数据安全审计

实践教程

腾讯云

文档目录

实践教程
- 等保实践教程 SaaS 型
- 等保实践教程传统型
- MySQL 加密审计实践教程
- 混合云资产统一审计实践教程
- 轻量应用服务器部署 Agent 实践教程
- 容器服务部署 Agent 实践教程
- 云原生审计实践教程
- 敏感数据操作精准溯源与风险监控

实践教程
等保实践教程 SaaS 型

最近更新时间：2025-02-14 18:23:32

为助力企业等保合规，本文为您介绍数据安全审计 SaaS 型各能力与等保相关条款的对应关系，以便有针对性地提供佐证材料。

> **说明**
> 若您使用的是数据安全审计传统型，请参见 数据安全审计传统型 文档。

前提条件

已购买 数据安全审计 SaaS 型，并按照 快速入门 完成产品初始化和部署工作。

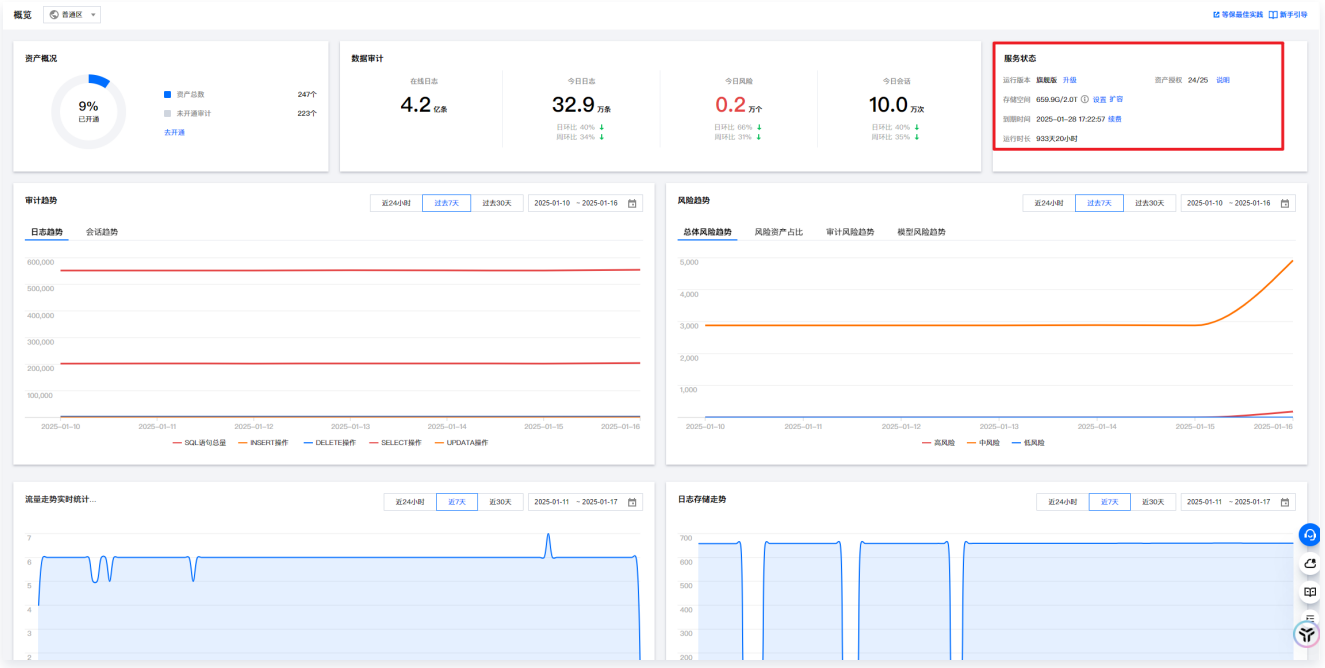
等保二级

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

本条款主要考察如下三点：

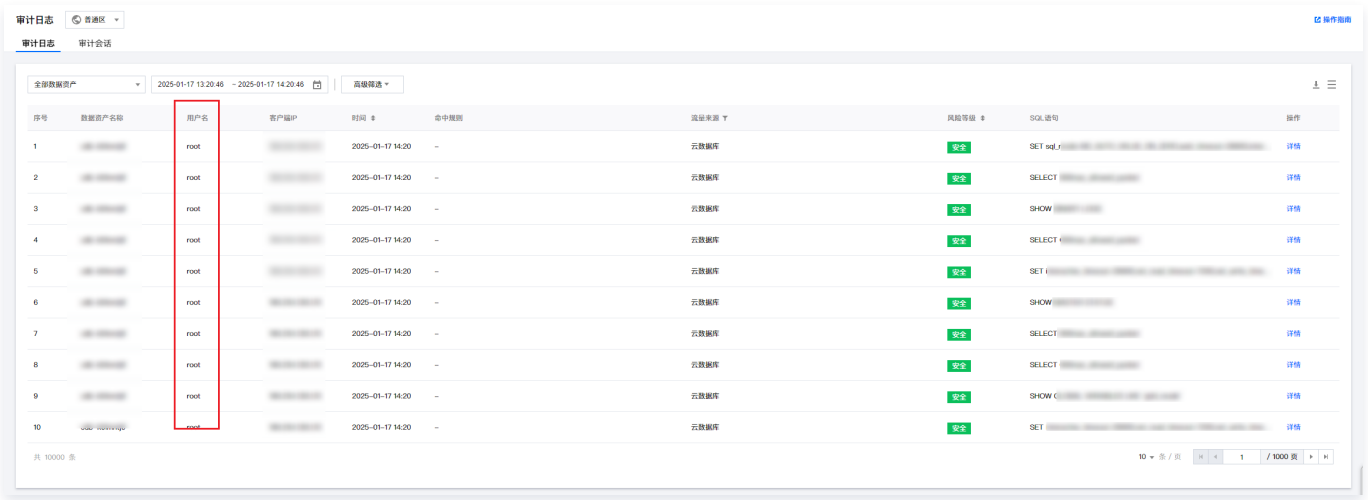
- **是否开启了安全审计功能**

  1.1 登录 数据安全审计控制台，显示立即进入，可以查看到产品服务状态及资产安全概况，证明产品已正常运行。



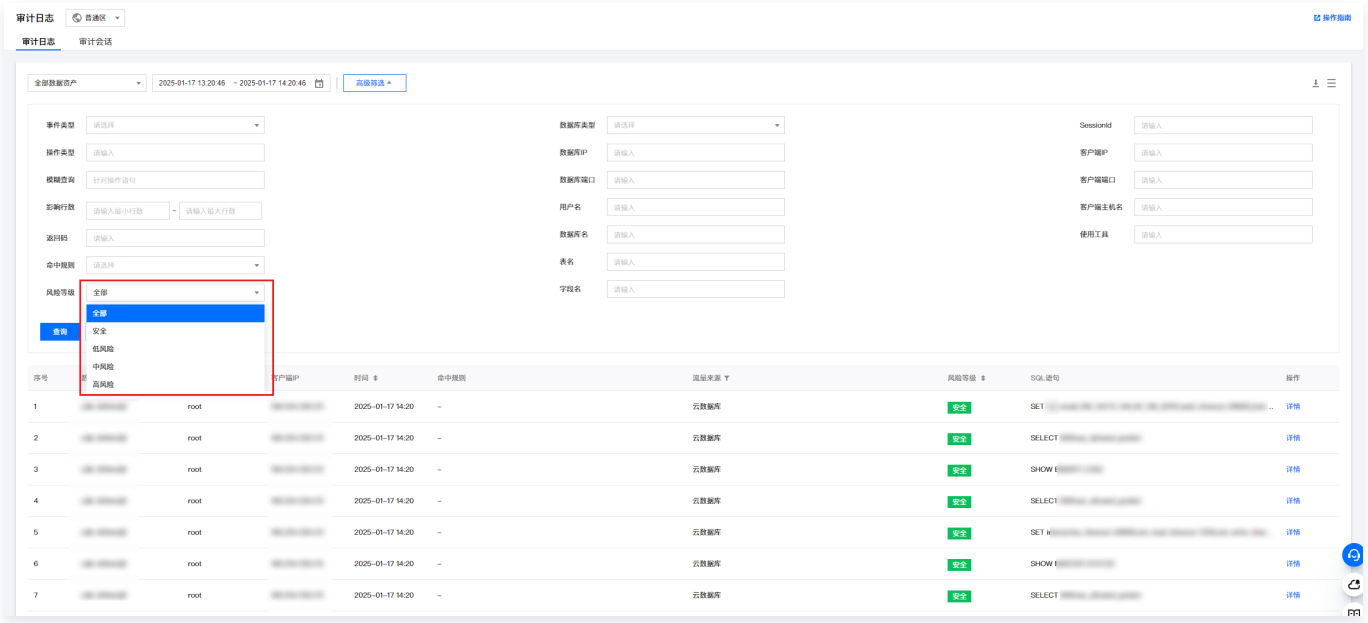
- **审计范围是否覆盖到每个用户**

  在 审计日志页面，可以审计到每个用户名。



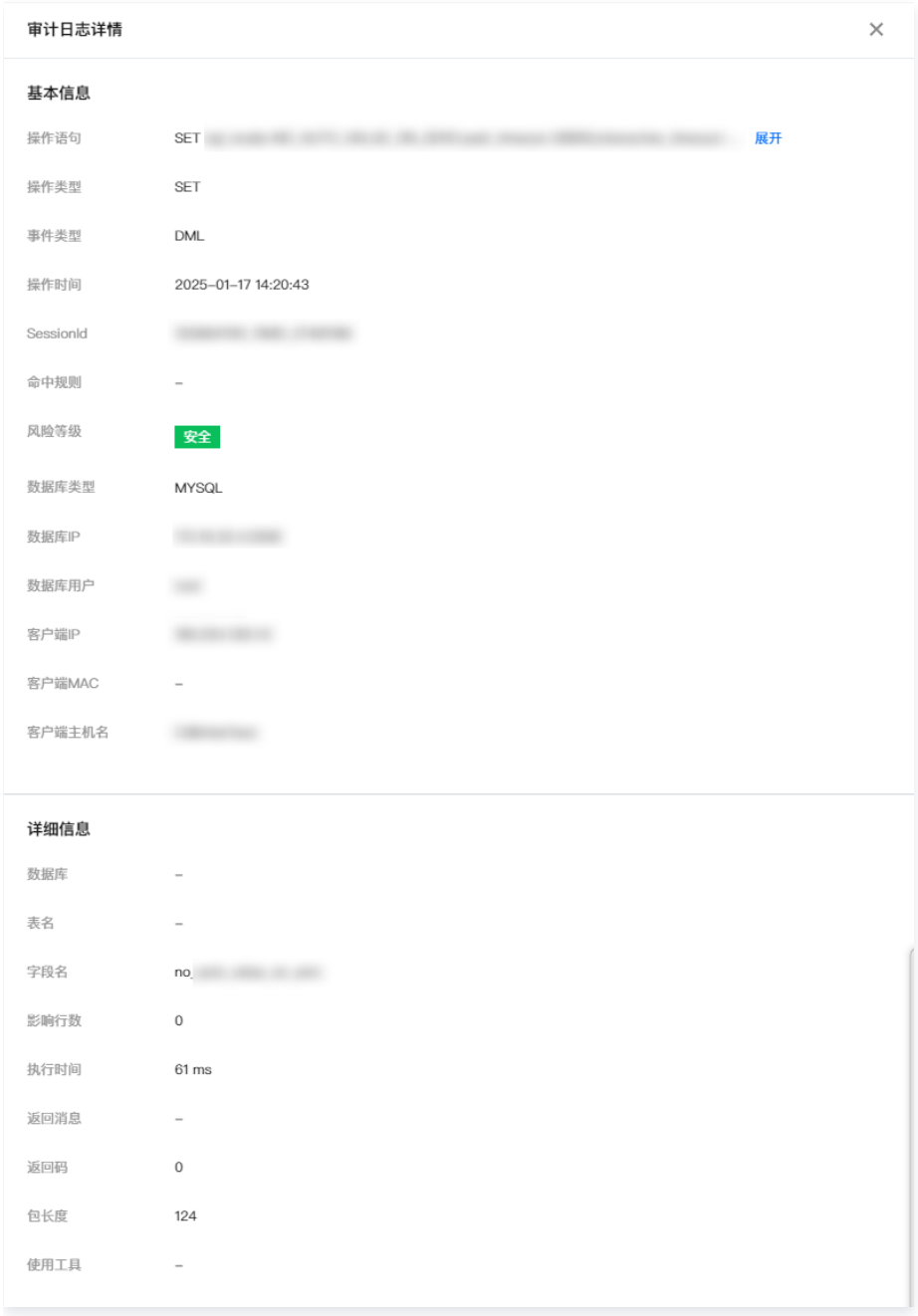
- **是否对重要的用户行为和重要安全事件进行审计**

  通过 **审计日志** 或 **审计风险** 页面，可以筛选风险等级（即重要的用户行为和重要安全事件）查看日志。



b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

在 审计日志页面，单击任意一条日志后方的**详情**，弹出审计日志详情，可以查看相关的信息。



c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

数据安全审计 SaaS 型的审计日志存储于腾讯云 Elasticsearch Service，通过多可用区部署、定期备份方式保证数据可用性。可在概览页的服务状态栏，存储空间的详情说明中查看存储机制及预计可继续存储时长。

