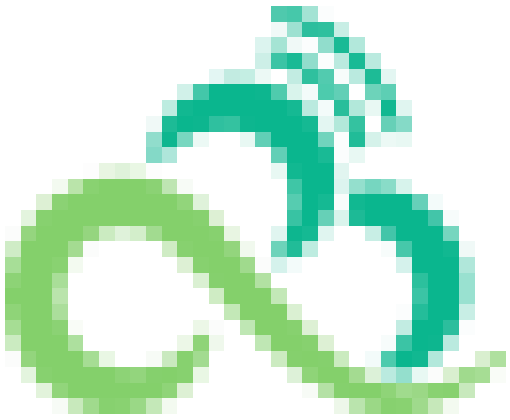
数据安全审计（DSAuditSaaS）

产品文档



版权所有：尚航云_V1

文档目录

常见问题
- 无法在审计日志页面查询到日志，如何处理？

操作指南
- 数据资产
  - 管理云数据库
  - 管理自建数据库
- 查询分析
  - 检索审计日志
  - 查看审计日志
  - 检索审计风险
  - 查看审计风险
  - 检索审计会话
  - 查看会话详情
- 审计规则
  - 新建规则
  - 快速配置规则
  - 启用规则
- 审计报表
  - 新建报表
  - 查看报表
- 配置管理
  - 下载Agent
  - Agent列表
  - 告警设置

快速入门
- 操作指引
- Agent部署

产品介绍
- 产品介绍

版权所有：尚航云_V1

常见问题

无法在审计日志页面查询到日志，如何处理？

最近更新时间: 2024-08-23 15:08:00

现象描述

已购买数据安全审计 SaaS 型，却无法在审计日志页面查询到审计日志，如下图所示：



可能原因

未正确添加对应数据库或未开启审计权限。

数据库在本地操作，未经过网络。

数据库开启了 SSL 加密。

未正确部署 Agent。

检查是否添加资产并且开启审计权限

步骤1：检查是否已在数据资产页面 中，添加对应数据库，并开启审计权限。只有已添加，且开启审计权限的数据库，才可正常审计。

步骤2：检查添加的资产 IP 是否与客户端访问连接串中的 IP 地址相同。例如，添加的资产 IP 为内网 IP，而客户端使用外网 IP 访问数据库，则无法审计该操作，应将外网 IP 也配置在数据资产中才可正常审计；对于数据库集群，配置为主节点地址，但实际通过集群地址访问数据库，也无法审计该操作，应配置为集群地址才可正常审计。

步骤3：由于数据安全审计通过 Agent 抓取网络流量方式获取日志，因此如果在安装 Agent 的数据库服务器上直接通过 MySQL 命令登录不走网络，将无法审计到数据。可以在数据资产页面 增加一个 IP 为127.0.0.1的资产并开启审计权限，并且 MySQL 命令后面带上 `-h 127.0.0.1` 参数就可以审计到数据。

检查是否开启了SSL

步骤1：在数据库中，输入如下命令，确认是否开启了 SSL 加密。

```
showglobal variables like '%ssl%';
```

步骤2：如下图所示，若 have_ssl 的值为 YES，则表明已经开启了 SSL，需要关闭 SSL 后才能审计到。

```
dba:(none)> show global variables like '%ssl%';
+---------------+-----------------+
| Variable_name | Value           |
+---------------+-----------------+
| have_openssl  | YES             |
| have_ssl      | YES             |    #已经开启了SSL
| ssl_ca        | ca.pem          |
| ssl_capath    |                 |
| ssl_cert      | server-cert.pem |
| ssl_cipher    |                 |
| ssl_crl       |                 |
| ssl_crlpath   |                 |
| ssl_key       | server-key.pem  |
+---------------+-----------------+
```

