 3- 65 修改个人资料

4. 安全管理

4.1. 概述

安全管理需使用安全管理员登录产品进行相关设置，安全管理员是数据库加密与访问控制网关三大管理员之一，主要负责业务流程管理。可管理数据资产、创建主密钥、管理数据加密密钥、添加加密对象、管理访问控制等。

安全管理包含内容见下表：

主菜单	分类	功能说明
首页	业务基础数据统计	当前备用、在用、历史密钥数量；当前数据源总量、数据源状态异常数量、数据源类型分布
		当前加密表数、未加密表数统计
		最新加密对象信息
	其他数据统计	当前加密卡信息和状态
		当前插件总量、插件状态异常数量
	系统资源统计	CPU、内存的准实时占用率统计；系统接口准实时接收/发送流量统计
资产管理	数据源管理	添加、查看、编辑数据源，对数据源进行架构扫描
	插件管理	添加、查看、编辑插件信息，下载插件，查看插件的运行日志
密钥管理	主密钥管理	创建主密钥（首次登陆时）、查看主密钥信息
	备用密钥库	添加、查看、删除密钥
	在用密钥库	查看密钥详情、查看密钥的应用情况
	历史密钥库	查看、删除密钥
	密钥模板管理	添加、查看、删除密钥模板
策略管理	加密配置	选择、配置、取消加密方案
		添加、编辑、删除加密对象
		加密、解密、还原加密对象

	读保护	开启或关闭读保护、配置读保护的例外规则
	访问控制	切换访问控制模式、创建访问控制规则
用户与角色	用户管理	授权（可授权为安全操作员或自定义角色）、编辑、查看用户详情
系统信息	系统状态	CPU、内存的近 1 小时占用率统计；数据空间、总储存空间使用情况
	帮助手册	查看系统使用中相关的配置指导手册
个人中心	修改资料	修改个人资料
	修改密码	修改个人密码

4.2. 首页

安全管理员在登录后默认进入首页界面，页面内容与系统管理员登录后的首页一致，详情可查看 3.2 章节。

4.3. 资产管理

资产管理功能主要包括数据源管理和插件管理两部分，此处数据源即为数据库。若所添加数据库的加密方案选择表空间加密，那该加密方案的实现需要依赖加密插件，在对数据库进行加密配置之前，需将加密插件安装部署到数据库的操作系统中。不同数据库的环境不同，部署方案也不一致。插件与数据库可以为一对多的关系，即一个插件同时被多个数据库使用。一般情况下，单库部署的数据库对应安装一个插件即可；集群部署的数据库需要依据集群的工作机制，在数据存储节点上部署插件，或在集群各节点上分别部署插件，具体可咨询售后支持人员。

4.3.1. 数据源管理

安全管理员登录系统后，点击“资产管理”->“数据源管理”进入到数据源列表页面。用户可以在此查看数据源信息，包括数据源名称、服务类型、地址:端口、部署方式、连接状态、检测时间等，见下图：

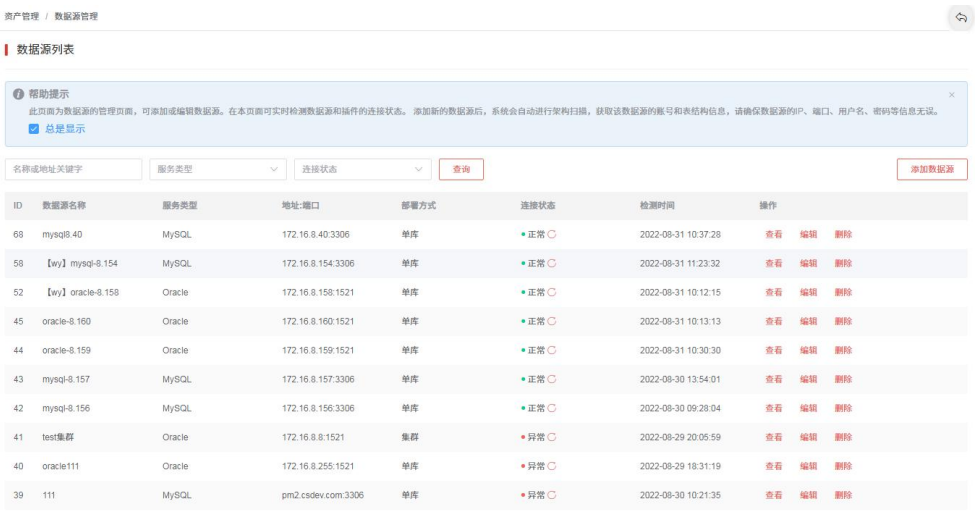

图 4-1 数据源列表

4.3.1.1. 添加数据源

在操作区通过点击<添加数据源>按钮，添加新数据源，相关配置内容如下表：

配置项	是否必填	说明
名称	是	数据源名称应具有唯一性，不可重复，30 个字符以内
服务类型	是	数据库的服务类型，如 MySQL
IP	是	数据库的 IP 地址，支持 IPv4 格式
端口	是	数据库的服务端口
使用 SSL	否	MySQL、PostgreSQL、GaussDB 等数据库需选择：“不启用 SSL”、“启用 SSL，但不强制使用”、“启用 SSL，并强制使用”，三选一
部署方式	是	数据库的部署方式：单库或集群
集群同步方式	特定数据库时必填	PostgreSQL 数据库集群部署时需在流复制与逻辑复制中二选一；MySQL 数据库集群部署时需在双主模式和主从模式中二选一；Oracle 数据库集群部署时需在 RAC 和 DG 中二选一
子库地址	是	数据库为集群时，其子库的 IP 地址，要求 IPv4 格式
子库端口	是	数据库为集群时，其子库的服务端口
服务名	特定数据库时必填	连接 Oracle 数据库时使用的服务名
数据库名	特定数据库时必填	连接 PostgreSQL、GaussDB、AtlasDB、SQL Server 等数据库时使用的数据库名

用户名	是	连接数据库时使用的账号
账号角色	Oracle 数据库时必填	连接 Oracle 数据库时使用的账号角色，可选项包括：Normal、DBA、SYSOPER
密码	是	填写连接数据库时使用的密码，可选择空密码

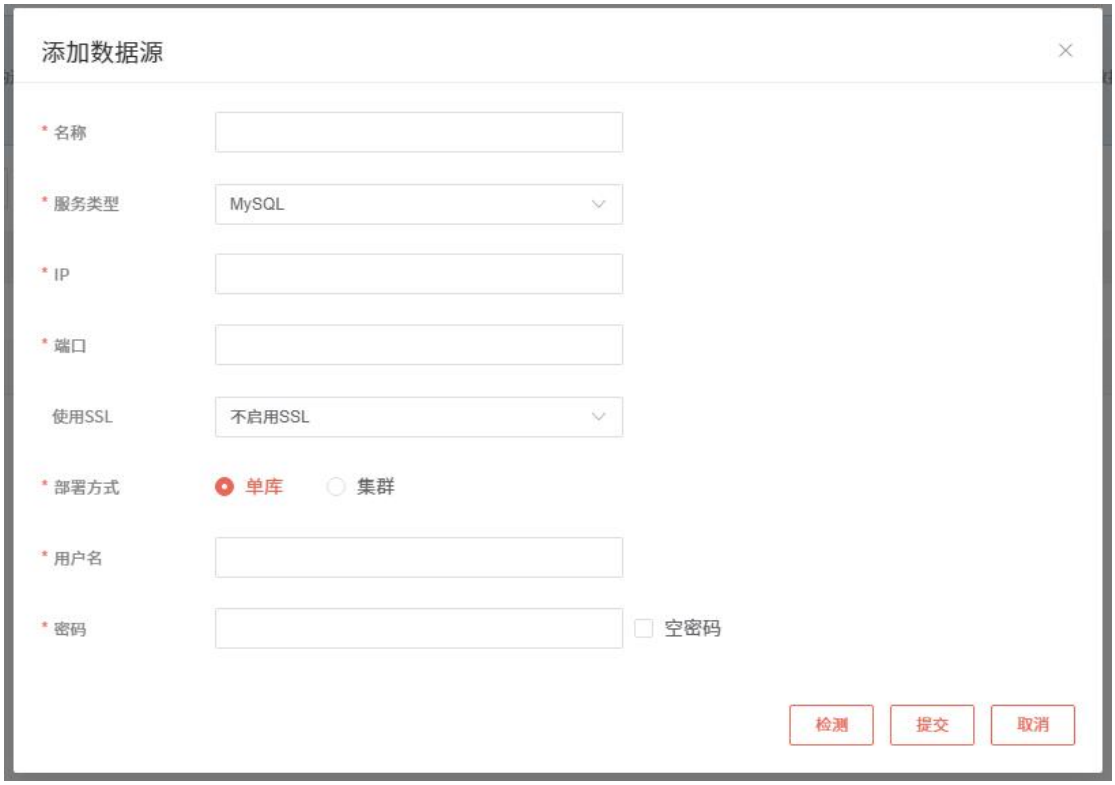

图 4- 2 添加数据源-单库

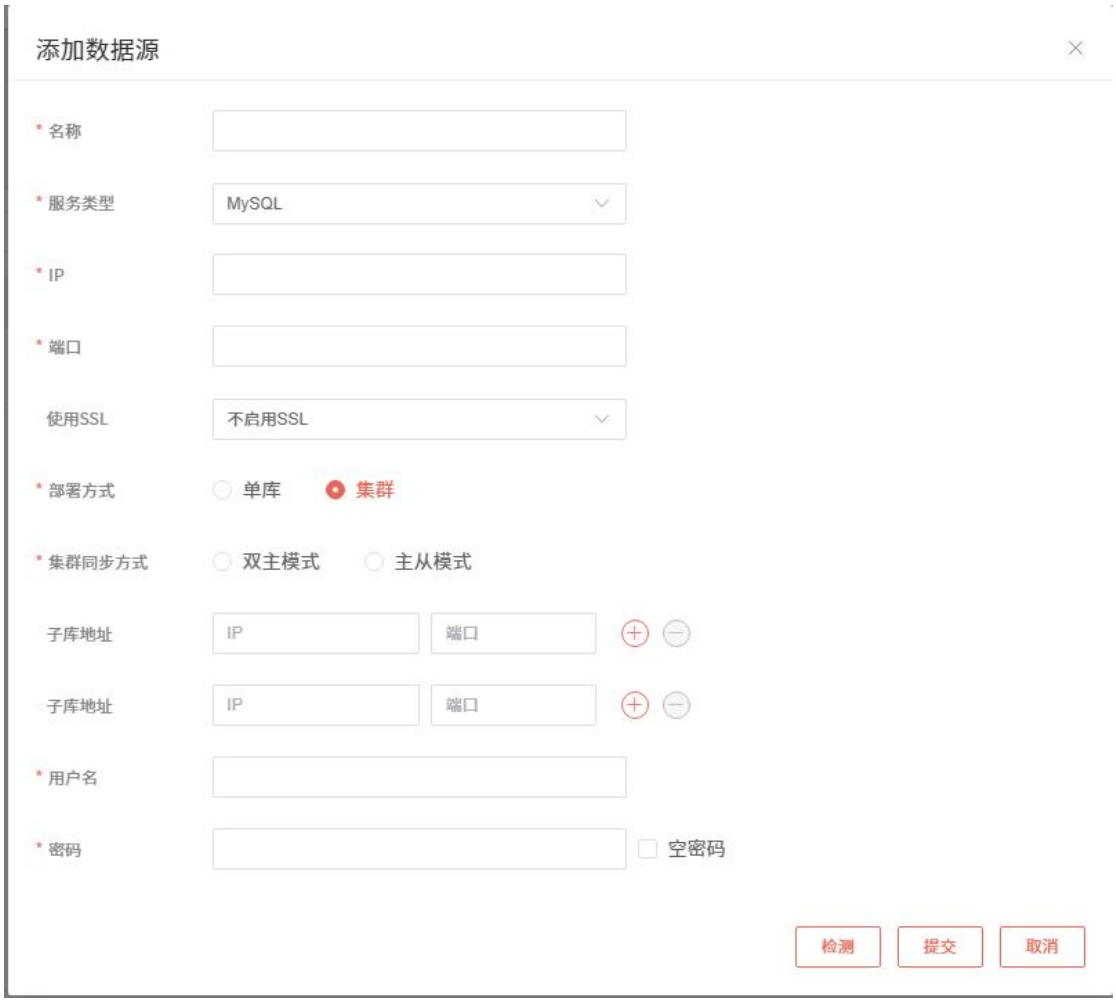

图 4-3 添加数据源-集群

在弹窗底部点击<检测>按钮，可预先检测填写内容正确性和数据库的联通性。

在弹窗底部点击<提交>按钮，完成数据源的添加，在数据源列表中形成一条新的数据。添加完成后，连接正常的数据源会自动做一次架构扫描和账户扫描。

4.3.1.2. 查看数据源

在操作区通过点击<查看>按钮，可查看数据源的详情，内容包括：名称、服务类型、部署方式、集群同步方式（若有）、连接状态、SSL 状态（若有）、创建时间、修改时间、架构扫描状态、最近扫描时间、IP、端口、数据库名（若有）、服务名（若有）、账号角色（若有）、用户名、密码（隐藏）。若该数据源已使用插件，还可以查看插件配置状态、插件地址、插件通信端口等信息。

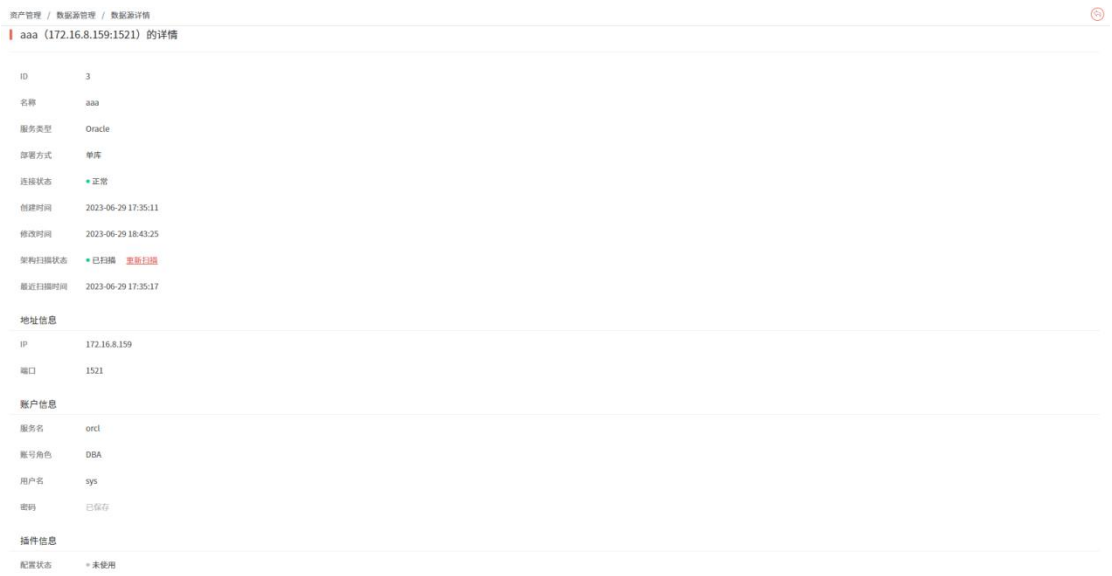

图 4- 4 数据源详情

4.3.1.3. 修改数据源

在操作区通过点击<编辑>按钮，可编辑数据源信息，支持修改内容包括：名称、IP、端口、用户名、密码。数据源类型为 Oracle 时，应支持修改服务名和账号角色；服务类型为 PostgreSQL、GaussDB、KADB、KingbaseES、AtlasDB、SQL Server 时，应支持修改数据库名；服务类型为 MySQL、PostgreSQL、GaussDB 时，支持修改使用 SSL 连接方式。

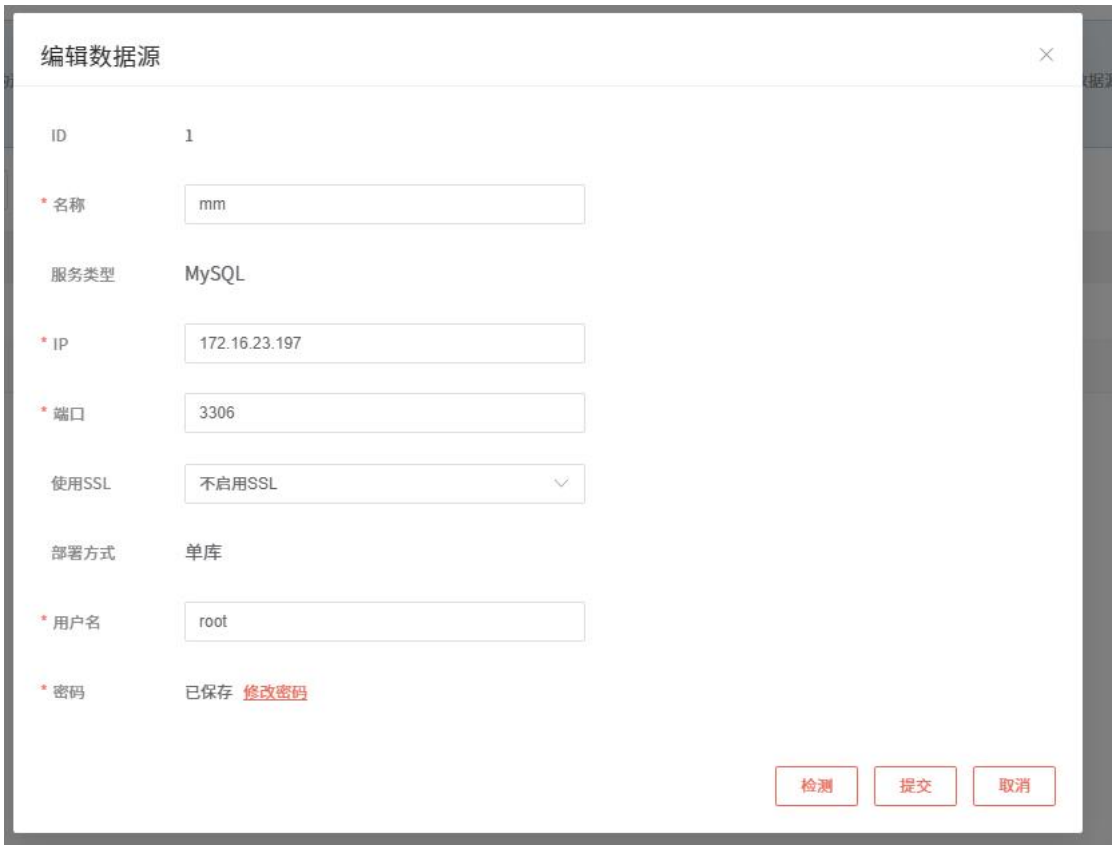

图 4-5 编辑数据源

在弹窗底部点击<检测>按钮，可预先检测填写内容正确性和数据库的联通性。

在弹窗内点击<修改密码>按钮，可修改数据库账号密码。

在弹窗底部点击<提交>按钮，完成数据源的信息修改。

※注意：①服务类型、部署方式、集群同步方式不支持修改；②子库地址不支持在此处修改，可在子库管理页面修改；③数据库账户密码只支持在此处修改。

4.3.1.4. 删除数据源

在操作区通过点击<删除>按钮，可删除此数据源。删除操作需要数据当前账号登录密码进行二次确认。

※注意：以下情况时，不允许删除数据源：①数据源处于架构扫描中或停止中状态；②数据源存在已设置的加密对象；③数据源存在已设置的完整性保护对象。本操作将会删除系统中所有与此数据源相关的数据，且不可恢复，请谨慎使用。

