

CECSTACK 5.2.0

数据库审计 DAS 用户指南（上）

文档密级：公开

文档版本：01

发布日期：2024-05-30

【版权声明】

版权所有 © 中电云计算技术有限公司 2024。保留一切权利。

本文档的版权归中电云计算技术有限公司所有。非经中电云计算技术有限公司书面许可，任何人不得以包括通过程序或设备监视、复制、传播、展示、镜像、上载、下载、摘编等方式或以其他方式擅自使用本文档的任何内容。

【商标声明】

 和本文档所示其他中电云计算技术有限公司及/或其他关联公司的商标均为中电云计算技术有限公司及/或其关联公司所有。未经中电云计算技术有限公司及/或其关联公司书面许可，任何人不得以任何形式使用，也不得向他人表明您有权展示、使用或做其他处理。如您有宣传、展示等任何使用需要，您必须取得中电云计算技术有限公司及/或其关联公司事先书面授权。

本文档中出现的其他公司的商标或注册商标，由各自的所有人拥有。

【注意】

您购买的产品、服务或特性等应以中电云计算技术有限公司商业合同中的约定为准，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，中电云计算技术有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容可能会不定期进行更新。本文档仅作为使用指导，其中的陈述、信息或建议等均不构成任何明示或暗示的担保。

前言

概述

本文档主要介绍数据库审计 DAS 的产品介绍、实例开通、安装 Agent、实例扩容、实例续订、实例释放、功能界面访问等操作，以便读者快速了解、使用数据库审计 DAS。

读者对象

本文档适用于以下读者：

- 维护工程师
- 技术支持工程师
- 系统管理员

本书约定

符号标志约定

本书采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。 “注意”不涉及人身伤害。
 说明	对正文的重点信息进行必要的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。
 提示	配置、操作、或使用产品的技巧、窍门。

修订记录

文档版本	发布时间	修订说明
01	2024-05-30	第一次正式发布。

目 录

1 产品介绍	1
1.1 什么是数据库审计	1
1.2 为什么选数据库审计	1
1.3 产品优势	1
1.4 产品功能	2
1.5 应用场景	3
1.6 使用限制	3
2 登录 DAS 控制台	1
3 快速入门	2
3.1 操作流程	2
3.2 开通数据库审计	2
3.3 安装 Agent	3
3.3.1 下载 Agent	3
3.3.2 Windows-agent 安装	4
3.3.3 Linux-agent 安装	9
3.4 配置报文转发	10
3.4.1 Linux 配置报文转发	10
3.4.2 Windows 配置报文转发	12
3.5 配置审计对象及规则	16
3.5.1 配置审计对象	16
3.5.2 配置审计规则	17
4 实例管理	18
4.1 扩容数据库审计	18
4.2 续费数据库审计	18
4.3 启动数据库审计	18
4.4 关闭数据库审计	18
4.5 退订数据库审计	18
4.6 DAS 实例到期/欠费	19
4.6.1 包周期计费模式下实例到期后状态变化	19
4.6.2 按需计费模式下账户欠费时实例变化	19
5 常见问题	20

1 产品介绍

1.1 什么是数据库审计

数据库审计 DAS (Database Auditor service, 以下简称 DAS) 能够实现数据库操作行为审计、事件追踪、威胁分析、实时告警等多种功能, 保障云环境下核心数据的安全防护, 以高性能的产品, 为云用户提供稳定可靠的数据库审计能力。

1.2 为什么选数据库审计

数据库存储着系统的核心数据, 其安全方面的问题在传统环境中已经很突出, 成为数据泄漏的重要根源。而在云端, 数据库所面临的威胁被进一步的放大。其安全问题主要来自于以下几方面:

- 来自于其他租户的攻击
同一个云平台上的其它租户, 有可能通过虚拟机逃逸等攻击方法, 得到数据库中的数据。
- 来自租户自身内部人员的威胁
租户内部人员能够直接使用帐号密码登录到数据库, 从而进行越权或者违规的数据操作。
- 更广泛的攻击
有价值的数据放在云上之后, 各种来源的攻击者, 都“惦记”着这些数据。可能通过各种方法来进行攻击以获取数据, 如近年来频发的 SQL 注入攻击事件, 就导致了大量云端数据的泄漏。
要解决如上所述的数据安全问题, 需要多方面的防御手段。但是对数据库访问情况的记录和审计, 是最基本的安全需求。租户需要清楚的知道, 自己的数据库, 在什么时间, 被什么人, 以什么工具, 具体做什么访问, 又拿到了什么数据。并且需要知道什么时候出现了攻击行为和异常的访问情况。所以, 需要云上数据库审计产品。