检查是否正确部署Agent

步骤1：检查是否采用合适的 Agent 安装包，需要确保使用了与部署位置相对应的 Agent 安装包，才能正常审计。

步骤2：若部署 Agent 的机器为 Windows 操作系统，请确保安装目录中不包含空格。

步骤3：若 Agent 部署在应用服务器上，检查该服务器是否执行过对需审计数据库的 SQL 操作。在其他服务器上执行的 SQL 无法被本 Agent 采集到。

操作指南
数据资产
管理云数据库

最近更新时间: 2024-08-23 15:08:00

步骤1：进入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。

步骤2：在关系型云数据库页面，单击更新资产列表，自动拉取您在云账号内的数据库，同步成功则会在列表显示。





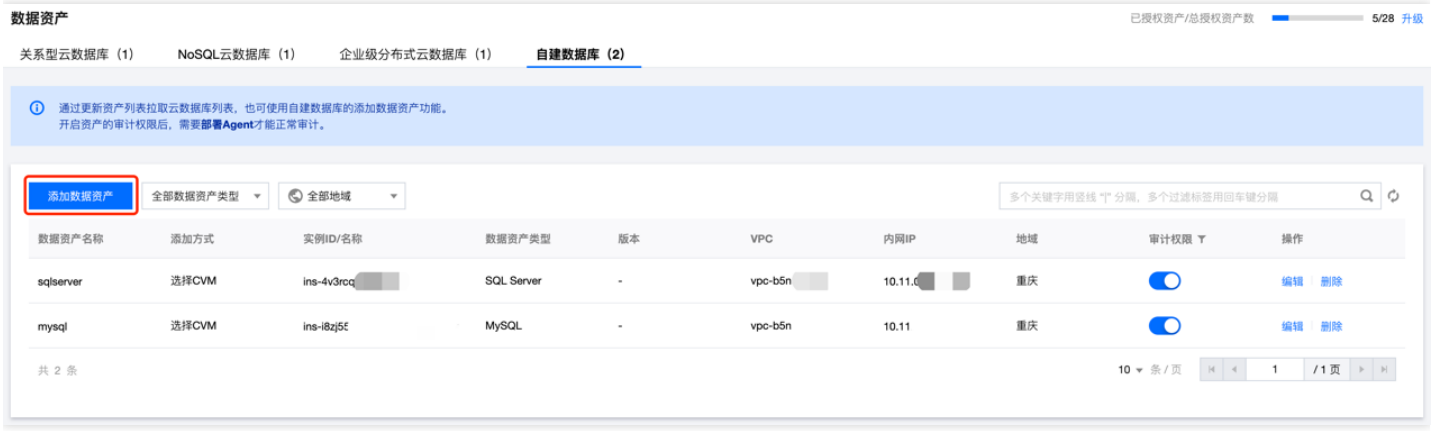
步骤3：选择一个实例，单击审计权限的 ，即审计权限开启成功。如关闭审计权限，将不再审计该资产。

管理自建数据库

最近更新时间: 2024-08-23 15:08:00

步骤1：进入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，进入关系型云数据库页面。

步骤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。



步骤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。





参数说明：

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。
VPC	可选项，可通过选择资产所在 VPC ，缩小 CVM 实例查找范围。
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。

版权所有：尚航云_V1

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。
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。 - MariaDB：5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3。 - SQL Server：2008、2012、2014、2016、2017。 - PostgreSQL：9、10、11。 - Oracle：9i、10g、llg、12c、18c、19c。 - Redis：所有版本都支持。 - MongoDB：2.x、3.x、4.x。 - Hive：所有版本都支持。 - HBase：所有版本都支持。
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。详情参见页面的配置参考链接。
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。

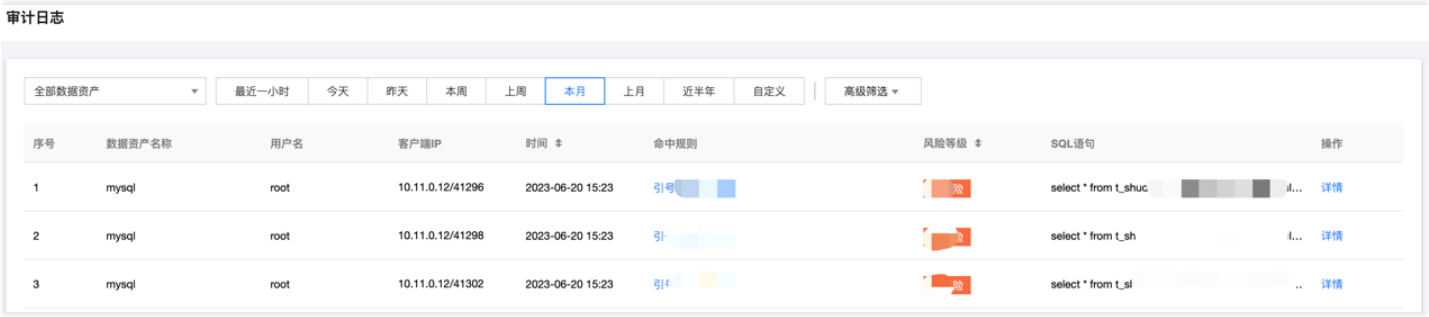
版权所有：尚航云_V1

查询分析
检索审计日志

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击查询分析 > 审计日志，进入审计日志页面。

步骤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。



步骤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 等关键字，输入具体值，单击查询，即可查看相关信息。

版权所有：尚航云_V1

查看审计日志

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击查询分析 > 审计日志，进入审计日志页面。

步骤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。

步骤3：在审计日志详情页面，可查看该条日志的基本信息和详细信息。

版权所有：尚航云_V1

审计日志详情

基本信息

操作语句	select @@vers 展开
操作类型	SELECT
操作时间	2023-06-20 15:23:15
SessionId	1687190400000-1407031
命中规则	-
风险等级	安全
数据库	-
数据库IP	10.11
数据库用户	root

详细信息

表名	-
影响行数	1
执行时间	0 ms
返回消息	-
返回码	0
客户端IP	10.11.0

检索审计风险

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击查询分析 > 审计风险，进入审计风险页面。

步骤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。



步骤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。

版权所有：尚航云_V1

查看审计风险

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击查询分析 > 审计风险，进入审计风险页面

步骤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。

步骤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。

版权所有：尚航云_V1

审计风险详情

基本信息

操作语句	select * from t_shu ; 展开
操作类型	SELECT
操作时间	2023-06-20 15:23:15
SessionId	1687190400000-1401
命中规则	探测
风险等级	高风险
数据库	-
数据库IP	10.11.
数据库用户	root

详细信息

表名	-
影响行数	0
执行时间	1 ms
返回消息	No database selected
返回码	1046
客户端IP	10.11.

