

# 数据库审计

用户使用指南

天翼云科技有限公司

# 前言

## 概述

本手册对天翼云数据库审计系统（以下简称“系统”）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意，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  |
|------------|---|
| <b>粗体字</b> | Web 界面上的各类控件名称以及内容。例如：“在菜单栏选择 <b>‘系统状态’</b> 进入 <b>系统状态</b> 页面，选择 <b>接口状态</b> 页签”。 |
| <>         | Web 界面上的按钮。例如：“微信认证失败，点击< <b>我要上网</b> >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                                       |

| 内容  | 说明   |
|-----|--|
|     | 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。       |

## 修订记录

| 日期         | 修订版本 | 修改记录         |
|------------|------|--------------|
| 2025-01-20 | 02   | 优化文档结构和部分描述。 |
| 2023-06-30 | 01   | 初次发布。        |

# 目录

|          |             |           |
|----------|-------------|-----------|
| <b>1</b> | <b>快速入门</b> | <b>1</b>  |
| 1.1      | 产品简介        | 1         |
| 1.1.1    | 产品功能        | 1         |
| 1.1.2    | 产品特点        | 5         |
| 1.1.3    | 典型应用场景      | 5         |
| 1.2      | 登录系统        | 6         |
| 1.3      | 主要业务流程      | 6         |
| <b>2</b> | <b>总览</b>   | <b>7</b>  |
| 2.1      | 仪表盘         | 7         |
| 2.2      | 实时监控        | 8         |
| <b>3</b> | <b>资产</b>   | <b>10</b> |
| 3.1      | 添加资产组       | 10        |
| 3.2      | 添加资产        | 11        |
| 3.2.1    | 手动添加        | 11        |
| 3.2.2    | 资产自发现       | 14        |
| 3.3      | 关注资产        | 15        |

|          |              |           |
|----------|--------------|-----------|
| <b>4</b> | <b>查询分析</b>  | <b>16</b> |
| 4.1      | 查询审计日志       | 16        |
| 4.1.1    | 搜索审计日志       | 16        |
| 4.1.2    | 在查询结果中添加查询条件 | 18        |
| 4.1.3    | 保存查询条件       | 19        |
| 4.1.4    | 修改查询配置       | 20        |
| 4.1.5    | 查看审计日志详情     | 20        |
| 4.1.6    | 分析筛选         | 22        |
| 4.2      | 查询告警日志       | 24        |
| 4.2.1    | 告警日志         | 24        |
| 4.2.2    | 告警分析         | 26        |
| 4.3      | 查询会话日志       | 29        |
| 4.3.1    | 查询历史会话       | 29        |
| 4.3.2    | 查询在线会话       | 30        |
| 4.4      | 查询 SQL 模板    | 31        |
| <b>5</b> | <b>报表中心</b>  | <b>33</b> |
| 5.1      | 报表预览         | 33        |

|                     |           |
|---------------------|-----------|
| 5.2 报表订阅.....       | 34        |
| 5.3 自定义报表.....      | 36        |
| 5.3.1 报表数据管理.....   | 36        |
| 5.3.2 报表管理.....     | 38        |
| <b>6 智能分析.....</b>  | <b>42</b> |
| 6.1 添加行为模型学习任务..... | 42        |
| 6.2 设置模型查询.....     | 43        |
| <b>7 规则配置.....</b>  | <b>45</b> |
| 7.1 安全规则.....       | 45        |
| 7.1.1 规则管理.....     | 45        |
| 7.1.2 启用规则.....     | 51        |
| 7.1.3 禁用规则.....     | 52        |
| 7.1.4 白名单管理.....    | 53        |
| 7.1.5 设置.....       | 55        |
| 7.2 信任规则.....       | 55        |
| 7.3 过滤规则.....       | 56        |
| 7.3.1 按 IP 过滤.....  | 57        |

|                       |           |
|-----------------------|-----------|
| 7.3.2 按 SQL 模板过滤..... | 58        |
| 7.3.3 按规则过滤.....      | 58        |
| 7.4 规则维护.....         | 59        |
| 7.5 关联数据.....         | 60        |
| 7.5.1 IP 组管理.....     | 60        |
| 7.5.2 数据库账号组管理.....   | 62        |
| 7.5.3 应用用户组管理.....    | 63        |
| 7.5.4 时间组管理.....      | 64        |
| 7.5.5 对象组管理.....      | 65        |
| 7.5.6 人员管理.....       | 67        |
| <b>8 系统管理.....</b>    | <b>70</b> |
| 8.1 用户管理.....         | 70        |
| 8.1.1 角色管理.....       | 70        |
| 8.1.2 用户管理.....       | 71        |
| 8.1.3 授权数据库.....      | 72        |
| 8.1.4 远程认证.....       | 73        |
| 8.1.5 动态令牌管理.....     | 75        |

|                              |     |
|------------------------------|-----|
| 8.1.6 用户安全配置.....            | 77  |
| 8.2 Agent 管理.....            | 78  |
| 8.2.1 通过 SSH 远程安装 Agent..... | 79  |
| 8.2.2 手动安装 Agent.....        | 81  |
| 8.2.3 Agent 管理.....          | 90  |
| 8.3 系统配置.....                | 95  |
| 8.3.1 网络.....                | 95  |
| 8.3.2 SNMP.....              | 98  |
| 8.3.3 许可证.....               | 100 |
| 8.3.4 分布式部署.....             | 101 |
| 8.3.5 流量接收方式.....            | 106 |
| 8.4 系统维护.....                | 107 |
| 8.4.1 时间.....                | 107 |
| 8.4.2 资源使用.....              | 108 |
| 8.4.3 软件升级.....              | 109 |
| 8.4.4 调试工具.....              | 110 |
| 8.4.5 数据清理.....              | 114 |
| 8.4.6 业务数据备份和恢复.....         | 115 |

|                          |            |
|--------------------------|------------|
| 8.4.7 系统配置备份恢复.....      | 118        |
| 8.4.8 设备管理.....          | 119        |
| 8.5 辅助功能.....            | 121        |
| 8.5.1 IP 别名.....         | 121        |
| 8.5.2 数据脱敏.....          | 122        |
| 8.5.3 应用身份识别.....        | 123        |
| 8.5.4 设备联动.....          | 125        |
| 8.6 系统告警.....            | 127        |
| 8.6.1 告警查询.....          | 127        |
| 8.6.2 告警通知.....          | 129        |
| 8.7 操作日志.....            | 130        |
| <b>9 术语&amp;缩略语.....</b> | <b>131</b> |

# 1 快速入门

## 1.1 产品简介

天翼云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           |
|       | 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                               |
|       | 2          | v80、v81、v82、v95、v97、v10.5、v11.1、v11.5   |

| 数据库分类 | 数据库系统           | 版本                                  |
|-------|-----------------|-------------------------------------|
|       | 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                           |
|       | Maria           | 5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3 |
|       | Hana            | 1.0、2.0                             |
|       | Gauss           | 100、200、300                         |
|       | LibrA           | 6                                   |
|       | K-              | 11                                  |
|       | Sybase IQ       | 15.4                                |
|       | Ti              | 4.X、5.X                             |
|       | Vertica         | 7、8、9、10、11                         |
|       | OceanBase       | 2.X                                 |
|       | Polar           | MySQL、PostgreSQL、兼容 Oracle 语法       |

| 数据库分类  | 数据库系统               | 版本                                 |
|--------|---------------------|------------------------------------|
|        | Polar-X             | 1.0/MySQL5、1.0/MySQL8、2.0/MySQL5.7 |
|        | Analytic            | MySQL、PostgreSQL                   |
| 非关系型   | Mongo               | 2.x、3.x、4.x、5.x                    |
|        | HBase (protobuf)    | 所有版本                               |
|        | HBase (thrift)      | Thrift1、thrift2                    |
|        | 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                            |
|        | SS                  | 所有版本                               |
|        | Arango              | 3.4.9                              |
|        | Neo4j               | 4.2.0                              |
| Orient | 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         |
|       | SS                  | 所有版本            |
| 图形    | Graphbase           | 6               |
|       | Arango              | 3.4.9           |
|       | Neo4j               | 4.2.0           |
|       | Orient              | 3.1.6           |
| 全文检索  | Elasticsearch       | 所有版本            |
| 文档    | Mongo               | 2.x、3.x、4.x、5.x |
|       | Arango              | 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、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

数据库审计支持两种不同的流量采集方式：通过交换机进行端口镜像和通过在宿主机上安装流量代理插件。

### 1.1.3.1 端口镜像模式

在交换机上将访问数据库系统的流量通过端口镜像的方式镜像到数据库审计连接的交换机端口上。

### 1.1.3.2 流量代理模式

除了端口镜像方式，数据库审计还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，并将报文发送到数据库审计上。

## 1.2 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。

## 1.3 主要业务流程

系统主要业务流程如下：

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

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。

## 2 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。

### 2.1 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。

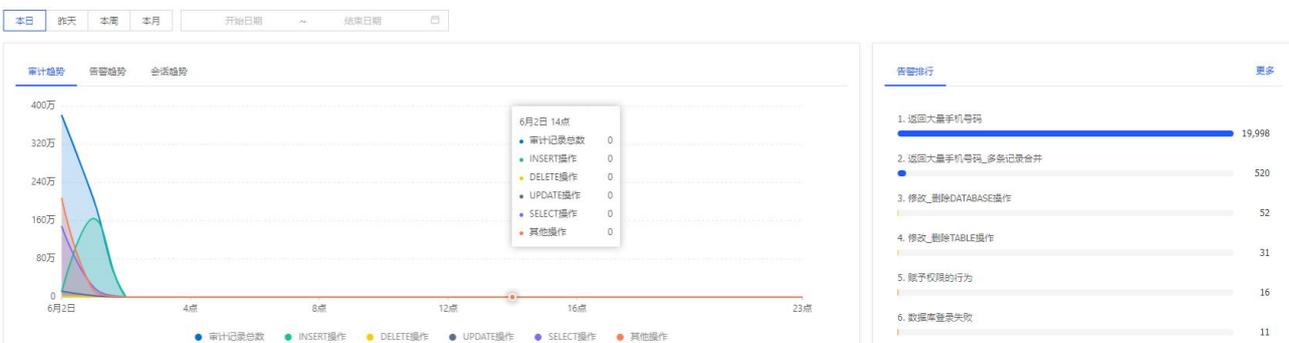
在菜单栏选择“总览>仪表盘”进入仪表盘页面。用户可在仪表盘查看以下信息，或执行以下操作。

◆ 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](#)。



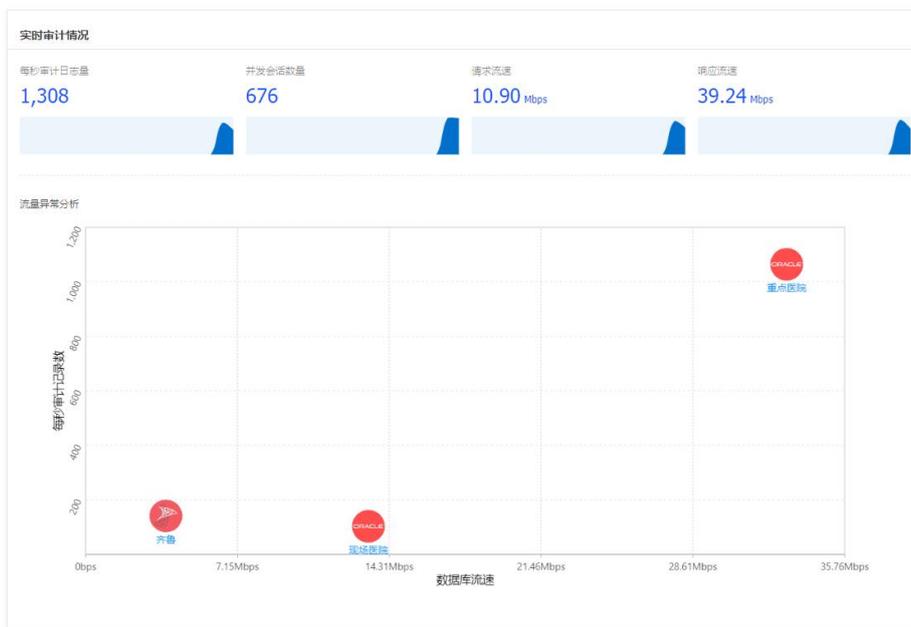
◆ 查看指定时间段内资产汇总信息。可分别根据审计数量、告警数量、会话数量、执行失败数量和登录失败数量进行排序。

| 资产名称                   | 类型         | IP端口信息   | 审计数量       | 告警数量    | 会话数量    | 执行失败数量  | 登录失败数量 |
|------------------------|------------|--|------------|---------|---------|---------|--------|
| ☆ autotestOraclenew    | Oracle     | 134.96.38.190:1524,134.96.96.15:1521,10.200.72.3:1521,134.96.93.199:1521,10.24.250.2:1521,10.33.30.32:1541,192.168.16.162:1521,192.168.10.28:152...  | 18,492,915 | 10      | 39,473  | 184,030 | 4      |
| ☆ autotestMySQLnew     | MySQL      | 192.168.30.242:3306,192.168.30.251:3306,192.168.30.136:3306,192.168.115:3306,192.168.50.36:3306,10.33.60.38:3306,10.33.70.2:3306,10.33.64.36:33...   | 4,933,615  | 329,654 | 327,983 | 0       | 0      |
| ☆ autotestSQLServernew | SQL Server | 210.72.0.3:1433,192.168.9.90:1433,10.154.128.209:1433,160.160.160.80:1433,160.160.160.5:1048,192.168.0.188:1433,19.127.1.10:1433,19.127.1.28:143...  | 555,097    | 0       | 9,938   | 2,950   | 0      |
| ☆ autotestSybasenew    | Sybase ASE | 192.168.50.221:5000,10.101.75.11:5000,10.109.15.20:5000,10.101.233.20:5000,192.168.50.107:5000,134.97.5.5:7000,134.97.5.41:5000,134.97.16.1:5000,... | 0          | 0       | 0       | 0       | 0      |
| ☆ autotestDB2new       | DB2        | 172.16.2.11:60000,133.96.71.1:50000,192.168.10.12:50000,10.168.4.40:60000,133.96.71.182:61000,192.168.10.31:50000,194.1.2.150:50080                  | 4,125,436  | 0       | 6,758   | 84      | 2      |
| ☆ autotestCachenew     | Cache      | 192.168.30.249:57772,10.1.12.3:1972,10.1.12.2:1972,192.168.245.1:1972,192.168.2.3:1972,172.22.134.10:1972,172.22.134.10:23,172.22.5.1:1972,172.22... | 177,699    | 0       | 6,346   | 3,863   | 0      |

## 2.2 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。

**最新告警**

|                     |                 |               |
|---------------------|-----------------|---------------|
| 2021-06-21 14:55:32 | 无               | 192.168.8.115 |
| <b>中风险</b>          | 创建_修改_删除TABLE操作 |               |
| 2021-06-21 14:55:31 | orcl            | 172.16.200.19 |
| <b>低风险</b>          | Oracle_查询版本     |               |
| 2021-06-21 14:55:31 | orcl            | 1             |
| <b>低风险</b>          | Oracle_查询版本     |               |
| 2021-06-21 14:55:31 | orcl            |               |
| <b>高风险</b>          | 无WHERE条件修改数据    |               |

◆ 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 |
|-----------------------|--------|------|------|----------|
| autotestOracnew       | 3,412  | 0bps | 0bps | 0        |
| autotestMySQLnew      | 11,241 | 0bps | 0bps | 0        |
| autotestSQLServernew  | 2,375  | 0bps | 0bps | 0        |
| autotestDB2new        | 4,908  | 0bps | 0bps | 0        |
| autotestCachnew       | 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 < 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 < 1 > 10 条/页 跳至 页

### 3 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。资产必须隶属于资产组，因此在添加资产前需要首先添加资产组。

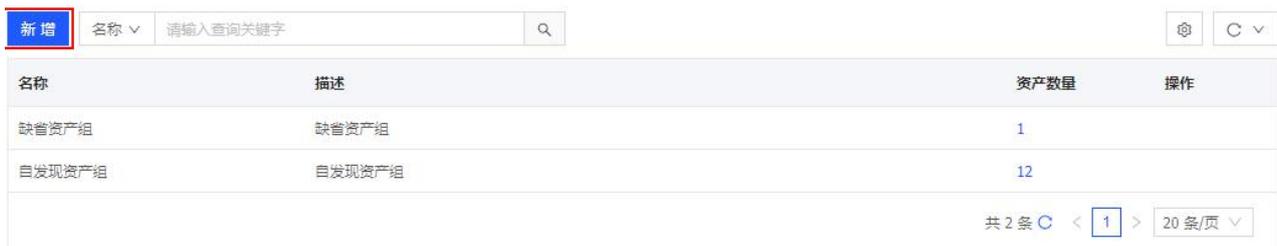
#### 3.1 添加资产组

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。

添加资产组的操作方法如下：

- 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。

##### 资产组管理



The screenshot shows the 'Asset Group Management' interface. At the top, there is a search bar with a '新增' (Add) button highlighted in red. Below the search bar is a table with columns: '名称' (Name), '描述' (Description), '资产数量' (Asset Count), and '操作' (Action). The table contains two rows: '缺省资产组' (Default Asset Group) with a count of 1, and '自发现资产组' (Self-discovered Asset Group) with a count of 12. At the bottom right of the table, there is a pagination control showing '共 2 条' (Total 2 items), a page number '1', and '20 条/页' (20 items per page).

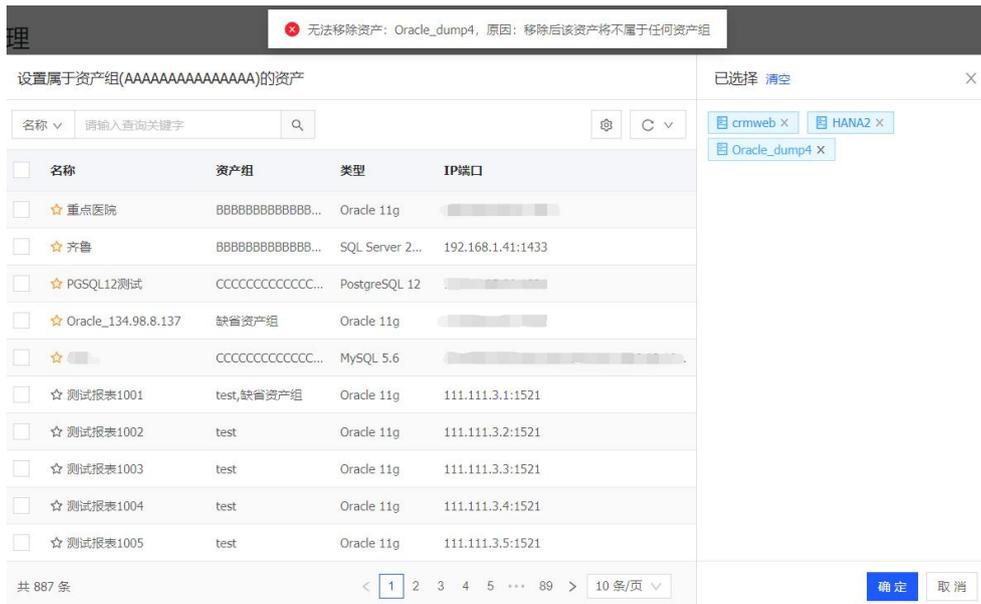
| 名称     | 描述     | 资产数量 | 操作 |
|--------|--------|------|----|
| 缺省资产组  | 缺省资产组  | 1    |    |
| 自发现资产组 | 自发现资产组 | 12   |    |

- 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>。



The screenshot shows the '新增资产组' (Add Asset Group) dialog box. It has a title bar with the text '新增资产组' and a close button 'X'. The main area contains two input fields: '\* 名称:' (Name) with the value '网站数据库' (Website Database) and '描述:' (Description) which is empty. At the bottom right, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

选择任意资产组，点击资产数量列的数字，可以设置属于该资产组的资产。可以增加或者减少该资产组的资产，且当某资产的所属资产组只有一个时，不允许从此资产组移除该资产。



## 3.2 添加资产

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。

### 3.2.1 手动添加

手动添加资产包括单个添加和批量导入两种方式。

◆ 单个添加的操作方法如下：

步骤 1. 在菜单栏选择“资产>资产管理”进入资产管理页面，点击<添加>。

#### 资产管理



步骤 2. 在弹出的添加资产页面编辑相关信息。

添加资产  保存后不关闭, 继续添加资产  保存时启用推荐的规则 ×

---

\* 类型:

资产组:  管理

\* 名称:

\* 操作系统:

\* IP端口:

+ 增加IP与端口

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 <a href="#">规则配置</a> 。 |
| 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、键值和其他八大类, 每个大类之下还有其他小类。  |
| 资产组        | 设置资产所隶属的资产组, 不选择则默认为“缺省资产组”。   |
| 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 1. 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。

单双向审计配置

流量方向  双向审计  单向审计

保存行数:  行  
可配范围: 0~999, 填0表示不保存返回结果, 最多存储64K

最大保存长度:  K  
可配范围: 1~64K, 确保整行显示

加密协议审计配置

解密私钥:   
导入

证书密码:

详细配置项和说明请参见下表。

| 配置项    | 说明   |
|--------|--|
| 流量方向   | <ul style="list-style-type: none"> <li>◆ 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。</li> <li>◆ 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。</li> </ul> |
| 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: 1~64K, 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 2. 点击<保存>。

◆ 批量导入的操作方法如下:

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。

步骤 3. 点击<导入>, 选择编辑好的模板文件, 即可批量导入资产。



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](#)。

可对已添加的资产进行管理：

- ◆ 点击<编辑>对资产信息进行修改。
- ◆ 点击<删除>，在弹出的对话框中点击<确定>删除资产。

### 资产管理

| 资产管理                     |                    | 数据库自动发现            |                      |  |                               |                               |                               |                               |                                       |
|--------------------------|--------------------|--------------------|----------------------|--|-------------------------------|-------------------------------|-------------------------------|-------------------------------|---------------------------------------|
| <a href="#">添加</a>       | <a href="#">导入</a> | <a href="#">导出</a> | <a href="#">下载模板</a> | 名称 <input type="text" value="请输入查询关键字"/> | <input type="text" value=""/>         |
| <input type="checkbox"/> | 名称                 | 资产组                | 类型                   | IP/端口                                    | 编码                            | 操作系统                          | 状态                            | 流量方向                          | 操作                                    |
| <input type="checkbox"/> | ★ 10.123.36.40     | 缺省资产组              | MySQL 8.0            | 10.123.36.40:3323                        | 自动识别                          | Linux                         | 启用                            | 双向审计                          | <a href="#">编辑</a> <a href="#">删除</a> |
| <input type="checkbox"/> | ★ test             | 缺省资产组              | Oracle 19c           | 180.0.0.13:1521,10.50.3...               | 自动识别                          | Linux                         | 启用                            | 双向审计                          | <a href="#">编辑</a> <a href="#">删除</a> |

## 3.2.2 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。

### 资产管理

| 资产管理  |                     | 数据库自动发现                                  |                               |                               |                               |      |   |
|---|---------------------|--|-------------------------------|-------------------------------|-------------------------------|------|---|
| 数据库自动发现: 启用, 自动发现截止时间: 不定时, 点此修改; 自动添加: <input checked="" type="checkbox"/> |                     |  |                               |                               |                               |      |   |
| 新发现数据库  |                     | 已忽略数据库                                   |                               | 已添加数据库                        |                               |      |   |
| <a href="#">添加</a>  | <a href="#">忽略</a>  | IP <input type="text" value="请输入查询关键字"/> | <input type="text" value=""/> | <input type="text" value=""/> | <input type="text" value=""/> |      |   |
| <input type="checkbox"/>  | 发现时间                | IP                                       | 端口                            | 数据库类型                         | 版本                            | 运行环境 | 操作  |
| <input type="checkbox"/>  | 2022-05-31 20:43:44 | 192.168.1.164                            | 1521                          | Oracle                        | 11g                           |      | <a href="#">添加到现有资产</a> <a href="#">添加到新资产</a> <a href="#">忽略</a> |
| <input type="checkbox"/>  | 2022-05-31 20:43:44 | 192.168.4.232                            | 1521                          | Oracle                        | 11g                           |      | <a href="#">添加到现有资产</a> <a href="#">添加到新资产</a> <a href="#">忽略</a> |
| <input type="checkbox"/>  | 2022-05-31 20:43:44 | 192.168.30.8                             | 1521                          | Oracle                        | 11g                           |      | <a href="#">添加到现有资产</a> <a href="#">添加到新资产</a> <a href="#">忽略</a> |
| <input type="checkbox"/>  | 2022-05-31 20:43:44 | 192.168.60.8                             | 1521                          | Oracle                        | 11g                           |      | <a href="#">添加到现有资产</a> <a href="#">添加到新资产</a> <a href="#">忽略</a> |
| <input type="checkbox"/>  | 2022-05-31 20:43:44 | 192.168.40.8                             | 4324                          | Oracle                        | 11g                           |      | <a href="#">添加到现有资产</a> <a href="#">添加到新资产</a> <a href="#">忽略</a> |