1.3 产品优势

1. 支持多种数据库类型

数据库审计系统支持对 Oracle、MS-SQL、DB2、MYSQL、Caché DB、Sybase、PostgreSQL, 并支持达梦、人大金仓国产等主流数据库提供自动化评估、审计和保护功能; 同时支持对多个系统的审计; 同时支持多个不同类型的数据库审计。

2. 审计全面细致

- 全面性: 针对业务层、应用层、数据库等层面的操作进行跟踪定位, 包括数据库 SQL 执行情况、数据库返回值等。
- 细粒度: 精确到表、对象、记录内容的细粒度审计策略, 实现对敏感信息的精细监控。

3. 事件准确定位

审计产品的技术意义在于：一旦发生安全事件时，可取得确凿的“证据”定位到人，数据库审计系统能够提供详细的记录内容以供溯源定位，包括：谁做了操作、在什么时候做的操作、做过哪些操作、做过多少次操作、是什么操作类型、以什么身份进行的操作、操作是否成功等。

4. 事件关联性分析

数据库审计系统可对响应事件进行关联，如根据 IP 关联出某段时间内该 IP 所触发的告警数量等；根据一段时间内的数据库或应用系统登录失败次数判断出暴力破解密码的可能性；根据账号的多次登录判断账号信息泄密或共享账号的可能性；相似 SQL 语句执行时间过长从而判断该语句设计的合理性等。根据事件关联性分析，自动涌现一批对客户具有实用价值的信息，帮助客户管理和维护好现有应用。

5. 事件场景还原

数据库审计系统可根据审计日志，通过事件、端口等因素构建出事件的关联性及其现场，通过模拟回放，模拟出整个事件的行动轨迹，通过大屏幕显示可方便分析人员及技术人员通过回放线索，直观的追溯事件的前后关联性及其风险蕴含较深的操作行为。

6. 丰富的策略库

数据库审计系统根据不同的行业应用提供了不同的策略库，如根据 drop、delete、alter 等危险操作行为制订了数据库危险操作策略，如根据不同工具的数据库备份信息制定了数据库备份策略库等。

数据库审计系统提供了细腻度更高的规则设置界面，用户可根据规则设置定义出自己想要的策略满足不同的安全审计需求。

1.4 产品功能

1. 基础配置

用于定义待审计对象的基本信息，包括系统基本配置、数据维护、系统日志、通知服务等，是整个数据库审计配置的前提条件。

2. 策略管理

针对常见的数据库实例，提供不同类别的审计模板，用户也可以根据自身需求，自定义策略规则。将审计策略与风险告警进行关联，可以实现多维度、分级别的审计告警。

3. 风险管理

提供细粒度的审计检索能力，可以按照时间、资产、行为、风险等多种维度查看审计结果。按照常见的审计场景，提供服务器分析、源分析、合规分析等报表导出功能。

1.5 应用场景

1. 满足等保合规要求

数据库审计系统为核心数据库系统提供了独立的审计解决方案，有助于完善组织的 IT 内控体系，从而满足合规性要求，并且使组织能够顺利通过 IT 审计。

2. 减少核心信息资产的破坏和泄露

通过使用数据库安全审计系统，加强对数据库的审计，有效地减少对核心信息资产的破坏和数据泄露。

3. 追踪溯源

负责运维的部门通常拥有数据库管理系统的最高权限(掌握 DBA 账号的口令)，因而也承担着很高的风险(误操作或者是个别人员的恶意破坏)。审计系统能够帮助客户进行事后追查原因与界定责任。

4. 满足内控审计要求

从内控的角度来看，系统的使用权、管理权与监督权必须三权分立。审计系统实现独立审计，帮助监督人员获得有效的技术手段，从而完善客户的 IT 内控机制。

1.6 使用限制

- 请确保数据库审计 DAS 实例与被扫描资产在同一个 region。
- 数据库审计 DAS 只能对中国电子云上的数据库实例进行审计操作。
- 单个数据库审计 DAS 实例支持的最大数据库实例为 32 个。