其他：《网络安全法》要求网络日志保留六个月以上。

在 审计日志页面，选中**近半年**，可以查看近六个月的日志。

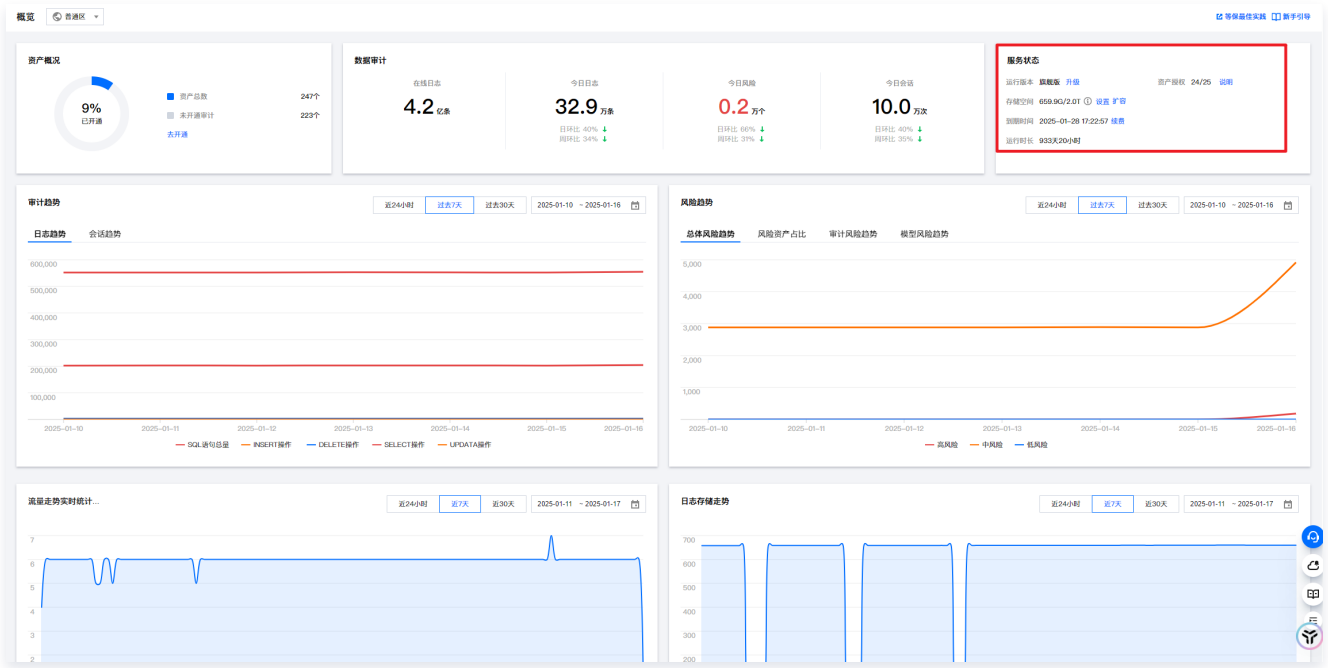
等保三级

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

本条款主要考察如下三点：

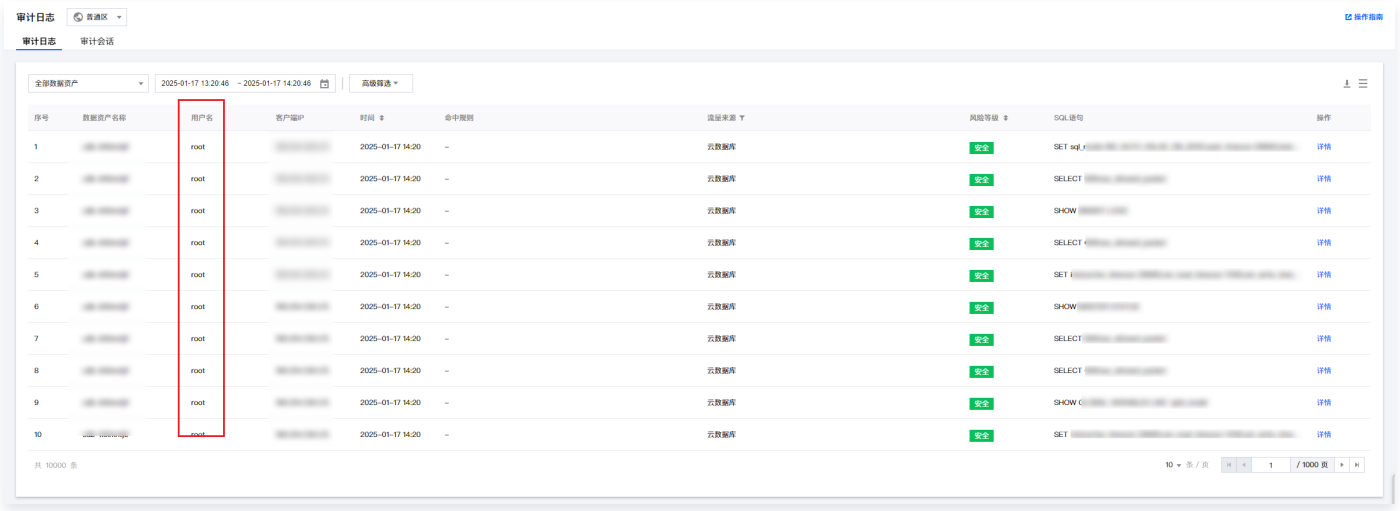
- **是否开启了安全审计功能**

  1.1 登录 数据安全审计控制台，显示立即进入，可以查看到产品服务状态及资产安全概况，证明产品已正常运行。



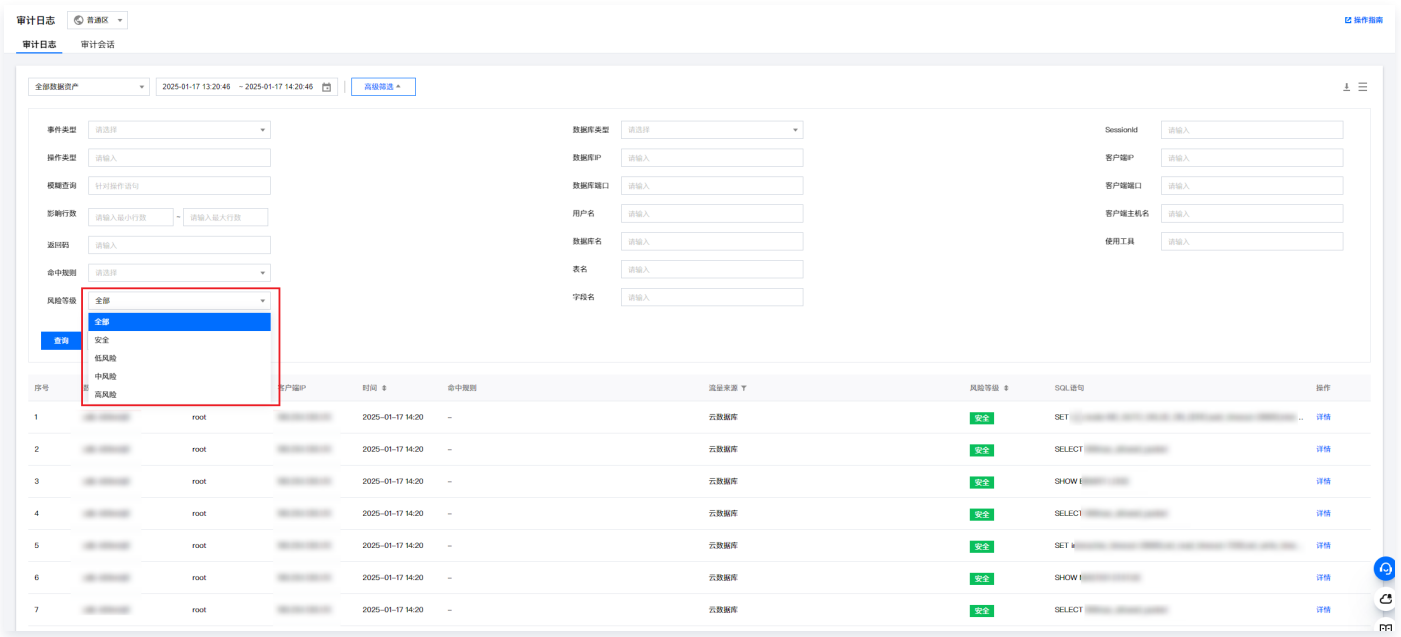
- **审计范围是否覆盖到每个用户**

  在 审计日志页面，可以审计到每个用户名。



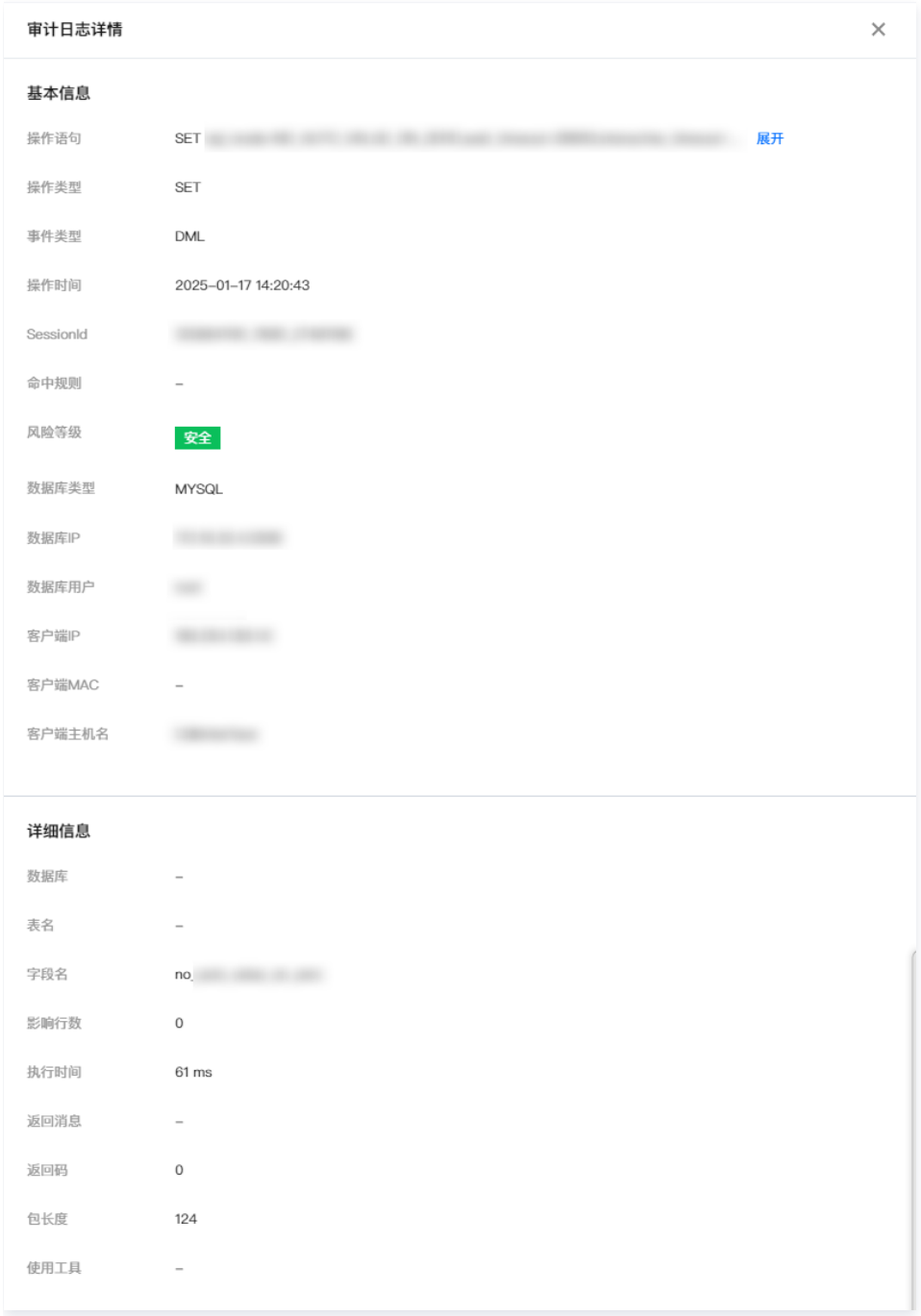
- **是否对重要的用户行为和重要安全事件进行审计**

  通过 审计日志 或 审计风险 页面，可以筛选风险等级（即重要的用户行为和重要安全事件）查看日志。