- ◆ 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）。

修改资产自动发现配置 ×

自动发现： 启用  禁用

运行截止时间：30分钟 3小时 12小时 24小时 3天 不限时

不填即为不限时

确定
取消

### 3.3 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。

#### 资产管理

| 名称                     | 资产组      | 类型            | IP端口                | 编码   | 操作系统  | 状态 | 流量方向 | 操作    |
|------------------------|----------|---------------|---------------------|------|-------|----|------|-------|
| ☆ autotest-postgre     | autotest | PostgreSQL 11 | 192.168.22.21:5432  | 自动识别 | Linux | 启用 | 双向审计 | 编辑 删除 |
| ☆ autotest-redis-00001 | autotest | Redis         | 192.168.21.215:6379 | 自动识别 | Linux | 启用 | 双向审计 | 编辑 删除 |

## 4 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。

### 4.1 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。

#### 4.1.1 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，设置查询条件（如时间范围、报文、资产等），点击**<搜索>**即可查询相关审计日志。

审计日志

最大返回条数: 100000, 最大查询时间: 10秒 [修改](#)

---

查询条件: 时间范围: 昨天(2022-06-01 00:00:00~2022-06-01 23:59:59) [保存](#) [搜索](#) [重置](#)

时间范围: [最近5分钟](#) [最近30分钟](#) [最近1小时](#) [最近6小时](#) [本日](#) [昨天](#) [本周](#) [本月](#) 2022-06-01 00:00:00 ~ 2022-06-01 23:59:59 [日历](#)

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:

[更多条件](#)

分析筛选:

---

日志列表 [↓](#) [⊗](#)

| 发生时间                | 客户端IP           | 数据库账号 | 报文   | 影响行数 | 执行时长     | 执行状态 | 操作                 |
|---------------------|-----------------|-------|--|------|----------|------|--------------------|
| 2022-06-01 23:59:59 | 202.112.102.121 | -     | SELECT matter.id, matter.mattercode, matter.name, matter.type, matter.type1, matter.specification, matter.package limit, matter.limit, matter.unit, matter.price, sum(matstore.curamount) as amount FROM matstore, matter WHERE ( matstore.matter_id = matter.id ) and ( matter.isvalid=1)and (matter.type < 11) and (( matter.abbrev_name like 'WS... | 5    | 26.68 毫秒 | 成功   | <a href="#">详细</a> |
|                     |                 |       | SELECT id, said, type, detail, exectime, totalfee, elseprocess_id, price, number, pnumber, ybtype FROM elsercord2  |      |          |      |                    |

共 100000 条 < 1 2 3 4 5 ... 5000 > 20 条/页 跳至  页

#### 相关操作

- ◆ 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。

更多条件
✕

---

全选

审计ID

会话ID

SQL模板ID

资产

数据库账号

客户端IP

客户端端口

客户端MAC

服务端IP

服务端端口

服务端MAC

数据库名/实例名

对象

客户端工具

主机名

操作系统用户名

影响行数

执行时长(us)

执行结果描述

返回结果集

关联IP

关联账号

操作类型

数据库类型

执行状态

恢复默认 确定 取消

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。                               |
| 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。                                    |

| 选项       | 说明  |
|----------|---|
| 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。                                      |
| 关联 IP/账号 | 关联用户的客户端 IP 和账号。  |
| 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

查询结果显示在查询条件的下方。点击  图标，勾选需要展示的显示列，点击<确定>即可设置查询结果显示的列。

| 日志列表 | 发生时间                | 客户端IP           | 数据库账号 | 报文   | 影响行数 | 执行时长     | 执行状态 | 操作 |
|------|---------------------|-----------------|-------|--|------|----------|------|----|
|      | 2022-06-01 23:59:59 | 202.112.102.121 | -     | SELECT matter.id, matter.mattercode, matter.name, matter.type, matter.type1, matter.specification, matter.package limit, matter.limit, matter.unit, matter.price, sum(matstore.curamount) as amount FROM matstore, matter WHERE ( matstore.matter_id = matter.id ) and ( matter.isvalid=1)and (matter.type < 11) and (( matter.abbrev_name like 'WS... | 5    | 26.68 毫秒 | 成功   | 详细 |
|      | 2022-06-01 23:59:58 | 10.10.71.203    | -     | SELECT id, said, type, detail, exectime, totalfee, elseprocess_id, price, number, pnumber, ybtype FROM elsercord2 where inhospital_id=231764 and depid=402 and iscompleted=1 and iscanceled=0 and type<>4 and isaccount=0 and totalfee <> 0 and isaccounted is null  | 130  | 2.58 毫秒  | 成功   | 详细 |

共 100000 条 < 1 2 3 4 5 ... 5000 > 20 条/页 跳至 页

#### ◆ 导出查询结果

可导出查询结果。点击  图标，可将查询结果导出至本地。

## 4.1.2 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。

## 审计日志

最大返回条数: 100000, 最大查询时间: 10秒 [修改](#)

查询条件 v: 时间范围: 昨天(2022-06-01 00:00:00~2022-06-01 23:59:59) 客户端IP: 202.112.102.121 X 保存 [搜索](#) [重置](#)

时间范围: 最近5分钟 最近30分钟 最近1小时 最近6小时 本日 昨天 本周 本月 2022-06-01 00:00:00 ~ 2022-06-01 23:59:59

报文: 请输入报文关键字, 多个关键字用“,”隔开为“或者”的关系, 用空格隔开为“并且”的关系

资产: 全部 数据库账号: 请输入数据库账号, 多个值使用“,”隔开 客户端IP: 202.112.102.121

服务端IP: 请输入服务端IP, 多个值使用“,”隔开 操作类型: 执行状态:

[更多条件](#)

分析筛选:

日志列表 [↓](#) [☰](#)

| 发生时间                | 客户端IP           | 数据库账号 | 报文  | 影响行数 | 执行时长     | 执行状态 | 操作                 |
|---------------------|-----------------|-------|---|------|----------|------|--------------------|
| 2022-06-01 23:59:59 | 202.112.102.121 | -     | SELECT matter_id, matter.mattercode, matter.name, matter.type, matter.type1, matter.specification, matter.packageli<br>mit, matter.limit, matter.unit, matter.price, sum(matstore.curamount) as amount FROM matstore, matter WHERE ( m<br>atstore.matter_id = matter_id ) and ( matter.isvalid=1)and (matter.type < 11) and (( matter.abbrev_name like 'WS... | 5    | 26.68 毫秒 | 成功   | <a href="#">详细</a> |

共 67 条 < 1 2 3 4 > 20 条/页 跳至 页

### 4.1.3 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>**。

#### 审计日志

最大返回条数: 100000, 最大查询时间: 10秒 [修改](#)

查询条件 v: 时间范围: 2021-11-26 17:22:26~2021-11-26 17:27:26 客户端IP: 10.100.4.101 X **保存** [搜索](#) [重置](#)

时间范围: 最近5分钟 最近30分钟 最近1小时 最近6小时 本日 昨天 本周 本月 2021-11-26 17:22:26 ~ 2021-11-26 17:27:26

报文: 请输入报文关键字, 多个关键字用“,”隔开为“或者”的关系, 用空格隔开为“并且”的关系

资产: 全部 数据库账号: 请输入数据库账号, 多个值使用“,”隔开 客户端IP: 10.100.4.101

服务端IP: 请输入服务端IP, 多个值使用“,”隔开 操作类型: 执行状态:

[更多条件](#)

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>**。

保存查询条件 X

---

\* 名称:

---

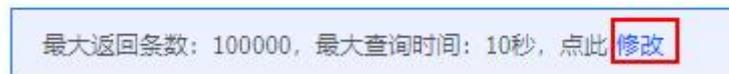
点击**查询条件**后的 图标, 可查看已保存的查询条件。



#### 4.1.4 修改查询配置

步骤 1. 在审计日志页面左上方点击<修改>。

### 审计日志



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。 |

#### 4.1.5 查看审计日志详情

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。

**基本信息**

|      |                               |      |                    |
|------|-------------------------------|------|--------------------|
| 发生时间 | 2022-06-01 17:56:25           | 是否告警 | 否                  |
| 审计ID | 366617486881522721            | 会话ID | 366600517239637027 |
| 资产名称 | 022_Oracle_200.200.200.3_1521 |      |                    |

**客户端**

|        |                   |         |                                     |
|--------|-------------------|---------|-------------------------------------|
| 客户端IP  | 172.16.200.2      | 客户端端口   | 53288                               |
| 客户端MAC | 14:14:4b:5d:74:68 | 客户端工具   | C:\Windows\SysWOW64\inetrv\w3wp.exe |
| 主机名    | WORKGROUP\MIDDLE1 | 操作系统用户名 | EMRS                                |
| 执行人    | -                 |         |                                     |

**服务端**

|        |                   |          |        |
|--------|-------------------|----------|--------|
| 服务端IP  | 200.200.200.3     | 服务端端口    | 1521   |
| 服务端MAC | 6c:ae:8b:77:a4:4c | 数据库类型    | ORACLE |
| 数据库账号  | ihd               | 数据库名/实例名 | ord    |

**请求**

|         |   |            |     |
|---------|---|------------|-----|
| 操作类型    | Select  | 原始SQL长度(B) | 446 |
| SQL模板ID | 1515730785117271691   |            |     |
| 对象      | 表: DEPT_DICT, DEPT_VS_WARD, STAFF_DICT, STAFF_VS_GROUP 字段: DEPT_NAME, WARD_CODE, DEPT_CODE, GROUP_CODE                |            |     |
| SQL语句概述 | 查询中DEPT_DICT表的DEPT_NAME字段, 查询中DEPT_VS_WARD表的WARD_CODE字段, 查询中STAFF_DICT表的DEPT_CODE字段, 查询中STAFF_VS_GROUP表的GROUP_CODE字段。 |            |     |

[报文\(原文\)](#)
[报文\(高亮\)](#)
[SQL模板](#)

```
select T1.DEPT_CODE,T2.DEPT_NAME DeptName,T3.GROUP_CODE,T4.DEPT_NAME GroupName,T5.WARD_CODE,T6.DEPT_NAME WardName from DEPT_DICT T2,DEPT_DICT T4,STAFF_DICT T1,STAFF_VS_GROUP T3,DEPT_DICT T6,DEPT_VS_WARD T5 where T1.DEPT_CODE=T2.DEPT_CODE and T3.GROUP_CODE=T4.DEPT_CODE and T1.EMP_NO=T3.EMP_NO and T3.GROUP_CODE=T5.DEPT_CODE(+) and T5.WARD_CODE=T6.DEPT_CODE(+) and upper(T1.USER_NAME)='ZCF' and T3.GROUP_CLASS='病区护士' order by T3.GROUP_CODE
```

[C/S应用用户名提取](#)
[取证](#)
[上一条](#)
[下一条](#)
[取消](#)

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](#)。

资产：022\_Oracle\_200.200.200.3\_1521

SQL模板：  
 select T1.DEPT\_CODE,T2.DEPT\_NAME  
 DeptName,T3.GROUP\_CODE,T4.DEPT\_NAME  
 GroupName,T5.WARD\_CODE,T6.DEPT\_NAME WardName from DEPT\_DICT  
 T2,DEPT\_DICT T4,STAFF\_DICT T1,STAFF\_VS\_GROUP T3,DEPT\_DICT  
 T6,DEPT\_VS\_WARD T5 where T1.DEPT\_CODE=T2.DEPT\_CODE and  
 T3.GROUP\_CODE=T4.DEPT\_CODE and T1.EMP\_NO=T3.EMP\_NO and  
 T3.GROUP\_CODE=T5.DEPT\_CODE(+) and T5.WARD\_CODE=T6.DEPT\_CODE(+)  
 and upper(T1.USER\_NAME)= :1 and T3.GROUP\_CLASS= :2 order by  
 T3.GROUP\_CODE

\* 参数位置: :1 ('ZCF')

请选择应用用户名所在的参数位置

确定 取消

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](#)。

审计日志详细

数据库账号 ihd 数据库名/实例名 orcl

请求

操作类型 Select 原始SQL长度(B) 446

SQL模板ID 1515730785117271691

对象 表：DEPT\_DICT, DEPT\_VS\_WARD, STAFF\_DICT, STAFF\_VS\_GROUP 字段：DEPT\_NAME, WARD\_CODE, DEPT\_CODE, GROUP\_CODE

SQL语句概述 查询中DEPT\_DICT表的DEPT\_NAME字段，查询中DEPT\_VS\_WARD表的WARD\_CODE字段，查询中STAFF\_DICT表的DEPT\_CODE字段，查询中STAFF\_VS\_GROUP表的GROUP\_CODE字段。

报文(原文) 报文(高亮) **SQL模板**

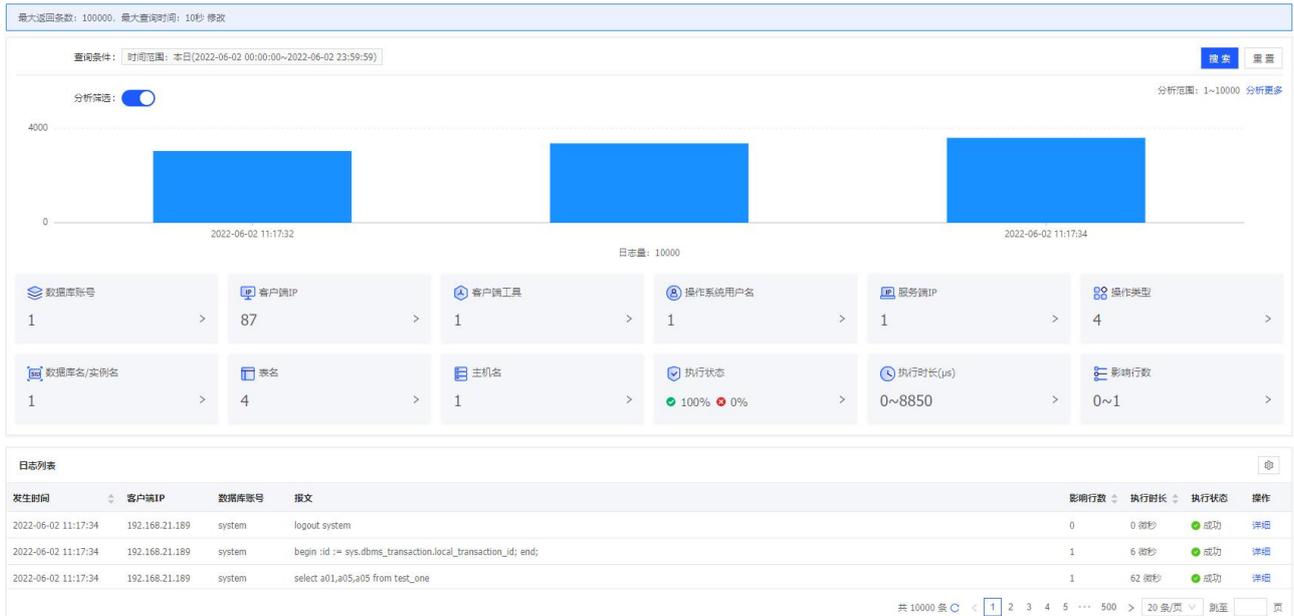
```
select T1.DEPT_CODE,T2.DEPT_NAME DeptName,T3.GROUP_CODE,T4.DEPT_NAME GroupName,T5.WARD_CODE,T6.DEPT_NAME WardName from DEPT_DICT T2,DEPT_DICT T4,STAFF_DICT T1,STAFF_VS_GROUP T3,DEPT_DICT T6,DEPT_VS_WARD T5 where T1.DEPT_CODE=T2.DEPT_CODE and T3.GROUP_CODE=T4.DEPT_CODE and T1.EMP_NO=T3.EMP_NO and T3.GROUP_CODE=T5.DEPT_CODE(+) and T5.WARD_CODE=T6.DEPT_CODE(+) and upper(T1.USER_NAME)= :1 and T3.GROUP_CLASS= :2 order by T3.GROUP_CODE
```

**过滤该模板**

### 4.1.6 分析筛选

在审计日志界面开启分析筛选开关，可以对已查询的审计日志结果进行分析和二次查询。

## 审计日志

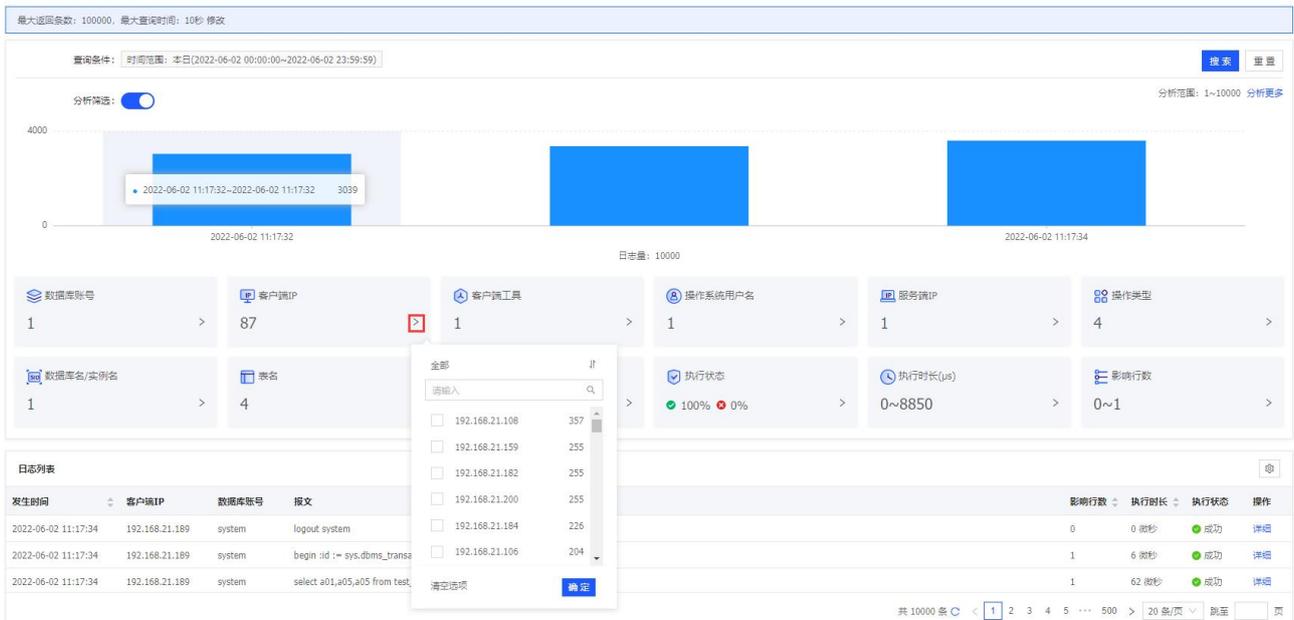


每次分析拉取 1 万条审计日志进行分析, 如果超过 1 万条可点击<分析更多>再拉取 1 万条审计日志与上一万条审计日志一起进行分析。

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。

## 审计日志



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分布统计。    |
| 客户端 IP   | 对首次查询结果根据客户端 IP 维度进行分布统计。  |
| 客户端工具    | 对首次查询结果根据客户端工具维度进行分布统计。    |
| 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分布统计。  |
| 服务端 IP   | 对首次查询结果根据服务端 IP 维度进行分布统计。  |
| 操作类型     | 对首次查询结果根据操作类型维度进行分布统计。     |
| 数据库名/实例名 | 对首次查询结果根据数据库名/实例名维度进行分布统计。 |
| 表名       | 对首次查询结果根据表名维度进行分布统计。       |
| 主机名      | 对首次查询结果根据主机名维度进行分布统计。      |
| 执行状态     | 对首次查询结果根据执行状态维度进行分布统计。     |
| 执行时长     | 对首次查询结果根据执行时长维度进行分布统计。     |
| 影响行数     | 对首次查询结果根据影响行数维度进行分布统计。     |

## 4.2 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。

### 4.2.1 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，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。

## 告警日志

告警日志
告警分析

最大返回页数: 100000, 最大查询时间: 10秒 [修改](#)

查询条件 v: 时间范围: 本日(2022-06-02 00:00:00~2022-06-02 23:59:59) [保存](#) [清空](#)

时间范围: [最近5分钟](#) [最近30分钟](#) [最近1小时](#) [最近6小时](#) [本日](#) [昨天](#) [本周](#) [本月](#) 2022-06-02 00:00:00 ~ 2022-06-02 23:59:59

报文: 请输入报文关键字; 多个关键字用“,”隔开为“或者”的关系, 用空格隔开为“并且”的关系

资产:  规则名称:  告警等级:

数据库账号:  操作类型:  执行状态:

[更多条件](#)

日志列表 [↓](#) [🔍](#)

| 发生时间                | 是否为统计规则 | 规则名称              | 告警等级 | 客户端IP         | 数据库账号  | 报文  | 影响行数 | 执行时长    | 执行状态 | 操作                 |
|---------------------|---------|-------------------|------|---------------|--------|---|------|---------|------|--------------------|
| 2022-06-02 03:05:49 | 普通规则    | 执行时长超过10秒         | 中风险  | 192.168.50.99 | -      | SELECT defacdad FROM pg_catalog.pg_default_acl dad WHERE dad.defacdnamespac = 2200::oid AND defacobjtype = 'T'  | 0    | 40.85 秒 | 成功   | <a href="#">详细</a> |
| 2022-06-02 03:05:08 | 普通规则    | 执行时长超过10秒         | 中风险  | 192.168.50.99 | -      | SELECT 2 AS nspobj, nsp.nspname, nsp.oid, pg_get_userbyid(nspowner) AS namespaceowner, nspod.description, FALSE as concrate FROM pg_namespace nsp LEFT OUTER JOIN pg_description des ON (des.objid=nsp.oid AND des.classoid=pg_namespace::regclass) WHERE ((nspname = 'pg_catalog' AND EXISTS (SELECT 1 FROM pg_class WHERE rela... | 2    | 40.86 秒 | 成功   | <a href="#">详细</a> |
| 2022-06-02 03:03:46 | 普通规则    | PostgreSQL_重连系统信息 | 低风险  | 192.168.50.99 | -      | SELECT setting FROM pg_settings WHERE name IN ('autovacuum', 'track_counts')  | 2    | 128 微秒  | 成功   | <a href="#">详细</a> |
| 2022-06-02 02:57:38 | 普通规则    | Oracle_表或视图不存在    | 低风险  | 10.11.33.177  | system | select * from staff   | 0    | 77 微秒   | 失败   | <a href="#">详细</a> |
| 2022-06-02 02:57:38 | 普通规则    | 修改_删除TABLE操作      | 中风险  | 10.11.33.177  | system | drop table staff  | 0    | 233 微秒  | 成功   | <a href="#">详细</a> |
| 2022-06-02 02:56:16 | 普通规则    | 无WHERE条件修改数据      | 高风险  | 10.11.33.177  | system | update staff set name='oracle'  | 9    | 191 微秒  | 成功   | <a href="#">详细</a> |
| 2022-06-02 02:53:32 | 普通规则    | 数据库登录失败           | 中风险  | 10.11.33.177  | syste  | login syste   | 0    | 130 微秒  | 失败   | <a href="#">详细</a> |

共 20766 条 1 2 3 4 5 ... 1039 > 20 条/页 跳至  页

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。

### 告警日志详细

基本信息

|      |                       |         |                    |
|------|-----------------------|---------|--------------------|
| 发生时间 | 2022-06-02 03:05:49   | 是否为统计规则 | 普通规则               |
| 规则名称 | 执行时长超过10秒             | 告警ID    | 368885500210186257 |
| 告警等级 | 中风险                   | 审计ID    | 368882695116359696 |
| 资产名称 | autotestPostgreSQLnew | 会话ID    | 368874538321053716 |

客户端

|        |                   |         |      |
|--------|-------------------|---------|------|
| 客户端IP  | 192.168.50.99     | 客户端端口   | 1883 |
| 客户端MAC | 00:50:56:9d:4f:59 | 客户端工具   | -    |
| 主机名    | -                 | 操作系统用户名 | -    |
| 执行人    | -                 |         |      |

服务端

|        |                   |          |            |
|--------|-------------------|----------|------------|
| 服务端IP  | 192.168.50.95     | 服务端端口    | 5432       |
| 服务端MAC | 00:50:56:9d:4f:58 | 数据库类型    | POSTGRESQL |
| 数据库账号  | -                 | 数据库名/实例名 | -          |

请求

|         |                                 |            |     |
|---------|---------------------------------|------------|-----|
| 操作类型    | Select                          | 原始SQL长度(B) | 113 |
| SQL模板ID | 622503957166566705              |            |     |
| 对象      | 表: pg_default_acl 字段: defaclacl |            |     |
| SQL语句概述 | 查询中pg_default_acl表的defaclacl字段。 |            |     |

报文(原文) 报文(高亮)

```
SELECT defaclacl FROM pg_catalog.pg_default_acl dacl WHERE dacl.defaclnamespace = 2200::oid AND defaclobjtype='T'
```

响应

|      |         |        |          |
|------|---------|--------|----------|
| 影响行数 | 0       | 执行状态   | 执行成功     |
| 执行时长 | 40.85 秒 | 执行结果描述 | SUCCESS: |

取证 此类日志不告警 上一条 下一条 取消

## 4.2.2 告警分析

步骤 1. 在菜单栏选择“**查询分析>告警日志**”，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。

