数据安全审计

快速入门

腾讯云

文档目录

快速入门
数据安全审计 SaaS 型
操作指引

最近更新时间：2023-09-26 14:26:51

本文将为您介绍如何快速使用数据安全审计 SaaS 型。

前提条件

已购买 数据安全审计SaaS型 。

步骤1：同步数据资产

1. 登录 数据安全审计控制台，单击**立即进入**。

2. 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。

3. 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，当需要审计腾讯云外的数据资产时，可在腾讯云外数据库添加。

4. 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。

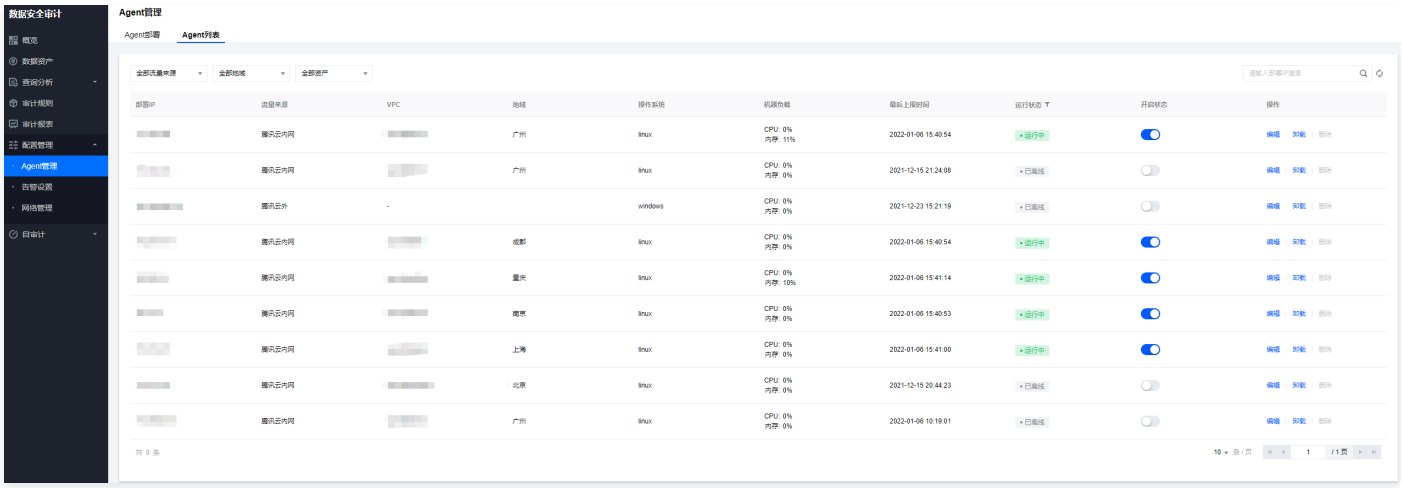
- 开启审计权限将消耗 License 授权资产数。
- 部分操作需要用户授权，只需按提示操作即可。

- 如果开启的是代理审计权限，则需要购买 云访问安全代理，并且将对应元数据与代理绑定。

步骤2： 部署 Agent

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。
2. 在 Agent 部署中，根据数据库和应用系统所在位置和操作系统，下载对应的 Agent，进行部署。

