# 数据库加密与访问控制网关 V5.0 用户手册

1.	前言		1
	1.1.	文档目的	1
	1.2.	读者对象	1
2.	产品机	既述	2
	2.1.	产品简介	2
	2.2.	系统登录	2
	2.3.	系统页面布局介绍	3
		2.3.1. 帮助提示	4
		2.3.2. 切换语言	5
3.	系统管	育理	6
	3.1.	概述	6
	3.2.	首页	7
		3.2.1. 业务基础数据统计	8
		3.2.2. 其他数据统计	10
		3.2.3. 系统信息	10
	3.3.	加密卡管理	11
		3.3.1. 加密卡用户角色	11
		3.3.2. 加密卡信息	11
		3.3.3. 加密卡状态	12
		3.3.4. 加密卡备份	14
	3.4.	用户与角色	16
		3.4.1. 权限管理	16
		3.4.2. 角色管理	17
		3.4.3. 用户管理	18
	3.5.	系统管理	22
		3.5.1. 许可证管理	23
		3.5.2. 接口管理	24
		3.5.3. 路由管理	25
		3.5.4. 时间管理	26
		3.5.5. 通知管理	27
		3.5.6. 系统升级	28
		3.5.7. 系统备份	28
		3.5.8. 安全设置	31
		3.5.9. 可靠性设置	32

		3.5.10. 服务设置	38
		3.5.11. 租户管理	42
	3.6.	系统信息	47
		3.6.1. 系统状态	47
		3.6.2. 帮助手册	47
	3.7.	个人中心	48
		3.7.1. 修改密码	48
		3.7.2. 修改资料	49
4.	安全管	拿理	50
	4.1.	概述	50
	4.2.	首页	51
	4.3.	资产管理	51
		4.3.1. 数据源管理	51
		4.3.2. 插件管理	58
	4.4.	密钥管理	62
		4.4.1. 主密钥管理	63
		4.4.2. 备用密钥库	64
		4.4.3. 在用密钥库	66
		4.4.4. 历史密钥库	68
		4.4.5. 密钥模板	70
	4.5.	策略管理	73
		4.5.1. 加密配置	73
		4.5.2. 读保护	97
		4.5.3. 完整性保护	105
		4.5.4. 访问控制	111
	4.6.	用户与角色	115
		4.6.1. 用户管理	115
	4.7.	系统信息	118
		4.7.1. 系统状态	118
		4.7.2. 帮助手册	118
	4.8.	个人中心	118
5.	审计管	<b></b> 寶理	119
	5.1.	概述	119
	5.2.	首页	119
	5.3.	用户与角色	120
		5.3.1. 用户管理	120

	5.4. 系统信息	
	5.4.1. 系统日志	
	5.4.2. 系统状态	
	5.4.3. 帮助手册	
	5.5. 个人中心	124
6.	系统用户体系	
	6.1. 预置用户与角色	125
	6.2. 用户创建	125
	6.3. 用户删除	125
	6.4. 角色创建	
	6.5. 授权操作	125

# 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:



※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。

の単原	系統管理 / 作可	2.管理	3					
	1 当前状态							
日加市十世世	01286	CARN						
A. MP486	5455							
© 548878	经代码规则	2024-03-17 12:06:03						
6.0259	CARAGER							
	neana	100						
除口管理	更新许可证							
務由管理	* 6402000	IncONDEDRATION		anter proteines	0			
NREE					٢			
NAME OF A	* 非可证文件	请上作许可证文件		上供件可证	15296			
6407148								
602Ø								
安全说面								
可称性设置								
RANK								
相合管理								
84448								

#### 图 2-2 系统页面

	用户与用色 / 和局管理					
	● 权限列表					
加密卡管理	0 #####					
	★ 在本页面可以定义系统的操作者 副 总是显示	2월,可以为松阳设置下属的手统器点。内置松阳在系统后始充地生成,	TTHANKER.			
	PROBADINES					ameni 5.240
用白紫斑	10 898.58	2000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	8247	Materia 2	*****	
电卢整理	101 设置加密方1	E SET_ENC_MODE	E.	2023-11-25 19:02:36	2023-11-25 19:02:36	
5422	C 100 BUILLAR	DELETE_FECAGE		2023-11-25 19:02:36	2023-13-25 19:02:36	86
FMICE	99 92RM#	USE_FECAGE		2023-11-25 19:02:36	2023-11-25 19:02:36	
	Palace 14 D	ADD_FECAGE	2	2023-11-25 19:02:36	2023-11-25 19:02:36	06
	57 切除肥户	SWITCH_TENANT	2	2023-11-25 19:02:36	2023-11-25 19:02:36	0.0
	S N ARTER	set_tenant_status	8	2023-11-25 19:02:36	2023-11-25 19:02:36	
	0 95 BR88A	DELETE_TENANT		2023-11-25 19:02:36	2023-11-25 19:02:36	
	П н <u>жин</u> е	EDIT_TENANT		2023-11-25 19:02:36	2023-11-25 19:02:36	
	0 93 (#208LP	ADD_TENANT	8	2023-11-25 19:02:36	2023-11-25 19:02:36	
	日 92 香萄根P	VIEW_TEMANT	2	2023-11-25 19:02:36	2023-11-25 19:02:36	
	91 HOWER	EDIT_WEB_SETTINGS		2023-11-25 19:02:36	2023-11-25 19:02:36	
	90 B BWEBB	NEW_WER_SETTINGS	2	2023-11-25 19:02:36	2023-11-25 19:02:36	88
				Total 101 12/page	× < 1 2 3 4 5	6 9 > Go to 1

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):

■ 权限列表 ⑦	
⑦ 帮助提示	×
在本页面可以定义系统的操作权限,可以为权限设置下面的系统路由。内置权限在系统初期化时生成,不可修成或删除。 2 总是显示	

#### 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。

户与角色 / 权限管理		
权限列表 ①		
0 帮助提示	隐藏帮助提示	
在本页面可以定义系统	() 请选择隐藏帮助提示的页面范围	
权限名称或标识关键字	所有页面不再显示 仅当前页面不再显示 取消	
ID 权限	名称 权服标识 是否内置 创建时间	更新时间
in		

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"⑦",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:



※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。

主菜单	分类	功能说明
	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、数据库类型分布
首页		最新加密对象信息
		当前加密卡信息和状态
	其他数据统计	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
加家卡管理	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
	权限管理	系统权限信息查看及新增权限
用户与角色	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
	许可证管理	导入 license、查看系统状态
系统管理	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

系统管理包含内容见下表:

	叶间竺珊	设定系统时间,包括手动和从时间服
	町町百埋	务器同步
		编辑和查看当前的 SYSLOG 通知配
	週知官理	置,可选择通知内容
	至休礼加	升级系统软件,并查看升级历史、恢
		复出厂设置
	互砍反爪	系统配置的手工或自动备份,并可进
		行异地上传
	一一一个小田	对系统登录的安全参数进行配置,以
	女主 叹且	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
	肥々辺里	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
	至纺业大	CPU、内存的近1小时占用率统计;
至伏伫自		数据空间、总储存空间使用情况
尔坎泊芯	邦田王冊	查看系统使用中相关的配置指导手
	市功丁加 	册
	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				
	当前备用、在用、历史密钥数量;当前数据源总量、数				
业权其如粉提公计	据源状态异常数量、数据源类型分布				
业分举础级据统计	当前加密表数、未加密表数统计				
	最新加密对象信息				
甘油粉坭纺斗	当前加密卡信息和状态				
丹他奴妬坑り	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/				





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。

最新加密对象						
所属数据源	库/模式	ā	字段	加密算法	状态	应用时间
172.16.23.200:3306	test	user	id	AES128	未加密	2023-09-14 15:32:30
172.16.23.200:3306	test	user	name	AES128	来加密	2023-09-14 15:32:30
172.16.23.200:3306	test	user	phone	AES128	已加密	2023-09-14 15:32:30
172.16.8.54:1521	SH	TIMES	END_OF_FIS_QUARTER,CALENDAR…	AES256	未加密	2023-09-14 15:26:30
172.16.23.200:3306	xqss	DBES_TMP_TAB_17EBDFA7A9895C78	Column1gga-	AES128	未加密	2023-09-14 15:13:26

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。

th an de	
Cpu使用率	
下行速率	
1 KB/s	
系统时间	
	cpu使用率 下行速率 1 KB/s 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。

加密卡管理 / 加8	· #+68	6
┃ 加密卡信息		
<ul> <li>帮助提示 在本页面可以 或工作模式。</li> <li>总是显示</li> </ul>	以四数、周点加速十分就点和工作规式、加速十就点为"已点用"时,系统可进行加速使操作。另外,工作规式为"规模式"时,可进行创建主电调操作;工作规式为"管理规工时,可进行加速十数级合动建筑算统件。切脱加速十的成点 可能点型网络规定在进行的点点,调谐频频件。 1示	×
加密卡状态	<ul> <li>         ・ 已合用(写真確)         ・ (写真確)         ・         ・         ・</li></ul>	
型号	PEM611	
唯一标识	2021121500104018	
操作	设罪状态	

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;
- 己启用(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。

加密卡信息          ·辺面の卡状态         ·ン         ·ジョン・         ·シュー         ·ジョン・         ·シュー         ·シュー         ·シュー         ·シュー         ·ジョン・         ·ジョン・         ·シュー         ·ジョン・         ·ジェン・         ·ジェン・	※卡管理 / 加密卡信息		
卸御子検索      已前用 ( 型弓 PEM511     日标状态 ・已約用 (常規模式)     日标状态    停用	加密卡信息	设置加密卡状态	×
	加密中状态 日点用 ( 型写 PEM611 唯一标识 2021121	当前状态 ・已点用(常規模式) 目标状态 停用 ● 島用	
	操作 设置(	LINGA BIOMAN	T-9

图 3-11 设置加密卡状态

加密卡管理 / 加速	要卡信息			
┃ 加密卡信息		设置加密卡料	犬态	×
加密卡状态	已启用(			
型号	PEM611	● 请在加密-	卡上插入第1位管理员的UKey,并在下方输入UKey密码	
唯一接訳	2021121	UKey密码	请输入当前UKey的密码	
操作	设置和	登录密码	请输入当前账号的登录密码	
				下一步 取消

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。

1 加密卡上一次	工作模式切换操作未完成,点击 继续或 放弃 (144 秒后自动放弃。)
加密卡状态	• 已禁用
型号	SJK1828 V2.0
唯一标识	2311000004003850
操作	设置状态

#### 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。

加速卡管理 / 加密卡备份										
□ 历史备份文件 ■										
<ul> <li>● 宿助提示 在支援周司以高倍加密卡数据,并预算历史备倍文件,进行备倍操作端,加密卡状态必须为"已向用",且工作模式为"管理模式。</li> <li>■ 总是显示</li> </ul>										
文件:	名关键字 查询 里	X						番份		
ID	文件名	文件大小	来源	备注	创建时间	操作				
3	backup_1681981215779.json	8 KB	备份	1245	2023-04-20 17:00:15	编辑 下载	MIRS.			
2	backup_1681981209466.json	8 KB	备份		2023-04-20 17:00:09	编辑 下载	MIR:			
1	backup_1681891110791.json	8 KB	备份	哈哈哈	2023-04-19 15:58:30	编辑 下载	MIRS.			
					Total 3 12/pe	le ~ <	1 > G	o to 1		

#### 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。

备份加密卡	数据	;
加密卡状态	- 已启用(管理模式)	
型号	vhsm-v0	
唯一标识	8bcc4d56bb74061433b651a20390483e	
备注		
		提交取消

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。

加密卡(	管理 / 加密卡备份										
■历史	电备份文件 💷										
		编辑文件	备注				×				
<b>0</b> #	書助提示 E本页面可以备份加密卡	ID		4							
8	▲ 总是显示										
-		文件名		backup_1661409024881.json							
X114	6大键子	备注									
ID	文件名			123123123	11				操作		
14	backup_1661409024						提交取消	6	编辑	下载	-
4	backup_1661409024	01.000	- 110			160160160	1011 US 10, 17, 00 1	4	编辑	下载	-
3	backup_16614085352	09.json	4 KB	备份		123123	2022-08-25 14:22:1	6	编辑	下载	

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。

加密卡管理	·····································								
┃ 历史备	份文件 📾								
<ul> <li>⑦ 帮助</li> <li>在本</li> <li>✓</li> <li>✓</li> <li>(2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4</li></ul>	<ul> <li>● 帮助提示 在本項面可以备份加密卡数据,并管理历史备份文件。进行备份操作前,加密卡状态必须为"已此用",且工作模式为"管理模式"。</li> <li>● 总是显示</li> </ul>								
ID	文件名	文件大小	来源	备注	创建时间	操作			
1	backup_1699499740380.json	4 KB	备份		2023-11-09 11:15:40	编辑下载量	影除		
					Total 1 12/page ∨	$\langle 1 \rangle$ G	o to 1		

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。

加密卡	管理 / 加密卡备份					
历9	史备份文件		提示	×		
ID	文件名	文件大小			创趣时间	操作
11	backup_1661494710373.json	4 KB	() 确定要删除备份文件 backup_1661494	1710373.json 吗?	2022-08-26 14:18:30	编辑 下载
10	backup_1661410544020.json	4 KB		确定取消	2022-08-25 14:55:44	编辑 下载
9	backup_1661410535729.json	4 KB	<b>ធ</b> ល	14:UD	2022-08-25 14:55:35	编辑 下载
8	backup_1661310250110.json	4 KB	上代	14:05	2022-08-25 14:55:19	编辑 下载
7	backup_1661410503540.json	4 KB	备份	14:55	2022-08-25 14:55:03	编辑 下载

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:

用户与角色 / 权服管理											
权限列	权限列表										
<ul> <li>⑦ 帮助</li> <li>本页面</li> <li>図 長</li> </ul>	<ul> <li>● 精助提示 本页面可以定义系统进行权限,可以为权限设置下属的系统流血,系统内置权用不可修改或删除。</li> <li>■ 总是显示</li> </ul>										
D ID	权限名称	权限标识	是否内置	创建时间	更新时间	操作					
77	下载Agent安装包	DOWNLOAD_AGENT_PKG	是	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
76	查看加密卡备份	VIEW_HSM_BAK	足	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
75	查看加密卡	VIEW_HSM	是	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
74	查看系统日志	VIEW_LOG	足	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
73	恢复出厂设置	RESET_SYS	是	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
. 72	管理系统升级	UPGRADE_SYS	是	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
71	查看系统存储空间	VIEW_STORAGE_SPACE	足	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
70	恢复系统数据	RESTORE_SYS_DATA	是	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
69	删除系统备份文件	DELETE_SYS_BAK	足	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					
68	上传系统备份文件	UPLOAD_SYS_BAK	是	2022-08-24 21:05:33	2022-08-24 21:05:33	查看					

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:

电户与	角色 /	角色管理				\$
角1	色列表					
0	幣助提 本页面可 2 总力	<b>示</b> 口以前建或编辑系统角色,可以为角色设置 是显示	可操作的积限。系统内置角色不可修	sex:callfor.		×
角色	名称关制	<b>查询</b>				添加角色 批量删除
	ID	角色名称	是否内置	包藏时间	更新时间	操作
	9	test_角色_数据源操作员	否	2022-08-29 10:29:35	2022-08-29 10:29:36	查看 编辑 删除
	8	test_角色-拥有所有的查看权限	否	2022-08-29 10:27:37	2022-08-29 10:28:55	查看 编辑 網除
	7	默认用户	是	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑
	6	审计操作员	是	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑
	5	系统操作员	是	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑
	4	安全操作员	足	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑
	3	审计管理员	是	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑
	2	系統管理员	是	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑
	1	安全管理员	足	2022-08-26 17:55:45	2022-08-26 17:55:45	查看 编辑