4.3.1.5. 管理子库

在操作区通过点击<查看>按钮，再选择“子库管理”标签，进入到子库列表页面，页面展示了子库信息，包括：子库地址:端口、插件地址:端口、插件配置等，

见下图：

图 4-6 子库管理

在操作区点击〈编辑〉按钮，可修改单条子库信息，如子库地址和子库端口。点击〈提交〉按钮，完成此条子库信息修改。

在操作区点击<添加>按钮，可添加新的子库信息，点击<提交>按钮，完成此条子库信息添加。

在操作区点击<删除>按钮，可删除单条子库信息，但子库总数不得少于 2 个，多于 99 个。

※注意：此功能在数据源为集群形式下才可查看；已做加密配置的集群类型数据源不支持添加或修改子库地址。

4.3.1.6. 架构扫描

架构扫描覆盖了除系统内置库/模式之外的其他所有库/模式，数据源状态正常且账号可以正常登陆下，还应保证已配置的用户具备查询数据源架构和账户信息的权限。

在操作区通过点击<查看>按钮，可查看架构扫描的状态，架构扫描一共有六种状态，包括：未扫描、扫描中、扫描失败、扫描中止、停止中、已扫描。

处于“未扫描”、“扫描中止”、“扫描失败”或“已扫描”状态的数据源，可以发起新的扫描；处于“扫描中”状态的数据源，可以强制停止扫描，停止中的状态为“停止中”，停止后的状态为“扫描中止”；若因系统故障导致扫描中的任务中断或挂起，系统恢复后会自动修复这些任务的执行状态。

点击<重新扫描>或<立刻扫描>，确认数据库信息正确后，点击<连接>按钮，连接正常时，系统才会展示该数据库下除系统内置模式之外的其他所有模式信息，包括：模式名、状态（已扫描/未扫描/扫描失败），上次扫描时间。可根据模式名搜索相关模式，选择所需扫描的单个或多个模式，点击<开始扫描>完成架构扫描操作。

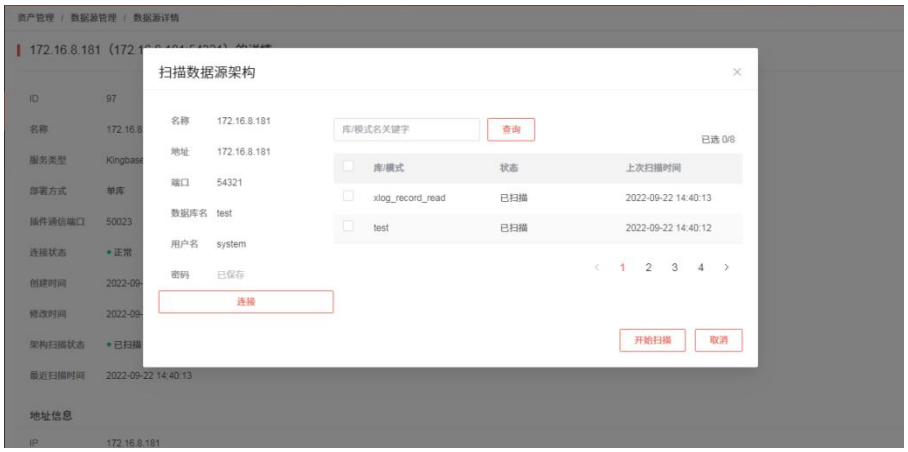

图 4-7 架构扫描

※注意：数据源处于架构扫描中状态时，无法进行以下操作：①删除数据源；②修改数据源的 IP 或端口；③添加或删除数据源的子库；④修改数据源子库的 IP 或端口；⑤添加或删除数据源的加密对象；⑥修改数据源加密对象的加密列；⑦开启或关闭数据源的“读保护”功能；⑧开启或关闭数据源的“完整性保护”功能；⑨添加或删除完整性保护对象。

4.3.2. 插件管理

加密系统与插件之间是纳管与被纳管关系，一个插件最多只能被一个加密系统纳管；数据源与插件之间是绑定与被绑定关系，同一个插件可以被多个数据源绑定。一般情况下，数据源和其绑定的插件应在同一个设备上。

安全管理员登录系统后，点击“资产管理”->“插件管理”进入到插件列表页面。用户可以在此查看已纳管插件信息，包括插件地址:通信端口、CPU 占用率、内存占用率、磁盘使用量、下属数据源数量、运行状态（状态正常/状态异常/地址变更）、检测时间等，见下图：

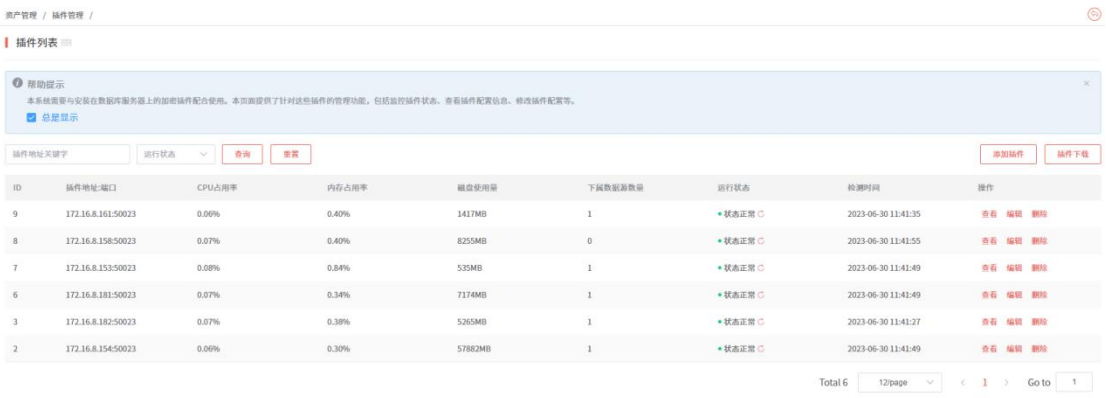

图 4-8 插件列表

4.3.2.1. 添加插件

在操作区通过点击<添加插件>按钮，可添加新插件，相关配置内容如下表：

配置项	是否必填	说明
插件 IP	是	支持 IPv4 格式
插件端口	是	插件的通信端口，默认 50023

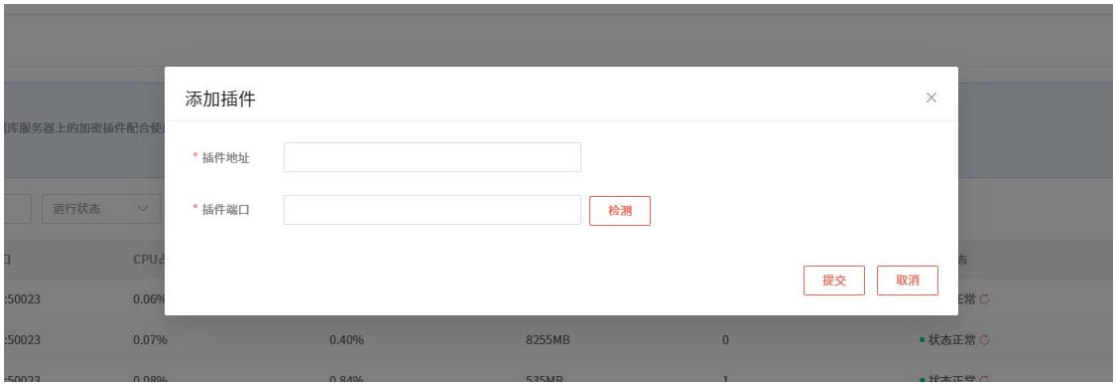

图 4-9 添加插件

在弹窗内点击插件端口的<检测>按钮，可检测插件的连通性，提示“未纳管”、“已被占用”或“连接失败”。只有未被纳管的插件，才能添加成功。

4.3.2.2. 查看插件

1）基本信息

在操作区通过点击<查看>按钮，可查看插件的详情，内容包括基本信息、下属数据源、运行日志。其中基本信息包括：插件地址、插件端口、当前状态、设备 CPU 使用率、设备内存使用率、设备磁盘总容量、插件的 CPU 占用率、插件的内存占用率、插件的磁盘使用量、下属数据源数量、创建时间、更新时间，见下图：

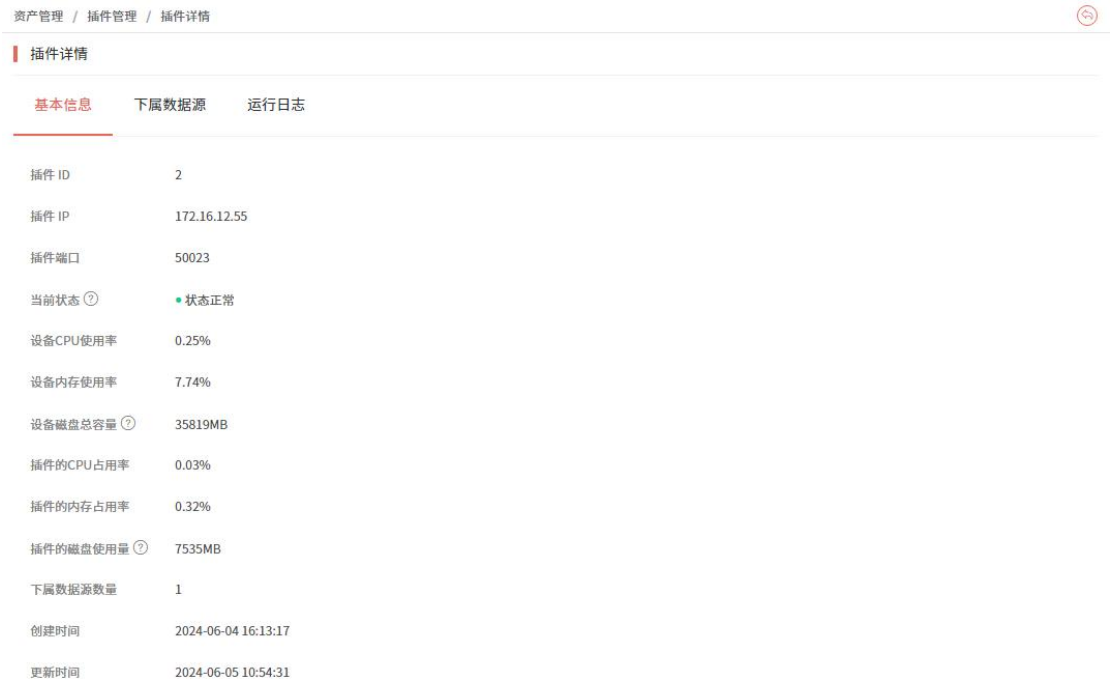

图 4- 10 插件详情

插件状态“连接失败”的可能原因：加密系统无法连接插件：插件 IP 或端口错误，路由不可达、插件监听端口（默认 50023）被本地或网络防火墙拦截、插件服务异常；插件无法连接加密系统：加密系统路由不可达、加密系统服务端口被本地或网络防火墙拦截。若出现状态异常情况，可先自行检测，或寻求厂家技术支持人员帮助。

插件基本信息中的磁盘，特指的是插件所在工作目录的磁盘。

2）下属数据源

在操作区通过点击“下属数据源”标签，可查看插件下属数据源详情，内容包括：数据源名称、服务类型、地址:端口、部署方式、子库地址:端口、工作目录、工作目录大小，见下图：

图 4- 11 插件详情-下属数据源

3）运行日志

在操作区通过点击“运行日志”标签，可查看插件运行日志详情，内容包括：插件地址、状态、持续时长、更新时间，见下图：

图 4- 12 插件详情-运行日志

4.3.2.3. 修改插件

在操作区通过点击<编辑>按钮，可编辑插件的通信端口信息。

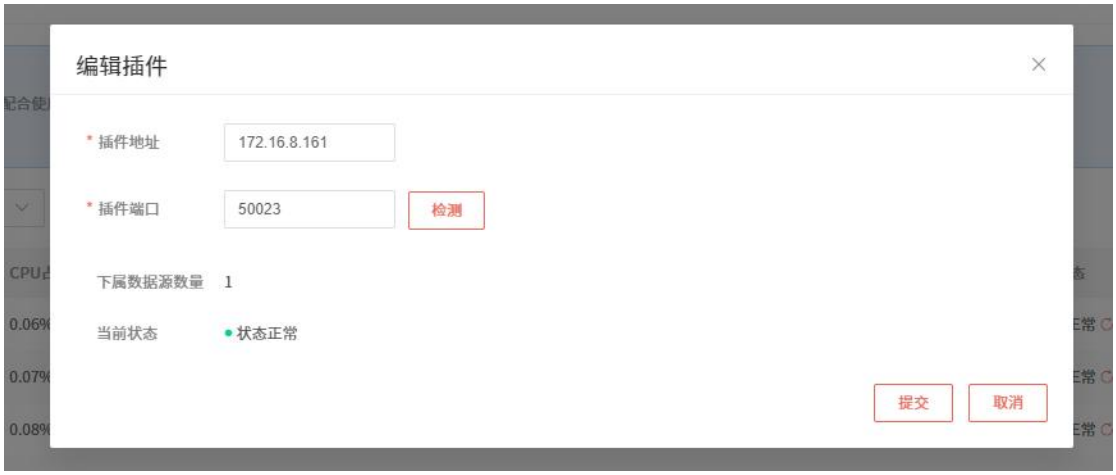

图 4- 13 编辑插件

在弹窗内点击插件端口的<检测>按钮，可检测插件的连通性。插件连接状态正常情况下，才能提交成功，并进行数据库加解密操作。

在弹窗底部点击<提交>按钮，完成插件的信息修改。

4.3.2.4. 插件下载

在操作区通过点击<插件下载>按钮，可进入到插件安装部署方法页面，在此页面可下载插件安装包和查看部署方法。请根据实际环境，下载安装包进行安装。

图 4- 14 插件下载

※注意：①数据库有加密对象时，禁止启/停插件，否则会造成数据损坏。②安装插件后，远程登录，用户登录权限会收到影响③目前页面仅提供支持 Linux x86_64 环境的插件安装包，若需要支持其他环境的安装包，请与我司售后支持人员联系。

4.4. 密钥管理

数据库加密与访问控制网关采用的是三级密钥保护机制，密钥管理中展示的是主密钥和数据加密密钥的基本信息。一个数据库加密与访问控制网关只有一个主密钥，密钥按照状态可分为备用密钥、在用密钥和历史密钥。

备用密钥是指创建以后未被任何加密对象绑定使用的密钥，新创建的密钥默认是备用密钥。在用密钥是指已被一个加密对象绑定使用的密钥。历史密钥存在两种情况，一种是备用密钥到期后一直未被使用，会变为历史密钥。另一种是在用密钥被解除与加密对象的绑定关系，且不再被任何加密对象绑定时，会变为历史密钥。

三种密钥之间的转换场景如下图所示：

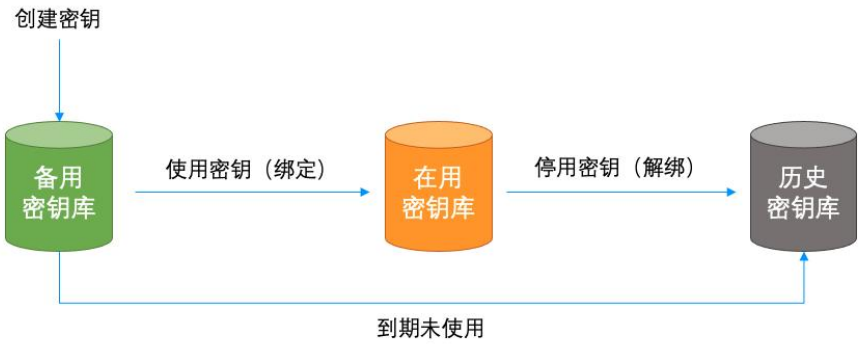

图 4-15 密钥转换场景

系统对应三个密钥库用于存放处于三种不同状态的密钥，分别是备用密钥库、在用密钥库、历史密钥库。当加密对象需要使用系统内密钥进行加密的，可从备用密钥库中获取。

所以，密钥管理功能主要包括主密钥管理、备用密钥库、在用密钥库、历史密钥库、密钥模板管理五部分。

※注意：各数据库的加密方案及算法（含分组模式）支持规格详见“帮助手册”。

4.4.1. 主密钥管理

4.4.1.1. 创建主密钥

安全管理员首次登录系统后，点击“密钥管理”->“主密钥管理”，页面会提示未创建主密钥，按操作提示点击<+>，二次确认需要创建主密钥，点击<确认>按钮完成主密钥添加。

图 4-16 创建主密钥

※注意：只有在加密卡进行过备份后，状态为已启用（常规模式）下，才可创建主密钥，请提前确认加密卡状态。

4.4.1.2. 查看主密钥

安全管理员登录系统，点击“密钥管理”->“主密钥管理”，若已创建主密

钥，页面会展示主密钥信息，包括：状态（已创建）、唯一标识、密钥长度（256bits）、创建时间，如下图：

图 4- 17 主密钥信息

4.4.2. 备用密钥库

安全管理员登录系统，点击“密钥管理”->“备用密钥库”，页面会展示备用密钥列表，字段包括：密钥标识、密钥别名、指定算法、密钥长度、创建时间，过期时间等，如下图：

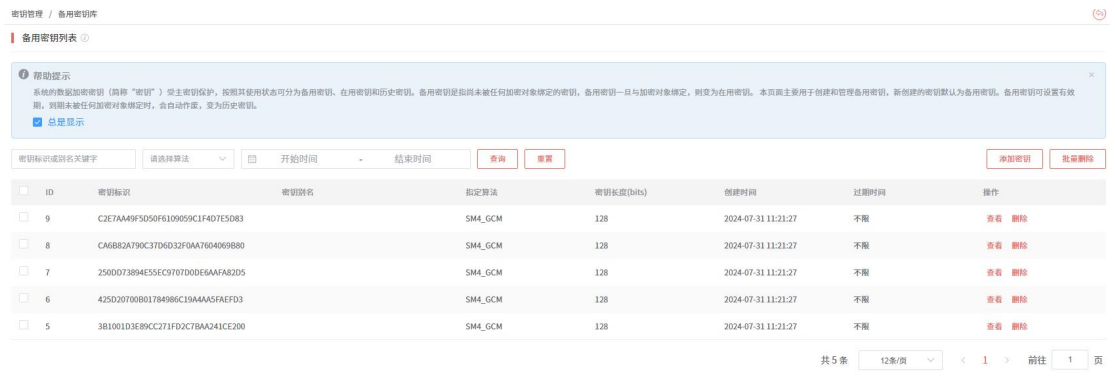

图 4- 18 备用密钥列表

4.4.2.1. 添加密钥

安全管理员登录系统，点击“密钥管理”->“备用密钥库”，点击<添加密钥>按钮，可做相关配置，如下表：

配置项	是否必填	说明
指定算法	是	SM1、HMAC_SHA256、SHA256、SM3、AES128_CBC、AES256_GCM、SM4_CBC 或 SM4_GCM 八选一
密钥模板	是	选择密钥模板
生成数量	是	可填写 1~1000

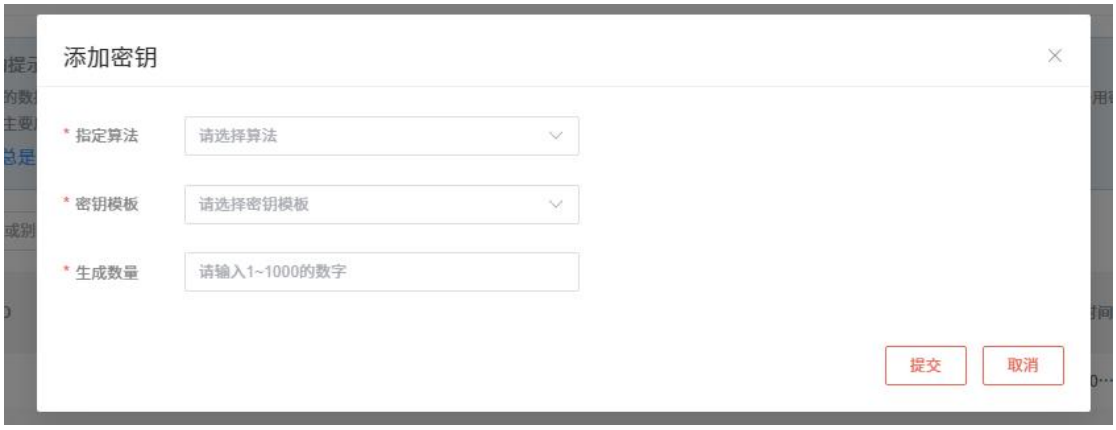

图 4- 19 添加密钥

在弹窗内点击<提交>按钮，完成密钥的添加，备用密钥列表生成相应数量的密钥。

※注意：①在加密卡状态为已启用（常规模式）下才可添加密钥。②SM1 算法只在硬件加密模式时显示。

4.4.2.2. 密钥别名

安全管理员登录系统，点击“密钥管理”->“备用密钥库”，鼠标移到需要命名的密钥别名列，点击“ ”按钮，可对密钥别名进行编辑，别名具有唯一性不可重复，不可超过 30 个字符，可为空。编辑完成后点击“ ”按钮才能保存，或者点击“ ”按钮取消编辑。

