数据安全专区

数据库安全网关用户指南

天翼云科技有限公司

目录

1 快速入门

1.1 产品主要功能

1.1.1 数据识别

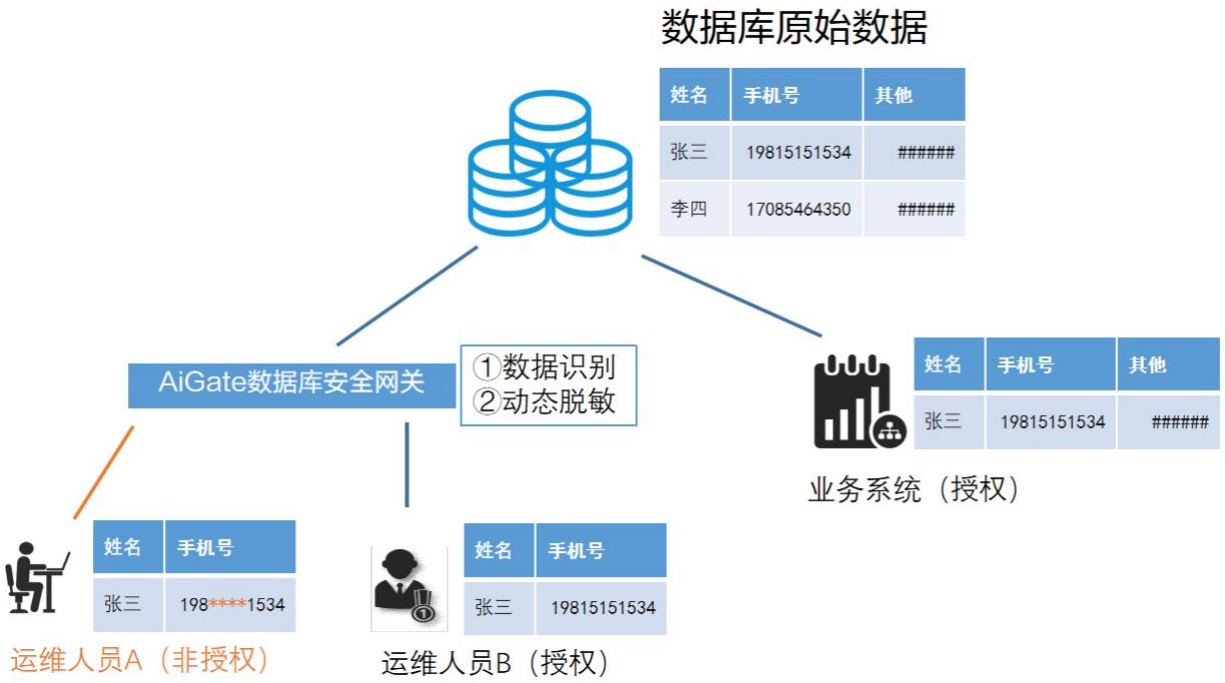
数据库安全网关支持多种关系型数据库、国产数据库、大数据组件、NoSQL 等多类型、多环境下的数据精准识别。支持通过对数据库的扫描，定位常见的敏感数据类别（如身份证、手机号、邮箱等），结合定义的数据级别，实现数据的分级分类功能。基于分级分类结果，支持细粒度的动态脱敏与安全规则配置。

1.1.2 访问控制

数据库安全网关通过对数据访问主、客体的组合，辅以访问行为与结果的配置，实现精细化访问控制。可针对多种复杂或特定业务场景自定义安全规则、信任规则等，同时内置多种常见的数据库攻击规则，可以有效防止对数据库的攻击、避免误操作行为造成的数据库安全隐患。

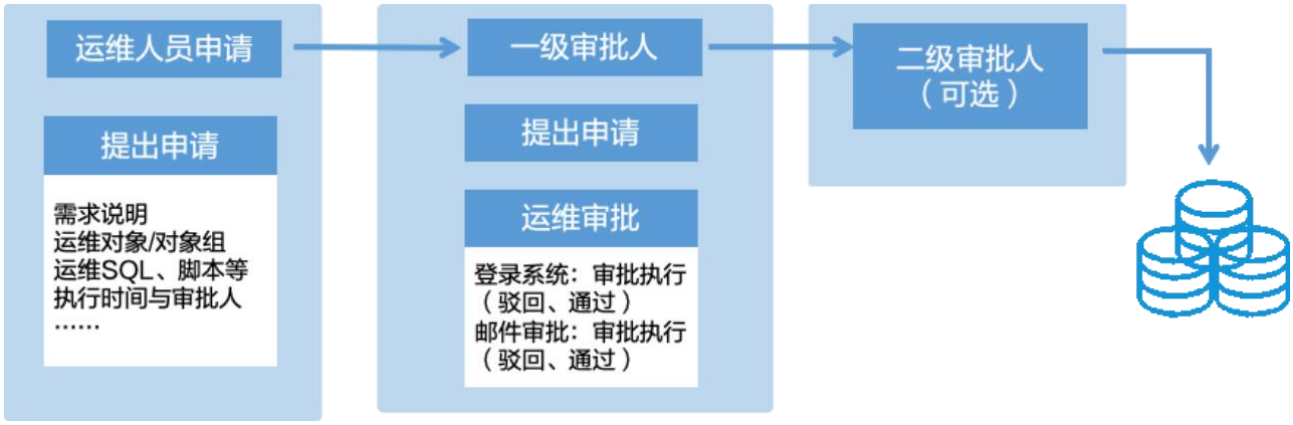
1.1.3 动态脱敏

数据库安全网关通过解析实时数据库访问流量，对 SQL 进行改写，在不影响运维人员正常操作的前提下，提供安全、符合规定的脱敏数据。且内置多种常见脱敏算法（如替换、截断、掩码、随机等），实现用户数据的“可用不可见”，有效降低数据泄露风险。



1.1.4 运维审批

为避免运维过程中因账号管理混乱、操作不透明等不合规现象导致的数据泄露，以及高危操作（如 Drop Table、Truncate Table）带来的巨大安全风险，运维人员需提交临时授权工单，经多级安全审批人逐级审批后方可进行操作。审批人可通过系统或邮件进行审批，确保操作流程的公开、透明和合规，保障数据库操作安全。



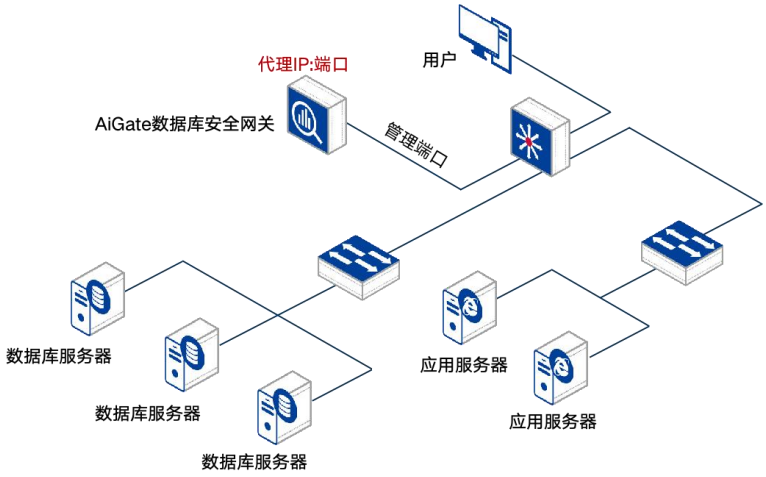
1.1.5 高可用及稳定性

- 支持双机热备，实现策略的实时或定期同步，保证业务连续性。
- 采用软/硬件 bypass 保证业务稳定性，系统出现问题时自动放通业务流量，不影响业务系统正常使用。

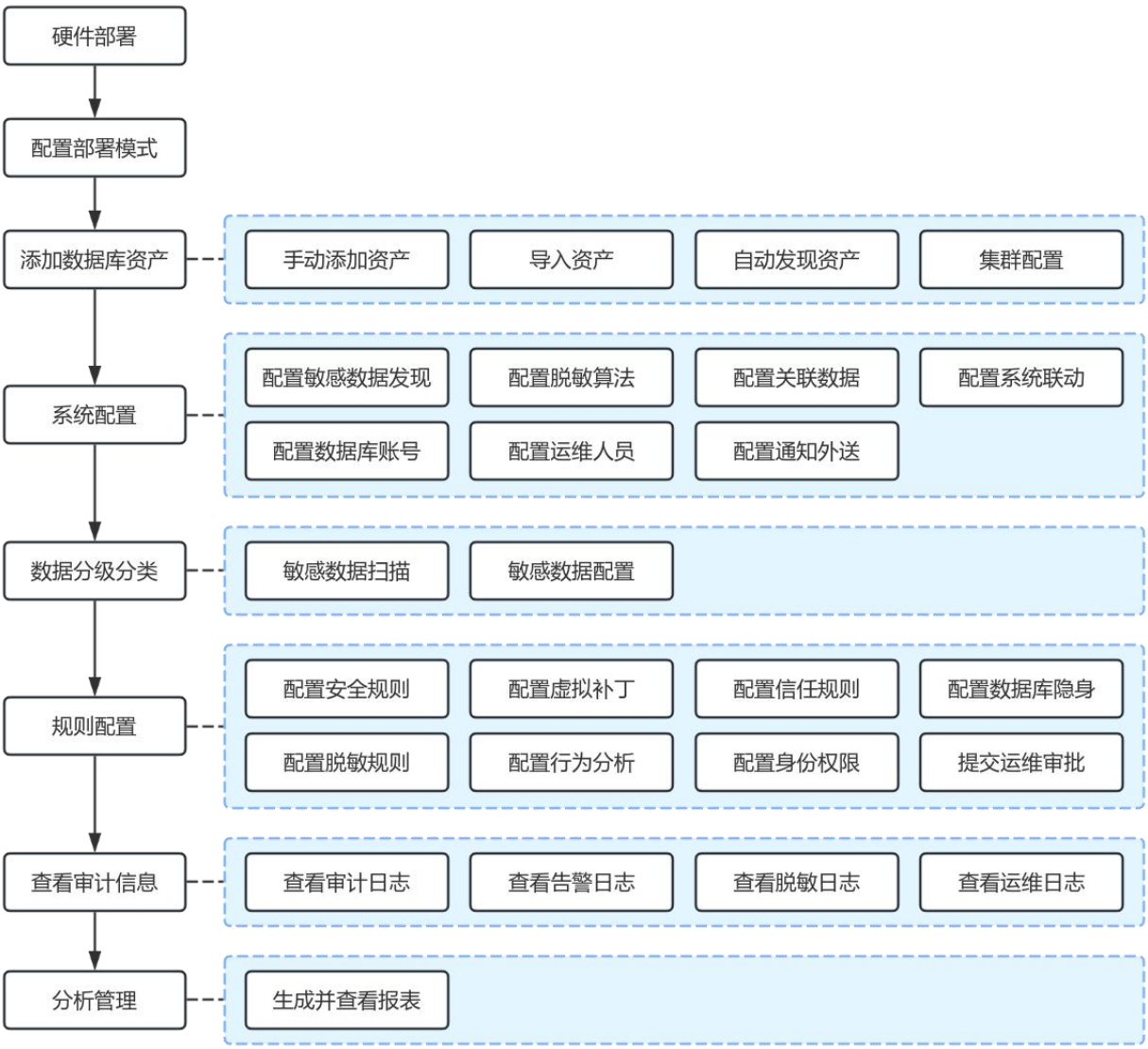
1.2 典型部署模式

1.2.1 反向代理

这种模式的网络架构设计简单，且无需对原有数据库服务器的物理网络拓扑环境进行任何改动。对于用户而言，使用数据库安全网关仅需简单地修改原本访问数据源配置连接串中的 IP 和端口，替换为数据库安全网关的代理 IP 与代理端口。部署方案，如下图所示：



1.3 主要业务流程



1. 配置部署模式：根据网络部署，在系统上配置对应的模式。请参见部署模式。

2. 添加数据库资产：添加系统需要防护的数据库，请参见资产管理。

3. （可选）系统配置：在使用审计、访问控制、运维审批功能前，您可个性化地进行系统特征、系统联动、通知外发等系统设置。

   (1) 配置敏感数据发现规则，请参考敏感数据发现；

   (2) 配置脱敏算法，请参考脱敏算法；

   (3) 配置关联数据（IP 组、对象组等），请参考关联数据；

(4) 配置系统联动（数据分类分级、AiTrust），请参考系统联动；

(5) 配置数据库账号/运维人员，请参考安全运维；

(6) 配置通知外送（告警、日志），请参考通知外送；

4. 数据分类分级：对用户数据库服务中的元数据进行分类分级，详情请参见敏感数据。

5. 规则配置：配置具体的策略，后续系统将会根据配置的策略对用户操作进行审计与访问控制。

(1) 配置安全规则，请参考安全规则；

(2) 配置虚拟补丁，请参考虚拟补丁；

(3) 配置信任规则，请参考信任规则；

(4) 配置数据库隐身，请参考数据库隐身；

(5) 配置脱敏规则，请参考脱敏规则；

(6) 配置行为分析，请参考行为分析；

(7) 配置身份权限，请参考身份权限；

(8) 使用运维审批，请参考运维申请与审批；

6. 查询分析：查看和分析审计日志、告警信息、运维日志、脱敏日志和在线会话，以便及时发现并处理潜在的安全风险，请参见查询分析。

7. 分析管理：针对日志信息，可进行报表生成或订阅等操作，请参见报表中心。

2 Web 配置页面简介

系统提供简便的 Web 配置页面，主要包含三个部分：1.产品名称；2.功能菜单；3.辅助功能；4.操作区。

序号	名称	说明
1	产品名称	显示当前系统的产品名称及 logo。
2	功能菜单	以不同的角色视角提供了各类管理功能的配置入口，方便用户根据实际需要进行切换，当前登录用户拥有的菜单权限同权限管理。
3	辅助功能	提供各类辅助功能的配置入口，包括用户信息、修改密码、退出登录、查看版本信息等。
4	操作区	该区域主要用户信息展示以及相关功能的配置。

左侧功能菜单来可以进行展开和收起，收起来时有更大的区域来展示操作区内容，以便用户更好地浏览数据。

2.1 用户信息

将光标悬停于用户名，显示辅助功能，如下所示：

2.1.1 修改用户信息

点击进入<**我的信息**>页面后，可修改基本信息及登录选项，修改后需点击<保存>才可生效。还可创建 API 访问键（AccessKey）。

API 访问键是为第三方开发人员提供访问和调试数据库安全网关应用接口的重要凭据，由

AccessKey ID 和 AccessKey Secret 两部分组成。AccessKey ID 作为用户身份的唯一标识符，确保请求的可追溯性；而 AccessKey Secret 则是验证用户身份的密钥，其高度保密性保障了 API 访问的安全性。

配置项	说明
手机号	用户的手机号。
邮箱	用户的邮箱，例如 zhangsan@tests.com。
备注	用户的说明信息。
登录选项	可设置认证方式、登录 IP/MAC 限制和登录时间限制，具体请参考用户管理。
创建 AccessKey	点击<创建 AccessKey>，可生成用户的 AccessKey ID 和 AccessKey Secrest。

2.1.2 修改密码

在我的信息页面，点击<**修改密码**>，显示修改密码弹框。在弹出窗口内输入当前用户的密码，输入新密码并确认密码（如果启用了强密码需要符合密码强度要求），点击<确定>即可。

2.1.3 退出系统

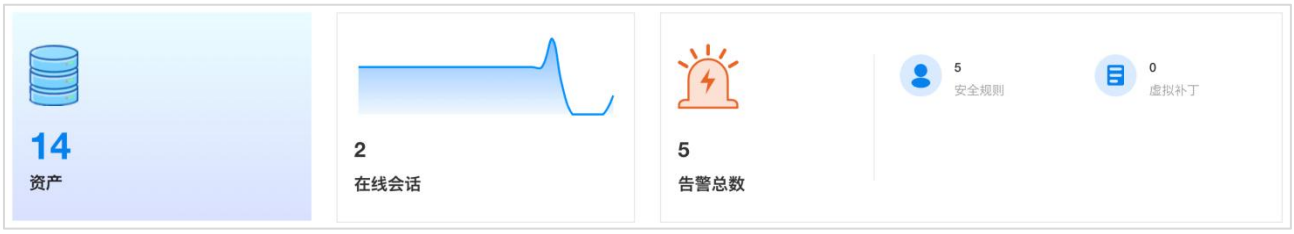
将光标悬停于用户头像，选择<退出>即可退出系统。

关闭浏览器不能使登录用户退出登录。

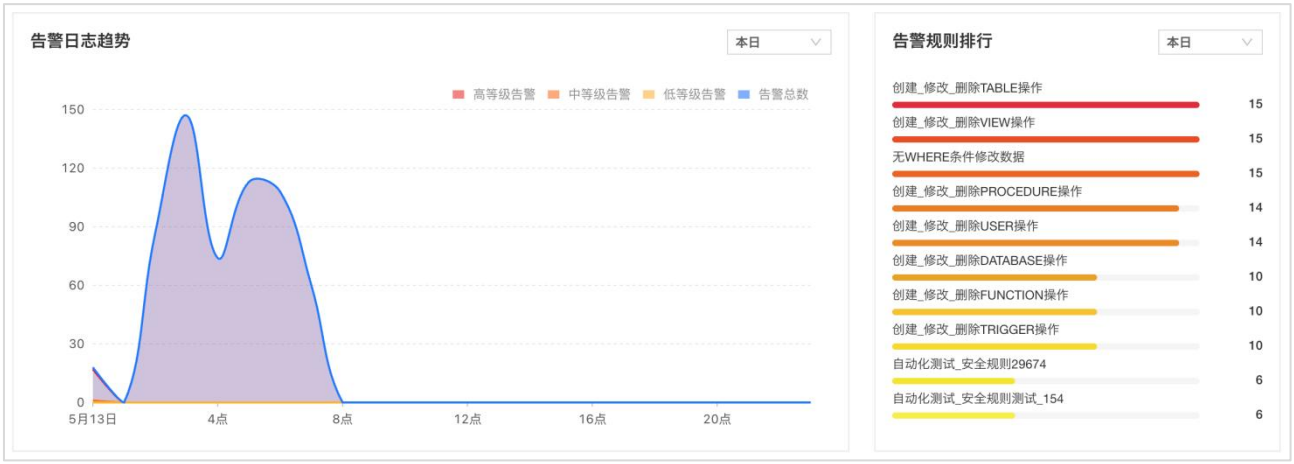
3 总览

登录系统 Web 管理平台后，默认进入总览页面。总览提供多种可视化图表，主要包括资产和在线会话信息汇总、告警趋势及统计、分级分类情况和最新脱敏日志。

- 查看资产数、在线会话数、告警总数和各规则类别触发的告警数。



◆ 查看指定时间段内的告警日志趋势和告警规则统计排行情况。



◆ 查看数据分级统计情况和最新脱敏日志情况。

4 资产

在数据库安全网关数据库安全网关中，资产是指系统需要防护和管理的数据库系统。资产管理是系统核心功能之一，涵盖了对各种数据库类型的安全监控与防护操作。

4.1 资产管理

4.1.1 手动添加资产

步骤 1. 在菜单栏选择“**资产** **资产管理**”进入**资产管理**页面，点击<**新增**>。

步骤 2. 在弹出的**新增资产**页面，填写数据库相关信息。

详细配置请参见下表：

配置项	说明
类型	选择数据库的类型，系统支持数据库类型如下： ◆ 通用数据库：Oracle(包含 RAC)、MySQL、MSSQL、Sybase ASE、DB2、Informix、Oscar、达梦(DM)、Cache、PostgreSQL、Teradata、人大金仓(Kingbase)、GBase、MariaDB、Hana、MongoDB、GaussDB、GreenPlum、TiDB、Vertica、GoldenDB、UXDB、Doris、虚谷、HifhGo、

配置项	说明
	OceanBase ◆ 大数据：HBase、Hive、Elasticsearch、Impala、Spark SQL、Clickhouse、Presto、 Tdh、 Odps ◆ 其他：HTTP、 Trino ◆ CT-cload：Teledb-MySQL、 Teledb-PostgreSQL
操作系统	设置资产所在主机的操作系统。
IP/域名	设置资产所在主机的 IPv4 或者 IPv6 或者域名。
端口	设置资产原生端口号。
代理端口	设置访问资产的反向代理端口。
防护模式	◆ 入侵检测模式：对数据库进行入侵检测，可以产生审计、告警、脱敏、运维日志，但不会对请求进行阻断和脱敏； ◆ 入侵防护模式：对数据库进行入侵检测和防护，除可以生成审计、告警、脱敏、运维日志外，还可以对请求进行阻断和脱敏。
默认数据源	默认关闭，启用后可配置连接信息进行测试连接。 默认数据源用途：1. 新增敏感数据扫描任务时，自动带出数据源信息，减少用户操作步骤；2. 安全规则配置“影响行数”维度，该规则匹配依赖资产的默认数据源；3. 运维审批任务配置自动执行 SQL 时，需依赖资产的默认数据源。
数据库名	填写数据库名。（MSSQL、DB2、PostgreSQL、UXDB 等）
用户名	填写数据库的用户名。
密码	填写数据库的密码。
测试	测试数据库的连通性。

Oracle 默认数据源配置请参见下表：

配置项	说明
SID/服务名	选择实例名或者服务名并填写。（18c 及以上版本可配置多个服务）
用户名	填写数据库的用户名。
密码	填写数据库的密码。
角色	选择 NORMAL、SYSDBA、SYSOPER。

Hive 默认数据源配置请参见下表：

配置项	说明
TLS **加密**	若 Hive 为加密传输请启用此开关，并上传证书。

PKCS 证书	上传 .pem 格式的证书（TLS 启用时必填）。
JKS 证书	上传 .jks 格式的信任库（TLS 启用时必填）。
JKS 证书密码	填写 JKS 证书的密码，支持修改（TLS 启用时必填）。
认证方式	选择 NORMAL 或者 KERBEROS。
Hive Principal	Hive 服务在 Kerberos 环境中注册的身份标识。 示例：hive@AHDB.COM
Kerberos Principal	唯一标识用户或服务的字符串，通常包括用户名、主机名和域名。 示例：hive/cdh1.ahdb.com@AHDB.com
Kerberos 配置文件	包含 Kerberos 客户端和服务器的配置信息的文件。
keytab 文件	包含加密密钥的文件。

Trino 加密配置请参见下表：

配置项	**说明**
TLS 加密	可选择启用，启用后需上传证书支持审计 TLS 加密的 Trino 数据库协议。 若启用，在客户端侧通过域名访问时，需在/etc/hosts 文件下添加一行内容，将 Trino 服务的域名映射至数据库安全网关服务器地址，如“192.168.30.100 test.trino.com”
证书	上传 pem 格式文件（使用 PKCS#12---公钥 crt 和私钥 key 的合并文件）

步骤 3. 如需要配置其他更多信息，可点击更多配置。

详细配置请参见下表：

配置项	说明
名称	自动生成，以 IP+端口+数据库类型的格式（点击更多配置可自定义名称）。
最大保存行数	取值范围 0~999，0 表示不保存返回结果，最多存储 64K。
最大保存长度	可配范围 1~64K，确保整行显示。
解密私钥	点击更多配置，导入私钥，只能通过 SSL 加密进行连接。 支持 Oracle、MySQL、MariaDB、MSSQL、PostgreSQL、Hive。
证书密码	解密私钥导入后所需密码，若无密码可不填写。

步骤 4. 点击<测试>。若信息无误，会提示测试连接成功。

步骤 5. 点击<保存>，弹出是否需要立即进行敏感数据扫描的提示框，点击<确定>，则跳转到“**资产　敏感数据　敏感数据扫描**”页面进行下一步。点击<取消>，则停留在资产管理页面。

4.1.2 导入资产

步骤 1. 在菜单栏选择“**资产　资产管理**”进入资产管理页面，点击<下载模版>。

步骤 2. 等待文件生成成功后，点击<下载>。

步骤 3. 打开下载的模版文件，并填写数据库相关信息后，保存。

资产ID(请勿修改此列)	类型与版本*	名称*	操作系统*	编码	IP*	端口*	代理端口*	最大保存行数(默认为5)	最大保存长度(单位K，默认64)	防护模式（默认为入侵检测模式）	默认数据源（默认为禁用）	SID/服务名(Oracle)	服务名	数据库名/实例名	数据库账号	数据库密码	角色	解密私钥(请勿修改此列)
	MySQL/5.7	Mysql测试资产	Linux		1.1.1.1	3306	46666				启用				root	123456		
	Oracle/11g	Oracle测试资产	Linux		2.2.2.2	1521	48888				启用	实例名		servicename	system	123456	NORMAL	

步骤 4. 返回资产管理页面，点击<导入>，上传按要求填写的模版文件即可。

4.1.3 资产发现

通过配置 IP 和端口或者 IP 段和端口范围自动发现数据库，扫描完成后，选择需要的数据库添加到资产。

步骤 1. 在菜单栏选择“**资产　资产管理　资产发现**”，点击<新增>。

步骤 2. 在弹出的新增资产发现任务框中，填写相关信息。

详细配置请参见下表：

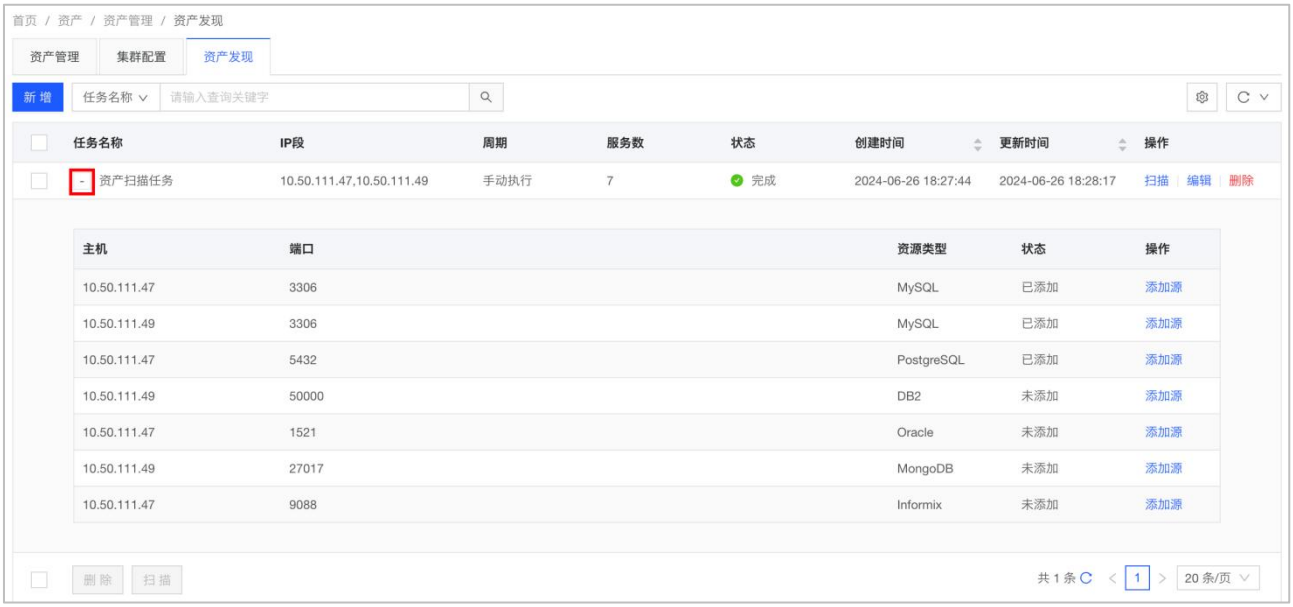
配置项	说明
任务名称	必填项，填写必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
IP 段	格式：支持多个 IP，使用逗号“,”分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20
导入	以表格的格式导入，可点击<下载模板>获取。
下载模板	点击<下载模板>，获取导入模板。
指定端口	指定要扫描的端口有效范围：1-65535，多个端口使用“,”隔开，正确格式例如：1,4-5,10（可不填写）。
周期	默认为手动执行，可选择每天、每周、每月。

步骤 3. 配置信息配置完毕后，点击<保存>，可保存成功，状态为待执行。

步骤 4. 点击<扫描>，可开始进行数据库自动发现扫描，扫描时，状态显示为执行中。

步骤 5. 扫描完毕后，状态显示为完成，并显示服务数量。

步骤 6. 点击<+>，查看已经扫描出的服务数详情。



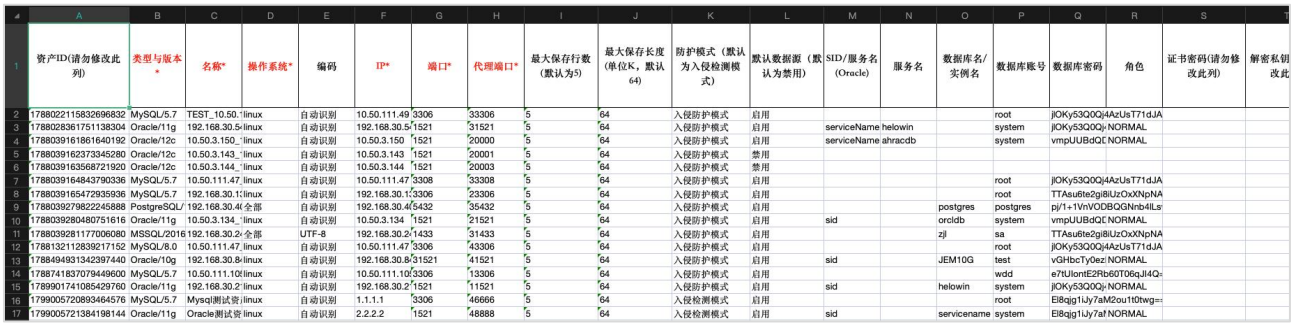
步骤 7. 点击<添加源>，弹出添加资产框，填写代理端口后，点击<保存>按钮，即可创建资产成功。

4.1.4 其他操作

在菜单栏选择“**资产　资产管理**”进入资产管理页面，您还可以进行以下操作：

- **编辑资产**：点击资产条目右侧的<编辑>按钮。在“编辑资产”页面可以修改资产的所有配置项。具体字段说明信息请参考添加资产的配置项，编辑完成后点击<保存>即可。
- **查询资产**：选择查询条件（包括资产的名称、IP、类型，以及可以选择平铺所有条件），填写查询内容，点击<🔍>即可完成单个条件或所有条件的查询。
- **设置显示列**：点击资产列表右上方的<⚙>按钮，弹出设置显示列的窗口，按实际所需勾选需要展示的列名称后，点击<确定>即可保存成功。

- **导出资产**：点击列表上方的<导出>按钮，等待文件生成成功后，点击<下载>即可。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	资产ID(请勿修改此列)	类型与版本*	名称*	操作系统*	编码	IP*	端口*	代理端口*	最大保存行数(默认为5)	最大保存长度(单位K，默认64)	防护模式（默认为入侵检测模式）	默认数据源（默认为禁用）	SID/服务名(Oracle)	服务名	数据库名/实例名	数据库账号	数据库密码	角色	证书密码(请勿修改此列)	解密私钥改此
2	1788022115832696832	MySQL/5.7	TEST_10.50.1	linux	自动识别	10.50.111.49	3306	33306	5	64	入侵防护模式	启用				root	jlOKy53Q0Qj4AzUsT71dJA			
3	1788028361751138304	Oracle/11g	192.168.30.5	linux	自动识别	192.168.30.5	1521	31521	5	64	入侵防护模式	启用	serviceName	helowin		system	jlOKy53Q0Qj	NORMAL		
4	1788039161861640192	Oracle/12c	10.50.3.150_	linux	自动识别	10.50.3.150	1521	20000	5	64	入侵防护模式	启用	serviceName	ahracdb		system	vmpUUBdQE	NORMAL		
5	1788039162373345280	Oracle/12c	10.50.3.143_	linux	自动识别	10.50.3.143	1521	20001	5	64	入侵防护模式	禁用								
6	1788039163568721920	Oracle/12c	10.50.3.144_	linux	自动识别	10.50.3.144	1521	20003	5	64	入侵防护模式	禁用								
7	1788039164843790336	MySQL/5.7	10.50.111.47_	linux	自动识别	10.50.111.47	3308	33308	5	64	入侵防护模式	启用				root	jlOKy53Q0Qj4AzUsT71dJA			
8	1788039165472935936	MySQL/5.7	192.168.30.1	linux	自动识别	192.168.30.1	3306	23306	5	64	入侵防护模式	启用				root	TTAsu6te2gi8iUzOxXNpNA			
9	1788039279822245888	PostgreSQL/	192.168.30.4(	全部	自动识别	192.168.30.4(	5432	35432	5	64	入侵防护模式	启用			postgres	postgres	pj/1+1VnVODBQGNnb4ILs			
10	1788039280480751616	Oracle/11g	10.50.3.134_	linux	自动识别	10.50.3.134	1521	21521	5	64	入侵防护模式	启用	sid		orcldb	system	vmpUUBdQE	NORMAL		
11	1788039281177006080	MSSQL/2016	192.168.30.2(	全部	UTF-8	192.168.30.2(	1433	31433	5	64	入侵防护模式	启用			zjl	sa	TTAsu6te2gi8iUzOxXNpNA			
12	1788132112839217152	MySQL/8.0	10.50.111.47_	linux	自动识别	10.50.111.47	3306	43306	5	64	入侵防护模式	启用				root	jlOKy53Q0Qj4AzUsT71dJA			
13	1788494931342397440	Oracle/10g	192.168.30.8	linux	自动识别	192.168.30.8	31521	41521	5	64	入侵防护模式	启用	sid		JEM10G	test	vGHbcTy0ez/	NORMAL		
14	1788741837079449600	MySQL/5.7	10.50.111.10(	linux	自动识别	10.50.111.10(	3306	13306	5	64	入侵防护模式	启用				wdd	e7tUlontE2Rb60T06qJI4Q=			
15	1789901741085429760	Oracle/11g	192.168.30.2	linux	自动识别	192.168.30.2	1521	11521	5	64	入侵防护模式	启用	sid		helowin	system	jlOKy53Q0Qj	NORMAL		
16	1799005720893464576	MySQL/5.7	Mysql测试资	linux	自动识别	1.1.1.1	3306	46666	5	64	入侵检测模式	启用				root	El8qjg1iJy7aM2ou1t0twg==			
17	1799005721384198144	Oracle/11g	Oracle测试资	linux	自动识别	2.2.2.2	1521	48888	5	64	入侵检测模式	启用	sid		servicename	system	El8qjg1iJy7aM	NORMAL		

- **删除资产**：点击资产条目右边的<删除>，或是选中资产列表前方的复选框，点击列表下方的<删除>。弹出二次确认窗口，点击<确认>即可。
- **资产的规则配置**：点击资产条目右边的<规则配置>，跳转到“**规则配置　安全规则　规则启用**”页面，可对该资产启用安全规则；有关规则配置的更多信息，请参考规则配置。

4.2 敏感数据

4.2.1 敏感数据扫描

若库、表、字段的名称或类型发生改变，请及时对所属资产重新扫描，否则容易造成您配置的部分规则失效。

4.2.1.1 数据库安全网关自主扫描

数据库安全网关自主扫描通过配置资产的数据库连接信息，自动获取数据库中的元数据（如库、表、字段等），并对这些数据进行分级和分类。

在数据库安全网关开始扫描前，您可以选择性的在“**规则配置　敏感数据发现**”页面自定义一些敏感数据的发现规则，这将丰富扫描出的敏感数据类型。自定义发现规则步骤具体请参考敏感数据发现规则。

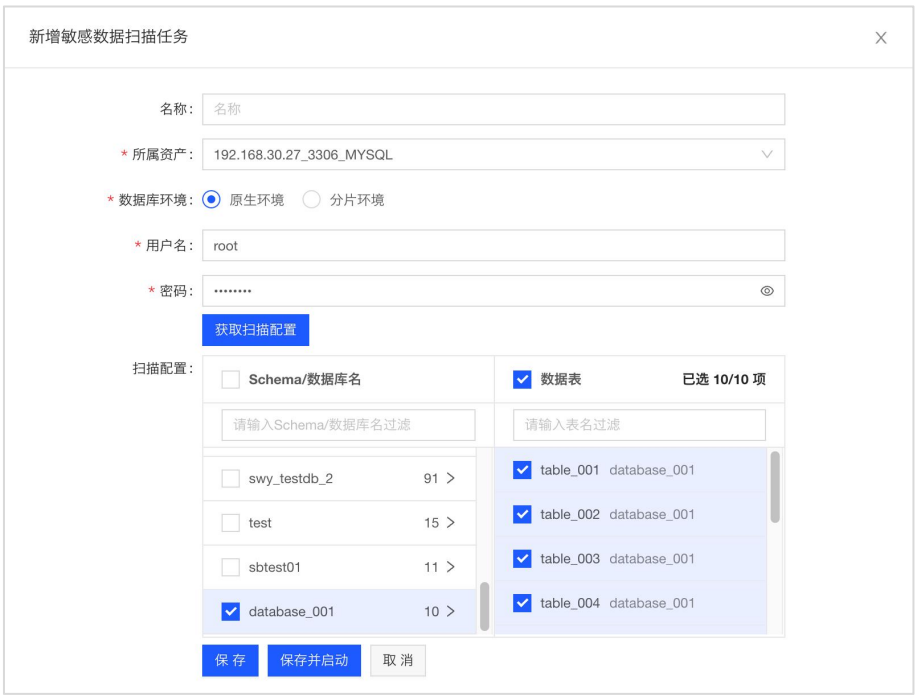
步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，点击<新增>。

新增敏感数据扫描任务时，若选择已配置默认数据源的资产（默认数据源在“添加资产”时配置），系统会自动识别并填充相应的用户名和密码。

步骤 2. 在弹出的“**新增敏感数据扫描任务**”页面编辑相关信息后。选择需要扫描的资产或是 Oralce，配置登录信息，点击<获取扫描配置>按钮，系统将自动检索并显示“Schema/数据库名”的列表，同时还会显示每个数据库所包含的数据表数量。

若由于数据表的数量过多，导致获取扫描配置失败，请前往“**系统管理　系统维护　设备管理**”页面，将后端服务配置中的“敏感数据扫描任务超时时间”改大。

步骤 3. 勾选需要扫描的“Schema/数据库名”，系统将自动检索出数据库下的所有数据表。



详细配置请参见下表（未提及项请参考资产详细配置项）：

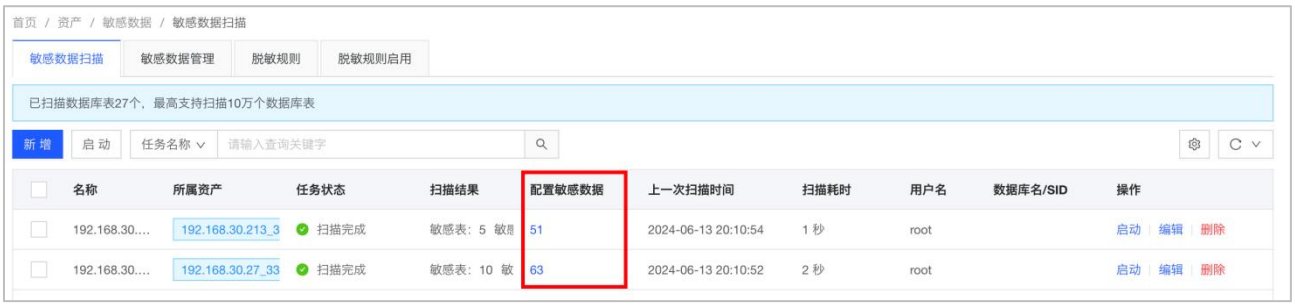
配置项	说明
名称	非必填项，不填则自动生成。填写必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
所属资产	设置数据来源所隶属的资产。
数据库环境	根据实际情况选择原生环境或分片环境。（仅限 MySQL 资产）
用户名	填写数据库的用户名。
密码	填写数据库的密码。
数据库名	填写数据库名。
获取扫描配置	点击获取扫描配置，系统将自动检索并显示“Schema/数据库名”的列表。
扫描配置	展示所属资产的“Schema/数据库”和“数据表”信息。