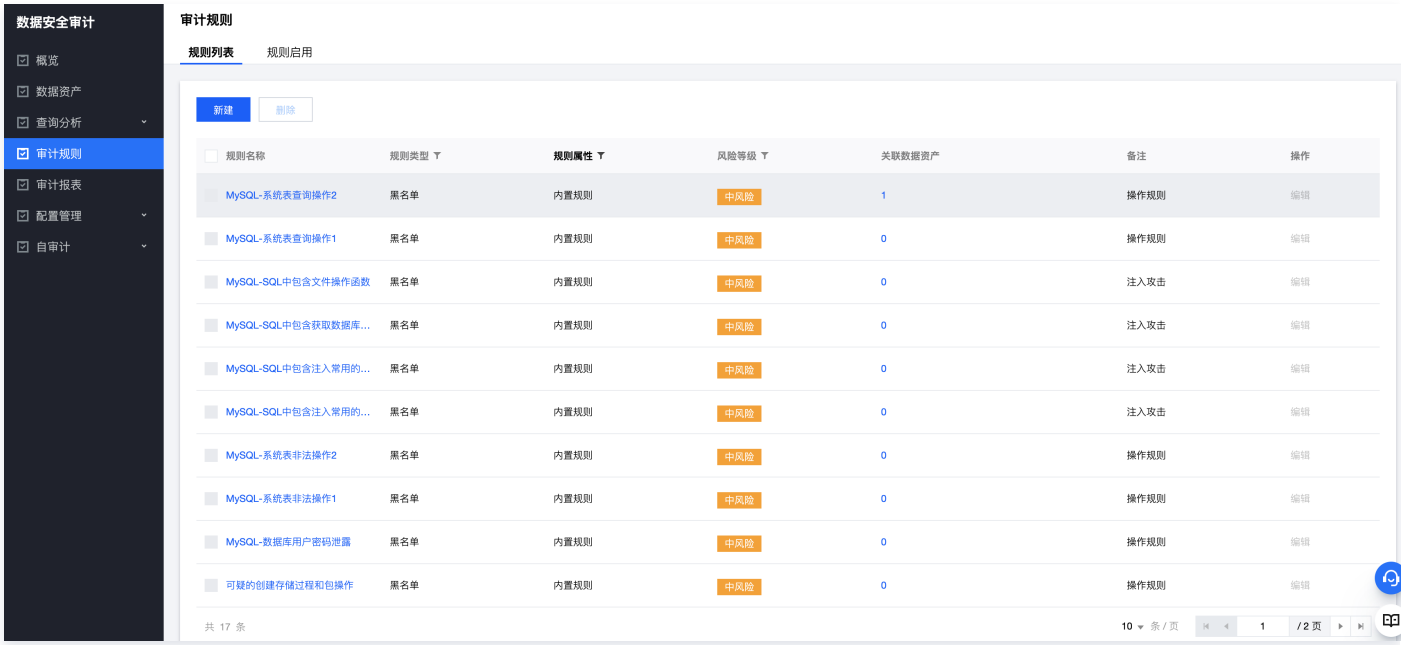
3. Agent 部署完成后，单击 **Agent 列表**，切换至 Agent 列表页面，验证 Agent 状态是否正常。



