数据库审计

用户使用指南

天翼云科技有限公司

文档说明

产品名称		数据库审计	
适用平台/版本		V4.0.68	
拟制人	8093	**评审组**	
发布人		**备注**	受控文档

修订记录

日期	修订版本	修改记录	修改人
2023-05-31	01	初次发布	8093

目录

前言

概述

感谢您选择天翼云的网络安全产品。本手册对数据库审计进行了简单介绍，并对系统 Web 管理平台的配置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、查询分析、报表中心、智能分析、规则配置、通知外送以及系统管理。

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例，不指代任何实际意义。

预期读者

本文档主要适用于使用数据库审计的人员，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 协议
- 数据库基础知识
- 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：“在菜单栏选择‘**系统状态**’进入**系统状态**页

内容	说明
	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”。
斜体字	可变参数，必须使用实际值进行替代。例如：“在浏览器地址栏输入‘http://*管理 IP*’，回车后进入系统 Web 管理平台登录页面”。

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。

1 快速入门

1.1 产品简介

数据库审计是专业的数据库应用安全防护产品，帮助用户应对网站运营中的安全风险，为数据库应用提供全方位的防护，提供覆盖数据库使用全生命周期的安全防护解决方案。

1.1.1 产品功能

数据库审计产品功能分成原始信息收集、审计信息标准化、审计信息筛选、预警与报表四大模块。

1、原始信息收集

- 通过旁路镜像的模式部署
- 不改变用户现有网络结构
- 不占用数据库服务器资源
- 不影响数据库性能
- 支持分布式部署
- 实现配置与报表的集中管理
- 并发流量采集与处理、多点存储、多级管理
- 自动定期发现功能，及时发现未知数据库

2、审计信息标准化

- 支持国内外主流数据库，包括传统的数据库系统、大数据系统和 Web 系统等，具体支持的系统和版本如下表所示。

数据库分类	数据库系统	版本
关系型	Oracle	8i、9i、10g、11g、12c、18c、19c、21c

数据库分类	数据库系统	版本
	MySQL	4.0、4.1、5.0、5.1、5.5、5.6、5.7、8.0
	SQL Server	2000、2005、2008、2012、2014、2016、2017、2019
	Sybase ASE	11.9、12.5
	DB2	v80、v81、v82、v95、v97、v10.5、v11.1、v11.5
	Informix	IDS9
	Oscar	5.5、5.7
	达梦（DM）	DM7、DM8
	Cache	2010、2016
	PostgreSQL	9、10、11、12、13、14
	Teradata	所有版本
	人大金仓（Kingbase）	V6、V7、V8
	GBase	8.5a、8.8s
	MariaDB	5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3
	Hana	1.0、2.0
	GaussDB	100、200、300

数据库分类	数据库系统	版本
	LibrA	6
	K-DB	11
	Sybase IQ	15.4
	TiDB	4.X、5.X
	Vertica	7、8、9、10、11
	OceanBase	2.X
	PolarDB	MySQL、PostgreSQL、兼容 Oracle 语法
	PolarDB-X	1.0/MySQL5、1.0/MySQL8、2.0/MySQL5.7
	AnalyticDB	MySQL、PostgreSQL
	TBase	V2
	HighGo	6.0
	TDSQL-C MySQL	5.7、8.0
	TDSQL-C PostgreSQL	10、14
非关系型	MongoDB	2.x、3.x、4.x、5.x
	HBase（protobuf）	所有版本
	HBase（thrift）	Thrift1、thrift2

数据库分类	数据库系统	版本
	Hive	1.X、2.X、3.X
	Redis	所有版本
	Elasticsearch	所有版本
	Cassandra	3.X
	HDFS	所有版本
	Impala	3.X
	Graphbase	6
	Greenplum	5、6
	Spark SQL（thrift）	1.x、2.x
	Spark SQL（RESTful）	1.x、2.x
	SSDB	所有版本
	ArangoDB	3.4.9
	Neo4j	4.2.0
	OrientDB	3.1.6
大数据	HBase（protobuf）	所有版本
	HBase（thrift）	thrift1、thrift2
	Hive	1.X、2.X、3.X
	Cassandra	3.X
	HDFS	所有版本
	Impala	3.X
	Graphbase	5、6

数据库分类	数据库系统	版本
	Spark SQL（thrift）	1.x、2.x
	Spark SQL（RESTful）	1.x、2.x
	SSDB	所有版本
	MAX COMPUTE	所有版本
图形	Graphbase	6
	ArangoDB	3.4.9
	Neo4j	4.2.0
	OrientDB	3.1.6
全文检索	Elasticsearch	所有版本
文档	MongoDB	2.x、3.x、4.x、5.x
	ArangoDB	3.4.9
键值	Redis	所有版本
其他	HTTP	所有版本
	Telnet	所有版本
	FTP	所有版本

- 将不同数据库协议按照标准化的格式进行展示，方便管理人员阅读和分析。

3、审计信息筛选

- 根据 5W1H（What、Where、When、Who、Why、How）分析模型进行规则设置，提供丰富的规则条件配置方法。
- 内置 900 多条安全相关的审计分析规则。
- 根据采集到的数据进行数据分析和产生行为模型。

- 审计结果查询。

4、预警与报表

- 提供 Syslog、短信、邮件、SNMP、钉钉、企业微信等告警通知方式，可第一时间通知管理人员。
- 可与综合日志审计分析平台等进行日志的整合。
- 内置 23 种高价值、符合法律法规的分析报表，可从数据库账号增删、密码修改、权限变更、高危操作、违规告警、账号复用、数据库性能分析等维度进行分析。
- 提供自定义报表功能，可根据客户的业务需要，选择不同的维度和指标对审计数据进行统计和分析。

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

数据库审计采用国际领先、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

数据库审计内置丰富的漏洞规则，在审计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审计规则。

3、智能关联分析

数据库审计通过同时提取 Web 业务端和数据库端的协议流量，提取出具体业务操作请求 URL、POST/GET 值、业务账号、原始客户端 IP、MAC 地址、提交参数等。通过智能自动多层关联，关联出每条 SQL 语句所对应 URL 以及其原始客户端 IP 地址等信息，实现追踪溯源。

4、双向审计

数据库审计可以实现真正的双向审计。双向审计不但包含了 SQL 语句执行状态、返回行数、执行时长等基本信息，同时包含数据库的返回结果内容。

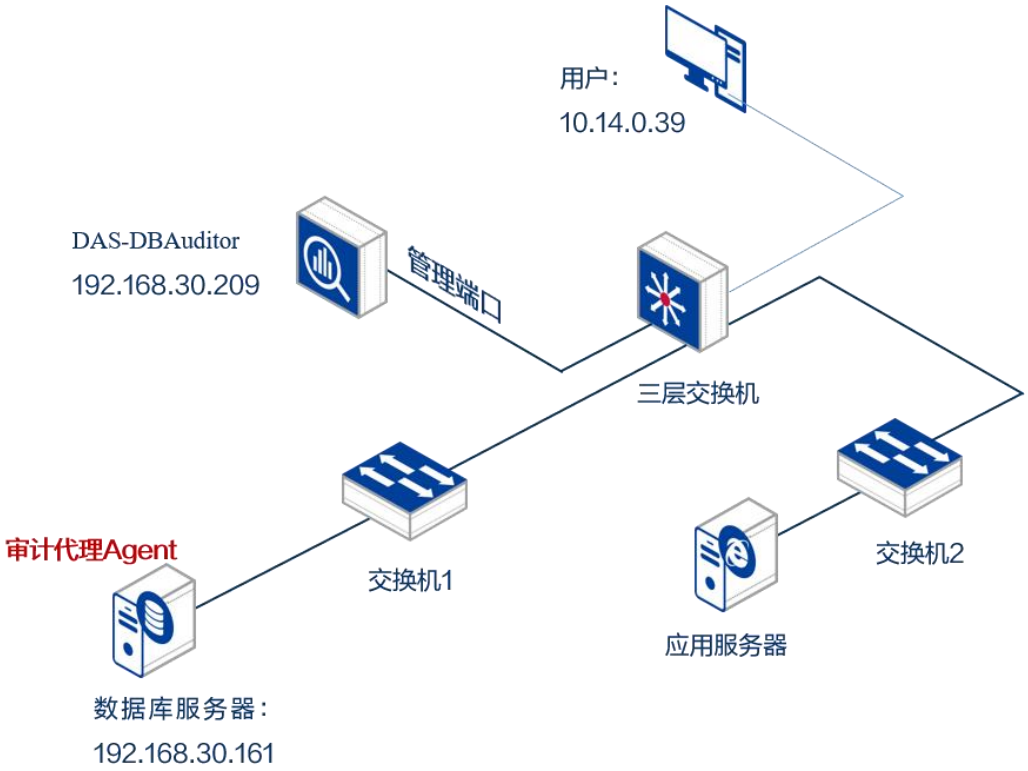
5、数据库行为模型分析

通过自动学习建立数据库行为模型，行为模型基于“总-分”逻辑分析思维，逐层展示整个数据库的行为状态。通过行为模型的变更分析，可方便用户掌握最新访问动态（即通过行为模型对比分析，得出两个不同时间段的行为差异，给出相应告警并及时告知用户）。

1.1.3 典型应用场景

1.1.3.1 流量代理模式

数据库审计产品支持通过在宿主机上安装流量代理插件的方式进行审计。宿主机可以是数据库系统所在主机，也可以是访问数据库系统的应用系统所在主机，或者是运维数据库的运维终端。流量代理根据数据库审计产品上配置的资产信息，通过在安装审计代理插件的服务器上的网卡抓取数据库请求和响应报文，并将报文发送到数审上。流量代理模式的网络拓扑如下图所示。



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。本文的操作内容以超级管理员举例说明。

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

产品仅支持从天翼云平台页面单点登录数据库审计产品的 web 管理页面。

1.4 主要业务流程

系统主要业务流程如下：

步骤 1. 安装 agent：在数据库系统或业务系统上安装数据采集插件，详情请参见 Agent 管理。

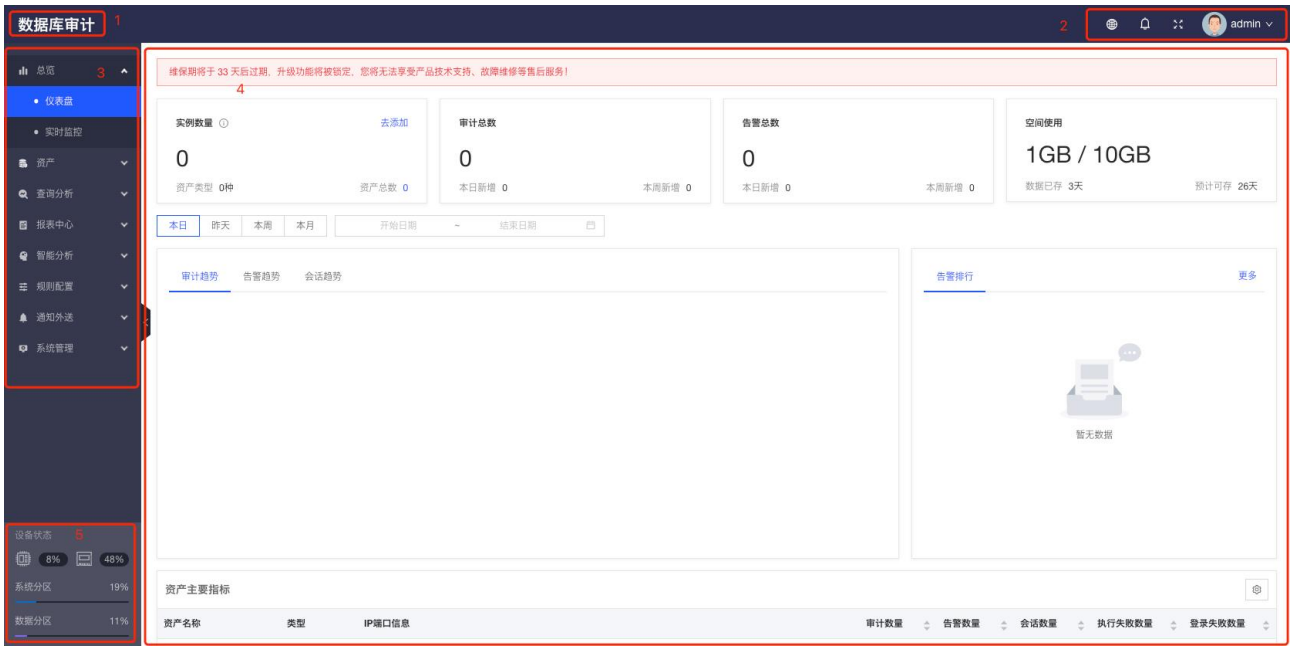
步骤 2. 添加资产：添加系统需要审计的数据库，详情请参见资产。

步骤 3. 配置规则：配置数据库的安全规则和过滤规则，详情请参见规则配置。

步骤 4. 订阅报表和设置告警通知：便于管理员及时了解数据库的运行状态及安全告警信息，详情请参见报表订阅和告警通知。

2 Web 配置页面简介

系统提供简单的 Web 配置页面，主要包含五个部分：1.产品名称；2.辅助功能区；3.菜单栏；4.操作区；5.设备状态。



各部分功能说明请参见下表。

序号	名称	说明
1	产品名称	点击产品名称可返回至**仪表盘**页面。
2	辅助功能区	提供各类辅助功能的配置入口，包括查看帮助文档、切换系统界面语言、查看通知消息、全屏显示、设置用户信息。
3	菜单栏	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。
4	操作区	该区域主要用于信息展示以及相关功能的配置。
5	设备状态	该区域用于显示设备状态信息，包括 CPU 使用率、内存使用率、系统分区使用率和数据分区使用率。

2.1 切换系统界面语言

将光标悬停至图标，选择语言（“English”或“简体中文”），即可切换系统界面语言。

2.2 通知信息

在页面右上角点击图标查看系统通知消息，右上角数字表示未读消息数。在待办事项下方点击该事件条目可快速处理待办事项。

2.3 全屏显示

在页面右上角点击图标可进入全屏模式，按“Esc”键或点击页面右上角的图标，即可退出全屏模式。

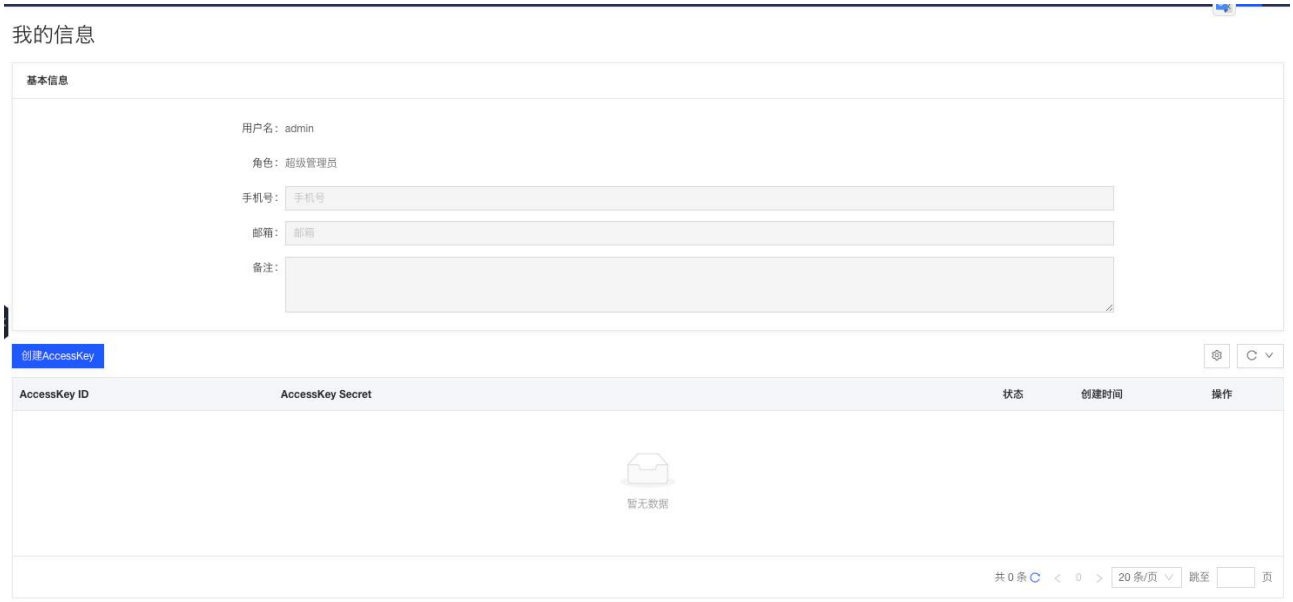
2.4 用户信息

2.4.1 修改用户信息

步骤 5. 将光标悬停于用户头像，选择<**我的信息**>。

步骤 6. 进入**我的信息**页面后，可查看基本信息以及创建 API 访问键（AccessKey）。

API 访问键用于为第三方开发人员提供访问及调试数据库审计的应用接口，包括 AccessKey ID 和 AcessKey Secret 两部分。AccessKey ID 用于标识用户，AcessKey Secret 是用于验证用户的密钥。



详细配置项和说明请参见下表。

配置项	说明
创建 AccessKey	点击<**创建 AccessKey**>，可生成用户的 AccessKey ID 和 AcessKey Secret。

2.4.2 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
天翼云
系统名称
数据库审计
软件版本
V4.0
设备厂商
天翼云科技有限公司
公司网站
https://www.ctyun.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、告警排行和资产信息汇总。

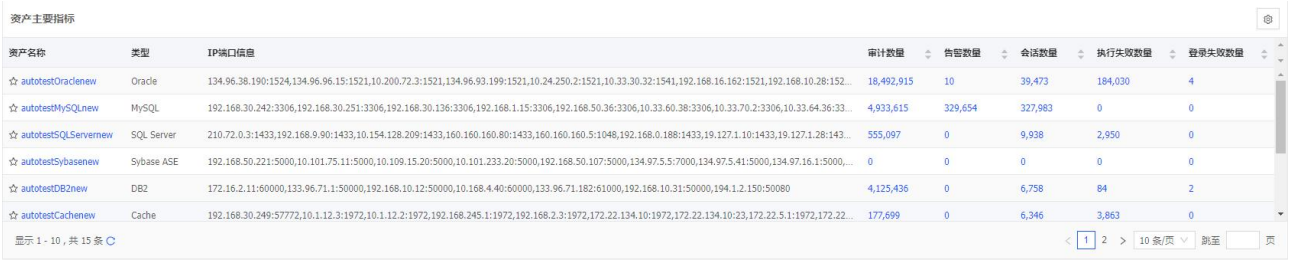
在菜单栏选择“**总览➤仪表盘**”进入**仪表盘**页面。用户可在仪表盘查看以下信息，或执行以下操作。

◆ 查看实例数量、审计总数、告警总数和空间使用等参数。

- 在实例数量中点击<**去添加**>可添加新的资产。有关资产的详细信息，请参见资产。
- 在告警总数中点击<**告警优化**>可在告警分析页面优化告警。有关告警优化的详细信息，请参见告警分析。

◆ 查看指定时间段内的审计趋势、告警趋势、会话趋势和告警统计情况。在告警排行中点击<**更多**>可在告警分析页面优化告警。有关告警优化的详细信息，请参见告警分析。

◆ 查看指定时间段内资产汇总信息。可分别根据审计数量、告警数量、会话数量、执行失败数量和登录失败数量进行排序。

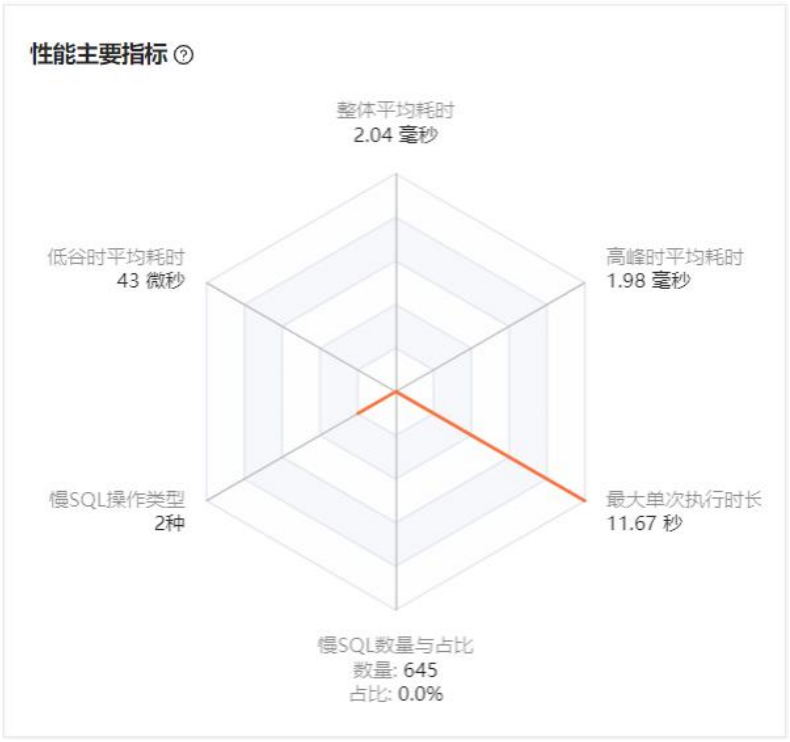


3.2 性能分析

在菜单栏选择“**总览➤性能分析**”进入**性能分析**页面，可查看审计到 SQL 的性能，包括执行时长和执行次数等信息，为 DBA 改进数据库性能提供参考数据。

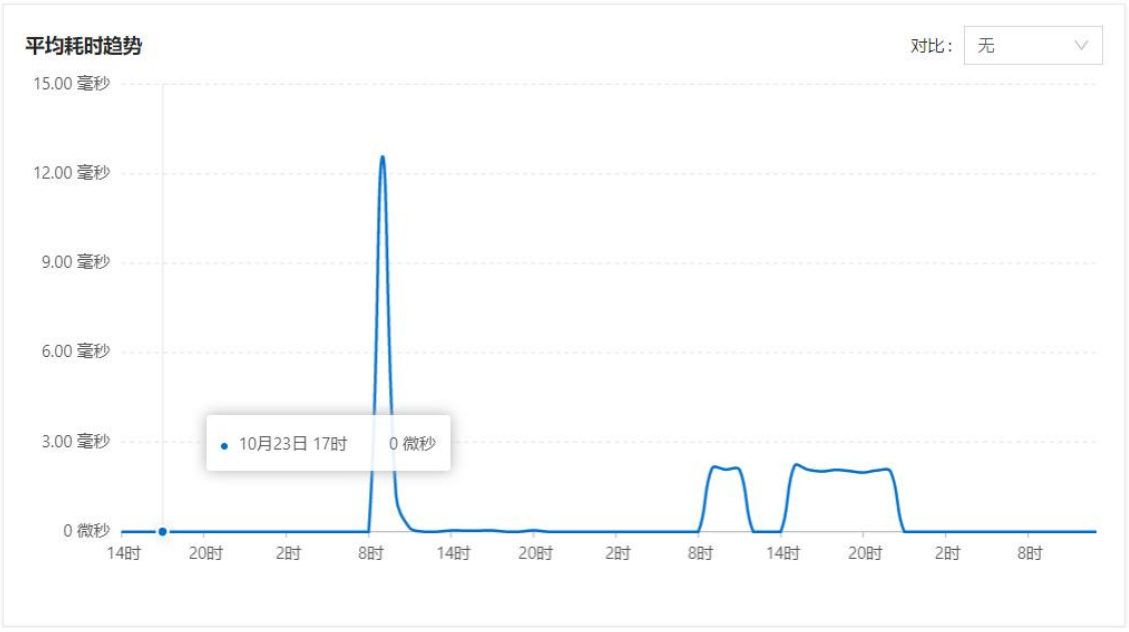
◆ 支持查看 SQL 性能的主要指标。

- 整体平均耗时：指定时间范围内，SQL 总执行时长/执行总数，耗时 1s 及以上，雷达图满格。
- 低谷时平均耗时：指定时间范围内有且 SQL 数量最少的时段，耗时 1ms 及以上，雷达图满格。
- 高峰时平均耗时：时间范围内，审计日志数量最多的单位小时内总执行时长/执行总数，耗时 1s 及以上，雷达图满格。
- 慢 SQL 操作类型：时间范围内，执行时长超过 1s 的语句的操作类型，15 种及以上，雷达图满格。
- 慢 SQL 数量与占比：时间范围内，执行时长超过 1s 的语句数量/语句总数，占比 100%，雷达图满格。



- 平均耗时趋势。

  可查看 SQL 平均耗时趋势图，支持与昨天、上周和上月进行对比。

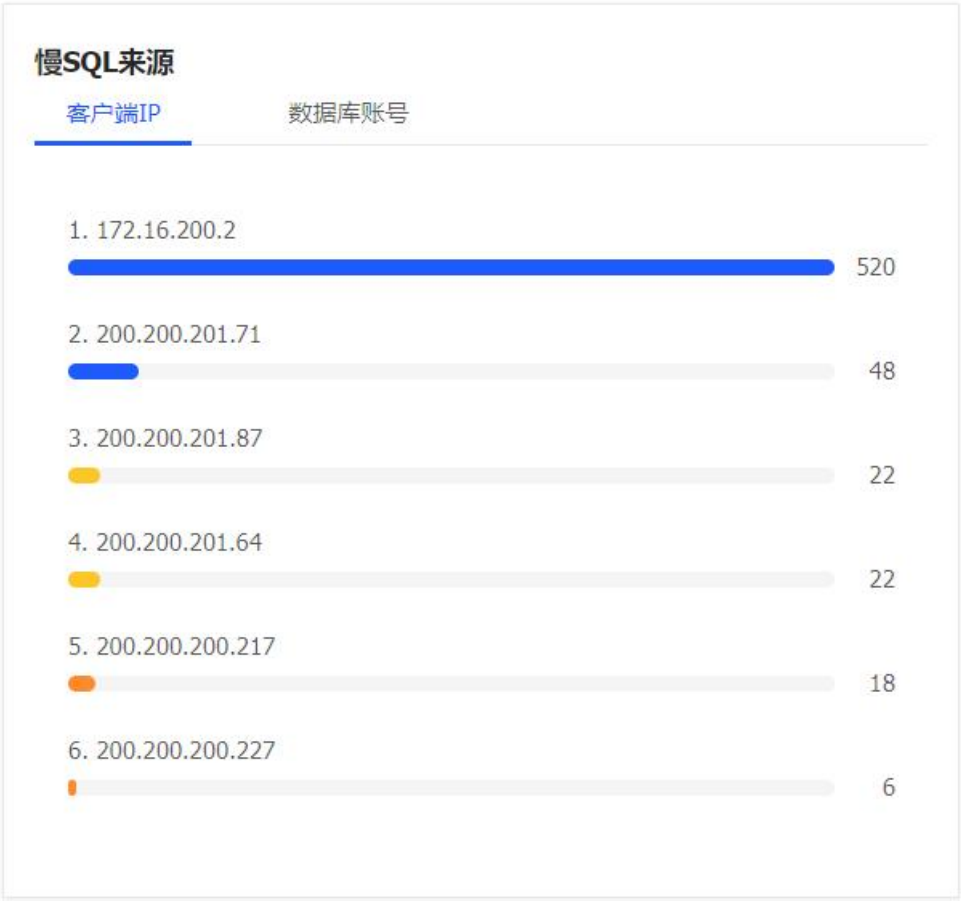


- 支持查看审计日志的执行时长的分布情况。

  面积越大即代表平均耗时越长，颜色越深即代表 SQL 数量越多。将光标悬停于对应的区域可以看到具体的信息，包含资产、IP 和端口、数据库名、平均耗时和执行次数。

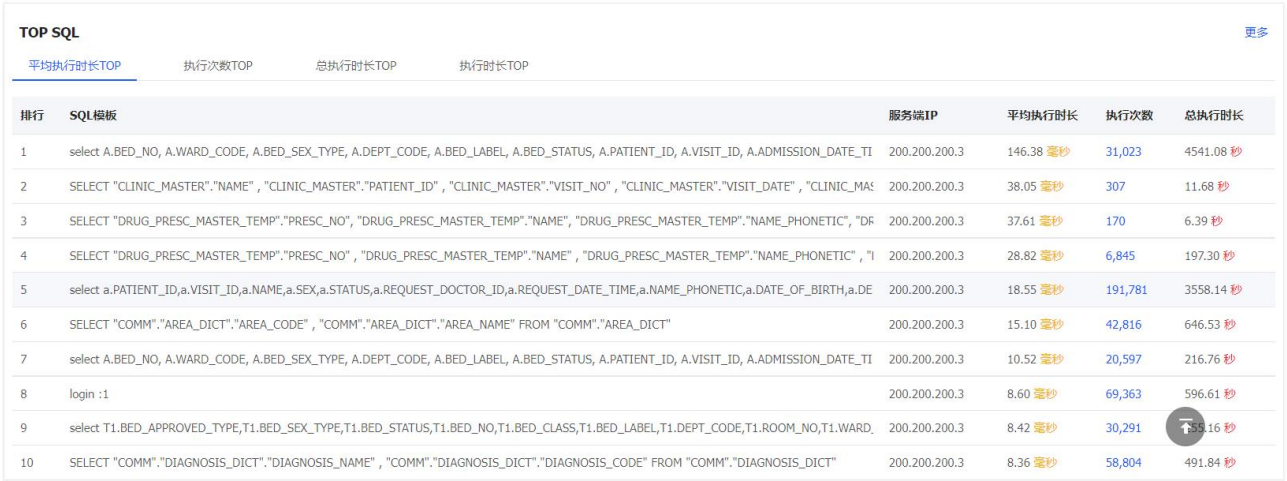
- 支持查看慢 SQL 来源。

  支持从客户端 IP 和数据库账号两个维度统计慢 SQL 的数量。



◆ 支持查看 SQL 语句的性能排行。

分四个 TOP 排行，分别是平均执行时长 TOP、执行次数 TOP、总执行时长 TOP 和执行时长 TOP。其中前三个 TOP 根据 SQL 模板进行统计，最后一个执行时长 TOP 根据审计日志进行统计。点击<**更多**>可以跳转到 **TOP SQL** 页面查看更多的排行信息。



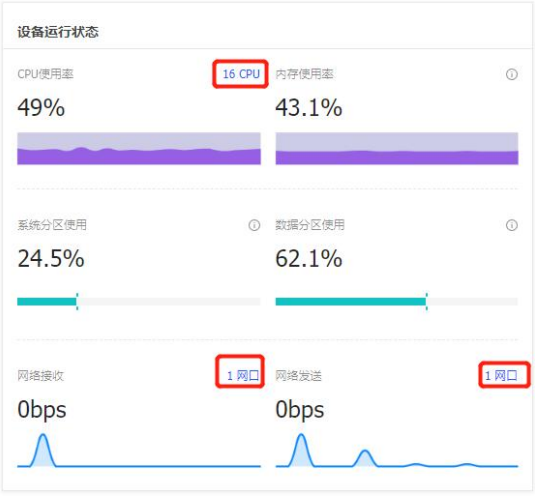
排行	SQL模板	服务端IP	平均执行时长	执行次数	总执行时长
1	select A.BED_NO, A.WARD_CODE, A.BED_SEX_TYPE, A.DEPT_CODE, A.BED_LABEL, A.BED_STATUS, A.PATIENT_ID, A.VISIT_ID, A.ADMISSION_DATE_TI	200.200.200.3	146.38 毫秒	31,023	4541.08 秒
2	SELECT "CLINIC_MASTER"."NAME" , "CLINIC_MASTER"."PATIENT_ID" , "CLINIC_MASTER"."VISIT_NO" , "CLINIC_MASTER"."VISIT_DATE" , "CLINIC_MAS	200.200.200.3	38.05 毫秒	307	11.68 秒
3	SELECT "DRUG_PRESC_MASTER_TEMP"."PRESC_NO", "DRUG_PRESC_MASTER_TEMP"."NAME", "DRUG_PRESC_MASTER_TEMP"."NAME_PHONETIC", "DR	200.200.200.3	37.61 毫秒	170	6.39 秒
4	SELECT "DRUG_PRESC_MASTER_TEMP"."PRESC_NO" , "DRUG_PRESC_MASTER_TEMP"."NAME" , "DRUG_PRESC_MASTER_TEMP"."NAME_PHONETIC" , "I	200.200.200.3	28.82 毫秒	6,845	197.30 秒
5	select a.PATIENT_ID,a.VISIT_ID,a.NAME,a.SEX,a.STATUS,a.REQUEST_DOCTOR_ID,a.REQUEST_DATE_TIME,a.NAME_PHONETIC,a.DATE_OF_BIRTH,a.DE	200.200.200.3	18.55 毫秒	191,781	3558.14 秒
6	SELECT "COMM"."AREA_DICT"."AREA_CODE" , "COMM"."AREA_DICT"."AREA_NAME" FROM "COMM"."AREA_DICT"	200.200.200.3	15.10 毫秒	42,816	646.53 秒
7	select A.BED_NO, A.WARD_CODE, A.BED_SEX_TYPE, A.DEPT_CODE, A.BED_LABEL, A.BED_STATUS, A.PATIENT_ID, A.VISIT_ID, A.ADMISSION_DATE_TI	200.200.200.3	10.52 毫秒	20,597	216.76 秒
8	login :1	200.200.200.3	8.60 毫秒	69,363	596.61 秒
9	select T1.BED_APPROVED_TYPE,T1.BED_SEX_TYPE,T1.BED_STATUS,T1.BED_NO,T1.BED_CLASS,T1.BED_LABEL,T1.DEPT_CODE,T1.ROOM_NO,T1.WARD_	200.200.200.3	8.42 毫秒	30,291	255.16 秒
10	SELECT "COMM"."DIAGNOSIS_DICT"."DIAGNOSIS_NAME" , "COMM"."DIAGNOSIS_DICT"."DIAGNOSIS_CODE" FROM "COMM"."DIAGNOSIS_DICT"	200.200.200.3	8.36 毫秒	58,804	491.84 秒

3.3 实时监控

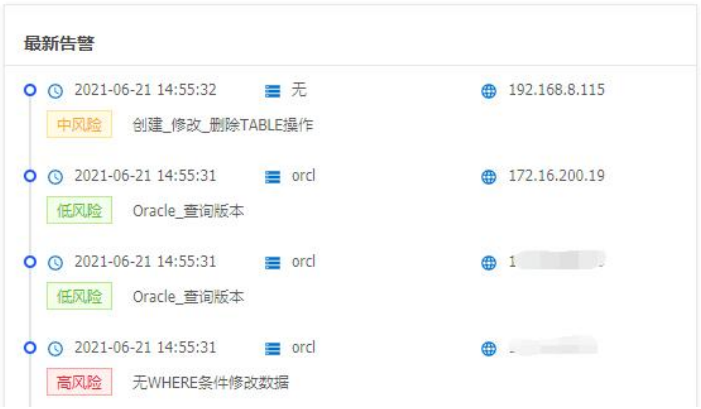
在菜单栏选择“**总览➤实时监控**”进入**实时监控**页面，可实时监控系统状态。

- 可查看实时审计情况。

- 可查看设备运行状态。点击<***CPU***>可查看设备所有 CPU 的使用率；点击<***网口***>可查看设备所有网口的网络速率（“*”为数字，请以实际情况为准）。



- 可查看最新告警信息。



◆ 可查看资产负载状态。

资产负载状态 实时刷新

资产名称	并发会话数	请求流速	返回流速	每秒SQL吞吐量
autotestOraclenew	3,412	0bps	0bps	0
autotestMySQLnew	11,241	0bps	0bps	0
autotestSQLServernew	2,375	0bps	0bps	0
autotestDB2new	4,908	0bps	0bps	0
autotestCachenew	1,460	0bps	0bps	0
autotestPostgreSQLnew	46	0bps	0bps	0
autotestMongoDBnew	252	0bps	0bps	0
autotest-mysql	1	0bps	0bps	0
autotest-oracle	3	0bps	0bps	0

显示 1 - 9，共 9 条 C < 1 > 10 条/页 跳至 页

点击**并发会话数**列中的数字可查看资产会话的详细信息。

返回 autotest-oracle的当前会话 实时刷新

来源	目的	客户端主机名	连接时长	累计SQL数量	请求流速	响应流速	每秒SQL吞吐量	当前是否活跃
10.11.33.177:4613	192.168.21.243:1521	WORKGROUP...	82	24	0B	0B	0	否
10.11.33.177:4204	192.168.21.243:1521	WORKGROUP...	164	37	0B	0B	0	否
10.11.33.177:4197	192.168.21.243:1521		0	3	0B	0B	0	否

显示 1 - 3，共 3 条 C < 1 > 10 条/页 跳至 页

4 资产

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。

4.1 资产管理

添加资产后，系统可对资产进行安全审计。添加资产的方法包括手动添加和资产自发现两种方式。

4.1.1 添加资产

手动添加资产包括单个添加和批量导入两种方式。

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

步骤 2. 在弹出的**添加资产**页面编辑相关信息。

详细配置项和说明请参见下表。

配置项	说明
保存时启用推荐的规则	勾选此选项，则保存时添加的资产会使用系统推荐的规则；不勾选此选项，保存时添加的资产不会使用系统推荐的规则。有关内置推荐的规则的更多信息，请参考规则配置。
类型	设置资产类型，包括关系型、非关系型、大数据、图形、全文、文档、键值、其他八个大类。
资产组	设置资产所隶属的资产组，有关资产组的更多信息请参考资产组管理。
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 及端口号。

- 本地运维行为审计是指通过安装本地 Agent 捕获本地数据库客户端程序中实际响应的 SQL 指令，实现对本地运维人员数据库操作行为的审计，支持 Oracle、PostgreSQL、MySQL、

SQL Server 等主流数据库。

- 当使用本地运维行为审计方式时，需要添加回环 IP 地址 127.0.0.1 和端口号，端口号需根据数据库类型进行填写。
- 如果使用的 IP 类型为 IPv6，IP 地址需填写为::1。

步骤 3. 如需配置其他更多信息，可点击<**更多配置**>，选择单向审计或双向审计，设置加密协议审计。

详细配置项和说明请参见下表。

配置项	说明
流量方向	◆ 单向审计：审计内容包括请求信息、客户端信息、服务端信息，不包括返回结果集。 ◆ 双向审计：审计内容包括请求信息、客户端信息、服务端信息、返回结果集。
保持行数	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	取值范围：1~64KB，确保整行显示。
解密私钥	加密协议导入解密私钥，目前支持 MySQL、SQL Server、HTTPS 加密解析，证书支持导入和编辑两种方式。
证书密码	安全证书的密码。

步骤 4. 点击<**保存**>。

资产添加之后，需要确认部署模式。若选择流量代理模式，需要部署 Agent 程序才能完成数据审计，具体请参见 Agent 管理。

4.1.2 编辑资产

编辑资产的操作方法如下所示。

步骤 1. 在**资产管理**页面，选择**资产管理**页签，点击资产列表右边的<**编辑**>。

步骤 2. 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和说明。

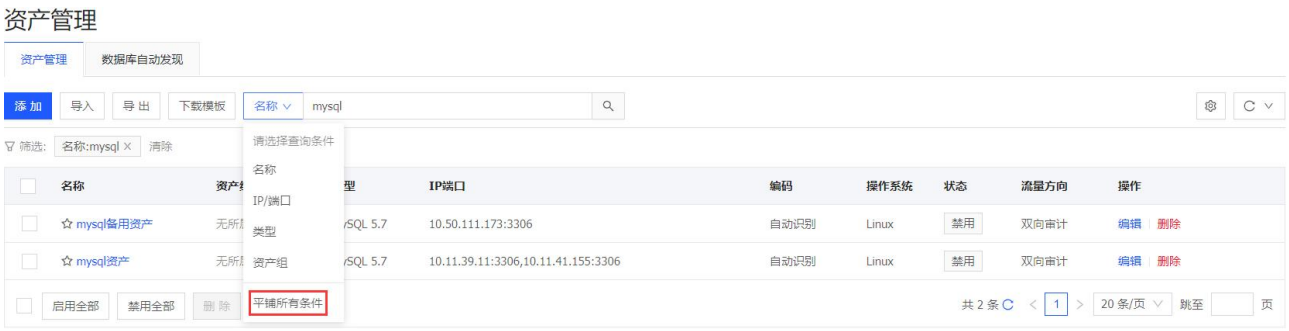
步骤 3. 编辑完成后点击<**完成**>按钮即可完成对资产的编辑.

