数据安全审计

操作指南

腾讯云

文档目录

- 审计报表
- 数据资产与 Agent
- 配置管理
  - 审计单元配置
  - 访问源配置
  - 部门业务配置
- 操作日志管理

v5.0.7

- 系统管理
  - 系统资源监控
  - 用户管理
  - OTP 设置
  - 告警设置
  - 时间服务器
  - 备份服务器设置
- 审计管理
  - 安全审计与分析
    - 审计数据
    - 规则配置
    - 审计报表
  - 数据资产与 Agent
  - 配置管理
    - 审计单元配置
    - 访问源配置
    - 部门业务配置
- 操作日志管理

v5.0.6

- 系统管理
  - 系统资源监控
  - 用户管理
  - OTP 设置
  - 告警设置
  - 时间服务器
  - 备份服务器
- 审计管理
  - 安全审计与分析
    - 审计数据
    - 规则配置
    - 审计报表
  - 数据资产与 Agent
  - 配置管理
    - 审计组配置
    - 访问源配置
    - 部门业务配置
- 操作日志管理

v5.0.5

- 系统管理
  - 系统资源监控
  - 用户管理
  - Agent 管理
    - Agent 配置
    - Agent 列表
  - 时间服务器

操作指南
数据安全审计SaaS型
权限管理

最近更新时间：2024-05-24 17:32:21

数据安全审计产品基于访问管理（Cloud Access Management，CAM）进行访问权限的控制，为确保子用户正常操作和使用数据安全审计产品，本文提供相关权限授予操作指引。

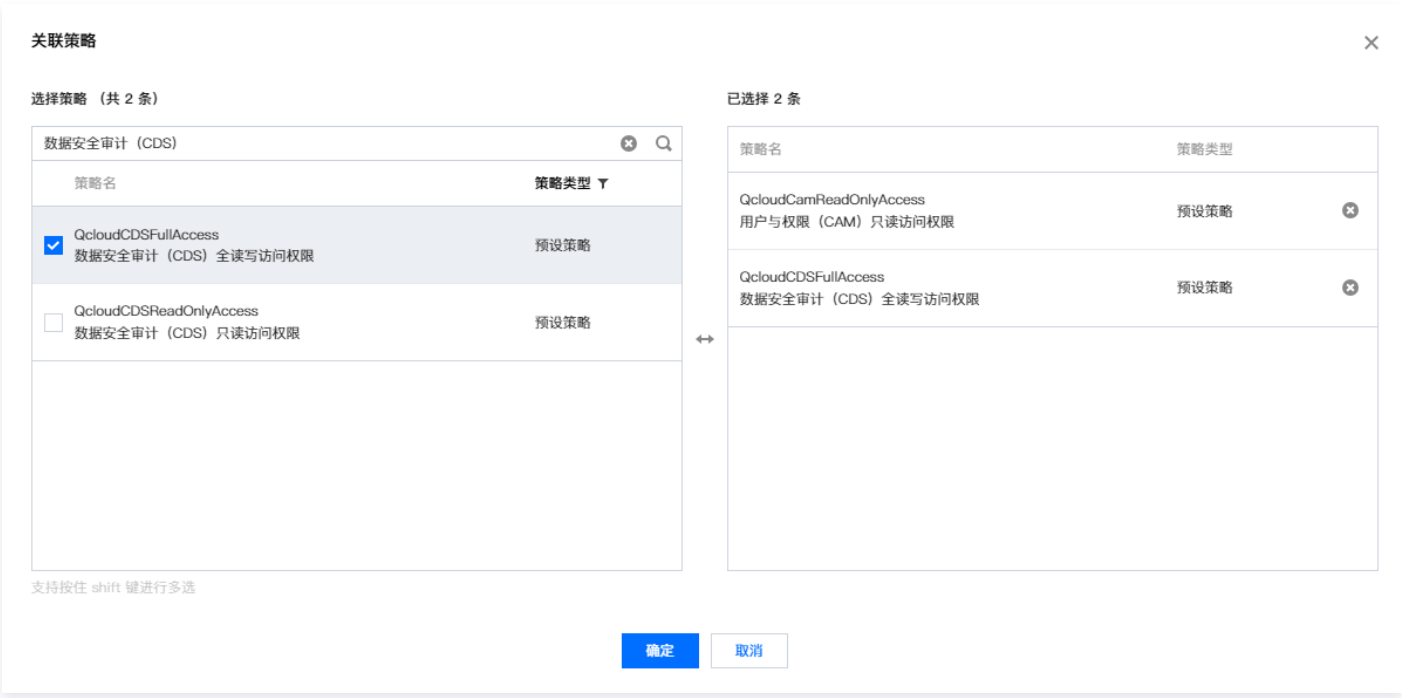
权限策略总览

策略名	描述	是否必选	说明
QcloudCamReadOnlyAccess	用户与权限（CAM）只读访问权限	是	角色授权相关权限
QcloudCDSFullAccess	数据安全审计（CDS）全读写访问权限	是（二选一）	数据安全审计产品所有功能操作权限
QcloudCDSReadOnlyAccess	数据安全审计（CDS）只读访问权限		数据安全审计产品只读与访问权限

操作步骤

1. 登录 访问管理控制台，在左侧导航栏中，单击**用户 > 用户列表**。
2. 在用户列表页面，找到目标子用户，单击**授权**。

3. 在关联策略弹窗中，搜索需要授权的策略名并选中，单击**确定**即可。

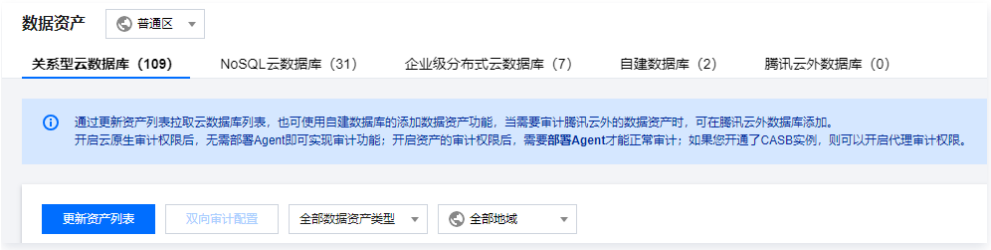

关联策略
选择策略 （共 2 条）
数据安全审计（CDS）
策略名
策略类型
QcloudCDSFullAccess
数据安全审计（CDS）全读写访问权限
预设策略
QcloudCDSReadOnlyAccess
数据安全审计（CDS）只读访问权限
预设策略
支持按住 shift 键进行多选
已选择 2 条
策略名
策略类型
QcloudCamReadOnlyAccess
用户与权限（CAM）只读访问权限
预设策略
QcloudCDSFullAccess
数据安全审计（CDS）全读写访问权限
预设策略
确定
取消

数据资产

最近更新时间：2025-05-06 17:06:32

管理云数据库

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**数据资产** > **关系型云数据库**，进入关系型云数据库页面。
2. 在关系型云数据库页面，单击**更新资产列表**，自动拉取您在腾讯云账号内的关系型云数据库、NoSQL 云数据库、企业级分布式云数据库，同步成功则会在列表显示。



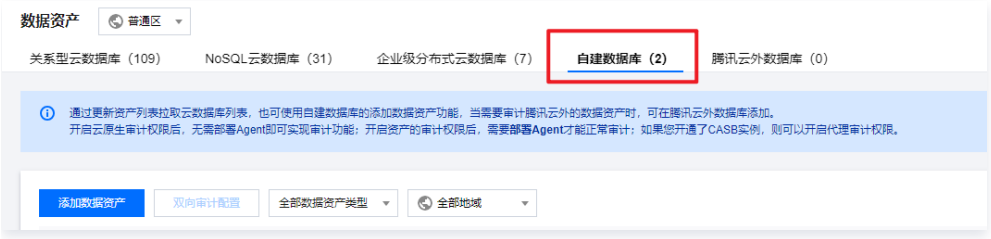
3. 选择一个实例，单击审计权限的 ，即审计权限开启成功。如关闭审计权限，将不再审计该资产，也无法查看该资产的审计日志。

注意

- 开启审计权限将消耗 License 授权资产数。
- 部分操作需要用户授权，只需按提示操作即可。
- 如果开启的是 CASB 审计权限，则需要购买云访问安全代理（CASB），并且将对应元数据与代理绑定。
- 云原生审计权限无需安装 Agent 即可实现云原生审计功能，当前只支持云数据库 MySQL。

管理自建数据库

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**数据资产** > **自建数据库**，进入自建数据库页面。
2. 在自建数据库页面，单击**添加数据资产**，弹出添加数据资产弹窗。



3. 在添加数据资产弹窗中，配置相关参数，单击**提交并继续添加**可再次添加。

参数名称	描述
添加方式	根据实际需求选择 选择 CVM 或手动输入 IP。 • 选择 CVM：部署在私有网络CVM上的资产。 • 手动输入 IP：通过专线等方式与私有网络打通的资产。
地域	支持广州、上海、南京、北京、成都、重庆。添加成功后，不可更改。
VPC	可选项，可通过选择资产所在 VPC ，缩小 CVM 实例查找范围。
CVM实例	选择自建数据库所在的CVM实例。
数据资产名称	自定义名称，在64个字符之内，不能重复。
操作系统	选择数据库所在的操作系统。
数据库资产类型及对应版本	• MySQL：5.1、5.2、5.3、5.4、5.5、5.6、5.7、8.0。 • PostgreSQL：9、10、11、12、13、14。 • SQL Server：2008、2012、2014、2016、2017、2019。 • Oracle：8i、9i、10g、llg、12c、18c、19c。 • Redis：所有版本都支持。 • MongoDB：2.x、3.x、4.x。 • TDSQL-MySQL：5.7、8.0、10.1。 • MariarDB：5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3、10.4、10.5、10.6。 • Hive：所有版本都支持。 • HBase：所有版本都支持。 • TDSQL-C MySQL：5.7、8.0。 • DM：V7、V8。 • KingbaseES：V8。 • GaussDB：200、300。

	• TIDB：4.5、5.0、6.5。 • OCEANBASE：4.2。
端口	1-65535。
加密审计协议	仅当数据资产类型为 MySQL 或 MariaDB 时，此选项可见。开启此选项后，支持用户上传密钥文件，审计开启了 SSL 加密的数据库。详情请参见 配置参考 。
密钥文件	上传密钥文件，大小限制在1MB 以内。
私钥密码	可选项，若密钥带有密码，请在此输入，限64字符以内。

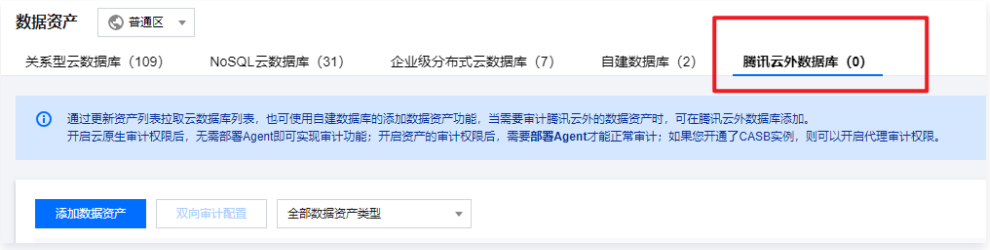
4. 添加成功后可自行开启审计权限或修改取消审计权限。

管理腾讯云外数据库

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**数据资产** > **腾讯云外数据库**，进入腾讯云外数据库页面。

> **说明**
> 腾讯云外数据库，适合部署在友商云或 IDC，而没有通过专线等方式与私有网络打通，需要通过公网进行流量采集的资产。

2. 在腾讯云外数据库页面，单击**添加数据资产**，弹出添加数据资产弹窗。



3. 在添加数据资产弹窗中，配置相关参数，单击**确定**完成添加。

参数名称	描述
数据资产名称	自定义名称，在64个字符之内，不能重复。
操作系统	选择数据库所在的操作系统。
数据库资产类型及对应版本	• MySQL：5.1、5.2、5.3、5.4、5.5、5.6、5.7、8.0。 • PostgreSQL：9、10、11、12、13、14。 • SQL Server：2008、2012、2014、2016、2017、2019。 • Oracle：8i、9i、10g、llg、12c、18c、19c。 • Redis：所有版本都支持。 • MongoDB：2.x、3.x、4.x。 • TDSQL-MySQL：5.7、8.0、10.1。 • MariarDB：5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3、10.4、10.5、10.6。 • Hive：所有版本都支持。 • HBase：所有版本都支持。 • TDSQL-C MySQL：5.7、8.0。 • DM：V7、V8。 • KingbaseES：V8。 • GaussDB：200、300。 • TIDB：4.5、5.0、6.5。 • OCEANBASE：4.2。
IP	根据实际需求输入所需 IP。
端口	1-65535。
加密审计协议	仅当数据资产类型为 MySQL 或 MariaDB 时，此选项可见。开启此选项后，支持用户上传密钥文件，审计开启了 SSL 加密

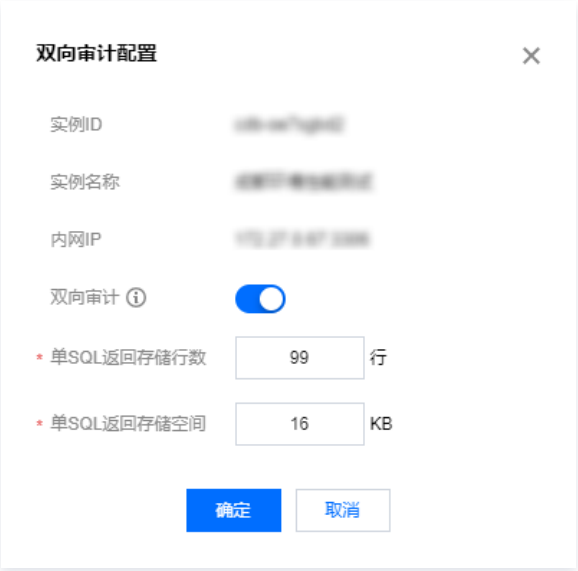
	的数据库。详情请参见 配置参考 。
密钥文件	上传密钥文件，大小限制在1MB 以内。
私钥密码	可选项，若密钥带有密码，请在此输入，限64字符以内。

4. 选择一个实例，单击审计权限开关的，即审计权限开启成功。

双向审计配置

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**数据资产**，进入数据资产管理页面。
2. 选择需要配置**双向审计**的数据库资产，单击操作栏中的**编辑**，弹出双向审计配置弹窗。

3. 在双向审计配置弹窗中，单击开启**双向审计**，并设置**单 SQL 返回存储行数**、**单 SQL 返回存储空间**。



4. 单击**确定**，即可开启成功。

> **说明：**
> - 选中多个数据库资产，单击**双向审计配置**，支持批量开启并配置双向审计。
> - 启用双向审计之后，存储空间占用将有所提高；返回数据您可到 审计日志 中查看。

审计日志
审计日志

最近更新时间：2025-05-26 18:00:22

审计日志从 SQL 语句的维度，帮您进行安全分析。

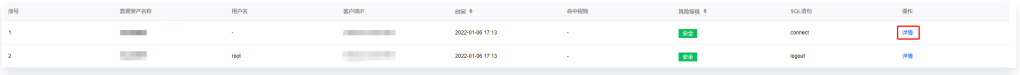
检索审计日志

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 审计日志**。
2. 在审计日志页面，可根据具体数据资产名称检索，还可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期检索。

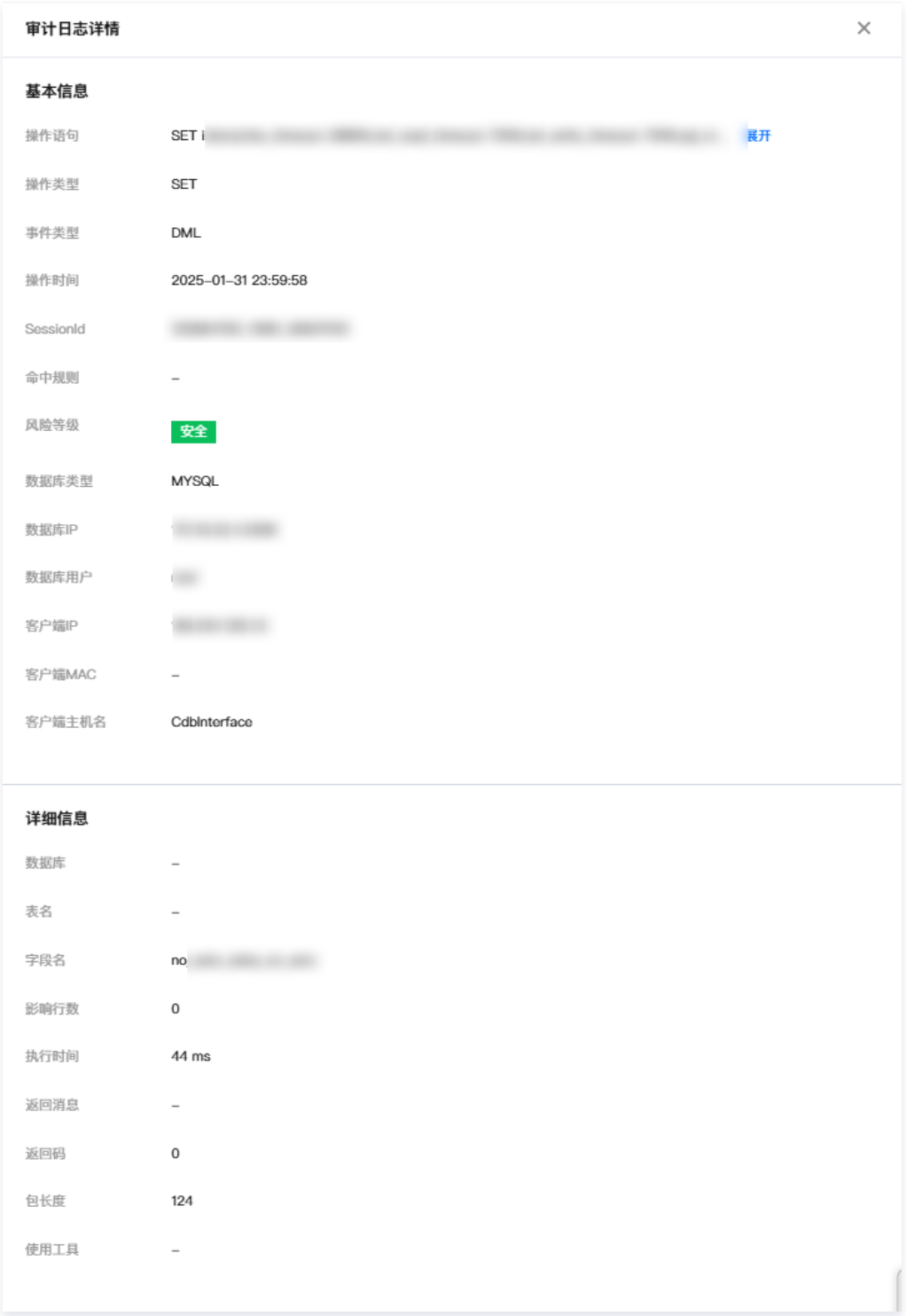
3. 如需对审计日志进行指定检索。单击**高级筛选**，可根据用户名、命中规则、风险等级、客户端 IP 、事件类型、表名、字段名等关键字，输入具体值，单击**查询**，即可查看相关信息。

查看审计日志

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 审计日志**。
2. 在审计日志页面的日志列表中，选择所需日志，单击**详情**，进入审计日志详情页面。



3. 在审计日志详情页面，可查看该条日志的基本信息、详细信息。



下载审计日志

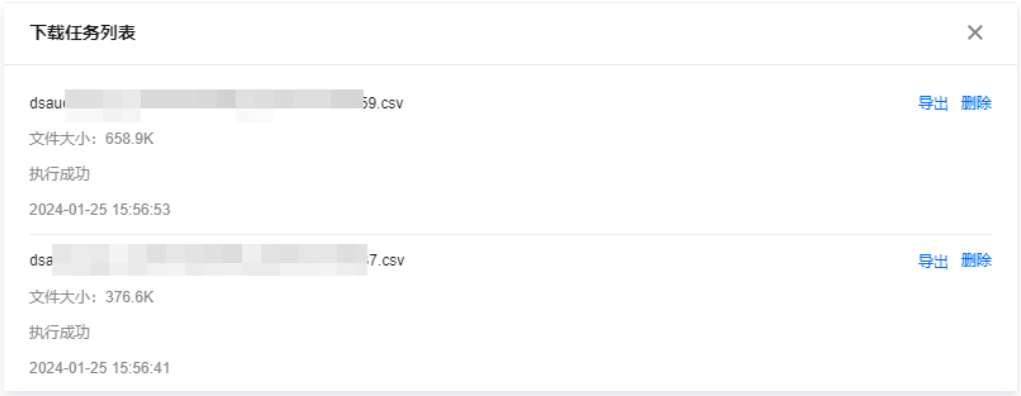
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 审计日志**。

2. 在审计日志页面，单击右侧的，进行审计日志的下载。

3. 审计日志将根据当前筛选条件进行下载，单击**确定**。

4. 单击 前往下载任务列表，查看并管理下载任务。
   - 单击**导出**，即可将任务下载至本地。
   - 单击**删除**，经过二次确认后，即可删除所选任务。

> **注意：**
> 日志每次最大可导出 1 GB，已完成的任务仅保留一天，请及时下载日志。



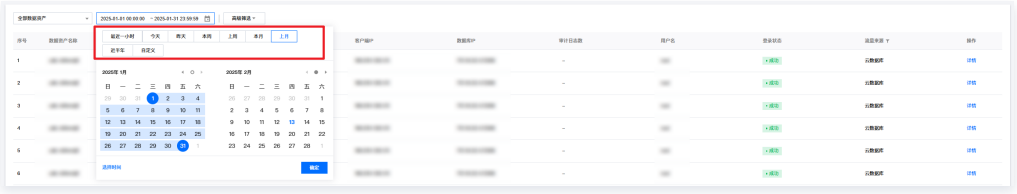
审计会话

最近更新时间：2025-05-26 18:00:22

审计会话从数据库连接会话的维度，帮您进行安全分析。

检索审计会话

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 审计日志**。
2. 在审计日志页面，单击**审计会话**。
3. 在审计会话页面，可根据具体数据资产名称检索，还可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期检索。

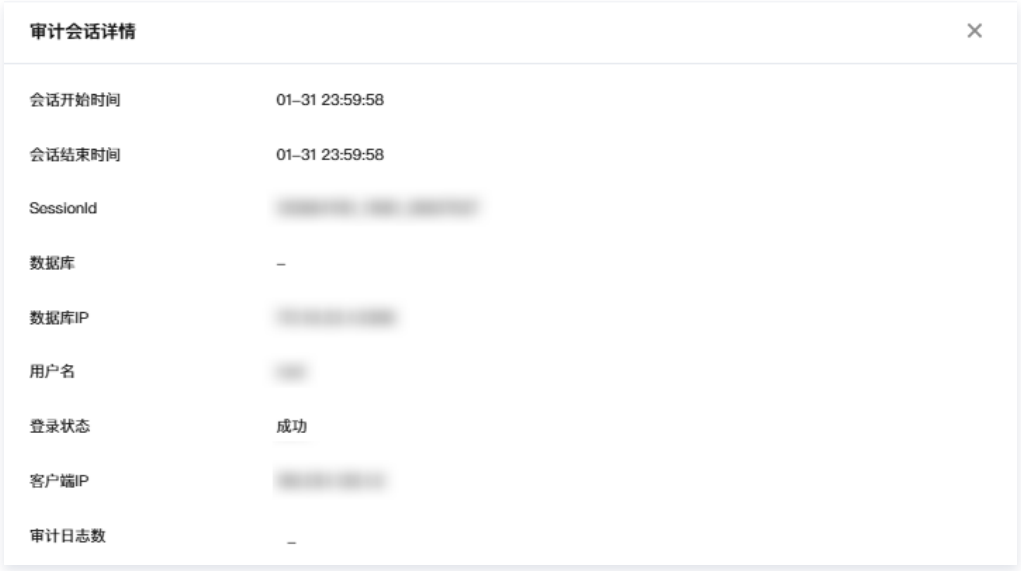


4. 如需对审计会话进行指定检索。单击**高级筛选**，可根据用户名、命中规则、风险等级、客户端 IP 等关键字，输入具体值，单击**查询**，即可查看相关信息。

查看数据详情

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 审计日志**。
2. 在审计日志页面，单击**审计会话**。
3. 在审计会话页面，可单击某条记录**详情**，进入审计会话详情页面。

4. 在审计会话详情页面，可查看该条日志的详细信息。



日志投递

最近更新时间：2025-05-26 18:00:22

前提条件

- 已开通日志投递功能，费用详情请参见 计费概述 。
- 已完成角色授权操作。
- 已购买腾讯云 消息队列 CKafka 实例，按照实际日志用量来配置 CKafka 实例的带宽规格。
- 支撑环境接入 CKafka 时需 提交工单 。

配置日志投递

1. 登录 数据安全审计控制台，在左侧导航栏选择**基础审计 > 日志投递**。
2. 如果日志投递未配置，则直接进入配置页面；如果日志投递已配置，单击**重新配置**进入配置页面。
3. 在配置页面，配置日志投递信息。

参数列表：

参数名称	参数说明
网络接入方式	选择消息队列的接入方式。
消息队列实例	选择日志投递的消息队列实例。
网络	选择需使用的网络，支持 PLAINTEXT 类型。
用户名	设置用户名。仅公网域名接入方式需要填写。
密码	设置密码。仅公网域名接入方式需要填写。
Topic ID/名称	选择投递的 Topic。

4. 输入参数后，单击**保存生效**。

日志管理
日志备份管理

最近更新时间：2025-05-26 18:00:22

用户日志存储空间划分为在线日志、备份日志两部分，两者比例为7：3。最新产生的日志为在线日志，可在查询分析页面查看。当在线日志存储空间占用达到80%后，系统将把早期日志压缩存储，以节约空间，压缩比约为4：1。

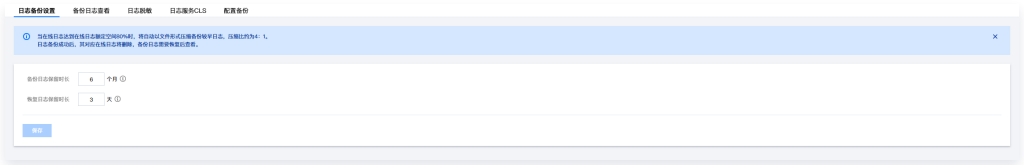
说明：

- 例如：24 年01月23 日，用户在线日志存储空间达到80%，触发了日志备份，系统把用户在线日志中最早期的一段（如 23 年04月01日-23 年04月30日）取出来进行压缩备份，备份后这段时间的日志会从在线空间删除，无法在审计日志页面查看，用户的在线存储空间从 80% 降低到了70%，备份后的文件可以在备份日志查看页面获取。

  而在日志备份设置页面，用户设定了“备份日志保留时长”为 6 个月，代表该日志备份文件如果 6 个月内未手动恢复（操作单击 恢复 ）则永久清理。如果用户希望查看这段时间的日志，需要在**在线存储空间足够**的前提下，从备份日志查看页面对目标文件进行恢复。恢复后的日志会被放回在线日志存储空间，用户可以在审计日志页面重新查询到。
- 如果在线存储空间不足，可以通过存储扩容保留更久时长的日志。

备份设置

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**日志备份设置**。
3. 在日志备份设置页面，设置日志备份的相关参数，单击**保存**。



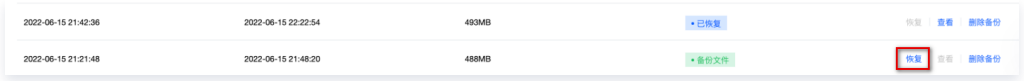
参数说明：

- 备份日志保留时长：备份日志存储超过该时长即永久删除。
- 恢复日志保留时长：备份日志只有执行恢复操作后才能查看，恢复日志最多保留7天（含恢复当日）。

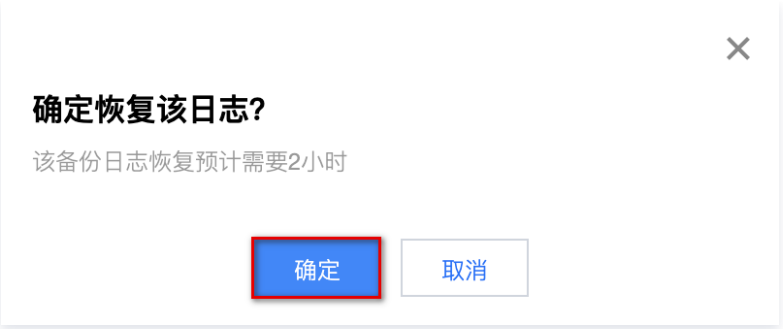
备份日志查看

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**备份日志查看**。
3. 在备份日志查看页面，通过日志起始时间、结束时间确认需要查看的备份日志。