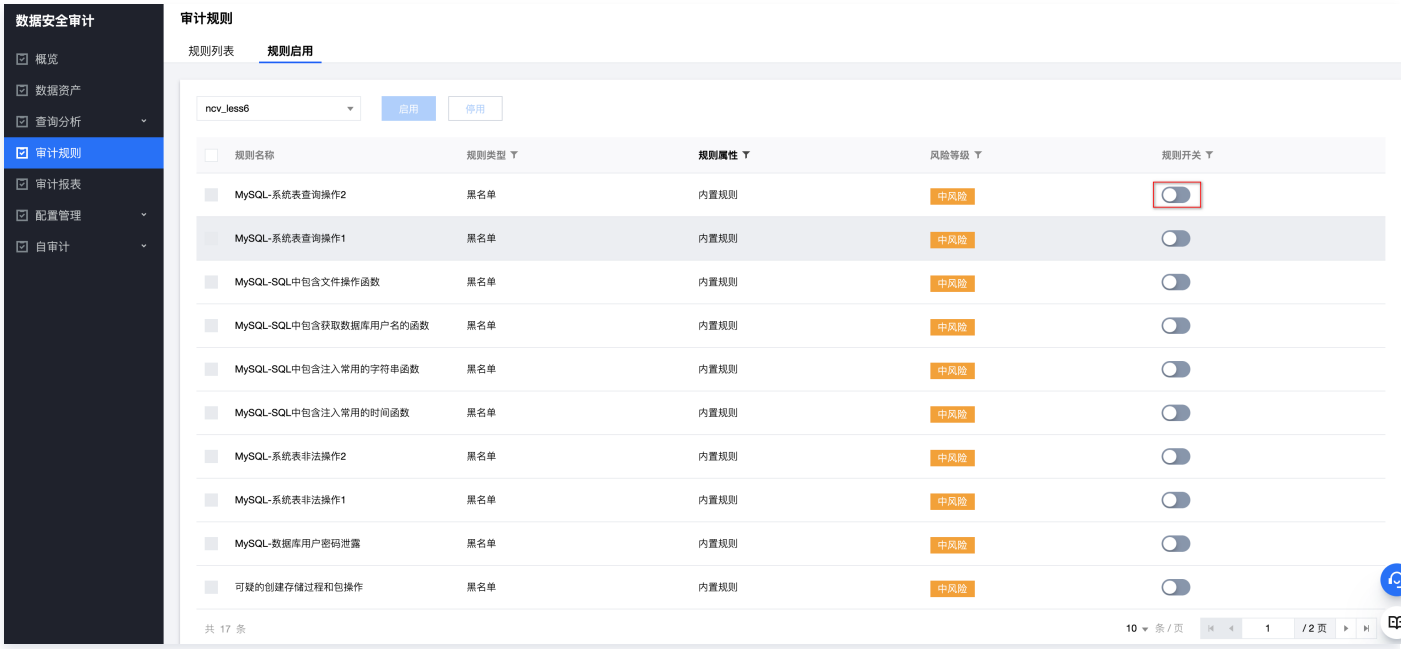
步骤3：配置审计规则

开启数据资产的审计权限后，将默认启用常见内置审计规则。用户可在审计规则页面对规则进行进一步管理。

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。

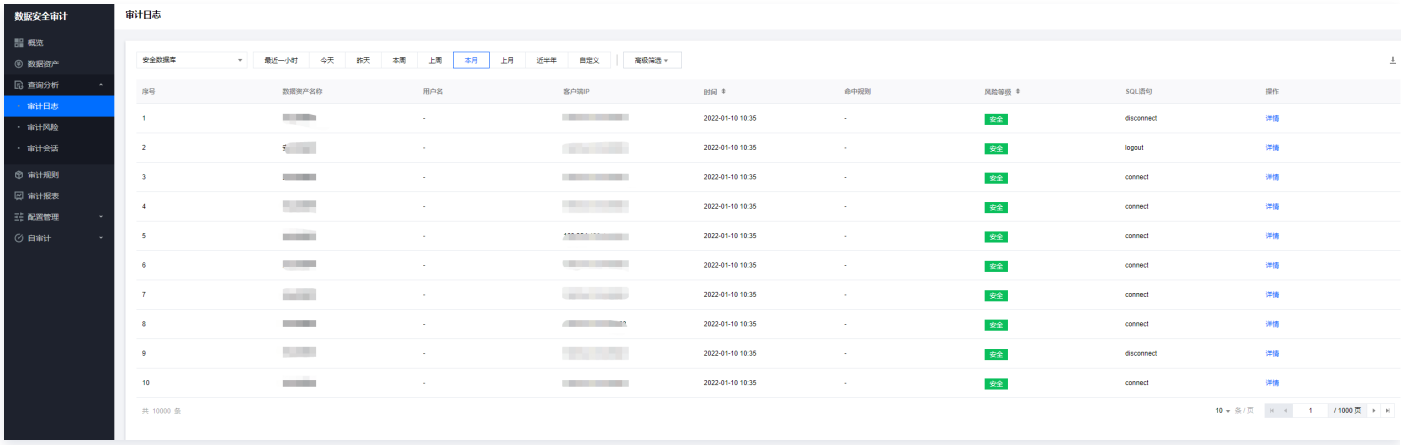


2. 单击**规则启用**，进入规则启用页面，选择数据资产，为其启用需要的审计规则。

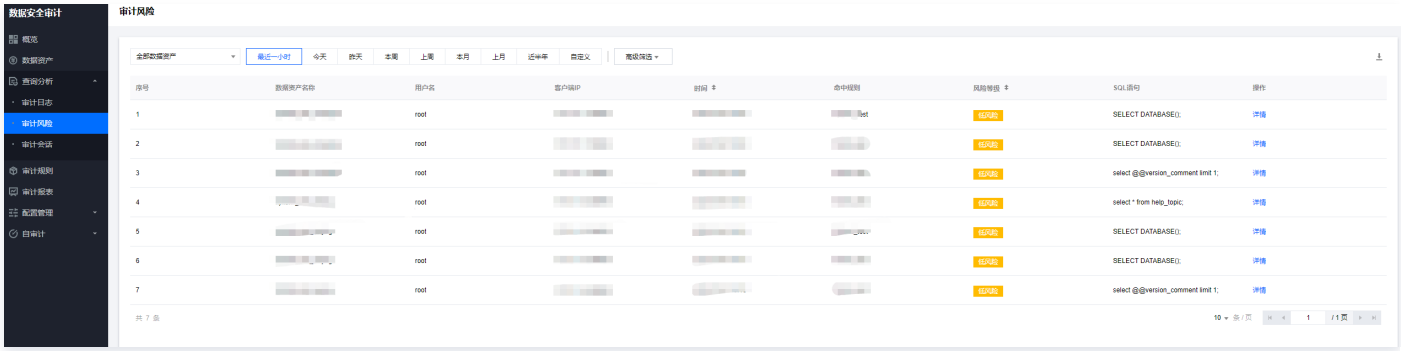


步骤4：查看审计日志

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。



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。



Agent 部署

最近更新时间：2024-01-11 14:06:21

数据安全审计部署的核心目标是把 Agent 安装到数据库服务器或访问数据库的应用服务器中。Agent 部署流程如下所示：

1. 配置数据资产实例，操作详情请参见 管理自建数据库 。
2. 开启审计权限，操作详情请参见 管理云数据库 。
3. 部署 Agent，支持在线部署或下载 Agent。
4. Agent 安装。