2 登录 DAS 控制台

前提条件

已获取系统的登录地址。

已有对应账户登录时的用户名和密码。

操作步骤

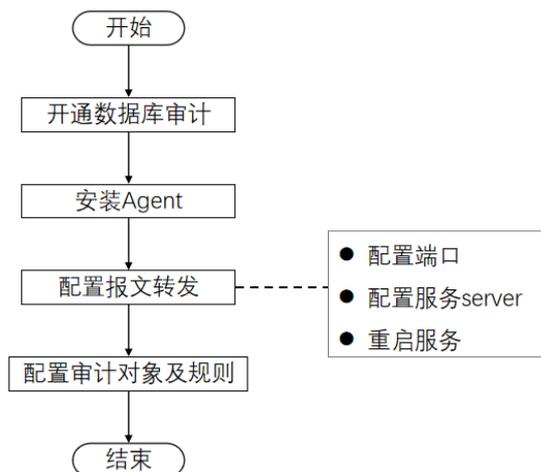
- (1) 打开浏览器，在 Web 地址栏输入系统登录地址，进入登录页面。
- (2) 输入对应账户的用户名/密码、验证码，单击“登录”，进入系统主页。
- (3) 单击顶部导航菜单栏的“云服务”，选择“安全 > 数据库审计 DAS”，进入“数据库审计 DAS”功能界面。

后续操作

您可以根据快速入门了解产品的基本配置流程，根据开通数据库审计创建实例，并根据实例管理使用产品。

3 快速入门

3.1 操作流程



3.2 开通数据库审计

注意事项

- 请确保数据库审计 DAS 实例与被扫描资产在同一个 region。
- 数据库审计 DAS 只能对中国电子云上的数据库实例进行审计操作。

操作步骤

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 单击“开通数据库审计”。
- (3) 根据下表参数说明配置参数信息。

参数	说明
租户 / 部门 / 资源集	选择此实例所属的租户、部门和资源组。 此处即要求运营管理员已创建好租户、部门和资源集；如果未创建资源集或需创建新的资源集，您可以在此处单击“去创建”创建。
区域	根据就近原则选择 DAS 服务所在的区域。 区域指的是 DAS 的物理数据中心所在的位置。 购买前请确认安全产品与被保护的服务资产处于同一个区域，否则无法做到有效防护。
可用区	选择数据库审计的可用区。 可用区是同一地域内电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。

参数	说明
计费模式	<p>根据需要选择包年包月计费模式或按需计费模式。</p> <ul style="list-style-type: none"> 包年包月是预付费模式，数据库审计 DAS 从创建成功开始计费到退订或费用到期后结束计费，按实际使用时长计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。 按需是一种先使用后付费的付费模式，按实际使用时间收费。
设备名称	可根据需要自定义数据库审计实例名称或使用系统缺省名称。
授权数	可按需配置数据库审计可审计数据库实例的数量，范围为3-32。
购买时长	当选择包周期计费模式时，需要配置此项；可按需配置购买时长，可选时长为1-9个月、1-3年。
开通时长	计费模式选择“包年包月”时，需选择使用SOC的使用时长，请在开通页面的左下角“开通时长”选框中选择使用时长，可选时长为1-9个月、1-3年。

提示

计费模式选择“包年包月”时，在设置完购买参数后，鼠标悬停在“查看费用明细”上，可查看详细收费项、目录价、折扣和折后价格。

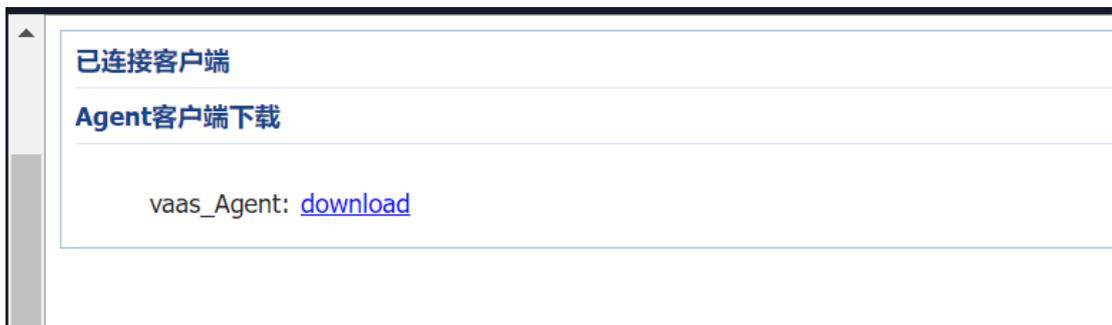
计费模式选择“按需”时，在设置完购买参数后，开通页面下方展示具体费用说明。

- (4) 确认要购买的 DAS 的配置信息无误后，单击“下一步”，进入确认配置页面。
- (5) 确认配置信息以及参考价格无误后，单击“确定新建”。
系统自动返回至“实例管理”页面，新建的实例显示为“创建中”，等待片刻后，实例状态显示为“运行中”表示创建成功。

