安恒信息
DAS-security 安全中国

AiGate 数据安全网关

用户手册

目 录

前言

概述

感谢您选择安恒信息的网络安全产品。本手册对安恒信息 AiGate 数据安全网关（以下简称“系统”或“AiGate”）进行了简单介绍，并对系统的使用方法进行了详细描述。主要包括快速入门、Web 配置页面简介、总览、资产、访问控制、查询分析、规则配置、系统管理以及操作日志。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于使用 AiGate 的人员，包括超级管理员、安全管理员、系统管理员、审计管理员等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP 等基础网络通讯协议
- 数据库、服务器、路由器、交换机等常见设备（系统）的基本工作原理和配置
- 数据库攻击相关知识，包括 SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段

格式约定

本手册内容格式约定如下：

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如：“在菜单栏中选择**系统状态**进入**系统状态**页面，选择**接口状态**页签。”
< >	Web 界面上的按钮。例如：“微信认证失败，点击<**我要上网**>不弹出微信认证界面”。
➤	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等），例如：“在菜单栏选择‘**策略配置➤认证管理➤认证策略**’查看是否开启了认证策略”。

本手册图标格式约定如下：

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1. 快速入门

1.1. 产品简介

AiGate 是安恒信息在多年数据安全访问控制理论和实践经验积累的基础上，结合数据最小够用原则、可用不可见理念，采用 B/S 架构，集身份认证、数据分级分类、访问控制和动态脱敏于一体的数据库安全防护产品，支持 Oracle、MySQL、MariaDB、PostgreSQL、MSSQL、DB2 等关系型数据库，为数据库提供全方位的防护，提供覆盖数据库使用全生命周期的安全防护解决方案。

产品分为硬件版和云上版两种版本，两种版本功能基本相同，用户可根据需要进行购买。

1.1.1. 产品功能

AiGate 产品功能分成身份认证、数据分级分类、访问控制、动态脱敏、运维审批五大功能。

1、身份认证

数据安全网关基于基于通过 IP、客户端主机名、操作系统用户名、客户端工具名和数据库账号等多个维度对用户身份进行管理，确保你就是你，设备是可信的设备，应用是认证应用。通过全面的身份化，实现对网络参与的各个实体在统一的框架下进行统一的身份认证。

2、数据分级分类

提供自动获取用户数据服务中的元数据的功能，在配置合适的账号密码后，自动获取数据的基本信息包括：库、表和字段等信息。同时支持按元数据手动配置和 API 接口方式对接第三方数据分级分类系统。内置了姓名、证件号、金额、日期、住址、电话号码、Email 地址等敏感数据识别规则，可以协助用户快速完成手动分类分级。

3、访问控制

数据安全网关结合数据分级分类实现基于数据的访问控制功能，用户只需要简单的配置好什么级别的用户允许访问什么级别的数据和越级访问时候的处理动作，就可以完成配置，实现数据的访问控制功能。数据安全网关采用反向代理或者串联部署，通过实时的数据协议代理彻底地实现了精细化的访问控制，对维护人员和业务系统的请求进行有效的访问控制，对进出核心数据服务的访问流量进行高效、精准的解析和精细的访问控制，根据预设的自定义规则有效的识别各种可疑、违规的访问行为，实时放行或者阻断对应的 SQL 请求或者会话，有效地阻止不允许访问的，深度地检测授权的访问是否合规，从而达到数据访问的合规。

4、动态脱敏

数据安全网关内置了替换、截断、取整、掩码等常见的脱敏方法，在实现数据模糊化后，还具有一定的运算和分析价值，真正的实现用户数据的可用不可见。

5、运维审批

数据安全网关可以通过申请人登录，创建运维任务，客户端执行相关 SQL 时，后台会通过相关规则，产生运维日志，或者阻断。

1.1.2.产品特点

1、采用多核、多线程并行处理技术，处理性能领先

AiGate 采用国际领先、适合审计产品特性的硬件平台。依托 Intel 多核 CPU 的强大计算能力以及安恒信息独有的多线程分布式处理技术，使得系统处理能力大大提升，领先于国内同类型产品。

2、数据库安全分析

AiGate 内置丰富的漏洞规则，在防护过程中通过规则匹配发现数据库的配置不合理项和安全漏洞，并可根据漏洞情况提供合理的安全建议和防护规则。

3、虚拟补丁防护

数据安全网关使用数据库虚拟补丁技术，通过控制数据库的请求参数、类型和个数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，极大地保护了未升级漏洞补丁的数据库服务器，极大降低了用户数据篡改和泄露的可能。

4、安全规则防护

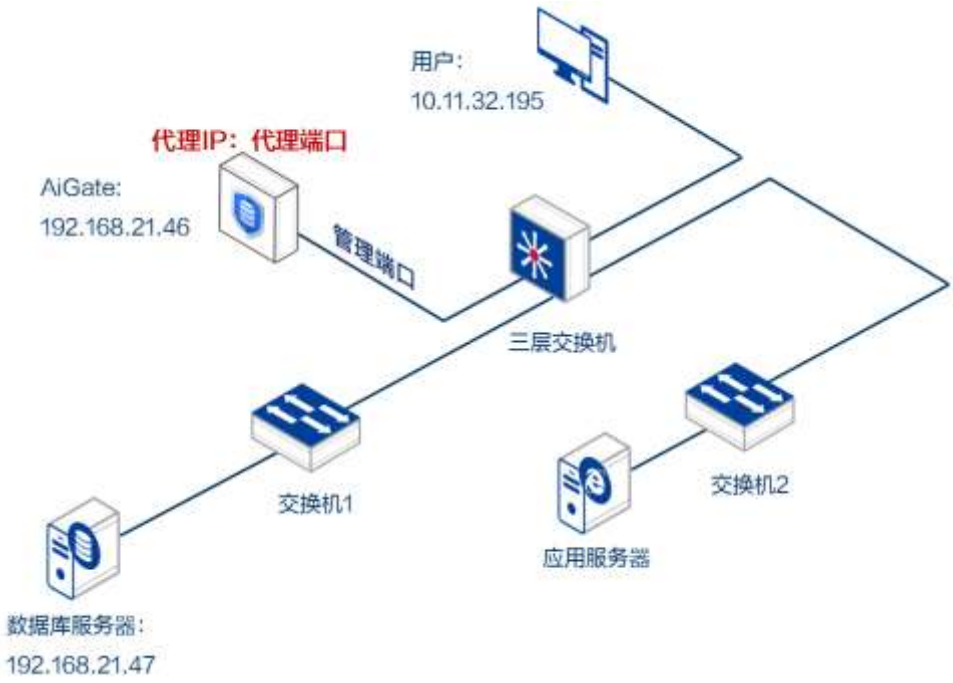
数据安全网关内置的多种常见的数据攻击规则，针对多种攻击场景提供有效防护。可有效减少数据破坏，数据勒索，数据窃取，数据误操作等带来的数据风险。数据安全网关提供灵活且细粒度的自定义防护规则，支持根据数据库、用户名、客户端工具、源 IP、主机名、SQL 关键词、操作类型、返回行数、执行时长、SQL 错误代码等设定规则。

1.1.3. 典型应用场景

AiGate 支持反向代理的流量采集方式。

1.1.3.1. 反向代理模式

AiGate 支持通过在自身设备上配置数据库资产信息及对应的代理 IP 和代理端口，应用系统或者运维数据库的运维终端并不通过实际的数据库服务器资产信息访问数据库系统，而是通过访问 AiGate 设备的代理 IP 和代理端口对实际的数据库系统进行访问。如下图所示。



1.2. 角色与权限说明

不同角色的用户具有的权限不同，超级管理员可自定义角色。系统默认的角色及权限可参考下表，具体请以实际情况为准。

角色	权限
超级管理员	具有系统所有权限。
安全管理员	查看日志、管理数据库、管理安全员。
系统管理员	系统的配置与维护、管理系统配置员。
审计管理员	查看操作日志和管理审计员。
安全员	查看审计日志、告警日志和会话日志。
系统配置员	配置系统、系统维护、管理辅助功能、查看系统告警。

审计员	查看其他用户的操作日志。

1.3. 登录系统

设备安装上架并连接网线、电源后，用户需要搭建合适的配置环境进行设备的初始配置（即网络配置）。

AiGate 支持 CLI 和 Web 两种配置方式，CLI 支持 Console 通信管理协议。

云上版仅支持 Web 配置。

设备出厂时设置的默认管理口地址 192.168.1.100，子网掩码 255.255.255.0。默认的管理员用户名为 admin，密码为 Dbapp@2013，登录系统后请及时修改密码。

1.3.1. CLI 配置

请参考以下步骤搭建 CLI 配置环境：

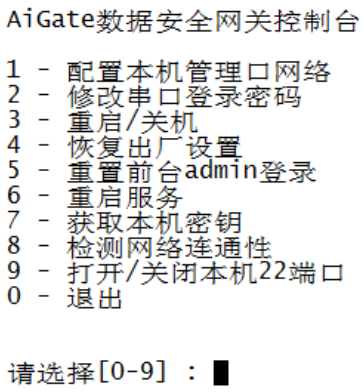
步骤1. 将配置线缆的 DB-9 插头连接至配置 PC 的串口。

步骤2. 将配置线缆的 RJ-45 插头连接至设备的 Console 口。

步骤3. 在 PC 上运行终端仿真程序（如 SecureCRT、XShell 等），并按照下表所示设置参数。

配置项	说明
波特率	115200 bit/s
数据位	8
奇偶校验	无
停止位	1
数据流控制	无

步骤4. 打开设备电源开关，设备会进行自检并且自动进行初始化配置，输入默认用户名和密码并回车，成功登录系统并且进入 CLI 界面，如下图所示。



1.3.2. Web 配置

本文仅以硬件版举例说明，云上版需保证配置 PC 与系统路由可达即可。

用户可通过管理口登录到设备的 Web 管理平台进行配置，操作方法如下：

步骤1. 将配置 PC 的 IP 地址设置为与 192.168.1.100/24 同网段的 IP 地址，并用网线将 PC 的网口与设备的管理口连接起来。

步骤2. 在配置 PC 的 Web 浏览器（建议使用 Chrome 浏览器）地址栏中输入“https://192.168.1.100”并回车，进入系统 Web 管理平台登录页面，如下图所示。

步骤3. 输入默认用户名和密码，点击<**登录**>进入系统 Web 管理平台主界面（首次登录系统会提示修改密码）。

1.4. 主要业务流程

系统主要业务流程如下图所示。

步骤1. 修改管理口 IP：为适配用户的实际网络环境，需要修改设备管理口 IP，详情请参见 11.2.1.网络。

步骤2. 添加资产：添加系统需要防护的数据库，详情请参见资产。

步骤3. 数据分类分级：对用户数据服务中的元数据进行分类分级，详情请参见数据分类分级。

步骤4. 配置访问控制：配置身份认证和数据访问，实现人员级别对数据级别的访问控制功能，详情请参见访问控制。

步骤5. 规则配置：配置数据库的安全规则和脱敏规则，详情请参考规则配置。

步骤6. 查询分析：对匹配的安全规则的级别产生相应级别的告警信息和脱敏信息进行查看和分析，详情请参见查询分析。

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.上边栏；2.菜单栏；3.操作区。

2.1. 用户头像

2.1.1. 修改用户信息

步骤1. 将光标悬停于用户头像，选择**我的信息**。

步骤2. 进入**我的信息**页面后，可修改基本信息。

2.1.2. 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系统。

2.1.3. 查看系统版本

将光标悬停于用户头像，选择**关于本系统**查看软件版本信息，按“Shift+V”组合键可查看系统的详细软件版本号。

关于本系统 ×

系统名称	数据库安全网关
软件版本	V2.1.3.220224.0935
设备型号	P1600
服务代码（SN）	[redacted]
设备厂商	杭州安恒信息技术股份有限公司
公司网站	http://www.dbappsecurity.com.cn

3. 总览

总览页面展示了系统的资源使用情况和实时监控状态。

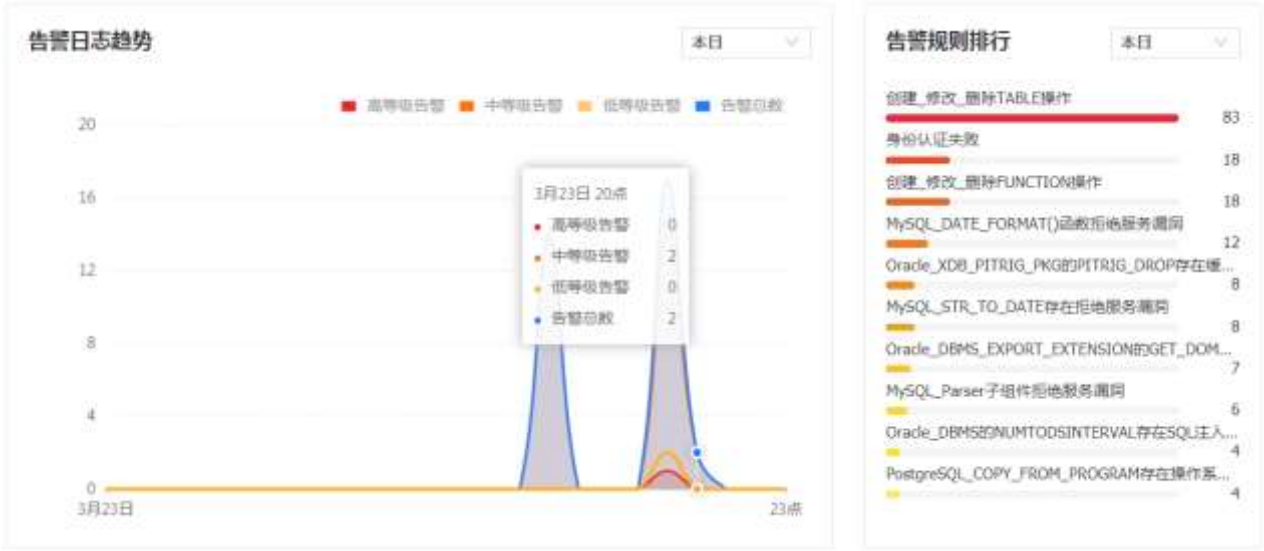
3.1. 仪表盘

登录系统 Web 管理平台后默认进入仪表盘页面。仪表盘提供可视化图表直观展示系统运行状态，主要包括系统资源使用汇总、态势分析和资产信息汇总。

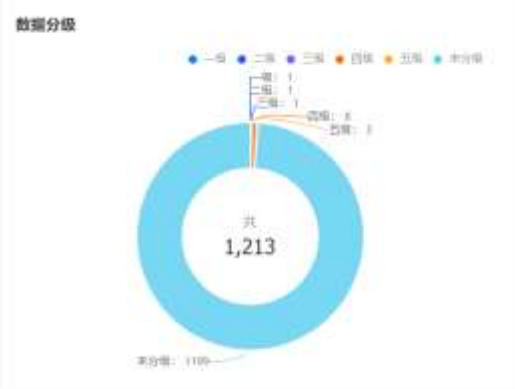
在菜单栏选择“**总览**”进入仪表盘页面。用户可在仪表盘查看以下信息，或执行以下操作。

◆查看资产数、在线会话数、告警总数和各规则类别触发告警数等参数。

◆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排序情况。



4. 资产

资产是指系统需要防护管理的数据库系统。

4.1. 资产管理

添加资产后，系统可对资产进行安全防护。添加资产的操作方法如下：

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**添加资产**页面编辑相关信息。

详细配置请参见下表。

配置项	说明
类型	设置资产类型，包括 Oracle、MySQL、MariaDB 和 PostgreSQL 等通用数据库，HBase、Hive 两种大数据数据库、ODPS 的 HTTP 类型数据库。
名称	非必填项，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，不填则自动生成，格式为：ip_数据库类型_

配置项	说明
	数据库名。
日志记录	是否记录审计及动态脱敏日志开关。
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。
最大保存行数	取值范围 0~999，0 表示不保存返回结果，最大保存内容为 64KB。
最大保存长度	可配范围 1~64K，确保整行显示。
运维审批	开启后，启用运维审批功能
IP 白名单	运维审批开关开启，填写需要加白的 IP，IP 默认不走运维审批流程
防护模式	入侵检测模式：对数据库进行入侵检测,不阻断任何操作； 入侵防护模式：对数据库进行入侵检测和防护。
默认数据源	默认关闭，可启用
SID/服务名	选择实例名或者服务名（Oracle）
数据库名	填写数据库名（pgsql、DB2、mysql、mssql、MariaDB）
用户名	数据库的用户名
密码	数据库用户名的密码

配置项	说明
角色	可以选择 NORMAL、SYSDBA、SYSOPER（Oracle）
表名	数据库中存在的表名
测试	测试数据库的连通性

步骤3. 点击<**保存**>。

点击<**保存**>后，弹出是否立即同步数据框，点击<**确定**>，则跳转到**【资产】-【敏感数据】-【敏感数据扫描】**页面，开始同步数据。注：如果配置 AiSort 关联，则默认从 AiSort 同步数据，反之则从网关同步数据。

点击<**取消**>，则不同步数据，不会跳转页面。

步骤4.

可对已添加的资产进行管理：点击<**编辑**>对资产信息进行修改；点击<**删除**>，在弹出的对话框中点击<**确定**>删除资产；点击“**更多➤启用全部内置规则**”对该资产启用内置规则；点击“**更多➤禁用全部内置规则**”对该资产禁用内置规则。有关内置规则的更多信息，请参考规则配置。

4.2. 敏感数据

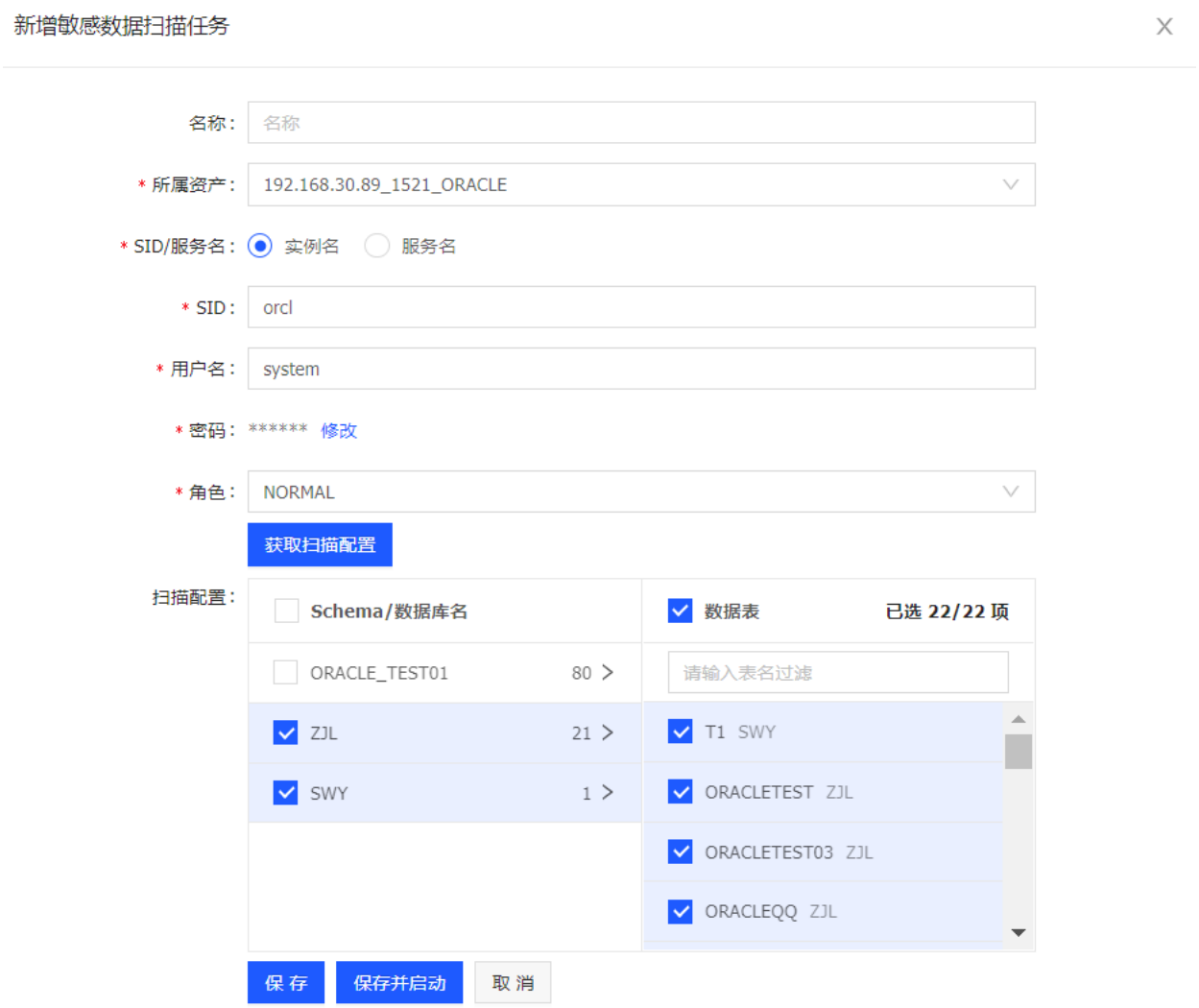
敏感数据扫描提供自动获取用户数据服务中的元数据的功能，在配置合适的账号密码后，自动获取数据的库、表和字段等基本信息。支持配置数据来源拉取元数据后进行手动配置和 API 接口方式对接第三方数据分级分类系统。

4.2.1. 敏感数据扫描

敏感数据扫描是配置资产的数据库连接信息，新增扫描任务的操作方法如下：

步骤1. 在菜单栏选择“**资产➤敏感数据**”进入**敏感数据扫描**管理页面，点击<**新增**>。

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。



详细配置请参见下表。（未提及项参考资产详细）

配置项	说明
名称	非必填项，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，不填则生成格式为：ip_数据库类型_数据库名。不填则自动生成，格式为：数据源名称+yymmddhh24。

配置项	说明
所属资产	设置数据来源所隶属的资产。
用户名	数据库的用户名。
密码	数据库的密码。
数据库名/SID	数据库名称或者实例名称。
扫描配置	当填写正确的数据库信息后，点击“获取扫描配置”按钮，即可获取到当前用户下的数据信息

步骤3. 点击<**保存**>，仅保存数据，不执行扫描任务。（必须选择到数据表才可以保存）。

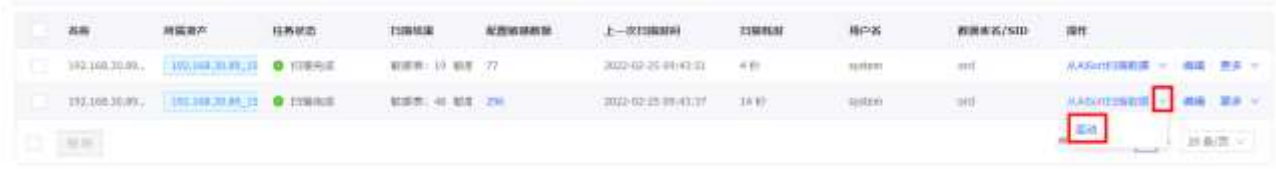
步骤4. 点击<**保存并启动**>。保存数据并立即执行任务。（必须选择到数据表才可以保存）。