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。
- Linux 在线部署：对于腾讯云内网的 Linux 系统，推荐使用在线部署。

> ⚠ 注意
> - 腾讯云内网 Agent：确保部署 Agent 的 VPC 已在 VPC 通道列表中，添加该 VPC 的资产即可自动创建 VPC 通道。
> - 腾讯云外 Agent：需要开通白名单，腾讯云外 Agent 才能正常上报流量。请 联系我们 协助开通。
> - 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）。

部署 Agent

在线部署

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。
1. 在 Agent 部署页面，单击 **Linux 在线部署**。
2. 在 Agent 在线部署页面，选择 CVM 所在的地域和 VPC ，在需要部署 Agent 的 CVM 后单击**部署**，即可自动部署 Agent 。已经部署的 Agent ，可执行卸载操作（即使 Agent 未连接，在此也可以在线卸载）。还可以选中多个 CVM ，进行批量部署。

> ⚠ 注意
> - 在线部署暂时仅支持腾讯云内网的 Linux 操作系统。
> - 使用在线部署的前提是该 CVM 实例已安装 自动化助手 。

下载 Agent

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

> **注意**
> Agent 安装包已通过文件名区分部署场景，在部署前仔细检查，避免出错。
> - 如 dsaagent_innernet_linux _xxx.zip 是腾讯云内网 Linux Agent。
> - 如 dsaagent_outnet_win_xxx.zip 是腾讯云外 Windows Agent。

Agent 安装

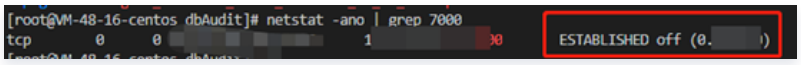
下载 Agent 完成后，需要将 Agent 安装在相应服务器上才能实现审计效果。

- 如果您使用的是云服务器 + 自建数据库模式，则建议您将 Agent 安装在数据库服务器上。
- 如果您使用的是云数据库，则需要在连接数据库的应用服务器上安装 Agent。

Linux 版本

> **注意**
> Linux 需在部署 Agent 之前，安装 python2。

1. 将 `dsaagent_innernet_linux _xxx.zip` 安装包上传到需要安装的机器上，如 /data。
2. 使用 `unzip dsaagent_innernet_xxx.zip` 命令进行解压，得到 /data/CapAgent 目录。
3. 执行命令 `chmod -R 755 CapAgent` 。
4. 执行 `cd CapAgent/bin` ，再执行 `nohup ./start.sh 1>/dev/null 2>/dev/nul` 。
5. 在命令行，执行 `netstat -ano | grep 7000` 如下图即确认连接成功。



> **说明**
> 其他命令。

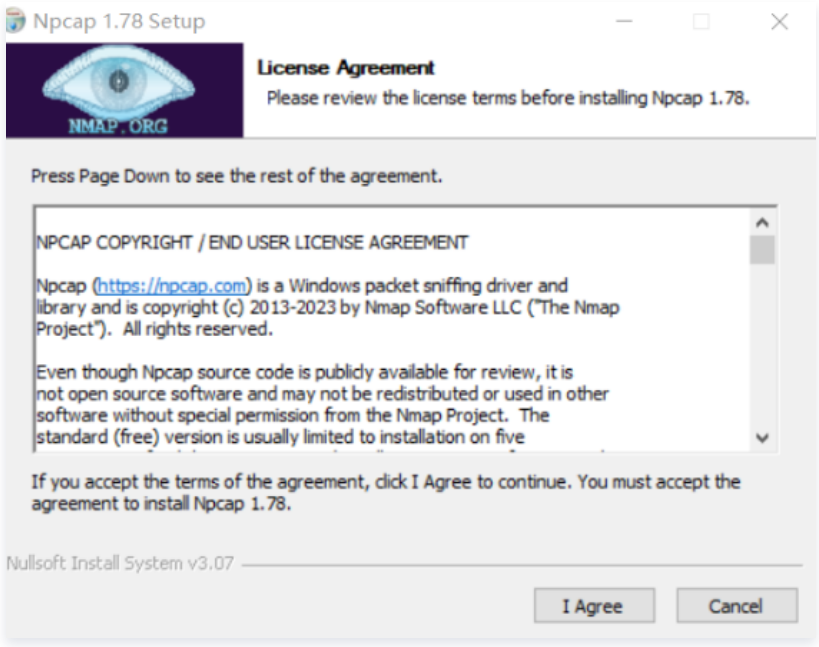
- 停止 agent：`nohup ./stop.sh 1>/dev/null 2>/dev/nul` 。
- 重启 agent：`nohup ./restart.sh 1>/dev/null 2>/dev/nul` 。