b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

在 **审计日志页面**，单击任意一条日志后方的**操作**，弹出审计日志详情，可以查看相关的信息。



c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

数据安全审计 SaaS 型的审计日志存储于腾讯云 Elasticsearch Service，通过多可用区部署、定期备份方式保证数据可用性。后续版本将在产品页面添加相关说明。

d) 应对审计进程进行保护，防止未经授权的中断。

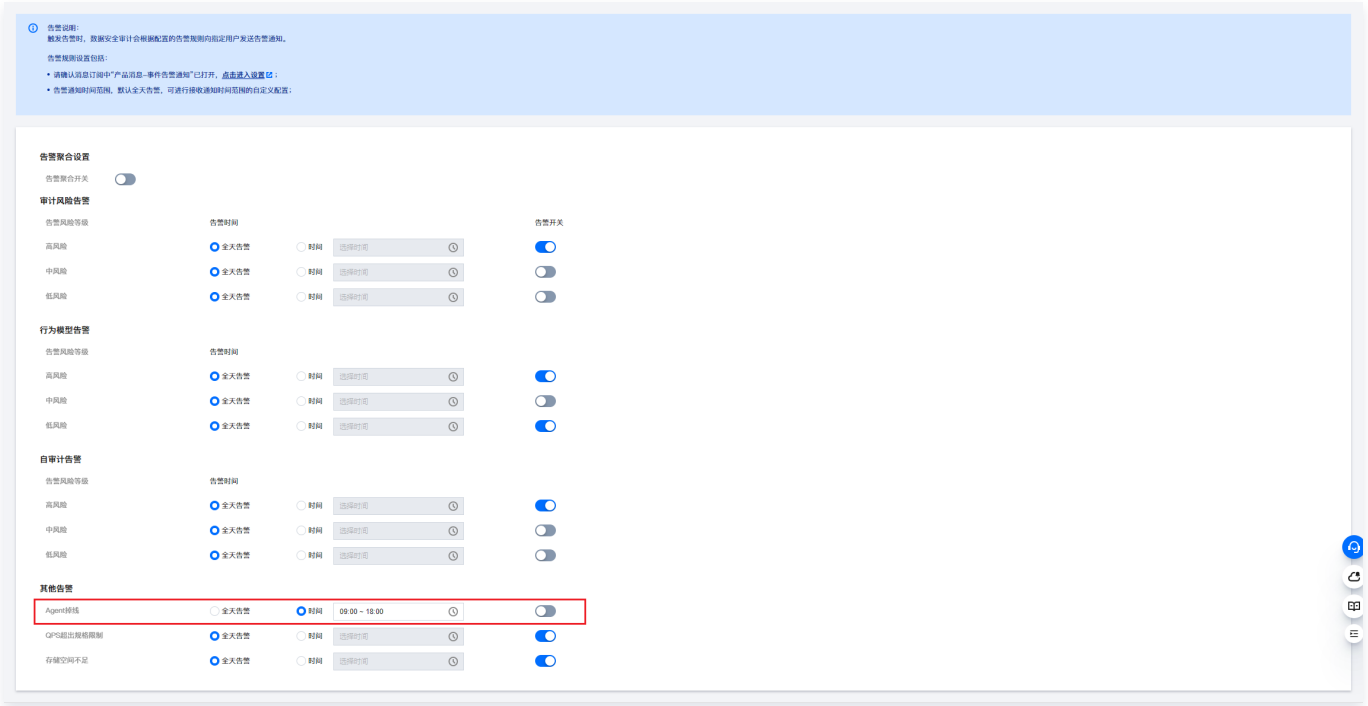
审计进程包含两部分：审计服务器的进程和 Agent 进程。

- **审计服务器的进程**

  审计服务器部署在腾讯云侧，由腾讯云进行相关安全保障，用户不具有直接进入产品后台操作的权限。当确有必要，需要进入后台操作时，根据腾讯云流程，需要用户 提交工单，由腾讯云技术人员得到授权后进行操作。会留存详细的工单记录，便于事后查证。