4.1.3 查询资产

查询资产的操作方法如下所示。

步骤 1. 在**资产管理**页面，选择**资产管理**页签，选择查询条件（包括名称、IP/端口、类型和资产组）填写查询内容即可完成单个条件的查询。

步骤 2. 鼠标移到名称查询条件展开下拉列表，再点击<**平铺所有条件**>可以展开所有查询条件。



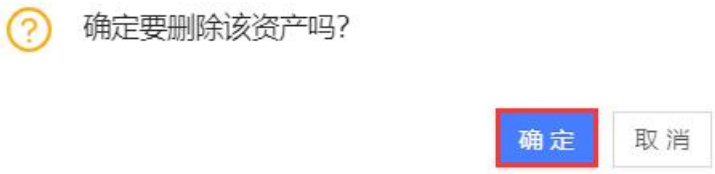
步骤 3. 可以同时输入名称、IP/端口、类型和资产组四个条件进行查询。点击<**收起查询条件**>可以恢复到默认的展示样式。

4.1.4 删除资产

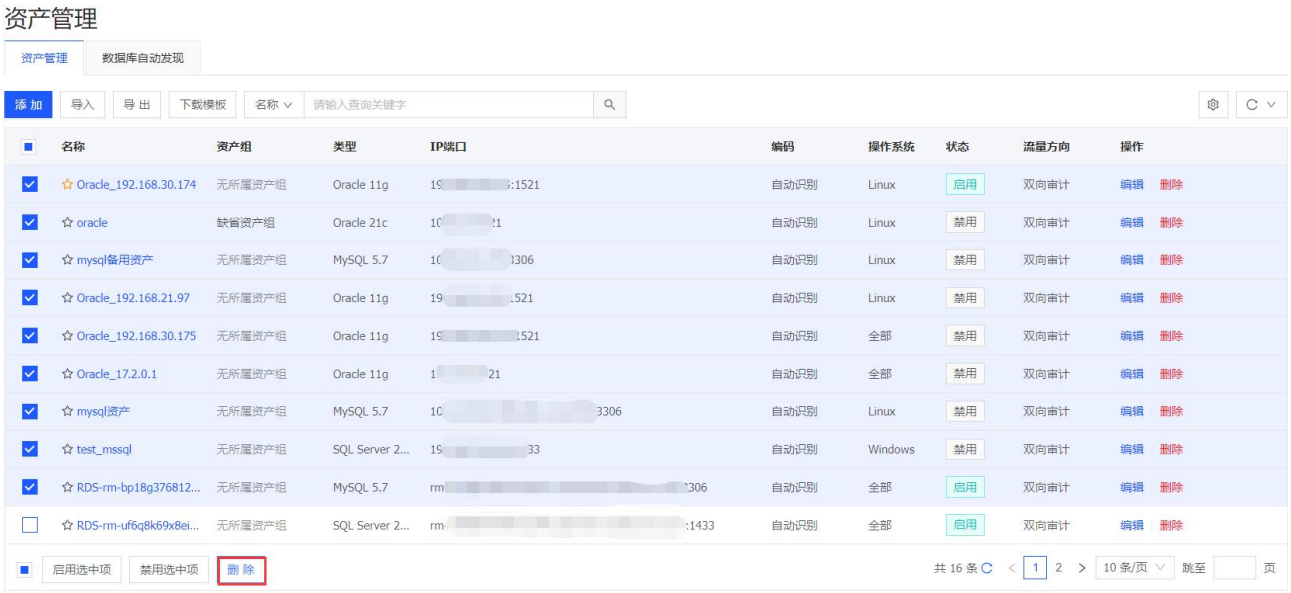
删除资产的操作方法如下所示。

步骤 1. 在**资产管理**页面，选择**资产管理**页签，点击资产列表右边的<**删除**>。

步骤 2. 弹出二次确认模态框，点击<**确定**>即可删除该资产。



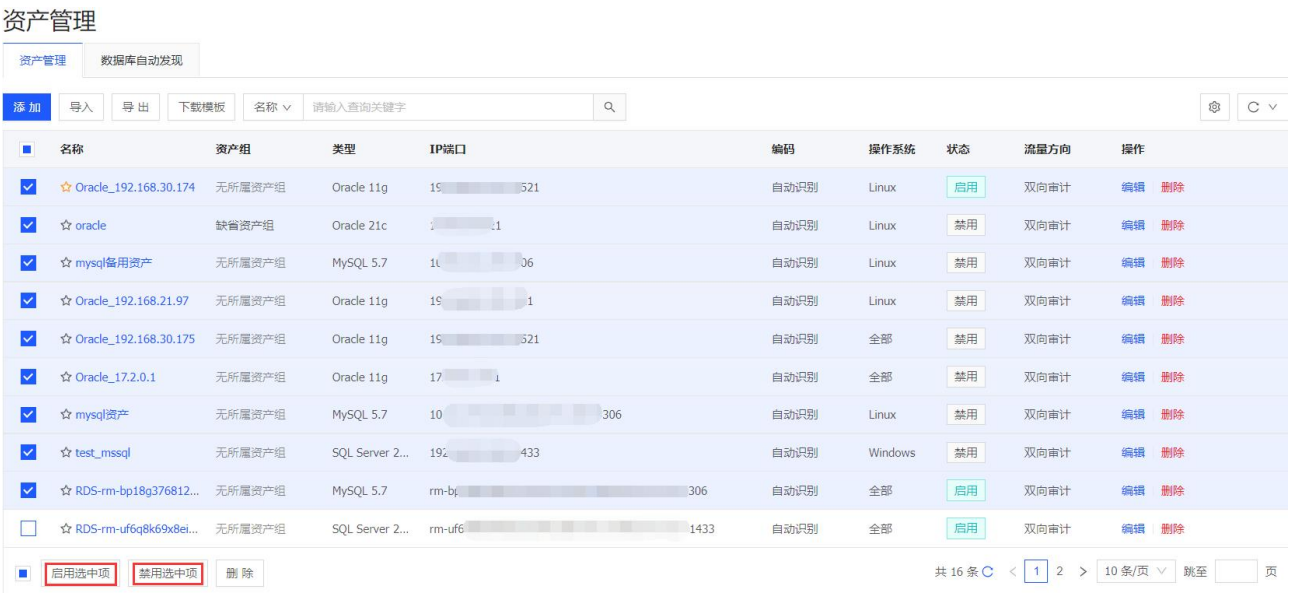
步骤 3. 选中资产列表前方的复选框，点击列表下方的<**删除**>按钮，二次确认页面点击<**确定**>，完成批量删除资产。



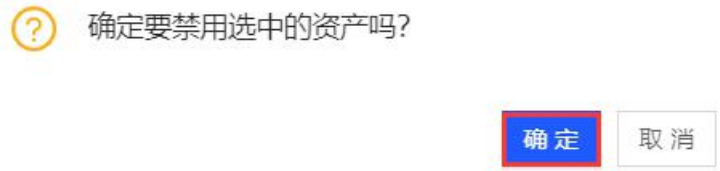
4.1.5 启用禁用资产

启用禁用的操作方法如下：

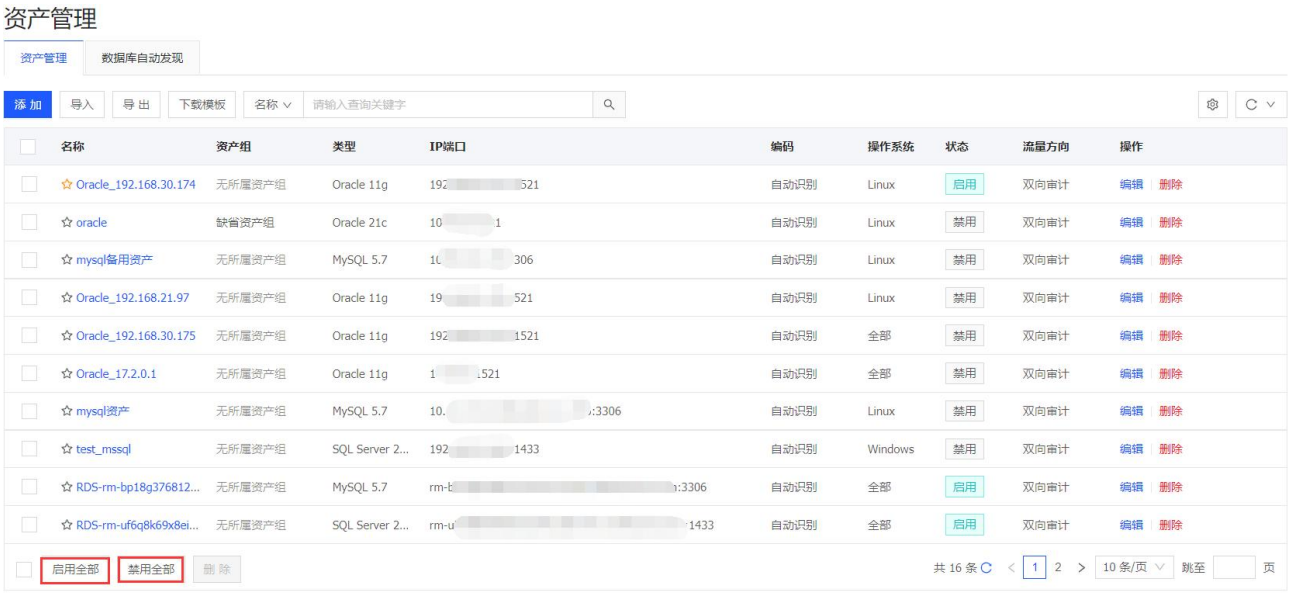
步骤 1. 选中资产列表前方的复选框，点击列表下方的<**启用选中项**>或者<**禁用选中项**>按钮。



步骤 2. 二次确认页面点击<**确定**>即可完成对选中资产的启用或者禁用。



步骤 3. 不选中资产列表前方的复选框，可以点击资产列表下方的<**启用全部**>或者<**禁用全部**>按钮对所有资产进行启用或者禁用。



4.1.6 导出导入资产

导入导出资产的操作方法如下：

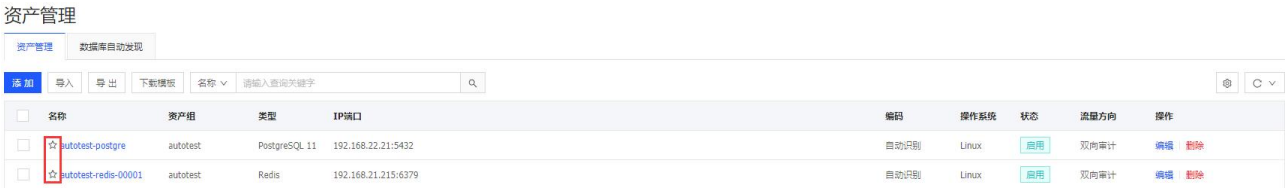
步骤 1. 点击<**下载模板**>，将模板文件下载至本地。

步骤 2. 编辑模板文件并保存。点击<**导入**>，选择编辑好的模板文件，即可批量导入资产。

步骤 3. 点击<**导出**>可以导出全部资产。

4.1.7 关注资产

关注资产是指当前用户较为关心的资产。点击资产名称左侧的☆图标即为关注此资产，关注后此资产会置顶；再次点击☆图标可取消关注，该资产会回到原来的位置。



4.1.8 资产自发现

资产自发现是指系统能自动发现数据包中包含的资产信息。资产自发现的原理是通过识别镜像流量中的数据库协议特征和知名端口信息，确认需要被审计的数据库资产的类型和版本。

可将系统自发现的资产添加到资产组中，操作方法如下：

在菜单栏选择“**资产➤资产管理**”进入**资产管理**页面，选择**数据库自动发现**页签，设置查询条件（IP、类型、端口、时间范围），点击<**搜索**>可进行资产查询。

- 在数据库列表**操作**列中点击<**添加到现有资产**>可将该资产添加到现有资产中，点击<**添加到新资产**>可将该资产添加到新建资产中。

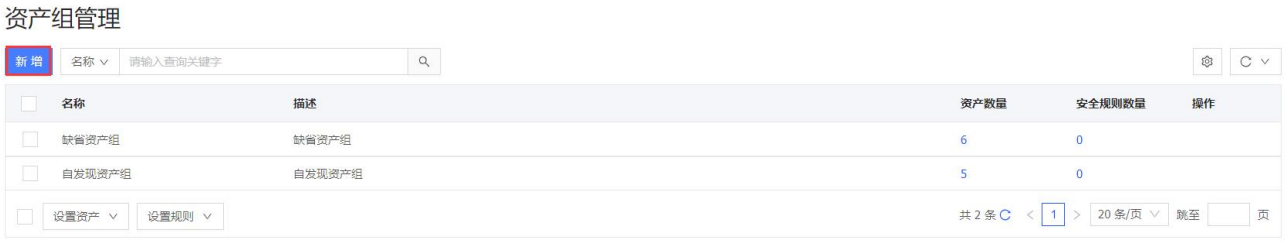
- 点击<**忽略**>，可将资产移动至**已忽略数据库**列表中。
- 点击<**修改**>可修改资产自动发现配置（选择“**启用**”时，可设置启用资产自发现功能的生效时长）。

4.2 资产组管理

资产组是具有相同或相似属性资产的集合，例如 A 单位有 3 个信息系统，可以将不同信息系统中的数据库资产绑定在不同的资产组内，通过资产组可以方便地进行资产管理、报表查看和数据分析。系统默认的资产组包括自发现资产组和缺省资产组。

- **添加资产组**

步骤 1. 在菜单栏选择“**资产➤资产组管理**”进入**资产组管理**页面，可查看资产组信息。点击 图标设置资产组列表的显示列；点击 图标设置资产组列表的刷新间隔。



步骤 2. 点击<**新增**>，在弹出的**新增资产组**对话框中编辑名称（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），点击<**确定**>。

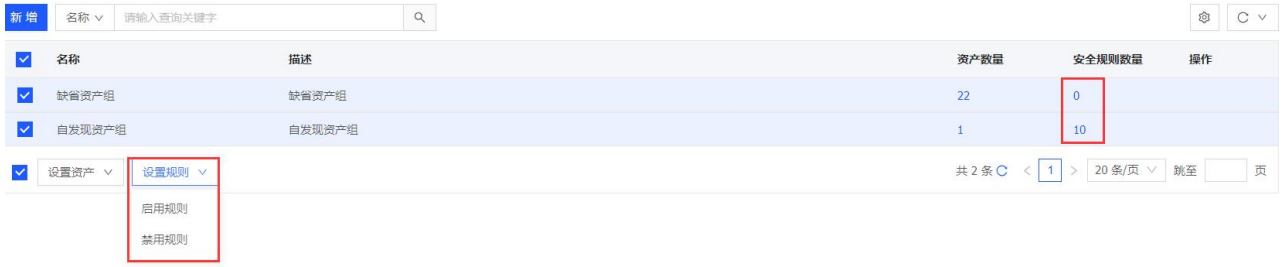
◆ **设置资产**

- 选择任意资产组，点击资产数量列的数字或勾选资产组列表前面的复选框，点击**设置资产**下的<**添加资产**>，可以设置属于该资产组的资产。
- 勾选资产组列表前面的复选框，点击**设置资产**下的<**移除资产**>或点击资产数量列下的数字，取消勾选资产列表前面的复选框，可以将资产移除至资产组。

◆ **设置规则**

- 选择任意资产组，点击安全规则数量列的数字或勾选资产组列表前面的复选框，点击**设置规则**下的<**启用规则**>，可以在资产组上设置安全规则。
- 勾选资产组列表前面的复选框，点击**设置规则**下的<**禁用规则**>或点击安全规则数量列下的数字，取消勾选安全规则列表前面的复选框，可以禁用该资产组所设置的安全规则。

资产组管理



5 查询分析

数据库审计支持从多个维度查看数据库的访问操作记录。

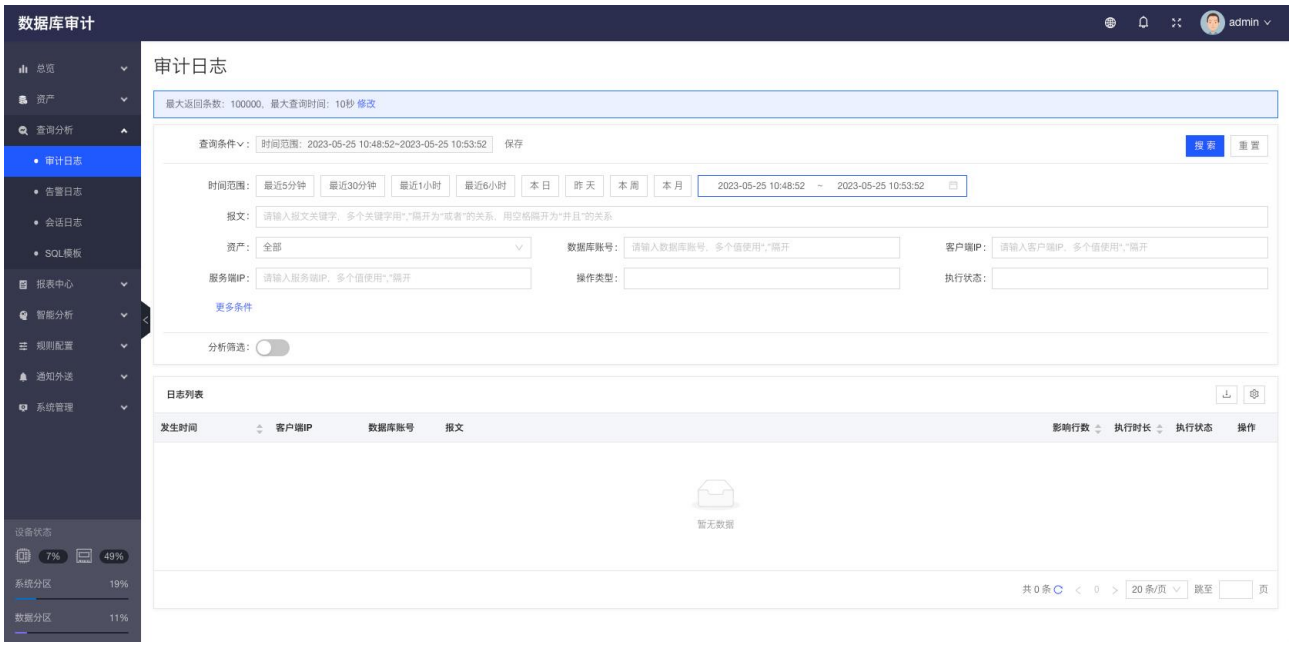
- 可以根据审计日志查询所有的访问行为。
- 通过告警日志查看可疑的访问行为。
- 通过会话日志可以查看每一次访问行为内所有的访问记录。
- 通过 SQL 模板查询 SQL 语句操作记录。

5.1 查询审计日志

数据库审计通过对双向数据包进行解析、识别以及还原，不仅可以对数据库操作请求进行实时审计，还可对数据库系统返回结果进行完整的还原和审计。包括 SQL 报文、数据库命令执行时长、执行的结果集、客户端工具、客户端 IP 地址、服务端端口、数据库账号、对象、执行状态、数据库类型以及报文长度等内容。

5.1.1 搜索审计日志

在菜单栏选择“**查询分析➤审计日志**”进入**审计日志**页面，选择**审计日志**页签，设置查询条件（时间范围、报文、资产、数据库账号、客户端 IP、服务端 IP、操作类型、执行状态等），点击**<搜索>**即可查询相关审计日志。



◆ 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。

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	唯一标识审计记录的 ID。

选项	说明
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	可选择资产组或资产，资产组和资产可多选和混合选择，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。
客户端 MAC	客户端的 MAC 地址。
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。
服务端 MAC	服务端的 MAC 地址。
数据库名/实例名	数据库名称或者实例名称。
对象	数据库的库、表、字段、视图、存储过程、函数、触发器、索引、用户、角色、权限等数据库对象
客户端工具	客户端工具名称。
主机名	客户端主机名称。
操作系统用户名	客户端所在操作系统的用户名。
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。
执行结果描述	SQL 语句执行完成后的结果描述，如：ORA-00942: table or view does not exist。
返回结果集	Select 等语句执行后产生的返回结果集。默认保存 5 行数据，最大保存长度 64KB。 可在**资产管理**页面，点击<**编辑资产**>，修改保存行数和最大保存长度。
关联 IP/账号	关联用户的客户端 IP 和账号。

选项	说明
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。

◆ **设置查询结果显示列**

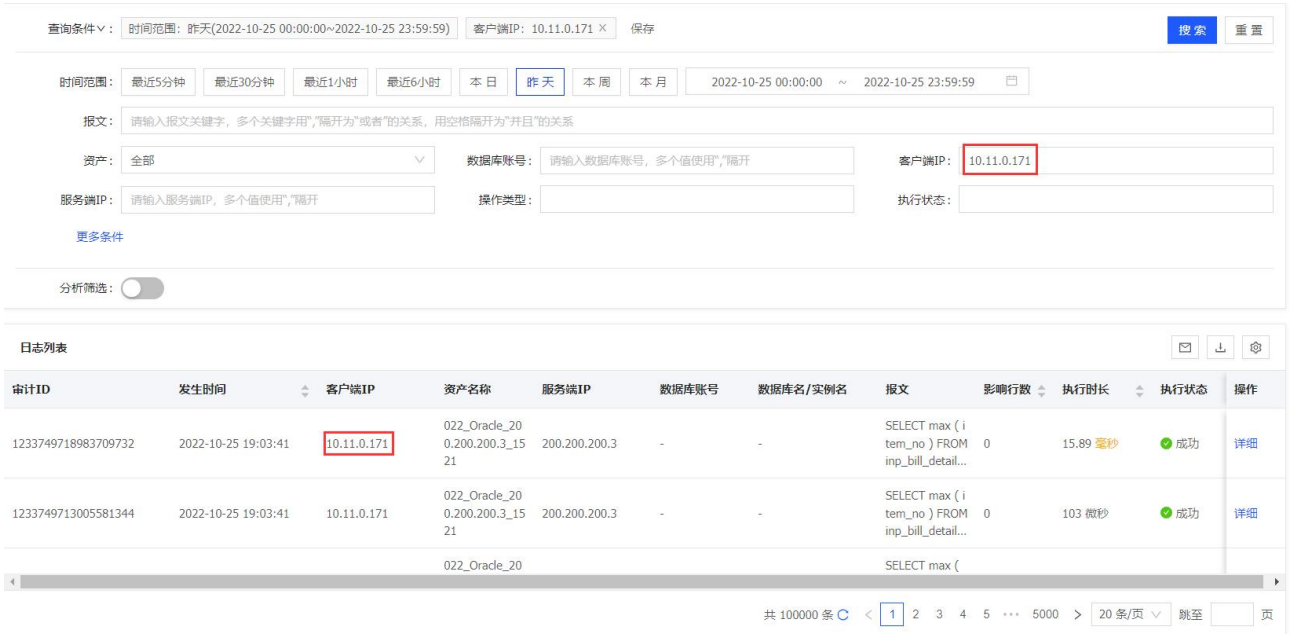
点击 图标，即可设置查询结果的展示列。

◆ **导出查询结果**

点击图标，可将查询结果导出至本地。

5.1.2 在查询结果中添加查询条件

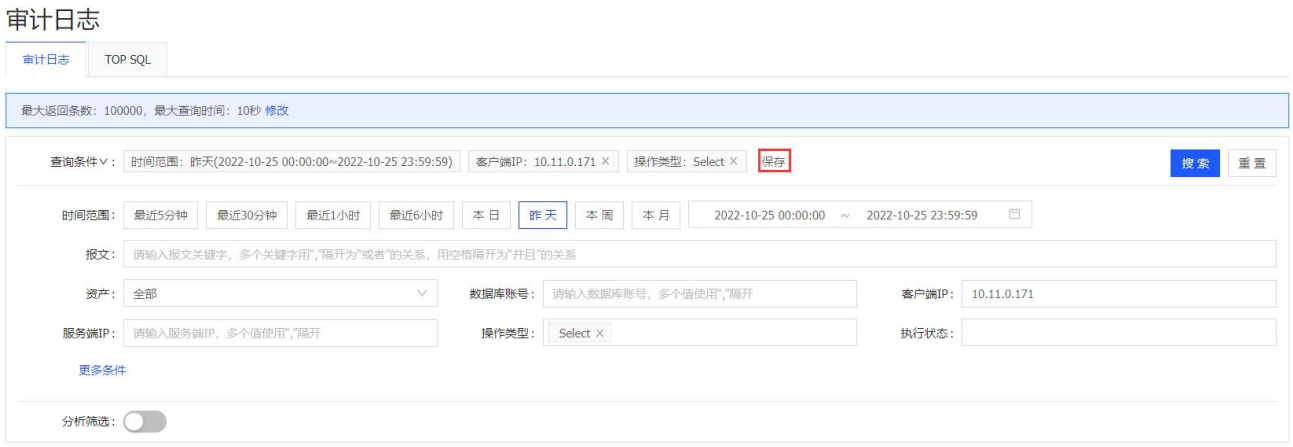
查询结果的会话 ID、客户端 IP、客户端工具、主机名、操作系统用户名、服务端 IP、数据库账号、数据库名/实例名、关联 IP、关联账号，可以通过点击以上列的内容实现添加到查询条件并进行查询。



5.1.3 保存查询条件

可对查询条件进行保存，方便后续查询，操作方法如下：

步骤 1. 点击**查询条件**文本框中的<**保存**>。

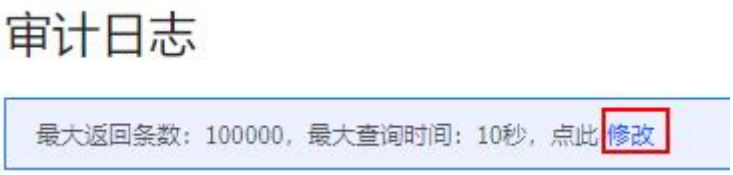


步骤 2. 在弹出的**保存查询条件**对话框中编辑名称（必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符），点击<**确定**>。

点击**查询条件**后的图标，可查看已保存的查询条件。

5.1.4 修改查询配置

步骤 1. 在**审计日志**页面，点击<**修改**>。



步骤 2. 在弹出**修改查询配置**对话框中编辑相关信息，点击<**确定**>。

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：1~1,000,000，默认为 100,000。
最大查询时间	最大查询时长，取值范围：1~3,600，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。

5.1.5 查看审计日志详细

在查询结果列表中，在**操作**列下点击**<详细>**，可查看审计日志的详细信息。

点击客户端 IP 右边的<**设置别名**>,可以带着 IP 跳转到新增或者编辑 **IP 别名**页面。

点击数据库账号右边的<**设置别名**>,可以带着数据库账号跳转到新增或者编辑**账号别名**页面。

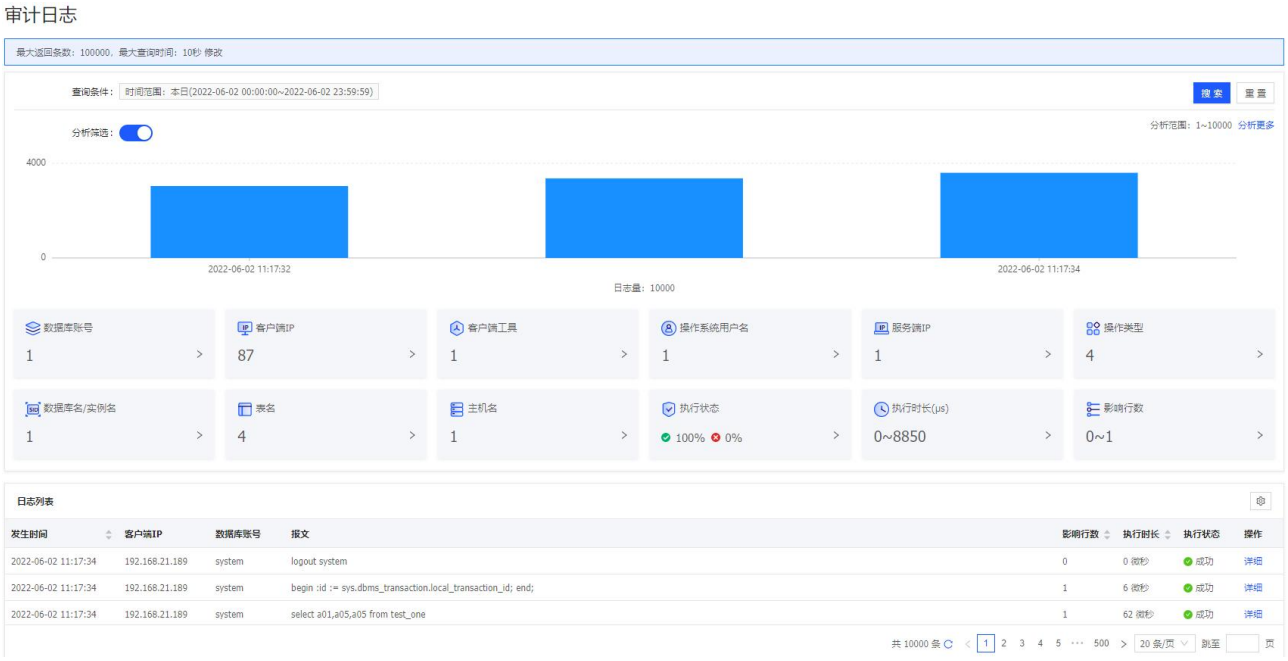
点击<**C/S 应用用户名提取**>，弹出**新增 C/S 应用身份识别配置**对话框，包括设置资产、SQL 模板、以及参数的位置，点击<**确定**>。设置 C/S 应用用户名提取后，该设置将新增至 C/S 应用身份识别列表中。详情请参见 C/S 应用身份识别。

在审计日志详情页面右下角点击<**取证**>弹出**下载**对话框，可下载本条审计日志详情的完整页面。点击<**上一条**>或<**下一条**>可切换至临近的审计日志。

在审计日志详情页面的请求部分，点击<**SQL 模板**>可查看该报文的 SQL 模板，点击<**过滤改模板**>可以将该 SQL 模板添加过滤条件，也可以将已经添加为过滤条件的 SQL 模板取消过滤。详情请参见按 SQL 模板过滤。

5.1.6 分析筛选

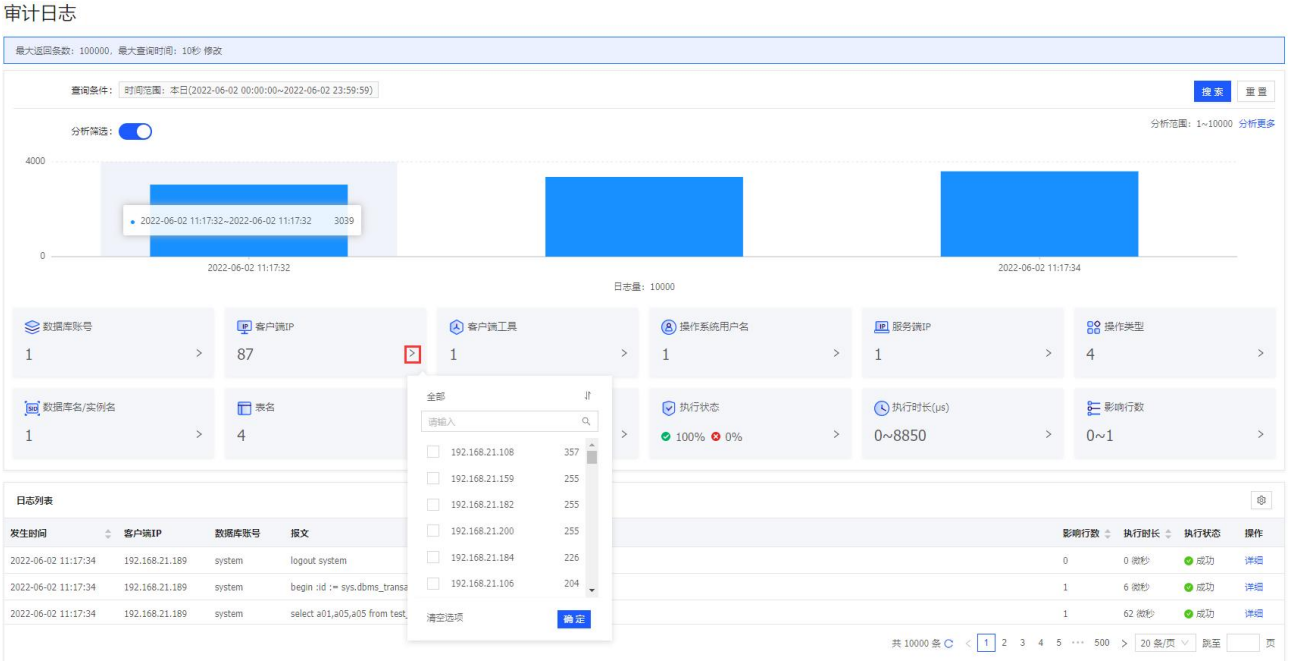
在**审计日志**页面，启用**分析筛选**开关，可以对已查询的审计日志结果进行分析和二次查询。



每次分析拉取 1 万条审计日志进行分析，如果超过 1 万条可点击<**分析更多**>再拉取 1 万条审计日志与上一万条审计日志一起进行分析。

柱状图显示在分析范围内的审计日志在时间上的分布情况。

点击任一维度（如“客户端 IP”）的>图标，在弹出的对话框中可以查看该维度的审计日志分布情况。勾选对应内容，点击<**确定**>，即可进行二次查询。



分析维度请参见下表。

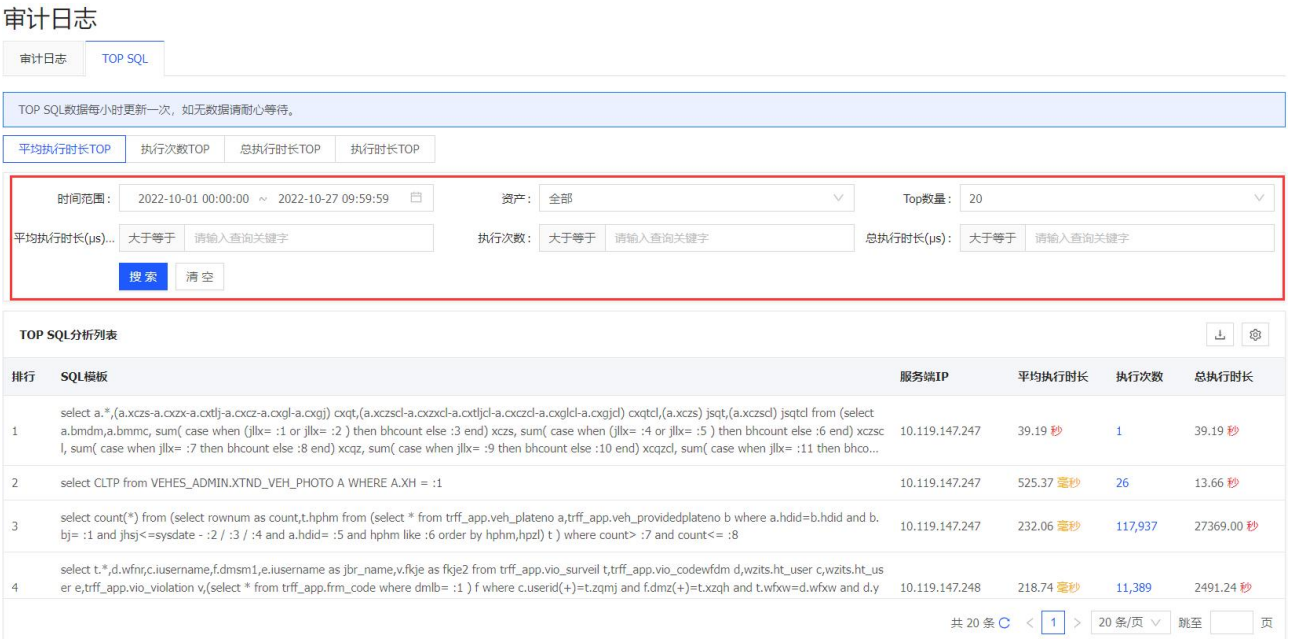
分析维度	说明
数据库账号	对首次查询结果根据数据库账号维度进行统计。
客户端 IP	对首次查询结果根据客户端 IP 维度进行统计。
客户端工具	对首次查询结果根据客户端工具维度进行统计。
操作系统用户名	对首次查询结果根据操作系统用户名维度进行统计。
服务端 IP	对首次查询结果根据服务端 IP 维度进行统计。
操作类型	对首次查询结果根据操作类型维度进行统计。
数据库名/实例名	对首次查询结果根据数据库名/实例名维度进行统计。
表名	对首次查询结果根据表名维度进行统计。