#### 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

添加角色					
● 帮助提示 ※加权限时 ● 总是当	,需选择该角色器有的权限或路由,支持; 1示	5 th.			
色名称	這输入角色名称				
也择权限	未选	0/35	日已选	0/1	
	<ul> <li>支持模糊搜索</li> </ul>		〇 支持模糊搜索		
	□ 查看例外规则	•	🔲 基本权限		
	》 本加例外规则				
	()修改例外规则				
	_ 启停例外规则				
	● 翻除例外规则				
	下载插件安装包				
	222				

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內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:

用户与加	角色 /	用户管理											6
用用	口列表												
01	帮助提; 在本页面	示 可以添加和管理所 [显示	月用户,新添加的用户角色为"默认用户"	,可以授权为养	系統操作员,ゼ	可以取消授权。内	置用户在系统初始化时生成,	不可修改或删除。					×
用档	名关键字		查询 重置						绑定	UKEY	<b></b>	加用户	批量删除
	ID	用户名	所属角色	是否内置	状态	UKEY	最近登录时间	创建时间	操作				
	5	test002	默认用户	否	<ul> <li>         第用     </li> </ul>	• 未绑定		2022-11-24 16:56:04	启用	授权	查看	编辑	删除
	4	test001	默认用户*	香	• 正常	<ul> <li>未绑定</li> </ul>		2022-11-24 16:55:19	禁用	授权	查看	编辑	删除
	3	Auditor	审计管理员	是	<ul> <li>正常</li> </ul>	<ul> <li>未绑定</li> </ul>	2022-11-21 18:18:08	2022-11-17 21:22:00	查看				
	2	SysAdmin	系统管理员	是	• 正常	<ul> <li>未绑定</li> </ul>	2022-11-24 16:54:33	2022-11-17 21:22:00	查看				
	1	SecAdmin	安全管理员	Đ	<ul> <li>正常</li> </ul>	<ul> <li>未绑定</li> </ul>	2022-11-24 16:13:14	2022-11-17 21:22:00	查看				

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
		填写用户名,长度 6-30 个字符,应具备唯一性,
用户名	是	区分大小写,且只能由以下字符组成:英文字
		母、数字、下划线;
		填写密码,长度要求 10-20 个字符;至少包含
家印	日.	大写字母、小写字母、数字、特殊字符
	定	(`~!@#\$%^&*()=+\ [{}];:''',<.>/? 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
		填写手机号,长度 11 个字符。且应 13、14、
手机号	否	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

8关键 5		添加用户				×	
ID	用户名						操作
32	testsearch	* 用户名	请输入用户名				熱用
31	testuser17	* 密码	请输入密码				熱用
30	testuser16	*确认密码	请再次输入密码				献用
29	testuser15	直定姓名	法输入真实姓名				禁用
28	testuser14	PARALI	ALL				裁开
27	testuser13	手机号码	请输入手机号码				熱用
26	testuser12	电子邮箱	请输入电子邮箱				慧用
25	testuser11	状态	◎ 启用 ○ 禁用				計
24	testuser10						200 E
23	testuser9					提交 取消	<b>默</b> 月
22	testuser8		AA MAJISIP"	-13	- 46.m	2022/00/23 18:90:20	耕
21	testuser7		默认用户	否	• 正常	2022-08-29 14:48:16	22

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。

户与	18 /	用户管理						
用戶	<sup>1</sup> 列表	8	切换用户	角色			×	
0 #	帮助提》 "页面可	天 以準加或編組系 1日二	用户ID	32				
		E are die	用户名	testsearch				
用户	8关键的	4	当前角色	默认用户				
P	ID	用户名	切换角色	默认用户	~		58/1°	
<b>a</b> );	32	testsearch					887	8 授权
	31	testuser17	重置密码	2			20	8 授权
	30	testuser16	* 被码	请输入密码			56.7	8 投权
	29	testuser15	* 38-11 (8750),	请而发输入源码			an )	8 授权
Q.	28	testuser14	HE PLACES	H1270382 (34123			88.9	8 授权
	27	testuser13					提交 取消 節	8 授权
D)	26	testuser12				-14	tta	目授权
	25	testuser11		默认用户	西	•正常	2022-08-29 14:49:12	日授权

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:

	查看用户		×
	用户ID	4	
	用户名	test001	
	所属角色	默认用户	
与用户	真实姓名	12	
	手机号码	12	
	电子邮箱	12	
	状态	•正常	
	UKEY	<ul> <li>未绑定</li> </ul>	14.1
	是否内置	否	14 1
	登录次数	0	7.2
	最近登录IP		72
	最近登录时间		7 2
	创建时间	2022-11-24 16:55:19	
	更新时间	2022-11-24 16:55:20	23
			关闭

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
		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
密码	否	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。

2 总员					
名关键与	7	编辑用户		×	
ID	用户名	田内口	20		9
20	testuser6	767 10	20		
19	testuser5	用户名	testuser6		
18	testuser4	密码	留空表示不修改密码		8
17	testuser3	确认密码	留空表示不修改密码		2 (d)
16	testuser2				
15	testuser1	所属角色	默认用户		
14		真实姓名	请输入真实姓名		
12	1	手机号码	请输入手机号码		<b>1</b> 3
10	www001				
9	test001	电子邮相	· 咱搁入电于即和		e l
8	testuser	状态	• 正常		G
3	Auditor				
				提交    取消	ge 🗸

#### 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 1111111)。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:

系统管理 / 许可证	7	
当前状态		
许可证状态	已沒教	
系统版本	中交星云数据库加密中动间控制网关 15.0	
授权有效期	2024 03-17 12:06:03	
已授权模块	教育政策部、法则控制、每户管理	
数据源数量	10	
更新许可证		
* 系统识别码	tectingRolloCsub7cY	
*许可证文件	ա上传许可证文件 上代许可证	

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。

MGT HA			E2/1	E2/2	E2/3 E2/4	E3/1	E3/2	E3/3	E3/4	E3/5	E3/6	E3/7	E3/8
口状态													
网卡重排													
5#	IPv4	IPv6		MA	AC	Mask			18.	a			12:11
IGT	172.16.8.114			00	22:46:47:a6:a6	255.25	5.0.0		Æ	æ			
A	192,168,100,100			00	22.46.47.a6.a7	255.25	5.255.0		BF	Я			10110

#### 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。

	×
MGT	
172.16.8.114	
255.255.0.0	
	提交 取消
	MGT 172.16.8.114 255.255.0.0

#### 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

169.254.0.0	255,255.0.0	0.0.0.0		1003	Gane	
169.254.0.0	法加魏太败由				erp4	
169 254 0 0	AND HE READ DO				enp5	
169.254.0.0	* 选择接口 1	634			enp0	
169.254.0.0	* El 091P				erp1	
172.16.0.0					enp0	
175.0.0.0	* 子同掩码				erp1	
192.168.2.129	* 同关				enp0	
192.168.2.229	伏先级				enpű	
192.158.100.0					enp1	
▮ 系统路由表 (IPv6)			确定	RE 18		制新
BOPMA	子用新编长度	7—Ц		成先編	1813	
			No Cata			
静态路由表						1830
BINPAN	子网络药	用关于一篇	C.R.B.	MI	80	
			No Data			

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
	手工设置系统时间
町间能直 	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。

1管理 / 时间1	3 <b>2</b>					
系统时间配	t i					
当前时间	2022-08-29 17	05:43				
设置方式	○ 手动设置		从时	间服务器	间步	
设置时间	· 2022-08-	29 00 00	00			
	2022-08-29			00.00.00		
	« «	2022	2 .			
	Sun Mon	Tue	w			
	31 1	2	1	00	00	00
	7 8	9	1	02	02	02
	14 15	16	1		Carrel	OK
	21 22	23	24	13	20 21	Sh
	28 23	30	31	1	2 3	
	4 5	6	7	8	9 10	

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。

WILLIE POINTED	a	\$
▲ 系统时间配置	t	
当新时间	2022-08-29 17:09:34	
设置方式	○ 手动设置 ● 从时间服务器同步	
* 时间服务器	11回顧告題: ジョン	
* 服务器地址	服务器地址	
"細口号	123	
	RI RR	

#### 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	默认关闭状态,可开启
	<u> </u>	
编码格式	UTF-8 或 GBK 二	默认 UTF-8,可选择
	选一	
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。

系統管理 / SYSLOG	5株管理 / 579LOS通知管理							
SYSLOG通知	印尼亚							
状态	○ 关闭 ○ 开启							
编码格式	UTF-0 V							
* 目的服务器IP	127.0.0.1							
* 端口	514							
* 通知内容	□ 系統运行日志 □ 系统操作日志							
	M00 000							

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。

[管理 / 系统升级			
系统升级			
' 升级文件	道上传升量文件		яa
升级版本	版申福述	升级时间	升级结果
		No Data	

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。

系统管理 / 系统备份 存储空间								(9)
(0.01%							已占用(6.6M/52G)	
备份记录							自动备份 未开启 配置	备份
请输入文件名称	全部来源	~ 备份状	\$	~ 上传状态	> 搜索	ł		
备份时间	文件名	系统版本	文件大小	备份方式	备份状态	上传状态	操作	
2024-07-31 10:39:12	backup_1722393	Database Encrypt…	6677 KB	人工备份	备份成功	未上传	下载  删除	
					共1条	12条/页 🛛 🗸	〈 1 → 前往	1 页

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:

系统管理 / 自动备份			6
自动备份配置			
启用状态	• 已禁用		
备份频率	每小时0分自动备份一次		
是否自动上传	否		
*本地清理	保留最近1次备份文件		
	编辑 返回		

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

配置项	是否必填	说明
启用状态	启用或禁用	默认为禁用,启用后,自动备份配置即时
	二选一	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	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

表:

上传方式	FTP 或 SFTP 二	若选择自动上传需填写,默认为 FTP,FTP
	选一	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	若选择自动上传需填写,默认为 UTF-8,可
	二选一	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。

系统管理 / 自动备份		C
自动备份配置		
启用状态 ⑦	○ 启用   ◎ 禁用	
备份频率	每小时 🗸 0 🗸 分自动备份一次	
是否自动上传	◎ 是 ○ 否	
上传方式	● FTP ○ SFTP 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 GBK	
*目标服务器IP	仅支持编写IPv4格式	
* 目标服务器端口	0	
* 登录账户		
* 登录密码	留空表示不修改密码 <b>空密码</b>	
上传目录 ⑦		
失败重传次数	0	
*本地清理	保留最近 1 次备份文件	
	检测 保存 取消	
	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。

31

系统管理 / 安全设置			
安全设置			
* 亞灵安全參数	60	秒之内,用户管试管梁的失败次数超过 4 · · · 次,镇定适用户 2 分钟	
* 登录会话超时	30	分钟不得作。自动跟出(可选规图10~60)	
*密码长度参数	10	- 20 (可應思問 10 - 30)	
密码过期参数	◎ 关闭 ○ 开启		
* 密码过期时间		天(可造思闻1-7天)	
双因子身份验证	◎ 关闭 ု 开启		
文件下载密码给证	○ 关闭 ◎ 开启		
* 文件下载密码	留空表示不继改密码	长度 6-30 位,至少包含学母、数字、轻振学符中的两种	
* 确认密码	留空表示不修改密码		
	保存 取測		

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:
系统管理 / 可靠性设置 / 可靠性设置 HA管理 ① HA设置 HA运行日志 ● 帮助提示 开启HA高可靠模式,主机和备机硬件和软件版本需满足如下要求: ① 加密主机硬件型号相同(虚拟化版本无需关注此项) ② 同型号硬件需要为相同的硬件版本,内存容量,CPU 型号,硬盘容量; ③相同的软件版本; ④相同的LICESEN授权模块、系统语言; ⑤ 加密卡型号相同均已初始化,且KEK已同步(需厂家支持); ⑥双机建立连接成功时,备机设备上信息会被初始化,建立双机前需保证备机无绑定插件,数据源下无加密对象; ☑ 总是显示 双机信息 刷新 设备信息 设备SN码 运行模式 HA接口IP HA启用时间 本机信息 tq50h0k0k0l32n3l9 单机模式 对端信息

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:

双机信息					刷新
设备信息	设备SN码	运行模式	HA接口IP	HA启用时间	
本机信息	tq50h0k0k0l32n3l9	主备模式(备机)	172.16.23.196	2024-06-04 18:26:53	
对端信息	tq50h0k0k0l32n3l9	主备模式(主机)	172.16.23.198	2024-06-04 18:26:53	
HA设置					刷新
当前工作模式	主备				
当前运行状态	•正常(双机)				
当前运行角色	备机				
本机HA接口	ens33 <mark>详情</mark>				
本机HA-IP	172.16.23.196				
对端HA-IP	172.16.23.198 检测				
浮动IP	ens33   172.16.23.199 <u>详情 编辑</u>				
主备配置一致性	• 正常 <u>详情</u>				

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:

33

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	在主机和备机中二选一,默认为主机
	机二选一	
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。

	HA设置			×		1
统管理 / 可靠性设置	工作模式	主备模式				
HA管理	• 本机运行角色	<ul> <li>○ 主机</li> <li>○ 备机</li> </ul>				
0 帮助提示	本机信息					
开启HA高可靠模式,主机和备机 ① 加密主机硬件型号相同(虚拟化 ② 同型号硬件重要为相同的硬件器	•本机HA搜口⑦	请选择接口				
<ol> <li>4時的軟件版本;</li> <li>4時的LICESEN授权模块;</li> <li>10時時本計算了2011年前約5月</li> </ol>	*HA-IP地址	请选择HA-IP地址	<u>去设置</u>			
◎ 从和建立建設面が向う,由440日 ■ 总是显示	* 子网掩码					
<b>R68</b>	对端信息					
设备信息	• 对端HA-IP		<b>松湖</b>			наелина
本机信息	浮动IP信息					
对端信息	* 浮动P接口②	请选择按口				
НА设置	* 浮动叩⑦					
当前运行模式 单机模式 切换为	* 子网换码					
			Witz I	跳	小时17分26秒	

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"。 系统管理 / 可靠性设置 / 可靠性设置

HA管理

创建主备模式 1/8 (当前选择角色:主机) 主备模式建立中,这可能会需要些时间,请耐心等待。

	检查连通性
2	检测对端设备中,倒计时:596 s 检测配置条件
	待执行
(3)	停止双机定时任务
4	<sup>待执行</sup> 准备配置文件
	待执行
(5)	启动MySQL数据同步
6	<sup>待执行</sup> 启动rsync文件同步
	待执行
0	启动keepalive
8	<sup>待执行</sup> 启动定时任务
	待执行

#### 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。

系统	"管理 / 可靠性设置 / 可靠性设置	(3)
Н	HA管理	
<b>创</b> 建	建主备模式 1/8 (当前选择角色:主机) 注备模式失败,请检查是否符合双机建立条件。您可以选择还颇为单机模式修改。	
	检查连通性	
	失败:本机和对端都是主机角色 还愿为单机模式 ) 检测配置条件	
Ĭ	待执行	
3	)停止双机定时任务	
	特执行	
(4)	)准备配置文件	
1	转换行	
(5)	) 启动MySQL数据同步	
4	特执行	
Ŷ	后动rsync文件问步	
0	特殊行	
Y		
6	6380	
0	/ F=YU/L=>1上,77 法指行	
	נואנטו	

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。

HA设置		刷新
当前工作模式	主备 <u>切换为单机模式</u>	
当前运行状态	•正常 (双机)	
当前运行角色	主机 <u>手工切换</u>	
本机HA接口	ens33 <u>详情</u>	
本机HA-IP	172.16.23.198	
对端HA-IP	172.16.23.196	
浮动IP	ens33   172.16.23.199 详情 编辑	
主备配置一致性	• 正常 <u>详情</u>	