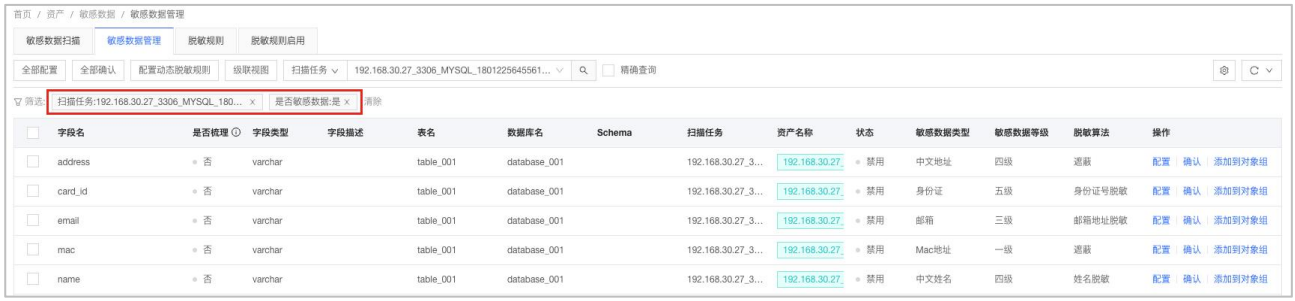
步骤 4. 勾选需要扫描的数据表，点击<保存并启动>。保存敏感数据扫描任务配置并立即执行任务。任务状态为“扫描中”。

有且仅有一个敏感数据扫描任务在扫描中，若同时存在多个扫描任务则排队扫描。

步骤 5. 元数据获取完成后，任务状态会显示“扫描完成”，元数据将保存在“敏感数据管理”中。

步骤 6. 点击敏感数据扫描任务条目中的<配置敏感数据列的数字>，将会跳转到“**资产　敏感数据　敏感数据管理**”页面，且默认带上“扫描任务”和“是否敏感数据”两个查询条件。





4.2.1.2　数据分类分级同步拉取

从数据分类分级拉取是通过配置数据分类分级服务的 IP 地址和端口等信息，连接数据分类分级服务接口，从中获取在数据分类分级系统中已分级分类过的元数据信息。

步骤 1. 在菜单栏选择“**系统管理　系统配置　系统联动**”进入系统联动配置页面，点击<修改>数据分类分级关联配置，在修改弹窗中将状态置为启用。

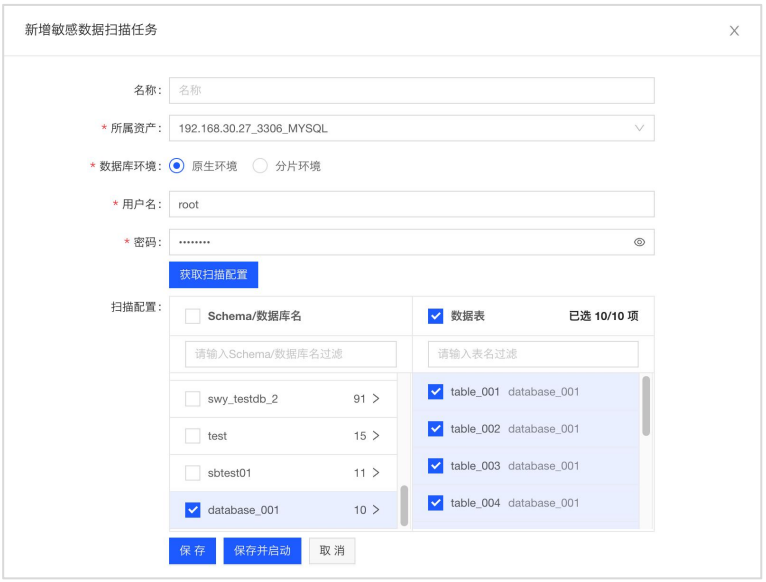
步骤 2. 根据实际情况配置数据分类分级 的 IP 地址和服务端口等信息后，点击<测试连接>，提示连接成功后方可点击<确定>保存配置。

请确保数据库安全网关数据库安全网关设备地址与数据分类分级服务接口的网络连通性正常。

步骤 3. 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，点击<新增>。

步骤 4. 在弹出的“**新增敏感数据扫描任务**”页面编辑相关信息后。点击<获取扫描配置>按钮，系统将自动检索并显示“Schema/数据库名”的列表，同时还会显示每个数据库所包含的数据表数量。

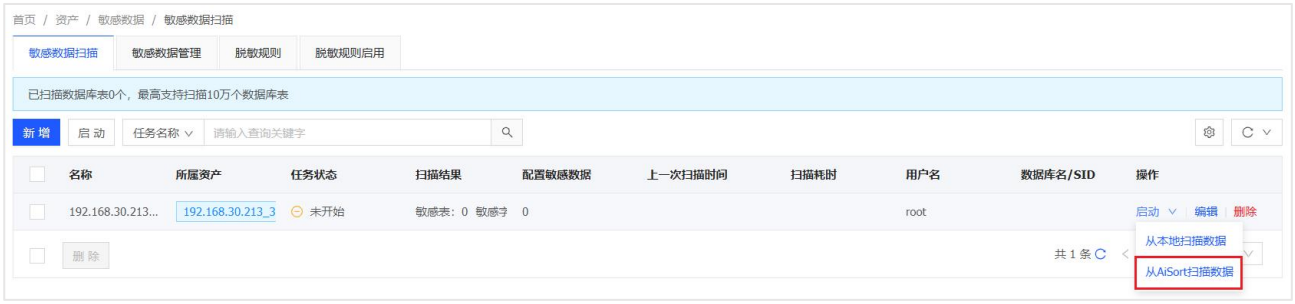
步骤 5. 勾选需要扫描的“Schema/数据库名”，系统将自动检索出数据库下的所有数据表。



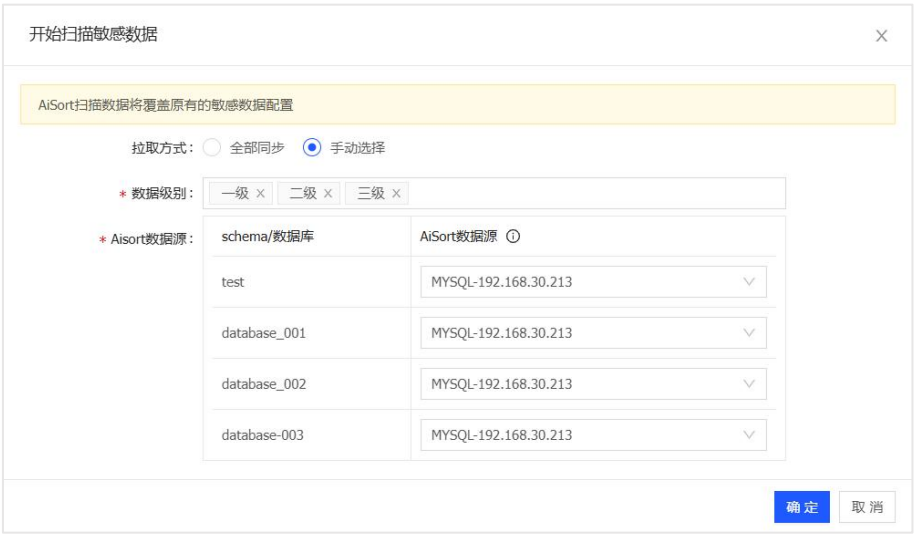
请确保所勾选的“Schema/数据库名”在“数据分类分级数据安全分级与风险评估系统”中已进行分类分级。否则扫描将失败，在扫描结果中展示“没有从 api 获取到匹配的源，请先配置好后重试”。

步骤 6. 勾选需要扫描的数据表，点击<保存>。保存敏感数据扫描任务配置，但不会立即执行任务。任务状态为“未开始”。

步骤 7. 点击下拉扫描任务条目右侧的<启动>按钮，选择<从数据分类分级扫描数据>。

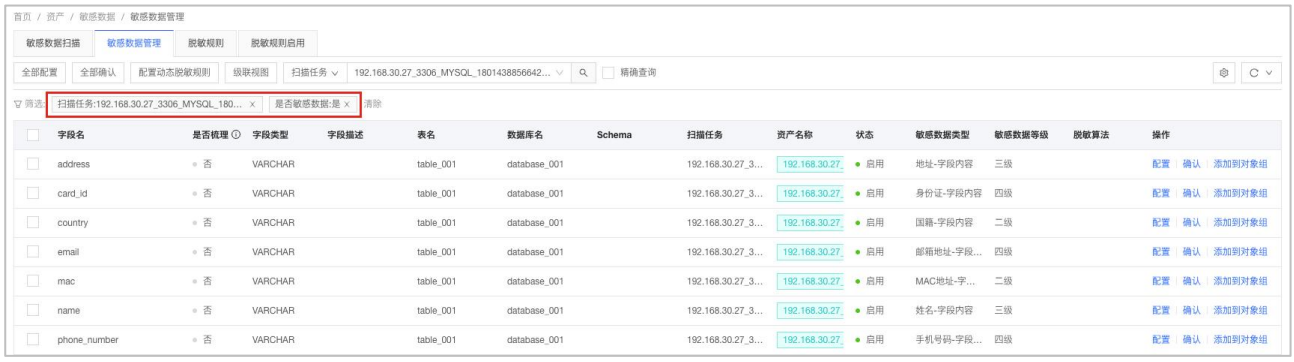


步骤 8. 在弹出的窗口中选择拉取方式及所拉取的数据分类分级数据源，点击<确定>开始进行拉取。①拉取方式分为全部拉取和手动选择，前者从数据分类分级自动同步该数据源下所有分级分类结果（覆盖全部数据级别），后者可拉取指定数据级别的字段（可灵活选择一级、二级、三级敏感数据）。②数据库安全网关 将同一 IP 端口的数据库视为单一资产，而数据分类分级 支持对同一 IP 端口配置多个独立数据源（如不同 Schema 或数据库），故在列表中选择需要拉取的具体数据源。



步骤 9. 元数据获取完成后，任务状态会显示“扫描完成”，元数据将保存在“敏感数据管理”中。

步骤 10.点击敏感数据扫描任务条目中的<配置敏感数据列的数字>，将会跳转到“**资产　敏感数据　敏感数据管理**”页面，且默认带上“扫描任务”和“是否敏感数据”两个查询条件。



数据库安全网关的敏感数据类型和等级分别对应数据分类分级的敏感数据标签和分级。

4.2.1.3　编辑扫描任务

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，点击扫描任务条目右侧的<编辑>按钮。

步骤 2. 在“编辑敏感数据扫描任务”的窗口中，点击<修改扫描配置>按钮，扫描配置内容被清空。

步骤 3. 再点击<获取扫描配置>，选择需要重新扫描的库表后，点击<保存>或<保存并启动>即可。

4.2.1.4 停止扫描任务

步骤 1. 任务状态为“扫描中”的任务，可以点击<停止>来终止拉取数据动作。

4.2.1.5 删除扫描任务

方法 1. 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，点击扫描任务条目右侧的<删除>按钮。

方法 2. 选中扫描任务列表前方的复选框，点击列表下方的<删除>，弹出二次确认窗口，点击<确认>即可。扫描任务删除后，**敏感数据管理**中的元数据信息也将被级连删除。

4.2.2 敏感数据管理

敏感数据管理主要展示并管理数据库表结构和字段信息，支持对敏感数据进行详细配置。通过定义敏感数据等级和类型，配置脱敏算法，便于在后续使用过程中保障敏感数据的安全性。

4.2.2.1 配置元数据

对数据库中获取到的元数据信息进行筛选和配置。包括定义数据的敏感级别、敏感数据类型和脱敏算法等。关于敏感数据类型和脱敏算法的更多操作及配置，请参考敏感数据类型与脱敏算法。

4.2.2.1.1 单个配置

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入敏感数据管理页面，点击元数据条目的右侧的<配置>按钮。

步骤 2. 在**编辑分类分级配置**窗口中，选择状态、敏感数据等级和类型、脱敏算法后，点击<保存>。

详细配置请参见下表：

配置项	说明
状态	启用或禁用该配置。
敏感数据等级	默认可选一级、二级、三级、四级和五级。
敏感数据类型	默认可选无、身份证、银行卡、手机号、邮箱、座机号、军官证、护照号、车牌号、MAC 地址、日期、时间、港澳台通行证、台胞证、中文名字。其他新增敏感数据类型详见敏感数据类型。
脱敏算法	配置数据字段的脱敏算法。内置及自定义的脱敏算法配置详见脱敏算法。

4.2.2.1.2 全部配置

步骤 1. ① 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，点击扫描任务条目中配置敏感数据字段中的数字，带条件跳转至**敏感数据管理页面**；② 或在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入敏感数据管理页面，展示所有元数据；③ 或在方法 2 的基础上，选择过滤条件，查询出需要配置的元数据。

步骤 2. 点击列表上方的<全部配置>按钮，弹出批量配置框（其中“批量配置”字段根据敏感数据管理列表中所含有的敏感数据类型展示）。

步骤 3. 根据需要启禁用字段，也可自定义字段的脱敏算法和数据级别，点击保存即可配置成功。（非敏感字段可自定义敏感数据类型和等级）

4.2.2.1.3 勾选配置

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入敏感数据管理页面，选中需要配置的字段，点击列表下方的<配置选中项>按钮，弹出批量配置框，其他步骤与全部配置相同。

4.2.2.1.4　级联视图配置

级联视图是敏感数据管理中的一种展示和配置方式。它以数据来源、数据库/Schema、表、字段和分类分级配置的关联性，层次化地呈现和管理元数据信息。

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入敏感数据管理页面，点击列表上方<级联视图>按钮，进入级联视图界面。点击条目可一级一级展开显示。

步骤 2. 选择状态、敏感数据等级和类型、脱敏算法后，点击<保存>即可。

4.2.2.2　确认元数据

确认元数据的重要性在于确保用户在修改敏感数据的相关配置后，这些更改能够得以保留，从而避免系统错误地重新拉取并恢复为默认配置。

在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入页面，您可以用下方三种方法进行确认：

- **单个确认**：选择需要确认的元数据，点击条目右侧的<确认>按钮。
- **全部确认**：点击列表上方<全部确认>按钮。
- **勾选确认**：选中需要确认的字段，点击列表下方的<确认选中项>按钮。

点击<确认>后，需在弹窗中进行二次确认。确认成功后元数据的“是否梳理”列将变更为“是”。

4.2.2.3　添加到对象组

对象组通过将相关或具备相同业务管理规范的库、表、字段归类到一个组中，简化管理流程，提高管理效率。便于对同一对象组内的所有字段应用统一的安全规则和访问控制策略等，确保安全措施的一致性。

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入敏感数据管理页面，点击元数据条目右侧的<添加到对象组>按钮，或是勾选需要加到同一对象组中的元数据，点击列表下方的<添加到对象组>的按钮。

步骤 2. 在弹出的窗口中，展示步骤 1 中所勾选的对象信息，可选择添加到已有的对象组，或者新对象组，选择完毕点击<确定>即可。（关于对象组的详细配置请参考关联数据中的对象组管理）

步骤 3. 添加到对象组后，在菜单栏选择“**规则配置　关联数据　对象组**”进入对象组管理页面，可查看对象组列表，点击对象组条目右侧的<编辑>可查看步骤 2 所添加的对象信息。

4.2.2.4　查询元数据

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据管理**”进入敏感数据管理页面，选择查询条件（包括扫描任务、资产、数据来源、数据库名、Schema、表名、字段名、是否梳理、字段描述、状态、是否敏感数据、敏感数据类型、敏感数据等级，以及可以选择平铺所有条件），填写查询内容，可勾选是否需要精确查询，点击<🔍>即可完成单个条件或所有条件的查询。

步骤 2. 点击敏感数据管理列表右上方的<⚙>按钮，弹出设置显示列的窗口。

步骤 3. 按实际所需勾选需要展示的列名称后，点击<确定>即可保存成功。

4.2.3 脱敏规则

通过配置脱敏规则，对敏感数据进行实时脱敏，确保数据在使用过程中不会泄露。支持根据客户端、服务端、行为、数据级别等多个维度进行脱敏规则的配置，满足不同场景的需求。

目前支持动态脱敏的数据库有：Oracle，MySQL，MSSQL，DB2，达梦(DM)，PostgreSQL，人大金仓(Kingbase)，MariaDB，TIDB，UXDB，Doris，OceanBase，Trino，Hive，Clickhouse(jdbc)，Tdh，Teledb-MySQL，Teledb-PostgreSQL。

动态脱敏模块（DAS-ABL-数据库安全网关-S-DM）和运维管理功能模块（DAS-ABL-数据库安全网关-S-OP）是需要额外购买的增值功能，标准许可未包含，页面默认隐藏，需要授权激活开启。另旁路模式下这两个功能不支持，页面默认不显示。

4.2.3.1 新增脱敏规则

步骤 1. 在菜单栏选择“**资产　敏感数据　脱敏规则**”进入脱敏规则页面，点击<新增规则>按钮。

步骤 2. 在弹出的新增规则窗口内，根据用户需求填写规则相关信息后，点击<保存>。

详细配置请参见下表：

项目	配置项	说明
基本信息	名称	设置规则名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
	动作	支持“动态脱敏”或“允许访问”。
客户端	客户端来源	访问业务类型的客户端 IP 或 IP 组。 支持多个 IP，使用逗号“,”分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20 有关 IP 组的更多信息，请参考 IP 组管理。
	客户端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例如：

项目	配置项	说明
		10-15,20,25,30-40。
	客户端工具名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可配多个客户端工具名，使用逗号“,”分隔，例：db2bp.exe,javaw.exe,plsqldev.exe 有关分组选择的方式，请参考客户端工具名组管理。
	操作系统用户	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关分组选择的方式，请参考操作系统用户名组管理。
	客户端主机名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关分组选择的方式，请参考客户端主机名组管理。
	密码桥账号	支持下拉框选择，需要存在支持密码代填的运维人员。详细请参考密码桥功能。 若不支持密码代填的数据库配置该项后会导致规则匹配失效。
服务端	数据库账号	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关数据库账号组的更多信息，请参考数据库账号组管理。
行为	敏感数据	可选择“数据级别”或“敏感数据类型”
	数据级别	指定什么敏感数据等级需要触发脱敏，可选级别一级、二级、三级、四级、五级，可单选或多选。
	敏感数据类型	指定什么敏感数据类型需要触发脱敏，可选内置类型或后续新增的类型（详见敏感数据类型），类型间为“或”的关系，可单选或多选。
	操作类型	指定什么操作类型需要触发脱敏，支持的操作类型有 Select、Update、Merge、With、Replace、Insert Into Table Select、Create(Materialized) View、Create Table As Select。

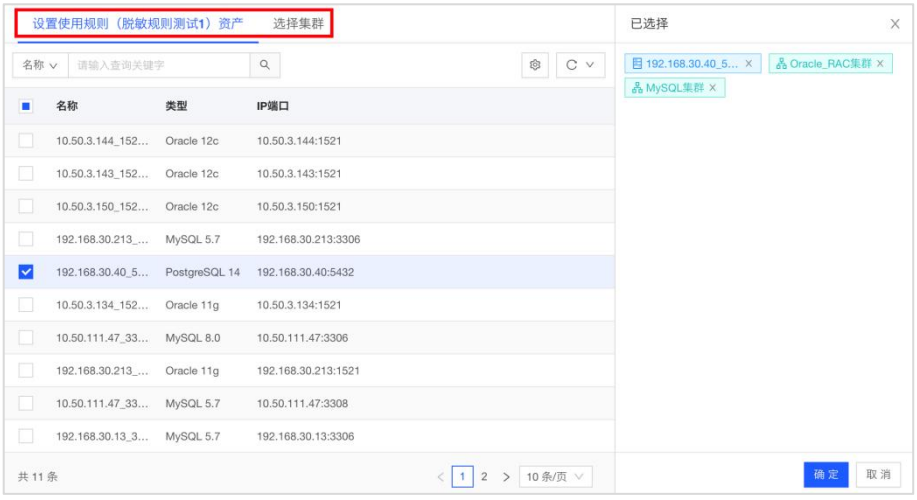
项目	配置项	说明
其它	生效时间	可自定义或者选择时间组。 自定义时间可选择任意时间、每天、每周、每月或节假日。 有关时间组配置的更多信息，请参考时间组管理。

4.2.3.2 给脱敏规则绑定资产

方法一：单条规则绑定资产

步骤 1. 在菜单栏选择“**资产　敏感数据　脱敏规则**”进入脱敏规则页面，选择需要启用的脱敏规则，点击该条目的资产数量字段中的< 0 0 >图标按钮，弹出“设置使用规则资产”窗口。

步骤 2. 在“**设置使用规则资产**”窗口内可选择按“资产”进行绑定，勾选需要绑定的“资产”点击<确定>。

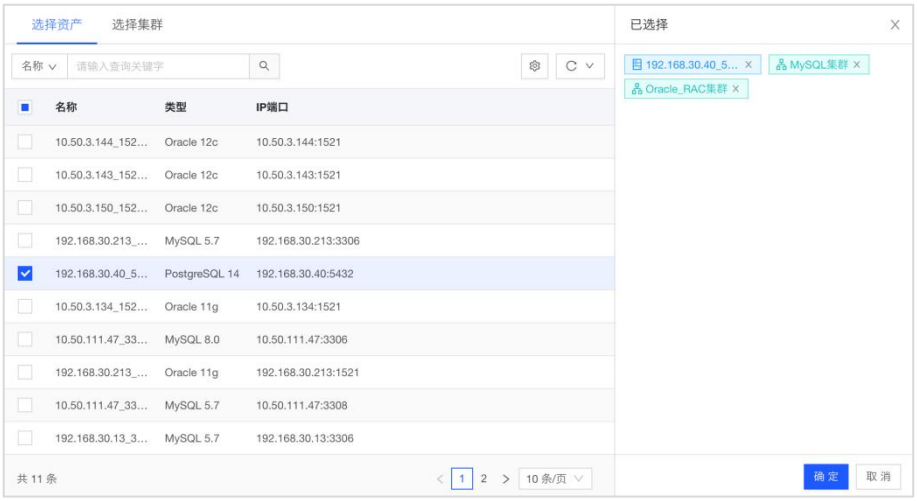


步骤 3. 该条目对应的“资产数量”字段中的数值将相应地增加。

方法二：多条规则绑定资产

步骤 1. 在菜单栏选择“**资产　敏感数据　脱敏规则**”进入脱敏规则页面，勾选多条需要启用的脱敏规则，点击列表下方的<启用选中项>，弹出“设置使用规则资产”窗口。（<禁用选中项>同理）

步骤 2. 在“**设置使用规则资产**”窗口内可选择按“资产”进行绑定，勾选需要绑定的“资产”，点击<确定>。

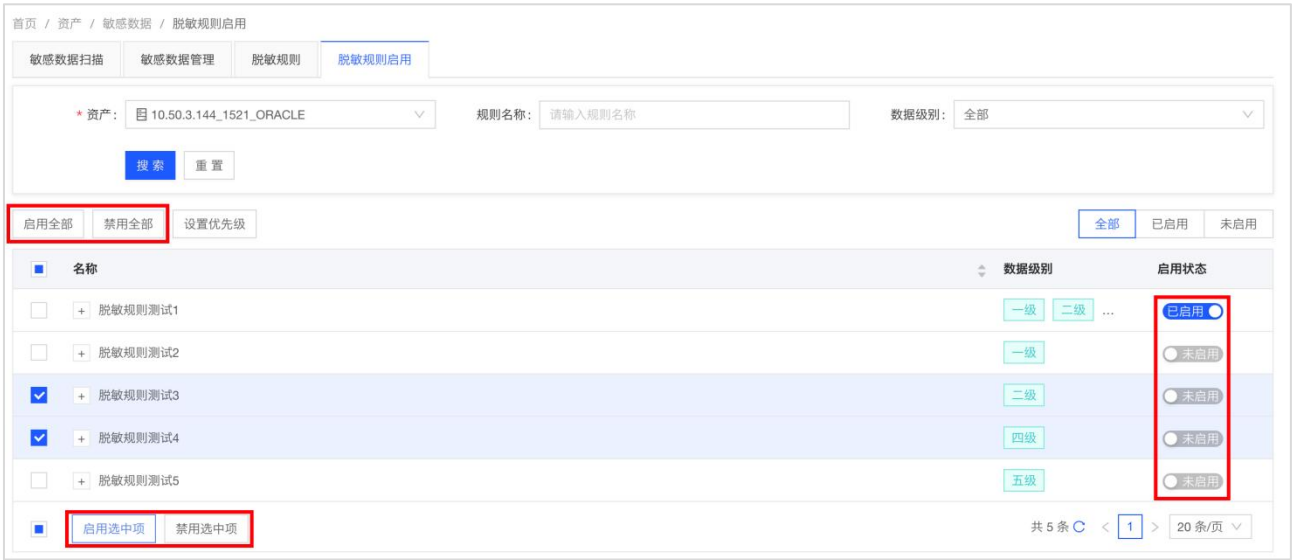


步骤 3. 所勾选的脱敏规则对应的“资产数量”字段中的数值将相应地增加。

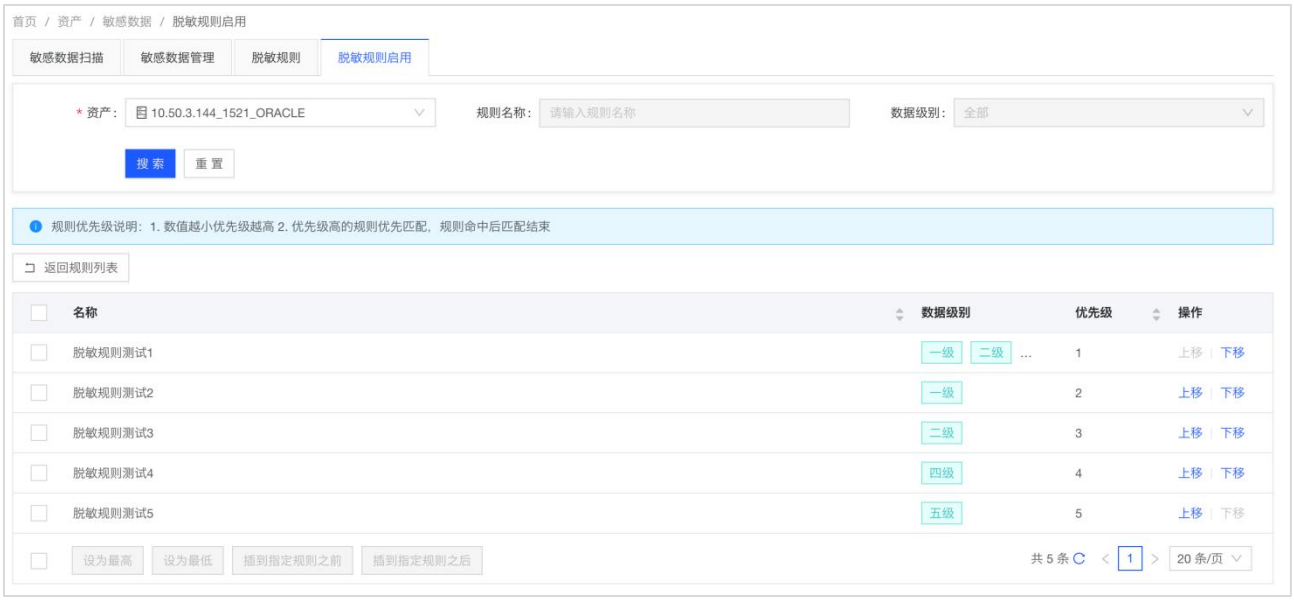
4.2.3.3 给资产启用脱敏规则

步骤 1. 在菜单栏选择“**资产　敏感数据　脱敏规则启用**”进入脱敏规则启用页面，在页面上方选择资产，下方列表展示已配置的脱敏规则。

步骤 2. ① 可点击脱敏规则列表上方的<启用全部>或<禁用全部>来修改脱敏规则的启用状态；② 可勾选脱敏规则，点击列表下方的<启用选中项>或<禁用选中项>来修改脱敏规则的启用状态；③ 可点击脱敏规则条目右侧的按钮，调整规则的启用状态。



步骤 3. 脱敏规则启用状态配置完成后，可点击列表上方的<设置优先级>按钮，可对已启用的脱敏规则进行优先级设置。支持对单条规则进行上移或下移操作，支持勾选规则将其设为最高/最低优先级，支持勾选规则将其插到指定规则之前/之后。



规则优先级说明：1.数值越小优先级越高 2.优先级高的规则优先匹配，规则命中后匹配结束。

4.2.3.4 编辑脱敏规则

步骤 1. 在菜单栏选择“**资产　敏感数据　脱敏规则**”进入脱敏规则页面，点击规则条目右边的<编辑>。

步骤 2. 在“编辑规则”页面可以修改规则的所有配置项。具体字段说明请参考添加脱敏规则的配置项。

步骤 3. 编辑完成后点击<保存>即可完成对该脱敏规则的编辑。

4.2.3.5 删除脱敏规则

方法 1. 在菜单栏选择“**资产　敏感数据　脱敏规则**”进入脱敏规则页面，点击规则条目右侧的<删除>按钮。

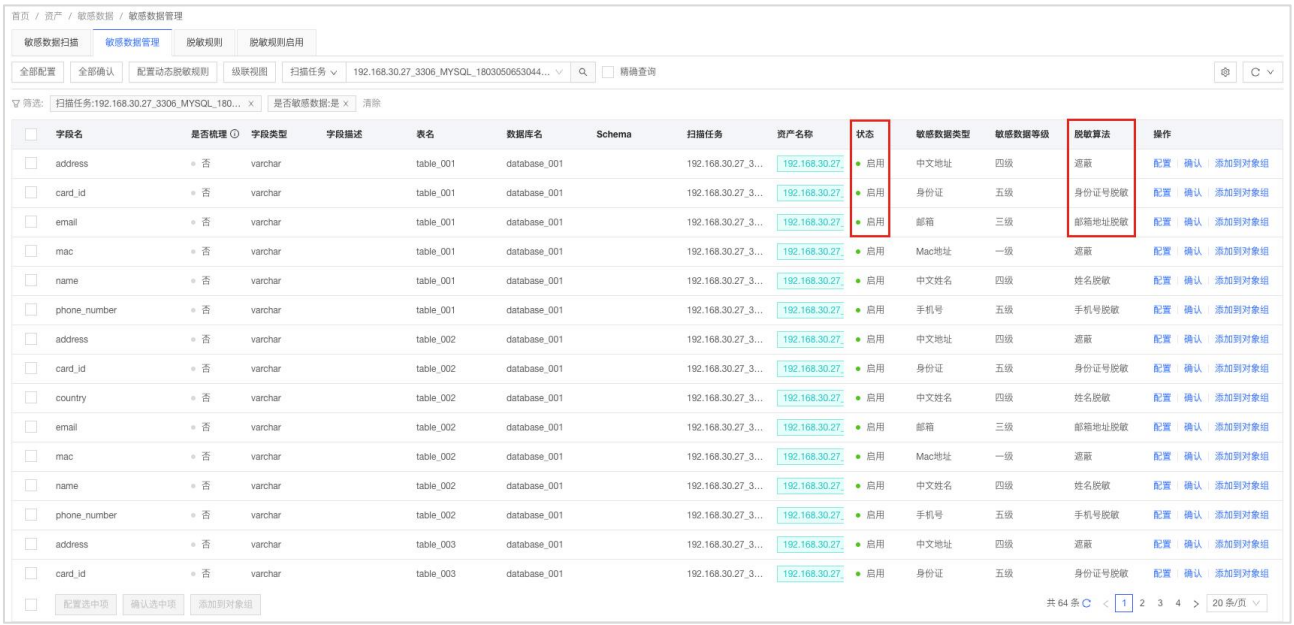
方法 2. 选中脱敏规则列表前方的复选框，点击列表下方的<删除>，弹出二次确认窗口，点击<确认>即可。若脱敏规则存在绑定的资产，不支持删除，提示“规则已挂载到资产下，不能删除”。

4.2.4 动态脱敏典型配置案例

- 案例描述：通过配置脱敏规则，实现用户查询 1-5 级敏感数据时自动脱敏处理。
- 前提条件：确认您的数据库资产是“入侵防护模式”。

步骤 1. 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，为您的数据库资产新增并启用敏感数据扫描任务。完成后如下图所示，具体请参见敏感数据扫描。

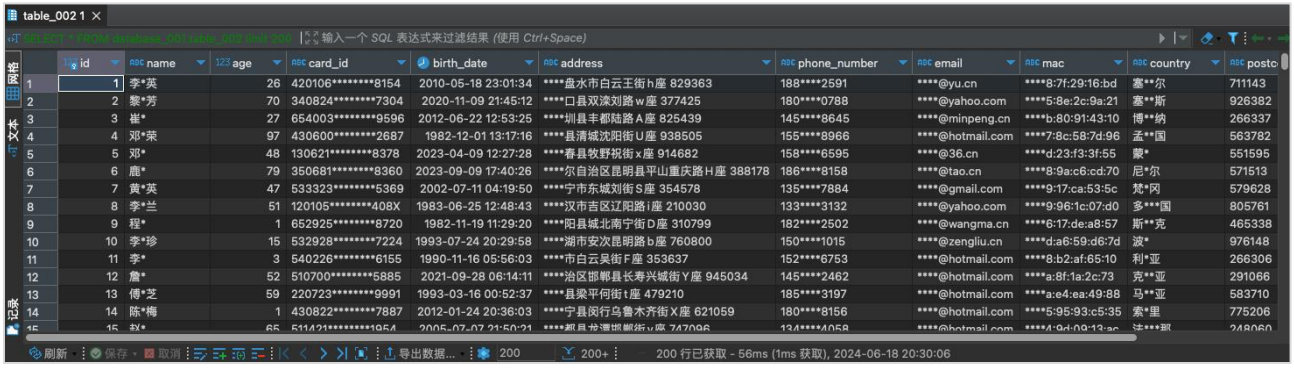
步骤 2. 等待扫描任务完成后，点击该扫描任务条目中“配置敏感数据”字段中的数字链接，跳转至“**资产　敏感数据　敏感数据管理**”页面，点击<全部配置>，批量启用并配置元数据。完成后如下图所示，具体请参见敏感数据管理。



步骤 3. 在菜单栏选择“**资产　敏感数据　脱敏规则**”进入脱敏规则页面，新增脱敏规则（最简单的脱敏规则即可，如下图所示）。点击该脱敏规则条目的资产数量字段中的< 0 0 >图标按钮，配置需脱敏的数据库资产。完成后如下图所示，具体请参见脱敏规则。

步骤 4. 在菜单栏选择“**系统管理　系统维护　设备管理**”进入设备管理页面，修改后端服务配置中的“数据包转发超时时间”为 200 毫秒。（脱敏 SQL 执行时长超过默认设置的 10 毫秒时，则脱敏失败，返回数据仍为原始数据，但是会有脱敏日志生成。若遇此情况，通常是由于未执行该步骤导致。）

步骤 5. 使用客户端工具通过反向代理连接数据库，执行 SQL 请求数据表（该表内含敏感数据），返回结果做脱敏处理，并会生成脱敏日志。



4.3　数据恢复

数据恢复目前只支持 Oracle。Oracle 的闪回归档功能为用户提供了一个简单、可靠的方式来恢复误删除的数据，通过自动生成和执行 SQL 恢复语句，实现了数据的快速恢复。具体步骤如下：

步骤 1. 在菜单栏选择“**资产　数据恢复**”进入数据恢复页面。

步骤 2. 点击<修改>，进入闪回归档配置界面。

详细配置项说明：

配置项	说明
状态	启用或禁用该配置。启用后不可再修改闪回归档配置。
资产	选择 Oracle 资产。（必须要配置 Oracle 的默认数据源，详见章节 4.1.1）
保存天数	配置备份数据保留天数，1~1000 天。
数据文件	配置保留数据存放的路径： Windows 路径：例如：C:\Users Linux 路径：连接 Oracle 数据库，执行命令 select * from dba_data_files; 即可查看
初始大小	1-32768M。如果选择支持扩展，扩展空间需要大于初始空间，且不能超过 32768M。

步骤 3. 按实际情况配置完成后，点击<确定>，页面即可展示闪回归档配置信息。

步骤 4. 点击闪回归档配置中的<清理>按钮，可以对闪回归档存放路径下的空间进行清理。

步骤 5. 点击“数据恢复范围管理”模块中的<新增>按钮，弹出新增数据恢复范围框，填写正确的 Schema 和表名后，点击<保存>（最多添加五对库表）。

步骤 6. 客户端登录 Oracle 数据库，在数据恢复范围管理的库表中执行 Delete、Update、Truncate、Alter 操作，查看数据恢复页面的删除日志模块，有日志记录。

步骤 7. 点击日志条目右侧的<恢复 SQL>，即可弹出窗口生成恢复子句。将该语句在客户端内执行，即可恢复步骤 6 删除修改过的数据。

步骤 8. 按照相关提示在客户端上执行相关命令，进行恢复操作。

4.3.1 恢复子句典型配置案例

- 案例描述：客户端执行 SQL 删除一条表数据后，通过数据恢复功能恢复数据。
- 前提条件：数据库安全网关已启用并配置数据恢复功能，具体操作请查看本章节前半部分。

步骤 1. 客户端执行 SQL “DELETE FROM EMPLOYEES WHERE EMPLOYEE_ID=5;”删除表数据后；

步骤 2. 在“资产 数据恢复”页面的删除日志模块中会生成步骤 1 行为对应的日志，点击该日志条目右侧的<恢复 SQL>按钮，获取到恢复子句“AS OF TIMESTAMP TO_TIMESTAMP ('2024-06-14 19:03:11','yyyy-mm-dd hh24:mi:ss')”。

步骤 3. 在客户端执行补全的查询语句“SELCT * FROM EMPLOYEES AS OF TIMESTAMP TO_TIMESTAMP ('2024-06-14 19:03:11','yyyy-mm-dd hh24:mi:ss') WHERE EMPLOYEE_ID=5”可查看当时删掉数据。

步骤 4. 或者执行补全的插入语句“INSERT INTO EMPLOYEES SELECT * FROM EMPLOYEES AS OF TIMESTAMP TO_TIMESTAMP ('2024-06-14 19:03:11','yyyy-mm-dd hh24:mi:ss') WHERE EMPLOYEE_ID=5”可将删除的数据加回数据表中。

5 查询分析

查询分析模块旨在记录、监控和分析数据库访问及操作日志。通过对日志信息的查询和分析，用户可以了解数据库访问行为、识别潜在的安全威胁、并确保数据库操作的合规性。

5.1 审计日志

当系统根据既定配置成功捕获到客户端的访问行为时，它会详尽地记录审计日志。这些日志为用户提供了一个全面的视角，以查看所有触发审计的 SQL 语句的详细信息。为了方便用户快速定位和分析，系统支持在审计日志页面根据时间范围、客户端 IP、数据库账号、报文内容等多个维度进行灵活的筛选操作，从而确保用户能够迅速获取所需的关键信息。