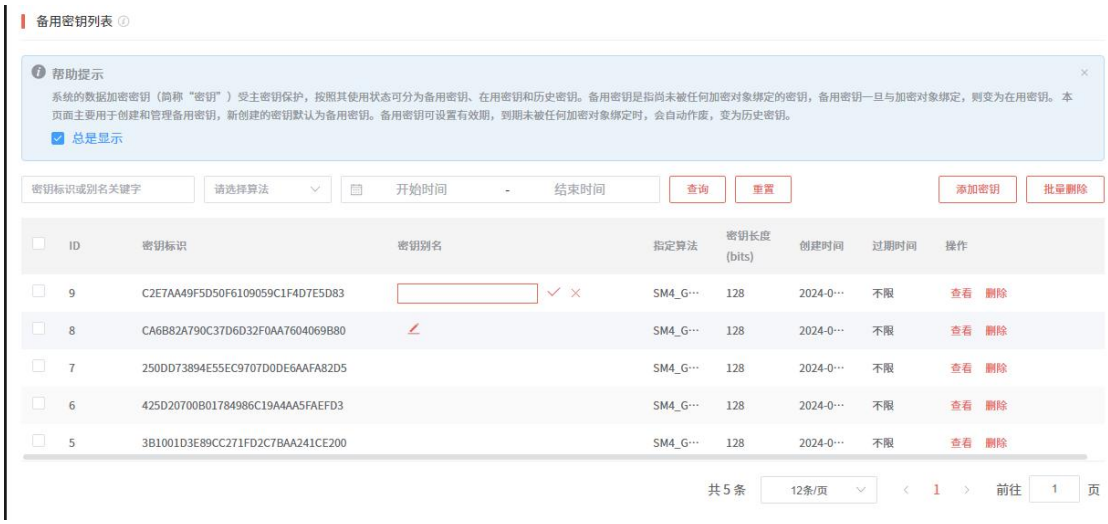

图 4- 20 密钥别名

※注意：此功能在在用密钥库、历史密钥库都可以使用。

4.4.2.3. 查看密钥

安全管理员登录系统，点击“密钥管理”->“备用密钥库”，点击<查看>按钮，页面将显示备用密钥详情，内容包括：密钥标识、密钥别名、指定算法、密钥长度、密钥算法、创建时间、过期时间，如下图：

图 4-21 查看备用密钥

4.4.2.4. 查找密钥

在操作区输入框内填写密钥标识或别名关键字，或者选择指定算法，点击<查询>按钮，可以筛选查找密钥。

4.4.2.5. 删除密钥

安全管理员登录系统，点击“密钥管理”->“备用密钥库”，点击<删除>或<批量删除>按钮，可删除单个或多个指定密钥。

4.4.3. 在用密钥库

安全管理员登录系统，点击“密钥管理”->“在用密钥库”，页面会展示在用密钥列表，字段包括：密钥标识、密钥别名、指定算法、密钥长度、创建时间等，如下图：

图 4- 22 在用密钥列表

4.4.3.1. 查看密钥

安全管理员登录系统，点击“密钥管理”->“在用密钥库”，点击<查看>按钮，页面将显示在用密钥详情，内容包括：密钥标识、密钥别名、密钥长度、密钥算法、创建时间，如下图：

图 4- 23 在用密钥详情

4.4.3.2. 密钥别名

安全管理员登录系统，点击“密钥管理”->“在用密钥库”，鼠标移到需要命名的密钥别名列，点击“ ”按钮，可对密钥别名进行编辑，别名具有唯一性不可重复，不可超过 30 个字符，可为空。编辑完成后点击“ ”按钮才能保存，或者点击“ ”按钮取消编辑。

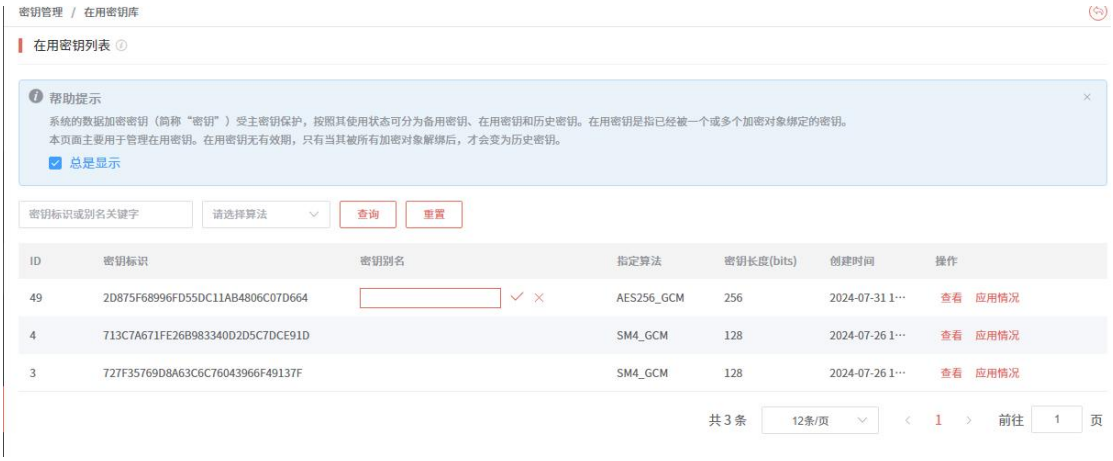

图 4- 24 密钥别名

※注意：此功能在备用密钥库、历史密钥库都可以使用。

4.4.3.3. 查找密钥

在操作区输入框内填写密钥标识或别名关键字，或者选择指定算法，点击<查询>按钮，可以筛选查找密钥。

4.4.3.4. 应用范围

安全管理员登录系统，点击“密钥管理”->“在用密钥库”，点击<应用范围>按钮，可查看当前密钥的应用范围，内容包括：所属数据源、地址：端口、库/模式、表、状态、应用时间。

图 4- 25 应用情况

在弹窗输入框内填写数据源名称、地址、模式名或表关键字，点击<查询>按钮，可以筛选查找相关应用情况。

4.4.4. 历史密钥库

安全管理员登录系统，点击“密钥管理”->“历史密钥库”，页面会展示历史密钥列表，字段包括：密钥标识、密钥别名、指定算法、密钥长度、创建时间

等，如下图：

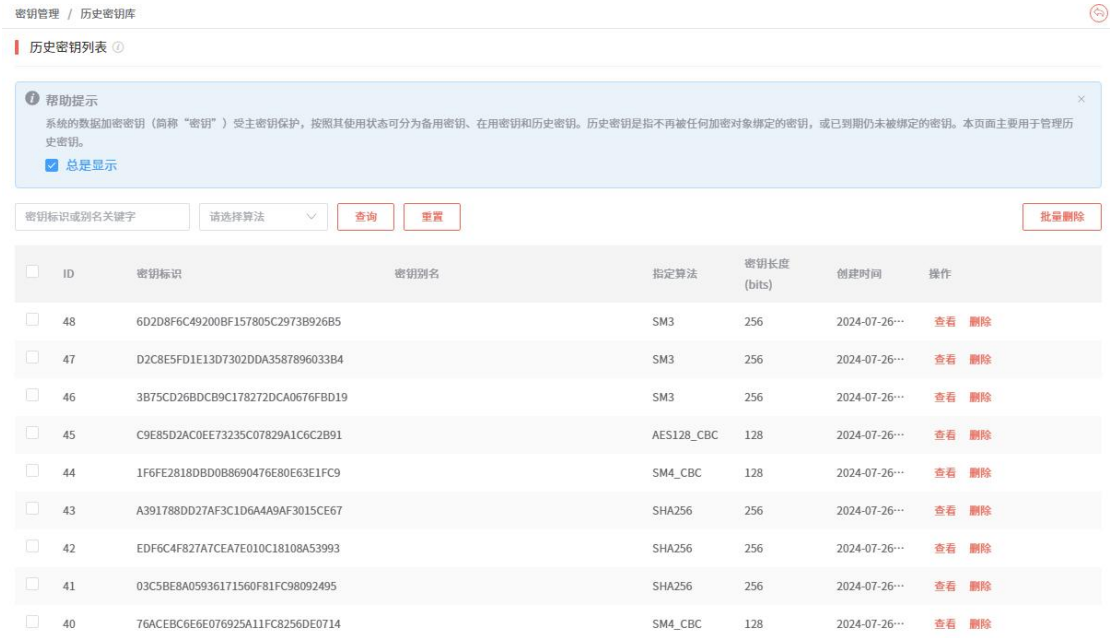

图 4- 26 历史密钥列表

4.4.4.1. 密钥别名

安全管理员登录系统，点击“密钥管理”->“历史密钥库”，鼠标移到需要命名的密钥别名列，点击“ ”按钮，可对密钥别名进行编辑，别名具有唯一性不可重复，不可超过 30 个字符，可为空。编辑完成后点击“ ”按钮才能保存，或者点击“ ”按钮取消编辑。

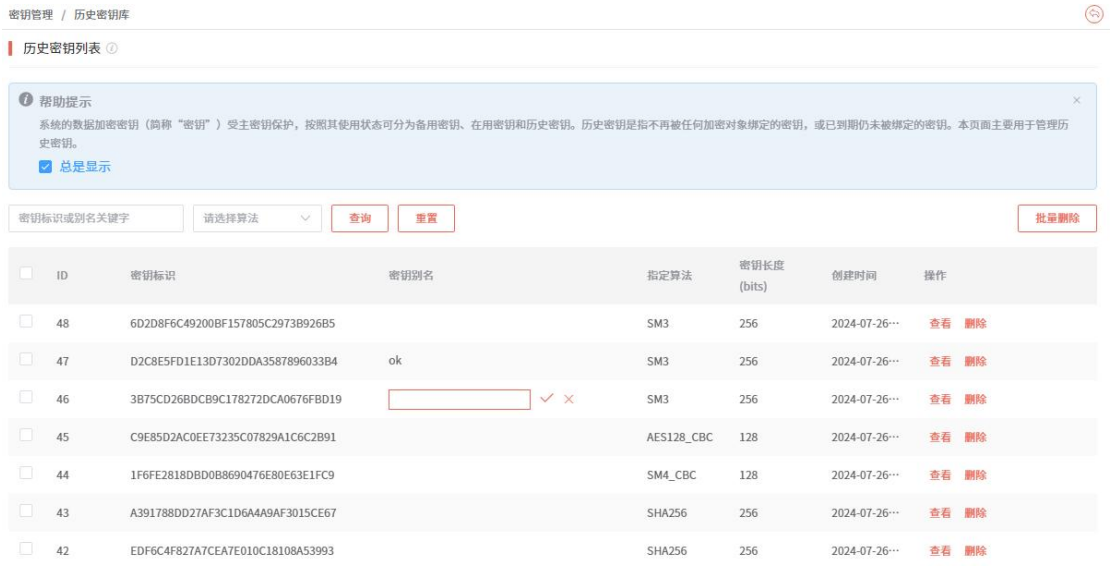

图 4- 27 密钥别名

※注意：此功能在备用密钥库、在用密钥库都可以使用。

4.4.4.2. 查看密钥

安全管理员登录系统，点击“密钥管理”->“历史密钥库”，点击<查看>按钮，页面将显示历史密钥详情，内容包括：密钥标识、密钥别名、指定算法、密钥长度、密钥算法、创建时间、停用时间，如下图：

图 4- 28 查看历史密钥

4.4.4.3. 查找密钥

在操作区输入框内填写密钥标识或别名关键字，或选择指定算法，点击<查询>按钮，可以筛选查找密钥。

4.4.4.4. 删除密钥

安全管理员登录系统，点击“密钥管理”->“历史密钥库”，点击<删除>或<批量删除>按钮，可删除单个或多个指定密钥。

4.4.5. 密钥模板

安全管理员登录系统后，点击“密钥管理”->“密钥模板管理”进入到密钥模板列表页面。用户可以在此查看密钥模板信息，包括模板名称、加密算法、密钥长度、有效时长等，见下图：

图 4- 29 密钥模板列表

4.4.5.1. 默认模板

密钥模板内置 8 个默认模板，分别为 SM1、HMAC_SHA256、SHA256、SM3、AES128_CBC、AES256_GCM、SM4_CBC 或 SM4_GCM 算法模板（含分组模式）。默认模板不可编辑，不可删除。

图 4- 30 默认模板

※注意：SM1 算法只在硬件加密模式时显示。

4.4.5.2. 添加模板

安全管理员登录系统，点击“密钥管理”->“密钥模板管理”，点击<添加>

按钮，可做相关配置，如下表：

配置项	是否必填	说明
模板名称	是	填写模板名称，不可重复，30 字符以内
指定算法	是	SM1、HMAC_SHA256、SHA256、SM3、AES128_CBC、AES256_GCM、SM4_CBC 或 SM4_GCM 八选一
有效时长	否	单位：天，取值范围 0~1000，留空或填 0 表示不限时长

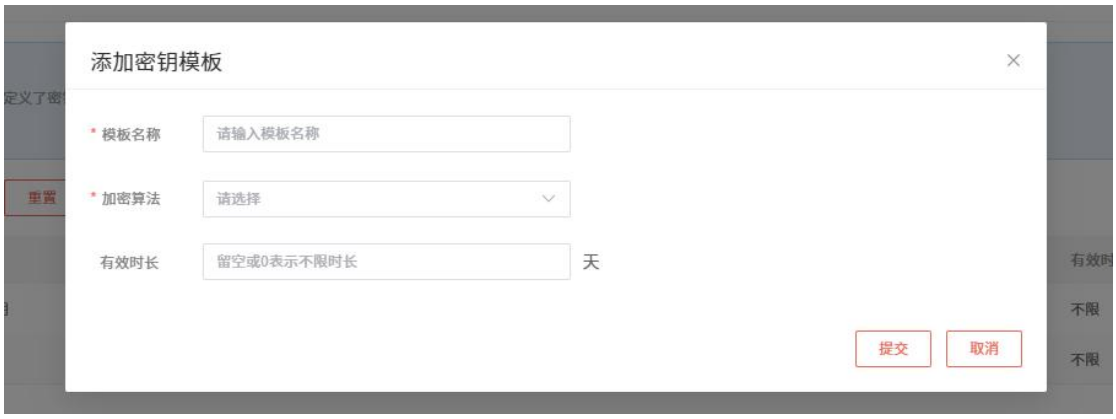

图 4-31 添加密钥模板

在弹窗内点击<提交>按钮，完成密钥模板的添加，密钥模板列表生成一条密钥模板信息。

4.4.5.3. 编辑模板

安全管理员登录系统，点击“密钥管理”->“密钥模板管理”，点击<编辑>按钮，可修改密钥模板的名称、加密算法和有效时长。点击<提交>按钮，完成密钥模板的修改。

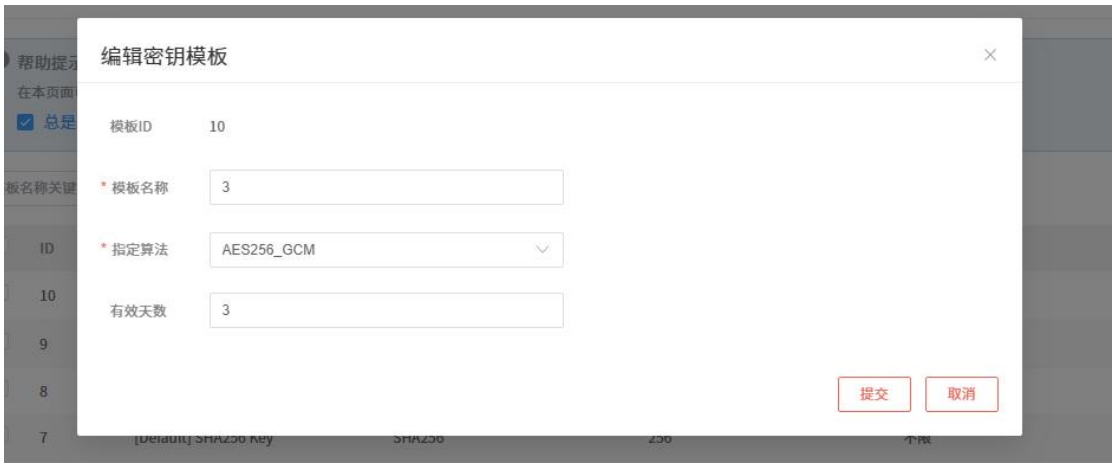

图 4-32 编辑密钥模板

4.4.5.4. 查找模板

在操作区输入框内填写模板名称关键字，点击<查询>按钮，可以筛选查找模板。

4.4.5.5. 删除模板

在操作区内点击<删除>或<批量删除>按钮，可删除单个或多个指定模板。

4.5. 策略管理

策略管理功能主要包括加密配置和访问控制两部分，在此模块中可以选择加密方案、管理加密对象、处理加解密业务、切换“读保护”开关状态、管理“读保护”例外规则、切换“完整性保护”开关状态、管理“完整性保护”对象，切换访问控制模式、管理访问控制规则。

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。用户可以在此查看数据源加密配置数据，包括数据源名称、服务类型、地址：端口、服务类型、连接状态、插件配置、加密方式、读保护状态、加密对象总数（已加密数量/加密对象总数）等，见下图：

图 4-33 加密配置

在操作区数据源列表上方输入框内，输入数据数据源名称或地址关键字，点击<查询>按钮，可按条件筛选搜索相关数据源。

在操作区左侧数据源列表内，可选择以名称或地址的展现方式来展示数据源。

在操作区左侧数据源列表内选择数据源，可快速进入数据源加密配置页面。在上方输入框内输入数据源地址关键字，可筛选搜索相关数据源。

4.5.1. 加密配置

数据库加密与访问控制网关目前支持三种加密技术方案，分别是基于表空间的加密技术（表空间加密）、基于数据库 NTE 模块的加密技术（原生加密）和

基于代理网关的加密技术（网关加密）。原生加密（NTE，Native Encryption）是指可以在文件层对数据和文件进行实时加密和解密，落盘的文件是加密后的内容，而对于上层应用系统和开发人员而言，加解密过程是无感知的，写入和读取的内容是明文内容。

每个数据源可以选择配置一种加密方案，不同加密方案的应用条件、配置过程、加密效果都有一定的差距，对于管理员而言，需要结合实际的业务需求，为数据源选择合适的加密方案。不同加密方案的使用场景见下表：

加密方案	适用场景
表空间加密	数据库支持表空间，且表空间数据文件的位置可自定义；数据库服务器采用 Linux 操作系统，可以安装插件
原生加密	数据库不支持表空间或无法安装插件，但支持 NTE 功能
网关加密	数据库不支持表空间或无法安装插件，也不支持 NTE 功能

支持 NTE 模块的数据库有限， 因此原生加密可应用的数据库也有限，目前支持以下数据库：Oracle 11g（单库、rac 集群）、Oracle 12c（单库、rac 集群）、Oracle19c（单库、rac 集群）。

网关加密支持以下数据库：单库部署的 SQL Server（2012、2016、2017、2019 版本）、单库或主-主集群或主-从集群部署的 MySQL（5.7 及 5.7 以上版本）、单库或集群部署的 Oracle（11g、12c、19c 版本）。

4.5.1.1. 选择加密方案

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。若该数据源未配置过加密方案，页面如下图：

图 4-34 选择加密方案

未配置加密方案的数据源，加密方案配置栏默认是展开状态，可点击右上角

“ ”按钮来收起加密方案配置信息；收起后，可点击右上角“ ”按钮来展开加密方案配置信息。

在操作区点击<选择加密方案>，或在对应的加密方案下点击<使用该方案>，可进入到该加密方案的配置页面。

1) 表空间加密

选择表空间加密方案，进入到表空间加密配置弹窗，弹窗中展示数据源基本信息，包括数据源地址:端口、服务类型、部署方式、加密方案、插件地址、插件端口、读保护、防绕过等。需根据实际情况进行配置，配置情况如下表：

配置项	是否必填	说明
插件地址	是	可选择已纳管插件或添加新插件
插件端口	是	填写插件端口
读保护	禁用或启用二选一	禁用或启用二选一，默认为关闭
防绕过	禁用或启用二选一	读保护开启时需选择，禁用或启用二选一，默认为禁用
连接方式	默认或自定义二选一	开启高级设置时需选择，默认或自定义二选一，默认为默认，若选择自定义需填写连接参数，如 socket 或 ip:port