主机名	对首次查询结果根据主机名维度进行统计。
执行状态	对首次查询结果根据执行状态维度进行统计。
执行时长	对首次查询结果根据执行时长维度进行统计。
影响行数	对首次查询结果根据影响行数维度进行统计。

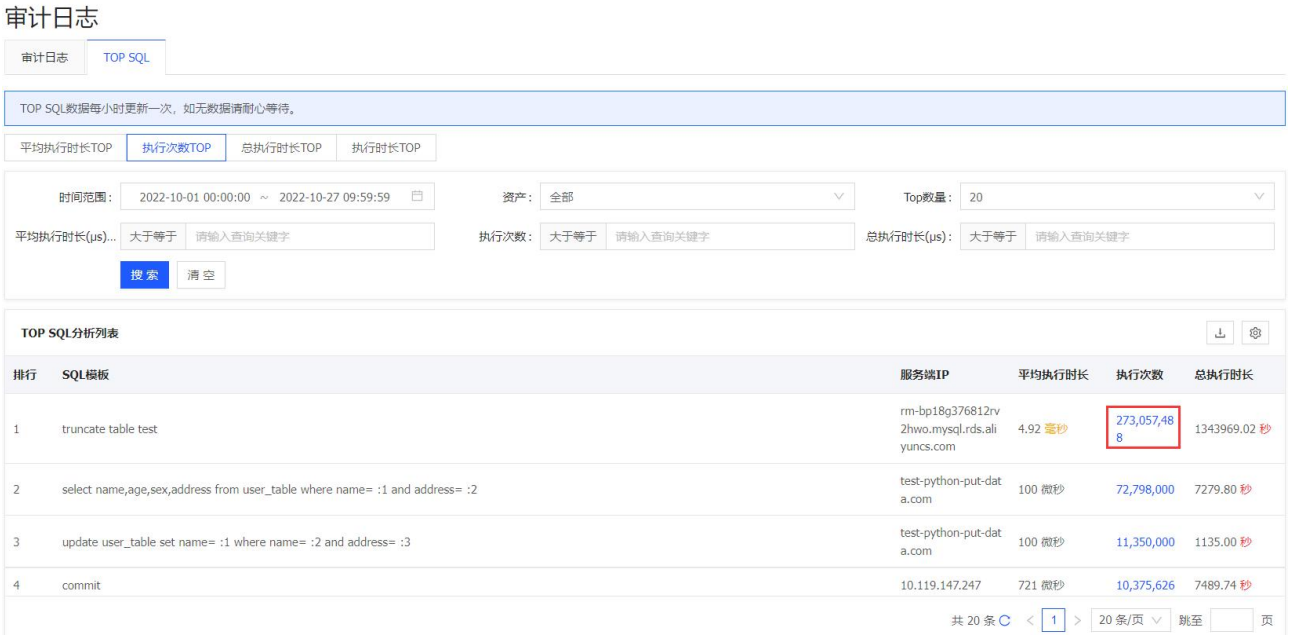
5.1.7 TOP SQL

数据库是较大型的应用，对于繁忙的数据库，需要消耗大量的内存、CPU、IO、网络资源。SQL 优化是数据库优化的手段之一，而为了达到 SQL 优化的最佳效果，您首先需要了解最消耗资源的 SQL（Top SQL）。

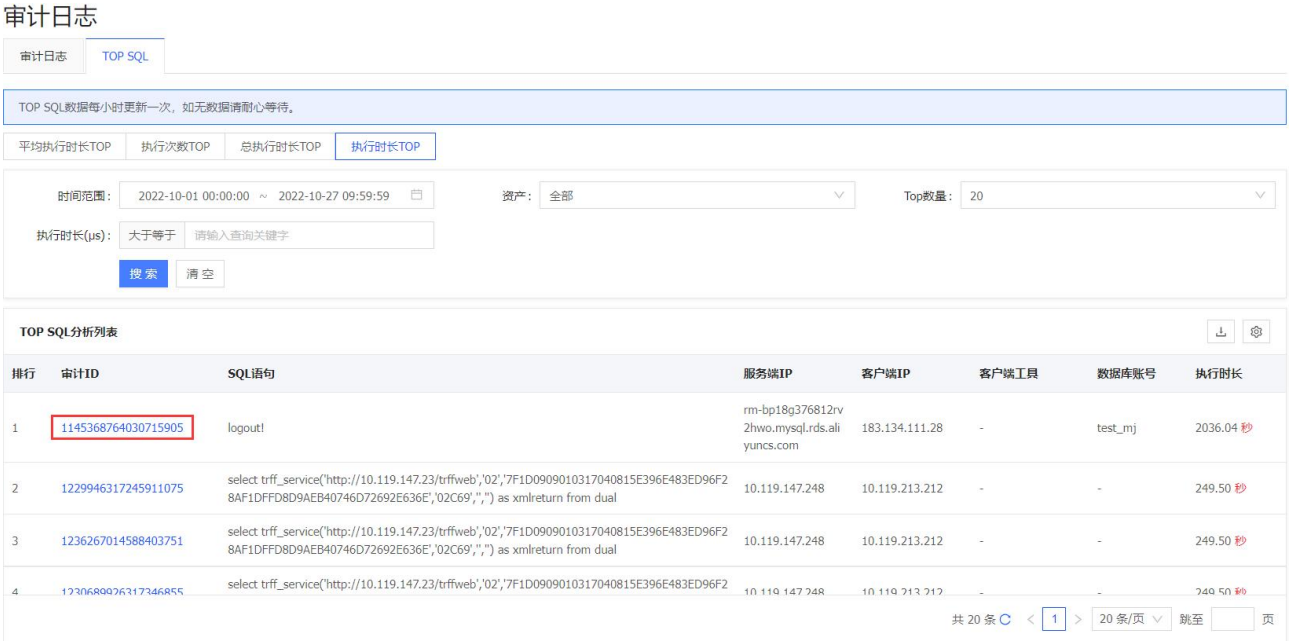
在菜单栏选择“**查询分析➤审计日志**”进入**审计日志**页面，选择 **TOP SQL** 页签，可设置过滤条件（时间范围、资产、Top 数量、平均执行时长、执行次数、总执行时长），查询符合过滤条件的 TOP SQL 信息。



在**平均执行时长 TOP**、**执行次数 TOP** 和**总执行时长 TOP** 的 TOP SQL 分析列表中点击执行次数对应的显示列，可以跳转到**审计日志**页面。



在**执行时长 TOP** 的 TOP SQL 分析列表中，点击审计日志 ID 可以跳转到**审计日志**页面查看更详细的日志信息。



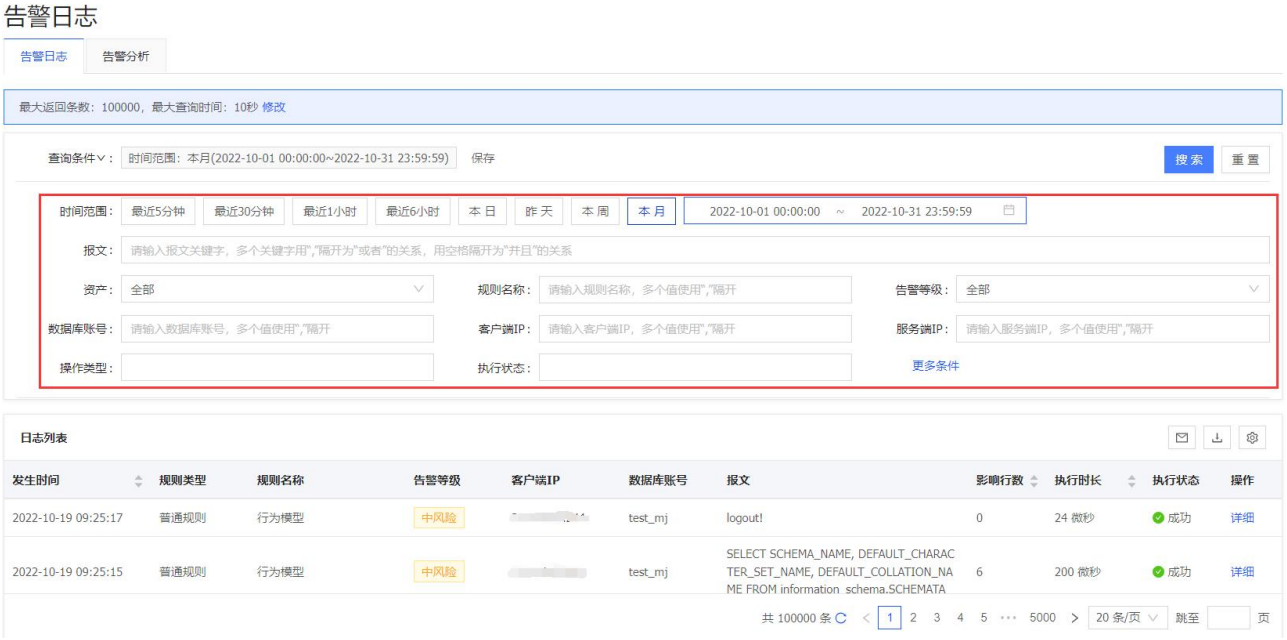
5.2 查询告警日志

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。

5.2.1 告警日志

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，选择**告警日志**页签，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。



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、响应详情。

当触发的规则为统计规则告警时，需要进入**告警详情**页面才能查看客户端、服务端等信息。统计规则是根据不同维度来对多条审计日志进行统计展示，存在多条日志客户端 IP/连接工具/数据库类型/SQL 模板一致但报文等信息不一致的情况，所以必须进入至**告警详情**页面才可查看。

在**告警日志**页面，点击统计规则告警项操作列的**<详细>**，进入**告警日志详细**页面，点击**<统计数据>**，可查看客户端、数据库账号等信息。

5.2.2 告警分析

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，选择**告警分析**页签，可设置过滤条件（时间范围、规则名称、资产、数据库账号、客户端 IP），查询符合过滤条件的告警信息。

步骤 2. 点击**操作**列下的<**详情**>，可查看告警统计详情，包含规则详情、告警资产、各资产下的告警趋势、告警来源（维度包含客户端 IP 和数据库账号）和触发告警的 SQL 模板。

步骤 3. 在**规则详情**区域点击资产数量链接可编辑已启用该规则的资产，点击白名单数量链接可以编辑该规则上启用的白名单。

步骤 4. 在**告警资产**区域点击**规则启用状态**开关可以变更规则在某资产上的启用状态。

步骤 5. 在**告警来源**区域，点击**操作**列下的<**不再告警**>。

步骤 6. 在弹出的**不再告警**对话框中编辑相关信息，点击<**确定**>。

将满足条件的客户端 IP 添加到信任规则和添加到规则白名单。对于普通规则产生的告警，选择<**添加到白名单**>，点击<**确定**>。添加为白名单后，系统对于此规则符合选中项的条件的相关操作不再产生告警。

选择<**添加到信任规则**>，点击<**确定**>。添加为信任规则后，对于资产符合信任规则可选属性的将不再发生告警。

步骤 7. 在**触发告警的 SQL 模板**区域，点击**操作**列下的<**不再告警**>。

步骤 8. 在弹出的**不再告警**对话框中编辑相关信息，点击<**确定**>。

将满足条件的 SQL 模板添加到信任规则和添加到规则白名单。对于普通规则产生的告警，选择<**添加到白名单**>，点击<**确定**>。添加为白名单后，系统对于此规则符白名单的条件的相关操作不再产生告警。

选择<添加到信任规则>，点击<**确定**>。添加为信任规则后，对于资产符合信任规则的行为将不再发生告警。有关规则的更多信息，请参考规则配置。

5.3 查询会话日志

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。

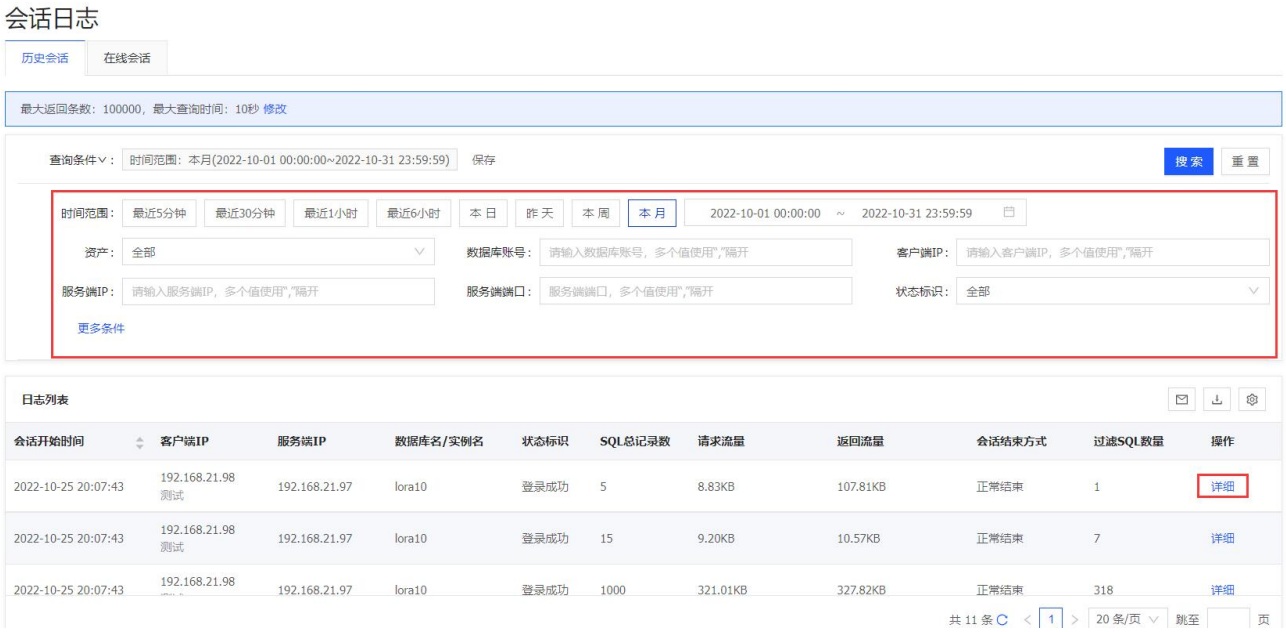
可以根据会话的状态将其分成在线会话和历史会话。

- 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。

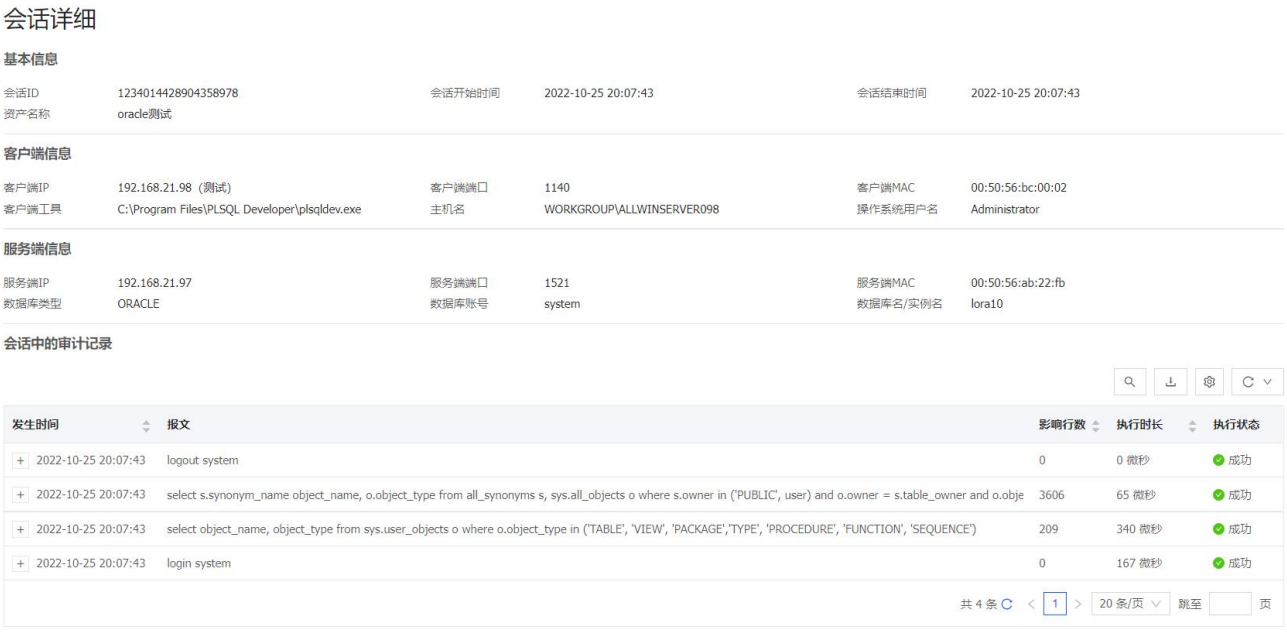
会话的基本四元素是指客户端 IP、客户端端口、服务端 IP 和服务端端口。会话的四元素可以定位在同时刻的唯一会话信息。系统支持查看历史会话和在线会话，并支持通过会话信息查看一次会话过程中产生的所有请求或响应日志。

5.3.1 查询历史会话

在菜单栏选择“**查询分析➤会话日志**”进入**会话日志**页面，选择**历史会话**页签，设置查询条件（如时间范围、资产等），点击**<搜索>**即可查询相关历史会话。

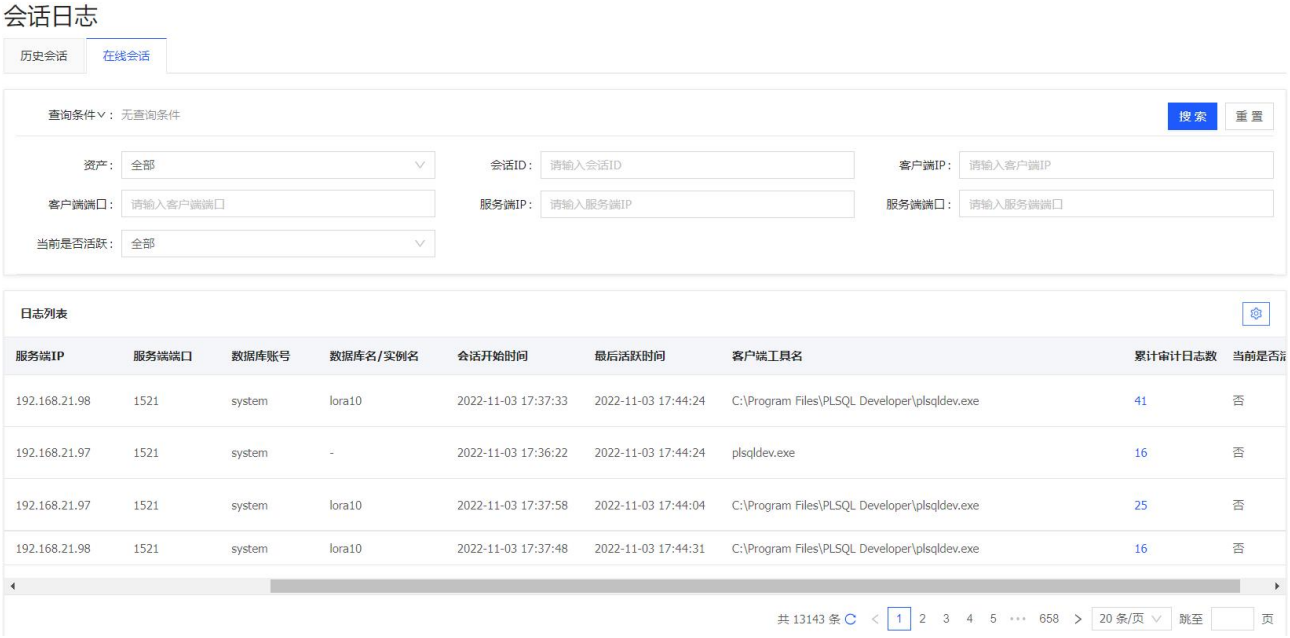


点击**操作**列中的**<详细>**可查看会话详情。



5.3.2 查询在线会话

在**会话日志**页面，选择**在线会话**页签，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。



点击**累计审计日志数量**列对应的数字可跳转到**审计日志**页面查看属于该会话的日志。

5.4 查询 SQL 模板

SQL 模板（SQL Template）是去参数化的 S QL 语句。系统支持将访问数据库系统的 SQL 语句使用的模板信息提取并存储到磁盘中，用户可以通过 Web 页面查看 SQL 模板集合。通常认为应用在访问数据库时使用的模板是固定的，如果出现了新的 SQL 模板，可以怀疑是否是存在异常访问行为。

系统可对审计结果去参数化的 SQL 模板进行查询，操作方法如下：

- SQL 模板默认为开启状态，如需关闭 SQL 模版，需要点击<**修改**>，弹出 **SQL 模版数量上限配置**对话框，关闭 SQL 模板收集开关，关闭后 SQL 模板数量将不在增加。

◆ 系统可对审计结果去参数化的 SQL 模板进行查询。

在菜单栏选择“**查询分析➢SQL 模板**”进入 **SQL 模板**页面，设置查询条件（如时间范围、SQL 模板等），点击<**搜索**>即可查询相关 SQL 模板。

◆ 当前版本一次最多可查询展示 10,000 条记录。

◆ SQL 模板数量默认最大为 30 万条，点击<**修改**>修改此配置。

◆ 在 SQL 模板列表中点击<**详细**>可以查看该 SQL 模板记录的详细信息，包括基本信息、模板、首次发生报文、不审计匹配的报文和数据库信息。其中请求详情中可以查看报文，返回详情可以查看 SQL 语句的返回信息。

SQL模板详情

基本信息

服务端ip	192.168.2.3	操作类型	Do
模板ID	655096106115265290	首次发生时间	2022-06-02 01:43:14

模板 | 首次发生报文 | SQL模板

```
do ##class(web.DHCRisApplication).UpPrint2( :1 ,"13965147|:2",:3",:4")
```

数据库信息

数据库名称	autotestCachenew	数据库类型	Cache

IP端口：192.168.30.249:57772 | 10.1.12.3:1972 | 10.1.12.2:1972 | 192.168.245.1:1972 点击显示其余ip端口

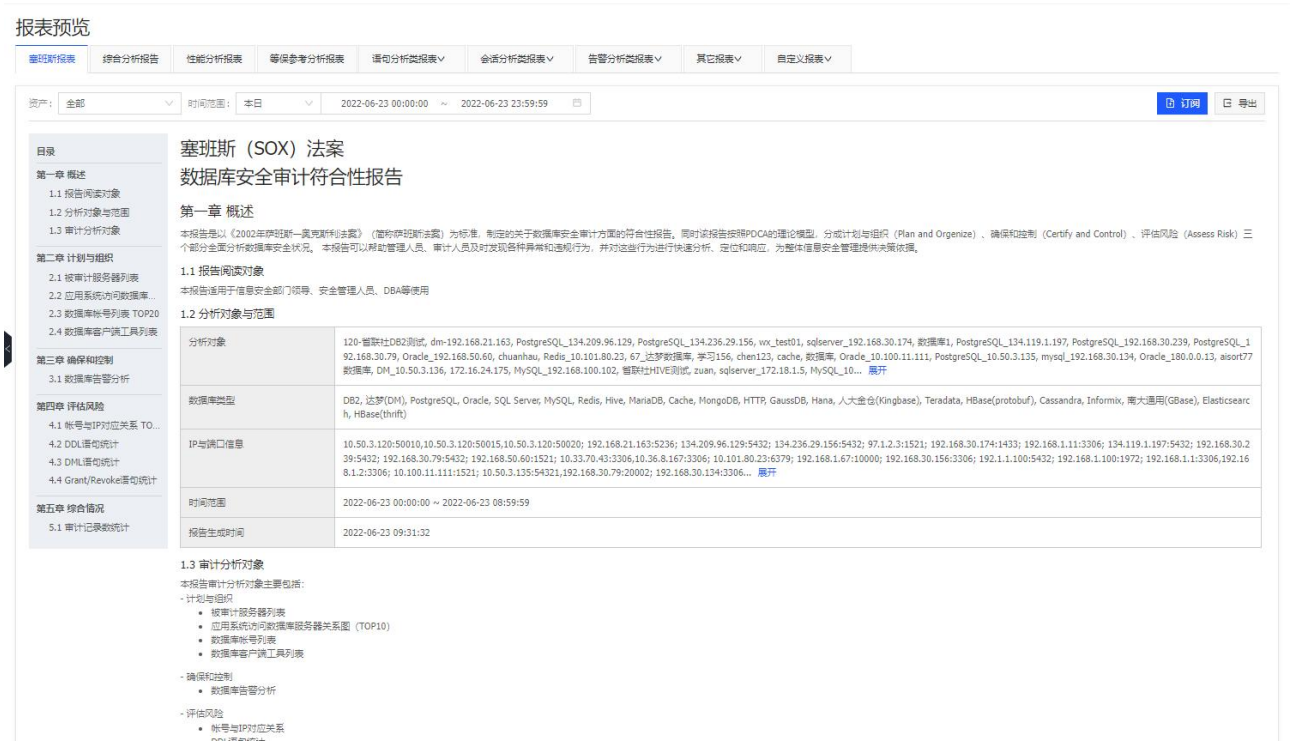
6 报表中心

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日志、告警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

报表预览展示系统各类型报表信息，操作方法如下：

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、资产或者资产组、报表时间范围，即可生成所需的报表文件。可以直接阅读已生成的报表，也可以点击右上角的**<导出>**，选择导出格式（HTML、PDF、PNG、WORD、EXCEL 和 CSV）即可将报表按指定文件格式导出至本地。



内置报表类型请参见下表。

报表类型	说明
塞班斯报表	从计划与组织、确保和控制、评估风险、综合情况四个方面，全面分析数据库安全状

报表类型	说明
	况。
综合分析报告	从 SQL 语句执行情况分析、会话连接分析、风险事件分析和 SQL 性能分析四个角度对数据库态势进行综合分析。
性能分析报表	从性能变化趋势、性能最差的数据库/SID、耗时最久的 SQL、性能最差的 SQL、执行最多的 SQL 五个方面对数据库的性能做出分析。
等保参考分析报表	紧密切合当前信息安全技术网络安全等级保护评测要求 GB/T 28448-2019（以下简称“等级保护 2.0”）的大趋势，针对等级保护 2.0 里关注的安全审计中的入侵防范、恶意代码监测、安全审计监控等进行针对性的分析和展示。
语句分析类报表	从 SQL 语句分析、失败语句分析、SQL 语句变化趋势、审计趋势分析和执行次数最多 SQL 模板分析 5 个维度分析和展示当前语句类的信息。
会话分析类报表	包含新增会话分析、失败会话分析、并发会话分析和会话数量变化趋势分析 4 张报表。
告警分析类报表	从告警变化趋势、告警来源分析、告警对象分析、规则命中分析 4 个维度分析当前告警的情况。
其他报表	主要分为：表分析、客户端工具分析、数据库账号分析、数据库/SID 分析、数据库访问来源 IP 分析、数据库/实例名访问分析 6 张报表。
自定义报表	用户自定义创建的报表，有关自定义报表的详细信息请参考自定义报表。

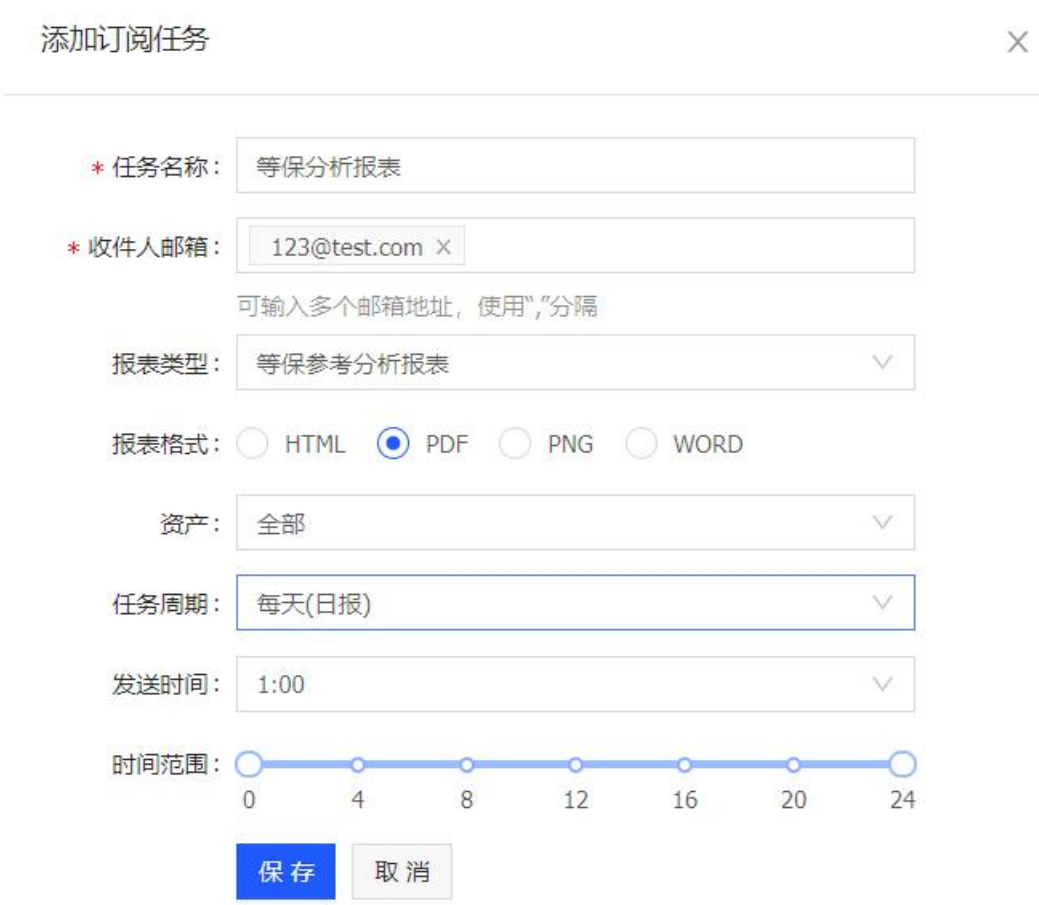
6.2 报表订阅

报表订阅实现根据需求周期性向指定对象定点发送报表的功能，配置方法有两种。

◆ 配置方法一

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，点击页面右上角的<**订阅**.>。

步骤 2. 进入**添加订阅任务**页面，编辑相关信息，点击<**保存**>。



详细配置项和说明请参见下表。

配置项	说明
任务名称	设置任务名称。必须为中文字符、字母、数字、下划线“_”、点“.”或短横线“-”，长度不超过 64 字符。
收件人邮箱	报表发送的接收人邮箱，可以设置多个。

配置项	说明
报表类型	选择报表类型。
报表格式	指定报表发送格式，支持 HTML、PDF、PNG 和 Word 四种格式，默认为“PDF”。
资产	指定要发送报表的资产，默认全部资产。
任务周期	选择任务周期（日报，周报，月报，年报），默认为“每天”。
发送时间	指定报表发送的时间。
时间范围	日报支持按小时进行外发（仅在任务周期选择“每天（日报）”时显示，只能选择连续的时间）。

◆ 配置方法二

步骤 1. 在菜单栏选择“**报表中心➤报表订阅**”进入**报表订阅**页面，点击<**添加**>。

步骤 2. 进入**添加订阅任务**页面，编辑相关信息（参数配置方法与配置方法一相同），点击<**保存**>。。

6.3 自定义报表

自定义报表，即用户可以自定义报表内容（包括文档架构以及报表数据）。

6.3.1 报表数据管理

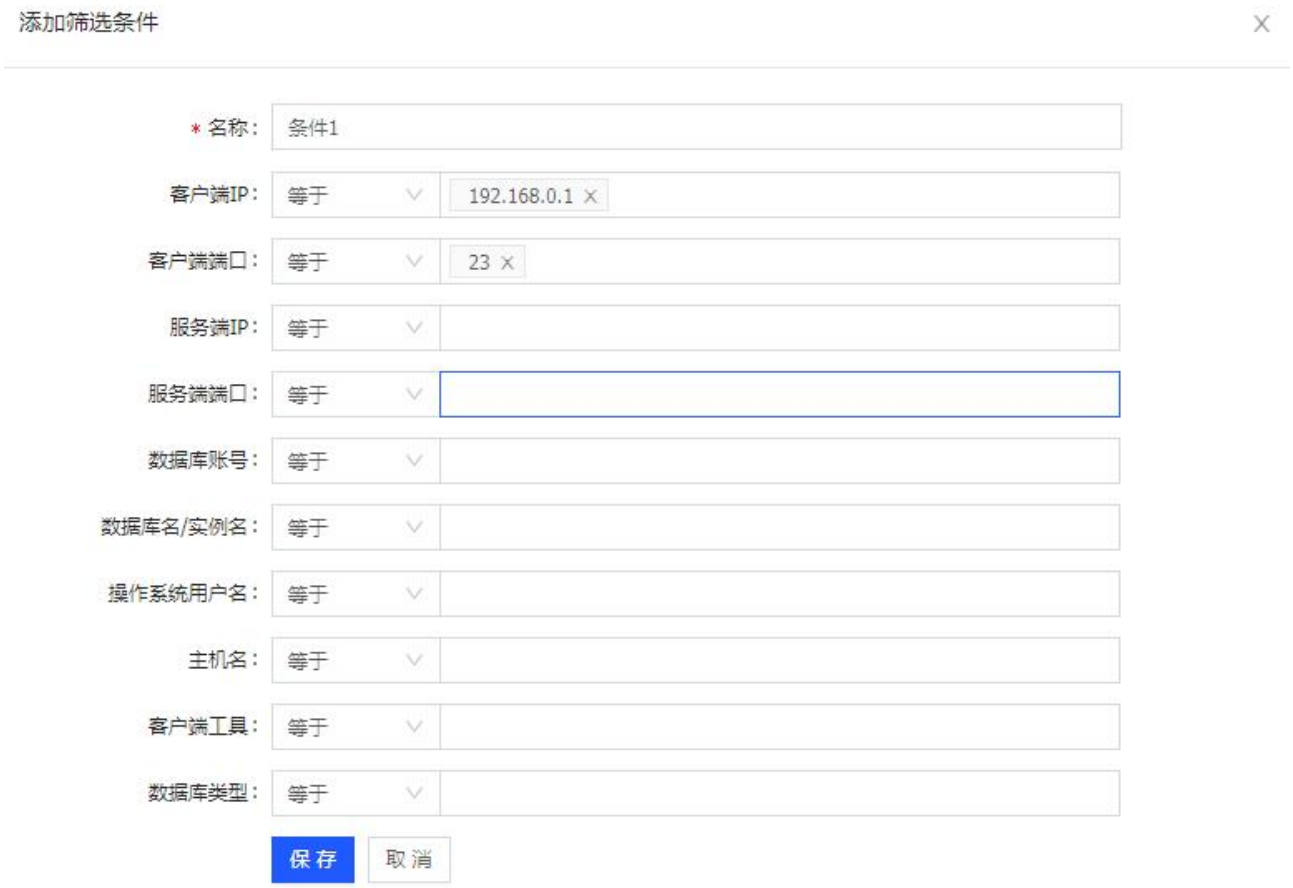
报表数据是自定义报表中展示的实际内容，是对告警日志、审计日志、会话日志从不同维度（例如客户端 IP、主机名等）进行统计分析。

6.3.1.1 添加报表数据

步骤 1. 在菜单栏选择“**报表中心➤自定义报表**”进入**自定义报表**页面，选择**报表数据管理**页签，点击<**添加**>。

步骤 2. 进入**添加报表数据**页面，编辑相关信息，点击<**保存**>。

1) 编辑名称（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）。
2) 选择统计维度和统计指标。
3) 设置筛选条件。点击<**添加**>。
4) 在弹出的**添加筛选条件**对话框中设置名称（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）和条件，点击<**保存**>。



5) 在**筛选条件**文本框中点击 图标，选择筛选条件。

6) 点击<**保存**>。

6.3.1.2 其他操作

- 在报表数据列表中点击**操作**列中的<**预览**>，可预览报表数据效果。
- 在报表数据列表中点击**操作**列中的<**编辑**>，可修改报表数据。
- 在报表数据列表中点击**操作**列中的<**删除**>，在弹出的对话框中点击<**确定**>，可删除报表数据。