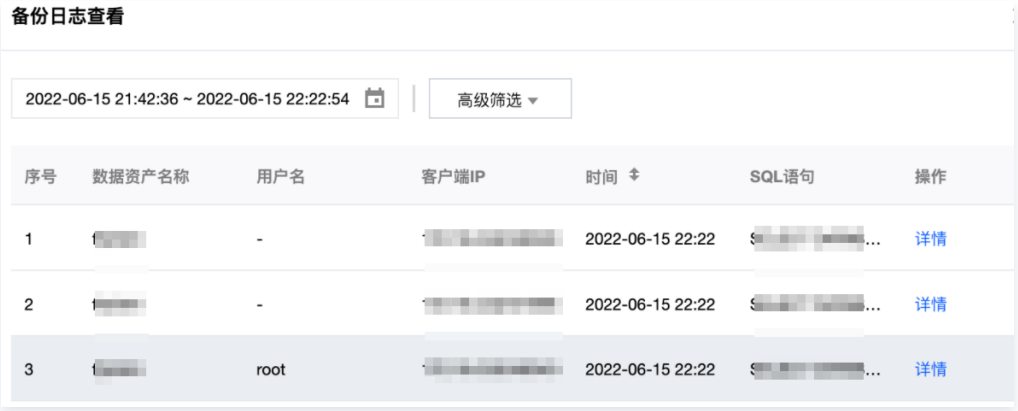
4. 日志状态为**备份文件**的日志，可以单击**恢复**。



5. 在确认恢复弹窗中，给出了预估的恢复时间，单击**确定**后等待恢复完成。



6. 恢复完成后，其日志状态变更为已恢复。单击操作列的**查看**，弹出日志查看页面。



7. 若要删除备份日志，单击操作列的**删除备份**，经过二次确认后即可删除。

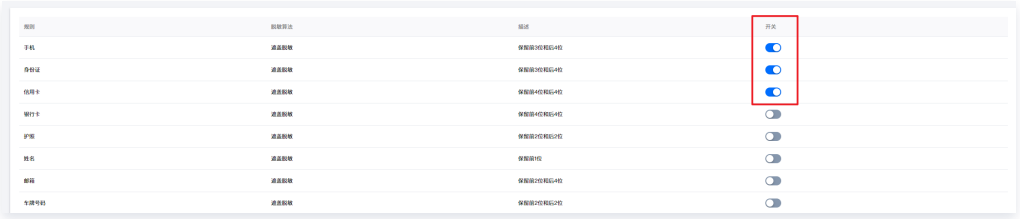
> **说明**
> - 备份文件只有恢复后才可查看。
> - 备份文件删除之后，无法恢复，请谨慎操作。

日志脱敏

最近更新时间：2025-05-26 18:00:22

日志脱敏是指对记录在日志中的敏感数据进行处理，以实现对敏感隐私数据的安全保护。

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**日志脱敏**。
3. 在日志脱敏页面，选择需要脱敏的数据规则，并将开关列中的“开启/关闭”切换为“开启”。



日志服务 CLS

最近更新时间：2025-05-26 18:00:22

数据安全审计支持将审计日志投递到日志服务 CLS，实现日志从采集、日志存储到日志检索等全方位的日志服务。

> **说明：**
> 日志服务 CLS 为第三方独立计费云产品，计费标准请参考 CLS 购买指南 。

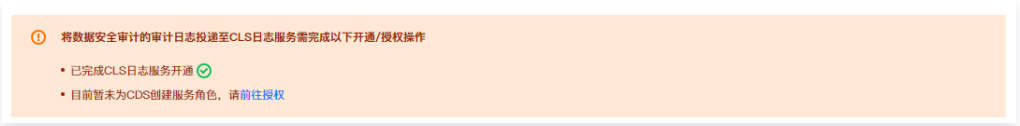
前置条件

- 已开通 数据安全审计服务 。
- 已开通 日志服务 。
- 当前账号已完成角色授权。

开通日志服务与角色授权

首次使用时，您需要 开通日志服务 并完成角色授权。

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**日志服务 CLS**。
3. 在日志服务 CLS 页面，单击**前往授权**，弹出服务授权弹窗。



4. 在服务授权弹窗中，单击**同意授权**，即可完成授权操作。
5. 操作完成后，即可使用日志服务 CLS，实现将审计日志、风险日志从采集、日志存储到日志检索等全方位的日志服务。

启用日志服务CLS

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**日志服务 CLS**。
3. 在日志服务 CLS 页面，选择需要启用的日志类型，单击**立即启用**，即可弹出开启日志投递的弹窗。

4. 在开启日志投递的弹窗中，选择目标地域、日志集、日志主题等配置。

参数	说明
目标地域	选择日志投递的地域，支持异地投递。

日志主题操作	日志主题是日志数据进行采集、存储、检索和分析的基本单元。支持选择已有日志主题或者创建日志主题。
日志主题	• 选择已有日志主题：可在搜索框筛选所选日志集下的日志主题。 • 创建日志主题：在所选日志集下创建新的日志主题。 **说明：** 您可对日志主题进行管理，详细请参见 管理日志主题 。
日志集操作	日志集是对日志主题的分类，方便您管理日志主题。支持选择已有的日志集或者创建日志集。仅当日志主题操作选择创建日志主题时可选。
日志集	• 选择已有日志集：可在搜索框筛选已有的日志集。 • 创建日志集：仅当日志主题操作选择创建日志主题时，此项可设置。

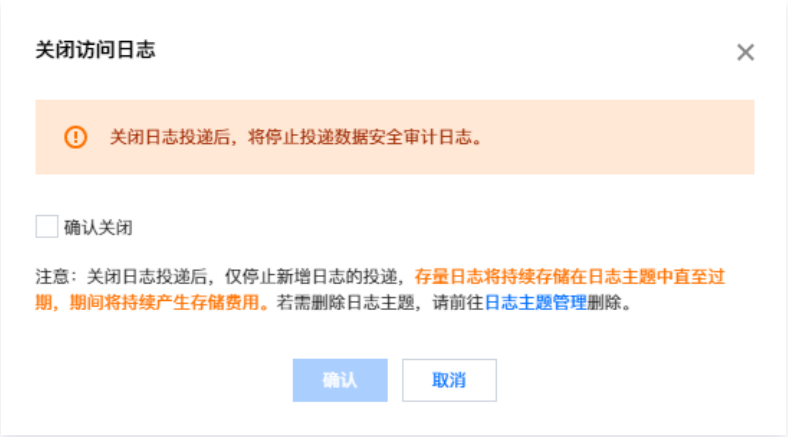
5. 选择参数配置后，单击**立即开启**即可。

检索分析

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**日志服务 CLS**。
3. 在日志服务 CLS 页面，选中需要查看的日志类型，单击**检索分析**，跳转至 日志服务控制台 。
4. 在日志服务中，检索分析提供对日志数据进行过滤、搜索和统计分析的功能。
5. 详细请参见 检索分析 。

关闭投递

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**基础审计 > 日志管理**。
2. 在日志管理页面，单击**日志服务 CLS**。
3. 在日志服务 CLS 页面，选择需要关闭的日志类型，单击**关闭投递**，弹出关闭投递的弹窗。
4. 在关闭访问日志弹窗中，阅读注意事项并勾选**确认关闭**，单击**确认**即可。



说明：

- 关闭日志投递后，将停止投递数据安全审计日志。
- 关闭日志投递后，仅停止新增日志的投递，存量日志将持续存储在日志主题中直至过期，期间将持续产生存储费用。若需删除日志主题，请前往 日志主题管理 删除。

风险识别
审计风险

最近更新时间：2025-05-26 18:00:22

审计风险从审计规则命中的风险等级维度，帮您进行安全分析。

检索审计风险

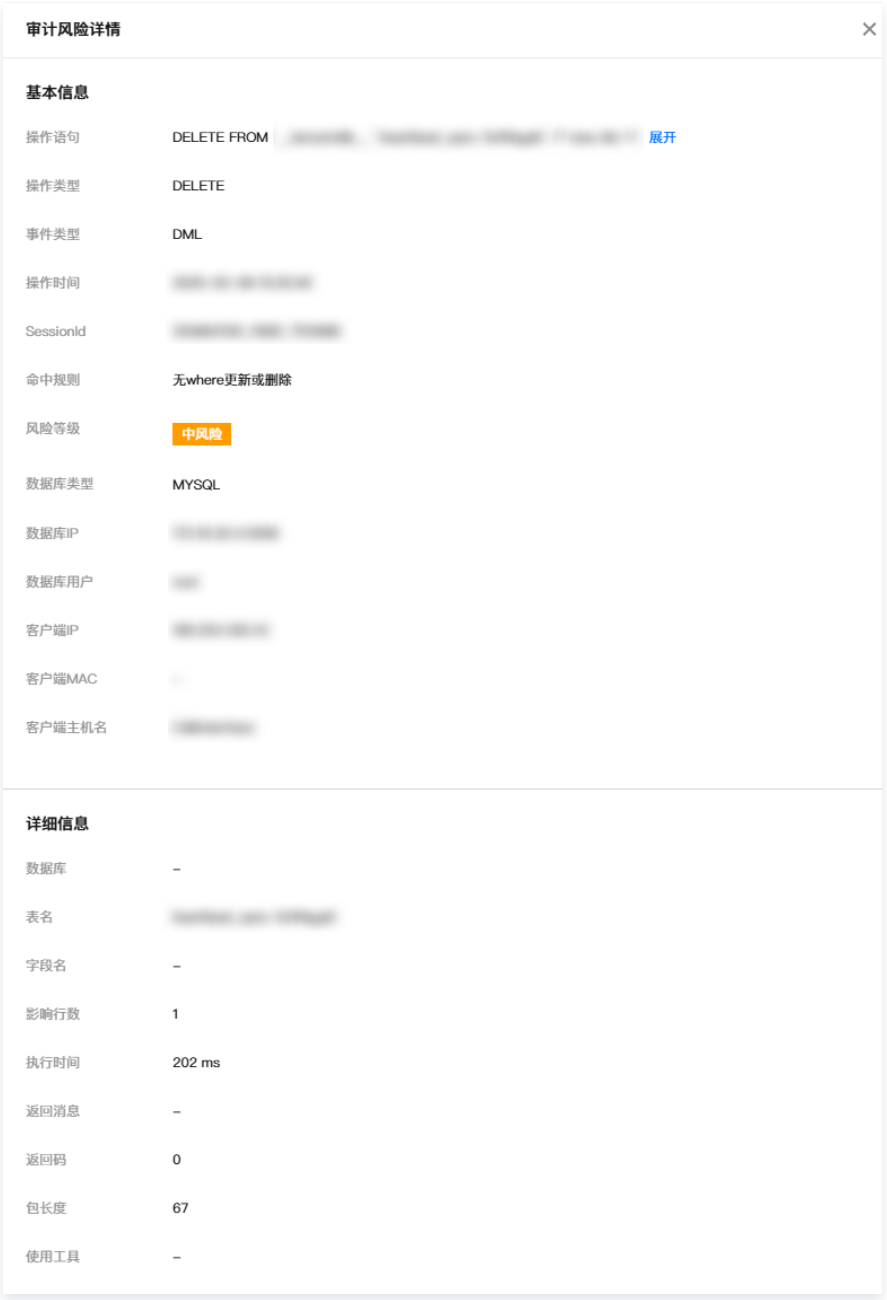
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 风险识别**。
2. 在审计风险页面，可根据具体数据资产名称检索，还可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期检索。

3. 如需对审计风险进行指定检索。单击**高级筛选**，可根据用户名、命中规则、风险等级、客户端 IP 等关键字，输入具体值，单击**查询**，即可查看相关信息。

查看数据详情

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 风险识别**。
2. 在审计风险页面的日志列表中，选择所需日志，单击**详情**，进入审计风险详情页面。

3. 在审计风险详情页面，可查看该条日志的基本信息和详细信息。



创建规则

您可以针对某一条风险的具体操作动作，单独创建一条审计风险规则。通过这一规则，精准锁定特定的客户端、服务端以及操作行为，实现针对性的风险管控。

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 风险识别**。
2. 在审计风险页面的日志列表中，选择所需日志，单击**创建规则**，进入创建规则页面。

3. 在创建规则页面，您可以看到触发数据安全风险的客户端信息、服务端信息、具体操作行为。您可以自定义规则类型、规则名称、规则备注、风险等级以及是否告警，单击**确定**保存。


创建规则
基础信息
规则类型:
黑名单
白名单
* 规则名称:
无where更新或删除_
规则备注:
操作规则
* 风险等级:
低风险
中风险
高风险
规则定义
客户端:
客户端ip:
包含
删除
服务端:
数据库ip:
数据库端口:
等于
3306
数据库用户:
数据库名:
可配置多个数据库名，英文逗号分隔，如：mysql,test
行为:
操作类型:
DELETE
操作语句:
DELETE FROM
表名:
输出定义
* 是否告警
是
否
确定
取消

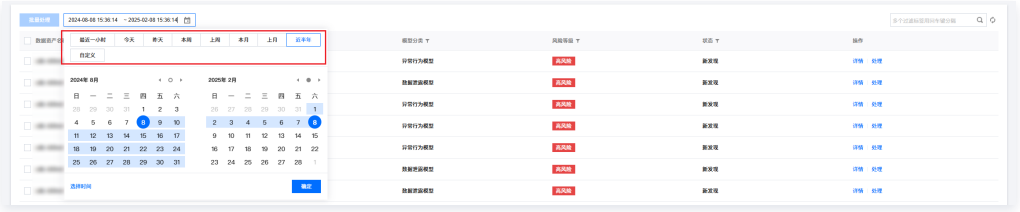
模型风险

最近更新时间：2025-05-26 18:00:22

模型风险基于智能风险模型监测结果进行统计，可以查看详细的风险信息，并支持对风险事件的状态进行更改。

检索模型风险

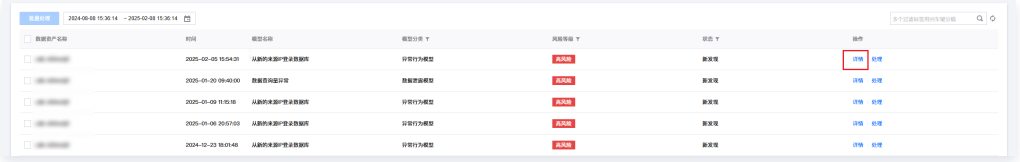
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 风险识别**。
2. 在审计风险页面，单击**模型风险**，进入模型风险页面。
3. 在模型风险页面，可以按最近一小时、今天、昨天、本周、上周、本月、上月、近半年、自定义日期进行风险检索。



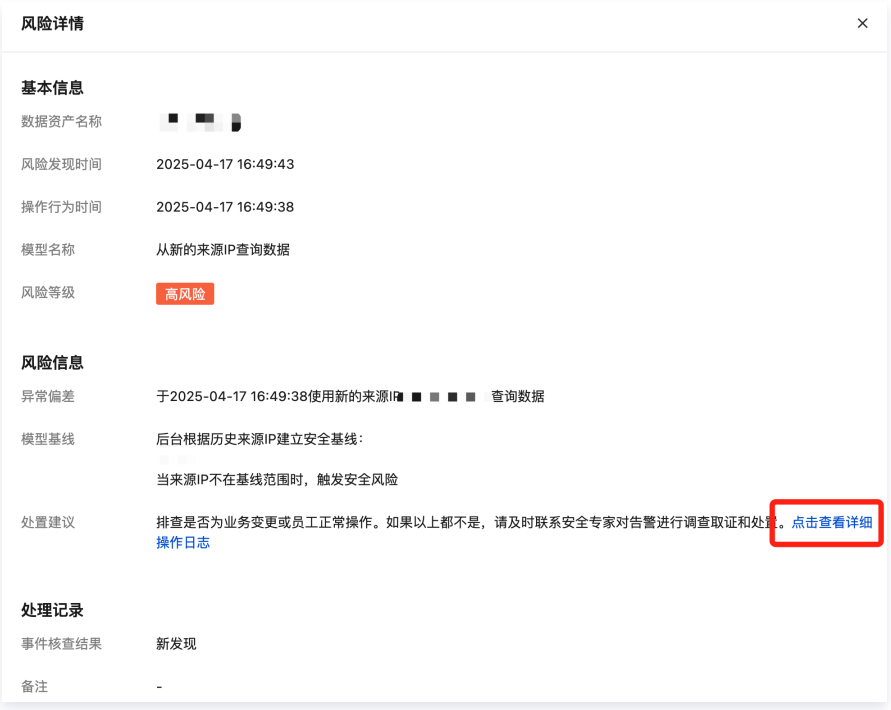
> **说明：**
> 因模型风险需要基于最近7天的时间动态建立基线，所以风险详情识别周期 ≥ 模型开启后7天。

查看模型风险详情

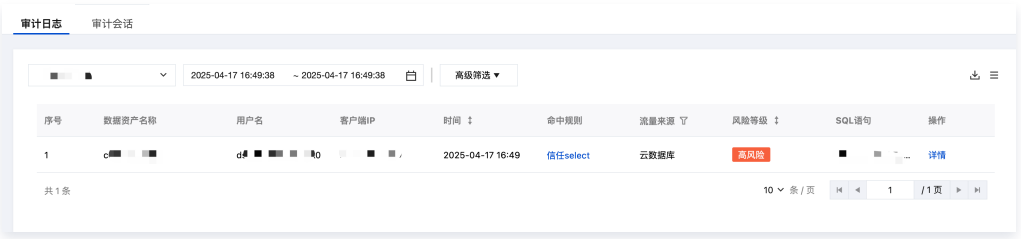
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 风险识别**。
2. 在审计风险页面，单击**模型风险**，进入模型风险页面。
3. 在模型风险页面的列表中，选择需要查看的风险，单击**详情**。



4. 在风险详情页面，可查看该条风险的基本信息、风险信息以及处理记录。



5. 单击**点击查看详细操作日志**，可跳转到对应的审计日志或者审计会话页面。



风险核查

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **风险识别**。
2. 在审计风险页面，单击**模型风险**，进入模型风险页面。
3. 在模型风险页面的列表中，选择需要查看的风险，单击**处理**。
4. 在处理窗口中，依据具体的风险详情进行风险事件核查状态标记，单击**确定**。

审计报表

最近更新时间：2025-05-26 18:00:22

数据安全审计报表提供了多种报表模板，以满足不同的分析需求。这些报表包括综合分析报表、等保参考报表、性能分析报表、语句分析报表、会话分析报表。

新建报表任务

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计报表**。
2. 在报表列表页面，单击**报表任务**，进入报表任务页面。
3. 在报表任务页面，单击**新建任务**。

4. 在新建任务弹窗中，可选择单次报表或周期报表，并配置相关参数。

- **单次报表：**数据安全审计管理系统支持即时生成报表，即生成某个时间段内的报表。

参数说明：

- 任务名称：自定义名称，在64个字符之内，不能重复。
- 报表说明：自定义描述，在256个字符之内。
- 报表模板：当前审计报表支持选择综合分析报表、等保参考报表、性能分析报表、语句分析报表、会话分析报表。
- 包含资产：根据实际需求选择资产。
- 时间范围：根据实际需求选择时间。

- **周期报表：**当重复周期选择定时时，数据安全审计管理系统则定时生成报表。

参数说明：

- 任务名称：自定义名称，在64个字符之内，不能重复。
- 报表说明：自定义描述，在256个字符之内。
- 报表模板：当前审计报表支持选择综合分析报表、等保参考报表、性能分析报表、语句分析报表、会话分析报表。
- 包含资产：根据实际需求选择资产。
- 时间范围：根据实际需求选择时间。
- 重复周期：选择生成报表的周期
- 任务启停：设置任务启动或停止。

查看报表

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计报表**。
2. 在审计列表页面，可查看内容包括报告名称、报表类型等字段。可按照报告名称对报告进行搜索。
3. 单击操作列的**预览**，可查看对应的报表。
4. 单击操作列的**下载**，可下载对应的报表至本地查看。

审计规则

最近更新时间：2025-05-26 18:00:22

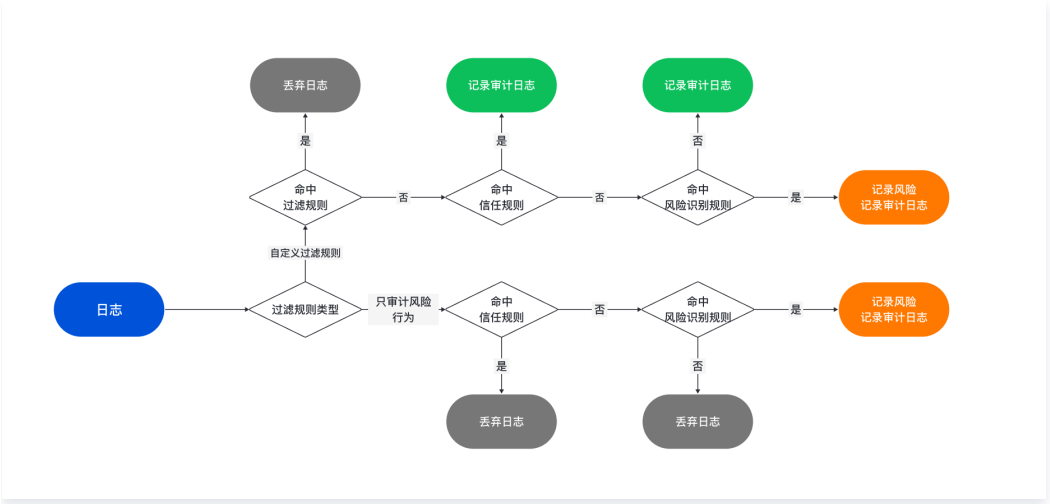
数据安全审计提供审计规则管理功能，您可以直接开启系统内置审计规则，也可自定义审计规则，以实现特性化场景需求。

规则说明

数据安全审计提供三种类型的规则：

类型	应用场景	说明
风险监测（黑名单）	用于检测数据库操作中的异常行为，当出现不符合正常操作模式的行为时触发告警。	使用风险识别规则检测异常操作。审计记录命中配置并启用的风险识别规则时，会触发告警。
信任规则（白名单）	适用于对已知安全、可信任的数据库操作进行定义，以便在审计过程中对这些操作进行特殊处理。 例如：互联网金融行业：对于已备案且合规的第三方支付机构按正常流程进行的资金结算、清算等数据库操作，设定信任规则，确保业务顺畅同时精准审计异常。	使用信任规则可定义您信任的操作。如果您需要审计某类数据库操作，但无需上报告警，您可以为此类数据库操作自定义信任规则，帮助您提高告警准确率。
过滤规则	主要用于筛选出不需要审计的操作，减少无效审计信息，优化审计日志管理。	使用过滤规则可定义您信任的操作。系统不审计您在过滤规则中定义的操作，帮助您提高告警准确率，并节省审计日志存储空间。

审计规则触发匹配的流程如下，通过以下流程处理最终判断和产生审计日志或风险：



规则启用

在规则启用页面，您可以针对数据资产维度，进行规则的启用和禁用。

快捷配置

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计规则**。
2. 在规则列表页面，单击**规则启用**，进入规则启用页面。
3. 在规则启用页面，单击**快捷配置**，弹出快捷配置弹窗。

4. 在快捷配置弹窗，选择需要快捷配置规则的资产（也可选择所有资产），并选择适合的快捷配置组，单击**确定**即可完成配置，配置后将覆盖当前该资产的规则启用配置。

> **说明**
> - 资产开启审计权限时，已默认开启常见配置规则。
> - 规则列表中，规则名称后已添加其所属的常见配置标识。

启用规则

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计规则**。
2. 在规则列表页面，单击**规则启用**，进入规则启用页面。
3. 在规则启用页面，支持启用单个规则或批量启用规则。
   - 单个：选择所需规则，单击规则开关列的，弹出“确认开启”弹窗。

   - 批量：选择一个或多个规则，单击左上角的**启用**，弹出“确认开启”弹窗。
4. 在“确认开启”弹窗中，单击**确定**，即可启用对应规则。

停用规则

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计规则**。
2. 在规则列表页面，单击**规则启用**，进入规则启用页面。
3. 在规则启用页面，支持停用单个规则或批量停用规则。
   - 单个：选择所需规则，单击规则开关列的，弹出“确认关闭”弹窗。

   - 批量：选择一个或多个规则，单击左上角的**停用**，弹出“确认关闭”弹窗。
4. 在“确认关闭”弹窗中，单击**确定**，即可停用对应规则。

规则管理

查看规则

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 审计规则**。
2. 在规则列表页面，可查看系统提供的内置规则和自定义规则。

新建规则

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 审计规则**。
2. 在规则列表页面，单击**新建**，进入新建规则页面，依次配置基础信息、规则定义和输出定义。

- **基础信息**

参数		参数说明
规则类型	风险监测（黑名单）	使用风险识别规则检测异常操作。审计记录命中配置并启用的风险识别规则时，会触发告警。
	信任规则（白名单）	使用信任规则可定义您信任的操作。如果您需要审计某类数据库操作，但无需上报告警，您可以为此类数据库操作自定义信任规则，帮助您提高告警准确率。
	过滤规则	使用过滤规则可定义您信任的操作。系统不审计您在过滤规则中定义的操作，帮助您提高告警准确率，并节省审计日志存储空间。
规则名称		自定义规则名称，用于标识具体规则，长度为1-64个字符，不可重复。
规则备注		规则描述信息。
风险等级		规则对应的风险等级，若命中规则，可在 审计风险页面 查看相关低、中、高风险日志信息。
过滤方式	只审计风险行为（命中风险检测规则）	仅对符合风险检测规则的操作进行审计记录，其他操作不记录，聚焦风险行为审计，减少非风险操作日志冗余。
	自定义过滤规则	根据自行设定的条件过滤操作，可灵活指定哪些操作不被审计，进一步精准控制审计范围，节省审计资源 。

> **说明：**
> 若一个资产同时关联“只审计风险行为”过滤规则和自定义过滤规则，仅前者生效。

- **规则定义**：以下三个规则仅作为示例，且规则类型为黑名单，用户可根据自身业务自行配置。

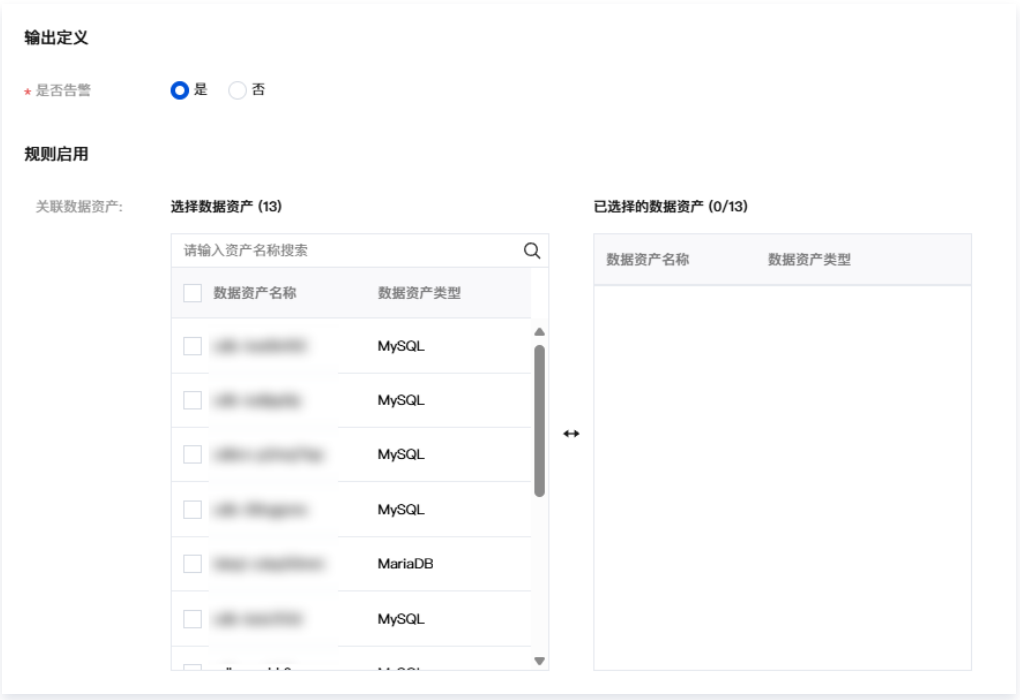
- 防爬取规则：防止使用例如 select 操作语句，爬取表数据。

- 慢查询发现规则：检查执行时间较长的 SQL 语句，便于进行优化。

- 危险操作规则：检查执行 delete、drop、alter 等类型的高危 SQL 语句。


规则定义
客户端:
客户端IP:
包含
可配置多个IP和网段，英文逗号分隔，如：192.168.1.1,192.168
添加
客户端端口:
大于等于
0
添加
客户端主机名:
包含
可配置多个，英文逗号分隔，如：diver,client
添加
使用工具:
包含
可配置多个，英文逗号分隔，如：diver,client
添加
服务端:
数据库IP:
包含
可配置多个IP和网段，英文逗号分隔，如：192.168.1.1,192.168
添加
数据库端口:
大于等于
0
添加
数据库用户:
包含
可配置多个，英文逗号分隔，如：sys,root,system
添加
数据库名:
包含
可配置多个，英文逗号分隔，如：mysql,test
添加
表名:
包含
请输入表名，多个用英文逗号分隔
添加
行为:
操作类型:
包含
drop
添加
操作语句:
包含
请输入操作语句，多个用英文逗号分隔
添加
语句执行:
执行时长:
大于等于
0
毫秒
添加
影响行数:
大于等于
0
行
添加
操作时间:
大于等于
请选择日期
添加
其他:
返回码:
大于等于
0
行
添加