### 告警日志

告警日志 告警分析

告警分析数据每小时更新一次，如无数据请耐心等待。

时间范围 2022-06-06 00:00:00 ~ 2022-06-06 14:59:59

筛选: 时间范围:2022-06-06 00:00:00~2022-06-06 ...

| 规则名称                  | 告警等级 | 告警数量 | 告警资产数量 | 数据库账号数量 | 客户端IP数量 | 描述                               | 操作 |
|-----------------------|------|------|--------|---------|---------|----------------------------------|----|
| MySQL_查询块具有不正确的结果列数   | 中风险  | 4    | 1      | 1       | 1       | MySQL错误码1222, 可能是sql注入猜测查询返回结果列数 | 详情 |
| 数据库登录失败               | 中风险  | 22   | 2      | 2       | 2       | 数据库登录失败                          | 详情 |
| Oracle_数据库登录密码错误      | 低风险  | 2    | 1      | 1       | 1       | oracle错误码01017                   | 详情 |
| MySQL_用户名密码错误导致登录失败   | 低风险  | 2    | 1      | 1       | 1       | MySQL错误码1045                     | 详情 |
| MySQL_使用MYSQLDUMP工具导出 | 中风险  | 1    | 1      | 1       | 1       | mysqldump是对数据库进行数据导出操作           | 详情 |

步骤 2. 点击操作列下的<详情>, 可查看告警统计详情, 页面包含规则详情、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。

告警统计详情 2021-06-21 00:00:00 ~ 2021-06-21 20:59:59

基本信息

名称: 执行时长超过5秒 所属规则组: /违规操作规则/应用账号违规操作

资产数量: 20

白名单数量: 0

规则类型: 普通规则

描述: 语句执行时长超过5秒

结果

执行时长: 大于等于 5000001 微秒

告警资产

| 资产名称         | 类型     | IP端口   | 告警数量    | 规则启用状态 |
|--------------|--------|--|---------|--------|
| crmweb       | WEB    | 134.96.41.7:80,134.96.41.16:80,134.96.41.47:80                                   | 418,459 | 已启用    |
| Oracle_dump4 | Oracle | 192.168.0.207:1521,192.168.0.19:1521,192.168.0.30:1521,192.168.0.18:1521,192.... | 125     | 已启用    |

crmweb Oracle\_dump4

告警趋势



告警趋势图显示了告警数量的波动，Y轴范围从3万到5万。图中显示告警数量在约4.2万至4.5万之间波动。

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。

规则详情

基本信息

名称: 大量拖库 所属规则组: /数据泄露规则/大流量返回

资产数量: 12

白名单数量: 0

规则类型: 普通规则

描述: 查询数据超过9999行

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。

告警资产

| 资产名称                     | 类型         | IP端口                | 告警数量 | 规则启用状态 |
|--------------------------|------------|---------------------|------|--------|
| sqlserver_192.168.128.34 | SQL Server | 192.168.128.34:1433 | 861  | 已启用    |

步骤 5. 在告警来源区域, 点击操作列下的<不再告警>。

| 告警来源 维度: <input checked="" type="checkbox"/> 客户端IP <input checked="" type="checkbox"/> 数据库账号 |       |      |             |
|--|-------|------|-------------|
| 客户端IP  | 数据库账号 | 告警数量 | 操作          |
| 192.168.100.179  | 未知    | 861  | <b>不再告警</b> |

显示 1 - 1, 共 1 条 < 1 > 10 条/页 跳至  页

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。

不再告警
X

---

\* 满足条件:  客户端IP: 192.168.100.179

\* 方式:  添加到白名单  添加到信任规则

仅对【大量拖库】有效

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>**。

| 触发告警的SQL模板  |      |             |
|---|------|-------------|
| SQL模板   | 告警数量 | 操作          |
| SELECT DealerCode,ProvinceCode INTO #base FROM LYDB.dbo.Dealer... | 861  | <b>不再告警</b> |

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，系统对于此规则符合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](#)。



## 4.3 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。

### 4.3.1 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，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。

## 会话日志

历史会话 在线会话

最大返回条数: 100000, 最大查询时间: 10秒 [修改](#)

查询条件: 时间范围: 本日(2022-06-02 00:00:00~2022-06-02 23:59:59) [保存](#) [搜索](#) [重置](#)

时间范围: 最近5分钟 最近30分钟 最近1小时 最近6小时 **本日** 昨天 本周 本月 2022-06-02 00:00:00 ~ 2022-06-02 23:59:59

资产: 全部 数据库账号: 请输入数据库账号, 多个值使用","隔开 客户端IP: 请输入客户端IP, 多个值使用","隔开

服务端IP: 请输入服务端IP, 多个值使用","隔开 服务端端口: 请输入服务端端口, 多个值使用","隔开 状态标识: 全部

[更多条件](#)

日志列表

| 会话开始时间              | 客户端IP        | 服务端IP          | 数据库名/实例名 | 状态标识 | SQL总记录数 | 请求流量   | 返回流量   | 会话结束方式 | 过滤SQL数量 | 操作                 |
|---------------------|--------------|----------------|----------|------|---------|--------|--------|--------|---------|--------------------|
| 2022-06-02 03:03:05 | 10.11.33.177 | 192.168.22.21  | d1       | 登录成功 | 12      | 3.07KB | 3.51KB | 异常结束   | 0       | <a href="#">详细</a> |
| 2022-06-02 03:01:43 | 10.11.33.177 | 192.168.21.243 | -        | 登录成功 | 2       | 917B   | 1.13KB | 正常结束   | 0       | <a href="#">详细</a> |
| 2022-06-02 02:59:40 | 10.11.33.177 | 192.168.21.243 | lora121  | 登录成功 | 13      | 8.39KB | 9.02KB | 正常结束   | 0       | <a href="#">详细</a> |
| 2022-06-02 02:58:59 | 10.11.33.177 | 192.168.21.243 | lora121  | 登录成功 | 13      | 8.39KB | 9.02KB | 正常结束   | 0       | <a href="#">详细</a> |

共 12549 条 < 1 2 3 4 5 ... 628 > 20 条/页 跳至 页

点击操作列中的<详细>可查看会话详情。

### 会话详情

#### 基本信息

|      |                    |        |                     |        |                     |
|------|--------------------|--------|---------------------|--------|---------------------|
| 会话ID | 368866154309552166 | 会话开始时间 | 2022-06-02 03:01:43 | 会话结束时间 | 2022-06-02 03:02:24 |
| 资产名称 | autotest-oracle    |        |                     |        |                     |

#### 客户端信息

|       |              |       |      |         |                   |
|-------|--------------|-------|------|---------|-------------------|
| 客户端IP | 10.11.33.177 | 客户端端口 | 4872 | 客户端MAC  | a0:a8:cd:90:02:40 |
| 客户端工具 | 无            | 主机名   | 无    | 操作系统用户名 | 无                 |

#### 服务端信息

|       |                |       |      |          |                   |
|-------|----------------|-------|------|----------|-------------------|
| 服务端IP | 192.168.21.243 | 服务端端口 | 1521 | 服务端MAC   | 70:57:bf:23:56:01 |
| 数据库类型 | ORACLE         | 数据库账号 | 无    | 数据库名/实例名 | 无                 |

#### 会话中的审计记录

| 发生时间                | 报文  | 影响行数 | 执行时长   | 执行状态 |
|---------------------|---|------|--------|------|
| 2022-06-02 03:02:24 | logout  | 0    | 0 微秒   | 成功   |
| 2022-06-02 03:01:43 | insert into staff values (9, 'hill', 5800, 185.5, 190.5, 'hill@nba.com', 4) | 0    | 570 微秒 | 成功   |

共 2 条 < 1 > 20 条/页 跳至 页

## 4.3.2 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。

## 会话日志

历史会话
在线会话

---

最大返回条数: 100000, 最大查询时间: 10秒 [修改](#)

查询条件: 时间范围: 本日(2022-06-02 00:00:00~2022-06-02 23:59:59) [保存](#)
[搜索](#) [重置](#)

时间范围:

最近5分钟
最近30分钟
最近1小时
最近6小时
本日
昨天
本周
本月

2022-06-02 00:00:00 ~ 2022-06-02 23:59:59 [🗄](#)

资产: 全部

数据库账号: 请输入数据库账号, 多个值使用","隔开

客户端IP: 请输入客户端IP, 多个值使用","隔开

服务端IP: 请输入服务端IP, 多个值使用","隔开

服务端端口: 服务端端口, 多个值使用","隔开

状态标识: 全部

[更多条件](#)

日志列表
[↓](#) [🔍](#)

| 会话开始时间              | 客户端IP        | 服务端IP          | 数据库名/实例名 | 状态标识 | SQL总记录数 | 请求流量   | 返回流量   | 会话结束方式 | 过滤SQL数量 | 操作                 |
|---------------------|--------------|----------------|----------|------|---------|--------|--------|--------|---------|--------------------|
| 2022-06-02 03:03:05 | 10.11.33.177 | 192.168.22.21  | d1       | 登录成功 | 12      | 3.07KB | 3.51KB | 异常结束   | 0       | <a href="#">详细</a> |
| 2022-06-02 03:01:43 | 10.11.33.177 | 192.168.21.243 | -        | 登录成功 | 2       | 917B   | 1.13KB | 正常结束   | 0       | <a href="#">详细</a> |
| 2022-06-02 02:59:40 | 10.11.33.177 | 192.168.21.243 | lora121  | 登录成功 | 13      | 8.39KB | 9.02KB | 正常结束   | 0       | <a href="#">详细</a> |
| 2022-06-02 02:58:59 | 10.11.33.177 | 192.168.21.243 | lora121  | 登录成功 | 13      | 8.39KB | 9.02KB | 正常结束   | 0       | <a href="#">详细</a> |

共 12549 条 [<](#) 1 [2](#) [3](#) [4](#) [5](#) ... [628](#) [>](#)

20 条/页 [跳至](#)   [页](#)

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。

## 4.4 查询 SQL 模板

SQL 模板 (SQL Template) 是去参数化的 SQL 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:

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。

## SQL模板

当前模板数量上限为30万, 点此 [修改](#)

查询条件 v: 时间范围: 本日(2022-06-02 00:00:00~2022-06-02 23:59:59) 保存 搜索 重置

时间范围: 最近5分钟 最近30分钟 最近1小时 最近6小时 **本日** 昨天 本周 本月 2022-06-02 00:00:00 ~ 2022-06-02 23:59:59

SQL模板: 请输入SQL模板关键字, 多个关键字用“,”隔开

服务端IP: 请输入服务端IP SQL模板ID: 请输入SQL模板ID, 多个值使用“,”隔开 操作类型:

[更多条件](#)

[分析查询结果](#)

---

日志列表 ⊞

| SQL模板ID            | SQL模板  | 发生时间                | 服务端IP       | 操作类型 | 操作                 |
|--------------------|--|---------------------|-------------|------|--------------------|
| 655096106115265290 | do ##class(web.DHCRisApplication).UpPrint2(:1,"13965147 :2";:3";:4")   | 2022-06-02 01:43:14 | 192.168.2.3 | Do   | <a href="#">详细</a> |
| 413289406215160616 | do ##class(web.DHCINSUDivideCit).InsertDivInfo(:1,"",^14852188^4170456^17472885^divide^1196.2^0511000202131105012137^0^20130963666884^1^10098713200X^0^0^225.67^^^100987132005^970.53^0^4407^20131105163936^^^林和廷^0^^1196.2^1141.8^0^54.4^0^54.4^799.26^342.54^0.00^171.27^0.00^0.00^^^0.00 0.00 0.00 0.00 610.00 0... | 2022-06-02 01:43:11 | 192.168.2.3 | Do   | <a href="#">详细</a> |
| 130236902124598304 | do ##class(web.DHCRisApplication).GetRDDetail(:1,"13972122 :2";:3";:4")  | 2022-06-02 01:42:43 | 192.168.2.3 | Do   | <a href="#">详细</a> |

共 679 条 < 1 2 3 4 5 ... 34 > 20 条/页 跳至  页



- ◆ 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

[点击显示其余ip端口](#)

## 5 报表中心

报表用表格、图表等形式来动态显示数据，直观明了。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。

### 5.1 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。

The screenshot shows the 'Report Preview' interface. At the top, there are tabs for different report types: '塞班斯报表', '综合分析报告', '性能分析报表', '等候参考分析报表', '会话分析类报表', '会话分析类报表', '告警分析类报表', '其它报表', and '自定义报表'. Below the tabs, there are filters for '资产' (Assets) and '时间范围' (Time Range). The main content area displays a report titled '塞班斯 (SOX) 法案 数据库安全审计符合性报告'. The report includes a table of contents on the left and a main content area with sections like '第一章 概述', '1.1 报告阅读对象', '1.2 分析对象与范围', and '1.3 审计分析对象'. The '1.2 分析对象与范围' section contains a table with columns for '分析对象', '数据库类型', 'IP与端口信息', '时间范围', and '报告生成时间'.

| 分析对象    | 120-智联社DB2测试, dm-192.168.21.163, PostgreSQL_134.209.96.129, PostgreSQL_134.236.29.156, wx_test01, sqlserver_192.168.30.174, 数据库1, PostgreSQL_134.119.1.197, PostgreSQL_192.168.30.239, PostgreSQL_192.168.30.79, Oracle_192.168.50.60, chuanhau, Redis_10.101.80.23, 67_达梦数据库, 学习156, chen123, cache, 数据库, Oracle_10.100.11.111, PostgreSQL_10.50.3.135, mysql_192.168.30.134, Oracle_180.0.0.13, asort77 数据库, DM_10.50.3.136, 172.16.24.175, MySQL_192.168.100.102, 智联社HIVE测试, zuan, sqlserver_172.18.1.5, MySQL_10... |
|---------|---|
| 数据库类型   | DB2, 达梦(DM), PostgreSQL, Oracle, SQL Server, MySQL, Redis, Hive, MariaDB, Cache, MongoDB, HTTP, GaussDB, Hana, 人大金仓(Kingbase), Teradata, HBase(protobuf), Cassandra, Informix, 南大通用(GBase), Elasticsearch, HBase(thrift)  |
| IP与端口信息 | 10.50.3.120:50010,10.50.3.120:50015,10.50.3.120:50020; 192.168.21.163:5236; 134.209.96.129:5432; 134.236.29.156:5432; 97.1.2.3:1521; 192.168.30.174:1433; 192.168.1.11:3306; 134.119.1.197:5432; 192.168.30.239:5432; 192.168.30.79:5432; 192.168.50.60:1521; 10.33.70.43:3306,10.36.8.167:3306; 10.101.80.23:6379; 192.168.1.67:10000; 192.168.30.156:3306; 192.1.1.100:5432; 192.168.1.100:1972; 192.168.1.13306,192.168.1.2:3306; 10.100.11.111:1521; 10.50.3.135:5432,192.168.30.79:20002; 192.168.30.134:3306...   |
| 时间范围    | 2022-06-23 00:00:00 ~ 2022-06-23 08:59:59   |
| 报告生成时间  | 2022-06-23 09:31:32   |

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况。                 |
| 综合分析报表 | 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             |

| 报表类型     | 说明  |
|----------|---|
|          | 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 <a href="#">自定义报表</a> 。  |

## 5.2 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**>。

#### 报表预览



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

## 添加订阅任务



\* 任务名称:

\* 收件人邮箱:

可输入多个邮箱地址, 使用","分隔

报表类型:

报表格式:  HTML  PDF  PNG  WORD

资产:

任务周期:

发送时间:

时间范围:

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。                                   |
| 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>。

## 报表订阅



| <input type="checkbox"/> | 名称    | 发送时间       | 报表类型   | 报表格式 | 资产    | 收件人   | 操作    |
|--------------------------|-------|------------|--------|------|-------|-------|-------|
| <input type="checkbox"/> | test2 | 每天 1:00    | 综合分析报告 | WORD | 全部数据库 | ei... | 编辑 删除 |
| <input type="checkbox"/> | test  | 每月 1日 1:00 | 麦班斯报表  | PDF  | 全部数据库 | h...  | 编辑 删除 |

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>。

## 5.3 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）。

### 5.3.1 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。

#### 5.3.1.1 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>。

## 自定义报表



| <input type="checkbox"/> | 名称   | 统计维度             | 统计指标                | 筛选条件 | 数据开始时间 | 操作       |
|--------------------------|------|------------------|---------------------|------|--------|----------|
| <input type="checkbox"/> | 3321 | 客户端工具,数据库账号,操作类型 | 最后一条记录时间,执行时长总和,... | 321  | 暂未入库   | 预览 编辑 删除 |

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>。

添加筛选条件

X

\* 名称:

客户端IP: 等于

客户端端口: 等于

服务端IP: 等于

服务端端口: 等于

数据库账号: 等于

数据库名/实例名: 等于

操作系统用户名: 等于

主机名: 等于

客户端工具: 等于

数据库类型: 等于

5) 在**筛选条件**文本框中点击  图标，选择筛选条件。

添加报表数据

X

报表数据是自定义报表中展示的实际内容，需先创建报表数据，再从自定义报表引用报表数据

\* 名称:

\* 统计维度:

\* 统计指标:

筛选条件:

仅统计满足以下条件的日志:

|         |    |             |
|---------|----|-------------|
| 1、客户端IP | 等于 | 192.168.0.1 |
| 2、客户端端口 | 等于 | 23          |

6) 点击<保存>。

### 5.3.1.2 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。

## 5.3.2 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）。

### 5.3.2.1 添加自定义报表

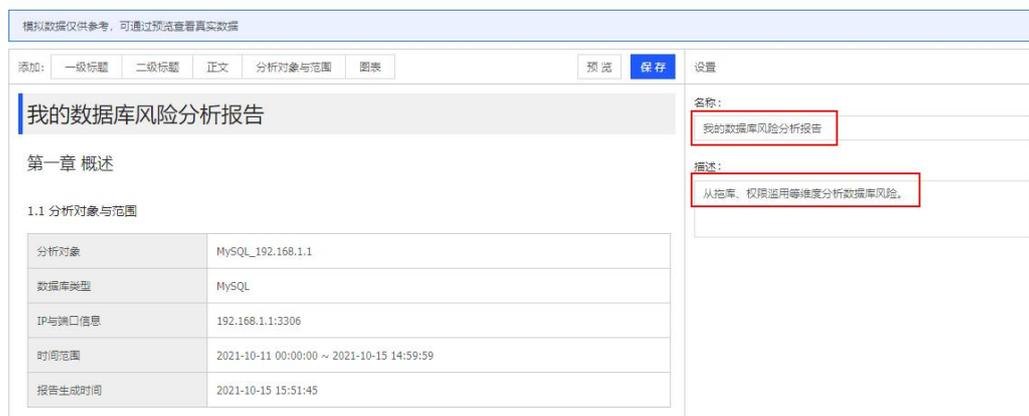
步骤 1. 在菜单栏选择“**报表中心**>**自定义报表**”进入**自定义报表**页面，选择**报表管理**页签，点击<添加>。

自定义报表



步骤 2. 进入**添加自定义报表**页面，编辑名称和描述。

添加自定义报表



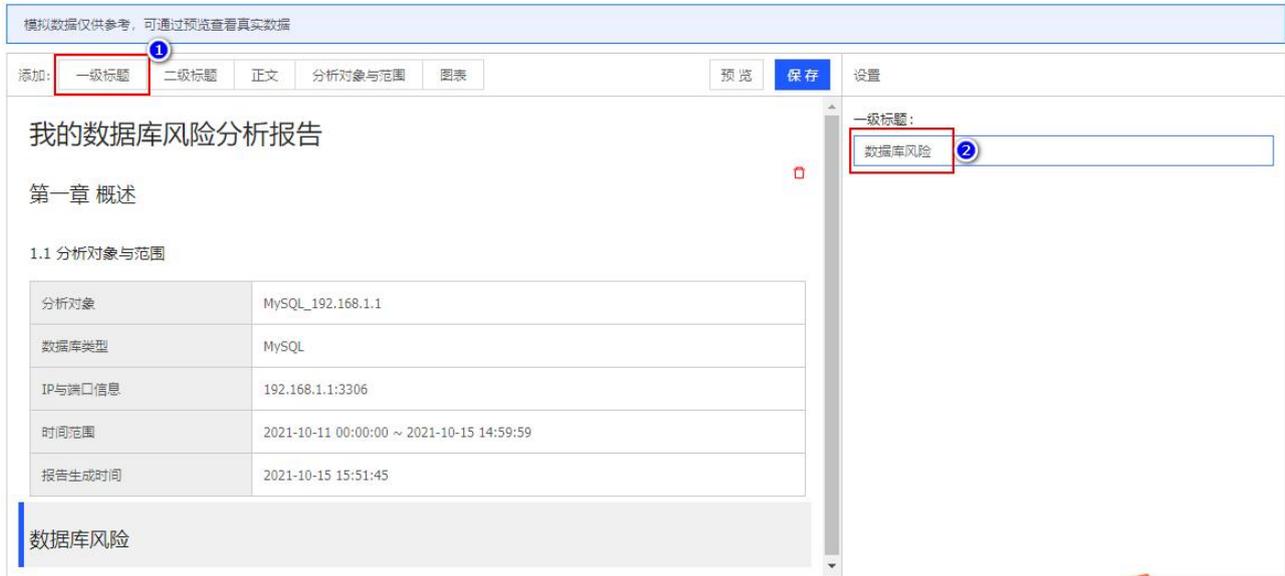
详细配置请参见下表。

| 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）。

#### 添加自定义报表



模拟数据仅供参考，可通过预览查看真实数据

添加：一级标题 二级标题 正文 分析对象与范围 图表 预览 保存 设置

## 我的数据库风险分析报告

### 第一章 概述

#### 1.1 分析对象与范围

|         |   |
|---------|---|
| 分析对象    | MySQL_192.168.1.1                         |
| 数据库类型   | MySQL                                     |
| IP与端口信息 | 192.168.1.1:3306                          |
| 时间范围    | 2021-10-11 00:00:00 ~ 2021-10-15 14:59:59 |
| 报告生成时间  | 2021-10-15 15:51:45                       |

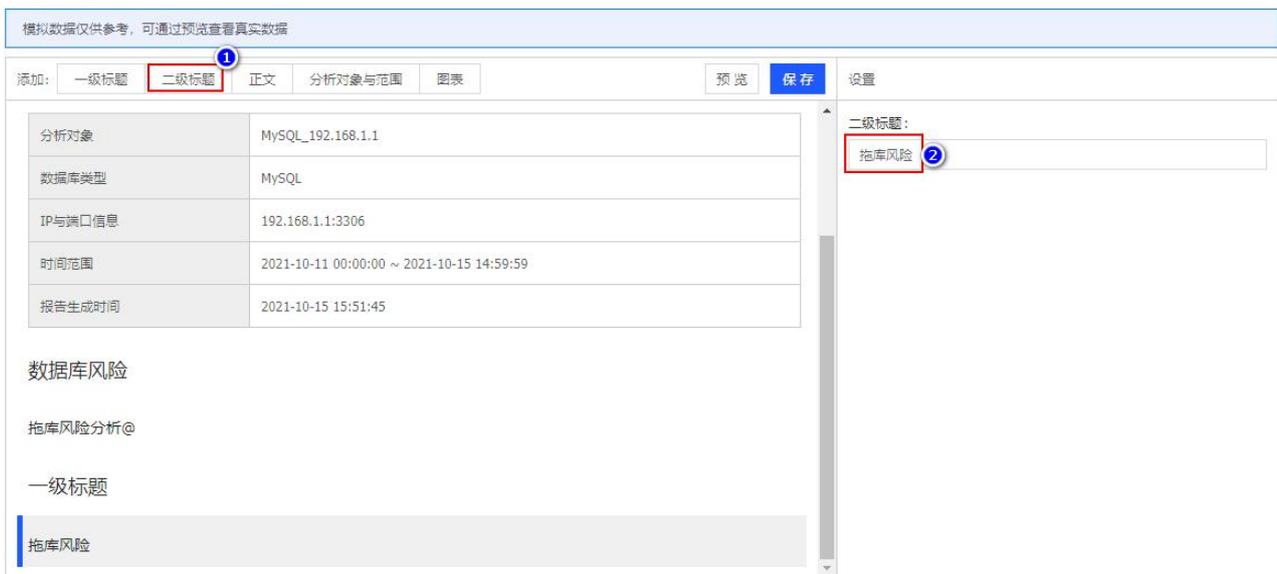
数据库风险

一级标题：  
数据库风险

### 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）。

#### 添加自定义报表



模拟数据仅供参考，可通过预览查看真实数据

添加：一级标题 二级标题 正文 分析对象与范围 图表 预览 保存 设置

|         |   |
|---------|---|
| 分析对象    | MySQL_192.168.1.1                         |
| 数据库类型   | MySQL                                     |
| IP与端口信息 | 192.168.1.1:3306                          |
| 时间范围    | 2021-10-11 00:00:00 ~ 2021-10-15 14:59:59 |
| 报告生成时间  | 2021-10-15 15:51:45                       |