步骤5. 点击<**取消**>。取消新增任务。

步骤6. 点击<**编辑**>对数据来源信息进行修改；点击<**删除**>，在弹出的对话框中点击<**确定**>删除数据来源。

- 网关获取的操作方法如下：

步骤1. 点击<**启动**>，从对应的数据来源获取元数据。



步骤2. 元数据获取完成后，状态会显示“扫描完成”，元数据将保存在**敏感数据管理**中。

网关获取元数据的方式需要保证 AiGate 数据安全网关设备地址与数据来源资产数据库的网络连通性正常。

- AiSort 获取的操作方法如下：

步骤1. **【系统管理】-【系统配置】-【AiSort 关联】**配置 AiSort 的 IP 地址和服务端口

步骤2. 点**【测试连接】**，连接成功，表示配置成功，点击**【保存】**，即可配置成功。

步骤3. 新增需要从 AiSort 获取元数据的**数据来源**。

步骤4. 点击<**从 AiSort 获取**>，从 AiSort 系统中获取元数据并保存在**敏感数据管理**中。

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

从 AiSort 获取元数据的方式需要保证 AiGate 数据安全网关设备地址与 AiSort 服务接口的网络连通性正常。

- 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**>按钮，终止拉取数据动作。

4.2.2.敏感数据管理

元数据管理是展现获取到的数据库表结构字段信息，能够进行数据类别和数据级别的定义，且能配置脱敏规则。元数据管理页面提供配置、批量配置查询结果和查询功能，以及级联视图展示数据分级分类配置功能，如下图所示。

4.2.2.1.配置

步骤1. 根据数据来源、库名、表名、字段名或者字段描述筛选要配置的元数据信息，在对应的字段名后面点击<**配置**>。

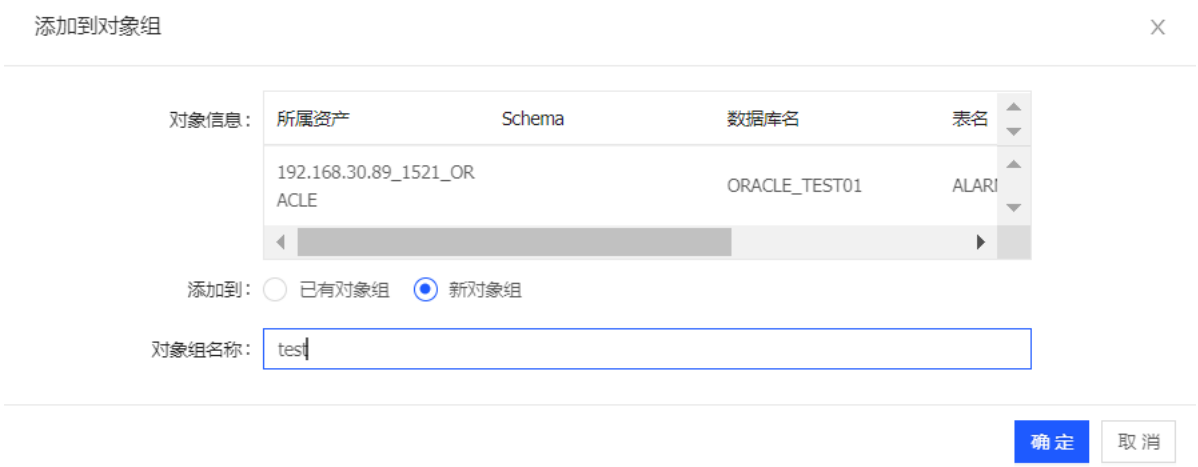
步骤2. 在**编辑分级分类配置**页面，编辑状态、敏感数据等级、敏感数据类型和脱敏规则，点击<**保存**>。

详细配置请参见下表。

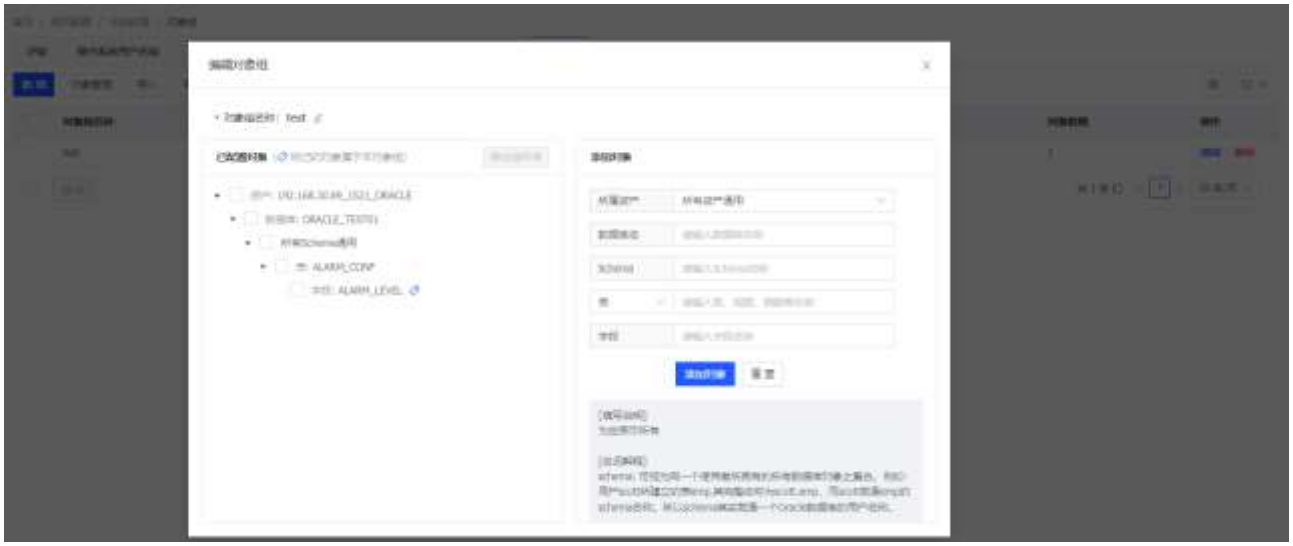
配置项	说明
状态	启用或禁用该配置。
敏感数据等级	敏感数据等级默认可选一级、二级、三级、四级和五级，等级高低逐渐升高，一级为最低，五级最高。
敏感数据类型	敏感数据类型默认可选无、身份证、银行卡、手机号、邮箱、座机号、军官证、护照号、车牌号、MAC 地址、日期、时间、港澳台通行证、台胞证、中文名字。
脱敏规则	配置数据字段的脱敏规则。有关内置脱敏规则的更多信息，请参考规则配置。

步骤 3. 根据数据来源、库名、表名、字段名或者字段描述筛选要配置的元数据信息，在对应的字段名后面点击<**添加到对象组**>。

步骤 4. 在添加到对象组 Tab 页，可选择添加到已有的对象组，或者新的对象组。



步骤 5. 添加到对象组后，可以到【**规则配置**】-【**关联数据**】-【**对象组**】中查看。



4.2.2.2.批量配置查询结果

批量配置查询结果可以提高数据分级分类配置的效率，操作方法如下：

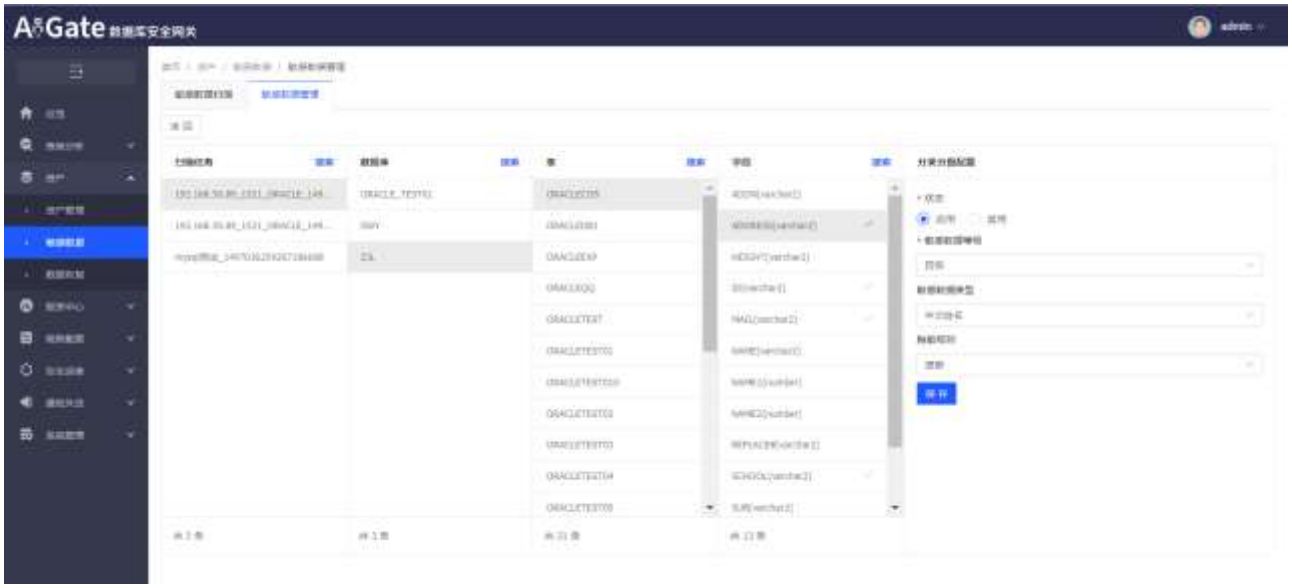
步骤1. 选中需要配置的字段名称，点击<**批量配置选中项**>或者点击<**批量添加到对象组**>。

步骤2. 在**批量配置**页面，编辑状态、敏感数据等级、敏感数据类型和脱敏规则，点击<**保存**>。

步骤3. 在批量**添加到对象组**页面，添加到已有对象组或新对象组，点击<**确定**>。

4.2.2.3.级联视图

级联视图以数据来源、数据库/Schema、表、字段和分类分级配置的关联性呈现和配置元数据。



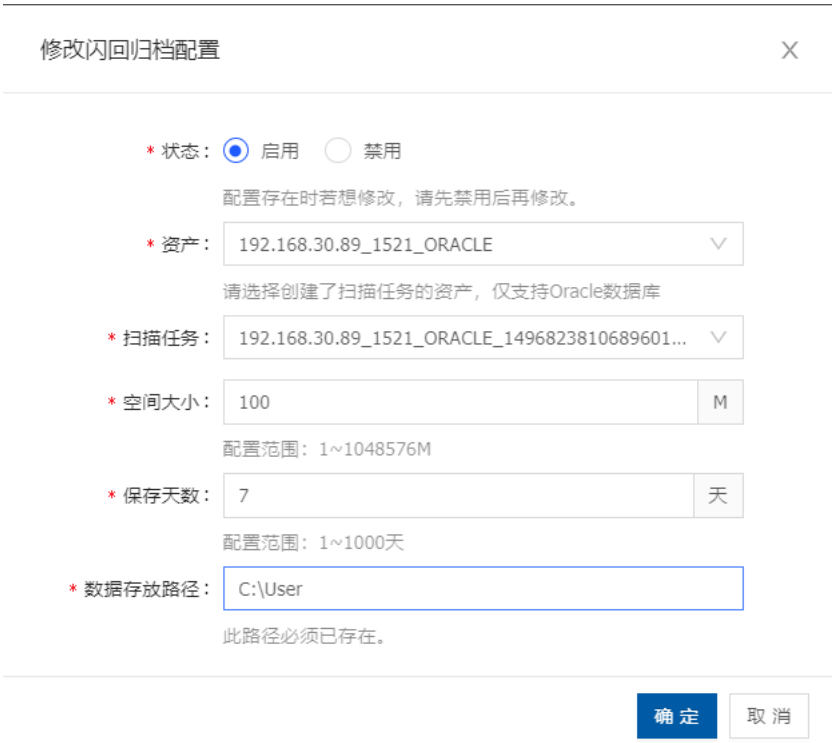
4.3.数据恢复

数据误删除恢复目前只支持 Oracle，当闪回归档配置中配置库表后，客户端执行 delete 或者 truncate 时，闪回归档配置中便会增加一条删除日志，在需要恢复数据的情况下，点击删除日志后的恢复按钮，可恢复

客户端删除掉的数据。

步骤 1.资产-数据恢复，配置页面如下图

步骤 2. 点击修改，可进入闪回归档配置界面框

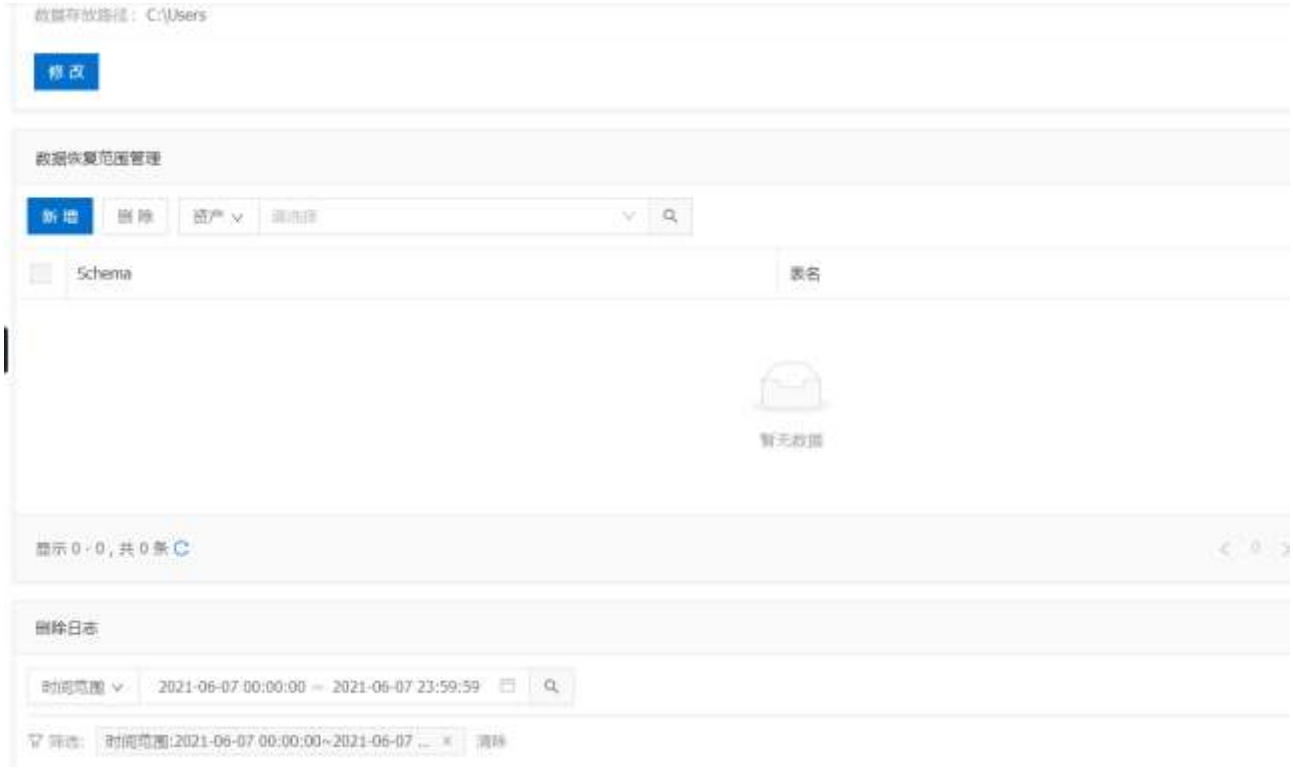


配置项说明：

配置项	说明

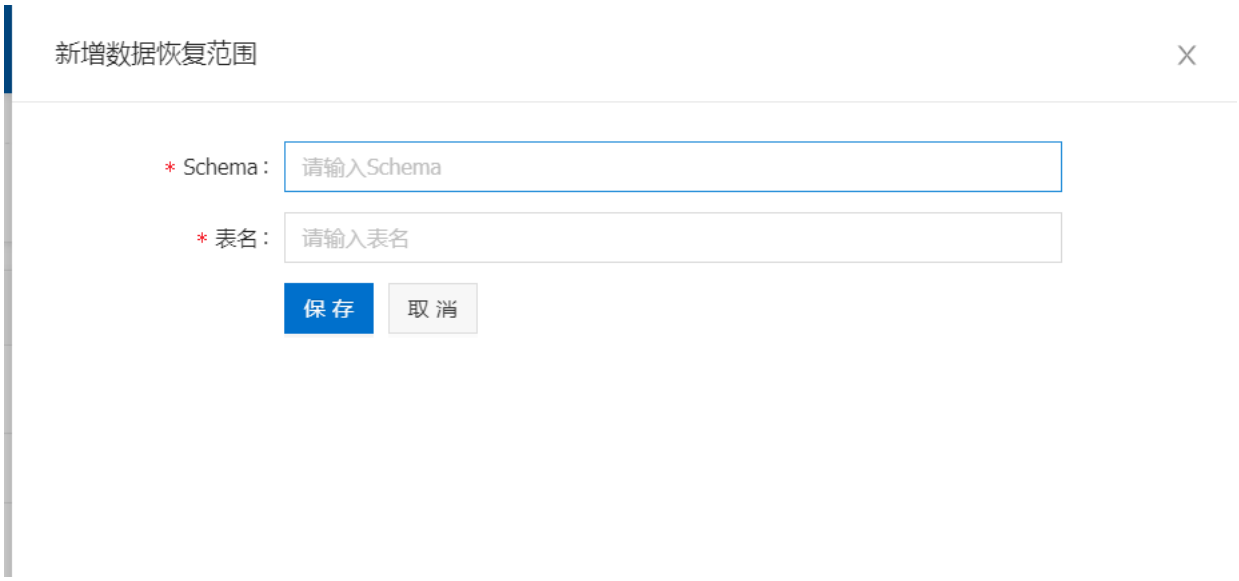
配置项	说明
状态	启用或禁用该配置。启用后不可修改；禁用后可修改，配置过的库表全部被清空
资产	选择 Oracle 资产
数据来源	选择 Oracle 数据来源
空间大小	配置存放备份数据的空间大小，1~1048576M 之间
保存天数	配置备份数据保留天数，最大 1000 天
数据存放路径	配置保留数据存放的路径，Windows 路径，例如：C:\Users；linux 路径，例如/home

启用后，显示如下页面



步骤 3.数据恢复范围管理添加

点击新增按钮，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 4. 客户端登录，执行 delete 或者 truncate 操作（数据恢复范围管理中的库表），删除日志有记录情况，点击恢复按钮，可恢复被删除的数据

5. 报表中心

AiGate 结合 SQL 语句、告警、脱敏、流量、运维等数据在报表中展示，并能通过邮件订阅发送到邮箱查看。

5.1. 报表预览

AiGate 后台产生的 SQL 语句、告警、脱敏、流量、运维等数据记录，会在报表预览中展示。报表预览包括 SQL 语句变化趋势分析、最大并发会话分析、数据脱敏分析、告警分析类报表、流量分析报表、运维审批分析报表。包含订阅功能和导出功能，订阅功能请参考 5.3 章节。

配置项	**说明**
分析对象	资产名称
数据库类型	数据库类型
IP 与端口信息	数据库 IP 和原生端口
时间范围	发生的时间范围
报告生成时间	报告生成时间

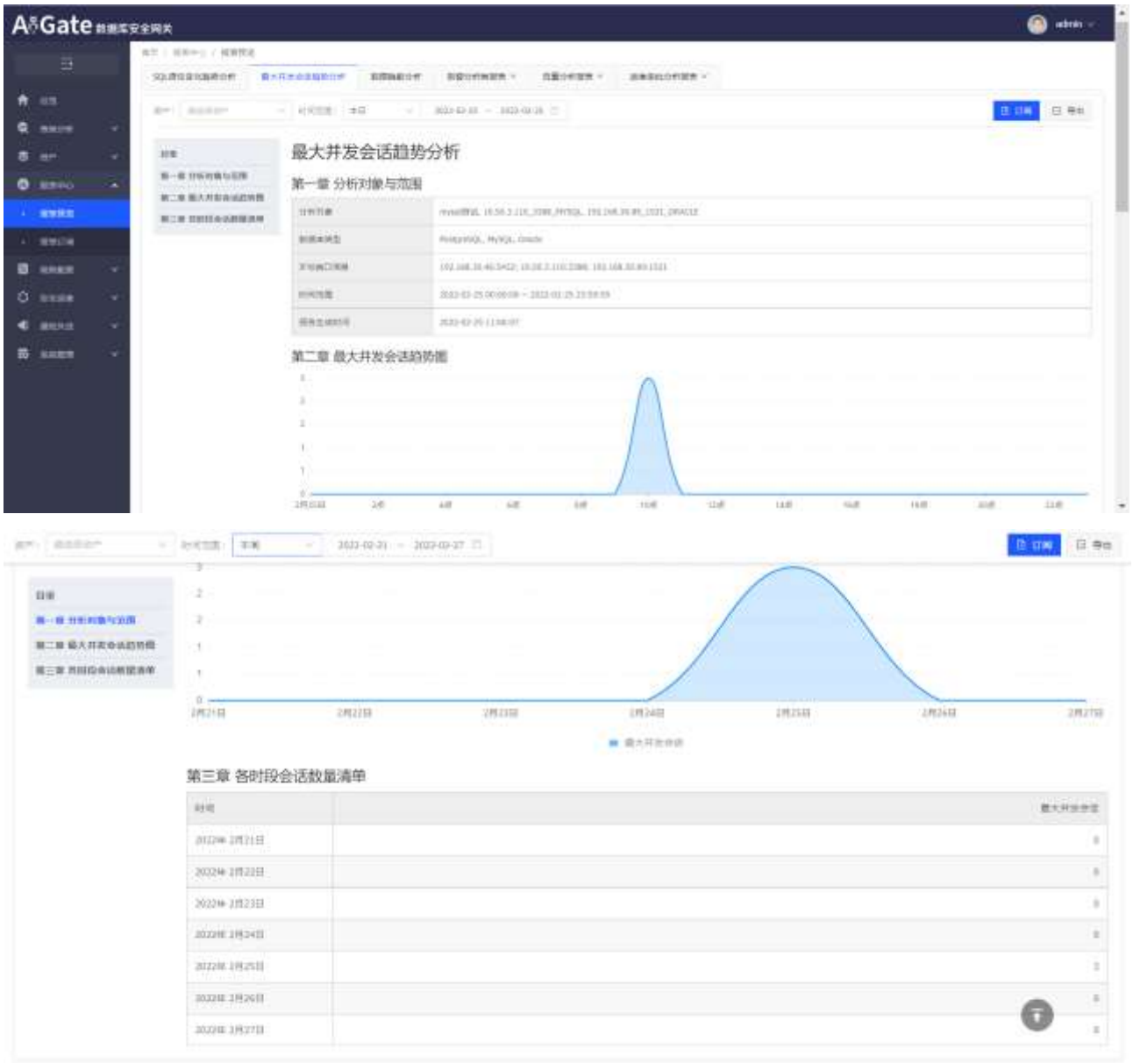
5.1.1. SQL 语句变化趋势分析表

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，点击 SQL 语句变化趋势分析表，分为三章。第一章分析对象与范围；第二章 SQL 语句数量变化趋势图；第三章 各时段 SQL 语句数量清单。