- **Agent 进程**

Agent 掉线告警：Agent 部署在用户的数据库或云服务器上，数据安全审计将对其进行守护检测，当检测到 Agent 中断时，将及时产生告警。



其他：《网络安全法》要求网络日志保留六个月以上。

在 **审计日志页面**，选中**近半年**，可以查看近六个月的日志。

等保实践教程传统型

最近更新时间：2025-01-10 19:17:23

为助力企业等保合规，本文为您介绍数据安全审计传统型各能力与等保相关条款的对应关系，以便有针对性地提供佐证材料。

> **说明**
> 若您使用的是数据安全审计 SaaS型，请参见 数据安全审计 SaaS 型 文档。

前提条件

已购买 数据安全审计传统型，并按照 快速入门 完成产品初始化和部署工作。

等保二级

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

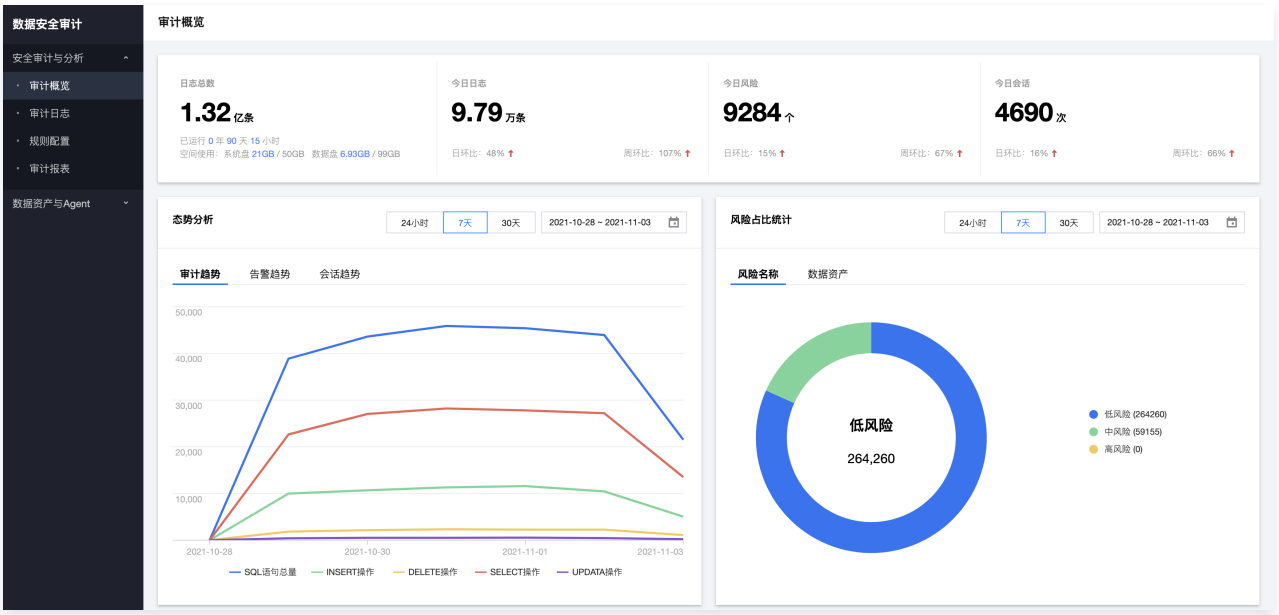
本条款主要考察如下三点：

- **是否开启了安全审计功能**

1.1 登录 数据安全审计控制台，查看数据安全审计产品列表，证明已购买相关产品。

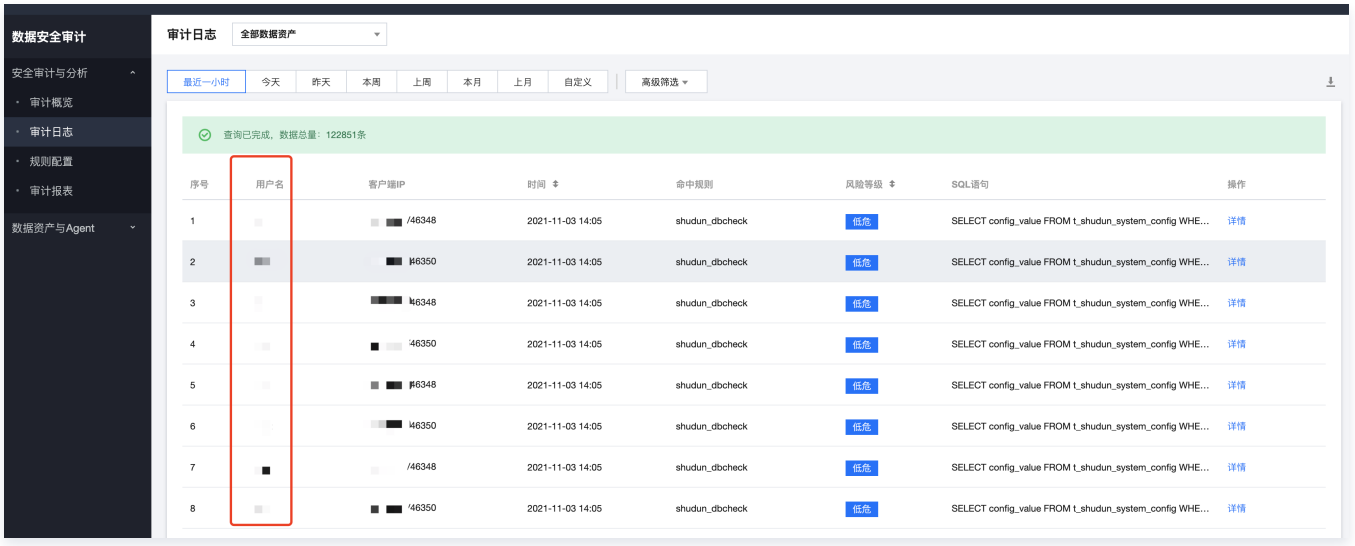
1.2 单击操作列下的**管理**，跳转至登录页面，使用 useradmin 账号登录数据安全审计。在左侧导航栏中，选择**安全审计与分析 > 审计概览**，进入审计概览页面。

1.3 查看审计概览页，证明产品已正常运行。



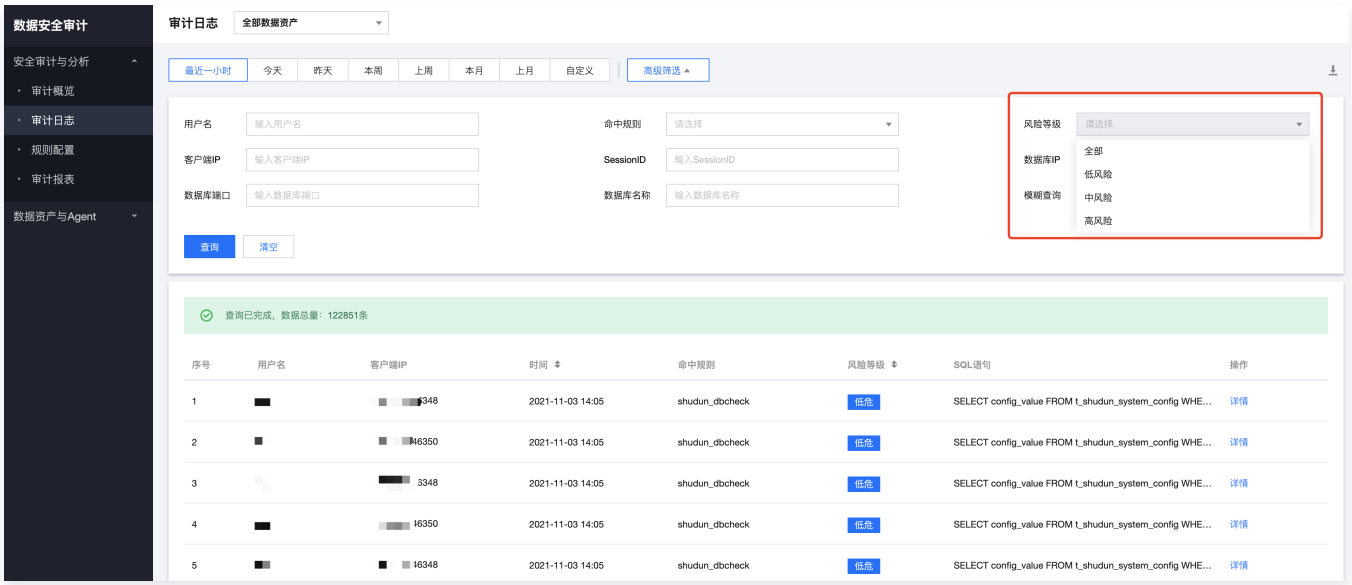
- **审计范围是否覆盖到每个用户**

  在审计日志页面，可以审计到每个用户名。



- **是否对重要的用户行为和重要安全事件进行审计**

  使用 useradmin 账号登录数据安全审计，通过审计日志页面，可以筛选风险等级（即重要的用户行为和重要安全事件）查看日志。

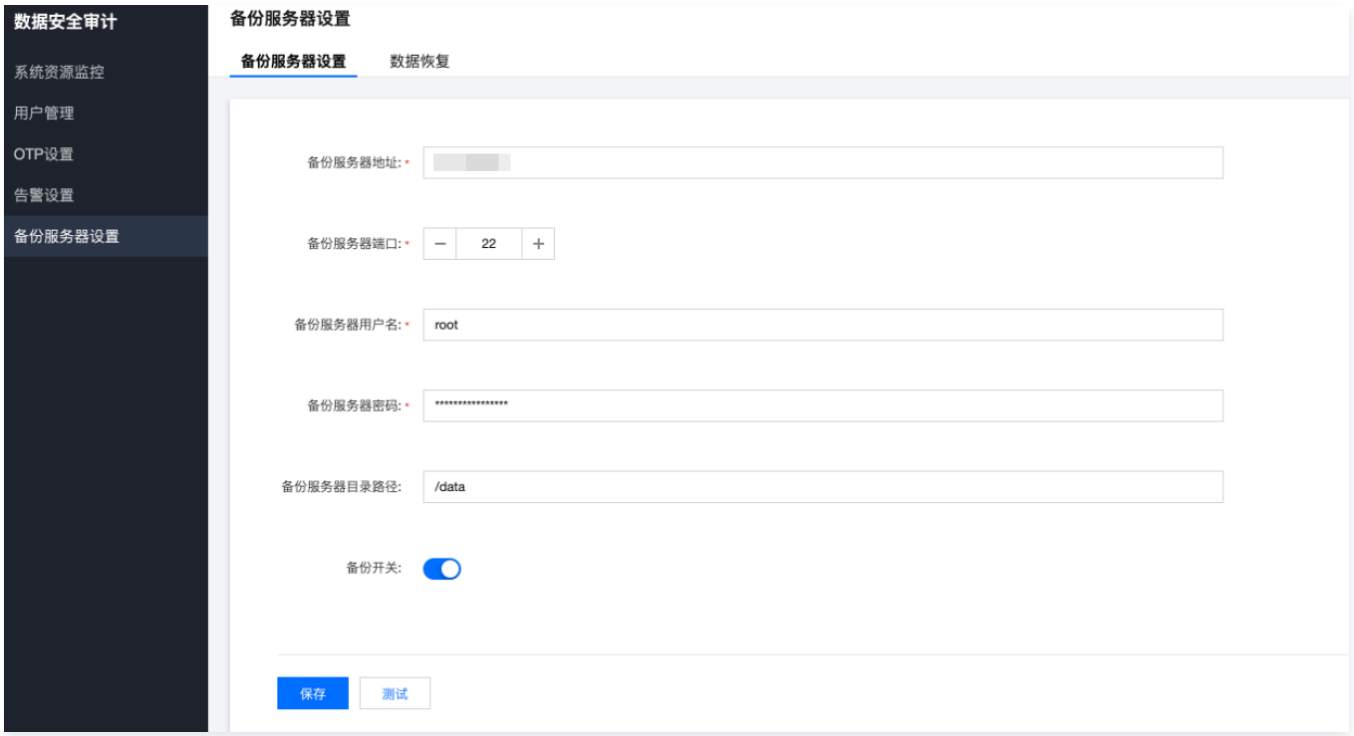


b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

在审计日志页面，单击任意一条日志后方的**操作**，弹出审计日志详情，可以查看相关的信息。

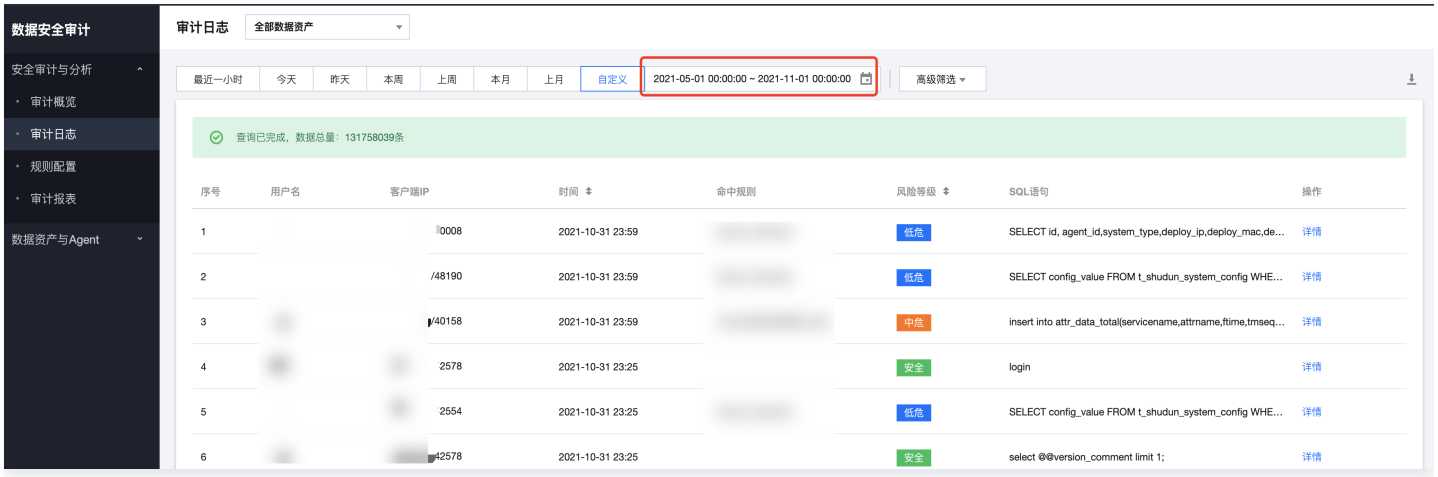
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