5.1.1 检索审计日志

步骤 1. 在菜单栏选择“**查询分析　审计日志**”进入审计日志页面，设置查询条件（如时间范围、资产、操作类型等），点击<搜索>即可查询相关审计日志。

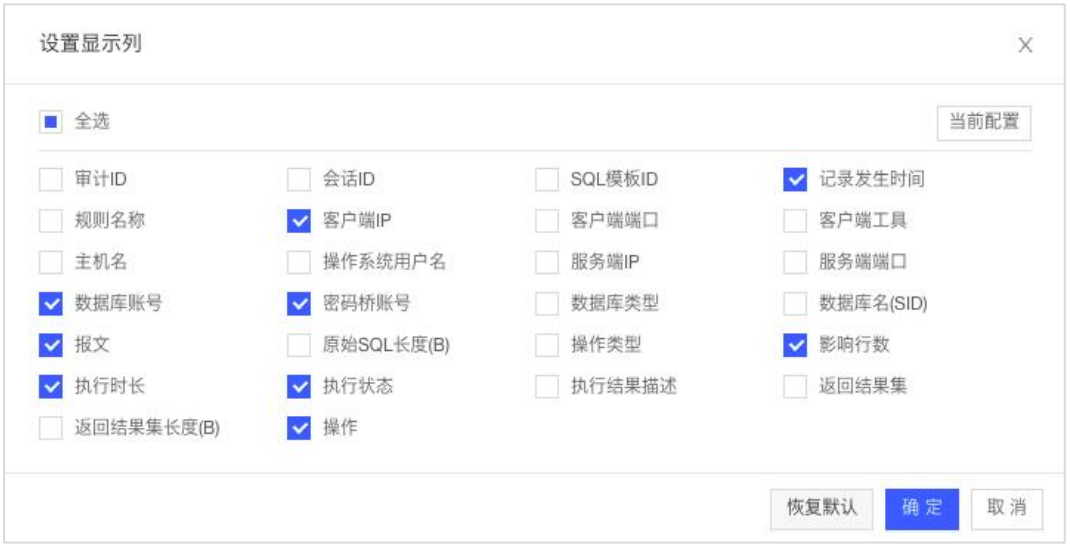
步骤 2. 点击查询条件下方的<更多条件>，在更多条件对话框中勾选需要的查询条件，点击<确认>即可添加相应的查询条件，点击<恢复默认>可以恢复至默认查询条件。

各查询条件的说明如下：

选项	说明
时间范围	设置日志查询的时间范围，默认为“最近 5 分钟”。

选项	说明
报文	审计到的 SQL 语句，可填多个关键字，用空格隔开，表示同时满足。
审计 ID	唯一标识日志记录的 ID。
会话 ID	唯一标识会话记录的 ID。
SQL 模板 ID	唯一标识 SQL 模板的 ID。
资产	选择资产，同时支持单选或多选，默认为全部资产。
数据库账号	登录到数据库的账号。
密码桥账号	密码代填功能登录数据库使用的账号。
客户端 IP	客户端 IP 地址，可填写 IPv4 和 IPv6 地址。
客户端端口	客户端端口号。
服务端 IP	服务端 IP 地址，可填写 IPv4 或 IPv6 地址。
服务端端口	服务端端口号。
数据库名(SID)	数据库名称或者实例名称。
客户端工具	客户端工具名称。
主机名	客户端主机名称。
影响行数	SQL 返回的影响行数，查询格式为 M-N，如：10-10，10-20。
执行时长	执行 SQL 所用时长，查询格式为 M-N，如：10-10，10-20。
操作类型	数据库操作的类型。
数据库类型	系统支持审计的数据库类型。
执行状态	可选择执行成功、执行失败、未知，默认为全部。

步骤 3. 查询结果显示在查询条件的下方。点击列表右上方<⚙>图标，勾选需要展示的显示列，点击<确定>即可设置查询结果展示的列。

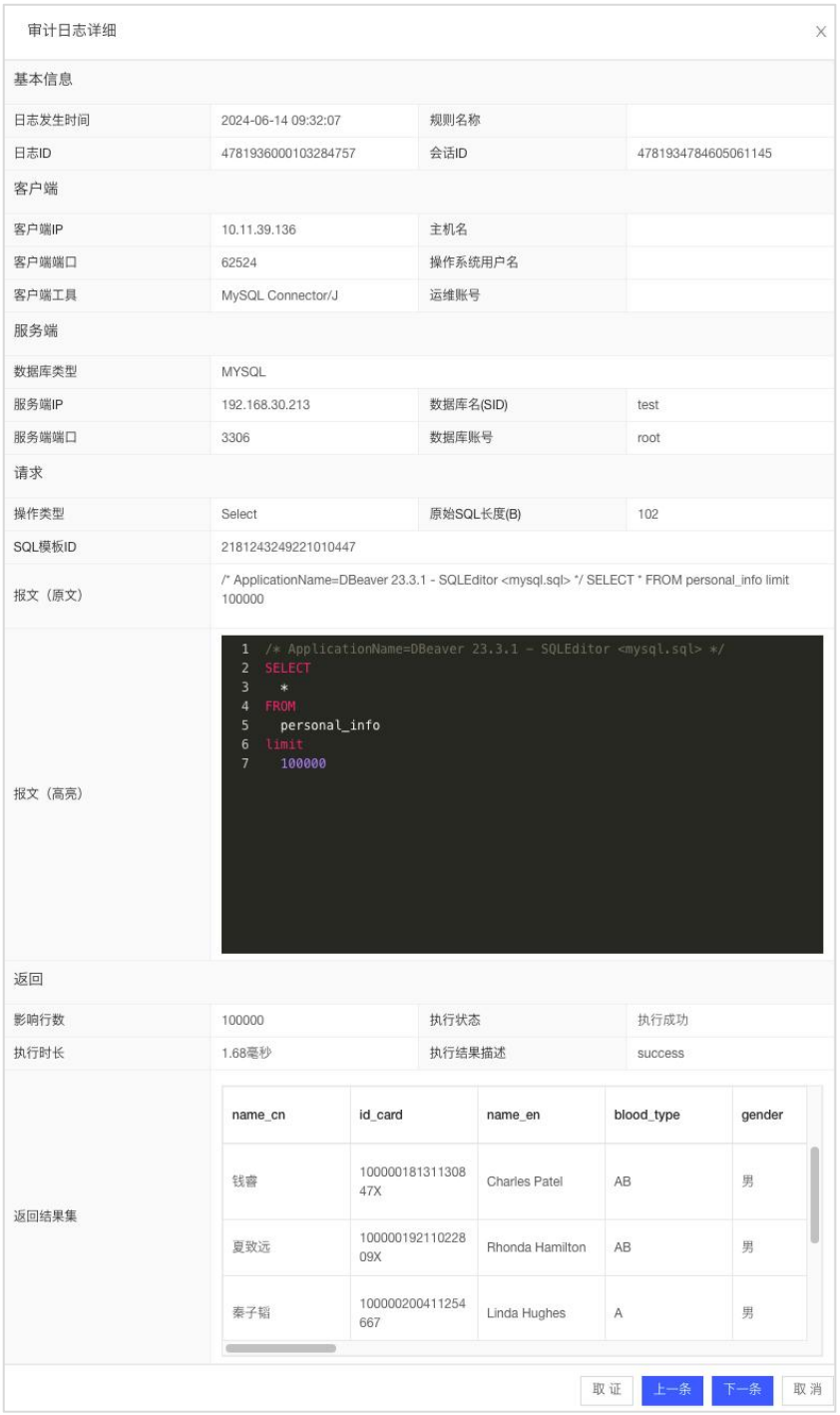


步骤 4. 点击<  >按钮，即可根据查询结果下载审计日志，最多支持 10 万条。

	记录发生时间	客户端地址	数据库账号	密码桥账号	报文	影响行数	执行时长	执行状态
2	2024-06-20 00:01:43	10.11.39.136	root		ha.TABLES tWHEREt.TAB	0	15263微秒	执行成功
3	2024-06-20 00:01:43	10.11.39.136	root		DBeaver 23.3.1 - Metadat	7	611微秒	执行成功
4	2024-06-20 00:01:43	10.11.39.136	root		Metadata */ SHOW VARIA	1	2300微秒	执行成功
5	2024-06-20 00:01:43	10.11.39.136	root		DBeaver 23.3.1 - Metadat	44	737微秒	执行成功
6	2024-06-20 00:01:43	10.11.39.136	root		*/ SELECT @@GLOBAL.c	1	4131微秒	执行成功
7	2024-06-20 00:01:43	10.11.39.136	root		Beaver 23.3.1 - Metadata	222	832微秒	执行成功
8	2024-06-20 00:01:43	10.11.39.136	root		DBeaver 23.3.1 - Metadat	41	538微秒	执行成功
9	2024-06-20 00:01:43	10.11.39.136	root		DBeaver 23.3.1 - Metadat	9	725微秒	执行成功
10	2024-06-20 00:01:43	10.11.39.136	root		eaver 23.3.1 - Metadata '	1	543微秒	执行成功
11	2024-06-20 00:01:43	10.11.39.136	root		Beaver 23.3.1 - Metadata	0	559微秒	执行成功
12	2024-06-20 00:01:43	10.11.39.136	root		SET autocommit=1	0	600微秒	执行成功
13	2024-06-20 00:01:43	10.11.39.136	root		character_set_results = N	0	436微秒	执行成功
14	2024-06-20 00:01:43	10.11.39.136	root		SHOW WARNINGS	2	345微秒	执行成功
15	2024-06-20 00:01:43	10.11.39.136	root		e_timeout AS interactive_t	1	747微秒	执行成功
16	2024-06-20 00:01:43	10.11.39.136	root		login root	0	515微秒	执行成功
17	2024-06-20 00:01:43	10.11.39.136	root		DBeaver 23.3.1 - Main */ S	1	15039微秒	执行成功
18	2024-06-20 00:01:43	10.11.39.136	root		=DBeaver 23.3.1 - Main */	0	759微秒	执行成功
19	2024-06-20 00:01:43	10.11.39.136	root		SET autocommit=1	0	4333微秒	执行成功

5.1.2 审计日志详情

步骤 1. 在菜单栏选择“**查询分析　审计日志**”进入审计日志页面，在审计日志列表中，点击日志条目右侧的<详细>可以查看该审计记录的详细信息，包括审计记录的基本信息、客户端信息、服务端信息、请求详情、返回详情。



步骤 2. 点击审计日志详情窗口右下角的<上一条>或<下一条>可切换查看临近的审计日志。

步骤 3. 在日志详细中，点击<取证>弹出下载框，等待文件生成成功后，点击<下载>即可下载 Png 图片格式的审计日志详情文件。

5.2 告警日志

当系统检测到违反安全策略或预定义规则的行为时，会生成对应等级的告警日志，以警示用户可能面临的

安全隐患。为了增强查询的便捷性和效率，系统还支持根据时间、特定字段、告警等级以及规则名称等多种条件进行精确筛选，确保用户能够迅速定位并处理潜在的安全风险。

5.2.1 检索告警日志

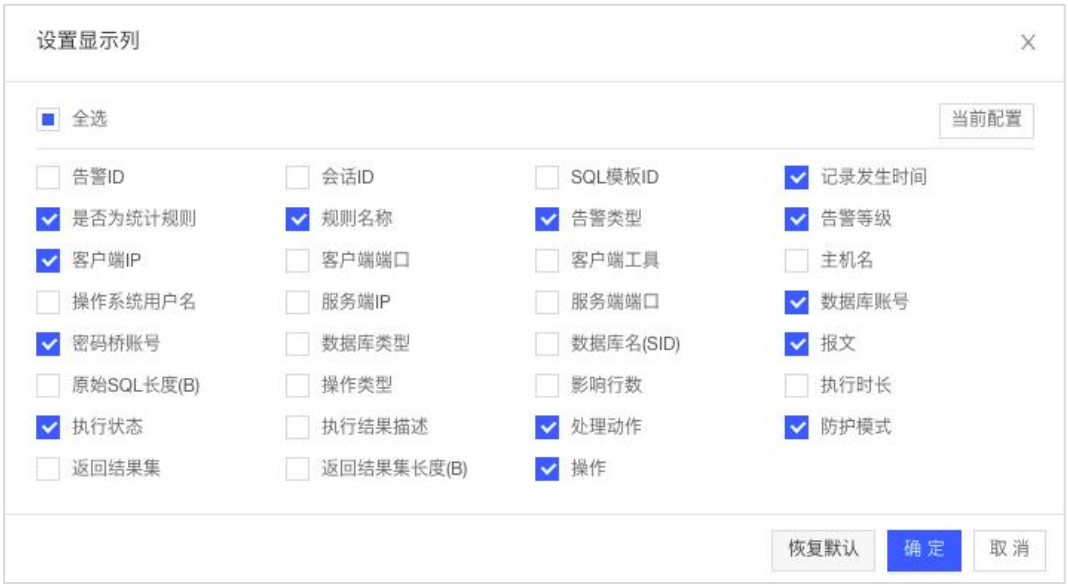
步骤 1. 在菜单栏选择“**查询分析　告警日志**”进入告警日志页面，设置查询条件（如时间范围、报文、资产等），点击<搜索>即可查询相关告警日志。

步骤 2. 点击查询条件下方的<更多条件>，在更多条件对话框中勾选需要的查询条件，点击<确认>即可添加相应的查询条件，点击<恢复默认>可以恢复至默认查询条件。重复查询条件说明请参考审计日志模块。

特有查询条件的说明如下：

选项	说明
告警 ID	唯一标识告警记录的 ID。
规则名称	系统里配置的安全规则的名称。
告警等级	可选高等级、中等级或低等级，默认为全部等级。
告警类型	可选虚拟补丁告警、内置规则告警等，默认为全部。
是否为统计规则	可选普通规则或统计规则。
处理动作	可选允许访问、命令阻断或会话阻断。

步骤 3. 查询结果显示在查询条件的下方。点击列表右上方<⚙>图标，勾选需要展示的显示列，点击<确定>即可设置查询结果展示的列。



步骤 4. 点击<>按钮，即可根据查询结果下载告警日志，最多支持 10 万条。

	记录发生时间	是否为统计规则	规则名称	告警类型	告警等级	客户端地址	数据库账号	密码桥账号	报文	执行状态	处理动作	防护模式
2	2024-06-17 15:17:37	身份权限	动化测试_安全规则6157	用户规则告警	高等级告警	192.168.30.116	system		arid, id, mac, mail, officer	执行失败	命令阻断	入侵防护
3	2024-06-17 15:16:55	身份权限	动化测试_安全规则6157	用户规则告警	高等级告警	192.168.30.116	system		login system	执行失败	命令阻断	入侵防护
4	2024-06-17 15:16:47	身份权限	全统计规则20784_737882	用户规则告警	高等级告警	192.168.30.116	system		RENXB.MYSQLTEST01 w	执行失败	命令阻断	入侵防护
5	2024-06-17 15:16:11	账号过期	化测试_安全统计规则20	用户规则告警	高等级告警					未知	放行	入侵防护
6	2024-06-17 15:15:51	身份权限	动化测试_安全规则3208	用户规则告警	高等级告警	192.168.30.116	system		d FROM C##RENXB.mys	执行失败	放行	入侵防护
7	2024-06-17 15:15:32	身份权限	动化测试_安全规则6673	用户规则告警	高等级告警	192.168.30.116	system		commit	执行成功	放行	入侵防护
8	2024-06-17 15:15:32	身份权限	动化测试_安全规则6673	用户规则告警	高等级告警	192.168.30.116	system		21234', '1000', '5', '6', '6	执行成功	放行	入侵防护
9	2024-06-17 15:15:32	身份权限	动化测试_安全规则6673	用户规则告警	高等级告警	192.168.30.116	system		login system	执行成功	放行	入侵防护
10	2024-06-17 15:15:13	身份权限	动化测试_安全规则8168	用户规则告警	高等级告警	192.168.30.116	system		ydd'@'%' identified by 'sj	执行失败	命令阻断	入侵防护
11	2024-06-17 15:14:54	身份权限	动化测试_安全规则9467	用户规则告警	高等级告警	192.168.30.116	system		bank, carid, mail FROM C	执行失败	命令阻断	入侵防护
12	2024-06-17 15:14:54	身份权限	动化测试_安全规则9467	用户规则告警	高等级告警	192.168.30.116	system		carid, mail, 姓名 FROM C	执行失败	命令阻断	入侵防护
13	2024-06-17 15:14:54	身份权限	动化测试_安全规则9467	用户规则告警	高等级告警	192.168.30.116	system		ss, bank, mail FROM C##	执行失败	命令阻断	入侵防护
14	2024-06-17 15:14:54	身份权限	动化测试_安全规则9467	用户规则告警	高等级告警	192.168.30.116	system		nk, carid, mail FROM C##	执行失败	命令阻断	入侵防护
15	2024-06-17 15:14:13	身份权限	动化测试_安全规则5112	用户规则告警	高等级告警	192.168.30.116	system		军官证, passport FROM	执行失败	命令阻断	入侵防护
16	2024-06-17 15:14:13	身份权限	动化测试_安全规则5112	用户规则告警	高等级告警	192.168.30.116	system		carid, bank FROM C##RE	执行失败	命令阻断	入侵防护
17	2024-06-17 15:14:13	身份权限	动化测试_安全规则5112	用户规则告警	高等级告警	192.168.30.116	system		arid FROM C##RENXB.m	执行失败	命令阻断	入侵防护
18	2024-06-17 15:13:40	账号过期	批量拖库	用户规则告警	高等级告警					未知	放行	入侵防护

5.2.2 告警日志详情

步骤 1. 在菜单栏选择“**查询分析　告警日志**”进入告警日志页面，在告警日志列表中，点击日志条目右侧的<详细>可以查看该告警记录的详细信息，包括告警记录的基本信息、客户端信息、服务端信息、请求详情、返回详情。

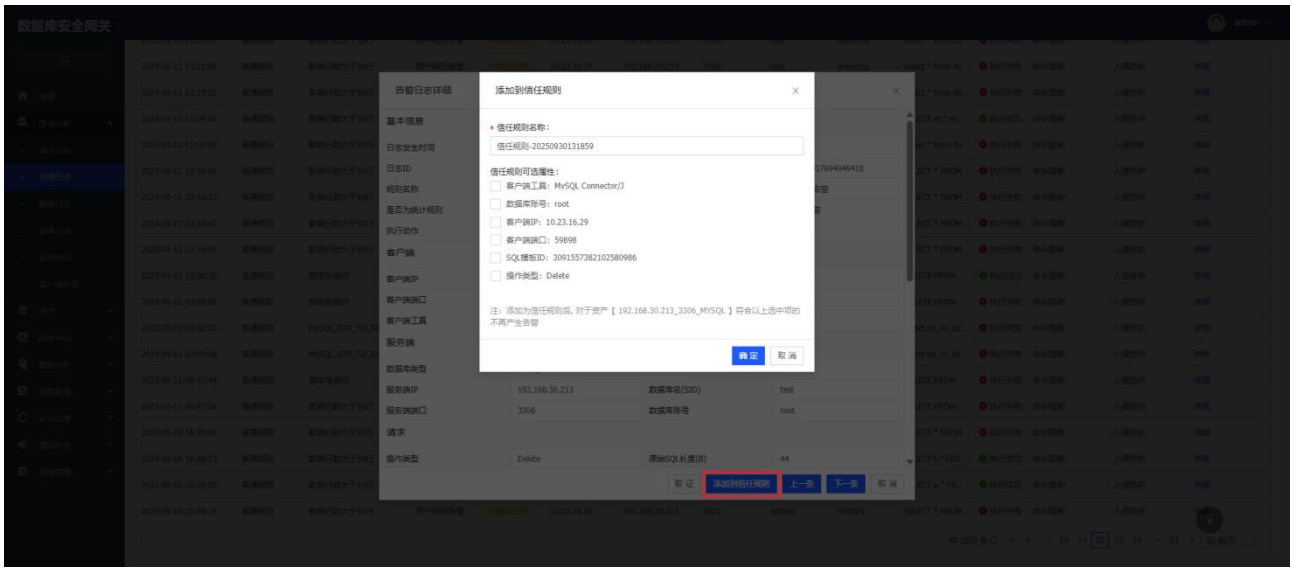
步骤 2. 点击审计日志详情窗口右下角的<上一条>或<下一条>可切换查看临近的审计日志。

步骤 3. 在日志详细中，点击<取证>弹出下载框，等待文件生成成功后，点击<下载>即可下载 Png 图片格式的审计日志详情文件。

5.2.3 添加到信任规则

根据告警日志里的信息，可以选择客户端工具、数据库账号、客户端 IP、操作类型等属性生成一条新的信任规则，对于符合信任规则的请求将不再告警。有关信任规则的更多信息，请参考规则配置。

步骤 1. 在菜单栏选择“**查询分析　告警日志**”进入告警日志页面，在告警日志列表中选择一条需要加到信任规则的告警日志，点击后方<详情>按钮，在告警日志详细页，点击下方<添加到信任规则>按钮。



步骤 2. 勾选需要的属性后，点击<确定>按钮，会提示操作成功信息。

步骤 3. 在菜单栏选择“**规则配置　信任规则**”进入信任规则页面，查看生成的信任规则。

5.3　脱敏日志

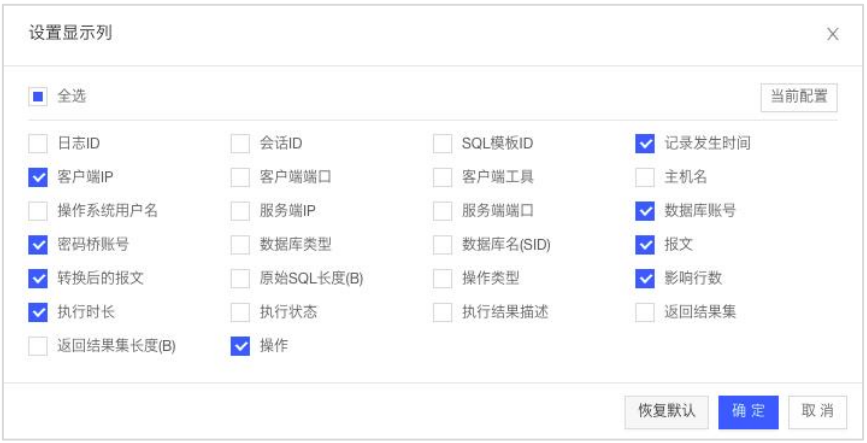
系统会记录所有触发数据脱敏的操作日志，详细记录脱敏前后的数据访问情况。通过对脱敏日志的查看和分析，用户可以验证脱敏操作的效果，确保敏感数据在访问过程中得到有效保护。

5.3.1 检索脱敏日志

步骤 1. 在菜单栏选择“**查询分析　脱敏日志**”进入脱敏日志页面，设置查询条件（如时间范围、资产和数据库账号等），点击<搜索>即可查询相关脱敏日志。

步骤 2. 点击查询条件下方的<更多条件>，在更多条件对话框中勾选需要的查询条件，点击<确认>即可添加相应的查询条件，点击<恢复默认>可以恢复至默认查询条件。各查询条件说明请参考审计日志模块。

步骤 3. 查询结果显示在查询条件的下方。点击列表右上方<⚙>图标，勾选需要展示的显示列，点击<确定>即可设置查询结果展示的列。



步骤 4. 点击<⬇>按钮，即可根据查询结果下载告警日志，最多支持 10 万条。

	记录发生时间	客户端地址	数据库账号	密码桥账号	报文	动态脱敏后的报文	影响行数	执行时长
2	2024-06-17 15:41:09	192.168.30.116	C##AIGATE		assport,carid,港澳台,mail,"	|| substr(trim(carid),5)) a	10	1818微秒
3	2024-06-17 15:41:09	192.168.30.116	C##AIGATE		assport,carid,港澳台,mail,"	|| substr(trim(carid),5)) a	10	1659微秒
4	2024-06-17 15:41:09	192.168.30.116	C##AIGATE		assport,carid,港澳台,mail,"	|| substr(trim(carid),5)) a	10	3415微秒
5	2024-06-17 15:41:09	192.168.30.116	C##AIGATE		assport,carid,港澳台,mail,"	|| substr(trim(carid),5)) a	10	2151微秒
6	2024-06-17 15:41:09	192.168.30.116	C##AIGATE		assport,carid,港澳台,mail,"	|| substr(trim(carid),5)) a	10	11518微秒
7	2024-06-17 15:37:53	192.168.30.116	C##AIGATE		' FROM C##RENXB.mysq	("BANK"),1,0) || '****' || sub	10	24905微秒
8	2024-06-17 15:37:53	192.168.30.116	C##AIGATE		rt,carid,mac,港澳台,台胞证	substr(trim(mac),5)) as mac	10	2076微秒
9	2024-06-17 15:37:53	192.168.30.116	C##AIGATE		rt,carid,mac,港澳台,台胞证	substr(trim(mac),5)) as mac	10	1878微秒
10	2024-06-17 15:37:53	192.168.30.116	C##AIGATE		rt,carid,mac,港澳台,台胞证	substr(trim(mac),5)) as mac	10	6618微秒
11	2024-06-17 15:37:53	192.168.30.116	C##AIGATE		rt,carid,mac,港澳台,台胞证	substr(trim(mac),5)) as mac	10	94272微秒
12	2024-06-17 14:12:28	192.168.30.116	system		' FROM C##RENXB.mysq	("BANK"),1,0) || '****' || sub	11	8536微秒

5.3.2 脱敏日志详情

步骤 1. 在菜单栏选择“**查询分析　脱敏日志**”进入脱敏日志页面，在脱敏日志列表中，点击日志条目右侧的<详细>可以查看该脱敏记录的详细信息，包括脱敏记录的基本信息、客户端信息、服务端信息、请求详情、返回详情。

步骤 2. 点击审计日志详情窗口右下角的<上一条>或<下一条>可切换查看临近的审计日志。

步骤 3. 在日志详细中，点击<取证>弹出下载框，等待文件生成成功后，点击<下载>即可下载 Png 图片格式的审计日志详情文件。

5.4 运维日志

运维日志模块是保障数据库运维操作安全和合规的重要工具，通过记录和分析与数据库运维相关的操作日志，帮助用户确保运维操作的透明性和合法性。该模块提供详细的日志信息和多条件筛选功能，支持安全监控和问题排查，确保运维操作的合规性，有效提升数据库的运维管理水平。

运维日志主要包含：身份权限相关日志、账号过期相关日志、僵尸账号相关日志、安全认证相关日志、登录超时相关日志、强管控阻断相关日志

5.4.1 检索运维日志

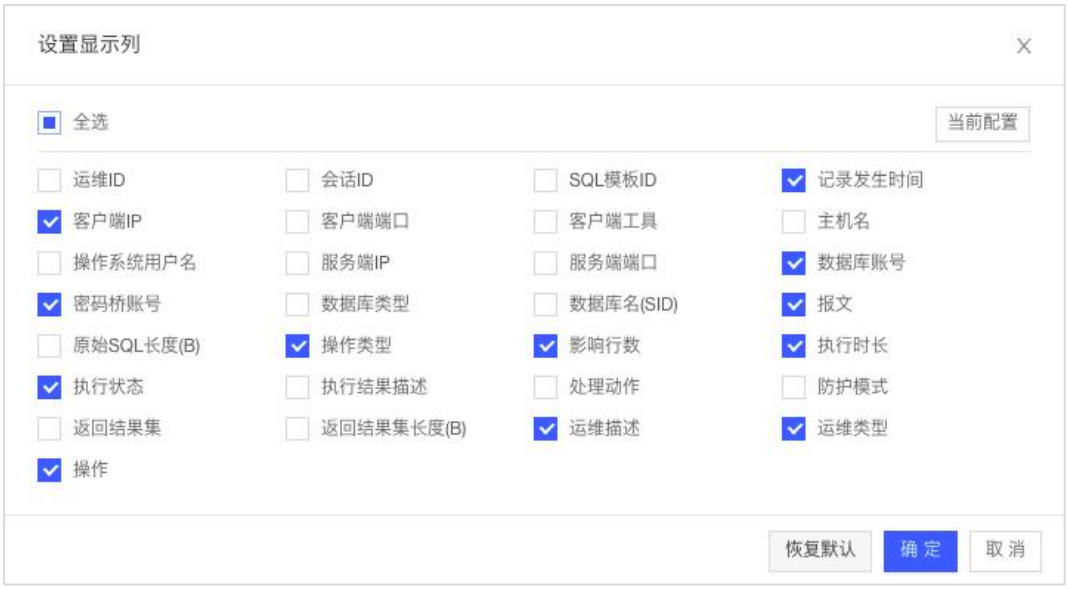
步骤 1. 在菜单栏选择“**查询分析　运维日志**”进入运维日志页面，设置查询条件（如时间范围、资产和数据库账号等），点击<搜索>即可查询相关运维日志。

步骤 2. 点击查询条件下方的<更多条件>，在更多条件对话框中勾选需要的查询条件，点击<确认>即可添加相应的查询条件，点击<恢复默认>可以恢复至默认查询条件。重复查询条件说明请参考审计日志模块。

特有查询条件的说明如下：

选项	说明
运维 ID	唯一标识运维记录的 ID。
运维描述	可选经过审批、未经过审批、账号已过期、未经过实名认证等。
运维类型	可选身份权限、账号过期、僵尸账号、安全认证等。

步骤 3. 查询结果显示在查询条件的下方。点击列表右上方<⚙>图标，勾选需要展示的显示列，点击<确定>即可设置查询结果展示的列。



步骤 4. 点击<>按钮，即可根据查询结果下载告警日志，最多支持 10 万条。

	记录发生时间	客户端地址	数据库账号	密码桥账号	报文	操作类型	影响行数	执行时长	执行状态	运维描述	运维类型
52	2024-06-17 11:37:58	192.168.30.116	root		m mysqltest01 where nar	Delete	0	0微秒	执行失败	未经过审批	身份权限
53	2024-06-17 11:37:58	192.168.30.116	root		m mysqltest01 where nar	Delete	0	0微秒	执行失败	未经过审批	身份权限
54	2024-06-17 11:37:30	192.168.30.116	root		m mysqltest01 where nar	Delete	0	0微秒	执行失败	未经过审批	身份权限
55	2024-06-17 11:37:30	192.168.30.116	root		m mysqltest01 where nar	Delete	0	0微秒	执行失败	未经过审批	身份权限
56	2024-06-17 10:54:52	192.168.30.116	root	auto_approval_013.452	lect mail from mysqltest0	Select	0	0微秒	执行失败	登录时间超时	登录超时
57	2024-06-17 10:51:28	192.168.30.116	root	auto_approval_011.270	lect mail from mysqltest0	Select	0	0微秒	执行失败	登录时间超时	登录超时
58	2024-06-17 10:43:09	192.168.30.116	root		lect mail from mysqltest0	Select	0	0微秒	执行失败	登录时间超时	登录超时
59	2024-06-17 10:40:26	192.168.30.116	root		lect mail from mysqltest0	Select	0	0微秒	执行失败	登录时间超时	登录超时
60	2024-06-17 10:37:02	192.168.30.116	root		login root	Login	0	0微秒	执行失败	强管控模式未识别账号	强管控阻断
61	2024-06-17 10:36:22	192.168.30.116	root		SET AUTOCOMMIT = 0	Set	0	1801微秒	执行成功	强管控模式未识别账号	强管控阻断
62	2024-06-17 10:36:22	192.168.30.116	root		SET NAMES utf8mb4	Set	0	1476微秒	执行成功	强管控模式未识别账号	强管控阻断
63	2024-06-17 10:30:30	192.168.30.116	root	auto_approval_007.185	gin auto_approval_007.18	Login	0	0微秒	执行失败	未经过实名认证	安全认证
64	2024-06-17 10:27:11	192.168.30.116	root		login root	Login	0	0微秒	执行失败	未经过实名认证	安全认证
65	2024-06-17 10:26:46	192.168.30.116	root		login root	Login	0	0微秒	执行失败	未经过实名认证	安全认证
66	2024-06-17 10:23:57	192.168.30.116	root		login root	Login	0	0微秒	执行失败	未经过实名认证	安全认证

5.4.2 运维日志详情

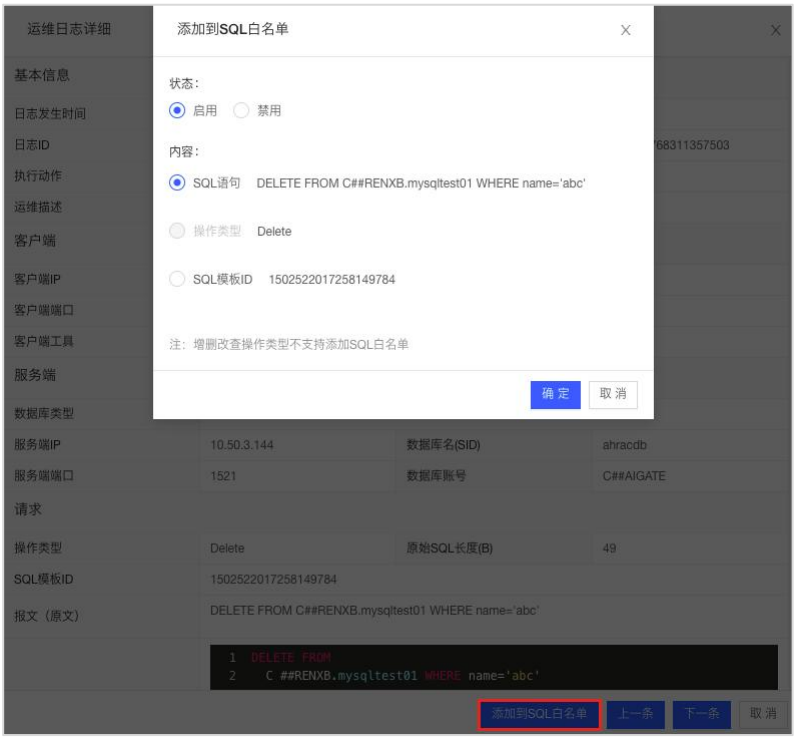
步骤 1. 在菜单栏选择“**查询分析　运维日志**”进入运维日志页面，在运维日志列表中，点击日志条目右侧的<详细>可以查看该运维记录的详细信息，包括运维记录的基本信息、客户端信息、服务端信息、请求详情、返回详情。

步骤 2. 点击审计日志详情窗口右下角的<上一条>或<下一条>可切换查看临近的审计日志。

5.4.3 添加到 SQL 白名单

根据运维日志里的信息，可以选择 SQL 语句、操作类型、SQL 模版 ID 属性生成一条新的 SQL 白名单，对于符合白名单的请求将不再告警。有关 SQL 白名单的更多信息，请参考规则配置。

步骤 1. 在菜单栏选择“**查询分析　运维日志**”进入告警日志页面，在运维日志列表中选择一条需要加到 SQL 白名单的未经过审批的运维日志，点击后方<详情>按钮，在运维日志详细页，点击下方<添加到 SQL 白名单>按钮。



步骤 2. 勾选需要加白的内容后，点击<确定>按钮，会提示操作成功信息。

步骤 3. 在菜单栏选择“**规则配置　信任规则　SQL 白名单**”进入 SQL 白名单页面，查看生成的规则。

5.5　在线会话

会话（Session）是客户端与数据库服务器之间的不中断的 SQL 请求和响应序列。一个会话中可能包含一个或多个 SQL 请求和响应。

步骤 1. 在菜单栏选择“**查询分析　在线日志**”进入在线会话页面，设置查询条件（如资产、会话 ID、客户端 IP、客户端端口、服务端 IP、服务端端口），点击<搜索>即可查询相关在线会话。

针对受信任的会话或长时间处于非活动状态的会话，系统将仅呈现概要信息（四元组）。

5.6　客户端告警

在启用可信应用配置的情况下，当用户身份未经过验证或用户使用的数据库连接工具未经过验证时，系统会生成对应的客户端告警。告警类型分为一下两种：1、未验证客户端：表示客户未安装或登陆安全客户端就请求数据库；2、未知应用拦截：表示用户使用了非可信应用或假冒应用请求数据库。

5.6.1 检索客户端告警

步骤 1. 在菜单栏选择“**查询分析　客户端告警**”进入客户端告警页面，设置查询条件（如时间范围、客户端 IP、客户端 MAC、可信应用 MD5 值等），点击<搜索>即可查询相关客户端告警。

步骤 2. 点击查询条件下方的<更多条件>，在更多条件对话框中勾选需要的查询条件，点击<确认>即可添加相应的查询条件，点击<恢复默认>可以恢复至默认查询条件。

查询条件的说明如下：

选项	说明
告警 ID	唯一标识告警记录的 ID。
客户端 IP	填写客户端 IP 地址。
客户端 MAC	填写客户端 MAC 地址。
客户端工具	填写客户端工具名称。
主机名	填写客户端主机名称。
操作系统用户名	填写客户端操作系统用户名。
假冒应用 MD5 值	填写假冒应用的 MD5 值。
可信应用 MD5 值	填写可信应用的 MD5 值。
告警类型	可选未验证客户端和未知应用拦截。

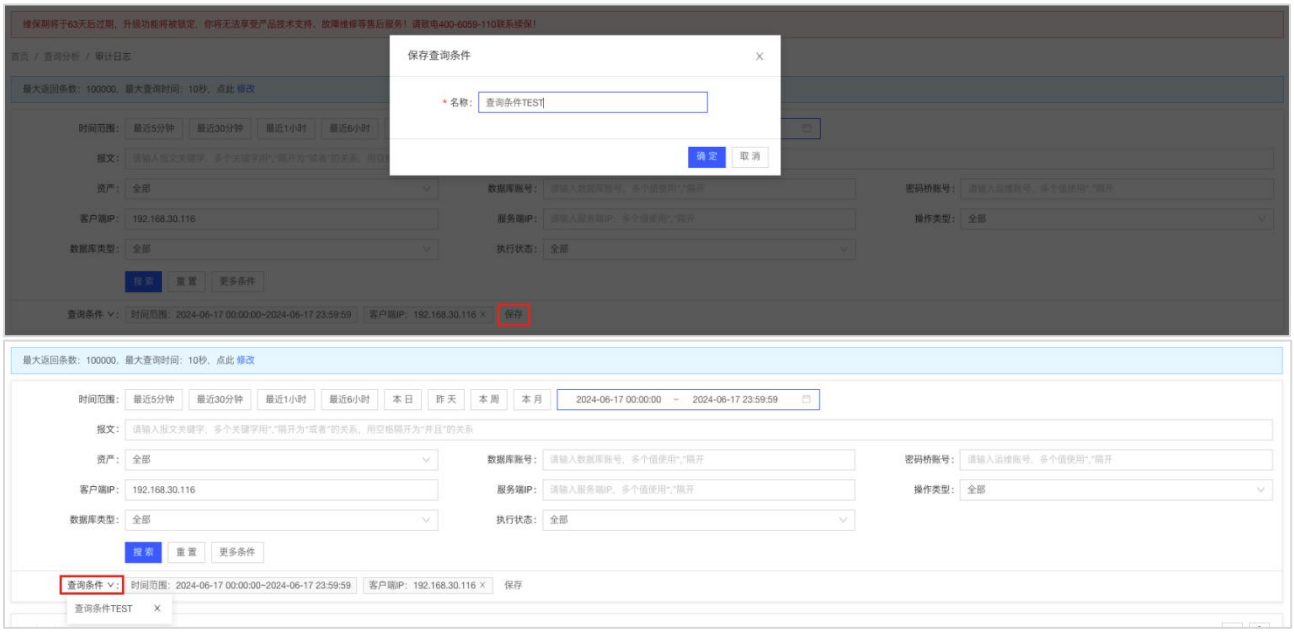
步骤 3. 查询结果显示在查询条件的下方。点击列表右上方<⚙>图标，勾选需要展示的显示列，点击<确定>即可设置查询结果展示的列。