5.1.2. 最大并发会话趋势分析

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，点击最大并发会话趋势分析表，分为

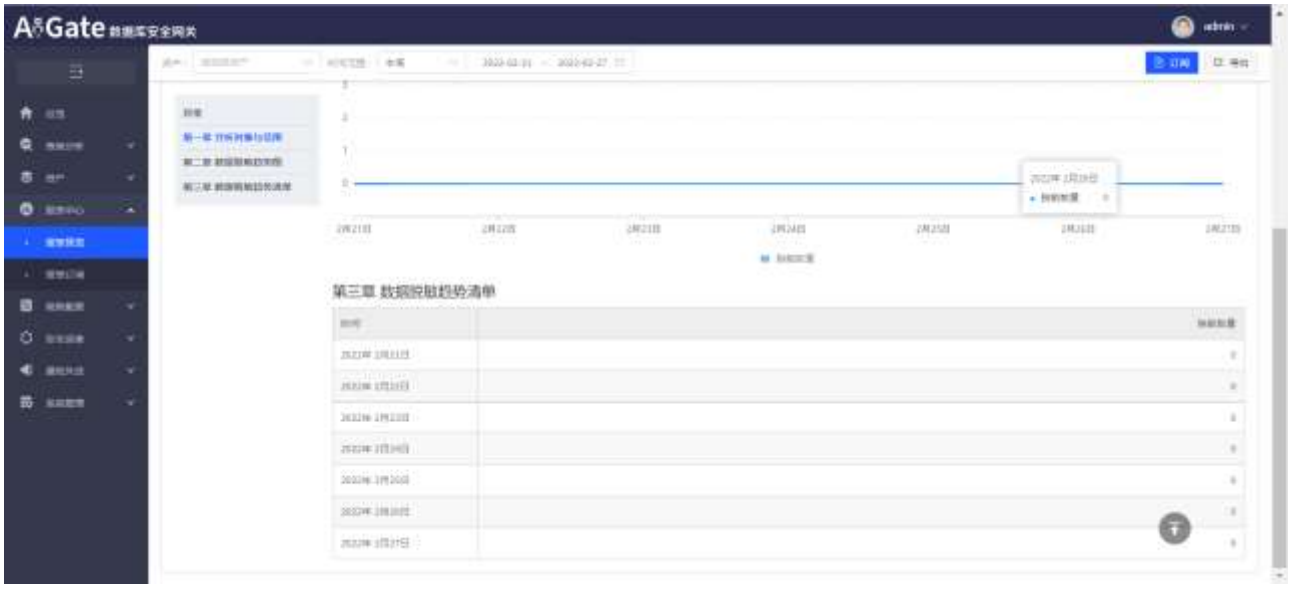
三章。第一章分析对象与范围；第二章最大并发会话化趋势图；第三章 各时段会话数量清单。



5.1.3. 数据脱敏分析

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，点击数据脱敏趋势分析表，分为三章。

第一章分析对象与范围；第二章数据脱敏趋势图；第三章 数据脱敏趋势清单。



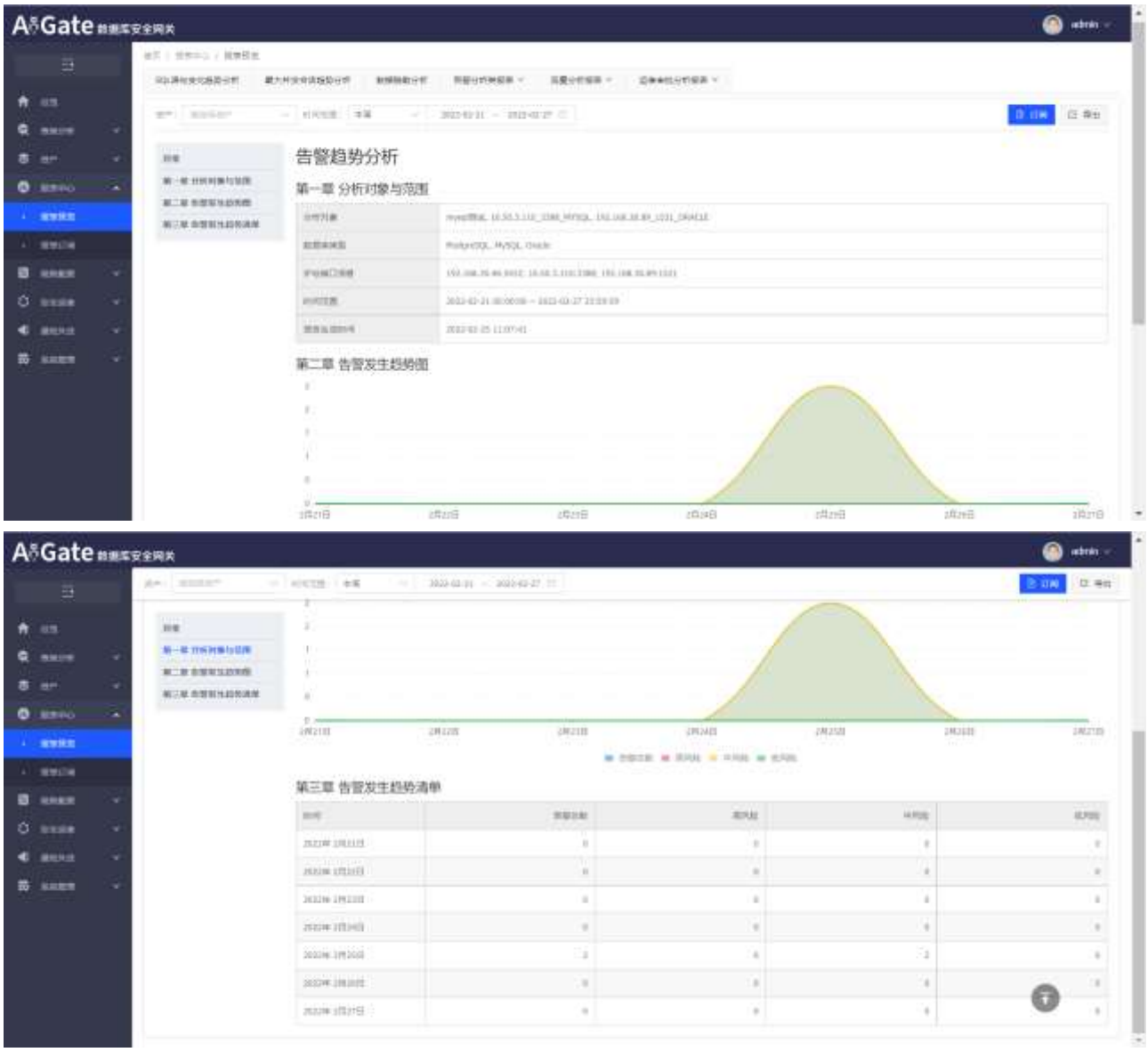
5.1.4. 告警分析类报表

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，点击告警分析类报表，包括告警趋势分析、告警处理动作分析、客户端 IP 分析、客户端工具分析、数据库账号分析、规则命中分析。

特别说明：告警趋势分析、告警处理动作分析、客户端 IP 分析、客户端工具分析、数据库账号分析、规则命中分析，他们的数据是相等的，因此手册中只展示一下告警趋势分析表图

步骤 2：在菜单栏选择“**报表中心➤报表预览**”进入报表预览页面，点击告警分析类报表➤告警趋势分析，

分为三章。第一章分析对象与范围；第二章告警发生趋势图；第三章 告警发生趋势清单



5.1.5. 数据库流量趋势分析

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，点击流量分析报表➤数据库流量趋势分析，分为两章。第一章分析对象与范围；第二章数据库流量趋势图。

5.1.6. 客户端流量趋势分析

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，点击流量分析报表➤客户端流量趋势分析，分为两章。第一章分析对象与范围；第二章客户端工具流量趋势图

5.1.7. 运维审批的 SQL 数量分析

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，点击运维审批分析报表➤运维审批的 SQL 数量分析，分为三章。第一章分析对象与范围；第二章运维审批的 SQL 数量趋势图；第三章运维审批的 SQL 数量清单

第三章 运维审批的SQL数量清单

时间	审批通过的SQL	审批不通过的SQL
2022年 2月21日	0	0
2022年 2月22日	0	0
2022年 2月23日	0	0
2022年 2月24日	0	0
2022年 2月25日	0	0
2022年 2月26日	0	0
2022年 2月27日	0	0

5.1.8. 人员的运维审批任务分析

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，点击运维审批分析报表➤人员的运维审批任务分析，分为两章。第一章分析对象与范围；第二章人员的运维审批任务清单

5.2.导出

导出，顾名思义为导出当前所选择报表的内容，导出格式有 HTML、PDF、Word、PNG 四种。

步骤 1.选择 SQL 语句变化趋势分析、最大并发会话分析、数据脱敏分析、告警分析类报表、流量分析报表、运维审批分析报表其中之一，点击页面右上角的导出按钮，选择一种格式，点击下载

步骤 2.找到下载路径，打开下载的文件

5.3.报表订阅

AiGate 可以订阅报表，以邮件的方式定时发送到邮箱。

步骤 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，点击添加，或直接点击 “**报表中心 报表订阅**” 右上角<**订阅**>按钮添加。

配置项	说明
任务名称	订阅任务的名字
收件人邮箱	正确的邮箱格式
报表类型	HTML、PNG、PDF、Word 四种格式
资产	选择已有的资产
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

6. 查询分析

AiGate 支持从多个维度查看数据库的访问操作记录。可以根据告警日志查看可疑的访问行为；通过脱敏日志查看触发动态脱敏的访问行为；通过会话日志可以查看每一次访问行为的会话信息。

6.1. 查询审计日志

当系统根据配置捕捉到客户端访问时，会记录审计日志。系统支持在审计日志页面查看的所有产生审计的 SQL 语句的信息，并可以根据时间、资产、数据库账号等条件进行筛选。

查询告警日志的操作方法如下：

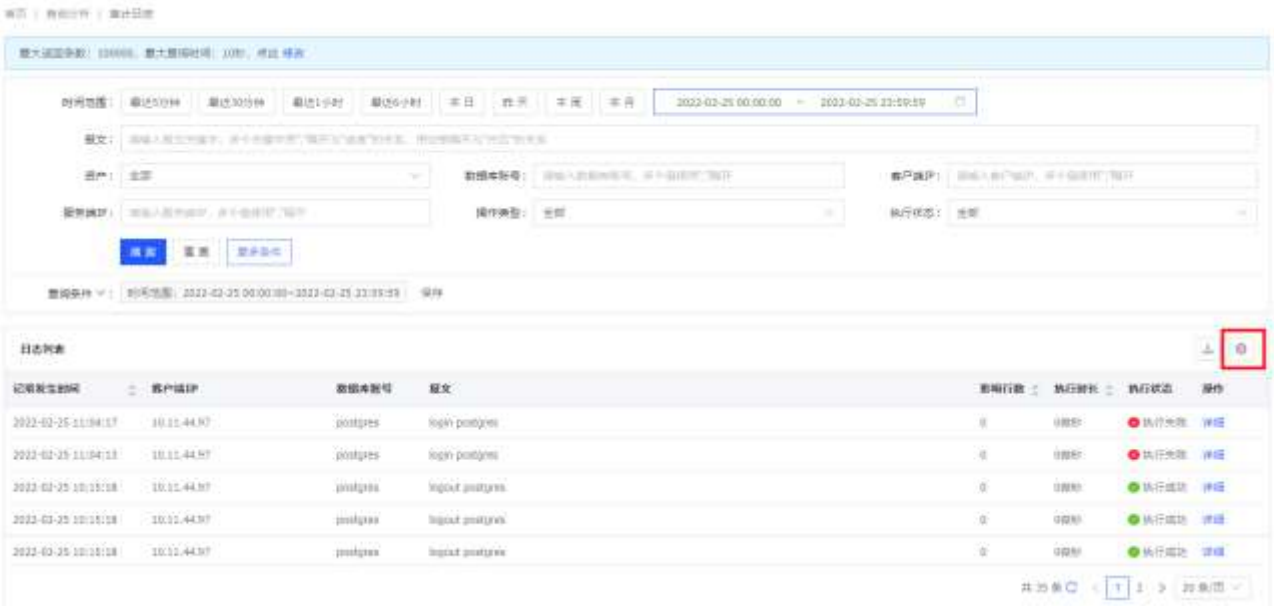
在菜单栏选择“**查询分析➤审计日志**”进入**审计日志**页面，设置查询条件（如时间范围、资产、操作类型等），点击<**搜索**>即可查询相关审计日志。

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”。

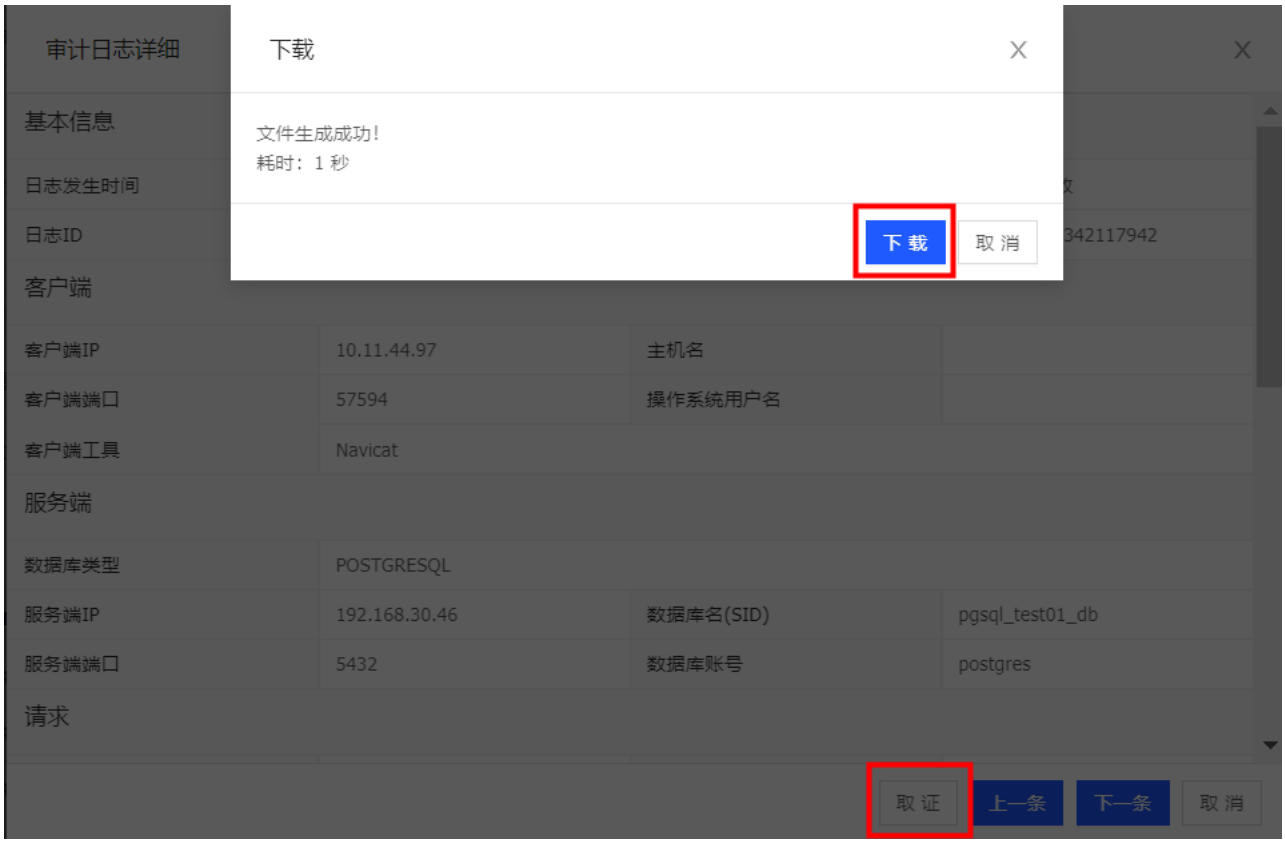
报文	审计到的 SQL 语句，可填多个关键字，用空格隔开，表示同时满足。
审计 ID	日志 ID，唯一标识日志记录的 ID，多个值用“,”隔开。
会话 ID	唯一标识会话记录的 ID。
SQL 模板 ID	标识 SQL 模板的 ID。
资产	可选资产，可选择单个资产，默认为全部资产。
数据库账号	登录到数据库的账号。
客户端 IP	客户端 IP 地址，可填写 IPv4 和 IPv6 地址。
客户端端口	客户端端口号。
服务端 IP	服务端 IP 地址，可填写 IPv4 或 IPv6 地址。
服务端端口	服务端端口号。
数据库名/实例名	数据库名称或者实例名称。
客户端工具	客户端工具名称。
主机名	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	审计到的数据库操作的类型。
数据库类型	系统支持审计的数据库类型。
执行状态	默认为全部，可选择执行成功、执行失败、未知。

查询结果显示在查询条件的下方。点击右方 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。



在审计日志列表中，点击右侧**操作**列中的<**详细**>可以查看该审计记录的详细信息，包括审计记录基本信息、客户端信息、服务端信息、请求详情、返回详情。

在日志详细中，点击<**取证**>即可取证，点击<**下载**>可下载取证日志。



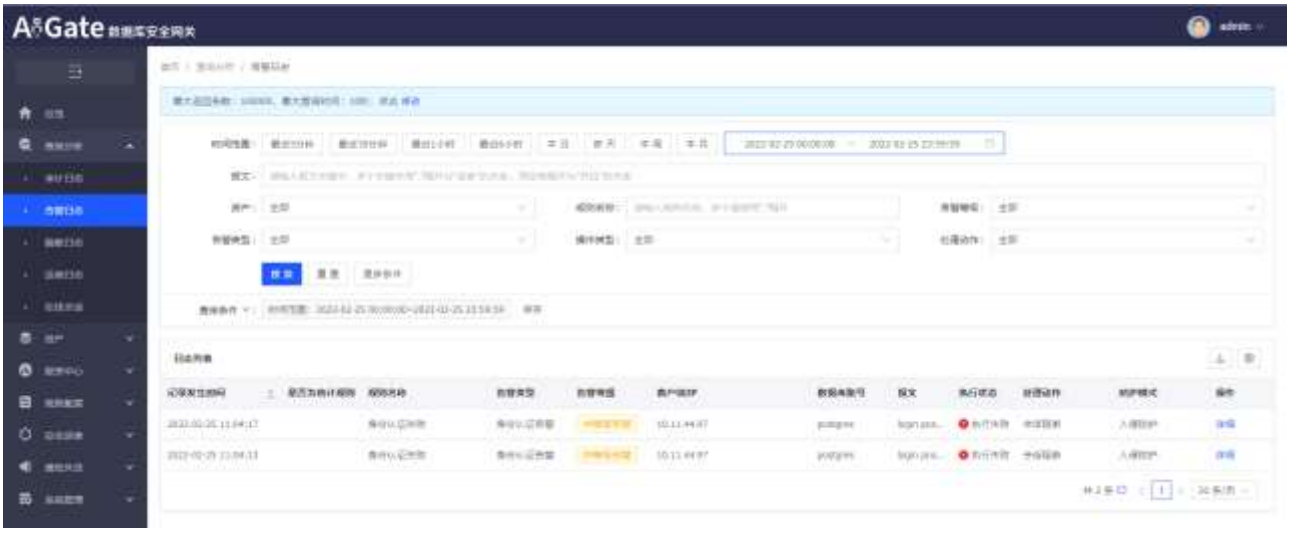
点击 按钮，即可下载审计日志，最多支持 10 万条

6.2. 查询告警日志

当系统根据安全规则捕捉到异常访问时，会根据匹配的安全规则的级别产生相应级别的告警信息。系统支持在告警日志页面查看的所有产生告警的 SQL 语句的信息和告警等级等相关内容，并可以根据时间、字段和告警等级、规则名称等条件进行筛选。

查询告警日志的操作方法如下：

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。



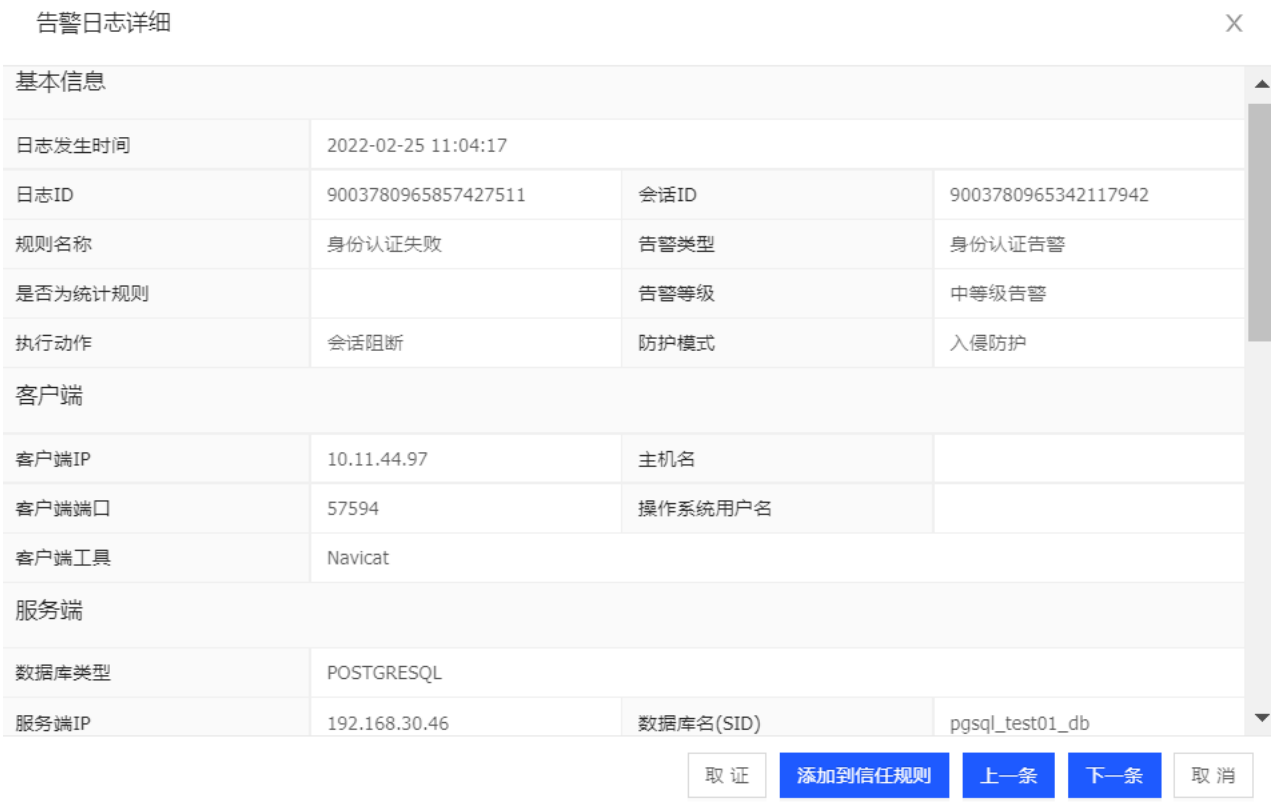
各查询条件的说明如下。

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”。
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。
告警 ID	唯一标识告警记录的 ID。
会话 ID	唯一标识会话记录的 ID。
SQL 模板 ID	标识 SQL 模板的 ID。
资产	可选资产，可选择单个资产，默认为全部资产。
规则名称	系统里配置的安全规则的名称。