若数据库为 MySQL v8.0.4 及以上版本，安装加密插件后，需将加密目录添加到 MySQL 服务配置文件中，否则无法加密。具体方法参考下图中 《MySQL v8.0.4 及以上版本配置加密目录的方法》。

开启“防绕过”功能后，所有未能成功解析的 SQL 请求（通常是由系统不支持的数据库客户端发起的）将会被拒绝，这可能会导致一些合法请求被阻断。该功能仅在“读保护”开启时生效。

图 4-35 配置表空间加密（单库）

在弹窗内点击插件端口的<检测>按钮，可检测插件的连通性，提示“未纳管”、“已被占用”或“连接失败”。

在弹窗内点击<上一步>按钮，重新选择加密方案。

在弹窗内点击<关闭>按钮，关闭弹窗取消加密方案配置。

在弹窗内点击<提交>按钮，需选择是否强制断开已有的连接。提交配置方案后，弹窗会显示配置进度表，及配置结果，全部配置成功弹窗自动关闭，如有配置失败则会提示相关信息。若纳管插件失败，则表示插件地址连接失败；若启用表空间加密失败，则表示配置下发失败。此时已确认选择表空间加密方案，可点击<返回>按钮修改配置，或关闭弹窗待确定配置信息后再修改配置或切换方案。

图 4-36 配置表空间加密提示是否强制断开已有连接

图 4-37 配置表空间加密进度显示

※注意：①MySQL 数据库配置表空间加密方案后，用户登录的权限可能会受到影响，如：原先限制只能本地登录的用户，应用加密方案后可以远程登录；原先限制只能远程登录的用户，应用加密方案后远程无法登录。②若配置加密方案后，数据源 IP 地址有修改，需在数据源管理页面和插件管理页面，均修改为正确 IP 后，方可正常使用。

2) 原生加密

选择原生加密方案，进入到原生加密配置弹窗，弹窗中展示数据源基本信息，包括数据源地址:端口、服务类型、部署方式、加密方案、密钥状态（未配置、已配置未保存、已配置已保存）、当前密钥、代理端口、读保护、防绕过等。需根据实际情况进行配置，配置情况如下表：

配置项	是否必填	说明
当前密钥	是	密钥状态为已配置未保存情况下显示，输入当前的加密密钥
设置密钥	是	设置加密密钥，至少由英文字母、数字、下划线中的两种组成，8-30 个字符
更换密钥	否	密钥状态为已配置未保存和已配置已保存情况下显示，默认为不勾选状态，勾选后需输入新密钥
新密钥	是	勾选更换密钥显示，输入新的加密密钥
确认密钥	是	重复输入加密密钥
代理端口	是	高级设置下可见，自定义端口可用范围为 59000-59999，或选择自动设置
读保护	禁用或启用二选一	禁用或启用二选一，默认为关闭
防绕过	禁用或启用	读保护开启时需选择，禁用或启用二选一，默认为

	二选一	禁用

开启“防绕过”功能后，所有未能成功解析的 SQL 请求（通常是由系统不支持的数据库客户端发起的）将会被拒绝，这可能会导致一些合法请求被阻断。该功能仅在“读保护”开启时生效。

图 4-38 配置原生加密-第一步

在弹窗内点击密钥状态的<重新检测>按钮，可检测密钥状态。

在弹窗内点击<关闭>按钮，关闭弹窗取消加密方案配置。

在弹窗内点击<上一步>按钮，重新选择加密方案。

在弹窗内点击<下一步>按钮，进入到配置原生加密的第二步。根据选择是否支持 SSH 连接，如用户授权加密系统可对数据源通过 SSH 连接，需要进行相关配置，配置项如下表：

配置项	是否必填	说明
主机 SSH	支持或不支持二选一	支持或不支持二选一，默认为不支持
主机地址	是	输入主机地址，支持 IPv4 格式
SSH 端口	是	输入 SSH 端口号，默认为 22
SSH 用户名	是	输入主机 SSH 用户名，默认为 oracle，不支持修改
SSH 密码	是	输入主机 SSH 密码
手动配置	是	选择不支持 SSH 连接显示，必须勾选确认完成

		手动配置

图 4-39 配置原生加密（单库）-第二步-支持主机 SSH

图 4-40 配置原生加密（单库）-第二步-不支持主机 SSH

可参考页面帮助文档《在数据库服务器上启用 NTE 模块的方法》，手动进行配置。手动配置后需勾选确认，方可提交。

在弹窗内点击<提交>按钮，需二次确认提交配置方案。弹窗会显示配置进度表，及配置结果，全部配置成功弹窗自动关闭，若有配置失败则会提示相关信息。若启用 NTE 功能失败，则表示配置下发失败。此时已确认选择原生加密方案，可点击<返回>按钮修改配置，或关闭弹窗待确定配置信息后再修改配置或切换方案。

图 4-41 配置原生加密进度显示

※注意：①使用原生加密方案进行加密时，需保证 Wallet（加密钱包）为“OPEN”状态，否则会导致加密失败。如需打开钱包，请参考图 4-40 中的《在数据库服务器上启用 NTE 模块的方法》文档。②设置原生加密，数据源的账号角色需选择 DBA，用户选择 sys 用户或拥有同等权限的用户。

3）网关加密

选择网关加密方案，进入到网关加密配置弹窗，弹窗中展示数据源基本信息，包括数据源地址:端口、服务类型、部署方式、加密方案、代理端口、读保护、防绕过等。需根据实际情况进行配置，配置情况如下表：

配置项	是否必填	说明
读保护	是	禁用或启用二选一，默认为关闭
防绕过	否	读保护开启时需选择，禁用或启用二选一，默认为禁用
代理端口	是	高级设置下可见，自定义端口可用范围为 59000-59999，或选择自动设置
存量数据处理	更新表和复制表二选一	高级设置下可见，更新表和复制表二选一，默认为更新表方式

开启“防绕过”功能后，所有未能成功解析的 SQL 请求（通常是由系统不支持的数据库客户端发起的）将会被拒绝，这可能会导致一些合法请求被阻断。该功能仅在“读保护”开启时生效。

图 4-42 配置网关加密

在弹窗内点击<上一步>按钮，重新选择加密方案。

在弹窗内点击<关闭>按钮，关闭弹窗取消加密方案配置。

在弹窗内点击<提交>按钮，需二次确认提交配置方案。弹窗会显示配置进度表，及配置结果，全部配置成功弹窗自动关闭，若有配置失败则会提示相关信息。此时已确认选择网关加密方案，可点击<返回>按钮修改配置，或关闭弹窗待确定配置信息后再修改配置或切换方案。

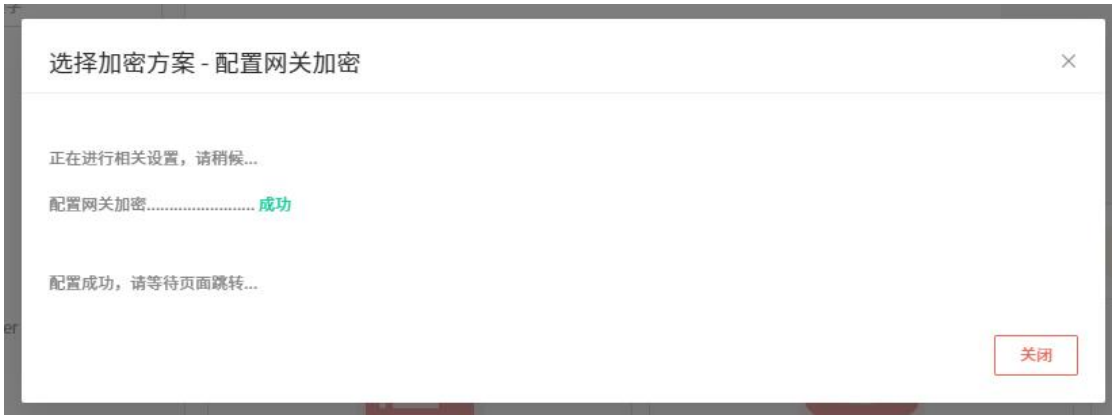

图 4-43 配置网关加密进度显示

※注意：MySQL 数据库可参照提示，为数据库安装 SM4 算法插件；SQL Server 数据库可参照提示，为数据库安装 SM4 算法插件。相关配置方法，可在“帮助手册”中查询。

4.5.1.2. 修改加密方案配置

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据源配置页面。若该数据源已配置过加密方案，页面如下图：

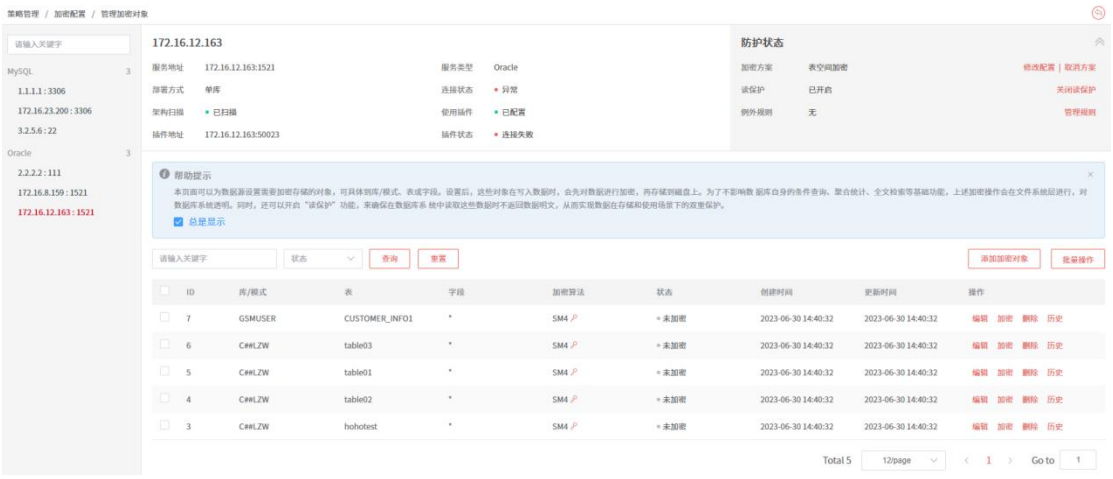

图 4-44 已配置表空间加密

图 4-45 已配置原生加密

图 4-46 已配置网关加密

1) 表空间加密

点击防护状态栏的<修改配置>按钮，弹出弹窗可修改加密方案的配置。弹窗中展示数据源基本信息，包括数据源地址:端口、服务类型、部署方式、加密方案、插件地址、插件端口等。需根据实际情况进行配置，配置情况如下表：

配置项	是否必填	说明
插件地址	是	可选择已纳管插件或添加新插件
插件端口	是	填写插件端口
连接方式	默认或自定义二选一	开启高级设置时需选择，默认或自定义二选一，默认为默认，若选择自定义需填写连接参数，如 socket 或 ip:port

图 4-47 修改表空间加密配置（单库）

在弹窗内点击插件端口的<检测>按钮，可检测插件的连通性，提示“未纳管”、“已被占用”或“连接失败”。

在弹窗内点击<上一步>按钮，可选择取消当前加密方案。

在弹窗内点击<关闭>按钮，关闭弹窗取消加密方案配置。

在弹窗内点击<提交>按钮，需二次确认提交配置方案。弹窗会显示配置进度表，及配置结果，全部配置成功弹窗自动关闭，若有配置失败则会提示相关信息。若纳管插件失败，则表示插件地址连接失败；若启用表空间加密失败，则表示配置下发失败。可点击<返回>按钮修改配置，或关闭弹窗待确定配置信息后再修改配置或切换方案。

图 4-48 配置表空间加密进度显示

※注意：存在加密对象情况下，禁止修改配置。

2) 原生加密

点击防护状态栏的<修改配置>按钮，进入到修改原生加密配置弹窗，弹窗中展示数据源基本信息，包括数据源地址:端口、服务类型、部署方式、加密方案、密钥状态（未配置、已配置未保存、已配置已保存）、代理端口、读保护等。需根据实际情况进行配置，配置情况如下表：

配置项	是否必填	说明
当前密钥	是	密钥状态为已配置未保存情况下显示，输入当前的加密密钥
更换密钥	否	密钥状态为已配置未保存和已配置已保存情况下显示，默认为不勾选状态，勾选后需输入旧密钥和新密钥
旧密钥	是	勾选更换密钥显示，输入原来的加密密钥
新密钥	是	勾选更换密钥显示，输入新的加密密钥

确认密钥	是	重复输入加密密钥
更换端口	否	高级设置下可见，自定义端口可用范围为59000-59999

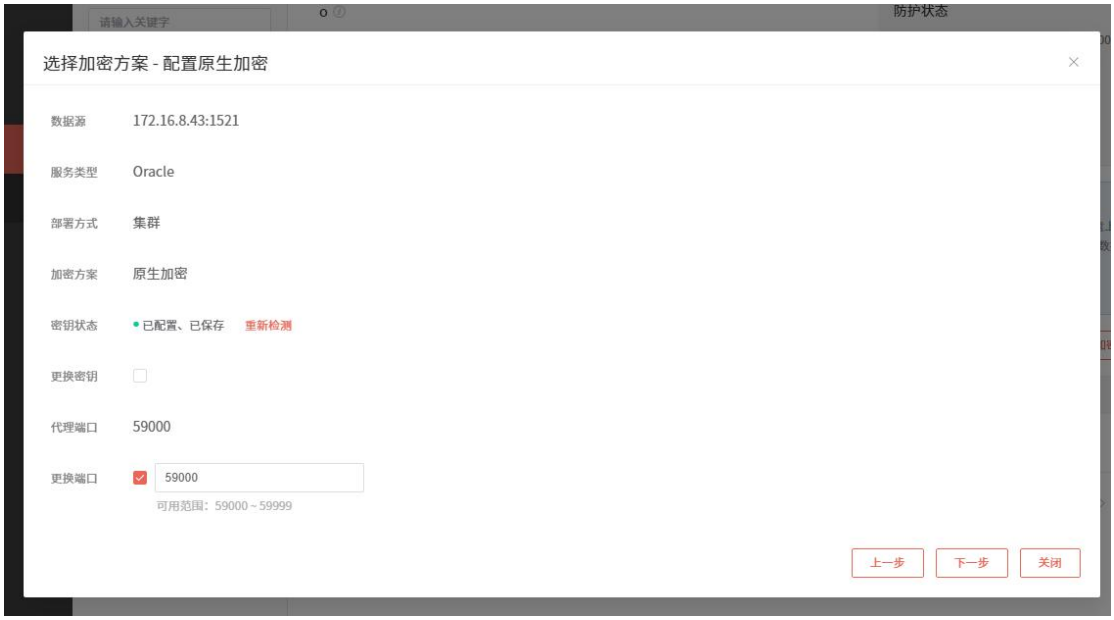

图 4- 49 修改原生加密配置（单库）

在弹窗内点击密钥状态的<重新检测>按钮，可检测密钥状态。

在弹窗内点击<关闭>按钮，关闭弹窗取消修改加密方案配置。

在弹窗内点击<上一步>按钮，可取消当前加密方案。

在弹窗内点击<下一步>按钮，进入到配置原生加密的第二步。根据选择是否支持 SSH 连接，如用户授权加密系统可对数据源通过 SSH 连接，需要进行相关配置，配置项如下表：

配置项	是否必填	说明
主机 SSH	支持或不支持二选一	支持或不支持二选一，默认为不支持
主机地址	是	输入主机地址，支持 IPv4 格式
SSH 端口	是	输入 SSH 端口号，默认为 22
SSH 用户名	是	输入主机 SSH 用户名，默认为 oracle，不支持修改
SSH 密码	是	输入主机 SSH 密码
手动配置	是	选择不支持 SSH 连接显示，必须勾选确认完成手动配置

图 4- 50 配置原生加密（单库）-第二步-支持主机 SSH

图 4- 51 配置原生加密（单库）-第二步-不支持主机 SSH

若选择不支持 SSH，可参考页面帮助文档《在数据库服务器上启用 NTE 模块的方法》，手动进行配置。手动配置后需勾选确认，方可提交。

在弹窗内点击<提交>按钮，需二次确认提交配置方案。弹窗会显示配置进度表，及配置结果，全部配置成功弹窗自动关闭，若有配置失败则会提示相关信息。若启用 NTE 功能失败，则表示配置下发失败。此时已确认选择原生加密方案，可点击<返回>按钮修改配置，或关闭弹窗待确定配置信息后再修改配置或切换方案。

图 4- 52 配置原生加密进度显示

※注意：存在加密对象情况下，禁止修改配置。

3）网关加密

点击防护状态栏的<修改配置>按钮，弹出弹窗可修改加密方案的配置。弹窗中展示数据源基本信息，包括数据源地址:端口、服务类型、部署方式、加密方案、代理端口、读保护、防绕过等。需根据实际情况进行配置，配置情况如下表：

配置项	是否必填	说明
代理端口	是	高级设置下可见，自定义端口可用范围为59000-59999，或选择自动设置
存量数据处理	更新表和复制表二选一	高级设置下可见，更新表和复制表二选一，默认为更新表方式

图 4-53 修改网关加密配置

在弹窗内点击<关闭>按钮，关闭弹窗取消修改加密方案配置。

在弹窗内点击<提交>按钮，需二次确认提交配置方案。弹窗会显示配置进度表，及配置结果，全部配置成功弹窗自动关闭，若有配置失败则会提示相关信息。此时已确认选择网关加密方案，可点击<返回>按钮修改配置，或关闭弹窗待确定配置信息后再修改配置或切换方案。

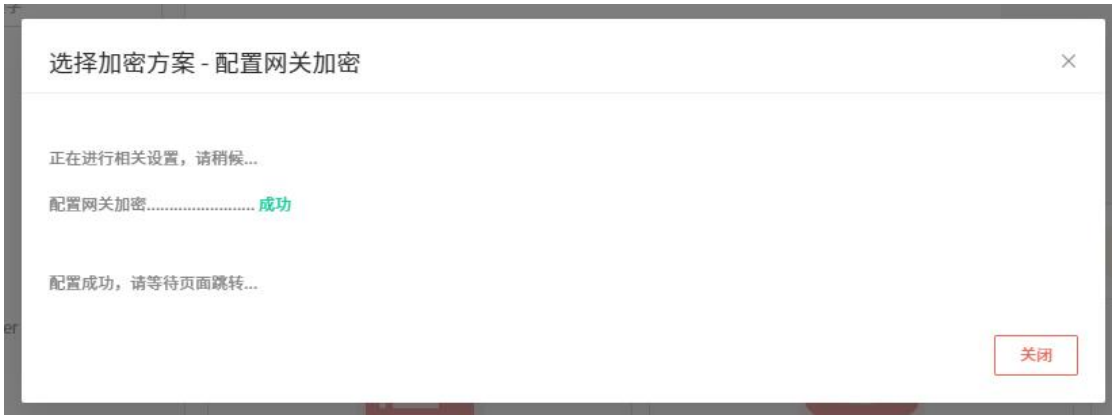

图 4-54 配置网关加密进度显示

※注意：存在加密对象和保护对象的情况下，禁止修改配置。

4.5.1.3. 取消/切换加密方案

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。在数据源加密列表中选择已进行表空间加密配置的数据源，点击对应的<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。点击防护状态栏的<取消方案>按钮，需二次确认取消当前方案。若想取消加密方案，需先删除所有的加密对象。

图 4-55 取消加密方案

取消加密方案后，可根据需求再次选择加密方案，详情参照 4.5.1.1 章节。

4.5.1.4. 添加加密对象

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。

1）表空间加密、原生加密

在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据源配置页面。在操作区点击<添加加密对象>按钮，弹出加密对象的配置页