- **输出定义、规则启用**



参数说明：

- 是否告警：根据实际需求选择是否告警。
- 关联数据资产：根据实际需求选择资产。（可选）

3. 配置完成后，单击**确定**即可。

修改规则

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计规则**。
2. 在规则列表页面，找到需要修改的规则，单击**编辑**，进入编辑规则页面。

3. 在编辑规则页面，修改信息后，单击**确定**即可。

删除规则

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营** > **审计规则**。
2. 在规则列表页面，找到需要删除的规则，单击**删除**，弹出确认删除弹窗。

3. 在确认删除弹窗中，单击**确定**即可。

智能分析

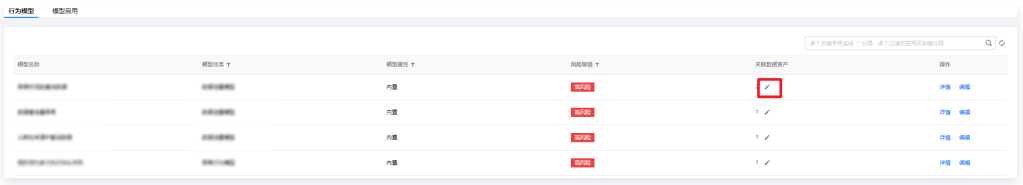
最近更新时间：2025-05-26 18:00:22

行为模型

行为模型通过对用户行为的分析，识别出用户的正常操作模式和行为特征，帮助识别潜在的安全威胁和异常行为。系统内置丰富的行为模型，以满足大多数数据安全场景。

关联 / 取消关联资产

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 智能分析**，进入行为模型页面。
2. 在行为模型页面，选择需要关联资产的行为模型，单击 。



3. 在关联资产页，选择需要关联 / 取消关联的数据资产，单击**确定**即可。

风险等级编辑

1. 在行为模型页面，选择需要查看的行为模型，单击操作栏中的**编辑**。

2. 在编辑模型页面，修改等级后，单击**确定**即可。

查看详情

在行为模型页面，选择需要查看的行为模型，单击操作栏中的**详情** ，即可进入详情页，查看该模型的具体风险信息。

模型启用

在模型启用页面，可以在数据资产维度，进行模型的启用和停用。

启用模型

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**安全运营 > 智能分析**，进入行为模型页面。
2. 在行为模型页面，单击模型启用页签，进入模型启用页面。
3. 在模型启用页面，支持启用单个模型或批量启用模型；
   - 单个：选择所需模型，单击模型开关列的 ，即可启用对应模型。

   - 批量：选择一个或多个模型，单击左上角的**启用**，即可启用对应模型。

停用模型

在模型启用页面，支持停用单个模型或批量停用模型。

- 单个：选择所需模型，单击模型开关列的 ，即可停用对应模型。

- 批量：选择一个或多个模型，单击左上角的**停用**，即可停用对应模型。

智能分析风险查看

智能分析模型开启后，需要有7天的时间动态建立基线，当基线建立后，即可通过 模型风险 查看具体风险内容。

告警管理
告警历史

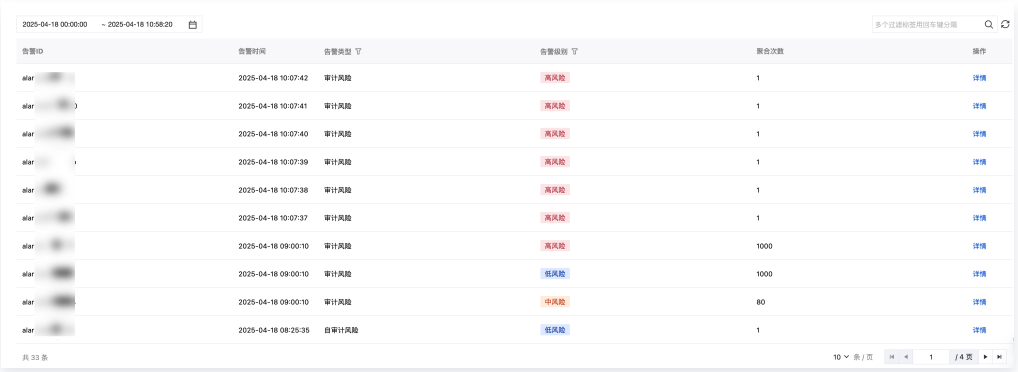
最近更新时间：2025-05-26 18:00:23

用户可以在告警历史页面查看近期收到的告警记录。

> **说明：**
> 支持查看近30天内的告警。

查看告警历史

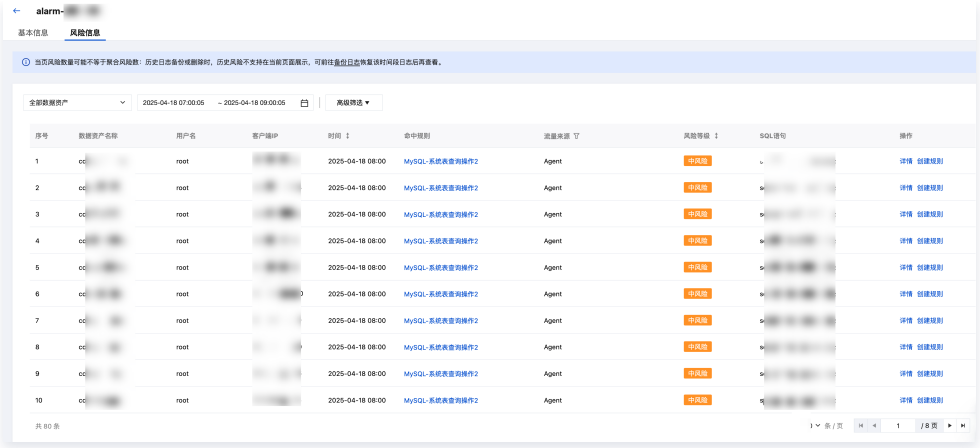
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **告警管理**。
2. 在告警历史页面，可以查看近期收到的告警。支持自定义时间段，以及根据告警类型、告警级别、告警 ID 进行筛选和匹配。
   - 告警 ID：告警记录的唯一ID。
   - 告警时间：该条告警产生的时间。
   - 告警类型：包含审计风险、模型风险、自审计风险、Agent 掉线、QPS 超限、存储超限，支持筛选。
   - 告警级别：包含高风险、中风险、低风险，支持筛选。
   - 聚合次数：表示该告警包含的风险数。若为实时风险触发的告警，聚合次数为 1；若为聚合后发出的告警，则记录了时段内包含的风险个数。



查看风险详情

1. 在 告警历史页面，选择目标告警，单击操作列的**详情**。
2. 在告警详情页，单击**基本信息**，查看告警的基本信息，包括告警时间、告警类型、告警级别、风险数量。

3. 在告警详情页，单击**风险信息**，在风险信息页面，详细的记录了该告警中的风险详情。包含审计风险和模型风险。您可以在风险信息内直接对相应风险进行查看和处置。
   - 审计风险告警关联的风险信息示例：



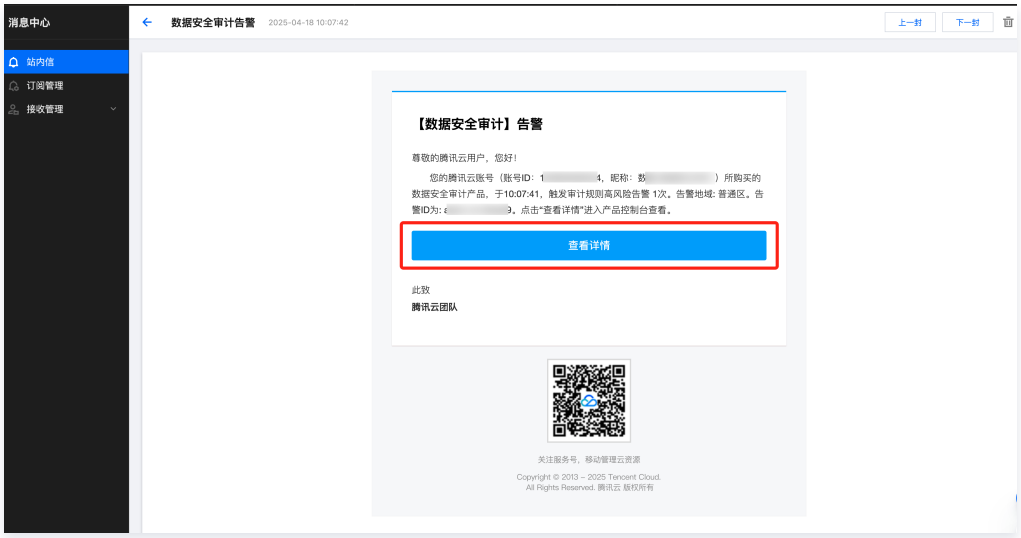
- 模型风险告警关联的风险信息示例：

告警跳转

用户可以通过收到的告警内的链接直接跳转到对应页面。

> **说明：**
> 支持站内信、邮件内容的告警跳转。

1. 在站内信页面，用户可以查看风险触发的告警信息。



2. 单击**查看详情**，可以跳转到告警相关页面，并通过告警 ID 自动定位到对应告警。可以参考上文进行告警详情的查看和处置。

说明：

1. 对于审计风险、模型风险、自审计风险，会跳转到**告警历史**页面，方便您进行告警处置。
2. 对于 Agent 掉线风险，会跳转到 **Agent 管理**页面，您可重新进行 Agent 部署。
3. 对于 QPS 超限风险、存储超限风险，会跳转到**概览**页面，您可查看当前 QPS 和存储情况。

告警设置

最近更新时间：2025-05-26 18:00:23

触发告警时，数据安全审计会根据配置的告警规则向指定用户发送告警通知。

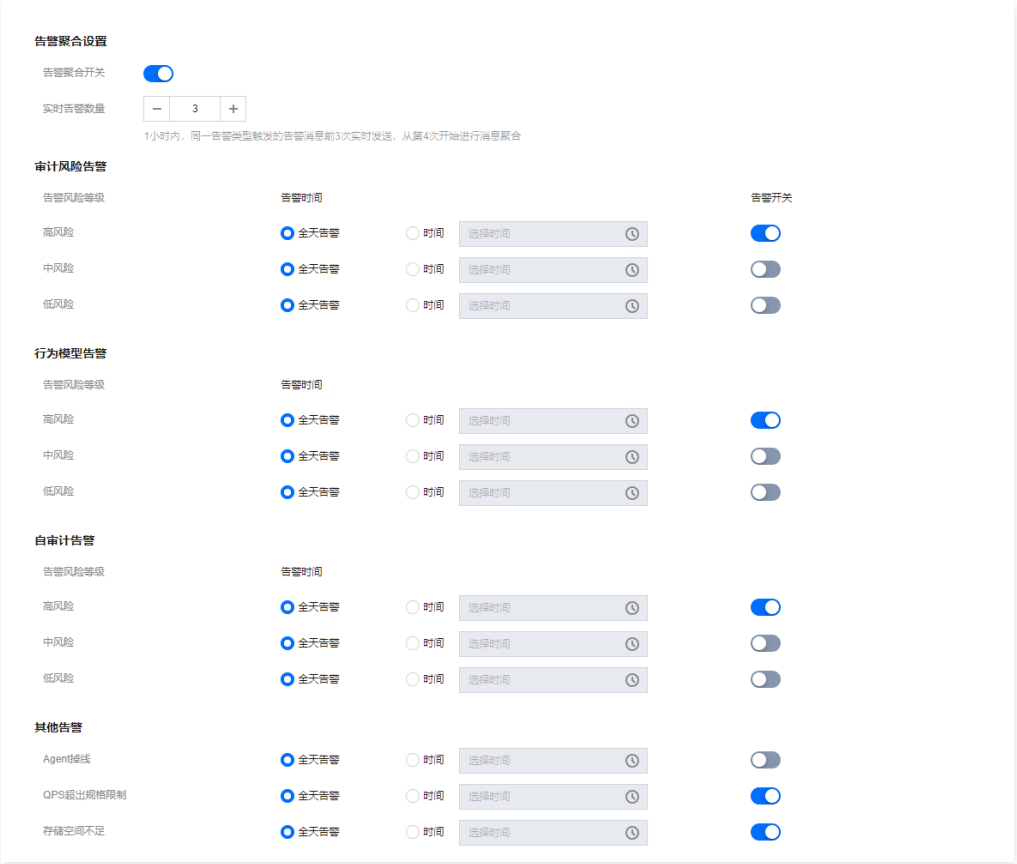
> **说明：**
> 支持微信，站内信，邮件接收告警通知。

前提条件

已开启事件告警通知，详情请参见 消息订阅管理 。

操作步骤

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **告警管理**。
2. 在告警历史页面，单击**告警设置**，进入告警设置页面。
3. 在告警设置页面，可按告警类型/等级设置告警时间。
   - 告警聚合设置：为应对告警风暴，您可以通过设置实时告警数量，将一小时内超过阈值的多个告警事件进行聚合通知。
   - 配置告警条件：根据审计规则和策略，配置相应的告警条件，单击告警开关 即可开启或关闭相应策略的告警通知。
   - 设置告警时间：根据实际需要，设置告警的时间范围和频率，默认全天告警，同时可进行接收通知时间范围的自定义配置。



> **注意**
> - 请确认消息订阅中“告警消息-安全告警通知”已打开，进入 消息订阅页面 设置。
> - 同一操作触发的告警消息超过设定的阈值时，超出阈值的告警信息将会聚合发送。

Agent 管理

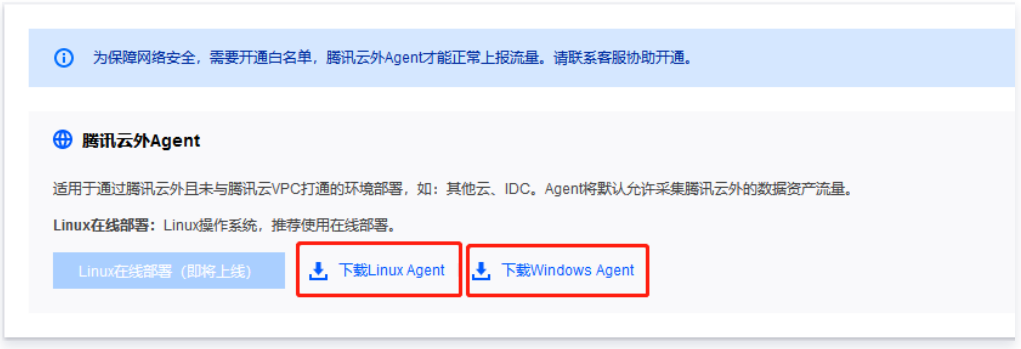
最近更新时间：2025-05-26 18:00:23

Agent 部署

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **Agent 管理**，进入 Agent 部署页面。
2. 在 Agent 部署页面，根据数据资产添加位置，提供下载链接。配置步骤以及配置注意事项，详情请参见 Agent 部署 。
3. 在 Agent 部署页面，分为腾讯云内网 Agent 和 腾讯云外 Agent。

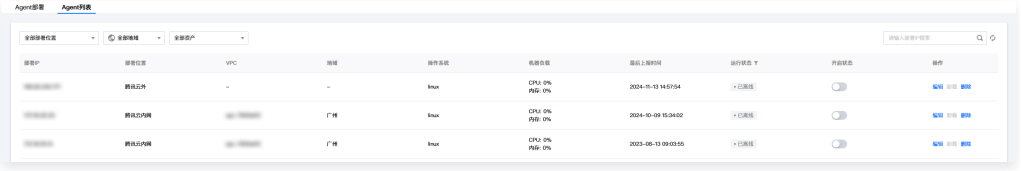
- 腾讯云内网 Agent
  数据资产为腾讯云内资产（关系型云数据库、NoSQL 云数据库、企业分布式云数据库、自建数据库），优先选择 Linux 在线部署，同时也可选择下载 Linux Agent 或下载 Windows Agent 后进行部署。

- 腾讯云外 Agent
  数据资产为腾讯云外资产（腾讯云外数据库）。即可下载 Linux Agent 或下载 Windows Agent。

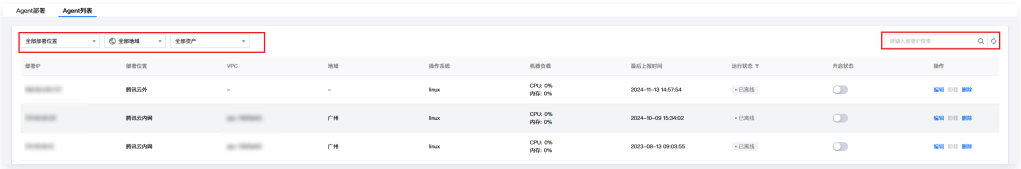


Agent 列表

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **Agent 管理**，进入 Agent 部署页面。
2. 在 Agent 部署页面，单击 **Agent 列表**，进入 Agent 列表页面。
3. 在 Agent 列表页面，可以查看所有已配置成功的 Agent。Agent 列表默认展示内容包括：部署 IP、部署位置、VPC、地域、操作系统、机器负载、最后上报时间、运行状态、开启状态及相关操作。



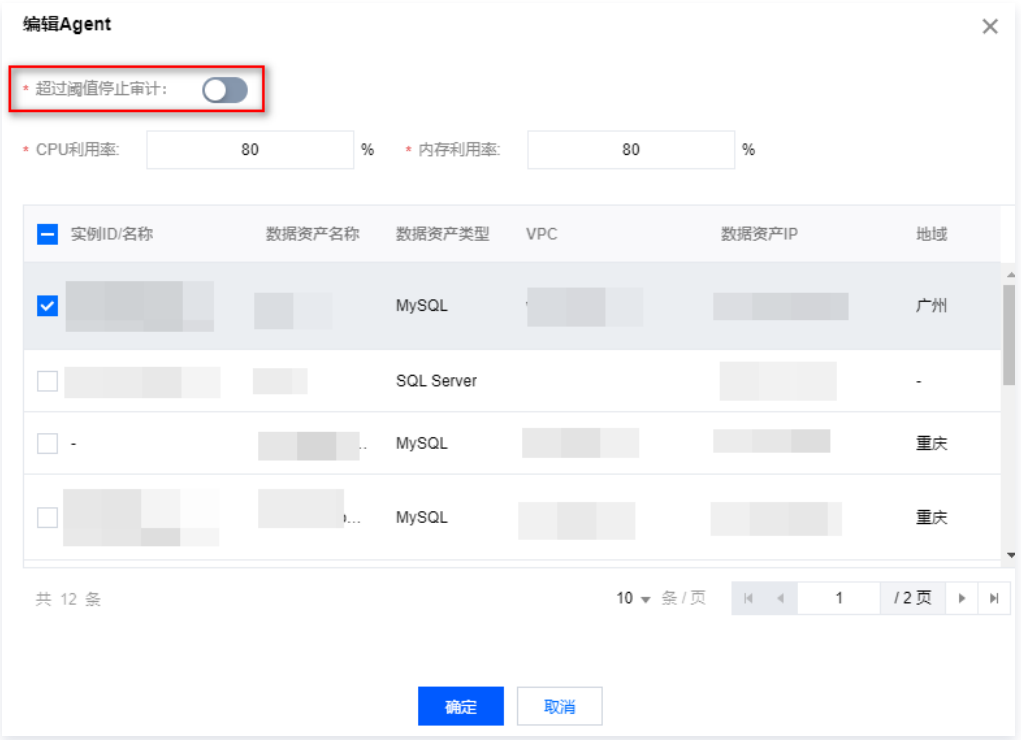
4. 在 Agent 列表页面，您可以按**部署位置**、**地域**、**数据资产**、**部署 IP**、**运行状态**对 Agent 进行搜索。



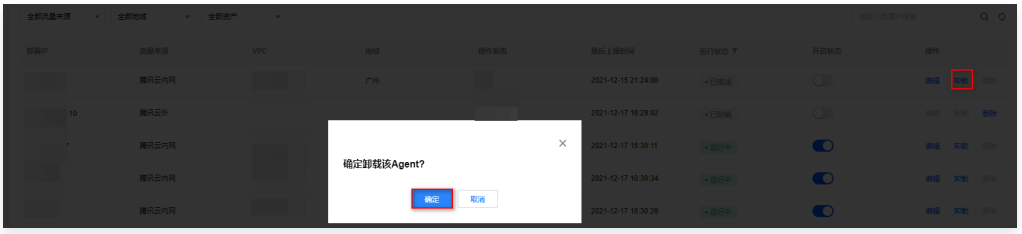
5. 在 Agent 列表页面，选择所需部署 IP，单击**编辑**，可以查看和修改 Agent 配置相关信息。

> **说明**

设置停止审计阈值。为尽最大可能保证业务运行不受影响，您可以设置基于 CPU 与内存使用率的阈值，当 Agent 宿主机性能超过阈值时，Agent 并暂停流量采集，待宿主机性能降回阈值以下时再恢复采集。如您要求 Agent 任何情况都进行工作，可将负载检测开关关闭，Agent 将持续审计数据。



6. 在 Agent 列表页面，选择所需部署 IP，单击**卸载** > **确定**，等待卸载完成后，单击**删除**即可删除该部署 IP。

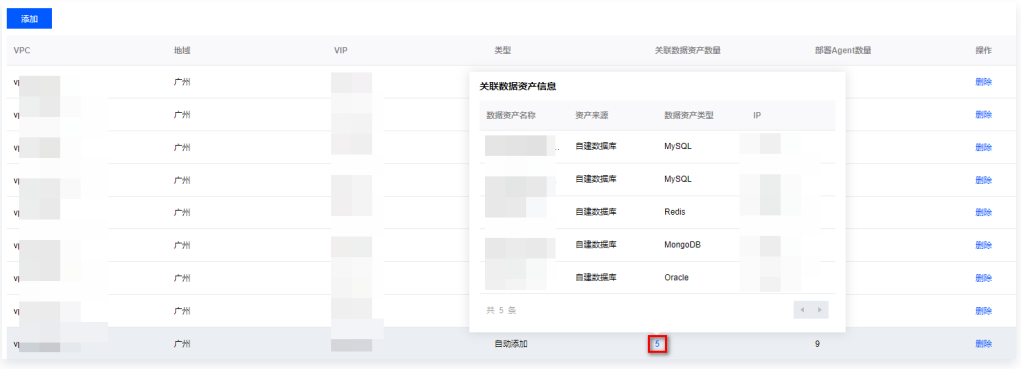


网络管理

最近更新时间：2025-05-26 18:00:23

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **网络管理**。
2. 在 VPC 通道列表中，显示 VPC、地域、VIP（Virtual IP）、添加类型、关联数据资产数量和部署 Agent 数量。

3. 如需具体查看同一 VPC、地域下的关联数据资产，单击关联数据资产数量栏下的**数字**，即可查看。



4. 用户可自主添加新的 VPC 通道列表。单击**添加**，即可弹出添加 VPC 通道弹窗。

5. 选择对应的地域、VPC 和子网 IP，单击**确定**即可完成添加。添加完成将在所选子网下创建名称以“DSAudit_”开头的终端节点，并占用一个 IP 地址。
6. 某些 VPC 通道若不再需要，可单击操作列的**删除**，经二次确认后，即可销毁该 VPC 通道。

> **说明**
> 删除后，将无法采集部署在该 VPC 的 Agent 流量。该 VPC 内的数据资产将无法审计。

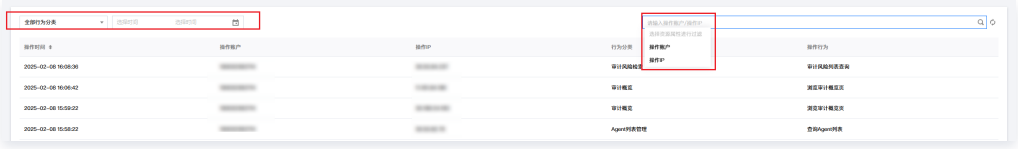
自审计

最近更新时间：2025-05-26 18:00:23

检索操作日志

操作日志负责审计数据安全审计账户的操作，能够浏览账户操作日志列表并对行为规则进行配置。

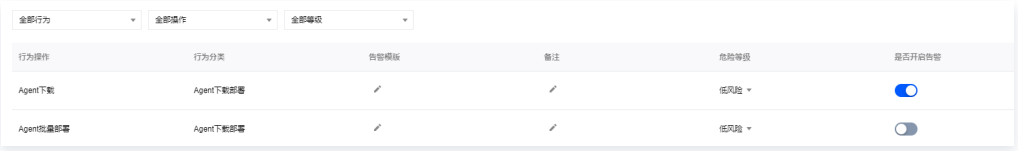
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **自审计**，进入操作日志页面。
2. 在操作日志页面，您可以根据行为分类、操作时间、操作账户、操作 IP 检索查看操作完整信息。



行为规则配置

1. 登录 数据安全审计控制台，在左侧导航栏中，单击**系统管理** > **自审计**，进入操作日志页面。
2. 在操作日志页面，单击行为规则配置页签，进入行为规则配置页面。
3. 在行为规则配置页面，显示行为操作、行为分类、告警模板、备注、危险等级及是否开启告警。您可根据行为分类、行为操作及危险等级搜索查看相关配置信息。

> **说明**
> 所有数据由系统内建生成，用户可以根据需求进行修改。



字段说明：

- 行为操作：用户对系统各个账户的功能操作。
- 行为分类：用户对系统功能操作所属的模块名。
- 告警模板：用户执行操作时邮件所发送的告警内容，单击 ，可修改告警模板。
- 备注：用户对行为规则的进一步说明，单击 ，可修改备注说明。
- 危险等级：对用户操作行为的评级，可设置行为危险等级，包括低风险、中风险及高风险。
- 是否开启告警：单击 开启后，触发行为规则审计，则会发送告警信息，单击 关闭后，只会记录操作，不会发送告警信息。

数据安全审计传统型
v5.1.0
系统管理
系统资源监控

最近更新时间：2021-09-28 11:13:36

以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击**系统资源监控**，即可进入资源监控页面，该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。

系统详细信息

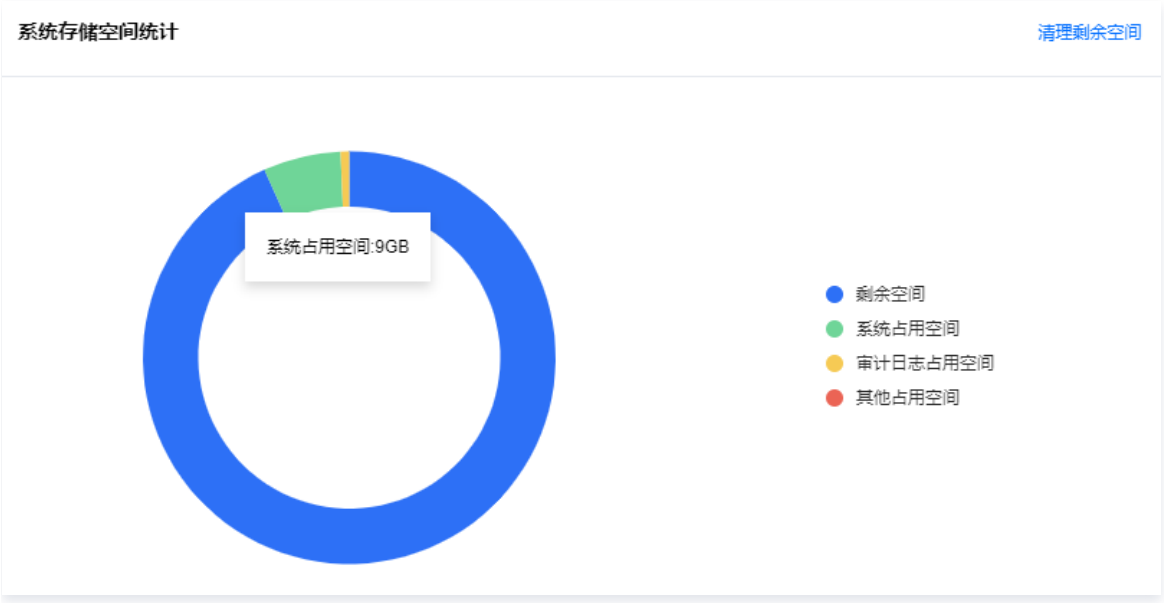
系统详细信息包含系统产品名称、系统版本、产品规格、已用/总数据资产数、连续运行时长、购买峰值流量、系统当前时间参数信息。