如果报表数据已被自定义报表引用，需要先删除自定义报表后才能删除报表数据。

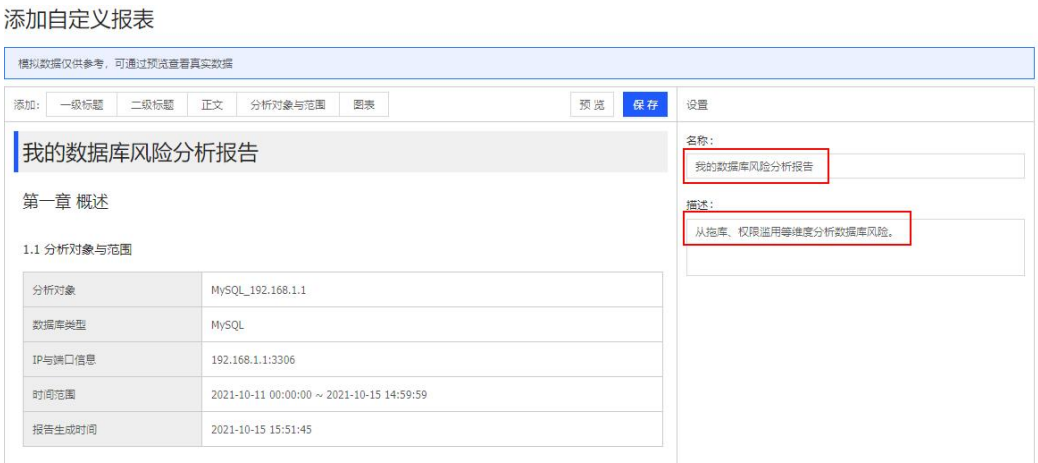
6.3.2 报表管理

自定义报表的内容包括一级标题、二级标题、正文、分析对象与范围、图表（即报表数据）。

6.3.2.1 添加自定义报表

步骤 1. 在菜单栏选择“**报表中心➤自定义报表**”进入**自定义报表**页面，选择**报表管理**页签，点击<**添加**>。

步骤 2. 进入**添加自定义报表**页面，编辑名称和描述。

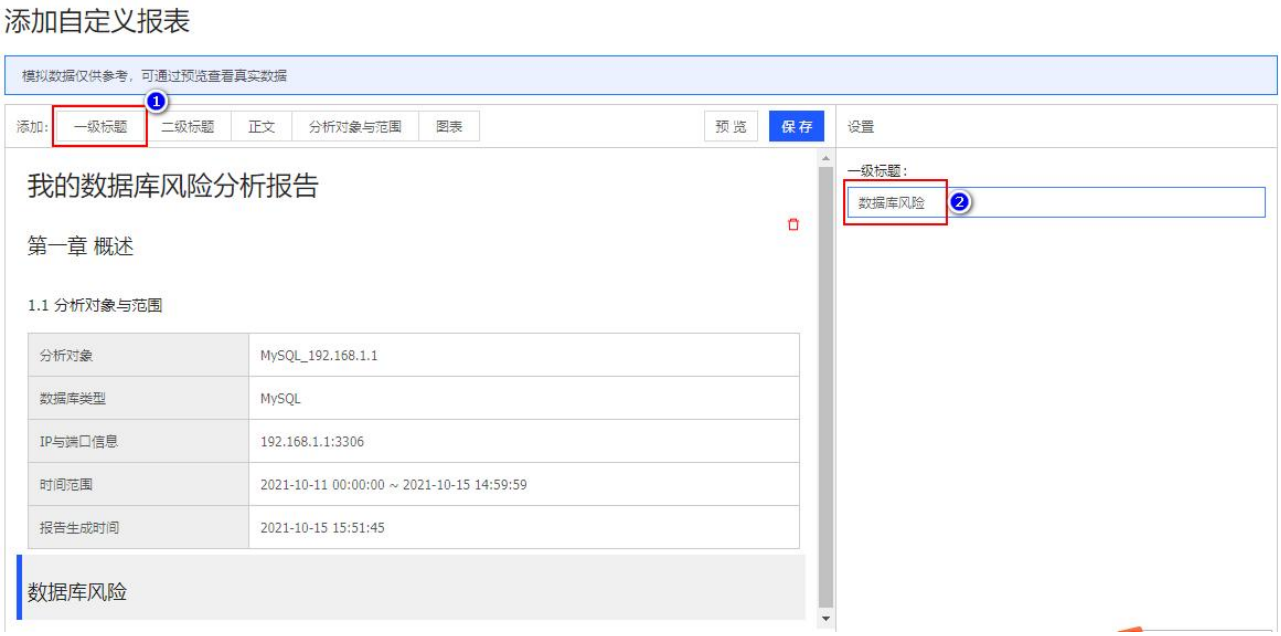


详细配置请参见下表。

配置项	说明
名称	用来标识自定义报表，必须为中文字符、字母、数字、下划线“_”或短横“-”，长度不超过 48 字符。
描述	自定义报表的描述信息，任意字符类型，长度不超过 64 字符。

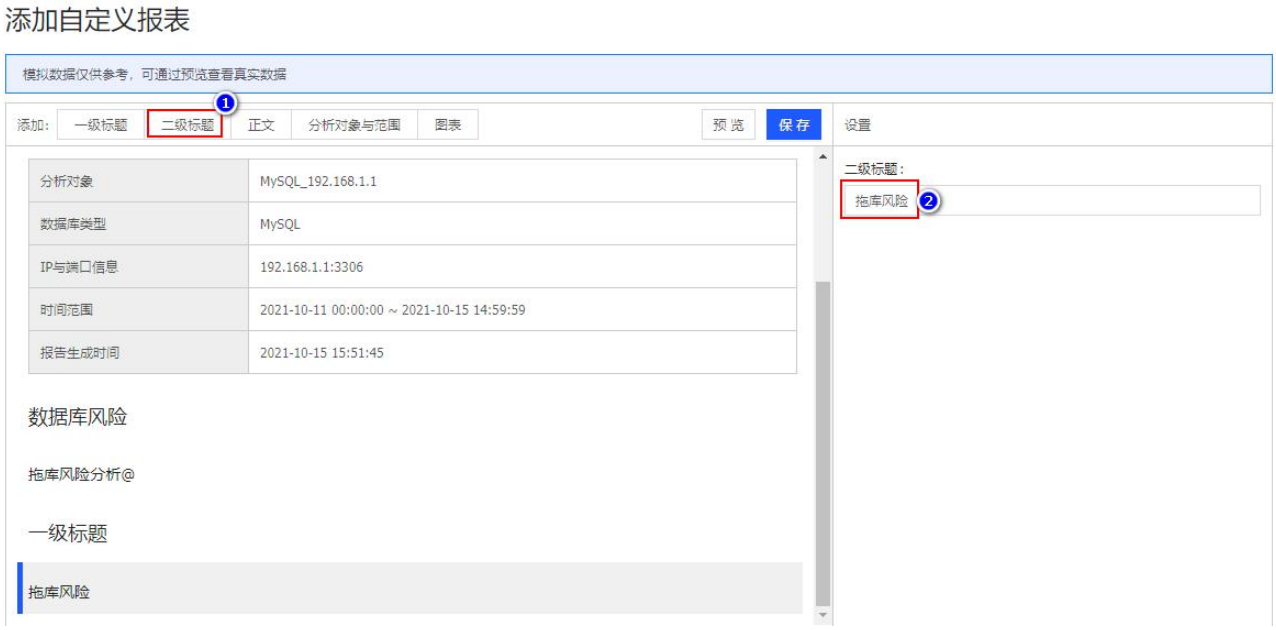
步骤 3. 设置一级标题。

点击**<一级标题>**，编辑一级标题（必须为中文字符、字母、数字、下划线“_”或短横“-”，长度不超过 48 字符）。



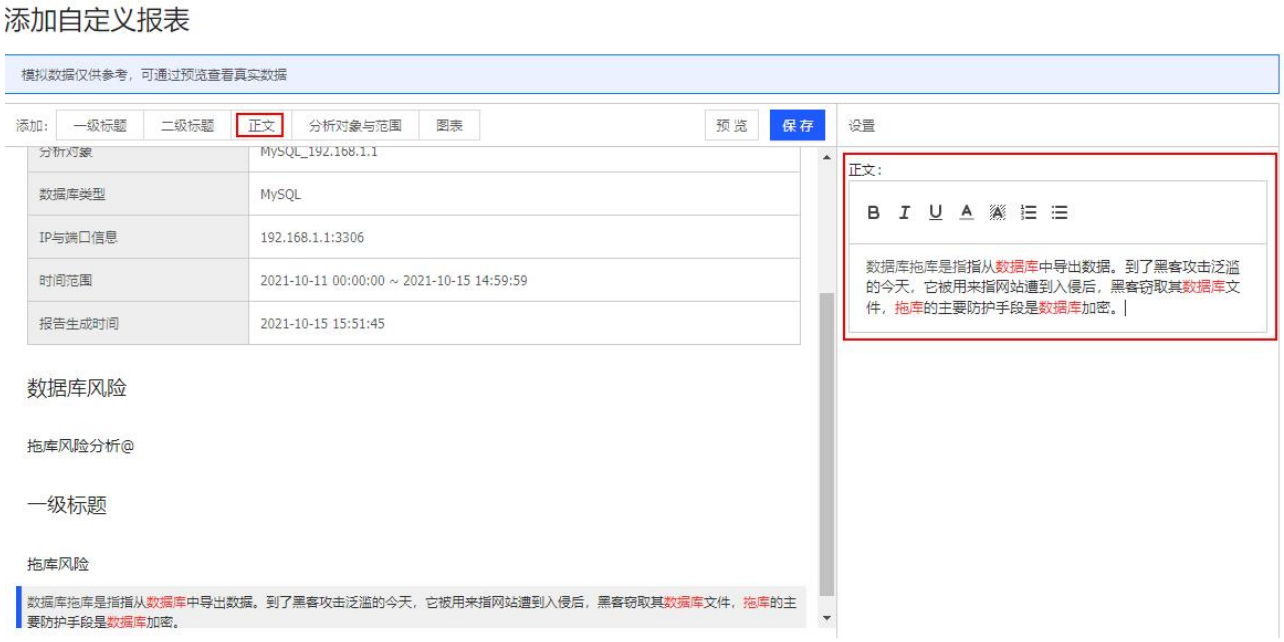
步骤 4. 设置二级标题。

点击**<二级标题>**，编辑二级标题（必须为中文字符、字母、数字、下划线“_”或短横“-”，长度不超过 48 字符）。



步骤 5. 设置正文。

点击<**正文**>，编辑正文（任意字符类型，长度不超过 1000 字符，系统提供了格式编辑工具，可使用格式编辑工具丰富正文格式）。



也可以在一级标题后插入正文。

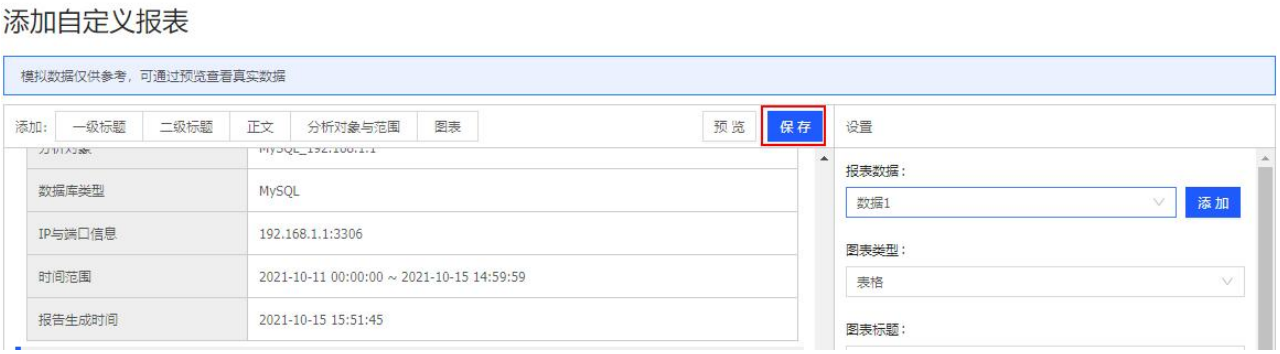
步骤 6. 选择分析对象与范围。

点击<**分析对象与范围**>，选择显示内容。

步骤 7. 设置图表（即设置要展示的报表数据）。

点击<**图表**>，选择报表数据，选择图表类型（包括表格、趋势图、柱状图和饼图），设置显示指标或显示维度。

步骤 8. 点击<**保存**>。



6.3.2.2 其他操作

- 在自定义报表列表中点击**操作**列中的<**预览**>，可预览自定义报表效果。
- 在自定义报表列表中点击**操作**列中的<**编辑**>，可修改自定义报表。
- 在自定义报表列表中点击**操作**列中的<**删除**>，在弹出的对话框中点击<**确定**>，可删除自定义报表。

7 智能分析

智能分析是指系统可以学习用户的数据库操作习惯，通过对用户操作所涉及的 IP、客户端操作工具等信息进行统计分析，可对异常行为进行告警。

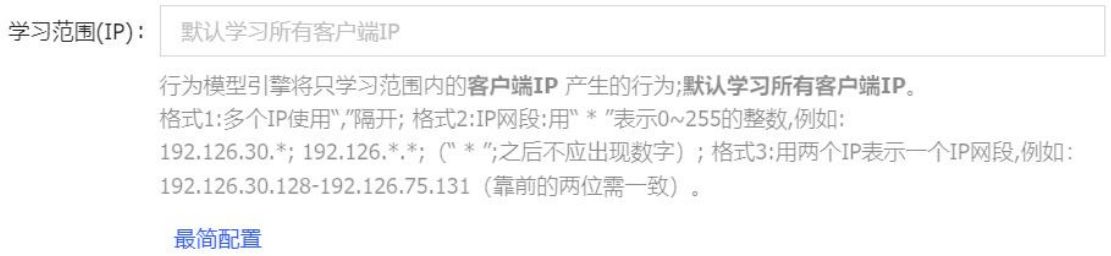
7.1 配置行为模型学习任务

行为模型学习任务是指系统对用户访问数据库的行为进行自学习，对用户行为所涉及到的资产 IP、数据库用户名、客户端工具等信息进行汇总统计。添加行为模型学习任务的操作方法如下：

步骤 1. 在菜单栏选择“**智能分析➤行为模型**”，选择**任务配置**页签，点击<**添加**>。

步骤 2. 进入**行为模型学习配置**页面，编辑相关信息，点击<**开始学习**>。

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

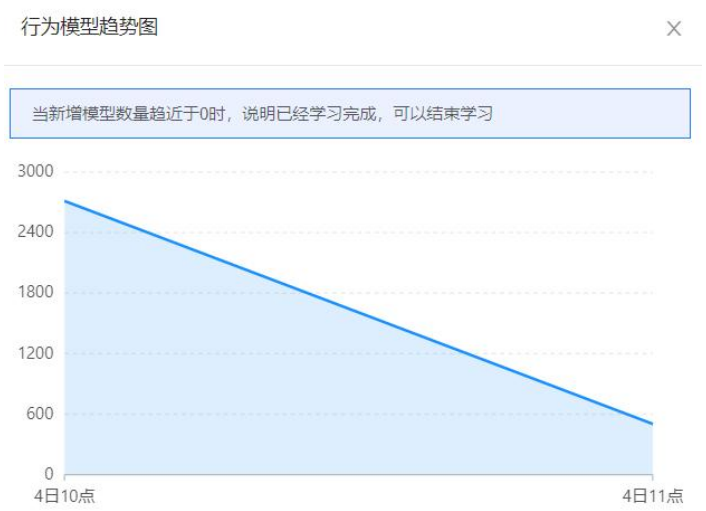


详细配置请参见下表。

配置项	说明
资产	选择已添加的资产。可通过名称、IP 等关键字搜索资产，从而实现快速选择。
学习维度	指定行为模型引擎所学习（即统计分析）的维度，包括客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、数据库的操作类型、服务端 IP、表对象。
学习截止时间	行为模型学习任务的学习截止时间。
告警等级	包括不告警、低等级、中等级、高等级告警，默认为低级告警。
学习范围（IP）	行为模型引擎学习客户端 IP 的范围。支持以下三种填写格式： ◆ 可填写多个 IP，每个 IP 之间用“,”隔开。 ◆ IP 网段，用“*”表示 0~255，例如：192.168.0.*、10.1.*.*。 ◆ IP 范围，例如：192.168.2.1-192.168.2.128。

7.2 模型学习趋势图

在**行为模型**页面，可对已添加的学习任务进行管理。点击**模型数量**对应的数字可以查看行为模型学习的趋势图。



7.3 结束学习

点击学习任务列表**操作**列下的**<结束学习>**后，该资产新产生的审计日志会根据学习的内容进行匹配，在学习到的模型之外的审计日志会根据配置的告警等级，不产生或者产生对应告警等级的行为模型告警。

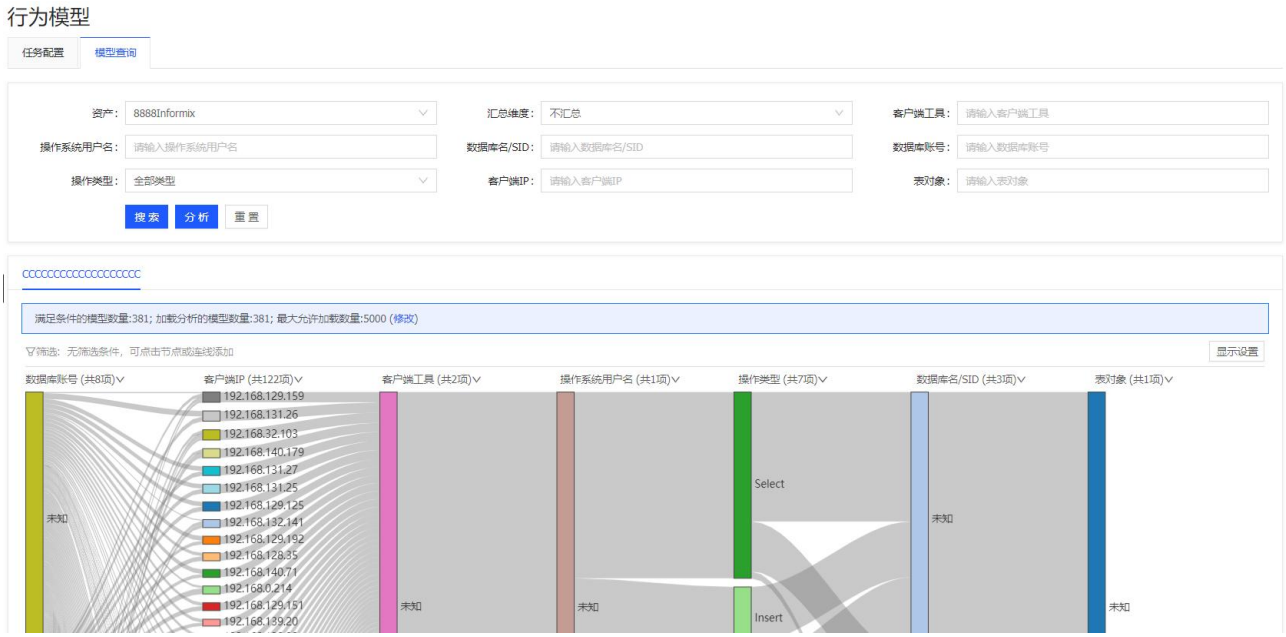
已经结束学习的学习任务，点击点击学习任务列表**操作**列下的**<重新学习>**可重新配置行为模型学习任务。

点击学习任务列表**操作**列下的点击**<修改告警等级>**可设置行为模型之外的审计日志是否告警和告警等级。

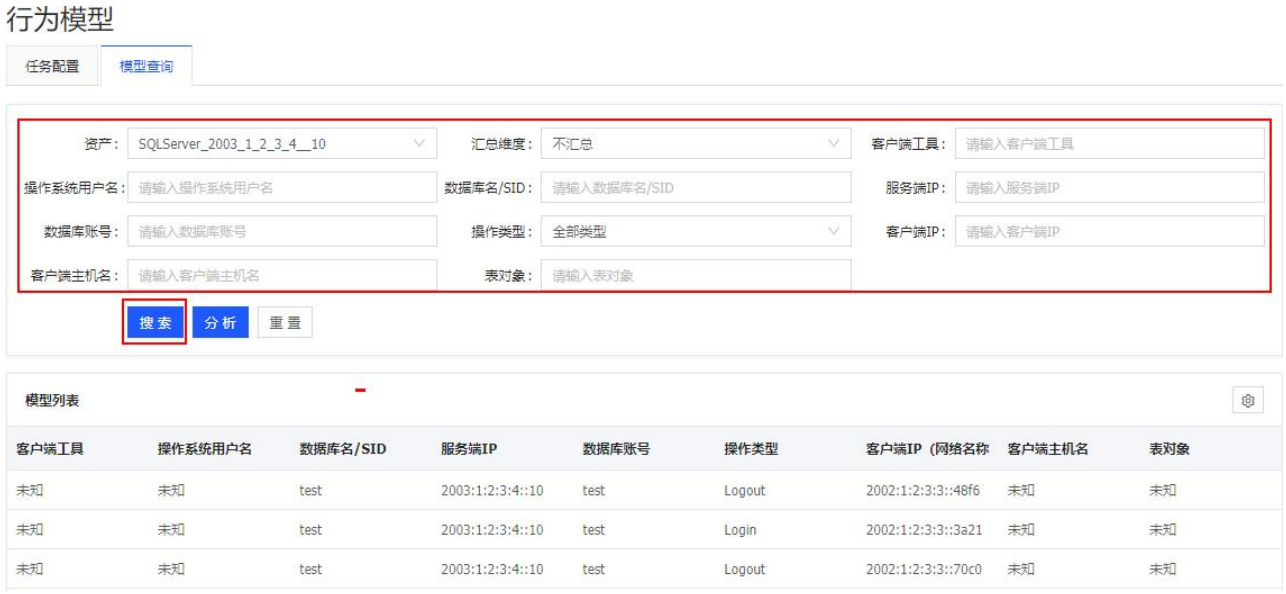
7.4 模型查询

步骤 1. 在行为模型学习任务列表中点击资产名链接或者选择**模型查询**页签再选择资产。

步骤 2. 进入模型查询页面，默认出现该资产学习行为发分析结果，可以选择筛选条件（如“客户端工具”等），点击<**分析**>下方会显示对应的分析结果。点击分析结果图中的节点，查看该节点关联的详细信息。



步骤 3.　设置查询条件（如客户端工具等），点击<**搜索**>即可查询相关行为模型信息。



8 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）、可以信任的行为（信任规则）和不审计的行为（过滤规则）。当系统审计到对数据库的操作匹配过滤规则的行为则不进行审计，对应匹配信任规则时不会触发告警，对应匹配安全规则时会触发告警。

系统匹配规则的顺序为：1）过滤规则；2）信任规则；3）安全规则。

8.1 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。系统通过将审计到的 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应用账号违规操作、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 900 多条安全规则，覆盖了主流的应用场景，并且在不断地丰富。此外，用户可以自定义安全规则。

8.1.1 规则管理

内置规则不可更改，默认为推荐规则，用户可以通过按钮切换到全部规则，操作方法如下：

内置规则包含特征规则及其他非特征规则，特征规则不可进行克隆和删除操作，非特征规则可进行克隆操作。

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，点击<**推荐**>，切换至<**全部**>。

用户也可以管理自定义的规则，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，点击<**新增**>。

步骤 2. 在**新增规则**对话框中编辑相关信息，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。
	描述	规则描述。

项目	配置项	说明
	等级	必选项，系统默认等级为中风险。等级包括高风险、中风险和低风险。
	所属规则组	必选项，可选择自定义的规则组，也可以选择系统默认规则组。用户可通过以下步骤对自定义规则组进行管理：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，点击页面右上角的<**规则组管理**>，可新增，修改和删除自定义规则组。
	规则类型	目前支持普通规则和统计规则两类。 ◆ **普通规则**：单条审计记录匹配配置的普通规则，会触发普通告警（例如一条 select 语句，可能会触发一条普通告警）。 ◆ **统计规则**：指定时间内多次匹配配置的统计规则，会触发一条统计告警（例如 5 分钟内 10 次 select 失败，可能会触发一条统计告警）。
	行为	目前支持告警和告警并阻断。 ◆ **告警**：操作命中规则后，仍正常执行，无特殊控制。 ◆ **告警并阻断**：操作命中规则后，该操作对应的数据库连接断开。
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	可配多个客户端工具，使用逗号“,”分隔，例如：db2bp.exe,java.exe。
	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 MAC 地址	可填多值，多个值间以逗号“,”分隔。
	操作系统用户	可以选择字符串或者正则表达式，字符串可填多值，多个值间以逗号

项目	配置项	说明
		“,” 分隔。
	主机名	可以选择字符串或者正则表达式，字符串可填多值，多个值间以逗号“,” 分隔。
	应用 IP	指定规则所匹配的应用 IP 或 IP 组，可填多值，多个值间以逗号 “,” 分隔。有关 IP 组的更多信息，请参考 IP 组管理。
	应用用户名	指定规则所匹配的应用用户或用户组，可填多值，多个值间以逗号“,” 分隔。有关应用用户组的更多信息，请参考应用用户组管理。
服务端	服务端 IP	可填多值，多个值间以逗号 “,” 分隔。
	服务端端口	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。
	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或者使用正则表达式，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。
	服务端 MAC 地址	可填多值，多个值间以逗号 “,” 分隔。
	数据库名（SID）	可以选择字符串或者正则表达式，Oracle 数据库输入 SID，其他数据库输入数据库名，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。

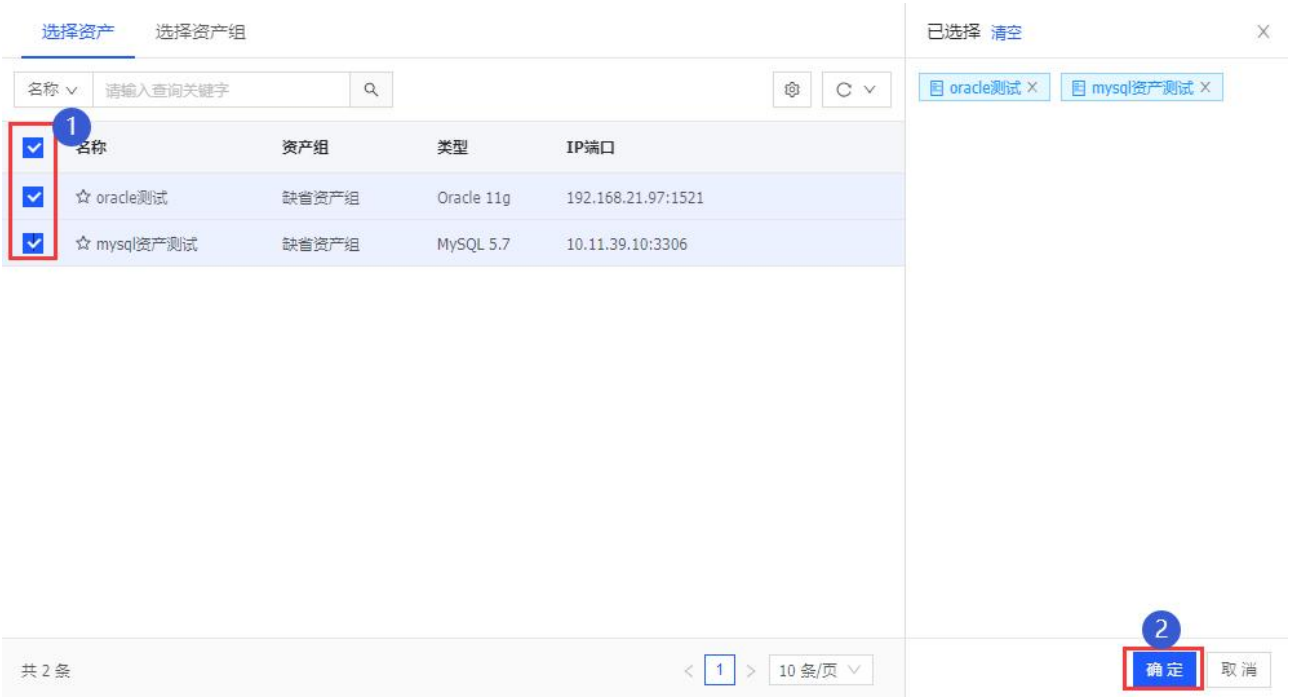
项目	配置项	说明
	SQL 模板 ID	可填项，可填多值，多个值间以逗号“,”分隔。有关 SQL 模板 ID 的更多信息，请参考查询 SQL 模板。
	SQL 关键字	SQL 关键字：支持以正则表达式方式匹配报文。单击<**正则验证**>输入报文内容，单击<**校验**>，验证输入内容与执行结果关键字中的正则表达式是否匹配。点击<**增加条件**>添加多个条件。 条件运算逻辑表达式：SQL 关键字填写后，此项为必填项。条件间的关系，支持与、或、非、括号运算(&：与；|：或；~：非)，条件使用序号表示，即“1”表示条件 1，例如：1&2，则代表有 2 个 SQL 关键字条件，且两个关键字都要满足才能告警。
	SQL 长度	取值范围：1B~64KB。
	关联表数	SQL 操作涉及表的个数大于等于此值时触发本规则，允许输入最大值为 255。
	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。默认为不判断。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：秒、毫秒、微秒，取值范围：0 到半个小时，SQL 执行时长属于此范围，则触发规则。
	影响行数	取值范围：0~999,999,999。SQL 操作返回的记录数或受影响的行数属

项目	配置项	说明
		于此范围，则触发规则。
	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<**校验**>，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：如正则表达式填写后，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。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。
	每日最大告警次数	取值范围：0~99,999，输入 0 表示没有限制。
	结果集存储策略	设置触发该规则的告警日志的返回结果集存储策略，包含使用资产设置、保存和不保存。

8.1.2 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**规则管理**页签，在规则列表中勾选目标规则，点击<**启用选中项**>。

步骤 2.　在弹出对话框中勾选资产，点击<**确定**>，则可将已启用的规则直接应用到选择的资产上。



8.1.3　禁用规则

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**规则管理**页签。

步骤 2.　在规则列表中勾选规则，然后点击<**禁用选中项**>。

步骤 3. 在弹出的对话框中勾选资产，点击<**确定**>即可禁用规则。

8.1.4 白名单管理

已经匹配到安全规则的审计日志如果符合白名单的条件就不会触发告警。条件包含客户端、服务端、基本信息、结果、行为等。

新增白名单的操作方法如下：

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**白名单管理**页签。

步骤 2. 点击<**新增**>，进入新增白名单页面，编辑相关配置项（配置方法与新增自定义规则的参数配置方法相同，请参考规则管理），点击<**保存**>。

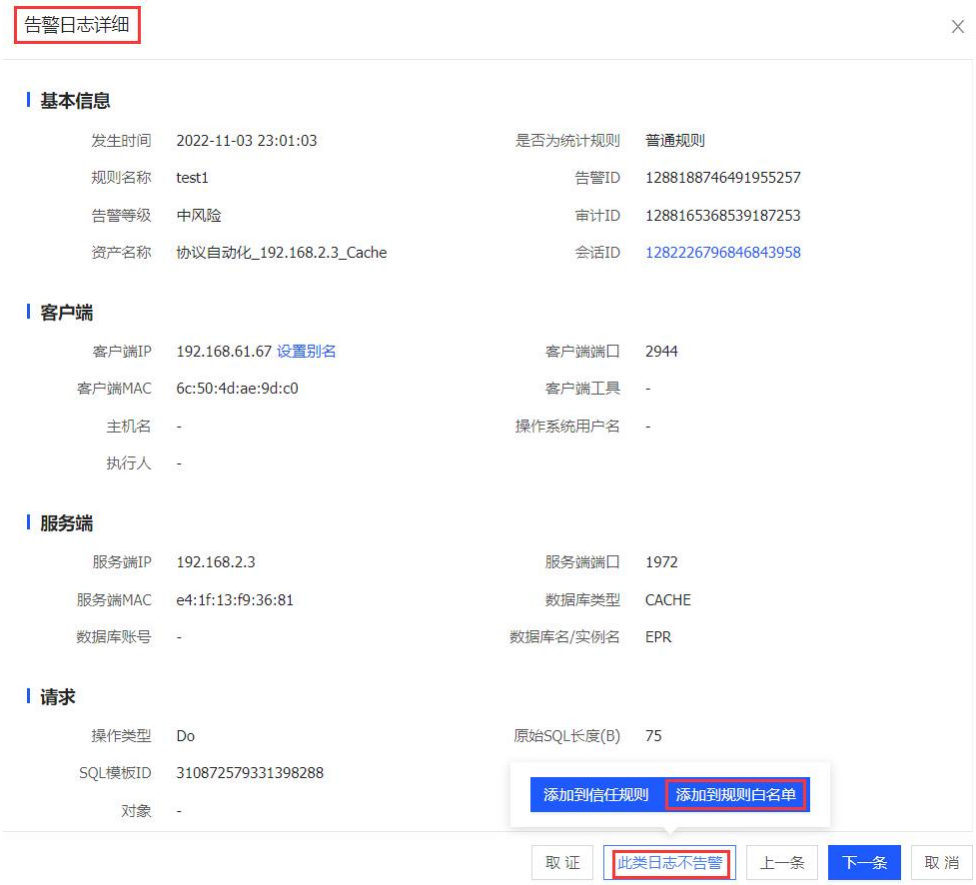
添加白名单后，需在对应的规则上启用该白名单才会生效。启用白名单的操作方法如下：

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。

步骤 2. 点击**白名单数量**列中的数字链接。

步骤 3. 在弹出的对话框中将状态设置为“启用”即可启用白名单。

在**告警日志**页面点击**<详细>**，进入**告警日志详细**页面，点击**<此类规则不告警>**选择“**添加到规则白名单**”，此种方式会自动将白名单挂载在告警日志对应的安全规则上。



需要将白名单上启用的所有安全规则禁用后才能删除该白名单。

8.1.5 设置

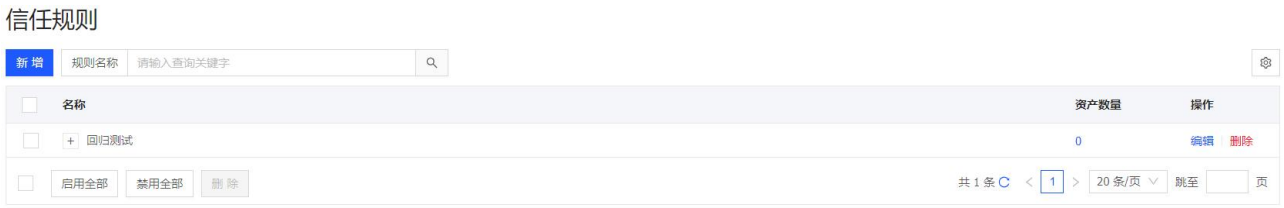
设置规则的优先级状态，启用优先级可自定义规则匹配顺序，匹配上某条规则后，优先级更低的规则就不再匹配。关闭规则的优先级后，每个数据库操作行为可以触发的所有满足条件的安全规则。

8.2 信任规则

当系统匹配信任规则后，不会再匹配安全规则，不产生告警信息。

新增信任规则的操作方法如下：

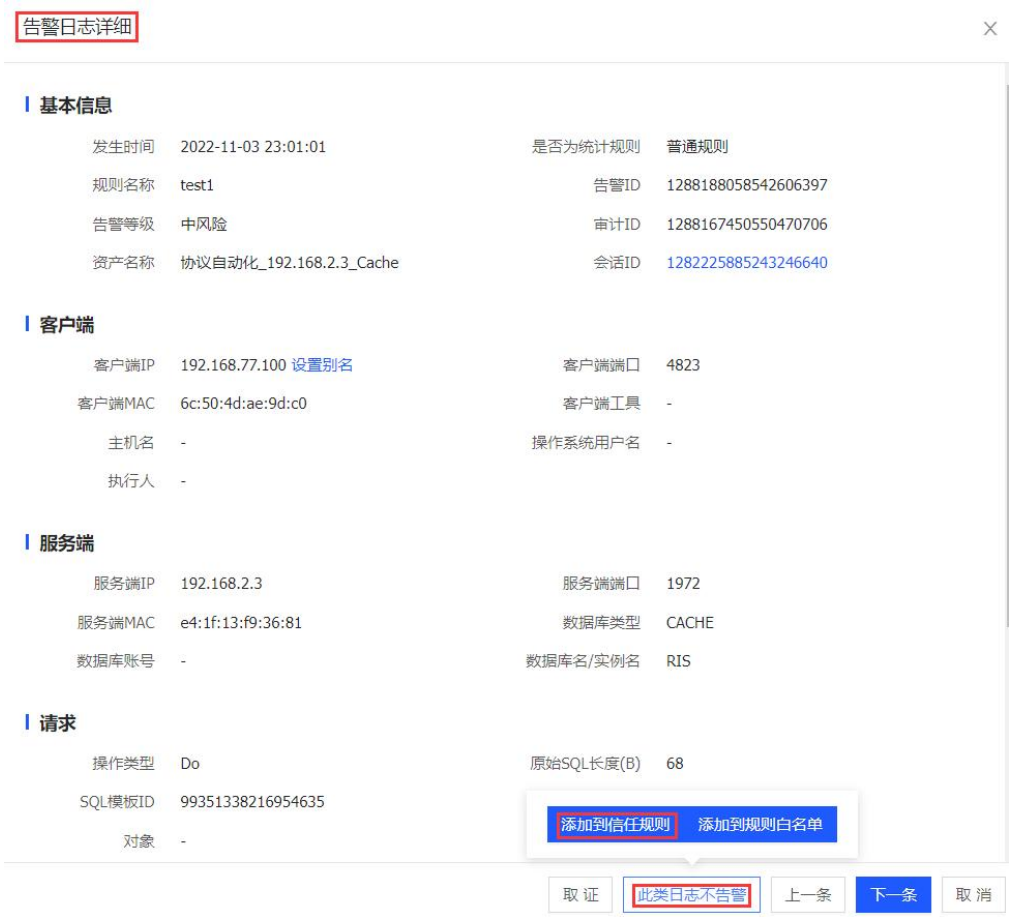
步骤 1. 在菜单栏中选择“**规则配置➤信任规则**”进入**信任规则**页面。



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

详细配置请参见规则管理。

在**告警日志**页面点击**<详情>**，进入**告警日志详细**页面，点击**<此类规则不告警>**选择**“添加到信任规则”**，此种方式会自动将信任规则启用到告警日志对应的资产上。



8.3 过滤规则

过滤规则的功能是根据某些特定的条件过滤一些操作，系统对这些操作不审计，从而节省设备的磁盘空间，将有限的资源用来存储更有价值的审计数据。

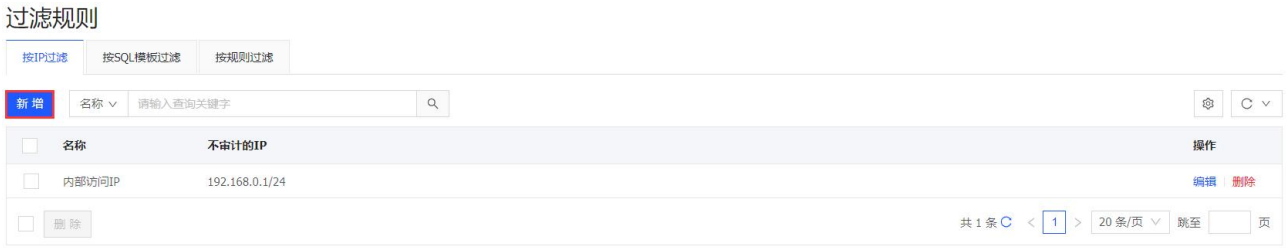
过滤规则的过滤方式有三种，分别是按 IP 过滤、按 SQL 模板过滤和按规则过滤。

- 按 IP 过滤是设置某些 IP 地址为信任的 IP 地址，系统对这些 IP 地址发起的 SQL 请求不审计。
- 按 SQL 模板过滤是设置 SQL 模板为可信任的模板，当访问的 SQL 语句的模板是设置的过滤模板，则不进行审计。
- 按规则过滤是指按照特定的条件进行审计过滤，规则包括客户端信息、服务端信息、SQL 请求和 SQL 结果等条件。