使用 sysadmin 账号登录数据安全审计，在备份服务器设置页面，查看备份服务器设置，具有备份功能及数据恢复功能。



其他：《网络安全法》要求网络日志保留六个月以上。

在审计日志页面，选中**自定义**，选择近六个月的区间，可以查看近六个月的日志。



等保三级

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

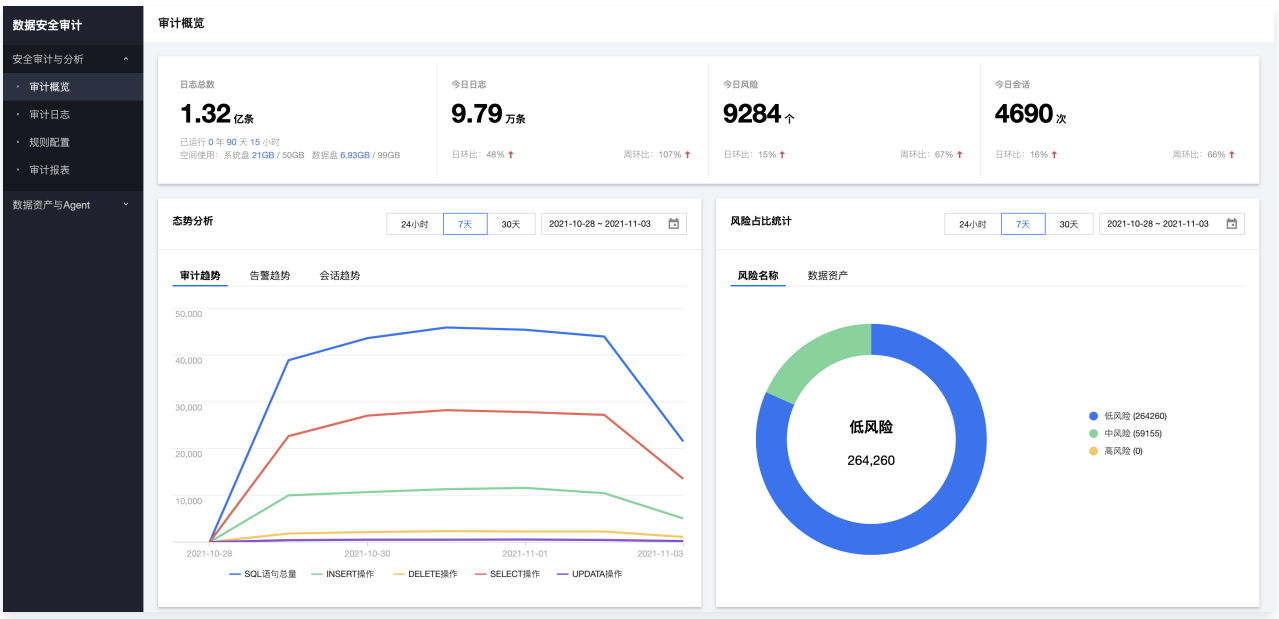
本条款主要考察如下三点：

- **是否开启了安全审计功能**

1.1 登录 数据安全审计控制台，查看数据安全审计产品列表，证明已购买相关产品。

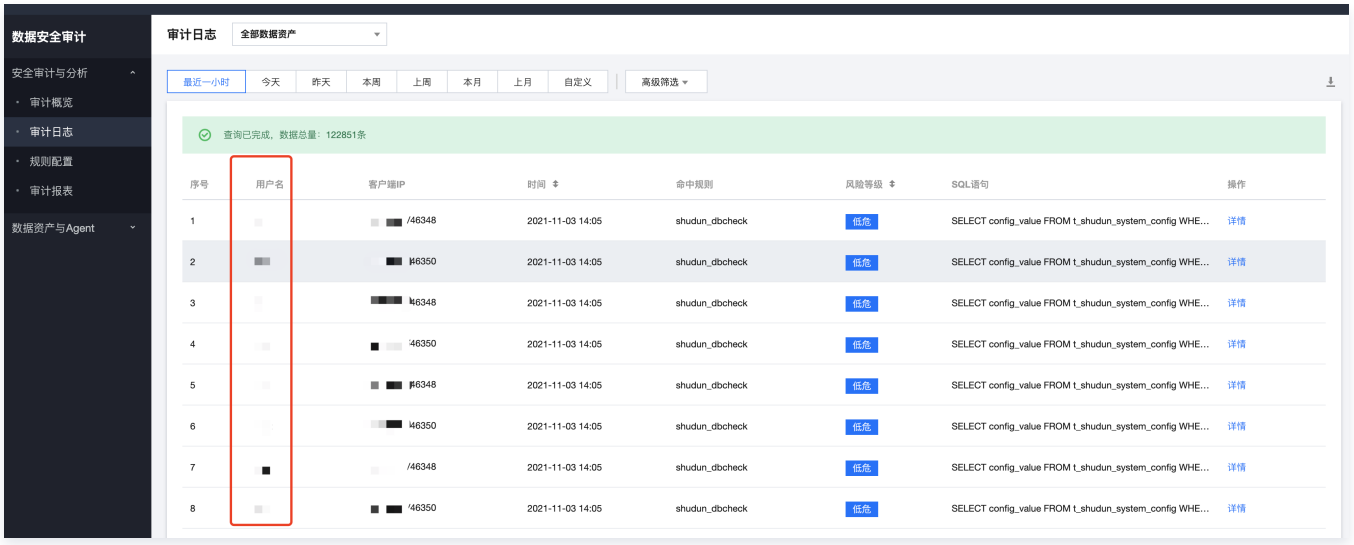
1.2 单击操作列下的**管理**，跳转至登录页面，使用 useradmin 账号登录数据安全审计。在左侧导航栏中，选择**安全审计与分析 > 审计概览**，进入审计概览页面。