系统存储空间统计

存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角，单击**清理剩余空间**，将清理的数据包含所选的日期。例如，选择了12月1日至12月3日，则会删除12月1日、2日、3日，3天的数据。

> **说明**
> 统计报表将磁盘空间分为四个类型：

- 剩余空间：数据安全审计实例存储剩余空间；
- 系统占用空间：数据安全审计自身代码所占存储空间；
- 审计日志占用空间：数据安全审计记录的数据库操作信息日志占用空间；
- 其他占用空间：数据安全审计实例其他代码、配置文件占用空间。



流量走势实时统计

流量走势实时统计能统计一定时间跨度（最近 30 分钟、最近 24小时、最近 7 天）内数据安全审计中所审计的所有数据库的 QPS，确认全网 QPS 峰值是否超过购买峰值，以帮助管理员了解数据安全审计性能状况，及时扩容升级产品。

用户管理

最近更新时间：2025-05-29 09:43:32

以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中单击**用户管理**即可进入用户页面。

查看账号信息

账号管理用于管理 DSA（Data Security Audit）实例所有账号。系统管理员可以通过列表查看所有账号信息，包括所属角色、真实姓名、创建日期以及联系方式等。

说明

- 密码有效期为90天，密码规则如下所示：
- 密码长度：在12-20位字符数以内。
- 复杂度：至少包含以下 3 类字符 小写字母（a-z）、大写字母（A-Z）、数字（0-9）、特殊符号（~!@#$%^&*()_+-=|{}[];:'<>,.?）。
- OTP（One-Time Password）二维码：如需开启 OTP 实现登录双重验证，可在相应账号右侧操作栏，单击 **OTP二维码**，或在数据安全审计管理页面右上角，找到管理员账号下的 OTP 验证，单击 **OTP二维码**，查看原图并扫描动态校验码。

添加账号

如需要增加管理员账号，单击**添加账号**，在弹框中填写账号信息，选择所属角色后，单击**确定**即可。

修改和删除账号

如需对账号进行修改或删除，可在相应账号操作列单击**编辑**或**删除**对账号进行调整。

> **注意**
>
> 系统默认创建账号不可删除。

OTP 设置

最近更新时间：2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验，并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

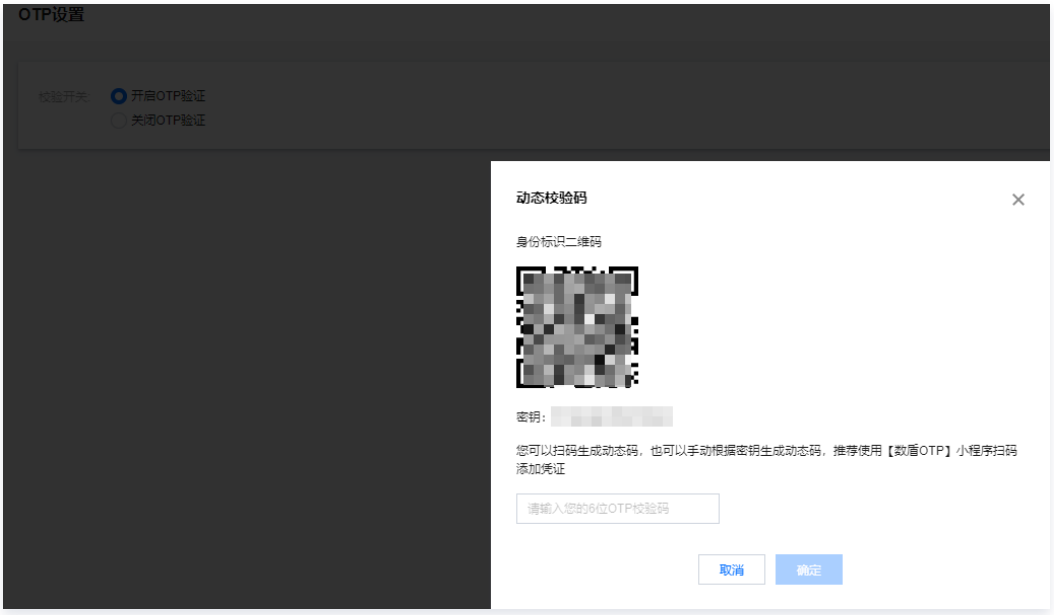
1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击 **OTP 设置**，即可进入 OTP 设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在 OTP 设置页面，设置校验开关，如需开启 OTP 验证选项，选中开启 OTP 验证，出现弹窗，根据提示扫 OTP 码，输入正确的 OTP 码，单击**确定**，退出登录系统即可。

> **说明**
> 建议开启 OTP 验证之前，提前通知各管理员登录系统扫描 OTP 验证二维码，避免其无法登录该系统。



4. 再次登录数据安全审计管理页面，需要输入OTP 校验码。

告警设置

最近更新时间：2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警，告警支持邮件告警、syslog 告警、短信告警、企业微信告警，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击**告警设置**，即可进入告警设置页面。

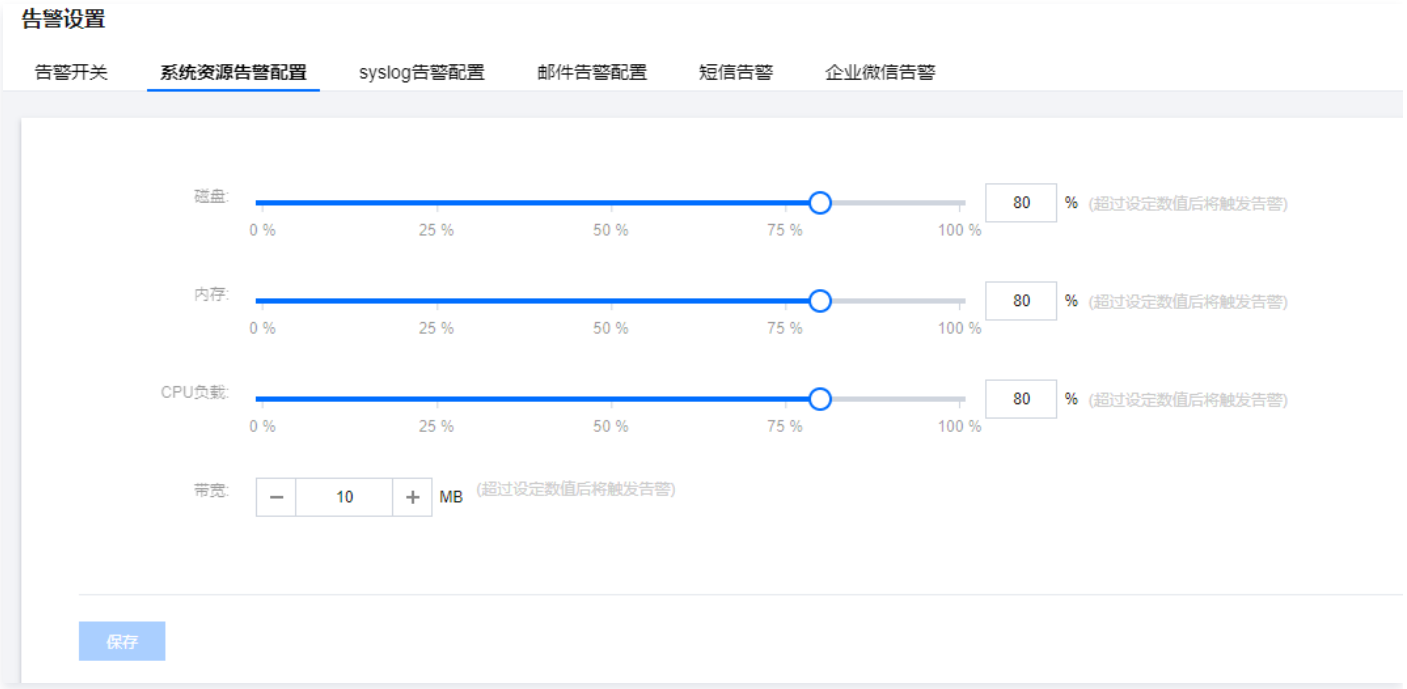
> **说明：**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在告警设置页面，分别对告警开关、系统资源告警配置、syslog 告警配置、邮件告警配置、短信告警及企业微信告警功能进行设置。

- **告警开关**
  在告警设置页面，单击**告警开关**，分为**告警方式**和**告警内容**，打开需要开启告警的选项，单击**提交**，即可对 syslog 告警配置 中所设置的服务器进行监控，且当满足告警条件时，将触发告警，并发送邮件至您所 配置的告警邮箱 中。

> **说明：**
> 若需要接收告警信息，需打开邮件告警开关，且已在 邮件告警配置 中设置告警接收邮箱，否则无法接收告警信息。

- **系统资源告警配置**
  在告警设置页面，单击**系统资源告警配置**，设置系统资源告警的触发条件，可将磁盘、内存、CPU 负载在0 – 100%之间调整，可自定义带宽值，单击**提交**，即可对 syslog 告警配置 中所设置的服务器进行监控。



- **syslog 告警配置**

> **注意：**
> 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面，单击**syslog 告警配置**，输入需要记录的 syslog 服务器 IP 和端口，单击**提交**，即可完成 syslog 告警条件配置，设置完成后将监控所配置的服务器。

- **邮件告警配置**

单击**邮件告警配置**，依次填入邮件服务器的相关配置信息，如需添加多个收件人，请以英文分号分隔，填写完成后，单击**提交**，当满足告警条件时，将发送邮件至所配置的邮箱中。

> **说明：**
> 若填写 QQ 邮箱账号，密码需填写所设置的邮箱密码。

- **短信告警设置**

  单击**短信告警**，依次填写短信告警设置相关配置信息。如需添加多个手机号，单击添加，填写完成后，单击**保存**，当满足告警条件时，将发送信息至所配置的

手机号中。

- **企业微信告警**

  单击企业微信告警，填写相关配置信息，单击保存，当满足告警条件时，将发送信息至所配置的企业微信中。

备份服务器设置

最近更新时间：2025-05-27 16:30:32

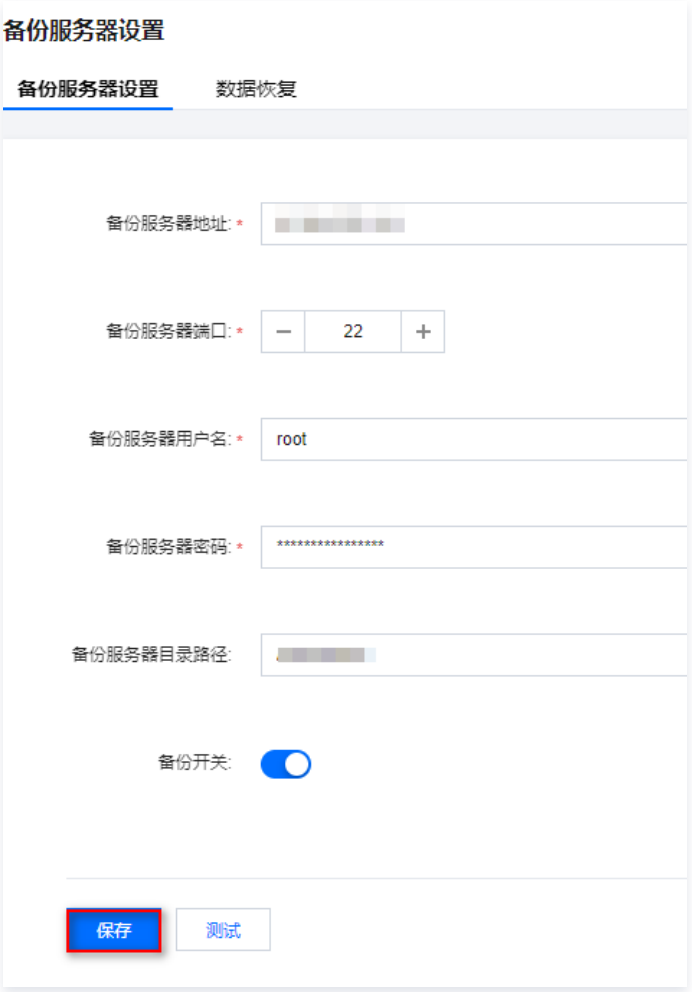
1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击**备份服务器设置**，即可进入备份服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在备份服务器设置页面，依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径，打开备份开关，单击**保存**即可完成备份服务器设置。

> **说明**
> - 备份服务器地址需为公网 IP 地址，并且入站安全组是放通状态，详情请参见 添加安全组规则 。
> - 备份服务器通过 SSH 的方式进行备份，备份服务器设置成功后，系统每日02:00（UTC+8）定时备份前一天的数据到目标机器目录。



4. 设置完成后，数据安全审计管理系统中的数据将会按照设置路径进行备份。
5. （可选）如需恢复之前存在的数据，在备份服务器设置页面，单击**数据恢复**页签。

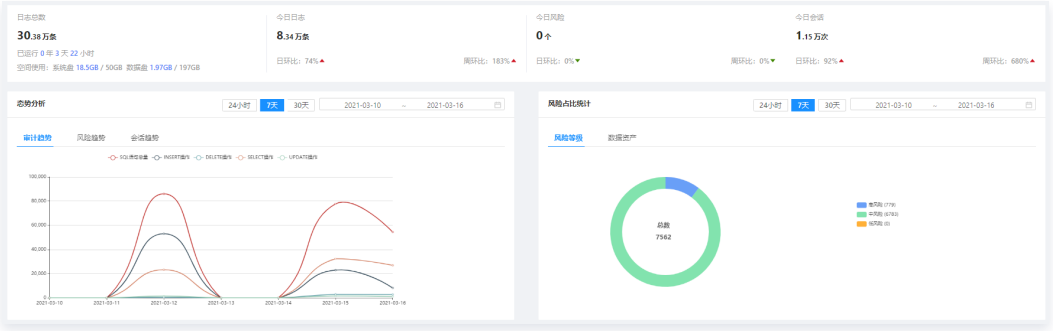
6.（可选）在数据恢复页签中，单击**数据恢复**，选择恢复日期并导入恢复数据即可。

审计管理
安全审计与分析
审计数据

最近更新时间：2025-05-27 16:30:32

审计概览

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**安全审计与分析 > 审计概览**，即可进入审计概览页面。
3. 在审计概览页面中，可总览全网数据库日志信息，态势分析，风险占比以及查询单个数据库资产详细信息，如需了解数据库资产审计详细内容，可在审计概览页面下方查询详细信息。
   - **日志总数**：用于统计全网各数据资产日志总数。
   - **今日日志**：用于统计全网各数据资产今日日志总数。
   - **今日风险**：用于统计全网各数据资产今日风险总数。
   - **今日会话**：用于统计全网各数据资产今日会话总数。
   - **态势分析**：可查看您所配置的审计单元的审计趋势，风险趋势，会话趋势，还可按照高风险、中风险、低风险进行查看各个风险级别详细数据，每个报表可展示三种走势图及三类风险级别数据：
     - **审计趋势**：用于展示数据资产的审计单元语句压力，展示时间有24小时、7天、30天。
     - **风险趋势**：用于展示数据资产的审计单元高中低三类风险的统计信息，展示时间有24小时、7天、30天。
     - **会话趋势**：用于展示数据资产的审计单元各类会话信息，展示时间有24小时、7天、30天。
   - **风险占比统计**：用于显示数据资产对应的命中风险等级。
     - **风险等级**：用于展示数据资产审计单元有关的自定义规则命中风险信息，展示时间有24小时、7天、30天。
     - **数据资产**：用于展示被命中的数据资产，展示时间有24小时、7天、30天。
   - **资产审计**：主要展示单个数据资产的会话总数，DDL 操作数量、失败会话数量、最大并发会话及风险数等信息。



日志检索

日志检索主要提供日志查询与导出功能。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**安全审计与分析>审计日志**，即可进入审计日志页面。
3. 管理员通过 审计概览 定位到疑似有风险的数据资产，或者企业网络已经发生数据库安全问题时，可在日志检索页面查询并导出日志信息。

日志查询

在日志检索页面，您可以按照数据资产、风险等级、用户名、命中规则及时间，对日志进行查询。

查看数据详情

在日志列表中，可单击某条记录查看其详细内容。

日志导出

检索出需要导出的数据，现已支持不限数量导出，在列表上方单击 ，弹出导出数据弹窗，单击**确定**即可将数据导出，导出文件类型为 Excel（.xlsx格式）。

> **注意**
> 尽量缩小导出范围，导出数量过多，会影响服务器性能。


Excel文件生成
导出记录16,075,835条，确认要导出吗?
注：尽量缩小范围导出，导出数量过多，会影响服务性能
取 消
确 定

规则配置

最近更新时间：2025-05-27 16:30:32

规则配置页面可配置触发风险告警的命中规则。数据安全审计已提供17个内置规则，可满足大多数安全场景，内置规则不可删除、不可编辑。您也可以根据业务需要，添加自定义规则，下面将为您详细介绍配置操作。

操作步骤

以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择**安全审计与分析** > **规则配置**即可进入规则配置页面。

新建规则

如需自定义规则满足个性化审计需求，单击**添加规则**，进入新建规则页面，填写规则名称等，单击**保存**即可。

> **注意**
> - 规则配置支持同一规则配置多个条件，多个条件之间为 “与” 关系，必须全部匹配才能够触发规则和告警。
> - 自定义规则默认为黑名单，触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计单元的存储空间，指定部分操作行为不记录不入库，可在规则中指定相关操作后，选择 “白名单” 选项，并且将告警选项都取消。

以上操作完成后，即可实现白名单类型规则配置，减少误报、减轻数据安全审计的审计单元存储压力。

- **规则示例**
  在规则配置页面，单击**添加规则**，按下图配置规则，表名和阈值根据您的业务场景自行设定，单击**保存**即可。

- **规则配置建议**
  以下三个建议规则仅作为示例，用户可根据自身业务自行配置。

- **防爬取规则**：防止使用例如 select 操作语句，爬取表数据。

> **注意**
> 影响行数可以根据业务自行配置。

- **慢查询发现规则**：检查执行时间较长的 SQL 语句，便于进行优化。

> **注意**
> 执行时间可以根据业务自行配置。

- **危险操作规则**：检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

修改规则

在规则列表中，找到需要修改的规则，在右侧操作栏中，单击**编辑**，修改信息后单击**保存**即可。

删除规则

在规则列表中，找到需要删除的规则，在右侧操作栏中，单击**删除**，再单击询问窗**确定**即可。

审计报表

最近更新时间：2025-01-10 19:17:22

审计报表功能主要展示所有配置过的审计组数据，并提供搜索、查看及 PDF 下载功能，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**安全审计与分析** > **审计报表**，即可进入审计报表页面。

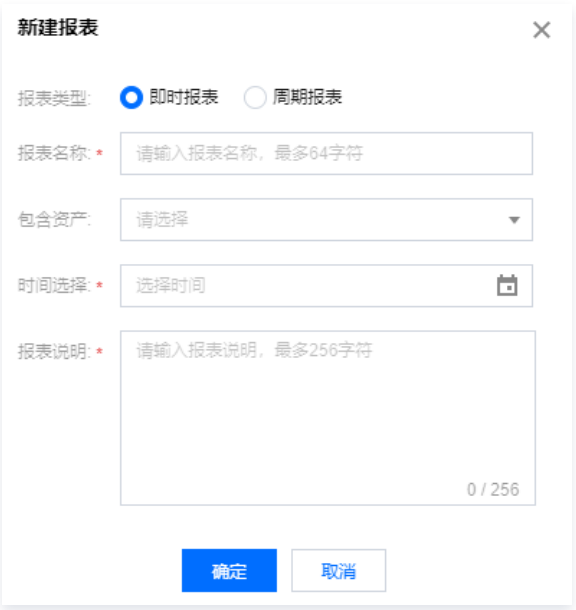
> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在审计报表页面中，可查看内容包括报告名称、报告说明及发送目标等字段，同时可以进行相关操作，每个页面默认展示20条数据，可按照报告名称、生成方式、开始时间及结束时间，对报告进行搜索，还可下载 PDF 报告。

- **定时生成报表**
  数据安全审计管理系统支持定时生成报表。
  在报表上方单击**新建报表**，弹出新建报表弹窗，选择“周期报表”，并依次输入模板名称、重复周期（可选择定时执行、每天、每周、每月）、执行时间（精确到时分秒）、报告说明，设置完成后，单击**确定**，即可在您设定的执行时间定时生成报表。

- **即时生成报表**
  数据安全审计管理系统支持即时生成报表，即生成某个时间段内的报表。
  在报表上方单击**新建报表**，弹出新建报表弹窗，选择“即时报表”，依次输入报告名称、包含资产、时间选择、报告说明，单击**确定**，即可输出您规定的时间范围内的报表。

> **注意**
> 开始时间应早于结束时间。


新建报表
报表类型:
即时报表
周期报表
报表名称: *
请输入报表名称，最多64字符
包含资产:
请选择
时间选择: *
选择时间
报表说明: *
请输入报表说明，最多256字符
0 / 256
确定
取消

数据资产与 Agent

最近更新时间：2025-05-27 16:30:32

Agent 下载

1. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择**数据资产与Agent > 审计用Agent**，即可进入审计用 Agent 页面。
2. Agent 部署。在审计用 Agent 页面，选择 **Agent 下载 > 添加**，可配置审计 Agent 的各类参数并提供下载链接，配置步骤以及配置注意事项，请参见 Agent 部署 。
3. 添加完成 Agent 后，在 Agent 配置页面，可查看所有已正确安装且能实现 DSA（Data Security Audit）实例网络互通的 Agent 信息。

列表各字段含义如下：

- Agent 名称：用于配置该 Agent 的名称。
- 审计服务 IP： Agent 回传数据的源 IP。
- 审计服务端口：该 Agent 配置的审计端口。
- 数据库资产：可查看该 Agent 审计的数据库的所有 IP 地址。
- 操作：用于下载该 Agent 的链接。
  - 在右侧操作栏，选择**下载 > 下载 Linux Agent**或**下载 Windows Agent**，弹出部署 IP 窗口，单击**确定**即可开始下载 Agent 。

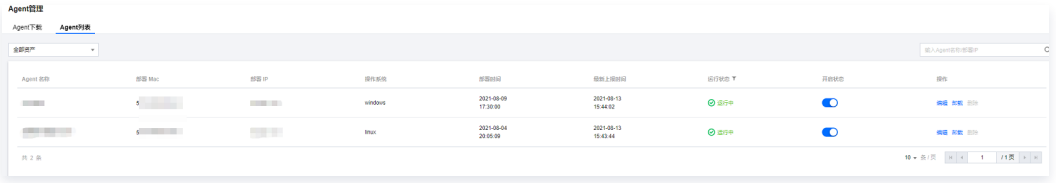
> **注意**
> - 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11，必须勾选下方说明，否则无法部署 Agent。
> - 请添加安装包需要部署机器的 IP 或 IP 列表。
> - 如未添加 IP 信息却部署了会导致 Agent 无法启动。
> - 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

  - 在右侧操作栏，选择**下载 > Linux 批量部署** ，输入部署地址，支持按 IP 或按 IP 段部署，支持添加多行，输入服务器 IP 、SSH 端口号、用户名、密码， 输入完成后单击**确定**即可。

- 在右侧操作栏，单击**删除**，可删除该条 Agent 信息。

Agent 列表

1. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择**审计用 Agent > Agent 列表**，即可进入审计列表中。
2. 在审计列表中，可以查看所有已配置的 Agent。Agent 列表默认展示内容包括：Agent 名称、部署 Mac、部署 IP、操作系统、部署时间、最新上报时间、运行状态、开启状态及相关操作。
   - **搜索**：您可以按数据资产、Agent 状态、Agent名称、IP、对 Agent 进行搜索。
   - **查看 Agent 配置详情**：在“操作”栏中，单击**编辑**，可以查看 Agent 配置相关信息。
   - **相关操作**：在右侧操作栏，可以对 Agent 进行启动、停止、编辑、卸载、删除的相关操作。



操作日志管理

最近更新时间：2025-01-10 19:17:22

操作审计员负责审计数据安全审计各管理员的操作，防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后，能够阅览管理员操作日志列表并对行为规则进行配置。

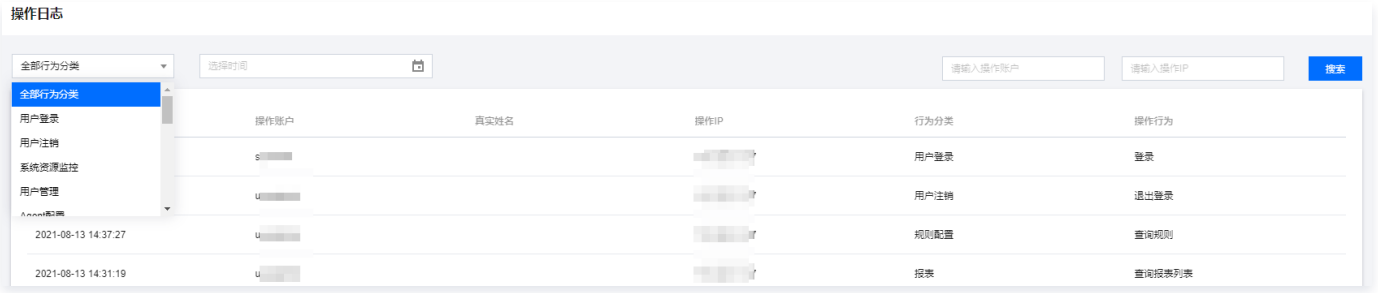
日志检索

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入操作日志页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在操作日志页面，您可以根据操作事件、操作 IP、行为分类、操作时间检索还原非法操作完整信息。



行为规则配置

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**操作日志**，即可进入行为规则配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在行为规则配置页面，可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作，同时可按照行为分类、行为操作及危险等级，对行为规则进行搜索。

> **说明**
> 所有数据由系统内置生成，用户可以根据需求进行修改。

字段说明：

- **行为操作：用户对系统各个账户的功能操作。**
- **行为分类：用户对系统功能操作所属的模块名**
- **告警模板：用户执行操作时邮件所发送的告警内容**
- **备注：用户对行为规则的进一步说明。**
- **危险等级：对用户操作行为的评级，可设置行为危险等级，包括低级、中级及高级。**
- **是否开启告警：用户开启后，触发行为规则审计，则会发送告警信息，关闭后，只会记录操作，不会发送告警信息。**
- **操作：在告警模板操作栏，单击 ，即可对行为操作信息进行修改。**

v5.0.8
系统管理
系统资源监控

最近更新时间：2021-08-06 10:22:15

以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【系统资源监控】，即可进入资源监控页面，该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。

系统详细信息

系统详细信息包含系统产品名称、产品规格、当前版本等基础信息，以及数据安全审计总审计单元数参数信息。

系统存储空间统计

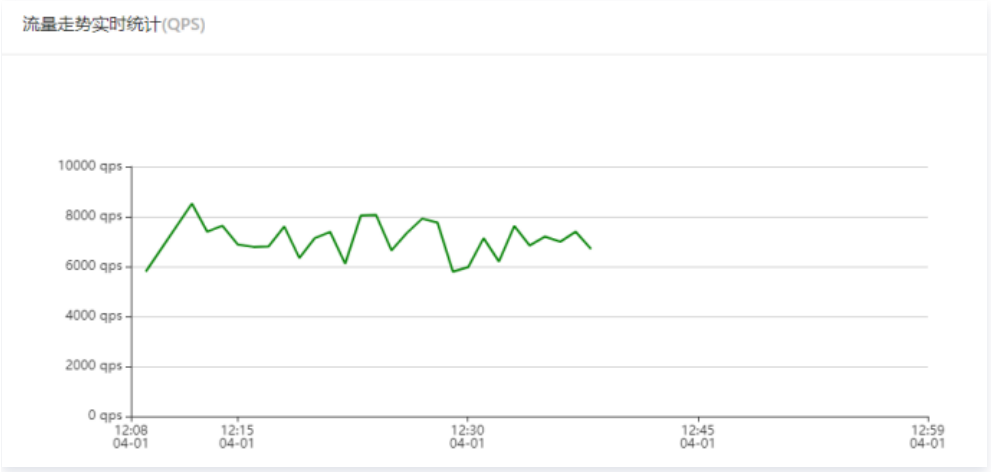
存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角，单击【清理剩余空间】，将清理的数据包含所选的日期。例如，选择了12月1日至12月3日，则会删除12月1日、2日、3日，3天的数据。

> **说明**
> 统计报表将磁盘空间分为四个类型：

- 剩余空间：数据安全审计实例存储剩余空间；
- 系统占用空间：数据安全审计自身代码所占存储空间；
- 审计日志占用空间：数据安全审计记录的数据库操作信息日志占用空间；
- 其他占用空间：数据安全审计实例其他代码、配置文件占用空间。