步骤 4. 点击<>按钮，即可根据查询结果下载告警日志，最多支持 10 万条。

	A	B	C	D	E	F	G	H	I
1	记录发生时间	客户端地址	客户端工具	主机名	操作系统用户名	假冒客户端MD5	可信客户端MD5	客户端MAC	告警类型
2	2024-10-09 15:33:34	10.50.111.60	dbeaver.exe	任小兵RENXB	root	d8871f76a2da99c268140	871f76a2da99c26814045	00:0c:29:88:63:04	未知应用拦截
3	2024-10-09 15:24:47	10.11.39.136	dbeaver	MacBook-Pro.local	leah	668969d5633b76f0eefbe	569d5633b76f0eefbe554e	9c:3e:53:87:c4:77	未知应用拦截
4	2024-10-09 15:23:47	10.11.39.136	dbeaver	MacBook-Pro.local	leah	668969d5633b76f0eefbe	569d5633b76f0eefbe554e	9c:3e:53:87:c4:77	未知应用拦截
5	2024-10-09 15:23:37	10.11.39.136	dbeaver	MacBook-Pro.local	leah	668969d5633b76f0eefbe	569d5633b76f0eefbe554e	9c:3e:53:87:c4:77	未知应用拦截
6	2024-10-09 15:12:23	10.11.39.136	dbeaver	MacBook-Pro.local	leah	668969d5633b76f0eefbe	569d5633b76f0eefbe554e	9c:3e:53:87:c4:77	未知应用拦截
7	2024-10-09 15:12:13	10.11.39.136	dbeaver	MacBook-Pro.local	leah	668969d5633b76f0eefbe	569d5633b76f0eefbe554e	9c:3e:53:87:c4:77	未知应用拦截
8	2024-10-09 15:12:07	10.11.39.136	MySQL Connector/J						未验证客户端
9	2024-10-09 14:16:53	10.50.111.60	dbeaver.exe	任小兵RENXB	root	d8871f76a2da99c268140	871f76a2da99c26814045	00:0c:29:88:63:04	未知应用拦截
10	2024-10-09 14:13:34	10.11.39.136	dbeaver	MacBook-Pro.local	leah			9c:3e:53:87:c4:77	未知应用拦截
11	2024-10-09 14:09:24	10.11.39.136	Navicat Premium	MacBook-Pro.local	leah			9c:3e:53:87:c4:77	未知应用拦截
12	2024-10-09 13:54:49	10.11.39.136	Navicat Premium	MacBook-Pro.local	leah			9c:3e:53:87:c4:77	未知应用拦截
13	2024-10-09 13:54:24	10.11.39.136	dbeaver	MacBook-Pro.local	leah			9c:3e:53:87:c4:77	未知应用拦截
14	2024-10-09 13:54:14	10.11.39.136	dbeaver	MacBook-Pro.local	leah			9c:3e:53:87:c4:77	未知应用拦截
15	2024-10-09 13:52:09	10.11.39.136	MySQL Connector/J						未验证客户端
16	2024-10-09 13:50:52	10.11.39.136	MySQL Connector/J						未验证客户端
17	2024-10-09 13:50:49	10.11.39.136	MySQL Connector/J						未验证客户端

5.7 保存查询条件

步骤 1. 搜索完成后，点击查询条件右侧的<保存>按钮，在弹出窗口中填写查询条件名称，点击<确定>即可将本次查询条件组合保存。



5.8 修改查询配置

步骤 1. 在菜单栏选择任意二级菜单进入，点击页面上方蓝色提示框中的<修改>。

步骤 2. 在弹出的修改查询配置对话框中编辑相关信息，点击<确定>，即可修改对应页面查询配置。

详细配置请参见下表：

配置项	说明
最大返回条数	查询时返回查询结果的最大条目数，取值范围：1～1000000，默认为 100000。
最大查询时间	最大查询时长，取值范围：1～3600，单位为秒，默认为 10 秒。查询时间设置过短可能查询不到最大返回条数。

6 报表中心

系统支持使用表格、图表等形式动态显示数据。报表中心通过公式化、逻辑化处理访问审计、告警、脱敏、运维、在线日志等信息后形成各种不同类型的报表数据。

6.1 报表预览

用户可以在生成和导出报表之前，通过报表预览功能查看报表的详细内容，包括数据、图表、统计信息等。

步骤 1. 在菜单栏选择“**报表中心　报表预览**”进入报表预览页面，选择希望查阅的报表类型、资产，报表时间范围，即可生成所需的报表视图。

内置报表类型请参见下表：

报表类型	说明
最大并发会话趋势分析	根据数据库最大并发会话数量的变化趋势使用户了解数据库的使用情况及性能状况。
数据脱敏分析	通过分析一段时间内的数据脱敏的次数，使用户了解敏感数据在系统中的访问和使用情况，确保脱敏措施发挥了其应有的作用。
语句分析类报表	根据 SQL 语句数量变化趋势及 SQL 语句涵盖的操作类型、数据库/SID、客户端 IP、账号等，使用户可以了解数据库的活动信息。
告警分析类报表	从告警趋势分析、告警处理动作分析、客户端工具分析、客户端 IP 分析、数据库账号分析、规则命中分析这 6 个维度分析当前告警情况。
流量分析类报表	支持从数据库或客户端维度查看流量趋势，用于监控和分析数据库的网络流量，了解数据传输的情况和趋势。
运维审批分析报表	从运维审批的 SQL 数量及人员的运维审批任务 2 个维度分析当前运维审批使用的情况。

6.2 报表导出

步骤 1. 在菜单栏选择“**报表中心　报表预览**”进入报表预览页面，选择生成好所需报表后，点击右上角的<导出>，选择导出格式（HTML、PDF、PNG、WORD）弹出下载窗口，等待文件生成成功后，即可点击<下载>将导出文件下载至本地。

6.3 报表订阅

允许用户定期接收生成的报表，以便持续监控和分析数据库的运行状态和安全状况。

步骤 1. 在菜单栏选择“**系统管理　系统配置　通知外送**”进入系统通知外送页面，需要启用并配置邮件发送服务器，详情请参考系统通知外送。

步骤 2. ① 在菜单栏选择“**报表中心　报表订阅**”进入管理订阅任务页面，点击<新增>；② 在菜单栏选择“**报表中心　报表预览**”进入报表预览页面，选择需要订阅报表及资产，点击页面右上角<订阅>。

步骤 3. 在添加订阅任务窗口内编辑相关信息，点击<保存>。

内置报表类型请参见下表：

配置项	说明
任务名称	订阅任务的名字，必须为中文字符、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 64。
收件人邮箱	正确的邮箱格式，可输入多个邮箱地址，使用“,”分隔。
报表类型	内置的多种报表类型，具体以您下拉显示为准。
报表格式	HTML、PNG、PDF、Word 四种格式。
资产	选择报表统计的资产。
任务周期	选择时间（日报、周报、月报和年报）。
发送时间	选择发送时间，具体按选择的任务周期显示。

7 智能分析

智能分析模块，主要是通过一段时间的学习，学习正常的业务模型，生成用户行为模型，可根据行为模型区分出业务侧习惯操作的 SQL 语句，在此基础上针对异常的行为进行告警，此模块不支持阻断。

7.1 行为分析

7.1.1 任务配置

7.1.1.1 新增行为模型学习任务

行为模型学习任务是指系统对用户访问数据库行为进行学习，对用户行为涉及到的资产、数据库、客户端、操作类型等信息进行汇总。具体添加行为模型学习任务步骤如下：

步骤 1. 在菜单栏选择“**智能分析　行为分析　任务配置**”进入行为分析任务配置页面，点击<新增>按钮，弹出行为模型学习配置。

步骤 2. 在**行为模型学习配置**窗口内，填写相关配置。

步骤 3. 如需配置其他更多信息，点击<更多配置>，可配置学习范围（IP）。

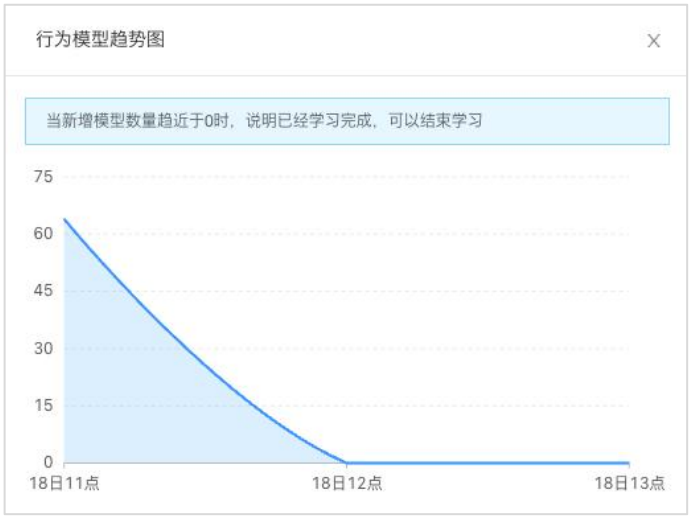
具体配置项请参见下表：

配置项	说明
资产	选择已添加过的资产（单选）。
学习维度	默认已选客户端工具名、数据库账号、客户端 IP、操作系统用户名；可自主勾选客户端主机名、数据库名/SID、操作类型、服务端 IP、表对象。
学习截止时间	默认学习一周，结束后自动停止，可自主选择时间。
告警等级	可选不告警、低风险、中风险、高风险。
学习范围	配置后只学习范围内的客户端 IP 产生的行为，默认学习所有客户端 IP。 支持多个 IP，使用逗号“,“分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20

步骤 4. 配置完成后点击<开始学习>，此时任务状态将更新为“学习中”。系统将智能地分析并学习用户的访问行为模式，一旦学习到数据后，该任务的模型数量将会增加。

7.1.1.2 行为模型趋势图

步骤 1. 在菜单栏选择“**智能分析　行为分析　任务配置**”进入行为分析任务配置页面，点击学习任务条目右侧模型数量字段中的数字，弹出行为模型趋势图窗口。若图中新增模型数量逐渐趋近于 0，这通常意味着系统已经基本完成了对用户访问行为的学习。



7.1.1.3 结束行为模型学习任务

步骤 1. 在菜单栏选择“**智能分析　行为分析　任务配置**”进入行为分析任务配置页面，① 点击任务条目右侧的<结束学习>按钮；② 或等待系统自动到达预定的结束学习时间点。任务结束后，其状态将更新为“告警中”，标志着学习阶段结束，并进入了告警监控的新阶段。

步骤 2. 针对该资产新生成的审计日志，系统会依据先前学习的内容进行智能匹配。对于符合已学习模型的行为，系统将进行正常处理；而对于那些超出已学习模型范围的审计日志，系统将根据预先配置的告警等级，选择性地触发相应告警等级的行为模型告警。

7.1.1.4 其他操作

步骤 1. 选择学习任务点击<重新学习>按钮，弹出学习任务配置窗口（相较于首次新增任务配置时，重新学习配置增添了一个“是否删除老数据”的选项），完成新配置后，行为模型学习任务将立即启动新一轮的学习过程，此时任务状态会自动更新为“学习中”。

步骤 2. 选择学习任务点击<修改告警等级>按钮，可在弹出框中修改告警等级。

步骤 3. 选择学习任务点击<删除>按钮，可删除任务。

7.1.2 模型查询

步骤 1. ① 在菜单栏选择“**智能分析　行为分析　任务配置**”进入行为分析任务配置页面，选择学习任务点击资产名链接跳转至模型查询页面；② 在菜单栏选择“**智能分析　行为分析　模型查询**”直接进入模型查询页面。

步骤 2. 进入模型查询页面后，系统将自动呈现该资产学习行为分析的详尽结果。为了更精确地获取所需信息，您可以选择多样化的查询条件（如客户端工具、操作类型、表对象等），点击<分析>按钮会显示对应的分析结果。

步骤 3. 点击分析结果图中的节点/连线，或者下拉各维度选择节点，即可查看更详细信息。

步骤 4. 除分析外，还支持设置查询条件（如汇总维度、客户端工具、操作类型等），点击<搜索>即可以列表形式查询相关行为的模型信息。

步骤 5. 点击页面蓝色框中的<修改>按钮，弹出最大允许加载数量设置名，修改后点击<确定并重新加载>即可。（有效值：500~300000，不建议配置很大的数值。加载数量过大会导致加载时间很长，同时可能会引发浏览器因内存使用过大而崩溃）

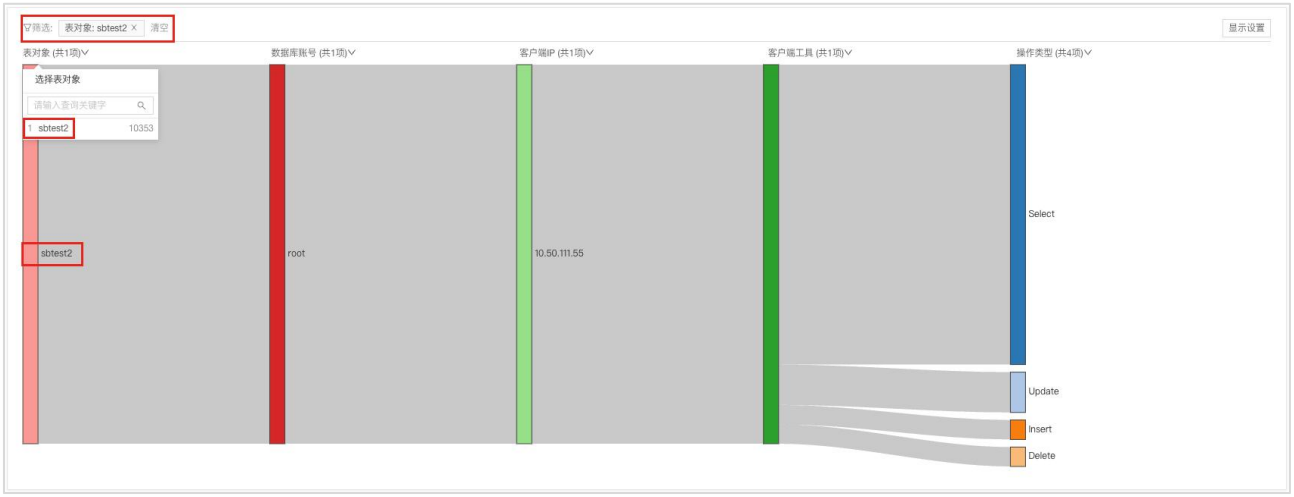
7.1.3 敏感表访问分析

敏感表访问分析是指系统对用户访问敏感数据表（请参考第 4.2 章敏感数据）的行为进行分析。

针对敏感表的访问分析数据，我们设定了每小时的第 05 分钟进行自动统计。

步骤 1. 在菜单栏选择“**智能分析　行为分析　敏感表访问分析**”进入敏感表访问分析页面，您可以选择多样化的查询条件（如客户端 IP、操作类型、表对象等），点击<分析>按钮会显示对应的分析结果。

步骤 2. 点击分析结果图中的节点/连线，或者下拉各维度选择节点，即可查看更详细信息。



8 规则配置

规则配置主要负责定义和管理各种安全策略和操作规则，以确保数据库系统的安全性、合规性。

系统内匹配规则的顺序为：1）安全客户端；2）账号安全，如强管控、实名认证、僵尸账号、账号过期、登录超时；3）数据库隐身；4）信任规则；5）运维审批单；6）身份权限；7）虚拟补丁；8）安全规则；9）动态脱敏。

8.1 安全规则

数据库安全网关对捕获到的数据包进行深度协议解析，精确提取其中的各项字段信息，并与预先设定的安全规则在多个维度上进行细致比对，从而判断 SQL 语句中是否包含异常行为。一旦识别到任何异常行为，系统能够迅速做出响应，并根据预设的访问控制策略对相关操作进行限制或拦截。同时，系统会详细记录这一操作，并生成告警日志，以供后续分析和审计使用。

系统内置了 40 多条安全规则，安全规则与产品版本同步升级。此外，用户可以自定义安全规则。

8.1.1 规则组管理

规则组将多个单独的安全规则进行组合，形成一个统一的管理单元。这样可以简化安全策略的管理过程，使管理员能够更方便地进行规则的配置、调整和维护。

◆ 内置规则组不可编辑或删除。

步骤 1. 在菜单栏选择“**规则配置　安全规则**”进入安全规则页面，页面左侧即为规则组管理模块。点击模块下方<新增规则组>按钮，在显示的输出框内填写规则组的名称，点击<✓>即可。

步骤 2. 选择自定义规则组，点击其右侧的<>按钮，即可对规则组名称进行编辑。

步骤 3. 选择自定义规则组，点击其右侧的<>按钮，即可删除该自定义规则组。

8.1.2 安全规则管理

8.1.2.1 新增安全规则

步骤 1. 在菜单栏选择“**规则配置 安全规则 规则管理**”进入安全规则页面，左侧选择规则组，右侧展示该规则组内的安全规则列表。点击列表上方的 <新增规则>按钮。

步骤 2. 在弹出的新增规则窗口内，根据用户实际需求填写配置项后，点击<保存>。

详细配置项说明请参见下表：

项目	配置项	说明
基本信息	名称	设置规则名称，必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
	描述	规则描述，长度不超过 1000 字符。
	等级	可选高风险、中风险、低风险，默认选择高风险。
	适用场景	默认选择缺省场景，可根据场景进行选择。

项目	配置项	说明
	动作	可选允许访问、命令阻断、会话阻断。 若为旁路部署模式，可选允许访问、会话阻断、IP 阻断。
	规则类型	可选普通规则和统计规则。 ◆ **普通规则**：单条审计记录匹配到普通规则，会触发生成一条普通告警（例如一条 Select 语句，可能会触发一条告警）。 ◆ **统计规则**：指定时间内多次匹配到统计规则，触发至阈值后，会触发生成一条统计规则告警（例如 5 分钟内 10 次 Select 失败，可能会触发一条统计告警），并会为客户端生成一条普通阻断规则。
	统计方式	可选频次统计和累加统计。（统计规则配置项） ◆ **频次统计**：指定时间内匹配统计规则达到累计次数。 ◆ **累加统计**：指定时间内匹配统计规则达到累计行数。
	统计时长	若为频次统计，允许范围 10 秒到 30 分钟，默认 10 秒。 若为累加统计，允许范围 1 分钟到 44640 分钟，默认 1440 分钟。 （统计规则的配置项）
	累计次数	允许范围 2 到 30 次，默认 2 次。 （统计规则-频次统计的配置项）
	累计行数	允许范围 1 到 100000 行，默认 1000 行。 （统计规则-累加统计的配置项）
	累计条件	若为频次统计，可选同一会话、同一客户端 IP、同一数据库账号、同一客户端工具。 若为累加统计，可选同一客户端 IP、同一数据库账号。 （统计规则的配置项）
	阻断时长	允许范围为 1 分钟到 9999 天。 触发统计规则后，生成的阻断规则将具有一定的生效时长。 （统计规则的配置项）
客户端	客户端来源	访问业务类型的客户端 IP 或 IP 组。可填写多个，以逗号“,”分隔。 有关 IP 组的更多信息，请参考 IP 组管理。

项目	配置项	说明
	客户端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例如：10-15,20,25,30-40。
	客户端工具名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可配多个客户端工具名，使用逗号“,”分隔，例：db2bp.exe,javaw.exe,plsqldev.exe。 有关客户端工具名组的更多信息，请参考客户端工具名组管理。
	操作系统用户	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关操作系统用户组的更多信息，请参考操作系统用户组管理。
	客户端主机名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关客户端主机名组的更多信息，请参考客户端主机名组管理。
服务端	数据库账号	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关数据库账号组的更多信息，请参考数据库账号组管理。
	数据库名（SID）	支持字符串匹配、正则表达式匹配。Oracle 数据库输入 SID，其他数据库输入数据库名。 选择字符串，可填多值，多个值间以逗号“,”分隔。
行为	对象组	指定规则所匹配的对象组。 支持“包含任一对象则满足”或“包含所有对象才满足”。 有关对象组的更多信息，请参考对象组管理。 PS：对象组、数据级别、敏感数据类型间是“或”的关系，与其他规则配置是“与”的关系。
	数据级别	多选项，可选一级、二级、三级、四级、五级。
	敏感数据类型	多选项，可选内置类型或后续新增的类型。 支持“包含任一类型则满足”或“包含所有类型才满足”。

项目	配置项	说明
		有关敏感数据类型的更多信息，请参考敏感数据类型。
	操作类型	指定 SQL 语句的操作类型，如 Select、Update、Delete 等。可根据 DDL\DML\DCL 来选择。
	SQL 模板 ID	可填多值，多个值间以逗号“,”分隔。在审计日志详情中可查看。
	SQL 关键字	◆ SQL 关键字：支持以正则表达式方式匹配报文。单击<正则验证>输入表达式和校验内容，单击<提交>，验证输入内容与 SQL 关键字中的正则表达式是否匹配。点击<添加条件>可添加多个关键字。 ◆ 条件运算逻辑表达式：SQL 关键字填写后，此项为必填项。条件间的关系，支持与、或、非、括号运算(&：与；|：或；~：非)。条件使用序号表示，即“1”表示条件 1，例如：1&2，则代表有 2 个 SQL 关键字条件，且两个关键字都要满足才能告警。
	SQL 长度	取值范围 1B~64KB。
	WHERE 子句	是否包含 WHERE，支持三个选项：不判断、有 WHERE 子句、没有 WHERE 子句。WHERE 子句用于提取满足指定条件的 SQL 记录，语法如下： SELECT column_name,column_name FROM table_name WHERE column_name operator value;
结果	执行时长	允许配置从 0 到半个小时之间的任意范围。 SQL 执行时长属于此范围，则触发规则。
	影响行数	允许配置从 0 到 999999999 之间的任意范围，单位为行。 SQL 操作返回的影响的行数属于此范围，则触发规则。 当且仅当关联该规则的资产配置了默认数据源时，配置影响行数维度的规则命令阻断生效。(目前支持 Oracle、Mysql、OceanBase、PostgreSQL、MSSQL、Hive)
	返回结果集	返回结果集：支持以正则表达式方式匹配结果集。单击<正则验

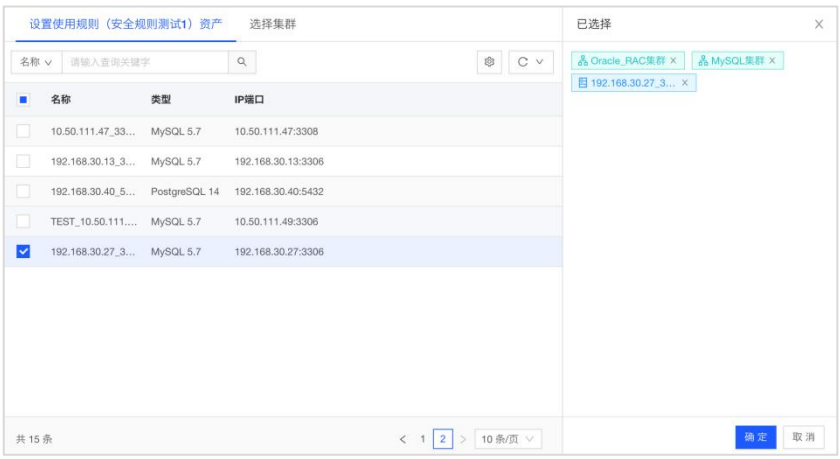
项目	配置项	说明
		证>输入结果集内容，单击<提交>，验证输入内容与返回结果关键字的正则表达式是否匹配。可通过<添加条件>添加多个条件。条件运算逻辑表达式：条件间的关系，支持“与、或、非、括号”运算(&：与；|：或；~：非)，条件使用序号表示，即“1”表示条件 1，例如：1&2，则代表有 2 个结果集条件，且结果集中需要同时满足这两个条件才能告警。
	执行状态	可选全部、成功、失败，默认为全部。
	执行结果描述	支持以正则表达式方式匹配。
其它	生效周期	可自定义或者选择时间组。 自定义时间可选择任意时间、每天、每周、每月或节假日。 有关时间组配置的更多信息，请参考时间组管理。
	生效时间	设定具体的日期和时间范围，以确定其生效时间。 规则的最终生效时间是生效周期和设定时间范围的交集。

8.1.2.2 给安全规则绑定资产

方法一：单条规则绑定资产

步骤 1. 在菜单栏选择“**规则配置　安全规则　规则管理**”进入安全规则管理页面，选择需要启用的安全规则，点击该条目的资产数量字段中的< 0 0 >图标按钮，弹出“设置使用规则资产”窗口。

步骤 2. 在“**设置使用规则资产**”窗口内可选择按“资产”进行绑定，勾选需要绑定的“资产”，点击<确定>。

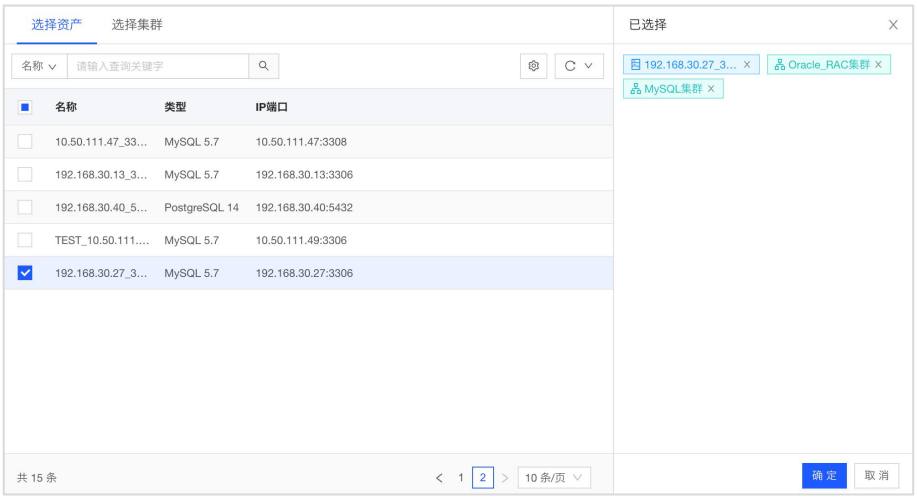


步骤 3. 资产设置成功，该条目对应的“资产数量”字段中的数值将相应地增加。

方法二：多条规则绑定资产

步骤 1. 在菜单栏选择“**规则配置　安全规则　规则管理**”进入安全规则管理页面，勾选多条需要启用的安全规则，点击列表下方的<启用选中项>，弹出“设置使用规则资产”窗口。（<禁用选中项>同理）

步骤 2. 在“**设置使用规则资产**”窗口内可选择按“资产”进行绑定，勾选需要绑定的“资产”，点击<确定>。



步骤 3. 资产设置成功，所勾选的安全规则对应的“资产数量”字段中的数值将相应地增加。

8.1.2.3 给资产启用安全规则

步骤 1. 在菜单栏选择“**规则配置　安全规则　规则启用**”进入安全规则启用页面，在页面上方选择资产，下方列表展示已配置的安全规则。

步骤 2. ① 可点击安全规则列表上方的<启用全部>或<禁用全部>来修改安全规则的启用状态；② 可勾选安全规则，点击列表下方的<启用选中项>或<禁用选中项>来修改安全规则的启用状态；③ 可点击安全规则条目右侧的按钮，调整规则的启用状态。

步骤 3. 安全规则启用状态配置完成后，可点击列表上方的<设置优先级>按钮，可对已启用的安全规则进行优先级设置。支持对单条规则进行<上移>或<下移>操作，支持勾选规则将其<设为最高/最低>优先级，支持勾选规则将其<插到指定规则之前/之后>。

8.1.2.4 其他操作

在菜单栏选择“**规则配置　安全规则　规则管理**”进入安全规则页面，您还可以进行以下操作：

- 编辑安全规则：点击规则条目右边的<编辑>，在“编辑规则”页面可以修改规则的所有配置项，编辑完成后点击<保存>即可。具体字段说明请参考添加安全规则的配置项。
- 删除安全规则：① 点击规则条目右侧的<删除>按钮；② 选中安全规则列表前方的复选框，点击列表下方的<删除>；弹出二次确认窗口，点击<确认>即可。
- 移动安全规则：① 点击规则条目右侧< ··· >按钮，选择<移动分组>；② 选中安全规则列表前方的复选框，点击列表下方的<移动分组>；弹出的窗口内选择规则组，点击<确认>即可。

内置规则不支持编辑、删除、移动分组。

已绑定资产的自定义安全规则不支持删除、移动分组。

8.1.3 安全规则典型配置案例

案例一：实现数据库高危操作的实时阻断

- 案例描述：依托数据库安全网关系统访问控制实现数据库高危操作的实时阻断，阻断规则包括修改表结构、修改用户信息、删除数据库、删除索引、删除表、删除表空间、删除用户、创建索引、创建存储过程、创建表、创建用户、授予权限、重命名、清空表。
- 前提条件：确认您的数据库资产是“入侵防护模式”，若是“入侵检测模式”则只告警不阻断。

步骤 1. 在菜单栏选择“**规则配置 安全规则 规则管理**”进入安全规则管理页面，新增一条名为“高危操作阻断”的安全规则（动作：命令阻断；操作类型：Delete、Drop、Truncate、Alter 等高危操作类型）。配置完成后给该安全规则设置数据库资产。完成后如下图所示，具体请参见安全规则。

步骤 2. 使用反代地址和反向代理端口连接到数据库，尝试 Delete、Drop、Truncate、Alter 等高危操作时，请求将被阻断，并返回“数据库安全网关 reject”错误信息，明确告知您的操作已被安全机制所拦截。被阻断的日志条目将被自动记录到告警日志页面。

案例二：重点数据表单次查询结果不得超过 50 行

- 案例描述：实现数据查询结果返回行数限制，重点数据表单次查询结果超过 50 行则被阻断。
- 前提条件：① 确认您的数据库资产是“入侵防护模式”，若是“入侵检测模式”则只告警不阻断。② 确认您的数据库资产已开启默认数据源配置，以确保与返回行数相关的安全规则配置生效。

步骤 1. 在菜单栏选择“**规则配置　关联数据　对象组**”进入对象组管理页面，新增一个名为“重点数据表”的对象组，并将重点数据表（这里以 table_001、table_002、table_003 为例）添加到对象组中。完成后如下图所示，具体请参见对象组管理。

步骤 2. 在菜单栏选择“**规则配置　安全规则　规则管理**”进入安全规则管理页面，新增一条名为“重点数据表单次查询结果不得超过 50 行”的安全规则（动作：命令阻断；对象组：重点数据表；操作类型：Select；影响行数：大于等于 50）。配置完成后给该安全规则设置数据库资产。完成后如下图所示，具体请参见安全规则。

步骤 3. 使用反代地址和反向代理端口连接到数据库，尝试查询重点数据表 table_001 超过 50 行，请求将被阻断，并返回“数据库安全网关 reject”错误信息，明确告知您的操作已被安全机制所拦截。被阻断的日志条目将被自动记录到告警日志页面。

步骤 4. 尝试查询重点数据表小于 50 行，数据能正常返回。尝试访问非重点数据表，查询超过 50 行，数据也可以正常返回。符合预期。

案例三：一分钟内查询重点数据表次数不得超过 10 次

- 案例说明：实现数据查询次数限制，若在一分钟内查询重点数据表超过 10 次则该客户端被阻断。
- 前提条件：确认您的数据库资产是“入侵防护模式”，若是“入侵检测模式”则只告警不阻断。

步骤 1. 在菜单栏选择“**规则配置　关联数据　对象组**”进入对象组管理页面，新增一个名为“重点数据表”的对象组，并将重点数据表（这里以 table_001、table_002、table_003 为例）添加到对象组中。完成后如下图所示，具体请参见对象组管理。

步骤 2. 在菜单栏选择“**规则配置　安全规则　规则管理**”进入安全规则管理页面，新增一条名为“一分钟内查询次数不得超过 10 次”的安全规则（动作：命令阻断；规则类型：统计规则；统计方式：频次统计；统计时长：1 分组；累计次数：10 次；累计条件：同一个客户端 IP；对象组：重点数据表；操作类型：Select）。配置完成后给该安全规则设置数据库资产。完成后如下图所示，具体请参见安全规则。

步骤 3. 使用反代地址和反向代理端口连接到数据库，尝试在 1 分钟内查询重点数据表 table_001 超过 10 次，请求将被阻断，并返回“数据库安全网关 reject”错误信息，明确告知您的操作已被安全机制所拦截。且在安全规则列表中会自动为该客户端生成一条新的阻断规则，被阻断的日志条目将被自动记录到告警日志页面。

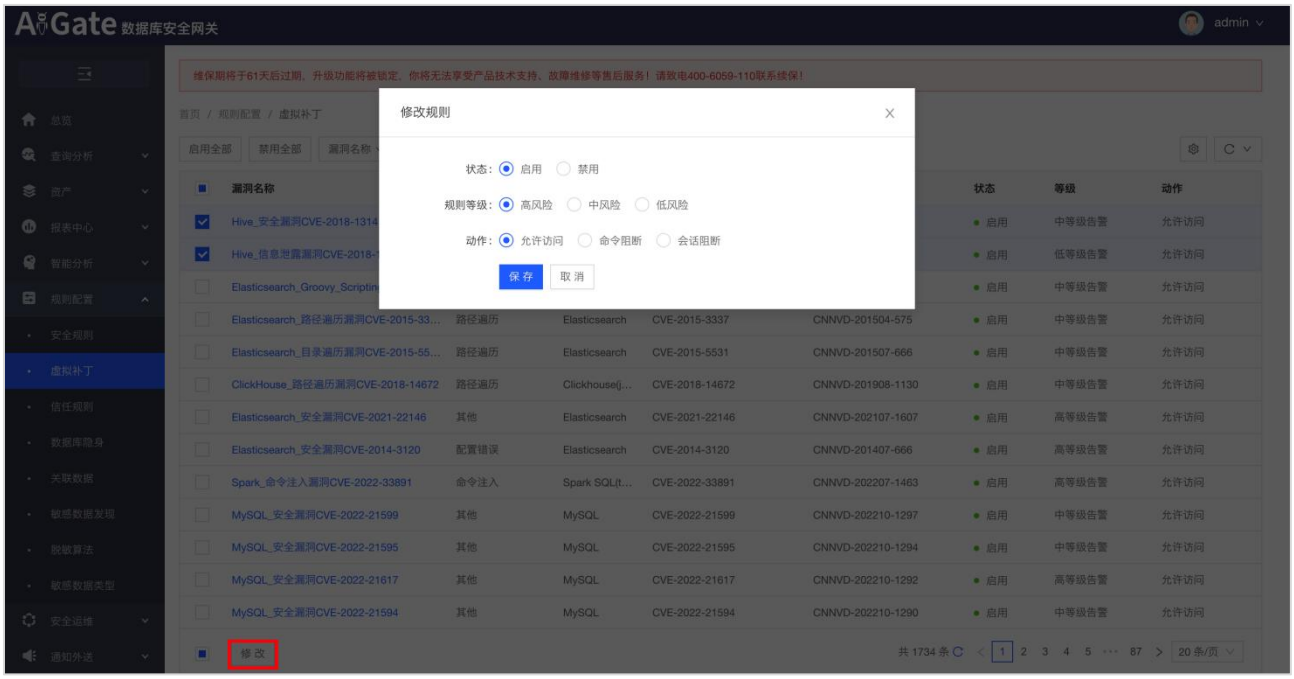
8.2 虚拟补丁

数据库安全网关使用数据库虚拟补丁技术，在一定层面防御黑客利用已公开的数据库安全漏洞攻击数据库，对数据库的安全漏洞起到一定的的防御作用，极大的保护了未升级漏洞补丁的数据库服务器，有效降低了用户数据篡改和泄露的可能。

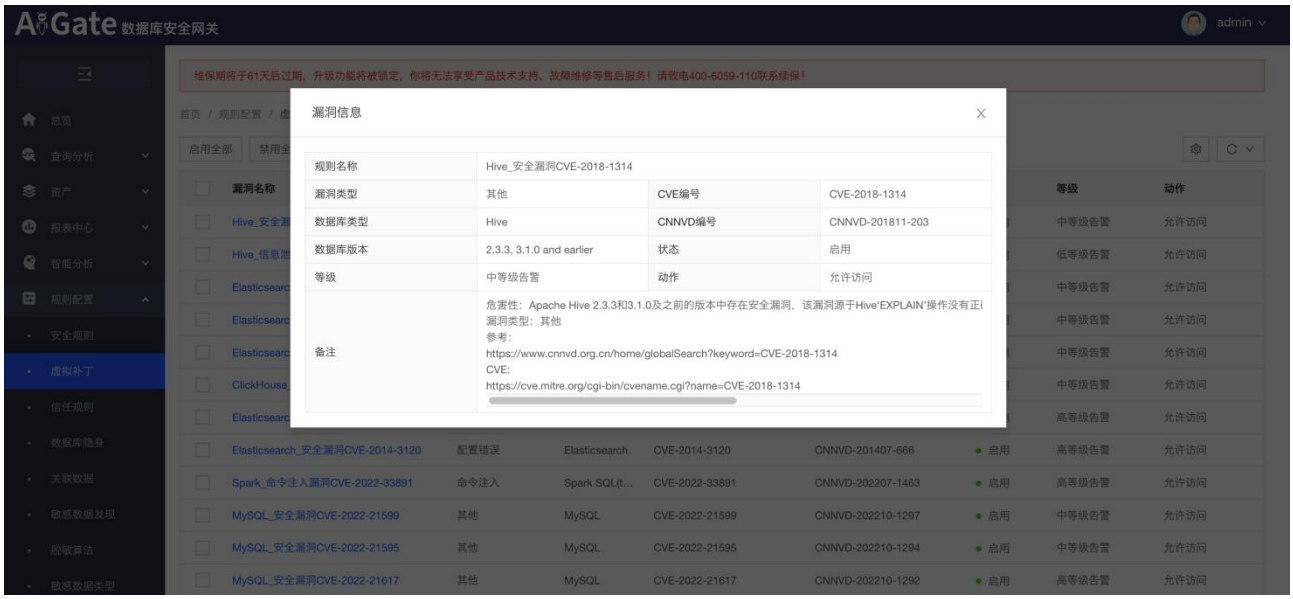
系统内置了超过 1800 条的虚拟补丁，这些补丁均默认启用且允许访问。用户可以在此页面进行一系列操作，包括启用、禁用、修改、查询虚拟补丁，以及查看详细的漏洞信息。以下是具体操作的简要步骤：

步骤 1. 在菜单栏选择“**规则配置　虚拟补丁**”进入虚拟补丁页面，点击列表上方<启用全部>或<禁用全部>来修改虚拟补丁的启用状态。

步骤 2. 勾选虚拟补丁，点击列表下方的<修改>，在弹出的修改规则窗口中，可以对虚拟补丁的状态、规则等级和动作进行修改，修改后点击<保存>即可。



步骤 3. 选择需要查看的虚拟补丁，点击条目中漏洞名称的链接即可查看漏洞详细信息。



8.3 信任规则

数据库安全网关对捕获到的数据包进行深度协议解析，精确提取其中的各项字段信息，并与预先设定的信任规则在多个维度上进行细致比对，从而判断 SQL 语句是否值得信任。若符合规则条件则在生效范围内放行请求，确保其顺畅无阻地通过，同时避免触发任何不必要的阻断或告警。

8.3.1 信任规则管理

8.3.1.1 新增信任规则

步骤 1. 在菜单栏选择“**规则配置　信任规则**”进入信任规则页面，点击列表上方的 <新增>按钮。

步骤 2. 在弹出的新增规则窗口内，根据用户实际需求填写配置项后，点击<保存>。（具体配置项说明请参见安全规则配置项说明）

信任规则特有配置项说明如下：

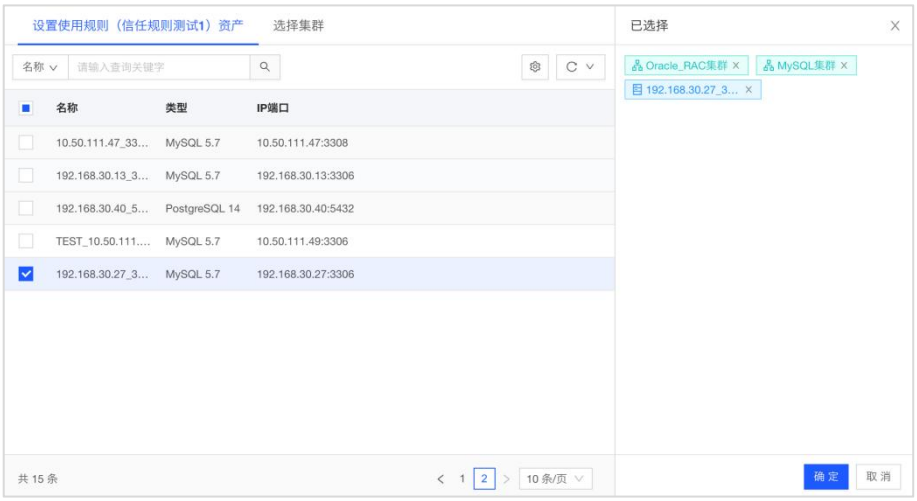
项目	配置项	说明
基本信息	生效范围	支持多选，可选身份权限、虚拟补丁、安全规则、脱敏规则。若匹配上信任规则，则在生效范围内放行该请求。