检索审计会话

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击查询分析 > 审计会话，进入审计会话页面。

步骤2：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。



步骤3：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。

版权所有：尚航云_V1

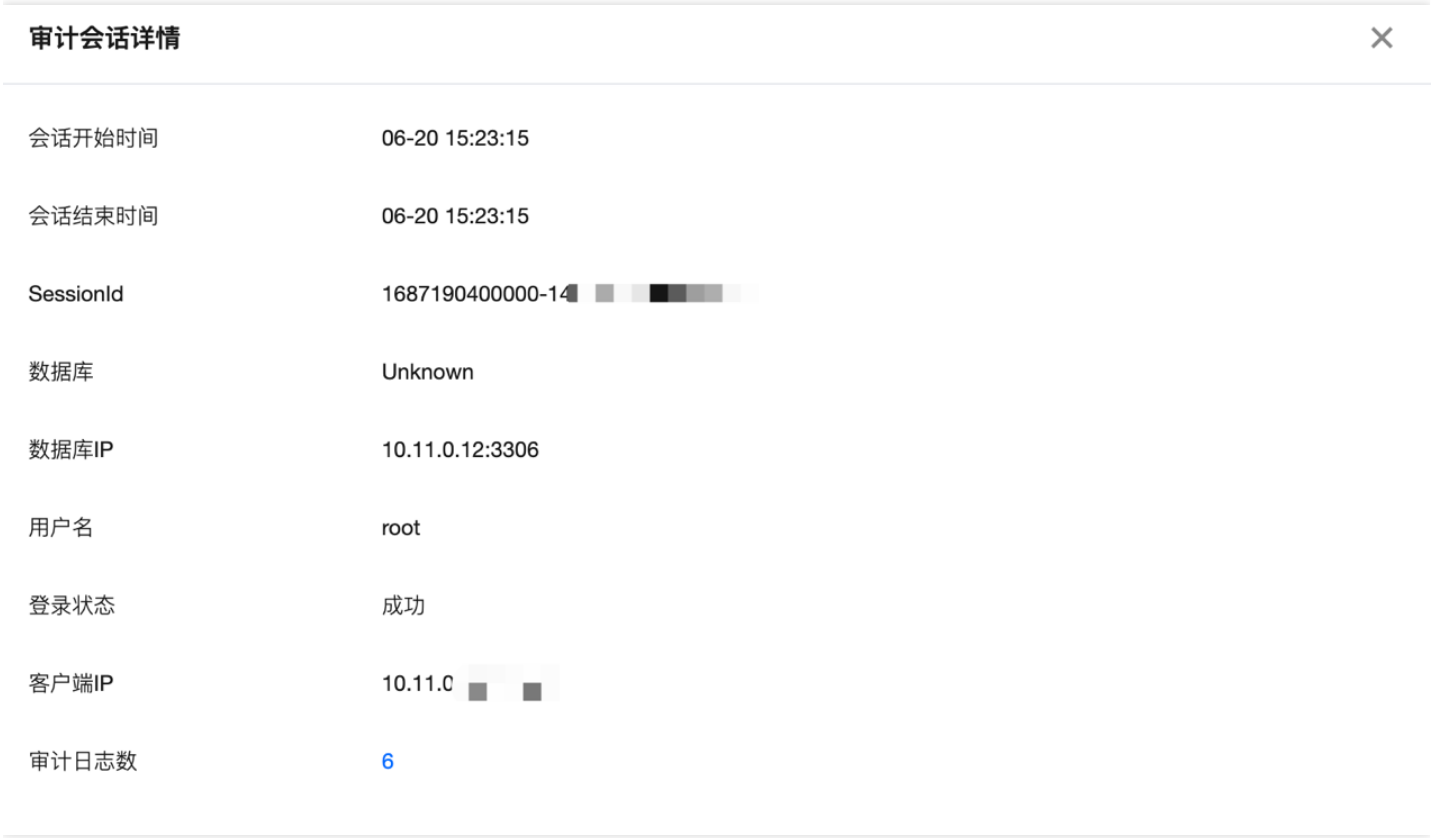
查看会话详情

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击查询分析 > 审计会话，进入审计会话页面。

步骤2：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。

步骤3：在审计会话详情页面，可查看该条日志的详细信息。



审计规则
新建规则

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击审计规则 > 规则列表。

步骤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。

版权所有：尚航云_V1



步骤3：配置完成后，单击确定即可。

版权所有：尚航云_V1

快速配置规则

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击审计规则 > 规则启用。

步骤2：在规则启用页面，单击快捷配置，弹出快捷配置弹窗。



步骤3：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。

版权所有：尚航云_V1


快捷配置确认
数据资产
tdsqlshard-
常见配置
宽松配置
严格配置
启用常见风险规则，适用于大多数场景。
确定
取消

启用规则

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，在左侧导航栏中，单击审计规则 > 规则启用。

步骤2：在规则启用页面，支持启用单个规则或批量启用规则。



审计报表

新建报表

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击审计报表 > 报表任务。

步骤2：在报表任务页面，单击新建任务。

步骤3：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。


新建任务
* 报表类型:
单次报表
即时生成报表
周期报表
建立周期性报表任务，届时自动生成报表
* 任务名称:
输入报表名称，最多64字符
报表名称将复用此任务名称
报表说明:
输入报表说明，最多256字符
0 / 256
* 报表模板:
综合分析报告
* 包含资产:
全部资产
* 时间范围:
近24小时
报表通知:
报表生成后将自动发送到所配置的通知范围
确定
取消