#### 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。

系统管理 / 可靠性	设置		
双机信息	编辑浮动IP		×
设备信息	* 浮动P接口⑦	enp0 🗸	HARAH
本机信息			
对端信息	* 浮动IP ⑦	10.10.10.10	
HA设置	* 子网掩码	255.255.0.0	
当前运行模式	-		· 确定 · 取消
当前运行状态	* WRIE		

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

1

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。

主备配置一致性检测详情					
状态:● 异常			检测		
ID	检测项	检测结果			
1	系统版本	• 通过			
2	授权状态	<ul> <li>通过</li> </ul>			
3	安装参数	• 通过			
4	系统运行环境	<ul> <li>●通过</li> </ul>			
5	业务数据	加密卡状态不一致;			
6	加密卡状态	•不通过 ⑦			
			关闭		

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:

可靠性设置	Ē					
HA设置	HA运行日志					
青输入日志II	D或日志描述关键字	向重置高	级搜索			
D	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
79570…	已还原为单机模式	还原为单机模式	•成功	SysAdmin	172.16.2.62	2024-05-29 14:20:17
79570	HA双机模式初始化失败	初始化HA	●失敗	SysAdmin	172.16.2.62	2024-05-29 14:15:05
79569…	已切换为双机模式	切换为双机模式	• 成功	SysAdmin	172.16.2.62	2024-05-29 14:05:02
				共3条	12条/页 🗸 🔇	1 > 前往 1

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	关闭即不设置 web 访问策略,所有地址均可
	二选一	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)

系統管理 / 服务	2 WEB総合は営業	6
服务设置		
WEB服务配	图 SNAP服务配置	
<ul> <li>帮助提示</li> <li>WEB设置中</li> <li>总是量</li> </ul>	, яцинажиющалегаж, римоялагосе, высопфгизициясы, хиегосе, вистигевие. Б <mark>л</mark>	×
- 端口	443 #14-8200 F994021: 1-1024 (4438699) , 2222, 3306, 6379, 8000, 8000, 50024, 50025, 50012	
IP白名单	<ul> <li>又將 ○ 开始</li> <li>द27</li> </ul>	

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。

系統管理 / 服务设置	I / SNMP服务配置				
服务设置					
WEB服务配置	SNMP服务配置				
<ul> <li>帮助提示</li> <li>SNMP服务配置</li> <li>总是显示</li> </ul>	中,可设置SNMP状态、版本、认证加密等信息。在	服务开启状态下,可查看常用节点OID给息。			×
状态	已开启				
SNMP版本	V3				
用户名	root				
认证加密方式	不认证不加密				
设备名称	5				
物理位置					
联系方式					
	10010				
常用节点信息					
OID		名称	描述	操作	
.1.3.6.1.4.1.2021	1.4	memonry	系统内存信息	查看	
.1.3.6.1.2.1.25.2	3	hrStorage	系统磁盘信息	查看	
.1.3.6.1.4.1.2021	1,10.1.3	laLoad	系统CPU负载	查看	

图 3-50 SNMP 配置

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

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	不认证不加	仅选择 V3 版本时需要选择认证加密方式		
式	密或认证加			
	密或仅认			
	证,三选一			
认证方式	SHA 或 MD5	当选择认证时需选择,SHA 和 MD5 为认证方式		
	二选一	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	当选择加密时需选择, DES 和 AES 为认证方式的		
	二选一	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		

状态	○ 关闭   ◎ 开启
SNMP版本	O V1&V2 ○ V3
*团体名	public
设备名称	请输入设备名称
物理位置	请输入物理位置
联系方式	请输入联系方式
	保存取消

图 3-51SNMP-V1&V2

状态	○ 关闭   ◎ 开启	
SNMP版本	○ V1&V2 <b>○</b> V3	
* 用户名	root	
认证加密方式	不认证不加密	×
设备名称	请输入设备名称	
物理位置	请输入物理位置	
联系方式	请输入联系方式	
	保存取消	

图 3-52SNMP-V3 不认证不加密

状态	○ 关闭   ● 开启
SNMP版本	○ V1&V2 <b>④</b> V3
* 用户名	root
认证加密方式	认证及加密
认证方式	SHA O MD5
认证密码	留空表示不修改密码
加密方式	O DES O AES
加密密码	留空表示不修改密码 长度 8 ~ 30 位,至少包含字母、数字、特殊字符中的两种
设备名称	请输入设备名称
物理位置	请输入物理位置
联系方式	请输入联系方式
	保存取消

图 3-53SNMP-V3 认证及加密

状态	○ 关闭   ◎ 开启
SNMP版本	○ V1&V2 ○ V3
* 用户名	root
认证加密方式	仅认证
认证方式	SHA O MD5
认证密码	留空表示不修改密码 长度 8 ~ 30 位,至少包含字母、数字、特殊字符中的两种
设备名称	请输入设备名称
物理位置	请输入物理位置
联系方式	请输入联系方式
	保存取消

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:

系統管理 / 相	11户管理								0
┃ 租户管理	and the								
<ul> <li>⑦ 帮助提 利用租户</li> <li>☑ 总别</li> </ul>	示 中可以实现系统数据 是显示	B权限的隔离,同一袒产下的用户拥有相同的数据权限,可以	查看租户内部所有的业务数据,十	旦不能查看其他租户的业务数据。系统最	多可源加20个租户。				×
请输入关键	2	查询 重置						添加相户	批量删除
D ID	租户名称	安全管理员	系统管理员	审计管理员	状态	创建时间	操作		
5	sdasdas	test4user2	test4user3	test5user1	• 正常	2023-04-14 17:35:17	禁用 编辑	删除	
3	租户3	test3user2	test3user3	test4user1	• 禁用	2023-04-14 16:27:13	启用 编辑	删除	
2	租户2	test2user2	test2user3	test3user1	• 正常	2023-04-14 16:27:12	禁用 编辑	删除	
0.1	粗户1	test1user1	test1user2	test2user1	• 正常	2023-04-14 16:27:11	禁用 编辑	删除	
						Total 4 12/page	~ <	1 > Go	o to 1

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
亥法签理吕	曰.	只可选择角色为"默认用户"且状态为启用
<i>新</i> 筑目埋贝	定	的用户
富计管理目	是	只可选择角色为"默认用户"且状态为启用
甲耳官理贝		的用户
业大	启用或禁用	<b>黔江为白田壮太</b> 司林田
八心	二选一	纵以乃后用状态,可示用 
反计	不	填写该租户的备注信息,长度不超过100个
	<b>首</b>	字符

租户名称	请输入租户名称		
安全管理员	请选择安全管理员	Ŷ	
系统管理员	请选择系统管理员	$\checkmark$	
审计管理员	请选择审计管理员	~	
状态	◎ 启用 ○ 禁用		
备注说明			

图 3-56 添加柤户

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	揖。
编辑租户		×
租户ID	5	
* 租户名	sdasdas	
状态	• 正常	
备注说明		
创建时间	2023-04-14 17:35:17	
更新时间	2023-04-14 17:35:18	
		提交取消
	图 3-57 编辑和户	

# 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。

2	test4user3	test5user1	●正常
2	test3user3	test4user1	●禁用
2	提示	×	• 正常
1	. 确定要禁用该租户吗?		●正常
		确认取消	

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,

:4user2	test4user3	test5user1	• 正常
3user2	test3user3	test4user1	●禁用
2user2	提示	×	• 正常
:1user1	④ 确定要启用该租户吗?		• 正常
		确认取消	

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:

	La print of the data we did has also be	0
加密插件的下载与安装	加密插件的下载与安装	
启用和配置 Oracle 数据库 TDE 功 能的方法	一、安装包下载	
MySQL v8.0.4及以上版本配置加密 目录的方法	For Linux(x86_64): fecage-v2 release.c86127.el7.tar.gz	
各数据库的加密方案及算法支持规 格	二、安装部署方法	
MySQL 数据库安装 SM4 算法插件 的方法	1. 上传安装包至数据库服务器任意目录下;	
SQL Server 数据库安装 SM4 算法 插件的方法	2. 使用以下命令解压缩安装包: tar xf fecage-v*.tar.gz	
	3. 进入解压缩后的目录,执行以下命令开始安装: sh fecage_install.sh	
	<ol> <li>4. 安装过程中会要求输入加密数据存放的目录,此时有两种选择:</li> <li>1)使用安装脚本推荐的设置,直接回车即可(推荐设置使用的是当前磁盘剩余空间最大的分区);</li> <li>2)自定义加密数据存放目录,需输入自定义目录的绝对路径;</li> </ol>	
	<ol> <li>安装过程中还会要求输入插件提供服务使用的端口号,此时:</li> <li>1)使用默认端口 50023,直接回车即可;</li> <li>2)使用自定义的端口号,可输入 1024~65535 范围内的端口号(需避免使用已被其他服务占用的端口号);</li> </ol>	
	6. 安装过程中会要求输入两次用于离线解密的密码,请妥善保管此密码;	
	注意:加密目录不能和数据库数据目录在同一文件夹	
	三、插件服务管理命令	
	1. 启动插件服务命令: systemctl start fecage	

# 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。

	修改登录密码					×	
编辑系统用户,	用户名	SysAdmin					
<u></u>	所属角色	系统管理员				- 1	
	* 旧密码					- 1	
r6	*新密码					4:4	8:04
r4	* 确认密码					4:4	7:37
173					提交	4:4	7:24
12	8411 m ch		<u>.</u>	- 744		4:4	7:14
	默认用户	2	а Б	• 正常		2022-08-29 14:4	1:54

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。

	修改个人资料					×		
、神國或編輯和如用广。 显示	用户名	SysAdmin						
1	所属角色	系统管理员						
用户名	真实姓名							操作
testuser6	手机号码						4:48:04	禁用
testuser5	5 00 505						4:47:47	禁用
testuser4	邮箱地址						4:47:37	禁用
testuser3						- The Tab	4:47:24	禁用
testuser2					提交		4:47:14	禁用
testuser1	默认用户	1	否	<ul> <li>正常</li> </ul>		2022-08-29	14:42:27	禁用
	默认用户		否	<ul> <li>正常</li> </ul>		2022-08-29	14:41:54	禁用

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。

主菜单	分类	功能说明
		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
	业务基础数据统计	当前加密表数、未加密表数统计
首页		最新加密对象信息
		当前加密卡信息和状态
	其他数据统计	当前插件总量、插件状态异常数量
	至姑次酒姑斗	CPU、内存的准实时占用率统计;系
	<i>杀</i> 须页砺须日	统接口准实时接收/发送流量统计
		添加、查看、编辑数据源,对数据源
资产管理		进行架构扫描
贝)自在	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
	   主密钥管理	创建主密钥(首次登陆时)、查看主
		密钥信息
宓鈤管理	备用密钥库	添加、查看、删除密钥
山内日生	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
		选择、配置、取消加密方案
策略管理	加密配置	添加、编辑、删除加密对象
		加密、解密、还原加密对象

安全管理包含内容见下表:

	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
至法信自	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
<i>杀</i> 须信芯	帮助手册	查看系统使用中相关的配置指导手 册
<b>人</b> 上中心	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:

资产管	理 / 数据源管理								\$
数	据源列表								
0	帮助提示 比页面为数据源的管理页面, ☑ 总是显示	,可添加或编辑数据源。在	本页面可实时检测数据源和插件的连接	状态。 添加新的数据源	后,系统会自动进行架构扫描,更	大取该数据源的账号和表结构信息,证	输保数据源的	P、端口、用户名、	× 密码等信息无误。
名称	或地址关键字	服务类型	~ 连接状态	~ 查询					漆加数据源
ID	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	操作		
68	mysql8.40	MySQL	172.16.8.40:3306	单库	• 正常 😋	2022-08-31 10:37:28	查看	编辑删除	
58	[wy] mysql-8.154	MySQL	172.16.8.154:3306	单库	• 正常 〇	2022-08-31 11:23:32	查看	编辑剧除	
52	[wy] oracle-8.158	Oracle	172.16.8.158:1521	单库	• 正常 〇	2022-08-31 10:12:15	查看	编辑 删除	
45	oracle-8.160	Oracle	172.16.8.160:1521	单库	• 正常 〇	2022-08-31 10:13:13	查看	编辑 删除	
44	oracle-8.159	Oracle	172.16.8.159:1521	单库	• 正常 〇	2022-08-31 10:30:30	查看	编辑 删除	
43	mysql-8.157	MySQL	172.16.8.157:3306	单库	• 正常 〇	2022-08-30 13:54:01	查看	编辑 删除	
42	mysql-8.156	MySQL	172.16.8.156:3306	单库	• 正常 〇	2022-08-30 09:28:04	查看	编辑 删除	
41	test集群	Oracle	172.16.8.8:1521	集群	●异常○	2022-08-29 20:05:59	查看	编辑 删除	
40	oracle111	Oracle	172.16.8.255:1521	单库	●异常℃	2022-08-29 18:31:19	查看	编辑 删除	
39	111	MySQL	pm2.csdev.com:3306	单库	• 异常 😋	2022-08-30 10:21:35	查看	编辑 删除	

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	特定数据库	PostgreSQL 数据库集群部署时需在流复制与逻
方式	时必填	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	连接 Oracle 数据库时使用的服务名
	时必填	
数据库名	特定数据库	连接 PostgreSQL、GaussDB、AtlasDB、SQL Server
	时必填	等数据库时使用的数据库名

52

用户名	是	连接数据库时使用的账号
账号角色	Oracle 数据	连接 Oracle 数据库时使用的账号角色,可选项
	库时必填	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

添加数据源			×
* 名称			
* 服务类型	MySQL $\lor$		
* IÞ			
* 端口			
使用SSL	不启用SSL V		
* 部署方式	● 单库 ○ 集群		
* 用户名			
* 密码		空密码	
		检测 提交 耳	2消

图 4-2 添加数据源-单库

添加数据源		×
* 名称		
*服务类型	MySQL 🗸	
* IP		
* 端口		
使用SSL	不启用SSL 🗸	
* 部署方式	○ 单库	
*集群同步方式	○ 双主模式 ○ 主从模式	
子库地址	IP 端口 (十) (一)	
子库地址		
* 用户名		
* 密码	空密码	
	检测 提交 取法	肖

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。

资产管理 / 数据3	· · · · · · · · · · · · · · · · · · ·	6
aaa (172.1	5.8.159:1521) 的详情	
10	2	
10	-	
名称	283	
服务类型	Orade	
部署方式	95	
连接状态	•22	
创建时间	203-66-29 17:35:11	
修改时间	2033 66-29 18:43 25	
架构扫描状态	- CDM	
最近扫描时间	203 66-29 17:35:17	
地址信息		
Ib	172.16.8.159	
端口	1531	
账户信息		
服务名	ard	
账号角色	DBA	
用户名	595	
截码	2647	
插件信息		
配置状态	- ±0-#	

#### 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。

编辑数据源				×
ID	1			
* 名称	mm			
服务类型	MySQL			
* IP	172.16.23.197			
* 端口	3306			
使用SSL	不启用SSL V			
部署方式	单库			
* 用户名	root			
* 密码	已保存 修改密码			
		检测	提交	取消

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:

资产管理 / 数据源管理 / 数据源子库管理			
233 (3.2.5.6:22) 的子库列表			
基本信息 子库管理			
			海加子库
10 子序地址:编口	插件地址:础口	括件配置	操作
2 2.4.5.4:55		- 未使用	662381 BRFP;
1 5.4.5.1:55		= 未使用	NGTRE BRAD
			Total 2 12/bace V (1) Go to 1