8.3.1.2 给信任规则绑定资产

方法一：单条规则绑定资产

步骤 1. 在菜单栏选择“**规则配置　信任规则**”进入信任规则管理页面，选择需要启用的信任规则，点击该条目的资产数量字段中的< 0 0 >图标按钮，弹出“设置使用规则资产”窗口。

步骤 2. 在“**设置使用规则资产**”窗口内可选择按“资产”进行绑定，勾选需要绑定的“资产”，点击<确定>。

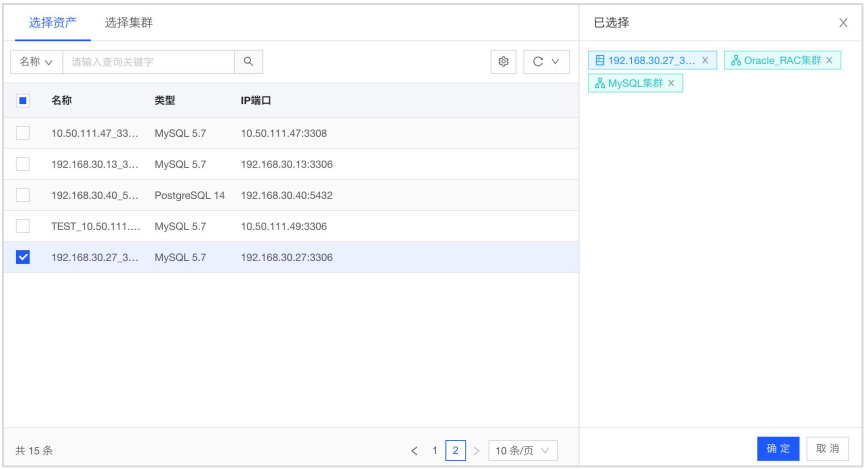


步骤 3. 资产设置成功，该条目对应的“资产数量”字段中的数值将相应地增加。

方法二：多条规则绑定资产

步骤 1. 在菜单栏选择“**规则配置　信任规则**”进入信任规则管理页面，勾选多条需要启用的信任规则，点击列表下方的<启用选中项>，弹出“设置使用规则资产”窗口。（<禁用选中项>同理）

步骤 2. 在“**设置使用规则资产**”窗口内可选择按“资产”进行绑定，勾选需要绑定的“资产”，点击<确定>。



步骤 3. 资产设置成功，所勾选的安全规则对应的“资产数量”字段中的数值将相应地增加。

8.3.1.3 给资产启用安全规则

步骤 1. 在菜单栏选择“**规则配置　信任规则　规则启用**”进入信任规则启用页面，在页面上方选择资产，下方列表展示已配置的信任规则。

步骤 2. ① 可点击信任规则列表上方的<启用全部>或<禁用全部>来修改信任规则的启用状态；② 可勾选信任规则，点击列表下方的<启用选中项>或<禁用选中项>来修改信任规则的启用状态；③ 可点击信任规则条目右侧的按钮，调整规则的启用状态。

8.3.1.4 其他操作

在菜单栏选择“**规则配置　信任规则**”进入信任规则页面，您还可以进行以下操作：

- 编辑信任规则：点击规则条目右边的<编辑>，在“编辑规则”页面可以修改规则的所有配置项，编辑完成后点击<保存>即可。具体字段说明请参考添加安全规则的配置项。

- 删除信任规则：① 点击规则条目右侧的<删除>按钮；② 选中信任规则列表前方的复选框，点击列表下方的<删除>；弹出二次确认窗口，点击<确认>即可。

8.3.2 SQL 白名单

SQL 白名单同信任规则作用一致，区别在于信任规则基于匹配客户端、服务端及行为特征进行判断用户行为是否可信，而 SQL 白名单则是基于具体 SQL 语句、操作类型及 SQL 模版 ID（可在审计日志中查看 SQL 模版 ID）判断用户行为是否可信。若满足 SQL 白名单条件，则放行操作，不进行任何阻断和告警。

8.3.2.1 新增 SQL 白名单

步骤 1. 在菜单栏中选择“**规则设置　信任规则　SQL 白名单**”进入 SQL 白名单页面，点击<添加>。

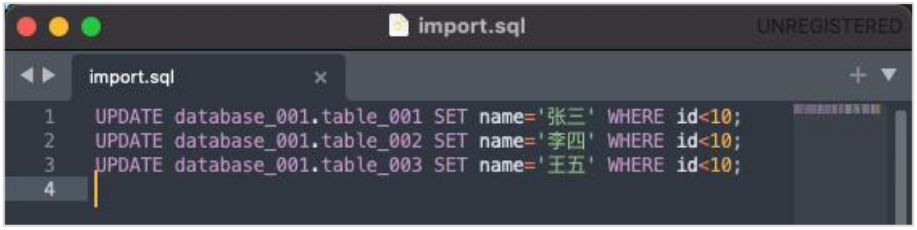
步骤 2. 在弹出新增 SQL 白名单窗口中，填写相关信息，点击<保存>。

具体配置项请参见下表：

配置项	说明
状态	选择启用或者禁用。
类型	支持加白 SQL 语句、操作类型、SQL 模版 ID。
SQL 语句	填写 SQL 语句。
操作类型	可多选数据库操作类型。
SQL 模版 ID	SQL 模板 ID 可以从审计日志或者告警日志中获取。

8.3.2.2 导入 SQL 白名单

步骤 1. 要在您自己的电脑上创建一个导入文件（例如 import.sql），在文件中逐行编写需要加白的 SQL 语句，并确保每条语句都以分号（;）作为结尾。如果 SQL 语句中包含中文字符，请务必检查文件的编码格式是否为 UTF-8。



步骤 2. 在菜单栏中选择“**规则设置　信任规则　SQL 白名单**”进入 SQL 白名单页面，点击<导入 SQL 文件>，选择步骤 1 中的文件进行上传。

8.3.2.3　其他操作

在菜单栏选择“**规则配置　信任规则　SQL 白名单**”进入 SQL 白名单页面，您还可以进行以下操作：

- 启用/禁用 SQL 白名单：① 点击列表上方的<启用全部>/<禁用全部>；② 选中 SQL 白名单列表前方的复选框，点击列表下方的<启用选中项>/<禁用选中项>；可修改 SQL 白名单的状态。
- 删除 SQL 白名单：选中 SQL 白名单列表前方的复选框，点击列表下方的<删除>；弹出二次确认窗口，点击<确认>即可。

8.4　数据库隐身

数据库隐身功能通过一些内置策略，实现了对扫描工具特征的精准识别与智能行为分析。数据库安全网关根据这些策略针对性的下发防漏扫策略，有效地阻断并规避了潜在的扫描行为，从而达到数据库防漏扫的效果。

启用数据库隐身后一旦系统检测到任何扫描活动，它会自动将该用户操作纳入数据库的隐身策略（隐身策略包含三元组，分别为客户端 IP、服务端 IP、服务端端口）中，并触发告警机制。若用户认为识别探测行为有误，可将隐身策略进行加白操作。隐身策略上限为 100 条，隐身白名单上限为 200 条。

8.4.1　数据库隐身策略

步骤 1. 在菜单栏选择“**规则配置　数据库隐身**”进入数据库隐身页面，点击滑块，开启数据库隐身功能。

反代模式下，请确保您已经进行闪灯操作，否则不允许开启数据库隐身功能。

步骤 2. 使用扫描器对数据库资产进行探测扫描。数据库安全网关能够识别到该行为，并自动为被扫描的数据库资产生成相应的数据库隐身策略（包含客户端 IP、服务端 IP、服务端端口），且在页面上方会提供最近新增隐身策略的提示。

步骤 3. 生成隐身策略后，扫描器应无法扫描出数据库的漏洞。且在有数据库隐身策略的前提下，若探测器仍对数据库有所操作将遭到系统阻断，并记录告警日志。

8.4.2 数据库隐身白名单

方法一：手动新增隐身白名单

步骤 1. 在菜单栏选择“**规则配置　数据库隐身**”进入数据库隐身页面，点击白名单列表模块<新增>。

步骤 2. 在新增数据库隐身白名单窗口内，填写相关配置，点击<保存>。

具体配置项请参见下表：

配置项	说明
客户端 IP	必填项，填写客户端的 IP。
服务端 IP	填写需要访问的服务端 IP，一般为资产中已配置的资产 IP。
服务端端口	允许配置范围 1~65535。

方法二：通过自动识别出的隐身策略加白

步骤 1. 在菜单栏选择“**规则配置　数据库隐身**”进入数据库隐身配置页面，点击滑块，开启数据库隐身。

步骤 2. 使用扫描器对数据库资产进行探测，产生数据库隐身策略。

步骤 3. 点击需要加白策略后的<加白>按钮，或是勾选需要加白的策略点击<批量加白>，均可添加白名单。

8.5 身份认证

身份认证模块，必须在“**系统配置　系统联动**”中的 AiTrust 关联配置开启后才展示在规则配置菜单中，具体请参考系统联动。该模块主要是对接零信任后，阻断告警不信任的身份，放行信任的身份。

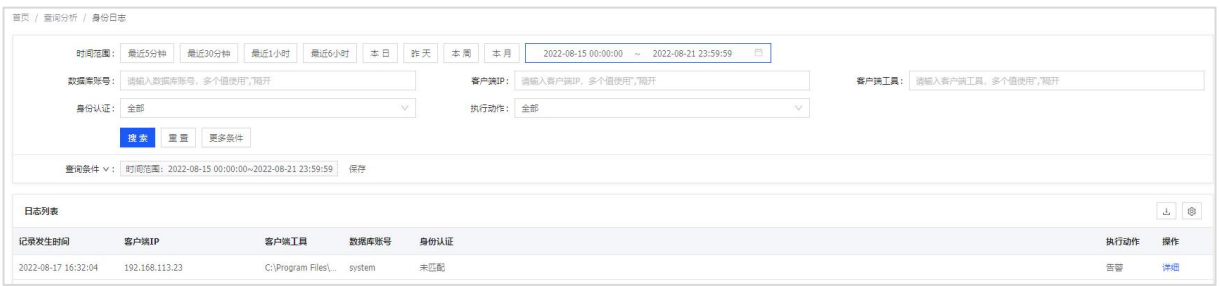
步骤 1. 在菜单栏选择“**规则配置　身份认证**”进入身份认证页面，点击<修改>按钮。

步骤 2. 在弹出的修改身份认证策略的窗口中，修改填写相关配置后，点击<确定>。

详细配置请参见下表：

配置项	说明
状态	可选启用或禁用。
认证策略	同一身份时间间隔设置，5-10080 之间，每次都以 5 分钟增加或减少。其中身份指的是同一客户端 IP、客户端工具、数据库账号等多个维度组合的唯一认证标识。
等级	可选高风险、中风险、低风险。
IP 白名单	可不填，填写后，匹配到直接放行，不会阻断或告警。

步骤 3. 配置完身份认证后，客户端操作未匹配到认证策略，则会产生相应的身份日志。在菜单栏选择“**查询分析　身份日志**”进入身份日志页面查看日志。



8.6　关联数据

关联数据将一些具有相同或类似属性的资源划分到某一个组内，方便对这些资源进行批量设置。系统支持 IP 组、操作系统用户名组、客户端主机名组、客户端工具名组、数据库账号组、时间组和对象组七种类型。

8.6.1 IP 组管理

IP 组管理是为用户提供管理特定组的 IP 集合。如自定义某规则需要在某固定 IP 集合内有效时，可以在 IP 组中加以管理，便于用户在规则中使用。

在菜单栏选择“规则配置　关联数据　IP 组”进入 IP 组管理页面，您可以进行以下操作：

- **新增 IP 组**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
IP	支持多个 IP，使用逗号“,”分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20

- **导入 IP 组**：点击列表上方<下载模版>按钮，打开下载文件按要求填写名称、IP、备注后保存文件，返回 IP 组页面，点击<导入>上传该文件即可。
- **导出 IP 组**：点击列表上方<导出>按钮即可下载 IP 组列表文件。
- **编辑 IP 组**：选择需要修改的 IP 组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除 IP 组**：选择需要删除的 IP 组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该 IP 组，不允许删除。

8.6.2 操作系统用户名组管理

操作系统用户名组管理是为用户提供管理特定组的操作系统用户名集合。如自定义某规则需要在某固定操作系统用户名集合内有效时，可以在操作系统用户名组中加以管理，便于用户在规则中使用。

在菜单栏选择“**规则配置　关联数据　操作系统用户名组**”进入管理页面，您可以进行以下操作：

- **新增操作系统用户名组**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。

配置项	说明
操作系统用户名	支持字符串匹配、正则表达式匹配。 选择字符串时，多个操作系统用户名使用“,”隔开,例如"aaa,bbb"。

- **编辑操作系统用户名组**：选择需要修改的操作系统用户名组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除操作系统用户名组**：选择需要删除的操作系统用户名组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该操作系统用户名组，不允许删除。

8.6.3 客户端主机名组管理

客户端主机名组管理是为用户提供管理特定组的客户端主机名集合。如自定义某规则需要在某固定客户端主机名集合内有效时，可以在客户端主机名组中加以管理，便于用户在规则中使用。

在菜单栏选择“**规则配置　关联数据　客户端主机名组**”进入管理页面，您可以进行以下操作：

- **新增客户端主机名组**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。

配置项	说明
客户端主机名	支持字符串匹配、正则表达式匹配。 选择字符串时，多个客户端主机名使用“,”隔开,例如"aaa,bbb"。

- **编辑客户端主机名组**：选择需要修改的客户端主机名组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除客户端主机名组**：选择需要删除的客户端主机名组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该客户端主机名组，不允许删除。

8.6.4 客户端工具名组管理

客户端主机名组管理是为用户提供管理特定组的客户端主机名集合。如自定义某规则需要在某固定客户端主机名集合内有效时，可以在客户端主机名组中加以管理，便于用户在规则中使用。

在菜单栏选择“**规则配置　关联数据　客户端工具名组**”进入管理页面，您可以进行以下操作：

- **新增客户端工具名组**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。

配置项	说明
客户端工具名	支持字符串匹配、正则表达式匹配。 选择字符串时，多个客户端工具名使用“,”隔开,例如"aaa,bbb"。

- **编辑客户端工具名组**：选择需要修改的客户端工具名组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除客户端工具名组**：选择需要删除的客户端工具名组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该客户端工具名组，不允许删除。

8.6.5 数据库账号组管理

数据库账号组管理是为用户提供管理特定组的数据库账号集合。如自定义某规则需要在某固定数据库账号集合内有效时，可以在数据库账号组中加以管理，便于用户在规则中使用。

在菜单栏选择“**规则配置　关联数据　数据库账号组**”进入数据库账号组管理页面，您可以进行以下操作：

- **新增数据库账号组**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不

配置项	说明
	超过 64 字符。
数据库账号	支持字符串匹配、正则表达式匹配。 选择字符串时，多个数据库账号使用“,”隔开,例如"user1,user2"。

- **导入数据库账号组**：点击列表上方<下载模版>按钮，打开下载文件按要求填写名称、数据库账号后保存文件，返回数据库账号组页面，点击<导入>上传该文件即可。
- **导出数据库账号组**：点击列表上方<导出>按钮即可下载数据库账号组列表文件。
- **编辑数据库账号组**：选择需要修改的数据库账号组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除数据库账号组**：选择需要删除的数据库账号组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该数据库账号组，不允许删除。

8.6.6 时间组管理

时间组管理是为用户提供管理特定组的时间集合。如自定义某规则需要在某固定时间集合内有效时，可以在时间组中加以管理，便于用户在规则中使用。

在菜单栏选择“**规则配置　关联数据　时间组**”进入时间组管理页面，您可以进行以下操作：

- **新增时间组**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

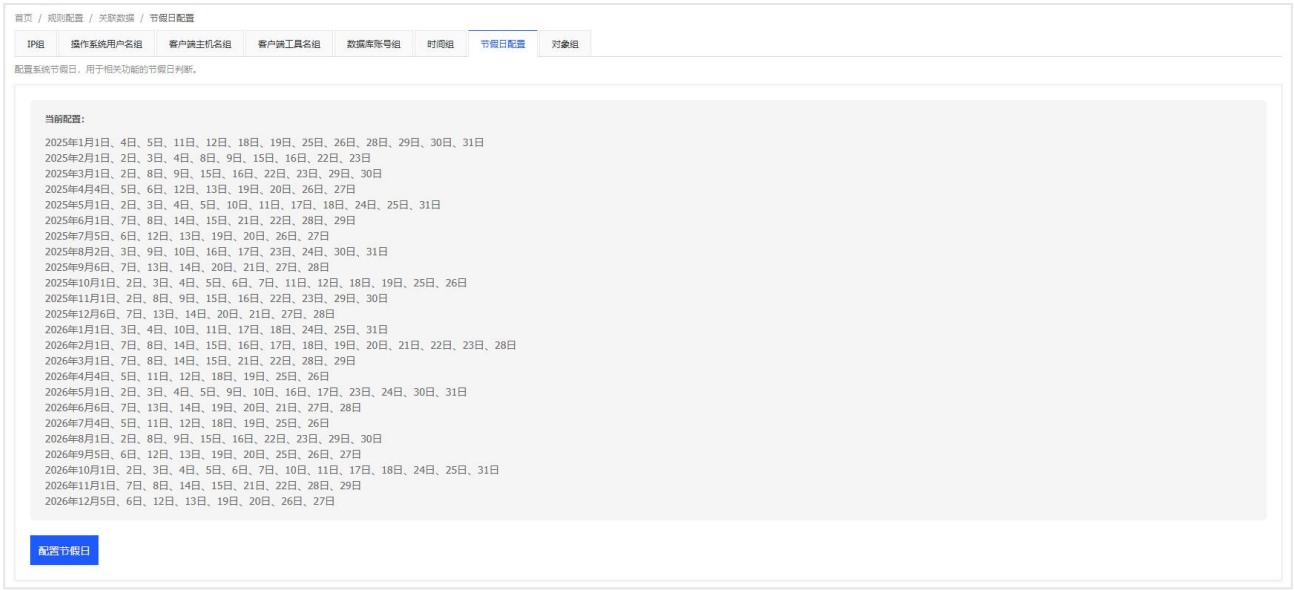
配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
时间	支持选择每天、每周、每月。 每天：需选择每天的几点? 每周：需选择每周的周几？每天的几点? 每月：需选择每月的几号？每天的几点?

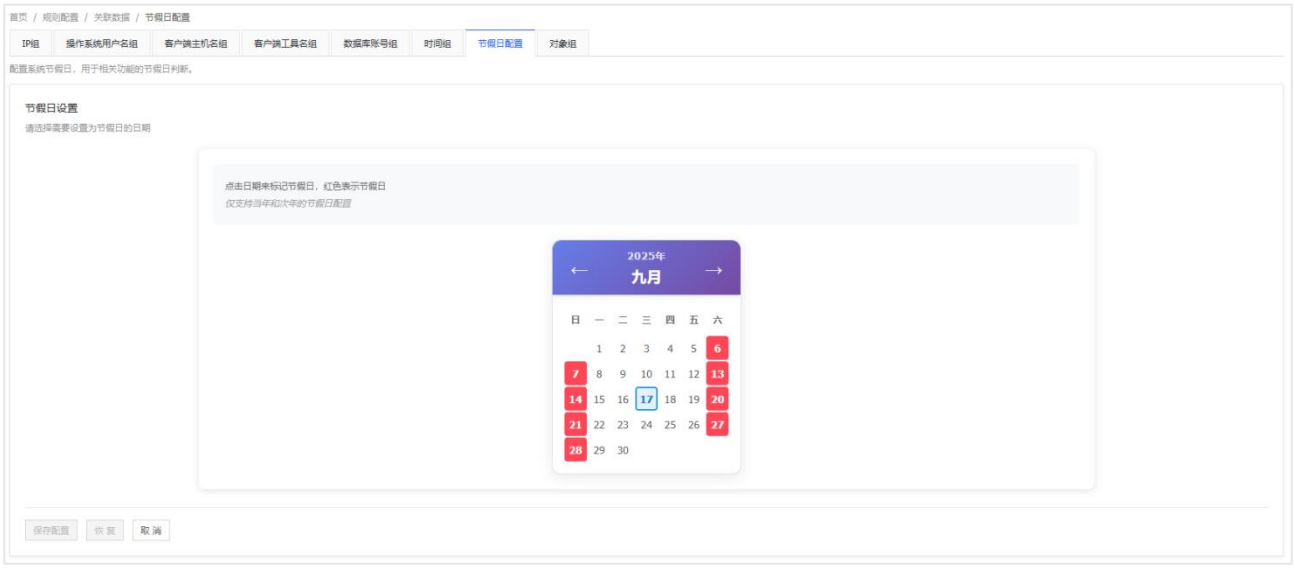
- **导入时间组**：点击列表上方<下载模版>按钮，打开下载文件按要求填写名称、时间范围后保存文件，返回时间组页面，点击<导入>上传该文件即可。
- **导出时间组**：点击列表上方<导出>按钮即可下载时间组列表文件。
- **编辑时间组**：选择需要修改的时间组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除时间组**：选择需要删除的时间组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该时间组，不允许删除。

8.6.7 节假日配置

系统内置近两年节假日默认模板，支持用户根据实际需求灵活调整。配置完成后，这些自定义节假日可作为时间条件参数，应用于各类规则策略中，实现精准的时间控制。

在菜单栏选择“**规则配置 关联数据 节假日配置**”进入节假日配置页面，点击<配置节假日>按钮打开日历界面，单击日期即可标记节假日（红色表示节假日）。完成设置后点击<保存配置>生效，如需撤销本次修改，点击<恢复>按钮即可回退到操作前状态。





8.6.8 对象组管理

对象组管理是为用户提供管理特定组的对象集合。如自定义某规则需要在某固定对象集合内有效时，可以在对象组中加以管理，便于用户在规则中使用。

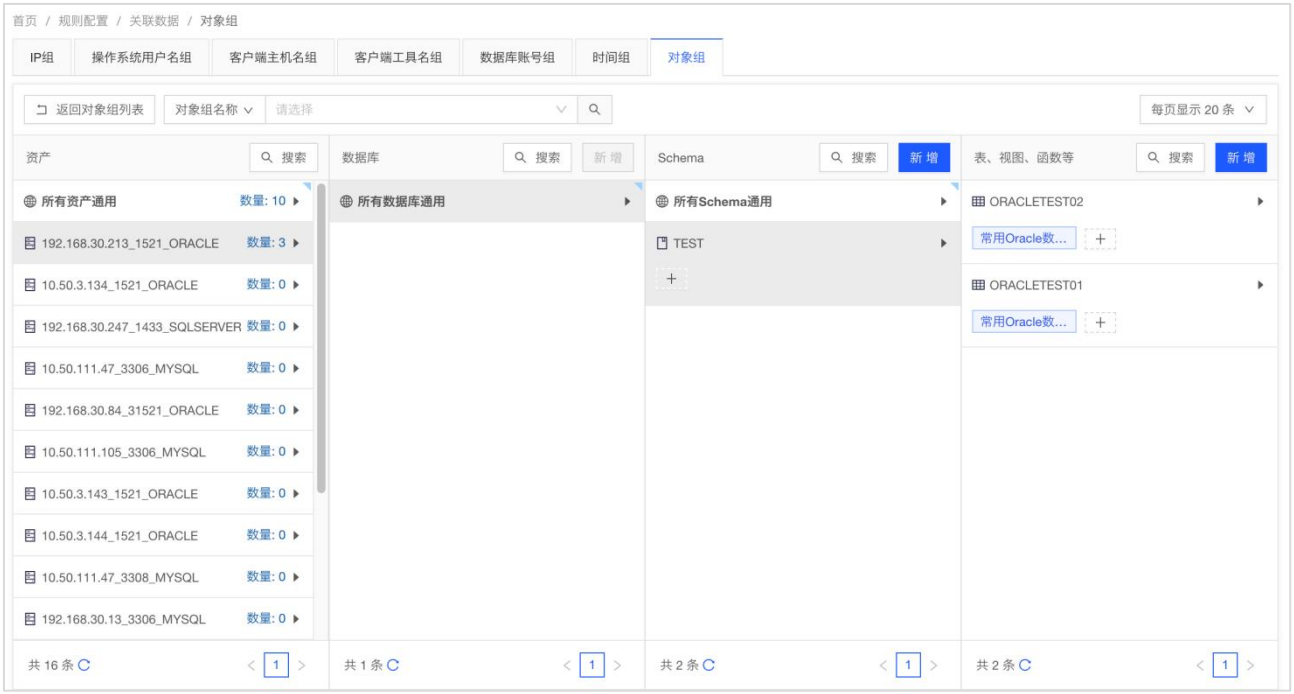
在菜单栏选择“**规则配置　关联数据　对象组**”进入对象组管理页面，您可以进行以下操作：

- **新增对象组**：点击列表上方<新增>按钮，填写对象组名称后，点击<保存并添加对象>。在编辑对象组窗口内，填写数据库相关信息后，点击<添加对象>，可添加多个。添加结束后关闭窗口即可。

详细配置请参见下表：

配置项	说明
所属资产	下拉列表可选择对象组所对应的要选择的资产，默认为所有资产通用。
数据库名	填写数据库名，为空表示所有。选择 Oracle 资产时，该字段不需填写。
Schema	填写 Schema 名称。Schema 可视为同一个使用者所拥有的所有数据库对象之集合。例如：用户 scott 所建立的表 emp,其完整名称为 scott.emp，而 scott 就是 emp 的 schema 名称。所以 schema 其实就是一个 Oracle 数据库的用户名称。
表/用户/视图/存储过程/函数	填写要添加的表名/用户/视图/存储过程/函数，为空表示所有。
字段	填写要添加的字段名，为空表示所有。

- **导入对象组**：点击列表上方<下载模版>按钮，打开下载文件按要求填写对象组名称、资产名称等字段后保存文件，返回对象组页面，点击<导入>上传该文件即可。
- **导出对象组**：点击列表上方<导出>按钮即可下载对象组列表文件。
- **编辑对象组**：选择需要修改的对象组，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除对象组**：选择需要删除的对象组，点击条目右侧的<删除>，在二次确认窗口中点击<确认>。若有规则在使用该对象组，不允许删除。
- **对象管理**：点击列表上方<对象管理>按钮，将切换成联视图的样式展示对象组列表。



8.7 敏感数据发现

数据库安全网关内置多种敏感数据发现规则，如身份证、手机号、邮箱等；用户也可以自定义敏感数据发现规则，可使扫描到的敏感数据类型更精准更多样化。

在菜单栏选择“**规则配置　关联数据　敏感数据发现**”进入页面，您可以进行以下操作：

- **新增敏感数据发现规则**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
规则名称	必须为中文字符、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 30。
状态	启用或者禁用，默认为启用。
发现规则表达式	填写正则表达式，保证该规则生效。
规则验证	填写内容，点击验证。内容正确提示验证成功；内容错误提示验证失败。
默认敏感级别	有一级至五级可以选择，默认为三级

- **导入**：点击列表上方<下载模版>按钮，打开下载文件按要求填写规则名称、发现表达式、默认级别后保存文件，返回敏感数据发现页面，点击<导入>上传该文件即可。
- **导出**：点击列表上方<导出>按钮即可下载敏感数据发现规则列表文件。
- **编辑**：选择需要修改的自定义的敏感数据发现规则，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除**：① 选择需要删除的自定义的敏感数据发现规则，点击条目右侧的<删除>；② 勾选需要删除的自定义的敏感数据发现规则，点击列表下方的<删除>；在二次确认窗口中点击<确认>。
- **启用 / 禁用**：① 选择敏感数据发现规则，点击条目右侧的<启用>/<禁用>；② 勾选敏感数据发现规则，点击列表下方的<启用选中项>/<禁用选中项>；③ 点击列表上方的<启用全部>/<禁用全部>；可对敏感数据发现规则状态进行修改变更。

8.7.1 自定义敏感数据发现规则案例

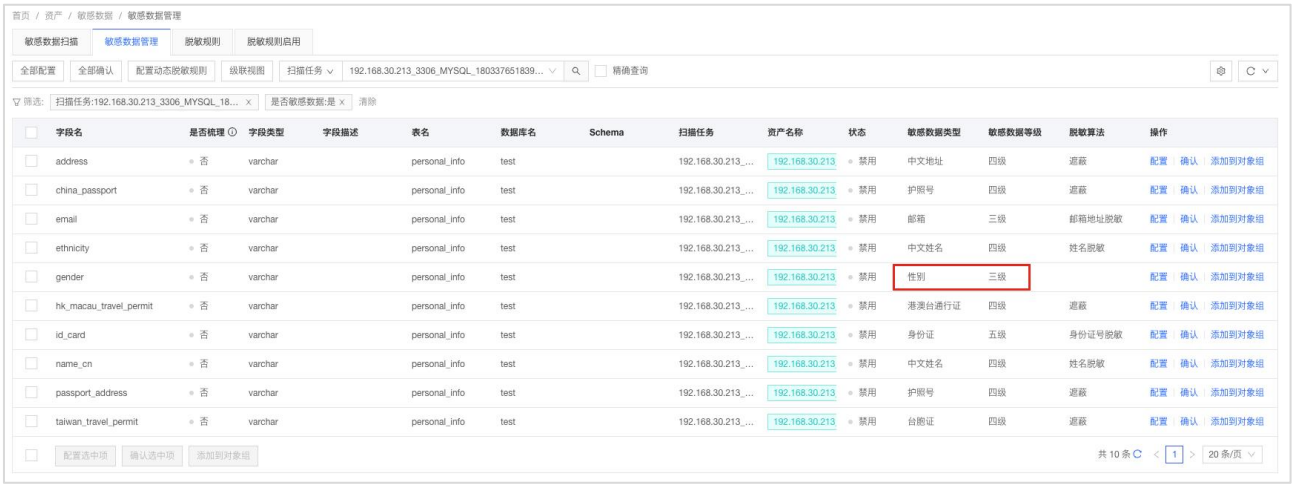
- 案例说明：通过配置自定义的敏感数据发现规则，实现对数据库中“性别”字段的扫描和识别，并给识别到的字段打上敏感数据类型标签。

◆ 前提条件：测试数据库中含有性别字段（如字段名为 gender，字段内容为男或女）。

步骤 1. 在菜单栏选择“**规则配置　关联数据　敏感数据发现**”进入页面，新增一条名为“性别”的自定义规则（发现表达式：男|女）。完成后如下图所示。

步骤 2. 在菜单栏选择“**资产　敏感数据　敏感数据扫描**”进入敏感数据扫描任务页面，为您的数据库资产新增并启用敏感数据扫描任务（确保您扫描的数据表中含有符合性别类型的字段）。完成后如下图所示，具体请参见敏感数据扫描。

步骤 3. 等待扫描任务完成后，点击该扫描任务条目中“配置敏感数据”字段中的数字链接，跳转至“资产　敏感数据　敏感数据管理”页面，查看扫描结果中有字段匹配上“性别”类型。如下图所示。



8.8 脱敏算法

数据库安全网关内置了多种常用的脱敏规则算法，涵盖替换、截断、取整、掩码、加密等，旨在实现对敏感数据的模糊化处理。同时，数据库安全网关也允许用户基于内置的脱敏算法进行个性化配置，灵活添加自定义的脱敏策略，以满足更为精细化的数据处理要求。

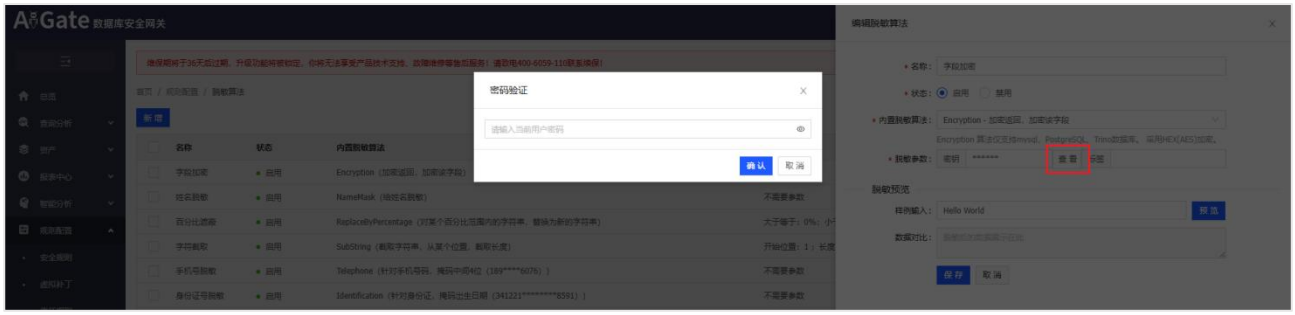
在菜单栏选择“**规则配置　关联数据　脱敏算法**”进入脱敏算法页面，您可以进行以下操作：

- **新增脱敏算法**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
状态	启用或禁用该算法。
脱敏算法	实现数据模糊化的算法。
脱敏参数	根据脱敏算法不同，展示不同参数配置。
样本输入	输入样本信息，可根据脱敏算法，点击预览生成数据对比。
数据对比	点击预览后，生成的脱敏后的结果。

- **编辑脱敏算法：**选择需要修改的脱敏算法，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除脱敏算法**：① 选择需要删除的自定义的脱敏算法，点击条目右侧的<删除>；② 勾选需要删除的自定义的脱敏算法，点击列表下方的<删除>；在二次确认窗口中点击<确认>。
- **启用 / 禁用脱敏算法**：① 选择脱敏算法，点击条目右侧的<启用>/<禁用>；② 勾选脱敏算法，点击列表下方的<启用选中项>/<禁用选中项>；可对脱敏算法状态进行修改变更。
- **查看密钥**：如果内置脱敏算法为“字段加密”，则查看密钥要求输入当前用户密码。



8.9 敏感数据类型

敏感数据类型是指在数据库中包含个人信息、财务数据、商业秘密等需要保护的数据类型，如手机号、身份证、邮箱等。在数据库安全网关系统中，敏感数据类型首要功能在于为通过扫描识别出的元数据（在数据库安全网关中如何获取元数据请参考敏感数据扫描）贴上精确的标识并进行分类处理。

系统已内置了部分敏感数据类型，但这些敏感数据类型固定不可由用户直接添加或删除。为了使用户分类更精准，数据库安全网关提供了 2 中途径拓展敏感数据类型，方法如下：1、用户可自定义敏感数据发现规则，一旦在数据扫描中匹配上这些规则后，将会自动新增该敏感数据类型；2、数据分类分级平台擅长细化数据分类，为每个敏感字段匹配专属的规则名称。数据库安全网关通过与其联动，通过接口自动拉取数据分类分级的扫描数据，并将这些规则名称融入自身敏感数据类型体系。

8.9.1 新增类型方法 1：数据库安全网关中自定义发现

步骤 1. 在菜单栏中选择“**规则配置　敏感数据发现**”进入页面，新增自定义的敏感数据发现规则。完成后如下图所示，具体请参见敏感数据发现。

步骤 2. 在菜单栏中选择“**资产　敏感数据　敏感数据扫描**”进入页面，为您的数据库资产新增并启用敏感数据扫描任务（确保您扫描的数据表中含有符合步骤 1 中敏感数据发现规则的字段）。完成后如下图所示，具体请参见敏感数据扫描。

步骤 3. 在菜单栏中选择“**规则配置　敏感数据类型**”进入页面，查看敏感数据类型列表，新增了步骤 1 中自定义敏感数据发现规则的类型。

8.9.2 新增类型方法 2：数据分类分级同步时新增

步骤 1. 前往“**系统管理　系统配置　系统联动**”页面启用数据分类分级关联配置。

步骤 2. 在菜单栏中选择“**资产　敏感数据　敏感数据扫描**”进入页面，为您的数据库资产新增并启用敏感数据扫描任务，并选择<从数据分类分级扫描数据>，扫描完毕后查看扫描结果。完成后如下图所示，具体请参见敏感数据扫描。

步骤 3. 在菜单栏中选择“**规则配置　敏感数据类型**”进入页面，查看敏感数据类型列表，新增了与数据分类分级中相同的敏感数据类型。

8.9.3 配置脱敏算法

步骤 1. 勾选多个需要配置的类型，点击<配置选中项>，在窗口中选择算法后，点击<保存>。

步骤 2. 选择需要配置的类型，点击<配置脱敏算法>，选择算法后，点击<保存>。

步骤 3. 等待下一次敏感任务扫描，该脱敏算法会直接应用至元数据的脱敏算法字段上。

9 安全运维

安全运维是对运维人员进行精细化访问控制的模块，包括运维人员管理、数据库账号管理、运维权限管理、实名认证、运维审批等功能。以下是有关该模块的一些关键概念：

- **数据库账号**：是指访问数据库资产的原始账号。
- **数据库访问账号**：是指实际访问数据库资产使用的账号，包括原始账号及密码桥账号。
- **运维人员**：属于本系统的用户，主要用于运维申请与审批、做密码桥账号使用、安全认证等。
- **密码桥**：允许在不直接暴露原始数据库账号密码的情况下进行身份认证和授权。在本系统中概括来讲就是将“数据库账号+密码”多对一映射至“运维人员账号+密码”，达到使用该数据库实际账号对应的运维账号登录数据库的目的。
- **安全认证**：功能启用后，数据库安全网关将接管所有的数据库访问账号，若运维人员未使用 Authenticator 身份验证器进行身份认证，则该运维人员所持有的数据库访问账号将无法登录使用。
- **僵尸账号**：是指在预设时间段内没有任何登录或操作记录的数据库访问账号。
- **运维申请与审批**：运维人员提交操作申请，经过审批流程后方可执行，确保所有运维操作都经过审查。
- **身份权限**：通过多因素（客户端 IP、工具、主机名等）验证用户身份，并赋予其适当的权限，确保只有符合身份条件的用户才能在特定数据库中执行权限范围内的操作。

动态脱敏模块（DAS-ABL-数据库安全网关-S-DM）和运维管理功能模块（DAS-ABL-数据库安全网关-S-OP）是需要额外购买的增值功能，标准许可未包含，页面默认隐藏，需要授权激活开启。另旁路模式下这两个功能不支持，页面默认不显示。

9.1 数据库账号

数据库安全网关中数据库账号是指访问数据库资产的原始账号。数据库账号模块主要负责管理和配置数据库账号，用户可以创建新的数据库账号，并填写相关信息如资产、数据库类型、账号和密码。同时支持部分数据库类型的密码桥功能，可以通过开启密码桥开关来设置密码桥账号。

目前支持密码桥功能的数据库有：MySQL、Oracle、MSSQL、PostgreSQL、DM、Kingbase、GBase、MariaDB、GaussDB、Greenplum、TiDB、GoldenDB、UXDB、Doris、HighGo、Teledb-MySQL、Teledb-PostgreSQL

在菜单栏选择“**安全运维　数据库账号**”进入数据库账号管理页面，您可以进行以下操作：

- **新增数据库账号**：点击列表上方<新增>按钮，填写相关配置，点击<保存>。

详细配置请参见下表：

配置项	说明
资产	下拉框选择当前系统内已添加的数据库资产。
数据库类型	选定资产后，该字段自动带出。
数据库账号	实现数据模糊化的算法。
密码	非必填项，填写数据库密码。若启用密码桥后，该字段则必填。
密码桥	支持启用或禁用。使用该账号作为密码桥账号。
测试连接	测试使用填写数据库账号密码是否能正确连接数据库。

一个数据库资产有且仅能有一个密码桥账号。

- **编辑：**选择需要修改的数据库账号，点击条目右侧的<编辑>，按需修改后点击<保存>。
- **删除**：① 选择需要删除的数据库账号，点击条目右侧的<删除>；② 勾选需要删除的数据库账号，点击列表下方的<删除>；在二次确认窗口中点击<确认>。