Windows 版本

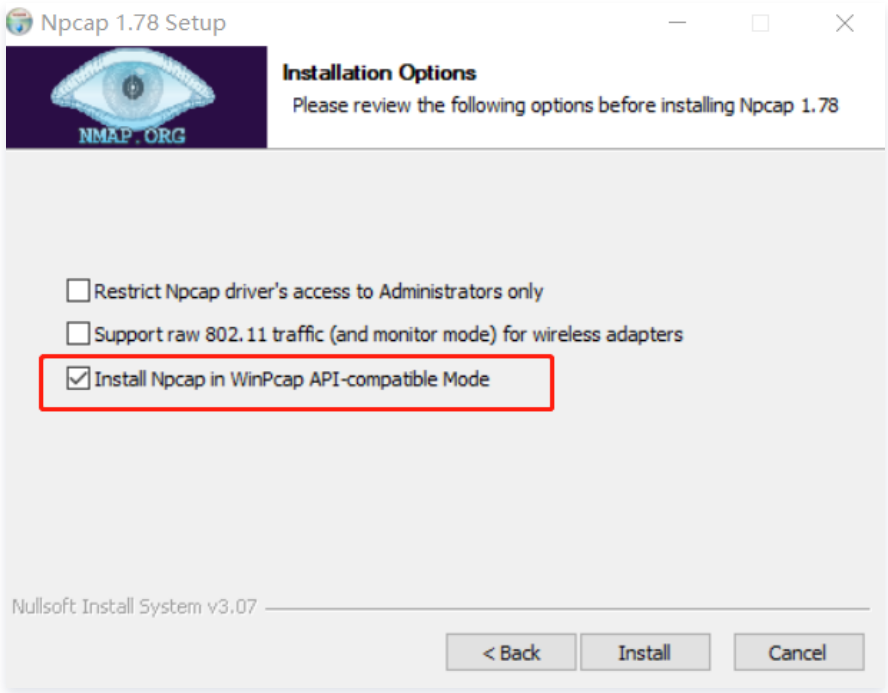
数据安全审计 Agent Windows 版本只支持 Windows vista/2008 及以上版本。

1. 下载 Windows 版本 Agent 后，解压到安装目录。
2. 安装 Npcap。

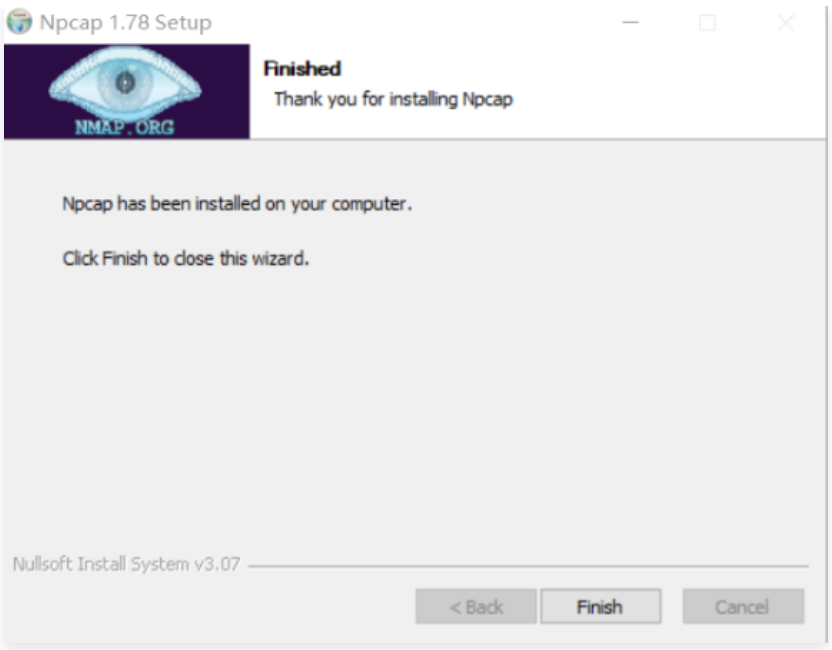
2.1 进入 CapAgent 下的 thirdparty 目录，双击 npcap-1.78.exe，单击 **I Agree**。



