

数据安全审计

故障处理



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分內容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

故障处理

无法在审计日志页面查询到日志

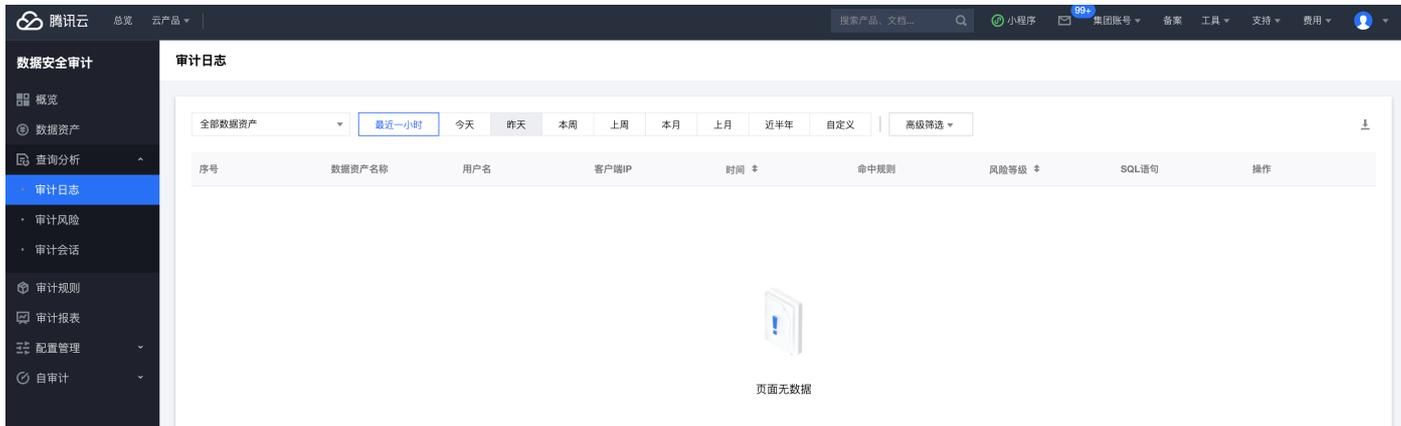
故障处理

无法在审计日志页面查询到日志

最近更新时间：2023-09-26 14:26:53

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：



说明

此处以 SaaS 型为例，大部分场景可供传统型参考，若无法确定，请 [联系我们](#) 协助您处理。

可能原因

1. 未正确添加对应数据库或未开启审计权限。
2. 数据库在本地操作，未经过网络。
3. 数据库开启了 SSL 加密。
4. 未正确部署 Agent。

解决思路

根据以上4种可能的原因，逐项排查。

处理步骤

按以下顺序，逐个排查，直到发现真正的问题原因，得到解决。

步骤1：检查是否已正确添加对应资产且开启审计权限

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。



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。

数据资产名称	添加方式	实例ID名称	数据资产类型	版本	VPC	内网IP	地域	审计权限	操作
			MySQL	-	vpc-		广州	<input type="checkbox"/>	编辑 删除
			MySQL	5.1	vpc-		广州	<input type="checkbox"/>	编辑 删除

步骤2：检查是否为本地审计

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。具体操作详情请参见 [数据资产](#)。

步骤3：检查数据库开启了 SSL 加密

若数据库开启了 SSL，则流量数据包处于加密状态，数据安全审计无法解析。

1. 在数据库中，输入如下命令，确认是否开启了 SSL 加密。

说明

命令仅支持 MySQL 数据库，其他类型数据库请自行查找。

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

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_cpath     |        |
| ssl_cert      | server-cert.pem |
| ssl_cipher    |        |
| ssl_crl       |        |
| ssl_crlpath   |        |
| ssl_key       | server-key.pem |
+-----+-----+
```

步骤4：排查是否已正确部署 Agent

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。

说明

下载的 Agent 安装包名为：dsaagent_部署位置_操作系统_xxx.zip。不同操作系统的安装包名如下所示：

- dsaagent_innernet_linux_xxx.zip 表示为腾讯云内网、操作系统为 Linux 的 Agent。

○ dsaagent_outnet_win_xxx.zip 表示为腾讯云外、操作系统为 Windows 的 Agent。

2. 若为腾讯云内网 Agent，需要在下载 Agent 之前，已完成待部署 Agent 的 VPC 打通（开通该 VPC 资产的审计权限即可打通），可在 [VPC 通道列表](#) 查看已打通了的 VPC。



3. 若为腾讯云外 Agent，请 [联系我们](#) 并提供 Agent 所属主机的外网 IP，我们将为您开通白名单。

4. 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。

5. 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。

若经上述操作排查后，仍无法看到日志，请 [联系我们](#) 并提供 Agent 所属主机的外网 IP，我们将协助您进一步排查问题。