面。

第一步：选择按表选择、按列选择、按库选择加密对象。可在输入框内输入关键字查找目标表、列或者库。

弹窗内依据选择方式，显示该数据源下的所有表、所有列、所有库信息。勾选需要加密的表、列或者库。点击<下一步>按钮，进入加密算法配置弹窗页。

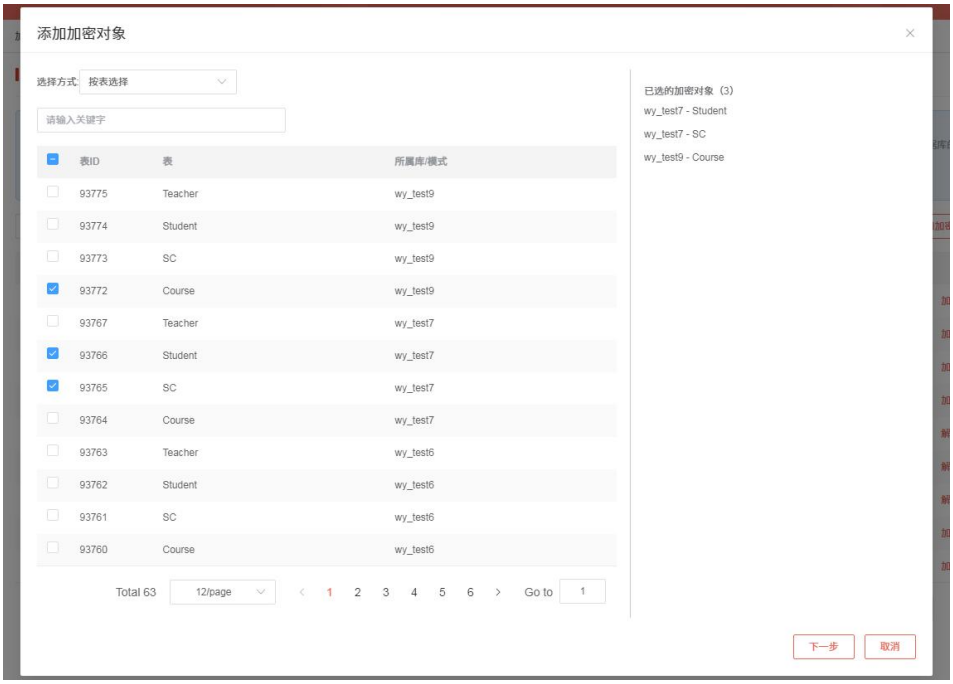

图 4-56 添加加密对象-第一步

第二步：配置加密算法，不同数据库支持的加密算法不同，具体算法支持情况可见“帮助手册”中的《各数据库的加密方案及算法支持规格》。可在输入框内输入关键字对指定表做相关配置。

系统默认为加密对象匹配随机密钥和默认加密算法，使用指定加密算法为指定表进行加密，点击对应表行的<默认>下拉框，选择指定加密算法，可以选择默认或其他算法。原生加密不支持选择加密算法，默认为 AES256。

点击<提交>按钮保存设置，或点击<取消>按钮取消添加加密对象，若想修改加密对象可点击<上一步>，对加密对象进行修改。

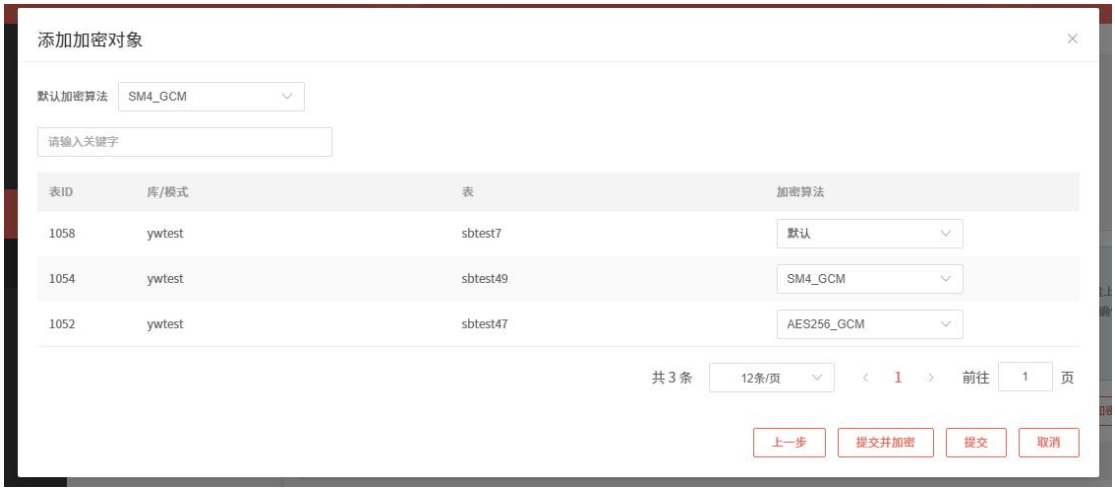

图 4-57 添加加密对象-第二步

第三步：确认添加加密对象，点击<提交并加密>系统添加加密对象并自动执行加密操作，点击<提交>完成添加，点击<取消>取消添加，或点击<上一步>修改加密对象配置信息。

图 4-58 添加加密对象-第三步

添加加密对象完成后，会在加密对象信息列表形成一条新的信息，状态为“未加密”状态，系统加密完成后，状态变为“已加密”状态。

以下情况不支持加密：

①DM7、DM8 较早版本（非官网当前版本）、MySQL 分区表配置表空间加密后，存在触发器、外键约束的表；

②Oracle、MySQL、GaussDB 等数据库在配置表空间加密方案后，包含子分区的分区表不支持加密；

③Oracle 数据库中若表中包含 LONG 类型字段，则该表中所有字段均不支持加密；

④Oracle 数据库配置原生加密方案后，表中同时包含 LONG 类型字段和以下任一类型字段时，不支持加密：BFILE；BINARY_DOUBLE；BINARY_FLOAT；BLOB；CLOB；INTERVAL_DAY_TO_SECOND；INTERVAL_YEAR_TO_MONTH；NCLOB；TIMESTAMP；TIMESTAMP_WITH_LOCAL_TIME_ZONE；TIMESTAMP_WITH_TIME_ZONE；

※注意：①MySQL 数据库默认存储引擎为 Innodb，其他类型皆不支持加密。②PostgreSQL 逻辑复制集群配置表空间加密方案后，仅支持发布订阅的主从节点数据库名、表名一致的情况，即当主从节点的数据库名或表名不一致时，针对表的加密会失败。③表空间加密下数据库存在加密对象时，禁止启/停插件，否则会造成数据损坏。④原生加密不支持选择加密算法，默认为 AES256，分组模式为 CBC。

2）网关加密

在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据源配置页面。

第一步：添加表。在操作区左侧，点击<+>按钮，选择需要添加的表，点击<下一步>选择对应的存量数据处理方案，可在更新原表数据和复制表并迁移数据中选择。

图 4-59 网关加密-添加加密表

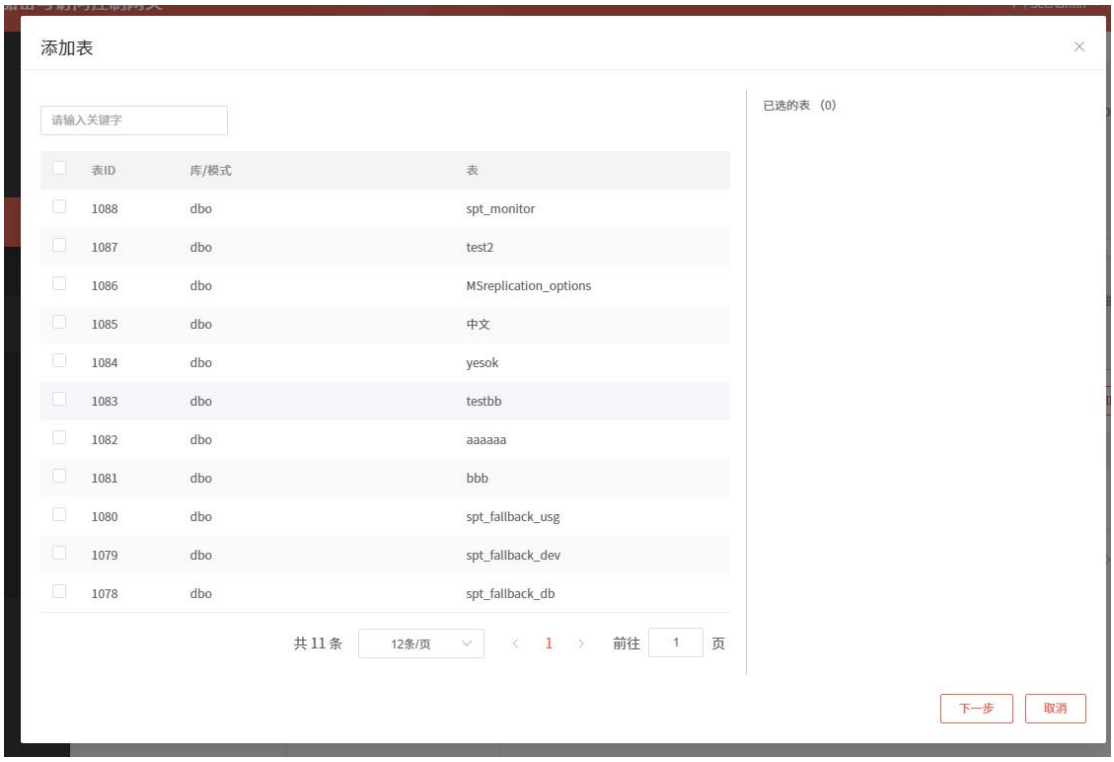

图 4-60 网关加密-添加加密表

图 4-61 网关加密-选择存量数据处理方案

第二步：添加加密对象（字段）。在对应的表下，点击<添加加密对象>按钮，选择需要加密的字段，弹窗内会展示字段的数据类型，和禁止加密的受限原因。

图 4-62 网关加密-添加加密对象

若加密对象字段的受限原因提示“未检测状态”，可点击<检测>按钮进行字段检测。若字段信息（新增字段、删除字段、数据类型更改等）发生变化，建议重新架构扫描，再添加加密对象。点击<下一步>按钮，进入加密算法配置弹窗页。

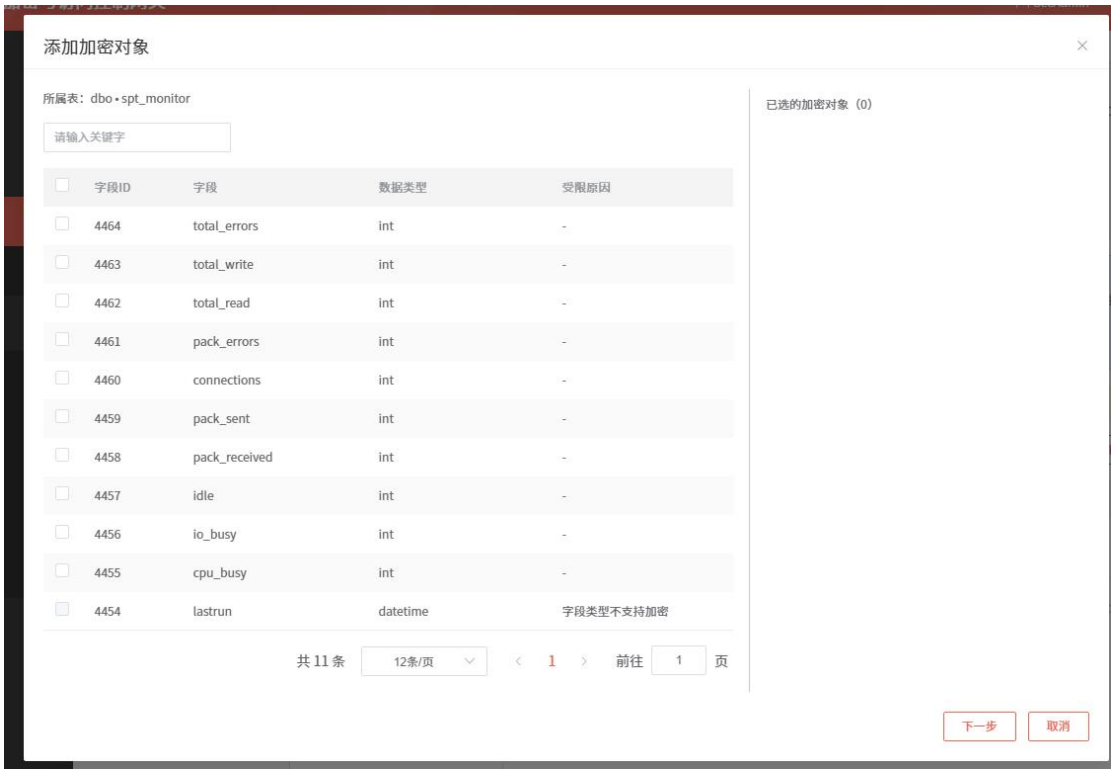

图 4-63 网关加密-添加加密对象

第三步：选择加密算法。不同数据库支持的加密算法不同，具体算法支持情

况可见“帮助手册”中的《各数据库的加密方案及算法支持规格》。可在输入框内输入关键字对指定表做相关配置。

系统默认为加密对象匹配随机密钥和默认加密算法，使用指定加密算法为指定表进行加密，点击对应表行的<默认>下拉框，选择指定加密算法，可以选择默认或其他算法。

点击<提交>按钮保存设置，或点击<取消>按钮取消添加加密对象，若想修改加密对象可点击<上一步>，对加密对象进行修改。

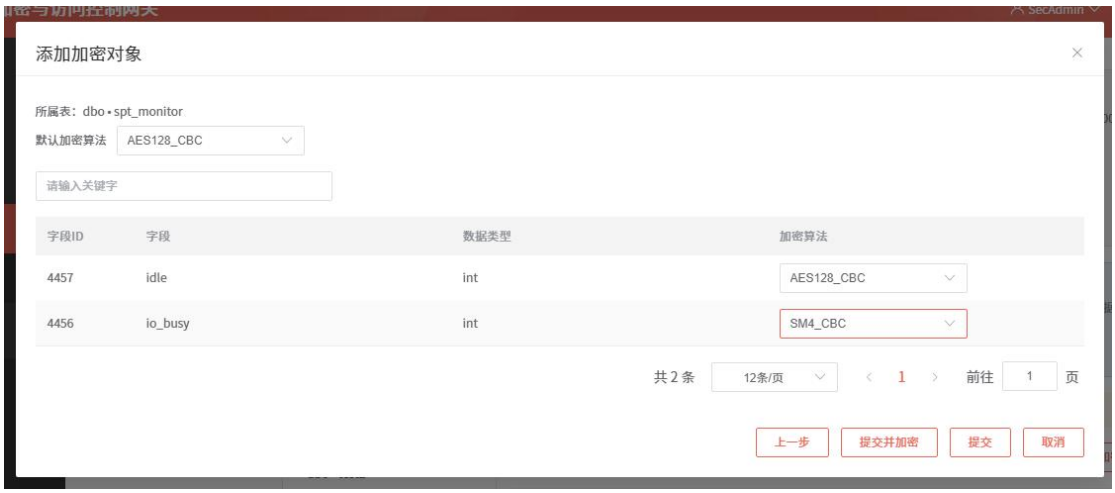

图 4-64 网关加密-选择加密算法

第四步：确认添加加密对象。点击<提交并加密>系统添加加密对象并自动执行加密操作，点击<提交>完成添加，点击<取消>取消添加，或点击<上一步>修改加密对象配置信息。

图 4-65 网关加密-确认加密

※注意：Oracle 数据库中若表中包含 LONG 类型字段，则该表中所有字段均不支持加密

4.5.1.5. 编辑加密对象

加密对象配置完成后，不支持修改加密参数，如加密算法。表空间加密、原生加密加密方案下，支持修改加密对象中包含的列。网关加密不支持修改加密对象。

若选择的加密方案为表空间加密或原生加密，在操作区对应加密对象操作列点击<编辑>按钮，弹出编辑加密列弹窗，展示所属库/模式、所属表信息，可选择包含全部列还是自定义包含列（字段）。

若选择包含全部列，在字段范围单选框中选择“全部列”，点击<提交>按钮完成加密对象编辑。

图 4- 66 编辑加密列-全部

若选择自定义包含列，在字段范围单选框中选择“自定义”，展示目前已选列信息，用户可继续选择包含列，也可取消已选列。点击<提交>按钮完成加密对象编辑。

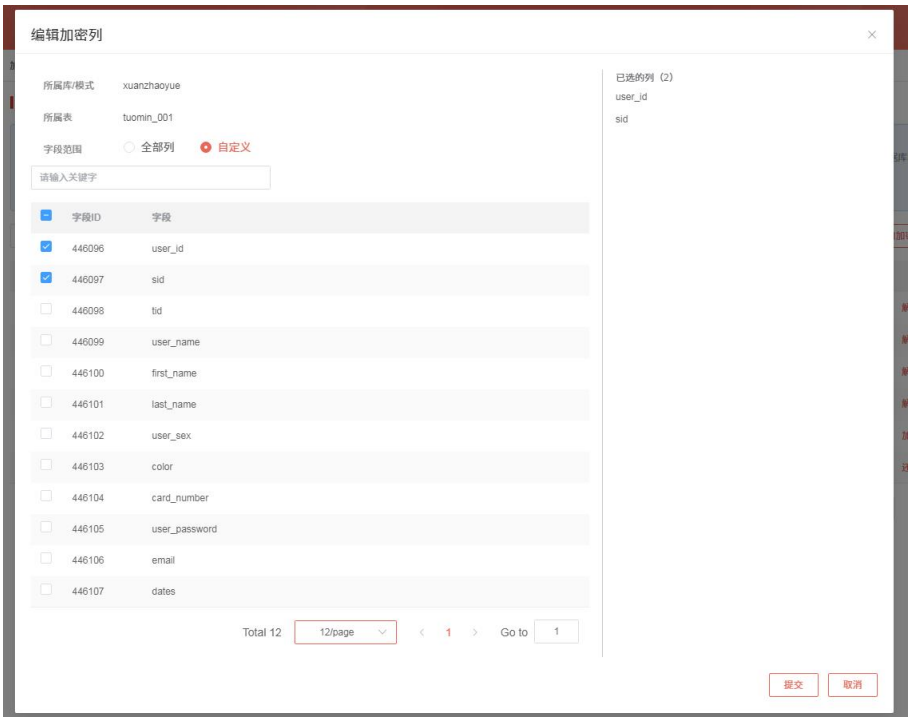

图 4- 67 编辑加密列-自定义

4.5.1.6. 删除加密对象

在操作区对应加密对象操作列点击<删除>或<批量删除>按钮，二次确认是否删除该加密对象。

※注意：仅可删除处于“未加密”状态的对象，不允许删除其他状态的对象。对象被删除后，可以再次添加。

4.5.1.7. 加解密业务处理

加密业务处理操作有三种，包括加密、解密、还原。

1) 加密

加密操作是用于对某个未加密或已解密的对象开启加密。

在操作区对应加密对象操作列点击<加密>按钮，加密对象状态由“未加密”变为“待加密”到“加密中”，待加密完成后变为“已加密”。若执行加密操作出现其他问题中断或加密卡非已开启时，状态将变为 “加密失败”。多个加密对象的加密操作可同时进行。

※注意：数据源的架构扫描任务处于“扫描中”或“停止中”状态时，无法进行加密操作。

2) 解密

解密操作是用于对某个已加密的对象开启解密。

在操作区对应加密对象操作列点击<解密>按钮，加密对象状态由“已加密”变为 “待解密”到“解密中”，待解密完成后变为“未加密”。 若执行解密操作出现其他问题中断或加密卡非已开启时，状态将变为 “加密失败”。多个加密对象的解密操作可同时进行。

※注意：数据源的架构扫描任务处于“扫描中”或“停止中”状态时，无法进行解密操作。

3) 还原

还原操作是为了当加密或解密发生问题中断时，用于恢复对象的状态。

在操作区对应加密对象操作列点击<还原>按钮，加密对象状态由“加密失败”或“解密失败”或“还原失败”变为 “还原中”，待还原完成后变为处理失败前的状态，即“加密失败”经还原后变回“未加密”，“解密失败”经还原后变回“已加密”“未加密”。若执行解密操作出现其他问题中断时，状态将变为 “还原失败”。多个加密对象的还原操作可同时进行。