1.3 查看审计概览页，证明产品已正常运行。



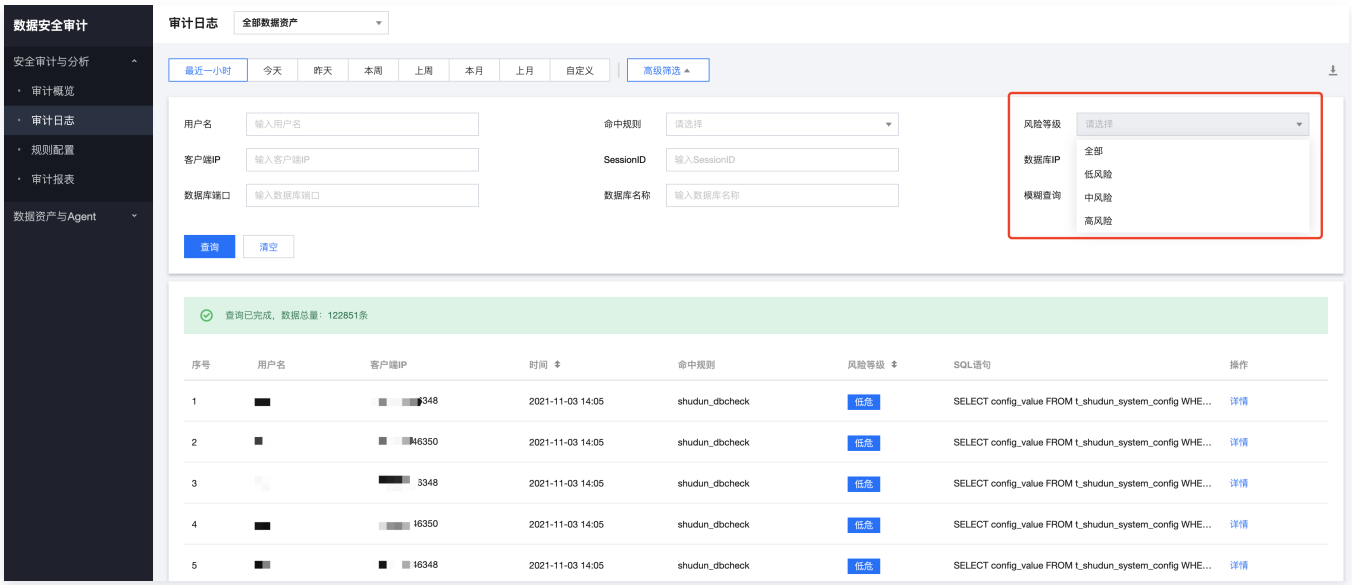
- **审计范围是否覆盖到每个用户**

  在审计日志页面，可以审计到每个用户名。



- **是否对重要的用户行为和重要安全事件进行审计**

  使用 useradmin 账号登录数据安全审计，通过审计日志页面，可以筛选风险等级（即重要的用户行为和重要安全事件）查看日志。

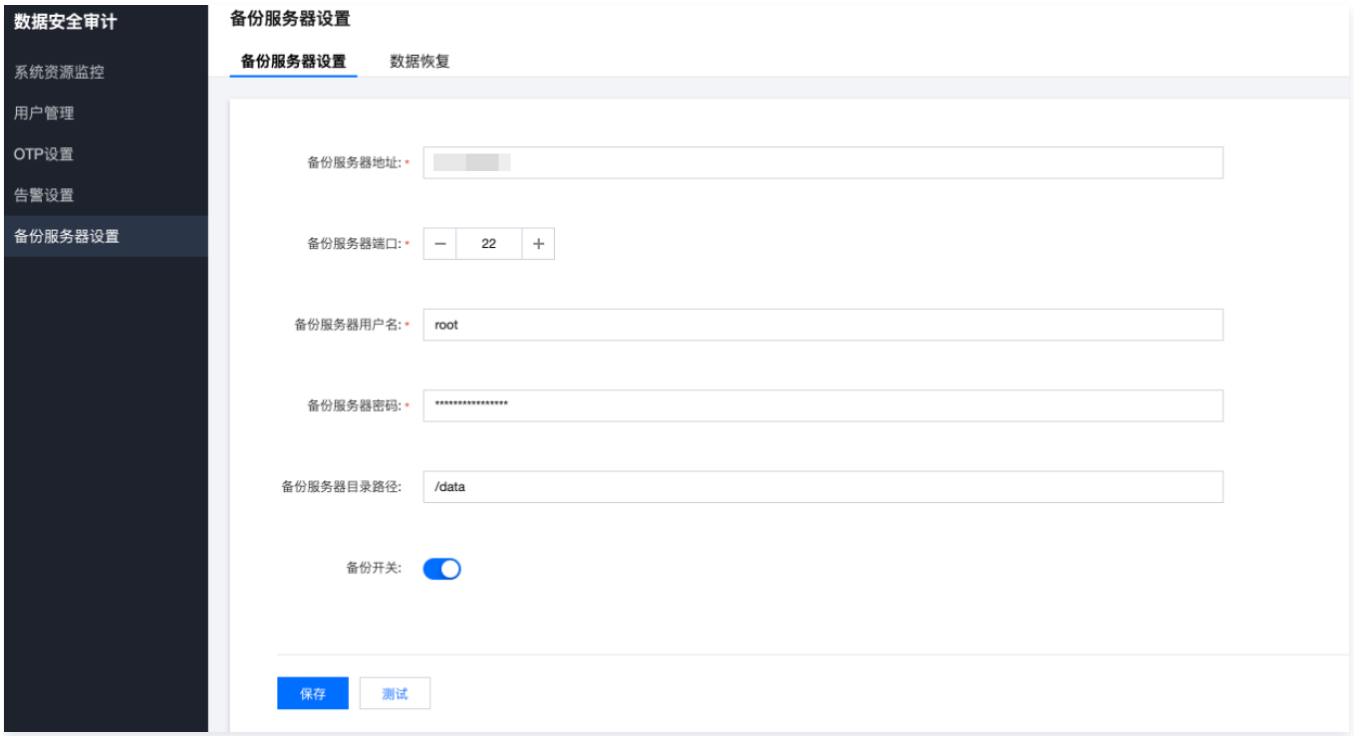


b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

在审计日志页面，单击任意一条日志后方的**操作**，弹出审计日志详情，可以查看相关的信息。

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

使用 sysadmin 账号登录数据安全审计，在备份服务器设置页面，查看备份服务器设置，具有备份功能及数据恢复功能。



d) 应对审计进程进行保护，防止未经授权的中断。

审计进程包含两部分：审计服务器的进程和 Agent 进程。

- **审计服务器的进程**

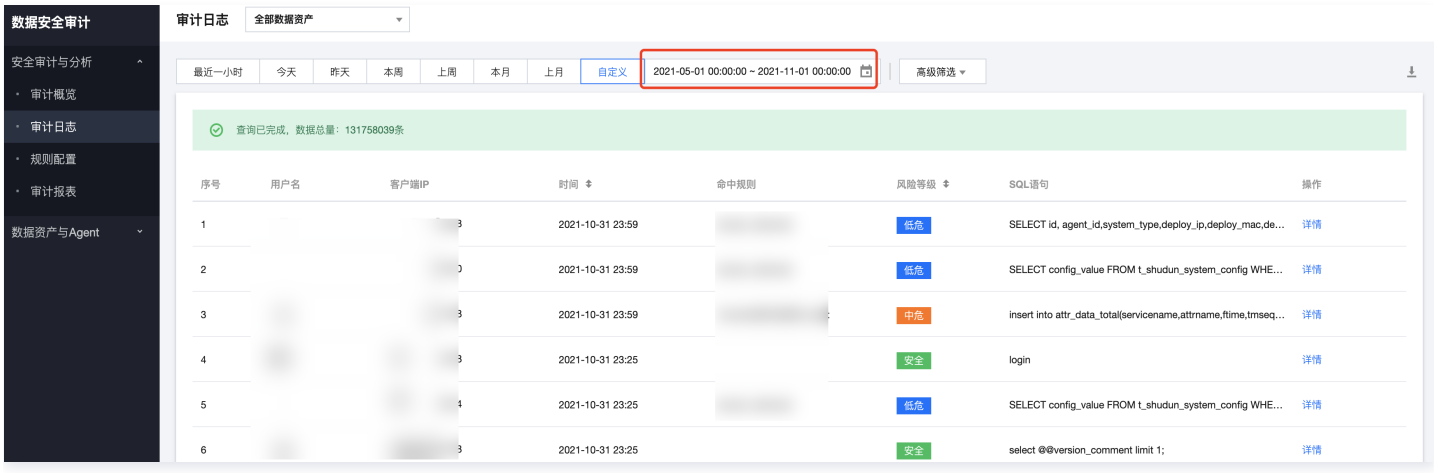
  审计服务器部署在腾讯云侧，由腾讯云进行相关安全保障，用户不具有直接进入产品后台操作的权限。当确有必要，需要进入后台操作时，根据腾讯云流程，需要用户 提交工单，由腾讯云技术人员得到授权后进行操作。会留存详细的工单记录，便于事后查证。

- **Agent 进程**

  Agent 部署在用户的数据库或云服务器上，数据安全审计将对其进行守护检测，当检测到 Agent 中断时，将及时产生告警。

其他：《网络安全法》要求网络日志保留六个月以上。

在审计日志页面，选中**自定义**，选择近六个月的区间，可以查看近六个月的日志。


数据安全审计
安全审计与分析
审计概览
审计日志
规则配置
审计报表
数据资产与Agent
审计日志
全部数据资产
最近一小时
今天
昨天
本周
上周
本月
上月
自定义
2021-05-01 00:00:00 ~ 2021-11-01 00:00:00
高级筛选
查询已完成，数据总量：131758039条
序号
用户名
客户端IP
时间
命中规则
风险等级
SQL语句
操作
1
2021-10-31 23:59
低危
SELECT id, agent_id,system_type,deploy_ip,deploy_mac,de...
详情
2
2021-10-31 23:59
低危
SELECT config_value FROM t_shudun_system_config WHE...
详情
3
2021-10-31 23:59
中危
insert into attr_data_total(servicename,attrname,ftime,trmseq...
详情
4
2021-10-31 23:25
安全
login
详情
5
2021-10-31 23:25
低危
SELECT config_value FROM t_shudun_system_config WHE...
详情
6
2021-10-31 23:25
安全
select @@version_comment limit 1;
详情

MySQL 加密审计实践教程

最近更新时间：2025-05-26 18:00:23

应用场景

数据安全审计 SaaS 型自6.0.2版本起，已支持自建 MySQL、MariaDB 的 SSL 加密审计。本文档对该功能的限制、配置、常见问题做必要说明。

功能限制

本功能限制如下：

- 仅支持自建的 MySQL、MariaDB；云数据库 MySQL 通过云原生审计方式可支持加密审计，无需单独配置。
- 支持的加密算法：TLS_RSA_WITH_AES_128_CBC_SHA 、TLS_RSA_WITH_AES_256_CBC_SHA 、TLS_RSA_WITH_AES_128_CBC_SHA256、 TLS_RSA_WITH_AES_256_CBC_SHA256。

检测方式

步骤1：检测是否开启加密

1. 在数据库中，输入如下命令，确认是否开启了 SSL 加密。

```
show global variables like '%ssl%';
```

2. 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  |
+---------------+-----------------+
```

步骤2：检测加密算法

1. 在数据库中，输入如下命令，检测加密算法。

```
show global variables like 'ssl_cipher';
```

2. 若 ssl_cipher 的值中只包含 AES128-SHA、AES256-SHA、AES128-SHA256、AES256-SHA256 四个中的一个或多个，则表示是支持的，否则表示不支持，需要进行修改。

```
dba:(none)> show global variables like 'ssl_cipher';
+---------------+-----------------+
| Variable_name | Value           |
+---------------+-----------------+
| ssl_cipher    |                 |     #此处为空，需要修改
+---------------+-----------------+
```

修改方式

通过修改数据库的相关配置，使数据安全审计可以审计到数据库语句。可根据实际情况，任意选择如下一种修改方式。

关闭 SSL 加密

MySQL 的 SSL 虽然提高了安全性，但也牺牲了部分性能。如果用户单位没有必须开启 SSL 加密的规定，可以考虑直接关闭 SSL 加密。

> ⚠ **注意**
> 该方法需要重启数据库。

1. 修改配置文件 my.cnf，在[mysqld]下增加如下内容：

```
[mysqld]
# disable_ssl
skip_ssl
```

2. 输入如下指令，重启 MySQL。

```
service mysqld restart
```

3. 使用上述 检测方式，验证是否修改成功。

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

设置加密算法

在配置文件中，设置加密算法，该方法可以对数据库的所有连接生效。

> ⚠ **注意**
> 该方法需要重启数据库。

1. 修改配置文件 my.cnf，在[mysqld]下增加如下内容：

```
[mysqld]
# 设置加密算法
ssl_cipher="AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256"
```

2. 输入如下指令，重启 MySQL。

```
service mysqld restart
```

3. 使用上述 检测方式，验证是否修改成功。

```
dba:(none)> show global variables like 'ssl_cipher';
+---------------+-------------------------------------------------+
| Variable_name | Value                                           |
+---------------+-------------------------------------------------+
| ssl_cipher    | AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256|
+---------------+-------------------------------------------------+
```

在客户端连接时指定参数

若不想修改数据库配置，可以在客户端建立连接时，指定参数，如：