9.2 数据库访问账号

数据库安全网关中数据库访问账号是指实际访问数据库资产使用的账号，包括原始账号及密码代填的账号。数据库访问账号不可在页面直接添加，需要添加数据库账号或者添加绑定密码桥账号的运维人员后自动生成。

9.2.1 数据库访问账号管理

9.2.1.1 新建数据库访问账号

◆ **方法一：通过新增数据库账号生成**

步骤 1. 在菜单栏选择“**安全运维　数据库账号**”进入数据库账号页面，新增一个数据账号。完成后如下图所示，具体请参见数据库账号。

步骤 2. 在菜单栏选择“**安全运维　数据库访问账号**”进入数据库访问账号页面，查看数据库访问账号管理列表，列表中新增了一个与数据库账号相同的数据库访问账号。

◆ **方法二：通过新增绑定密码桥账号的运维人员生成**

步骤 1. 在菜单栏选择“**安全运维　数据库账号**”进入数据库账号页面，新增一个启用密码桥的 MySQL 数据账号。完成后如下图所示，具体请参见数据库账号。

步骤 2. 在菜单栏选择“**安全运维　运维人员**”进入运维人员页面，新增一个运维人员并绑定步骤 1 新增的密码桥账号。完成后如下图所示，具体请参见运维人员。

步骤 3. 在菜单栏选择“**安全运维　数据库访问账号**”进入数据库访问账号页面，查看数据库访问账号管理列表，列表中新增了一个与运维人员账号相同的数据库访问账号。

删除数据库访问账号同理：不可直接在页面上操作删除，需要删除数据库账号或是运维人员账号后，系统会自动级联删除相关的数据库访问账号。

9.2.1.2 其他操作

在菜单栏选择“**安全运维　数据库访问账号　数据库访问账号**”进入页面，您还可以进行以下操作：

- **变更有效期**：需在“**安全运维　数据库访问账号　账号安全配置**”页面，启用账号有效期后，数据库访问账号列表才会显示<变更有效期>的操作。点击<变更有效期>，可选择修改账号有效期的具体时间，修改后点击<保存>即可。关于账号有效期具体请参考账号安全配置中的账号有效期配置。

- **解除**：需在“**安全运维　数据库访问账号　僵尸账号管理**”页面，启用僵尸账号。当数据库访问账号因长时间未使用等原因被系统自动判定为“僵尸账号”并冻结时，操作列将显示<解除>按钮。点击<解除>按钮，可使该数据库访问账号解除冻结，具体请参见僵尸账号管理。

9.2.2　账号安全配置

数据库安全网关目前支持配置安全认证、登录超时、账号有效期策略，默认都不开启。

- **安全认证**：当启用安全认证后，若运维人员未能及时前往进行身份验证，系统将自动禁止其使用已分配的数据库访问账号进行数据库的登录操作。若验证通过后在验证有效时间段内访问数据库方可登录。
- **登录超时**：当启用登录超时后，若数据库访问账号在设定的时长内未对数据库进行任何操作，系统将自动默认阻断其会话连接，若该账号需要重新进行数据库操作，必须重新进行登录验证。
- **账号有效期**：当启用账号有效期后，新建的数据库访问账号将自动被赋予一个默认的有效期限，一旦账号达到其设定的有效期，系统将自动阻断该账号对数据库的访问权限，直至账号更新有效期。

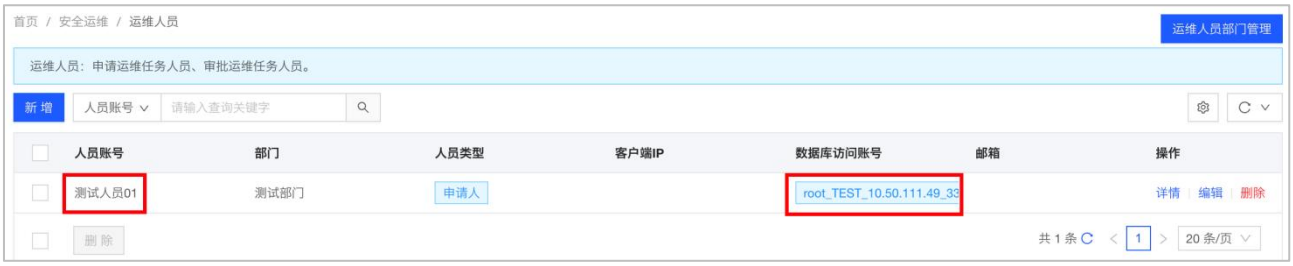
各策略的详细配置请参见下表：

配置项	说明

配置项	说明
安全认证	可启用或禁用，默认禁用。
验证有效时间	有效值 1-43200 分钟，默认 5 分钟，验证通过后该时间段内访问数据库登录方行。
登录超时	可启用或禁用，默认禁用。
登录超时时间	有效值 1-120 分钟，默认 10 分钟，当数据库访问账号超过设定时长对数据库无操作时默认阻断，再次操作需重新登录。
账号有效期	可启用或禁用，默认禁用。
账号有效期时间	有效值 15-9999 天，默认值 180 天，数据库访问账号新建时默认有有效期，若超过有效期则阻断。

9.2.2.1 安全认证典型案例

- 案例描述：数据库帐号登录除帐号密码外还需进行实名认证。
- 前提条件：已创建数据库账号“root”（详细步骤请参考数据库账号）；已创建分配该数据库访问账号的运维人员“测试人员 01”（详细步骤请参考运维人员）。完成后如下图所示：



步骤 1. 在菜单栏选择“**安全运维　数据库访问账号　账号安全配置**”进入页面，点击用户认证模块的<修改>按钮，开启**安全认证**开关，设置验证有效时间，点击<确定>。完成后如下图所示。

步骤 2. 此时安全认证已开启，若用户尝试未经身份验证就直接使用数据库账号进行登录，系统将立即阻断这一非法登录尝试，并自动记录这一行为至运维日志中。

```
[root@localhost ~]# mysql -h192.168.30.33 -P33306 -uroot -p
Enter password:
ERROR 2013 (HY000): Lost connection to MySQL server at 'reading authorization packet', system error: 0
```

步骤 3. 登录创建好的运维人员账号“测试人员 01”，在菜单栏选择“**安全运维　安全认证**”进入页面，点击<立即认证>按钮，在弹出的窗口中输入 6 位验证码，点击<确认>即可完成身份验证。完成后如下图所示，如何获取验证码具体请参见安全认证。

步骤 4. 在预设的有效时间内使用数据库账号进行登录，由于已进行安全认证故登录成功。（若超过预设时间后使用数据库账号进行登录，系统将立即阻断该行为，并自动记录这一行为至运维日志中。）

```
[root@localhost ~]# mysql -h192.168.30.33 -P33306 -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 16705
Server version: 5.7.44 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

步骤 5. ① 若您持续保持步骤 4 建立的连接未断开，那么后续的新连接请求都将成功。② 若您在步骤 4 建立的连接持续未断开超过两小时，那么后续的新连接请求都将失败。③ 若您断开步骤 4 的连接，且超过预设的有效时间范围，那么您也将无法再成功建立新的连接，因为此时安全认证的有效期已经过期。

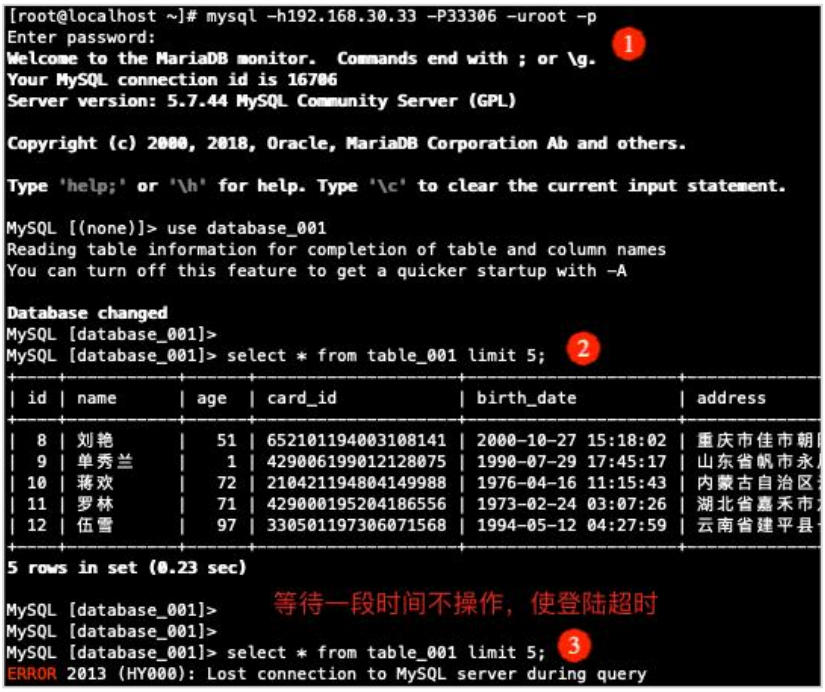
安全认证验证有效期的时间存在 1 分钟误差。

9.2.2.2 登录超时典型案例

- 案例描述：10 分钟内对数据库无操作自动登出帐号，若想继续操作则需重新验证登录。
- 前提条件：已创建数据库账号“root”（详细步骤请参考数据库账号）。

步骤 1. 在菜单栏选择“**安全运维　数据库访问账号　账号安全配置**”进入页面，点击用户安全设置模块的<修改>按钮，开启**登录超时**开关，设置验证有效时间，点击<确定>。完成后如下图所示。

步骤 2. 在登录超时机制已启用的情况下，如果用户成功登录数据库后，在预设的超时时间限制内未能进行任何操作，那么当用户再次尝试进行数据库操作时，系统将视为非法活动，并立即阻断其后续操作。同时，系统会自动记录这一非法登录尝试的详细信息至运维日志中。



登录超时时间存在 1 分钟误差。

9.2.2.3 账号有效期典型案例

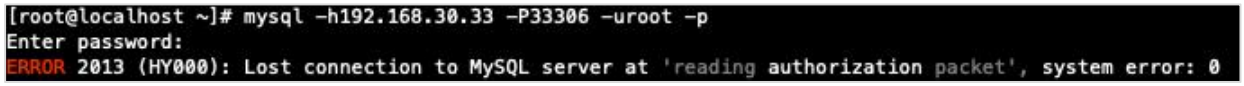
◆ 案例描述：具备帐号默认最长有效期（180 天）管理机制，到期后冻结，申请续期后方可解冻。

◆ 前提条件：已新建数据库访问账号（详细步骤请参考新建数据库访问账号）；

步骤 1. 在菜单栏选择“**安全运维　数据库访问账号　账号安全配置**”进入页面，点击用户安全设置模块的<修改>按钮，开启**账号有效期**开关，设置账号有效期时间，点击<确定>。完成后如下图所示。

步骤 2. 开启账号有效期策略后，返回“**安全运维　数据库访问账号　数据库访问账号**”页面，查看列表中的账号有效期从“永久有效”变更为具体的时间点，且操作列中新增了<变更有效期>按钮。

步骤 3. 若账号有效期已过，则通过数据库访问账号进行登录会被系统阻断。



步骤 4. 在“**安全运维　数据库访问账号　数据库访问账号**”页面，点击该数据库访问账号条目右侧的<变更有效期>按钮，在编辑窗口中修改账号有效期至一个月后。完成后如下图所示。

步骤 5. 此时账号已续期处于有效期内，再次尝试使用数据访问账号进行登录，可登录成功。

```
[root@localhost ~]# mysql -h192.168.30.33 -P33306 -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 16709
Server version: 5.7.44 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

9.2.3 僵尸账号管理

数据库安全网关中僵尸账号是指在预设时间段内没有任何登录或操作记录的数据库访问账号。功能启用后系统会自动检测长时间未使用的账号，并将其标记为僵尸账号。账号被标记为僵尸账号时，系统会发出预警通知邮件，提醒运维人员进行处理。运维人员可以选择冻结或删除僵尸账号，防止其被滥用。除此之外，对于确实需要保留但长时间未使用的账号，可以通过加白操作将其从僵尸账号列表中移除。

在菜单栏选择“**安全运维　数据库访问账号　僵尸账号管理**”进入页面，您可以进行以下操作：

- **配置僵尸账号**：点击<僵尸账号配置>按钮，在配置窗口中启用并编辑配置项后，点击<确定>。

各策略的详细配置请参见下表：

配置项	说明
可疑僵尸账号冻结时间	若数据库访问账号在设置的冻结时间内无任何操作，则被冻结。 账号冻结即判定为僵尸账号，可在僵尸账号管理页面解除冻结。
可疑僵尸账号清理时间	到设置的清理时间后会发送一封邮件，提醒管理员及时清理僵尸账号。 前提条件：需该数据库账号关联的运维人员配置邮箱地址。
僵尸账号预警时间	在数据库访问账号即将成为僵尸账号前，提前一段时间邮件通知管理人员。 前提条件：需该数据库账号关联的运维人员配置邮箱地址。
账号白名单	选择需要加白的数据库访问账号，加白后永久不会被判定为僵尸账号。

- **解除僵尸账号**：选择需要解除的僵尸账号，点击条目右侧的<解除>按钮。账号解除后将从僵尸账号管理列表中删除。判定僵尸账号的冻结时间也将更新。
- **加白僵尸账号**：选择需要解除的僵尸账号，点击条目右侧的<加白>按钮。账号加白后将从僵尸账号管理列表中删除。但加白后在僵尸账号配置窗口中的“账号白名单”字段可见。

9.2.3.1 僵尸账号典型案例

- 案例描述：及时冻结僵尸帐号权限，若账号 30 天内未登录数据库进行操作，则该账号会被系统判定为僵尸账号并冻结，账号被冻结后则无法再登陆数据库。
- 前提条件：已新建数据库访问账号（详细步骤请参考新建数据库访问账号）；

步骤 1. 在菜单栏选择“**安全运维　数据库访问账号　僵尸账号管理**”进入页面，启用僵尸账号配置。详情请参见僵尸账号管理。

步骤 2. 在设置的冻结时间内不使用数据库访问账号进行任何操作，那么数据库访问账号会被系统判定为僵尸账号，可在“**安全运维　数据库访问账号　僵尸账号管理**”页面查看，或在“**安全运维　数据库访问账号　数据库访问账号**”页面查看。

步骤 3. 尝试使用已被识别并标记为“僵尸账号”的数据库访问账号登录数据库时，系统会立即启动安全机制，自动阻断该登录请求，并同步生成详尽的运维日志。

```
[root@localhost ~]# mysql -h192.168.30.33 -P33306 -u测试人员01 -p
Enter password:
ERROR 2013 (HY000): Lost connection to MySQL server at 'reading authorization packet', system error: 0
```

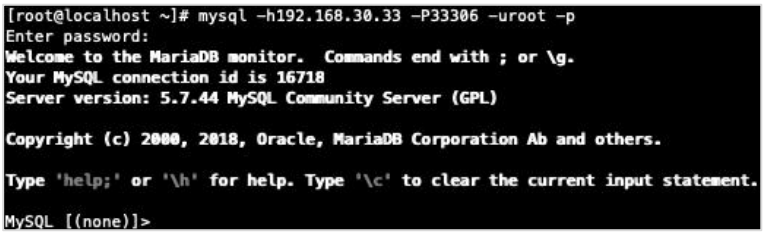
```
[root@localhost ~]# mysql -h192.168.30.33 -P33306 -uroot -p
Enter password:
ERROR 2013 (HY000): Lost connection to MySQL server at 'reading authorization packet', system error: 0
```