告警等级	告警等级可选高风险、中风险或低风险。
数据库账号	登录到数据库的账号。
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/实例名	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。
告警类型	可选身份认证告警、安全规则告警等。
操作类型	审计到的数据库操作的类型。
数据库类型	系统支持审计的数据库类型。
执行状态	默认为全部，可选择执行成功、执行失败、未知。
处理动作	可选允许访问、命令阻断或会话阻断。

查询结果显示在查询条件的下方。点击 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。

在告警日志列表中，点击右侧**操作**列中的<**详细**>可以查看该告警记录的详细信息，包括告警记录基本信息、客户端信息、服务端信息、请求详情、返回详情。

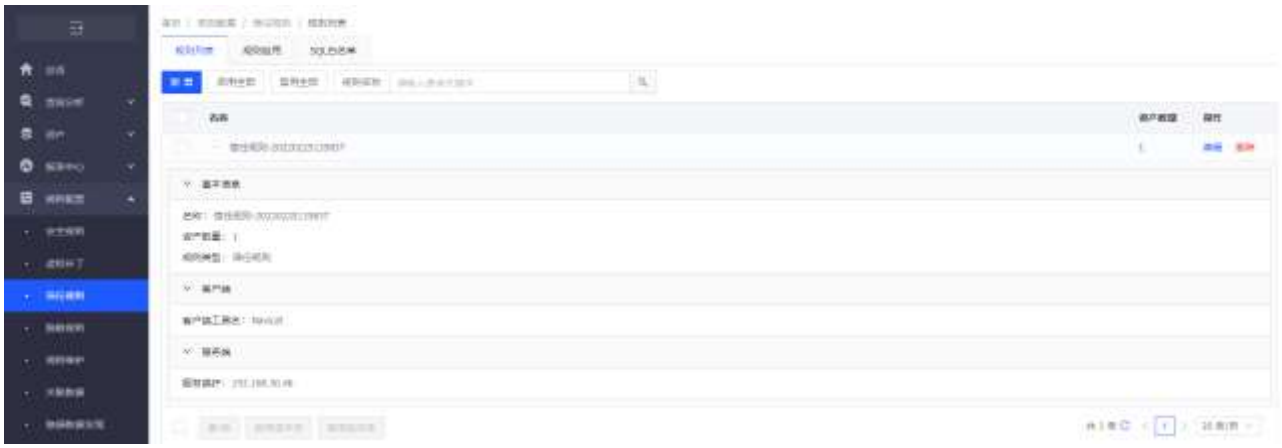


根据告警日志里的信息，可以选择客户端工具、服务端 IP、服务端端口号、数据库账号、客户端 IP、客户端端口号、SQL 模板 ID、操作类型这些属性生成一条新的信任规则。

添加信任规则的操作方法如下：

步骤 1. 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. 选中需要的属性后，点击<**确定**>按钮，会提示操作成功信息。进入<**规则配置　信任规则**>查看生成的信任规则。

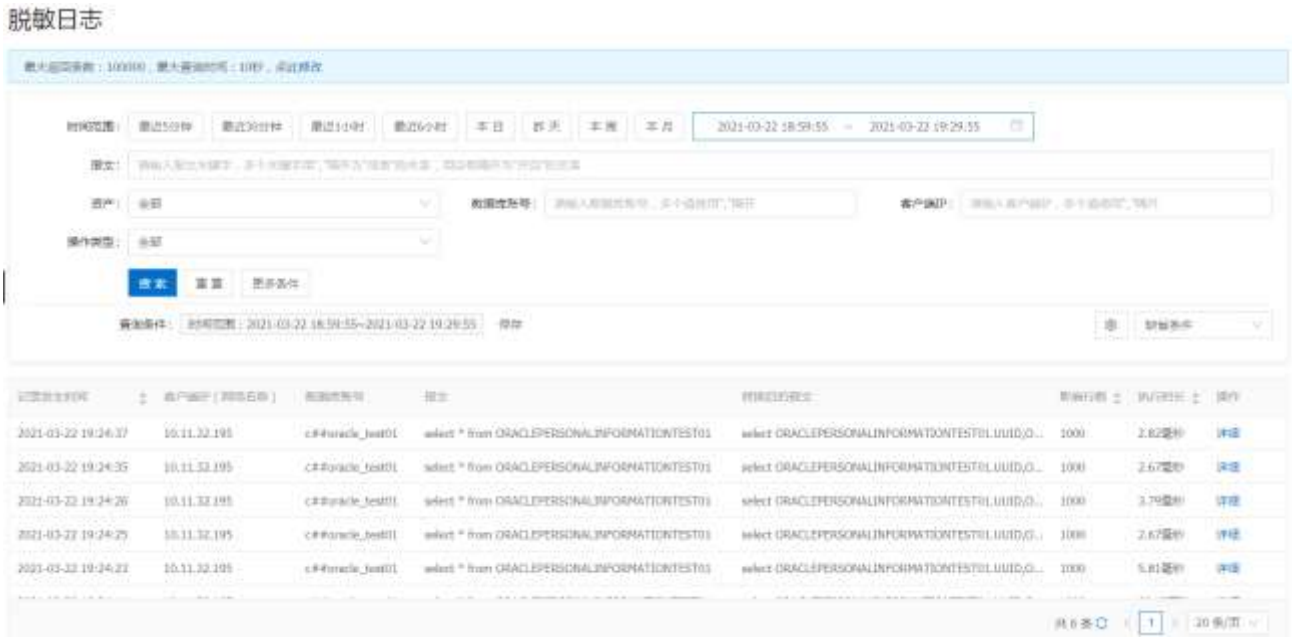


6.3. 查询脱敏日志

AiGate 数据安全网关内置了替换、截断、取整、掩码等常见的脱敏方法，对在实现数据模糊化处理。系统支持在脱敏日志页面查看的触发动态脱敏动作的 SQL 语句的信息和脱敏结果等相关内容，并可以根据时间、资产、数据库账号和客户端 IP 等条件进行筛选。

查询脱敏日志的操作方法如下：

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。

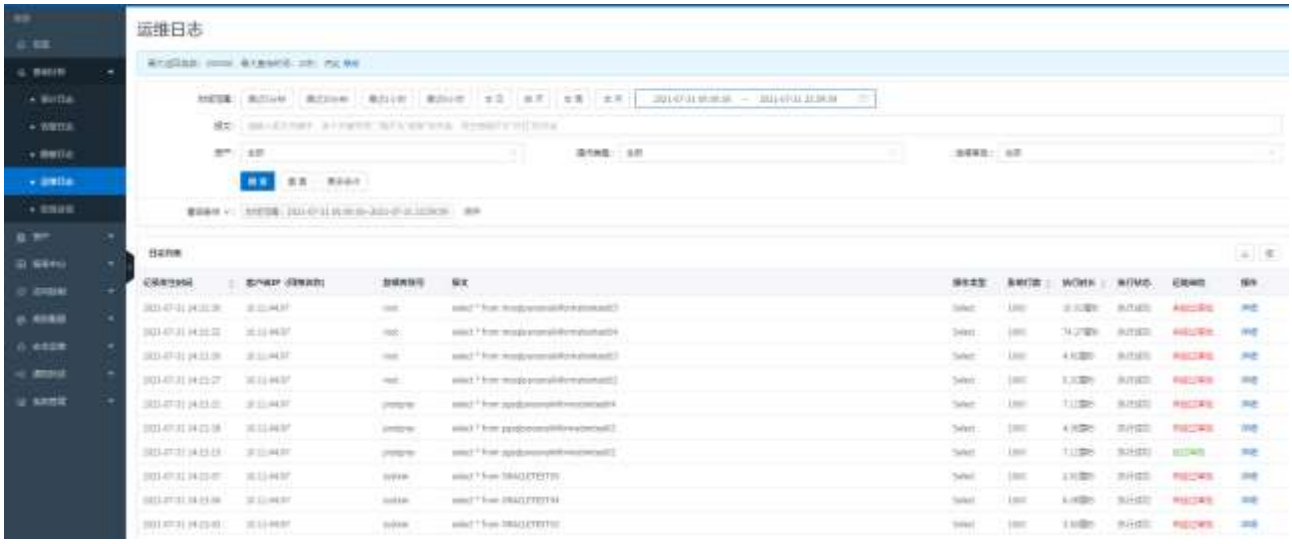


点击<**更多条件**>弹出**更多条件**对话框，勾选查询条件，点击<**确定**>添加相应查询条件，点击<**恢复默认**>可恢复至默认查询条件。

6.4. 查询运维审批日志

AiGate 数据安全网关可对客户端执行的 SQL 进行运维审批，在运维任务中的库表或者运维 SQL 才允许客户端执行，客户端执行不在运维任务中的 SQL，直接阻断（入侵检测模式下，可执行，日志显示为未经过审批）。系统支持在运维审批日志页面查看的触发运维审批动作的 SQL 语句的信息和运维审批结果等相关内容，并可以根据时间、资产、数据库账号和客户端 IP 等条件进行筛选。

在菜单栏选择“**查询分析➤运维审批日志**”进入**运维审批日志**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**>即可查询相关运维审批日志。



点击<**更多条件**>弹出**更多条件**对话框，勾选查询条件，点击<**确定**>添加相应查询条件，点击<**恢复默认**>可恢复至默认查询条件。

6.5. 查询在线会话

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。

可以根据会话的状态将其分成在线会话和历史会话。

- 在线会话是根据会话的状态区分，指的是会话还没有结束，仍然有后续的请求或响应。
- 历史会话指的是已经结束的会话，会话双方已经断开了本次会话的连接。

会话的基本四元素是指客户端 IP、客户端端口、服务端 IP 和服务端端口。会话的四元素可以定位在同时刻的唯一会话信息。系统支持查看在线会话，并支持通过会话信息查看一次会话过程中产生的所有请求或响应日志。

在**会话日志**页面，设置查询条件（如客户端 IP 等），点击<**搜索**>即可查询相关在线会话。

7. 规则配置

规则配置是指根据一些特征（如客户端、服务端、SQL 语句）定义危险行为（安全规则），及可以信任的行为（过滤规则）。当系统检测到对数据库的操作匹配安全规则时会触发告警。

系统匹配规则的顺序为：1）信任规则；2）虚拟补丁；3）安全规则。

7.1. 安全规则

安全规则库用来保存已发现的不安全 SQL 语句的特征信息。系统通过将检测到的 SQL 语句和安全规则进行匹配从而判断 SQL 语句中是否包含可疑行为。

根据不安全 SQL 的特征，安全规则分成 SQL 注入攻击规则、漏洞攻击规则、账号安全规则、数据泄露规则和违规操作规则。

- SQL 注入攻击是一种将 SQL 代码插入或添加到应用（用户）的输入参数中的攻击，之后再将这些参数传递给后台的数据库服务器加以解析并执行，SQL 注入规则可以有效的发现此类攻击行为并产生告警。
- 漏洞攻击规则是根据已知的 SQL 漏洞信息而制定的，漏洞安全规则按照不同的漏洞类型可以分成缓冲区溢出和存储过程滥用。
- 账号安全规则是针对对数据库服务器进行暴力破解和登录失败场景下的安全规则。
- 数据泄露规则根据泄露场景分成拖库攻击、数据库外联、大流量返回、非授权访问，系统可以有效地发现这几种泄露场景并及时通知告警。
- 违规操作规则是针对于运维人员的违规操作、数据库探测和异常语句场景。

系统内置了安全规则，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。

7.1.1. 规则管理

内置规则组不可更改，用户可以管理自定义的规则组、内置规则不可更改，用户可以管理自定义的规则。

内置规则不可以被移动，自定义的规则可以移动到内置规则组里。

内置规则不可以被删除，自定义规则未绑定资产时可以被删除。

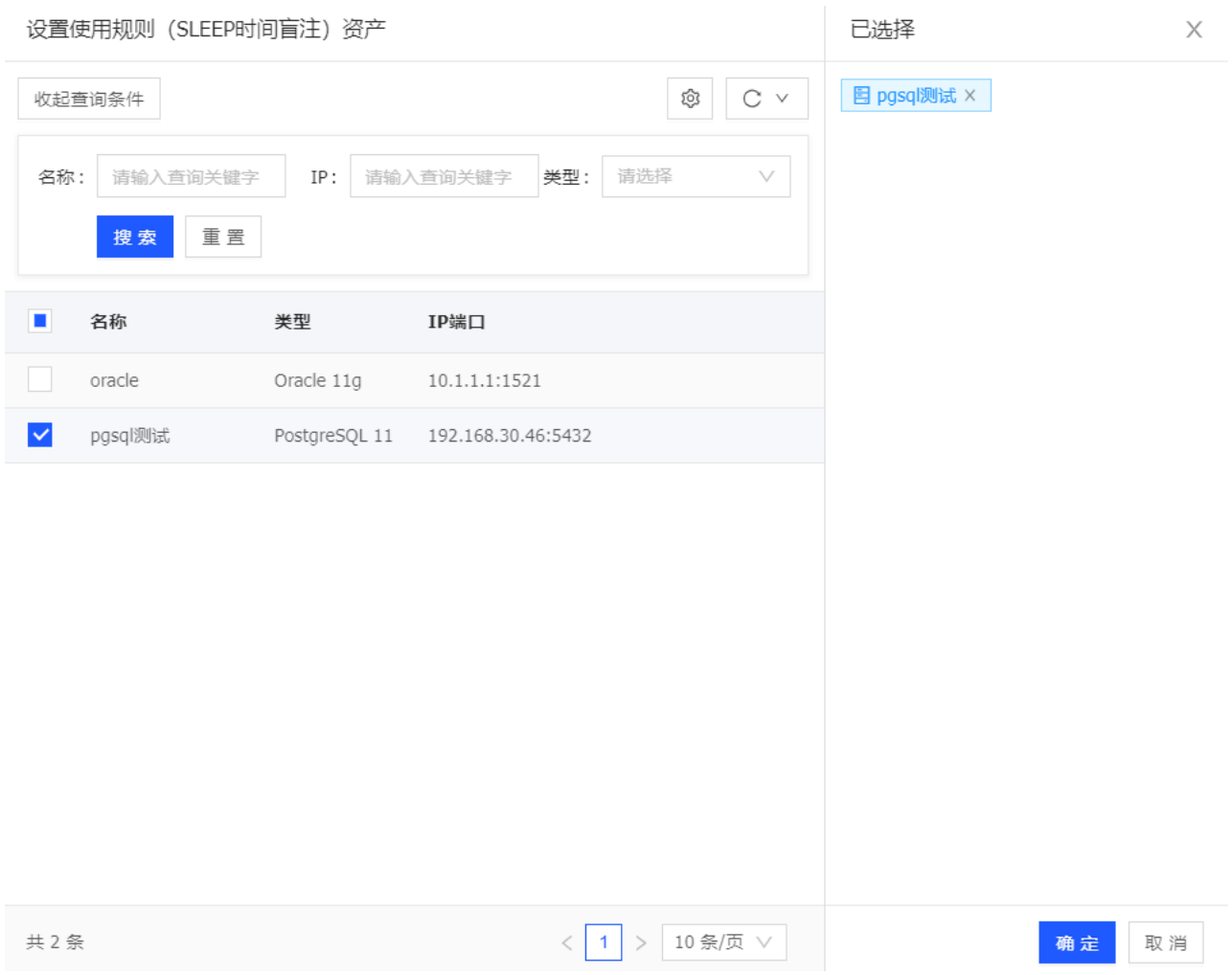
绑定了资产的自定义规则不可以被移动到其他类型的内置规则组里。

可以把规则关联到具体的资产，操作如下：

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，选择**规则管理**页签进入规则管理页面。

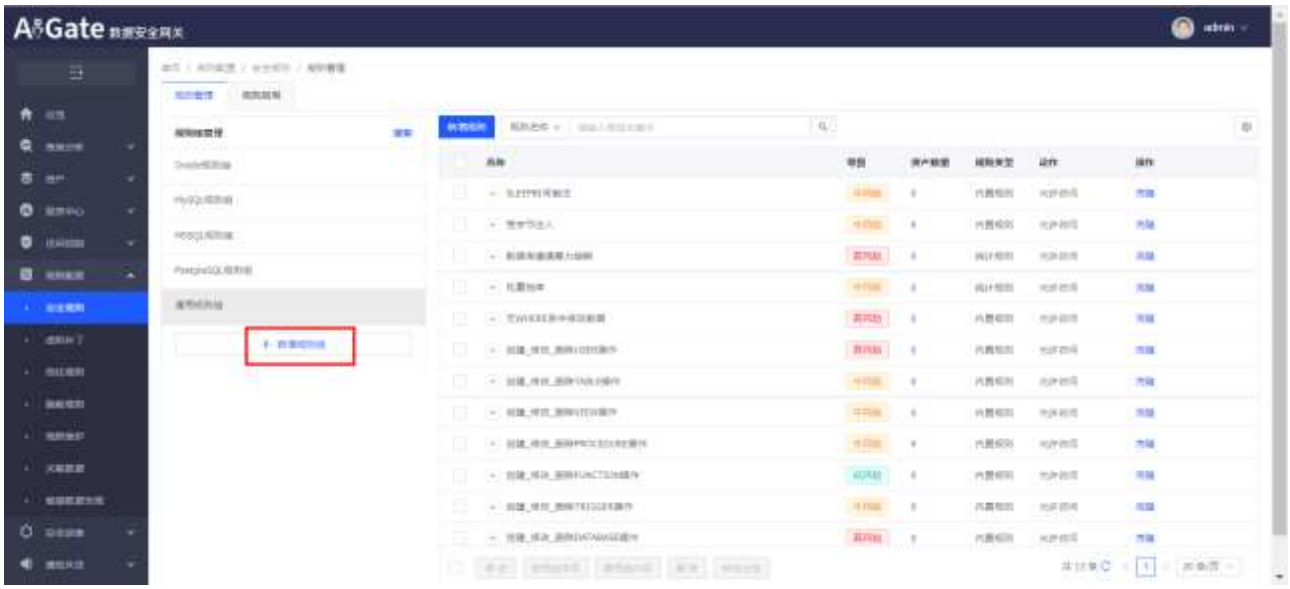
步骤 2. 选择对应的规则组后，点击规则后方资产数量下的数字。

步骤 3. 选中需要挂载的资产后，点击<**确定**>按钮。



新增自定义安全规则组的操作方法如下：

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，选择**规则管理**页签进入规则管理页面。



步骤 2. 编辑相关信息完成以后，点击<**保存**>。

新增自定义安全规则的操作方法如下：

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，选择**规则管理**页签进入规则管理页面。

步骤2. 选中需要新增规则的规则组，点击<**新增**>，编辑相关信息完成以后，点击<**保存**>。


编辑规则
基本信息
* 名称：
zjl的安全规则
描述：
等级：
高风险
中风险
低风险
上级目录：
缺省规则组
动作：
允许访问
命令阻断
会话阻断
规则类型：
普通规则
统计规则
客户端
客户端来源：
IP
IP组
等于
10.11.44.97
可配多个IP，使用逗号","分隔，例：192.168.1.2,192.168.1.3
客户端端口：
可配置多个值或区间，多个值间以逗号","分隔，例：10-15,20,25,30-40
客户端工具名：
字符串
正则表达式
分组选择
等于
可配多个客户端工具名，使用逗号","分隔，例：db2bp.exe,javaw.exe,plsqldev.exe
操作系统用户名：
字符串
正则表达式
分组选择
等于
可填多值，多个值间以逗号","分隔，例：xxx,yyy
客户端主机名：
字符串
正则表达式
分组选择
等于

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。
	描述	规则描述，长度不超过 1000 字符。
	等级	必选项，系统默认等级为高风险。等级包括高风险、中风险和低风险。
	适用场景	默认为缺省场景，可根据场景进行选择。
	规则类型	普通规则和统计规则，选择统计规则，则开启防撞库脱库功能。
	统计时长	默认 10s，最长 30 分钟（统计规则选项）
	累计次数	默认 2 次，最大 30 次，在统计时长内，触发设置次数，则会触发撞库（登录）或者脱库（执行 SQL）功能，自动创建安全规则。（统计规则选项）
	累积条件	可以选择同一会话、同一客户端 IP、同意数据库账号和同一客户端工具。（统计规则选项）
	动作	规则动作支持允许访问、命令阻断、会话阻断和动态脱敏。
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。
	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。 可配多个客户端工具，使用逗号“,”分隔，例如：db2bp.exe,java.exe。

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。
	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。 可填多值，多个值间以逗号“,”分隔。
	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。 可填多值，多个值间以逗号“,”分隔。
服务端	数据库账号	指定规则所匹配的数据库登录用户账号或账号组，可填多值，多个值之间以“,”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）	Oracle 数据库输入 SID，其他数据库输入数据库名，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。有关对象组的更多信息，请参考对象组管理。
	操作类型	指关注的操作类型，如 select、update、delete 等。可根据 DDL\DML\DCL 来选择。
	SQL 模板 ID	可填项，可填多值，多个值间以逗号“,”分隔。

项目	配置项	说明
	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**>输入报文内容，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<**增加条件**>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	可填项，单位：微秒，取值范围：0~2,147,483,647，SQL 执行时长属于此范围，则触发规则。
	影响行数	取值范围：0~2,147,483,647 之间的任意范围。SQL 操作返回的记录数或受影响的行数属于此范围，则触发规则。