流量走势实时统计

流量走势实时统计能统计一定时间跨度（最近 30 分钟、最近 24小时、最近 7 天）内数据安全审计中所审计的所有数据库的 QPS，确认全网 QPS 峰值是否超过购买峰值，以帮助管理员了解数据安全审计性能状况，及时扩容升级产品。



用户管理

最近更新时间：2025-05-27 16:30:32

以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中单击【用户管理】即可进入用户页面。

查看账号信息

账号管理用于管理 DSA 实例所有账号。系统管理员可以通过列表查看所有账号信息，包括所属角色、真实姓名、创建日期以及联系方式等。

> **说明**
> OTP 二维码：如需开启 OTP 实现登录双重验证，可在相应账号右侧操作栏，单击【OTP二维码】，或在数据安全审计管理页面右上角，找到管理员账号下的 OTP 验证，单击【OTP 验证】，查看原图并扫描动态校验码。

添加账号

如需要增加管理员账号，单击【添加账号】，在弹框中填写账号信息，选择所属角色后，单击【确定】即可。

修改和删除账号

如需对账号进行修改或删除，可在相应账号操作列单击【编辑】或【删除】对账号进行调整。

> **注意**
> 系统默认创建账号不可删除。


帐号名称
所属角色
真实姓名
创建日期
创建人
最后修改人
最后修改时间
联系方式
登录IP范围
操作
sysadmin
系统管理员
2020-09-28 10:00
系统默认创建
/
2020-10-20 16:52
电话：
邮箱：
微信：
详情
OTP二维码
编辑
useradmin
审计管理员
2020-09-28 10:00
系统默认创建
/
2020-09-28 10:00
电话：
邮箱：
微信：
详情
OTP二维码
编辑
sysaudit
操作审计管理员
2020-09-28 10:00
系统默认创建
/
2020-09-28 10:00
电话：
邮箱：
微信：
详情
OTP二维码
编辑
审计管理员
2020-11-12 11:45
sysadmin
/
2020-11-12 11:45
电话：
邮箱：
微信：
详情
OTP二维码
编辑
删除

OTP 设置

最近更新时间：2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验，并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【OTP 设置】，即可进入 OTP 设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在 OTP 设置页面，设置校验开关，如需开启 OTP 验证选项，选中开启 OTP 验证，出现弹窗，根据提示扫 OTP 码，输入正确的 OTP 码，单击【确定】，退出登录系统即可。

> **说明**
> 建议开启 OTP 验证之前，提前通知各管理员登录系统扫描OTP验证二维码，避免其无法登录该系统。

4. 再次登录数据安全审计管理页面，需要输入OTP 校验码。

告警设置

最近更新时间：2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警，告警支持邮件告警、syslog 告警，具体操作步骤如下：

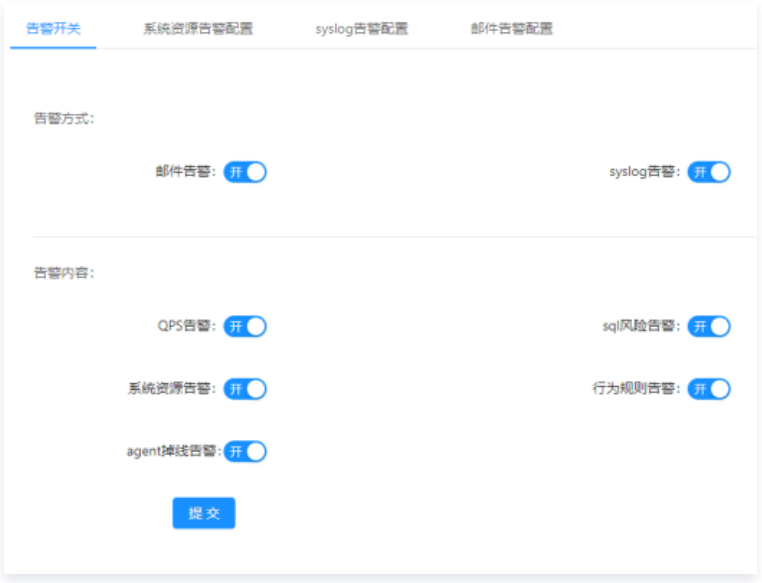
1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【告警设置】，即可进入告警设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在告警设置页面，分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。
   - **告警开关**
     在告警设置页面，单击【告警开关】，分为【告警方式】和【告警内容】，打开需要开启告警的选项，单击【提交】，即可对 syslog 告警配置 中所设置的服务器进行监控，且当满足告警条件时，将触发告警，并发送邮件至您所 配置的告警邮箱 中。

     > **注意**
     > 若需要接收告警信息，需打开邮件告警开关，且已在 邮件告警配置 中设置告警接收邮箱，否则无法接收告警信息。



   - **系统资源告警配置**
     在告警设置页面，单击【系统资源告警配置】，设置系统资源告警的触发条件，可将磁盘、内存、CPU 负载在0 - 100%之间调整，可自定义带宽值，单

击【提交】，即可对 syslog 告警配置 中所设置的服务器进行监控。

- **syslog 告警配置**

> **注意**
> 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面，单击【syslog 告警配置】，输入需要记录的 syslog 服务器 IP 和端口，单击【提交】，即可完成 syslog 告警条件配置，设置完成后将监控所配置的服务器。

- **邮件告警配置**

单击【邮件告警配置】，依次填入邮件服务器的相关配置信息，如需添加多个收件人，请以英文分号分隔，填写完成后，单击【提交】，当满足告警条件时，将发送邮件至所配置的邮箱中。

> **注意**
> 若填写 QQ 邮箱账号，密码需填写所设置的邮箱密码。


告警开关
系统资源告警配置
syslog告警配置
邮件告警配置
* SMTP服务器:
第三方邮件服务容易受服务器反垃圾机制影响，如遇到不可用的，建议尝试切换其他邮件服务
* 端口:
* 邮件账号:
* 密码:
此密码非邮箱登录密码
* 发件人:
收件人:
多个收件人请以分号；分隔
SSL:
测试
提交
重置

时间服务器

最近更新时间：2025-05-27 16:30:32

时间服务器主要用于同步时间，找到您需要同步时间的服务器IP进行设置即可，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击【管理】，进入数据安全审计登录界面。

2. 使用 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【时间服务器】，即可进入时间服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在时间服务器设置页面，输入 NTP 服务器 IP，单击【提交】，即可完成设置。

4. 设置完成后，数据安全审计系统时间会与您设置的 NTP 服务器地址所在时间进行同步。

备份服务器设置

最近更新时间：2025-05-27 16:30:32

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【备份服务器设置】，即可进入备份服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在备份服务器设置页面，依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径，打开备份开关，单击【保存】即可完成备份服务器设置。

> **说明**
> - 备份服务器地址需为公网 IP 地址，并且入站安全组是放通状态，详情请参见 添加安全组规则 。
> - 备份服务器通过 SSH 的方式进行备份，备份服务器设置成功后，系统每日02:00（UTC+8）定时备份前一天的数据到目标机器目录。

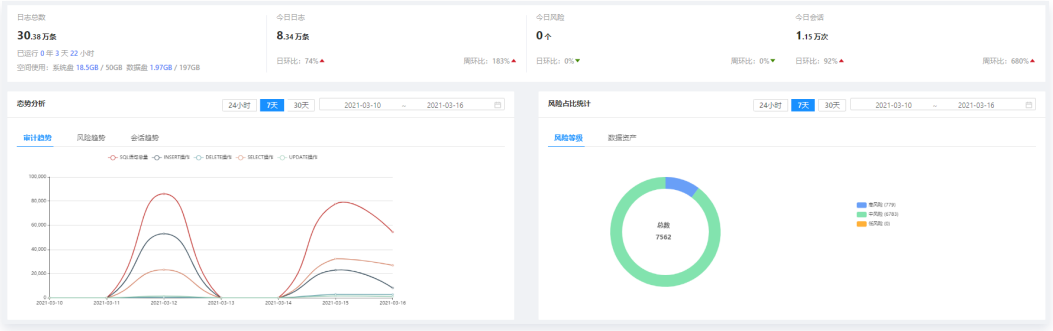
4. 设置完成后，数据安全审计管理系统中的数据将会按照设置路径进行备份。
5. （可选）如需恢复之前存在的数据，在备份服务器设置页面，单击【数据恢复】页签。
6. （可选）在数据恢复页签中，单击【数据恢复】，选择恢复日期并导入恢复数据即可。

审计管理
安全审计与分析
审计数据

最近更新时间：2025-05-27 16:30:32

审计概览

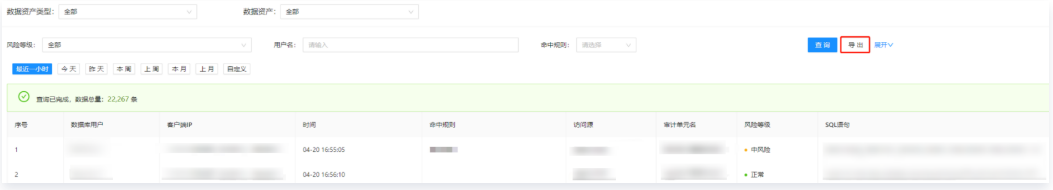
1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**安全审计与分析 > 审计概览**，即可进入审计概览页面。
3. 在审计概览页面中，可总览全网数据库日志信息，态势分析，风险占比以及查询单个数据库资产详细信息，如需了解数据库资产审计详细内容，可在审计概览页面下方查询详细信息。
   - **日志总数**：用于统计全网各数据资产日志总数。
   - **今日日志**：用于统计全网各数据资产今日日志总数。
   - **今日风险**：用于统计全网各数据资产今日风险总数。
   - **今日会话**：用于统计全网各数据资产今日会话总数。
   - **态势分析**：可查看您所配置的审计单元的审计趋势，风险趋势，会话趋势，还可按照高风险、中风险、低风险进行查看各个风险级别详细数据，每个报表可展示三种走势图及三类风险级别数据：
     - **审计趋势**：用于展示数据资产的审计单元语句压力，展示时间有24小时、7天、30天。
     - **风险趋势**：用于展示数据资产的审计单元高中低三类风险的统计信息，展示时间有24小时、7天、30天。
     - **会话趋势**：用于展示数据资产的审计单元各类会话信息，展示时间有24小时、7天、30天。
   - **风险占比统计**：用于显示数据资产对应的命中风险等级。
     - **风险等级**：用于展示数据资产审计单元有关的自定义规则命中风险信息，展示时间有24小时、7天、30天。
     - **数据资产**：用于展示被命中的数据资产，展示时间有24小时、7天、30天。
   - **资产审计**：主要展示单个数据资产的会话总数，DDL 操作数量、失败会话数量、最大并发会话及风险数等信息。



日志检索

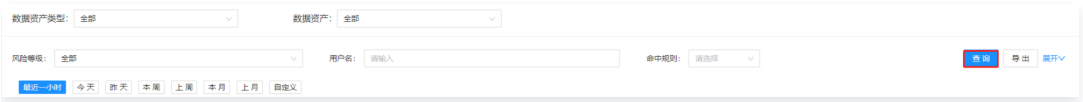
日志检索主要提供日志查询与导出功能。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**安全审计与分析 > 审计日志**，即可进入审计日志页面。
3. 管理员通过 审计概览 定位到疑似有风险的数据库审计单元，或者企业网络已经发生数据库安全问题时，可在日志检索页面查询并导出日志信息。



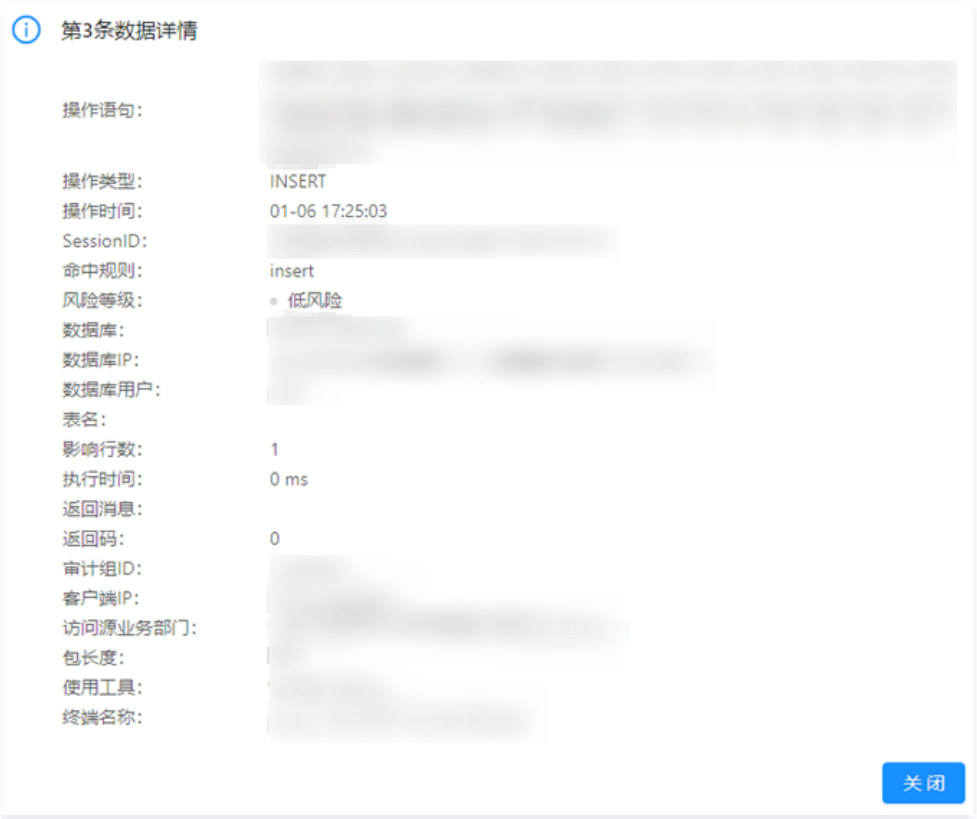
日志查询

在日志检索页面，您可以按照审计单元、风险等级、用户名、命中规则及时间，对日志进行查询。



查看数据详情

在日志列表中，可单击某条记录查看其详细内容。



日志导出

检索出需要导出的数据，现已支持不限数量导出，在列表上方单击**导出**，弹出导出数据弹窗，单击**确定**即可将数据导出，导出文件类型为 Excel（.xlsx格式）。

> **注意**
> 尽量缩小导出范围，导出数量过多，会影响服务器性能。

规则配置

最近更新时间：2025-05-27 16:30:32

规则配置页面可配置触发风险告警的命中规则。数据安全审计已提供17个内置规则，可满足大多数安全场景，内置规则不可删除、不可编辑。您也可以根据业务需要，添加自定义规则，下面将为您详细介绍配置操作。

操作步骤

以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【安全审计与分析】>【规则配置】即可进入规则配置页面。

新建规则

如需自定义规则满足个性化审计需求，单击【添加规则】，进入新建规则页面，填写规则名称等，单击【保存】即可。

> **注意**
> - 规则配置支持同一规则配置多个条件，多个条件之间为 “与” 关系，必须全部匹配才能够触发规则和告警。
> - 自定义规则默认为黑名单，触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计单元的存储空间，指定部分操作行为不记录不入库，可在规则中指定相关操作后，选择 “白名单” 选项，并且将告警选项都取消。

以上操作完成后，即可实现白名单类型规则配置，减少误报、减轻数据安全审计的审计单元存储压力。

- **规则示例**
  在规则配置页面，单击【添加规则】，按下图配置规则，表名和阈值根据您的业务场景自行设定，单击【保存】即可。

- **规则配置建议**
  以下三个建议规则仅作为示例，用户可根据自身业务自行配置。

- **防爬取规则**：防止使用例如 select 操作语句，爬取表数据。

> **注意**
> 影响行数可以根据业务自行配置。

- **慢查询发现规则**：检查执行时间较长的 SQL 语句，便于进行优化。

> **注意**
> 执行时间可以根据业务自行配置。

- **危险操作规则**：检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

修改规则

在规则列表中，找到需要修改的规则，在右侧操作栏中，单击【编辑】，修改信息后单击【保存】即可。

删除规则

在规则列表中，找到需要删除的规则，在右侧操作栏中，单击【删除】，再单击询问窗【确定】即可。

审计报表

最近更新时间：2025-05-27 16:30:32

审计报表功能主要展示所有配置过的审计组数据，并提供搜索、查看及 PDF 下载功能，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计报表】，即可进入审计报表页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在审计报表页面中，可查看内容包括报告名称、报告说明及发送目标等字段，同时可以进行相关操作，每个页面默认展示10条数据，可按照报告名称、生成方式、开始时间及结束时间，对报告进行搜索，还可下载 PDF 报告。

- **定时生成报表**

  数据安全审计管理系统支持定时生成报表。

  在报表上方单击【新建报表】，弹出新建报表弹窗，选择“定时报表”，并依次输入模板名称、统计周期（可选择定时执行、每天一次、每周一次、每月一次）、执行时间（精确到时分秒）、报告说明，设置完成后，单击【确定】，即可在您设定的执行时间定时生成报表。

- **即时生成报表**

  数据安全审计管理系统支持即时生成报表，即生成某个时间段内的报表。

  在报表上方单击【新建报表】，弹出新建报表弹窗，选择“即时报表”，依次输入报告名称、审计单元、统计开始时间、统计结束时间、报告说明，单击【确定】，即可输出您规定的时间范围内的报表。

> **注意**
> 开始时间应早于结束时间。


新建报表
报告类型：
即时报表
定时报表
* 报告名称：
最多30个字符
审计单元：
* 统计开始时间：
2021-03-15 00:00:00
* 统计结束时间：
2021-03-15 23:59:59
* 报告说明：
最多200个字符
取 消
确 定

数据资产与 Agent

最近更新时间：2025-05-27 16:30:32

Agent 下载

1. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择**数据资产与Agent > 审计用Agent**，即可进入审计用 Agent 页面。
2. Agent 部署。在审计用 Agent 页面，选择**Agent 下载 > 添加 Agent**，可配置审计 Agent 的各类参数并提供下载链接，配置步骤以及配置注意事项，请参见 Agent 部署 。
3. 添加完成 Agent 后，在 Agent 配置页面，可查看所有已正确安装且能实现 DSA（Data Security Audit）实例网络互通的 Agent 信息。

列表各字段含义如下：

- Agent 名称：用于配置该 Agent 的名称。
- 审计服务 IP： Agent 回传数据的源 IP。
- 审计服务端口：该 Agent 配置的审计端口。
- 数据库资产：可查看该 Agent 审计的数据库的所有 IP 地址。
- 操作：用于下载该 Agent 的链接。
  - 在右侧操作栏，选择**下载 > 下载 Linux Agent**或**下载 Windows Agent**，弹出部署 IP 窗口，单击**确定**即可开始下载 Agent 。

> **注意**
> - 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11，必须勾选下方说明，否则无法部署 Agent。
> - 请添加安装包需要部署机器的 IP 或 IP 列表。
> - 如未添加 IP 信息却部署了会导致 Agent 无法启动。
> - 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

  - 在右侧操作栏，选择**下载 > Linux 批量部署** ，输入部署地址，支持按 IP 或按 IP 段部署，支持添加多行，输入服务器 IP 、SSH 端口号、用户名、密码， 输入完成后单击**确定**即可。

- 在右侧操作栏，单击**删除**，可删除该条 Agent 信息。

Agent 列表

1. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择**审计用 Agent > Agent 列表**，即可进入审计列表中。
2. 在审计列表中，可以查看所有已配置的 Agent。Agent 列表默认展示内容包括：Agent 名称、部署 Mac、部署 IP、操作系统、部署时间、最新上报时间、运行状态、开启状态及相关操作。
   - **搜索**：您可以按数据资产、Agent 状态、Agent名称、IP、对 Agent 进行搜索。
   - **查看 Agent 配置详情**：在“操作”栏中，单击**编辑**，可以查看 Agent 配置相关信息。
   - **相关操作**：在右侧操作栏，可以对 Agent 进行启动、停止、编辑、卸载、删除的相关操作。

配置管理
审计单元配置

最近更新时间：2025-01-10 19:17:22

审计单元配置可为从属于一个应用的一台或多台数据库服务器进行命名，方便后续规则配置或审计信息时，使用直观的名字来表达数据库信息，优化策略和报表可读性。下面将为您详细介绍配置操作。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**配置管理** > **审计单元**，即可进入审计单元配置页面。

> **说明**
> 若审计 Agent 部署成功，会默认添加审计单元，无需自己新建。

3. 在审计单元列表中，找到需要修改的审计单元（建议以业务应用名称为基础命名），在右侧操作栏单击**编辑**，在弹框中修改信息后，单击**确定**即可。

访问源配置

最近更新时间：2021-11-24 10:28:35

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名，方便后续规则配置、审计信息使用直观名字来表达数据库访问端信息，优化策略以及报表可读性。下面将为您详细介绍配置操作。

以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择**配置管理** > **访问源**，即可进入访问源配置列表页面。

- **添加访问源**

  单击列表上方**添加**，在弹出窗口中，填写业务名、访问源名称、访问源包含 IP 段、备注信息，单击**确定**即可。

- **修改访问源**

  在访问源列表中，找到需要修改的访问源，在右侧操作栏中，单击**修改**，在弹框中修改信息后，单击**确定**即可。

- **删除访问源**

  在访问源列表中，找到需要删除的访问源，在右侧操作栏中，单击**删除**，再单击询问窗中的**确定**即可。

部门业务配置

最近更新时间：2025-01-10 19:17:22

部门业务配置功能主要是部门配置与业务配置的相关功能，具体配置步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择**配置管理>部门&业务**，即可进入部门业务配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在部门业务配置页面，可进行部门配置及业务配置。

- **部门配置**

3.1 在部门业务配置页面，单击**部门配置**，可添加并查看部门名、部门负责人及备注，同时可进行相关操作。

3.2 在部门设置页面，单击**添加部门**，在弹出的添加部门窗口中，填写部门名、部门负责人以及备注信息，单击**确定**即可完成添加。

3.3 添加完成后，已添加的部门将出现在部门配置列表中，支持对已添加的部门进行修改或删除，且支持对部门信息批量选择删除。

- **修改**
  找到需要修改的部门信息，在右侧操作栏单击**修改**，在弹出框中可以修改对应部门信息。
- **删除**
- **方式1**：找到需要删除的部门信息，在右侧操作栏单击**删除**，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的部门，在列表上方单击**删除**，即可批量删除部门信息。

- **业务配置**

3.1 在部门业务配置页面，单击**业务配置**，可添加并查看业务名、业务负责人、部门名及备注，同时可进行相关操作。

3.2 在业务配置页面，单击**添加业务**，在弹出的添加业务窗口中，填写部门名、业务名、业务负责人以及备注信息，填写完成后，单击**确定**即可完成添加。

3.3 添加完成后，已添加的业务将出现在业务配置列表中，支持对已添加的业务进行修改或删除，且支持对业务信息进行批量选择删除。

- **修改**
  找到需要修改的业务信息，在右侧操作栏单击**修改**，在弹出框中可以修改对应业务信息。
- **删除**
- **方式1**：找到需要删除的业务信息，在右侧操作栏单击**删除**，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的业务，在列表上方单击**删除**，在弹出框中确认删除，即可批量删除业务信息。

操作日志管理

最近更新时间：2025-01-10 19:17:22

操作审计员负责审计数据安全审计各管理员的操作，防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后，能够阅览管理员操作日志列表并对行为规则进行配置。

日志检索

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入操作日志页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在操作日志页面，您可以根据操作事件、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

行为规则配置

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入行为规则配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在行为规则配置页面，可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作，同时可按照行为分类、行为操作及危险等级，对行为规则进行搜索。

> **说明**
> 所有数据由系统内置生成，用户可以根据需求进行修改。

字段说明：

- **行为操作：用户对系统各个账户的功能操作。**
- **行为分类：用户对系统功能操作所属的模块名**
- **告警模板：用户执行操作时邮件所发送的告警内容**
- **备注：用户对行为规则的进一步说明。**
- **危险等级：对用户操作行为的评级，可设置行为危险等级，包括低级、中级及高级。**
- **是否开启告警：用户开启后，触发行为规则审计，则会发送告警信息，关闭后，只会记录操作，不会发送告警信息。**
- **操作：在目标行为右侧操作栏，单击修改，即可对行为操作信息进行修改。**

v5.0.7
系统管理
系统资源监控

最近更新时间：2021-08-06 10:23:47

以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【系统资源监控】，即可进入资源监控页面，该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。

系统详细信息

系统详细信息包含系统产品名称、产品规格、当前版本等基础信息，以及数据安全审计总审计单元数参数信息。

系统存储空间统计

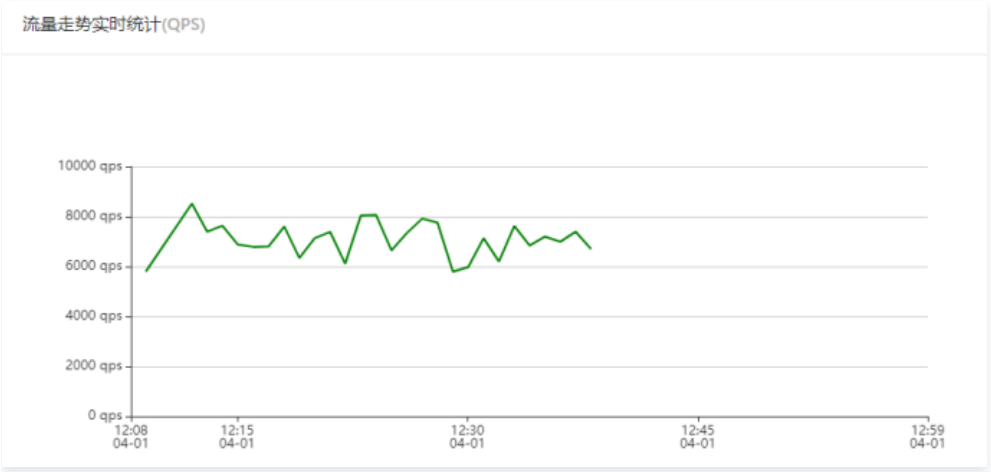
存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角，单击【清理剩余空间】，将清理的数据包含所选的日期。例如，选择了12月1日至12月3日，则会删除12月1日、2日、3日，3天的数据。

> **说明**
> 统计报表将磁盘空间分为四个类型：

- 剩余空间：数据安全审计实例存储剩余空间；
- 系统占用空间：数据安全审计自身代码所占存储空间；
- 审计日志占用空间：数据安全审计记录的数据库操作信息日志占用空间；
- 其他占用空间：数据安全审计实例其他代码、配置文件占用空间。

流量走势实时统计

流量走势实时统计能统计一定时间跨度（最近 30 分钟、最近 24小时、最近 7 天）内数据安全审计中所审计的所有数据库的 QPS，确认全网 QPS 峰值是否超过购买峰值，以帮助管理员了解数据安全审计性能状况，及时扩容升级产品。



用户管理

最近更新时间：2025-05-27 16:30:32

以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中单击【用户管理】即可进入用户页面。

查看账号信息

账号管理用于管理 DSA 实例所有账号。系统管理员可以通过列表查看所有账号信息，包括所属角色、真实姓名、创建日期以及联系方式等。

> **说明**
> OTP 二维码：如需开启 OTP 实现登录双重验证，可在相应账号右侧操作栏，单击【OTP二维码】，或在数据安全审计管理页面右上角，找到管理员账号下的 OTP 验证，单击【OTP 验证】，查看原图并扫描动态校验码。

添加账号

如需要增加管理员账号，单击【添加账号】，在弹框中填写账号信息，选择所属角色后，单击【确定】即可。

修改和删除账号

如需对账号进行修改或删除，可在相应账号操作列单击【编辑】或【删除】对账号进行调整。

> **注意**
> 系统默认创建账号不可删除。


帐号名称
所属角色
真实姓名
创建日期
创建人
最后修改人
最后修改时间
联系方式
登录IP范围
操作
sysadmin
系统管理员
2020-09-28 10:00
系统默认创建
/
2020-10-20 16:52
详情
OTP二维码
编辑
useradmin
审计管理员
2020-09-28 10:00
系统默认创建
/
2020-09-28 10:00
详情
OTP二维码
编辑
sysaudit
操作审计管理员
2020-09-28 10:00
系统默认创建
/
2020-09-28 10:00
详情
OTP二维码
编辑
审计管理员
2020-11-12 11:45
sysadmin
/
2020-11-12 11:45
详情
OTP二维码
编辑
删除

OTP 设置

最近更新时间：2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验，并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【OTP 设置】，即可进入 OTP 设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在 OTP 设置页面，设置校验开关，如需开启 OTP 验证选项，选中开启 OTP 验证，出现弹窗，根据提示扫 OTP 码，输入正确的 OTP 码，单击【确定】，退出登录系统即可。

> **说明**
> 建议开启 OTP 验证之前，提前通知各管理员登录系统扫描OTP验证二维码，避免其无法登录该系统。

4. 再次登录数据安全审计管理页面，需要输入OTP 校验码。

告警设置

最近更新时间：2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警，告警支持邮件告警、syslog 告警，具体操作步骤如下：