## 数据库风险

### 拖库风险分析@

#### 一级标题

拖库风险

二级标题：  
拖库风险

### 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)。

## 添加自定义报表

模拟数据仅供参考, 可通过预览查看真实数据

添加: 一级标题 二级标题 **正文** 分析对象与范围 图表 预览 保存 设置

|         |   |
|---------|---|
| 分析对象    | MySQL_192.168.1.1                         |
| 数据库类型   | MySQL                                     |
| IP与端口信息 | 192.168.1.1:3306                          |
| 时间范围    | 2021-10-11 00:00:00 ~ 2021-10-15 14:59:59 |
| 报告生成时间  | 2021-10-15 15:51:45                       |

数据库风险

拖库风险分析@

一级标题

拖库风险

数据库拖库是指指从**数据库**中导出数据。到了黑客攻击泛滥的今天, 它被用来指网站遭到入侵后, 黑客窃取其**数据库**文件, **拖库**的主要防护手段是**数据库**加密。

正文:

**B I U A** 列表 列表

数据库拖库是指指从**数据库**中导出数据。到了黑客攻击泛滥的今天, 它被用来指网站遭到入侵后, 黑客窃取其**数据库**文件, **拖库**的主要防护手段是**数据库**加密。



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。

## 添加自定义报表

模拟数据仅供参考, 可通过预览查看真实数据

添加: 一级标题 二级标题 正文 **分析对象与范围** 图表 预览 保存 设置

拖库风险分析@

一级标题

拖库风险

数据库拖库是指指从**数据库**中导出数据。到了黑客攻击泛滥的今天, 它被用来指网站遭到入侵后, 黑客窃取其**数据库**文件, **拖库**的主要防护手段是**数据库**加密。

|         |   |
|---------|---|
| 分析对象    | MySQL_192.168.1.1                         |
| 数据库类型   | MySQL                                     |
| IP与端口信息 | 192.168.1.1:3306                          |
| 时间范围    | 2021-10-11 00:00:00 ~ 2021-10-15 14:59:59 |
| 报告生成时间  | 2021-10-15 15:51:45                       |

显示内容: 全部 仅显示对象 仅显示范围

## 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。

### 添加自定义报表

模拟数据仅供参考，可通过预览查看真实数据

添加：一级标题 二级标题 正文 分析对象与范围 **图表** 预览 保存 设置

报表名称

第一章 概述

1.1 分析对象与范围

|         |   |
|---------|---|
| 分析对象    | MySQL_192.168.1.1                         |
| 数据库类型   | MySQL                                     |
| IP与端口信息 | 192.168.1.1:3306                          |
| 时间范围    | 2021-10-11 00:00:00 ~ 2021-10-15 14:59:59 |
| 报告生成时间  | 2021-10-15 15:51:45                       |

数据库分析

| 显示                                  | 列名     | 宽度 |
|-------------------------------------|--------|----|
| <input checked="" type="checkbox"/> | 资产名称   | 自动 |
| <input checked="" type="checkbox"/> | 客户端IP  | 自动 |
| <input checked="" type="checkbox"/> | 平均请求流量 | 自动 |

步骤 8. 点击<保存>。

### 添加自定义报表

模拟数据仅供参考，可通过预览查看真实数据

添加：一级标题 二级标题 正文 分析对象与范围 图表 预览 **保存** 设置

## 5.3.2.2 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。

自定义报表

报表管理 报表数据管理

添加 名称 请输入查询关键字

| 名称                                | 报表数据  | 描述   | 操作              |
|-----------------------------------|---|------|-----------------|
| <input type="checkbox"/> zuan     | 客户端IP_top100_byceshi                          | 报表描述 | <b>预览 编辑 删除</b> |
| <input type="checkbox"/> 报表名称111  | 913test                                       | 报表描述 | 预览 编辑 删除        |
| <input type="checkbox"/> 统计IP访问次数 | 1471728874688614400                           | 报表描述 | 预览 编辑 删除        |
| <input type="checkbox"/> 统计IP访问   | 1471685737794506752                           | 报表描述 | 预览 编辑 删除        |
| <input type="checkbox"/> 操作类型数量统计 | 1469180762229051392,1465927165122973696,14... | 报表描述 | 预览 编辑 删除        |

## 6 智能分析

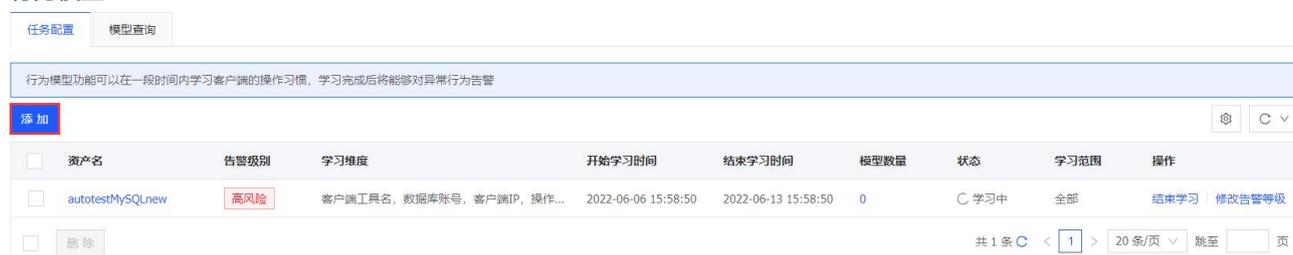
智能分析是指系统可以学习用户的数据库操作习惯，通过对用户操作所涉及的 IP、客户端操作工具等信息进行统计分析，可对异常行为进行告警。

### 6.1 添加行为模型学习任务

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>。

行为模型



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）。

学习范围(IP):

行为模型引擎将只学习范围内的客户端IP 产生的行为;默认学习所有客户端IP。  
 格式1:多个IP使用“,”隔开; 格式2:IP网段:用“\*”表示0~255的整数,例如:  
 192.126.30.\*; 192.126.\*.\*; (“\*”之后不应出现数字); 格式3:用两个IP表示一个IP网段,例如:  
 192.126.30.128-192.126.75.131 (靠前的两位需一致)。

[最简配置](#)

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：<br>◆ 可填写多个 IP，每个 IP 之间用 “,” 隔开。<br>◆ IP 网段，用 “*” 表示 0~255，例如：192.168.0.*、10.1.*.*。<br>◆ IP 范围，例如：192.168.2.1-192.168.2.128。 |

## 6.2 设置模型查询

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。

行为模型

任务配置
模型查询

行为模型功能可以在一段时间内学习客户端的操作习惯，学习完成后将能够对异常行为告警

添加
⚙️ C v

| <input type="checkbox"/> | 资产名  | 告警级别 | 学习维度        | 开始学习时间              | 结束学习时间              | 模型数量 | 状态  | 学习范围       | 操作  |
|--------------------------|--|------|-------------|---------------------|---------------------|------|-----|------------|---|
| <input type="checkbox"/> | <span style="border: 1px solid red; padding: 2px;">mysql_10.100.4.108</span> | 不告警  | 客户端工具名, ... | 2021-01-26 14:06:33 | 2021-01-28 14:43:14 | 25   | 告警中 | 10.100.*.* | <a href="#">重新学习</a>   <a href="#">修改告警等级</a> |
| <input type="checkbox"/> | <span style="border: 1px solid #ccc; padding: 2px;">删除</span>                |      |             |                     |                     |      |     |            |   |

共 1 条 C < 1 > 20 条/页 v

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。

### 行为模型

任务配置
模型查询

资产: 8888Informix

操作系统用户名: 请输入操作系统用户名

操作类型: 全部类型

汇总维度: 不汇总

数据库名/SID: 请输入数据库名/SID

客户端IP: 请输入客户端IP

客户端工具: 请输入客户端工具

数据库账号: 请输入数据库账号

表对象: 请输入表对象

搜索
分析
重置

CCCCCCCCCCCCCCCC

满足条件的模型数量:381;加载分析的模型数量:381;最大允许加载数量:5000 (修改)

▽筛选: 无筛选条件, 可点击节点或连线添加 显示设置

数据库账号 (共8项) ▾

客户端IP (共122项) ▾

客户端工具 (共2项) ▾

操作系统用户名 (共1项) ▾

操作类型 (共7项) ▾

数据库名/SID (共3项) ▾

表对象 (共1项) ▾

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。

### 行为模型

任务配置
模型查询

资产: SQLServer\_2003\_1\_2\_3\_4\_10

操作系统用户名: 请输入操作系统用户名

数据库账号: 请输入数据库账号

客户端主机名: 请输入客户端主机名

汇总维度: 不汇总

数据库名/SID: 请输入数据库名/SID

操作类型: 全部类型

表对象: 请输入表对象

客户端工具: 请输入客户端工具

服务端IP: 请输入服务端IP

客户端IP: 请输入客户端IP

搜索
分析
重置

模型列表 🔍

| 客户端工具 | 操作系统用户名 | 数据库名/SID | 服务端IP            | 数据库账号 | 操作类型   | 客户端IP (网络名称)       | 客户端主机名 | 表对象 |
|-------|---------|----------|------------------|-------|--------|--------------------|--------|-----|
| 未知    | 未知      | test     | 2003:1:2:3:4::10 | test  | Logout | 2002:1:2:3:3::48f6 | 未知     | 未知  |
| 未知    | 未知      | test     | 2003:1:2:3:4::10 | test  | Login  | 2002:1:2:3:3::3a21 | 未知     | 未知  |
| 未知    | 未知      | test     | 2003:1:2:3:4::10 | test  | Logout | 2002:1:2:3:3::70c0 | 未知     | 未知  |

## 7 规则配置

规则配置是指根据一些特征（如客户端、服务端、SQL 语句）定义危险行为（安全规则）和可以信任的行为（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。

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。

### 7.1 安全规则

安全规则库用来保存已发现的不安全 SQL 语句的特征信息。系统通过将审计到的 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。

#### 7.1.1 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：

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>。

## 安全规则

| 规则管理                     |                                  | 白名单管理                               | 设置      |       |   |
|--------------------------|----------------------------------|-------------------------------------|---------|-------|---|
| <b>新增</b>                | 规则名称 ▾                           | 请输入查询关键字                            |         |       |   |
|                          |                                  | <input checked="" type="radio"/> 推荐 | 仅显示特征规则 |       |   |
| <input type="checkbox"/> | 名称                               | 等级                                  | 资产数量    | 白名单数量 | 操作                                      |
| <input type="checkbox"/> | + MySQL_安全漏洞CVE-2018-2696        | 高风险                                 | 0       | 0     | <a href="#">编辑</a>                      |
| <input type="checkbox"/> | + SQLServer_创建程序集                | 中风险                                 | 0       | 0     | <a href="#">编辑</a>   <a href="#">克隆</a> |
| <input type="checkbox"/> | + DM_SP_DEL_BAK_EXPIRED过程内存破坏漏洞  | 中风险                                 | 0       | 0     | <a href="#">编辑</a>                      |
| <input type="checkbox"/> | + MySQL_使用DUMPFIL导出              | 高风险                                 | 0       | 0     | <a href="#">编辑</a>   <a href="#">克隆</a> |
| <input type="checkbox"/> | + MySQL_注入恶意配置提升权限漏洞             | 高风险                                 | 0       | 0     | <a href="#">编辑</a>                      |
| <input type="checkbox"/> | + MySQL_udf权限提升漏洞                | 中风险                                 | 0       | 0     | <a href="#">编辑</a>                      |
| <input type="checkbox"/> | + MySQL_Parser子组件拒绝服务漏洞          | 中风险                                 | 0       | 0     | <a href="#">编辑</a>                      |
| <input type="checkbox"/> | + MySQL_指定特质几何功能拒绝服务漏洞           | 中风险                                 | 0       | 0     | <a href="#">编辑</a>                      |
| <input type="checkbox"/> | + PostgreSQL_利用SEARCH_PATH提升权限漏洞 | 高风险                                 | 0       | 0     | <a href="#">编辑</a>                      |

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>。

## 安全规则

| 规则管理                     |                           | 白名单管理                    | 设置      |       |  |
|--------------------------|---------------------------|--------------------------|---------|-------|--|
| <b>新增</b>                | 规则名称 ▾                    | 请输入查询关键字                 |         |       |  |
|                          |                           | <input type="radio"/> 推荐 | 仅显示特征规则 |       |  |
| <input type="checkbox"/> | 名称                        | 等级                       | 资产数量    | 白名单数量 | 操作   |
| <input type="checkbox"/> | + test                    | 中风险                      | 2       | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>   <a href="#">删除</a> |
| <input type="checkbox"/> | + MySQL_安全漏洞CVE-2018-2696 | 高风险                      | 0       | 0     | <a href="#">编辑</a>   |

步骤 2. 在新增规则对话框中编辑相关信息，点击<保存>。

**基本信息**

\* 名称:

描述:

等级:  高风险  中风险  低风险

所属规则组:  规则组管理

规则类型:  普通规则  统计规则

行为:  告警  告警并阻断

**客户端**

客户端来源:  IP  IP组

可配多个IP, 使用逗号"/"分隔, 支持末尾两位为\*。例: 192.168.1.2,192.168.1.3

客户端工具:  字符串  正则表达式

字符串 可配多个客户端工具, 使用逗号"/"分隔, 例: db2bp.exe,javaw.exe,plsqldev.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: 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, 例: fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf

操作系统用户名:  字符串  正则表达式

字符串 可填多值, 多个值间以逗号"/"分隔, 例: xxx,yyy

主机名:  字符串  正则表达式

字符串 可填多值, 多个值间以逗号"/"分隔, 例: xxx,yyy

应用IP:  IP  IP组

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。   |
|      | 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。                      |

| 项目  | 配置项        | 说明   |
|-----|------------|--|
|     | 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。<br><ul style="list-style-type: none"> <li>◆ <b>普通规则</b>：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）。</li> <li>◆ <b>统计规则</b>：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）。</li> </ul> |
|     | 行为         | 目前支持告警和告警并阻断。<br><ul style="list-style-type: none"> <li>◆ <b>告警</b>：操作命中规则后，仍正常执行，无特殊控制。</li> <li>◆ <b>告警并阻断</b>：操作命中规则后，该操作对应的数据库连接断开。</li> </ul>   |
| 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 <a href="#">IP 组管理</a> 。  |
|     | 客户端工具      | 可配多个客户端工具，使用逗号 “,” 分隔，例如：2bp.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 “,” 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 <a href="#">IP 组管理</a> 。   |

| 项目  | 配置项        | 说明  |
|-----|------------|---|
|     | 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 <a href="#">应用用户组管理</a> 。   |
| 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 <a href="#">数据库账号组管理</a> 。  |
|     | 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        | 指定规则所匹配的对象组。有关对象组的更多信息，请参考 <a href="#">对象组管理</a> 。  |
|     | 操作类型       | 指关注的操作类型，如 select、update、delete 等。  |
|     | 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 <a href="#">查询 SQL 模板</a> 。  |
|     | 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。单击<增加条件>添加多个条件。<br>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。   |

| 项目 | 配置项      | 说明   |
|----|----------|--|
|    | 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：<br>SELECT column_name,column_name<br>FROM table_name<br>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。<br>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 <a href="#">时间组管理</a> 。   |
|    | 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。  |

## 7.1.2 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。

### 安全规则

| 安全规则  |                                  |     |      |       |  |
|---|----------------------------------|-----|------|-------|--|
| 规则管理   白名单管理   设置   |                                  |     |      |       |  |
| 新增 <input type="text" value="规则名称"/> 请输入查询关键字 <input type="text" value=""/> |                                  |     |      |       |  |
| 推荐 <input type="radio"/> 仅显示特征规则 <input type="radio"/>                      |                                  |     |      |       |  |
| <input type="checkbox"/>  | 名称                               | 等级  | 资产数量 | 白名单数量 | 操作   |
| <input type="checkbox"/>  | + test                           | 中风险 | 2    | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>   <a href="#">删除</a> |
| <input type="checkbox"/>  | + MySQL_安全漏洞CVE-2018-2696        | 高风险 | 0    | 0     | <a href="#">编辑</a>   |
| <input type="checkbox"/>  | + SQLServer_创建程序集                | 中风险 | 0    | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>                      |
| <input type="checkbox"/>  | + DM_SP_DEL_BAK_EXPIRED)过程内存破坏漏洞 | 中风险 | 0    | 0     | <a href="#">编辑</a>   |
| <input type="checkbox"/>  | + MySQL_使用DUMPFIL导出              | 高风险 | 0    | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>                      |
| <input type="checkbox"/>  | + MySQL_注入恶意配置提升权限漏洞             | 高风险 | 0    | 0     | <a href="#">编辑</a>   |

启用全部  禁用全部  删除

共 275 条  2 3 4 5 ... 14 > 20 条/页 跳至  页

步骤 2. 在规则列表中勾选目标规则，然后点击<启用选中项>。

### 安全规则

| 安全规则  |                                  |     |      |       |  |
|---|----------------------------------|-----|------|-------|--|
| 规则管理   白名单管理   设置   |                                  |     |      |       |  |
| 新增 <input type="text" value="规则名称"/> 请输入查询关键字 <input type="text" value=""/> |                                  |     |      |       |  |
| 推荐 <input type="radio"/> 仅显示特征规则 <input type="radio"/>                      |                                  |     |      |       |  |
| <input type="checkbox"/>  | 名称                               | 等级  | 资产数量 | 白名单数量 | 操作   |
| <input checked="" type="checkbox"/>   | 1 test                           | 中风险 | 2    | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>   <a href="#">删除</a> |
| <input checked="" type="checkbox"/>   | + MySQL_安全漏洞CVE-2018-2696        | 高风险 | 0    | 0     | <a href="#">编辑</a>   |
| <input type="checkbox"/>  | + SQLServer_创建程序集                | 中风险 | 0    | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>                      |
| <input type="checkbox"/>  | + DM_SP_DEL_BAK_EXPIRED)过程内存破坏漏洞 | 中风险 | 0    | 0     | <a href="#">编辑</a>   |
| <input type="checkbox"/>  | + MySQL_使用DUMPFIL导出              | 高风险 | 0    | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>                      |
| <input type="checkbox"/>  | + MySQL_注入恶意配置提升权限漏洞             | 高风险 | 0    | 0     | <a href="#">编辑</a>   |
| <input type="checkbox"/>  | 2 + MySQL_udf权限提升漏洞              | 中风险 | 0    | 0     | <a href="#">编辑</a>   |

启用选中项  禁用选中项  删除

共 275 条  2 3 4 5 ... 14 > 20 条/页 跳至  页

步骤 3. 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。

设置使用规则(SQLServer\_创建程序集)资产

已选择 清空

名称 请输入查询关键字

| 名称   | 资产组    | 类型              | IP端口                     |
|--|--------|-----------------|--------------------------|
| <input type="checkbox"/> ☆ DB2_192.168.50.84                     | 自发现资产组 | DB2 v95         | 192.168.50.84:50000      |
| <input checked="" type="checkbox"/> ☆ SQLServer_2003_1_2_3_4_10  | 自发现资产组 | SQL Server 2003 | [2003:1:2:3:4::10]:1433  |
| <input checked="" type="checkbox"/> ☆ PostgreSQL_2003_1_2_3_4_10 | 自发现资产组 | PostgreSQL 11   | [2003:1:2:3:4::10]:5432  |
| <input checked="" type="checkbox"/> ☆ Oracle_2003_1_2_3_4_10     | 自发现资产组 | Oracle 11g      | [2003:1:2:3:4::10]:1521  |
| <input type="checkbox"/> ☆ MySQL_2003_1_2_3_4_10                 | 自发现资产组 | MySQL 5.0       | [2003:1:2:3:4::10]:3306  |
| <input type="checkbox"/> ☆ DB2_2003_1_2_3_4_10                   | 自发现资产组 | DB2 v95         | [2003:1:2:3:4::10]:50000 |
| <input type="checkbox"/> ☆ sqlserver_192.168.128.34              | 缺失资产组  | SQL Server 2003 | 192.168.128.34:1433      |
| <input type="checkbox"/> ☆ Oracle_17.2.0.1                       | 自发现资产组 | Oracle 11g      | 17.2.0.1:1521            |
| <input type="checkbox"/> ☆ DB2_17.2.0.1                          | 自发现资产组 | DB2 v95         | 17.2.0.1:50000           |
| <input type="checkbox"/> ☆ PostgreSQL_17.2.0.1                   | 自发现资产组 | PostgreSQL 11   | 17.2.0.1:5432            |

共 13 条

1 2 > 10 条/页

2 确定 取消

### 7.1.3 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>。

#### 安全规则

规则管理 白名单管理 设置

新增 规则名称 请输入查询关键字

推荐 仅显示特征规则

| 名称  | 等级  | 资产数量 | 白名单数量 | 操作       |
|---|-----|------|-------|----------|
| <input checked="" type="checkbox"/> + test                    | 中风险 | 2    | 0     | 编辑 克隆 删除 |
| <input checked="" type="checkbox"/> + MySQL_安全漏洞CVE-2018-2696 | 高风险 | 0    | 0     | 编辑       |
| <input type="checkbox"/> + SQLServer_创建程序集                    | 中风险 | 0    | 0     | 编辑 克隆    |
| <input type="checkbox"/> + DM_SP_DEL_BAK_EXPIRED过程内存破坏漏洞      | 中风险 | 0    | 0     | 编辑       |
| <input type="checkbox"/> + MySQL_使用DUMPFIL导出                  | 高风险 | 0    | 0     | 编辑 克隆    |
| <input type="checkbox"/> + MySQL_注入恶意配置提升权限漏洞                 | 高风险 | 0    | 0     | 编辑       |
| <input type="checkbox"/> + MySQL_udf权限提升漏洞                    | 中风险 | 0    | 0     | 编辑       |

2

启用选中项  禁用选中项 删除

共 275 条 < 1 2 3 4 5 ... 14 > 20 条/页 跳至 页

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。

## 7.1.4 白名单管理

符合规则白名单中条件的审计记录，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。

### 安全规则



| <input type="checkbox"/> | 名称       | 启用该白名单的规则   | 描述 | 操作      |
|--------------------------|----------|---|----|---------|
| <input type="checkbox"/> | test白名单1 | test x MySQL_注入恶意配置提升权限漏洞 x<br>MySQL_指定特质几何功能拒绝服务漏洞 x |    | 编辑   删除 |
| <input type="checkbox"/> | test白名单2 | test x MySQL_注入恶意配置提升权限漏洞 x<br>MySQL_指定特质几何功能拒绝服务漏洞 x |    | 编辑   删除 |
| <input type="checkbox"/> | test白名单3 | test x  |    | 编辑   删除 |

共 3 条 < 1 > 20 条/页 跳至 页

步骤 2. 点击<新增>，进入新增白名单页面，编辑相关参数（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>。

新增白名单
✕

**基本信息**

\* 名称:

描述:

**客户端**

客户端来源:  IP  IP组

等于  ✕

可配多个IP, 使用逗号","分隔, 例: 192.168.1.2,192.168.1.3

客户端工具: 等于

可配多个客户端工具, 使用逗号","分隔, 例: db2bp.exe,javaw.exe,PLSqlDev.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: 10-15,20,25,30-40

客户端MAC地址: 等于

可填多值, 多个值间以逗号","分隔, 例: fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf

操作系统用户名: 等于

可填多值, 多个值间以逗号","分隔, 例: xxx,yyy

主机名: 等于

保存
取消

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。

## 安全规则

| 规则管理 |                                 | 白名单管理    | 设置   |       |  |
|------|---------------------------------|----------|--|-------|--|
| 新增   | 规则名称 ▾                          | 请输入查询关键字 | <span style="background-color: #007bff; color: white; padding: 2px 5px;">推荐</span> <span style="padding: 2px 5px; margin-left: 5px;">仅显示特征规则</span> <span style="font-size: 1em; padding: 2px 5px;">⊞</span> |       |  |
| ☐    | 名称                              | 等级       | 资产数量   | 白名单数量 | 操作   |
| ☐    | + test                          | 中风险      | 2  | 3     | <a href="#">编辑</a>   <a href="#">克隆</a>   <a href="#">删除</a> |
| ☐    | + MySQL_安全漏洞CVE-2018-2696       | 高风险      | 0  | 0     | <a href="#">编辑</a>   |
| ☐    | + SQLServer_创建程序集               | 中风险      | 0  | 0     | <a href="#">编辑</a>   <a href="#">克隆</a>                      |
| ☐    | + DM_SP_DEL_BAK_EXPIRED过程内存破坏漏洞 | 中风险      | 0  | 0     | <a href="#">编辑</a>   |

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。

设置规则(test)的白名单 X

---

| 名称/描述    | 请输入查询关键字 | Q                                      | ⊞ | C | ∨ |
|----------|----------|--|---|---|---|
| 名称       | 描述       | 状态                                     |   |   |   |
| test白名单1 |          | 启用 <input checked="" type="checkbox"/> |   |   |   |
| test白名单2 |          | 启用 <input checked="" type="checkbox"/> |   |   |   |
| test白名单3 |          | 启用 <input checked="" type="checkbox"/> |   |   |   |

共 3 条  < 1 > 20 条/页 ∨ 跳至  页



需要将启用白名单的所有规则禁用白名单后才能删除该白名单。

## 7.1.5 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，可以匹配每个行为触发的所有规则。

### 安全规则

规则管理
白名单管理
设置

**规则优先级** 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

如需检测出每个行为的全部风险，请禁用规则优先级

状态： 开启

## 7.2 信任规则

当系统匹配信任规则时，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。

## 信任规则

| 名称                              | 资产数量 | 操作  |
|---------------------------------|------|---|
| <input type="checkbox"/> + 回归测试 | 0    | <input type="button" value="编辑"/> <input type="button" value="删除"/> |