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。

		扫描数据	『源架构			×	
	97						
B稗	172.16.8	名称	172.16.8.181	库/模式名关键字	查询	已选 0/8	
服务类型	Kingbase	地址	172.16.8.181	库/模式	状态	上次扫描时间	
部署方式	单库	端口	54321	xlog_record_read	已扫描	2022-09-22 14:40:13	
插件通信端口	50023	数据库名	test	test	已扫描	2022-09-22 14:40:12	
连接状态	<ul> <li>正常</li> </ul>	用户名	system				
创建时间	2022-09-	8563	已保存			(1 2 3 4 )	
修改时间	2022-09-		连接				
聚构扫描状态	<ul> <li>已扫描</li> </ul>					开始扫描 取消	
evened a	2022-09-22	14:40:13					

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:

资产管理 /	植作管理 /							6
插件列	表 ==							
<ul> <li>● 税助</li> <li>本系</li> <li>● 公</li> </ul>	提示 最需要与安装在数据库服务器上的加 总是显示	<b>告稿件配合使用。本页面提供了</b>	针对这些插作的管理功能,包括盖拉插	件状态、查看插件配置信息、终改抽	作配置等。			×
8649-1832	关键字 运行状况	s v 🕅	22 2					潭加插件
ID	插件地址: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	检测时间	操作
9	172.16.8.161:50023	0.06%	0.40%	1417MB	1	• 状态正常 〇	2023-06-30 11:41:35	查看 编辑 删除
8	172.16.8.158:50023	0.07%	0.40%	8255MB	0	• 状态正常 C	2023-06-30 11:41:55	查看 编辑 删除
7	172.16.8.153:50023	0.08%	0.84%	535MB	1	● 秋志正常 〇	2023-06-30 11:41:49	查看 编辑 删除
6	172.16.8.181:50023	0.07%	0.34%	7174MB	1	• 秋杰正常 G	2023-06-30 11:41:49	查看 编辑 删除
3	172.16.8.182:50023	0.07%	0.38%	5265MB	1	• 状态正常 G	2023-06-30 11:41:27	查看 编辑 删除
2	172.16.8.154:50023	0.06%	0.30%	57882MB	1	• 状态正常 G	2023-06-30 11:41:49	查看 编辑 删除
							Total 6 12/mane	( 1 ) Coto 1

图 4-8 插件列表

# 4.3.2.1. 添加插件

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				

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:

	添加插件				×
<b>律服务器上的加</b> 制	8插件配合使]				
运行状态	≰ ✓ *插件端口		检测		
Ĵ	CPUŁ				援交 取消
:50023	0.06%				E#C
:50023	0.07%	0.40%	8255MB	0	●状态正常 〇
					10 1

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: 资产管理 / 插件管理 / 插件详情

1	插件详情	<b>番件详情</b>						
	基本信息 下属	数据源 运行日志						
	插件 ID	2						
	插件 IP	172.16.12.55						
	插件端口	50023						
	当前状态 ⑦	• 状态正常						
	设备CPU使用率	0.25%						
	设备内存使用率	7.74%						
	设备磁盘总容量 🕐	35819MB						
	插件的CPU占用率	0.03%						
	插件的内存占用率	0.32%						
	插件的磁盘使用量 ②	7535MB						
	下属数据源数量	1						
	创建时间	2024-06-04 16:13:17						
	更新时间	2024-06-05 10:54:31						

#### 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:

资产管理 /	插件管理 / 下属数据源						6		
┃ 插件详	插件详细								
基本信	基本信息 下翼教教源 运行日志								
请输入数	· 湖榆入西部F在市場地址:   即至方式   ✓								
ID	数据游名称	服务类型	地址:磁口	部署方式	子库地址:编口	工作目录	工作目录大小		
6	kingbases8.181	KingbaseES	172.16.8.181:54321	单库		/var/tib/fecage/plain/6	OMB		
						Total 1 12/page	$\langle 1 \rangle$ Go to 1		

#### 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:

6

资产管理 / 插	资产管理 / 插件管理 / 插件运行日志							
插件详情								
基本信息	下属数据源	运行日志						
日志ID	插件IP		状态	持续时长	更新时间			
179790	172.16.12.55		状态正常	0天18小时48分9秒	2024-06-05 11:01:27			
				共1条 12条/页	$\vee$ 〈 $1$ 〉 前往 1 页			

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。

I	编辑插件		×	
記合使	* 插件地址	172.16.8.161		
~	* 插件端口	50023 检测		
CPUŁ	下属数据源数量	1	Ś	
0.06%	当前状态	• 状态正常	E	當(
0.07%		提本 取	3H	常C
0.08%		JEX 44	/H	常(

#### 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。 加密插件的下载与安装

```
-、安装包下载

    For Linux(x86_64): fecage-v2.1.17-release.c86127.el7.tar.gz

二、安装部署方法
  1. 上传安装包至数据库服务器任意目录下;
 2. 使用以下命令解压缩安装包:
   tar xf fecage-v*.tar.gz
 3. 进入解压缩后的目录,执行以下命令开始安装:
   sh fecage_install.sh
  4. 安装过程中会要求输入加密数据存放的目录,此时有两种选择:
   1)使用安装脚本推荐的设置,直接回车即可(推荐设置使用的是当前磁盘剩余空间最大的分区);
   2) 自定义加密数据存放目录,需输入自定义目录的绝对路径;
  5. 安装过程中还会要求输入插件提供服务使用的端口号,此时:
   1) 使用默认端口 50023, 直接回车即可;
   2)使用自定义的端口号,可输入1024~65535范围内的端口号(需避免使用已被其他服务占用的端口号);
  6. 安装过程中会要求输入两次用于离线解密的密码,请妥善保管此密码;
  注意:加密日录不能和数据库数据日录在同一文件夹
三、插件服务管理命令
  1. 启动插件服务命令:
   systemctl start fecage
  2. 停止插件服务命令:
   systemctl stop fecage
```

#### 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。

电切管理 / 主电切管理	
主密钥信息 □	
<ul> <li>● 帮助提示 系统的主电则把用来保护我就加密电话的密切,通过加密十主点。</li> <li>在本原面可以是在主意切的状态,若来创建,可以选择创建主电话,创建主电话,简确保加密十处子"记出动 (常规规定)"状态,主电引一旦创建,不可协改。</li> <li>● 总是显示</li> </ul>	×
+	
主密钥尚未创建,可点击"+"创建	

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:

密钥管理 / 主(	·忠衍哲理	
┃ 主密钥信』	8 ==	
<ul> <li>⑦ 帮助提示 系统的主题 在本页面:</li> <li>☑ 总是</li> </ul>	示 常知是从来保护教派加密密切的密切,通过加密卡生成。 可以各看主要的的状态,若来创建,可以选择创建主审切。创建主密切前,教确保加密卡处于"已命运(流频模式)"就态,主密切一旦创建,不可接动。 2 <u>型示</u>	×
状态	• EMM	
唯一标识	85326D09AE28AC062ALF329A27F8LAC4	
密钥长度	256 (bits)	
创建时间	2023-09-14-14-49-41	

#### 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:

备用密钥列	友 ②							
⑦ 帮助提示 系统的数量 期,到期未 ☑ 总是累	加密密切(简称"密切")受主密切保护,按照其6 被任何加密对象绑定时,会自动作废,变为历史密切 12 <del>元</del>	E用状态可分为备用密钥、在F ]。	8密钥和历史密钥。备用密管	別是指尚未被任何加密对象標定的密發	1,备用密钥一旦与加密对象绑实	2,则变为在用密钥。 本页商主要用于创	<b>电和管理备用密钥,新创建的</b> 诸	的對默认为备用密钥。备用密钥可设置有效
密钥标识或别名	送键字 请选择算法 ~ [	日 开始时间	- 结束时间	查询 重置				<b>本加密钥</b> 批量
ID	密钥标识	密钥别名		指定算法	密钥长度(bits)	创建时间	过期时间	操作
9	C2E7AA49F5D50F6109059C1F4D7E5D83			SM4_GCM	128	2024-07-31 11:21:27	不服	查看 删除
8	CA6B82A790C37D6D32F0AA7604069B80			SM4_GCM	128	2024-07-31 11:21:27	不限	查看 删除
7	250DD73894E55EC9707D0DE6AAFA82D5			SM4_GCM	128	2024-07-31 11:21:27	不限	查看 删除
6	425D20700B01784986C19A4AA5FAEFD3			SM4_GCM	128	2024-07-31 11:21:27	不限	查看 删除
1.2	28100102580002715020784424105200			SM4 GCM	128	2024-07-31 11-21-27	不限	

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

添加	密钥				\$
* 指定	算法	请选择算法	X		
*密钥	模板	请选择密钥模板	×		
* 牛成	教量	请输入1~1000的数字			

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" 2"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。

5) 有 形 可 12	帮助提示 系统的数据加密 页面主要用于创 2 总是显示	密钥(简称"密钥")受主密钥保护,按照其使用起 建和管理备用密钥,新创建的密钥数认为备用密钥。	《态可分为备用密钥、 备用密钥可设置有效	在用密钥和历 5期,到期未被	史密钥。备用密钥 任何加密对象绑定	]是指尚未被任何加 "时,会自动作废,	I密对象绑定的 变为历史密钥	)密钥,备用密钥 ]。	]一旦与加密对	象绑定,频	则变为在用	密钥。 本
时间	示识或别名关键	字 请选择算法 > 🗐	开始时间	-	结束时间	查询	重置			添加	密钥	批量
	ID	密钥标识	密钥别名			指定算法	密钥长度 (bits)	创建时间	过期时间	操作		
	9	C2E7AA49F5D50F6109059C1F4D7E5D83			✓ ×	SM4_G	128	2024-0	不限	查看	删除	
	8	CA6B82A790C37D6D32F0AA7604069B80	2			SM4_G	128	2024-0	不限	查看	删除	
	7	250DD73894E55EC9707D0DE6AAFA82D5				SM4_G····	128	2024-0	不限	查看	删除	
	6	425D20700B01784986C19A4AA5FAEFD3				SM4_G····	128	2024-0···	不限	查看	删除	
	5	3B1001D3E89CC271FD2C7BAA241CE200				SM4_G	128	2024-0	不限	查看	删除	

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:

查看备用密	钥详情	×
ID	9	
密钥标识	C2E7AA49F5D50F6109059C1F4D7E5D83	
密钥别名		
指定算法	SM4_GCM	
密钥长度	128 (bits)	
创建时间	2024-07-31 11:21:27	
过期时间	不限	ŭ
		关闭

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:

在用密	發钥列表 ②							
帮助 新納本页	助提示 的数据加密密钥(崩称"密钥")受主密钥保护, 面主要用于管理在用密钥。在用密钥无有效期,只 总是显示	按照其使用状态可分为备用密钥、在用密钥和历史 有当其被所有加密对象解绑后,才会变为历史密钥	密钥。在用密钥是指已经被一个 。	个或多个加密对象绑定的	內密钥。			×
密钥标识	R或别名关键字 请选择算法	✓ 査询 重置						
ID	密钥标识	密钥别名	指定算法	密钥长度(bits)	创建时间	操作		
49	2D875F68996FD55DC11AB4806C07D664		AES256_GCM	256	2024-07-31 1	查看	应用情况	
49 4	2D875F68996FD55DC11AB4806C07D664 713C7A671FE26B983340D2D5C7DCE91D		AES256_GCM SM4_GCM	256 128	2024-07-31 1··· 2024-07-26 1···	查看 查看	应用情况应用情况	

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:

提升	查看在用密	钥详情	×
的数	ID	49	
	密钥标识	2D875F68996FD55DC11AB4806C07D664	
或别	密钥别名		
	指定算法	AES256_GCM	
	密钥长度	256 (bits)	
	创建时间	2024-07-31 11:29:31	
			关闭

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" 2"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。

密钥管理	/ 在用密钥库						6
在用密	閉列表 ①						
<ul> <li>帮助</li> <li>系約</li> <li>本页</li> <li></li> </ul>	<mark>劝提示</mark> 的数或加密密钥(简称"密钥")受主密钥保护,按照 面主要用于管理在用密钥。在用密钥无有效用,只有当 <mark>总是显示</mark>	具使用状态可分为备用密钥、在用密钥和历史密钥。 其被所有加密对象解绑后,才会变为历史密钥。	,在用密钥是指已经被一	个或多个加密对象绑定的	内密钥。		×
密钥标识	就别名关键字 请选择算法 >>	查询    重置					
ID	密钥标识	密钥别名	指定算法	密钥长度(bits)	创建时间	操作	
49	2D875F68996FD55DC11AB4806C07D664	✓ ×	AES256_GCM	256	2024-07-31 1	查看 应用情况	
4	713C7A671FE26B983340D2D5C7DCE91D		SM4_GCM	128	2024-07-26 1…	查看 应用情况	
3	727F35769D8A63C6C76043966F49137F		SM4_GCM	128	2024-07-26 1…	查看 应用情况	
				共3条 12第	/页 >> <	1 > 前往	1 页

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。

	应用情况	5						×	
钥(简柄 理在用键	数据源名和	邻、地址、模式名或表	查询						
	ID	所属数据源	地址:端口	库/模式	表	字段	状态	应用时间	
	11	11	172.16.23.200:3306	test	user	phone	<ul> <li>已加密</li> </ul>	2023-09-14 15:32:30	
识						Total 1 12/r		Go to 1	
04D20CE						Total 1			5:32:30
A742BE								关闭	5:32:30
88AC2D14	45889101DD25	55B41D0A			AES128	1	28	2023-09-14	15:32:30

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:

密钥管理	密钥管理 / 历史密钥库									
历史	历史密钥列表 ①									
<ul> <li>✔ 帮助提示</li> <li>系统均数超加密密钥(简称"密钥")受主密钥保护,按照其使用状态可分为备用密钥、在用密钥和历史密钥。历史密钥是指不再被任何加密对象绑定的密钥,或已到期仍未被绑定的密钥。本页面主要用于管理历史密钥。</li> <li>☑ 总是显示</li> </ul>										
密钥棒	示识或别名关键	字 请选择算法 🗸 🧕	重置						批量删除	
	ID	密钥标识	密钥别名	指定算法	密钥长度 (bits)	创建时间	操作			
	48	6D2D8F6C49200BF157805C2973B926B5		SM3	256	2024-07-26	查看	删除		
	47	D2C8E5FD1E13D7302DDA3587896033B4		SM3	256	2024-07-26	查看	删除		
	46	3B75CD26BDCB9C178272DCA0676FBD19		SM3	256	2024-07-26…	查看	删除		
	45	C9E85D2AC0EE73235C07829A1C6C2B91		AES128_CBC	128	2024-07-26…	查看	删除		
	44	1F6FE2818DBD0B8690476E80E63E1FC9		SM4_CBC	128	2024-07-26…	查看	删除		
	43	A391788DD27AF3C1D6A4A9AF3015CE67		SHA256	256	2024-07-26…	查看	删除		
	42	EDF6C4F827A7CEA7E010C18108A53993		SHA256	256	2024-07-26…	查看	删除		
	41	03C5BE8A05936171560F81FC98092495		SHA256	256	2024-07-26…	查看	删除		
	40	76ACEBC6E6E076925A11FC8256DE0714		SM4_CBC	128	2024-07-26…	查看	删除		