```
mysql -u root  -pxxxx -h 10.x.x.x --ssl-cipher=AES128-SHA
```

> **说明**
> 该方法只针对本连接，不会影响其他连接。

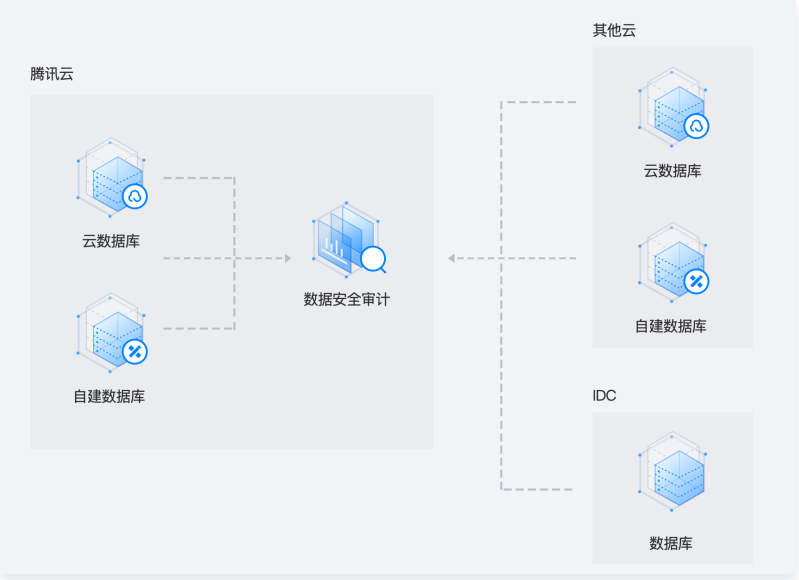
混合云资产统一审计实践教程

最近更新时间：2025-07-30 17:21:22

企业的业务往往采用混合云部署方式，即同时部署在腾讯云、其他云及 IDC 的两个或多个位置。数据安全审计能够帮助企业对位于多个位置的数据资产纳入统一的审计管理，实时感知其安全风险并预警，为企业的业务安全运行保驾护航。本文将介绍混合云资产开启审计的实践教程。

资产类型

企业常见混合云资产分布如下所示：



数据库类型		说明
腾讯云内	云数据库	腾讯云数据库，如TencentDB for MySQL 、TDSQL-C 、TencentDB for Redis 等。
	自建数据库	在腾讯云上服务器、容器自建的数据库，如MYSQL、SQL Server、Hive、Hbase等。
腾讯云外	云数据库	其他云的云数据库，如OceanBase、GaussDB等。
	自建数据库	在本地机房/其他云上服务器、容器自建的数据库，如MYSQL、SQL Server、Hive、Hbase等。 **说明：** 当云外自建数据库与腾讯云已基于专线等方式打通网络时，可等同于云内自建数据库。

说明：
上方仅举例部分数据源类型，所有支持类型请参考 支持的数据库 。

审计方案

针对混合云资产中不同位置资产的特点，腾讯云数据安全审计提供多种日志采集方案，并将日志汇总到数据安全审计控制台进行存储、分析和展示，支持企业完成统一管理和审计。

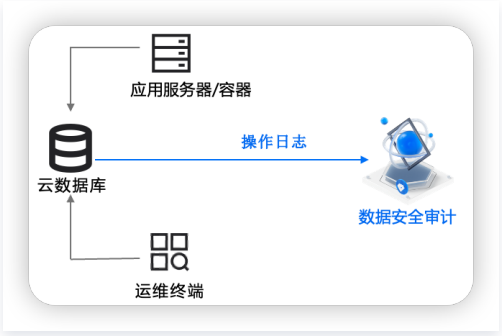
腾讯云数据库

- **同步云数据库清单**

支持一键同步云上资产，无需人工手动添加和排查。操作详情参见 云数据库资产 。

- **云原生审计**

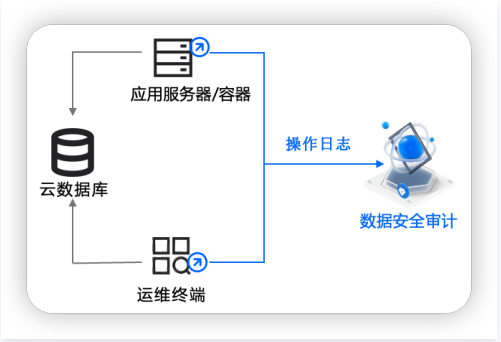
无需部署 Agent，云数据库自动上报操作日志。操作详情请参见 开启云原生审计 。



- **Agent 审计**

部署 Agent 在数据库应用端服务器/容器，部分服务器支持在线批量部署。操作详情请参见：

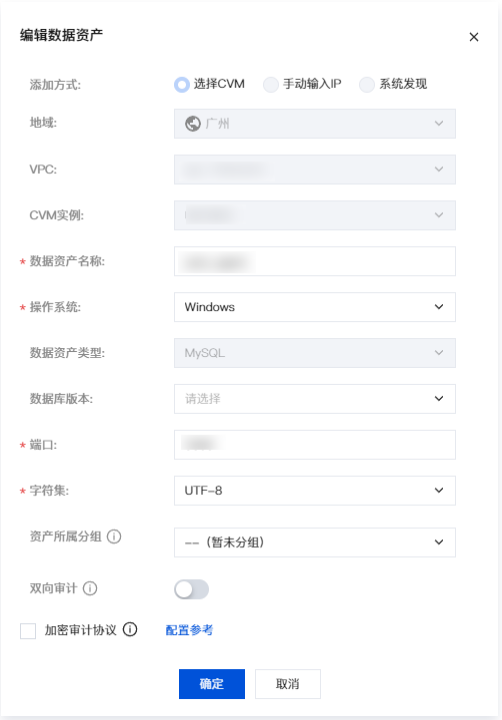
- 在服务器、容器节点部署 Agent：Agent 部署说明 。
- 在容器部署 Agent：容器部署 Agent 实践 。



腾讯云自建数据库

- **手动添加数据库**

支持选择 CVM 和手动输入 IP 两种手动添加数据库方式，操作详情参见 自建数据库资产 。



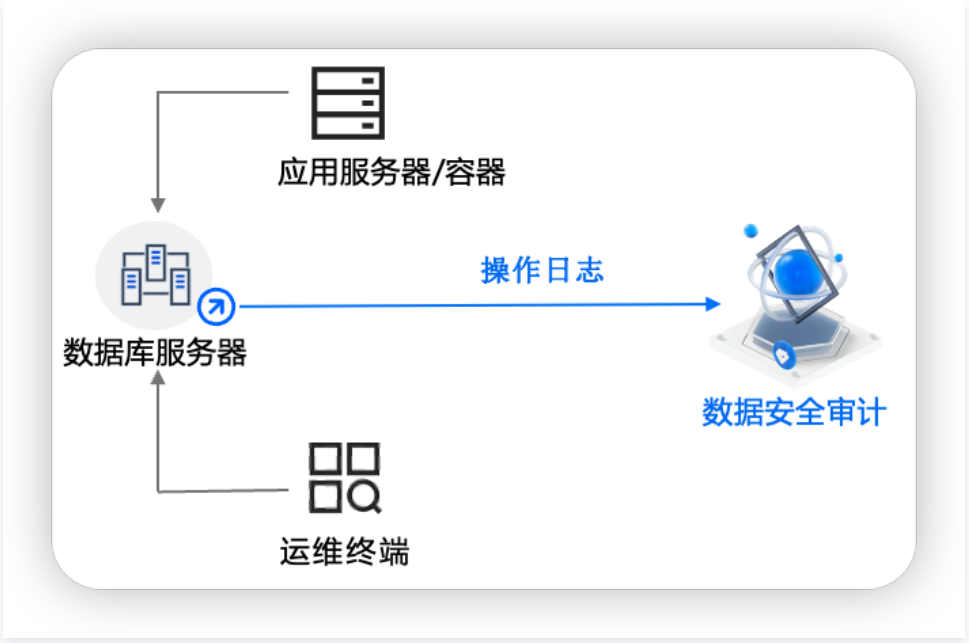
- **同步自建数据库清单**

针对已开启主机安全的用户，支持一键同步主机上自建数据库清单，无需人工手动添加和排查。

- **Agent 审计**

部署 Agent 在数据库服务端服务器/容器，部分服务器支持在线批量部署。操作详情请参见：

- 在服务器、容器节点部署 Agent：Agent 部署说明 。
- 在容器部署 Agent：容器部署 Agent 实践 。



云外云数据库

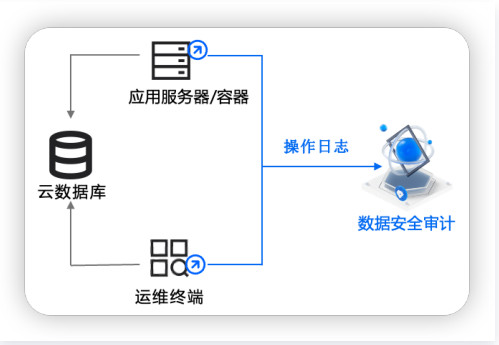
- **手动添加数据库**

云外数据库需手动添加，操作详情参见 云外数据库资产 。

- **Agent 审计**

部署 Agent 在数据库应用端服务器/容器，部分服务器支持在线批量部署。操作详情请参见：

- 在服务器、容器节点部署 Agent：Agent 部署说明 。
- 在容器部署 Agent：容器部署 Agent 实践 。



> **注意：** Agent区分腾讯云内Agent和云外Agent，根据Agent部署的应用服务器位置选择对应Agent。

云外自建数据库

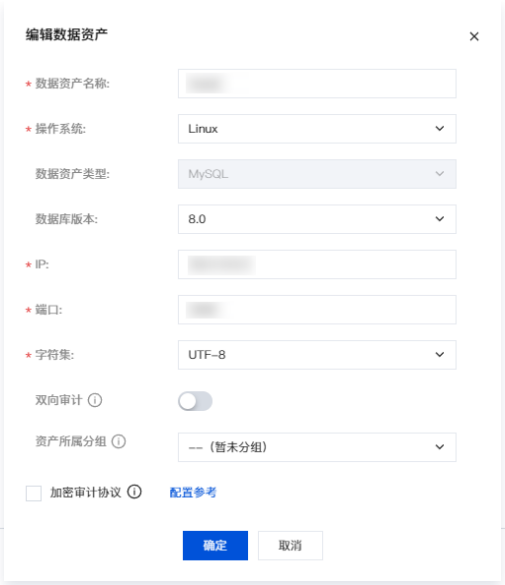
- **手动添加数据库**

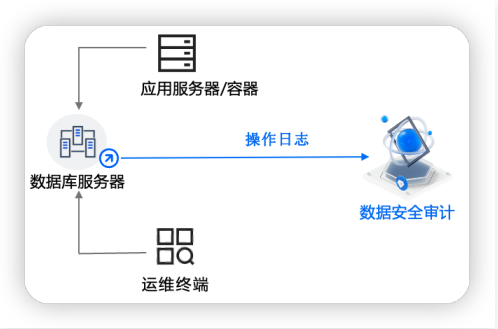
云外数据库需手动添加，操作详情参见 云外数据库资产 。

- **Agent 审计**

部署 Agent 在数据库服务端（服务器/容器），部分服务器支持在线批量部署。操作详情请参见：

- 在服务器、容器节点部署 Agent：Agent 部署说明 。
- 在容器部署 Agent：容器部署 Agent 实践 。





注意：

Agent 区分腾讯云内 Agent 和云外 Agent，根据 Agent 部署的应用服务器位置选择对应 Agent。

轻量应用服务器部署 Agent 实践教程

最近更新时间：2025-07-30 17:21:22

应用场景

大部分用户都在使用腾讯云轻量应用服务器，在使用数据安全审计时面临两个问题：

- 场景1：自建数据库部署在轻量应用服务器中，应怎么在数据安全审计中添加资产？
- 场景2：应用系统部署在轻量应用服务器中，应怎么部署 Agent？

本文将介绍如何解决上述轻量应用服务器部署问题。

场景解析

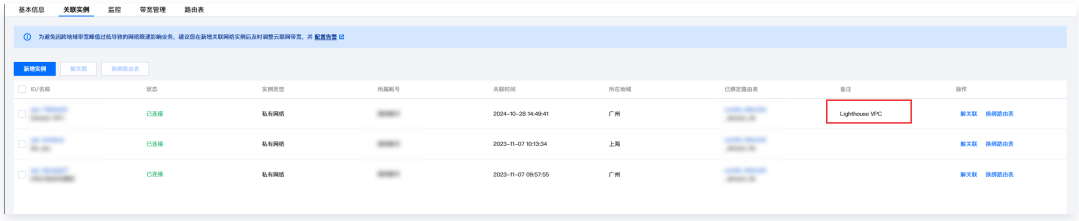
由于轻量应用服务器在单独的私有网络 VPC 中，与其他腾讯云资源（包括数据安全审计）默认未实现内网互联。因此需要通过关联云联网，与其他 VPC 实现内网互联，才可正常使用数据安全审计。

操作步骤

内网互联

1. 进入轻量应用服务器的 内网互联，在需要的地域关联云联网。可参考对应的 帮助文档。
2. 关联成功后，在 云联网页面 单击**管理实例**查看对应的实例详情。

3. 在关联实例页面，备注为 `Lighthouse VPC` 的即为该轻量服务器的 VPC，另一 VPC 则为与之互联的私有网络 VPC。



场景1：添加资产

若数据库部署在轻量应用服务器上，则需要通过以下方式添加资产。

> **说明**
> 已完成该轻量应用服务器对应地域的 内网互联 设置。

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** > **自建数据库**。

2. 在自建数据库页面，单击**添加数据资产**，选择所需参数，单击**提交并关闭**即可完成添加。

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。 • MariaDB：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。详情请参见添加页面的 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。

场景2：部署 Agent

本场景包含两种子场景，可根据实际需求选择如下任意方案。

> **说明**
> 已完成该轻量应用服务器对应地域的 内网互联 设置。

- 数据库**在轻量应用服务器**中：在按照 场景1 的方法添加资产后，在 Agent 管理页面 下载 Agent，参考 Agent 管理文档，在数据库所在轻量应用服务器或应用系统所在轻量应用服务器部署即可。

- 数据库**不在轻量应用服务器**中（如使用云数据库、CVM 中的自建数据库）：请确保内网互联中的云联网对端 VPC 为数据库所在 VPC，并在 Agent 管理页面 下载 Agent，参考 Agent 管理文档，在应用系统所在轻量应用服务器部署即可。

容器服务部署 Agent 实践教程

最近更新时间：2025-04-30 17:51:52

前提条件

已 添加资产并开启审计权限，Agent 配置才能正常监听资产。

操作步骤

1. 在 Agent 管理页面，下载 Agent。
2. 解压 Agent，目录为 CapAgent。
3. 将解压后的 Agent 目录 CapAgent 放在业务容器 Dockerfile 目录。
4. 在业务容器的 Dockerfile 中，添加如下 Agent 启动命令，Agent 的启动目录支持自定义，本文将其设置为 /data/dbagent。