启用全部
 

共 1 条 < 1 > 20 条/页 跳至  页

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>。

新增规则
✕

**基本信息**

\* 名称:

描述:

**客户端**

**服务端**

服务端IP:

可配多个IP, 使用逗号","分隔, 支持末尾两位为\*。例: 192.168.1.2,192.168.1.3

服务端端口:

可配置多个值或区间, 多个值间以逗号","分隔, 例: 10-15,20,25,30-40

数据库账号:  字符串  正则表达式  分组选择

字符串 可填多值, 多个值间以逗号","分隔, 例: xxx,yyy

服务端MAC地址:

可填多值, 多个值间以逗号","分隔, 例: fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf

数据库名(SID):  字符串  正则表达式

详细配置请参见[规则管理](#)。

## 7.3 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信任的操作, 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。

过滤规则的过滤条件有三种, 分别是按 IP 过滤、按 SQL 模板过滤和按规则过滤。

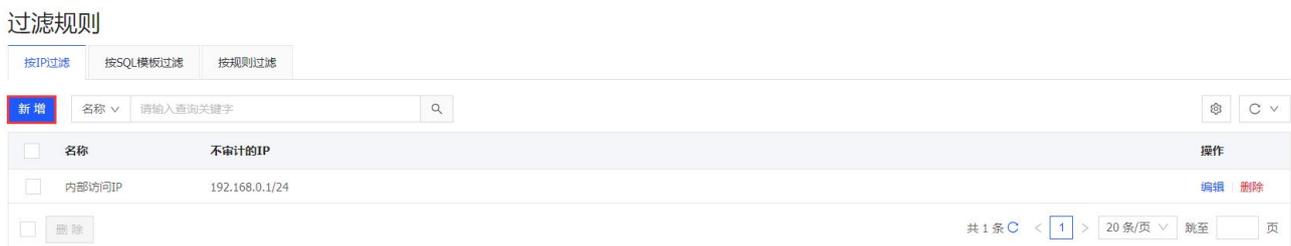
◆ 按 IP 过滤是设置某些 IP 地址为信任的 IP 地址, 系统对这些 IP 地址发起的 SQL 请求不审计。

- ◆ 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。

### 7.3.1 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 默认对全部资产有效。即添加后，全部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。

## 7.3.2 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>。

### 过滤规则



| 报文模板  | 数据库类型  | 针对数据库 | 是否内置模板 | 是否启用 | 操作   |
|---|--------|-------|--------|------|------|
| <input checked="" type="checkbox"/> SELECT PRIVILEGE FROM SYS.SESSION_PRI...  | Oracle | 所有数据库 | 是      | 禁用   | 查看模板 |
| <input checked="" type="checkbox"/> SELECT LENGTH(CHR( :1 )) L4, LENGTH(CH... | Oracle | 所有数据库 | 是      | 禁用   | 查看模板 |
| <input checked="" type="checkbox"/> SELECT BANNER FROM V\$VERSION             | Oracle | 所有数据库 | 是      | 禁用   | 查看模板 |
| <input type="checkbox"/> SELECT * FROM V\$VERSION                             | Oracle | 所有数据库 | 是      | 禁用   | 查看模板 |
| <input type="checkbox"/> SELECT GRANTEE, NAME FROM SYS.PLSQLD...              | Oracle | 所有数据库 | 是      | 禁用   | 查看模板 |
| <input type="checkbox"/> SELECT STATE AS `Status`, ROUND(SUM(D...             | MySQL  | 所有数据库 | 是      | 禁用   | 查看模板 |
| <input type="checkbox"/> SELECT QUERY_ID, SUM(DURATION) AS SU...              | MySQL  | 所有数据库 | 是      | 禁用   | 查看模板 |

共 78 条 < 1 2 3 4 > 20 条/页 跳至 页

启用选中项 禁用选中项 删除

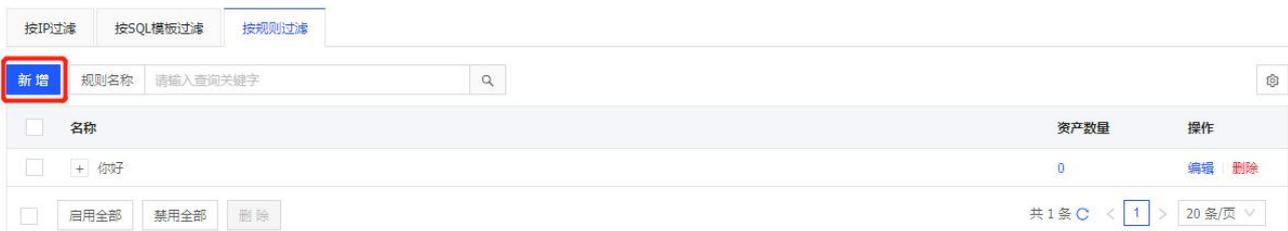
步骤 2. 在弹出的对话框中点击<确定>。

## 7.3.3 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再被审计。

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](#)。

### 过滤规则



新增 规则名称 请输入查询关键字

| 名称                            | 资产数量 | 操作    |
|-------------------------------|------|-------|
| <input type="checkbox"/> + 你好 | 0    | 编辑 删除 |

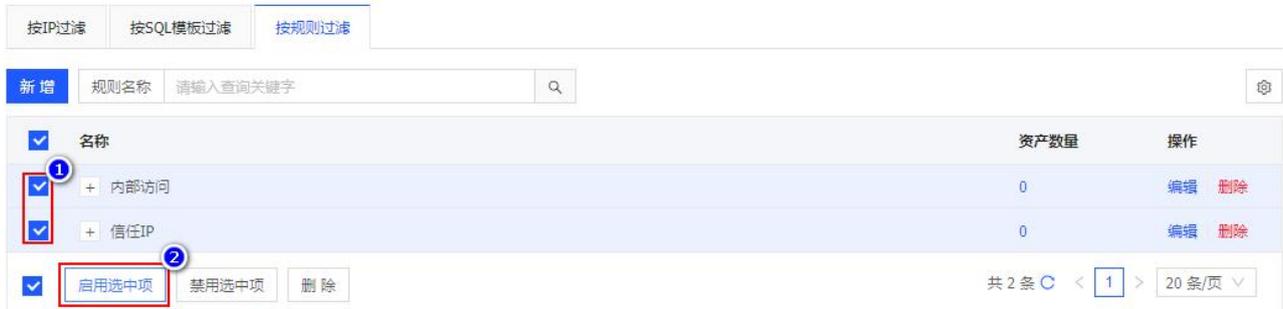
启用全部 禁用全部 删除

共 1 条 < 1 > 20 条/页

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**>。

### 过滤规则



| 名称     | 资产数量 | 操作    |
|--------|------|-------|
| + 内部访问 | 0    | 编辑 删除 |
| + 信任IP | 0    | 编辑 删除 |

共 2 条 < 1 > 20 条/页

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



| 名称                           | 资产组    | 类型              | IP端口                     |
|------------------------------|--------|-----------------|--------------------------|
| ☆ DB2_192.168.50.84          | 自发现资产组 | DB2 v95         | 192.168.50.84:50000      |
| ☆ SQLServer_2003_1_2_3_4_10  | 自发现资产组 | SQL Server 2... | [2003:1:2:3:4::10]:1433  |
| ☆ PostgreSQL_2003_1_2_3_4_10 | 自发现资产组 | PostgreSQL 11   | [2003:1:2:3:4::10]:5432  |
| ☆ Oracle_2003_1_2_3_4_10     | 自发现资产组 | Oracle 11g      | [2003:1:2:3:4::10]:1521  |
| ☆ MySQL_2003_1_2_3_4_10      | 自发现资产组 | MySQL 5.0       | [2003:1:2:3:4::10]:3306  |
| ☆ DB2_2003_1_2_3_4_10        | 自发现资产组 | DB2 v95         | [2003:1:2:3:4::10]:50000 |
| ☆ sqlserver_192.168.128.34   | 缺货资产组  | SQL Server 2... | 192.168.128.34:1433      |
| ☆ Oracle_17.2.0.1            | 自发现资产组 | Oracle 11g      | 17.2.0.1:1521            |
| ☆ DB2_17.2.0.1               | 自发现资产组 | DB2 v95         | 17.2.0.1:50000           |
| ☆ PostgreSQL_17.2.0.1        | 自发现资产组 | PostgreSQL 11   | 17.2.0.1:5432            |

共 13 条 < 1 2 > 10 条/页

## 7.4 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。

## 规则维护

升级与备份

**内置规则升级** 包括安全规则和SQL模板过滤

当前版本: V1.0\_20210531.1

上传升级包

**自定义规则导入导出**

导出的规则包括: 自定义的安全规则, 信任规则和过滤规则

导出规则
导入规则

## 7.5 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。

### 7.5.1 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。

#### 关联数据

|  | IP组   | 数据库账号组 | 应用用户组         | 时间组           | 对象组        | 人员  |
|--|---|--------|---------------|---------------|------------|---|
| <span style="border: 2px solid red; padding: 2px;">新增</span> | 导入  | 导出     | 下载模板          | 名称 ▾          | 请输入查询关键字   | Q   |
|  | 创建时间  | 名称     | IP            |               | 备注         | 操作  |
| <input type="checkbox"/>                                     | 2021-05-24 17:18:50   | 医院内网   | 200.200.200.* | 200.200.201.* | 而法国然后有人... | <span style="color: #007bff;">编辑</span> <span style="color: #dc3545;">删除</span> |
| <input type="checkbox"/>                                     | <span style="border: 1px solid #ccc; padding: 2px 5px;">删除</span> |        |               |               |            | 共 1 条 <span style="font-size: 0.8em;">C</span> < 1 > 20 条/页 ▾                   |

#### 7.5.1.1 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>。

\* 名称:

\* IP:

示例:  
 10.10.1.1,10.10.1.2  
 10.1.1.10-10.1.1.20  
 10.10.\*.\*  
 10.10.1.\*

备注:

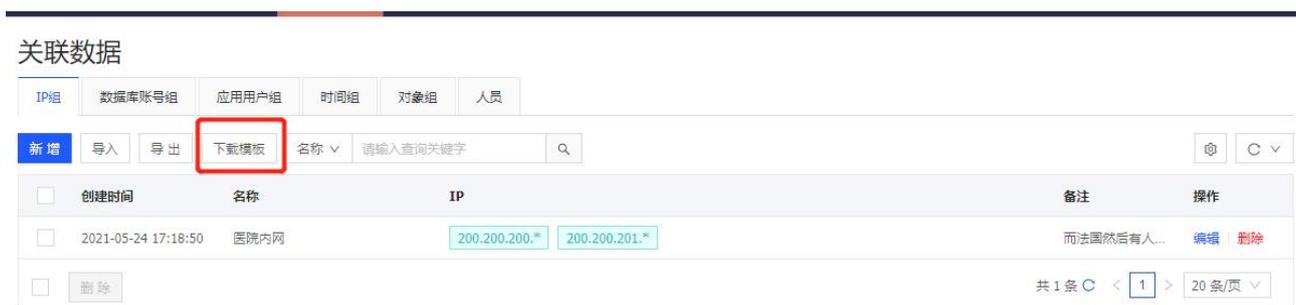
详细配置请参见下表。

| 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  | <ul style="list-style-type: none"> <li>◆ 可输入多个IP地址，用英文逗号隔开。</li> <li>◆ 可输入地址范围，例如：10.1.1.10-10.1.1.20。</li> <li>◆ 可输入地址段，例如：10.10.*.*，“*”表示0~255。</li> </ul> |

### 7.5.1.2 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。

## 关联数据

| IP组                 | 数据库账号组 | 应用用户组         | 时间组          | 对象组 | 人员       |
|---------------------|--------|---------------|--------------|-----|----------|
| 新增                  | 导入     | 导出            | 下载模板         | 名称  | 请输入查询关键字 |
| 创建时间                | 名称     | IP            | 备注           | 操作  |          |
| 2021-11-16 16:29:05 | 数据字典   | 192.168.1.193 | 配置SQL类型翻译... | 编辑  | 删除       |

## 7.5.2 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。

### 关联数据

| IP组                 | 数据库账号组 | 应用用户组 | 时间组   | 对象组 | 人员       |
|---------------------|--------|-------|-------|-----|----------|
| 新增                  | 导入     | 导出    | 下载模板  | 名称  | 请输入查询关键字 |
| 创建时间                | 名称     | 数据库账号 | 操作    |     |          |
| 2021-06-22 17:54:15 | 测试     | admin | 编辑    | 删除  |          |
| 删除                  |        |       | 共 1 条 | 1   | 20 条/页   |

### 7.5.2.1 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，选择数据库账号组页签，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>。

新增数据库账号 ×

---

\* 名称:

\* 数据库账号:

多个数据库账号使用“,”隔开,例如"user1,user2"

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。                               |

## 7.5.2.2 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。

## 7.5.3 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。

关联数据



### 7.5.3.1 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>。



### 7.5.3.2 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。

## 7.5.4 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。

关联数据



### 7.5.4.1 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>。

新增时间组
X

---

\* 名称:

时间范围:  每天  每周  每月

每周的周几? (工作日 非工作日)

周一 周二 周三 周四 周五 周六 周日

每天的几点? (工作时间 非工作时间)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

## 7.5.4.2 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。

## 7.5.5 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。

关联数据

| 对象组名称                                       | 规则数量 | 对象数量 | 操作                                    |
|---|------|------|---------------------------------------|
| <input type="checkbox"/> test               | 0    | 1    | <a href="#">编辑</a> <a href="#">删除</a> |
| <input type="checkbox"/> <a href="#">删除</a> |      |      |                                       |

共 1 条 < 1 > 20 条/页 跳至 页

### 7.5.5.1 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>。

新增对象组 ×

---

\* 对象组名称:  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>。

\* 对象组名称: 测试

已配置对象 (标记的对象属于本对象组) 移出选中项

- 资产: 重点医院
- Schema/数据库: dfvswse
  - 表: wedweq

添加对象

资产 所有资产通用

数据库/Schema 所有数据库/Schema通用

表 所有表、视图、函数等通用

字段 请输入字段或索引名称

添加对象
重置

[填写说明]  
为空表示所有

[名词解释]  
schema: 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。

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）的值进行排序的结构。  |

### 7.5.5.2 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。

## 7.5.6 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。

关联数据

IP组 数据库账号组 应用用户组 时间组 对象组 人员

新增 导入 导出 下载模板 工号 请输入查询关键字

| <input type="checkbox"/> | 应用用户名         | IP地址        | 工号  | 姓名 | 手机         | 科室  | 房间      | 主机名      | Mac地址 | 操作    |
|--------------------------|---------------|-------------|-----|----|------------|-----|---------|----------|-------|-------|
| <input type="checkbox"/> | 001,张三,zha... | 192.168.0.1 | 001 | 张三 | 1888888... | 住院部 | 测试房间001 | hostname |       | 编辑 删除 |

删除

共 1 条 < 1 > 20 条/页 跳至 页

### 7.5.6.1 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>。

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

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.\*

 人员相关信息 

工号:

姓名:

手机:

科室:

房间:

主机名:

Mac地址:

详细配置请参见下表。

| 配置项   | 说明   |
|-------|--|
| 应用用户名 | <ul style="list-style-type: none"> <li>◆ 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。</li> <li>◆ 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。</li> </ul> |
| 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：<br>10.10.1.1,10.10.1.2,10.1.1.10-10.1.1.20,10.10.*.*,10.10.1.*<br>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。   |
| 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。  |

| 配置项    | 说明                 |
|--------|--------------------|
| Mac 地址 | 人员所对应资产的物理 Mac 地址。 |

### 7.5.6.2 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。

## 8 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。

### 8.1 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。

#### 8.1.1 角色管理

角色可以看做是具有相同权限的用户的集合。系统将权限分配给角色，然后为用户指定角色。配置用户时通过设定用户所属角色，限制用户的操作权限范围。

用户的操作权限包括菜单显示和功能权限。只有赋予操作权限，用户才能进行相应的操作。

创建角色的操作方法如下：

步骤 1. 在菜单栏选择“系统管理>用户管理”，选择角色管理页签进入角色管理页面。



步骤 2. 点击<添加>进入新增角色页面，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），选择权限，点击<保存>。



The 'Add Role' form contains the following fields and buttons:

- Name: test
- Permissions: Total View, Asset Management
- Note: (empty)
- Buttons: Save, Cancel

## 8.1.2 用户管理

添加角色后即可增加该角色的用户。

系统内置了以下四个默认用户：

- ◆ admin：超级管理员，具备系统所有权限。系统只有一个超级管理员。
- ◆ security：具备安全管理员权限，可配置数据库与规则、查看各类告警报告、管理安全员。
- ◆ system：具备系统管理员权限，进行系统权限的配置和维护。
- ◆ audit：具备审计管理员权限，查看其他用户的操作日志、管理审计员。

添加用户的操作方法如下：

步骤 1. 在菜单栏选择“系统管理>用户管理”进入用户管理页面，点击<添加用户>。

用户管理

| 用户名          | 状态                                    | 角色    | 认证方式 | 备注                      | 操作                                    |
|--------------|---------------------------------------|-------|------|-------------------------|---------------------------------------|
| zhanxiaolong | <span style="color: green;">启用</span> | 系统管理员 | 密码登录 | 系统管理                    | <a href="#">编辑</a> <a href="#">删除</a> |
| admin        | <span style="color: green;">启用</span> | 超级管理员 | 密码登录 | 超级管理员，拥有系统所有权限。         | <a href="#">编辑</a>                    |
| security     | <span style="color: green;">启用</span> | 安全管理员 | 密码登录 | 配置数据库与规则、查看各类告警数据。      | <a href="#">编辑</a>                    |
| system       | <span style="color: green;">启用</span> | 系统管理员 | 密码登录 | 系统的配置和维护。               | <a href="#">编辑</a>                    |
| audit        | <span style="color: green;">启用</span> | 审计管理员 | 密码登录 | 查看“系统管理员”和“安全管理员”的操作日志。 | <a href="#">编辑</a>                    |

共 5 条 < 1 > 20 条/页

步骤 2. 进入添加用户页面，编辑相关信息，点击<保存>。

添加用户

\* 用户名: test\_1

启用:

\* 角色: 安全员 拥有查看审计日志、告警日志和会话日志的权限

\* 密码: .....

\* 确认密码: .....

手机号: 手机号

邮箱: 邮箱

备注:

登录选项

\* 认证方式:  密码登录  密码+动态令牌登录

登录IP/MAC限制:  不限制IP/MAC  黑名单模式  白名单模式

登录时间限制:  不限制时间  限制时间

[保存](#) [取消](#)

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 <b>启用</b> 后的开关，设置添加用户后是否立即启用用户。   |
| 角色           | 指定用户角色，包括内置角色和用户自定义角色，必填。有关角色设置的更多信息，请参考 <a href="#">角色管理</a> 。              |
| 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 <a href="#">动态令牌管理</a> 。 |
| 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。   |

### 8.1.3 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>。

新增授权规则 X

---

\* 名称:

状态:  启用  禁用

\* 用户:

\* 资产:

备注:

## 8.1.4 远程认证

系统支持 LDAP 远程认证，通过对接 LDAP 服务器对 LDAP 用户进行认证，实现更安全可靠的用户管理。

LDAP 是轻量目录访问协议（Lightweight Directory Access Protocol）的缩写，是互联网上目录服务的通用访问协议。LDAP 服务可以有效解决众多网络服务的用户账户问题，LDAP 服务器是用于查询和更新 LDAP 目录的服务器，包括用户账号目录。

配置 LDAP 认证的操作方法如下：

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**远程认证**页签进入**LDAP 认证配置**页面。

**用户管理**

---

**LDAP认证配置**

状态: 未启用  
 端口: 389  
 SSL: 否  
 过滤串: (&(objectClass=user))  
 用户属性名: sAMAccountName

步骤 2. 点击<**修改 LDAP 配置**>，在弹出的**修改 LDAP 认证配置**对话框中编辑相关信息，点击<**确定**>。

状态:  启用

\* 服务器地址:

\* 端口:

SSL:  否

\* Base DN:   
导入用户时, 只能添加在Base DN下面的账号

\* 绑定 DN:   
连接LDAP服务器时使用的账号

\* 密码:    
绑定DN对应的密码

过滤串:   
导入用户时, 只能添加符合过滤串的账号, 如: (&(objectClass=user))

\* 用户属性名:   
填写远程服务器上表示用户名的属性名, 如: name, cn或sAMAccountName

邮箱属性名:   
填写远程服务器上表示邮箱的属性名, 如: mail

手机号属性名:   
填写远程服务器上表示手机号的属性名, 如: mobile

详细配置项和说明请参见下表。

| 配置项                            | 说明   |
|--------------------------------|--|
| 状态                             | 点击 <b>状态</b> 开关至“启用”，允许数据库审计连接第三方 LDAP 服务器进行用户认证。                        |
| 服务器地址                          | 设置 LDAP 服务器地址，可为 IP 或者域名。  |
| 端口                             | 设置 LDAP 服务器的端口，默认 389。   |
| SSL                            | 是否启用 SSL 协议，启用 SSL 协议可增强认证的安全性。  |
| Base DN                        | 指定 LDAP 服务器的 base DN（Distinguished Name，区分名），即导入用户时，只能添加在 Base DN 下面的账号。 |
| 绑定 DN                          | 绑定 LDAP 服务器的 Base DN 下的一个账户，与 LDAP 服务端设置保持一致。                            |
| 密码                             | 输入绑定 DN 的密码。   |
| 过滤串                            | 从 LDAP 服务器导入用户时，只添加符合过滤串的账号，如：(&(objectClass=user))。                     |
| 用户属性名<br>/邮箱属性<br>名/手机号<br>属性名 | 填写远程服务器上表示用户、邮箱、手机号的属性名。   |

步骤 3. 修改 LDAP 配置完成后点击<测试连接>, 确认系统与 LDAP 服务器连接成功。点击<添加 LDAP 用户>, 点击<点此重新获取>自动获取用户, 选择 LDAP 用户, 设置用户角色, 点击<确定>。

添加LDAP用户 ×

\* LDAP用户:

未获取到LDAP用户或LDAP用户发生变更, [点此重新获取](#)

角色:



修改 LDAP 配置完成后, 系统会提示 “是否立即从 LDAP 服务器获取用户”, 建议选择<是>。

步骤 4. 切换到系统登录页面, 使用 LDAP 方式登录系统。



### 8.1.5 动态令牌管理

动态令牌硬件如下图所示。



根据动态令牌硬件背面的序列号向产品服务人员获取动态令牌导入文件, 动态令牌导入文件为 XML 文件。

使用动态令牌登录系统的操作方法如下：

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，选择动态令牌管理页签，点击<导入>。

### 用户管理



用户管理

用户管理 远程认证 角色管理 用户安全配置 **动态令牌管理** 授权数据库

导入 序列号 请输入查询关键字

| 序列号 | 生产时间                | 失效时间                | 操作 |
|-----|---------------------|---------------------|----|
| 2   | 2017-01-20 17:36:41 | 2022-01-19 09:54:11 | 删除 |

步骤 2. 选择获取到的动态令牌导入文件，上传成功后，动态令牌文件导入后效果如下图所示。

### 用户管理



用户管理

用户管理 远程认证 角色管理 用户安全配置 **动态令牌管理** 授权数据库

导入 序列号 请输入查询关键字

| 序列号 | 生产时间                | 失效时间                | 操作 |
|-----|---------------------|---------------------|----|
|     | 2020-12-07 13:39:47 | 2025-11-24 11:05:44 | 删除 |
|     | 2020-12-07 13:39:47 | 2025-11-24 11:05:44 | 删除 |
|     | 2020-12-07 13:39:47 | 2025-11-24 11:05:44 | 删除 |

共 3 条 < 1 > 20 条/页

步骤 3. 在菜单栏选择“系统管理>用户管理”，选择待绑定的用户 admin，点击<编辑>，选择认证方式为<密码+动态令牌登录>，并选择动态令牌序列号，点击<保存>。



编辑用户

用户名：admin

启用：

角色：超级管理员

密码：[修改密码](#)

手机号：

邮箱：

备注：

登录选项

\* 认证方式： 密码登录  密码+动态令牌登录

\* 动态令牌序列号：

请选择一个动态令牌序列号，可从动态令牌背面查看序列号

登录IP/MAC限制： 不限制IP/MAC  黑名单模式  白名单模式

登录时间限制： 不限制时间  限制时间

步骤 4. 进入系统 Web 管理平台登录页面，选择动态令牌登录方式，输入用户名、密码和动态令牌（动态令牌硬件上显示的数字串），点击<登录>。



The image shows a login interface with two tabs: '密码登录' (Password Login) and '动态令牌登录' (Dynamic Token Login). The 'Dynamic Token Login' tab is selected. Below the tabs are three input fields: '用户名' (Username), '密码' (Password), and '动态令牌' (Dynamic Token). A blue '登录' (Login) button is at the bottom.