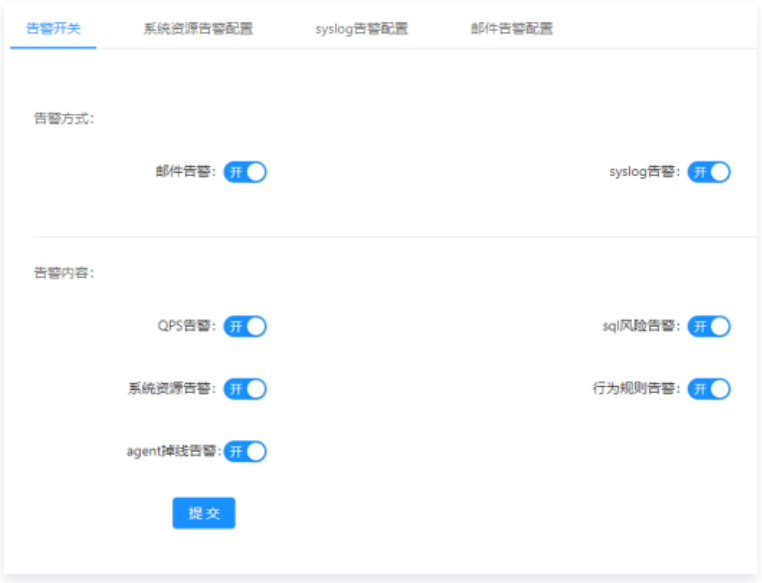
1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击**告警设置**，即可进入告警设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在告警设置页面，分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。
   - **告警开关**
     在告警设置页面，单击**告警开关**，分为**告警方式**和**告警内容**，打开需要开启告警的选项，单击**提交**，即可对 syslog 告警配置 中所设置的服务器进行监控，且当满足告警条件时，将触发告警，并发送邮件至您所 配置的告警邮箱 中。

     > **注意**
     > 若需要接收告警信息，需打开邮件告警开关，且已在 邮件告警配置 中设置告警接收邮箱，否则无法接收告警信息。



   - **系统资源告警配置**
     在告警设置页面，单击**系统资源告警配置**，设置系统资源告警的触发条件，可将磁盘、内存、CPU 负载在0 – 100%之间调整，可自定义带宽值，单击**提**

交，即可对 syslog 告警配置 中所设置的服务器进行监控。

- **syslog 告警配置**

> **注意**
> 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面，单击**syslog 告警配置**，输入需要记录的 syslog 服务器 IP 和端口，单击**提交**，即可完成 syslog 告警条件配置，设置完成后将监控所配置的服务器。

- **邮件告警配置**

单击**邮件告警配置**，依次填入邮件服务器的相关配置信息，如需添加多个收件人，请以英文分号分隔，填写完成后，单击**提交**，当满足告警条件时，将发送邮件至所配置的邮箱中。

> **注意**
> 若填写 QQ 邮箱账号，密码需填写所设置的邮箱密码。


告警开关
系统资源告警配置
syslog告警配置
邮件告警配置
* SMTP服务器:
第三方邮件服务容易受服务器反垃圾机制影响，如遇到不可用的，建议尝试切换其他邮件服务
* 端口:
* 邮件账号:
* 密码:
此密码非邮箱登录密码
* 发件人:
收件人:
多个收件人请以分号；分隔
SSL:
测试
提交
重置

时间服务器

最近更新时间：2025-05-27 16:30:32

时间服务器主要用于同步时间，找到您需要同步时间的服务器IP进行设置即可，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击**管理**，进入数据安全审计登录界面。

2. 使用 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击**时间服务器**，即可进入时间服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在时间服务器设置页面，输入 NTP 服务器 IP，单击**提交**，即可完成设置。

4. 设置完成后，数据安全审计系统时间会与您设置的 NTP 服务器地址所在时间进行同步。

备份服务器设置

最近更新时间：2025-05-27 16:30:32

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【备份服务器设置】，即可进入备份服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在备份服务器设置页面，依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径，打开备份开关，单击【保存】即可完成备份服务器设置。

> **说明**
> - 备份服务器地址需为公网 IP 地址，并且入站安全组是放通状态，详情请参见 添加安全组规则 。
> - 备份服务器通过 SSH 的方式进行备份，备份服务器设置成功后，系统每日02:00（UTC+8）定时备份上一天的数据到目标机器目录。

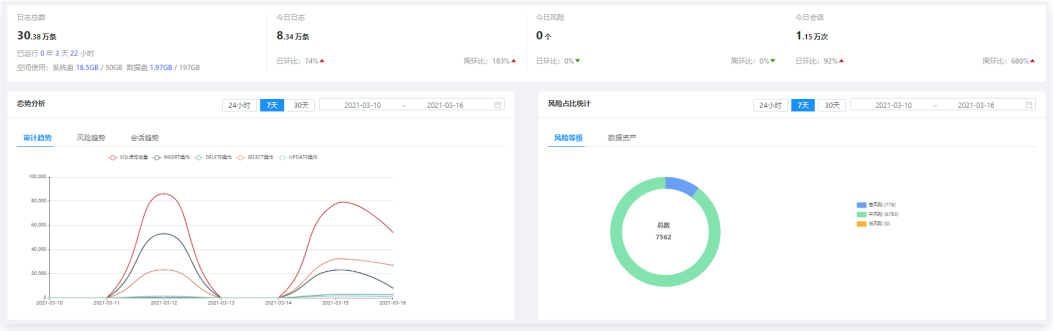
4. 设置完成后，数据安全审计管理系统中的数据将会按照设置路径进行备份。
5. （可选）如需恢复之前存在的数据，在备份服务器设置页面，单击【数据恢复】页签。
6. （可选）在数据恢复页签中，单击【数据恢复】，选择恢复日期并导入恢复数据即可。

审计管理
安全审计与分析
审计数据

最近更新时间：2025-05-27 16:30:32

审计概览

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计概览】，即可进入审计概览页面。
3. 在审计概览页面中，可总览全网数据库日志信息，态势分析，风险占比以及查询单个数据库资产详细信息，如需了解数据库资产审计详细内容，可在审计概览页面下方查询详细信息。
   - **日志总数**：用于统计全网各数据资产日志总数。
   - **今日日志**：用于统计全网各数据资产今日日志总数。
   - **今日风险**：用于统计全网各数据资产今日风险总数。
   - **今日会话**：用于统计全网各数据资产今日会话总数。
   - **态势分析**：可查看您所配置的审计单元的审计趋势，风险趋势，会话趋势，还可按照高风险、中风险、低风险进行查看各个风险级别详细数据，每个报表可展示三种走势图及三类风险级别数据：
     - **审计趋势**：用于展示数据资产的审计单元语句压力，展示时间有24小时、7天、30天。
     - **风险趋势**：用于展示数据资产的审计单元高中低三类风险的统计信息，展示时间有24小时、7天、30天。
     - **会话趋势**：用于展示数据资产的审计单元各类会话信息，展示时间有24小时、7天、30天。
   - **风险占比统计**：用于显示数据资产对应的命中风险等级。
     - **风险等级**：用于展示数据资产审计单元有关的自定义规则命中风险信息，展示时间有24小时、7天、30天。
     - **数据资产**：用于展示被命中的数据资产，展示时间有24小时、7天、30天。
   - **资产审计**：主要展示单个数据资产的会话总数，DDL 操作数量、失败会话数量、最大并发会话及风险数等信息。



日志检索

日志检索主要提供日志查询与导出功能。

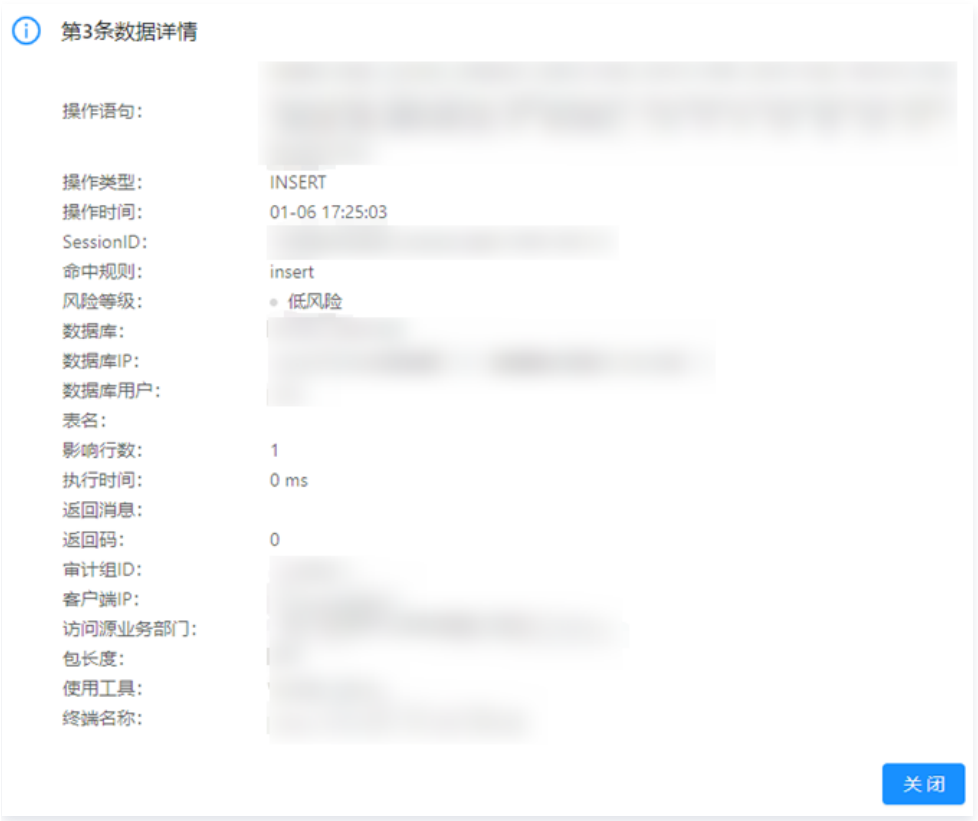
1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计日志】，即可进入审计日志页面。
3. 管理员通过 审计概览 定位到疑似有风险的数据库审计单元，或者企业网络已经发生数据库安全问题时，可在日志检索页面查询并导出日志信息。

日志查询

在日志检索页面，您可以按照审计单元、风险等级、用户名、命中规则及时间，对日志进行查询。

查看数据详情

在日志列表中，可单击某条记录查看其详细内容。



日志导出

检索出需要导出的数据，现已支持不限数量导出，在列表上方单击【导出】，弹出导出数据弹窗，单击【确定】即可将数据导出，导出文件类型为 Excel（.xlsx 格式）。

> **注意**
> 尽量缩小导出范围，导出数量过多，会影响服务器性能。

规则配置

最近更新时间：2025-05-27 16:30:32

规则配置可定义数据安全审计的审计单元的安全规则。数据安全审计具备两个默认规则，AI 引擎规则和 CVE 引擎规则，默认规则不可删除、不可编辑。下面将为您详细介绍配置操作。

操作步骤

以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【安全审计与分析】>【规则配置】即可进入规则配置页面。

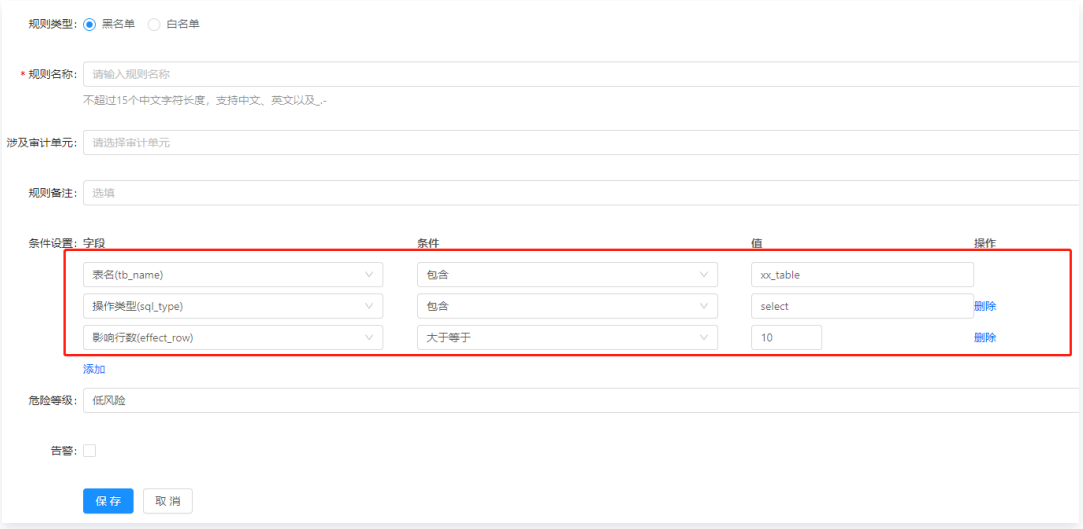
新建规则

如需自定义规则满足个性化审计需求，单击【添加规则】，进入新建规则页面，填写规则名称等，单击【保存】即可。

> **注意**
> - 规则配置支持同一规则配置多个条件，多个条件之间为 “与” 关系，必须全部匹配才能够触发规则和告警。
> - 自定义规则默认为黑名单，触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计单元的存储空间，指定部分操作行为不记录不入库，可在规则中指定相关操作后，选择 “白名单” 选项，并且将告警选项都取消。

以上操作完成后，即可实现白名单类型规则配置，减少误报、减轻数据安全审计的审计单元存储压力。

- **规则示例**
  在规则配置页面，单击【添加规则】，按下图配置规则，表名和阈值根据您的业务场景自行设定，单击【保存】即可。



- **规则配置建议**
  以下三个建议规则仅作为示例，用户可根据自身业务自行配置。

- **防爬取规则**：防止使用例如 select 操作语句，爬取表数据。

> **注意**
> 影响行数可以根据业务自行配置。

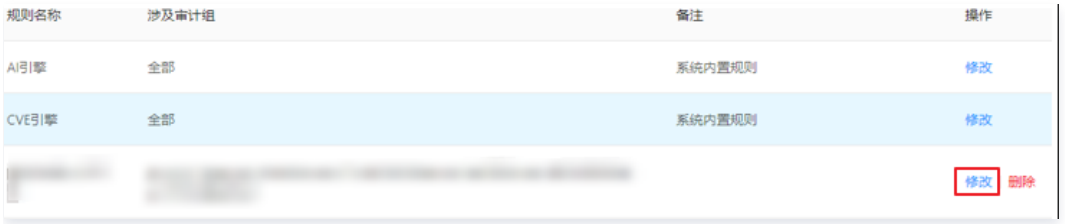
- **慢查询发现规则**：检查执行时间较长的 SQL 语句，便于进行优化。

> **注意**
> 执行时间可以根据业务自行配置。

- **危险操作规则**：检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

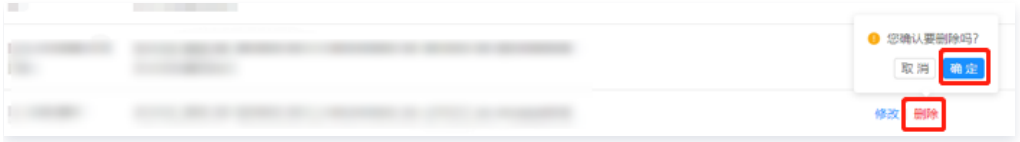
修改规则

在规则列表中，找到需要修改的规则，在右侧操作栏中，单击【修改】，修改信息后单击【保存】即可。



删除规则

在规则列表中，找到需要删除的规则，在右侧操作栏中，单击【删除】，再单击询问窗【确定】即可。



审计报表

最近更新时间：2025-05-27 16:30:32

审计报表功能主要展示所有配置过的审计组数据，并提供搜索、查看及 PDF 下载功能，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计报表】，即可进入审计报表页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在审计报表页面中，可查看内容包括报告名称、报告说明及发送目标等字段，同时可以进行相关操作，每个页面默认展示10条数据，可按照报告名称、生成方式、开始时间及结束时间，对报告进行搜索，还可下载 PDF 报告。

- **定时生成报表**

  数据安全审计管理系统支持定时生成报表。

  在报表上方单击【新建报表】，弹出新建报表报表弹窗，选择“定时报表”，并依次输入模板名称、统计周期（可选择定时执行、每天一次、每周一次、每月一次）、执行时间（精确到时分秒）、报告说明，设置完成后，单击【确定】，即可在您设定的执行时间定时生成报表。

- **即时生成报表**

  数据安全审计管理系统支持即时生成报表，即生成某个时间段内的报表。

  在报表上方单击【新建报表】，弹出新建报表弹窗，选择“即时报表”，依次输入报告名称、审计单元、统计开始时间、统计结束时间、报告说明，单击【确定】，即可输出您规定的时间范围内的报表。

> **注意**
> 开始时间应早于结束时间。


新建报表
报告类型：
即时报表
定时报表
* 报告名称：
最多30个字符
审计单元：
* 统计开始时间：
2021-03-15 00:00:00
* 统计结束时间：
2021-03-15 23:59:59
* 报告说明：
最多200个字符
取 消
确 定

数据资产与 Agent

最近更新时间：2025-05-27 16:30:32

Agent 配置

1. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【数据资产与Agent】>【审计用Agent】，即可进入审计用 Agent 页面。
2. Agent 部署。在审计用 Agent 页面，选择【Agent 配置】>【添加 Agent】，可配置审计 Agent 的各类参数并提供下载链接，配置步骤以及配置注意事项，请参见 Agent 部署 。
3. 添加完成 Agent 后，在 Agent 配置页面，可查看所有已正确安装且能实现 DSA(Data Security Audit）实例网络互通的 Agent 信息。

列表各字段含义如下：

- Agent 名称：用于配置该 Agent 的名称。
- 审计服务 IP： Agent 回传数据的源 IP。
- 审计服务端口：该 Agent 配置的审计端口。
- 数据库 IP：单击【详情】可查看该 Agent 审计的数据库的所有 IP 地址。
- 审计 IP：用于显示该 Agent 配置的审计范围，由于 IP 范围内容较多，可单击【详情】进行阅览。
- 操作：用于下载该 Agent 的链接。
  - 单击【下载 Linux Agent】或【下载 Windows Agent】，弹出部署 IP 窗口，可以按 IP 部署或按 IP 段部署（IP 段支持全段审计），单击【确定】即可开始下载 Agent 。

> **注意**
> - 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11，必须勾选下方说明，否则无法部署 Agent。
> - 请添加安装包需要部署机器的 IP 或 IP 列表。
> - 如未添加 IP 信息却部署了会导致 Agent 无法启动。
> - 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

  - 单击【删除】，可删除该条 Agent 信息。

审计列表

1. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【审计用 Agent】>【审计列表】，即可进入审计列表中。
2. 在审计列表中，可以查看所有已配置的 Agent。审计列表默认展示内容包括：deployMac、部署服务器 IP、审计服务、部署状态、Agent 状态、系统类型、部署时间运行时长及相关操作。
   - **搜索**：您可以按照部署状态、Agent 状态、审计服务 IP、Port（端口）对 Agent 进行搜索。。
   - **查看 Agent 配置详情**：在“审计服务”栏中，单击【Agent 配置详情】，可以查看 Agent 配置相关信息。

- **相关操作**：在右侧操作栏，可以对 Agent 进行启动、停止、卸载、删除的相关操作。

配置管理
审计单元配置

最近更新时间：2025-01-10 19:17:22

审计单元配置可为从属于一个应用的一台或多台数据库服务器进行命名，方便后续规则配置或审计信息时，使用直观的名字来表达数据库信息，优化策略和报表可读性。下面将为您详细介绍配置操作。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【配置管理】>【审计单元】，即可进入审计单元配置页面。

> **说明**
> 若审计 Agent 部署成功，会默认添加审计单元，无需自己新建。

3. 在审计单元列表中，找到需要修改的审计单元（建议以业务应用名称为基础命名），在右侧操作栏单击【编辑】，在弹框中修改信息后，单击【确定】即可。

访问源配置

最近更新时间：2025-05-27 16:30:32

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名，方便后续规则配置、审计信息通过直观命名标识数据库访问端来源，优化策略以及报表可读性。下面将为您详细介绍配置操作。

以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【配置管理】>【访问源】，即可进入访问源配置列表页面。

- **添加访问源**

  单击列表上方【添加】，在弹出窗口中，填写业务名、访问源名称、访问源包含 IP 段、备注信息，单击【确定】即可。

- **修改访问源**

  在访问源列表中，找到需要修改的访问源，在右侧操作栏中，单击【修改】，在弹框中修改信息后，单击【确定】即可。

- **删除访问源**

  在访问源列表中，找到需要删除的访问源，在右侧操作栏中，单击【删除】，再单击询问窗中的【确定】即可。

部门业务配置

最近更新时间：2025-01-10 19:17:22

部门业务配置功能主要是部门配置与业务配置的相关功能，具体配置步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【配置管理】>【部门&业务】，即可进入部门业务配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在部门业务配置页面，可进行部门配置及业务配置。

- **部门配置**

3.1 在部门业务配置页面，单击【部门配置】，可添加并查看部门名、部门负责人及备注，同时可进行相关操作。

3.2 在部门设置页面，单击【添加部门】，在弹出的添加部门窗口中，填写部门名、部门负责人以及备注信息，单击【确定】即可完成添加。

3.3 添加完成后，已添加的部门将出现在部门配置列表中，支持对已添加的部门进行修改或删除，且支持对部门信息批量选择删除。

- **修改**
  找到需要修改的部门信息，在右侧操作栏单击【修改】，在弹出框中可以修改对应部门信息。
- **删除**
- **方式1**：找到需要删除的部门信息，在右侧操作栏单击【删除】，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的部门，在列表上方单击【删除】，即可批量删除部门信息。

- **业务配置**

3.1 在部门业务配置页面，单击【业务配置】，可添加并查看业务名、业务负责人、部门名及备注，同时可进行相关操作。

3.2 在业务配置页面，单击【添加业务】，在弹出的添加业务窗口中，填写部门名、业务名、业务负责人以及备注信息，填写完成后，单击【确定】即可完成添加。

3.3 添加完成后，已添加的业务将出现在业务配置列表中，支持对已添加的业务进行修改或删除，且支持对业务信息进行批量选择删除。

- **修改**
  找到需要修改的业务信息，在右侧操作栏单击【修改】，在弹出框中可以修改对应业务信息。
- **删除**
- **方式1**：找到需要删除的业务信息，在右侧操作栏单击【删除】，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的业务，在列表上方单击【删除】，在弹出框中确认删除，即可批量删除业务信息。

操作日志管理

最近更新时间：2025-01-10 19:17:22

操作审计员负责审计数据安全审计各管理员的操作，防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后，能够阅览管理员操作日志列表并对行为规则进行配置。

日志检索

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击【行为规则配置】，即可进入操作日志页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在操作日志页面，您可以根据操作账户、操作 IP、行为分类、操作时间检索还原非法操作完整信息。

行为规则配置

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击【行为规则配置】，即可进入行为规则配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在行为规则配置页面，可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作，同时可按照行为分类、行为操作及危险等级，对行为规则进行搜索。

> **说明**
> 所有数据由系统内建生成，用户可以根据需求进行修改。

字段说明：

- **行为操作：用户对系统各个账户的功能操作。**
- **行为分类：用户对系统功能操作所属的模块名**
- **告警信息模板：用户执行操作时邮件所发送的告警内容**
- **备注：用户对行为规则的进一步说明。**
- **危险等级：对用户操作行为的评级，可设置行为危险等级，包括低级、中级及高级。**
- **是否开启告警：用户开启后，触发行为规则审计，则会发送告警信息，关闭后，只会记录操作，不会发送告警信息。**
- **操作：在目标行为右侧操作栏，单击【修改】，即可对行为操作信息进行修改。**

v5.0.6
系统管理
系统资源监控

最近更新时间：2025-01-10 19:17:22

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【系统资源监控】，即可进入资源监控页面，该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

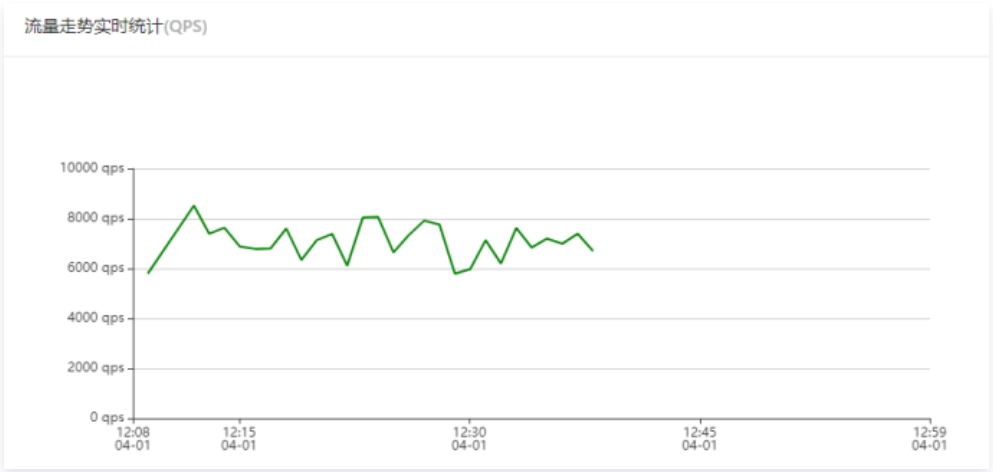
- **系统详细信息**
  系统详细信息包含系统产品名称、产品规格、当前版本等基础信息，以及数据安全审计总审计组数参数信息。

- **系统存储空间统计**
  存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角，单击【清理剩余空间】，将清理的数据包含所选的日期。例如，选择了12月1日至12月3日，则会删除12月1日、2日、3日，3天的数据。

> **说明**
> 统计报表将磁盘空间分为四个类型：
> - 剩余空间：数据安全审计实例存储剩余空间；
> - 系统占用空间：数据安全审计自身代码所占存储空间；
> - 审计日志占用空间：数据安全审计记录的数据库操作信息日志占用空间；
> - 其他占用空间：数据安全审计实例其他代码、配置文件占用空间。

- **流量走势实时统计**

  流量走势实时统计能统计一定时间跨度（最近30分钟、最近24小时、最近7天）内数据安全审计中所审计的所有数据库的 QPS，确认全网 QPS 峰值是否超过购买峰值，以帮助管理员了解数据安全审计性能状况，及时扩容升级产品。



用户管理

最近更新时间：2025-05-27 16:30:32

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中单击【用户管理】即可进入用户页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

- **查看账号信息**

  账号管理用于管理 DSA 实例所有账号。系统管理员可以通过列表查看所有账号信息，包括所属角色、真实姓名、创建日期以及联系方式等。

  > **说明**
  > OTP 二维码：如需开启 OTP 实现登录双重验证，可在相应账号右侧操作栏，单击【OTP二维码】，或在数据安全审计管理页面右上角，找到管理员账号下的 OTP 验证，单击【OTP 验证】，查看原图并扫描动态校验码。

- **添加账号**

  如需要增加管理员账号，单击【添加账号】，在弹框中填写账号信息，选择所属角色后，单击【确定】即可。

- **修改和删除账号**

  如需对账号进行修改或删除，可在相应账号操作列单击【编辑】或【删除】对账号进行调整。

> **注意**
>
> 系统默认创建账号不可删除。

OTP 设置

最近更新时间：2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验，并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【OTP 设置】，即可进入 OTP 设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在 OTP 设置页面，设置校验开关，如需开启 OTP 验证选项，选中开启 OTP 验证，根据提示扫描 OTP 码，输入正确的 OTP 码，单击【确定】，退出登录系统即可。

> **说明**
> 建议开启 OTP 验证之前，提前通知各管理员登录系统扫描 OTP 验证二维码，避免其无法登录该系统。

4. 再次登录数据安全审计管理页面，需要输入OTP 校验码。

告警设置

最近更新时间：2025-01-10 19:17:22

告警支持针对每个审计规则策略进行告警，告警支持邮件告警、syslog 告警，具体操作步骤如下：

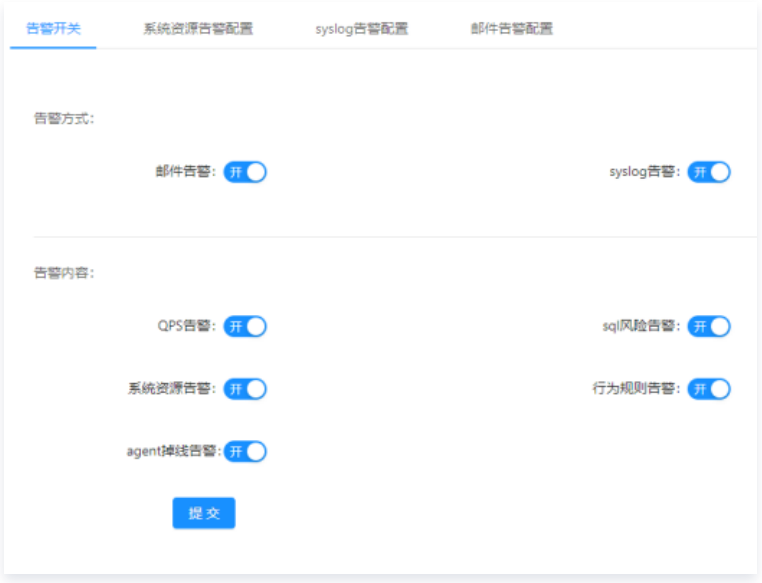
1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【告警设置】，即可进入告警设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在告警设置页面，分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。
   - **告警开关**
     在告警设置页面，单击【告警开关】，分为【告警方式】和【告警内容】，打开需要开启告警的选项，单击【提交】，即可对 syslog 告警配置 中所设置的服务器进行监控，且当满足告警条件时，将触发告警，并发送邮件至您所 配置的告警邮箱 中。