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。

密钥管	理 / 历史密钥	库							6
历史	的名词列表 ⑦								
	界助提示 系统的数据加密 史密钥。 2 总是显示	密钥(简称"密钥")受主密钥保护,按照其使用状。	5可分为备用密钥、在用密钥和历史密钥。历史密钥	是指不再被任何加密	对象绑定的密钥,	或已到期仍未被绑定	的密钥。	本页面主要	× 用于管理历
密钥	标识或别名关键	字 请选择算法 > 查询	重置						批量删除
	ID	密钥标识	密钥别名	指定算法	密钥长度 (bits)	创建时间	操作		
	48	6D2D8F6C49200BF157805C2973B926B5		SM3	256	2024-07-26…	查看	删除	
	47	D2C8E5FD1E13D7302DDA3587896033B4	ok	SM3	256	2024-07-26…	查看	删除	
	46	3B75CD26BDCB9C178272DCA0676FBD19	✓ ×	SM3	256	2024-07-26…	查看	删除	
	45	C9E85D2AC0EE73235C07829A1C6C2B91		AES128_CBC	128	2024-07-26…	查看	删除	
	44	1F6FE2818DBD0B8690476E80E63E1FC9		SM4_CBC	128	2024-07-26…	查看	删除	
	43	A391788DD27AF3C1D6A4A9AF3015CE67		SHA256	256	2024-07-26	查看	删除	
	42	EDF6C4F827A7CEA7E010C18108A53993		SHA256	256	2024-07-26	查看	删除	

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:

D.	查看历史密钥	引详情	×	
刻	ID	45		B
2	1D	40		
	密钥标识	3B75CD26BDCB9C178272DCA0676FBD19		f
31	密钥别名			
L	指定算法	SM3		ŧ
Ŀ	密钥长度	256		
l	创建时间	2024-07-26 16:35:05		2
L	停用时间	2024-07-26 16:36:09		2
				2
			关闭	2
100				

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:

密钥管	理 / 密钥模)	扳管理				9
密	月模板列表(					
0	帮助提示 在本页面可以深 2 总是显示	季加和管理密钥模板,密钥模板定义了密	铜的长度、有效时长等规格参数	(,在创建密钥时,可以选择使用这些模板。		×
模板	名称关键字	查询 重置				漆加模板 批量删除
	ID	模板名称	指定算法	密钥长度(bits)	有效天数	操作
	8	[Default] HMAC_SHA256 Key	HMAC_SHA256	256	不限	
	7	[Default] SHA256 Key	SHA256	256	不限	
	6	[Default] SM3 Key	SM3	256	不限	
	5	[Default] AES128_CBC Key	AES128_CBC	128	不限	
	4	[Default] AES256_GCM Key	AES256_GCM	256	不限	
	3	[Default] SM4_CBC Key	SM4_CBC	128	不限	
	2	[Default] SM4_GCM Key	SM4_GCM	128	不限	
					共7条 12条/页	< 1 > 前往 1 页

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。

密钥官 图 密钥	理 / 密钥模 月模板列表	<b>放管理</b> ②				9
0	帮助提示 在本页面可以 2 总是显示	率加和管理密钥模板,密钥模板定义了要 、	销的长度、有效时长等规格参数,	在创建密钥时,可以选择使用这些模板	e.	×
模板	名称关键字	查询 重置				添加模板 批量删除
	ID	模板名称	指定算法	密钥长度(bits)	有效天数	操作
	8	[Default] HMAC_SHA256 Key	HMAC_SHA256	256	不限	
	7	[Default] SHA256 Key	SHA256	256	不限	
	6	[Default] SM3 Key	SM3	256	不限	
	5	[Default] AES128_CBC Key	AES128_CBC	128	不限	
	4	[Default] AES256_GCM Key	AES256_GCM	256	不限	
	3	[Default] SM4_CBC Key	SM4_CBC	128	不限	
	2	[Default] SM4_GCM Key	SM4_GCM	128	不限	
					共7条 12条/页 V	< 1 → 前往 1 页

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	说明
	填	
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

7 580-1	添加密钥机	莫板		×	
- 12	*模板名称	请输入模板名称			
	*加密算法	请选择	~		
l	有效时长	留空或0表示不限时长	Æ		
				提交取消	

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。

)帮助提示	编辑密钥	莫板			×
在本页面	模板ID	10			
板名称关键	* 模板名称	3			
ID	* 指定算法	AES256_GCM	$\sim$		
10 9	有效天数	3			
8					提交取消
7	[Delault]	энагэо кеу энагэо		200	小限

#### 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(己加密数量/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	禁用或启用二选一,默认为关闭
	二选一	
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
连接方式	默认或自定	开启高级设置时需选择,默认或自定义二选一,默
	义二选一	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。

选择加密方案 - 配置表空间加密								
() 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 <u>(在MySQL v8.0服务器上配置加密目录访问权限的方法)</u>							
数据源	172.16.23.197:3306							
服务类型	MySQL							
部署方式	单库							
加密方案	表空间加密							
读保护	● 禁用 ○ 启用							
防绕过⑦	• 禁用 ③ 启用							
* 插件地址	请选择插件地址 🗸							
* 插件端口	清输入所件端口 检测							
连接方式	<ul> <li></li></ul>							
	上一步    提交	关闭						

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

1.1 自库	选择加密方案-配置表空间加密		× .
未	正在进行相关设置,请稍候…		191
	纳管插件成功		
<b>军</b> 御	启用表空间加密		
L	配置失败,请返回修改配置后重试		
		返回	关闭

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、 己配置未保存、己配置已保存)、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	密钥状态为己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	禁用或启用二选一,默认为关闭
	二选一	
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。

选择加密	方案 - 配置原生加密	×
数据源	172.16.8.43:1521	
服务类型	Oracle	
部署方式	集祥	
加密方案	原生加密	
读保护	● 禁用 ○ 启用	
防绕过⑦	<ul> <li>● 禁用</li> <li>◎ 启用</li> </ul>	
密钥状态	•已配置、未保存 重新检测	
* 当前密钥	请输入当前的加密密钥	
更换密钥		
高级设置		
		上一步 下一步 关闭

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	支持或不支持二选一,默认为不支持			
	二选一				
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	
r			
选择加密方	5案 - 配置原生加密		×
主机SSH	<ul> <li>支持</li> <li>〇 不支持</li> </ul>		
* 主机地址	请输入主机地址		
* SSH端口	22		
* SSH用户名	oracle		
* SSH密码	请输入主机的SSH密码	检测	
			上一步 提交 关闭

图 4-39 配置原生加密(单库)-第二步-支持主机 SSH

选择加密	方案 - 配置原生加密	×
主机SSH	○ 支持   ● 不支持	
手动配置	请参考以下帮助文档,在数据库服务器上启用TDE模块 《在数据库服务器上启用TDE模块的方法》	
	□ 确认已完成手动配置	
	上一步    提交	关闭

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。

选择加密方案 - 配置原生加密	×
正在进行相关设置,请稍候	
连接主机 <b>成功</b>	
启用NTE功能	
配置成功,请等待页面跳转	
	关闭

#### 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	高级设置下可见,更新表和复制表二选一,默
	表二选一	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。

选择加密方	案 - 配置网关加密	×
() MySQL网关	加密默认不支持SM4国密算法,如需支持,害先在数据库中安装相关扩展模块,具体方法参考 <u>(MySQL数据库安装 SM4 算法插件的方法)</u>	
数据源	172.16.23.197:3306	
服务类型	MySQL	
部署方式	单库	
加密方案	网关加密	
读保护	◎ 禁用 ○ 启用	
防绕过⑦	⊙ 禁用 □ ◎ 启用	
* 代理端口	👩 自动设置	
存量数据处理	<ul> <li>通过更新原表数据对存量数据进行加密,适合数据库对象复杂但数据量不大的场景</li> <li>通过复制表并迁移数据对存量数据进行加密,适合数据量大但数据库对象不复杂的场景</li> </ul>	
	上一歩 提交 笑	闭

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。

选择加密方案 - 配置网关加密	×
正在进行相关设置,请稍候	
配置网关加密	
配置成功,请等待页面跳转	
1	关闭

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:

策略管理 / 加密配置 / 管理	e too verset a	R																							
请输入关键字		172.16.1	2.163					防护状态						~											
MySQL	3	服务地址	172.16.12.163:1521		服务类型	Oracle		加密方案	表空间加密			,	6改纪第	取消方案											
172.16.23.200 : 3306		架构扫描	• 已扫描		使用插件	• 已配置		例外规则	£					管理规则											
Oracle	3	插件地址	172.16.12.163:50023		插件状态	<ul> <li>连接失敗</li> </ul>																			
2.2.2.2 : 111 172.16.8.159 : 1521 172.16.12.163 : 1521				● 帮助打 本页面 数据内 2	提示 1可以为数据算设置需要加密存缩 1系统透明。同时,还可以开启"1 3. <mark>是显示</mark>	的对象,可具体到床/模式、表或字 决保护"功能,来确保在数据库系。	段。设置后,1 统中读取这些表	5些对象在写入数据时,会先对数据进行 18时不返回数据明文,从而实现数据在1	加密,两存储到磁盘上。为了 存储和使用场景下的双重保护。	不影响数 泥库立身伤等	件查询、聚合统	计、全文检察等基础功能,	上述加密操	作会在文	件系统层	× 进行,对									
											请输入关键	#F 状态	~ 查询	東置						源加	0加速对\$		批量操作		
			ID ID	库/模式	农	学级	起带导派	状态	创建时间		更新时间	操作													
			□ <i>1</i>	GSMUSER	CUSTOMER_INF01	1.00	SM4 🔑	* 未加密	2023-06-30	14:40:32	2023-06-30 14:40:32	编辑	2018	明稔 历	速										
			6	C##LZW	table03	0.50	SM4 🖉	= 未加密	2023-06-30	14:40:32	2023-06-30 14:40:32	编辑	2045 H	MAR DA	史										
															5	C##LZW	table01		SM4 P	* 未加密	2023-06-30	14:40:32	2023-06-30 14:40:32	1610	2018
		□ 4	C#WLZW	table02		SM4 P	* 未加密	2023-06-30	14:40:32	2023-06-30 14:40:32	编辑	2018: I	明除 历	速											
		3	C##LZW	hohotest		SM4 🖉	= 未加密	2023-06-30	14:40:32	2023-06-30 14:40:32	编辑	2018: 1	删除 历	使											
									Total 5	12/page 🗸 🗸	< 1		Go to	1											

### 图 4-44 已配置表空间加密

莱略管理 / 加密配置 / 管理	加密对象											
请输入关键字		aaa					防护状态			~		
MySQL	3	服务地址	172.16.8.159:1521	服务类	한 Oraci	cle	加密方案	原生加密	修改配置 取消方	*		
1.1.1.1:3306		部第方式	单库	连接状	古 • 正?	<b>宮</b>	读保护	未开启	开启读保	æ.		
172.16.23.200 : 3306		果构扫描	<ul> <li>已扫描</li> </ul>	使用插	件 * 未作	使用	例外规则	无	管理频	则		
3.2.5.6:22		插件地址		插件状	<u>6</u> .		代理端口	59001				
<b>172.16.8.159 : 1521</b> 172.16.12.163 : 1521				本页面 数据库	可以为数据源设置需要加密存储的对 系统中读取这些数据时不返回数据明 是显示	象,可具体到你/模式、表成字段。 设置/ 文,从而实现数据在存储和使用场景下的	5,这些对象) 双重保护。	在写入数据时,会先对数据进行加密,两存储到磁盘上。上述加	<sup>要操作由数据库内</sup>	部的TDE模块完成,对上层应用透明。同	时,还可以开启"读保护"功能,来确保在	
		请输入关键	字 状态	✓ 查询 重置					添加加密对象 批量操	PF-		
		III ID	库/模式	*	字段	秋志 创	建时间	更新时间	操作			
						No Data						
								Total 0 12/page V	$\sim$ 1 $\rightarrow$ Go to 1			

图 4-45 已配置原生加密

请输入关键字		o 🕖				防护状态			
	夕和 抽屉	服务地址	172.16.8.43:1521	服务类型	Oracle	加密方案	网关加密	(端口: 59000)修改配置	取消方案
	10100 1011	部署方式	集群	连接状态	•正常	读保护	◎ 未开启	1	设置读保护
) MySQL	2	架构扫描	<ul> <li>已扫描</li> </ul>	使用插件	◎ 未使用	例外规则	无		管理规则
m 主从		插件地址	-	插件状态	2	完整性保	户 ◎ 未开启		启用
		● 帮助提;	7						×
0   SQL Server ss	1	⑦ 帮助提; 本页面可 时,还可 ☑ 总是	示 以为数据源设置需要加速 以开启"读保护"功能, 显示 む表名关键字	存储的对象,应具体到字段。 来确保在数据库系统中读取) 话输入关键字	。设置后,这些字段在写, 这些数据时不返回数据明3	入数据时,会先对数据进行加限 文,从而实现数据在存储和使序	,再存储。上述加 场景下的双重保护。	密操作由数据库自身来完成 , 流加加密对象	× (, 同 #88#
0 ] SQL Server SS	1	<ul> <li>帮助提;</li> <li>本页面可</li> <li>时,还可</li> <li>总是</li> <li>请输入库/模式</li> </ul>	示 以为数据源设置需要加密 以开启"读保护"功能, 显示 却表名关键字 十	存储的对象,应具体到字段。 来确保在数据库系统中读取3 请输入关键字 表 字	<ul> <li>、没置后,这些字段在写,</li> <li>这些教協时不返回数据明3</li> <li>状态</li> <li>段 加密算法</li> </ul>	<ul> <li>入数銀时,会先対数据进行加速 文,从而实现数据在存储和使序     </li> <li> <u>変</u>)             <u>変</u> <u>変</u> </li> <li> <del>双</del> <u>変</u> <u>微</u> <u>微</u> </li> </ul>	, 再存储。上述加 场景下的双重保护。 1	密操作由数据库自身来完成 , <b>添加加密对象</b>	× 8,同 批量操作
0 ) SQL Server SS	1	<ul> <li>⑦ 帮助提;</li> <li>本页面可时,还可</li> <li>☑ 总是</li> <li>请输入库/概5</li> </ul>	示 以为数据游设置需要加速 以开启"读保护"功能, 显示 10表名关键字 十	存缩的对象,应具体到字段。 来确保在数据库系统中读取3 请输入关键字 	。设置后,这些字段在写。 这些数据时不返回数据明3 状态 段 加密算法	<ul> <li>入数振时,会先对数据进行加速 (文、从而实现数据在存储和使序)</li> <li> <u>変</u>)             <u>変</u> <u>変</u></li></ul>	;, 再存储。上述加 场景下的双重保护。 1	密操作由数据库自身来完成 , <b>净加加密对象</b> 1 操作	× む,同 批量操作

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	开启高级设置时需选择,默认或自定义二选一,默
	义二选一	认为默认,若选择自定义需填写连接参数,如 socket
		或 ip:port

选择加密	四方案 - 配置表空间加密	×
MySQ	L v8.0.4 及以上版本安装加密操件后,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 <u>【在MySQL_v8.0服务器上配置加密目录访问权限的方法】</u>	
数据源	172.16.23.197:3306	
服务类型	MySQL	
部署方式	单库	
加密方案	表空间加密	
* 插件地址	172.16.23.197 V	
* 插件端口	2323 检测	
高级设置		
	上一步 提交	关闭

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。

1.1 自库	选择加密方案-配置表空间加密	×	密保
未	正在进行相关设置,请稍候…		191-1
	纳管插件成功		
11	启用表空间加密		
	配置失败,请返回修改配置后重试		
	返回 关i	闭	I

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	密钥状态为己配置未保存和己配置已保存情况下
		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	

请输	↓ 父従字 000	PULU TANGA
选择加密方	案-配置原生加密	×
数据源	172.16.8.43:1521	
服务类型	Oracle	
部署方式	集群	
加密方案	原生加密	
密钥状态	• 已配置、已保存 重新检测	
更换密钥		
代理端口	59000	
更换端口	59000 可用范围: 59000~59999	
	1	:一步 下一步 关闭

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

选择加密方	5案 - 配置原生加密		×
主机SSH	<ul> <li>● 支持</li> <li>○ 不支持</li> </ul>		
* 主机地址	请输入主机地址		
* SSH端口	22		
* SSH用户名	oracle		
* SSH密码	请输入主机的SSH密码	检测	
			上一步    提交    关闭