8.3.1 按 IP 过滤

按 IP 过滤则是将新增的客户端 IP 认为是白名单，不审计该 IP 下任何信息。新增按 IP 过滤规则的操作方法如下：

步骤 1. 在菜单栏选择“**规则配置➤过滤规则**”进入**过滤规则**页面。



步骤 2. 点击<**新增**>，进入**新增 IP 过滤**页面，编辑名称和不审计的 IP，点击<**保存**>。

详细配置项和说明请参见下表。

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。
不审计的 IP	格式为“IP/掩码长度”，可配置多组，用“,”隔开。例如：1.2.3.4/32,10.0.0.0/8。

此处添加的不审计的 IP 默认对 RDS 的资产除外的全部资产有效。即添加后，资产中有符合上述不审计 IP 条件的客户端和服务端均不做任何审计，请谨慎添加。

8.3.2 按 SQL 模板过滤

按 SQL 模板过滤是为用户提供常见的可信任的 SQL 模板，减少误告警，提高告警准确率。系统内置部分常见数据库的常见非违规 SQL 语句模板，且默认对全部对应的数据库生效。

用户可启用或禁用指定模板，操作方法如下：

步骤 1. 在**过滤规则**页面选择按 **SQL 模板过滤**页签，勾选 SQL 模板，点击<**启用选中项**>或<**禁用选中项**>。

步骤 2. 在弹出的对话框中点击<**确定**>。

8.3.3 按规则过滤

按规则过滤是为用户提供自定义的过滤规则，支持用户按照特定的条件设置过滤规则，规则包括客户端信息、服务端信息、SQL 请求和 SQL 结果等条件。在资产上启用了过滤规则后，符合规则的内容则不会被审计。

添加按规则过滤的规则的操作方法与添加安全规则的方法相同，请参见规则管理。

添加自定义过滤规则后，需要在资产上启用过滤规则后才能生效。

步骤 1. 在**过滤规则**页面选择按**规则过滤**页签，勾选规则，点击<**启用选中项**>。

步骤 2. 在弹出的**选择资产**对话框中勾选资产，点击<**确定**>。

8.4 规则维护

规则维护包括升级内置安全规则和导入/导出自定义安全规则。

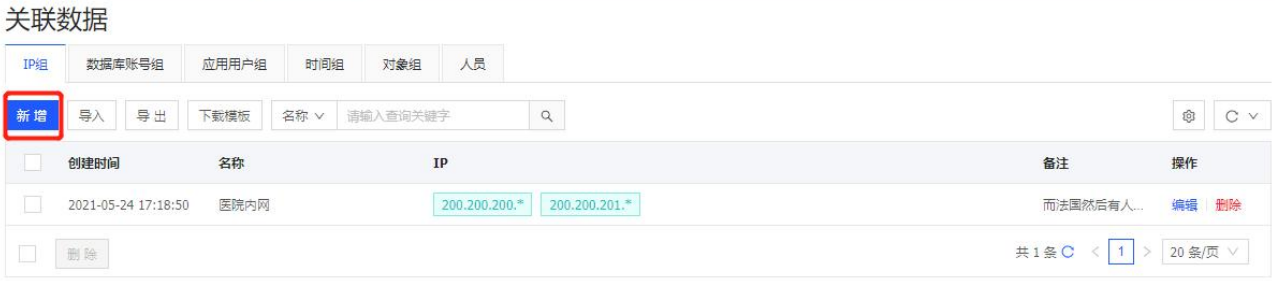
在菜单栏选择“**规则设置➤规则维护**”进入**规则维护**页面。点击<**上传升级包**>，选择升级包文件即可升级内置安全规则；点击<**导入规则**>，选择自定义规则文件，即可导入自定义规则；点击<**导出规则**>即可导出自定义规则至本地。

8.5 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、数据库账号组、应用用户组、时间组和对象组以及人员六种类型。

8.5.1 IP 组管理

IP 组是特定 IP 的集合。如自定义某规则需要在某固定 IP 集合内有效时，可以将此固定 IP 集合添加至 IP 组，便于用户在规则中使用。IP 组管理页面提供新增、导入、导出、编辑、删除和查询功能。



8.5.1.1 新增 IP 组

步骤 1. 在菜单栏选择“**规则配置➤关联数据**”进入**关联数据**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**>。

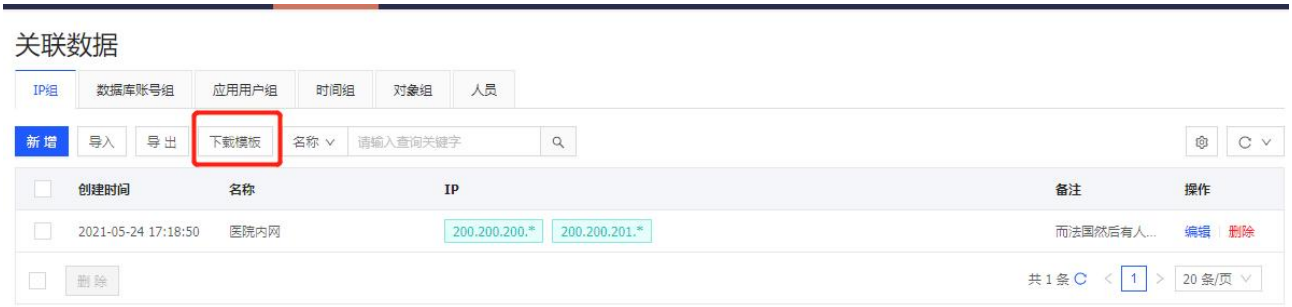
详细配置请参见下表。

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。

8.5.1.2 导入 IP 组

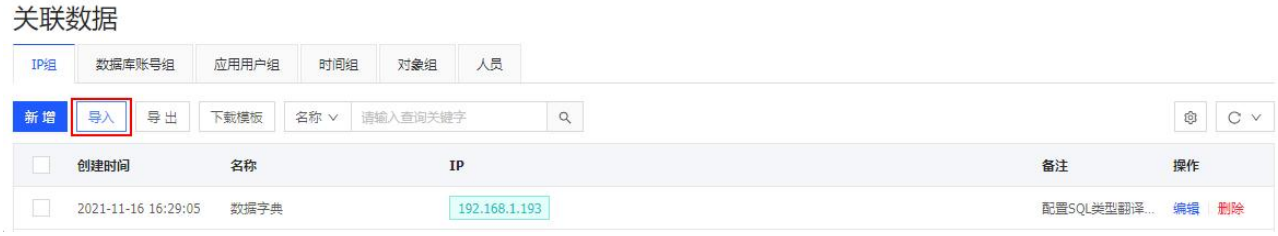
通过批量导入 IP 组的方法可以提高创建 IP 组的效率，操作方法如下：

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。

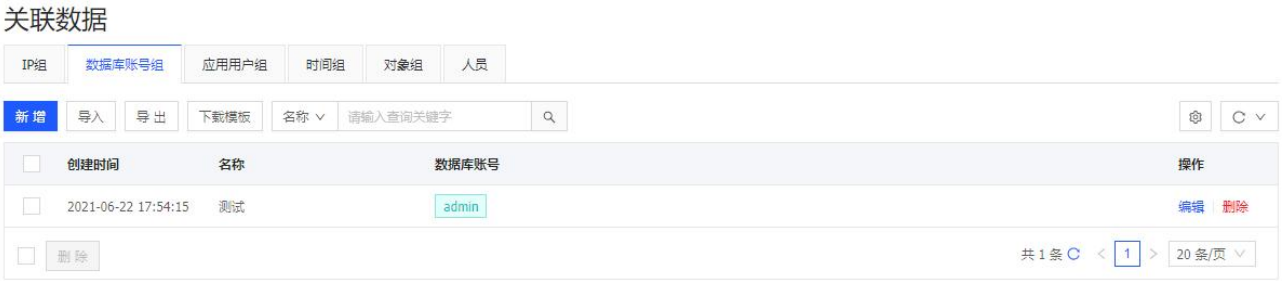
步骤 3. 点击<**导入**>，在弹出的对话框中选择编辑好的模板文件，导入文件成功后页面会弹出提示信息，并将模板文件中的 IP 组添加至 IP 组列表中。



8.5.2 数据库账号组管理

数据库账号组是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。



8.5.2.1 新增数据库账号组

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➤关联数据**”进入**关联数据**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。
数据库账号	可输入多项，用英文逗号隔开。

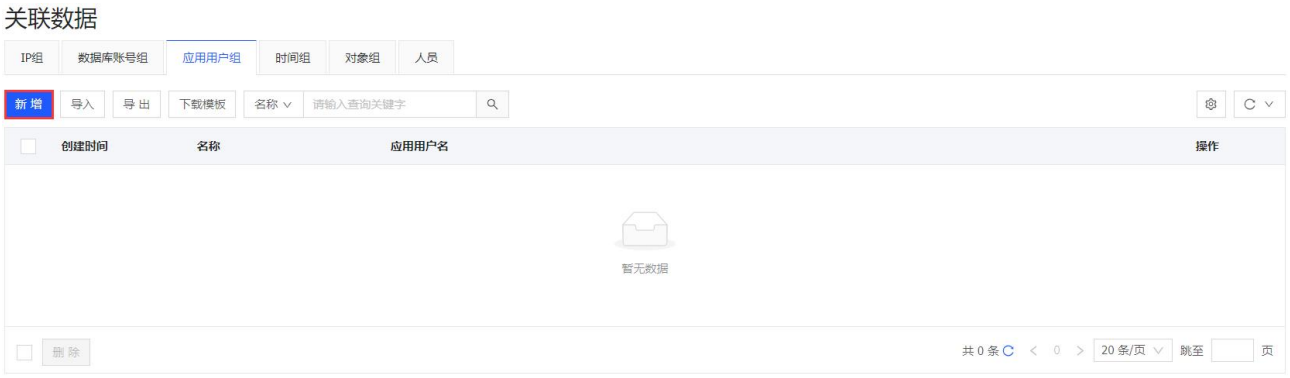
8.5.2.2 导入数据库账号组

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。

8.5.3 应用用户组管理

应用用户组是特定应用用户的集合。如自定义某规则需要在某固定应用用户集合内有效时，可以将这些应用用户加入到应用用户组，在创建规则时选择该应用用户组即可。

应用用户组管理页面提供增加、编辑、删除和查询功能。



8.5.3.1 新增应用用户组

新增应用用户组的操作方法如下：

步骤 1. 在菜单栏选择“**规则配置➤关联数据**”进入**关联数据**页面，选择**应用用户组**页签，点击<**新增**>。

步骤 2. 进入**新增应用用户**页面，编辑名称和应用用户名，点击<**保存**>。

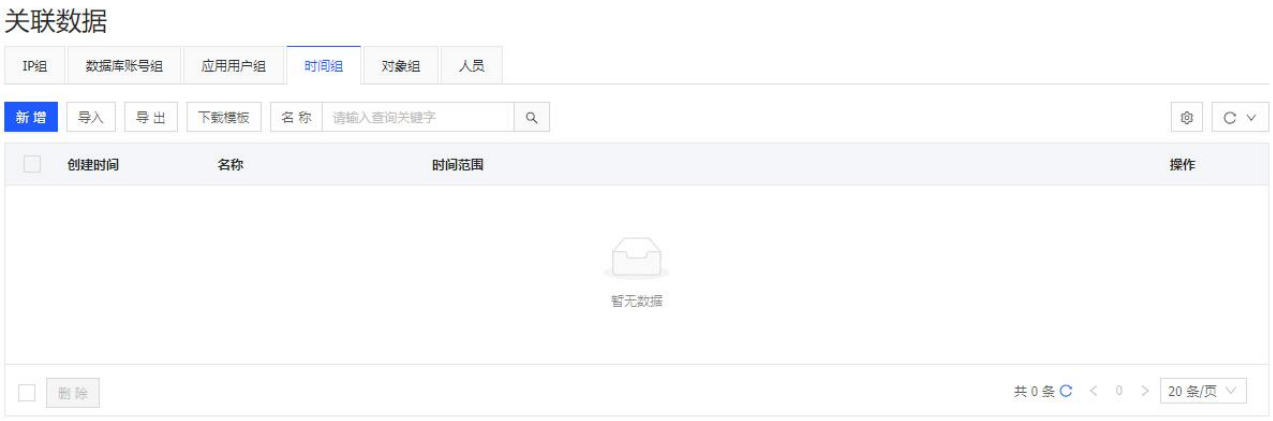
8.5.3.2 导入应用用户组

导入应用用户组的操作方法与导入 IP 组的方法类似，不再赘述。

8.5.4 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。



8.5.4.1 新建时间组

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➤关联数据**”进入**关联数据**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**>。

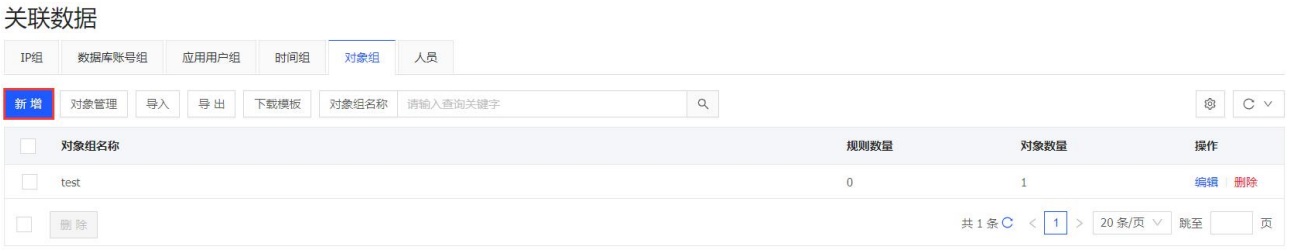
8.5.4.2 导入时间组

导入时间组的操作方法与导入 IP 组方法相似，不再赘述。

8.5.5 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。

对象组管理页面提供增加、编辑、删除、导入、导出和下载模板功能。



8.5.5.1 新增对象组

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➤关联数据**”进入**关联数据**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，编辑资产、数据库/Schema 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
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/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。
表	填写要添加的表名。
用户	数据库系统的用户。
视图	视图是从一个或几个基本表（或视图）中导出的虚拟的表。
存储过程	存储过程（Stored Procedure）是一种在数据库中存储复杂程序，以便外部程序调用的一种数据库对象。
函数	数据库系统定义的函数，例如：SUBSTRING('abcde',1,2)。
字段	填写要添加的字段名。
索引	是对数据库表中一个或多个列（例如，employee 表的姓名（name）列）的值进行排序的

配置项	说明
	结构。

8.5.5.2 导入对象组

导入对象组的操作方法与导入 IP 组方法相似，不再赘述。

8.5.6 人员管理

系统支持对人员进行管理，包括新增、编辑、导入、导出和删除等。

8.5.6.1 新增人员

新增人员的操作方法如下：

步骤 1. 在菜单栏选择“**规则配置➤关联数据**”进入**关联数据**页面，选择**人员**页签，点击<**新增**>。

步骤 2. 在弹出的**新增人员**对话框中编辑工号、IP 地址、姓名、手机号等信息，点击<**保存**>。

详细配置请参见下表。

配置项	说明
应用用户名	◆ 人员登录应用所使用的账号，可能是工号、英文名等信息。支持配置多个，多个值间以逗号“,”分隔。例：001,张三,zhangsan。 ◆ 审计日志中的关联账号满足该条件时，系统将会把人员当做此日志的执行人。
IP 地址	人员所使用终端的 IP 地址。可配置多个，支持配置网段，示例： 10.10.1.1,10.10.1.2,10.1.1.10-10.1.1.20,10.10.*.*,10.10.1.* 审计日志中的客户端 IP 或关联 IP 满足该条件时，系统将会把人员当做此日志的执行人，该条件优先级低于应用用户名。
工号	人员对应的工号。
姓名	人员对应的姓名。

配置项	说明
手机	人员对应的手机号。
科室	人员所在部门。
房间	人员所在房间号。
主机名	人员所对应资产的主机名称。
Mac 地址	人员所对应资产的物理 Mac 地址。

8.5.6.2 导入人员

导入人员的操作方法与导入 IP 组方法相似，不再赘述。

9 通知外送

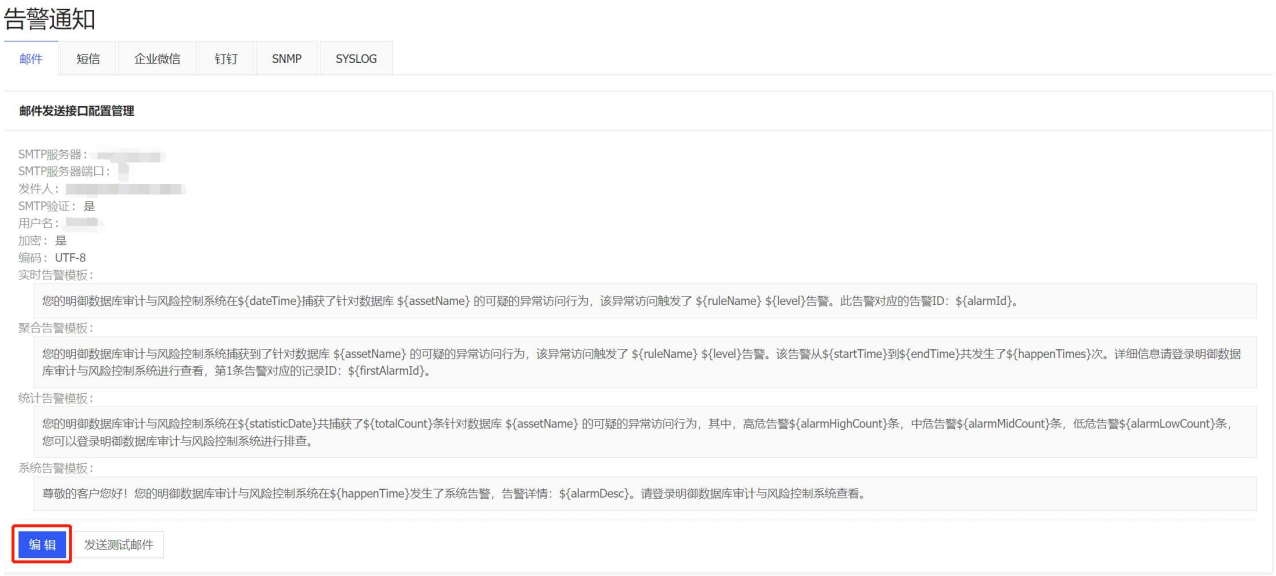
通知外送是指将资产及系统的告警信息和日志信息发送给指定的外部对象。

9.1 告警通知

系统支持多种消息通知模式，可及时将当前资产告警情况以及系统本身的状态信息提供给管理员，目前支持邮件、短信、企业微信、钉钉、SNMP、Syslog 六种通知方式。

9.1.1 邮件方式通知告警

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**>，在弹出的**邮箱配置**对话框中编辑相关信息，点击<**确定**>。

详细配置请参见下表。

配置项	说明
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。
发件人	发件人的邮箱。
SMTP 验证	邮箱是否开启 SMTP 验证。
用户名	邮箱的用户名。
密码	与邮箱用户名对应的用户密码。
是否加密	邮箱是否进行加密。

配置项	说明
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.　配置邮件发送接口后，可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**>。

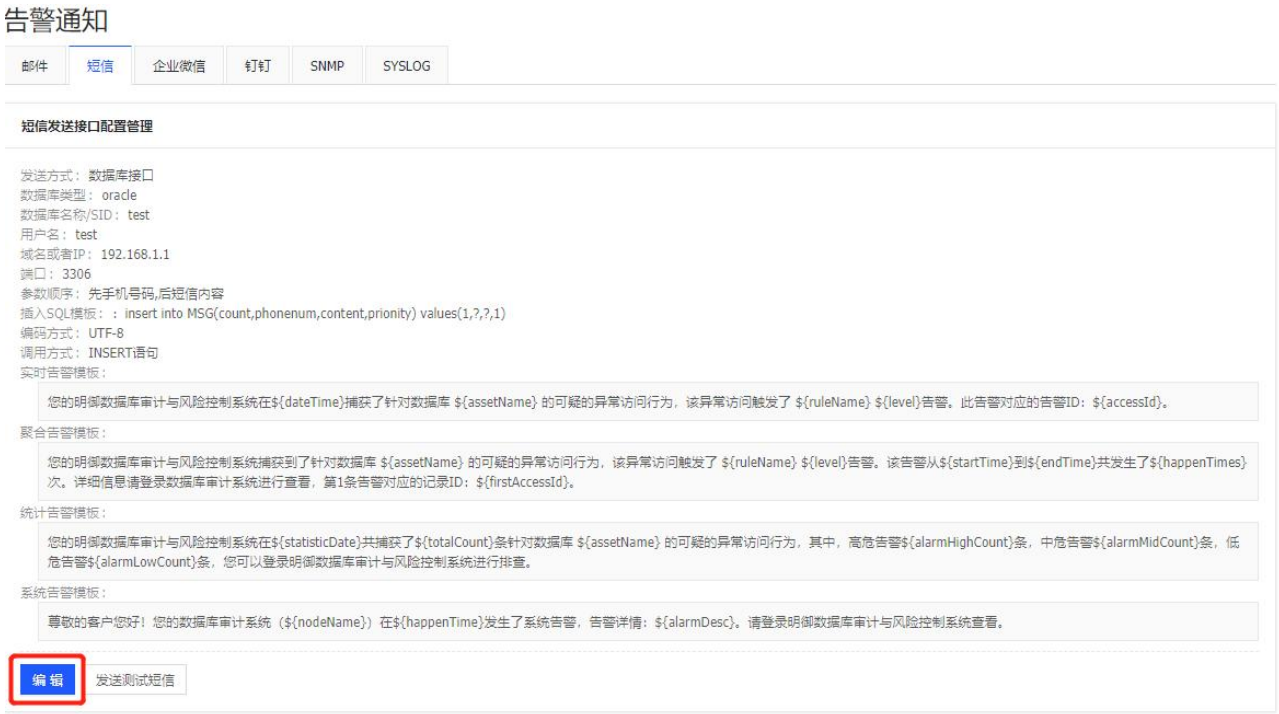
步骤 4.　在弹出的对话框中编辑相关信息，点击<**保存**>。

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，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（“*”为具体数值）。
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。

9.1.2 短信方式通知告警

步骤 1. 在**告警通知**页面选择**短信**页签，进入如下页面。



步骤 2. 点击<**编辑**>，在弹出的**短信配置**对话框中编辑相关信息，点击<**确定**>。

详细配置请参见下表。

配置项	说明
发送方式	选择短信发送方式，支持 Web 接口和数据库接口。
发送方法（Web 接口）	请求方法，支持 GET、POST 请求。
URL（Web 接口）	短信网关的接入 URL。
头信息（Web 接口）	请求头。可添加多个请求头信息。
Post 参数（Web 接口 Post 方法）	请求 Post 参数内容，如果使用 Json 方式，该值填写 Json 内容。
数据库类型	选择数据库的类型，支持 MySQL、Oracle、DB2 和 SQL Server。
数据库名称/SID（数据库接口）	短信通知接口数据库名称。
用户名/密码（数据库接口）	短信通知接口数据库的用户名和密码。

配置项	说明
域名或者 IP（数据库接口）	短信通知接口数据库的 IP 或域名。
端口（数据库接口）	短信通知接口数据库的端口。
参数顺序（数据库接口）	支持“先手机号码，后短信内容”和“先短信内容，后手机号码”。
插入 SQL 模板（数据库接口）	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。例如：insert into MSG(count,phonenum,content,priority) values(1,?,?,1)。注意事项：语句最后不用加分号“;”。
调用方式（数据库接口）	可选择 INSERT 语句或者存储过程。
编码方式	服务器支持的编码方式，主要为：UTF-8、GBK。 以上配置与短信服务器端保持一致即可。
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. 配置短信通知接口页面的相关信息后，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，可选择多个。
接收者	接收告警信息的手机号，可设置多个手机号。
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：0~86,400，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	开启或关闭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。

短信网关由专门提供短信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。

9.1.3 企业微信通知告警

步骤 1. 在**告警通知**页面选择**企业微信**页签，进入如下页面。

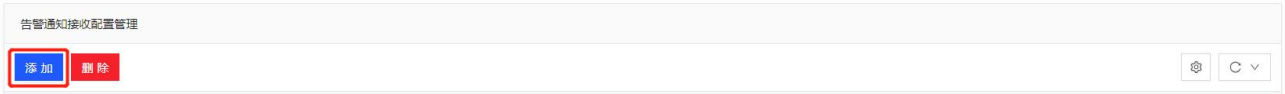
步骤 2. 点击<**编辑**>，在弹出的**企业微信配置**对话框中编辑相关信息，点击<**确定**>。

详细配置请参见下表。

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，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，

配置项	说明
	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。
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。

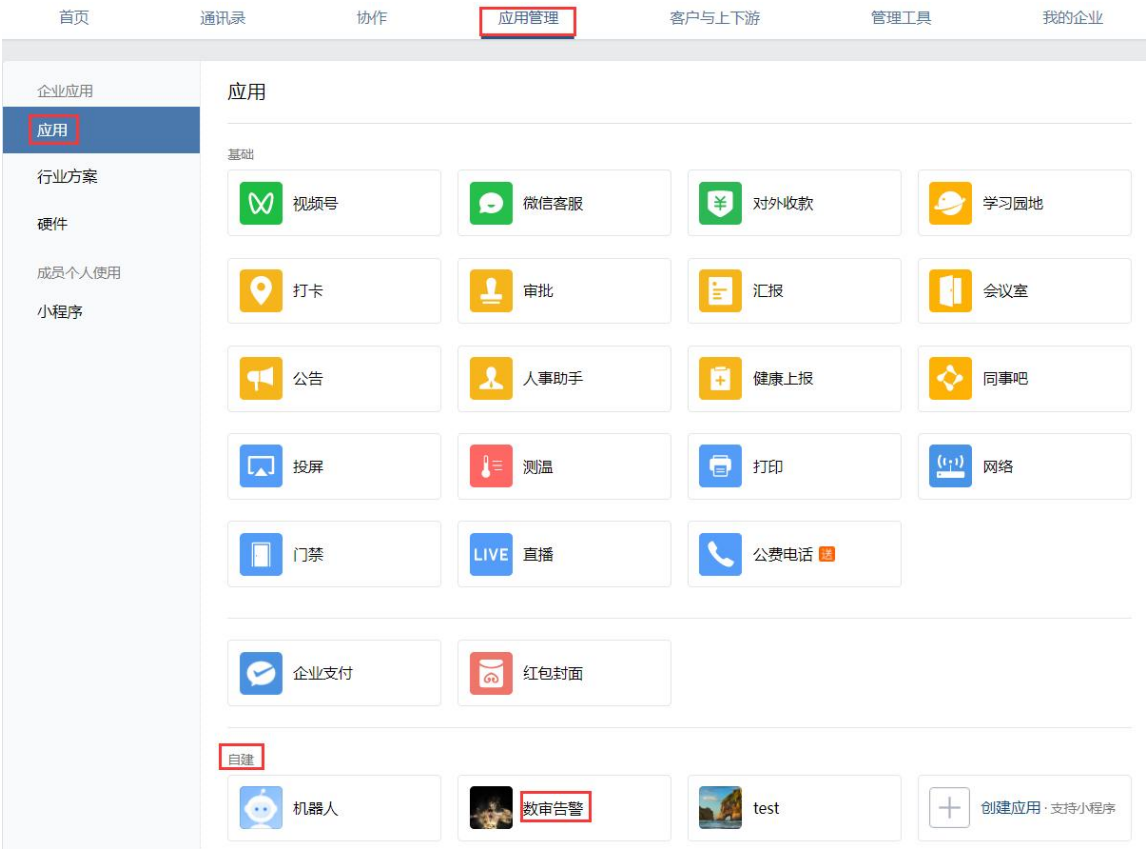
步骤 3. 配置企业微信通知接口后，可给需要通过企业微信通知接口发送通知的资产配置发送方式。点击<**添加**>。



步骤 4. 在弹出的对话框中编辑相关信息（配置方法与短信方式通知告警相同，**接收者**需要设置为企业微信通讯录中的账号），点击<**保存**>。

步骤 5. 在企业微信配置受信任的 IP。

1) 使用管理员账号登录企业微信管理后台，在菜单栏选择“**应用管理➤企业应用➤应用**”进入**应用**页面， 在**自建**区域点击用用名称。



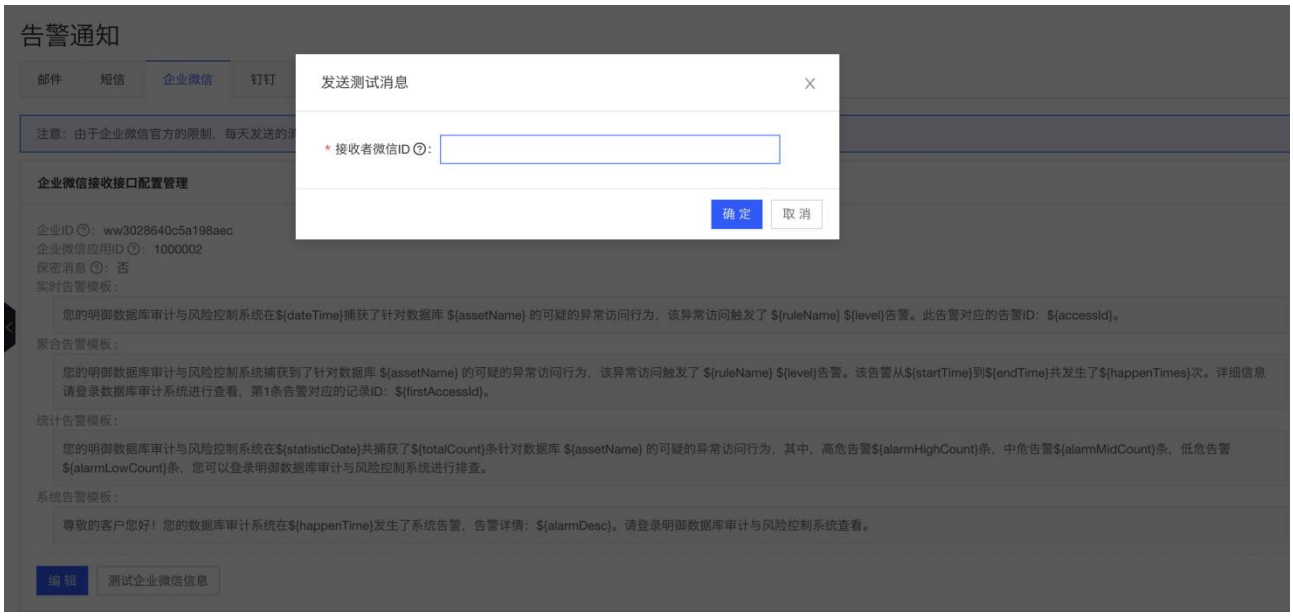
2) 在**开发者接口**区域可以查看到企业可信 IP，点击<**配置**>配置数据库审计服务器公网 IP。

步骤 6. 获取成员 ID。

使用管理员账号登录企业微信管理后台，在通讯录中点开某个成员的姓名，即可看到“账号”。

步骤 7. 测试发送企业微信信息。

在菜单栏选择“**通知外送➤告警通知**”进入**告警通知**页面，选择**企业微信**页签，点击<**测试企业微信消息**>，填写接收者微信 ID，多个接收者用英文逗号隔开，最多支持添加 1000 个成员，点击<**确定**>。



9.1.4 钉钉方式通知告警

- 需要在钉钉管理后台将数据库审计的出口公网 IP 添加为白名单，并进行相关配置（例如开通钉钉通讯录权限等，具体操作请参见《数据库审计与风险控制系统 V4.0.69 配置案例手册》）。
- 在步骤 4 中需要将**接收者**设置为钉钉通讯录中的手机号。

步骤 1. 在**告警通知**页面选择**钉钉**页签，进入如下页面。

步骤 2. 点击<**编辑**>，在弹出的**钉钉配置**对话框中编辑相关参数，点击<**确定**>。

详细配置请参见下表。

配置项	说明
发送方式	选择钉钉发送方式，支持微应用和机器人。
微应用 ID	用于发送消息的应用 ID。获取方法：使用钉钉开放平台，在“**应用开发（企业内部开发）➤基础信息**”查看应用凭证 AgentId。
公司组织 ID	企业唯一标识。获取方法同微应用 ID，为 AppKey。
公司组织 ID 密钥	用于发送消息的应用密钥。获取方法同微应用 ID，为 AppSecret。
Webhook 地址	机器人方式，使用 webhook 地址向钉钉群推送消息，机器人添加完成后自动生成。
密钥	机器人方式，安全设置勾选了加签规则时需要填写。用于发送告警信息的密钥。 获取方法：在机器人安全设置中勾选加签选项
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。

配置项	说明
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。

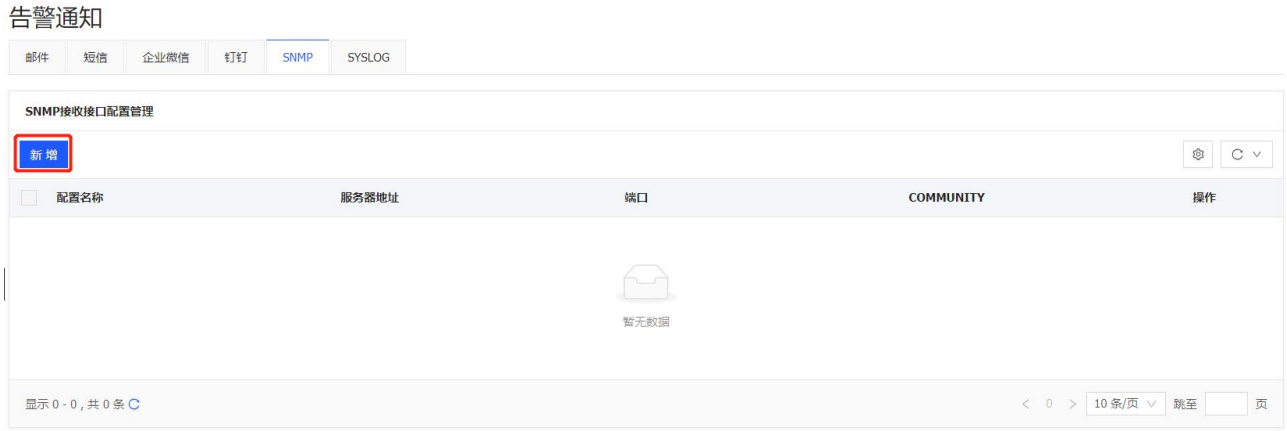
步骤 3.　配置钉钉通知接口后，可给需要通过钉钉通知接口发送通知的资产配置发送方式。点击<**添加**>。

步骤 4.　在弹出的对话框中编辑相关信息（配置方法与短信方式通知告警相同），点击<**保存**>。

9.1.5 SNMP 方式通知告警

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。数据库审计支持将告警信息发送到指定的 SNMP 服务器，以方便其他网络管理系统的远程监控。

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



步骤 2. 点击<**新增**>，进入**新增 SNMP 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	SNMP 接收接口的配置名称。
服务器地址	SNMP 服务器地址，可输入 IP 或者域名。
端口	SNMP 服务器端口，默认为 162。
COMMUNITY	定义信息流向，填写“public”，即公开。 以上 SNMP 相关配置与服务器端保持一致即可。
实时告警模板	发送实时告警信息的模板，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，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，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，具体字段请依据**填写说明**编辑。

步骤 3.　配置好 SNMP 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，可选择多个。
接收者	选择 SNMP 接收接口，请参见前面的步骤 1 和步骤 2。
告警等级	选择要发送的告警信息的告警等级。

配置项	说明
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	开启或关闭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。

9.1.6 Syslog 方式通知告警

用户可通过配置 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。

配置项	说明
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。

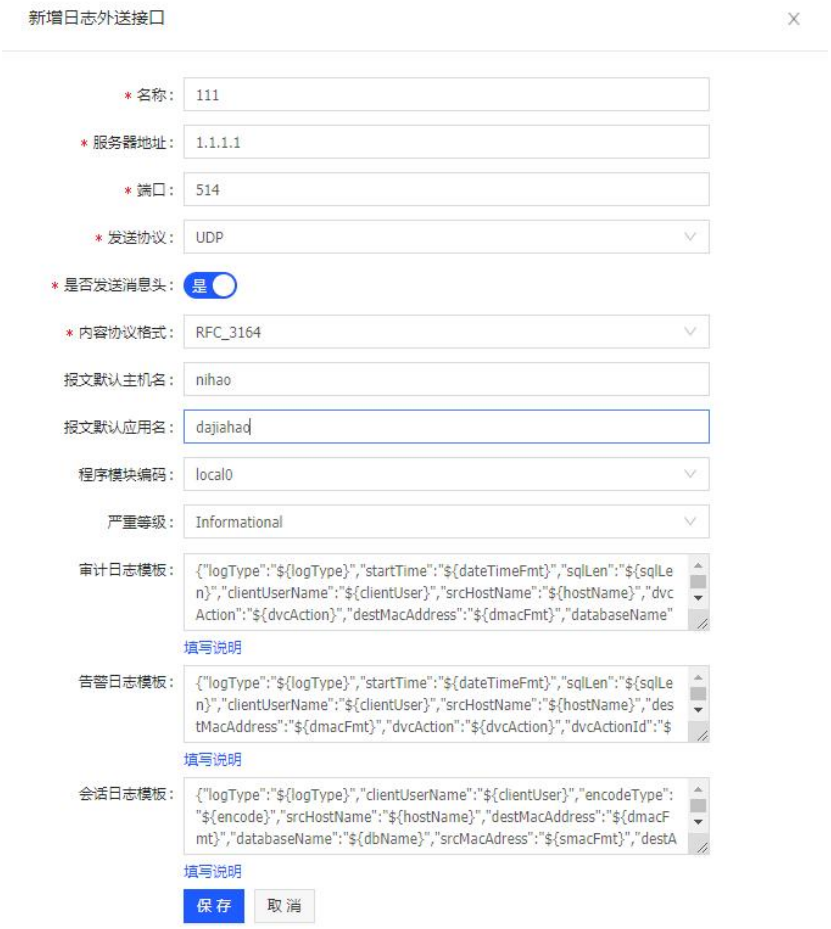
9.2 日志外送

系统通过日志外送接口将日志发送到第三方管理平台，目前系统支持通过 Syslog、Kafka 和邮件三种不同的方式外发日志。发送日志的格式可以根据实际的情况进行调整，并且只有将日志外送接口挂载到数据库资产下才能外发日志。