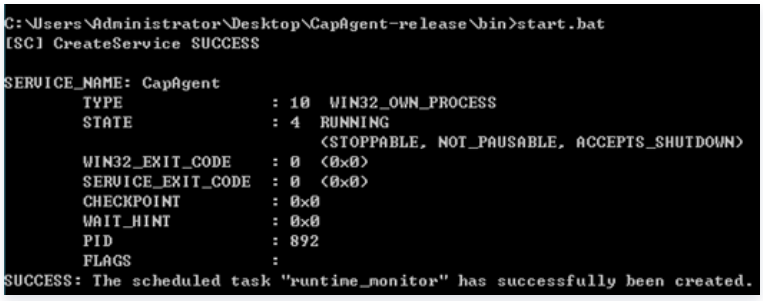
2.2 勾选 **Install Npcap in WinPcap API-compatible Mode**，单击 **Install**。



2.3 单击 **Next** > **Finish**，Npcap 安装成功。

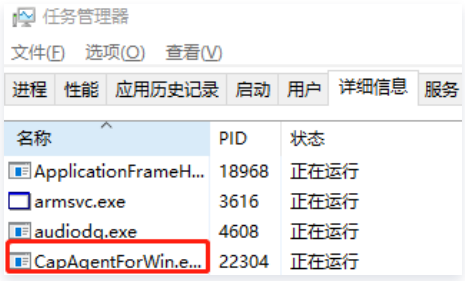


3. 进入 CapAgent下的 bin 目录，使用管理员用户双击 star.bat 文件。
4. 执行成功后，Console 显示结果如下图所示。同时，可以在任务管理器中，看到 CapAgentForWin.exe 进程。

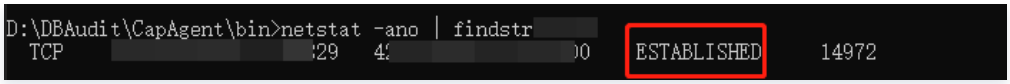


5. 检查 CapAgentForWin 是否成功启动并连接审计服务成功。

   5.1 在任务管理器中确认 CapAgentForWin 进程已运行。



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



> **说明**
> 如果 CapAgentForWin 不能运行或 `netstat -ano | findstr 7000` 命令执行不成功，请 联系我们 获得支持。

6. Agent 停止。
   在 CapAgent_win/bin 目录下双击 stop.bat 文件即可。

数据安全审计传统型
产品初始化

最近更新时间：2021-12-06 16:50:13

购买数据安全审计传统型后，初次使用前，需要进行初始化操作。下面为您详细介绍如何初始化。

1. 登录 数据安全审计控制台，单击**查看传统型**。
2. 在数据安全审计传统型控制台，可以看到您已购买的数据安全审计实例，选择尚未初始化的数据安全审计实例，单击右侧**初始化**。

3. 在弹出的初始化窗口，选择与需要审计的数据库对应的地域和 VPC、子网。

> **说明**
> - 每套数据安全审计，仅支持审计同一 VPC，若您的数据库在不同 VPC 中，请购买多套数据库安全审计。
> - 若需要在金融区中部署，请单击初始化窗口中的**详情**。

控制台登录

最近更新时间：2021-12-06 16:53:29

购买数据安全审计传统型后，您可进入数据安全审计管理界面进行配置，下面将为您详细介绍如何进入管理页面。

1. 登录 数据安全审计控制台，单击**查看传统型**。

2. 在数据安全审计传统型控制台，可以看到您已购买的数据安全审计实例，选择任意数据安全审计实例，单击右侧**管理**。

3. 浏览器将弹出新窗口以显示数据安全审计登录界面。

4. 在登录界面输入系统管理员账户 sysadmin 与密码（默认密码在购买时将通过站内信发送）进入管理界面，即可开始配置。

> **说明**
> 若忘记密码，可以 联系我们 进行密码重置。

产品部署
账户体系说明

最近更新时间：2022-11-17 15:28:05

数据安全审计为严格确保自身系统安全，防止单一管理员账号权力过大导致内部失控，提供了三权分立账户体系。该体系具备三类管理员：系统管理员、审计管理员、操作审计员，三者相互制约，确保安全。每个管理员的职责和权限如下：