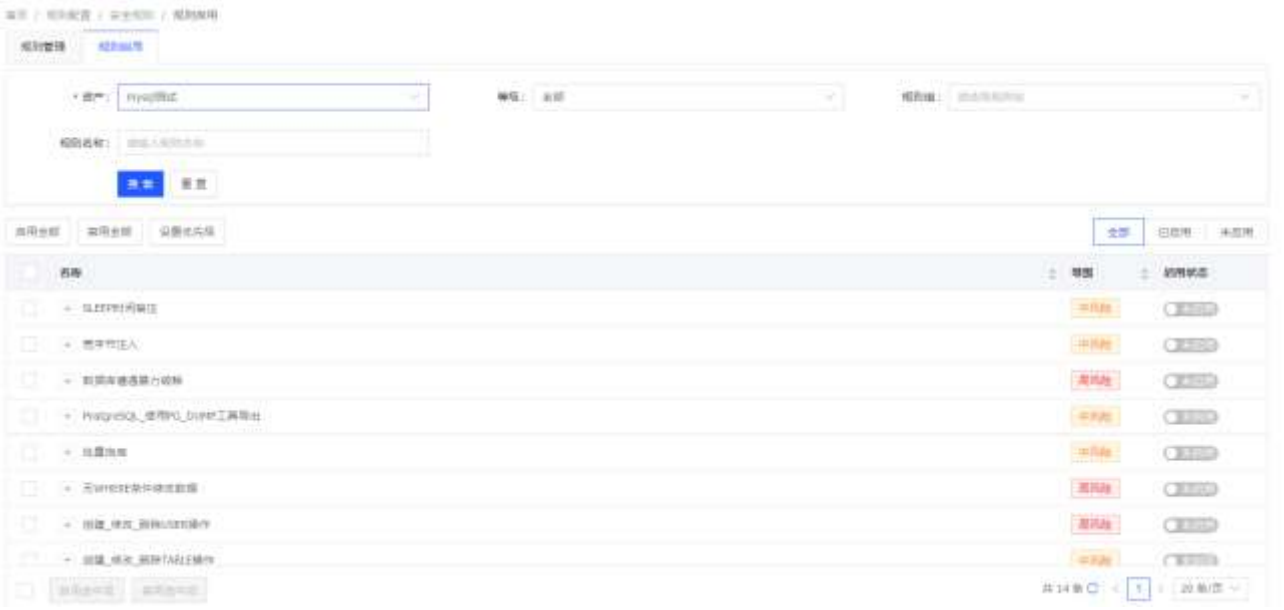
项目	配置项	说明
	返回结果集	支持以正则表达式方式匹配结果集。单击<**正则验证**>输入结果集内容，单击<**提交**>，验证输入内容与返回结果关键字的正则表达式是否匹配。可通过<**添加条件**>添加多个条件。 条件运算逻辑表达式：条件间的关系，支持“与、或、非、括号”运算(&：与；|：或；~：非)，条件使用序号表示，即“1”表示条件 1，例如：1&2，则代表有 2 个结果集条件，且结果集中需要同时满足这两个条件才能告警。
	执行状态	包含三个执行状态：全部、成功、失败。
	执行结果描述	支持以正则表达式方式匹配。
其它	生效时间	可自定义或者选择时间组。有关时间组配置的更多信息，请参考时间组管理。

7.1.2. 规则启用

规则启用后，即关联到对应的资产。

在菜单栏选择“**规则配置➤安全规则**”进入**安全规则**页面，选择**规则启用**页签进入规则管理页面。

如下图所示。

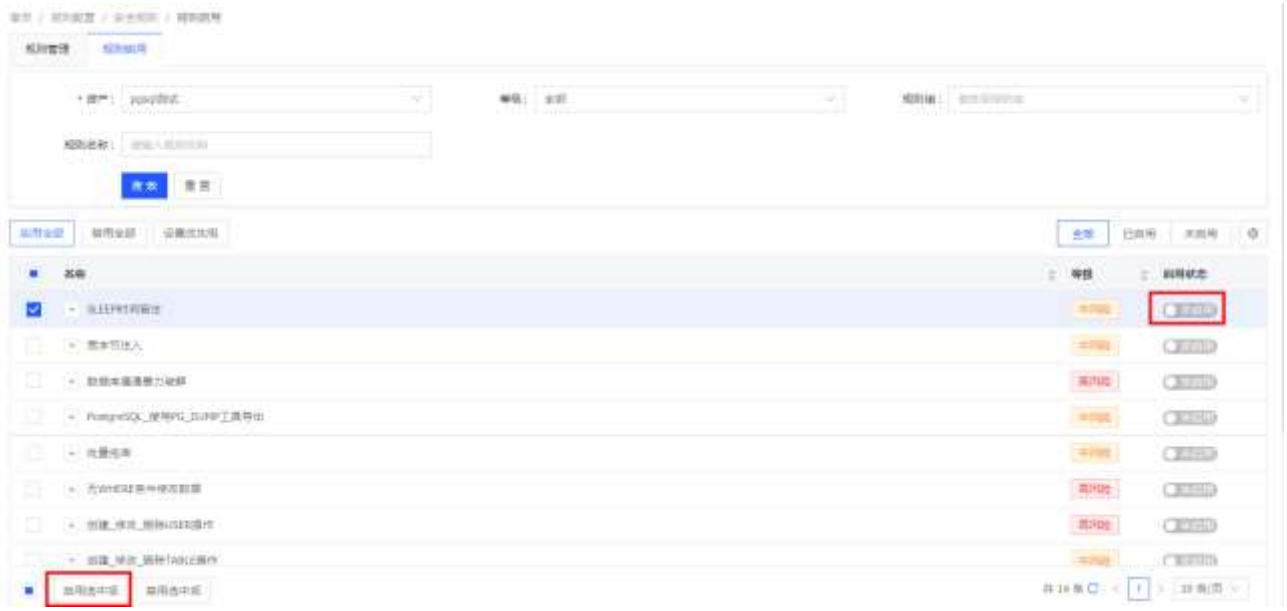


可以根据资产、等级、规则组、规则名称进行组合查询。默认搜索条件为最新创建的资产。

- 启用规则

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，选择**规则启用**页签进入规则管理页面。

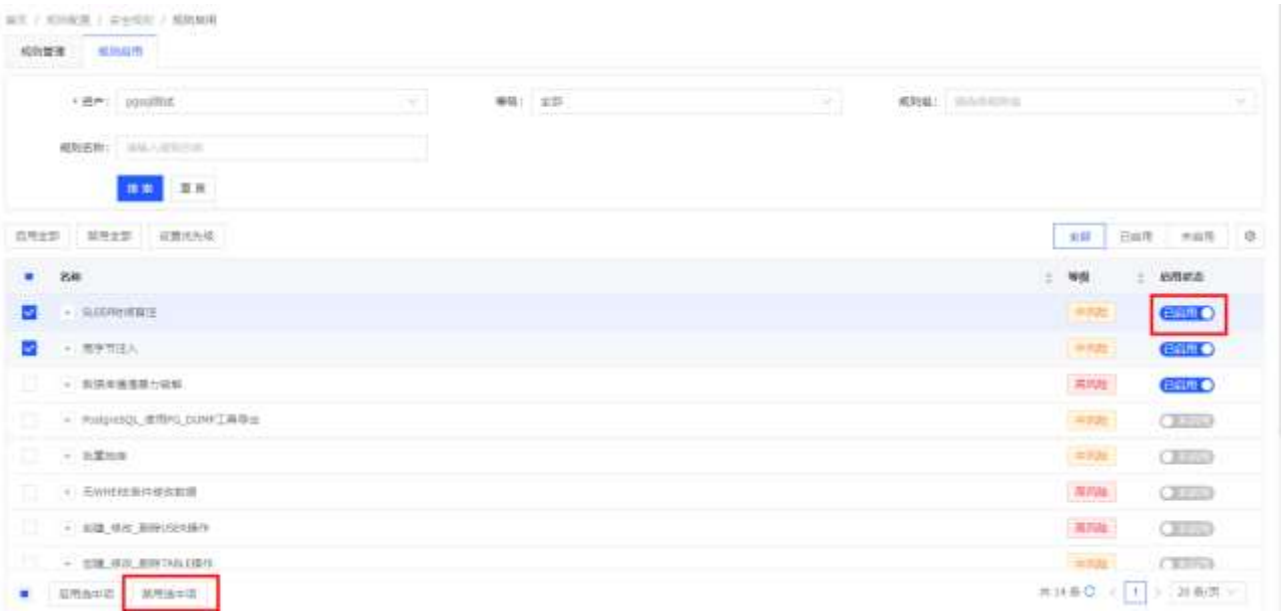
步骤2. 根据筛选条件筛选后，在规则列表中勾选目标规则，然后点击<**启用选中项**>，或直接点击规则后方启用状态下的滑块。



- 启用规则

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，选择**规则启用**页签进入规则管理页面。

步骤2. 根据筛选条件筛选后，在规则列表中勾选目标规则，然后点击<**禁用选中项**>，或直接点击已启用的规则后方启用状态下的滑块。



◆ 启用全部或禁用全部

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，选择**规则启用**页签进入规则管理页面。

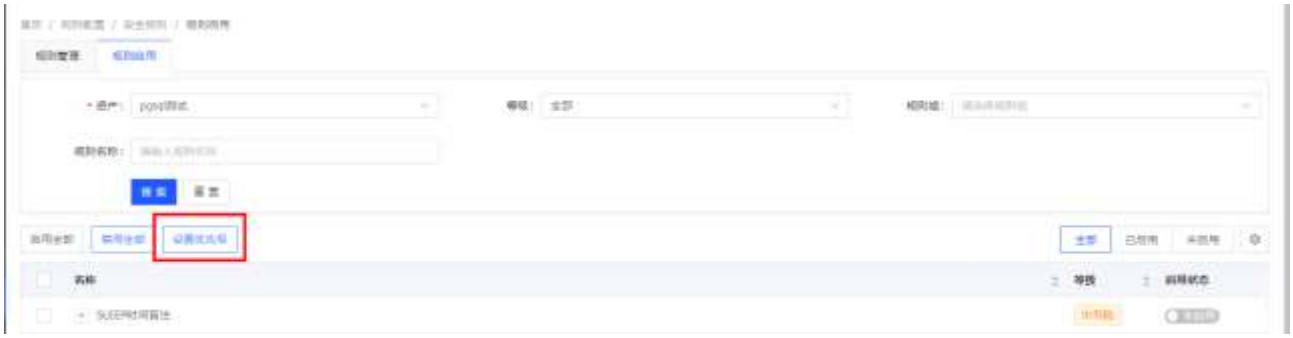
步骤 2. 根据筛选条件筛选后，在规则列表中点击<**禁用全部**>，或<**启用全部**>按钮。

◆ 设置优先级

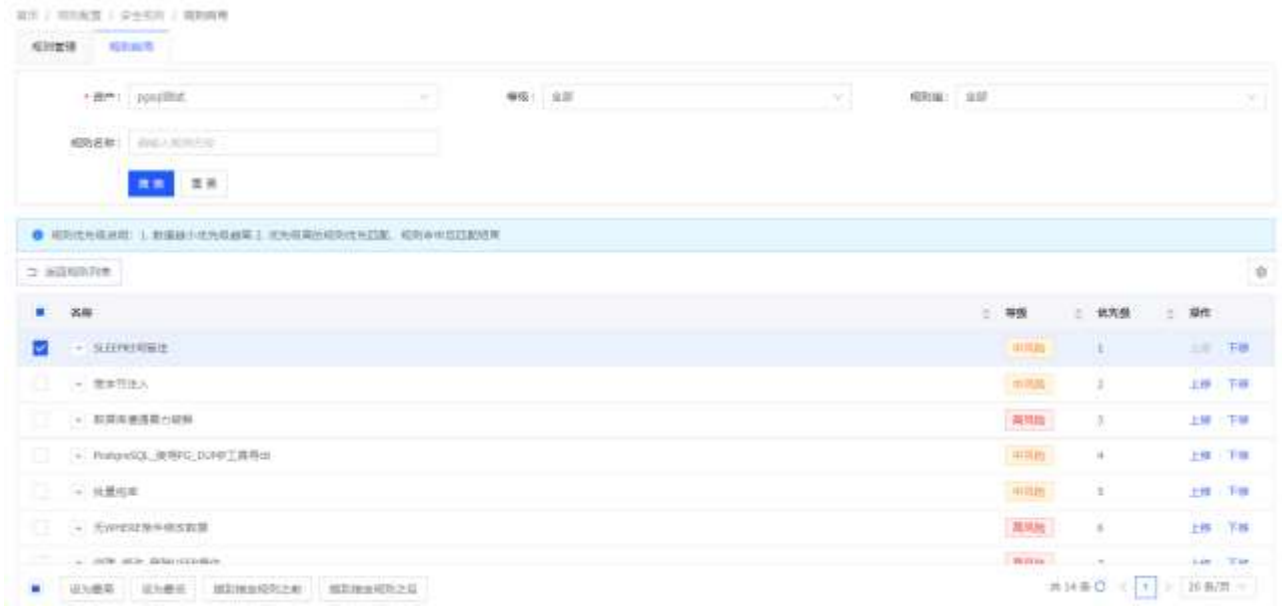
只有开启状态的规则才会出现在优先级列表内。

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，选择**规则启用**页签进入规则管理页面。

步骤 2. 根据筛选条件筛选后，点击<**设置优先级**>按钮。



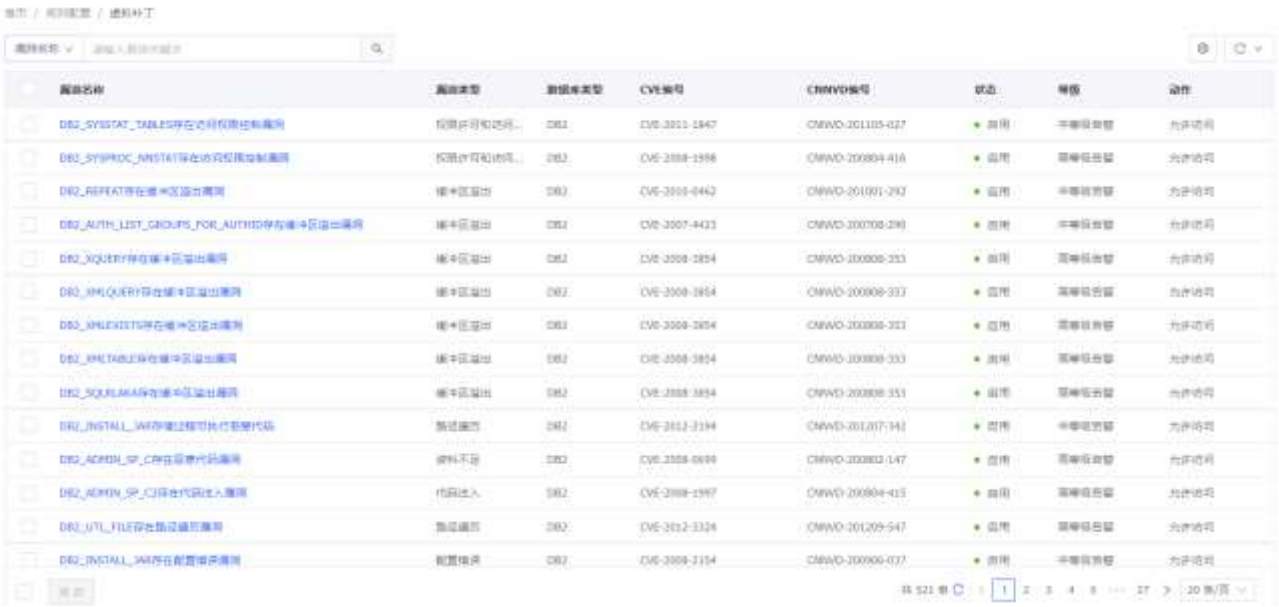
步骤 3. 点击规则后方的<上移>、<下移>按钮，可以修改规则的优先级；选中规则的多选框，可以将此规则的优先级设为最高或最低；选中规则的多选框，可以将此规则的优先级插到指定规则之前或之后。



7.2. 虚拟补丁

AiGate 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

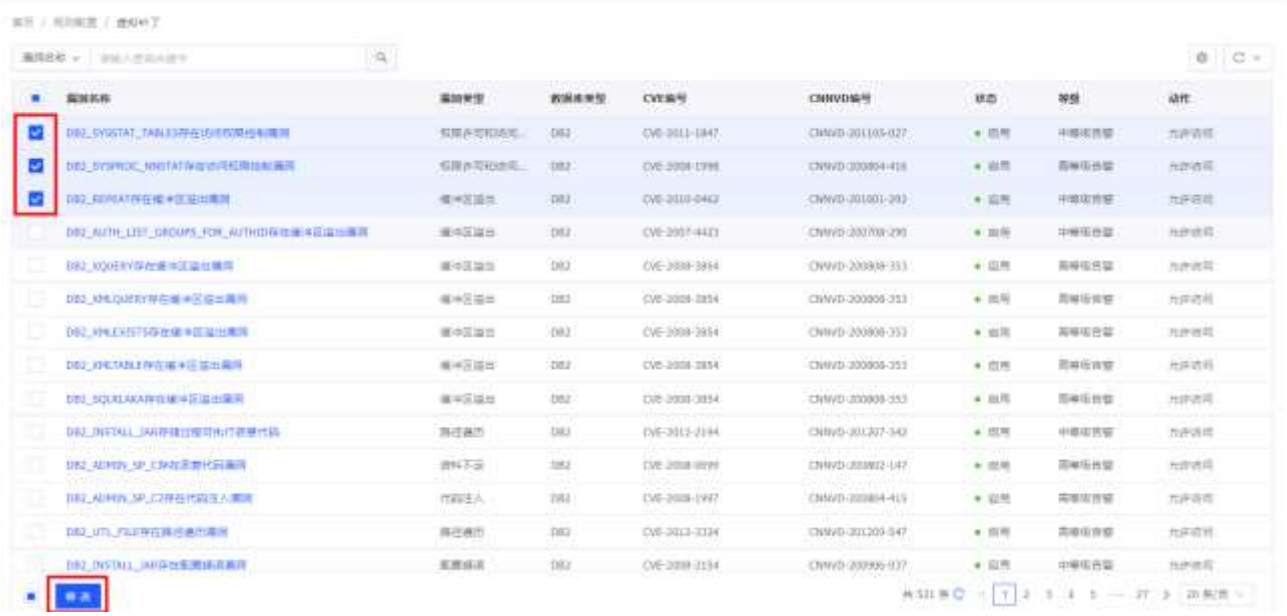
库的安全漏洞起到一定的的防御作用，极大的保护了未升级漏洞补丁的数据库服务器，有效降低了用户数据篡改和泄露的可能。



修改虚拟补丁规则的操作方法如下：

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，进入虚拟补丁管理页面。

步骤2. 在虚拟补丁列表中勾选目标虚拟补丁规则，然后点击<**修改**>。



步骤3. 在修改规则页面，编辑相关信息完成以后，点击<**保存**>。

7.3. 信任规则

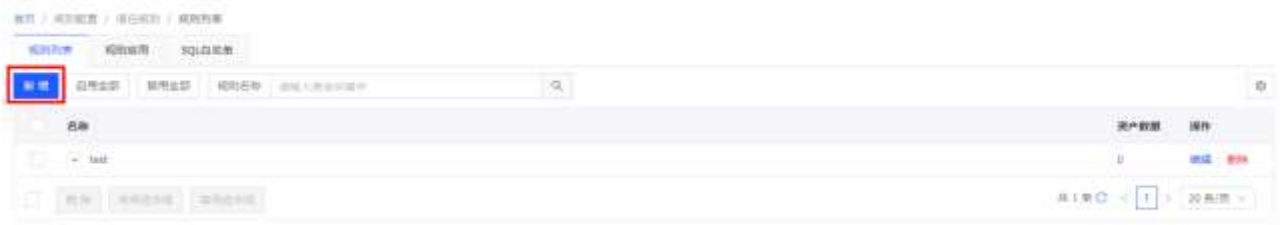
当系统匹配信任规则时，不产生告警信息。

8.3.1 规则列表

可以新增规则、启用全部规则、禁用全部规则、批量启用规则、批量禁用规则、搜索对应规则、编辑对应规则、删除对应规则、关联到对应资产（同安全规则）。

新增信任规则的操作方法如下：

步骤 1. 在菜单栏中选择“**规则设置➤信任规则**”进入**信任规则**页面。选择**规则列表**页签进入规则列表页面。



步骤 2. 点击<**新增**>弹出**新增规则**对话框，编辑相关信息，点击<**保存**>。

详细配置请参见规则管理。

8.3.2 规则启用

可以启用全部规则、禁用全部规则、批量启用规则、批量禁用规则；

可以根据资产、规则名称、状态搜索对应规则。

8.3.3 SQL 白名单

可以对具体的 SQL 语句进行加白；可以对具体的数据库操作类型进行加白；可以对 SQL 模板进行加白。

可以启用/禁用全部白名单、批量启用/批量禁用白名单；可以根据关键字、状态、类型搜索白名单。

可以导入 SQL 文件、新增或删除 SQL 白名单。

新增白名单操作如下：

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

步骤 2. 点击<**添加**>弹出**新增 SQL 白名单**框，编辑相关信息，点击<**保存**>。

7.4. 脱敏规则

AiGate 内置了替换、截断、取整、掩码等常见的脱敏规则算法，实现敏感数据的模糊化后。系统考虑了各种场景下的脱敏需求，减少用户根据实际需求编写自定义算法的过程，用户也可以根据内置脱敏算法进行自定义添加脱敏规则。

新增脱敏规则的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤脱敏规则**”进入**脱敏规则**页面，选择**脱敏规则管理**页签进入规则管理页面。

步骤2. 点击<**新增**>，编辑相关信息完成以后，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 字符。
状态	启用或禁用该规则。
脱敏算法	实现数据模糊化的算法。
开始位置	开始替换的字符位置。
长度	数据串中被替换的字符长度。
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，达到预期效果
数据对比	点击预览后，生成的结果

7.5. 规则维护

规则维护包括升级内置安全规则和。

在菜单栏中选择“**规则设置➤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。

7.6. 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。

7.6.1. 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。IP 组管理页面提供增加、导入、编辑、删除和查询功能，如下图所示。

7.6.1.1.新增 IP 组

步骤1. 在菜单栏选择“**规则配置➤分组管理**” 进入**分组管理**页面，选择 **IP 组**页签，点击<**新增**>。

步骤2. 在**新增 IP 组**页面，编辑名称和 IP，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	◆ 可输入多个 IP 地址，用英文逗号隔开。 ◆ 可输入地址范围，例如：10.1.1.10-10.1.1.20。 ◆ 可输入地址段，例如：10.10.*.*，“*”表示 0~255。