查看报表

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击审计报表 > 报表列表。

步骤2：单击操作列的预览，可查看对应的报表。

步骤3：单击操作列的下载，可下载对应的报表至本地查看。

配置管理
下载Agent

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击配置管理 > Agent 管理 > Agent 部署，进入 Agent 部署页面。

步骤2：在报表任务页面，单击新建任务。

步骤3：在 Agent 部署页面，根据操作系统类型，选择要下载的 Agent。

版权所有：尚航云_V1

Agent列表

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击配置管理 > Agent 管理 > Agent 列表，进入 Agent 列表页面。

步骤2：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。

步骤3：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。

步骤4：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。

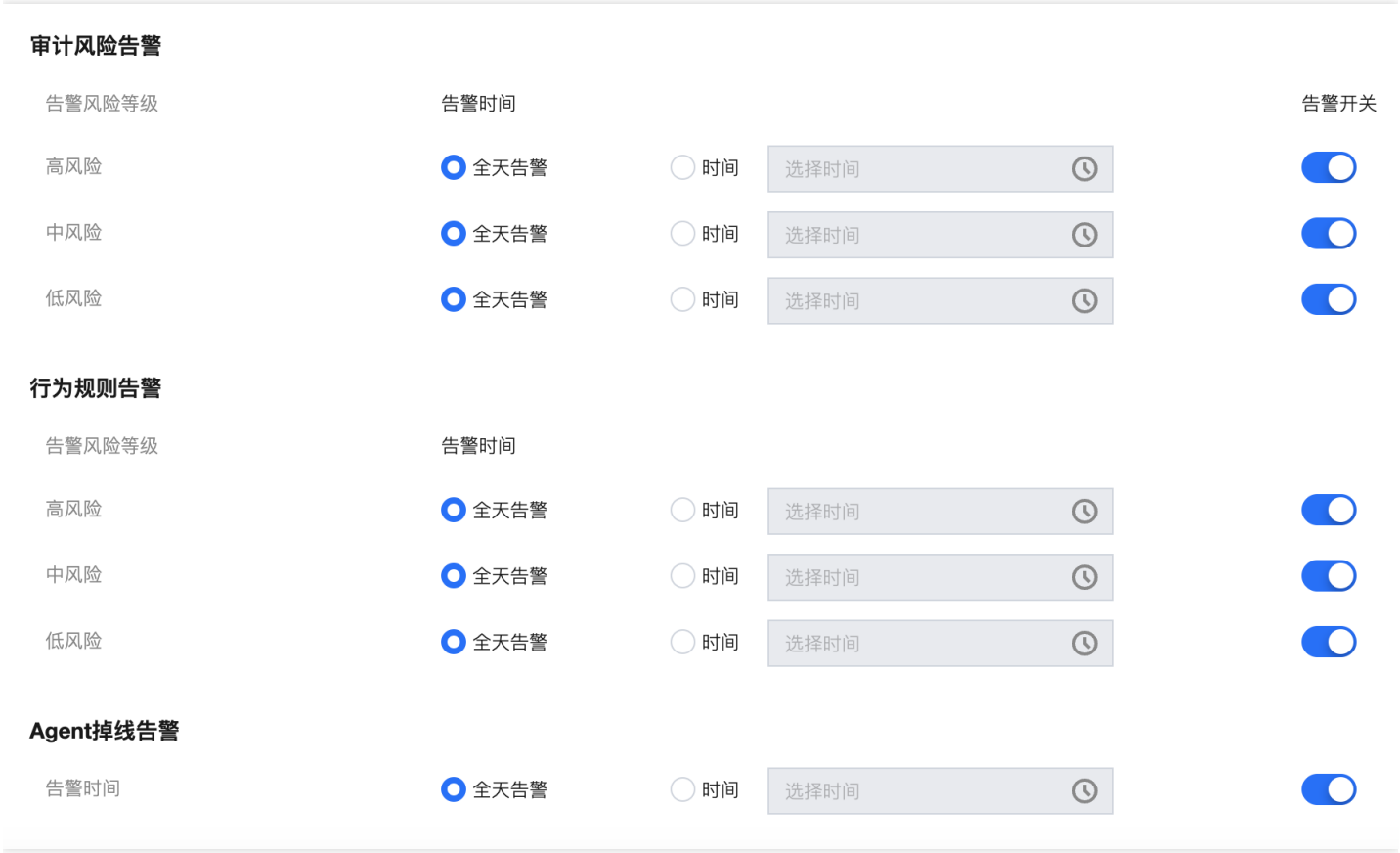
版权所有：尚航云_V1

告警设置

最近更新时间: 2024-08-23 15:08:00

步骤1：进入数据安全审计控制台，在左侧导航栏中，单击配置管理 > 告警设置，进入告警设置页面。

步骤2：在 告警设置页面，可以针对不同类型的告警和告警等级设置告警时间。



快速入门
操作指引

最近更新时间: 2024-08-23 15:08:00

同步数据资产

步骤1：进入数据安全审计服务之后，单击侧边栏的数据资产，进入数据资产页面。

步骤2：通过单击更新资产列表拉取云数据库列表，也可使用自建数据库的添加数据资产功能。



步骤3：添加数据库后，可通过单击对应数据库后面的 ，开启审计权限，允许数据安全审计采集其日志进行安全分析。

部署Agent

步骤1：完成资产添加，并开启审计权限后，进入 Agent 管理 > Agent 部署 页面。

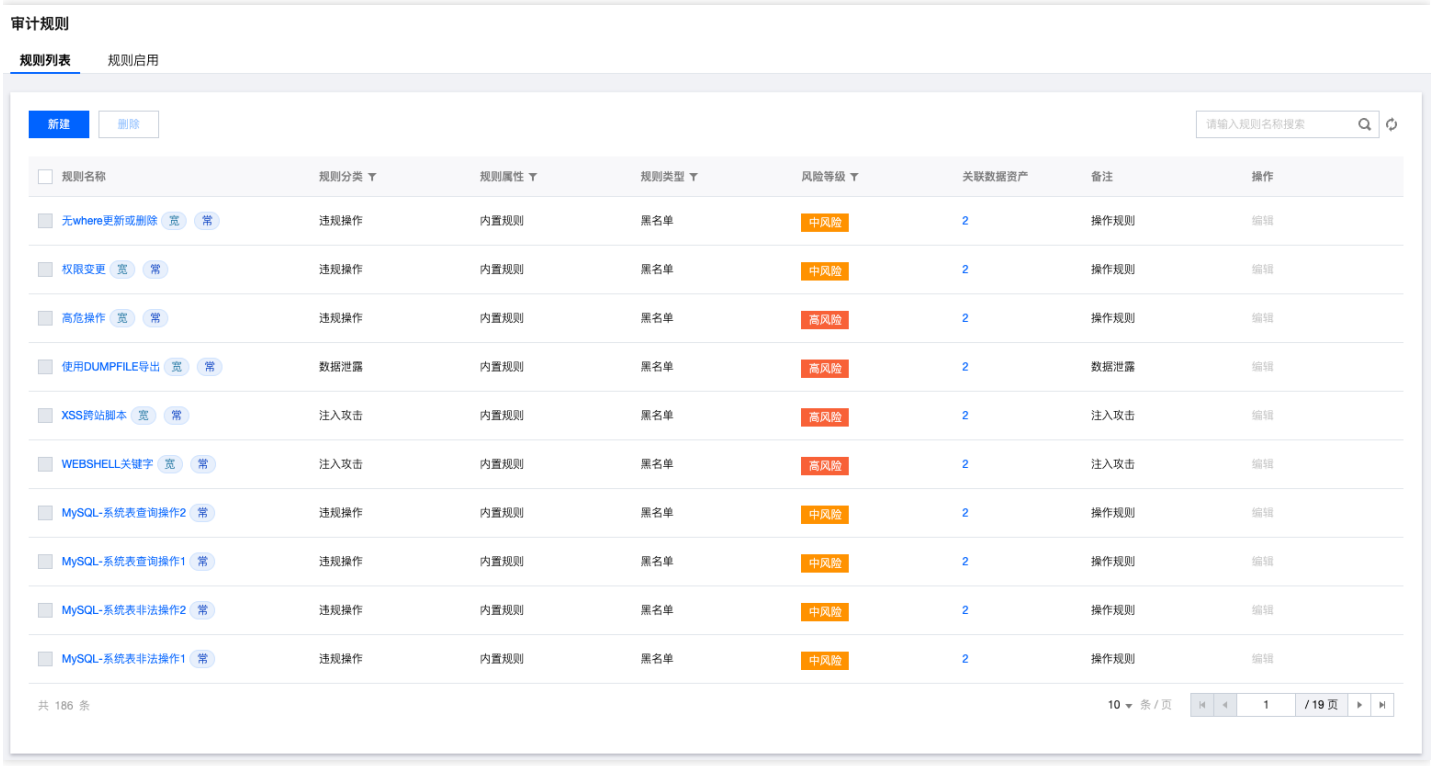
步骤2：在 Agent 部署页面，下载对应的 Agent，进行部署。