9.2.1 通过 Syslog 方式外发日志

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

步骤 2.　在**日志外送接口管理**区域点击<**新增**>，进入**新增日志外送接口**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
名称	日志外送接口的配置名称。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。
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	发送日志的传输层协议，可选择 UDP 或者 TCP。
是否发送消息头	选择是否发送消息头。如果选择“否”，发送日志不会包含消息头，只包含数据部分。
内容协议格式	设置发送日志内容所采用的协议格式。请以 Syslog 服务器的实际情况为准。
报文默认主机名	如果选择发送消息头，需要配置默认发送的主机名。此项与 Syslog 服务端配置一致即可。
报文默认应用名	如果选择发送消息头，需要配置默认发送的应用名。此项与 Syslog 服务端配置一致即可。
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 发送日志所标记的严重等级。等级分为：Emergency、Alert、Critical、Error、Warning、Notice、Informational、Debug。
审计日志警模板	设置发送审计日志的模板，具体字段请依据**填写说明**编辑。
告警日志模板	设置发送告警日志的模板，具体字段请依据**填写说明**编辑。
会话日志模板	设置发送会话日志的模板，具体字段请依据**填写说明**编辑

步骤 3. 配置好日志外送接口后，可以给需要发送日志的资产配置发送方式。在**日志外送任务管理**区域点击<**新增**>。

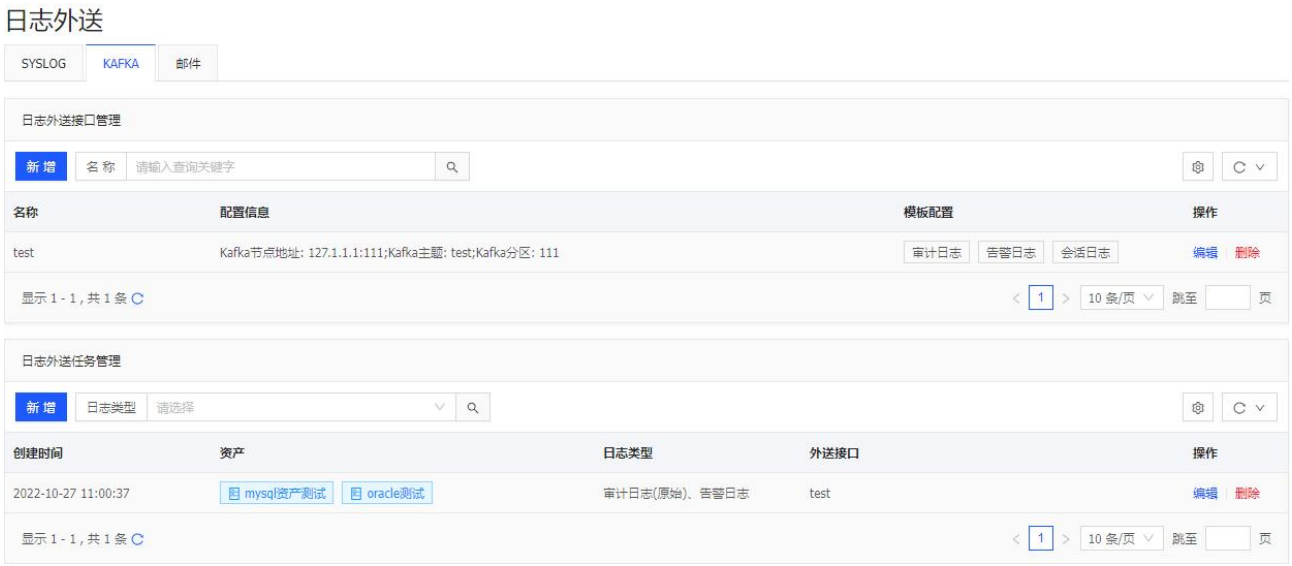
步骤 4. 在弹出的**新增日志外送任务**对话框中编辑相关信息，点击<**确定**>。

详细配置请参见下表。

配置项	说明
资产	选择要发送日志信息的资产，可选择多个。
日志类型	选择要发送的日志类型，可选择多个，包括审计日志(原始)、审计日志(汇聚)、告警日志和会话日志。有关日志类型的更多信息，请参考查询分析。审计日志(汇聚)用于与 AiThink 平台对接时使用。
外送接口	选择 Syslog 日志外送接口，关于 Syslog 日志外送接口可参考前文的步骤 1 和步骤 2。
外送选项	过滤不完整日志，过滤数据库账号为空的日志。用于与 AiThink 平台对接时使用，其他情况建议取消。

9.2.2 通过 Kafka 方式外发日志

步骤 1. 在**日志外送**页面选择 **KAFKA** 页签，进入如下页面。



步骤 2.　在**日志外送接口管理**区域点击<**新增**>，进入**新增日志外送接口**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

配置项	说明
名称	日志外送接口的名称。必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，长度不超过 64 字符。
Kafka 节点地址	Kafka 服务器的 IP（域名）及端口号。例如：192.168.0.1:9200 或者 www.123.com:9200。
Kafka 主题	消息投放到 Kafka 服务器的主题。
Kafka 分区	消息投放到的 Kafka 服务器的分区。Kafka 服务器通过主题（topic）、分区（partition）和消费组（consumer group）三个概念灵活适应各种消息场合，通过提升硬件资源利用率提高系统吞吐量。 以上 Kafka 相关配置与服务器端保持一致即可。
审计日志警模板	设置发送审计日志的模板，具体字段请依据**填写说明**编辑。
告警日志模板	设置发送告警日志的模板，具体字段请依据**填写说明**编辑。
会话日志模板	设置发送会话日志的模板，具体字段请依据**填写说明**编辑

步骤 3. 配置好 Kafka 日志外送接口后，可以为需要发送日志的资产设置发送方式。在**日志外送任务管理**区域点击<**新增**>。

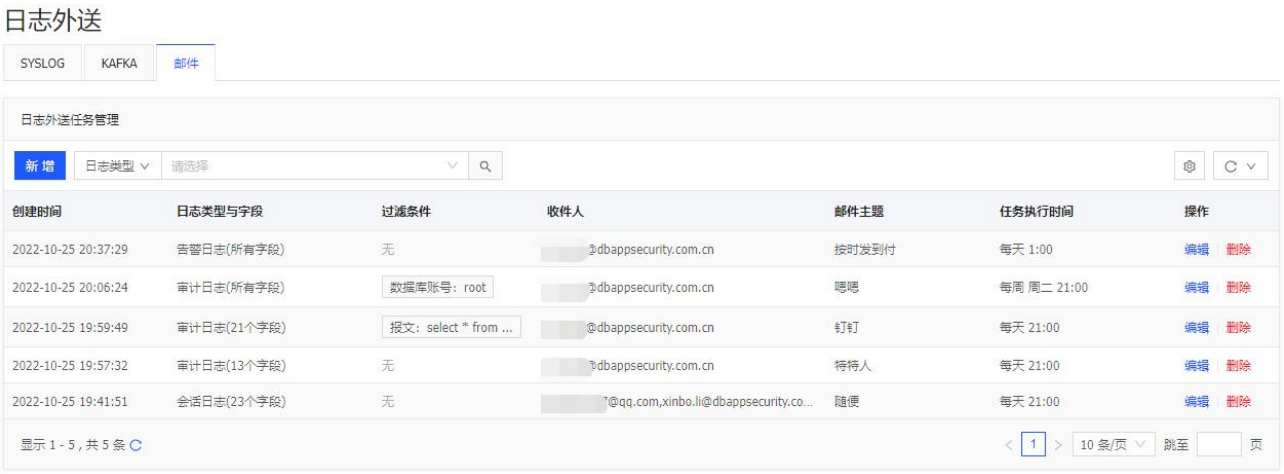
步骤 4. 在弹出的**新增日志外送任务**对话框中编辑相关信息，点击<**确定**>。

详细配置请参见下表。

配置项	说明
资产	选择要发送日志信息的资产，可选择多个。
日志类型	选择要发送的日志类型，可选择多个，包括审计日志(原始)、审计日志(汇聚)、告警日志和会话日志。有关日志类型的更多信息，请参考查询分析。审计日志(汇聚)用于与 AiThink 平台对接时使用。
外送接口	选择 Kafka 日志外送接口，关于 Kafka 日志外送接口可参考前文的步骤 1 和步骤 2。
外送选项	过滤不完整日志，过滤数据库账号为空的日志。用于与 AiThink 平台对接时使用，其他情况建议取消。

9.2.3 通过邮件方式外送日志

步骤 1. 在**日志外送**页面选择**邮件**页签，进入如下页面。



步骤 2. 在**日志外送任务管理**区域点击<**新增**>，进入**新增日志外送接口**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
日志类型	选择发送的日志类型，单选。可以选择审计日志、告警日志、会话日志。
外送字段	选择发送的字段，例如审计 ID、数据库账号、执行时长等。默认为空表示全选。
筛选条件	可根据审计 ID、数据库账号、执行时长进行筛选，同日志模块搜索筛选。
收件人	填写邮件发送对象的收件人，可填写多个，使用“，”进行分割。
邮件主题	设置发送邮件的主题。
邮件正文	设置发送邮件的正文。
任务周期	选择任务周期（日报，周报，月报，年报），默认为“每天”。
发送时间	指定日志发送的时间。

10 系统管理

系统管理是指超级管理员或系统管理员对系统运行参数的设置、对系统资源的维护等，使系统更好地适配实际业务场景。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、系统告警和操作日志。

10.1 用户管理

用户管理主要是指对用户权限及用户认证等进行管理。包括用户管理、远程认证配置、角色管理、用户安全配置、动态令牌管理以及授权数据库。

10.1.1 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，点击<**添加用户**>。

步骤 2. 进入**添加用户**页面，编辑相关信息，点击<**保存**>。

详细配置项和说明请参见下表。

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。

配置项	说明
角色	指定用户角色，包括内置角色和用户自定义角色，必填。有关角色设置的更多信息，请参考角色管理。
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”或者“密码+动态令牌登录”。有关动态令牌配置的更多信息，请参考动态令牌管理。
登录 IP/MAC 限制	对用户登录系统时使用的 IP/MAC 进行限制。包括不限制、黑名单和白名单三种模式。
登录时间限制	限制用户登录系统的时间。

10.1.2 授权数据库

授权数据库是为用户授权指定的数据库，即允许用户审计对指定数据库的操作。

添加授权的操作方法如下：

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，选择**授权数据库**页签，点击<**添加授权**>。

步骤 2. 进入**新增授权规则**页面，编辑名称，选择状态、用户、资产，点击<**保存**>。

10.2 Agent 管理

审计代理插件（Agent）是安装在数据库系统或者业务系统上的插件，其功能是捕获访问数据库系统的数据包，并将数据包发送至数据库审计。当数据库系统部署在公有云、私有云或者实际场景下无法进行端口镜像时，可以通过流量代理的方式抓取数据库流量。

Agent 工作原理

- Agent 在数据库服务器的接口上抓取属于资产下发的 IP+Port 的数据库操作的流量。
- Agent 包含两个进程：dbagent.exe 和 dbMonitor.exe。DBAgent 与数据库审计的 13001 端口建立连接负责流量转发，DBMonitor 与数据库审计的 13002 端口建立连接负责控制部分，包含接收数审下发的资产和其他配置。

Agent 支持的宿主机的类型如下表所示。

操作系统	系统位数	支持版本

操作系统	系统位数	支持版本
Ubuntu	X64	14.04、16.04、18.04
Debian	X64	7.6、8.7、9.5、10.11、11.2
CentOS	X64	5.11、6.0、7.4、7.6、8
RedHat	X64	6.5、7.0、7.5
SUSE	X64	11SP4、12SP4
Solaris X86	X86	5.10、5.11
Solaris Sparc	X64	5.10
AIX		5.3、6.1、7.1
Windows	X64	7、10
Windows	X86	7
Windows Server	X64	2003、2008、2012、2016、2022
euleros（欧拉）	x64	EulerOS2.0 SP9
银河麒麟	aarch64	V10 服务版
兆芯 cpu+银河麒麟系统	X64	V10 服务器版
兆芯 cpu+中标麒麟系统	X64	7

操作系统	系统位数	支持版本
兆芯 cpu+统信 UOS	X86	V20
海光 cpu+统信 UOS	X64	V20
鲲鹏 cpu+统信 UOS	aarch64	V20

Agent 管理用于对审计代理 Agent 的管理维护。用户可通过 SSH 远程安装、下载后手动安装，以及对安装好的 Agent 进行管理。

10.2.1 通过 SSH 远程安装 Agent

用户可以通过 SSH 协议将 Agent 自动安装到需要审计的服务器上，目前仅支持 Linux 系统。

用户在界面上输入需要审计的服务器 IP、SSH 端口、root 用户名、密码，数据库审计通过 scp 协议将 agent 安装包传输到宿主机上并自动安装。

步骤 1. 在菜单栏选择“**系统管理➢Agent 管理**”进入 **Agent 管理**页面，选择 **Agent 安装**页签。

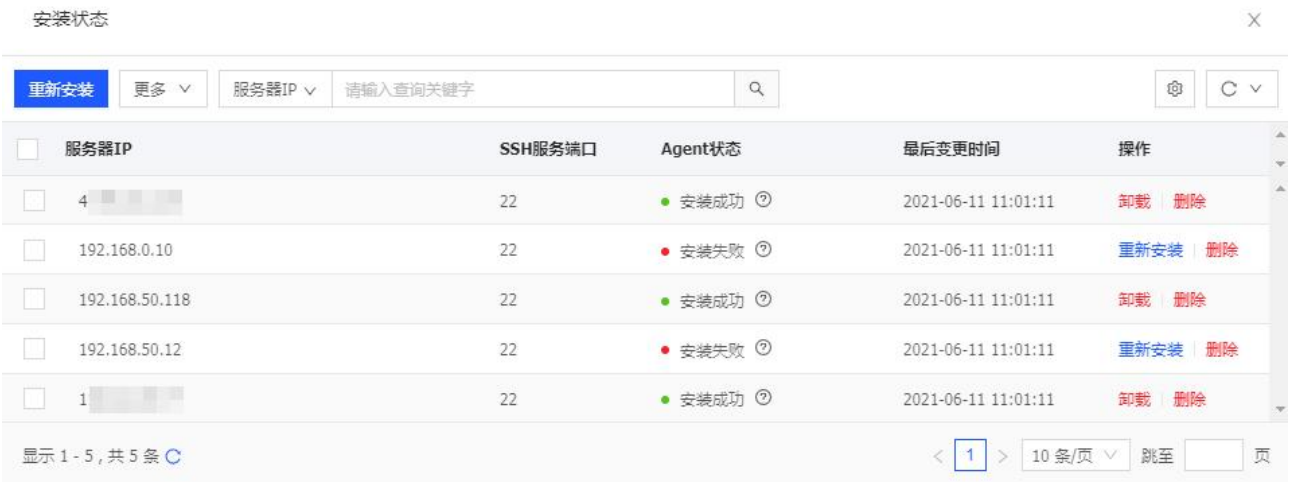
步骤 2. 点击<**开始安装**>进入**通过 SSH 远程安装 Agent** 页面，编辑审计服务器 IP，并添加安装 Agent 的服务器，点击<**安装**>。

详细配置项和说明请参见下表。

配置项	说明
审计服务器 IP	一般默认为当前的审计服务器 IP，用户可以根据需要修改。
安装 Agent 的服务器	支持表单格式和文本格式输入。输入需要安装 Agent 的服务器 IP 及该服务器 root 账户的密码，默认端口为 22，用户可以根据实际情况修改。支持 IPv4 和 IPv6，最多填写 20 个。

点击<**安装状态**>进入安装状态查看页面，可执行以下操作：

- 点击<**卸载**>可远程卸载已经成功安装了的 Agent。
- 点击<**重新安装**>可对未成功安装 Agent 的服务器重新安装。
- 将光标悬停至“安装失败”后的图标，查看安装失败原因。



10.2.2 手动安装 Agent

10.2.2.1 下载 Agent 安装包

用户可手动下载 Agent 安装包，并将其手动安装到需要审计的服务器上。目前支持 Windows 系统和部分 Linux 系统。

下载 Agent 安装包的操作方法如下：

在菜单栏选择“**系统管理➢Agent 管理**”进入 **Agent 管理**页面，选择 **Agent 安装**页签，点击下载对应版本的 Agent 安装包。

- 下载的 Agent 默认会将流量转发给当前的数据库审计。如需转发到其他数据库审计，请在解压后的 Agent 路径下 agent.ini 配置文件中找到 serviceIp 选项进行地址修改。
- 无论是 Linux 版本安装包、AIX 版本安装包还是 Windows 版本安装包，文件夹中均有“ReadMe”文档，文档内包含使用说明、文件说明、注意事项、运行环境说明、配置文件说明。在安装前请仔细阅读该文档并严格按照要求进行操作。

10.2.2.2 Linux 操作系统安装 Agent 程序

10.2.2.2.1 离线安装

步骤 1. 安装包下载完之后，将 Agent 安装包上传到 Linux 服务器指定目录。

- 禁止直接运行二进制文件。
- 解压目录不能出现空格。
- 每次更换运行或解压目录需重新运行安装脚本。
- Linux 环境需以 root 用户运行脚本，指定解释器 bash，或不指定解释器直接运行。

步骤 1. 使用“tar –xf dbAgent_V2.28.tar.gz”命令解压 Agent 安装包，进入 Agent 安装目录。

```
[root@oracle dbagent2.29]# ll
总用量 16032
-rw-r--r-- 1 root root      864 6月   2 16:32 agent.ini
drwxr-xr-x 2 root root     4096 6月   2 16:32 certificate
-rwxr-xr-x 1 root root 12485304 6月   2 16:32 dbAgent
-rwxr-xr-x 1 root root   144016 6月   2 16:32 dbAgentHookMysql.so
-rwxr-xr-x 1 root root   193896 6月   2 16:32 dbAgentHookOracle.so
-rwxr-xr-x 1 root root   143808 6月   2 16:32 dbAgentHookPGsql.so
-rwxr-xr-x 1 root root     4477 6月   2 16:32 dbagent_start.sh
-rwxr-xr-x 1 root root     1384 6月   2 16:32 dbagent_stop.sh
-rwxr-xr-x 1 root root  3375960 6月   2 16:32 dbMonitor
-rwxr-xr-x 1 root root     2266 6月   2 16:32 installHook.sh
-rwxr-xr-x 1 root root     6732 6月   2 16:32 install.sh
-rw-r--r-- 1 root root       82 6月   2 16:32 md5sum.txt
-rw-r--r-- 1 root root     2003 6月   2 16:32 ReadMe
drwxr-xr-x 2 root root     4096 6月   2 16:32 tool
-rwxr-xr-x 1 root root      778 6月   2 16:32 uninstallHook.sh
-rwxr-xr-x 1 root root     3866 6月   2 16:32 uninstall.sh
-rw-r--r-- 1 root root       46 6月   2 16:32 version.txt
```

步骤 2. 在安装目录执行“./install.sh”命令即可安装 Agent 程序。

```
[root@oracle dbagent2.29]# ./install.sh
2022年 06月 02日 星期四 16:43:32 CST
Install dbagent...
Install dbagent success
Start dbagent...
Start dbagent success
[root@oracle dbagent2.29]#
```

10.2.2.2.2 在线安装

以 root 用户登录 Linux 服务器操作系统 CLI 界面，执行在线安装命令。

wget https://10.20.49.201/linux64/dbagent.sh --no-check-certificate -O dbagent.sh && chmod 755 dbagent.sh && ./dbagent.sh 10.20.49.201

Agent 程序安装完成并运行之后，登录系统 Web 管理平台，在菜单栏选择“**系统管理➢Agent 管理**”，选择 **Agent 管理**页签进入 Agent 管理列表页面，查看 Agent 连接状态信息。

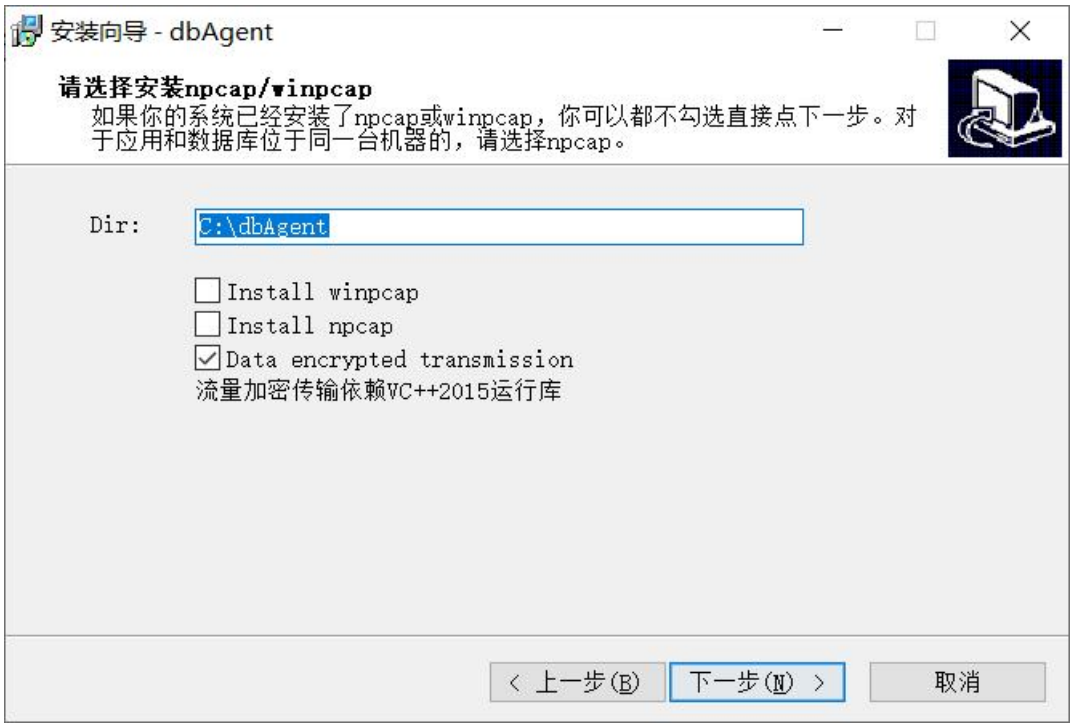
10.2.2.3 Windows 操作系统安装 Agent 程序

10.2.2.3.1 离线安装

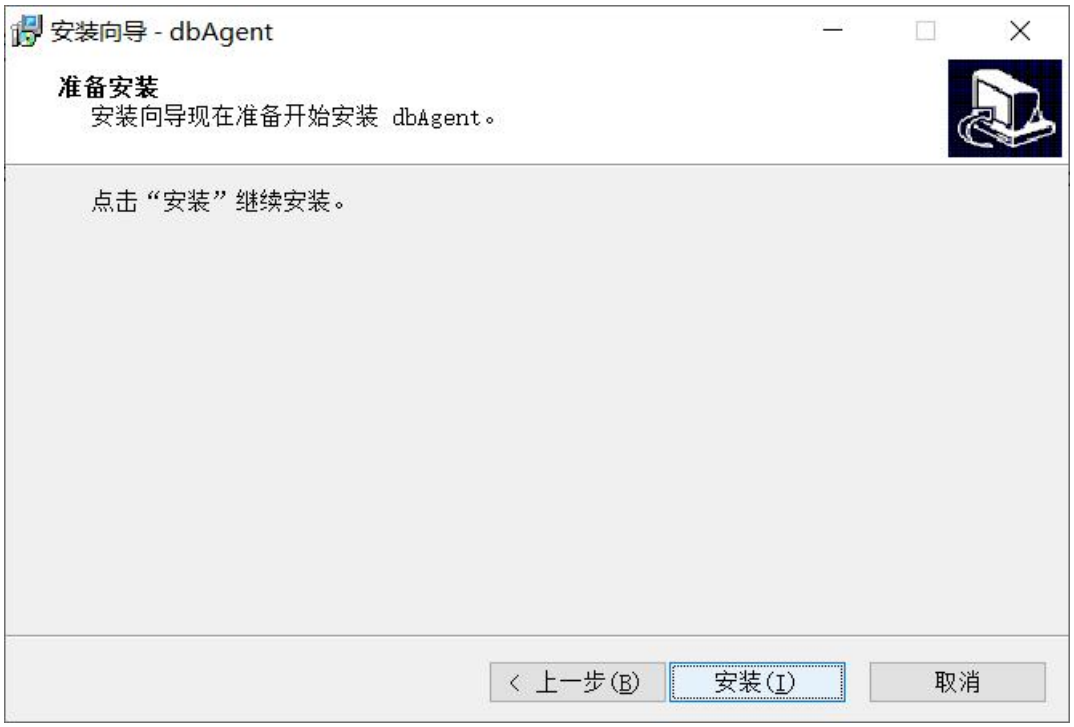
步骤 1. 安装包下载完成之后，将 Agent 安装包上传到 Windows 服务器上。

步骤 2. 解压压缩包到指定运行目录。在 Agent 的安装目录以管理员身份运行“dbAgent-setup.exe”进入安装向导，点击<**下一步>**，如下图所示。

步骤 3. 点击<**下一步**>之后显示“Install winpcap”和“Install npcap”两个选项。如果没有本地审计的需求请选择“Install winpcap”；如果需要部署本地审计，则选择“Install npcap”。默认推荐使用“Install winpcap”安装方式，对于 Windows 操作系统的兼容性较好。“Data encrypted transmission”仅需要配置 agent 数据传输加密情况下才需要勾选。并点击<**下一步**>。

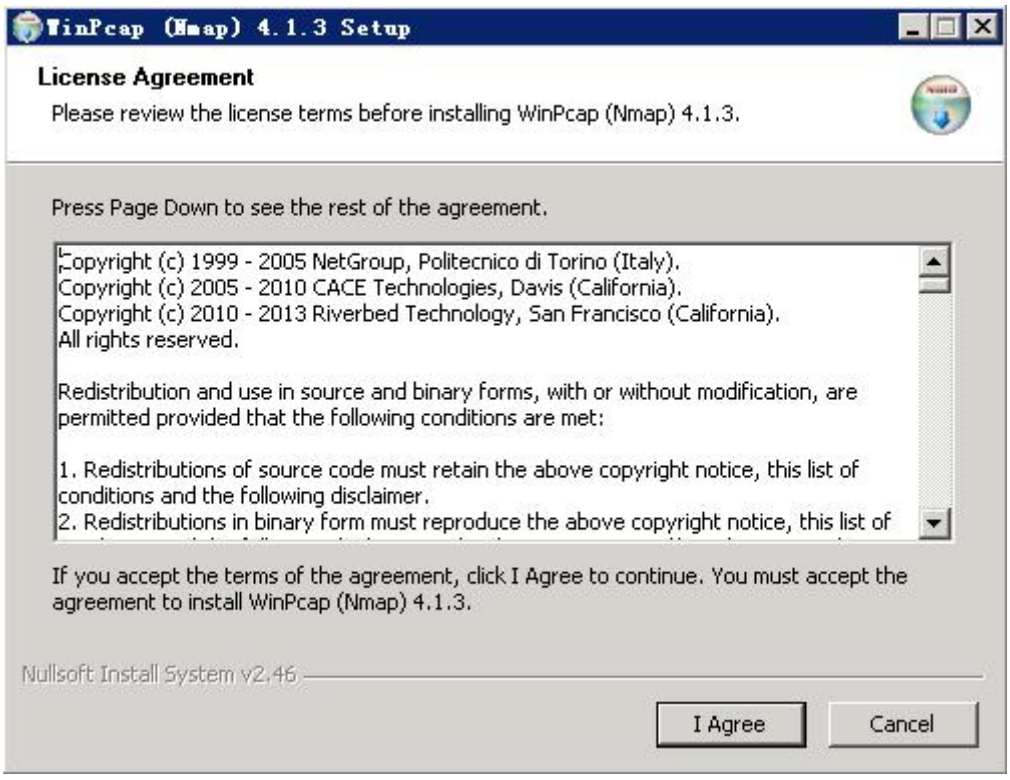


步骤 4. 点击<**安装**>。

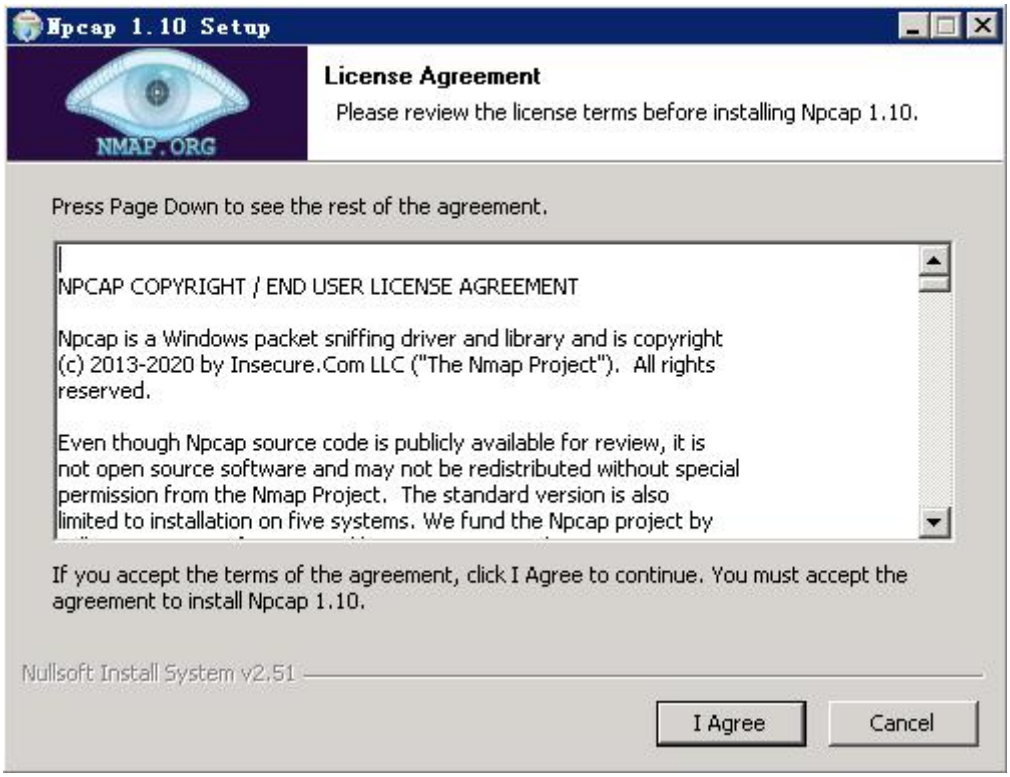


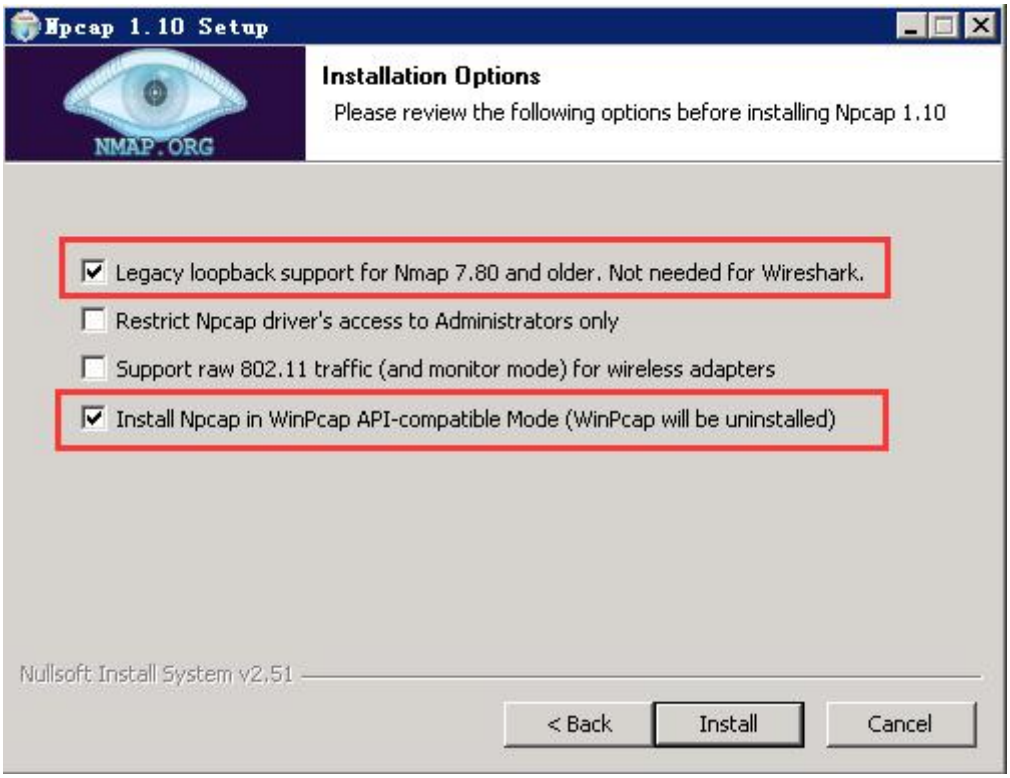
步骤 5. 点击<**I Agree**>同意安装协议后，之后按照提示进行操作。

由于上述步骤 3 中选择的项不同，具体操作有所区别，“Winpcap”插件默认安装即可。



“Npcap”插件需要按照下图中的示例勾选第一项和默认勾选的最后一项，随后按照提示默认安装即可，安装完成后即可退出。





MICROSOFT VISUAL STUDIO 2015 仅配置 agent 数据传输加密才需要安装。

步骤 6. 安装完成后点击<**完成**>退出安装向导。

10.2.2.3.2 在线安装

步骤 1. 登录 Windows 服务器，用浏览器访问在线安装链接下载安装包。

步骤 2. 使用安装包安装 Agent，具体操作请参见离线安装。

Agent 程序安装完成并运行之后，登录系统 Web 管理平台，在菜单栏选择“**系统管理➤Agent 管理**”，选择 **Agent 管理**页签进入 Agent 管理列表页面，查看 Agent 的连接状态。

- 禁止直接运行二进制文件。
- 解压目录不能出现以下特殊字符：<space>()[]{}^=;!'+,`~(&()，若必需要在含特殊字符的目录中运行脚本，请选择以管理员权限进入 DOS 命令行运行脚本。此外，解压目录不能为中文字符。
- 如要自行更改配置文件，请确保不要更改文件编码格式。
- 若要强制结束 Agent 进程运行，请先结束 dbMonitor 进程，然后结束 dbAgent 进程。

10.2.2.4 AIX 操作系统安装 Agent 程序

步骤 1. 安装包下载完之后，将 Agent 安装包上传到 AIX 服务器指定目录。

```
root@localhost test]#ll
total 13696
-rw-r--r--    1 root     system      7011142 Jun 05 18:43 dbagent_aix5.3_V2.257.tar.gz
root@localhost test]#
```

- 禁止直接运行二进制文件。
- 解压目录不能出现空格。
- 每次更换运行或解压目录需重新运行安装脚本。
- AIX 环境需以 root 用户运行脚本，指定解释器 bash，或不指定解释器直接运行。

步骤 2. 先使用“gunzip dbagent_aix5.3_V2.257.tar.gz”命令解压 Agent 安装包，生成 tar 包，再使用“tar -xvf dbagent_aix5.3_V2.257.tar”命令解压 tar 包。

```
root@localhost test]#gunzip dbagent_aix5.3_V2.257.tar.gz
root@localhost test]#ll
total 50080
-rw-r--r--    1 root     system     25640960 Jun 05 18:43 dbagent_aix5.3_V2.257.tar
root@localhost test]#tar -xvf dbagent_aix5.3_V2.257.tar
x dbagent2.257
x dbagent2.257/agent.ini, 684 bytes, 2 media blocks.
x dbagent2.257/dbAgent, 6558783 bytes, 12811 media blocks.
x dbagent2.257/dbagent_start.sh, 2105 bytes, 5 media blocks.
x dbagent2.257/dbagent_stop.sh, 1165 bytes, 3 media blocks.
x dbagent2.257/dbMonitor, 2480126 bytes, 4844 media blocks.
x dbagent2.257/install.sh, 3847 bytes, 8 media blocks.
x dbagent2.257/lib
x dbagent2.257/lib/libpcap.a, 1405067 bytes, 2745 media blocks.
x dbagent2.257/lib/libgcc_s.a, 1004984 bytes, 1963 media blocks.
x dbagent2.257/lib/libstdc++.a, 11509097 bytes, 22479 media blocks.
x dbagent2.257/rpm
x dbagent2.257/rpm/bash-5.0-8.aix5.1.ppc.rpm, 2584873 bytes, 5049 media blocks.
x dbagent2.257/tool
x dbagent2.257/tool/agent.conf, 48 bytes, 1 media blocks.
x dbagent2.257/tool/getip, 8929 bytes, 18 media blocks.
x dbagent2.257/tool/cpulimit, 50857 bytes, 100 media blocks.
x dbagent2.257/tool/update.sh, 1934 bytes, 4 media blocks.
x dbagent2.257/tool/get_io_usage.sh, 581 bytes, 2 media blocks.
x dbagent2.257/tool/prepare_update.sh, 246 bytes, 1 media blocks.
x dbagent2.257/uninstall.sh, 2051 bytes, 5 media blocks.
x dbagent2.257/version.txt, 47 bytes, 1 media blocks.
root@localhost test]#
```

步骤 3.　在安装目录执行“./install.sh”命令即可安装 Agent 程序。

```
root@localhost dbagent2.257]#./install.sh
Install dbagent...
Install dbagent success
/test/dbagent2.257/dbAgent needs:
        /usr/lib/libc.a(shr.o)
        /usr/lib/libpthread.a(shr_xpg5.o)
        /test/dbagent2.257/lib/libstdc++.a(libstdc++.so.6)
        /test/dbagent2.257/lib/libgcc_s.a(shr.o)
        /test/dbagent2.257/lib/libpcap.a(shr.o)
        /unix
        /usr/lib/libcrypt.a(shr.o)
        /usr/lib/libpthreads.a(shr_comm.o)
        /usr/lib/libodm.a(shr.o)
        /usr/lib/libcfg.a(shr.o)
Start dbagent...
Start dbagent success
root@localhost dbagent2.257]#
```