7.6.1.2.导入 IP 组

通过批量导入 IP 组的方法可以提高创建 IP 组的效率，操作方法如下：

步骤1. 点击<**下载模板**>，下载模板文件至本地。

步骤2. 编辑模板文件，并保存。

步骤3. 点击<**导入**>，在弹出的对话框中选择编辑好的模板文件，导入文件成功后页面会弹出提示信息，并将模板文件中的 IP 组添加至 IP 组列表中。

7.6.2. 操作系统用户名组管理

操作系统用户名组管理是为方便用户管理特定操作系统用户名的集合。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，可将这些操作系统用户名加入操作系统用户名组，在自定义规则时选择该操作系统用户名组即可。

操作系统用户名组管理页面提供增加、编辑、删除和查询功能，如下图所示。

新增操作系统用户名组的操作方法如下：

步骤1. 在菜单栏选择 "**规则配置➤分组管理**" 进入**分组管理**页面，选择**操作系统用户名组**页签，点击<**新增**>。

步骤1. 进入**新增操作系统用户名**页面，编辑名称和操作系统用户名，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。
操作系统用户名	可输入多项，用英文逗号隔开；也可输入正则表达式。

7.6.3. 客户端主机名组管理

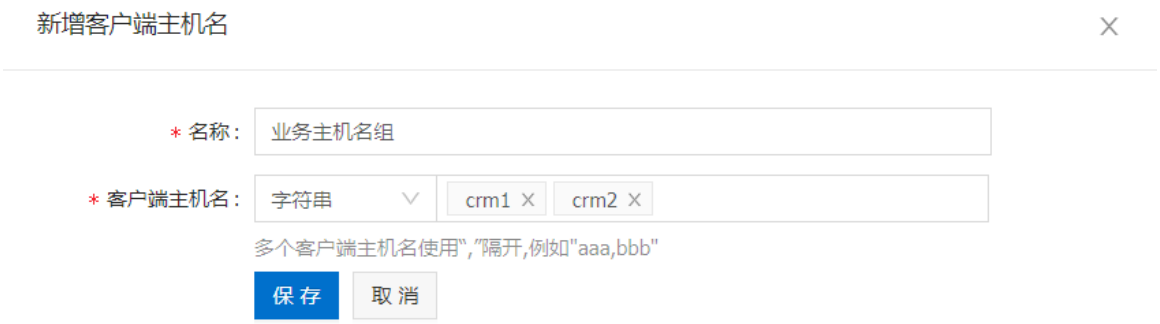
客户端主机名组管理是为方便用户管理特定客户端主机名的集合。如自定义某规则需要在某固定客户端主机名集合内有效时，可将这些客户端主机名加入客户端主机名组，在自定义规则时选择该客户端主机名组即可。

客户端主机名组管理页面提供增加、编辑、删除和查询功能，如下图所示。

新增客户端主机名组的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤分组管理**”进入**分组管理**页面，选择**客户端主机名组**页签，点击<**新增**>。

步骤2. 进入**新增客户端主机名**页面，编辑名称和客户端主机名，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。
客户端主机名	可输入多项，用英文逗号隔开；也可输入正则表达式。

7.6.4. 客户端工具名组管理

客户端工具名组管理是为方便用户管理特定客户端工具名的集合。如自定义某规则需要在某固定客户端工具名集合内有效时，可将这些客户端工具名加入客户端工具名组，在自定义规则时选择该客户端工具名组即可。

客户端工具名组管理页面提供增加、编辑、删除和查询功能，如下图所示。

新增客户端工具名组的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤分组管理**”进入**分组管理**页面，选择**客户端工具名组**页签，点击<**新增**>。

步骤2. 进入**新增客户端工具名**页面，编辑名称和客户端工具名，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。
客户端工具名	可输入多项，用英文逗号隔开；也可输入正则表达式。

7.6.5. 数据库账号组管理

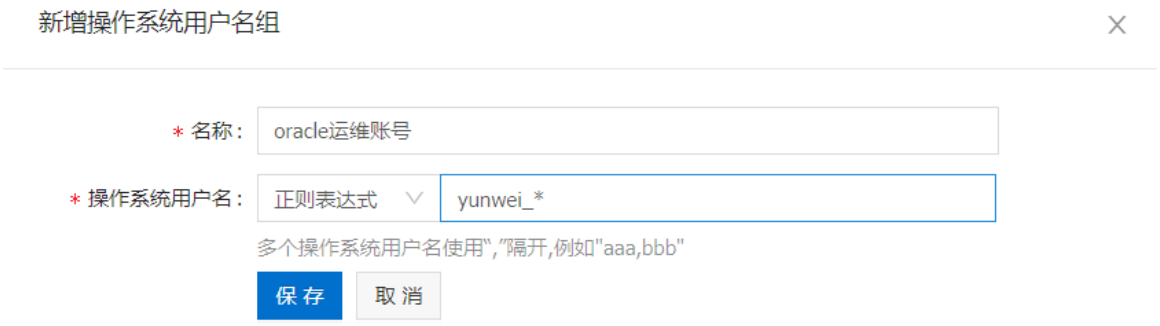
数据库账号组管理是为方便用户管理特定数据库账号的集合。如自定义某规则需要在某固定数据库账号集合内有效时，可将这些数据库账号加入数据库账号组，在自定义规则时选择该数据库账号组即可。

数据库账号组管理页面提供增加、编辑、删除和查询功能，如下图所示。

新增数据库账号组的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤分组管理**”进入**分组管理**页面，选择**数据库账户组**页签，点击<**新增**>。

步骤2. 进入**新增数据库账号**页面，编辑名称和数据库账号，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
数据库账号	可输入多项，用英文逗号隔开。

导入数据库账号组的方法与导入 IP 组的方法类似，不再赘述。

7.6.6. 时间组管理

时间组是一组特定组时间的集合。如自定义某规则需要在特定时间集合内有效时，可将这些时间加入到时间组，在创建规则时选择该时间组即可。

时间组管理页面提供增加、编辑、删除和查询功能，如下图所示。

新增时间组的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤分组管理**”进入**分组管理**页面，选择**时间组**页签，点击<**新增**>。

步骤2. 进入**新增时间组**页面，编辑名称，选择时间范围，点击<**保存**>。

导入时间组的操作方法与导入 IP 组方法相似，不再赘述。

7.6.7. 对象组管理

对象组是一组关键数据库的关键表及关键字段编辑行为对象集合。如自定义某规则需要在某固定对象集合内有效时，可将这些对象加入对象组，创建规则时选择该对象所在组即可。

新增对象组的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤分组管理**”进入**分组管理**页面。

步骤2. 选择**对象组**页签，点击<**新增**>，编辑对象组名称，点击<**保存并添加对象**>。

步骤3. 进入**编辑对象组**页面，编辑数据库等相关信息，点击<**添加对象**>。

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	填写要添加的数据库名，为空表示所有。
Schema	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，为空表示所有。
表	填写要添加的表名，为空表示所有。

字段	填写要添加的字段名，为空表示所有。

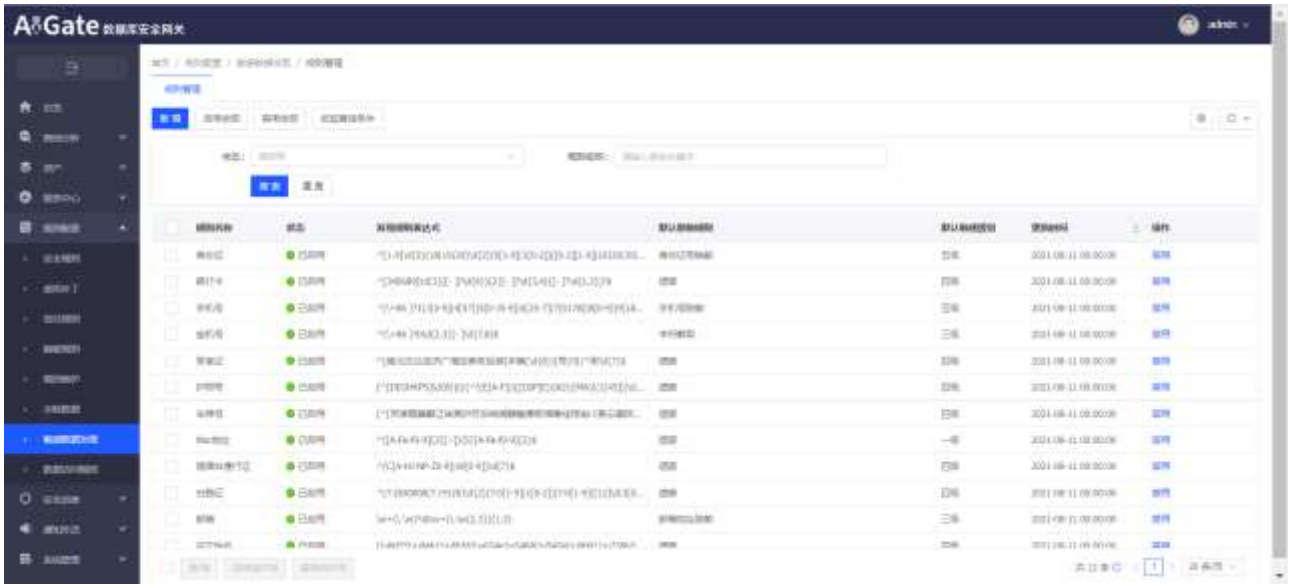
导入对象组的方法与导入 IP 组的方法类似，不再赘述。

7.7. 敏感数据发现

展示出内置的敏感数据发现规则，也可以自定义敏感数据发现规则，可使拉取到的网关或者 AiSort 数据进行更多更广的标为敏感表。

新增自定义敏感数据发现规则的操作方法如下：

步骤 1.在菜单栏选择“**规则配置➤敏感数据发现**”进入**规则管理**页面。



步骤 2.点击<**新增**>，填写相关信息

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
脱敏规则	可选择字符截取、替换、遮蔽、邮箱地址脱敏、手机号脱敏、身份证脱敏、随机、添加噪声
默认敏感级别	有一级至五级可以选择，默认为三级

7.8. 数据访问规则

AiGate 结合数据分级分类实现基于数据的访问控制功能，通过配置身份认证的用户级别和数据访问控制权限，就可以完成配置，实现数据的访问控制功能。

通过 IP、MAC、操作系统用户名、客户端主机名、客户端工具名和数据库账号等多个维度对用户身份认证规则进行管理。身份认证失败后的动作可配置允许访问或者会话阻断两种动作中的其中一种，还可以配置失败后分配给用户身份的默认等级，默认为一级。

根据配置的数据分级分类和身份认证规则，可以对数据访问进行有效的管理。用户默认身份级别为一级，访问大于 1 默认均为动态脱敏；数据级别的访问控制可以配置允许访问、阻断命令、阻断会话和返回结果动态脱敏的动作，有效地阻止不允许访问的，深度地检测授权的访问是否合规，从而达到数据访问的合规。

添加数据访问规则的操作方法如下：

步骤1. 在菜单栏选择“**规则配置➤数据访问规则**”进入**数据访问规则**页面，可查看访问控制规则信息。点击 图标设置身份认证管理的显示列；点击 图标设置身份认证规则列表的刷新间隔。

步骤2. 点击<**新增**>，在弹出的**新增身份认证**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
规则名称	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。
状态	启用或禁用该配置。
所属资产	设置身份认证规则所隶属的资产。
IP 地址	访问所属资产的客户端 IP 地址或 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。
操作系统用户名	访问所属资产的客户端操作系统用户名或操作系统用户名组。可填多值，多个值间以逗号“,”分隔。有关操作系统用户名组的更多信息，请参考 IP 组管理。

配置项	说明
客户端主机名	访问所属资产的客户端客户端主机名或客户端主机名组。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 IP 组管理。
客户端工具名	访问所属资产的客户端客户端工具名或客户端工具名组。可配多个客户端工具，使用逗号“,”分隔，例如：db2bp.exe,java.exe。有关客户端工具名组的更多信息，请参考 IP 组管理。
数据库账号	指定规则所匹配的所属资产数据库登录用户账号或账号组，可填多值，多个值之间以“,”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。
默认级别	身份级别默认可选一级、二级、三级、四级和五级，等级高低逐渐增高，一级为最低，五级最高。
一级数据访问控制	配置访问数据分级为一级的数据后采取的动作，可选允许访问、阻断命令、阻断会话和返回结果动态脱敏四种其中的一种。
二级数据访问控制	配置访问数据分级为二级的数据后采取的动作，可选允许访问、阻断命令、阻断会话和返回结果动态脱敏四种其中的一种。
三级数据访问控制	配置访问数据分级为三级的数据后采取的动作，可选允许访问、阻断命令、阻断会话和返回结果动态脱敏四种其中的一种。
四级数据访问控制	配置访问数据分级为四级的数据后采取的动作，可选允许访问、阻断命令、阻断会话和返回结果动态脱敏四种其中的一种。

配置项	说明
五级数据访问控制	配置访问数据分级为五级的数据后采取的动作，可选允许访问、阻断命令、阻断会话和返回结果动态脱敏四种其中的一种。

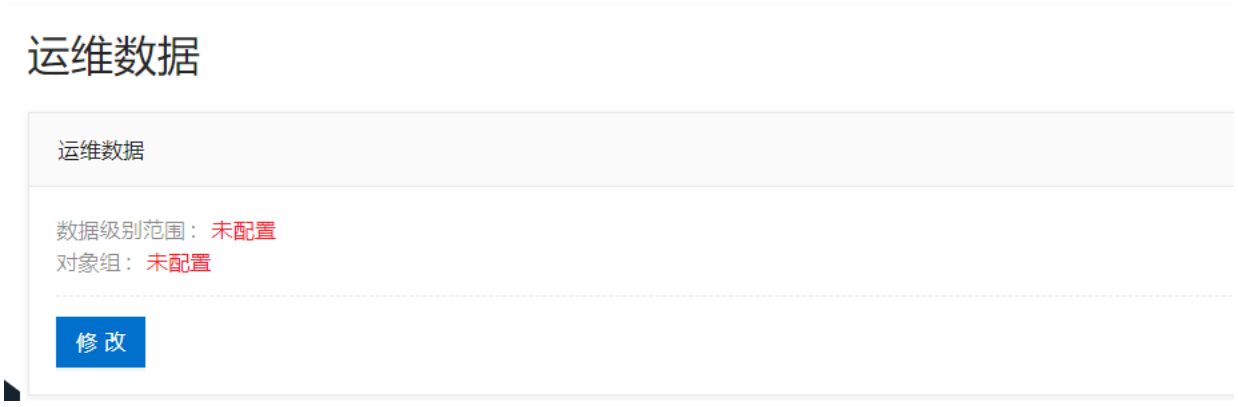
数据访问控制动作为返回结果动态脱敏时，会产生脱敏日志。记录动态脱敏日志的功能可关闭或者开启。

8. 安全运维

运维审批是指用户在客户端执行的 SQL 操作满足审批表时，根据相关配置，则允许或者阻断相关操作，并打印运维审批日志

8.1. 运维数据

步骤 1. 安全运维->运维数据



点击修改，进入运维数据配置页面

配置项	说明
数据级别范围	配置的级别及以上数据的访问需要进行运维审批。五级为最高级别。（级别参考 4.2.2.1）
对象组	关联配置过的对象组（参考 7.6.9）

8.2. 运维人员

8.2.1. 新建运维人员账号

步骤 1.安全运维->运维人员，进入运维人员添加页面

步骤 2.点击新增，弹出添加运维人员框，配置相关信息，点击保存即可

配置项	说明
运维账号	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：审批运维任务
运维资产	选择运维资产，可多选

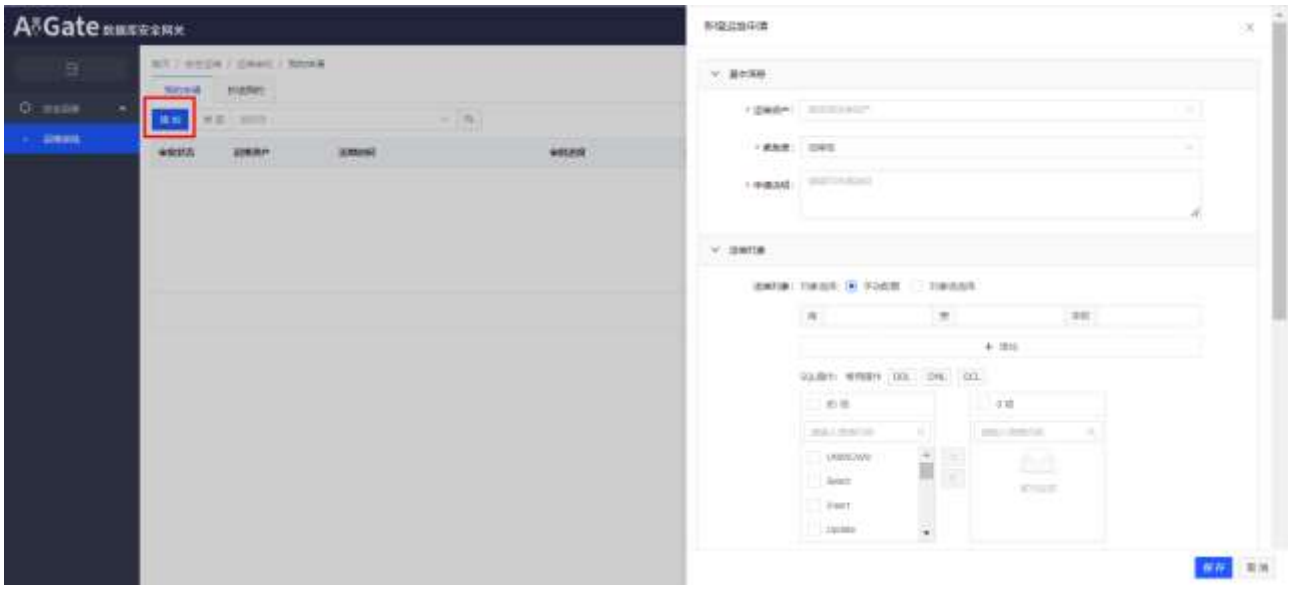
数据库账号	与运维资产相对应（例如 Oracle 默认账号 system）
所属部门	选择该运维人员所属的部门（可点击管理，管理部门）
运维 IP	运维人员使用的 IP
邮箱	运维任务新建、取消，由该邮箱接收通知邮件，可在邮件正文审批或者不审批运维任务
备注	备注信息

点击《编辑》按钮，可以编辑已创建的运维人员，点击《删除》按钮，可删除运维人员

9.2.2 运维申请人登录

步骤 1. 退出 admin 账号，使用运维人员账号登录，进入到运维审批页面（test1 为运维申请人账号）

步骤 2. 点击添加，弹出新增运维申请页面，配置相关项，点击保存即可



配置项	说明
运维资产	选择运维资产（新建运维人员时添加的运维资产）
紧急度	紧急度分为低等级、中等级和高等级
申请说明	说明申请运维任务的理由
运维对象	手动配置：填写一一对应的库表和字段（可单独填写库，可单独填写表）
	对象组选择：点击下拉框，选择配置好的对象组（对象组配置参考 7.6.9）
SQL 操作	可选项
运维 SQL	填写需要运维的 SQL 语句，填写完毕后，点击添加即可，可添加多条 SQL 语句（运维对象和运维 SQL，二者有一即可生成运维任务）
运维时间	点击后，选择运维时间，可是本日、明天、本周、本月，也可自选时间段
一级审批人	选择审批人作为一级审批人，登录审批人后，可以审批运维任务

二级审批人	只有一级审批人审批运维任务后，二级审批人才可以审批运维任务
抄送	抄送相关人员

步骤 3. 选择一条运维任务，点击《复制》按钮，弹出新增运维详情框

直接点击保存，创建一个新的运维任务；

修改运维内容，点击保存，创建一个新的运维任务。

步骤 4. 点击《查看》按钮，可查看运维内容信息，点击《取消任务》，可取消运维任务

9.2.3 运维审批人登录

步骤 1. 退出登录，输入运维审批人账号和密码，点击登录，进入运维审批页面

（说明：审批人页面添加按钮和申请人页面的添加按钮功能和弹出框内容相同；审批人既可以是审批人，也可以是申请人，前提是存在其他的审批人）

步骤 2. 点击我的审批，进入审批列表

步骤 3. 选择审批状态为待审批的运维任务，点击审批按钮，弹出运维任务审批详细框，选择审批通过或者审批驳回，可填写审批意见

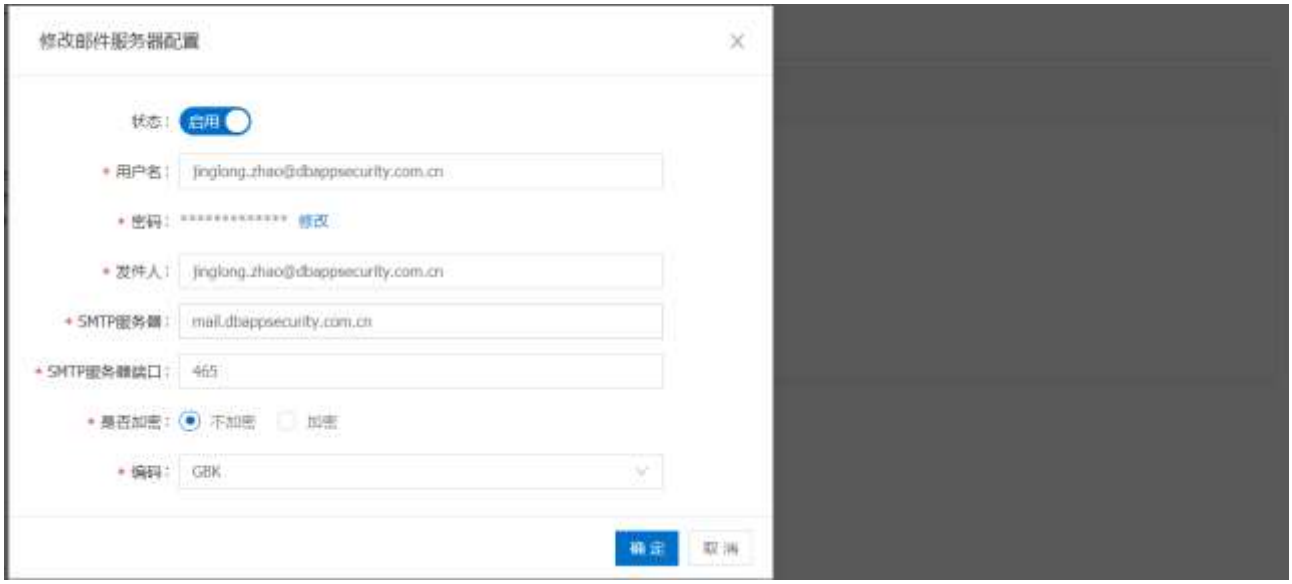
审批后，登录运维申请人页面可查看运维任务申请状态

9.2.4 通知外送

步骤 1. 系统管理->系统配置->通知外送

点击编辑按钮，打开邮件服务器配置状态

步骤 2. 填写相关配置



配置项	说明
状态	启用
用户名	邮箱用户名（收件人的用户名）
密码	邮箱用户名的密码
发件人	发件人的邮箱
SMTP 服务器	填写服务器 IP 或者域名
SMTP 服务器端口	填写发件服务器端口
是否加密	不加密：邮件正文中，点击链接显示正常信息 加密：邮件正文中，点击链接显示加密信息
编码	支持 UTF-8 和 GBK