步骤 4. ① 在“**安全运维　数据库访问账号　僵尸账号管理**”页面，选择僵尸账号，点击其条目右侧的<解除>按钮；② 在“**安全运维　数据库访问账号　数据库访问账号**”页面，选择是僵尸账号的数据库访问账号，点击其条目右侧的<解除>按钮；账号解除成功后再次使用此数据库访问账号登录数据库执行操作，则操作成功。

```
[root@localhost ~]# mysql -h192.168.30.33 -P33306 -u测试人员01 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 16716
Server version: 5.7.44 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

举例说明：若数据库访问账号在 2024 年 7 月 20 日被判定为僵尸账号，在 2024 年 7 月 25 日被解除冻结。那么当该账号的下一次冻结检测时间为 2024 年 8 月 25 日。

步骤 5. 在“**安全运维　数据库访问账号　僵尸账号管理**”页面，选择僵尸账号，点击其条目右侧的<加白>按钮，在二次确认窗口中点击<确认>账号即可加白。加白后在僵尸账号配置中可查看编辑。账号加白成功后再次使用此数据库访问账号登录数据库执行操作，则操作成功。



9.3 运维人员

在运维管理的流程中，运维人员扮演着至关重要的角色，他们负责维护和执行各项运维任务，确保系统的稳定运行。同时，为了满足不同业务场景的需求，运维申请人可以向系统提交针对不同资产的访问权限申请；运维审批人将根据实际情况对这些申请进行严格的审核，给予通过或驳回的决定。除此之外，针对部分数据库，可启用密码桥功能，做到运维账号一人一密，数据库账号的密码不暴露，数据库密码可定期更换以及在同一运维账号关联多个数据库账号的情况下可对运维人员进行权限控制。

9.3.1 运维人员账号管理

9.3.1.1 新建运维人员

步骤 1. 在菜单栏选择“**安全运维　运维人员**”进入运维人员管理页面，点击<新增>。

步骤 2. 在弹出的添加运维人员窗口中，配置相关信息，点击<保存>即可。

具体配置说明请参见下表：

配置项	说明
人员账号	必须为中文字符、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 64。
密码	长度 8-64，并包含大写字母、小写字母、数字和非字母符号(如@,#,$)。
人员类型	◆ 申请人：申请运维任务； ◆ 审批人：申请和审批运维任务； 申请人和审批人均可支持密码桥账号功能。
所属部门	选择该运维人员所属的部门。 可在“安全运维 运维人员”页面点击<运维人员部门管理>，或在新增运维人员窗口中点击所属部门右侧的<管理>按钮，方可管理部门。
用户有效期	设置运维人员的有效期。若不设置，则视为永久有效；若运维人员已过期，则该用户将无法再登录数据库安全网关系统，已经提交的运维审批任务仍生效。

配置项	说明
数据库访问账号	选择该运维人员所绑定的数据库访问账号，用于后续运维审批或是安全认证。 若该运维人员用来做密码桥使用，则需在新建数据库账号时启用密码桥后（具体操作详见数据库账号）；在新建运维人员时选择“密码桥账号_资产名称”格式的数据库访问账号。
客户端 IP	支持多个 IP，使用逗号“,”分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20
手机号	手机号信息。
邮箱	当新建/取消运维任务时，相关通知邮件都将发送至该邮箱接，收件人可在邮件正文中进行审批操作。 若想使用邮件审批请前往“系统管理　系统配置　通知外送”配置邮箱地址和邮件服务器。具体配置操作请参考系统通知外送。
备注	备注信息。

9.3.1.2 其他操作

在菜单栏选择“**安全运维　运维人员**”进入运维人员管理页面，您还可以进行以下操作：

- **管理运维人员部门**：点击页面右上方的<运维人员部门管理>按钮，在弹出的窗口中支持增删改部门，完成后点击<保存>即可。

- **编辑运维人员**：点击运维人员条目右边的<编辑>，在编辑运维人员窗口可以修改运维人员的所有配置项，编辑完成后点击<保存>即可。

- **删除运维人员**：① 点击运维人员条目右侧的<删除>按钮；② 选中运维人员列表前方的复选框，点击列表下方的<删除>；弹出二次确认窗口，点击<确认>即可。

- **查看运维人员详情**：选择需要查看详情的运维人员，点击该条目右侧的<详情>按钮即可查看。

- **查看运维人员身份信息**：使用运维人员账号登录数据库安全网关系统后，前往“安全运维　身份信息”页面即可查看运维人员具体信息。

9.3.2　密码桥功能

为了做到运维账号一人一密，数据库账号密码不暴露，数据库密码可定期更换，以及在同一运维账号关联多个数据库账号的情况下可对运维人员进行权限控制，数据库安全网关引入了“密码桥”方案。

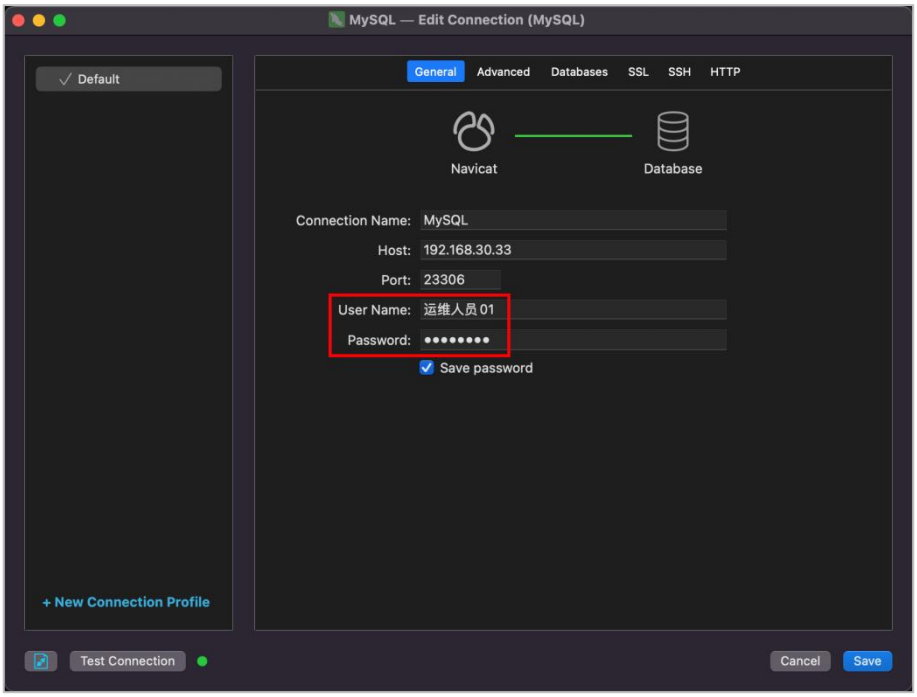
概括来讲就是“运维人员账号+密码”和“数据库账号+密码”在数据库安全网关运维管理系统上已提前配置完成并形成映射关系，此时运维账号通过数据库连接工具（如 DBeaver、Navicat 等）登录数据库，数据库安全网关会在数据库连接过程中对用户密码进行替换（两套账号密码的映射关系），达到使用该数据库实际账号对应的运维账号登录数据库的目的；同时，能对运维账号和密码匹配的正确与否进行校验，也可以对数据库账号和密码的正确性进行校验。

目前支持密码桥功能的数据库有：MySQL、Oracle、MSSQL、PostgreSQL、DM、Kingbase、GBase、MariaDB、GaussDB、Greenplum、TiDB、GoldenDB、UXDB、Doris、HighGo、Teledb-MySQL、Teledb-PostgreSQL

步骤 1. 在菜单栏选择“**安全运维　数据库账号**”进入数据库账号页面，新增 MySQL 资产的数据库账号，填写账号密码并开启密码桥，保存。完成后如下图所示，具体配置操作详见数据库账号。

步骤 2. 在菜单栏选择“**安全运维　运维人员**”进入运维人员管理页面，新增运维人员账号，绑定步骤 1 中新增数据库账号对应的密码桥账号，填写其他参数后保存。完成后如下图所示，具体配置操作详见新建运维人员。

步骤 3. 使用本地客户端工具连接数据库资产，填写反向代理地址和端口，并填写步骤 2 中运维人员的账号和密码进行登录。



步骤 4. 登录成功后前往“**查询分析　审计日志**”页面，可查看登录所用的密码桥账号及原生数据库账号。

9.3.3 安全认证

由于安全认证功能的案例已在章节 9.2.2 账号安全配置中进行了详尽的描述，因此本章节将不再重复讨论安全认证案例，而是说明如何获取安全认证所需的验证信息。

安全认证有两个状态：① 未认证：当前账号未经过身份认证，禁止登录访问数据库资产。② 认证成功：在认证有效期内允许使用该账号所绑定的数据库访问账号登录访问数据库资产。

用户需要在“安全运维数据库访问账号账号安全配置”页面中启用安全认证功能后，“安全运维安全认证”菜单才会对运维人员可见。

步骤 1. 在菜单栏选择“**安全运维　数据库访问账号　账号安全配置**”进入页面，点击用户认证模块中的<修改>按钮，开启安全认证开关，设置验证有效时间，点击<确定>保存。

步骤 2. 在菜单栏选择“**安全运维　运维人员**”进入页面，新增运维人员并关联数据库访问账号，填写其他条件后保存即可。完成后如下图所示，具体请参见新建运维人员。

步骤 3. 使用此运维人员账号登录数据库安全网关系统后，鼠标悬停于右上角的头像后，点击<我的信息>。进入信息页面后可查看该运维人员的认证二维码。

步骤 4. 使用 Authenticator 身份验证器（可在手机应用商店中搜索下载）中的“扫描 QR 码”功能扫描此二维码进行绑定。（具体步骤可点击安全认证流程后的<下载文件>按钮，下载流程文件进行查看）

步骤 5. 在菜单栏选择“**安全运维　安全认证**”进入页面，此时账号还处于未认证状态。点击<立即认证>按钮，在弹窗中输入 Authenticator 身份验证器生成的六位验证码点击<确认>即可完成认证。

步骤 6. 在用户首次认证成功后，个人信息中将不再展示二维码，而是展示<重新生成>的按钮。若点击此按钮，会重新生成一个新的二维码，且使步骤 4 中的认证失效。

若验证码正确但无法通过认证，需要检查设备时间和时区设置是否正确。

9.3.4　运维申请与审批

用户在执行其身份权限外的操作时需要进行运维审批。数据库安全网关系统内置了一套审批流程，包括申请、审核、批准这三个环节。审批过程中，操作请求会被提交给具有相应权限的运维审批人进行审查，确定操作的必要性和合理性后，方可执行申请的操作。

通过多层审批机制，可以有效防止恶意攻击或内部人员的误操作，降低数据库被不当访问或修改的风险。除此之外，审批流程中记录的操作申请和批准历史，为后续的审计和事件调查提供了详细的审计线索，便于追踪操作的责任人和决策过程。

9.3.4.1　日志查询

“查询分析”模块为运维人员提供专属的审计追溯功能。运维人员可在此集中查看其通过密码桥账号执行的所有操作日志，包括告警日志、脱敏日志及运维日志。该功能旨在帮助运维人员精准定位因安全规则或身份权限不足导致的操作拦截，以及因脱敏规则引发的数据遮蔽问题，从而为申请调整权限或策略提供确凿依据，高效解决运维障碍。

步骤 1. 使用运维人员账号（申请人或审批人均可）登录数据库安全网关系统。

步骤 2. 在菜单栏选择“**查询分析　告警日志/脱敏日志/运维日志**”进入页面，支持按条件检索及查看日志详情，具体内容请参考查询分析模块。

步骤 3. 若需为被拦截的 SQL 语句申请权限，可直接点击该日志条目的<申请工单> 按钮。系统将自动跳转至申请页面，并预填充该日志条目的关键信息（如资产、运维 SQL），简化运维人员的操作。

9.3.4.2　运维申请

步骤 1.　使用运维人员账号（申请人或审批人均可）登录数据库安全网关系统。

步骤 2. 在菜单栏选择“**安全运维　运维审批　我的申请**”进入页面，点击<添加>按钮，在弹出的新增运维申请窗口中，填写相关配置项，点击<保存>即可。

具体配置项请参见下表：

项目	配置项	说明
基本信息	紧急度	可选低等级、中等级、高等级。
	申请说明	填写申请运维任务的理由。
客户端身份	客户端身份类型	必选项，多选。可选择数据库访问账号、运维 IP。
	数据库访问账号	选择客户端执行请求所用的数据库访问账号。 下拉框内仅支持选择该运维人员所绑定的数据库访问账号，可在“安全运维　运维人员”页面新增/编辑运维人员时配置数据库访问账号。
	运维 IP	填写运维人员使用的 IP。 如果运维人员信息内填写了此项，新增运维任务时会自动带出。
动态脱敏	明文访问	勾选后，满足运维审批的语句可以明文查看实际数据。
运维对象	运维资产	选择客户端执行请求所属的数据库资产。 若选择了数据库访问账号，则该字段会自动带出对应的资产。
	运维内容	运维对象和运维 SQL 二选一。
	运维对象	手动配置：填写执行请求的 Schema 库表（至少填写一项）
		对象组选择：选择配置好的对象组（具体配置参考对象组管理）
	SQL 操作	多选项，如 Select、Update、Delete 等。可根据 DDL\DML\DCL 来选择。
	自动执行	可勾选是否让系统自动执行审批的运维 SQL。 若选择自动执行选项，则必须确保运维资产已预先配置有正确的默认数据源，否则系统将无法成功连接到数据库。此外，自

项目	配置项	说明
		动执行操作将严格遵循预设的运维审批时间，在到达该时间点后才会触发执行。
	运维 SQL	◆ 添加方式：支持在文本框手动填写后点击 <添加>，或直接导入 SQL 文件。 ◆ 批量处理特性：无论在何种方式下，一旦启用“多条自动分隔”功能（默认以分号;为分隔符，也可自定义分隔符），系统即可自动将内容分割为多条独立的 SQL 语句添加至列表。
	服务名	此字段仅在“自动执行”功能已开启，且资产所配置的 Oracle（18c 及以上版本）数据源包含多个服务名的环境下显示。
运维时间与审批人	运维时间	选择运维任务的起始和结束时间。
	执行次数	配置的有效范围是 1-9999 次，不配置表示不限制执行次数。
	一级审批人	选择一级审批人。
	二级审批人	选择二级审批人。需一级审批后，二级才可审批。
	抄送	抄送该运维任务至相关人员。

9.3.4.3 运维审批

步骤 1. 使用运维人员账号（审批人）登录数据库安全网关系统。

步骤 2. 在菜单栏选择“**安全运维　运维审批　我的审批**”进入页面，选择审批状态为待审批的运维任务，点击条目右侧的<审批>按钮，弹出运维任务审批详细框，填写审批意见后，可选择<审批通过>或者<审批驳回>。

9.3.4.4 其他操作

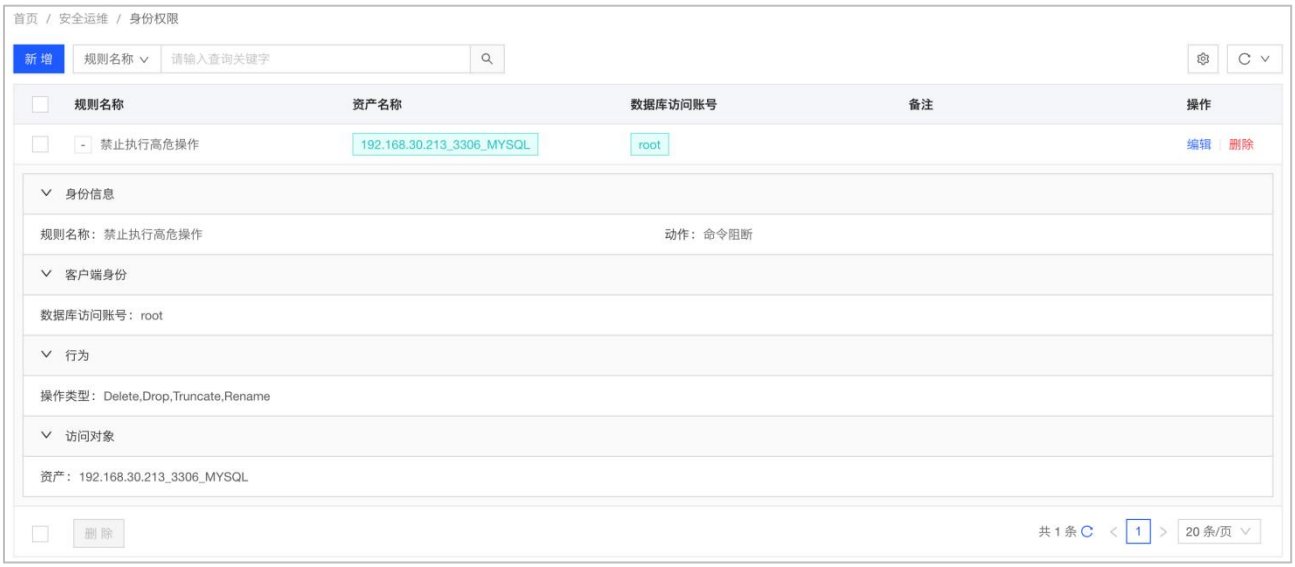
- **复制运维任务**：在“**安全运维　运维审批　我的申请**”页面，可选择列表中已存在的运维任务，点击其右侧的<复制>按钮，可在弹出的新增运维任务窗口内自动填入被复制任务的信息。
- **取消运维任务**：在“**安全运维　运维审批　我的申请**”页面，选择运维任务点击其右侧的<取消任务>按钮，在弹出窗口内填写取消说明后，点击<确定>即可。取消后该任务将不再需要往下审批，审批人可看到任务为取消状态及取消说明；若任务已审批通过后取消，则该运维任务将不再生效。

- **查看审批任务**：在“**安全运维　运维审批　我的申请/我的审批/抄送我的**”页面，点击运维任务条目右侧的<查看>按钮可查看详细信息及审批进度。

9.3.4.5　运维申请与审批典型案例

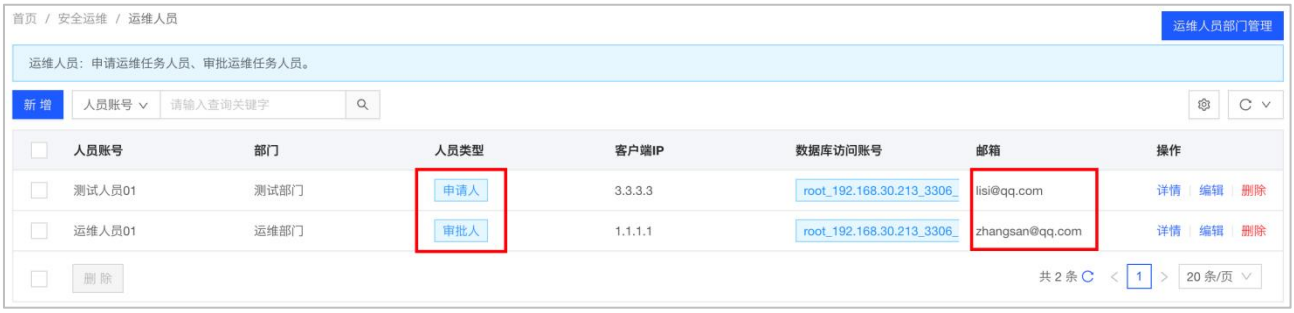
- 案例描述：实现用户高危操作报备审批机制，并将审批流程通过邮件通知到相关运维人员进行处理。
- 前提条件：在“系统管理　系统配置　通知外送”页面配置邮件发送服务器，请参考系统通知外送。

步骤 1. 请参考身份权限案例新增一条身份权限配置。完成后如下图所示。

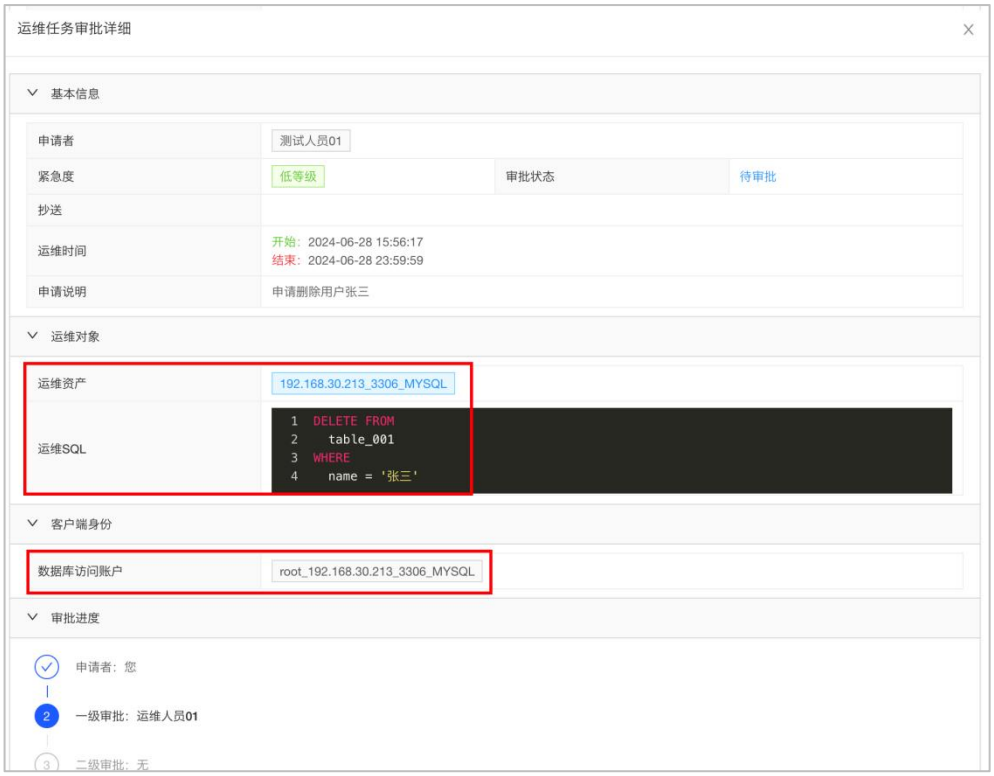


步骤 2. 此时使用反代地址和反向代理端口连接到数据库，尝试 Delete、Drop、Truncate、Alter 等高危操作时，请求将被阻断并记录运维日志。

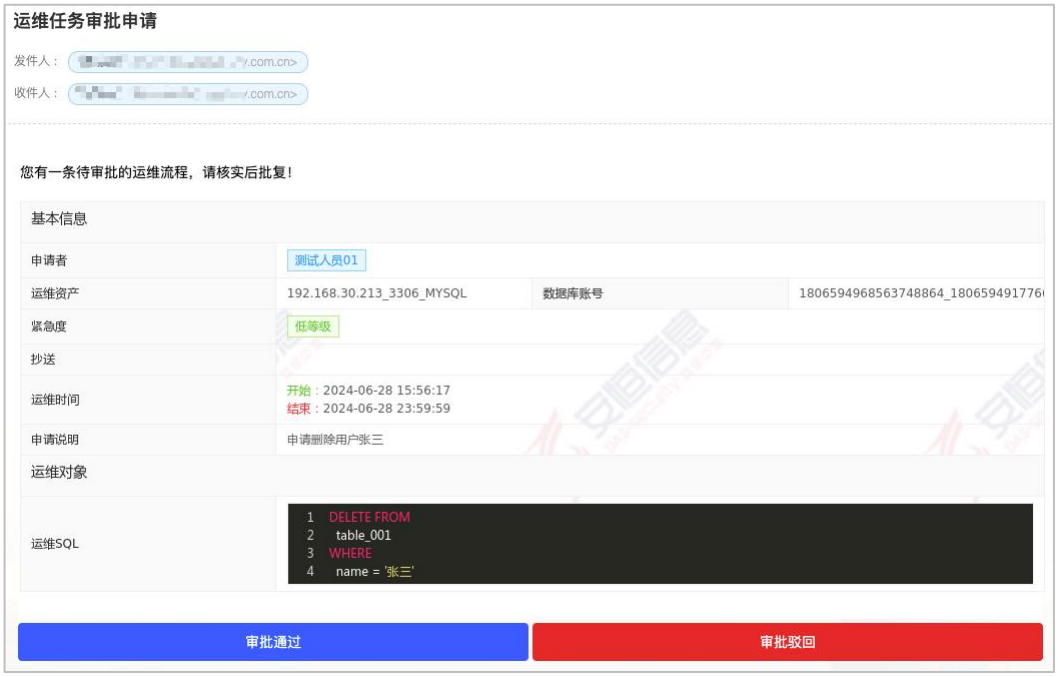
步骤 3. 在“**安全运维　运维人员**”页面分别新建运维申请人和审批人，选择绑定数据库访问账号，并填写邮箱便于后续进行邮件审批。完成后如下图所示，具体步骤请参考新建运维人员。



步骤 4. 登录运维申请人账号，在“**安全运维　运维审批　我的申请**”页面新增运维任务，选择客户端身份并填写运维 SQL（步骤 2 所执行的高危操作语句）及其他配置。完成后如下图所示，具体请参考[运维申请]。

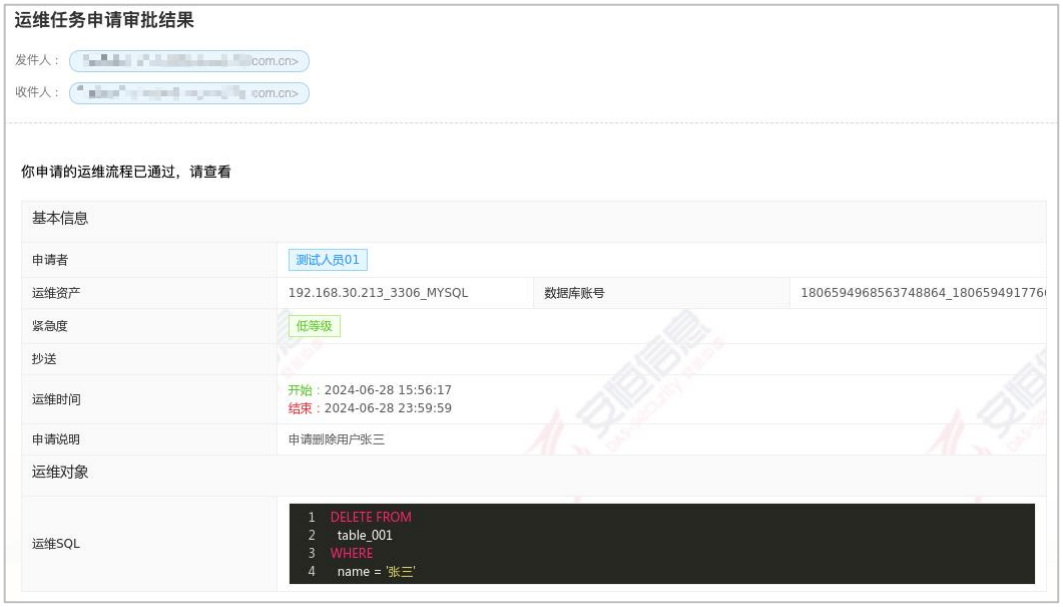


步骤 5. 由于配置了邮箱发送服务器以及运维人员邮件审批功能，故运维审批人的邮箱内将收到一封运维申请的邮件，运维申请人可在邮件内选择审批通过或驳回。



步骤 6. （若运维审批人已在步骤 5 的邮件中进行审批，则跳过该步骤）登录运维审批人账号，在“**安全运维　运维审批　我的审批**”页面选择步骤 4 中的运维任务进行审批且审批通过。完成后如下图所示，具体请参考运维审批。

步骤 7. 运维任务审批过后，运维申请人也将收到一封运维任务审批结果的邮件。



步骤 8. 审批通过后重复步骤 3 操作，尝试 Delete、Drop、Truncate、Alter 等高危操作时，请求被放行并记录运维日志。

9.4 身份权限

身份权限模块用于细致管理和控制用户的访问权限，通过多因素（如数据库访问账号、客户端 IP、工具名等）认证验证用户身份，并根据身份分配相应的权限，确保只有授权用户才能访问和操作特定数据库资源。

9.4.1 新建身份权限

步骤 1. 在菜单栏选择“安全运维　身份权限”进入身份权限页面，点击<新增>按钮。

步骤 2. 在弹出的新增身份权限窗口中，编辑相关信息（至少选择一个客户端身份），点击<保存>即可。

具体配置项请参见下表：

项目	配置项	说明
基本信息	规则名称	必须为中文、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 64。
	备注	填写规则的备注信息。
	动作	可选命令阻断或会话阻断。 若资产不支持命令阻断，则配置后也无拦截效果，仅产生运维日志。
客户端身份	数据库访问账号	选择客户端使用的数据库访问账号。 关于数据库访问账号的更多信息请参考数据库访问账号。
	客户端来源 IP	支持字符串匹配、IP 组匹配。 支持多个 IP，使用逗号“,”分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20 有关 IP 组的更多信息，请参考 IP 组管理。
	客户端工具名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可配多个客户端工具名，使用逗号“,”分隔，例：

项目	配置项	说明
		db2bp.exe,javaw.exe,plsqldev.exe。 有关分组选择的方式，请参考客户端工具名组管理。
	操作系统用户名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关分组选择的方式，请参考操作系统用户名组管理。
	客户端主机名	支持字符串匹配、正则表达式匹配、分组选择方式匹配。 选择字符串，可填多值，多个值间以逗号“,”分隔。 有关分组选择的方式，请参考客户端主机名组管理。
行为	操作类型	设置操作权限，如 Select、Update、Delete 等。可根据 DDL\DML\DCL 来选择。 PS：“操作类型”和“SQL”至少填写一项。
	SQL	◆ 添加方式：支持在文本框手动填写后点击 <添加>，或直接导入 SQL 文件。 ◆ 批量处理特性：无论在何种方式下，一旦启用“多条自动分隔”功能（默认以分号;为分隔符，也可自定义分隔符），系统即可自动将内容分割为多条独立的 SQL 语句添加至列表。
访问对象	运维资产	下拉选择，选择需要进行权限控制的资产，可多选。 若选择了数据库访问账号，则该字段会自动带出对应的资产。
	对象组	指定规则所匹配的对象组。 有关对象组的更多信息，请参考对象组管理。 PS：对象组、数据级别、敏感数据类型间是或的关系，与其他规则配置是与的关系。
	数据级别	多选项，可选一级、二级、三级、四级、五级。
	敏感数据类型	多选项，可选内置类型或后续新增的类型。 有关敏感数据类型的更多信息，请参考敏感数据类型。
其他	生效时间	可自定义或者选择时间组。 自定义时间可选择任意时间、每天、每周、每月或节假日。 有关时间组配置的更多信息，请参考时间组管理。

9.4.2 身份权限案例介绍

案例描述：指定用户赋予不含高危操作的权限，若执行高危操作则会遭到阻断。

前提条件：确认您的数据库资产是“入侵防护模式”。

步骤 1. 在“**安全运维　数据库账号**”页面新增数据库账号。完成后如下图所示。

步骤 2. （可选）在“**规则配置　关联数据　对象组**”页面，新增一个名为“重点数据表”的对象组，并将 table_001、table_002、table_003 三个表加入到该组中。作为后续身份权限配置对象的一部分，完成后如下图所示。

步骤 3. 在“**安全运维　身份权限**”页面新增规则，在客户端身份选项卡中选择步骤 1 添加的数据库账号，其他客户端身份条件按需填写（匹配身份权限时，需要同时满足所有客户端身份条件），对象组选择步骤 2 创建的对象组，操作类型选择相关高危操作（如 Delete、Drop 等），动作为命令阻断。

步骤 4. 使用客户端工具通过数据库原始账号连接数据库，尝试访问“重点数据表”对象组中的三张表，确认可正常查询，因为未对 Select 查询语句做限制。

步骤 5. 使用客户端工具通过数据库原始账号连接数据库，尝试访问非“重点数据表”并执行高危操作，确认可正常执行，因为未对“重点数据表”对象组外的数据表做限制。

步骤 6. 使用客户端工具通过数据库原始账号连接数据库，尝试访问“重点数据表”对象组中的三张表并执行一些高危操作，确认操作被阻断，并记录运维日志，运维描述为“未经过审批”。

9.5 安全客户端

安全客户端的主要用途是加强对运维人员访问数据库时的身份认证机制。通过对客户端工具的特征（名称及 MD5）识别，确保只有经过验证的工具才能连接到数据库，从而减少恶意软件或未经授权的应用程序对数据的篡改风险。

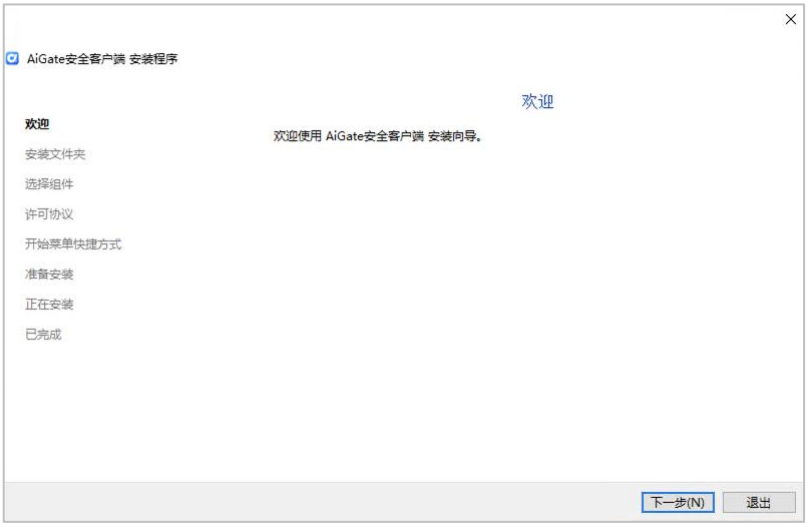
9.5.1 安全客户端下载安装

在菜单栏选择“安全运维　安全客户端　客户端下载”进入页面，点击<下载>按钮，在弹出的窗口中可选择下载 Windows 版本（支持 win7、win10、win11）或 Mac 版本。

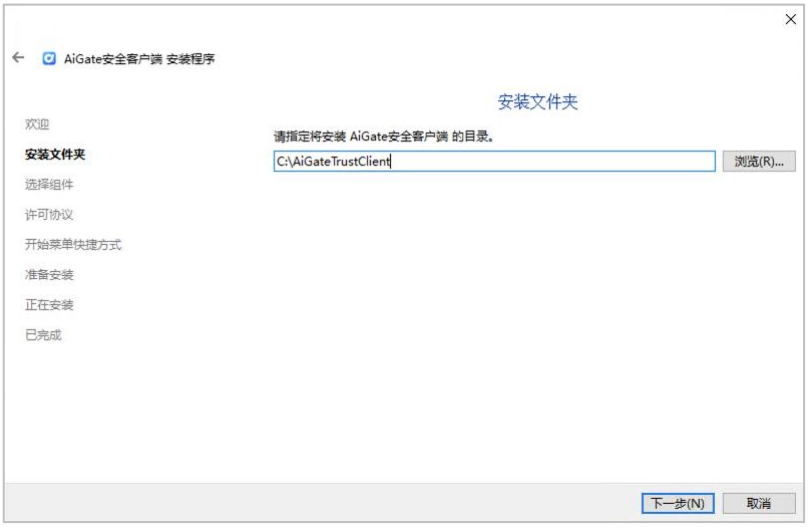
若提示文件不存在，则需要在技术支持中心或联系产品团队获取安全客户端升级包（如 trust_client-V1.0R24C00.240904.1535.tar.gz），并前往“系统管理 系统维护 软件升级”页面，点击<上传升级包>，选择安全客户端升级包上传即可。

◆ **Windows 版本安装**

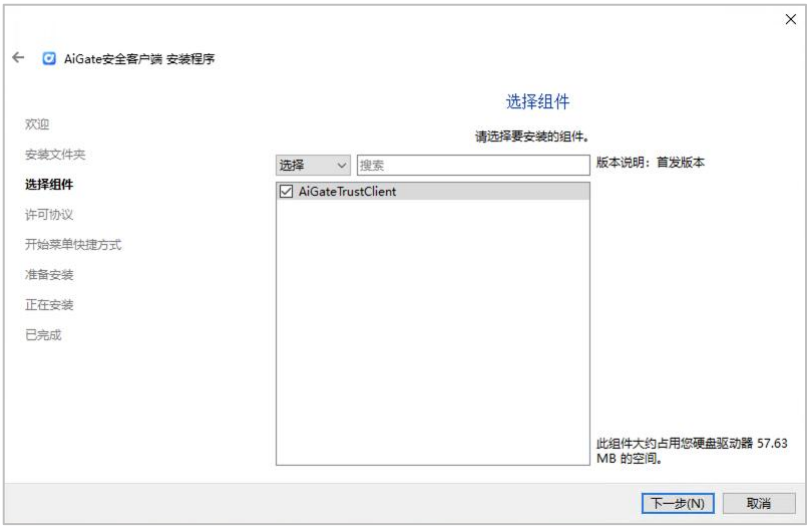
步骤 1. 双击下载的安装包数据库安全网关 TrustClient.install.package.exe，在弹窗中点击<下一步>。



步骤 2. 选择安全客户端的安装路径后，继续点击<下一步>。

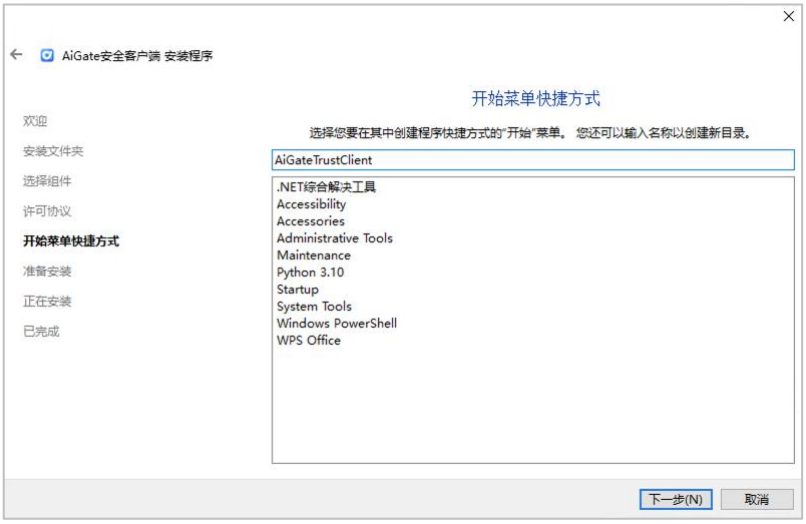


步骤 3. 继续点击<下一步>。

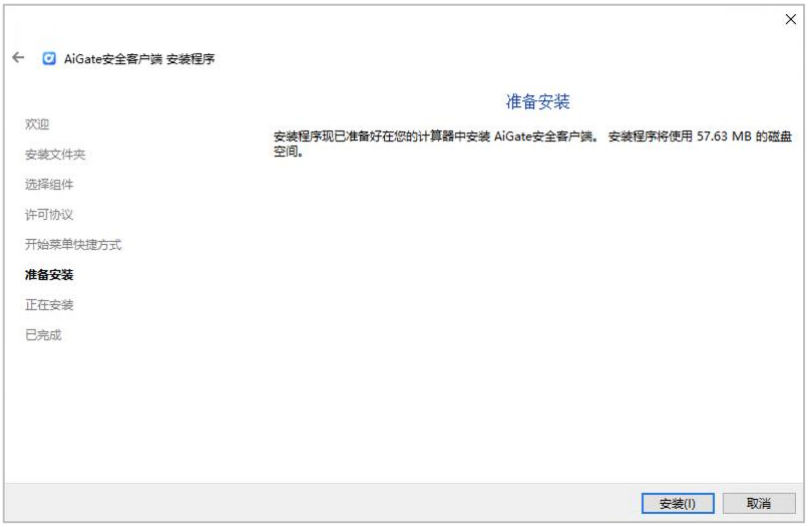


步骤 4. 勾选“我接收此许可”后，点击<下一步>。

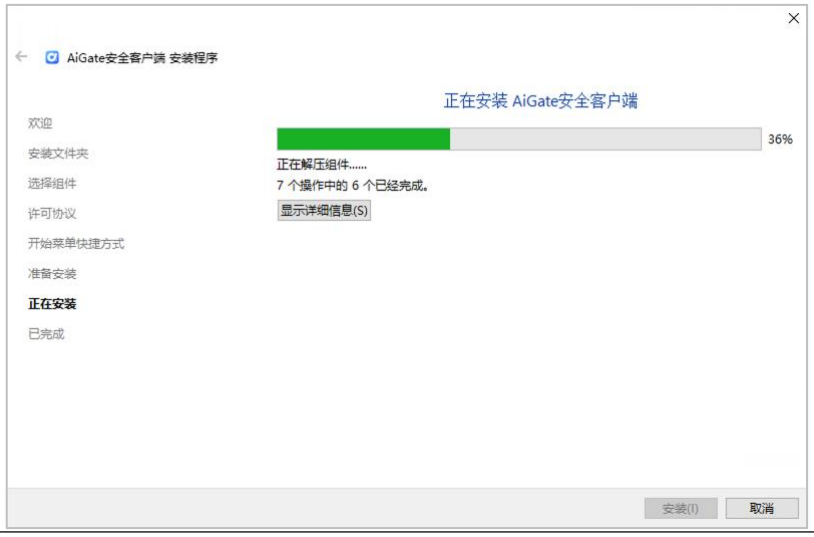
步骤 5. 继续点击<下一步>。



步骤 6. 点击<安装>。



步骤 7. 等待安装完成即可。

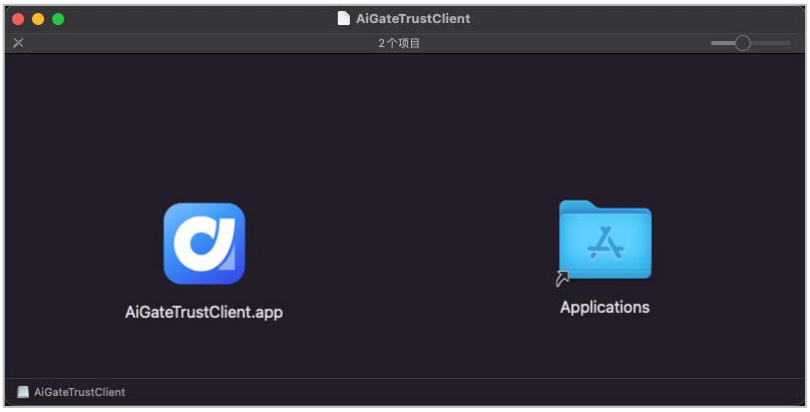


1、如需卸载，请双击安装目录下的 maintenancetool.exe 程序进行卸载。

2、若在安装过程中遇到任何问题，请及时与我们的产品支持团队取得联系，以获得帮助。

◆ **Mac 版本安装**

双击下载的安装包数据库安全网关 TrustClient.dmg，在弹出窗口中将数据库安全网关 TrustClient.app 拖入右侧 Applications 文件夹即可。



9.5.2 安全客户端使用说明

在未启用可信应用配置情况下，安全客户端不起任何作用。在启用可信应用配置的情况下，以下四种场景请求数据库将遭到阻断，并记录客户端告警日志（关于此告警日志详见客户端告警）：

1、未安装安全客户端软件的；

2、已安装安全客户端但未进行登陆的；

3、已安装登陆安全客户端，但使用的数据库连接工具不在可信应用配置中的；

4、已安装登陆安全客户端，但使用的数据库连接工具 MD5 值与配置不一致的；

前两种场景下，连接或请求数据库将遭到命令阻断；后两种场景分别被视为“非可信应用”和“假冒应用”，连接或请求数据库将导致数据库连接工具被关闭。

- **可信应用配置**：在菜单栏选择“安全运维 安全客户端 可信应用”进入页面，点击<修改>，在弹出窗口中启用该功能，并配置可信应用的名称及其 MD5 值后，点击<确定>。

  详细配置请参见下表：

配置项	说明
可信应用	启用或禁用可信应用的验证功能。
可信应用名称	填写数据库连接工具的名称。 Windows 可在任务管理器的详细信息中查看； Mac 可在活动监视器中查看。
可信应用 MD5 值	填写数据库连接工具的 MD5 值，一个应用支持配置多个可信 MD5 值，使用逗号“,” 分隔。 Windows 可使用命令“certutil -hashfile 文件路径 MD5”计算； Mac 可使用命令“md5 文件路径”计算。

配置项	说明
IP 白名单	支持多个 IP，使用逗号“,”分隔，例：10.10.1.1,10.10.1.2 支持子网掩码配置，例：10.10.1.1/24 支持 IP 段配置，例：10.1.1.10-10.1.1.20

- **安全客户端登陆**：打开安全客户端后，需要输入服务地址（IP 或 IP:端口）、运维人员账号及密码，点击<立即登录>即可。

- **安全客户端更新**：若您电脑上安装的安全客户端版本落后于数据库安全网关服务器端所使用的安全客户端版本，系统将会提示您执行更新操作。此时，只需点击“立即更新”按钮，即可在线完成版本的升级更新。

- **安全客户端主页**：登陆后可查看该运维人员的个人信息，及其所关联的数据库访问账号。点击左侧菜单栏中的头像，再点击<关于>可查看安全客户端的版本信息。

- **安全客户端的安全认证**：在“安全运维　数据库访问账号　账号安全配置”页面启用安全认证功能后，登录安全客户端时，您将能够看到安全认证模块。该模块的使用方法与安全认证流程相同。

10 通知外送

通知外送模块用于配置和管理系统通知的外送方式，通过邮件、短信、企业微信、SYSLOG 等渠道，将审计日志、匹配规则产生的告警日志、系统告警日志及时发送给相关人员。

10.1 告警通知

10.1.1 邮件

用户可以配置通过邮件通知方式将资产告警日志和系统告警日志发送到指定的邮箱。

步骤 1. 在菜单栏选择“**通知外送　告警通知　邮件**”进入告警通知页面，点击页面中的<编辑>按钮。

步骤 2. 弹出邮件配置对话框，编辑相关信息，点击<确定>。

具体配置项请参见下表：

配置项	说明
实时告警模板	发送实时告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
聚合告警模板	发送聚合告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
统计告警模板	发送统计告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
系统告警模板	发送系统告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

步骤 3. 配置好邮件发送模板后，可以配置需要发送邮件通知的资产及接收人，点击<添加>。

步骤 4. 在弹出的页面中，编辑相关信息，点击<保存>。

具体配置项请参见下表：

配置项	说明
资产	选择需要邮件监测告警的资产，可多选。
接收者	填写接收告警信息的邮箱，可设置多个邮箱。
告警等级	选择需要邮件通知的告警等级，支持低、中、高，可多选。
实时告警	可启用或关闭。 启用后，若有告警日志则立即按“**实时告警模板**”发送邮件通知相关人员。
通知周期	取值范围为 1-1440 分钟。（聚合通知启用后，通知周期才生效） 同一个规则在通知周期内多次触发告警时只通知第一次触发的告警。
聚合通知	可启用或关闭，在通知周期内按匹配规则进行告警聚合。 启用后，在通知周期结束时会立即按“**聚合告警模版**”发送邮件通知相关人员。
告警统计	可启用或关闭，统计范围是昨天 00:00~23:59 的告警数据。

配置项	说明
	启用后，每天在发送时间点都将按“**统计告警模版**”发送邮件通知相关人员。
发送时间	每天发送告警统计邮件的具体时间。

10.1.2 短信

用户可配置通过短信通知方式将资产告警日志和系统告警日志发送到指定的 web 接口或者数据库接口。

步骤 1. 在菜单栏选择“**通知外送　告警通知　短信**”进入告警通知页面。

步骤 2. 点击页面中的<编辑>按钮，弹出短信配置对话框，编辑相关信息，点击<确定>。

- **发送方式一：web 接口**

- **发送方式二：数据库接口**

具体配置项请参见下表：

配置项		说明
不发送		产生告警后，不会发送告警
Web 接口	发送方法	可以选择 GET 或者 POST 方式。
	URL	URL 填写，例如：http://192.168.30.87:5000/?Uid=username&key=password&Mobil=[$PHONE]&Text=[$SMSTEXT]
	头信息	填写 HTTP 协议中的头信息，左侧输入框填写 Key，右侧输入框填写 Value，支持填写多组。
	Post 参数	可以使用 [$PHONE] 和 [$SMSTEXT] 两个参数，分别表示手机号码和短信内容。 例：Uid=username&key=password&Mobil=[$PHONE]&Text=[$SMSTEXT]
	编码方式	默认 UTF-8，可选 GBK。
数据库接口	数据库类型	选择数据库类型，支持 Oracle、SQL Server、DB2、MySQL。
	数据库名称/SID	如果是 Oracle 数据库，请输入 SID；其他数据库请输入数据库名称。
	用户名	填写数据库的用户名。
	密码	填写数据库的密码。

配置项		说明
	域名或者 IP	填写数据库的域名或数据库的 IP。
	端口	填写数据库的端口。
	参数顺序	可选“先手机号码，后短信内容”或“先短信内容，后手机号码”。
	插入 SQL 模板	可使用两个参数（1.手机号码，2.短信内容），用?表示，顺序可在“参数顺序”中设置。 例：insert into MSG(count,phonenum,content,priority) values(1,?,?,1) 注意事项：1.语句最后不用加分号“;”
	编码方式	默认 UTF-8，可选 GBK。
	调用方式	可选 Insert 语句或者存储过程。
实时告警模板		发送实时告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
聚合告警模板		发送聚合告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
统计告警模板		发送统计告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
系统告警模板		发送系统告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

步骤 3. 配置好短信发送模板后，可以配置需要发送短信通知的资产及接收人，点击<添加>。（具体配置说明已在“通知外送-邮件”模块中说明，此处不再重复说明；注意短信的接收人需填写手机号）

短信网关由专门提供短息转发业务的服务商提供。短信网关用户通过网络将短信发送到短信网关，由短信网关负责将短信发送给短信接收者，系统通过短信网关转发告警短信。用户需要事先向第三方服务商申请短信网关服务。

10.1.3 企业微信

用户可以配置通过企业微信通知方式将资产告警日志和系统告警日志发送到指定的企业微信。

步骤 1. 在菜单栏选择“**通知外送 告警通知 企业微信**”进入告警通知页面。

步骤 2. 点击页面中的<编辑>按钮，弹出企业微信配置对话框，编辑相关信息，点击<确定>。

具体配置项请参见下表：

配置项	**说明**
企业 ID	企业唯一标识。获取方法：使用企业微信管理员账号登录企业微信管理后台，在“我的企业　企业信息”下查看<企业 ID>。
企业微信应用 ID	用于发送消息的应用 ID，获取方法：使用企业微信管理员账号登录企业微信管理后台，在“应用管理　应用　自建”，点开用于发送消息的应用，AgentId 即为应用 ID。
企业微信应用密钥	用于发送消息的应用密钥，获取方法：使用企业微信管理员账号登录企业微信管理后台，在“应用管理　应用　自建”，点开用于发送消息的应用应用，点击 Secret 旁的“查看”，根据提示操作即可获取 Secret。
保密消息	是否是保密消息。非保密消息可对外分享，保密消息不能分享且内容显示水印，默认为非保密消息。
实时告警模板	发送实时告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
聚合告警模板	发送聚合告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
统计告警模板	发送统计告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

配置项	说明
系统告警模板	发送系统告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

步骤 3. 配置完后点击<测试企业微信信息>，弹出发送测试消息框，填写接收者微信 ID 即可发送成功。

步骤 4. 配置好企业微信发送模板后，可以配置需要发送通知的资产及接收人，点击<添加>。（具体配置说明已在“通知外送-邮件”模块中说明，此处不再重复说明；注意企业微信的接收人需填写企业微信通讯录中的微信账号）

10.1.4 SYSLOG

用户可配置通过 Syslog 通知方式将资产告警日志和系统告警日志发送到指定的 Syslog 服务器。

步骤 1. 在菜单栏选择“**通知外送　告警通知　SYSLOG**”进入告警通知页面。

步骤 2. 点击页面中的<新增>按钮，弹出 SYSLOG 配置对话框，编辑相关信息，点击<保存>。

具体配置项请参见下表：

配置项	说明

配置项	说明
配置名称	Syslog 接收接口的配置名称。
服务器地址	Syslog 服务器地址，可为 IP 或者域名。
端口	Syslog 服务器端口，默认为 514。
程序模块编码	Syslog 协议 RFC 5424 规定，消息中必须包含“程序模块编码”，Syslog 服务端使用该编码区分发送消息的程序来源。建议选择默认值 local0。
严重等级	选择向 Syslog 服务器发送告警所标记的严重等级。等级分为：Emergency、Alert、Critical、Error、Warning、Notice、Informational、Debug。 以上 Syslog 相关配置与服务器端配置保持一致即可。
实时告警模板	发送实时告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
聚合告警模板	发送聚合告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
统计告警模板	发送统计告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。
系统告警模板	发送系统告警信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

步骤 3. 配置好 SYSLOG 发送模板后，可以配置需要发送通知的资产及接收人，点击<添加>。（具体配置说明已在“通知外送-邮件”模块中说明，此处不再重复说明；注意 SYSLOG 的接收人需填步骤 2 中配置的 SYSLOG 服务器）

效果如图：

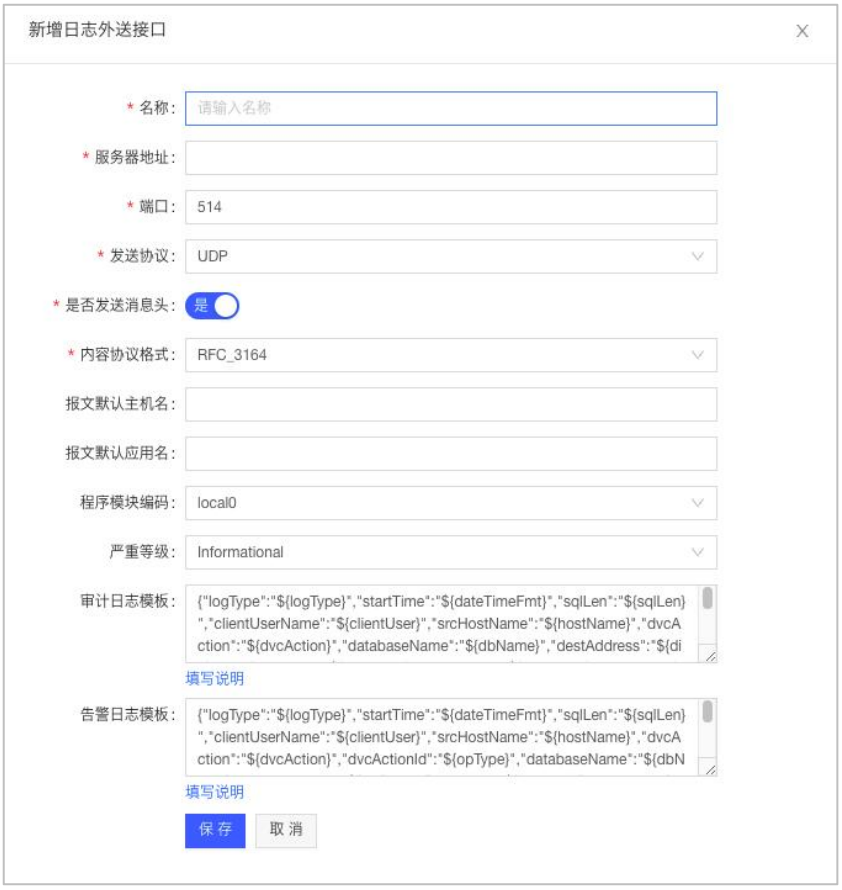
10.2 日志外送

10.2.1 SYSLOG

用户可配置通过 Syslog 通知方式将资产审计日志或资产告警日志发送到指定的 Syslog 服务器。

步骤 1. 在菜单栏选择“**通知外送 日志外送 SYSLOG**”进入告警通知页面。

步骤 2. 点击页面中的<新增>按钮，弹出 SYSLOG 配置对话框，编辑相关信息，点击<保存>。



具体配置项请参见下表：

配置项	说明
名称	Syslog 接收接口的配置名称。
服务器地址	Syslog 服务器地址，可为 IP 或者域名。
端口	Syslog 服务器端口，默认为 514。
发送协议	选择日志传输的协议类型，支持 UDP 或 TCP。
是否发送消息头	决定是否在日志数据前添加自定义 Syslog 消息头（含主机名及用户名）。
内容协议格式	定义日志数据的格式，默认为 RFC_3164。
报文默认主机名	可以指定日志中使用的默认主机名。
报文默认应用名	可以指定日志中使用的默认应用程序名。
程序模块编码	Syslog 协议 RFC 5424 规定，消息中必须包含“程序模块编码”，Syslog 服务端使用该编码区分发送消息的程序来源。与服务器端配置保持一致即可。
严重等级	选择向 Syslog 服务器发送告警所标记的严重等级。等级分为：Emergency、Alert、Critical、Error、Warning、Notice、Informational、Debug。与服务器端配置保持一致即可。
审计日志模板	发送审计日志信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

配置项	说明
告警日志模板	发送告警日志信息的模板，可修改默认模板，具体字段请依据**填写说明**编辑。

步骤 3. 配置好 SYSLOG 发送模板后，可以配置需要发送通知的资产及接收人，点击<添加>。（具体配置说明已在“通知外送-邮件”模块中说明，此处不再重复说明；注意 SYSLOG 的接收人需填步骤 2 中配置的 SYSLOG 服务器）