※注意：数据源的架构扫描任务处于“扫描中”或“停止中”状态时，无法进行还原操作。

4) 加解密操作历史

在操作区对应加密对象操作列点击<历史>按钮，用户可以在此查看指定加密对象的操作历史信息，包括加密对象的库/模式、加密对象表、操作类型、操作

人、操作时间、处理状态、处理结果（成功或失败）等，见下图：

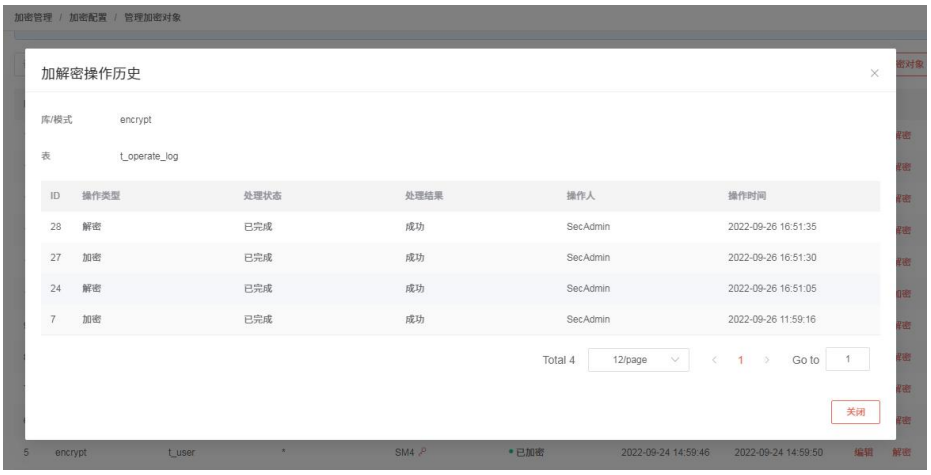

图 4- 68 加解密操作历史

4.5.2. 读保护

“读保护”指的是，用户通过数据库客户端工具访问数据库时，用户的 SQL 请求结果中需要保护的字段会进行脱敏处理，确保访问者无法读取明文数据。网关加密方案下，查看读保护字段内容可能以空白形式展示。

“读保护”开启后，统一采用全部遮蔽脱敏算法；支持基于不同的字段类型选择不同的遮蔽符，字符串类型采用“*”号遮蔽，整型、浮点型采用数字“0”遮蔽。

※注意：以下情形通过数据库客户端查询数据，数据将未被遮蔽脱敏：①表名带空格；②Oracle 数据库包含包（package）、同义词（synonym）的表加密并开启读保护后，通过包或同义词查询数据时。③表空间加密下配置时，选择“保持现有连接”。

4.5.2.1. 切换状态

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。在防护状态栏点击<开启读保护>按钮，需二次确认是否开启读保护。开启后可通过<关闭读保护>按钮关闭读保护。

图 4-69 开启读保护

※注意：①加密卡非已开启状态时、数据源所使用插件状态异常（选择表空间加密方案时），读保护功能无法开启。数据源未添加任何加密对象时，仍可以开启“读保护”功能，只是不会对任何字段做脱敏操作。②切换读保护状态，通过数据库客户端，不带模式名查询表时会提示表不存在，可通过重新打开 SQL 窗口再次尝试。

4.5.2.2. 例外规则管理

“读保护”的例外情况是指在“读保护”功能已开启的状态下，可能存在一些特定的场景，在这些场景中用户可以访问已保护对象的数据明文，即不进行脱敏处理。“读保护”的例外规则（以下简称“规则”）就是用来定义这些特定场景的一种规则模型，系统可以基于这些规则模型来自动判断是否需要对对象做脱敏处理。

例外规则可以任意设置，但仅在“读保护”功能已开启时才生效。当数据源存在多个已启用且在生效时间内的例外规则时，访问请求匹配到其中任意一个，即认为已命中规则。

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。在防护状态栏“例外规则”旁会显示已启用的规则条数，点击例外规则旁的<管理规则>按钮，进入到该数据源下的“读保护”例外规则列表页面，内容包括：读保护状态、规则名称、状态、创建时间、更新时间等，如下图：

图 4-70 例外规则列表

在操作区输入框内输入规则名称关键字或选择规则状态，点击<查询>按钮，按条件筛选查询例外规则。

1) 添加规则

在操作区点击<添加规则>按钮，进入到“添加规则”页面，添加新规则，相关配置内容如下表：

配置项	是否必填	说明
规则名称	是	填写规则名称，不能重复，30 个字符以内
规则状态	启用和禁用二选一	选择启用或者禁用，默认为启用
选择方式	全部已加密数据和自定义范围二选一	选择全部已加密数据或者自定义范围，默认全部已加密数据
选择范围	自定义范围下必填	根据库/模式、表、字段信息圈定的范围，已添加的加密对象范围的子集
数据库账号	否	选择数据库账号，支持选择多个
来源 IP	否	输入单个 IP、IP 段或 IP/子网表示 IP 范围，使用逗号“,”分隔。如：172.16.1.100（单个 IP），172.16.2.101-172.16.2.120（IP 段），172.16.10.0/24（IP/子网）
时间范围	否	选择生效的时间范围，精确到秒，如：2022-08-08 08:00:00 ~ 2022-08-10 12:00:00

图 4- 71 添加例外规则

当范围选择“自定义范围”时，用户需要点击“选择范围”中的<添加>按钮，在页面弹窗选择数据范围。弹窗中展示了该数据源下已被添加为加密对象的所有表，用户需要勾选指定的表，并选择是表中全部字段还是自定义字段。

若已选表的字段范围全为“全部”，点击<提交>按钮完成数据范围选择，选择范围列表会增加对应表信息，点击<删除>可删除单个自定义范围。

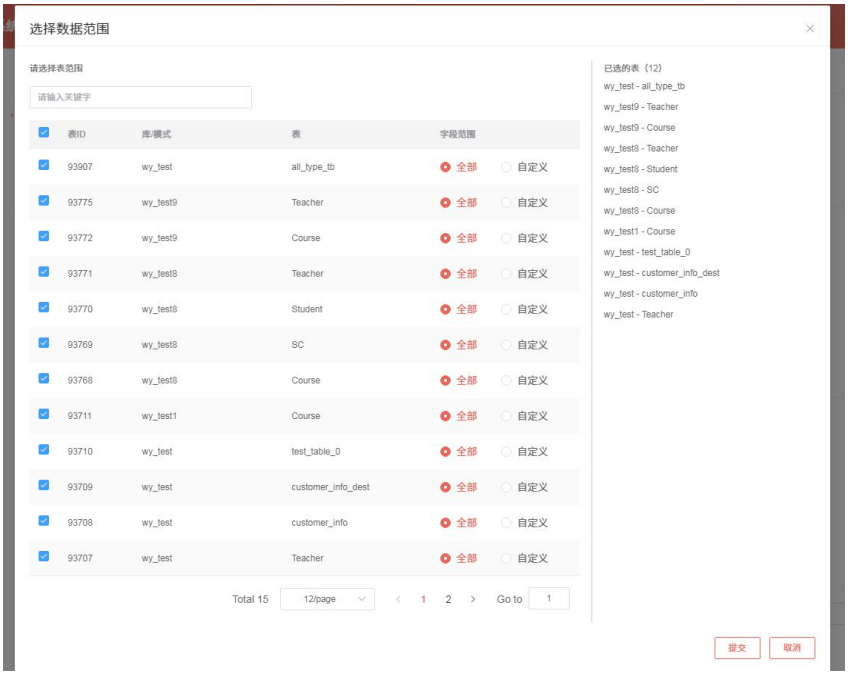

图 4- 72 选择数据范围-全部

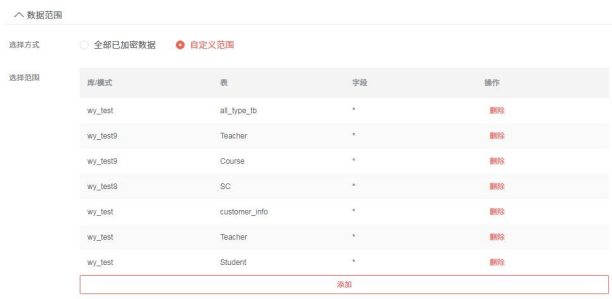

图 4-73 选择范围列表

若已选表的字段范围中含有“自定义”选择，用户需点击<下一步>按钮进一步选择字段，点击<提交>按钮完成数据范围选择，选择范围列表会增加对应表信息，点击<删除>可删除单个自定义范围。

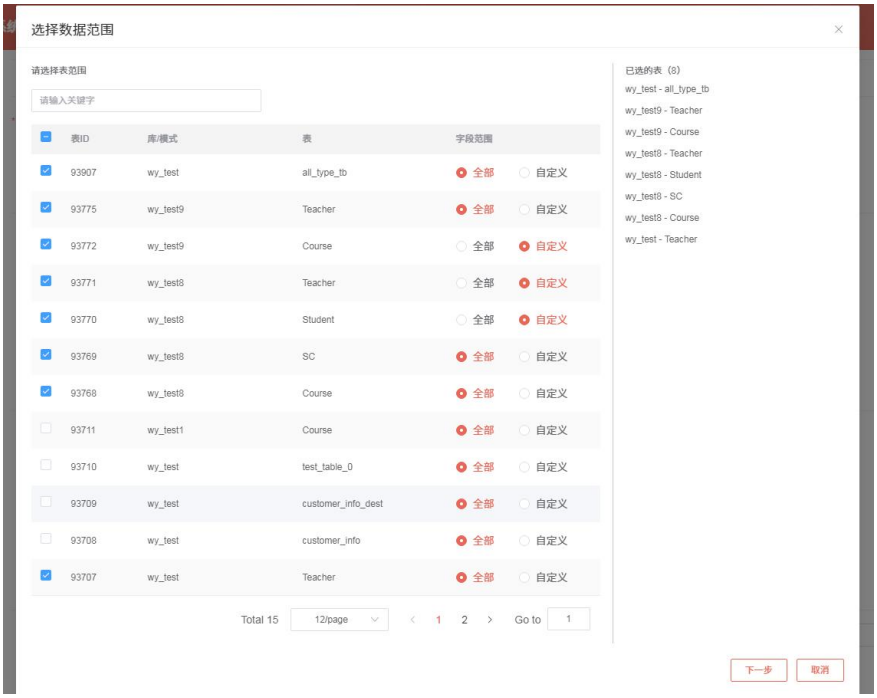

图 4-74 选择数据范围-自定义

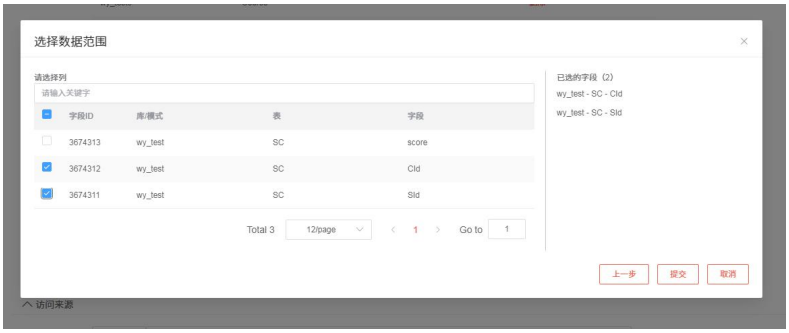

图 4-75 选择数据范围-自定义

图 4- 76 选择数据列表

2) 切换状态

在操作区操作列内点击<启用>按钮，二次确认是否要启用规则，点击<确定>完成启用操作。可勾选多条规则选择批量启用。

在操作区操作列内点击<停用>按钮，二次确认是否要停用规则，点击<确定>完成停用操作。可勾选多条规则选择批量停用。

3) 查看规则

在操作区点击<查看>按钮，进入到该例外规则的详情页面，内容包括：规则名称、规则状态、已选范围、数据库账号、来源 IP、时间范围等，见下图：

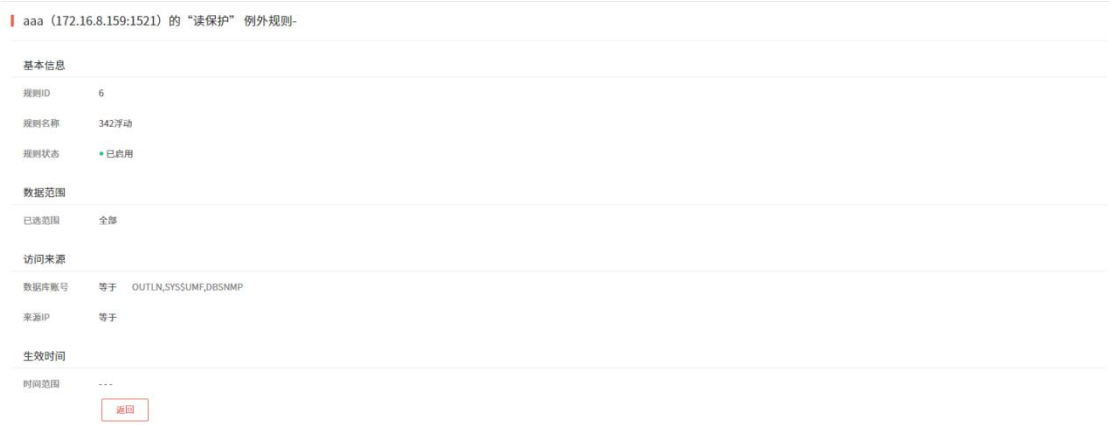

图 4- 77 规则详情

4) 查找规则

在操作区数据框内输入规则名称关键字，或者在状态下拉框中选择状态已启用或未启用，点击<查询>按钮完成按条件筛选查询规则。

5) 编辑规则

在操作区点击<编辑>按钮，进入到“编辑规则”页面，相关配置内容如下表：

配置项	是否必填	说明
规则名称	是	填写规则名称，不能重复，30 个字符以内
规则状态	启用和禁用二选一	选择启用或者禁用，默认为启用
选择方式	全部已加密数据和自定义范围二选一	选择全部已加密数据或者自定义范围，默认全部已加密数据
选择范围	自定义范围下必填	根据库/模式、表、字段信息圈定的范围，

		已添加的加密对象范围的子集
数据库账号	否	选择数据库账号，支持选择多个
来源 IP	否	输入单个 IP、IP 段或 IP/子网表示 IP 范围，使用逗号“,”分隔。如：172.16.1.100（单个 IP）, 172.16.2.101-172.16.2.120（IP 段）, 172.16.10.0/24（IP/子网）
时间范围	否	选择生效的时间范围，精确到秒，如：2022-08-08 08:00:00 ~ 2022-08-10 12:00:00

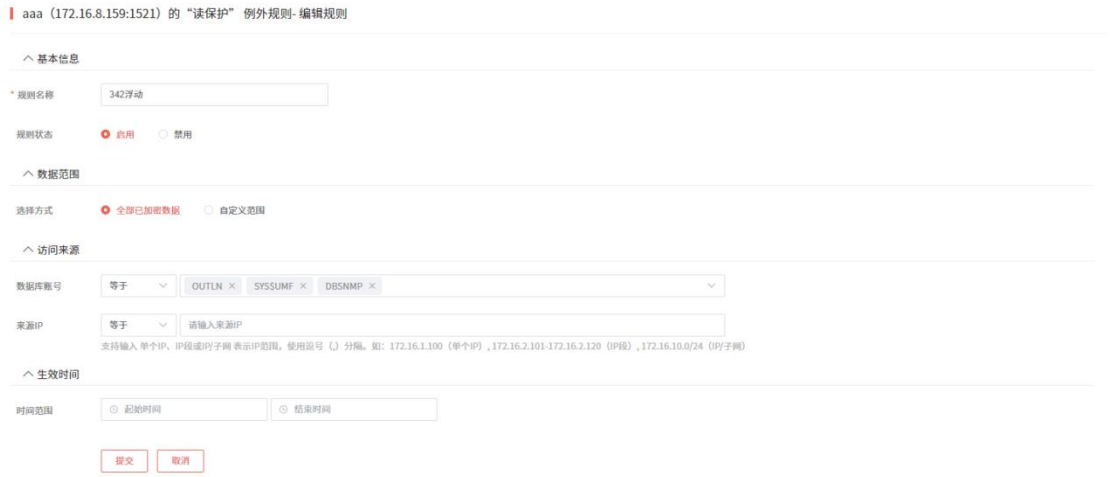

图 4- 78 编辑规则

当范围选择“自定义范围”时，用户需要点击“选择范围”中的<添加>按钮，在页面弹窗选择数据范围。弹窗中展示了该数据源下已被添加为加密对象的所有表，用户需要勾选指定的表，并选择是表中全部字段还是自定义字段。

若已选表的字段范围全为“全部”，点击<提交>按钮完成数据范围选择，选择范围列表会增加对应表信息，点击<删除>可删除单个范围。

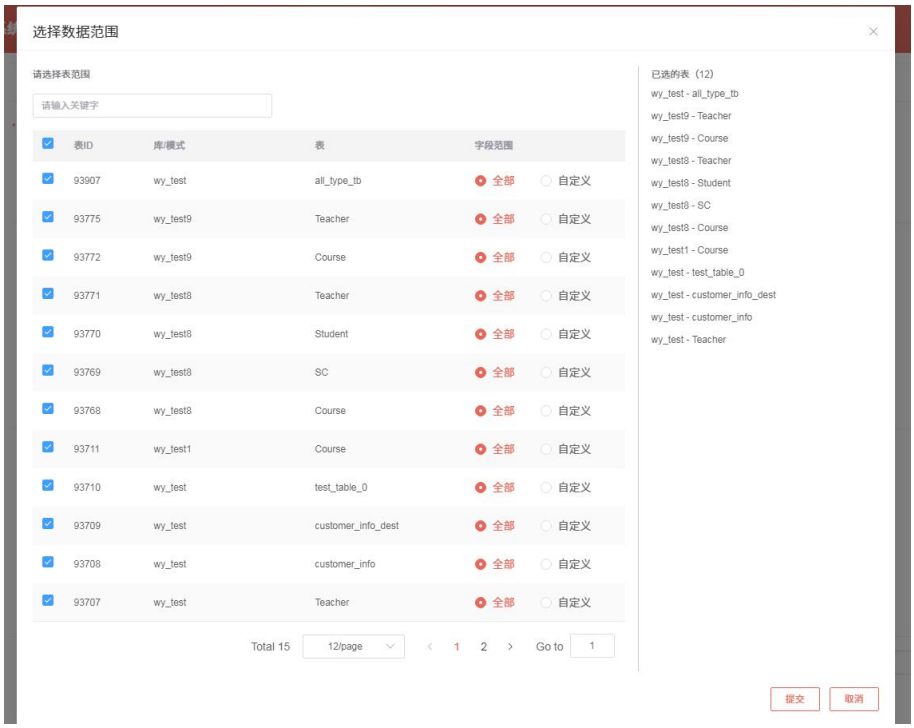

图 4-79 选择数据范围-全部

图 4-80 选择范围列表

若已选表的字段范围中含有“自定义”选择，用户需点击<下一步>按钮进一步选择字段，点击<提交>按钮完成数据范围选择，选择范围列表会增加对应表信息，点击<删除>可删除单个自定义范围。