步骤 3. 运维申请人已添加任务，查收邮件，打开收到的运维邮件

点击审批通过，运维任务则经过审批（如果存在二级审批人，会发送邮件发二级审批人进行审批）

点击审批不通过，运维任务被驳回

步骤 4.客户端通过代理端口登录，执行运维任务中的 SQL 语句和不在运维任务中 SQL 语句，查看运维日志信息

经过审批的运维 SQL 显示经过审批，未经过审批的 SQL 显示未经过审批

9. 通知外送

通知外送功能，可通过邮件、syslog 或者 Kafka 通知 AiGate 后台告警情况，可使运维人员及时发现后台告警情况，并作出相对于防护措施。

9.1. 告警通知

10.1.1 邮件

步骤1. 在菜单栏选择“**通知外送➤告警通知**”进入**告警通知**页面，选择**邮件**页签进入如下页面。

步骤2. 点击<**编辑**>弹出**邮箱配置**对话框，编辑相关信息，点击<**确定**>。

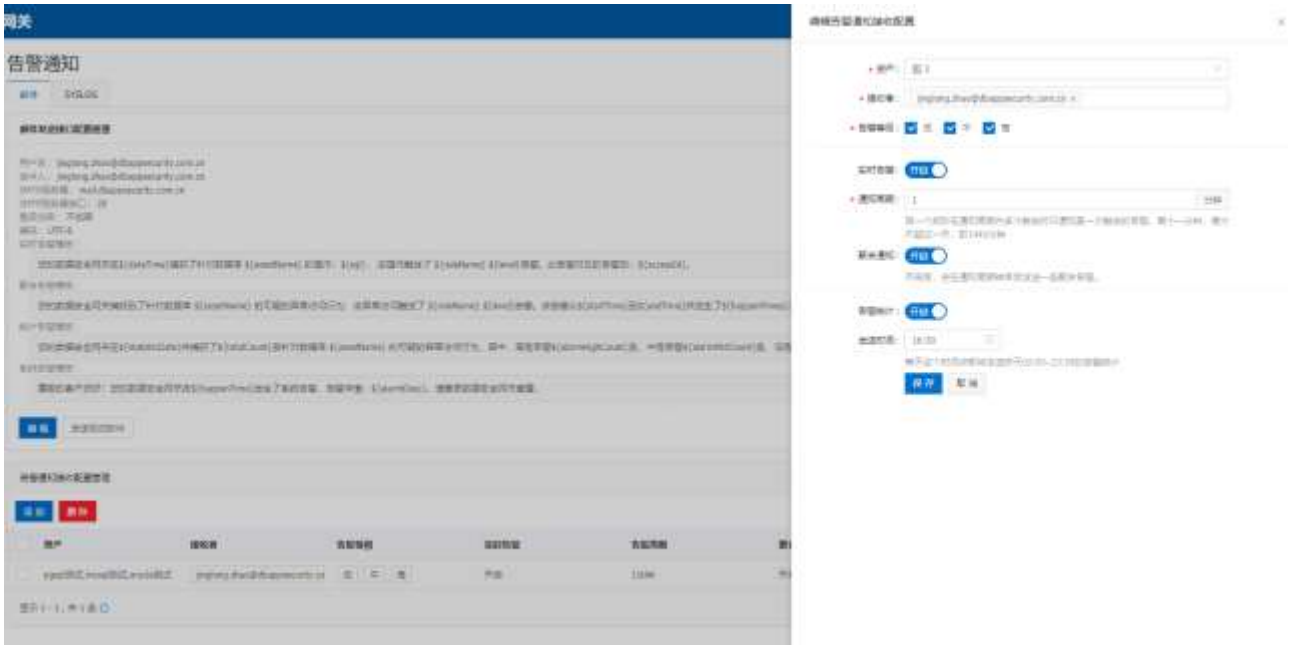
详细配置请参见下表。

配置项	**说明**
用户名	邮箱的用户名。
密码	与邮箱用户名对应的用户密码。
发件人	发件人的邮箱。
SMTP 服务器	SMTP 服务器的 IP 或者域名。
SMTP 服务器端口	SMTP 服务器所用端口。

配置项	说明
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。 以上 SMTP 服务器相关配置与服务器端设置保持一致即可。
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. 配置好邮件发送接口后，可以对需要通过邮件发送接口发送通知的资产配置发送方式。点击<**添加**>。

步骤4. 在弹出的页面中，编辑相关信息，点击<**保存**>。



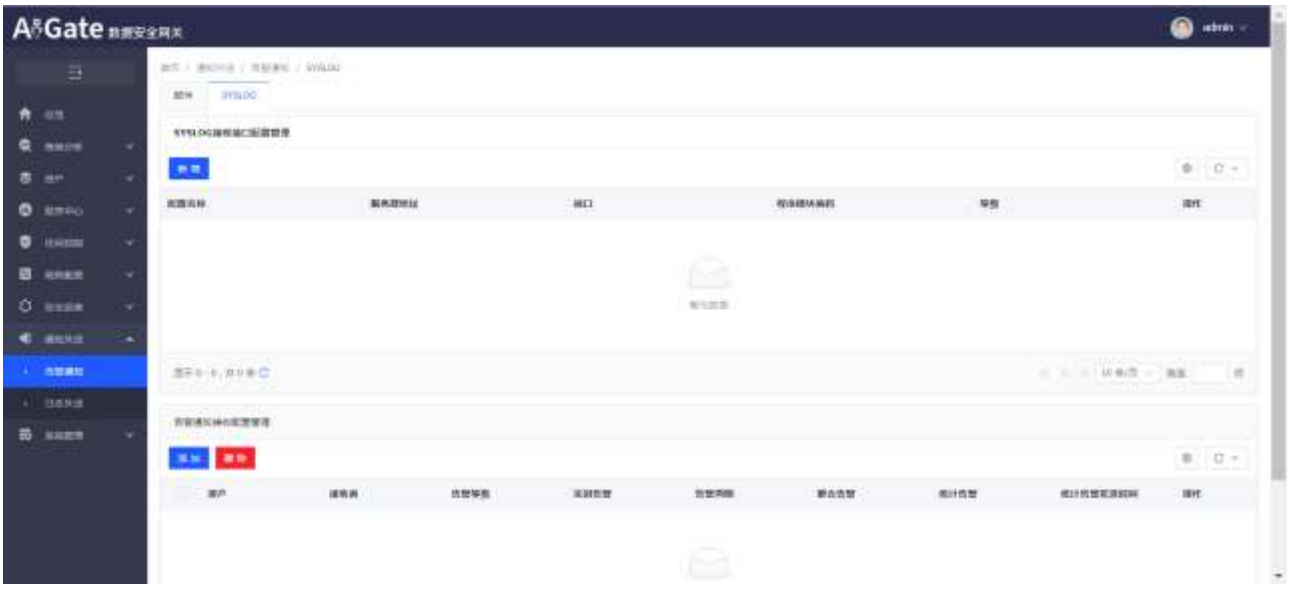
详细配置请参见下表。

配置项	说明
资产	选择要发送告警信息的资产，可选择多项。
接收者	接收告警信息的邮箱，可设置多个邮箱。
告警等级	选择要发送的告警信息的告警等级。
通知周期	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。取值范围：0~86400，单位为秒，0 表示发送全部告警。如果设置为 0，聚合通知功能将无法开启。
聚合通知	开启聚合通知功能后，系统会在通知周期结束后发送一条聚合告警信息。聚合消息示例如下：在过去*秒，总计触发*条告警。
告警统计	选择是否开启发送告警统计信息的功能。
发送时间	每天在设定的时间点发送前一天的告警统计信息。

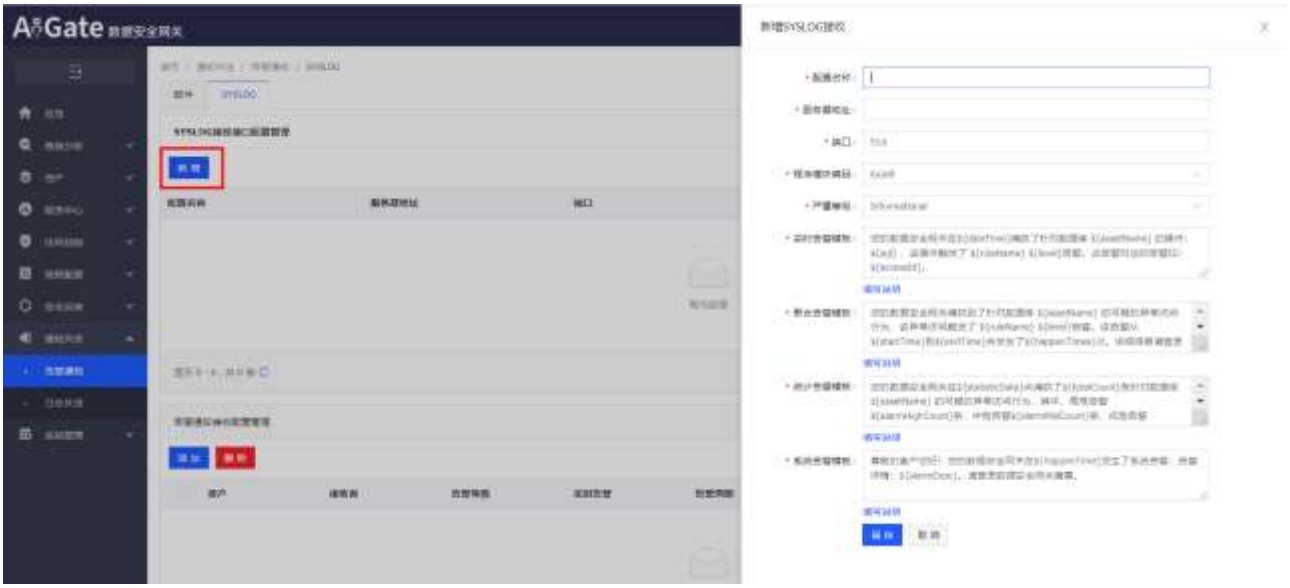
10.1.2 SYSLOG

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

步骤1. 在**告警通知**页面选择 **SYSLOG** 页签进入如下页面。



步骤2. 点击<**新增**>进入**新增 SYSLOG 接收**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**
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 Syslog 接收接口后，可以给需要发送通知的资产配置发送方式。点击<**添加**>。

步骤4. 在弹出的对话框中编辑相关信息，点击<**保存**>。

详细配置请参见下表。

配置项	**说明**
资产	选择要发送告警信息的资产。
接收者	选择 Syslog 接收接口，关于 Syslog 接收接口，可参见前文的步骤 1 和步骤 2。
告警等级	选择要发送的告警信息的告警等级。
通知周期	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。取值范围：0~86400，单位为秒，设为 0 时发送全部告警。如果设置为 0，聚合通知功能将无法开启。
聚合通知	开启聚合通知功能后，系统会在通知周期结束后发送一条聚合告警信息。聚合消息示

	例如下：在过去*秒，总计触发*条告警。
告警统计	是否开启发送告警统计信息的功能。
发送时间	每天在设定的时间发送前一天的告警统计信息。

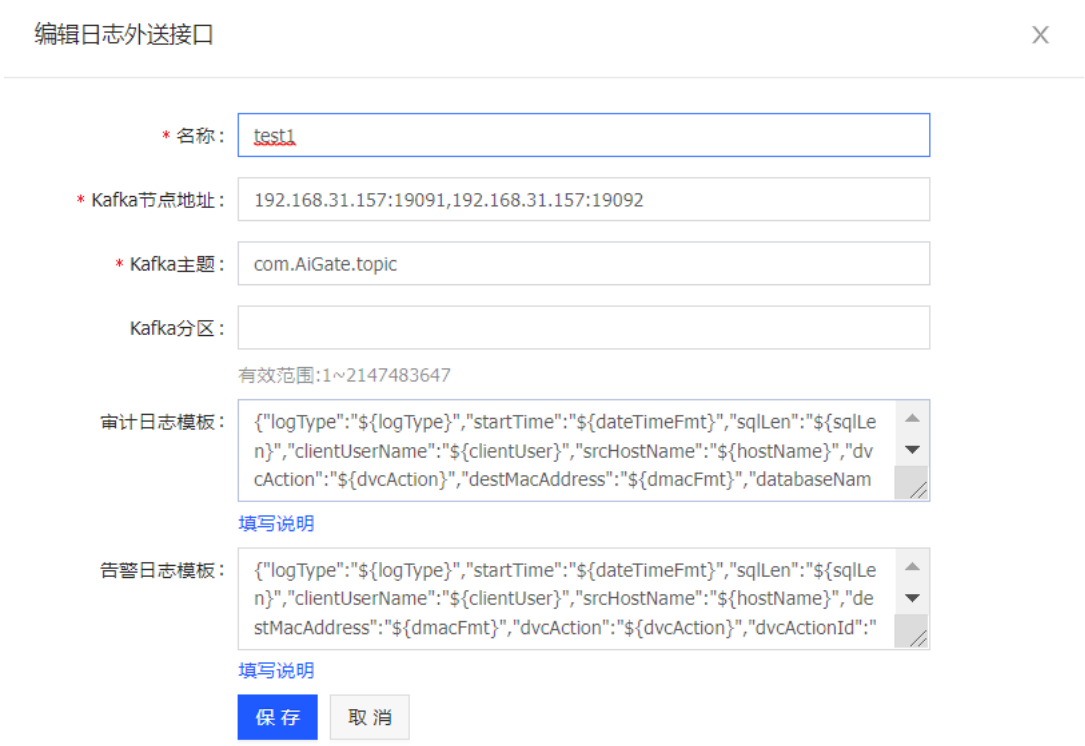
9.2. 日志外送

新增 Kafka 日志外送接口，可以对日志外送接口进行管理、可以对日志外送任务进行管理。

新增日志外送接口操作步骤如下：

步骤 1. 在菜单栏选择“**通知外送➤日志外送**”进入 Kafka 页面。

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



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
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	可以使用参数表达式指代日志的内容，具体表达式可以点击蓝字“填写说明”查看
告警日志模板	可以使用参数表达式指代日志的内容，具体表达式可以点击蓝字“填写说明”查看

新增日志外送任务管理操作步骤如下：

步骤 1. 在菜单栏选择“**通知外送➤日志外送**”进入 Kafka 页面。

步骤 2. 点击“**日志外送任务管理**”的<新增>按钮，填写各项参数后保存。

详细配置请参见下表。

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、Agent 管理、系统配置、系统维护、辅助功能和系统告警。

11.1.用户管理

用户管理主要是为用户设置权限。包括用户管理和用户安全配置。

11.1.1.添加用户

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**>。

详细配置请参见下表。

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。
角色	指定用户角色，系统内置了超级管理员、安全管理员、系统管理员、审计管理员、系统配置员、安全员和审计员七种角色。
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。
以下选项默认不显示，需点击<**更多配置**>显示。	

配置项	说明
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。
认证方式	用户登录系统时的认证方式，可选择“密码”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	限制用户登录系统的时间。

11.1.2.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（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）。

在菜单栏选择“**系统管理➢用户管理**”进入**用户管理**页面，选择**用户安全配置**页签进入**用户安全配置**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
用户安全设置	
登录超时	取值范围 1~43200，默认值为 5。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 0~999，默认值为 5，0 表示不锁定账户。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。
锁定时长	取值范围 1~10800，默认值为 30。
重置计数器	取值范围 1~10800，默认值为 5。密码尝试失败（未达到密码尝试次数设置值时），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	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。取值范围 0~999，0 表示密码不会过期。

11.2.系统配置

11.2.1.网络

系统支持修改管理口、DNS 服务器以及禁用/启用网口等功能。

11.2.1.1.配置管理口

修改管理口配置的操作方法如下：

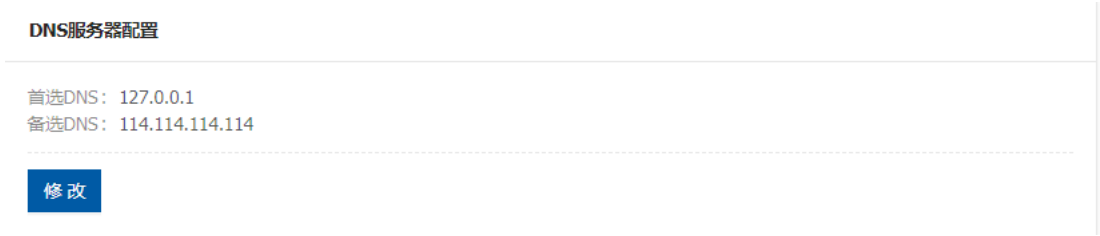
步骤1. 在菜单栏选择“**系统管理➤系统配置**”进入网络配置页面，如下图所示。

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，修改管理口的 IP 地址、子网掩码、IPv4 网关、IPv6 等配置信息，点击<**确定**>。

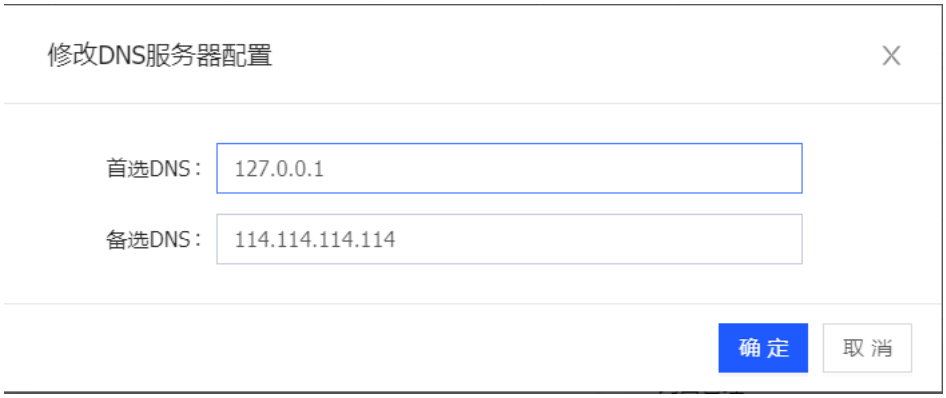
修改管理口 IP 后需要重新登录系统，即在浏览器地址栏中需要输入修改后的管理口 IP（使用 HTTPS 协议），重新输入账号密码登录系统才能继续使用。

11.2.1.2.配置 DNS 服务器

步骤1. 在 **DNS 服务器配置**区域点击<修改>。



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



11.2.1.3.禁用/启用网口

在**网口管理**区域的**操作**列中点击<**启用**>或<**禁用**>，可启用或禁用选中的网口。

11.2.1.4.透明代理

AiGate 数据安全网关支持反向代理部署和透明代理部署。透明代理模式开启后，客户端视数据安全网关为透明模式，配置网桥的两个网口透明成为一根网线，此时资产将不再配置代理端口，直接使用数据库的原生端口即可。

步骤 1.点击修改，选择串联透明代理模式，点击确定，切换到串联透明代理模式，等待切换成功（说明：切换透明代理前，需要清空反向代理模式建的资产）

步骤 2. 新增网桥，点击新增按钮，添加网桥；选择需要建网桥的两个网口，点击保存

步骤 3.在菜单栏选择“**资产➢资产管理**”进入**资产配置**页面，点击新增资产，配置相关项

详细配置请参见下表。

配置项	**说明**

配置项	说明
类型	设置资产类型，包括 Oracle、MySQL 和 PostgreSQL、MariaDB 四种通用数据库。
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。
操作系统	设置资产所在主机的操作系统。
IP 端口	设置资产所在主机的 IP 及原生端口号。
接入链路	选择已配置的网桥
SRC VLANID	源 vlan ID
DST VLANID	目的 vlan ID
最大保存行数	取值范围 0~999，0 表示不保存返回结果，最大保存内容为 64KB。
最大保存长度	可配范围 1~64K，确保整行显示。
运维审批	开启后，启用运维审批功能
应用 IP	运维审批开关开启，填写应用 IP，应用 IP 默认不走运维审批流程
防护模式	入侵检测模式：对数据库进行入侵检测,不阻断任何操作； 入侵防护模式：对数据库进行入侵检测和防护。

11.2.2. SNMP

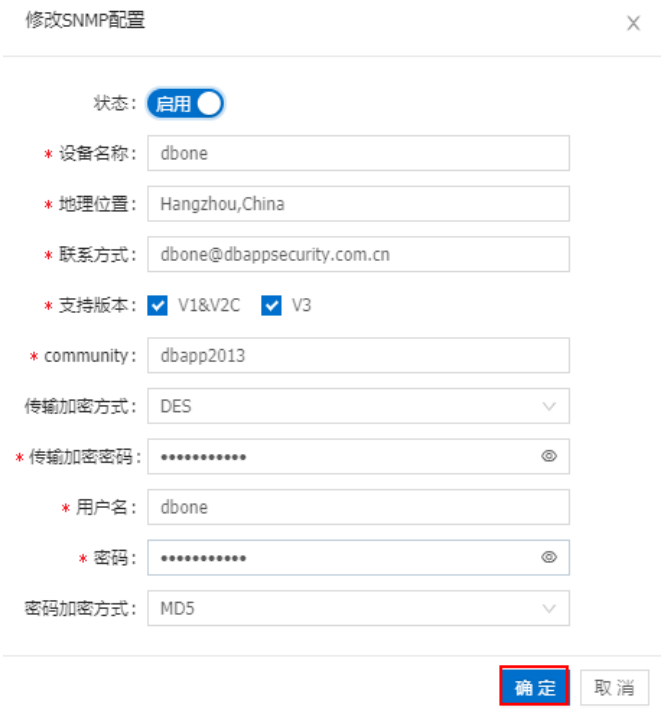
SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议，支

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 AiGate 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**”进入**系统配置**页面，选择 **SNMP** 页签。

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**>。



详细配置请参见下表。

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 AiGate 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。

配置项	说明
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。

11.2.3.许可证

许可证（License）是安恒信息颁发的设备使用许可信息，只有当系统导入了许可证的情况下，系统才能正常使用，否则将出现资产无法添加、设备无法审计的情况。系统通过许可证来限制系统可以审计数据库 IP 端口的数量。