步骤3：Agent 部署完成后，单击 Agent 列表，切换至 Agent 列表页面，验证 Agent 状态是否正常。

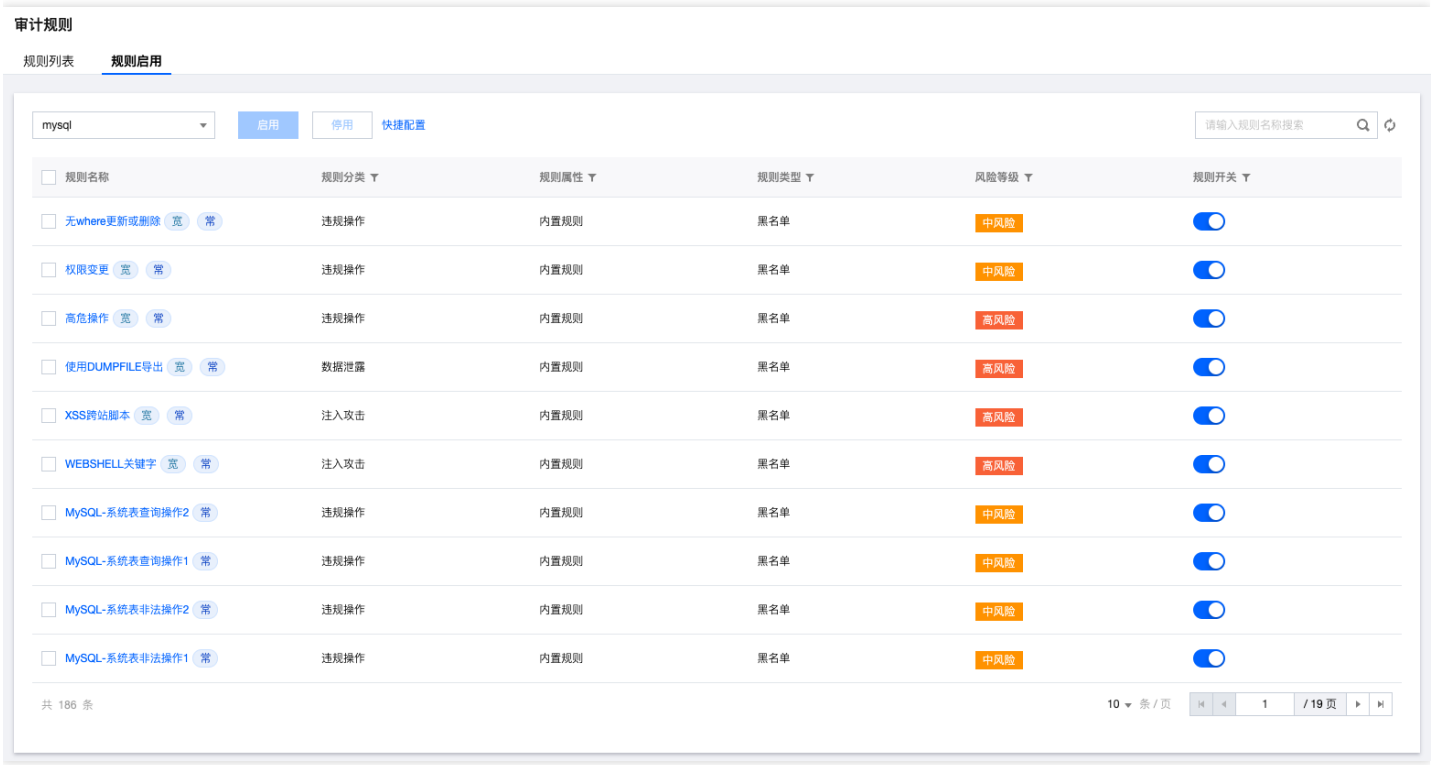
配置审计规则

步骤1：在 审计规则 > 规则列表页面，可查看系统中的审计规则，若内置规则无法满足您的特定需要，您可以单击新建创建自定义规则。

版权所有：尚航云_V1

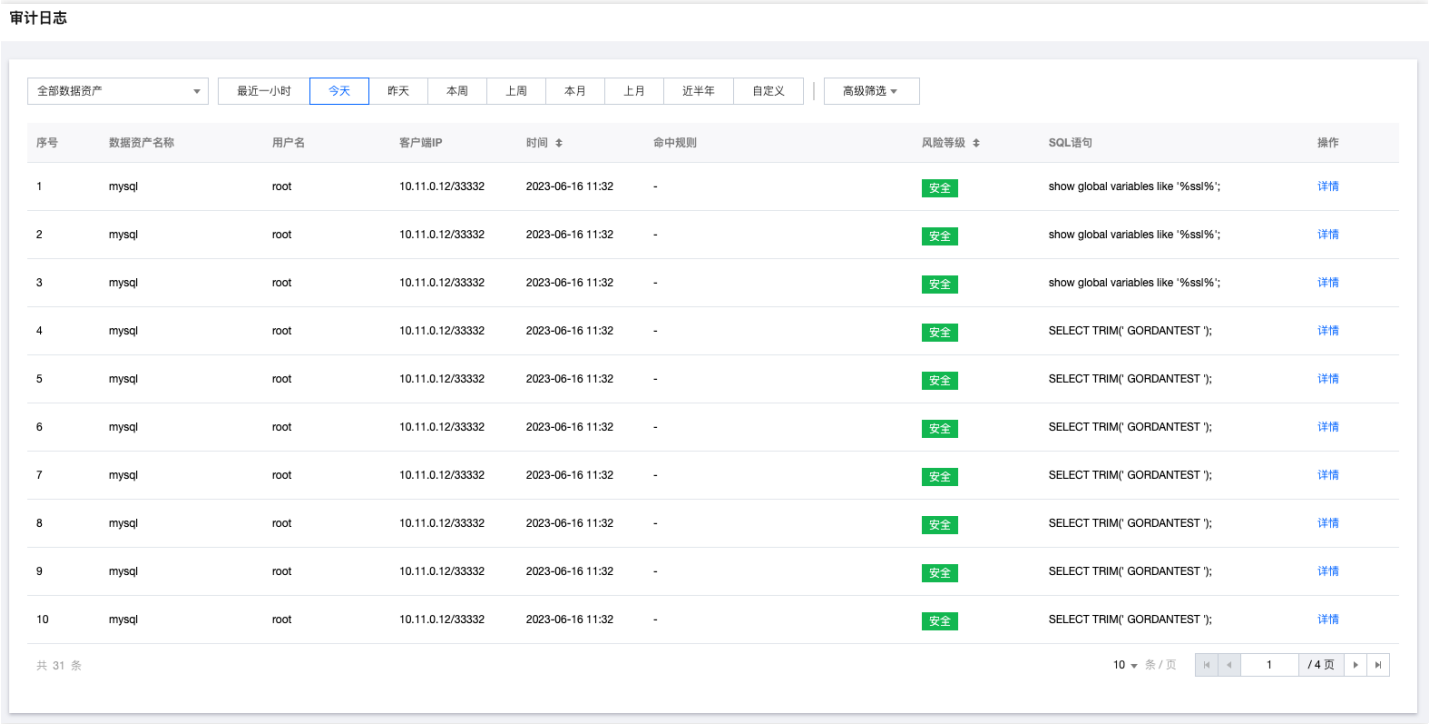


步骤2：单击规则启用，进入规则启用页面，选择数据资产，为其启用需要的审计规则。



查看审计日志

步骤1：完成以上配置后，在 审计日志 页面，可查看数据库的操作日志。



步骤2：在 审计风险 页面，可查看发现的数据安全风险，安全管理人员可根据风险提示，判断是否需要采取进一步措施。

版权所有：尚航云_V1

Agent部署

最近更新时间: 2024-08-23 15:08:00

Agent程序部署位置

根据所添加的数据库在云环境中的实际部署方式，您需要将 Agent 程序部署在以下位置：

- 云服务器自建数据库：Agent 程序需要部署在数据库所在的云服务器上。
- 云数据库：Agent 程序需要部署在对应的应用服务器上，通常为访问数据库的应用系统所在服务器。

部署 Agent 的服务器，出方向需要放通端口8081（心跳通讯端口）、7000（日志采集流量通讯端口）、7001（守护进程通信端口）。

下载Agent

步骤1：登录 数据安全审计控制台，在左侧导航栏中，单击配置管理 > Agent 管理 > Agent 部署，进入 Agent 部署页面。

步骤2：在 Agent 部署页面，选择下载 Linux Agent 或 Windows Agent。

安装Agent（Linux版本）

Linux 需在部署 Agent 之前，安装 python2。

步骤1：将Agent安装包 dsaagent_innernet_linux _xxx.zip 上传到需要安装的机器上，如 /data。

步骤2：使用 unzipdsaagent_innernet_xxx.zip 命令进行解压，得到 /data/CapAgent 目录。

步骤3：执行 cdCapAgent/bin，再执行./start.sh，结果如下。

```
[root@VM-48-16-centos bin]# ./start.sh
ilog_mod:65535
AGENT SUCCESS START
```