Agent 程序安装完成并运行之后，登录系统 Web 管理平台，在菜单栏选择“**系统管理➤Agent 管理**”，选择 **Agent 管理**页签进入 Agent 管理列表页面，查看 Agent 连接状态信息。

10.2.3 Agent 管理

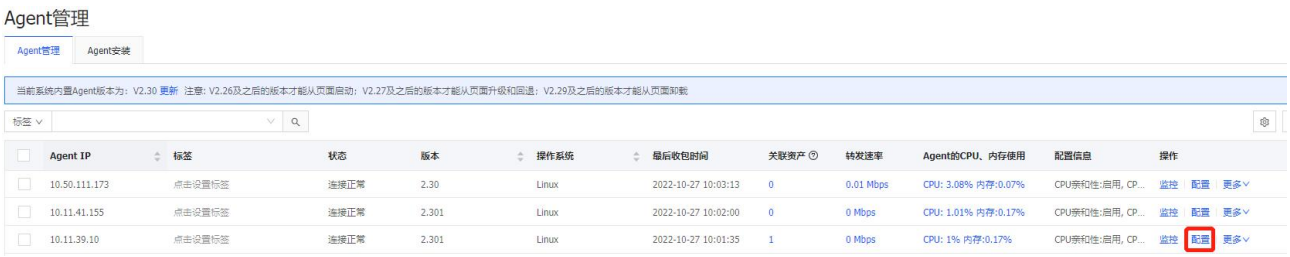
在菜单栏选择“**系统管理➤Agent 管理**”，选择 **Agent 管理**页签进入 **Agent 管理**页面。Agent 管理页面可展示全部成功连接过的 Agent 列表。列表中展示 Agent 的详细信息，并能监控 Agent 的运行状态。此外可配置 Agent 关键运行参数，实现远程挂起、停止、升级和回退 Agent 服务，下载当前 Agent 的近期日志和 Agent 运行状态诊断，提供标签和卸载删除 Agent 的功能。

10.2.3.1 监控 Agent 状态

在 **Agent 管理**页面，在已安装 Agent 列表的**操作**列下点击<**监控**>进入 Agent **监控信息**页面，用户可以根据需要设置监控的时段，或者选择不同的监控指标（CPU 占用、内存占用、转发速率、丢包数量、磁盘读写）。

10.2.3.2 修改 Agent 配置

步骤 1. 在 **Agent 管理**页面，在 Agent 列表中点击**操作**列中的<**配置**>。



步骤 2. 弹出**修改 Agent 配置**对话框，可根据需要修改相关参数，修改完成后点击<**确定**>。

◆ 资源使用限制

详细配置项和说明请参见下表。

配置项	说明
CPU 亲和性	启用后，Agent 将仅在单颗 CPU 核心上工作。

配置项	说明
	CPU 亲和性指的是进程在指定的 CPU 上尽量长时间运行而不被迁移到其他处理器，也称为 CPU 关联性。在多核运行的机器上，每个 CPU 会有缓存，缓存着进程使用信息，如果进程被调度到其他 CPU 上，CPU 缓存命中率会降低，导致处理性能降低。一旦修改配置，Agent 会自动重启生效。
CPU 使用上限	默认值为 100%，取值范围：0%~100%，填 0 表示不限制。
内存使用上限	Agent 缓存数据包所用的内存，默认值 200MB，不能超过设备的最大内存。

◆ 熔断保护（超过设置的任一阈值时，Agent 暂停工作）

详细配置请参见下表。

配置项	说明
系统 CPU 使用阈值	默认值 100%，取值范围：0%~100%，填 0 表示不限制。
系统内存使用阈值	默认值 100%，取值范围：0%~100%，填 0 表示不限制。

系统磁盘读 IO 阈值	默认值 0，表示不限制。不能超过系统磁盘的最大读速率。
系统磁盘写 IO 阈值	默认值 0，表示不限制。不能超过系统磁盘的最大写速率。

◆ 抓包与过滤设置

详细配置请参见下表。

配置项	**说明**
抓包网口	配置后将只抓取指定网口上的流量，为空时抓取全部网口上的流量，多个网口请用空格分隔。
抓包过滤串	配置后，抓包网口将只抓取匹配该过滤串（通常设置为指定主机的指定端口流量，例如：host 192.168.0.1 and port 3306）的流量。一旦配置，将不再根据配置的资产自动抓包。
按工具过滤	填写后将不再转发指定客户端工具的流量，可填写多个，多个值请用逗号分隔。
按账号过滤	填写后将不再转发指定数据库账号的流量，可填写多个，多个值请用逗号分隔。

◆ 本地回环审计配置

系统支持本地回环审计功能，此功能可以实现不通过 TCP/IP 连接的本地数据库访问审计。

本地回环审计是指 Agent 为客户端工具注入.so 程序，客户端工具与服务端的通信流量客户端工具会复制一份发送给 Agent，Agent 转发给数据库审计。

Agent 安装成功后，需要在 Web 界面开启“本地审计”功能。

详细配置项和说明请参见下表。

配置项	说明
回环网口	回环网口的名称，为空时会自动识别，不建议配置此项。
回环抓包过滤串	配置后回环网口将只抓取匹配该过滤串的流量。一旦配置，将不再根据配置的资产自动抓包。
回环网口替换 IP (v4/v6)	将流量中本地回环的 IPv4 或 IPv6 地址改为设置的值，为空则不替换。
远程登录审计	默认关闭。启用后，本地流量中的 IP 端口会被远程连接的 IP 端口所替换。需要在资产界面添加被远程连接的服务器 IP 地址，若没有远程连接，则不做替换。一旦开启，性能会明显下降。
本地审计	支持审计非网络形式（进程间通信等）的数据库通信数据，目前仅支持 Oracle，

配置项	说明
	PostgreSQL，MySQL，SQL Server 的特定版本。

◆ 其他

详细配置项和说明请参见下表。

配置项	说明
调试模式	默认关闭。开启后会记录下更详细的调试日志。
数据传输加密	默认关闭。开启后会对 Agent 转发的数据进行加密。
CPU 异常保护阈值	当 Agent 的 CPU 使用超过该值时，Agent 将自动修复异常。正常情况下，Agent 的 CPU 使用不会超出所配的上限,该配置可作为兜底保护，防止特殊情况发生。默认值 100%，填 0 表示关闭 CPU 异常保护功能。
内存异常保护阈值	当 Agent 的内存使用超过该值时，Agent 将自动修复异常。该配置可作为兜底保护，防止特殊情况发生。默认值 300M，填 0 表示关闭内存异常保护功能。

10.2.3.3 Agent 标签

在 Agent 比较多的场景下，Agent 标签方便区分该 Agent 的业务属性或者物理位置等。

◆ 快捷添加移除标签

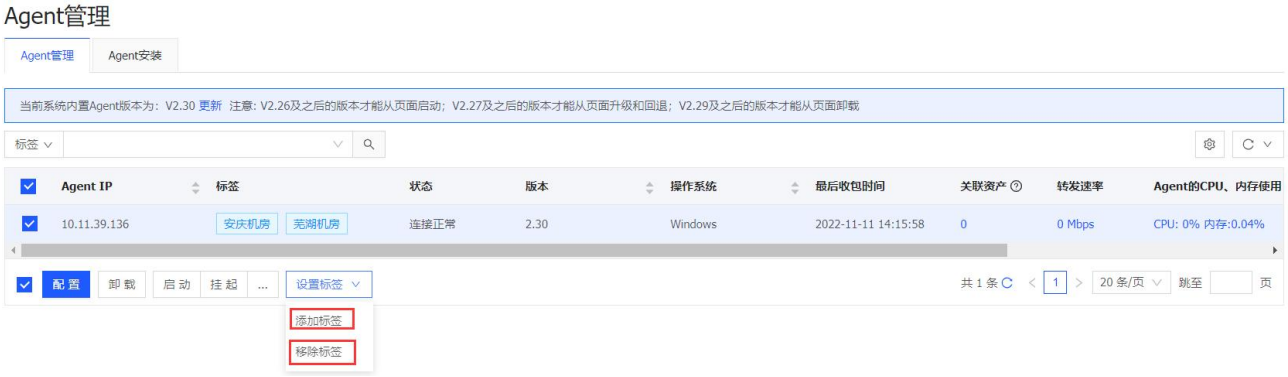
步骤 1. 在 **Agent 管理**页面，点击标签显示列对应区域。

步骤 2. 选择标签或者输入新的标签点击阅读即可完成标签添加。

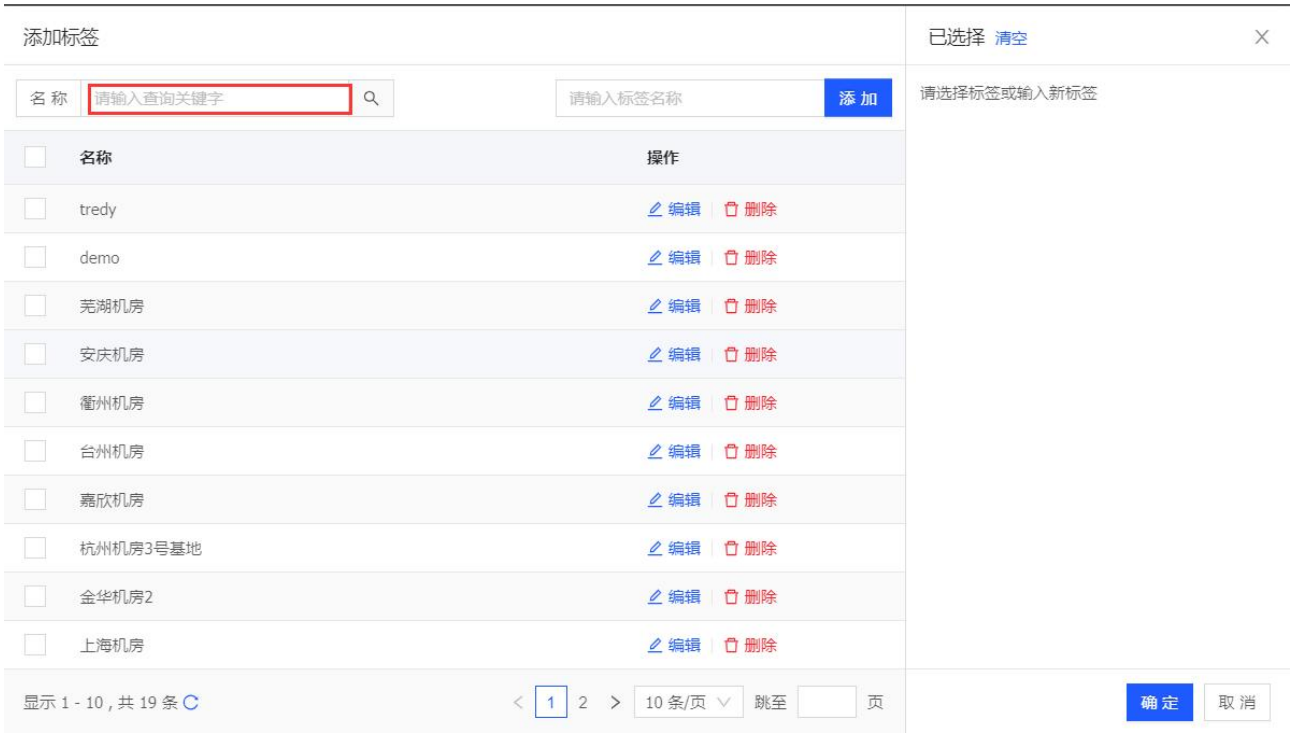
步骤 3. 对应已经有标签的 Agent，可以点击“X”移除该标签。

◆ 标签管理

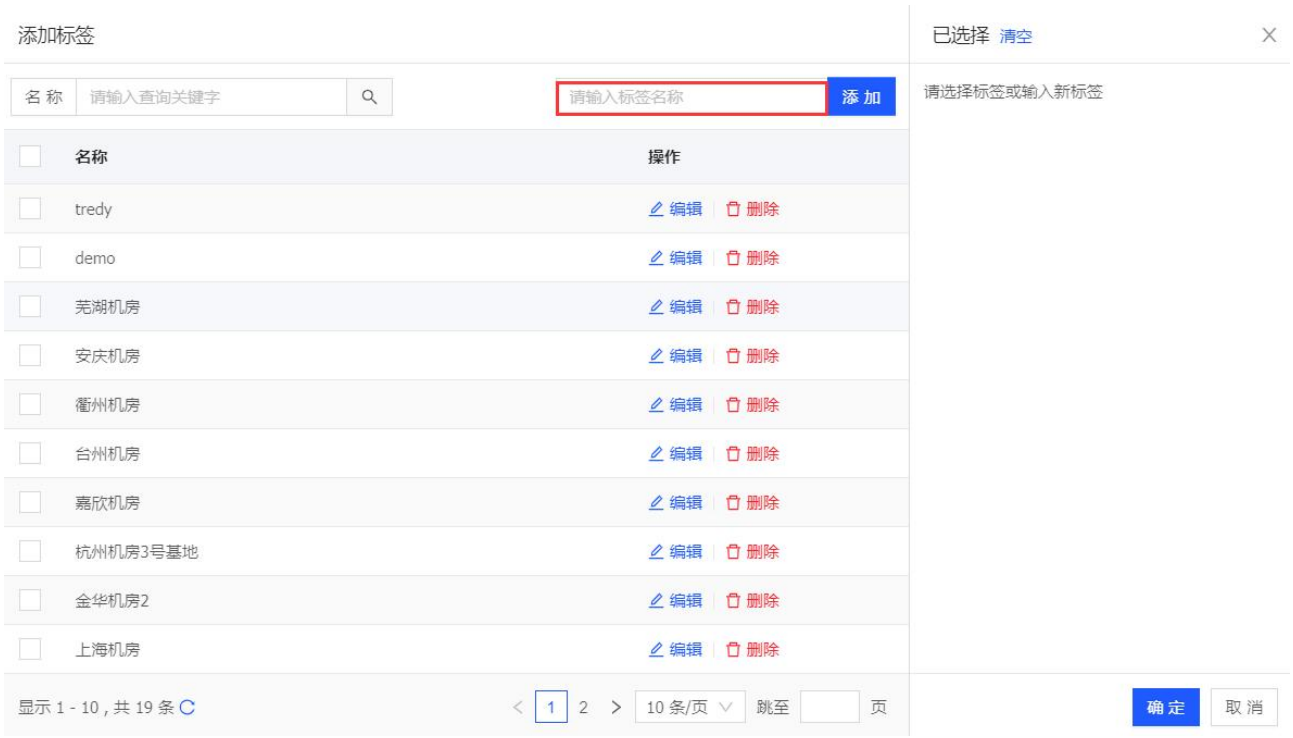
步骤 1. 选中 Agent 列表前方的复选框，鼠标移到设置标签，点击展开列表的<**添加标签**>或者<**移除标签**>可以批量添加或者移除 Agent 标签。



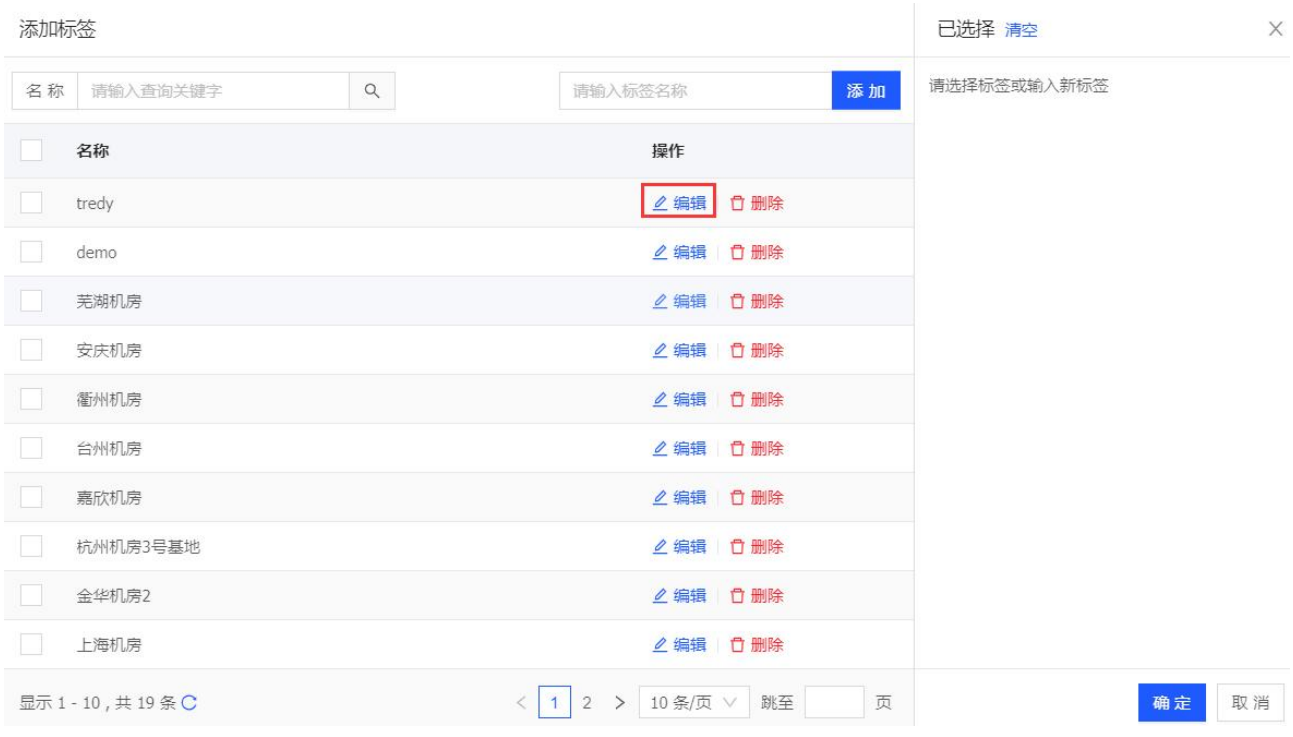
步骤 2. 输入关键字可以根据名称搜索标签。



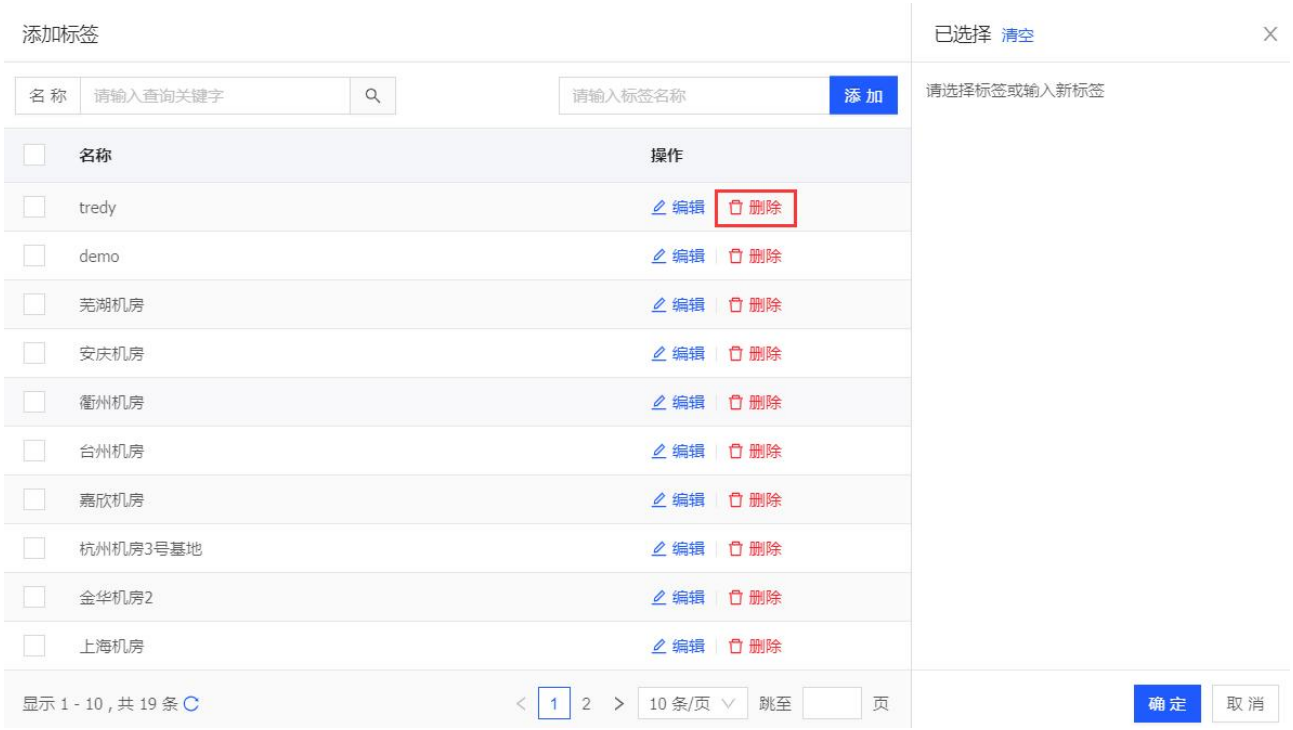
步骤 3. 输入标签名称，点击<**添加**>可以在标签列表中添加新标签。



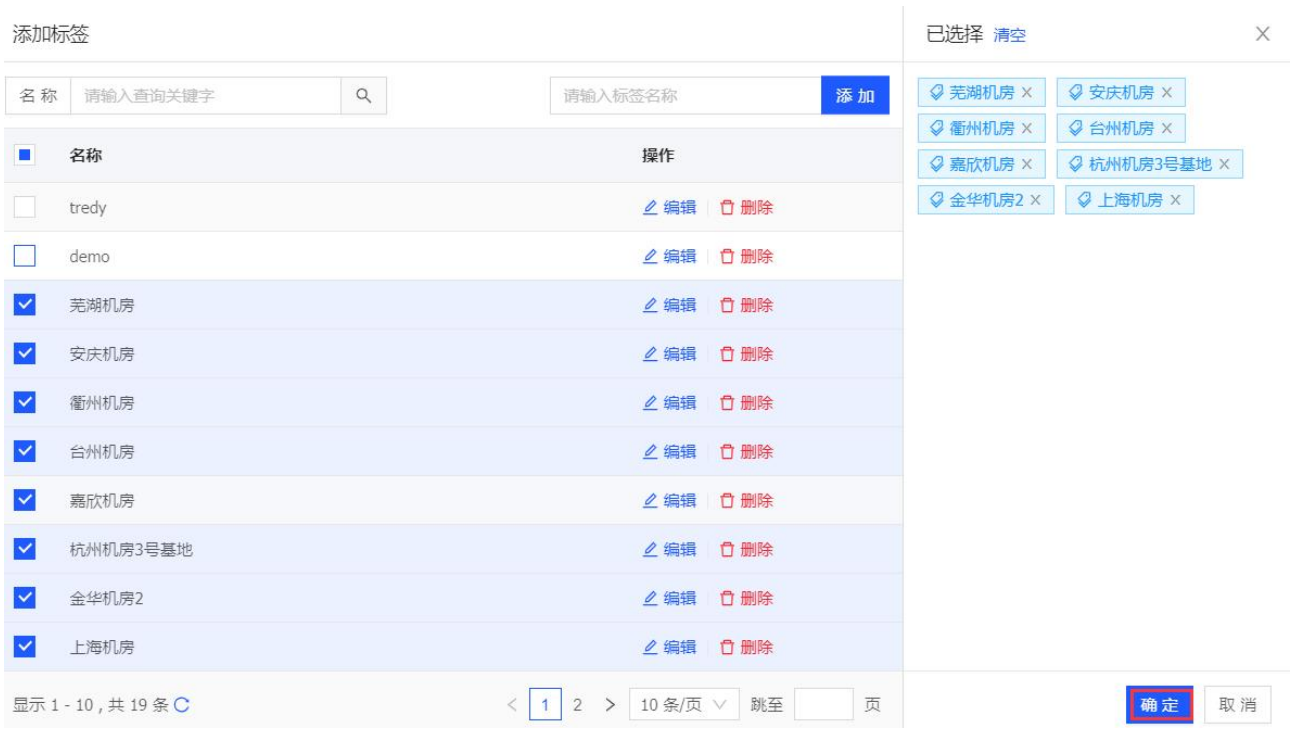
步骤 4.　点击标签列表的<**编辑**>可以对该标签名称进行编辑。



步骤 5.　点击标签列表的<**删除**>可以对该标签名称进行删除。



步骤 6. 选中标签列表前面的复选框，再点击<**确定**>即可完成批量添加或者移除标签。



10.2.3.4 其他操作

Agent 管理页面中的其他操作请参见下表。

操作	说明
挂起	勾选处于“连接正常”状态的 Agent，点击<**挂起**>可以让正在正常运行中的 Agent 不再传送数据，但保持连接状态。
唤醒	勾选处于“挂起”状态的 Agent，点击<**唤醒**>可将该 Agent 转为正常运行状态。
启动	勾选处于“停止”状态的 Agent，点击<**启动**>可将该 Agent 转为正常运行状态。 对于 V4.0.65 之前版本安装的 Agent，处于“停止”状态的 Agent 已经断开链路，不能远程启动，只能登录 Agent 所在服务器后手动启动。
停止	勾选处于“连接正常”或者“挂起”状态的 Agent，点击<**停止**>可停止 Agent。
升级	勾选处于“连接正常”状态的 Agent，点击<**升级**>可将当前 Agent 版本升级至内置 Agent 中的最新版本。
回退	勾选处于“连接正常”状态的 Agent，点击<**回退**>可将当前 Agent 版本退回至升级前的 Agent 版本。
日志	点击**操作**列中的“**更多➤日志**”可下载当前 Agent 的最近 1 天日志。
诊断	点击**操作**列中的“**更多➤诊断**”，查看当前 Agent 运行状态。
卸载	勾选处于“连接正常”、“停止”和“挂起”状态的 Agent，点击<**卸载**>可远程卸载该 Agent。
删除	勾选处于“异常”状态的 Agent，点击<**删除**>可将当前 Agent 重 Agent 列表中删除。

10.3 系统配置

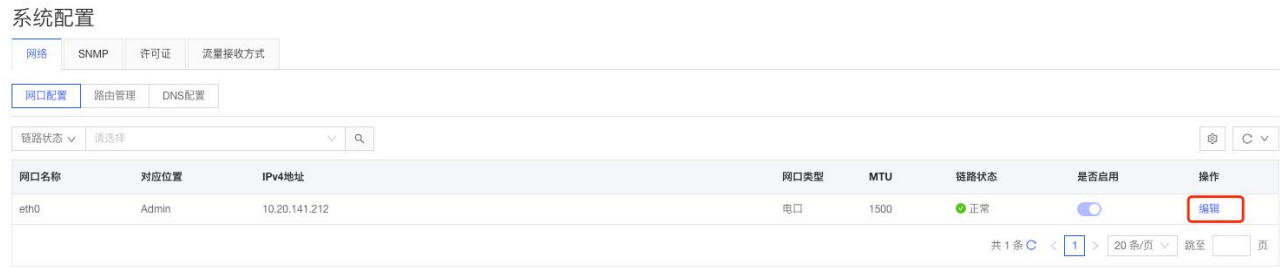
10.3.1 网络

系统支持网口管理、DNS 配置以及路由管理功能。

10.3.1.1 网口管理

修改网口的操作方法如下：

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**网络**页签，点击**操作**列中的<**编辑**>。

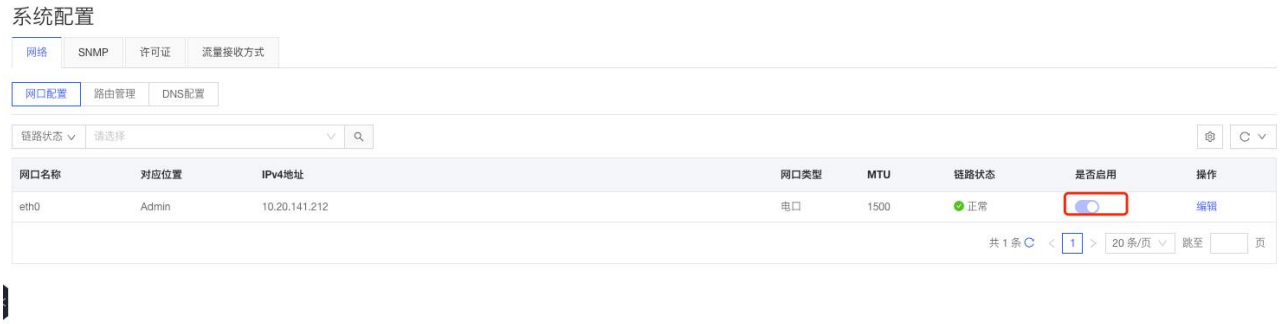


步骤 2. 在弹出的**编辑网口**对话框中修改网口的 IPv4 地址、子网掩码、IPv6 等配置信息，点击<**保存**>。

如果该网口是管理口，除修改网口的 IPv4 地址、子网掩码、IPv6 配置信息，还可设置 IPv4 网关。

修改管理口 IP 后等待 5 秒后页面会自动跳转到新的网址并且需要重新登录系统，重新输入账号密码登录系统才能继续使用。

在网口管理区域的操作列中点击**是否启用**开关，可启用或禁用选中的网口（管理口无法被禁用）。

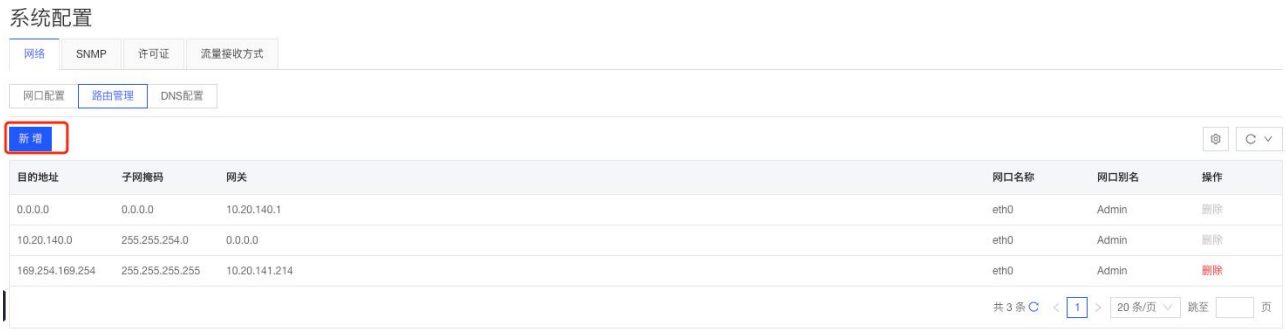


10.3.1.2 路由管理

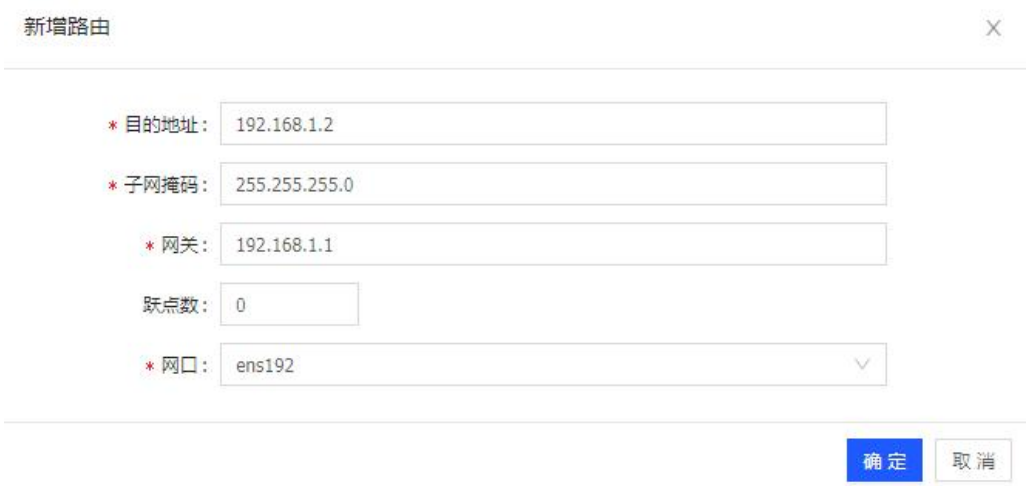
路由管理是指为系统添加静态路由。添加静态路由的目的：为数据库审计去往不同网段的流量指定不同的出接口，使数据库审计可以访问不同网段的主机。

添加静态路由的操作方法如下：

步骤 1. 在**系统配置**页面选择**网络**页签，再选择**路由管理**页签，点击<**新增**>。



步骤 2. 在弹出的对话框中设置路由信息，点击<**确定**>。



详细配置项和说明请参见下表。

配置项	**说明**
目的地址/子网掩码	目的地址与子网掩码定义了目标网络地址，例如 192.168.3.0/255.255.255.0 表示 192.168.3.1~192.168.3.254 的目标主机。
网关	去往目标网络的下一跳地址。
跃点数	报文传输过程中经过的路由设备（路由器或者其他有路由功能的网络设备）的个数，取值范围：0~32,766。

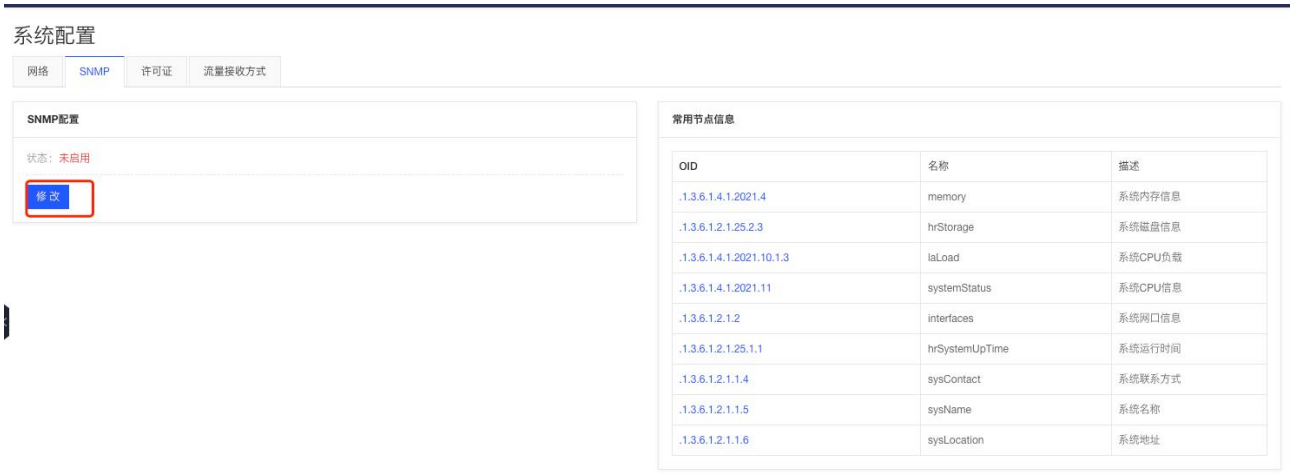
配置项	说明
网口	路由出接口，为设备上的端口。

10.3.2 SNMP

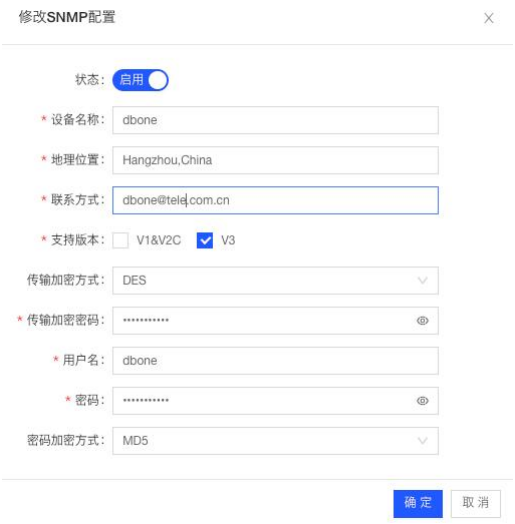
SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议，支持目前主流的网络管理系统，用于监测网络上的设备是否有存在异常情况。系统支持 SNMP，通过 V2 和 V3 版本 SNMP 协议对数据库审计进行远程监控。

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，点击<**修改**>。



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



详细配置项和说明请参见下表。

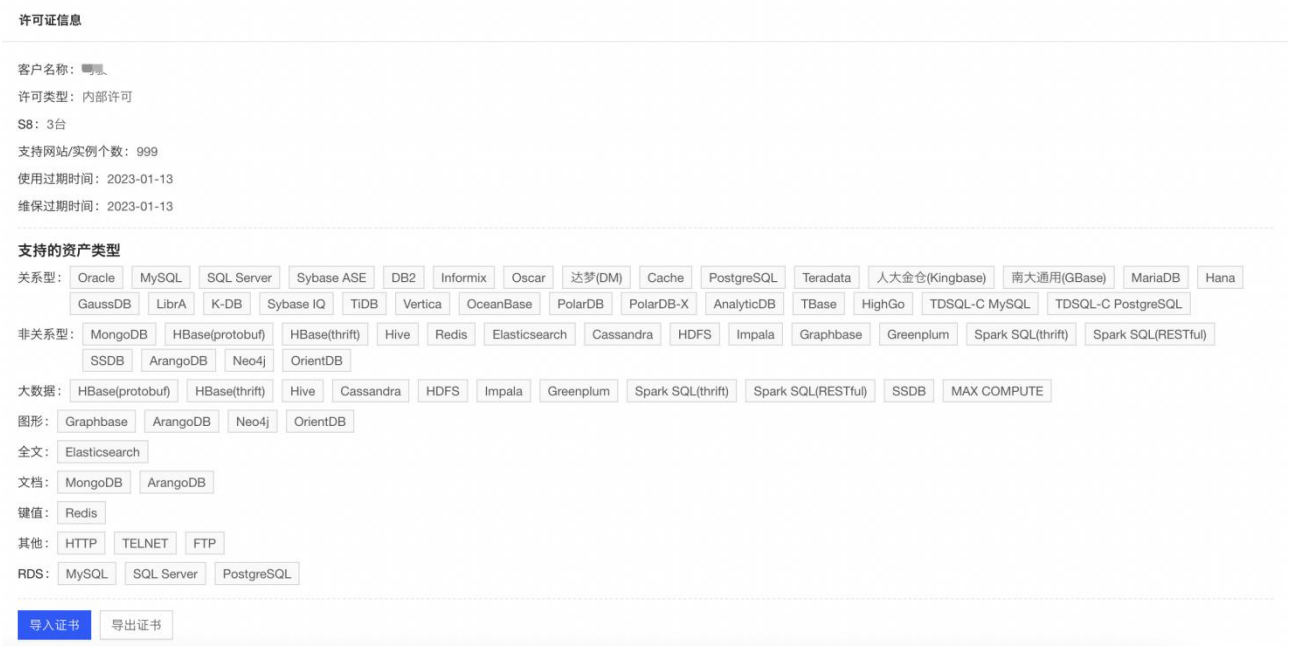
配置项	说明
状态	在设备上启用或禁用 SNMP 功能。
设备名称	设置数据库审计设备自身的名称以方便识别。
地理位置	设备的地理位置。
联系方式	设备管理员的联系方式，可设置为邮箱或电话号码。
支持版本	选择启用的 SNMP 版本，支持 V1&V2C、V3 版本。V1&V2C 版本使用团体字认证方式，V3 版本引入了基于用户的安全模型，比 V1&V2C 版本更安全。
community	定义信息流向，填写“public”，即公开。 当支持版本选择“V1&V2C”时，此参数可配。
传输加密方式	当支持版本选择“V3”时，此参数可配。 选择信息传输的加密方式，目前支持 DES 与 AES 两种方式：