系统管理员

负责数据安全审计系统自身相关信息的查询以及自身相关功能的配置，具备其他账号的增删改权限，该角色内置账号 sysadmin。

审计管理员

负责数据安全审计业务，包括资源管理、规则配置、审计信息查询等，该角色内置账号 useradmin。

操作审计员

负责审计数据安全审计各管理员账号的操作，防止其他管理员滥用职权进行非法操作，该角色内置账号 sysaudit。

> **注意**
> 上述账号默认密码将在购买后通过腾讯云站内信发送，请注意查收站内信消息。

Agent 部署

最近更新时间：2022-11-17 15:23:08

数据安全审计部署的核心目标是把 Agent 安装到数据库服务器或访问数据库的应用服务器中，并且确保数据库服务器或访问数据库的应用服务器，与数据安全审计的审计实例能实现网络连通。
Agent 部署流程如下图所示，其中前五步为参数配置操作：

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 TencentDB：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。

配置数据资产

1. 已完成 控制台登录 操作后，通过 useradmin 账号登录数据安全审计管理页面（默认密码在购买时将通过站内信发送），在左侧导航中，选择**数据资产与 Agent > 审计的数据资产**，进入审计的数据资产页面。
2. 在审计的数据资产页面，单击**添加数据资产**，进入添加数据资产框，输入数据资产名称，选择数据资产类型和数据资产 IP 和 Port。
   - 数据资产名称：数据库名称，必填140个字符内。
   - 数据资产类型：数据库的类型。
   - 数据资产 IP：数据库服务器 IP 地址。
   - Port：数据资产对应的端口。

3. 单击**确定**，提示添加成功。
4. Agent 下载。
   4.1 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Agent配置页面。
   4.2 在审计用 Agent 页面，选择 **Agent下载 > 添加**，输入 Agent 名称，勾选对应得数据资产。单击**确定**即可。
   4.3 配置成功后，可以下载选择**下载 Linux Agent**、**下载 Windows Agent**或**linux 批量部署**进行配置 Agent。

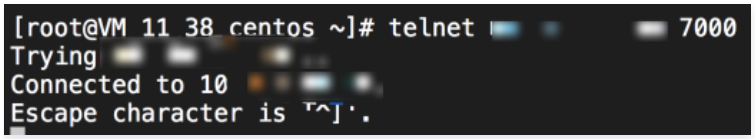
> **说明**
> - 设置停止审计阈值。若被审计数据库因性能导致濒临宕机，可以通过关闭更多服务和进程缓解宕机情况。您可以设置一个基于 CPU 与内存使用率的阈值，当被审计数据库超过阈值时，Agent 将发送告警信息并停止工作，缓解数据库的性能压力。
> - 如您要求 Agent 任何情况都进行工作，可将负载检测开关关闭，Agent将持续审计数据。

Agent 安装

下载 Agent 完成后，需要将 Agent 安装在相应服务器上才能实现审计效果。

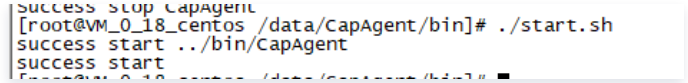
- 如果您使用的是云服务器 + 自建数据库模式，则建议您将 Agent 安装在数据库服务器上。
- 如果您使用的是 TencentDB，则需要在连接数据库的应用服务器上安装 Agent。

部署前确认 Agent 部署的机器和审计服务网络是否连通，使用 telnet 审计服务 IP 7000 （审计服务 IP 为 Agent 配置时审计服务 分配的 IP ），如下图所示，表示网络已经连通，如有问题请 提交工单 联系我们。



Linux 版本

1. 将 CapAgent_xxx.zip 安装包上传到需要安装的机器上，如 /data 目录。
2. 使用 `unzip CapAgent_xxx.zip` 命令进行解压，得到 /data/CapAgent 目录。
3. 执行命令 `chmod -R 755 CapAgent` 。
4. 执行 `cd CapAgent/bin` ，再执行 `./start.sh` ，结果如下，如未得到以下结果，请 提交工单 联系我们。