效果如图：

10.2.2 KAFKA

用户可配置通过 Kafka 通知方式，将资产审计日志或资产告警日志发送到指定的 Kafka 服务器。

步骤 1. 在菜单栏选择“**通知外送　日志外送　KAFKA**”进入日志外送页面。

步骤 2. 点击“日志外送接口管理”模块中的<新增>按钮，填写各项参数后保存。

具体配置项请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 64。
Kafka 节点地址	必须为已经存在的节点，支持 IP 加端口或域名加端口，多个以英文逗号相连。
Kafka 主题	必须填写已经存在的主题。
Kafka 分区	分区从 0 开始计算，如分区为 24，则最大位需填写 23。
审计日志模板	发送审计日志信息的模板，可修改默认模板，具体字段请依据填写说明编辑。
告警日志模板	发送告警日志信息的模板，可修改默认模板，具体字段请依据填写说明编辑。

步骤 3. 点击“日志外送任务管理”模块中的<新增>按钮，填写各项参数后保存。

具体配置项请参见下表：

配置项	说明
资产	选择要发送日志的资产。
日志类型	可以选择审计日志或告警日志。
外送接口	使用什么接口进行外送，下拉框为“日志外送接口列表”里的数据。

11系统管理

系统管理是指超级管理员或系统管理员对系统进行配置和维护，使系统更好地适配业务场景。系统管理包括用户管理、系统配置、系统维护、系统告警和操作日志。

11.1 用户管理

用户管理主要是为用户设置权限，包括用户管理、角色管理、用户安全配置、动态令牌管理及授权数据库。

11.1.1 角色管理

角色是拥有相同权限的用户集合，系统先将权限分配给角色，再为用户指定相应角色。在配置用户时，通过设定其所属角色来限定其操作权限范围（分为菜单权限和功能权限），实现权限的灵活管理。

创建角色的操作方法如下：

步骤 1. 在菜单栏选择“**系统管理　用户管理**”，选择**角色管理**页签。

步骤 2. 点击<添加>弹出新增角色页面，编辑角色名称，选择权限后，点击<保存>。

11.1.2 用户管理

添加角色后即可增加该角色的用户。

系统内置了以下四个默认用户：

- **admin**：超级管理员，具备系统所有权限。系统只有一个超级管理员。

- **security**：具备安全管理员权限，可配置数据库与规则、查看各类告警报告、管理安全员。
- **system**：具备系统管理员权限，进行系统权限的配置和维护。
- **audit**：具备审计管理员权限，查看其他用户的操作日志、管理审计员。

添加用户的操作方法如下：

步骤 1. 在菜单栏选择“**系统管理　用户管理**”进入用户管理页面，如下图所示。

步骤 2. 点击<添加用户>进入添加用户页面，编辑相关信息，点击<保存>。

具体配置项请参见下表：

配置项	说明
用户名	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，最大长度 64 字符。
启用	点击启用后的开关，设置添加用户后是否立即启用用户。
角色	指定用户角色，包括内置角色和用户自定义角色。有关角色设置的更多信息，请参考角色管理。

配置项	说明
密码/确认密码	创建并确认新建用户的登录密码。密码长度 6~64 位，当启用强密码功能后需符合密码强度要求。修改密码时新旧密码不能相同。
手机号	设置用户的手机号。
邮箱	设置用户的邮件地址。
认证方式	用户登录系统时的认证方式，可选择“密码”、“密码+硬件 OTP”、“密码+软件 OTP”、“密码+短信”认证方式。
登录 IP/MAC 限制	对用户登录系统时使用的 IP/MAC 进行限制。
登录时间限制	可选择限制用户登录系统的时间。
用户有效期	设置用户的有效期。若不设置，则视为永久有效；若用户已过期，则该用户将无法再登录数据库安全网关系统，且已登录的会话也将被登出。

11.1.2.1 认证方式介绍

数据库安全网关支持多种双因子认证方式，可在新增用户时选择认证方式，或是登录具体用户后在我的信息中去配置认证方式。各认证方式具体配置如下：

- **硬件 OTP 登录**：参考动态令牌管理章节导入令牌 XML 文件，勾选“密码+硬件 OTP 登录”后，点击下拉选择导入的动态令牌序列号，保存即可。
- **软件 OTP 登录**：勾选“密码+软件 OTP 登录”后，弹出修改软件 OTP 密钥窗口。使用 Authenticator 身份认证器输入设置密钥或是扫描二维码获取动态口令，输入至窗口中点击确认即可。

- **短信登录**：参考短信外发章节填写短信发送配置后，勾选“密码+短信登录”后点击配置短信登录手机号，在弹出窗口中填写手机号，点击<发送验证码>，将收取到的验证码填入后保存即可。

11.1.3 用户安全配置

用户安全配置是为了保证用户账户的使用安全，如：防止用户账户被暴力破解，或者当用户离开配置 PC 时防止被他人修改系统配置等。

步骤 1. 在菜单栏选择“**系统管理　用户管理　用户安全配置**”进入页面，可修改安全配置后，点击<保存>。

具体配置项请参见下表：

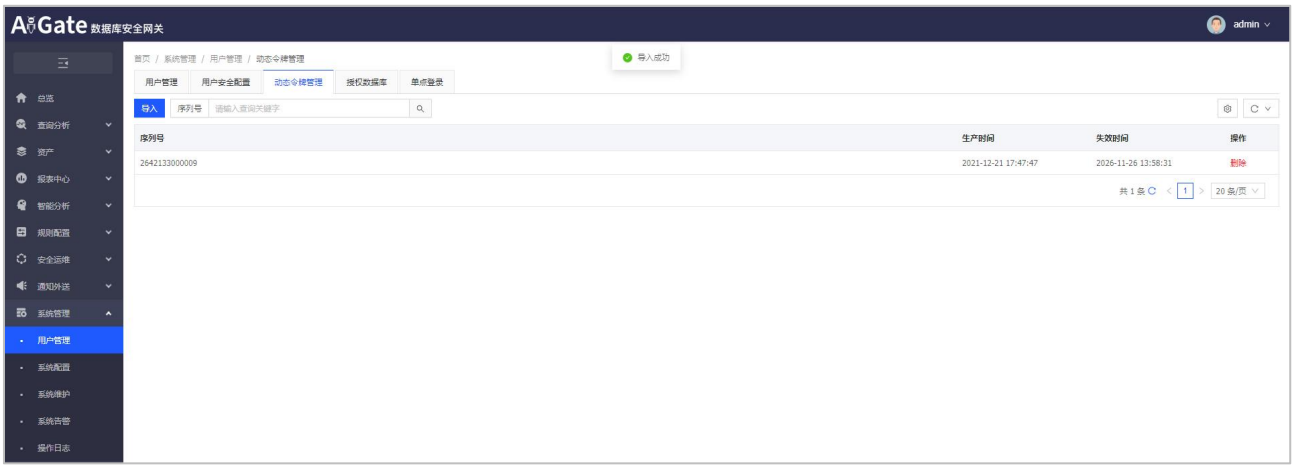
配置项	**说明**
用户安全设置	
登录超时	取值范围 1~43200 分钟，默认值为 5 分钟。当用户超过设置时长未操作时，再次操作需要重新登录系统。
验证码	设置用户登录系统时是否需要输入验证码。
用户锁定	
密码尝试次数	取值范围 1 ~ 10 次，默认值为 5 次。当用户输入密码错误次数达到设置定值时，系统将锁定此账户。

配置项	说明
锁定时长	取值范围 1~10800 分钟，默认值为 30 分钟。
重置计数器	取值范围 1~10800 分钟，默认值为 5 分钟。密码尝试失败后，若在设置时间长度内不再尝试输入密码，则系统将密码尝试次数重新设为 0。
密码策略	
启用强密码	启用强密码后，设置用户密码时必须要满足较高的复杂度。（8~64 个字符长度，必须包含大写字母、小写字母、数字和特殊字符）
密码使用期限	取值范围 0~999 天，默认为 0 天，0 表示密码不会过期。当用户密码使用时间达到设置值时，系统会强制用户修改密码。

11.1.4 动态令牌管理

启用动态令牌认证功能，需要拥有硬件设备，提供双因素认证。

步骤 1. 在菜单栏选择“**系统管理　用户管理　动态令牌管理**”，点击<导入>按钮，弹出本地目录，选择动态令牌的 xml 文件上传，即可导入成功。



步骤 2. 在菜单栏中选择“**系统管理　用户管理　用户管理**”进入页面，选择用户点击其右侧的<编辑>按钮，将认证方式修改为“密码+动态令牌登录”，并选择步骤 1 中导入的序列号。

步骤 3. 使用步骤 2 中的用户登录数据库安全网关系统，动态令牌框输入动态令牌上的数字，点击<登录>即可登录成功。

11.1.5 授权数据库

为了确保资产信息的安全性和管理的精准性，我们采取了一种细致的用户授权机制。通过为安全员或安全管理员用户进行特定权限的授予，我们能够将资产与他们紧密关联起来。这种关联确保只有在安全员或安全管理员用户成功登录系统后，他们才能访问并查看与之相关联的资产详细信息。

步骤 1. 在菜单栏选择“**系统管理　用户管理　授权数据库**”进入页面，点击<添加授权>按钮，弹出新增授权规则框，在窗口内填写相关配置后，点击<保存>。

具体配置项请参见下表：

配置项	说明
规则名称	授权数据库规则的名称，必须为中文字符、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 64。
状态	启用或者禁用。启用时生效，禁用时不生效。
用户	安全员或者安全管理员，包含 security。
资产	必选项，支持多选。可按资产进行选择。
备注	备注信息。

步骤 2. 若给用户 security 首选两个 MySQL 资产及一个 Oracle RAC。

步骤 3. 使用 security 用户登录数据库安全网关，前往“**资产　资产管理**”页面，可以看到 security 用户只能看到已经授权与他的几个资产。

11.2　系统配置

11.2.1　部署模式

关于部署模式的说明和配置在发布文档《数据库安全网关数据库安全网关 快速部署手册》中有详细讲解，本手册仅做简单操作说明。切换模式前建议先进行闪灯操作。

11.2.1.1　反向代理

软件安装完成后默认为“反向代理”模式，网络无需进行修改。

在反向代理模式下，对于客户端而言数据库安全网关作为代理服务器就像是原始服务器，并且客户端不需要进行任何特别的设置。客户端通过反向代理 IP 和反向代理端口连接数据库并发送普通请求，数据库安全网关 接收到数据后将自主判断向何处(原始服务器)转交请求，并将获得的内容返回给客户端。

11.2.2　网络

11.2.2.1　网口管理

前提条件：已根据《数据库安全网关数据库安全网关 快速部署手册》完成闪灯操作。

- **管理口配置**

步骤 1. 在菜单栏选择“**系统管理　系统配置　网络**”进入网络配置页面，如下图所示。

步骤 2. 在管理口配置区域点击<修改>，弹出修改管理口配置对话框，可修改管理口的 IPv4 地址、子网掩码、IPv4 网关以及 IPv6 配置信息等，修改后点击<确定>。

修改管理口 IP 后需要重新登录系统，即在浏览器地址栏中需要输入修改后的管理口 IP（使用 HTTPS 协议），重新输入账号密码登录系统才能继续使用。

◆ **其他网口配置**

步骤 1. 在菜单栏选择“**系统管理　系统配置　网络**”进入网络配置页面，如下图所示。

闪灯将网卡配置为管理口后，在网口管理列表中将不再显示该网卡。

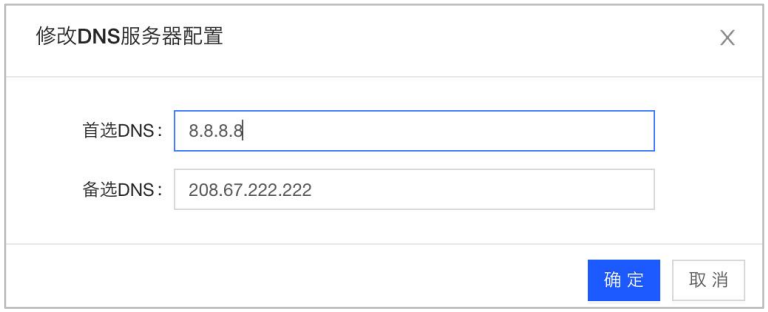
步骤 2. 在网口管理区域内选择网卡点击<编辑>按钮，弹出修改管理口配置对话框，可修改管理口的 IPv4 地址、子网掩码、IPv4 网关以及 IPv6 配置信息等，修改后点击<确定>。

步骤 3. 在网口管理区域内选择网卡点击<启用>或<禁用>按钮，可修改选中网口的状态。

11.2.2.2 DNS 服务器配置

步骤 1. 在菜单栏选择“**系统管理　系统配置　网络**”进入网络配置页面，在 DNS 服务器配置区域点击<修改>按钮。

步骤 2. 在弹出的对话框中设置首选 DNS 和备选 DNS，点击<确定>。



11.2.2.3 路由管理

步骤 1. 在菜单栏选择“**系统管理　系统配置　网络**”进入网络配置页面，在路由管理区域点击<新增>按钮。

步骤 2. 在弹出的对话框中设置新增路由的目的网段、目的网段掩码和下一跳路由，点击<保存>即可。

具体配置项请参见下表：

配置项	说明
目的网段	填写目的 IP 所在的网段，例如：172.18.1.0
目的网段掩码	填写目的网段的子网掩码，例如：255.255.255.0

配置项	说明
下一跳路由	填写访问目的网段的下一跳路由，一般为数据库安全网关收发数据口 IP 网段的网关

11.2.2.4 Web 服务端口修改

步骤 1. 在菜单栏选择“**系统管理　系统配置　网络**”进入网络配置页面，在 Web 服务配置区域点击<修改>。

步骤 2. 在弹出的对话框中设置新的服务器端口（确保服务端口网络可达，建议修改服务器端口前先打开 SSH 端口），点击<保存>即可。

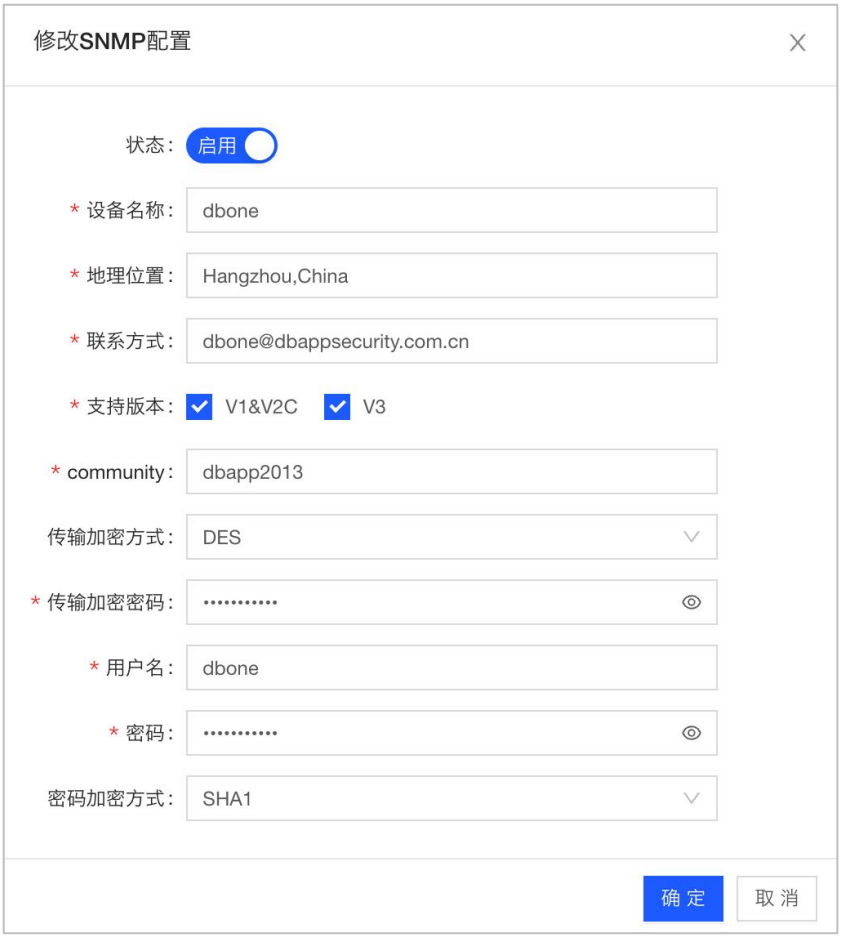
11.2.3 SNMP

SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议，支持目前主流的网络管理系统，用于监测网络上的设备是否有存在异常情况。系统支持 SNMP，通过 V2 和 V3 版本 SNMP 协议对数据库安全网关进行远程监控。

◆ **配置 SNMP 的操作方法如下：**

步骤 1. 在菜单栏选择“**系统管理　系统配置　SNMP**”进入页面。

步骤 2. 点击<修改>进入修改 SNMP 配置页面，编辑相关信息，点击<确定>。



具体配置项请参见下表：

配置项	说明
状态	在设备上启用或禁用 SNMP 功能。
设备名称	设置数据库安全网关设备自身的名称以方便识别。
地理位置	设备的地理位置。
联系方式	设备管理员的联系方式，可设置为邮箱或电话号码。
支持版本	选择启用的 SNMP 版本，支持 V1&V2C、V3 版本。V1&V2C 版本使用团体字认证方式，V3 版本引入了基于用户的安全模型，比 V1&V2C 版本更安全。
community (V1&V2C)	定义信息流向，填写“public”，即公开。
传输加密方式(V3)	选择信息传输的加密方式，目前支持 DES 与 AES 两种方式： ◆ DES：Data Encryption Standard，即数据加密标准，是一种使用密钥加密的块算法，1977 年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），并授权在非密级政府通信中使用，随

配置项	说明
	后该算法在国际上广泛流传开来。 ◆ AES：Advanced Encryption Standard，即高级加密标准，在密码学中又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广泛使用。
传输加密密码 V3)	指定传输过程中的加密密码。
用户名/密码(V3)	指定 SNMP 通讯双方认证使用的用户名和密码。
密码加密方式(V3)	指定 SNMP 密码的加密方式，支持 MD5 与 SHA1 两种方式。

11.2.4 通知外送

本系统的所有邮件发送功能均基于该模块进行配置，如运维审批邮件、报表订阅、资产告警通知、系统告警通知等。

◆ **配置邮件发送服务器信息，具体步骤如下：**

步骤 1. 在菜单栏选择“**系统管理 系统配置 通知外送**”进入通知外送页面，点击<修改>，在弹出修改邮件服务器配置窗口内填写相关配置后，点击 <确定>。

具体配置项请参见下表：

配置项	说明

配置项	说明
状态	在设备上启用或禁用邮件服务器。
用户名	登录邮件服务器的用户名称。
密码	登录邮件服务器的用户密码。
发件人	发件人的邮箱。
SMTP 服务器	SMTP 服务器的 IP 或域名。
SMTP 服务器端口	SMTP 服务器所用端口。
是否加密	邮箱是否进行加密。
编码	服务器支持的编码方式，主要为 UTF-8、GBK。

11.2.5 可靠性配置

- **软件直通**：是在业务层面监控 CPU 使用率、内存使用率等指标当达到预设阈值时，由软件触发 bypass 操作，可以在“系统管理 系统配置 可靠性配置”中修改这些阈值。
- **硬件直通**：是在硬件层面监控设备状态，例如断电、死机等故障时触发，只在硬件透明代理模式且串联一对硬件 bypass 网卡的情况下支持。当性能占用过高时，也可由软件触发硬件 bypass 切换。软件部署时硬件可靠性不支持配置默认置灰。

步骤 1. 在菜单栏选择“**系统管理 系统配置 可靠性配置**”进入配置页面。

硬件可靠性详细配置参考下表（透明模式下支持）：

配置项	说明
CPU 阈值	默认 80%，配置区间 60%-85%
内存阈值	默认 80%，配置区间 60%-85%
交换分区阈值	默认 80%，配置区间 60%-85%
根分区阈值	默认 80%，配置区间 60%-85%
数据分区阈值	默认 80%，配置区间 70%-85%（不包含 70%）

软件可靠性详细配置参考下表：

配置项	说明

配置项	说明
CPU 阈值	默认 80%，配置区间 60%-85%
内存阈值	默认 80%，配置区间 60%-85%
交换分区阈值	默认 80%，配置区间 60%-85%
根分区阈值	默认 80%，配置区间 60%-85%
数据分区阈值	默认 80%，配置区间 70%-85%（不包含 70%）

只要有一个配置项的实际数据超过配置数据，系统就切换成 bypass 模式，将不再对数据库进行检测或防护，适用所有部署模式。（透明代理显示硬件可靠性配置，其他模式不显示硬件可靠性配置）。

11.2.6 系统联动

系统联动包含数据分类分级关联配置和 AiTrust 关联配置。配置数据分类分级关联可使数据库安全网关和数据分类分级联动，数据库安全网关可以从数据分类分级上获取元数据；配置 AiTrust 关联，可实现数据库安全网关零信任对接。

◆ **数据分类分级关联配置**

步骤 1. 在菜单栏选择“**系统管理　系统配置　系统联动**”，进入系统联动页面，选择数据分类分级关联配置，点击<修改>按钮，在关联配置窗口内填写相关配置后，点击<确定>。

详细配置请参见下表：

配置项	说明
状态	启用或者禁用。
数据分类分级 IP 地址	数据分类分级环境的 IP 地址。
端口	数据分类分级环境的端口号，一般为 8080。
用户名	数据分类分级的用户名。
密码	数据分类分级的密码。
级别映射关系	数据库安全网关的级别为一级、二级、三级、四级、五级；对应的数据分类分级级别为数据分类分级系统内设置的级别。（数据分类分级级别填写不可重复）
测试连接	填写数据分类分级的 IP 和端口号后，点击测试连接，连接成功证明可用。

11.2.7 规则维护

支持内置规则（安全规则和虚拟补丁）升级，具体升级包请联系相关人员获取。

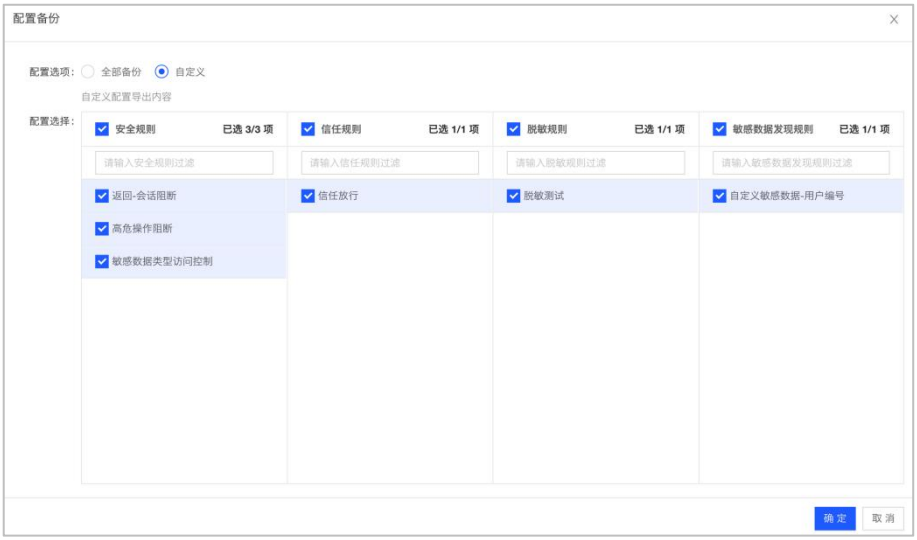
步骤 1. 在菜单栏中选择“**系统管理　系统配置　规则维护**”进入规则维护页面。点击<上传升级包>，选择升级包文件即可升级内置安全规则。

11.2.8　配置备份

配置的备份恢复可在系统配置出错或丢失时，对系统进行还原，减少系统配置工作量；或将备份文件导入至另一台全新的数据库安全网关环境中使用。在“**系统管理　系统配置　配置备份**”页面，可查看配置备份情况：

- **配置备份（全部备份）**：点击<配置备份>，默认选择全部备份，备份内容包含所有规则配置、资产、运维人运、数据库账号等，点击<确定>按钮，即可备份成功。

- **配置备份（自定义）**：点击<配置备份>，选择自定义，勾选需要备份的安全规则、信任规则、脱敏规则及敏感数据发现规则后，点击<确定>按钮，即可备份成功。



- **配置恢复**：选择需要的配置备份文件点击其右侧的<下载>获取文件，前往需要导入配置的服务器，在配置备份页面中点击<配置导入>，上传下载的配置文件即可。
- **导入日志**：点击配置备份文件列表上方的<导入日志下载>，可下载日志文件查看相关导入的情况。

11.3 系统维护

11.3.1 时间

系统支持通过同步浏览器时间和同步 NTP 时钟服务器两种方式调整系统当前时间信息。

步骤 1. 在菜单栏选择“**系统管理　系统维护　时间**”进入页面，点击<同步浏览器时间>可将系统时间与浏览器时间同步。

步骤 2. 点击<修改>弹出修改时间同步配置对话框，设置同步服务器的 IP 或者域名，选择是否启用自动同步，点击<确定>即可设置时间同步服务。

11.3.2 资源使用

在菜单栏选择“**系统管理　系统维护　资源使用**”进入页面，可查看系统资源使用情况，包括 CPU 使用率、内存使用率、SWAP 使用率、网络流量、磁盘读写、磁盘空间使用率，支持查询设备资源使用的历史情况。

11.3.3 调试工具

系统支持日志打包下载、连通性测试和 Tcpdump 抓包功能。下载日志有助于后续溯源或定位问题，若定位问题需数据库安全网关协同排查时，系统还支持在指定网口上进行抓包，抓包产生的文件可以下载到本地（系统不会以任何形式获取抓包文件）。

11.3.3.1 日志打包下载

系统支持在页面上下载系统的运行日志，便于后续遇到问题进行分析定位。

步骤 1. 在菜单栏选择“**系统管理　系统维护　调试工具**”进入页面，点击<下载>将日志文件下载至本地。下载日志如下图所示：

11.3.3.2 连通性检测

系统提供 ping、nc 和 traceroute 三种命令，以验证系统与目的主机是否网络连通。

- **PING**：测试系统与目标主机是否网络可达。

步骤 1. 在调试工具页面的连通性检测区域中，选择操作类型为 ping，输入 IP（支持 IPv4 和 IPv6），点击<查看输出结果>。

- **NC**：用来扫描目标主机的端口是否开放。

步骤 1. 在调试工具页面的连通性检测区域中，选择操作类型为 nc，选择协议（TCP 或 UDP），输入 IP（支持 IPv4 和 IPv6）和端口，点击<查看输出结果>。

- **TRACEROUTE**：用来查看系统与目标主机之间经过的网关。

步骤 1. 在调试工具页面的连通性检测区域中，选择操作类型为 traceroute，输入 IP（支持 IPv4 和 IPv6），点击<查看输出结果>。

11.3.3.3 TCPDUMP 抓包管理

系统支持在页面上选择指定网口进行抓包，抓包产生的文件可以下载到本地。

步骤 1. 在调试工具页面的 Tcpdump 抓包管理区域中，点击<新增抓包任务>进入新增 TCPDUMP 抓包页面，编辑相关信息，点击<保存>。

详细配置请参见下表：

配置项	说明
网口	抓包的网口。
过滤串	填写抓包过滤串，系统根据过滤串抓取相应报文。 例：port 80 and host 192.168.1.2
最大抓包时长	取值范围：1~86400，单位为秒。 抓包的最大时长，超过此限制，会自动停止抓包。
最大文件大小	取值范围：1~10480，单位为 MB。 抓包文件的最大大小，超过此限制，会自动停止抓包。

步骤 2. 抓包完成后，点击<下载>即可将抓包文件下载至本地。

11.3.4 软件升级

在“**系统管理　系统维护　软件升级**”页面中，可对系统软件及安全客户端进行升级操作。系统目前支持离线升级和在线升级两种方式，分别适用于无法访问互联网和可以访问互联网的场景。

11.3.4.1 离线升级

步骤 1. 在离线升级页面点击<获取升级包>，获取产品最新版本的二维码。（或通过技术支持中心、技术人员提供的网盘下载升级包）

步骤 2. 扫描二维码，获取最新版本升级包。

步骤 3. 点击<更多>查看升级版本信息，点击<复制链接>。

步骤 4. 在外网设备中打开链接下载升级包，然后点击页面上的<点击上传升级包>，选择升级包进行上传。

步骤 5. 等待升级完成后，扫描二维码获取校验码，完成升级操作。

11.3.5 数据清理

由于设备的磁盘空间有限，可对历史审计日志等信息进行定期清理以节约磁盘空间。

系统磁盘中存储的业务数据分为在线数据和备份数据。

- 在线数据是指可以直接通过页面进行检索查看的数据。在线数据进行压缩打包后占有的磁盘空间将缩小为原先的五分之一左右。
- 备份数据是压缩打包后的历史数据，需要通过数据恢复的方式进行检索查看。

系统支持按照不同数据占磁盘的百分比进行数据自动清理，其中在线数据至少会保留 2 天的数据。还可以设置在线数据保存的最小天数。当在线数据的磁盘使用率达到设定值后，即使没有超过保存天数，系统仍会清理部分在线数据。

步骤 1. 在菜单栏选择“**系统管理　系统维护　数据清理**”进入页面，默认配置如下。

步骤 2. 点击<修改>按钮，弹出修改页面，可按需修改配置后，点击<确定>。

详细配置如下表：

配置项	说明
在线数据最大占用空间百分比	设置在线数据最大占用空间百分比，默认为 55%。
备份数据最大占用空间百分比	设置备份数据最大占用空间百分比，默认为 10%。
所有数据最大占用空间百分比	设置所有数据最大占用空间百分比，默认为 75%。
日志留存天数	设置日志留存天数，取值范围：2～3650，默认为 180。
预留系统数据占用空间百分比	预留空间供抓包文件、日志等系统数据使用，不可修改，默认为 10%。

1、所有数据最大占用空间百分比需小于可靠性配置数据分区阈值，差值至少为 5%

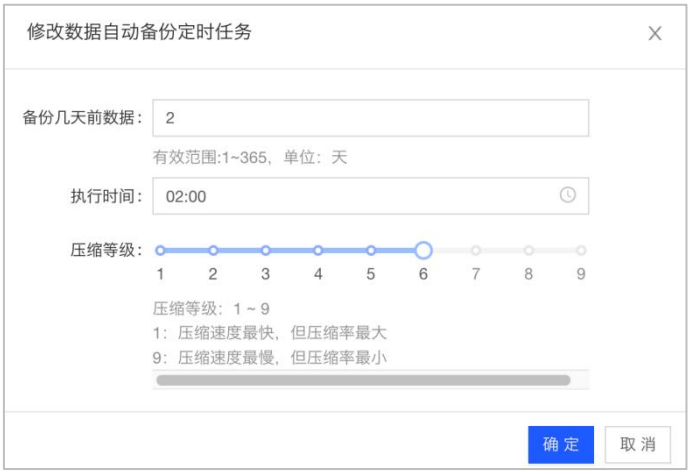
2、在线数据、备份数据、预留系统数据空间占比之和应小于所有数据空间占比

11.3.6 数据备份恢复

11.3.6.1 数据备份配置

默认设置为备份两天前的数据，执行时间为凌晨 2：00，压缩等级为 6 级。

步骤 1. 在菜单栏选择“**系统管理 系统维护 数据备份恢复**”页面，点击<修改>按钮。



详细配置如下表：

配置项	说明
备份几天前数据	默认为 2 天前，如 25 号备份 23 的数据。 根据实际情况填写需要备份几天前的数据，取值范围：1～365 天。
执行时间	数据自动备份的执行时间。
压缩等级	支持压缩等级为 1～9 级（1：压缩速度最快，但压缩率最大；9：压缩速度最慢，但压缩率最小）

11.3.6.2 备份外送 FTP 设置

步骤 1. 在菜单栏选择“**系统管理　系统维护　数据备份恢复**”页面，点击备份外送 FTP 配置下的<修改>按钮。填写各项参数后，可以点击<测试连接>按钮测试连通性。

详细配置如下表：

配置项	说明
状态	启用或禁用将备份数据外送至 FTP 服务器。
协议	支持 FTP 协议。
IP/端口	配置 FTP 服务器的 IP 和端口号。
用户名/密码	配置登录 FTP 服务器的用户名和密码。
上传目录	备份文件上传至 FTP 服务器的目录。

11.3.6.3 在线/备份数据管理在线数据

1. 备份：点击操作列中的<备份>可对在线数据进行备份，备份成功后可在本地备份数据页签中查看。备份中的数据，状态显示“备份中”。

2. 清理：点击操作列中的<清理>可对在线数据进行清理，清理后将查询不到该日志。

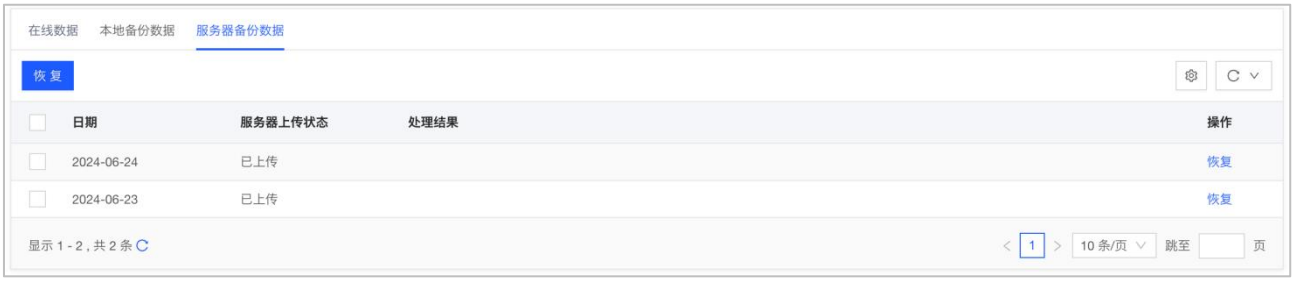
◆ **本地备份数据**

1. 恢复：点击操作列中的<恢复>可对备份数据进行恢复，恢复成功后可在在线数据页签中查看。恢复中的数据，状态显示“恢复中”。不可恢复本地已存在的数据。

2. 清理：点击操作列中的<清理>可对备份数据进行清理。

3. FTP 外送：点击操作列中的<FTP 外送>可将备份数据外送至 FTP 服务器，外送后可在服务器备份数据页签中查看。若未进行备份外送 FTP 配置，则无法外送。

◆ **服务器备份数据**



1. 恢复：点击操作列中的<恢复>可将 FTP 服务器上的备份数据恢复。不可恢复本地已存在的数据。

11.3.7 设备管理

设备管理模块允许管理员配置和调整设备的各种参数和设置，以保证设备的稳定运行，并适应不同的业务需求。

步骤 1. 在菜单栏选择“**系统管理　系统维护　设备管理**”进入页面，可查看相关配置和操作。

若为旁路部署模式，则后端服务配置项有所不同：

详细操作请参见下表：

操作	说明
运行模式	选中不同的运行模式后保存，可手动切换不同的运行模式。
关闭设备	点击<**关机**>，在弹出的对话框中点击<确定>即可关闭设备。
重启设备	点击<**重启设备**>，在弹出的对话框中点击<确定>即可重启设备。
重启服务	点击<**重启服务**>，在弹出的对话框中点击<确定>即可重启服务。
恢复出厂设置	点击<**恢复出厂设置**>，在弹出的对话框中点击<确定>即可恢复设备至出厂状态。
SSH 登录设置	调整 SSH 端口状态的开关至“开启”或“关闭”，以启用或禁用 SSH 登录功能。
水印展示	启用水印展示功能后，页面将显示水印。水印的默认格式为“用户名-时间”，但如果用户设置了手机号码，水印格式将更改为“用户名-手机号”。
审计日志	开启后记录审计日志，但审计日志会影响系统性能和稳定性。
数据包转发超时时间	默认为 10 毫秒，可配置范围为 1-1000 毫秒。 配置太小，可能解析超时，造成脱敏不生效等问题；配置太大，可能影响性能。
敏感数据扫描任务超时时间	默认为 30 秒，可配置范围为 30-600 秒。 若数据库表量极大，在敏感数据扫描任务中获取 Schema/数据库可能失败，需将该超时时间配置改大。
安全运维管控机制	默认为弱管控模式，支持弱管控或强管控。 ◆ 弱管控：所有账号均可访问数据库。 ◆ 强管控：对访问数据库的账号进行严格管控，仅“数据库访问账号”允许访问数据库，未经过账号托管的数据库账号（即原始数据库账号）默认阻断。
IPv6 配置	默认禁用通过 IPv6 访问 Web 页面。若修改此配置，需等待 2 分钟后再进行访问。
管理口隔离	启用后，将实现管理流量与业务流量的彻底分离。管理端口仅开放 SSH（默认端口 22）和 HTTPS（WEB 服务默认端口 443，支持自定义）；而业务端口则禁止访问这些端口，从而最小化网络暴露面，遵循零信任安全原则。
阻断方向（限旁路模式）	默认为服务端，可配置为服务端、客户端、全部(两个方向)。
会话阻断时长（限旁路模式）	当命中会话阻断的安全规则后，产生会话阻断策略对应的生效时长。
IP 阻断时长（限旁路模式）	当命中 IP 阻断的安全规则后，产生 IP 阻断策略对应的生效时长。 当命中 IP 阻断的虚拟补丁规则后，产生的 IP 阻断策略对应的生效时长。

- 关闭设备后，业务将不可用，请谨慎操作。
- 重启设备期间业务将不可用，请谨慎操作。
- 恢复出厂设置将删除系统所有数据，恢复到出厂状态，请谨慎操作。

11.3.8 HA 配置

数据库安全网关支持高可用性（简称 HA）部署，确保系统在出现故障时能够继续正常运行。可以避免单点故障（SPOF），即某个组件的故障导致整个系统不可用。在 HA 部署模式下，系统配置将由主机定期同步至备机，从而当主服务器发生故障时，备用服务器能够迅速接管工作，确保业务不中断。

所有模式均支持 HA 部署，其中反代和路由是十分钟主往备同步一次，透明是实时同步，互为主。

步骤 1. 在菜单栏选择“**系统管理　系统维护　HA 配置**”进入 HA 页面，默认为单机模式。

步骤 2. 配置 HA 主机：点击<修改>按钮，选择运行模式为 HA 主机，并填写相关配置后，点击<确定>。

配置完成后，在“系统管理　系统维护　HA 配置”页面中仍会显示运行模式为备机，需等待一小段时间后再次刷新页面方可显示成 HA 主机。

步骤 3. 配置 HA 备机：点击<修改>按钮，选择运行模式为 HA 备机，并填写相关配置后，点击<确定>。

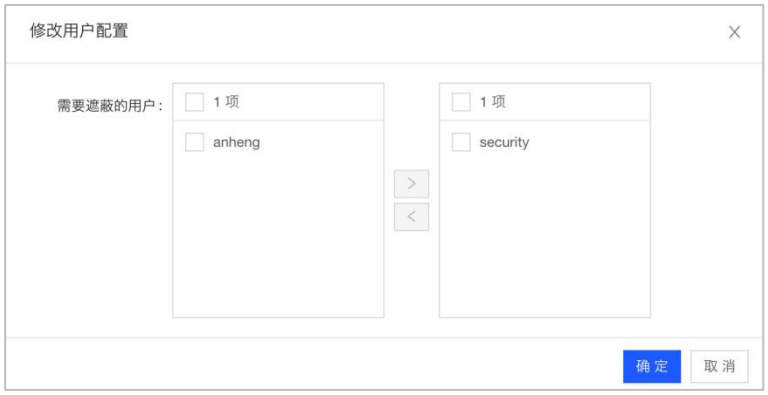
详细配置请参见下表：

配置项	说明
运行模式	主机上选则：热备模式-HA 主机 备机上选择：热备模式-HA 备机
检测网口	检测网络接口，本机接收数据的网口。
虚拟 ID	主备机的此项配置需保持一致，有效范围 1~99。
广播间隔	VRRP Multicast 广播周期秒数。
VRRP 虚拟地址	VRRP HA 虚拟地址。
主机/备机 IP	备机/主机的 IP。
备机登录用户	默认是 admin，也可以是自定义用户。
备机登录密码	admin 账户的密码，或者自定义用户的密码。

11.3.9 敏感数据遮蔽

启用敏感数据遮蔽功能后，安全管理员或安全员用户登录后查看带有敏感字段的日志将做遮蔽处理。

步骤 1. 在菜单栏选择“**系统管理　系统维护　敏感数据遮蔽**”，进入敏感数据遮蔽页面，点击<修改>按钮，弹出修改用户配置框，选择需要遮蔽的用户。



步骤 2. 点击<新增>按钮，弹出新增数据脱敏框，填写相关配置后，点击 <保存>。

详细配置请参见下表：

配置项	说明
名称	必须为中文字符、字母、数字、下划线(_)、点(.)或短横(-)，长度不超过 64。
状态	可选择启用或禁用。
正则表达式	依据填写的正则表达式来判断敏感字段符合哪种类型的遮蔽，例如邮箱的正则：\w+(\.\w)*@\w+(\.\w{2,3}){1,3}
过滤范围	填写要遮蔽的开始位置和长度。

11.3.10 IP 白名单

IP 白名单配置，可以放通配置的 IP，跳过所有配置的规则和审计。由于 IP 白名单在系统内匹配优先级最高，且不经过系统后续处理，对设备性能占用较少。当有大数据库流量远超设备性能时建议添加 IP 白名单处理，避免导致设备不可用。

步骤 1. 在菜单栏选择“**系统管理 系统维护 IP 白名单**”，进入 IP 白名单页面，点击状态按钮，开启或禁用此功能，默认是禁用。启用后如下图所示：

步骤 2. 点击 IP 白名单管理模块中的<新增>按钮，在新增窗口中填写要加白的 IP 后，点击<保存>。

步骤 3. 新增后的 IP，可以参考如下界面，支持“编辑”或者“删除”操作。

11.3.11 逃生机制

逃生机制作为最后一道防线在核心服务异常时保障业务不中断。该功能通过系统监控和自动切换机制，实现从故障检测到备用方案启用的全自动化处理，最大限度减少人工干预和业务停机时间。当系统触发逃生机制后，会在“**系统管理 系统告警**”页面记录具体触发逃生的原因和逃生记录。

步骤 1. 在菜单栏选择“**系统管理 系统维护 逃生机制**”进入页面，配置如下图所示：

步骤 2. 点击页面上的<修改>按钮，弹出修改逃生机制窗口，可设置逃生阈值。

具体配置项请参见下表：

配置项	说明

配置项	说明
逃生机制	默认启用。启用后自动检测系统异常情况，自动逃生确保业务可用。
代理连接异常状态数量阈值	默认设置为 5000。监控代理层 TCP 连接异常状态总数（CLOSE_WAIT + FIN_WAIT2）。当异常连接数超过此阈值时，表明连接池可能发生泄漏或阻塞，系统将触发逃生机制。
会话连接数占比阈值（仅适用于硬件设备）	默认设置为 95%。基于设备型号的并发会话数规格上限。当当前会话连接数达到最大承载能力的 95%时触发，确保系统不会因过载而崩溃。
数据库流量占比阈值（仅适用于硬件设备）	默认设置为 100%。基于设备型号的并发数据库流量规格上限。当网络流量达到最大承载能力时触发，确保系统不会因过载而崩溃。
连续触发次数（仅适用于硬件设备）	默认设置为 4 次。流量阈值触发的确认次数。当流量异常持续达到指定次数后才会激活逃生，避免瞬时峰值导致的误触发。
数据库连接状态检测	默认禁用。启用后主动探测后端数据库的可达性。当数据库连接失败时触发告警或逃生。

11.4 系统告警

11.4.1 告警查询

数据库安全网关支持系统自检功能，当出现系统资源使用率过高、系统服务异常、新增数据库隐身策略等情况时，会自动产生一条告警信息方便用户快速定位问题。

步骤 1. 在菜单栏选择“**系统管理　系统告警　告警查询**”进入系统告警页面。

步骤 2. 点击<修改>，弹出修改系统日志自动清理配置对话框，可设置日志保留天数，点击<确定>。

步骤 3. 支持通过配置时间范围、告警类型、告警级别查询相关告系统警日志信息。

11.4.2 告警通知

告警通知是指将系统日志发送至指定的接收者。新增系统日志外送任务的操作方法如下：

步骤 1. 在菜单栏选择“**系统管理　系统告警　告警通知**”进入告警通知页面。

步骤 2. 点击<新增>弹出新增系统日志外送任务对话框，编辑相关信息，点击<保存>。（若选择邮件通知方式，请配置邮件发送服务器，详见系统配置-通知外送；若选择 SYSLOG 通知方式，请进行 SYSLOG 接收配置，详见 SYSLOG 告警外发。外发模版在“**通知外送　告警通知**”页面进行配置，详见通知外送。）

11.5　操作日志

系统将记录所有用户的相关操作，审计管理员/审计员可查看操作日志进行溯源。

步骤 1. 在菜单栏选择“**系统管理　操作日志**”进入操作日志查询页面，可根据时间范围、用户、来源 IP、操作名称、操作内容和操作结果来搜索相应操作日志。

步骤 2. 点击列表左上方的<日志导出>按钮，可以以表格的形式导出操作日志。

12 术语&缩略语

术语	解释
SNMP	SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议，支持目前主流的网络管理系统。
SQL	SQL 是结构化查询语言（Structured Query Language）的简称，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统；同时也是数据库脚本文件的扩展名。
Syslog	Syslog 是一种行业标准的协议，可用来记录设备的日志。Syslog 日志消息既可以记录在本地文件中，也可以通过网络发送到接收 Syslog 的服务器。服务器可以对多个设备的 Syslog 消息进行统一的存储，或者解析其中的内容做相应的处理。常见的应用场景是网络管理工具、安全管理系统、日志审计系统。
数据库	数据库（Database）是用于存放数据的仓库，按照一定的数据结构（即数据的组织形式或数据之间的联系）来组织、存储，用户可以通过数据库提供的多种方法来管理数据库中的数据。
规则	本文中所述的规则是指根据一些特征 (如客户端、服务端、SQL 语句) 定义的危险行为 (安全规则）及可以信任的行为（过滤规则）。当系统审计到对数据库的操作匹配安全规则时会触发告警，对于匹配过滤规则的行为则不进行审计。
资产	本文中所述的资产是指系统需要审计管理的数据库系统、网站等信息系统。
对象组	具备相同业务属性或相似业务逻辑的敏感库、表、字段的集合。
密码桥	一种使用数据库安全网关后的密码替换技术，可实现隐藏真实的数据库账号密码，使用网关分配的数据库账号密码即可完成数据库的访问。
身份权限	一种基于客户端身份规则因子确定身份匹配相应权限的规则策略。
动态脱敏	动态脱敏是一种实时数据脱敏技术，通过 SQL 改写在不改动原始数据的前提下完成敏感数据的变形或替换，以保护隐私和数据安全。
数据库隐身	一种安全策略，通过识别扫描工具特征、智能分析扫描工具行为等一系列内置策略，智能下发防漏扫策略，阻断扫描行为，从而达到数据库防漏扫的效果。