步骤4：在命令行，执行 netstat-ano | grep 7000 如下图即确认连接成功。



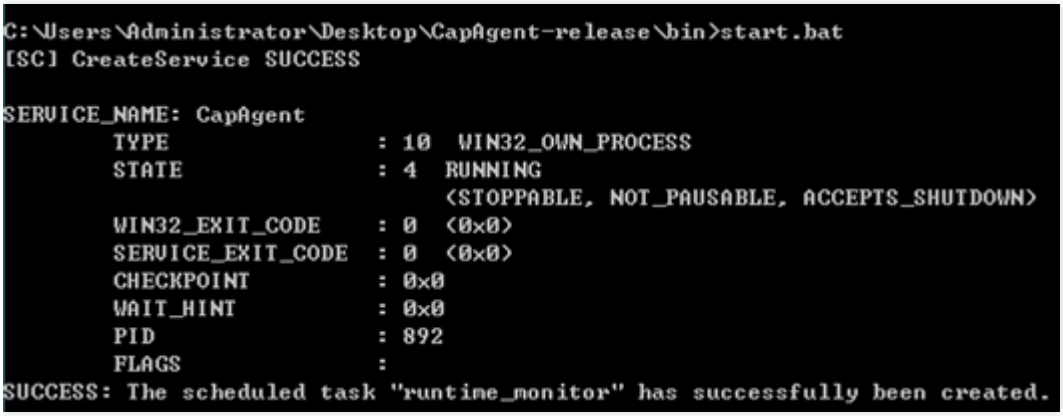
安装Agent（Windows版本）

数据安全审计 Agent Windows 版本只支持 Windows vista/2008 及以上版本。

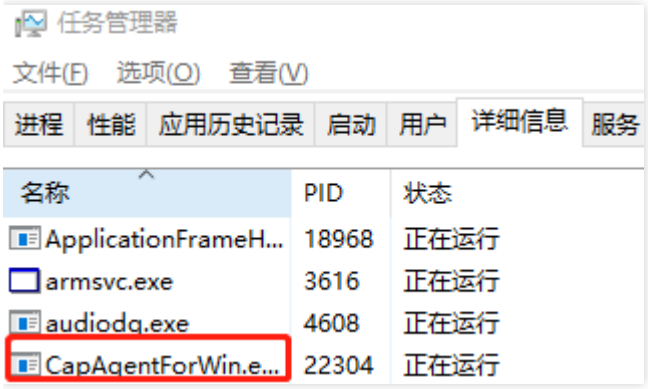
步骤1：下载 Windows 版本 Agent 后，解压到安装目录。

步骤2：进入 CapAgent下的 bin 目录，执行 start.bat。

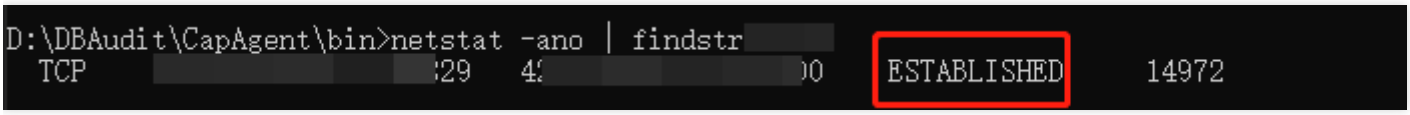
步骤3：执行成功后，Console 显示结果如下图所示。同时，可以在任务管理器中，看到CapAgentForWin.exe 进程。



步骤4：检查 CapAgentForWin 是否成功启动并连接审计服务成功，在任务管理器中确认CapAgentForWin 进程已运行。



步骤5：在 cmd 控制台，执行 netstat -ano | findstr 7000，如下图即确认连接成功。



步骤6：在 CapAgent_win/bin 目录下执行 stop.bat 即可停止 Agent。

产品介绍
产品介绍

最近更新时间: 2024-08-23 15:08:00

背景说明

随着社会信息化深度日益加深，企业IT系统飞速扩张，越来越多的业务数据搬上公有云。业务数据上云可以带来长久稳定的存储模式、快速高效的企业数据分析，享受云计算带来的便利，同时，企业仍然面临数据安全问题，并且在云上产生了新的变化。近几年频频发生公司因数据丢失受到重大损失的新闻，以及各类数据窃密的刑事案件，都是数据安全问题的真实写照。常见的公有云数据风险主要有以下几类：

- 审计信息不全，不满足网络安全法及网络安全等级保护要求。
- 恶意攻击日趋隐蔽，难以有效发现并制定应对措施。
- 内部防范措施不到位，内网人员有机可乘。
- 数据库压力监控不到位，突发性能问题。
- 获取泄密证据困难。

产品简介

针对上述数据安全问题，数据安全审计可对企业网络中的数据库各类会话信息、访问操作、SQL 语句进行全量审计入库。

助力企业满足网络安全法、等保三级要求。

获得审计数据后，数据安全审计能根据多种规则库和威胁检测引擎识别操作中的恶意行为，并及时通知管理员进行相应的安全防护措施。

对于已发生的安全事故，数据安全审计支持对数年的日志进行审计和分析，为企业还原安全事故全貌并定位责任人提供参考依据。

数据安全审计能够应对因数据访问量巨大而产生的审计难题。数据安全审计基于腾讯 TKE 技术的 SaaS 架构，可根据企业数据库流量随时扩展算力， SQL 吞吐量达十万级，每小时入库速率达千万级，帮助企业应对超高并发环境的

审计问题。

产品功能

丰富的数据库支持

数据安全审计支持常见的云数据库、自建数据库和大数据组件。

云数据库：关系型数据库 MySQL、PostgreSQL、SQL Server、MariaDB，NOSQL 数据库 Redis、MongoDB，企业级分布式数据库 TDSQL。

自建数据库：MySQL、PostgreSQL、SQL Server、Oracle、MariaDB、Redis、MongoDB、Hbase、Hive。

大数据组件：Hbase、Hive。

云数据库自动发现

数据安全审计基于云原生架构，在用户授权后，可自动获取云数据库列表，不需要手工录入，同时避免资产遗漏。

自定义规则审计

支持按照库、表、字段、访问源、数据库实例等多种维度进行审计规则设置，安全策略灵活且自由，实现精细化监控；可根据不同场景不同类型的应用进行个性化定制，精确掌控数据库访问信息。

全量审计

数据安全审计具备全量的数据库操作审计功能，超越传统安全审计概念，将数据库所有的 SQL 操作全部收入眼底。会话审计类别齐全，能够对各类数据操作行为进行审计，为数据库安全事件的溯源提供支持。

威胁告警

数据安全审计能够在识别威胁操作后，向相关管理员发送告警信息。告警方式支持企业微信告警、短信告警、邮件告警，类型丰富，多种途径确保警报及时通知管理员。