图 4-50 配置原生加密(单库)-第二步-支持主机 SSH

选择加密	方案 - 配置原生加密	×
主机SSH	○ 支持   ◎ 不支持	
手动配置	请参考以下帮助文档,在数据库服务器上启用TDE模块	
	《在数据库服务器上启用TDE模块的方法》	
	确认已完成手动配置	
	上一步    提交	关闭

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。

选择加密方案 - 配置原生加密	×
正在进行相关设置,请稍候…	
连接主机成功 启用NTE功能	
配置成功,请等待页面跳转	
	关闭

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	高级设置下可见,更新表和复制表二选一,
	二选一	默认为更新表方式

选择加密方	案 - 配置网关加密	×
9 SQL Server	周关加密默认不支持SM4国密算法,如需支持,需先在数据库中安装相关扩展模块,具体方法参考 <u>《SOL Server数据库安装 SM4 算法插件的方法》</u>	
数据源	172.16.8.18:1433	
服务类型	SQL Server	
部署方式	单库	
加密方案	网关加密	
* 代理端口	自动设置 59001 自定义端口可用范围: 59000~59999	
存量数据处理	<ul> <li>通过更新原表数据对存量数据进行加密,适合数据库对象复杂但数据库对象不复杂的场景</li> <li>通过复制表并迁移数据对存量数据进行加密,适合数据量大但数据库对象不复杂的场景</li> </ul>	
	上一步	专闭

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。

选择加密方案 - 配置网关加密	×
正在进行相关设置,请稍 <del>候</del> … 配置网关加密	
配置成功,请等待页面跳转	
	关闭

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。

提示			×
0	确定取消当前的加密方案吗?		
		确认	取消

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。

选择方:	式: 按表选择	~				已选的加密对象 (3)	
请输	入关键字					wy_test7 - Student	
	表ID	表		所属库/模式		wy_test9 - Course	
	93775	Teacher		wy_test9			
	93774	Student		wy_test9			
	93773	SC		wy_test9			
	93772	Course		wy_test9			
	93767	Teacher		wy_test7			
	93766	Student		wy_test7			
	93765	SC		wy_test7			
	93764	Course		wy_test7			
	93763	Teacher		wy_test6			
	93762	Student		wy_test6			
	93761	SC		wy_test6			
	93760	Course		wy_test6			
	Total	63 12/page ~	< 1 2	3 4 5 6	> Go to 1		

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。

认加密算法	SM4_GCM $\lor$			
请输入关键字				
表ID	库/模式	表	加密算法	
1058	ywtest	sbtest7	默认 シ	
1054	ywtest	sbtest49	SM4_GCM V	
1052	ywtest	sbtest47	AES256_GCM $\lor$	
			共3条 12条/页 🗸 👌	前往 1

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。

4	public	customer_info	test, create_datetime	AES256
		提示	page ~	$\langle 1  ightarrow$ Go to $1$
		④ 确定要添加这些加密对象吗?	±# [	提交并加密 提交 取消
			确认 取消 Data	

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。

服务地址 172	2. <b>1</b> 6.8.18:1433	服务类型	SQL Server	加密方	案 网关加密	(端口: 59002)修改配	置 取消方案
部署方式 单序	车	连接状态	• 正常	读保护	◎ 未开启		设置读保护
架构扫描 • E	已扫描	使用插件	◎ 未使用	例外规	则 无		管理规则
插件地址 -		插件状态		完整性	保护 * 未开启		启用
							3
帮助提示							
帮助提示 本页面可以为数 时、正可以为数	y据源设置需要加强	客存储的对象,应具体到字印	段。设置后,这些字段在写 <i>)</i>	入数据时,会先对数据进行が 、以下の限制になた(第9)	0密,再存储。上述加 ====================================	密操作由数据库自身来分	記成,同
帮助提示 本页面可以为数 时,还可以开启 区 总是显示	y据源设置需要加强 言"读保护"功能,	8存储的对象,应具体到字印 来确保在数据库系统中读时	没。设置后,这些字段在写 <i>)</i> 取这些数据时不返回数据明5	N数据时,会先对数据进行加 文,从而实现数据在存储和f	u密,再存储。上述加 吏用场景下的双重保护	密操作由数据库自身来另 。	<b>記</b> , 同
帮助提示 本页面可以为数 时,还可以开启 区 总是显示	数据源设置需要加强 3 "读保护"功能,	8存储的对象,应具体到字间 来确保在数据库系统中读时	退。设置后,这些字段在写 <i>)</i> 取这些数据时不返回数据明3	入数据时,会先对数据进行) 文,从而实现数据在存储和f	u密,再存储。上述加 使用场景下的双重保护	密操作由数据库自身来分 。	2成,同
<ul> <li>帮助提示 本页面可以为费时,还可以开启</li> <li>总是显示</li> <li>请输入库/模式/表名</li> </ul>	效据源设置需要加码 ∃ "读保护"功能, 关键字 +	8存储的对象,应具体到字6 来确保在数据库系统中读时 证输入关键字	级。设置后,这些字段在写力 取这些数据时不返回数据明3 状态	入数据时,会先对数据进行力 文,从而实现数据在存储和付 文 <b>查询</b>	印密,再存储。上述加 使用场景下的双重保护 重置	密操作由数据库自身来分。 。 <b>添加加密对象</b>	E成,同 批量操作
<ul> <li>帮助提示</li> <li>本页面可以为数</li> <li>时,还可以开启</li> <li>总是显示</li> <li>青输入库/模式/表名</li> </ul>	牧据源设置需要加码 雪"读保护"功能, 关键字 ┿	87存储的对象,应具体到字段 来确保在数据库系统中读明 详输入关键字 表	9。设置后,这些字段在写力 取这些数据时不返回数据明5 状态 字段 加密算法	入数据时,会先对数据进行加 文,从而实现数据在存储和何 查询     成     びある     なん     なん	印密,再存储。上述加 走用场景下的双重保护 重置 建时间 更新时间	密操作由数据库自身来デ 。 <b>添加加密对象</b> 到 操作	品成,同 批量操作
<ul> <li>         帮助提示         本页面可以为数         时,还可以为数         时,还可以为数         </li> <li>         总是显示         </li> <li>         精输入库/模式/表名     </li> </ul>	牧掘斎设置需要加码 含"读保护"功能, 关键案 ┿	87存储的对象,应具体到字印 来确保在数据库系统中读印 详输入关键字 表 :	Q。设置后,这些字段在写力 (双这些数据时不返回数据明5 (双这些数据时不返回数据明5 (双达 (双达 (双达)) (双达) (双达) (双达) (双达) (双达)	<ul> <li>入数据时,会先对数据进行加 文,从而实现数据在存储和何     </li> <li> <li></li> <li></li></li></ul> <li></li> <li> <li></li> <li> <li></li> <li> <li></li> <li> <li></li> <li> <li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li>	印密,再存储。上述加 定用场景下的双重保护 重置 建时间 更新时间	密操作由数据库自身来学。	E成,同 批量操作

图 4-59 网关加密-添加加密表

	添加	表							×
į	请输	入关键字						已选的表(0)	
		表ID	库/模式			表			
		1088	dbo			spt_monitor			
		1087	dbo			test2			
		1086	dbo			MSreplication_options			
		1085	dbo			中文			
		1084	dbo			yesok			
		1083	dbo			testbb			
		1082	dbo			аааааа			
		1081	dbo			bbb			
		1080	dbo			spt_fallback_usg			
		1079	dbo			spt_fallback_dev			
		1078	dbo			spt_fallback_db			
				共11条	12条/页	~ ( <b>1</b> )	前往 1 页	ſ	
	_							l	下一步 取消

图 4-60 网关加密-添加加密表

;	忝加表			×
	请输入关键字			
	表ID	库/模式	表	存量数据处理方案
	1088	dbo	spt_monitor	更新原表数据
	1087	dbo	test2	复制表并迁移数据 🗸
				共2条 12条页 > (1) 前往 1 页
				上一步 提交 取消

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。

ss 🕖				防护状态			
服务地址	172.16.8.18:1433	服务类型	SQL Server	加密方案	网关加密	(端口: 59002)修改配置	取消方案
部署方式	单库	连接状态	• 正常	读保护	• 未开启		设置读保护
架构扫描	<ul> <li>已扫描</li> </ul>	使用插件	◎ 未使用	例外规则	无		管理规则
插件地址	-	插件状态	÷	完整性保护	◎ 未开启		启用
本页面可以	以为数据源设置需要加密	存储的对象,应具体到字段。	设置后,这些字段在写入数据	时,会先对数据进行加密,再有	字储。上述加强	目操作由数据库自身来完成	t, 同
本页面可!; 时,还可!; <b>2</b> 总是! 育输入库/模式	、 以为数据源设置需要加密 以开启"读保护"功能, 显示 (表名关键字 +	存储的对象, 应具体到字段。 来倫保在数据库系统中读取过 ④ 该表采用"更新原表要	设置后,这些字段在写入数据 这些数据时不返回数据明文,从 数据"方案处理存量数据	时,会先对数据进行加密,再7 而实现数据在存储和使用场景	字儲。上述加强 下的双重保护。	8操作由数据库自身来完成	<b>党,同</b>
本页面可以 时,还可以 ご 总是 育输入库/模式 bo・spt_mon bo・test2	、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	存储的对象,应具体到字段。 来确保在数据库系统中读取过 ③ 该表采用"更新原表要 请输入关键字	设置后,这些字段在写入数据 这些数据时不返回数据明文,从 数据"方案处理存量数据 状态 ~	时,会先对数据进行加密,再7 而实现数据在存储和使用场景 查询 重置	穿锯。上述加强 下的双重保护。	5操作由数据库自身来完成 添加加密对象	£,同 批量操作
本页面可以 时,还可以 <b>ご 总是</b> 請输入库/模式 bo・spt_mon bo・test2	、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	存储的对象, 应具体到字段。 来确保在数据库系统中读取这 ④ 该表采用"更新旅表数 请输入关键字 — 表 字(	设置后,这些字段在写入数据 这些数据时不返回数据明文,从 数据"方案处理存量数据 状态 ~ 段 加密算法 状;	时,会先对数据进行加密,再7 而实现数据在存储和使用场景 查询 重置 & 创建时间	字硫。上述加强 下的双重保护。 更新时间	5操作由数据库自身来完成 添加加密对象 操作	党,同 批量操作
本页面可以 时, 还可以 2 总是	、 以为数据源设置需要加速 以开启"读保护"功能, 显示 /表名关键字	<ul> <li>存储的对象,应具体到字段。</li> <li>来确保在数据库系统中读取这</li> <li>③ 该表采用"更新原表数</li> <li>请输入关键字</li> <li>页 表 字(</li> </ul>	设置后,这些字段在写入数据 这些数据时不返回数据明文,从 数据"方案处理存量数据 状态 ~ 段 加密算法 状;	时,会先对数据进行加密,再7 而实现数据在存储和使用场景 查询 重置 数 创建时间 暂无数据	5桶。上述加3 下的双重保护。 更新时间	8操作由数据库自身来完成 添加加密对象 操作	<b>北量操作</b>

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。

ž	添加が	加密对象							×
戶	偏表:	dbo•spt_monit	or					已选的加密对象(0)	
	请输)	入关键字							
		字段ID	字段		数据类型		受限原因		
		4464	total_errors		int				
		4463	total_write		int		2		
		4462	total_read		int		м.		
		4461	pack_errors		int		-		
		4460	connections		int				
		4459	pack_sent		int		-		
		4458	pack_received		int		~		
		4457	idle		int		*		
		4456	io_busy		int				
		4455	cpu_busy		int		-		
_		4454	lastrun		datetime		字段类型不支持加密		
				共11条	12条/页 🛛 🗸	<	1 〉 前往 1 页		
								下一步	Ä

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。

µæ≃	ヨカ川出産剤	网大		🖂 SecAdmin 🗸
;	添加加密对	封象		×
F	新属表: dbo•s	spt_monitor		
3	默认加密算法	AES128_CBC	$\sim$	
[	请输入关键字			
	字段ID	字段	数据类型	加密算法
	4457	idle	int	AES128_CBC
	4456	io_busy	int	SM4_CBC V
				共2条 12条/页 > i社 1 页
				上一步 提交并加密 提交 取消

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。

1	编辑加密列						×	
	所属库/模式	xuanzhaoyue						辈的
	所属表	tuomin_001						
	字段范围	💿 全部列 🔷 自定义						0209
						提交	取消	
12	xuanznaoyue	tuomin_uu1	USEI_IQ,SIQ	SM4 X	<ul> <li>已加密</li> </ul>	2022-09-01 10:53:42	2011/201	解密

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。

编辑	加密列		×
1 956 956 956 756	ब库/模式 ब表 受范国	xuanzhaoyue         B時約列 (2)           user_jd         user_jd           tuomin_001         sid           全部列 0自定义	
请输	1入关键字		
	字段ID	字段	
	446096	user_id	
	446097	sid	
	446098	tid	
	446099	user_name	
	446100	first_name	
	446101	last_name	
	446102	user_sex	
	446103	color	
	446104	card_number	
	446105	user_password	
	446106	email	
	446107	dates	
		Total 12 12/page V ( 1 > Go to 1	
		援交 取7	1

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"己加密" 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"己加密""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:

加速	管理 / 1	加密配置 / 管理加密对象					
5	加解	密操作历史				2	< 都对象
ľ	库/模式	encrypt					星被
	农	t_operate_log					化密
	ID	操作类型	处理状态	处理结果	操作人	操作时间	保密
	28	解密	已完成	成功	SecAdmin	2022-09-26 16:51:35	星速
	27	加密	已完成	成功	SecAdmin	2022-09-26 16:51:30	释被
	24	解密	已完成	成功	SecAdmin	2022-09-26 16:51:05	0.65
	7	加密	已完成	成功	SecAdmin	2022-09-26 11:59:16	星迹
					Total 4 12/page V	< 1 → Goto 1 美闭	<b></b>
5	enci	rypt t_user	*	SM4 🖉 • 已加速	2022-09-24 14:59:46	2022-09-24 14:59:50 编辑	解密

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。

97



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:

98

000102	理 / 加	I密配置 / "读保护"例外规则								¢
0	vy] m	nysql-8.154 (172.16.8.154.3306)	的"读保护" 例外规则列表							
0	帮助提 Frait	茶 菜产功能后,当针对加密数据的访问请求卓中 是显示	中以下任意一条已启用的规则时,"读得	护动能不主效,即数据所度研究文数据。						×
规则	名称关制	12 状态	· 查询		读保护 (	зяя) 🛪	印規則	批型	鮒作	
	ID	规则名称	状态	创建时间	更新时间	操作				
	10	12	<ul> <li>已启用</li> </ul>	2022-09-01 12:03:34	2022-09-01 12:03:35	停开	<b>查看</b>	编辑	MH22	
	9	1	<ul> <li>已启用</li> </ul>	2022-09-01 12:03:08	2022-09-01 12:03:08	停用	- 28	编辑	删除	
	8	全一点	<ul> <li>已启用</li> </ul>	2022-09-01 11:54:45	2022-09-01 11:58:46	停开	章石	编制	MIT2	
	7	cs	• 未启用	2022-09-01 11:53:09	2022-09-01 11:53:20	前用		编辑	18132	
	6	测试	• 未启用	2022-09-01 11:39:40	2022-09-01 11:55:23	此用	查看	1638	翻称	
	5	012345678901234567890123456781	<ul> <li>未点用</li> </ul>	2022-09-01 11:37:38	2022-09-01 11:39:00	启用	28	编辑	<b>B</b> 579	
	4	012345678901234567890123456789	<ul> <li>未启用</li> </ul>	2022-09-01 09:32:03	2022-09-01 11:56:08	此用	<b>奈石</b>	1618	INTR.	