     > **注意**
     > 若需要接收告警信息，需打开邮件告警开关，且已在 邮件告警配置 中设置告警接收邮箱，否则无法接收告警信息。



   - **系统资源告警配置**
     在告警设置页面，单击【系统资源告警配置】，设置系统资源告警的触发条件，可将磁盘、内存、CPU 负载在0 - 100%之间调整，可自定义带宽值，单

击【提交】，即可对 syslog 告警配置 中所设置的服务器进行监控。

- **syslog 告警配置**

> **注意**
> 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面，单击【syslog 告警配置】，输入需要记录的 syslog 服务器 IP 和端口，单击【提交】，即可完成 syslog 告警条件配置，设置完成后将监控所配置的服务器。

- **邮件告警配置**

单击【邮件告警配置】，依次填入邮件服务器的相关配置信息，如需添加多个收件人，请以英文分号分隔，填写完成后，单击【提交】，当满足告警条件时，将发送邮件至所配置的邮箱中。

> **注意**
> 若填写 QQ 邮箱账号，密码需填写所设置的邮箱密码。


告警开关
系统资源告警配置
syslog告警配置
邮件告警配置
* SMTP服务器:
第三方邮件服务容易受服务器反垃圾机制影响，如遇到不可用的，建议尝试切换其他邮件服务
* 端口:
* 邮件账号:
* 密码:
此密码非邮箱登录密码
* 发件人:
收件人:
多个收件人请以分号；分隔
SSL:
测试
提交
重置

时间服务器

最近更新时间：2025-05-27 16:30:32

时间服务器主要用于同步时间，找到您需要同步时间的服务器 IP 进行设置即可，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击【管理】，进入数据安全审计登录界面。

2. 使用 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【时间服务器】，即可进入时间服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在时间服务器设置页面，输入 NTP 服务器 IP，单击【提交】，即可完成设置。

4. 设置完成后，数据安全审计系统时间会与您设置的 NTP 服务器地址所在时间进行同步。

备份服务器

最近更新时间：2025-05-27 16:30:32

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【备份服务器设置】，即可进入备份服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在备份服务器设置页面，依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径，打开备份开关，单击【保存】即可完成备份服务器设置。

> **说明**
> - 备份服务器地址需为公网 IP 地址，并且入站安全组是放通状态，详情请参见 添加安全组规则 。
> - 备份服务器通过 SSH 的方式进行备份，备份服务器设置成功后，系统每日02:00（UTC+8）定时备份上一天的数据到目标机器目录。

4. 设置完成后，数据安全审计管理系统中的数据将会按照设置路径进行备份。
5. （可选）如需恢复之前存在的数据，在备份服务器设置页面，单击【数据恢复】页签。
6. （可选）在数据恢复页签中，单击【数据恢复】，选择恢复日期并导入恢复数据即可。

审计管理
安全审计与分析
审计数据

最近更新时间：2025-05-27 16:30:32

审计概览

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计概览】，即可进入审计概览页面。
3. 在审计概览页面中，可总览全网数据库各类排行信息以及查询单个数据库实例概览信息，如需了解数据库审计组详细内容，可在审计概览页面下方查询审计组的详细信息。
   - **数据库排行统计**：上方条形统计图为数据库排行，排行统计数据内容如下：
     - **风险排行**：用于统计全网各数据库风险总数，降序排列。
     - **语句压力排行**：用于统计全网各数据库语句压力总数，降序排列。
   - **审计组详情**：审计组详情内可查看您所配置的审计组的风险分布 Top5、语句压力统计 Top5（QPS），会话分布 Top5，还可按照全部、高风险、中风险、低风险进行查看各个风险级别详细数据，每个报表可展示三种走势图及三类风险级别数据：
     - **风险分布**：用于展示本数据库审计组高中低三类风险的统计信息，展示时间范围可在1天到365天之间进行调整。
     - **自定义规则命中**：用于展示与本数据库审计组有关的自定义规则命中信息，展示时间范围可在1天到365天之间进行调整。
     - **语句压力统计**：用于展示本数据库审计组语句压力的统计信息，展示时间范围可在1天到365天之间进行调整。
     - **会话统计**：用于展示本数据库审计组各类会话信息，展示时间范围可在1天到365天之间进行调整。

日志检索

日志检索主要提供日志查询与导出功能。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计日志】，即可进入审计日志页面。

3. 管理员通过 审计概览 定位到疑似有风险的数据库审计组，或者企业网络已经发生数据库安全问题时，可在日志检索页面查询并导出日志信息。

日志查询

在日志检索页面，您可以按照审计组、风险等级、用户名、命中规则及时间，对日志进行查询。

查看数据详情

在日志列表中，可单击某条记录查看其详细内容。

日志导出

检索出需要导出的数据，现已支持不限数量导出，在列表上方单击【导出】，弹出导出数据弹窗，单击【确定】即可将数据导出，导出文件类型为 Excel（.xlsx 格式）。

> **注意**
> 尽量缩小导出范围，导出数量过多，会影响服务器性能。


Excel文件生成
导出记录16,075,835条，确认要导出吗?
注：尽量缩小范围导出，导出数量过多，会影响服务性能
取 消
确 定

规则配置

最近更新时间：2025-05-27 16:30:32

规则配置可定义数据安全审计的审计组的安全规则。数据安全审计具备两个默认规则，AI 引擎规则和 CVE 引擎规则，默认规则不可删除、不可编辑。下面将为您详细介绍配置操作。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【安全审计与分析】>【规则配置】即可进入规则配置页面。

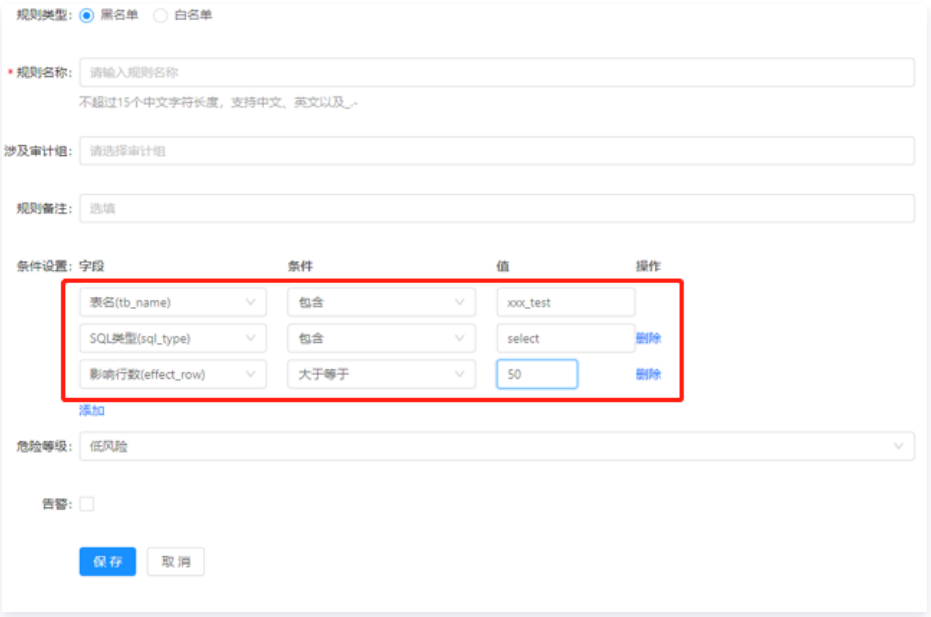
新建规则

如需自定义规则满足个性化审计需求，单击【添加规则】，进入新建规则页面，填写规则名称等，单击【保存】即可。

> **注意**
> - 规则配置支持同一规则配置多个条件，多个条件之间为 “与” 关系，必须全部匹配才能够触发规则和告警。
> - 自定义规则默认为黑名单，触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计组的存储空间，指定部分操作行为不记录不入库，可在规则中指定相关操作后，选择 “白名单” 选项，并且将告警选项都取消。

以上操作完成后，即可实现白名单类型规则配置，减少误报、减轻数据安全审计的审计组存储压力。

- **规则示例**
  在规则配置页面，单击【添加规则】，按下图配置规则，表名和阈值根据您的业务场景自行设定，单击【保存】即可。



- **规则配置建议**

  以下三个建议规则仅作为示例，用户可根据自身业务自行配置。

  - **防爬取规则**：防止使用例如 select 操作语句，爬取表数据。

    > **注意**
    > 影响行数可以根据业务自行配置。

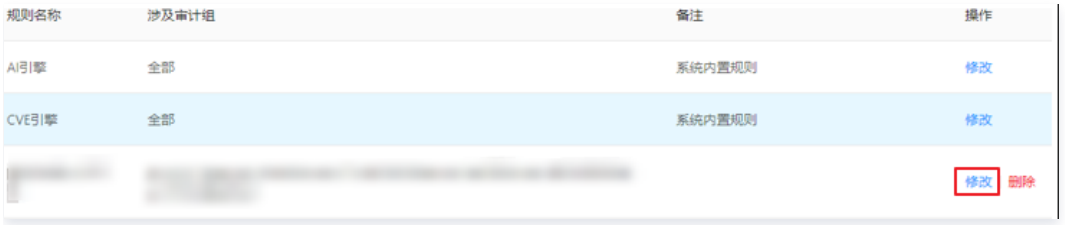
  - **慢查询发现规则**：检查执行时间较长的 SQL 语句，便于进行优化。

    > **注意**
    > 执行时间可以根据业务自行配置。

- **危险操作规则**：检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

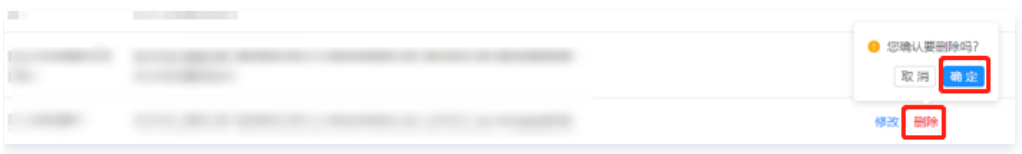
修改规则

在规则列表中，找到需要修改的规则，在右侧操作栏中，单击【修改】，修改信息后单击【保存】即可。



删除规则

在规则列表中，找到需要删除的规则，在右侧操作栏中，单击【删除】，再单击询问窗【确定】即可。



审计报表

最近更新时间：2025-05-27 16:30:32

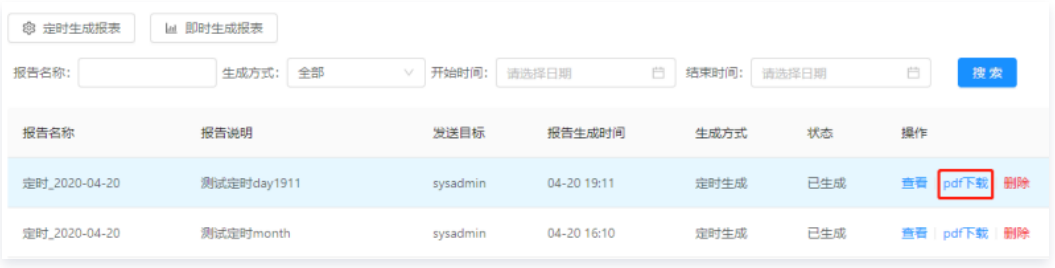
审计报表功能主要展示所有配置过的审计组数据，并提供搜索、导出及 PDF 下载功能，具体操作步骤如下：

1. **登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。**

2. **以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【安全审计与分析】>【审计报表】，即可进入审计报表页面。**

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. **在审计报表页面中，可查看内容包括报告名称、报告说明及发送目标等字段，同时可以进行相关操作，每个页面默认展示10条数据，可按照报告名称、生成方式、开始时间及结束时间，对报告进行搜索，还可下载 PDF 报告。**



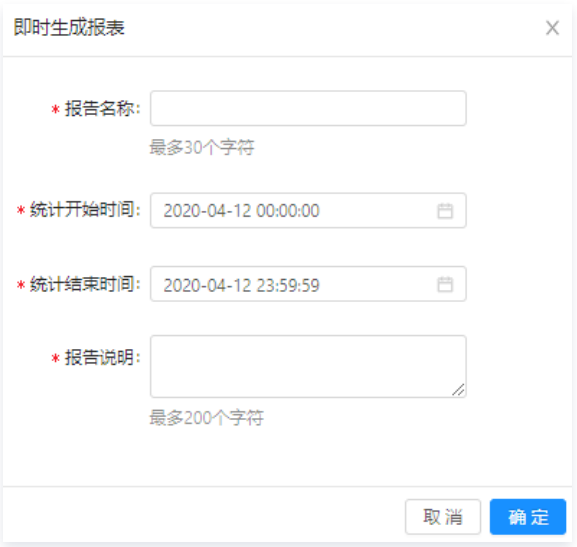
- **定时生成报表**

数据安全审计管理系统支持定时生成报表，在报表上方单击【定时生成报表】，弹出定时生成报表弹窗，依次输入模板名称、统计周期（可选择定时执行、每天一次、每周一次、每月一次）、执行时间（精确到时分秒）、报告说明，设置完成后，单击【确定】，即可在您设定的执行时间定时生成报表。

- **即时生成报表**

数据安全审计管理系统支持即时生成报表，即生成某个时间段内的报表，单击【即时生成报表】，依次输入报告名称、统计开始时间、统计结束时间、报告说明，单击【确定】，即可输出您规定的时间范围内的报表。

> **注意**
> 开始时间应早于结束时间。


即时生成报表
* 报告名称:
最多30个字符
* 统计开始时间:
2020-04-12 00:00:00
* 统计结束时间:
2020-04-12 23:59:59
* 报告说明:
最多200个字符
取 消
确 定

数据资产与 Agent

最近更新时间：2025-05-27 16:30:32

本文档将为您介绍如何部署审计 Agent，并指导您操作审计列表。

Agent 配置

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【数据资产与 Agent】>【审计用 Agent】，即可进入审计用 Agent 页面。
3. Agent 部署。在审计用 Agent 页面，选择【Agent 配置】>【添加 Agent】，可配置审计 Agent 的各类参数并提供下载链接，配置步骤以及配置注意事项，请参见 Agent 部署 。
4. 添加完成 Agent 后，在 Agent 配置页面，可查看所有已正确安装且能实现 DSA(Data Security Audit）实例网络互通的 Agent 信息。

列表各字段含义如下：

- Agent 名称：用于配置该 Agent 的名称。
- 审计服务 IP： Agent 回传数据的源 IP。
- 审计服务端口：该 Agent 配置的审计端口。
- 数据库 IP：单击【详情】可查看该 Agent 审计的数据库的所有 IP 地址。
- 审计 IP：用于显示该 Agent 配置的审计范围，由于 IP 范围内容较多，可单击【详情】进行阅览。
- 操作：用于下载该 Agent 的链接。
  - 单击【下载 Linux Agent】或【下载 Windows Agent】，弹出部署 IP 窗口，可以按 IP 部署或按 IP 段部署（IP 段支持全段审计），单击【确定】即可开始下载 Agent 。

> **注意**
> - 若部署机器操作系统 CentOS 版本号小于7 或者 Ubuntu 版本号小于11，必须勾选下方说明，否则无法部署 Agent。
> - 请添加安装包需要部署机器的 IP 或 IP 列表。
> - 如未添加 IP 信息却部署了会导致 Agent 无法启动。
> - 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

  - 单击【删除】，可删除该条 Agent 信息。

审计列表

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 useradmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【审计用 Agent】>【审计列表】，即可进入审计列表中。
3. 在审计列表中，可以查看所有已配置的 Agent。审计列表默认展示内容包括：deployMac、部署服务器 IP、审计服务、部署状态、Agent 状态、系统类型、部署时间运行时长及相关操作。
   - **搜索**：您可以按照部署状态、Agent 状态、审计服务 IP、Port（端口）对 Agent 进行搜索。
   - **查看 Agent 配置详情**：在“审计服务”栏中，单击【Agent 配置详情】，可以查看 Agent 配置相关信息。
   - **相关操作**：在右侧操作栏，可以对 Agent 进行启动、停止、卸载、删除的相关操作。

配置管理
审计组配置

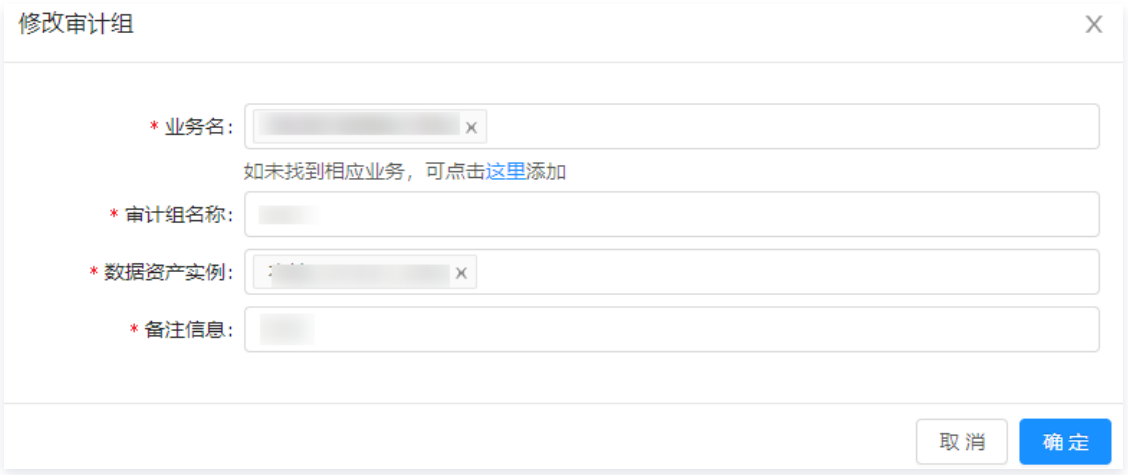
最近更新时间：2025-01-10 19:17:23

审计组配置可为从属于一个应用的一台或多台数据库服务器进行命名，方便后续规则配置或审计信息时，使用直观的名字来表达数据库信息，优化策略和报表可读性。下面将为您详细介绍配置操作。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录 。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【配置管理】>【审计组】，即可进入审计组配置页面。
   - **新增审计组**。
     在审计组列表上方单击【添加】，在新弹出的窗口中，填写业务名，审计组名称（建议以业务应用名称为基础命名）、数据资产实例、备注信息 后，单击【确定】，即可新增审计组。

     > **注意**
     > 数据库 IP 及端口必须填写需要审计数据库的 IP 和端口，不能为0.0.0.0。

   - **修改审计组**。
     在审计组列表中，找到需要修改的审计组，在右侧操作栏单击【修改】，在弹框中修改信息后单击【确定】即可。



   - **删除审计组**
     在审计组列表中，找到需要删除的审计组，在右侧操作栏单击【删除】，再单击询问窗中的【确定】即可。

     > **注意**
     > 删除审计组会解除该审计组下所有规则的绑定关系，如删除审计组所关联的规则仅和删除审计组有绑定关系时，该规则也会被删除。


+ 添加
删除
名称：数据安全审计，版本：合规版，最大审计组数：3，已添加审计组数：1
审计组名称
包含数据库台数
部门及业务名
备注
test1
1
测试部-数据审计测试
0105
修改
删除
删除审计组会解除该审计组下所有规则的绑定关系；如删除审计组所关联的规则仅和删除审计组有绑定关系时，该规则也会被删除。您确认删除所选的审计组吗？
取 消
确 定

访问源配置

最近更新时间：2025-01-10 19:17:23

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名，方便后续规则配置、审计信息使用直观名字来表达数据库访问端信息，优化策略以及报表可读性。下面将为您详细介绍配置操作。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【配置管理】>【访问源】，即可进入访问源配置列表页面。

- **添加访问源**

  单击列表上方【添加】，在弹出窗口中，填写业务名、访问源名称、访问源包含 IP 段、备注信息，单击【确定】即可。

- **修改访问源**

  在访问源列表中，找到需要修改的访问源，在右侧操作栏中，单击【修改】，在弹框中修改信息后，单击【确定】即可。

- **删除访问源**

  在访问源列表中，找到需要删除的访问源，在右侧操作栏中，单击【删除】，再单击询问窗中的【确定】即可。

部门业务配置

最近更新时间：2025-05-27 16:30:32

部门业务配置包含部门配置与业务配置两大模块功能，具体配置步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【配置管理】>【部门&业务】，即可进入部门业务配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在部门业务配置页面，可进行部门配置及业务配置。

- **部门配置**

3.1 在部门业务配置页面，单击【部门配置】，可添加并查看部门名、部门负责人及备注，同时可进行相关操作。

3.2 在部门设置页面，单击【添加部门】，在弹出的添加部门窗口中，填写部门名、部门负责人以及备注信息，单击【确定】即可完成添加。

3.3 添加完成后，已添加的部门将出现在部门配置列表中，支持对已添加的部门进行修改或删除，且支持对部门信息批量选择删除。

- **修改**
  找到需要修改的部门信息，在右侧操作栏单击【修改】，在弹出框中可以修改对应部门信息。
- **删除**
- **方式1**：找到需要删除的部门信息，在右侧操作栏单击【删除】，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的部门，在列表上方单击【删除】，即可批量删除部门信息。

- **业务配置**

3.1 在部门业务配置页面，单击【业务配置】，可添加并查看业务名、业务负责人、部门名及备注，同时可进行相关操作。

3.2 在业务配置页面，单击【添加业务】，在弹出的添加业务窗口中，填写部门名、业务名、业务负责人以及备注信息，填写完成后，单击【确定】即可完成添加。

3.3 添加完成后，已添加的业务将出现在业务配置列表中，支持对已添加的业务进行修改或删除，且支持对业务信息进行批量选择删除。

- **修改**
  找到需要修改的业务信息，在右侧操作栏单击【修改】，在弹出框中可以修改对应业务信息。
- **删除**
- **方式1**：找到需要删除的业务信息，在右侧操作栏单击【删除】，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的业务，在列表上方单击【删除】，在弹出框中确认删除，即可批量删除业务信息。

操作日志管理

最近更新时间：2025-01-10 19:17:23

操作审计员负责审计数据安全审计各管理员的操作，防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后，能够阅览管理员操作日志列表并对行为规则进行配置。

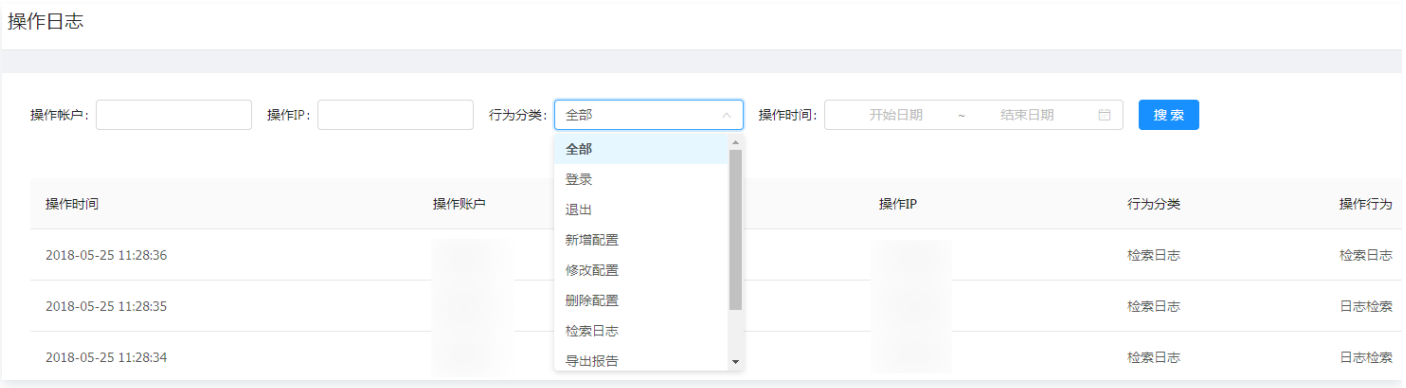
日志检索

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入操作日志页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在操作日志页面，您可以根据操作账户、操作 IP、行为分类、操作时间检索还原非法操作完整信息。



行为规则配置

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入行为规则配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在行为规则配置页面，可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作，同时可按照行为分类、行为操作及危险等级，对行为规则进行搜索。

> **说明**
> 所有数据由系统内置生成，用户可以根据需求进行修改。

字段说明：

- **行为操作：用户对系统各个账户的功能操作。**
- **行为分类：用户对系统功能操作所属的模块名**
- **告警模板：用户执行操作时邮件所发送的告警内容**
- **备注：用户对行为规则的进一步说明。**
- **危险等级：对用户操作行为的评级，可设置行为危险等级，包括低级、中级及高级。**
- **是否开启告警：用户开启后，触发行为规则审计，则会发送告警信息，关闭后，只会记录操作，不会发送告警信息。**
- **操作：在目标行为右侧操作栏，单击修改，即可对行为操作信息进行修改。**

v5.0.5
系统管理
系统资源监控

最近更新时间：2025-01-10 19:17:23

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【系统资源监控】，即可进入资源监控页面，该页面包括系统详细信息、系统存储空间统计和流量走势实时统计。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

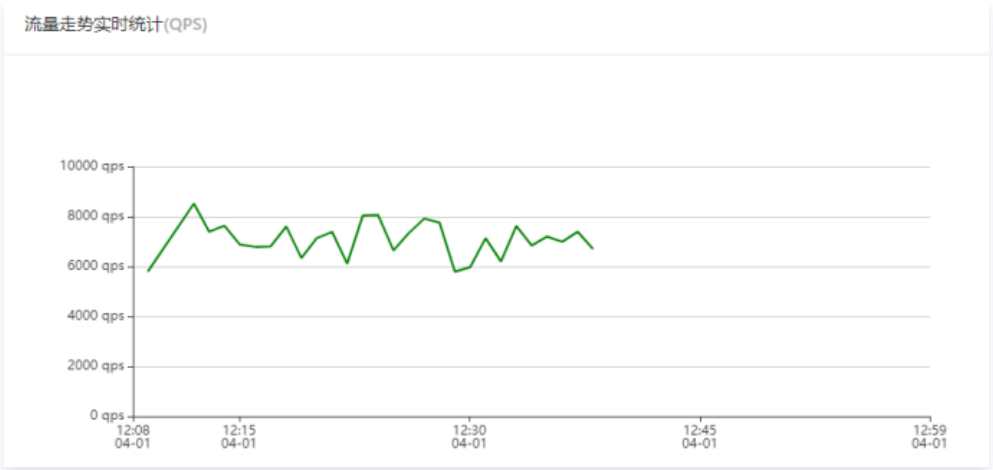
- **系统详细信息**
  系统详细信息包含系统产品名称、系统版本等基础信息，以及数据安全审计总审计组数参数信息。

- **系统存储空间统计**
  存储空间统计用于展示数据安全审计实例当前的存储状态。在系统存储空间统计右上角，单击【清理剩余空间】，将清理的数据包含所选的日期。例如，选择了12月1日至12月3日，则会删除12月1日、2日、3日，3天的数据。

> **说明**
> 统计报表将磁盘空间分为四个类型：
> - 剩余空间：数据安全审计实例存储剩余空间；
> - 系统占用空间：数据安全审计自身代码所占存储空间；
> - 审计日志占用空间：数据安全审计记录的数据库操作信息日志占用空间；
> - 其他占用空间：数据安全审计实例其他代码、配置文件占用空间。

- **流量走势实时统计**

  流量走势实时统计能统计一定时间跨度（最近30分钟、最近24小时、最近7天）内数据安全审计中所审计的所有数据库的 QPS，确认全网 QPS 峰值是否超过购买峰值，以帮助管理员了解数据安全审计性能状况，及时扩容升级产品。



用户管理

最近更新时间：2025-05-27 16:30:32

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中单击【用户管理】即可进入用户页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

- **查看账号信息**

  账号管理用于管理 DSA 实例所有账号。系统管理员可以通过列表查看所有账号信息，包括所属角色、真实姓名、创建日期以及联系方式等。

  > **说明**
  > OTP 二维码：如需开启 OTP 实现登录双重验证，可在相应账号右侧操作栏，单击【OTP二维码】，或在数据安全审计管理页面右上角，找到管理员账号下的 OTP 验证，单击【OTP 验证】，查看原图并扫描动态校验码。