5. 在命令行，执行 `netstat -ano | grep 7000` 如下图即确认连接成功。

Windows 版本

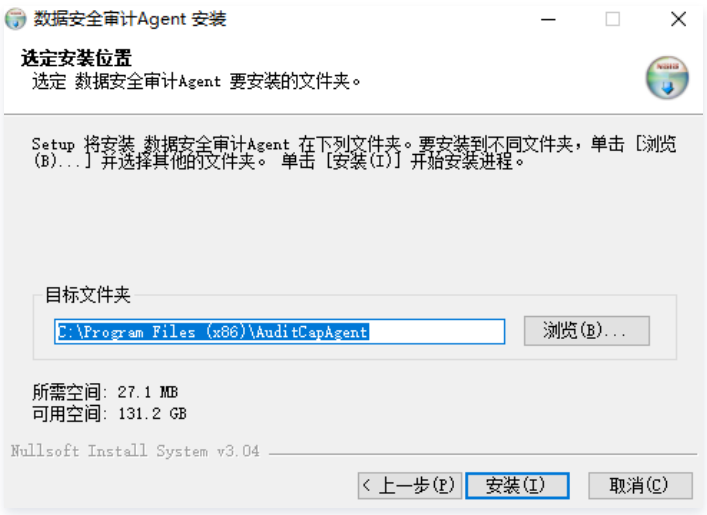
> **注意**
> 数据安全审计 Agent Windows 版本只支持 Windows vista/2008 及以上版本。

1. 下载 Windows 版本 Agent 后，解压到安装目录，进入 “CapAgent/conf” 目录，修改 config.ini 中 device 配置为本机访问数据库网卡的 IP（一般为内网 IP），如下图所示：

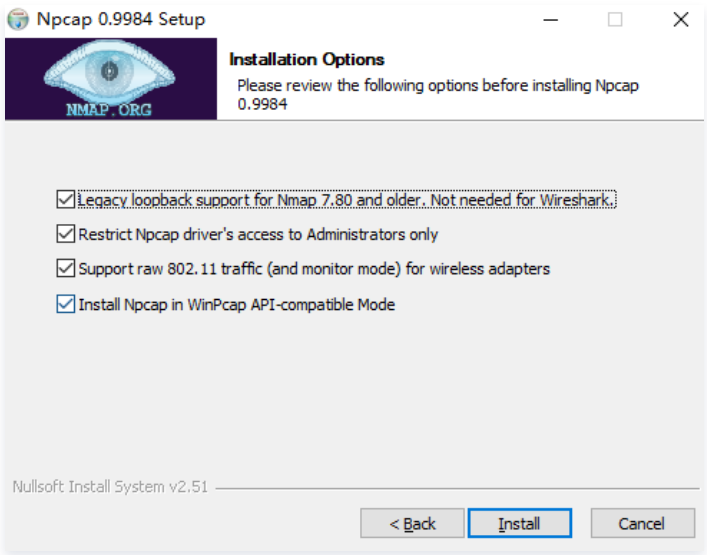
```
[local]
log_save_day=1

device=
loop_device=0.0.0.0
daemon=1

log=0
```

2. 进入 CapAgent_win 目录，执行文件夹中 AuditCapAgentSteup.exe 程序依次安装 Python3.8 环境、npcap0.9984、执行 CapAgent_win。

2.1 安装 Python3.8 环境，单击**下一步**，选择 Python3.8 安装的位置，单击**安装**。



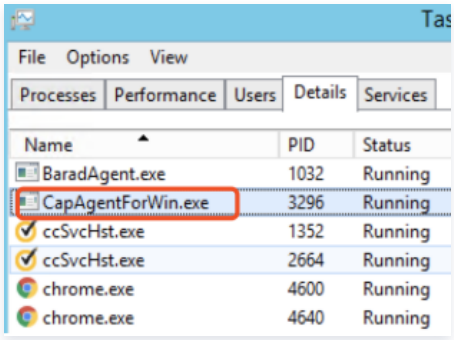
2.2 安装 Npcap0.9984，勾选全部，单击**Install**。



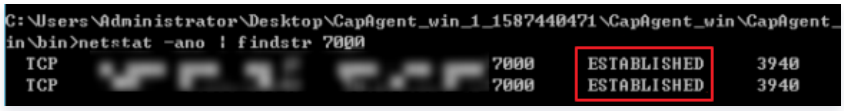
3. 执行成功后，Console 显示结果如下图所示。同时，可以在任务管理器中，看到 CapAgentForWin.exe 进程。

```
C:\Users\Administrator\Desktop\CapAgent-release\bin>start.bat
[SC] CreateService SUCCESS

SERVICE_NAME: CapAgent
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                             (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 892
        FLAGS              :
SUCCESS: The scheduled task "runtime_monitor" has successfully been created.
```

4. 检查 CapAgent_win 成功启动并连接审计服务成功。
   - 在任务管理器中确认 CapAgent_win 进程已运行，



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



5. Agent 停止。
   在 CapAgent_win/bin 目录下执行 stop.bat 即可。