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	选择启用或者禁用,默认为启用
	用二选一	
选择方式	全部已加	选择全部已加密数据或者自定义范围,默认全
	密数据和	部已加密数据
	自定义范	
	围二选一	
选择范围	自定义范	根据库/模式、表、字段信息圈定的范围,已添
	围下必填	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

oracle8.182	(172.16.8.182:1521)的"读保护"例外规则-添加规则
へ 基本信息	
* 规则名称	
规则状态	● £用 ○ 数用
へ数据范围	
选择方式	◎ 会部已加密数据 ○ 自定义规则
へ访问来源	
数据库账号	等于         >         请选择数据终期号         >
来源IP	<b>等于</b> >
	支持输入 举个IP、 IP贫威的学师 表示P范围, 使用巡号()分编。如:172.16.1.100(单个IP),172.16.2.101-172.16.2.120(IP简),172.16.10.0/24(IP]子纲)
へ 生效时间	
时间范围	<ul> <li>         · 認知时间         · · · · · · · · · · · · · · ·</li></ul>
	1838 R58

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。

选择	表范围							已选的表(12)
请输.	入关键字							wy_test - all_type_tb wv_test9 - Teacher
	表ID	库/模式		表	字段范	EN		wy_test9 - Course
	93907	wy_test		all_type_tb	<b>○</b> 全	部	〇 自定义	wy_test8 - Ieacher wy_test8 - Student
	93775	wy_test9		Teacher	<b>○</b> 全	部	〇 自定义	wy_test8 - SC wy_test8 - Course
~	93772	wy_test9		Course	<b>○</b> 全	部	○ 自定义	wy_test1 - Course
	93771	wy_test8		Teacher	<b>○</b> 全	部	○ 自定义	wy_test - customer_info_dest
<b>~</b>	93770	wy_test8		Student	<b>○</b> 全	部	○ 自定义	wy_test - customer_info wy_test - Teacher
<b>~</b>	93769	wy_test8		SC	<b>〇</b> 全	部	○ 自定义	
~	93768	wy_test8		Course	<b>○</b> 全	部	○ 自定义	
~	93711	wy_test1		Course	<b>○</b> 全	部	○ 自定义	
~	93710	wy_test		test_table_0	<b>○</b> 全	部	○ 自定义	
~	93709	wy_test		customer_info_dest	<b>○</b> 全	部	○ 自定义	
<b>~</b>	93708	wy_test		customer_info	<b>○</b> 全	部	○ 自定义	
	93707	wy_test		Teacher	<b>○</b> 全	部	○ 自定义	
			Total 15	12/page V	1 2	>	Go to 1	

图 4-72 选择数据范围-全部

へ 数据范围				
选择方式	② 全部已加密数据 ② 自定;	义范围		
选择范围	库/模式	8	字段	操作
	wy_test	al_type_tb		MHR9.
	wy_test9	Teacher		删除
	wy_test9	Course		HRRS.
	wy_test8	sc		<b>B</b> HP3
	wy_test	customer_info		
	wy_test	Teacher		BUS:
	wy_test	Student		IN 19
		3	820	

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。

选择	表范围						已选的表(8)	
请输)	入关键字						wy_test - all_type_tb wy_test9 - Teacher	
۲	表ID	库/模式		表	字段范围		wy_test9 - Course	
2	93907	wy_test		all_type_tb	● 全部	○ 自定义	wy_test8 - Student	
2	93775	wy_test9		Teacher	◎ 全部	〇 自定义	wy_test8 - SC wy_test8 - Course	
2	93772	wy_test9		Course	○ 全部	● 自定义	wy_test - Teacher	
2	93771	wy_test8		Teacher	○ 全部	● 自定义		
~	93770	wy_test8		Student	○ 全部	● 自定义		
~	93769	wy_test8		SC	◎ 全部	〇 自定义		
~	93768	wy_test8		Course	● 全部	〇 自定义		
	93711	wy_test1		Course	● 全部	〇 自定义		
	93710	wy_test		test_table_0	● 全部	〇 自定义		
	93709	wy_test		customer_info_dest	● 全部	〇 自定义		
	93708	wy_test		customer_info	● 全部	〇 自定义		
~	93707	wy_test		Teacher	◎ 全部	〇 自定义		
			Total 15	12/page V	1 2 >	Go to 1		

图 4-74 选择数据范围-自定义

青选择:	94				已选的字段(2)	
请锒.	入关键字				wy_test - SC - Cld	
٠	字段ID	库/模式	表	字段	wy_test - SC - SId	
	3674313	wy_test	SC	score		
	3674312	wy_test	SC	Cld		
	3674311	wy_test	SC	SId		
			Total 3 12/page	$\sim$ < 1 $\rightarrow$ Go to 1		
			Total 3 12/page	$\sim$ (1) Go to 1		

图 4-75 选择数据范围-自定义

へ 数据范围				
选择方式	○ 全部已加密数据	● 自定义范围		
选择范围	库模式	ą	字段	銀作
	wy_test9	Teacher		删除
	wy_test	al_type_tb	geometrycollection_f,tinytext_f	<b>M</b> 52
	wy_test	customer_info		删除
	wy_test	al_type_tb	varbinary_f,tinyint_f	MITS:
			at as	

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:

aaa (172.1	6.8.159:1521) 的"读保护"例外规则-
基本信息	
规则ID	6
规则名称	342河动
规则状态	*已启用
数据范围	
已透范围	全部
访问来源	
数据库账号	等于 OUTLN_SYSSUME,DBSNMP
来源IP	\$ <del>7</del>
生效时间	
时间范围	
	道田

#### 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	选择全部已加密数据或者自定义范围,默
	自定义范围二选一	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,

		己添加的加密对象范围的子集			
数据库账	否	选择数据库账号,支持选择多个			
号					
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			

| aaa(172.16.8.159:1521)的"读保护"例外规则-编辑规则

へ 基本信息	
• 规则名称	342793
规则状态	○ 余用 ○ 繁用
へ数据范围	
选择方式	● 全部已加密数据 ○ 自定文范围
へ访问来源	
数据库账号	等于 v Outln × SysSumf × DBSNMP × v
来源IP	<b>谷子</b> > 満施入実施P
へ 生效时间	支持輸入 単个中、中료(範円字列) 表示中范围, 使用语号()分Ⅰ%, 如: 172.16.1.00(単个中),172.16.2.101-172.16.2.120(甲径),172.16.10.0/24(甲字列)
时间范围	
	<b>安</b> 次 <b>取</b> 消

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。

选择数据范围			×
请选择表范围 请输入关键字			已选的表 (12) wy_test - all_type_tb wy_test9 - Teacher
☑ 表ID 库/模式	表	字段范围	wy_test9 - Course
☑ 93907 wy_test	all_type_tb	◎ 全部 ○ 自定义	wy_test8 - Student
☑ 93775 wy_test9	Teacher	● 全部 ○ 自定义	wy_test8 - SC wy_test8 - Course
☑ 93772 wy_test9	Course	◎ 全部 ○ 自定义	wy_test1 - Course
☑ 93771 wy_test8	Teacher		wy_test - customer_info_dest
✓ 93770 wy_test8	Student	◎ 全部 ○ 自定义	wy_test - customer_info wy_test - Teacher
☑ 93769 wy_test8	SC	◎ 全部 ○ 自定义	
☑ 93768 wy_test8	Course	◎ 全部 ○ 自定义	
93711 wy_test1	Course	全部     自定义	
☑ 93710 wy_test	test_table_0	◎ 全部 ○ 自定义	
☑ 93709 wy_test	customer_info_dest	◎ 全部 ○ 自定义	
☑ 93708 wy_test	customer_info	◎ 全部 ○ 自定义	
2 93707 wy_test	Teacher	◎ 全部 ○ 自定义	
	Total 15 12/page V	1 2 > Go to 1	
			提交 取消

图 4-79 选择数据范围-全部

へ 数据范围					
选择方式	○ 全部已刻密数据 ● 自定义范围				
法拜范围	库-模式	8	学段	操作	
	wy_test	all_type_tb	×	HIRS	
	wy_16609	Teacher		INTS	
	wy_test9	Course		BURS .	
	wy_test8	SC	•	BHFS	
	wy_test	customer_info		1000 ER103	
	wy_test	Teacher		1018	
	wy_test	Student		IH13	
		3	i#20		

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。
选择	数据范围								×
请选择	表范围 (入关键字							已透的表 (8) wy_test-all_type_tb wy_test9 - Teacher	
	表ID	库模式		表		字段范围		wy_test9 - Course wy_test8 - Teacher	
	93907	wy_test		all_type_tb		● 全部	○ 自定义	wy_test8 - Student	
~	93775	wy_test9		Teacher		● 全部	○ 自定义	wy_test8 - Course	
	93772	wy_test9		Course		○ 全部	● 自定义	wy_test - Teacher	
	93771	wy_test8		Teacher		○ 全部	● 自定义		
~	93770	wy_test8		Student		○ 全部	● 自定义		
	93769	wy_test8		SC		● 全部	○ 自定义		
<b>~</b>	93768	wy_test8		Course		● 全部	○ 自定义		
	93711	wy_test1		Course		● 全部	○ 自定义		
	93710	wy_test		test_table_0		<ul> <li>全部</li> </ul>	○ 自定义		
	93709	wy_test		customer_info_dest		● 全部	○ 自定义		
	93708	wy_test		customer_info		● 全部	○ 自定义		
	93707	wy_test		Teacher		● 全部	○ 自定义		
			Total 15	12/page $\vee$	< 1	2 >	Go to 1		
								下一步	取消

图 4-81 选择数据范围-自定义

					已选的字段(2)	
请输入关	长键字				wy_test - SC - Cld	
-	字段ID	库/模式	表	字段	wy_test - SC - SId	
	3674313	wy_test	SC	score		
	3674312	wy_test	SC	Cld		
<b>2</b> 3	3674311	wy_test	SC	SId		
			Total 3 12/page	$\checkmark$ ( 1 ) Go to 1		

图 4-82 选择数据范围-自定义

へ 数据范围				
选择方式	○ 全部已加密数据 🔹 自定	2义范围		
选择范围	库/模式	a	字段	操作
	wy_test9	Teacher		删除
	wy_test	all_type_tb	geometrycollection_f.tinytext_f	##R2
	wy_test	customer_info	*	删除
	wy_test	all_type_tb	varbinary_f,tinyint_f	删除
		2	pto	

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:

<ul> <li>⑦ 帮助提示</li> <li>本页面用于设置数据蒸需进行完整</li> <li>☑ 总是显示</li> </ul>	生保护的对象,即保护宇颈。设置后	,这些字段在写入数据时,系统	会自动调用数字签名算法进行签名6	<b>朵护。并能够通过</b> 验签操作来	识别数据是否被非法	<b>游改。</b>	×
请输入库/模式/表名关键字 +	③ 该表采用"更新原表数据"	方案处理存量数据					
hhh • 中文表名	请输入关键字	秋态	查询 重置				<b>添加保护对象</b> 批量操作
		字段	签名算法	保护状态	验证状态	验证时间	操作
	hhh•中文表名	中文	SHA256 🔑	<ul> <li>已签名</li> </ul>	◎ 未验证	12	验证 撤销 历史
	hhh · 中文表名	abc	SHA256 🔑	<ul> <li>已签名</li> </ul>	◎ 未验证		验证 撤销 历史
					4	共 2 条 12条/页	< 1 > 前往 1 页

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。

<ul> <li>⑦ 帮助提示</li> <li>本页面用于设置数据蒸需进行完整</li> <li>☑ 总是显示</li> </ul>	性保护的对象,即保护字段。说	置后,这些字段在写入数据时,系统	会自动调用数字签名算法进行签名	保护。并能够通过验签操作来	识别数据是否被非法慧	1改。	
请输入库/模式/表名关键字 🕂	请输入关键字	状态 >	查询 重置				添加保护对象 批量操
	□ 表	字段	签名算法	保护状态	验证状态	验证时间	操作
				暂无数据			
					Ŧ	0条 12条/页	◇ 〈 1 〉 前往 1

	添加	表						×
(	请输入	入关键字					已选的表(2)	
		表ID	库/模式		表		dbo • spt_fallback_usg dbo • bbb	
		1088	dbo		spt_monitor			
		1087	dbo		test2			
		1086	dbo		MSreplication_options			
		1085	dbo		中文			
		1084	dbo		yesok			
		1083	dbo		testbb			
		1082	dbo		аааааа			
		1081	dbo		bbb			
		1080	dbo		spt_fallback_usg			
		1079	dbo		spt_fallback_dev			
		1078	dbo		spt_fallback_db			
				共11条 12条/页	✓ < 1 > 前往	1 页		
								下一步取消

图 4-86 完整性保护-添加表

图 4-87 完整性保护-添加表

添加表			×
请输入关键	<del>7</del>		
表ID	库/模式	表	存量数据处理方案
1088	dbo	spt_monitor	更新原表数据
1087	dbo	test2	复制表并迁移数据
			共2条 12条页 > (1) 前往 1 页
			上一步 提交 取消

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。

<ul> <li>ss (172.16.8.18:1433) - 管理完</li> <li>② 帮助提示</li> <li>本页面用于设置数据涵凿进行完整(</li> <li>&gt; 总是显示</li> </ul>	整性保护对象 ⑦ 生保护的对象,即保护字段。说	置后,这些学段在写入数据时,系统	会自动调用数字签名算法进行签名6	R护。并能够通过验查操作来	识别数据是否被非法篡	改。		×
请输入库/模式/表名关键字	③ 该表采用"更新原表数" 请输入关键字	■ 方案处理存量数据       状态     ∨	查询 重置				潭加保护对象	批量操作
	□ <sub>表</sub>	字段	签名算法	保护状态	验证状态	验证时间	操作	
				暂无数据				
					共	0条 12条/页	◇ 〈 1 〉 前往	1页

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。

则密与访	回控制网天			A SecAdmin ∨
添加	保护对象			×
所属表	€: dbo•bbb			已选的保护对象 (2)
请输	认关键字			CARD
	字段ID	字段	受限原因	DH
	4410	CARD		
	4409	DH	(*),	
	4408	ID		
			共3条 12条页 ∨ 〈 1 〉 前往 1 页	
				下一步

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。

122-3 WINDEE BA	M 大		⊖ secauniii ~
添加保护对	象		×
所属表: dbo•b	bb		
默认加密算法:	SHA256 $\vee$		
请输入关键字			
字段ID	字段	加密算法	
4410	CARD	SHA256 🗸	
4409	DH	默认 🔗	
		共 2 条 12条/页 × < 1 >	前往 1 页
		上一步 提交并保护	提交取消

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。

		默认	Ŷ
提示	确定西签名亿拉汶此数据吗?		×
	WAE 安立百 体扩 丛 二 和 16 号:	确定	取消上一

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。

<ul> <li>● 帮助提示</li> <li>本页面用于设置数据源需进行:</li> <li>✓ 总是显示</li> </ul>	完整性保护的对象,即保护字段。设置	后,这些字段在写入数据时,系统	会自动调用数字签名算法进行签名	采护。并能够通过验签操作3	我识别数据是否被非法蓄	it.	
输入库/模式/表名关键字 +	0 该表采用"更新原表数据	"方案处理存量数据					
o•bbb o•spt_fallback_usg	请输入关键字	状态 ~	查询 重置				添加保护对象 批量操作
	表	字段	签名算法	保护状态	验证状态	验证时间	操作
	dbo • bbb	CARD	SHA256 🖉	<ul> <li>已签名</li> </ul>	• 未验证	2	验证 撤销 历史
	dbo • bbb	DH	SHA256 🔑	* 未签名	02	2	保护翻除历史

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:

完整	完整性保护历史										
表		dbo•bbb									
字段		CARD									
ID	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		
79	验证	已完成	成功	32.00 KB	1ms		31.25 MB/s	SecAdmin	2024-07-31 18:07:26		
78	验证	已完成	成功	32.00 KB	2ms		15.63 MB/s	SecAdmin	2024-07-31 18:07:24		
77	验证	已完成	成功	32.00 KB	3ms		10.42 MB/s	SecAdmin	2024-07-31 17:20:52		
76	签名	已完成	成功	32.00 KB	311ms		0.10 MB/s	SecAdmin	2024-07-31 17:20:13		
75	撤销签名	已完成	成功	32.00 KB	3ms		10.42 MB/s	SecAdmin	2024-07-31 17:18:23		
74	签名	已完成	成功	32.00 KB	268ms		0.12 MB/s	SecAdmin	2024-07-31 17:18:20		
73	撤销签名	已完成	成功	32.00 KB	32ms		0.98 MB/s	SecAdmin	2024-07-31 17:18:18		
72	签名	已完成	成功	32.00 KB	377ms		0.08 MB/s	SecAdmin	2024-07-31 17:04:27		
71	撤销签名	已完成	成功	32.00 KB	17ms		1.84 MB/s	SecAdmin	2024-07-31 17:03:26		
69	签名	已完成	成功	32.00 KB	333ms		0.09 MB/s	SecAdmin	2024-07-31 17:01:51		
						共10条	12条/页 >>	< 1	前往 1 页		
									关闭		

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:

策略管理 /	访问控制						0
访问控	制						
请输入关键	17 <b>(</b> )	R					
ID	数据源名称	服务类型	地址编口	已启用观明数量	未启用规则数量	控制模式	操作
6	172.16.12.163	Oracle	172.16.12.163:1521	0	0	◎ 未开启	管理规则 切换模式
5	233	MySQL	3.2.5.6:22	0	0	* 未开启	管理规则 切换模式
4	1	MySQL	172.16.23.200:3306	0	0	* 未开启	管理规则 切换模式
3	aaa	Oracle	172.16.8.159:1521	0	0	* 未开启	管理规则 切换模式
2	2.2.2.2	Oracle	2.2.2.2:111	0	0	* 未开启	管理规则 切换模式
1	1.1.1.1	MySQL	1.1.1.1:3306	0	0	* 未开启	管理规则 切换模式
						Total 6 12/page V	1 Go to 1

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。

策略管理 / 访问控制	el			
┃ 数据源访问报	切换控制模:	£	×	
请输入关键字	ID	3		
ID 数	数据源	172.16.12.162 (172.16.12.162:3306)		粮式
7 11	控制模式	○ 关闭   ◎ 阻斷   ○ 放行		开启
3 17.			19:28	Ħ
1 17.			J&X 4X/H	开启
			Total 3	12/page 🗸 🤇

#### 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。



### 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:

策略管理 / 访问招	2制 / 访问控制规则				
dm8-8.188	(172.16.8.188:5236)	的访问控制规则 🔤			
<ul> <li>● 帮助提示</li> <li>开启访问控制</li> <li>■ 总是显示</li> </ul>	防御后,若腔脉方式为"阳 示	新",系统将和新所有命中规则的访问请求,放行其他未命中的请求;若打	2财方式为"放行",系统将放行所有命中规则的访问请求,用时	后其他未命中的请求。	×
请输入关键字	状态	◆ 一 査询     重置			(投動構式 制制 切換) 深加規則 社会操作
Пір	规则名称	状态	(6) JE (14) (14)	更新时间	操作
□ <i>1</i>	hell	• 未应用	2023-07-04 11:37:10	2023-07-04 11:37:10	此用 放着 编辑 删除
5	test	<ul> <li>已応用</li> </ul>	2023-07-03 14:58:52	2023-07-03 14:58:53	停用 查看 编辑 删除
				То	tal 2 12/page $\checkmark$ < 1 > Go to 1

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

172.16.12.	162(172.16.12.162:3306)的访问控制规则 - 添加规则	
* 规则名称		
* 规则状态	(	
* 数据库账号	等于 ~ Iroot × test ×	Ŷ
	THE V INCEPT V HODATE V	×

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。

开启访问控 一 总是显	剧功能后,若控制。 示	方式为"阻断",1	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≉	多中的证
请输入关键字		状态	提示	×	(控制模式 開新 )	加換 添加	印规则
ID ID	规则名称		••••••••••••••••••••••••••••••••••••••		更新时间	操作	
6	333				2022-11-25 15:08:47	启用	查看
5	222		* 未启用	2022-11-25 15:05:38	2022-11-25 15:05:38	启用	查看

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:

alikati i Mel	STAR   EN-DEMONIA	
172.16.12	162 (172 16 12 162 3306)的话问控制规则 - 查看规则	
1080	4	
ALC: N	test	
MBN 6	* 15.0 M	
第11天型	₩F SELECT	
REARC	BT root	
创建村同	2022-11-24 18 25 20	
更新时间	2022-11-24 19 33 53	
	200	

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

172.16.12.1	162(172.16.12.162:3306)的访问控制规则 - 编辑规则		
规则名称	333		
规则状态	用語 ○ 用意		
数据库账号	本等チ ∨ test × root ×	v.	
144.01-31:31	本装手 V UPDATE × SFLECT ×	~	

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。

	北东	提示	×	( 控制模式 服新	tititika i in titititika in titititi	
				C straties a train	and a land	
ID	规则名称	100 C	70.31	更新时间	操作	
6	333		備以取消	2022-11-25 15:08:47	启用	查看 编
5		<ul> <li>未启用</li> </ul>	2022-11-25 15:05:38	2022-11-25 15:05:38	白田	香着 折

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:

用户与角色	/ 用户管理							0
用户列	表							
<ul> <li>● 相助 在本</li> <li>■</li> </ul>	提示 页面可以管理安全操作员、 总是显示	自定义角色和默认用户,可以	以將默认用户授权为安全操作	员或自定义的角色,也可以	lonee.			
用户名笑	健宇	查询 里質						
ID	用户名	所属角色	是否內實	状态	UKEY	最近登录时间	的建叶间	操作
4	test_user	test_role	否	<ul> <li>正常</li> </ul>	<ul> <li>未绑定</li> </ul>	2023-06-29 17:05:13	2023-06-29 17:03:11	授权 查看 编辑
1	SecAdmin	安全管理员	是	• 正常	<ul> <li>未绑定</li> </ul>	2023-07-04 11:15:48	2023-06-29 10:28:40	<b>\$</b> 6
							Total 2 12/page	$\sim$ ( 1 $\rightarrow$ Go to 1

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。

用户4	5角色 / 用户管理							
一用	1户列表	切换用户	角色	×				
0	帮助提示 本页面可以添加或编辑系 2 总是显示	用户ID	6					
用户	9名关键字	用户名	test003					
ID	用户名	当前角色	默认用户			操作		
9	test0006	切换角色	默认用户 ジ			查看	编辑	
8	Izwtest	重置密码				查看	编辑	
6	test003 test001	* 密码	请输入密码			授权	查看 编辑	编
1	SecAdmin	* 确认密码	请再次输入密码			查看		
		_		提交 取消	1	2/page 🗸		1

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:

查看用户		×
用户ID	4	
用户名	test_user	
所属角色	test_role	
真实姓名	2	
手机号码	4	
电子邮箱	2	
状态	• 正常	
UKEY	• 未绑定	
是否内置	否	
登录次数	5	
最近登录IP	172.16.2.32	
最近登录时间	2023-06-29 17:05:13	
创建时间	2023-06-29 17:03:11	
更新时间	2023-06-29 17:05:13	
		关闭

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
		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
密码	否	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
		填写手机号,长度 11 个字符。且应 13、
手机号	否	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。

用户与	前角色 / 用户管理				
Ⅰ用	户列表	编辑田户		×	
0	帮助提示 本页面可以添加或编辑 ☑ 总是显示	用户ID	9		
用户	9名关键字	用户名	test0006		
ID	用户名	密码	留空表示不修改密码		操作
9	test0006	确认密码	留空表示不修改密码		3 查看
8	Izwtest	所属角色	test0006		查看
6	test003	真实姓名	请输入真实姓名		查看
5	xqssss	手机号码	请输入手机号码		授权
1	SecAdmin	电子邮箱	请输入电子邮箱		· 查看
		状态	正常		6 12/page 🗸
				提交 取消	

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。

主菜单	分类	功能说明
		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
	业务基础数据统计	当前加密表数、未加密表数统计
首页		最新加密对象信息
		当前加密卡信息和状态
	其他数据统计	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
	系统日志	查看系统日志
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
	修改资料	修改个人资料
1`入屮心 	修改密码	修改个人密码

审计管理包含内容见下表:

# 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:

用户列	表 ==							
⑦ 帮助 在本	提示 向面可以管理审计操作员和 总是显示	BURP. SCREURPI	8数为审计操作员,也可以取	onese.				
用户名关	97	查询 重富						
ID	用户名	所属角色	是否内置	状态	UKEY	最近登录时间	创建时间	發作
6	ujhioyhl536	默认用户	*	• 禁用	<ul> <li>未绑定</li> </ul>		2023-07-04 11:46:24	授权 查看 编辑
5	43TFGHYYH	默认用户	西	<ul> <li>正常</li> </ul>	• 未绑定		2023-07-04 11:46:09	授权 查看 编辑
	hlllrrr	默认用户	否	<ul> <li>正常</li> </ul>	<ul> <li>未绑定</li> </ul>		2023-07-04 11:45:55	授权 查看 编辑
4					and the second	2022 02 04 11 12 02		

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。

用户	5角色 / 用户管理									
	用户列表	切换用户	角色			×				
e	<ul> <li>林明健小</li> <li>本页面可以添加或编辑系</li> <li>✓ 总是显示</li> </ul>	用户ID	6							
开	的名关键字	用户名	test003							
н	0 用户名	当前角色	默认用户					操作		
9	test0006	切换角色	默认用户 🗸					查看	编辑	
8	Izwtest	重置密码						查看	编辑	
6	test003	* 密码	诸输入密码					授权	查看	编辑
4	test001	* 确认密码	请再次输入密码					查看	编辑	
	Jechanin							24.18		
					提交取消		12/page			1

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:

查看用户			×
用户ID	6		
用户名	ujhioyhl536		
所属角色	默认用户		
真实姓名	ā.		
手机号码	5		
电子邮箱	<u>a</u>		
状态	用恭●		
UKEY	• 未绑定		
是否内置	否		
登录次数	0		
最近登录IP			
最近登录时间	ā.		
创建时间	2023-07-04 11:46:24		
更新时间	2023-07-04 11:46:25		
			关闭

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
		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
密码	否	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。

用户	与角色 / 用户管理				
1 /	用户列表	编辑用户		×	
0	<ul> <li>帮助提示</li> <li>本页面可以添加或编辑</li> <li>✓ 总是显示</li> </ul>	用户ID	9		
Æ	庐名关键字	用户名	test0006		
H	) 用户名	密码	留空表示不修改密码		操作
9	test0006	确认密码	留空表示不修改密码		• 查看
8	Izwtest	所属角色	test0006		查看
6	test003	真实姓名	请输入真实姓名		查看
5	xqssss test001	手机号码	请输入手机号码		投权查看
1	SecAdmin	电子邮箱	请输入电子邮箱	2	查看
		状态	正常		5 12/page 🗸
				提交取消	

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:

系统信息 / 担	系统改变 / 操作日本										
系统日志	系统日志列表										
日本印成內容关键字 查询 重赏 高级搜索											
ID	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	操作				
13167	使用用户名"Auditor"登录了系统	登录系统	成功	Auditor	172.16.0.5	2022-09-23 11:22:04	查看				
13166	"SysAdmin"退出了系统	退出系统	成功	SysAdmin	192.168.10.20	2022-09-23 11:21:52	查看				
13165	"SysAdmin"退出了系统	退出系统	成功	SysAdmin	172.16.0.5	2022-09-23 11:21:51	查看				
13164	禁用了用户'testtest'	禁用用户	成功	SysAdmin	192.168.10.20	2022-09-23 11:21:18	查看				
13163	發用用户"Sec.Admin"失败	禁用用户	失败	SysAdmin	192.168.10.20	2022-09-23 11:20:46	查看				
13162	"SecAdmin"遐出了系统	退出系统	成功	SecAdmin	172.16.2.62	2022-09-23 11:19:25	查看				
13161	"SecAdmin"遐出了系统	退出系统	成功	SecAdmin	172.16.2.62	2022-09-23 11:18:23	查看				
13160	修改用户"test001"的资料失败	修改用户资料	失败	SysAdmin	192.168.10.20	2022-09-23 11:18:15	查看				
13159	修改用户"test001"的资料失败	修改用户资料	失败	SysAdmin	192.168.10.20	2022-09-23 11:18:14	查看				
13158	修改用户*test001*的资料失败	修改用户资料	失敗	SysAdmin	192.168.10.20	2022-09-23 11:18:14	查看				
13157	修改用户"test001"的资料失败	修改用户资料	失败	SysAdmin	192.168.10.20	2022-09-23 11:18:14	查看				
13156	修改用户"test001"的资料失败	修改用户资料	失败	SysAdmin	192.168.10.20	2022-09-23 11:18:12	查看				

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:

查看日志详情		×
ID	216	
日志描述	使用用户名"Auditor"登录了系统	
操作类型	登录系统	
操作结果	成功	
操作人	Auditor	
操作客户端IP	172.16.2.79	
操作时间	2023-07-04 11:47:01	
		关闭

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。

氯純慈悲 / 銀作日本											
■ 系统日志列表											
关键字	日本10或描述内容关键字	操作人	请选择操作人			摄作春户询P	国际入资户到印	B 今週 P			
操作类型	遺伝経過作用型	操作结果	诸远择操作结果			10/13110	) 开始时间 -	结束时间			
100 E											
ID	日志描述		操作类型	操作结果	操作人	操作客户编P	操作时间	跟作			
376	使用用户名"Auditor"登录了系统		發展系統	成功	Auditor	172.16.2.79	2022-09-26 16:57:27	27			
375	使用用户名"SysAdmin"登录了系统		登录系统	成功	SysAdmin	172.16.2.56	2022-09-26 16:52:27	27			
374	"SysAdmin"退出了系统		退出系统	超功	SysAdmin	172.16.2.56	2022-09-26 16:52:17	22			
373	使用用户后"SysAdmin"登录了系统		登录系统	成功	SysAdmin	172.16.2.56	2022-09-26 16:49:20	22			
372	锁用密钥"B6BA270D4F4F9B5B29241A61D764F9E9"失敗		领用密钥	失敗		172.16.2.56	2022-09-26 16:47:57	22			
371	数据课 172.16.8.1681的加密对象"public Luser"加密成功		执行加密	虚助	SecAdmin	172.16.2.54	2022-09-26 16:43:44	22			
370	使用了密钥'443EA35C7CF651534237F90FB19E78E4'		领用密钥	成功		127.0.0.1	2022-09-26 16:43:44	22			
369	数据源*172.16.8.168*的加速对象*public.t_user*开始加速		自动加密	成功	SecAdmin	172.16.2.54	2022-09-26 16:43:43	22			
368	数据源*172.16.8.168*的加速对象*public t_user*还原点功		执行还原	成功	SecAdmin	172.16.2.54	2022-09-26 16:43:39	22			
367	数据源*172.16.8.168*的加密对象*public.t_user*开始还原		启动还原	成功	SecAdmin	172.16.2.54	2022-09-26 16:43:38	22			
366	数据源:172.16.8.1681的加密对象;public.t_user1加密共致		执行加密	失败	SecAdmin	172.16.2.54	2022-09-26 16:41:48	22			
365	使用了图用'443EA35C7CF651534237F90FB19E78E4'		初用密钥	成功		127.0.0.1	2022-09-26 16:41:48	22 22			

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。