配置项	说明
	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	指定传输过程中的加密密码。 当支持版本选择“V3”时，此参数可配。
用户名/密码	指定 SNMP 通讯双方认证使用的用户名和密码。 当支持版本选择“V3”时，此参数可配。
密码加密方式	指定 SNMP 密码的加密方式，支持 MD5 与 SHA1 两种方式。 当支持版本选择“V3”时，此参数可配。

10.3.3 许可证

许可证（License）是天翼云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，点击**<导出证书>**，可导出系统当前证书；点击**<导入证书>**，上传证书文件，即可更新证书。

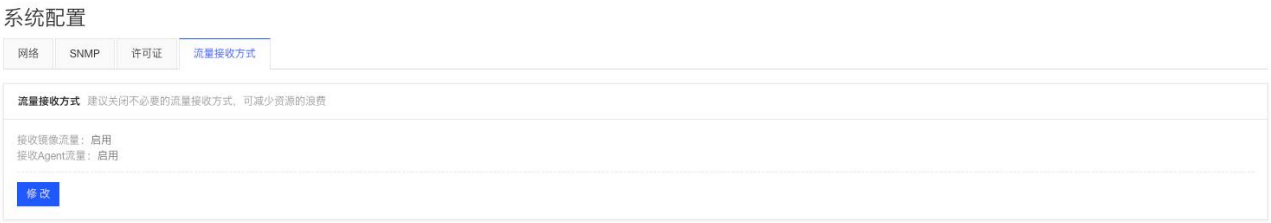


- 当证书使用快过期时，请及时致电天翼云客服热线获取新的证书。
- 建议在导入新的证书前首先导出系统当前证书。
- 请确认证书中允许审计的资产数目。

10.3.4 流量接收方式

流量接收方式显示目前系统配置的日志采集方式。开启哪种方式即代表系统以哪种方式获取数据库流量。建议关闭不必要的日志采集方式，可减少资源占用。

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**流量接收方式**页签，点击<**修改**>。



步骤 2. 弹出**流量接收方式**对话框，可对于流量接收方式进行启用和禁用，点击<**确定**>。

详细配置请参见下表。

配置项	说明
接收镜像流量	默认启用。启用后可以采集数审非 lo 口的所有网卡的流量。
接收 Agent 流量	默认启用。启用后可以安装 Agent，接收 Agent 转发的数据库流量。

10.4 系统维护

10.4.1 时间

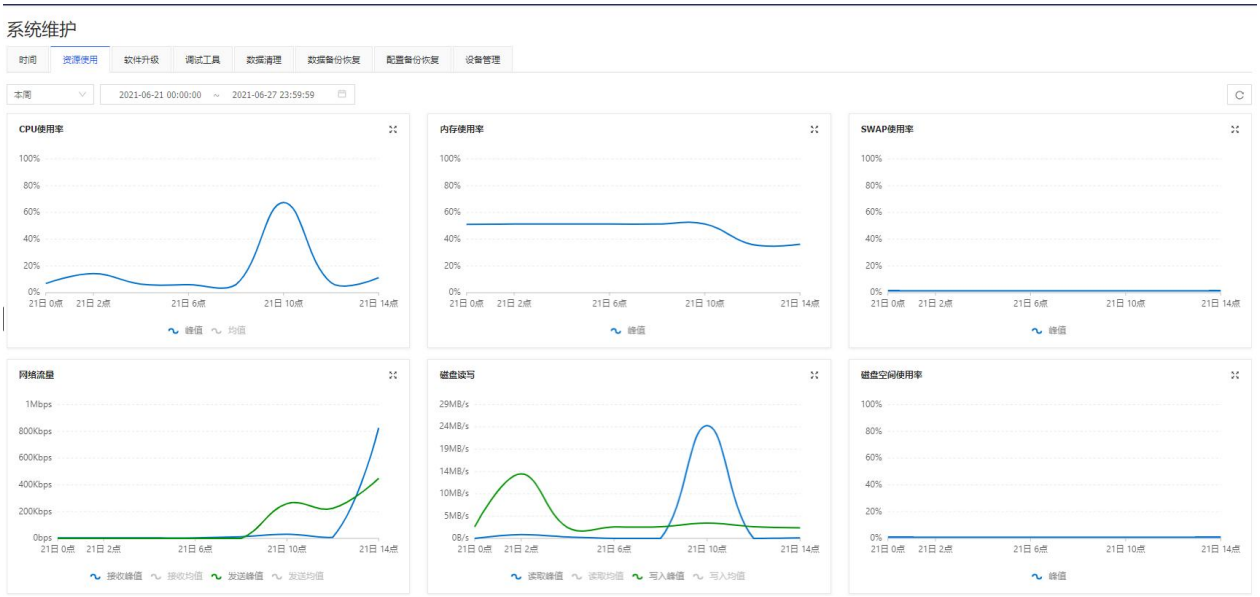
系统支持通过同步浏览器时间和同步 NTP 时钟服务器两种方式调整系统当前时间信息。

- 在菜单栏选择“**系统管理➤系统维护**”进入**系统维护**页面，选择**时间**页签，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。

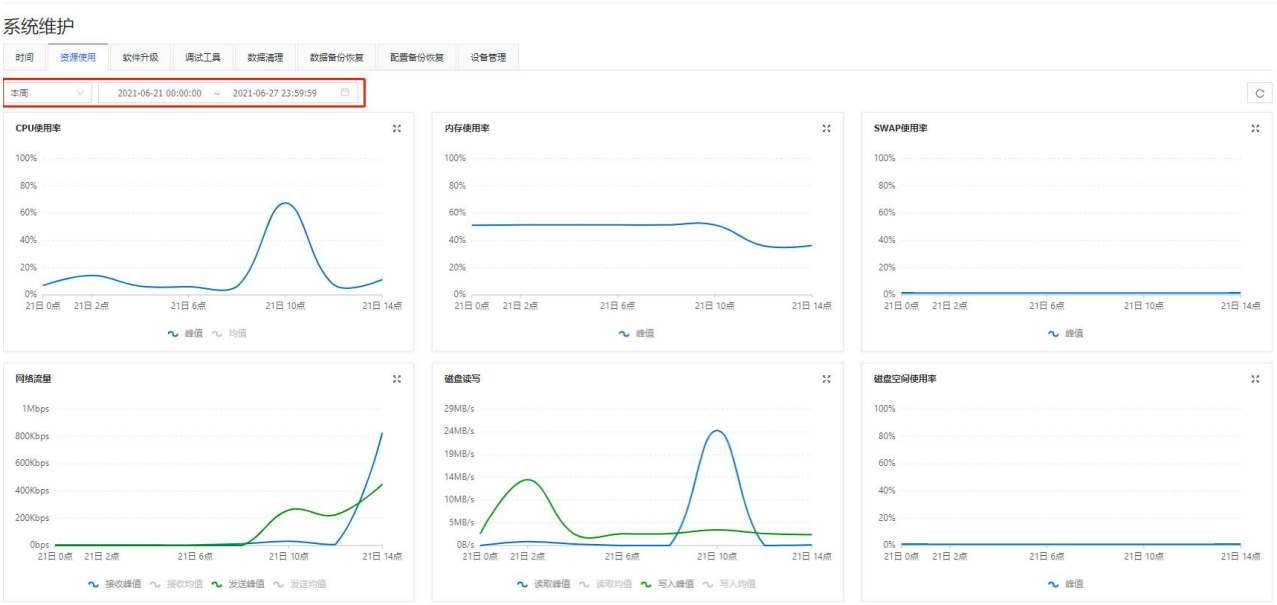
10.4.2 资源使用

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 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信息。



点击 可查看各资源的详细使用情况。

修改日期的查询条件，可查看资源的历史使用情况。



10.4.3 软件升级

在**系统维护**页面选择**软件升级**页签，在升级系统软件的同时会同时升级 Agent 安装包文件。软件升级的操作方法如下：

点击<**上传升级包**>，选择升级包文件，升级包上传成功后系统进行自动升级，升级成功后系统会重启，需要刷新页面并重新登录系统。

点击<**变更明细**>，可查看系统升级后的功能变化情况。

- 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。

10.4.4 调试工具

系统支持日志打包下载、连通性检测和 Tcpdump 抓包管理功能，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。

10.4.4.1 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。

10.4.4.2 连通性测试

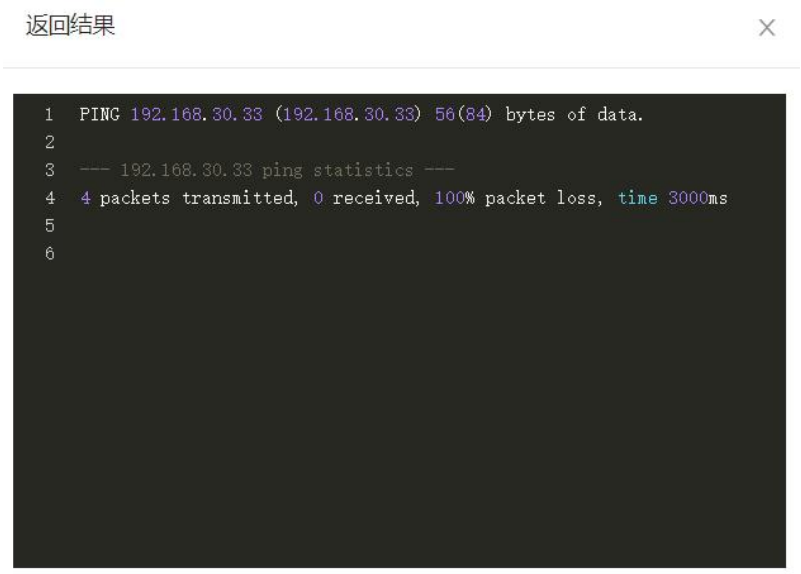
系统提供 Ping、NC 和 Traceroute 测试功能，以验证系统与目的主机是否网络连通。

- **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 地址），点击**<查看输出结果>**。

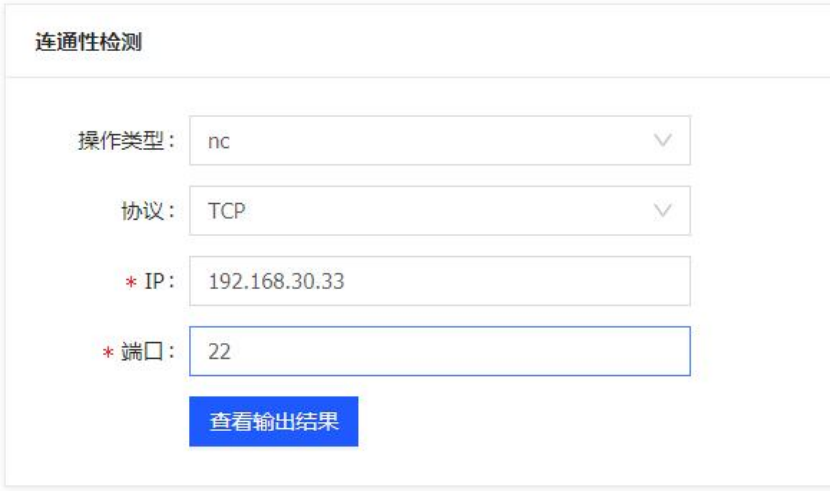
可在弹出的对话框中显示测试结果。



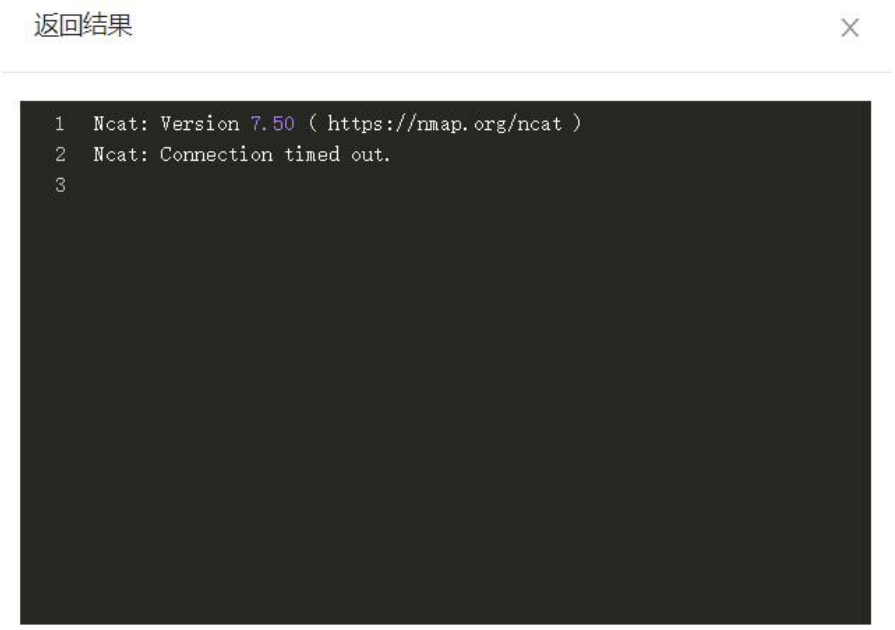
◆ **NC 测试**

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 地址）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。

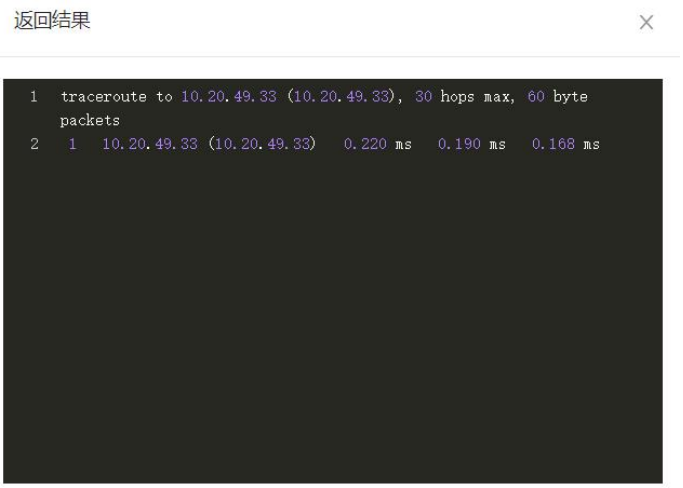


◆ **Traceroute**

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 地址），点击**<查看输出结果>**。

在弹出的对话框中显示测试结果。



10.4.4.3 Tcpdump 抓包管理

Tcpdump 抓包可以抓取到交换机转发给数据库审计的流量。

- **Agent 代理模式**：Agent 通过 13002 端口向数据库审计转发流量，抓包内容为 Agent 和数据库审计 IP 之间的通信流量，需要进一步转换才可获取用户环境中客户端与服务端之间的通信流量。
- **镜像流量模式**：交换机通过镜像口向数据库审计转发流量，抓包内容为用户环境中客户端与服务端之间的通信流量。
- 用户还可根据端口过滤的方式抓取数据库审计与其他接口的交互流量，例如与用户 Kafka 服务器间的数据流量。

Tcpdump 抓包操作步骤如下所示。

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**>。

步骤 2. 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 3. 抓包完成后，点击<**下载**>即可将抓包文件下载至本地，抓包文件可使用 WireShark 等工具打开。

10.4.5 数据清理

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，需要通过备份恢复的方式进行检索查看。

系统支持按照不同数据占据磁盘的百分比进行数据自动清理，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。

修改自动清理数据配置的操作方法如下：

步骤 1. 在**系统维护**页面选择**数据清理**页签进入**数据清理**页面，点击<**修改**>。

步骤 2. 弹出**修改自动清理**对话框，编辑相关参数，点击<**确定**>。

详细配置请参见下表。

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，取值范围：10~85，默认为 70。

日志留存天数	设置日志留存天数，取值范围：1~3650，默认为 180。
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，取值范围：10~85，默认为 70。
所有数据最大占用空间百分比	所有数据最大占用空间百分比，不可修改，默认 95。

此外系统也支持手动清除数据，点击<**清空业务数据**>，在弹出的对话框中点击<**确定**>可手动清除业务数据（包括审计日志、告警日志、会话日志、报表数据等保存在系统中的数据）。

清空业务数据后数据不可恢复，请谨慎操作。

10.4.6 业务数据备份和恢复

可以对业务数据进行备份和恢复等操作。

10.4.6.1 数据备份配置

步骤 1. 在**系统维护**页面选择**数据备份恢复**页签，可查看数据备份的相关信息。

步骤 2. 点击**备份几天前数据**后的<**修改**>，可以修改需要备份的数据，包括备份几天前数据、执行时间、压缩等级。

详细配置请参见下表。

配置项	**说明**
备份几天前数据	根据实际情况填写需要几天前的备份数据，取值范围：1~365。

配置项	说明
执行时间	数据自动备份的执行时间。
压缩等级	取值范围：1~9。1 级代表压缩速度最快，但压缩率最大；9 级代表压缩速度最慢，但压缩率最小。

10.4.6.2 备份外送 FTP 配置

此外，系统也支持将数据备份至外部 FTP 服务器。

步骤 1. 在**备份外送 FTP 配置**区域点击<**修改**>。

步骤 2. 在弹出的对话框中编辑相关信息，点击<**确定**>。

详细配置请参见下表。

配置项	说明
状态	启用或禁用将备份数据外送至 FTP 服务器。
协议	设置备份数据外送的协议，可选择 FTP 或 SFTP。
IP/端口	配置 FTP/SFTP 服务器的 IP 地址和端口号。
用户名/密码	配置 FTP/SFTP 服务器的登录用户名和密码。
上传目录	备份文件上传至 FTP/SFTP 服务器的目录。

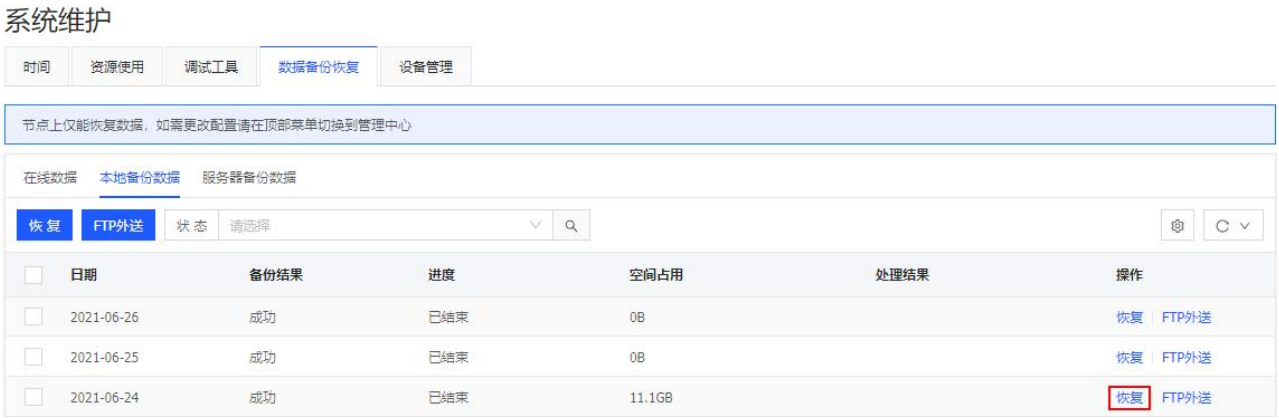
10.4.6.3 在线数据

数据备份恢复分为在线数据、本地备份数据、服务器备份数据。

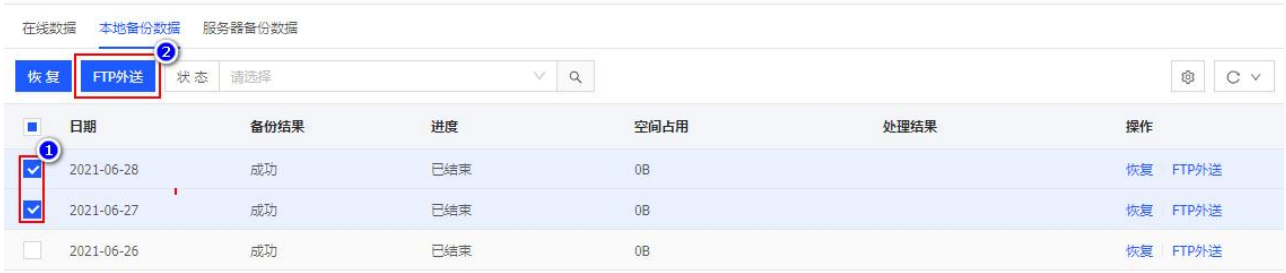
点击**操作列**中的**<备份>**可以对在线数据进行备份，备份成功后可在**本地备份数据**中进行查看。

10.4.6.4 本地备份数据

点击**操作**列中的**<恢复>**，在弹出的对话框中点击**<确定>**，对本地备份的数据进行恢复。



在数据备份恢复管理列表中勾选数据，点击**<FTP 外送>**即可将数据外送至 FTP 服务器。



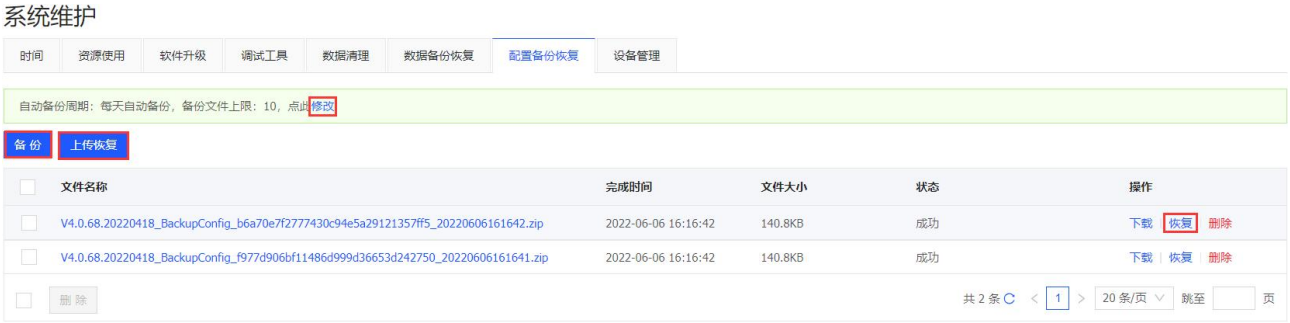
10.4.6.5 服务器备份数据

可查看 FTP 服务器备份数据的信息，包括日期、服务器上传的状态、处理结果等信息。以及对服务器的数据进行恢复操作。

10.4.7 系统配置备份恢复

配置备份恢复功能可在系统配置出错或者系统配置数据丢失时，对系统配置进行还原，减少系统配置工作量。

在**系统维护**页面选择**配置备份恢复**页签，可查看系统配置备份情况。



- 点击<**备份**>可备份系统当前配置。
- 点击<**上传恢复**>并上传配置文件，可将系统恢复至配置文件中的配置。
- 在**操作**列中点击<**恢复**>，在弹出的对话框中点击<**确定**>，可将系统恢复至备份文件中的配置。
- 点击<**修改**>，弹出**修改数据自动备份定时任务**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
备份周期	可选择不自动备份、每天、每周和每月自动备份。自动备份在凌晨两点进行。
备份文件上限	有效值 1~50，默认值 10。超出上限时，会自动删除自动备份的文件。

10.4.8 设备管理

在**系统维护**页面选择**设备管理**页签。

用户可在此页面关闭设备、重启设备，将设备恢复至出厂设置，打开/关闭远程登录设备的 SSH 端口和修改 Web 服务端口。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。
Web 服务配置	点击<**修改**>，在弹出的对话框中，填写端口号，再点击<**确定**>，即可修改 Web 服务端口号。

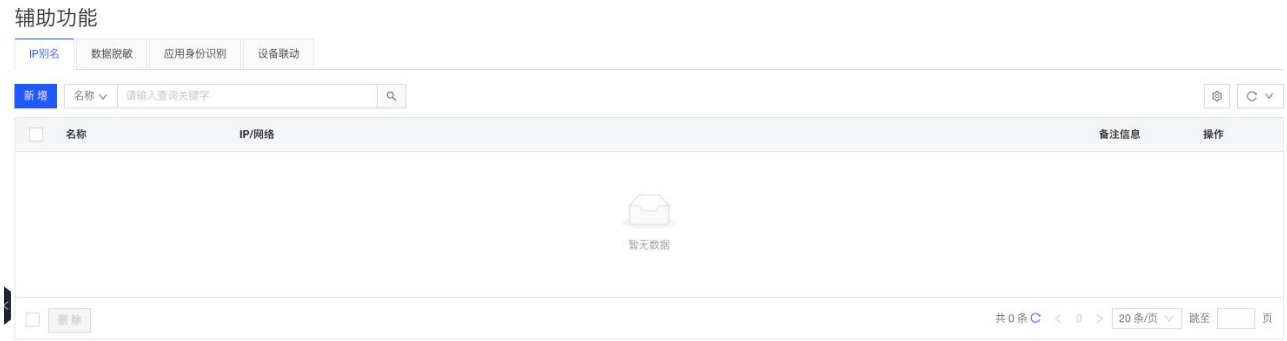
- 关闭设备后，业务将不可用，请谨慎操作。
- 重启设备期间业务将不可用，请谨慎操作。
- 恢复出厂设置将删除系统所有数据，恢复到出厂状态，请谨慎操作。
- 修改端口前需确认新端口网络可达。如不确定网络状况，建议先打开 SSH 端口后再进行修改。

10.5 辅助功能

10.5.1 IP 别名

为方便对网络进行识别，可对网段或 IP 地址设置别名。

步骤 1. 在菜单栏选择“**系统管理➤辅助功能**”进入**辅助功能**页面，选择 **IP 别名**页签，点击<**新增**>。



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

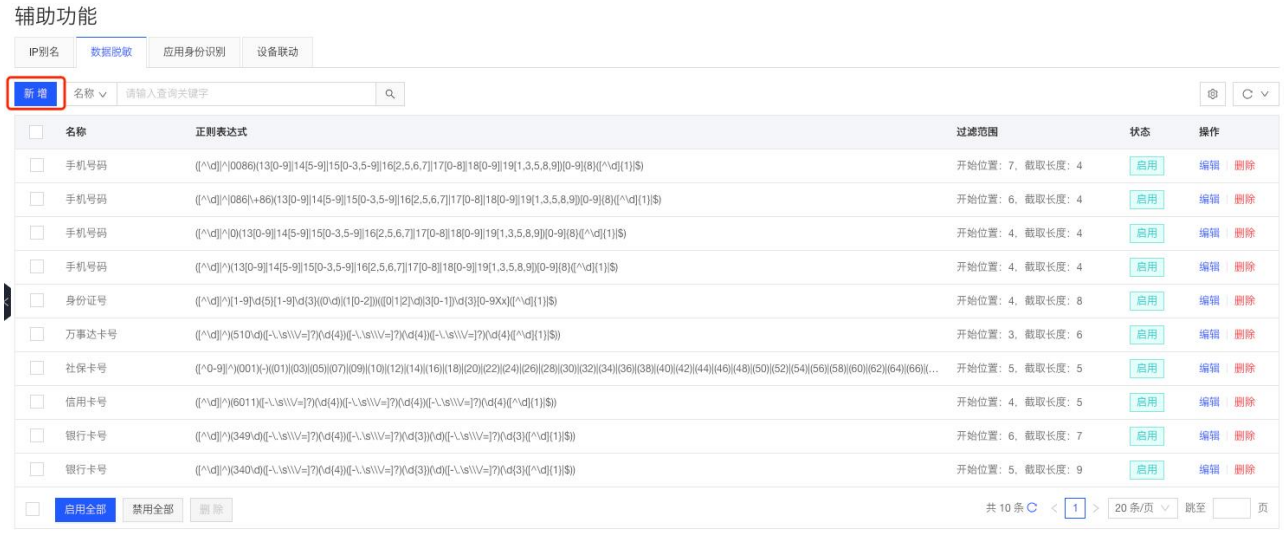
详细配置请参见下表。

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/网络	◆ 格式 1：输入多个 IP 地址，用英文逗号分隔。 ◆ 格式 2：输入 IP 网段，用“*”表示 0~255，例如：192.168.0.*。 ◆ 格式 3：IP 范围，仅支持 IPv4 格式，例如：10.1.1.10-10.1.1.20。

10.5.2 数据脱敏

数据脱敏可以将银行卡号、手机号码、身份证号码等敏感数据进行脱敏处理。

步骤 1. 在菜单栏选择“**系统管理➤辅助功能**”进入**辅助功能**页面，选择**数据脱敏**页签，点击<**新增**>。



步骤 2. 弹出**新增数据脱敏**对话框，编辑相关信息，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。
正则表达式	正则表达式用于检索、替换符合特定模式（规则）的文本，例如：([^d]|530)。

开始位置	开始替换的字符位置。
截取长度	数据串中被替换的字符长度。

10.5.3 应用身份识别

通俗来讲，应用身份识别功能就是三层关联功能。所谓三层审计，是将应用层区域的审计数据与数据库层区域的审计数据综合起来进行“关联分析”，从而将应用层操作准确对应到数据库层的操作。当发生安全事件时，根据关联审计记录的日志信息，可快速定位到网络中的责任人。所以通过三层审计即可实现应用与数据库的有效关联，追踪到最终用户端。

应用身份识别分为 B/S 应用身份识别和 C/S 应用身份识别。

10.5.3.1 B/S 应用身份识别

B/S 应用身份识别是指管理员添加应用身份识别后，系统会自动生成 jar 包，之后下载该 jar 包并安装到应用服务器。当有用户对应用的数据库进行操作时，系统会审计到用户、访问应用的 URL 以及使用的 IP。

B/S 应用身份识别功能需要对用户业务中的应用服务器配置文件进行一些改动，此功能必须得到用户同意，并在测试环境成功使用才可正式应用在实际业务中。

步骤 1. 在菜单栏选择“**系统管理➤辅助功能**”进入**辅助功能**页面，选择**应用身份识别**页签，再选择 **B/S 应用身份识别**页签。点击<**添加**>。

步骤 2. 弹出**新增 B/S 应用身份识别配置**对话框，编辑相关信息，点击<**保存**>。

详细配置请参见下表。

配置项	说明
应用名称	必须为中文字符、字母、数字、下划线“_”、点“.”或短横“-”，不超过 64 字符。
中间件类型	选择中间件类型，包括 Weblogic、Tomcat 和 Jboss。
中间件版本	选择中间件的版本。
JDK 版本	选择 JDK（Java 语言软件开发工具包）版本。
数据库类型	选择数据库类型，请根据应用的实际情况进行选择。
登录 URL 关键字	用户登录应用服务器的 URL 关键字。
登录用户关键字	用户登录应用服务器的用户名关键字。
客户端 IP 提取方式	分为 x-forwarded-for 和 proxy 两种。x-forwarded 适用于普通 Web 应用；proxy 适用于使用多层代理的 Web 应用。

步骤 3. 之后系统会自动生成 jar 包，点击**操作**列的<**下载**>下载 jar 包，将 jar 包安装至应用服务器（点击<**下载说明文档**>，可查看相应中间件类型的安装方法）。

步骤 4. 当有用户对应用的数据库进行操作时，系统可审计到用户的用户名、访问的 URL 和使用的 IP。

10.5.3.2 C/S 应用身份识别

C/S 应用身份识别是指管理员通过审计到的审计日志配置 C/S 应用用户名提取（请参见查看审计日志详情），指定配置后的 SQL 模板来判断用户名。当系统审计到相同的 SQL 模板，就会直接关联出用户名。

步骤 1. 在菜单栏中选择“**查询分析➤审计日志**”进入**审计日志**页面，查询 C/S 架构客户端访问数据库时产生的登录行为 SQL 语句的审计日志，在日志详情页面提取 C/S 应用用户名（详情请参见查看审计日志详情）。

步骤 2. 之后该记录将会自动添加至 C/S 应用身份识别列表中。

在菜单栏选择“**系统管理➤辅助功能**”进入**辅助功能**页面，选择**应用身份识别**页签，再选择 **C/S 应用身份识别**页签，可查看已添加的 C/S 应用身份识别条目。

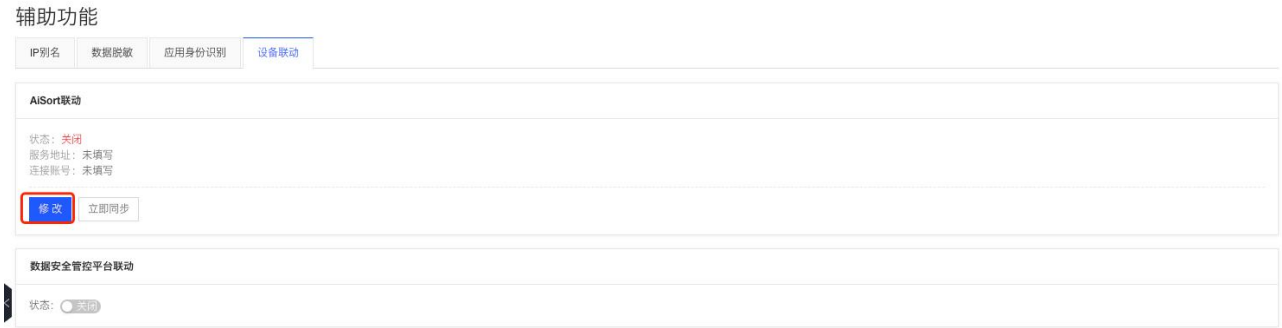
10.5.4 设备联动

数据库审计支持与 AiSort V2.1.4 及以上版本、数据安全管控平台支持与 V2.0 及以上版本进行联动，以便更好地识别出访问数据库系统的风险行为。

10.5.4.1 与 AiSort 联动

数据库审计与 AiSort 联动，可从 AiSort 获取数据分级分类配置，方便数据库审计更好地检测出数据库被访问数据的分级分类信息。

步骤 1. 在菜单栏选择“**系统管理➤辅助功能**”进入**辅助功能**页面，选择**设备联动**页签，点击<**修改**>。



步骤 2. 在弹出的**修改 AiSort 联动**对话框中将**状态**设置为“开启”，编辑相关信息，点击<**确定**>。

详细配置请参见下表。

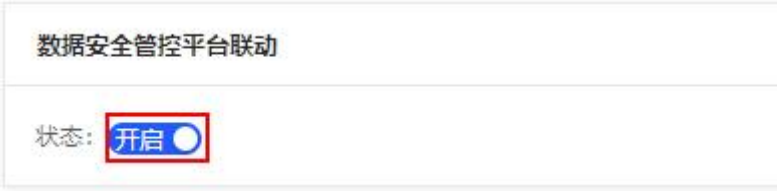
配置项	说明
状态	开启或关闭与 AiSort 联动功能。
服务器地址	AiSort 的地址信息，例如：https://www.aisorttest.com 或者 https://192.168.1.10
连接账号	AiSort 的用户名，建议设置为安全管理员账号。
密码	AiSort 的密码。

步骤 3.　点击<**立即同步**>，同步 AiSort 的敏感数据配置信息。

10.5.4.2　数据安全管控平台联动

将**状态**开关设置为“开启”，数据库审计会将审计数据发送给数据安全管控平台。

需要在数据安全管控平台进行相应配置，才能实现数据库审计与安全数据管控平台联动。



10.6　系统告警

10.6.1 告警查询

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

10.6.1.1 修改系统告警配置

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**告警查询**页签，点击<**修改**>。

步骤 2. 弹出**修改系统告警配置**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
日志保留天数	设置日志保留天数，取值范围：7~365。
CPU 阈值	设置 CPU 告警阈值，取值范围：1~100。
内存阈值	设置内存告警阈值，取值范围：1~100。

磁盘阈值	设置磁盘告警阈值，取值范围：1~100。
网口流量阈值	设置网口流量阈值，取值范围：1~100。
无日志告警	默认关闭。开启后可配置无日志告警阈值。
无日志阈值	设置无日志告警阈值，取值范围：6~360。

10.6.1.2 查询告警日志

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

10.6.2 告警通知

告警通知是指将系统日志发送至指定的接收者，支持邮件、短信、企业微信、钉钉、Syslog 和 SNMP 六种方式。

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，点击<**新增**>。

步骤 2. 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**>。各类通知方式的配置请参见[通知外送]。

10.7 操作日志

系统可记录所有用户的操作。审计员或超级管理员可以通过查看操作日志来审计其他用户的操作。

在菜单栏选择“**系统管理➤操作日志**”进入**操作日志**页面，可根据时间范围、用户、来源 IP、操作名称、操作类型、操作内容和操作结果来搜索相应操作日志。点击 图标可导出操作日志。

可修改操作日志的保留天数，操作方法如下：

步骤 1. 点击<**修改**>。

步骤 2. 弹出**修改操作日志自动清理配置**对话框，设置日志保留天数（取值范围：180~1,000），点击<**确定**>。

11 术语&缩略语

术语	解释
Agent	本文中所述的 Agent 指的是审计代理插件，是安装在数据库系统或者业务系统上的插件，其功能是捕获访问数据库系统的数据包，并将数据包发送至数据库审计。
Kafka	Kafka 是一种高吞吐量的分布式发布订阅消息系统，可以处理消费者规模的网站中所有动作流数据。这些数据通常由于吞吐量要求而通过处理日志和日志聚合来解决。
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。