## 8.1.6 用户安全配置

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

在菜单栏选择“系统管理>用户管理”进入用户管理页面，选择用户安全配置页签进入用户安全配置页面，编辑相关信息，点击<保存>。



The image shows the '用户管理' (User Management) page with the '用户安全配置' (User Security Configuration) tab selected. The page is divided into three sections: '用户安全设置' (User Security Settings), '用户锁定' (User Locking), and '密码策略' (Password Policy).

- 用户安全设置 (User Security Settings):**
  - 登录超时: 550 分钟 (有效值1-43200, 默认值5. 当用户超过设定时长无操作时, 再次操作需要重新登录. 变更后需重新登录才能生效)
  - 验证码:  启用验证码
- 用户锁定 (User Locking):**
  - 密码尝试次数: 5 次 (有效值0-999, 默认值5. 如果设置为0, 则不锁定帐户)
  - 锁定时长: 30 分钟 (有效值1-10080, 默认值30)
  - 重置计数器: 5 分钟 (有效值1-10080, 默认值5. 登录尝试密码失败之后, 将登录尝试失败计数器重置为0次所需要的时间)
- 密码策略 (Password Policy):**
  - 密码强度:  启用强密码 (8-64个可见字符, 必须包含以下4项: 1.大写字母A-Z; 2.小写字母a-z; 3.数字0-9; 4.非字母符号如@,#,\$.)
  - 密码使用期限: 0 天 (有效值0-999, 默认值0. 如果设置为0, 则密码不过期)

A blue '保存' (Save) button is located at the bottom left of the page.

详细配置项和说明请参见下表。

| 配置项           | 说明  |
|---------------|---|
| <b>用户安全设置</b> |   |
| 登录超时          | 取值范围：1~43200，默认值为 5。当用户超过设置时长未操作时，再次操作需要重新登录系统。                               |
| 验证码           | 设置用户登录系统时是否需要输入验证码。   |
| <b>用户锁定</b>   |   |
| 密码尝试次数        | 取值范围：0~999，默认值为 5，0 表示不锁定账户。当用户输入密码错误次数达到设定值时，系统将锁定此账户。                       |
| 锁定时长          | 取值范围：1~10080，默认值为 30。   |
| 重置计数器         | 取值范围：1~10080，默认值为 5。密码尝试失败（未达到密码尝试次数设置值时），若在设置时间长度内不再尝试输入密码，则系统将密码尝试次数重新设为 0。 |
| <b>密码策略</b>   |   |
| 启用强密码         | 启用强密码后，设置用户密码时必须满足较高的复杂度（8~64 个字符长度，必须包含大写字母、小写字母、数字和特殊字符）。                   |
| 密码使用期限        | 当用户密码使用时间达到设置值时，系统会强制用户修改密码。取值范围：0~999，0 表示密码不会过期。                            |

## 8.2 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 SQL 数据报文。Agent 支持的宿主机的类型如下表所示。

| 操作系统           | 支持版本                         |
|----------------|------------------------------|
| CentOS         | 6.8, 6.9, 7.2, 7.3, 7.4, 7.6 |
| Windows        | 10                           |
| Windows Server | 2008 R2, 2012 R2, 2016       |
| Red Hat        | 6.9, 7.4, 7.5                |

| 操作系统         | 支持版本           |
|--------------|----------------|
| Ubuntu       | 14.04, 16.04   |
| Debian Linux | 8.9, 9.2       |
| SUSE Linux   | 11 SP4, 12 SP2 |
| Open SUSE    | 42.3           |
| Aliyun Linux | 17.1           |
| AIX          | 5.3、6.1、7.1    |

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。

## 8.2.1 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。

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，如下图所示。

### Agent管理

Agent管理
Agent安装

#### SSH远程安装

通过SSH协议将Agent自动安装到您的服务器上，目前仅支持Linux系统

开始安装
安装状态

#### 手动安装Agent

\* Agent将流量发送到:

请根据您的操作系统选择相应的Agent安装包



**Linux系统** 可用于CentOS、Debian、Ubuntu和SUSE等主流发行版操作系统

离线安装: 下载与操作系统位数一致的安装包，拷贝到服务器上，解压后执行 `install.sh` 安装

↓ 64位

在线安装: 以管理员权限执行以下命令安装 [复制命令](#)

```

wget https://10.20.49.70/linux64/dbagent.sh --no-check-certificate -O dbagent.sh && chmod 755 dbagent.sh && ./dbagent.sh 10.20.49.70
                    
```

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>。



通过SSH远程安装Agent

审计服务器IP:  
192.168.30.204

安装Agent的服务器:  表单填写  文本输入

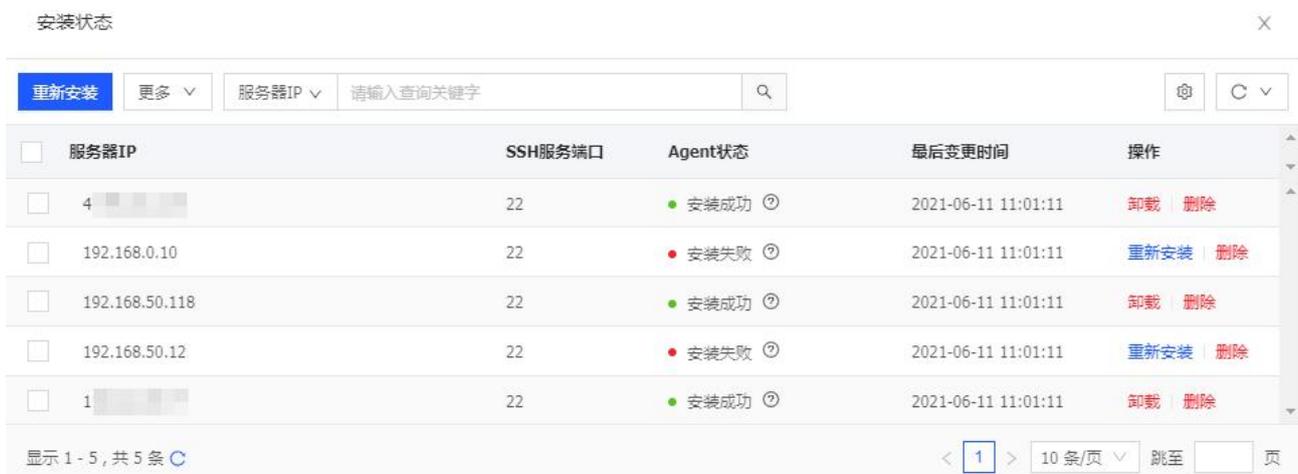
| 服务器IP | root密码 | 端口 |
|-------|--------|----|
|       | root   | 22 |
| + 增加  |        |    |

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 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。



安装状态

| 服务器IP          | SSH服务端口 | Agent状态  | 最后变更时间              | 操作        |
|----------------|---------|----------|---------------------|-----------|
| 4 [模糊]         | 22      | ● 安装成功 ? | 2021-06-11 11:01:11 | 卸载   删除   |
| 192.168.0.10   | 22      | ● 安装失败 ? | 2021-06-11 11:01:11 | 重新安装   删除 |
| 192.168.50.118 | 22      | ● 安装成功 ? | 2021-06-11 11:01:11 | 卸载   删除   |
| 192.168.50.12  | 22      | ● 安装失败 ? | 2021-06-11 11:01:11 | 重新安装   删除 |
| 1 [模糊]         | 22      | ● 安装成功 ? | 2021-06-11 11:01:11 | 卸载   删除   |

显示 1 - 5, 共 5 条

## 8.2.2 手动安装 Agent

### 8.2.2.1 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**”，选择 **Agent 安装** 页签，点击下载对应版本的 Agent 安装包。

手动安装Agent

Agent将流量发送到: Admin (10.20.49.70)

请根据您的操作系统选择相应的Agent安装包



**Linux系统** 可用于CentOS、Debian、Ubuntu和SUSE等主流发行版操作系统

离线安装: 下载与操作系统位数一致的安装包, 拷贝到服务器上, 解压后执行 `install.sh` 安装

[↓ 64位](#)

在线安装: 以管理员权限执行以下命令安装 [复制命令](#)

```
wget https://10.20.49.70/linux64/dbagent.sh --no-check-certificate -O dbagent.sh && chmod 755 dbagent.sh && ./dbagent.sh 10.20.49.70
```



**Windows系统** 可用于Windows Server 2008、Windows 7及以上版本

离线安装: 下载与操作系统位数一致的安装包, 拷贝到服务器上, 解压后双击 `dbAgent-setup.exe` 安装

[↓ 64位](#)

在线安装: 使用浏览器访问以下链接下载安装包 [复制链接](#)

```
https://10.20.49.70/dbagent/dbagent.zip?revIp=10.20.49.70
```



**AIX系统** 可用于IBM的AIX操作系统

离线安装: 下载与AIX版本一致的安装包, 拷贝到服务器上, 解压后执行 `install.sh` 安装

[↓ 5.3](#) [↓ 6.1](#) [↓ 7.1](#)

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，请仔细阅读该文档全部内容并严格按照要求进行操作。

### 8.2.2.2 Linux 操作系统安装 Agent 程序

#### 8.2.2.2.1 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。

```
[root@oracle test_1]# ll
总用量 8276
-rw-r--r-- 1 root root 8472119 6月  2 16:37 dbagent_linux_V2.29.tar.gz
```



- ◆ 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 2. 使用 “tar -xf Agent\_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 3. 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]#
```

### 8.2.2.2.2 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/agent.sh --no-check-certificate -O agent.sh && chmod 755 agent.sh
```

&& ./agent.sh 10.20.49.201

```

[root@oracle dbagent2.201] 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
--2022-06-02 16:55:39-- https://10.20.49.201/linux64/dbagent.sh
正在连接 10.20.49.201:443... 已连接。
警告：无法验证 10.20.49.201 的由 "/C=CN/ST=Zhejiang/L=Hangzhou/O=dbone/OU=dbone/OU=www.dbone.com" 颁发的证书：
  出现了自己签名的证书。
警告：证书通用名 "www.dbone.com" 与所要求的主机名 "10.20.49.201" 不符；
已发出 HTTP 请求，正在等待回应... 200 OK
长度：572 [text/plain]
正在保存至: "dbagent.sh"

100%[=====>] 572  ...K/s 用时 0s

2022-06-02 16:55:39 (123 PB/s) - 已保存 "dbagent.sh" (572/572)

[INFO] uninstall
2022年 06月 02日 星期四 16:55:39 CST
Uninstall dbagent success
delete /root/.bashrc hook
delete /home/oracle/.bashrc hook
delete /home/admin/.bashrc hook
delete /root/.bashrc hook
delete /home/oracle/.bashrc hook
delete /home/admin/.bashrc hook
Stop dbagent success
[INFO] download
--2022-06-02 16:55:39-- https://10.20.49.201/dbagent/dbagent.tar.gz?r=IP10.20.49.201
正在连接 10.20.49.201:443... 已连接。
警告：无法验证 10.20.49.201 的由 "/C=CN/ST=Zhejiang/L=Hangzhou/O=dbone/OU=dbone/OU=www.dbone.com" 颁发的证书：
  出现了自己签名的证书。
警告：证书通用名 "www.dbone.com" 与所要求的主机名 "10.20.49.201" 不符；
已发出 HTTP 请求，正在等待回应... 200 OK
长度：8472116 (8.1M) [application/gzip]
正在保存至: "agent.tar.gz"

100%[=====>] 8,472,116  50.5PB/s 用时 0.2s

2022-06-02 16:55:41 (50.5 PB/s) - 已保存 "agent.tar.gz" (8472116/8472116)

[INFO] install
2022年 06月 02日 星期四 16:55:41 CST
Install dbagent...
Install dbagent success
Start dbagent...
Start dbagent success
[INFO] r!nion
  
```

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。



## 8.2.2.3 Windows 操作系统安装 Agent 程序

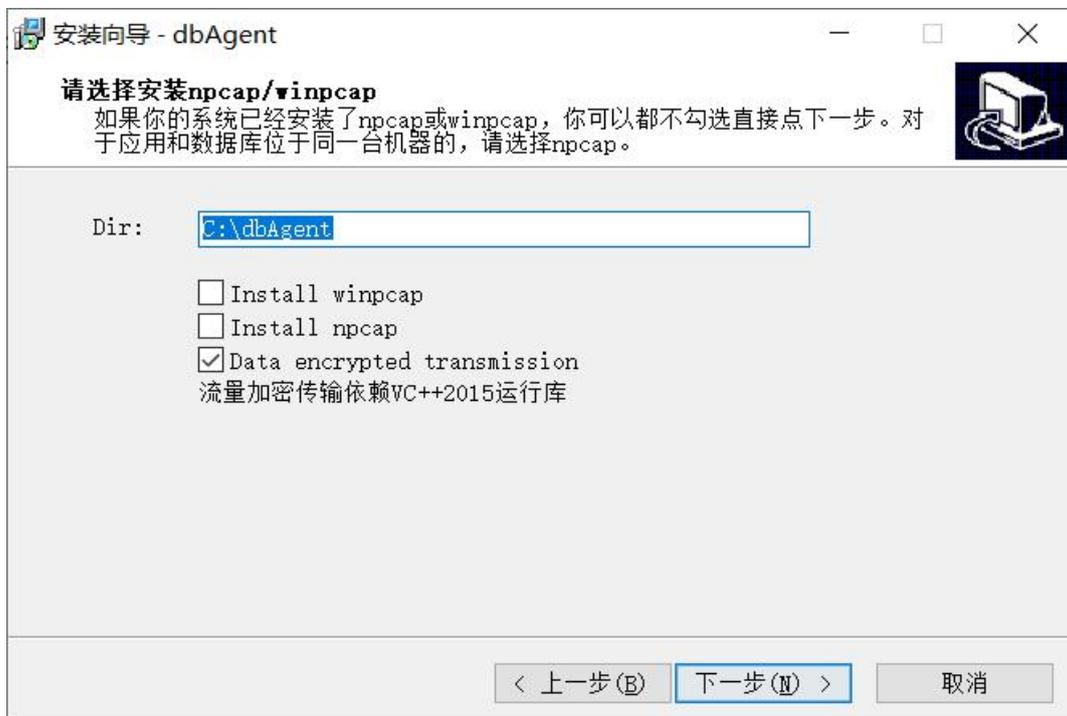
### 8.2.2.3.1 离线安装

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。

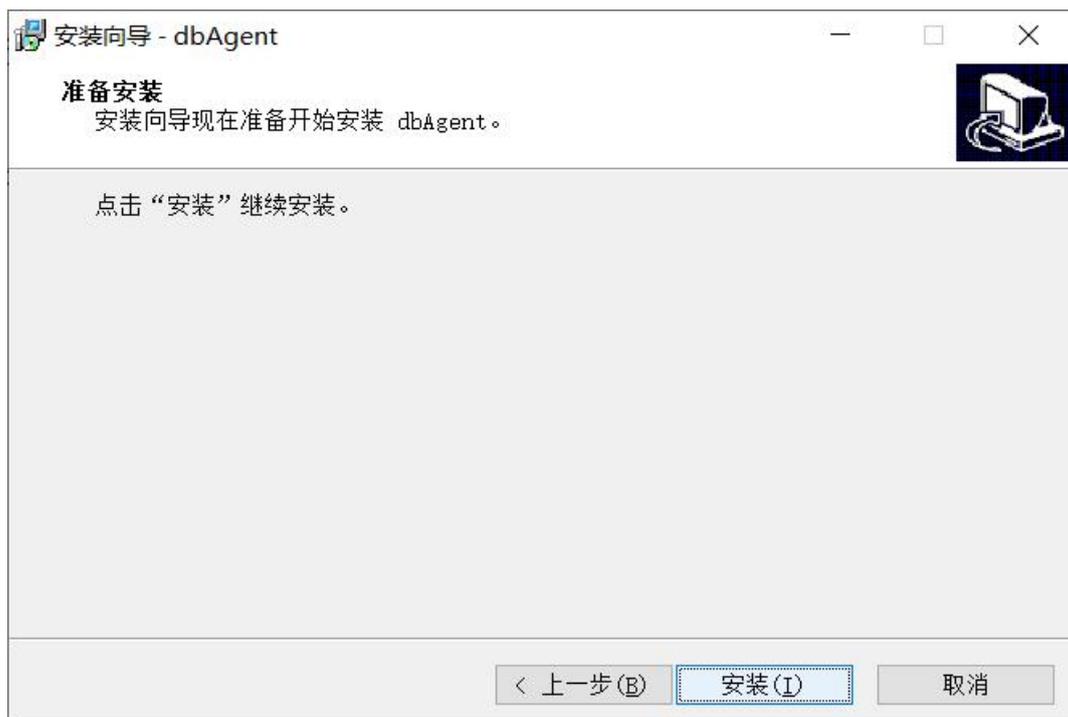
步骤 2. 解压压缩包到指定运行目录。在 Agent 的安装目录以管理员身份运行“Agent-setup.exe”进入安装向导，点击<下一步>，如下图所示。



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>。

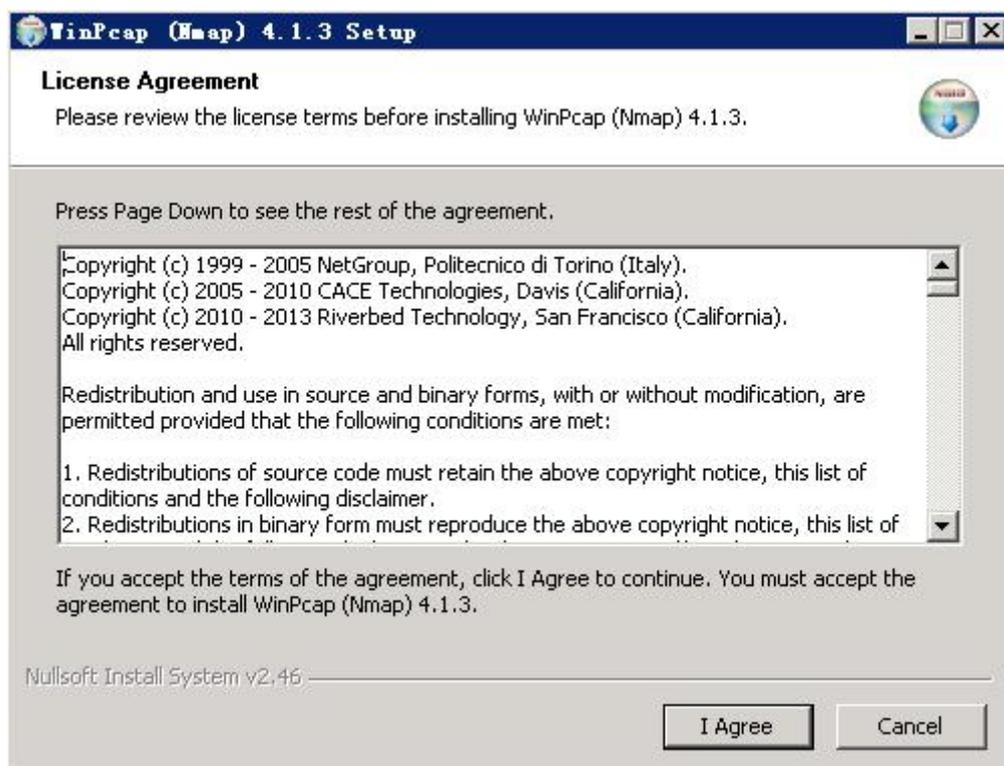


步骤 4. 点击<安装>。

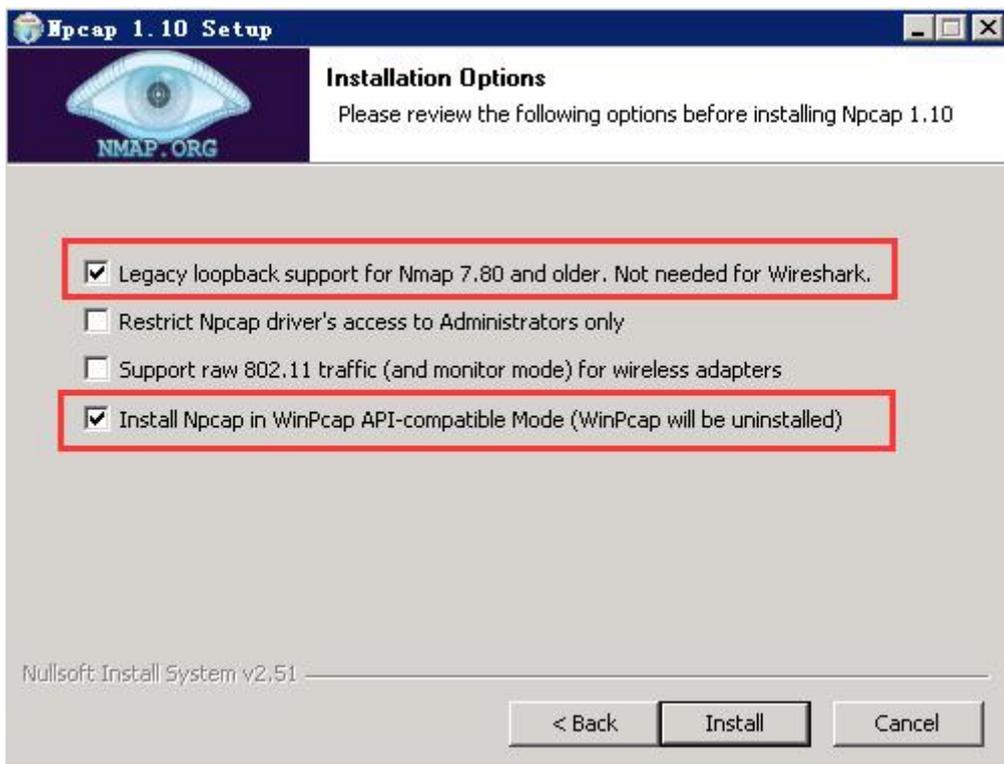
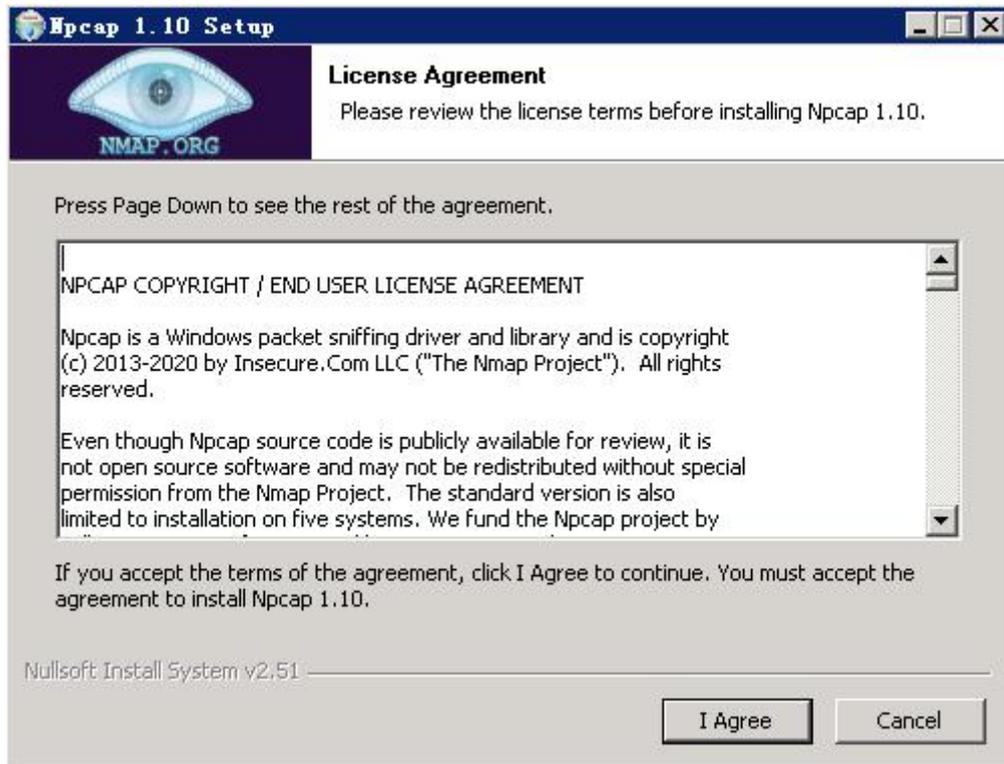


步骤 5. 点击<I Agree>同意安装协议后，之后按照提示进行操作。

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。



### 8.2.2.3.2 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。

### 手动安装Agent

Agent将流量发送到:

请根据您的操作系统选择相应的Agent安装包



**Linux系统** 可用于CentOS、Debian、Ubuntu和SUSE等主流发行版操作系统

离线安装: 下载与操作系统位数一致的安装包, 拷贝到服务器上, 解压后执行 `install.sh` 安装

[↓ 64位](#)

在线安装: 以管理员权限执行以下命令安装 [复制命令](#)

```
wget https://192.168.30.204/linux64/dbagent.sh --no-check-certificate -O dbagent.sh && chmod 755 dbagent.sh && ./dbagent.sh 192.168.30.204
```



**Windows系统** 可用于Windows Server 2008、Windows 7及以上版本

离线安装: 下载与操作系统位数一致的安装包, 拷贝到服务器上, 解压后双击 `dbAgent-setup.exe` 安装

[↓ 64位](#)