```
RUN     mkdir  -p /data/dbagent
COPY    ./CapAgent  /data/dbagent/CapAgent
COPY    ./start_agent.sh   /etc/kickStart.d/
RUN  chmod  +x /etc/kickStart.d/start_agent.sh
```

5. start_agent.sh 是用于 Agent 的脚本，请注意 Agent 的启动目录，内容如下：

```
#! /bin/bash
cd  /data/dbagent/CapAgent/bin/
nohup  ./start.sh   1> /dev/null  2> /dev/null
```

6. 创建镜像。

云原生审计实践教程

最近更新时间：2025-07-30 17:21:22

应用场景

数据安全审计支持云原生审计模式，只需要一键开启审计权限，即可对云数据库进行安全审计，无需安装 Agent 或插件。

功能限制

本功能当前仅支持腾讯云数据库 MySQL 的云原生审计 。

> **说明：**
> 云数据库 MySQL 支持数据库审计能力的版本为：MySQL 5.6 20180101及以上版本、MySQL 5.7 20190429及以上版本、MySQL 8.0 20210330及以上版本的双节点和三节点，MySQL 5.5版本和云数据库 MySQL 单节点、集群版都暂不支持数据库审计能力。

操作步骤

1. 在 数据资产页面，单击**更新资产列表**进行数据资产同步。

2. 选择目标数据库，单击云原生审计权限列的**开关**，启用云原生审计权限。

3. 云原生审计权限开启后，即可在 审计日志页面，查看目标数据库的**审计日志信息**。

4. 在 风险识别页面，查看是否触发安全风险。

敏感数据操作精准溯源与风险监控

最近更新时间：2025-07-16 17:59:22

数据安全审计与数据安全治理中心的深度集成，实现了分类分级结果向审计日志的自动同步，为企业提供敏感数据操作的精准溯源与风险监控能力。以下是详细说明：

前提条件

具备敏感数据识别资源：已 购买数据安全治理中心实例 。

配置步骤

持续自动化识别数据分类分级

步骤一：配置分类分级模板

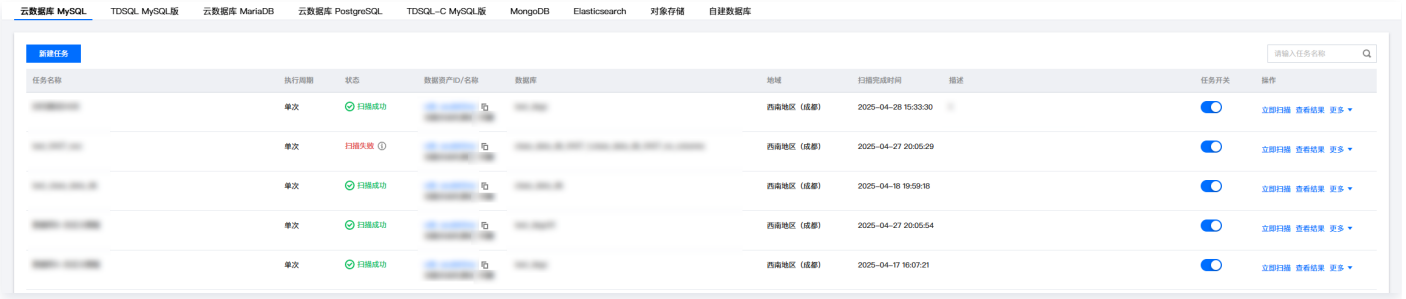
建立敏感数据 “识别标准”（定义分类、分级），为后续敏感数据识别与治理奠定基础。

1. 登录 数据安全治理中心控制台，在左侧导航栏中，单击**分类分级 > 分类分级配置**。
2. 在分类分级配置页面，参考 分类分级模板配置 进行新建/导入模板。

步骤二：定期执行分类分级任务

全面梳理敏感资产，持续动态发现敏感数据，解决 “数据资产不清晰” 问题，避免新增敏感字段无感知。

1. 登录 数据安全治理中心控制台，在左侧导航栏中，单击**分类分级 > 分类分级任务**。
2. 在分类分级配置页面，参考 分类分级任务 创建新的分类分级任务。

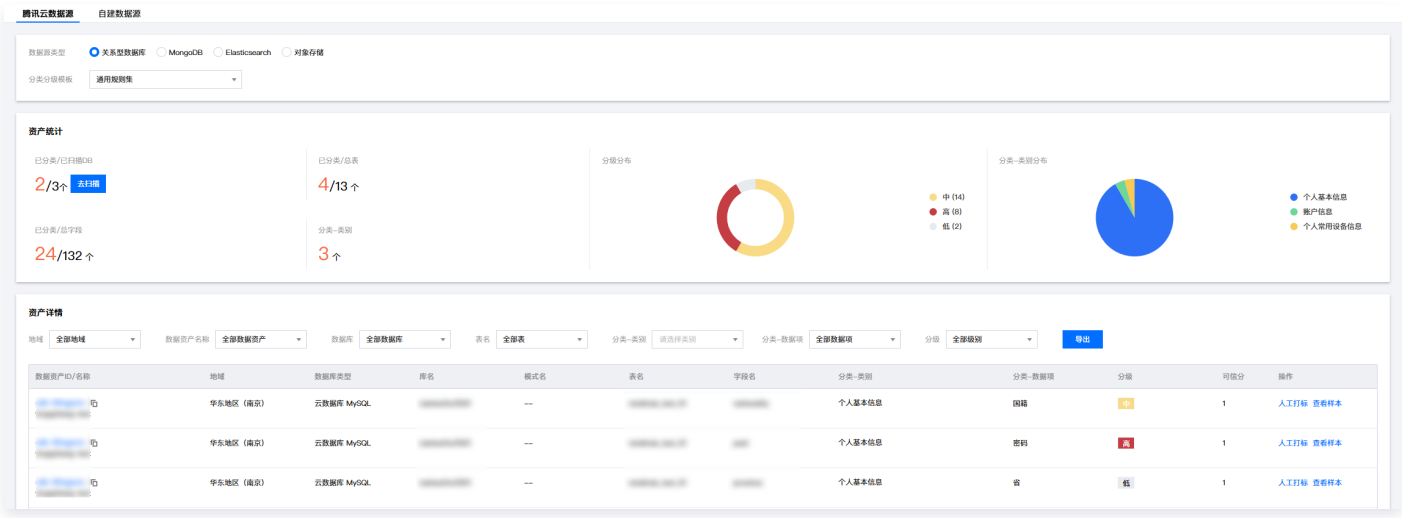


步骤三：分类分级结果查看与手动调整

人工矫正识别结果，可修正自动化识别误差（约 5%-10% 的模糊场景），确保分类分级结果贴合业务实际情况。

1. 登录 数据安全治理中心控制台，在左侧导航栏中，单击**分类分级 > 敏感数据资产**。
2. 在敏感数据资产页面，您可以查看指定数据库、表的敏感数据详情，同时也支持按照不同的分类、分级进行敏感数据的筛选。
3. 单击**查看样本**，可随机展示该字段的抽样数据信息，您可以依据抽样数据进行识别结果的判断。

4. 对误判字段（如 “普通编号” 被误标为 “身份证号”），您可以单击**人工打标**，对该字段进行识别结果的修改。



数据安全审计关联分类分级资源

数据安全审计与 DSGC 中分类分级资源关联，使 DSGC 中的分类分级结果能够同步至数据安全审计中，为后续对敏感数据操作的精准审计提供数据支持。

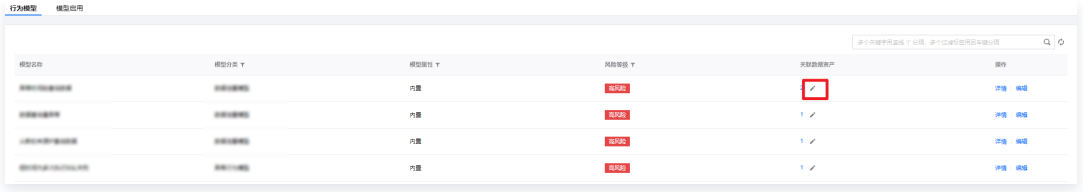
1. 登录 数据安全审计控制台，在左侧导航栏中，单击**数据资产**。
2. 在数据资产页面，单击右上角**敏感识别资源-配置**。

3. 在配置弹窗中，选择需要绑定的数据安全治理中心实例和分类分级模板，单击**确定**即可完成分类分级资源的配置。

智能行为模型关联资产

将智能行为模型与具体的资产关联起来，使模型能够针对这些资产中被分类分级的敏感数据进行监控和分析，确保模型的监控范围与需要重点关注的敏感数据所在资产一致。

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**。
2. 在行为模型页面，选择针对敏感数据的行为模型，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。

启用智能行为模型

启动智能行为模型，使其能够实时对关联资产中敏感数据的操作进行分析和识别，及时发现异常行为和风险操作，实现对敏感数据的动态监控和风险预警。

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**。
2. 在行为模型页面，单击**模型启用**。
3. 在模型启用页面，单击开启已配置关联资产的智能行为模型。

验证测试

测试用例1：敏感数据审计日志

1. 连接目标数据库，执行包含敏感字段的查询。
2. 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**。
3. 在审计日志页面，您可根据具体的数据资产名称进行日志检索。
4. 选择目标日志，单击操作栏中的**详情**，可查看日志详情，并在日志中验证是否包含分类分级信息。

测试用例2：触发智能行为告警（需等待模型建立基线）

1. 模拟异常行为：使用非管理员账号在非工作时间（如凌晨2点）查询大量敏感数据；
2. 预期结果：10分钟内，数据安全审计将触发异常操作告警（企业微信/短信/邮件），并在控制台的“风险事件”中生成记录。

常见问题

分类分级标签未出现在审计日志中怎么办?

检查步骤

1. 确认 DSGC 的分类分级任务已成功执行且包含目标字段。
2. 在 DSGC 的“敏感数据资产”页面中确认字段是否有被正确识别为敏感数据。
3. 在数据安全审计的“敏感识别资源”配置中确认关联的 DSGC 实例和模板正确。

智能行为模型未产生告警?

可能原因

- 模型尚未建立基线（默认7天），此期间不产生告警。
- 测试操作未达到异常阈值（如查询量过小）。
- 数据安全审计未开启行为模型告警。

排查步骤

1. 在 模型启用页面，检查模型状态是否已启用。
2. 在 模型风险页面，手动检查测试操作是否被记录（即使未告警）。
3. 在 告警设置页面，检查行为模型告警是否开启。