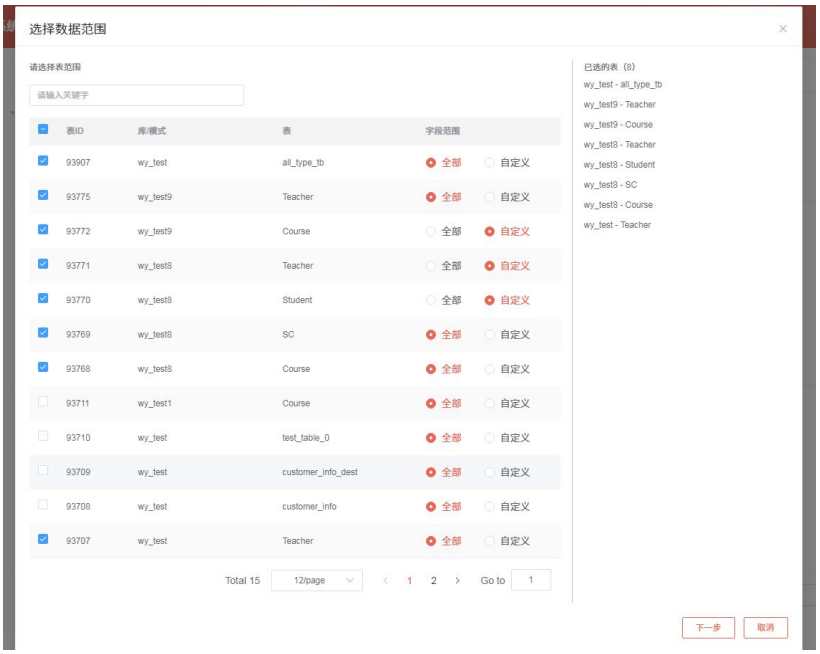

图 4-81 选择数据范围-自定义

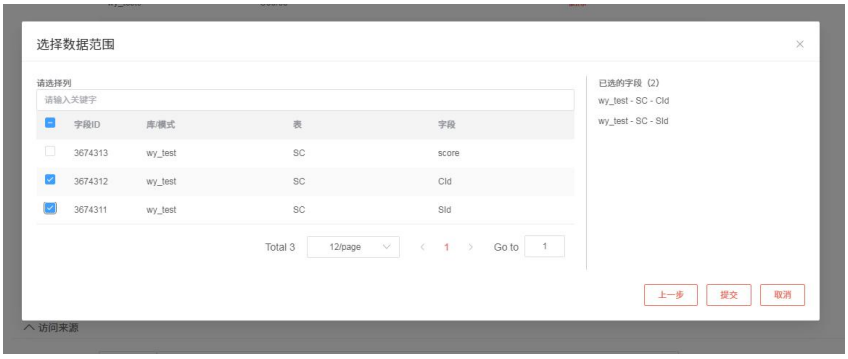

图 4-82 选择数据范围-自定义

图 4-83 选择数据列表

6) 删除规则

在操作区操作列内点击<删除>按钮，二次确认是否要删除规则，点击<确定>完成删除操作。可勾选多条规则选择批量删除。

4.5.3. 完整性保护

完整性保护是指，用户通过数据库客户端工具未通过代理方式，而是直接连接数据库时，若对保护字段的修改，可以通过加密系统验证，以便及时发现数据

是否被篡改，保证数据库中的数据完整性。

只有在网关加密方案下，可开启完整性保护功能，完整性保护和网关加密互不影响。

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。选择使用网关加密的数据源，在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。在完整性保护已开启的情况下，点击<管理保护对象>按钮，进入到管理完整性保护对象页面。内容包括：表、字段、签名算法、保护状态、验证状态、验证时间等，如下图：

图 4-84 管理保护对象

4.5.3.1. 切换状态

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加密配置列表页面。选择使用网关加密的数据源，在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。在防护状态栏完整性保护旁，点击<启用>按钮，需二次确认是否开启完整性保护。开启后可通过<关闭>按钮关闭完整性保护。

图 4-85 开启完整性保护

4.5.3.2. 添加保护对象

安全管理员登录系统后，点击“策略管理”->“加密配置”进入到数据源加

密配置列表页面。选择使用网关加密的数据源，在操作区点击<配置>按钮，或者在左侧数据源列表中点击对应数据源可进入到数据库配置页面。在完整性保护已开启的情况下，点击<管理保护对象>按钮，进入到管理完整性保护对象页面。

第一步：添加表。在操作区左侧，点击<+>按钮，选择需要添加的表，点击<下一步>选择对应的存量数据处理方案，可在更新原表数据和复制表并迁移数据中选择。

图 4-86 完整性保护-添加表

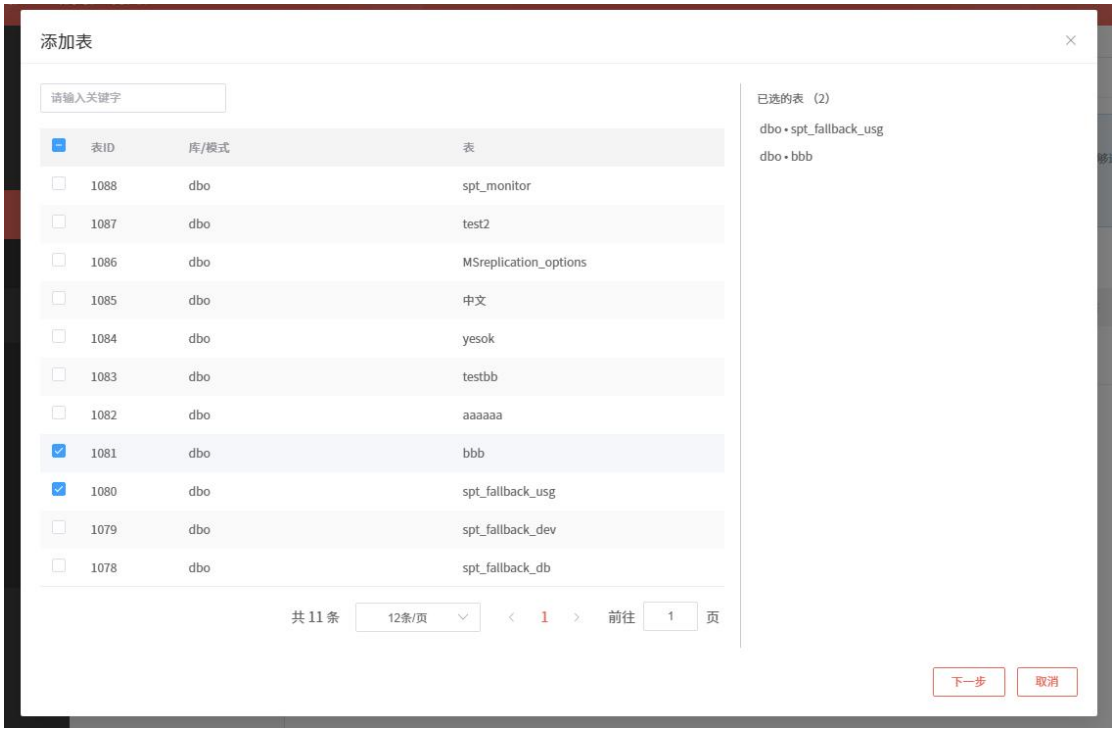

图 4-87 完整性保护-添加表

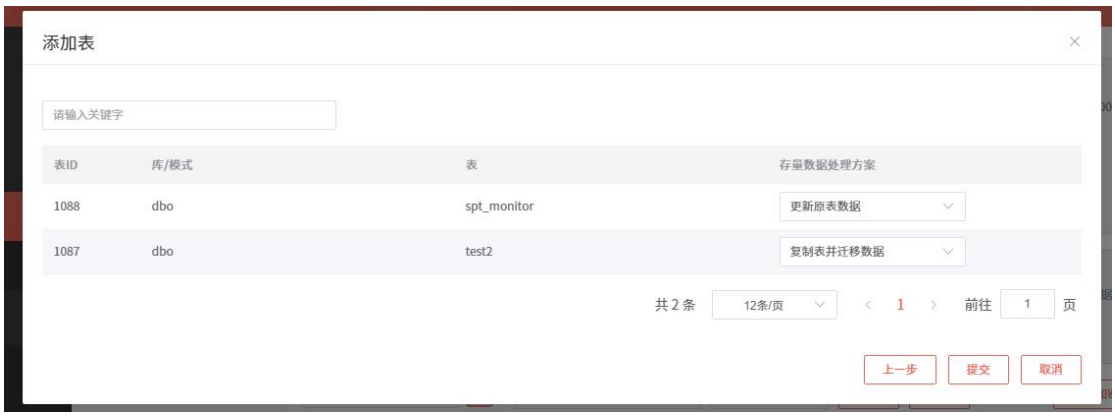

图 4-88 完整性保护-选择存量数据处理方案

第二步：添加保护对象（字段）。在对应的表下，点击<添加保护对象>按钮，选择需要保护的字段，弹窗内会展示字段的数据类型，和禁止签名的受限原因。

图 4-89 完整性保护-添加保护对象

若加密对象字段的受限原因提示“未检测状态”，可点击<检测>按钮进行字段检测。若字段信息（新增字段、删除字段、数据类型更改等）发生变化，建议重新架构扫描，再添加加密对象。点击<下一步>按钮，进入签名算法配置弹窗页。

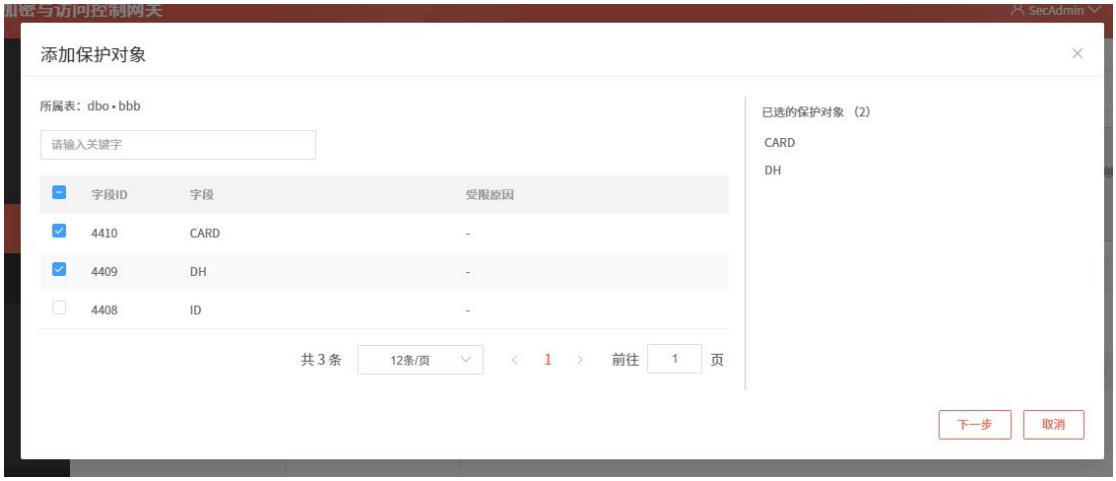

图 4-90 完整性保护-添加保护对象

第三步：选择签名算法。可在输入框内输入关键字对指定表做相关配置。

系统默认为加密对象匹配随机密钥和默认签名算法，使用指定签名算法为指定字段进行加密，点击对应表行的<默认>下拉框，选择指定签名算法，可以选择默认或其他算法。

点击<提交>按钮保存设置，或点击<取消>按钮取消添加加密对象，若想修改加密对象可点击<上一步>，对保护对象进行修改。

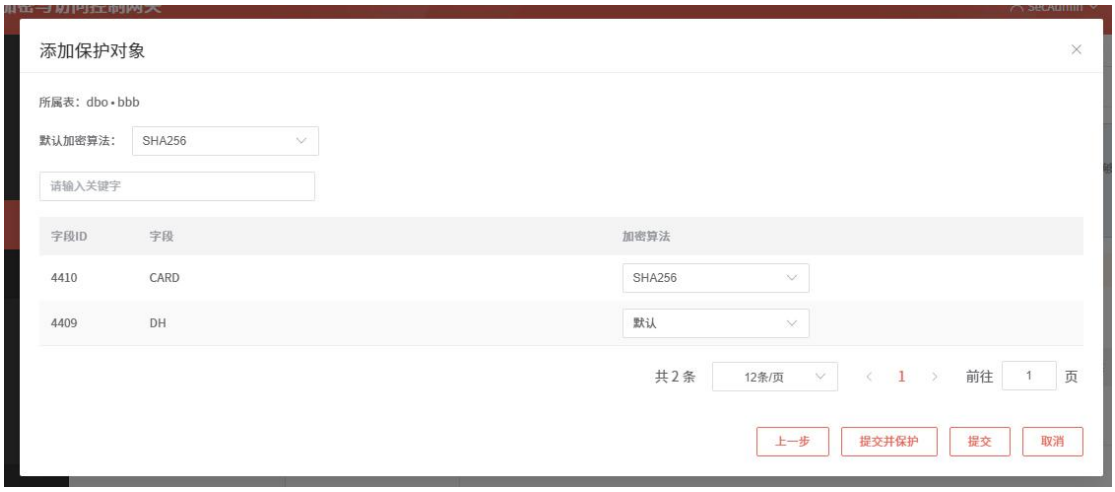

图 4-91 完整性保护-选择签名算法

第四步：确认添加保护对象。点击<提交并保护>系统添加保护对象并自动执行签名操作，点击<提交>完成添加，点击<取消>取消添加，或点击<上一步>修改保护对象配置信息。

图 4-92 完整性保护-确认添加保护对象

4.5.3.3. 签名保护对象

签名保护操作是用于对某个未签名的对象进行签名保护。

在操作区对应保护对象操作列点击<保护>按钮，加密对象状态由“未签名”变为“签名中”，待签名完成后变为“已签名”。若执行签名操作出现其他问题

中断时，状态将变为 “签名失败”。通过批量操作，多个保护对象的签名操作可同时进行。

图 4-93 签名保护操作

4.5.3.4. 验证数据完整性

验证操作是用于对某个已签名的对象进行数据的完整性校验。

在操作区对应已签名的保护对象操作列点击<验证>按钮，加密对象状态由“未验证”变为“验证中”，待验证完成后变为“验证通过”或“验证未通过”。若执行验证操作出现其他问题中断时，状态将变为 “验证失败”。

验证通过，即数据未被非法篡改。验证未通过，即数据被非法篡改。

已签名保护的数据列，当发生以下情况时，视为数据被篡改：

a)未经加密系统授权（即绕过加密系统的代理网关直接访问数据库），更新了数据内容；

b)未经加密系统授权（即绕过加密系统的代理网关直接访问数据库），添加了数据内容；

c)表名或列名被修改；

已签名保护的数据列，当发生以下情况时，视为针对数据的正常操作（数据未被篡改）：

a)经过加密系统代理网关，添加或更新了数据内容；

b)删除了数据（无论是否经过加密系统代理网关）；

4.5.3.5. 撤销签名保护

撤销保护操作是用于对某个已签名的对象撤销其签名保护。

在操作区对应保护对象操作列点击<撤销>按钮，加密对象状态由“已签名”变为“撤销中”，待签名完成后变为“未签名”。若执行签名操作出现其他问题中断时，状态将变为 “撤销失败”。通过批量操作，多个保护对象的签名操作可同时进行。

4.5.3.6. 删除保护对象

在操作区对应签名对象操作列点击<删除>或<批量删除>按钮，二次确认是否删除该签名对象。

※注意：仅可删除处于“未签名”状态的对象，不允许删除其他状态的保护对象。保护对象被删除后，可以再次添加。

4.5.3.7. 签名操作历史

在操作区对应加密对象操作列点击<历史>按钮，用户可以在此查看指定保护对象的操作历史信息，包括保护对象对一个的表和字段、处理类型、处理状态、处理结果、数据量、耗时、平均速率、操作人、操作时间等，见下图：

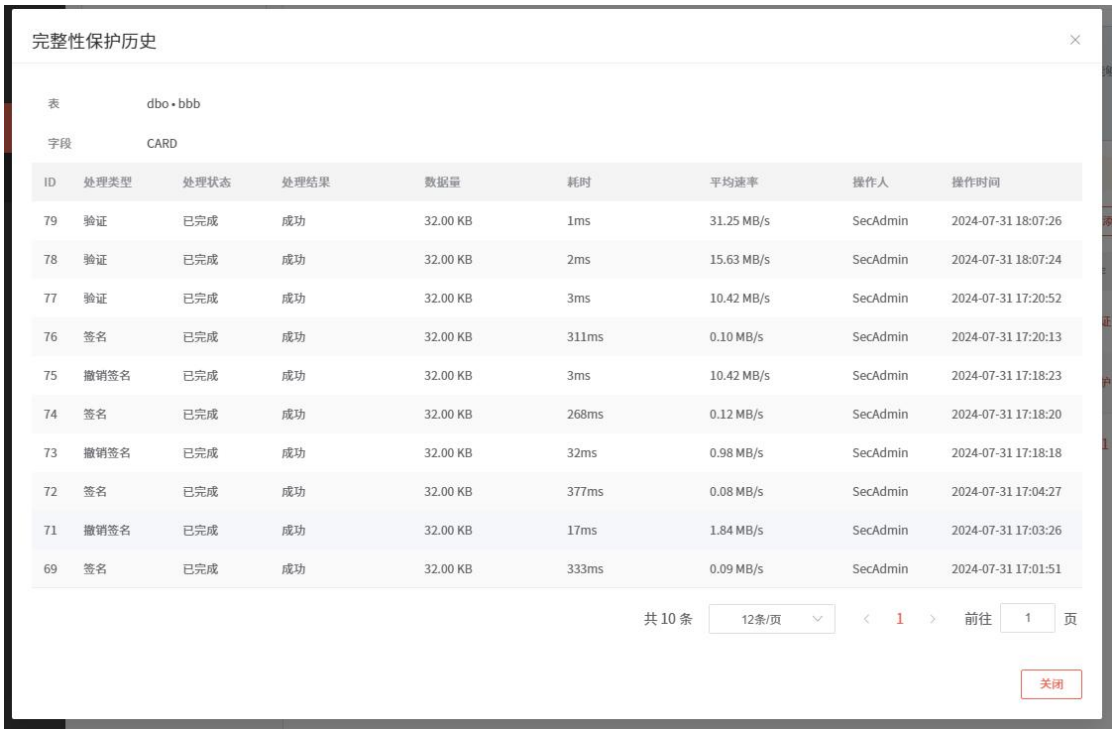

图 4-94 签名操作历史

4.5.4. 访问控制

访问控制是指，用户通过数据库客户端工具访问数据库时，指定用户的指定操作（增加、删除、修改、查询操作）会根据规则的设定而放行或阻断，来防止用户进行危险操作，保证数据库中的数据安全。

开启访问控制功能后，若控制方式为“阻断”，系统将阻断所有命中规则的访问请求，放行其他未命中的请求；若控制方式为“放行”，系统将放行所有命中规则的访问请求，阻断其他未命中的请求；若控制方式为“关闭”或“未开启”，则不对数据库用户或操作进行限制。

安全管理员登录系统后，点击“策略管理”->“访问控制”，进入到数据源

访问控制列表页面。用户可以在此查看数据源访问控制情况信息，包括数据源名称、服务类型、地址：端口、已启用规则数量、未启用规则数量、控制模式等，见下图：

图 4-95 数据源访问控制列表

在操作区输入框内数据关键字，点击<查询>按钮，可按条件筛选搜索相关数据源。

4.5.4.1. 切换模式

安全管理员登录系统后，点击“策略管理”->“访问控制”，未做设置的控制模式应为“未开启”状态，即对数据库账号和操作类型没有限制。点击指定数据源的<切换模式>按钮，可设置该数据源的控制模式。可选控制模式有三种：关闭、阻断、放行。

※注意：加密卡非已开启状态、数据源（包含插件）异常、数据源未进行架构扫描、未选择加密方案时，访问控制功能无法开启。

图 4-96 切换控制模式

另一种切换模式方式，点击“策略管理”->“访问控制”，指定数据源操作列点击<规则管理>按钮，进入到访问控制规则列表，在控制模式状态框中点击<切换>按钮，可设置该数据源的控制模式。可选控制模式有三种：关闭、阻断、放行。

图 4-97 控制模式状态框

4.5.4.2. 访问控制规则管理

访问控制规则可以任意设置，但仅在模式为“阻断”和“放行”时才生效。当数据源存在多个已启用的访问控制规则时，访问请求匹配到其中任意一个，即认为已命中规则。

安全管理员登录系统后，点击“策略管理”->“访问控制”，可查看该数据源下有访问控制规则的开启和关闭情况。点击指定数据源操作列的<规则管理>，进入到该数据源下的访问控制规则列表页面，内容包括：规则名称、状态、创建时间、更新时间等，如下图：

图 4-98 访问控制规则列表

1) 添加规则

在操作区点击<添加规则>按钮，进入到“添加规则”页面，添加新规则，相关配置内容如下表：

配置项	是否必填	说明
规则名称	是	填写规则名称，不能重复，30 个字符以内
规则状态	启用和禁用二选一	选择启用或者禁用，默认为启用
数据库账号	是	选择数据库账号，支持选择多个
操作类型	是	选择操作类型，由 INSERT、DELETE、UPDATE、SELECT 中单选或多选