在线安装: 使用浏览器访问以下链接下载安装包 [复制链接](#)

```
https://192.168.30.204/dbagent/dbagent.zip?revIp=192.168.30.204
```

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>()[]{}^=;!+',~(&()`, 若必要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 Monitor 进程, 然后结束 Agent 进程。



## 8.2.2.4 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 agent\_aix5.3\_V2.257.tar.gz” 命令解压 Agent 安装包，生成 tar 包，再使用 “tar -xvf agent\_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。

## 8.2.3 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，并提供下载当前 Agent 的近期日志和 Agent 运行状态诊断功能。

### Agent管理

当前系统内置Agent版本为: V2.28 **更新** 注意: V2.26及之后的版本才能从页面启动; V2.27及之后的版本才能从页面升级和回退

Agent IP 请输入查询关键字

| Agent IP      | 状态   | 版本   | 操作系统    | 最后收包时间              | 转发速率      | Agent的CPU、内存使用      | 配置信息        | 操作              |
|---------------|------|------|---------|---------------------|-----------|---------------------|-------------|-----------------|
| 192.168.30.60 | 连接正常 | 0.0  | Linux   | 2021-11-29 20:43:58 | 0 Mbps    | CPU: 0% 内存:0%       | CPU亲和性:后... | 监控 配置 <b>更多</b> |
| 10.20.49.119  | 连接正常 | 2.28 | Linux   | 2021-11-29 20:43:53 | 0.01 Mbps | CPU: 3.55% 内存:0.68% | CPU亲和性:后... | 监控 配置 <b>挂起</b> |
| 10.11.38.204  | 连接正常 | 2.28 | Windows | 2021-11-29 20:43:00 | 0 Mbps    | CPU: 0.97% 内存:0.46% | CPU亲和性:后... | 监控 配置 <b>停止</b> |

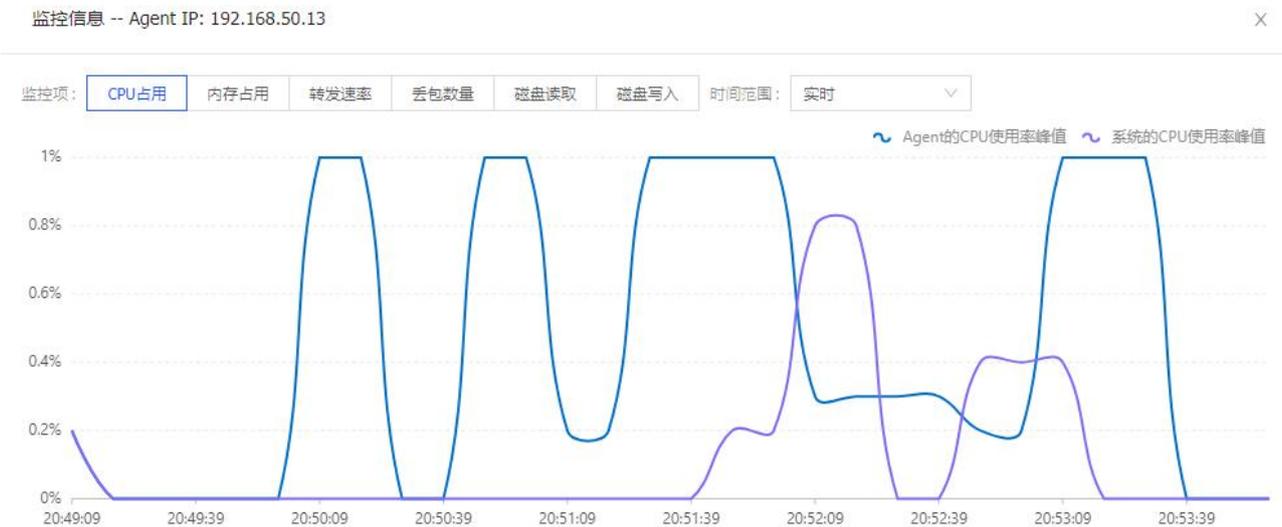
共 3 条 < 1 > 20 条/页 跳至 页

配置 删除 挂起 唤醒 启动 停止 升级 回退

升级 回退 日志 诊断

### 8.2.3.1 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、磁盘读取、磁盘写入）。



### 8.2.3.2 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**>。

## Agent管理

| Agent管理  |          | Agent安装 |                     |        |                      |             |  |
|--|----------|---------|---------------------|--------|----------------------|-------------|--|
| 当前系统内置Agent版本为: V2.28 <a href="#">更新</a> 注意: V2.26及之后的版本才能从页面启动; V2.27及之后的版本才能从页面升级和回退 |          |         |                     |        |                      |             |  |
| Agent IP   | 请输入查询关键字 |         |                     |        |                      |             |  |
| 状态   | 版本       | 操作系统    | 最后收包时间              | 转发速率   | Agent的CPU、内存使用       | 配置信息        | 操作   |
| 异常   | 2.26     | Linux   | 无数据                 | 无数据    | 无数据                  | CPU亲和性;启... | <a href="#">监控</a> <a href="#">配置</a> <a href="#">更多</a> |
| 异常   | 2.27     | Linux   | 无数据                 | 无数据    | 无数据                  | CPU亲和性;启... | <a href="#">监控</a> <a href="#">配置</a> <a href="#">更多</a> |
| 连接正常   | 2.25     | Linux   | 2021-12-05 17:02:42 | 0 Mbps | CPU: 19.14% 内存:0.89% | CPU亲和性;启... | <a href="#">监控</a> <a href="#">配置</a> <a href="#">更多</a> |

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>**。

修改配置 -- Agent IP: 192.168.36.133 ✕

▼ 资源使用限制

CPU亲和性 ⓘ:  启用

CPU使用上限:   
可填0, 填0表示不限制

内存使用上限 ⓘ:   
可配范围: 1~2000M

> 熔断保护 超出以下任一阈值时, Agent暂停工作, 直到所有指标低于阈值

> 抓包与过滤设置

> 本地回环审计配置

> 其他

### ◆ 资源使用限制

▼ 资源使用限制

CPU亲和性 ⓘ:  启用

CPU使用上限:   
可填0, 填0表示不限制

内存使用上限 ⓘ:   
可配范围: 1~2000M

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。<br>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）

▼ 熔断保护 超出以下任一阈值时，Agent暂停工作，直到所有指标低于阈值

系统CPU使用阈值：  
可填0，填0表示不限制

系统内存使用阈值：  
可填0，填0表示不限制

系统磁盘读IO阈值： KB/s  
可填0，填0表示不限制

系统磁盘写IO阈值： KB/s  
可填0，填0表示不限制

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

▼ 抓包与过滤设置

抓包网口:

配置后将只抓去指定网口上的流量，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的流量，填写示例：`(host 192.168.1.100 and port 3306) or (host 192.168.1.101 and port 3306)`。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，填写示例：`JDBC,Navicat Premium.exe`。

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，填写示例：`root,sa`。

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： <code>host 192.168.0.1 and port 3306</code> ）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

▼ 本地回环审计配置

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，填写示例：`( port 3306 ) or ( port 3307 )`。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):

将流量中本地回环的IPv4地址改为设置的值，为空则不替换

回环网口替换IP(v6):

将流量中本地回环的IPv6地址改为设置的值，为空则不替换

远程登录审计:  禁用

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:  禁用

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, PostgreSQL, MySQL, SQL Server 的特定版本。               |

#### ◆ 其他

▼ 其他

调试模式： 禁用  
开启后会记录下更详细的调试日志

数据传输加密： 禁用

CPU异常保护阈值  %  
可填0，填0表示关闭CPU异常保护

内存异常保护阈值  M  
可填0，填0表示关闭内存异常保护

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。                                     |

### 8.2.3.3 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。<br>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。  |

## 8.3 系统配置

### 8.3.1 网络

系统支持网口管理、DNS 配置以及路由管理功能。

#### 8.3.1.1 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>。

## 系统配置

| 网络                  |           |             |      |      |      |                                     |    |        |
|---------------------|-----------|-------------|------|------|------|-------------------------------------|----|--------|
| SNMP 许可证 分布式 流量接收方式 |           |             |      |      |      |                                     |    |        |
| 网口配置 路由管理 DNS配置     |           |             |      |      |      |                                     |    |        |
| 链路状态                | 请选择       |             |      |      |      |                                     | 🔍  | ⚙️ C v |
| 网口名称                | 对应位置      | IPv4地址      | 网口类型 | MTU  | 链路状态 | 是否启用                                | 操作 |        |
| eth0                | GE1       |             | 光口   | 1500 | 🔴 断开 | <input type="checkbox"/>            | 编辑 |        |
| eth1                | SLOT1/GE2 |             | 光口   | 1500 | 🔴 断开 | <input type="checkbox"/>            | 编辑 |        |
| eth2                | SLOT1/GE3 |             | 光口   | 1500 | 🔴 断开 | <input type="checkbox"/>            | 编辑 |        |
| eth3                | SLOT1/GE4 |             | 光口   | 1500 | 🔴 断开 | <input type="checkbox"/>            | 编辑 |        |
| eth4                | SLOT1/GE5 | 10.10.10.10 | 电口   | 1500 | 🟢 正常 | <input checked="" type="checkbox"/> | 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**>。

编辑网口
✕

---

网口名称:

IPv4地址:   
可以为空，为空代表删除此IP地址，不能通过修改前的IP地址访问

子网掩码:   
可以为空，为空代表删除此子网掩码

MTU:   
可以为空，为空系统会设置默认值

配置IPv6:  自动获取  手动配置

如果该网口是管理口，除了修改网口的 IPv4 地址、子网掩码、IPv6 配置信息还可以设置 IPv4 网关。

编辑网口
✕

---

网口名称:

IPv4地址:

子网掩码:

IPv4网关:

MTU:

配置IPv6:  自动获取  手动配置



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）。

## 系统配置

| 系统配置   |           |                |       |        |   |   |                    |
|--------|-----------|----------------|-------|--------|---|---|--------------------|
| 网络     |           | SNMP           | 许可证   | 流量接收方式 |   |   |                    |
| 网口配置   |           | 路由管理           | DNS配置 |        |   |   |                    |
| 链路状态   | 请选择       |                |       |        |   |   |                    |
| 网口名称   | 对应位置      | IPv4地址         | 网口类型  | MTU    | 链路状态                                    | 是否启用  | 操作                 |
| ens160 | Admin     | 192.168.30.156 | 电口    | 1500   | <span style="color: green;">●</span> 正常 | <input type="checkbox"/>  | <a href="#">编辑</a> |
| ens192 | SLOT1/GE1 | 192.168.30.112 | 电口    | 1500   | <span style="color: green;">●</span> 正常 | <input checked="" type="checkbox"/>   | <a href="#">编辑</a> |

共 2 条 < 1 > 20 条/页

### 8.3.1.2 DNS 配置

步骤 1. 在系统配置页面选择网络页签，再选择 DNS 配置页签，点击<修改>。



步骤 2. 在弹出的对话框中设置首选 DNS 服务器的 IP 地址和备选 DNS 服务器的 IP 地址，点击<确定>。

### 修改DNS服务器配置

✕

首选DNS:

备选DNS:

### 8.3.1.3 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>。

## 系统配置

网络 SNMP 许可证 分布式 流量接收方式

网口配置 路由管理 DNS配置

**新增** ⊗ C ▼

| 目的地址        | 子网掩码          | 网关           | 网口名称 | 网口别名      | 操作 |
|-------------|---------------|--------------|------|-----------|----|
| 0.0.0.0     | 0.0.0.0       | 192.168.30.1 | eth8 | Admin     | 删除 |
| 10.10.10.0  | 255.255.255.0 | 0.0.0.0      | eth4 | SLOT1/GE5 | 删除 |
| 169.254.0.0 | 255.255.0.0   | 0.0.0.0      | eth0 | GE1       | 删除 |

步骤 2. 在弹出的对话框中设置路由信息，点击<确定>。

新增路由 X

---

\* 目的地址:

\* 子网掩码:

\* 网关:

跃点数:

\* 网口:  ▼

---

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。                                 |
| 网口        | 路由出接口，为设备上的物理端口。  |

### 8.3.2 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>。

### 系统配置

网络 **SNMP** 许可证 流量接收方式

---

#### SNMP配置

状态: 未启用

**修改**

---

#### 常用节点信息

| OID                      | 名称           | 描述      |
|--------------------------|--------------|---------|
| .1.3.6.1.4.1.2021.4      | memory       | 系统内存信息  |
| .1.3.6.1.2.1.25.2.3      | hrStorage    | 系统磁盘信息  |
| .1.3.6.1.4.1.2021.10.1.3 | laLoad       | 系统CPU负载 |
| .1.3.6.1.4.1.2021.11     | systemStatus | 系统CPU信息 |

步骤 2. 进入修改 SNMP 配置页面，编辑相关信息，点击<确定>。

### 修改SNMP配置

状态:  启用

\* 设备名称:

\* 地理位置:

\* 联系方式:

\* 支持版本:  V1&V2C  V3

传输加密方式:

\* 传输加密密码:

\* 用户名:

\* 密码:

密码加密方式:

**确定** 取消

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。 |

| 配置项       | 说明   |
|-----------|--|
| 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。<br>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。<br>选择信息传输的加密方式，目前支持 DES 与 AES 两种方式：<br><b>DES</b> ：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。<br><b>AES</b> ：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。<br>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。<br>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。<br>当支持版本选择“V3”时，此参数可配。   |

### 8.3.3 许可证

许可证（License）是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。

## 系统配置

|    |      |     |        |
|----|------|-----|--------|
| 网络 | SNMP | 许可证 | 流量接收方式 |
|----|------|-----|--------|

---

许可证信息

客户名称:

许可类型: 内部许可

支持网站/实例个数: 999

使用过期时间: 2021-07-25

维保过期时间: 2021-07-25

支持数据库协议:  Oracle  MySQL  SQL Server  Sybase ASE  DB2  Informix  Oscar  达梦(DM)  Cache  PostgreSQL  Teradata

人大金仓(Kingbase)  GBase  MariaDB  Hana  MongoDB  Redis  GaussDB  Greenplum  K-DB  Sybase IQ

ArangoDB  Neo4j  OrientDB

支持大数据协议:  HBase(protobuf)  HBase(thrift)  Hive  Elasticsearch  Cassandra  HDFS  Impala  LibrA  Graphbase

其他协议:  TELNET  FTP  WEB

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, 请及时致电信息客服热线 400-6059-110 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。

### 8.3.4 分布式部署

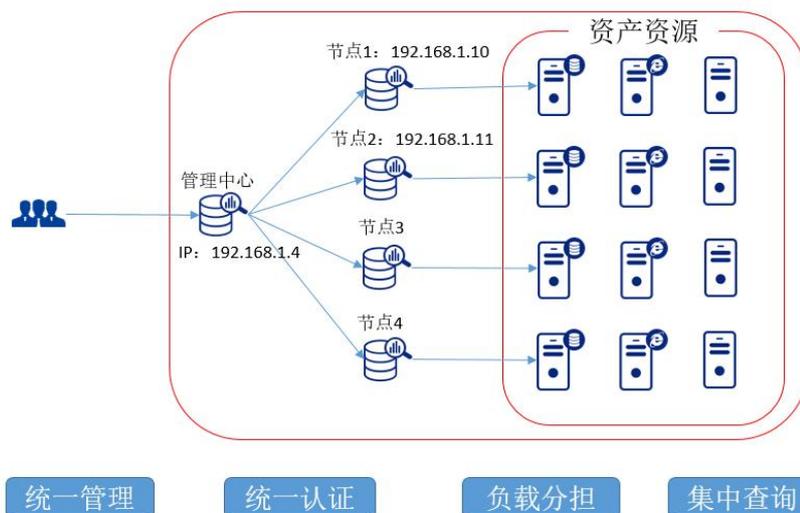
对于有多个分支机构的用户, 需要部署多台设备。采用分布式部署可实现在管理中心节点统一管理所有设备, 方便运维。



- ◆ 需要申请分布式许可才能使用分布式部署功能。
- ◆ 分布式部署的配置均在管理中心节点上进行操作。
- ◆ 分布式场景下, 登录审计节点时会提示“将跳转到管理节点”。
- ◆ 当子节点和管理中心节点网络不通时, 可以将子节点转成单机版本运行。

本文通过以下案例详细说明分布式部署的配置过程。

分布式部署网络拓扑如下图所示。



- ◆ 管理中心和子节点均为单台的数据库审计（硬件版或软件版皆可）。
- ◆ 所有配置（用户、资产、授权等）均在管理中心统一操作，子节点无须任何配置，实现管理中心统一认证、统一管理。
- ◆ 审计日志存储于真实承担审计任务的子节点，管理中心实现统一查询、实时监控。

配置步骤如下：

步骤 1. 配置管理口。



仅软件版需要配置此步骤，硬件版请忽略此步骤。

登录管理中心的 Web 管理平台，在菜单栏选择“**系统管理**”>“**系统配置**”，选择**网络**页签，按“Shift+S”组合键弹出**闪光灯校对网口位置**对话框，选择已配置管理 IP 的网口，设置为“Admin”，点击<保存>即可将该网口设置为管理口。

闪电校对网口位置 X

| 网口名称 | 对应位置  | 动作 |
|------|---|----|
| eth3 | <input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE4 | 闪电 |
| eth4 | <input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE5 | 闪电 |
| eth5 | <input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE6 | 闪电 |
| eth6 | <input type="radio"/> Admin <input checked="" type="radio"/> HA <input type="radio"/> 业务口           | 闪电 |
| eth7 | <input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT1 GE8 | 闪电 |
| eth8 | <input checked="" type="radio"/> Admin <input type="radio"/> HA <input type="radio"/> 业务口           | 闪电 |
| eth9 | <input type="radio"/> Admin <input type="radio"/> HA <input checked="" type="radio"/> 业务口 SLOT2 GE1 | 闪电 |

## 步骤 2. 新建管理中心节点。

- 1) 在菜单栏选择“系统管理>系统配置”，选择分布式页签，点击<转成管理节点>。

### 系统配置

网络 SNMP 许可证 分布式 流量接收方式

节点类型说明：  
 管理节点：具有配置存储、WEB管理、协议审计等全部功能  
 探测器节点：仅具有协议审计的功能，配置由管理节点下发

节点类型  
 设备正处于 单机运行模式，如需部署分布式审计集群，请点击以下按钮转换角色

- 2) 弹出转成管理节点对话框，编辑节点名称，选择节点类型，点击<确定>。

转成管理节点 X

\* 节点名称：  
 建议使用部门或位置命名，方便管理；如：北京总部、研发中心

\* 节点类型：

## 步骤 3. 添加子节点。

- 在菜单栏选择“系统管理>系统配置”，选择分布式页签，点击<添加>。有两种添加方式：直接添加和先安装再添加。



- 直接添加适用于子节点的软件版本与管理中心的软件版本一致的场景。只需要填写子节点名称、节点IP和节点型号。



- 先安装再添加适用于以下场景：子节点的软件版本与管理中心的软件版本不一致或者子节点没有安装数据库审计的主机。需要填写节点名称、节点IP、节点型号、SSH 服务端口、用户名和密码。



- 当子节点的软件版本与管理中心的软件版本不一样时，使用先安装再添加的方式，会重装子节点的数据库审计系统软件。重装会导致清空子节点的业务数据和配置数据。
- 建议先手动将子节点的软件版本升级到管理中心的软件版本，再使用直接添加的方式。

添加分布式节点  添加后不关闭, 继续添加节点 X

添加方式:  直接添加  先安装再添加

\* 节点名称:   
建议使用部门或位置命名, 方便管理; 如: 北京总部、研发中心

\* 节点IP:

\* 节点型号:

\* SSH服务端:   
安装需要通过SSH访问节点, 请填写SSH服务端

\* 用户名:   
建议使用root账号

\* 密码:

详细配置请参见下表。

| 配置项     | 说明   |
|---------|--|
| 节点名称    | 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。 |
| 节点IP    | 节点主机的IP，支持IPv4和IPv6。                       |
| 节点型号    | 建议设置为与管理中心一致即可。                            |
| SSH 服务端 | 设置SSH服务所用的端口，默认为22。                        |
| 用户名     | 节点主机的用户名，建议设置为root。                        |
| 密码      | 节点主机的密码。                                   |

- 2) 点击<确定>, 节点软件版本显示如果为“暂不可用”。等待一段时间后刷新页面, 节点软件版本显示为与管理中心相同的版本号。同时页面上边栏的<同步配置>亮起。

### 系统配置

SNMP 许可证 分布式

节点类型说明:  
 管理节点: 具有配置存储、WEB管理、协议审计等全部功能  
 探测器节点: 仅具有协议审计的功能, 配置由管理节点下发

添加 节点名称

| <input type="checkbox"/> | 节点名称 | 节点IP         | 节点类型  | 节点型号 | 软件版本               | 配置版本 | 审计资产 | 操作             |
|--------------------------|------|--------------|-------|------|--------------------|------|------|----------------|
| <input type="checkbox"/> | 杭州   | 10.20.49.201 | 管理节点  | S25  | 4.0.68.220531.2100 | 977  | 全部资产 | 设置审计资产 转为单机运行  |
| <input type="checkbox"/> | 北京   | 10.20.49.128 | 探测器节点 | S25  | 暂不可用               | 暂不可用 | 全部资产 | 设置审计资产 同步配置 更多 |

同步配置  
共 2 条 < 1 > 20 条/页 跳至  页

- 3) 页面上边栏的<同步配置>亮起, 并且发现新添加的节点的配置版本与管理中心不一致。



- 4) 点击页面上边栏的**<同步配置>**, 页面弹窗显示需要进行同步配置, 点击弹窗中的**<同步配置>**, 下发管理中心的全部配置, 使节点与管理中心配置保持一致。



- 5) 同步配置后, 节点的配置版本号与管理中心的配置版本号一致。



分布式部署配置完成后, 在菜单栏选择**“总览>节点信息”**, 可查看全部节点的当前状态。



### 8.3.5 流量接收方式

- 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>**。

## 系统配置

|    |      |     |     |        |
|----|------|-----|-----|--------|
| 网络 | SNMP | 许可证 | 分布式 | 流量接收方式 |
|----|------|-----|-----|--------|

**流量接收方式** 建议关闭不必要的流量接收方式,可减少资源的浪费

接收镜像流量: 启用  
接收Agent流量: 启用

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**>。

流量接收方式 ×

---

接收镜像流量:  启用  禁用

接收Agent流量:  启用  禁用

确定
取消

## 8.4 系统维护

### 8.4.1 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,点击<**同步浏览器时间**>可将系统时间与浏览器时间同步。

### 系统维护

|    |      |      |      |      |        |        |      |
|----|------|------|------|------|--------|--------|------|
| 时间 | 资源使用 | 软件升级 | 调试工具 | 数据清理 | 数据备份恢复 | 配置备份恢复 | 设备管理 |
|----|------|------|------|------|--------|--------|------|

---

**设备时间**

设备当前时间: 2021-06-21 15:02:59  
浏览器时间: 2021-06-21 15:02:59

同步浏览器时间

---

**时间同步配置**

同步服务器: 10.20.48.30  
自动同步: 已启用

修改
立即同步

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

### 修改时间同步配置



如果设备时间晚于同步服务器时间，同步时间后设备将重启引擎服务

同步服务器: 192.168.1.2

自动同步:  禁用

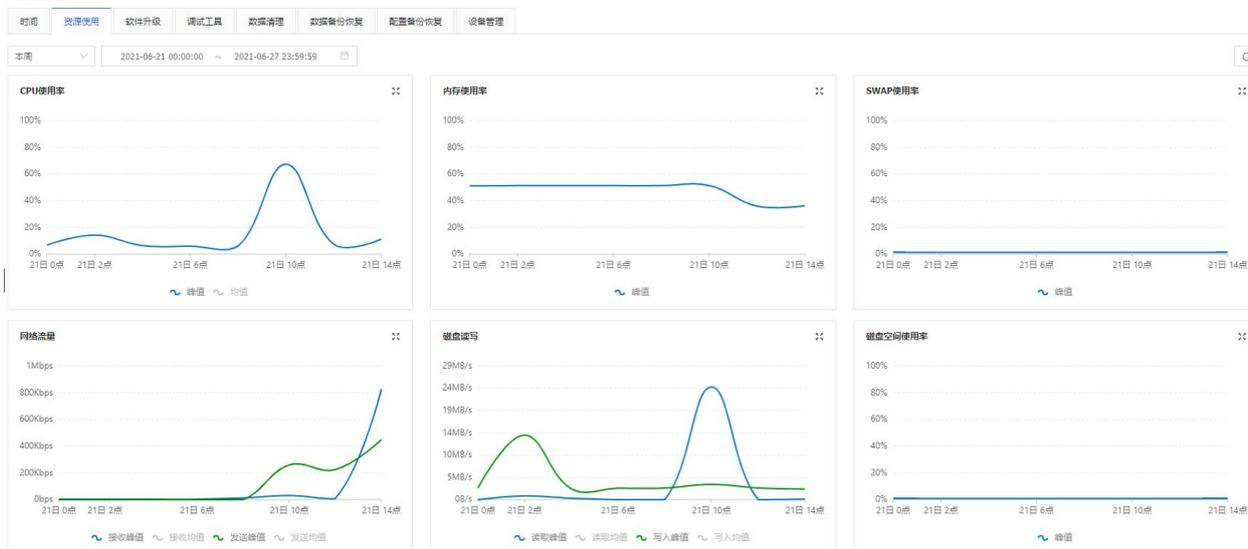
确定

取消

## 8.4.2 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。

### 系统维护



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。

### 系统维护



## 8.4.3 软件升级

在系统维护页面选择软件升级页签进入软件升级页面，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。

### 系统维护

The interface includes a table with the following columns: 升级时间 (Upgrade Time), 升级结果 (Upgrade Result), 升级包 (Upgrade Package), 升级包发布日期 (Upgrade Package Release Date), 版本变更信息 (Version Change Information), and 操作 (Action).