在**系统配置**页面选择**许可证**页签进入**许可证信息**页面，如下图所示。

当证书使用快过期时，请及时致电安恒信息客服热线 400-6059-110 获取新的证书。点击<**导入证书**>，上传证书文件，即可更新证书。

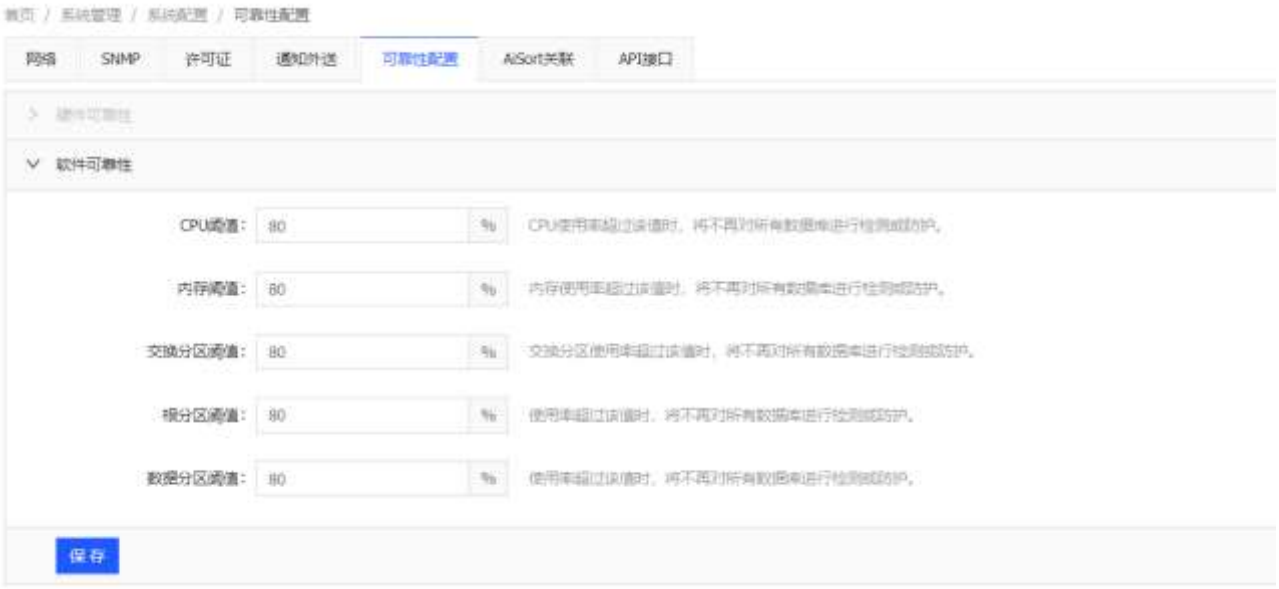
- ◆ 建议在导入新的证书前首先导出系统当前证书。
- ◆ 请确认证书中允许防护的资产数目。

11.2.4.通知外送

参考 9.2.4

11.2.5.可靠性配置

步骤 1. 系统管理->系统配置->可靠性配置



硬件可靠性详细配置参考下表

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

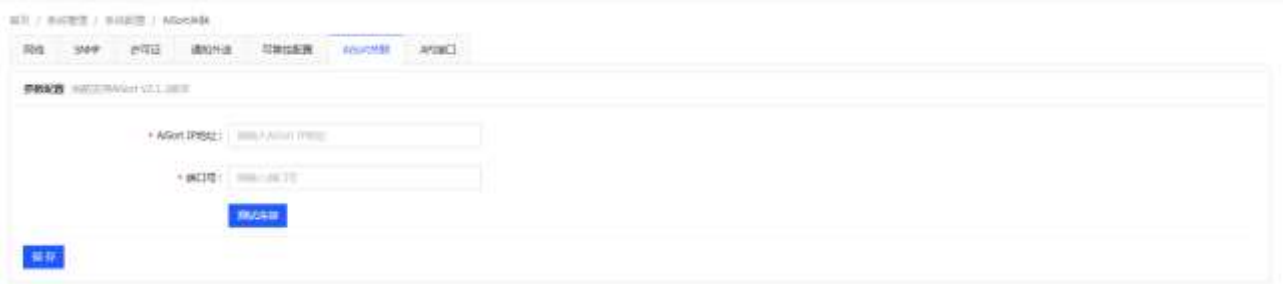
配置项	说明
CPU 阈值	默认 80%，配置区间 60%-85%
内存阈值	默认 80%，配置区间 60%-85%
交换分区阈值	默认 80%，配置区间 60%-85%
根分区阈值	默认 80%，配置区间 60%-85%
数据分区阈值	默认 80%，配置区间 70%-85%（不包含 70%）

说明：只要有一个配置项的实际数据超过配置数据，系统变成 bypass 模式，将不再对所有数据库进行检测或防护。

11.2.7.AiSort 关联

AiSort 关联，可使数据安全网关和 AiSort 联动，数据安全网关可以从 AiSort 上获取元数据。

步骤 1. 在菜单栏选择“**系统管理➤系统配置➤AiSort 关联**”，进入 AiSort 关联配置页面



配置项	说明
AiSort IP 地址	AiSort 的实际 IP

配置项	说明
端口号	AiSort 的端口号，8080
测试连接	填写 AiSort 的 IP 和端口号后，点击测试连接，连接成功证明可用

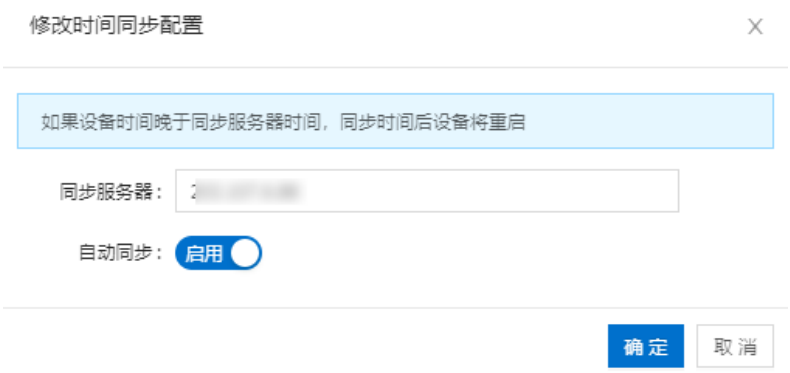
11.3.系统维护

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。

在菜单栏选择“**系统管理➤系统维护**”进入**系统维护**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。

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器。



11.3.2.资源使用

在**系统维护**页面选择**资源使用**页签，可查看系统资源使用情况，包括计算资源、存储空间、网络 I/O 和磁盘读写速率。

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，方便进行溯源追踪，当需要系统协同排查问题时，系统支持在指定接口上进行抓包。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

在**系统维护**页面选择**调试工具**页签，进入**调试工具**页面，点击<**下载**>将日志文件下载至本地。

11.3.3.2.连通性测试

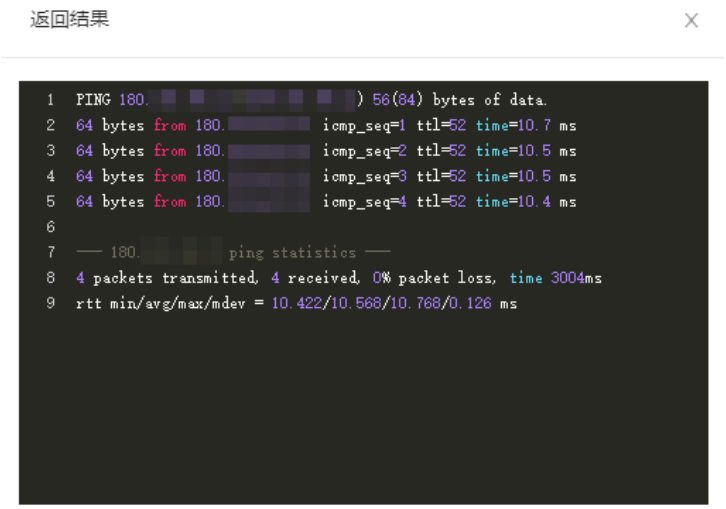
系统提供 ping、nc 和 Traceroute 测试功能，以验证系统与目的主机是否网络连通。

- ping 测试

ping 功能用来测试系统与目标主机是否网络可达。操作方法如下：

在**调试工具**页面，在**连通性检测**区域选择操作类型为 ping，输入 IP（支持 IPv4 和 IPv6），点击<**查看输出结果**>。

可在弹出的对话框中显示测试结果。

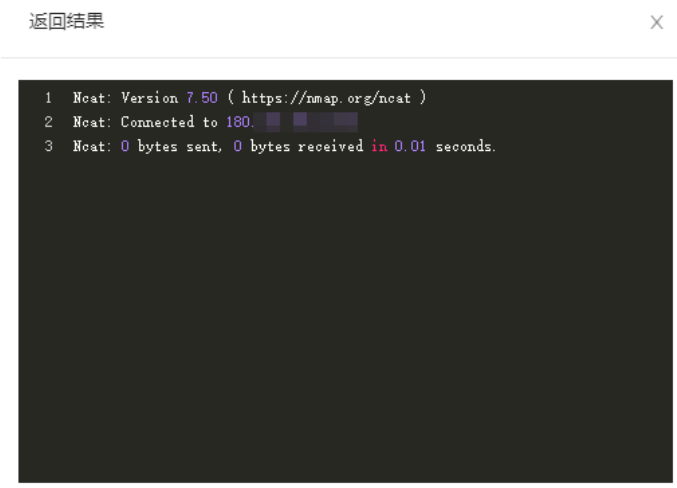


- nc 测试

nc 功能用来扫描目标主机的端口是否开放，操作方法如下：

在**调试工具**页面，在**连通性检测**区域选择操作类型为 nc，选择协议，输入 IP（支持 IPv4 和 IPv6）和端口，点击<**查看输出结果**>。

在弹出的对话框中可查看测试结果。



- Traceroute

Traceroute 功能用来查看系统与目标主机之间经过的网关。操作方法如下：

在**调试工具**页面，在**连通性检测**区域选择操作类型为 traceroute，输入 IP（支持 IPv4 和 IPv6），点击<**查看输出结果**>。

在弹出的对话框中显示测试结果。

11.3.3.3. TCPDUMP 抓包管理

步骤1. 在调试工具页面，在 Tcpdump 抓包管理区域点击<**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	包的过滤串，系统根据过滤串抓取相应报文，过滤串指 IP 和端口。

最大抓包时长	抓包的最大时长，超过此限制，会停止抓包。取值范围：1~86,400，单位为秒。
最大文件大小	抓包文件的最大大小，超过此限制，会停止抓包。取值范围：1~10,480，单位为 MB。

步骤2. 抓包完成后，点击**下载**即可将抓包文件下载至本地。

11.4.软件升级

在**系统维护**页面选择**软件升级**页签，进入如下页面。

步骤 1. 点击上传升级包按钮，弹出本地对话框，选择升级包打开，选择.gz 格式的文件

- 升级包不能大于 1024MB。
- 一次升级过程大概需要 5~10 分钟。如有多个升级包，切勿一次全部上传，需要等上一个升级完成后，再上传下一个。

11.5.数据清理

在**系统维护**页面选择**数据清理**页签，进入如下页面。

步骤 1. 点击修改按钮，弹出修改页面

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	默认 70%，可配置范围 10%-80%（不含 80%）
日志存留天数	默认 180 天，可配置范围 180-3650 天

11.6.数据备份恢复

用户可以在此模块进行数据备份的相关设置，定时备份数据。

在<**系统维护**>页面选择<**数据备份恢复**>页签，进入如下页面。

11.6.1.自动备份数据

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。

修改数据自动备份定时任务的操作步骤如下：

步骤 1. 进入<**系统维护　数据备份恢复**>页签，点击“**修改**”按钮。

配置项	说明

配置项	说明
备份几天前数据	默认两天前，如 25 号备份 23 的数据
执行时间	每天的具体备份操作时间
压缩等级	等级有 1 ~ 9，1：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

11.6.2.备份外送 FTP 设置

设置接受备份文件的服务器的操作步骤如下：

步骤 1. 进入<**系统维护　数据备份恢复**>页签，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。

配置项	说明
状态	在设备上启用或禁用 FTP 功能。
协议	支持 FTP 协议
IP	备份外送 FTP 服务器的 IP

配置项	说明
端口	备份外送 FTP 服务器的端口
用户名	登录 FTP 服务器的用户名
密码	登录 FTP 服务器的密码
上传目录	FTP 服务器上真实可用的目录地址

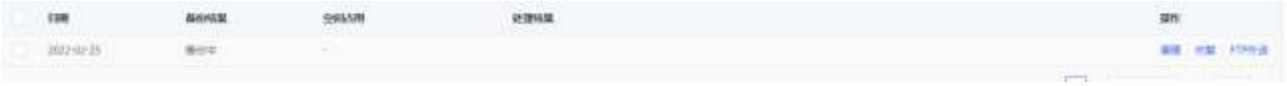
11.6.3.备份数据

11.6.3.1.在线数据

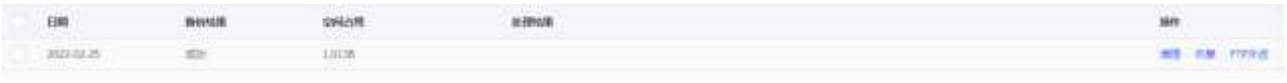
备份在线产生的数据操作步骤如下：

步骤 1. 进入<**系统维护　数据备份恢复**>页签，点击在线数据内数据后方的“**备份**”，或选中需要备份的数据点击上方的“**备份**”按钮。

点击备份后，会跳转至<**本地备份数据**>页签，备份中的数据，状态会变成“备份中”。



备份完成的数据，也会在<**本地备份数据**>页签展示出备份结果。



清理在线数据的操作步骤如下:

步骤 1. 进入<**系统维护　数据备份恢复**>页签，点击在线数据内数据后方的“**清理**”，或选中需要备份的数据点击上方的“**清理**”按钮。

11.6.3.2.本地备份数据

在线数据备份后会在<**本地备份数据**>模块展示，在此模块可对数据执行“**恢复**”和“**FTP 外送**”操作。

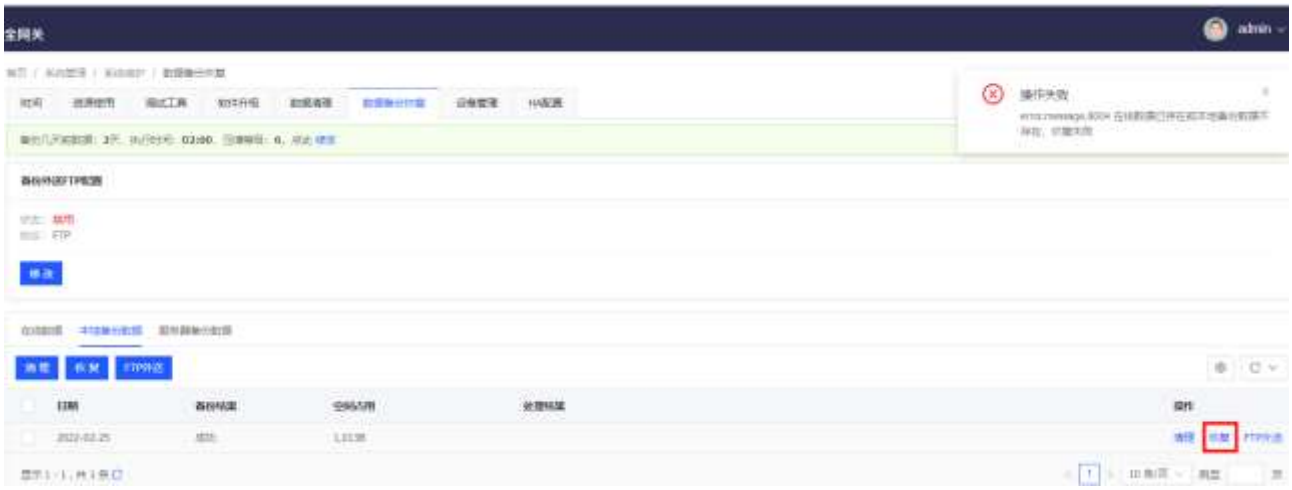
恢复本地备份数据的操作步骤如下：

步骤 1. 进入<**系统维护　数据备份恢复**>页签，点击本地备份数据后方的“**恢复**”，或选中需要恢复的数据点击上方的“**恢复**”按钮。

点击“**恢复**”后，会跳转至<**在线数据**>页签，恢复中的数据，状态会变成“恢复中”。

恢复完成的数据，也会在<**在线数据**>页签展示出恢复结果。

若是本地的数据已存在，则会提示操作失败 error.message.8004 在线数据已存在或本地备份数据不存在，恢复失败。



FTP 外送的操作步骤如下：

步骤 1. 进入<**系统维护　数据备份恢复**>页签，点击本地备份数据后方的“**FTP 外送**”，或选中需要恢复的数据点击上方的“**FTP 外送**”按钮。

点击“**FTP 外送**”后，会跳转至<**服务器备份数据**>页签，恢复中的数据，状态会变成“外送中”。

外送完成的数据，也会在<**服务器备份数据**>页签展示出服务器上传状态。

若是未进行备份外送 FTP 配置，则会提示操作失败 error.message.8111 FTP 外送配置：未配置或者处于禁用状态。

11.6.3.3.服务器备份数据

可以恢复备份到服务器上的数据，操作步骤如下：

步骤 1. 进入<**系统维护　数据备份恢复**>页签，点击服务器备份数据后方的“**恢复**”，或选中需要恢复的数据点击上方的“**恢复**”按钮。

点击“**恢复**”后，会跳转至<**在线数据**>页签，数据状态会变成“恢复中”。

恢复完成的数据，也会在<**在线数据**>页签中展示出恢复状态。

11.7.设备管理

在<**系统维护**>页面选择<**设备管理**>页签，进入如下页面。

用户可在此页面关闭、重启设备，将设备恢复至出厂设置，及打开/关闭远程登录设备的 SSH 端口。详细操作请参见下表。

操作	**说明**
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**>，在弹出的对话框中点击<**确定**>即可重启设备。
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	将 **SSH 端口状态**后的开关置于“开”或“关”，开启或关闭 SSH 登录功能。

- 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。

11.8.HA 配置

AiGate 作为串联设备，如果设备出故障将导致客户服务不可用，对于硬件出货的透明代理部署可以使用硬件 bypass 功能来避免此问题，而反向代理不能使用硬件 bypass。用一台 AiGate 设备，无论其可靠性多高，系统都可能会承受因为单点故障而导致网络中断的风险。为了防止一台设备意外故障而导致网络业务中断，可以采用两台设备形成双机备份。

双机热备的主要两种形式：主主、主备。

在<**系统维护**>页面选择<**HA 配置**>页签，进入如下页面。点击修改可以对配置进行修改。

修改 HA 配置的操作步骤如下：

步骤 1. 进入<**系统维护**>页面选择<**HA 配置**>页签，点击“**修改**”按钮。

步骤 2. 进入主机的<**系统维护**>页面选择<**HA 配置**>页签，配置如下：

步骤 3. 进入备机的<**系统维护**>页面选择<**HA 配置**>页签，配置如下：

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

配置项	说明
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

12.系统告警

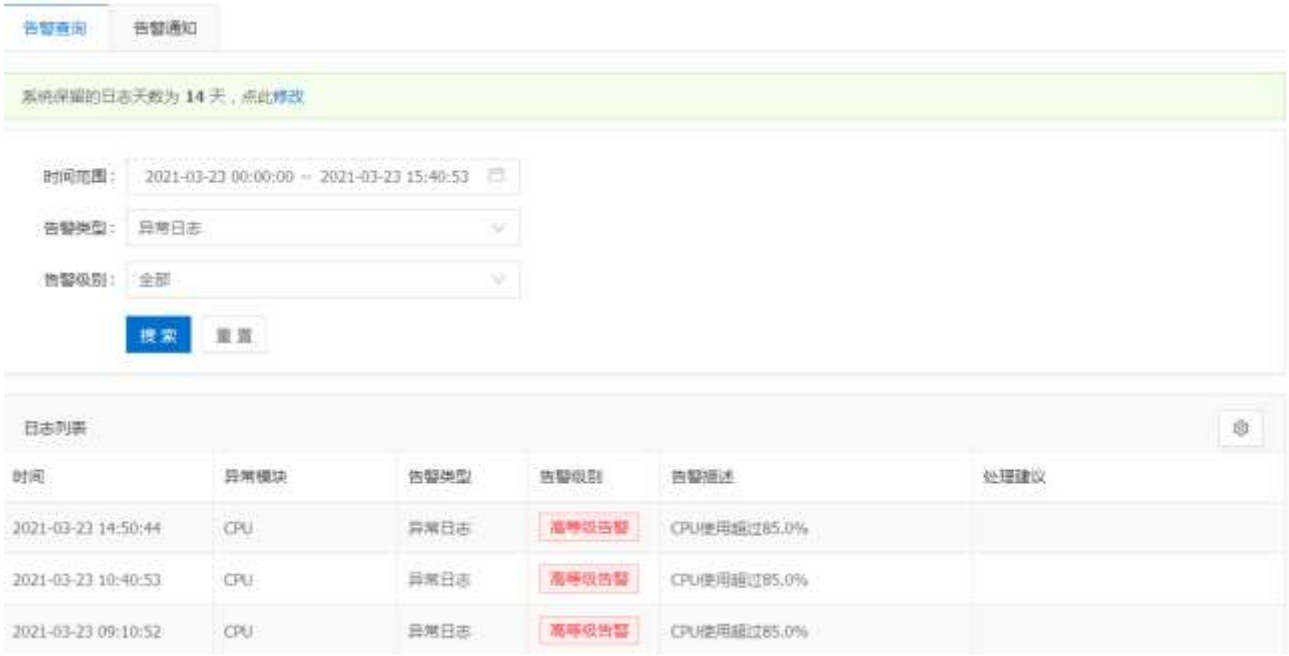
12.1.告警查询

AiGate 支持系统自检功能，当出现系统资源使用率过高、长时间没有告警日志等情况时，会自动产生一条告警信息方便用户快速定位问题。

在菜单栏选择“**系统管理➤系统告警**”进入**系统告警**页面。

点击<**修改**>弹出**修改系统日志自动清理配置**对话框，设置日志保留天数，点击<**确定**>。

设置时间范围，选择告警类型和告警级别，点击<**搜索**>可查询相关告警日志信息。



12.2.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**”进入**系统告警**页面，选择**告警通知**页签进入如下页面。

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**>。各类通知方式配置请参见**错误!未找到引用源。**。

13.操作日志

系统可记录所有用户的操作。审计员可以通过查看操作日志来审计其他用户的操作，操作方法如下：

在菜单栏选择**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。

14.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。