图 4- 99 添加规则

2) 切换状态

在操作区操作列内点击<启用>按钮，二次确认是否要启用规则，点击<确定>完成启用操作。可勾选多条规则选择批量启用。

图 4- 100 启用规则

在操作区操作列内点击<停用>按钮，二次确认是否要停用规则，点击<确定>完成停用操作。可勾选多条规则选择批量停用。

图 4- 101 停用规则

3) 查看规则

在操作区点击<查看>按钮，进入到该规则的详情页面，内容包括：规则名称、规则状态、操作类型、数据库账号、创建时间、更新时间等，见下图：

图 4- 102 规则详情

4) 查找规则

在操作区数据框内输入规则名称关键字，或者在状态下拉框中选择状态已启用或未启用，点击<查询>按钮完成按条件筛选查询规则。

5) 编辑规则

在操作区点击<编辑>按钮，进入到“编辑规则”页面，相关配置内容如下表：

配置项	是否必填	说明
规则名称	是	填写规则名称，不能重复，30 个字符以内
规则状态	启用和禁用二选一	选择启用或者禁用，默认为启用
数据库账号	是	选择数据库账号，支持选择多个
操作类型	是	选择操作类型，由 INSERT、DELETE、UPDATE、SELECT 中单选或多选

图 4- 103 编辑规则

6) 删除规则

在操作区操作列内点击<删除>按钮，二次确认是否要删除规则，点击<确定>完成删除操作。可勾选多条规则选择批量删除。

图 4- 104 删除规则

4.6. 用户与角色

安全管理员仅支持操作默认用户、安全管理员、安全操作员和自定义角色的用户。

4.6.1. 用户管理

安全管理员登录系统后，点击“用户与角色”->“用户管理”进入到用户列表页面。用户可以在此查看用户信息，包括用户名、所属角色、是否内置、状态（正常/禁用）、UKEY、最近登录时间、创建时间等，见下图：

图 4- 105 用户列表

4.6.1.1. 授权用户

在操作区通过点击<授权>按钮，用户可查看当前用户角色，选择切换角色（可在默认用户、安全操作员和自定义角色中选择），并选择是否重置密码。点击<提交>保存设置，若当前用户正在登录中，系统会主动注销该用户的会话，该用户需重新登录。

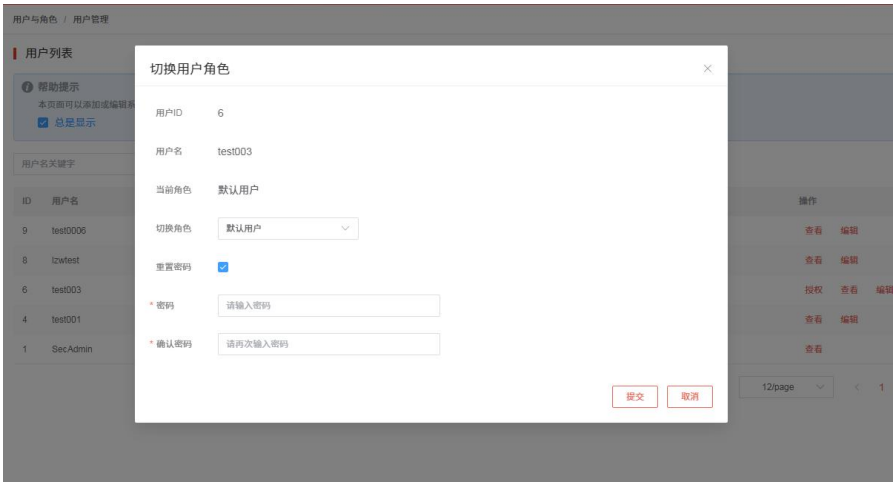

图 4- 106 切换用户角色

4.6.1.2. 查看用户

在操作区通过点击<查看>按钮，可以查看用户信息，包括：用户名、所属角色、真实姓名、手机号码、电子邮箱、状态、UKEY、是否内置、登录次数、最近登录 IP、最近登录时间、创建时间、更新时间，如下图：

图 4- 107 查看用户

在操作区输入框内填写用户名关键字，点击<查询>按钮，可以筛选查找相关用户。

4.6.1.3. 编辑用户

在操作区通过点击<编辑用户>按钮，编辑用户信息，相关配置内容如下表：

配置项	是否必填	说明
密码	否	填写密码，长度要求 10-20 个字符；至少包含大写字母、小写字母、数字、特殊字符（`~!@#$%^&*()-_=+|[{}];:'",<.>/? 和空格）中的三种；不能与用户名相同；留空表示不修改密码
确认密码	否	与密码相同
真实姓名	否	填写姓名
手机号	否	填写手机号，长度 11 个字符。且应 13、14、15、18 开头，14 开头的第三位只能是 5、7，15 和 18 开头第三位不能是 4
电子邮箱	否	填写电子邮箱

点击<提交>按钮保存设置；或者点击<取消>按钮取消编辑。

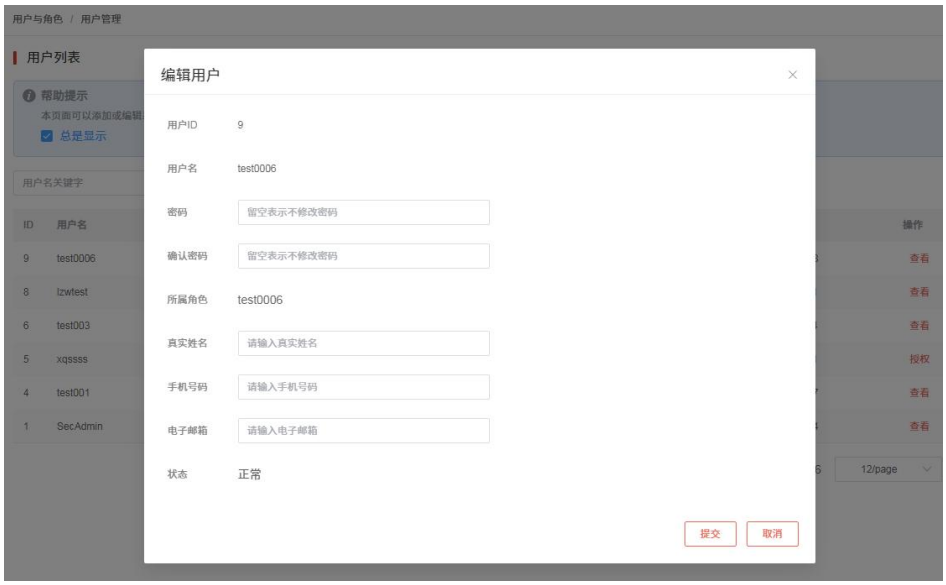

图 4-108 编辑用户

4.7. 系统信息系统状态

安全管理员登录后，点击 “系统信息”->“系统状态”进入该页面。页面内容与系统管理员登录后的系统状态一致，详情可查看 3.6.1 章节。

4.7.2. 帮助手册

安全管理员登录后，点击 “系统信息”->“帮助手册”进入该页面。页面内容与系统管理员登录后的系统状态一致，详情可查看 3.6.2 章节。

4.8. 个人中心

安全管理员修改密码与修改资料方法与系统管理员一致，详情可查看 3.7 章节。

5. 审计管理概述

审计管理需使用审计管理员登录产品进行相关设置，审计管理员是数据库加密与访问控制网关三大管理员之一，主要负责操作日志管理。

审计管理包含内容见下表：

主菜单	分类	功能说明
首页	业务基础数据统计	当前备用、在用、历史密钥数量；当前数据源总量、数据源状态异常数量、数据源类型分布
		当前加密表数、未加密表数统计
		最新加密对象信息
	其他数据统计	当前加密卡信息和状态
		当前插件总量、插件状态异常数量
	系统资源统计	CPU、内存的准实时占用率统计；系统接口准实时接收/发送流量统计
用户与角色	用户管理	授权（可授权为审计操作员或默认用户）、编辑、查看用户详情
系统信息	系统日志	查看系统日志
	系统状态	CPU、内存的近 1 小时占用率统计；数据空间、总储存空间使用情况
	帮助手册	查看系统使用中相关的配置指导手册
个人中心	修改资料	修改个人资料
	修改密码	修改个人密码

5.2. 首页

安全管理员在登录后默认进入首页界面，页面内容与系统管理员登录后的首页一致，详情可查看 3.2 章节。

5.3. 用户与角色

审计管理员仅支持操作默认用户、审计管理员和审计操作员。

5.3.1. 用户管理

审计管理员登录系统后，点击“用户与角色”->“用户管理”进入到用户列表页面。用户可以在此查看用户信息，包括用户名、所属角色、是否内置、状态（正常/禁用）、UKEY、最近登录时间、创建时间等，见下图：

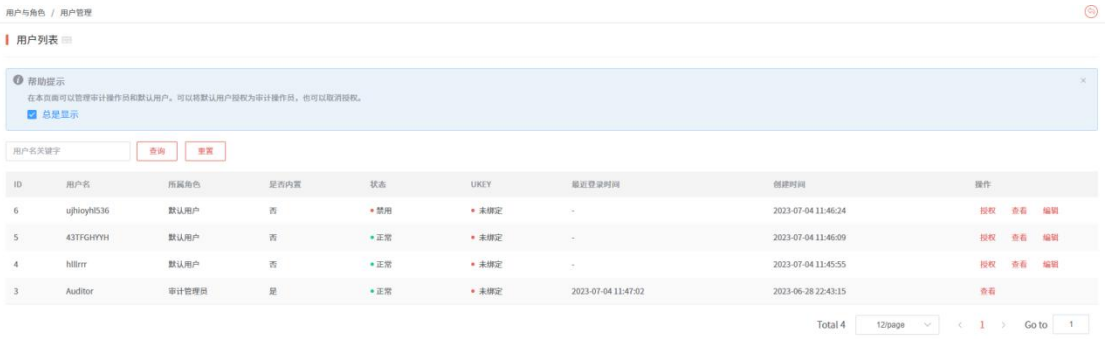

图 5-1 用户列表

5.3.1.1. 授权用户

在操作区通过点击<授权>按钮，用户可查看当前用户角色，选择切换角色（可在默认用户和审计操作员中选择），并选择是否重置密码。点击<提交>保存设置，若当前用户正在登录中，系统会主动注销该用户的会话，该用户需重新登录。

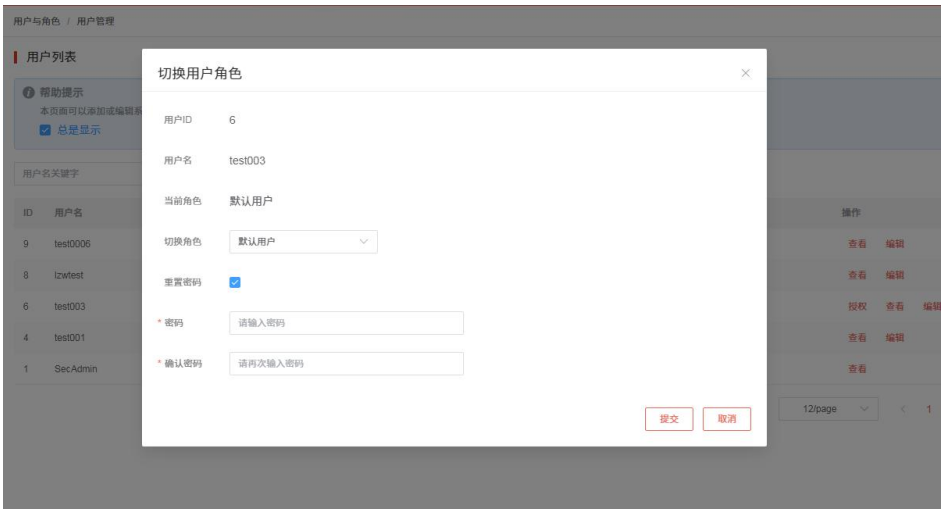

图 5-2 切换用户角色

※注意：授权操作只能对默认用户或者审计操作员进行。

5.3.1.2. 查看用户

在操作区通过点击<查看>按钮，可以查看用户信息，包括：用户名、所属角色、真实姓名、手机号码、电子邮箱、状态、是否内置、登录次数、最近登录 IP、最近登录时间、创建时间、更新时间，如下图：

图 5-3 查看用户

在操作区输入框内填写用户名关键字，点击<查询>按钮，可以筛选查找相关用户。

5.3.1.3. 编辑用户

在操作区通过点击<编辑用户>按钮，编辑用户信息，相关配置内容如下表：

配置项	是否必填	说明
密码	否	填写密码，长度要求 10-20 个字符；至少包含大写字母、小写字母、数字、特殊字符（`~!@#$%^&*()-_=+|[{}];:'",<.>/? 和空格）中的三种；不能与用户名相同；留空表示不修改密码
确认密码	否	与密码相同
真实姓名	否	填写姓名

手机号	否	填写手机号，长度 11 个字符。且应 13、14、15、18 开头，14 开头的第三位只能是 5、7，15 和 18 开头第三位不能是 4
电子邮箱	否	填写电子邮箱

点击<提交>按钮保存设置；或者点击<取消>按钮取消编辑。

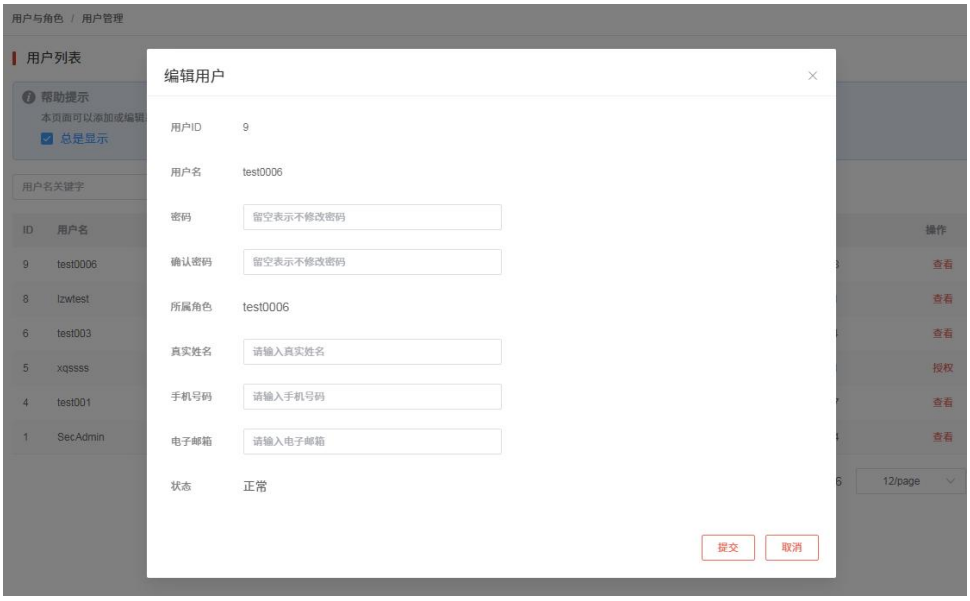

图 5-4 编辑用户

5.4. 系统信息

系统信息功能主要包括系统日志和系统状态两部分。

5.4.1. 系统日志

审计管理员登录后，点击 “系统信息”->“系统日志”进入到系统日志列表。用户可以在此查看日志信息，包括日志描述、操作类型、操作结果、操作人、操作客户端 IP、操作时间等，见下图：

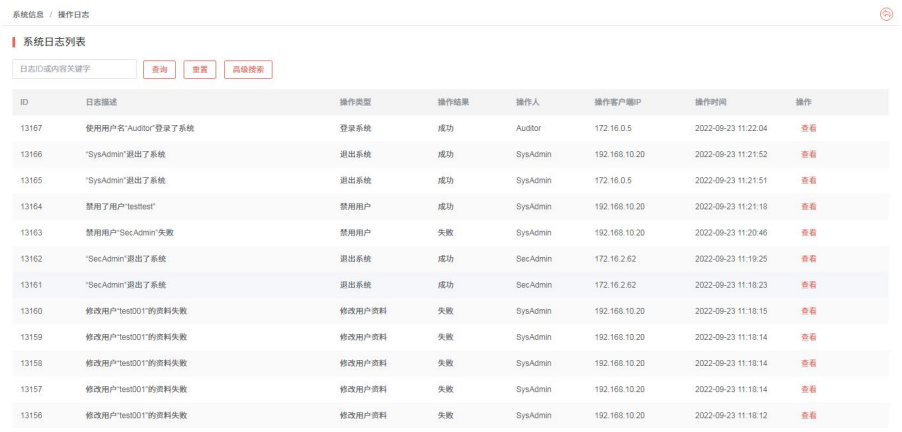

图 5-5 系统日志列表

5.4.1.1. 查看日志

在操作区通过点击<查看>按钮，可以查看日志信息，包括：日志描述、操作类型、操作结果、操作人、操作客户端 IP、操作时间，如下图：

图 5-6 查看日志详情

在操作区输入框内填写日志 ID 或内容关键字，点击<查询>按钮，通过简单查询可以筛选查找相关日志信息。

5.4.1.2. 高级搜索

在操作区通过点击<高级搜索>按钮，可以进行高级搜索查询，筛选内容包括：关键字、操作人、操作客户端 IP、操作类型、操作结果、操作时间范围。点击<查询>按钮，可以根据配置的条件进行查询。点击<重置>按钮，可以清空筛选条件和取消列表按条件展示。

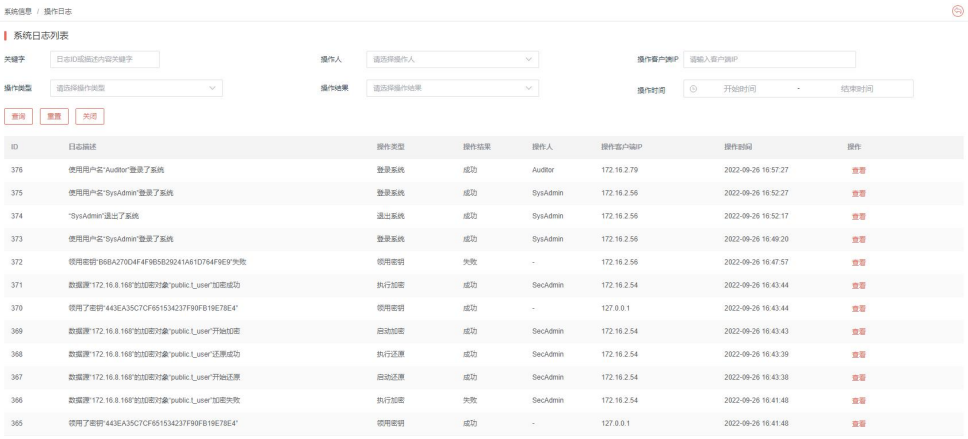

图 5-7 高级搜索

5.4.2. 系统状态

审计管理员登录后，点击 “系统信息”->“系统状态”进入该页面。页面内容与系统管理员登录后的系统状态一致，详情可查看 3.6.1 章节。

5.4.3. 帮助手册

审计管理员登录后，点击 “系统信息”->“帮助手册”进入该页面。页面内容与系统管理员登录后的系统状态一致，详情可查看 3.6.2 章节

5.5. 个人中心

审计管理员修改密码与修改资料方法与系统管理员一致，详情可查看 3.7 章节。

6. 系统用户体系

数据库加密与访问控制网关基于三权分立原则进行设计，系统管理员、安全管理员、审计管理员都会涉及对用户的操作。在系统管理、安全管理、审计管理章节中，我们都对用户管理进行了介绍。本章将从系统整体视角再次对用户管理进行说明。

6.1. 预置用户与角色

数据库加密与访问控制网关预置安全管理员、系统管理员、审计管理员、安全操作员、系统操作员、审计操作员、默认用户七个角色，并预置 SysAdmin、SecAdmin、Auditor 三个用户，分别对应系统管理员、安全管理员、审计管理员三个角色，且这三个角色下不允许再创建其他用户。

6.2. 用户创建

只有系统管理员具备用户创建权限，新建用户的角色为“默认用户”。状态为正常的用户，才可登录系统，新建用户初次登陆系统时，需要修改密码才可登录。

6.3. 用户删除

只有系统管理员具备用户删除权限。

6.4. 角色创建

只有系统管理员具备角色创建权限，新建角色时可以指定操作权限。

6.5. 授权操作

系统管理员、安全管理员、审计管理员均可对系统管理员创建的用户进行授权操作，但是一个自定义用户一次只能被一个预置管理员授权（即一个自定义用户只能与一个角色绑定）。

系统管理员对用户授权后，用户角色由默认用户变更为系统操作员，系统操作员可操作系统管理的首页、系统管理以及加密卡管理菜单。

审计管理员可直接授权默认用户为安全操作员，也可将默认用户授权为自定义角色。审计操作员只可操作审计管理的首页、操作日志菜单。

安全管理员可直接授权默认用户为安全操作员，也可将默认用户授权为自定

义角色。