| 升级时间                | 升级结果 | 升级包                                       | 升级包发布日期    | 版本变更信息  | 操作   |
|---------------------|------|---|------------|---|------|
| 2022-06-06 12:07:10 | 成功   | dbaudit-4.0.68.220531.2100-upgrade.tar.gz | 2022-05-31 | 系统版本: 从4.0.67.220406.1402 到 4.0.68.220531.2100; 规则版本: 从1.0_20211117.1 到 1.0_20220303.1; agent版本: 从2.28 到 2.29 | 变更明细 |

点击<变更明细>，可查看系统升级后的功能变化情况。

**变更明细** 4.0.67.220406.1402 到 4.0.68.220531.2100

- 新增支持审计DM 8、KingBase V7、KingBase V8、PostgreSQL 14等数据库
- 新增支持HDFS、Hive、PostgreSQL等场景下的Kerberos认证加密流量的解析
- 新增支持Oracle、PostgreSQL、MySQL、SQL Server等主流数据库的本地审计功能
- 新增支持在双向审计场景下，根据安全规则命中情况灵活、个性化设置结果集的存储策略
- 新增支持导出xls、csv格式的报表
- 新增支持设置CPU、内存、硬盘告警阈值，分布式部署时各节点支持分别设置不同的阈值
- 新增支持安全规则白名单检索
- 优化仪表盘，支持Tab页切换审计趋势、告警趋势、会话趋势，重新进入仪表盘页面时自动显示用户上一次选择的趋势图
- 优化统方场景下关联人员（执行人）的匹配逻辑
- 修复了已知问题，增强了系统稳定性

关闭

- ◆ 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。

## 8.4.4 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（系统不会以任何形式获取抓包文件）。

### 8.4.4.1 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。



### 8.4.4.2 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），点击<查看输出结果>。



可在弹出的对话框中显示测试结果。

```
返回结果 ×  
  
1 PING 192.168.30.33 (192.168.30.33) 56(84) bytes of data.  
2  
3 --- 192.168.30.33 ping statistics ---  
4 4 packets transmitted, 0 received, 100% packet loss, time 3000ms  
5  
6
```

#### ◆ NC 测试

NC 功能用来扫描目标主机的端口是否开放，操作方法如下：

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

**连通性检测**

操作类型:  ▼

协议:  ▼

\* IP:

\* 端口:

[查看输出结果](#)

在弹出的对话框中可查看测试结果。

返回结果

×

```
1 Ncat: Version 7.50 ( https://nmap.org/ncat )
2 Ncat: Connection timed out.
3
```

#### ◆ Traceroute

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

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

连通性检测

操作类型：

\* IP：

在弹出的对话框中显示测试结果。

返回结果

×

```
1 traceroute to 10.20.49.33 (10.20.49.33), 30 hops max, 60 byte
  packets
2  1  10.20.49.33 (10.20.49.33)  0.220 ms  0.190 ms  0.168 ms
```

### 8.4.4.3 Tcpdump 抓包管理

步骤 1. 在调试工具页面，在 Tcpdump 抓包管理区域点击<新增抓包任务>。

| Tcpdump抓包管理         |                       |                                  |      |    |      |                    |                    |
|---------------------|-----------------------|----------------------------------|------|----|------|--------------------|--------------------|
| 抓包开始时间              | 文件名称                  | MD5                              | 文件大小 | 状态 | 剩余时间 | 操作                 |                    |
| 2021-12-02 17:11:41 | tcpdump_p1_2021_12... | 82ab0237939eff877873efb90fe31afe | 24B  | 完成 | 0    | <a href="#">下载</a> | <a href="#">删除</a> |

步骤 2. 进入新增 Tcpdump 抓包页面，编辑相关信息，点击<保存>。

新增Tcpdump抓包 ✕

\* 网口:  ▼  
禁用网口无法抓包

过滤串:   
例: port 80 and host 192.168.1.2

\* 最大抓包时长:   
有效范围:1~86400, 单位: 秒

\* 最大文件大小:   
有效范围:1~10480, 单位: M

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。

| Tcpdump抓包管理         |                       |                                  |      |    |      |                    |                    |
|---------------------|-----------------------|----------------------------------|------|----|------|--------------------|--------------------|
| 抓包开始时间              | 文件名称                  | MD5                              | 文件大小 | 状态 | 剩余时间 | 操作                 |                    |
| 2021-06-28 16:33:14 | tcpdump_admin_2021... | ba9d4d068a471f55bbe31b439de75737 | 10KB | 完成 | 0    | <a href="#">下载</a> | <a href="#">删除</a> |

## 8.4.5 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，单击<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的功能，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。



## 8.4.6 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。

### 8.4.6.1 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进入如下页面，可查看数据备份的相关信息。

系统维护

时间 资源使用 软件升级 调试工具 数据清理 数据备份恢复 配置备份恢复 设备管理

备份几天前数据：2天，执行时间：02:00，压缩等级：6，点此修改

备份外送FTP配置

状态：启用  
协议：FTP  
IP：192.168.0.1  
端口：34  
用户名：root  
上传目录：/etc

修改

在线数据 本地备份数据 服务器备份数据

备份 状态 请选择

| 日期                                  | 数据状态 | 进度  | 空间占用 | 处理结果 | 操作 |
|-------------------------------------|------|-----|------|------|----|
| <input type="checkbox"/> 2021-06-29 | 在线   | 已结束 | 0B   |      | 备份 |

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。

修改数据自动备份定时任务
✕

---

备份几天前数据:  天

执行时间:

压缩等级:

压缩等级: 1~9  
 1: 压缩速度最快, 但压缩率最大  
 9: 压缩速度最慢, 但压缩率最小

确定
取消

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。                  |
| 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。 |

### 8.4.6.2 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。操作方法如下：

步骤 1. 在**备份外送 FTP 配置**区域点击<修改>。

系统维护

时间
资源使用
软件升级
调试工具
数据清理
数据备份恢复
配置备份恢复
设备管理

备份几天前数据: 2天, 执行时间: 02:00, 压缩等级: 6, 点此[修改](#)

**备份外送FTP配置**

状态: 禁用

协议: FTP

修改

步骤 2. 在弹出的对话框中编辑相关信息，点击<确定>。

修改备份外送FTP配置 ✕

状态:  启用  禁用

协议:  FTP  SFTP

\* IP:

\* 端口:

\* 用户名:

密码:  👁

\* 上传目录:

测试连接 确定 取消

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。    |

### 8.4.6.3 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。

| 在线数据 本地备份数据 服务器备份数据      |            |      |     |         |      |    |
|--------------------------|------------|------|-----|---------|------|----|
| 备份                       | 状态         | 请选择  |     |         |      |    |
| <input type="checkbox"/> | 日期         | 数据状态 | 进度  | 空间占用    | 处理结果 | 操作 |
| <input type="checkbox"/> | 2021-12-06 | 在线   | 已结束 | 347.3MB |      | 备份 |
| <input type="checkbox"/> | 2021-12-05 | 在线   | 已结束 | 911.9MB |      | 备份 |

## 8.4.6.4 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。

系统维护

时间 资源使用 调试工具 **数据备份恢复** 设备管理

节点上仅能恢复数据，如需更改配置请在顶部菜单切换到管理中心

在线数据 **本地备份数据** 服务器备份数据

恢复 FTP外送 状态 请选择

| <input type="checkbox"/> | 日期         | 备份结果 | 进度  | 空间占用   | 处理结果 | 操作       |
|--------------------------|------------|------|-----|--------|------|----------|
| <input type="checkbox"/> | 2021-06-26 | 成功   | 已结束 | 0B     |      | 恢复 FTP外送 |
| <input type="checkbox"/> | 2021-06-25 | 成功   | 已结束 | 0B     |      | 恢复 FTP外送 |
| <input type="checkbox"/> | 2021-06-24 | 成功   | 已结束 | 11.1GB |      | 恢复 FTP外送 |

步骤 3. 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。

在线数据 **本地备份数据** 服务器备份数据

恢复 **FTP外送** 状态 请选择

| <input type="checkbox"/>            | 日期         | 备份结果 | 进度  | 空间占用 | 处理结果 | 操作       |
|-------------------------------------|------------|------|-----|------|------|----------|
| <input checked="" type="checkbox"/> | 2021-06-28 | 成功   | 已结束 | 0B   |      | 恢复 FTP外送 |
| <input checked="" type="checkbox"/> | 2021-06-27 | 成功   | 已结束 | 0B   |      | 恢复 FTP外送 |
| <input type="checkbox"/>            | 2021-06-26 | 成功   | 已结束 | 0B   |      | 恢复 FTP外送 |

## 8.4.6.5 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。

在线数据 本地备份数据 **服务器备份数据**

恢复 从服务器刷新列表 状态 请选择

| <input type="checkbox"/> | 日期         | 服务器上传状态 | 进度  | 处理结果 | 操作 |
|--------------------------|------------|---------|-----|------|----|
| <input type="checkbox"/> | 2022-05-26 | 已上传     | 已结束 |      | 恢复 |
| <input type="checkbox"/> | 2022-05-25 | 已上传     | 已结束 |      | 恢复 |

## 8.4.7 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，进入如下页面。可查看系统配置备份的情况。

## 系统维护

时间 资源使用 软件升级 调试工具 数据清理 数据备份恢复 **配置备份恢复** 设备管理

自动备份周期: 每天自动备份, 备份文件上限: 10, 点此 **修改**

**备份** **上传恢复**

| 文件名称   | 完成时间                | 文件大小    | 状态 | 操作                |
|--|---------------------|---------|----|-------------------|
| <input type="checkbox"/> V4.0.68.20220418_BackupConfig_b6a70e7f2777430c94e5a29121357f5_20220606161642.zip  | 2022-06-06 16:16:42 | 140.8KB | 成功 | 下载 <b>恢复</b> 删除   |
| <input type="checkbox"/> V4.0.68.20220418_BackupConfig_f977d906bf11486d999d36653d242750_20220606161641.zip | 2022-06-06 16:16:42 | 140.8KB | 成功 | 下载   恢复 <b>删除</b> |

**删除** 共 2 条 < 1 > 20 条/页 跳至  页

可进行以下操作:

- ◆ 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>。

修改数据自动备份定时任务 ×

---

备份周期:

自动备份在凌晨2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

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。 |

## 8.4.8 设备管理

在**系统维护**页面选择**设备管理**页签, 进入如下页面。

## 系统维护

时间
资源使用
软件升级
调试工具
数据清理
数据备份恢复
配置备份恢复
设备管理

---

### 关机与重启

设备运行时间：23小时9分钟24秒

关机
重启

---

### 恢复出厂设置

恢复出厂设置将删除系统所有数据，恢复到出厂状态，请慎重执行！

出厂版本：V4.0

恢复出厂设置

---

### SSH登录设置

SSH端口状态：开

SSH登录KEY：XXXXXXXXXXXXXXXXXXXX (SSH登录KEY用于获取SSH登录密码)

---

### Web服务配置

修改端口前，请确保新端口网络可达。如不确定网络状况，建议先打开SSH端口再修改

服务端口：443

修改

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。

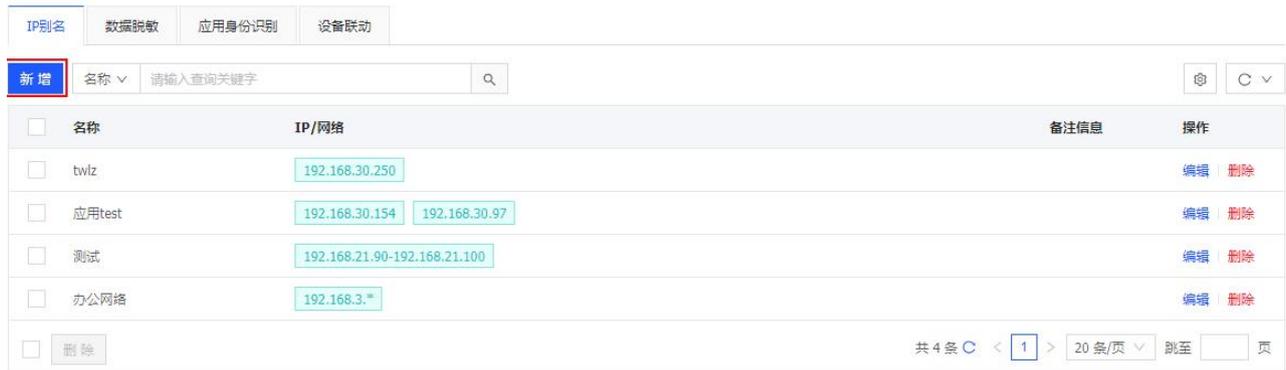
## 8.5 辅助功能

### 8.5.1 IP 别名

为方便对网络进行识别，可对网段或者 IP 地址设置别名。操作方法如下：

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，点击<新增>。

辅助功能



| 名称     | IP/网络                          | 备注信息 | 操作      |
|--------|--------------------------------|------|---------|
| twlz   | 192.168.30.250                 |      | 编辑   删除 |
| 应用test | 192.168.30.154   192.168.30.97 |      | 编辑   删除 |
| 测试     | 192.168.21.90-192.168.21.100   |      | 编辑   删除 |
| 办公网络   | 192.168.3.*                    |      | 编辑   删除 |

步骤 2. 弹出新增 IP 别名对话框，编辑相关信息，点击<保存>。



**\* 名称：** IP别名-1

**\* IP/网络：** 192.168.1.100-192.168.1.200

格式1:多个IP使用，“隔开；格式2:IP网段:用“\*”表示0~255的整数,例如:“192.126.30.\*”、“192.126.\*.\*” (“\*”之后不应出现数字)；格式3:支持范围配置，例如“10.1.1.10-10.1.1.20 (前面IP要小于后面IP，不支持IPv6，且靠前的两位需一致)”

备注：

保存 取消

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 | <ul style="list-style-type: none"> <li>◆ 格式 1：输入多个 IP 地址，用英文逗号分隔。</li> <li>◆ 格式 2：输入 IP 网段，用 “*” 表示 0~255，例如：192.168.0.*。</li> <li>◆ 格式 3：IP 范围，仅支持 IPv4，例如：10.1.1.10-10.1.1.20。</li> </ul> |

## 8.5.2 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。新增数据脱敏规则的操作方法如下：

步骤 1. 在菜单栏选择“系统管理>辅助功能”，选择数据脱敏页签进入如下页面，点击<新增>。

辅助功能

IP别名 数据脱敏 应用身份识别 设备联动

**新增** 名称 请输入查询关键字

| <input type="checkbox"/> | 名称   | 正则表达式  | 过滤范围             | 状态 | 操作    |
|--------------------------|------|--|------------------|----|-------|
| <input type="checkbox"/> | 银行卡号 | <code>((^\d ^)(349)d)([-\s\\V=]?)\d{4}([-\\s\\V=]?)\d{3}(\d)([-\s\\V=]?)\d{3}([\^d]{1}\$)</code>                   | 开始位置：7，截取长度：122  | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 密码   | <code>1twlz</code>   | 开始位置：1，截取长度：2222 | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 地名   | <code>twlzz</code>   | 开始位置：1，截取长度：22   | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 姓名   | <code>1123</code>  | 开始位置：11，截取长度：11  | 启用 | 编辑 删除 |
| <input type="checkbox"/> | twlz | <code>twlz</code>  | 开始位置：23，截取长度：5   | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 手机号码 | <code>((^\d ^)(0086)(13[0-9] 14[5-9] 15[0-3,5-9] 16[2,5,6,7] 17[0-8] 18[0-9] 19[1,3,5,8,9])[0-9]{8}[...]</code>    | 开始位置：7，截取长度：4    | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 手机号码 | <code>((^\d ^)(086 +86)(13[0-9] 14[5-9] 15[0-3,5-9] 16[2,5,6,7] 17[0-8] 18[0-9] 19[1,3,5,8,9])[0-9]{...}</code>    | 开始位置：6，截取长度：4    | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 手机号码 | <code>((^\d ^)(0)(13[0-9] 14[5-9] 15[0-3,5-9] 16[2,5,6,7] 17[0-8] 18[0-9] 19[1,3,5,8,9])[0-9]{8}([\^d]{...}</code> | 开始位置：4，截取长度：4    | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 手机号码 | <code>((^\d ^)(13[0-9] 14[5-9] 15[0-3,5-9] 16[2,5,6,7] 17[0-8] 18[0-9] 19[1,3,5,8,9])[0-9]{8}([\^d]{1...}</code>   | 开始位置：4，截取长度：4    | 启用 | 编辑 删除 |
| <input type="checkbox"/> | 身份证  | <code>((^\d ^)(1-9)d\d{5}(1-9)d\d{3}((0\d) (1[0-2]) (0 1 7)d)(13[0-17])d\d{3}(0-9xv)?([\^d]{1}\$)</code>           | 开始位置：4，截取长度：8    | 禁用 | 编辑 删除 |

共 15 条 < 1 > 20 条/页 跳至 页

步骤 2. 弹出新增数据脱敏对话框，编辑相关信息，点击<保存>。

新增数据脱敏

\* 名称：

\* 状态： 启用  禁用

\* 正则表达式：

\* 过滤范围：

开始位置有效范围:1~9999;截取长度有效范围:1~9999

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：([ <sup>^</sup> 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。   |

### 8.5.3 应用身份识别

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。

- ◆ 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。之后，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。
- ◆ 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。之后，当系统审计到相同的 SQL 模板，就会直接关联出用户名。

#### 8.5.3.1 B/S 应用身份识别

步骤 1. 在菜单栏选择“系统管理>辅助功能”，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>。

辅助功能



The screenshot shows the '辅助功能' (Auxiliary Function) interface. At the top, there are tabs for 'IP别名', '数据脱敏', '应用身份识别', and '设备联动'. Under '应用身份识别', there are sub-tabs for 'B/S应用身份识别' and 'C/S应用身份识别'. Below the sub-tabs, there is a search bar with a '添加' (Add) button highlighted in a red box. Below the search bar is a table with the following columns: '应用名称', '中间件类型', '中间件版本', 'JDK版本', '数据库类型', '登录URL关键字', '登录用户关键字', '客户端IP提取方', and '操作'. The table contains one row with the following data: 'oracle', 'Weblogic', '9', '1.6及以上', 'Oracle', 'Oracle', 'root', 'X-Forwarded-...', and '下载 | 编辑 | 删除'.

步骤 2. 在弹出的对话框中编辑相关信息，点击<保存>。

编辑B/S应用身份识别配置

\* 应用名称:

\* 中间件类型:

\* 中间件版本:

\* JDK版本:

\* 数据库类型:

\* 登录URL关键字:

\* 登录用户关键字:

客户端IP提取方式:

层级:

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>可查看安装方法）。

## 辅助功能

IP别名 数据脱敏 应用身份识别 设备联动

B/S应用身份识别 C/S应用身份识别

添加 删除 下载说明文档 应用名称 请输入查询关键字

| 应用名称   | 中间件类型    | 中间件版本 | JDK版本  | 数据库类型  | 登录URL关键字 | 登录用户关键字 | 客户端IP提取方        | 操作       |
|--------|----------|-------|--------|--------|----------|---------|-----------------|----------|
| oracle | Weblogic | 9     | 1.6及以上 | Oracle | Oracle   | root    | X-Forwarded-... | 下载 编辑 删除 |

步骤 4. 之后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 以及使用的 IP。

### 8.5.3.2 C/S 应用身份识别

步骤 1. 在菜单栏中选择“**查询分析>审计日志**”，找到 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](#)）。

新增C/S应用身份识别配置

资产: [选择]

SQL模板: select \* from `department` where `id` = :1

\* 参数位置: :1 ('8601')

请选择应用用户名所在的参数位置

确定 取消

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**”，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。

## 辅助功能

IP别名 数据脱敏 应用身份识别 设备联动

B/S应用身份识别 C/S应用身份识别

删除 资产名称 请输入查询关键字

| 资产名称                 | SQL模板               | 参数位置 | 客户端工具                             | 参数列表 | 操作    |
|----------------------|---------------------|------|-----------------------------------|------|-------|
| oracle_192.168.21.97 | select :1 from dual | :1   | C:\Program Files\PLSQL Develop... | :1   | 编辑 删除 |

显示 1 - 1, 共 1 条

< 1 > 10 条/页 跳至 页

## 8.5.4 设备联动

数据库审计支持与 AiSort、数据安全管控平台进行联动，以便更好地识别出访问数据库系统的风险行为。

### 8.5.4.1 与 AiSort 联动

数据库审计与 AiSort 联动后, 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”, 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。



### 8.5.4.2 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。



## 8.6 系统告警

### 8.6.1 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。

#### 8.6.1.1 修改日志保留天数

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，点击<修改>。

## 系统告警

[告警查询](#)
[告警通知](#)

日志保留天数: 365; CPU告警阈值: 80%, 内存告警阈值: 30%, 磁盘告警阈值: 80% [修改](#)

步骤 2. 弹出**修改系统日志自动清理配置**对话框，编辑相关信息，点击**<确定>**。

修改系统告警配置
✕

---

日志保留天数:

CPU告警阈值:  %

内存告警阈值:  %

磁盘告警阈值:  %

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 告警阈值 | 设置 CPU 告警阈值，取值范围：1~100。 |
| 内存告警阈值   | 设置内存告警阈值，取值范围：1~100。    |
| 磁盘告警阈值   | 设置磁盘告警阈值，取值范围：1~100。    |

### 8.6.1.2 查询告警日志

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

## 系统告警

告警查询
告警通知

日志保留天数: 365; CPU告警阈值: 80%; 内存告警阈值: 30%; 磁盘告警阈值: 80% [修改](#)

时间范围:  ~    
 告警类型:    
 告警级别:

日志列表

| 时间                  | 异常模块 | 告警类型 | 告警级别 | 告警描述                             |
|---------------------|------|------|------|----------------------------------|
| 2022-06-30 17:15:14 | 流量代理 | 通讯日志 | 高风险  | 流量代理连接异常: [192.168.21.180:55730] |
| 2022-06-30 17:15:14 | 流量代理 | 通讯日志 | 高风险  | 流量代理连接异常: [192.168.21.180:53500] |
| 2022-06-30 17:15:14 | 许可证  | 其他日志 | 高风险  | license已过期8天, 请及时处理              |
| 2022-06-30 17:14:22 | 内存   | 异常日志 | 高风险  | 内存使用超过30%                        |

## 8.6.2 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>。

告警查询
告警通知

新增
日志级别 ▼ 请选择
🔍
⚙️
C ▼

| <input type="checkbox"/> | 告警级别        | 通知方式   | 接收者           | 任务创建者 | 操作                                    |
|--------------------------|-------------|--------|---------------|-------|---------------------------------------|
| <input type="checkbox"/> | 低风险 高风险 中风险 | Syslog | 192.168.31.75 | admin | <a href="#">编辑</a> <a href="#">删除</a> |

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](#)。

新增系统日志外送任务
✕

\* 告警级别:  低风险  中风险  高风险

\* 通知方式:  邮件  短信  企业微信  钉钉  Syslog  Snmp

\* 接收者:

## 8.7 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，操作方法如下：

在菜单栏选择“**系统管理**”>**操作日志**”进入操作日志查询页面，可根据时间范围、用户、来源 IP、操作名称、操作类型、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。

### 操作日志

日志保留天数: 180 天 [修改](#)

时间范围  开始日期 ~ 结束日期

筛选: [操作类型:状态变更](#)  清除

| 时间                  | 用户    | 来源IP          | 操作名称     | 操作类型 | 操作内容 (点击查看详细)                          | 操作结果 | 操作                 |
|---------------------|-------|---------------|----------|------|--|------|--------------------|
| 2021-12-06 10:24:58 |       | 10.20.120.164 | 系统登录     | 状态变更 | 账号: admin, 登录方式: 密码登录                  | 成功   | <a href="#">详细</a> |
| 2021-12-06 10:24:44 |       | 10.20.120.164 | 系统登录     | 状态变更 | 账号: admin, 登录方式: 密码登录, 错误信息: 用...      | 失败   | <a href="#">详细</a> |
| 2021-12-06 10:15:55 | admin | 10.11.33.99   | 创建日志外送任务 | 状态变更 | 接收端ID: 1435502697900949504, 日志类型: 会... | 失败   | <a href="#">详细</a> |
| 2021-12-06 10:14:11 | admin | 10.11.33.99   | 创建日志外送任务 | 状态变更 | 接收端ID: 1435502697900949504, 日志类型: 会... | 失败   | <a href="#">详细</a> |

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**>。

### 操作日志

日志保留天数: 180 天 [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**>。

修改操作日志自动清理配置 ×

---

日志保留天数:

---

## 9 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。   |