- **添加账号**

  如需要增加管理员账号，单击【添加账号】，在弹框中填写账号信息，选择所属角色后，单击【确定】即可。

- **修改和删除账号**

  如需对账号进行修改或删除，可在相应账号操作列单击【编辑】或【删除】对账号进行调整。

> **注意**
>
> 系统默认创建账号不可删除。

Agent 管理
Agent 配置

最近更新时间：2025-05-27 16:30:32

配置 Agent 后可将 Agent 部署在 Linux 系统或 Windows 系统，进行具体审计组配置后，实现对数据库操作的管理。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【Agent 管理】>【Agent 配置】，即可进入 Agent 配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. Agent 部署。在 Agent 配置页面，单击【配置 Agent】，可配置审计 Agent 的各类参数并提供下载链接。
4. 配置 Agent。配置 Agent 用于展示所有已正确安装且能实现 DSA 实例网络互通的 Agent 信息。

列表各字段含义如下：

- 审计服务 IP： Agent 回传数据的源 IP。
- 审计服务端口：该 Agent 配置的审计端口。
- 数据库 IP：单击【详情】可查看该 Agent 审计的数据库的所有 IP 地址。
- 审计 IP：用于显示该 Agent 配置的审计范围，由于 IP 范围内容较多，可单击【详情】进行阅览。
- 操作：用于下载该 Agent 的链接。
  - 单击【下载 Linux Agent】或【下载 Windows Agent】，弹出部署 IP 窗口，可以按 IP 部署或按 IP 段部署（IP 段支持全段审计），单击【确定】即可开始下载 Agent 。

> **注意**
> - 若部署机器操作系统 centos 版本号小于7.0 或者ubuntu 版本号小于11，必须勾选下方说明，否则无法部署 Agent。
> - 请添加安装包需要部署机器的 IP 或 IP 列表。
> - 如未添加 IP 信息却部署了会导致 Agent 无法启动。
> - 如有新的机器要部署请重新下载安装包并填写机器的 IP 信息。

- 单击【Linux 批量部署】，输入部署地址，支持按 IP 或按 IP 段部署，支持添加多行，输入服务器 IP 、SSH 端口号、用户名、密码， 输入完成后单击【确定】即可。

Agent 列表

最近更新时间：2025-01-10 19:17:23

本文将为您介绍如何查看并操作 Agent 列表。

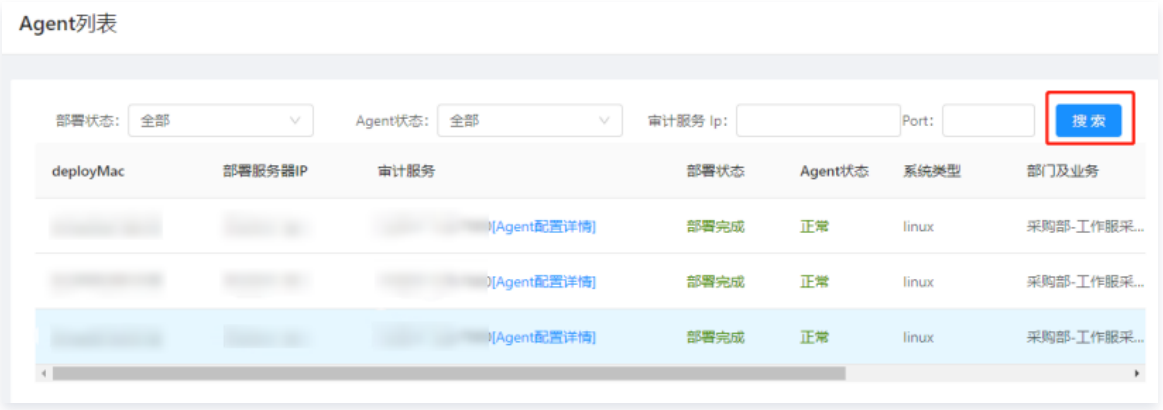
操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【Agent 管理】>【Agent 列表】，即可进入 Agent 列表中。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在 Agent 列表中，可以查看所有已配置的 Agent。Agent 列表默认展示内容包括：deployMac、部署服务器 IP、审计服务、部署状态、Agent 状态、系统类型、部门及业务。
   - **搜索**：您可以按照部署状态、Agent 状态、审计服务 IP、Port（端口）对 Agent 进行搜索。
   - **查看 Agent 配置详情**：在“审计服务”栏中，单击【Agent 配置详情】，可以查看 Agent 配置相关信息。
   - **相关操作**：在右侧操作栏，可以对 Agent 进行启动、停止、卸载、删除的相关操作。



时间服务器

最近更新时间：2025-05-27 16:30:32

时间服务器主要用于同步时间，找到您需要需要同步时间的服务器IP进行设置即可，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击【管理】，进入数据安全审计登录界面。

2. 使用 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，单击【时间服务器】，即可进入时间服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在时间服务器设置页面，输入 NTP 服务器 IP，单击【提交】，即可完成设置。

4. 设置完成后，数据安全审计系统时间会与您设置的 NTP 服务器为标准进行时间同步。

系统设置
告警设置

最近更新时间：2025-01-10 19:17:23

告警支持针对每个审计规则策略进行告警，告警方式支持邮件告警、syslog 告警，其中系统资源告警配置可根据您设置的磁盘、内存等告警阈值，当达到阈值时，进行告警；syslog 告警配置可配置您接收告警信息的 syslog 服务器；邮件告警配置可配置您接收告警信息的邮件服务器，具体操作步骤如下：

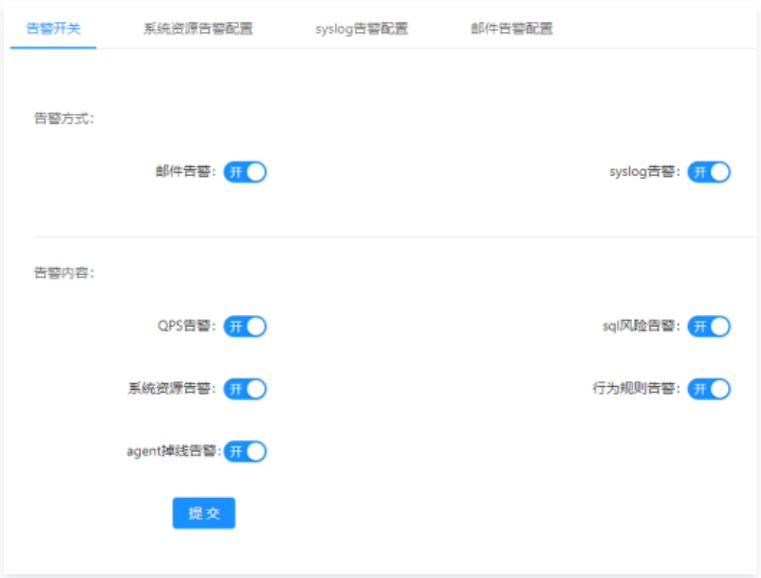
1. 登录 数据安全审计控制台，找到需要操作的审计系统，在右侧操作栏，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中选择【系统设置】>【告警设置】，即可进入告警设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在告警设置页面，分别对告警开关、系统资源告警配置、syslog 告警配置及邮件告警配置功能进行设置。
   - **告警开关**
     在告警设置页面，单击【告警开关】，分为【告警方式】和【告警内容】，打开需要开启告警的选项，单击【提交】，即可对 syslog 告警配置 中所设置的服务器进行监控，且当满足告警条件时，将触发告警，并发送邮件至您所 配置的告警邮箱 中。

     > **注意**
     > 若需要接收告警信息，需打开邮件告警开关，且已在 邮件告警配置 中设置告警接收邮箱，否则无法接收告警信息。



   - **系统资源告警配置**
     在告警设置页面，单击【系统资源告警配置】，设置系统资源告警的触发条件，可将磁盘、内存、CPU 负载在0 – 100%之间调整，可自定义带宽值，单

击【提交】，即可对 syslog 告警配置 中所设置的服务器进行监控。

- **syslog 告警配置**

> **注意**
> 目前 syslog 告警服务只支持 TCP 协议。

在告警设置页面，单击【syslog 告警配置】，输入需要记录的 syslog 服务器 IP 和端口，单击【提交】，即可完成 syslog 告警条件配置，设置完成后接收到相关告警信息。

- **邮件告警配置**

单击【邮件告警配置】，依次填入邮件服务器的相关配置信息，如需添加多个收件人，请以英文分号分隔，填写完成后，单击【提交】，当满足告警条件时，将发送邮件至所配置的邮箱中。

> **注意**
> 若填写 QQ 邮箱账号，密码需填写所设置的邮箱密码。


告警开关
系统资源告警配置
syslog告警配置
邮件告警配置
* SMTP服务器:
第三方邮件服务容易受服务器反垃圾机制影响，如遇到不可用的，建议尝试切换其他邮件服务
* 端口:
* 邮件账号:
* 密码:
此密码非邮箱登录密码
* 发件人:
收件人:
多个收件人请以分号；分隔
SSL:
测试
提交
重置

备份服务器

最近更新时间：2025-01-10 19:17:23

为了您审计数据的安全，我们为您提供了备份服务器设置，当设置了具体的服务器地址、路径等项目后，将按天备份审计数据。

> **注意**
> 建议您在配置好数据审计服务后，第一时间设置备份服务器，达到审计数据的及时安全备份。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【系统设置】>【备份服务器设置】，即可进入备份服务器设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在备份服务器设置页面，依次输入备份服务器地址、备份服务器端口、备份服务器用户名、备份服务器密码、备份服务器目录路径，打开备份开关，单击【保存】即可完成备份服务器设置。

4. 设置完成后，数据安全审计管理系统中的数据将会按照设置路径进行备份。

OTP 设置

最近更新时间：2025-05-27 16:30:32

本文档将为您介绍如何开启 OTP 校验，并通过 OTP 校验登录数据安全审计管理页面。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以 sysadmin 账号登录数据安全审计管理页面，在左侧导航栏中，选择【系统设置】>【OTP 设置】，即可进入 OTP 设置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在 OTP 设置页面，设置校验开关，如需开启 OTP 验证选项，选中开启 OTP 验证，单击【保存】，退出登录系统即可。

> **说明**
> 建议开启 OTP 验证之前，提前通知各管理员登录系统扫描OTP验证二维码，避免其无法登录该系统。

4. 再次登录数据安全审计管理页面，需要输入OTP 校验码。

审计管理
审计数据

最近更新时间：2025-05-27 16:30:32

审计概览

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【审计数据】>【审计概览】，即可进入审计概览页面。
3. 在审计概览页面中，可总览全网数据库各类排行信息以及查询单个数据库实例概览信息，如需了解数据库审计组详细内容，可在审计概览页面下方查询审计组的详细信息。
   - **数据库排行统计**：上方条形统计图为数据库排行，排行统计数据内容如下：
     - **风险排行**：用于统计全网各数据库风险总数，降序排列。
     - **语句压力排行**：用于统计全网各数据库语句压力总数，降序排列。
   - **审计组详情**：审计组详情内可查看您所配置的审计组的风险分布 Top5、语句压力统计 Top5（QPS），会话分布 Top5，还可按照全部、高风险、中风险、低风险进行查看各个风险级别详细数据，每个报表可展示三种走势图及三类风险级别数据：
     - **风险分布**：用于展示本数据库审计组高中低三类风险的统计信息，展示时间范围可在1天到365天之间进行调整。
     - **自定义规则命中**：用于展示与本数据库审计组有关的自定义规则命中信息，展示时间范围可在1天到365天之间进行调整。
     - **语句压力统计**：用于展示本数据库审计组语句压力的统计信息，展示时间范围可在1天到365天之间进行调整。
     - **会话统计**：用于展示本数据库审计组各类会话信息，展示时间范围可在1天到365天之间进行调整。

日志检索

日志检索主要提供日志查询与导出功能。

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【审计数据】>【日志检索】，即可进入日志检索页面。

3. 管理员通过 审计概览 定位到疑似有风险的数据库审计组，或者企业网络已经发生数据库安全问题时，可在日志检索页面查询并导出日志信息。

日志查询

在日志检索页面，您可以按照审计组、风险等级、用户名、命中规则及时间，对日志进行查询。

查看数据详情

在日志列表中，可单击某条记录查看其详细内容。

日志导出

检索出需要导出的数据，现已支持不限数量导出，在列表上方单击【导出】，弹出导出数据弹窗，单击【确定】即可将数据导出，导出文件类型为 Excel（.xlsx格式）。

> **注意**
> 尽量缩小导出范围，导出数量过多，会影响服务器性能。

审计配置
审计组配置

最近更新时间：2025-01-10 19:17:23

审计组配置可为从属于一个应用的一台或多台数据库服务器进行命名，方便后续规则配置或审计信息时，使用直观的名字来表达数据库信息，优化策略和报表可读性，下面将为您详细介绍配置操作。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面，详情可参见 控制台登录。
2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【审计配置】>【审计组配置】，即可进入审计组配置页面。
   - **新增审计组。**
     在审计组列表上方单击【添加】，在新弹出的窗口中，填写业务名，审计组名称（建议以业务应用名称为基础命名）、数据库类型、数据库 IP、数据库端口、版本信息、备注信息后，单击【确定】即可新增审计组。

     > **注意**
     > 数据库 IP 及端口必须填写需要审计数据库的 IP 和端口，不能为0.0.0.0。

   - **修改审计组。**
     在审计组列表中，找到需要修改的审计组，在右侧操作栏单击【修改】，在弹框中修改信息后单击【确定】即可。

   - **删除审计组**
     在审计组列表中，找到需要删除的审计组，在右侧操作栏单击【删除】，再单击询问窗中的【确定】即可。

注意

删除审计组会解除该审计组下所有规则的绑定关系，如删除审计组所关联的规则仅和删除审计组有绑定关系时，该规则也会被删除。

访问源配置

最近更新时间：2025-01-10 19:17:23

访问源配置可为从属于同一部门或同一网络区域的访问 IP 段进行命名，方便后续规则配置、审计信息使用直观名字来表达数据库访问端信息，优化策略以及报表可读性。下面将为您详细介绍配置操作。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中单击【审计配置】>【访问源配置】即可进入访问源配置列表页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

- **添加访问源**
  单击列表上方【添加】，在弹出窗口中，填写业务名、访问源名称、访问源包含 IP 段、备注信息，单击【确定】即可。

- **修改访问源**
  在访问源列表中，找到需要修改的访问源，在右侧操作栏中，单击【修改】，在弹框中修改信息后，单击【确定】即可。

- **删除访问源**
  在访问源列表中，找到需要删除的访问源，在右侧操作栏中，单击【删除】，再单击询问窗中的【确定】即可。


访问源名称
包含IP段数量
部门及业务名
备注
1
ds
1
ds
修改
删除
您确认要删除吗?
取消
确定

规则配置

最近更新时间：2025-05-27 16:30:32

规则配置可定义数据安全审计的审计组的安全规则。数据安全审计具备两个默认规则，AI 引擎规则和 CVE 引擎规则，默认规则不可删除、不可编辑，下面将为您详细介绍配置操作。

操作步骤

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【审计配置】>【规则配置】，即可进入规则配置页面。

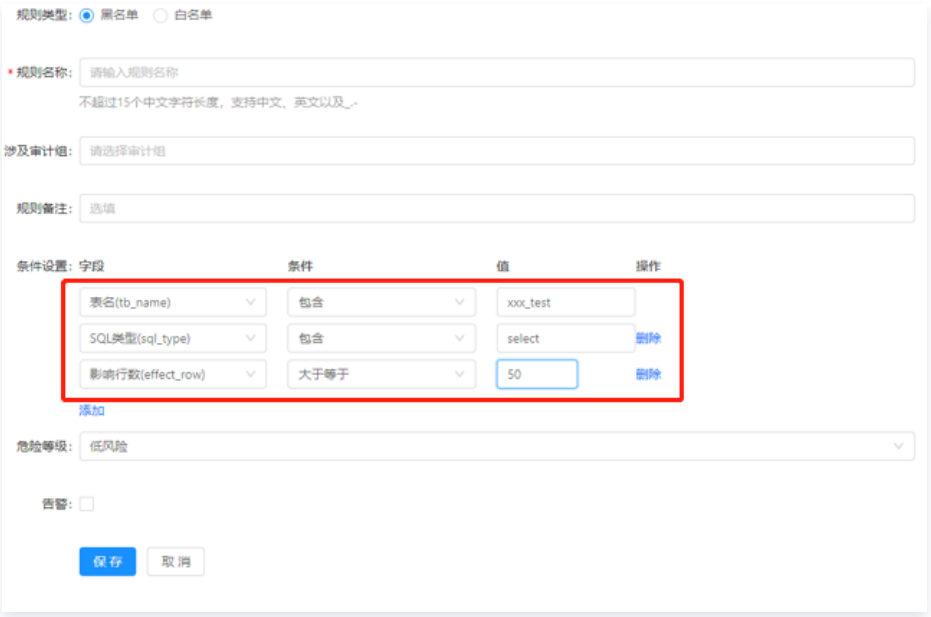
新建规则

如需自定义规则满足个性化审计需求，单击【添加规则】，进入新建规则页面，填写规则名称等，单击【保存】即可。

> **注意**
> - 规则配置支持同一规则配置多个条件，多个条件之间为 “与” 关系，必须全部匹配才能够触发规则和告警。
> - 自定义规则默认为黑名单，触发后将产生告警并且记录入库。如果管理员需要节省数据安全审计的审计组的存储空间，指定部分操作行为不记录不入库，可在规则中指定相关操作后，选择 “白名单” 选项，并且将告警选项都取消。

以上操作完成后，即可实现白名单类型规则配置，减少误报、减轻数据安全审计的审计组存储压力。

- **规则示例**
  在规则配置页面，单击【添加规则】，按下图配置规则，表名和阈值根据您的业务场景自行设定，单击【保存】即可。



- **规则配置建议**

  以下三个建议规则仅作为示例，用户可根据自身业务自行配置。

  - **防爬取规则**：防止使用例如 select 操作语句，爬取表数据。

    > **注意**
    > 影响行数可以根据业务自行配置。

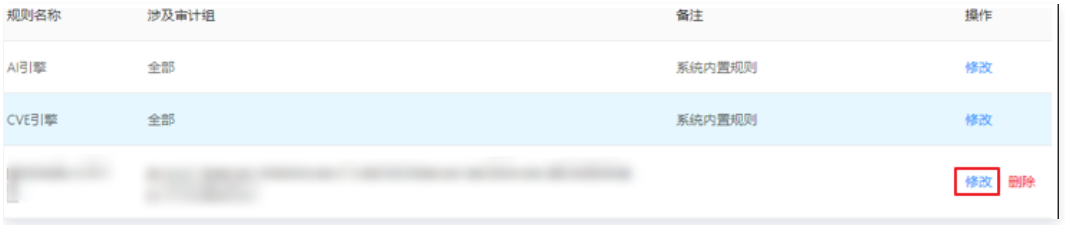
  - **慢查询发现规则**：检查执行时间较长的 SQL 语句，便于进行优化。

    > **注意**
    > 执行时间可以根据业务自行配置。

- **危险操作规则**：检查执行 DELETE/DROP/ALTER 等类型的高危 SQL 语句。

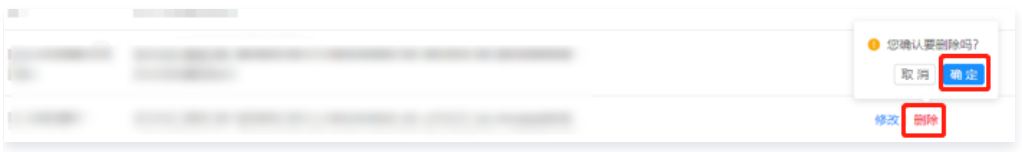
修改规则

在规则列表中，找到需要修改的规则，在右侧操作栏中，单击【修改】，修改信息后单击【保存】即可。



删除规则

在规则列表中，找到需要删除的规则，在右侧操作栏中，单击【删除】，再单击询问窗【确定】即可。



部门业务配置

最近更新时间：2025-01-10 19:17:23

部门业务配置功能主要是部门配置与业务配置的相关功能，具体配置步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中，选择【配置管理】>【部门&业务】，即可进入部门业务配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在部门业务配置页面，可进行部门配置及业务配置。

- **部门配置**

3.1 在部门业务配置页面，单击【部门配置】，可添加并查看部门名、部门负责人及备注，同时可进行相关操作。

3.2 在部门设置页面，单击【添加部门】，在弹出的添加部门窗口中，填写部门名、部门负责人以及备注信息，单击【确定】即可完成添加。

3.3 添加完成后，已添加的部门将出现在部门配置列表中，支持对已添加的部门进行修改或删除，且支持对部门信息批量选择删除。

- **修改**
  找到需要修改的部门信息，在右侧操作栏单击【修改】，在弹出框中可以修改对应部门信息。
- **删除**
- **方式1**：找到需要删除的部门信息，在右侧操作栏单击【删除】，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的部门，在列表上方单击【删除】，即可批量删除部门信息。

- **业务配置**

3.1 在部门业务配置页面，单击【业务配置】，可添加并查看业务名、业务负责人、部门名及备注，同时可进行相关操作。

3.2 在业务配置页面，单击【添加业务】，在弹出的添加业务窗口中，填写部门名、业务名、业务负责人以及备注信息，填写完成后，单击【确定】即可完成添加。

3.3 添加完成后，已添加的业务将出现在业务配置列表中，支持对已添加的业务进行修改或删除，且支持对业务信息进行批量选择删除。

- **修改**
  找到需要修改的业务信息，在右侧操作栏单击【修改】，在弹出框中可以修改对应业务信息。
- **删除**
- **方式1**：找到需要删除的业务信息，在右侧操作栏单击【删除】，在弹出框中确认删除，即可完成删除。
- **方式2**：选择需要删除的业务，在列表上方单击【删除】，在弹出框中确认删除，即可批量删除业务信息。

自定义报表

最近更新时间：2025-01-10 19:17:23

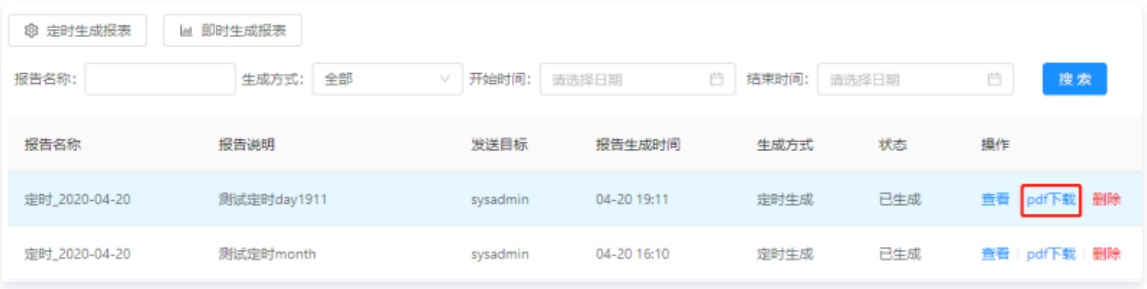
自定义列表功能主要展示所有配置过的审计组数据，并提供搜索、导出及 PDF 下载功能，具体操作步骤如下：

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击【管理】，进入数据安全审计管理系统登录界面。

2. 以审计管理员账号登录数据安全审计管理页面，在左侧导航栏中选择【报表】>【自定义报表】，即可进入自定义报表页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

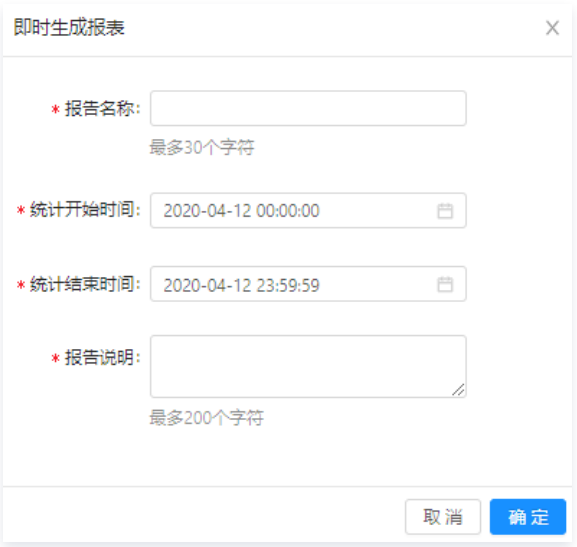
3. 在自定义报表页面中，可查看内容包括报告名称、报告说明及发送目标等字段，同时可以进行相关操作，每个页面默认展示10条数据，可按照报告名称、生成方式、开始时间及结束时间，对报告进行搜索，还可下载 PDF 报告。



- **定时生成报表**
  数据安全审计管理系统支持定时生成报表，在报表上方单击【定时生成报表】，弹出定时生成报表弹窗，依次输入模板名称、统计周期（可选择定时执行、每天一次、每周一次、每月一次）、执行时间（精确到时分秒）、报告说明，设置完成后，单击【确定】，即可在您设定的执行时间定时生成报表。

- **即时生成报表**
  数据安全审计管理系统支持即时生成报表，即生成某个时间段内的报表，单击【即时生成报表】，依次输入报告名称、统计开始时间、统计结束时间、报告说明，单击【确定】，即可输出您规定的时间范围内的报表。

> **注意**
> 开始时间应早于结束时间。


即时生成报表
* 报告名称:
最多30个字符
* 统计开始时间:
2020-04-12 00:00:00
* 统计结束时间:
2020-04-12 23:59:59
* 报告说明:
最多200个字符
取 消
确 定

操作日志管理

最近更新时间：2025-01-10 19:17:23

操作审计员负责审计数据安全审计各管理员的操作，防止其他管理员滥用职权进行非法操作。用操作管理员账号登录后，能够阅览管理员操作日志列表并对行为规则进行配置。

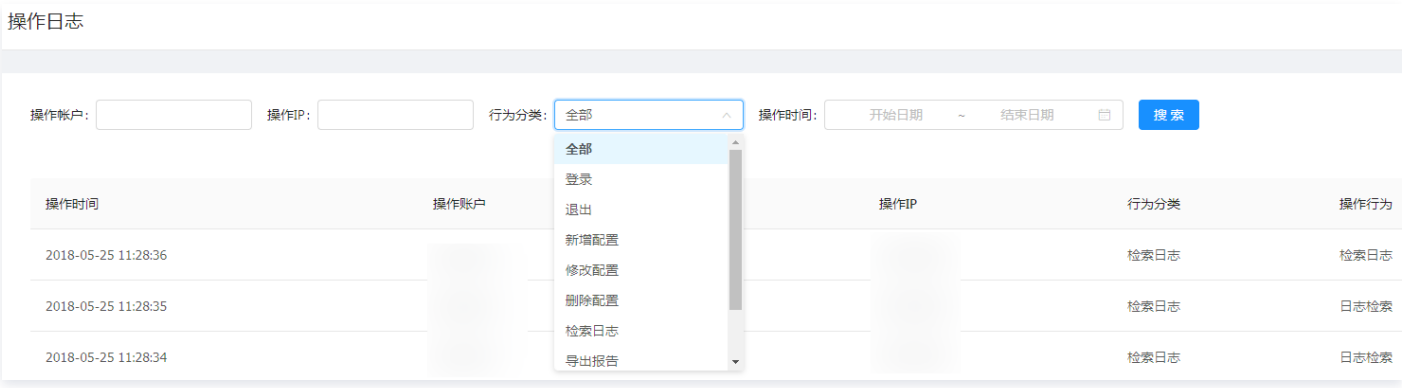
日志检索

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入操作日志页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在操作日志页面，您可以根据操作账户、操作 IP、行为分类、操作时间检索还原非法操作完整信息。



行为规则配置

1. 登录 数据安全审计控制台，找到需要操作的审计系统，单击**管理**，进入数据安全审计管理系统登录界面。

2. 以操作管理员账号登录操作日志页面，在左侧导航栏中单击**行为规则配置**，即可进入行为规则配置页面。

> **说明**
> 如忘记登录密码，可以 提交工单 找回密码。

3. 在行为规则配置页面，可以查看行为操作、行为分类、告警模板、备注、是否开启告警及相关操作，同时可按照行为分类、行为操作及危险等级，对行为规则进行搜索。

> **说明**
> 所有数据由系统内建生成，用户可以根据需求进行修改。

字段说明：

- **行为操作：用户对系统各个账户的功能操作。**
- **行为分类：用户对系统功能操作所属的模块名**
- **告警模板：用户执行操作时邮件所发送的告警内容。**
- **备注：用户对行为规则的进一步说明。**
- **危险等级：对用户操作行为的评级，可设置行为危险等级，包括低级、中级及高级。**
- **是否开启告警：用户开启后，触发行为规则审计，则会发送告警信息，关闭后，只会记录操作，不会发送告警信息。**
- **操作：在目标行为右侧操作栏，单击修改，即可对行为操作信息进行修改。**