3.3 安装Agent

3.3.1 下载 Agent

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 单击目标实例操作列的“访问”，进入产品配置界面。
- (3) 单击“系统管理 > Agent 配置”，单击“Agent 客户端下载 > download”，下载 Agent 安装包。

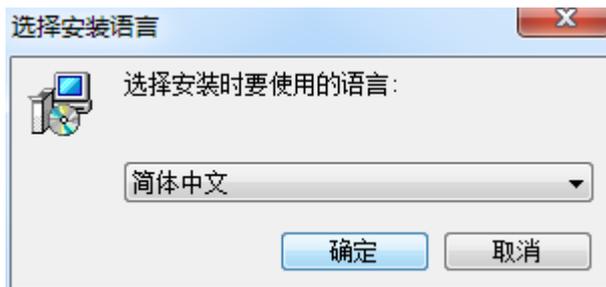


3.3.2 Windows-agent 安装

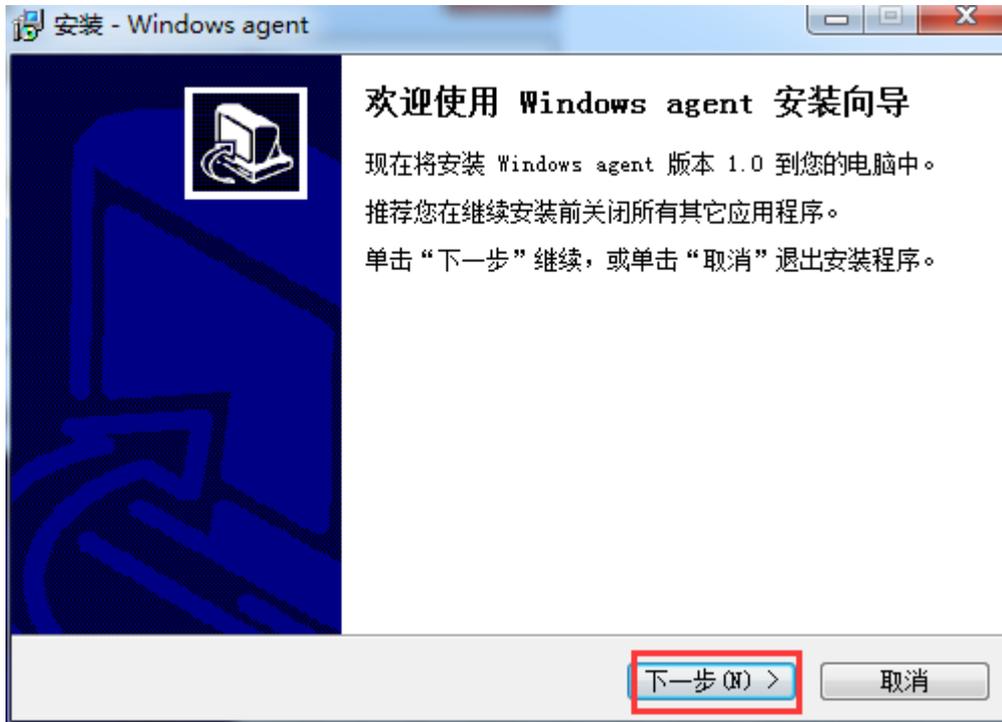
- (1) 将下载的 Windows 安装包上传到数据库所在的服务器上任意目录。
- (2) 双击安装包。



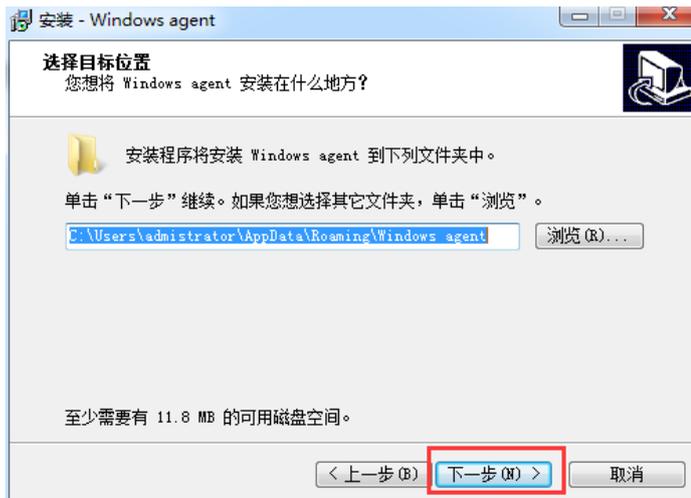
- (3) 选择安装语言，单击“确定”。

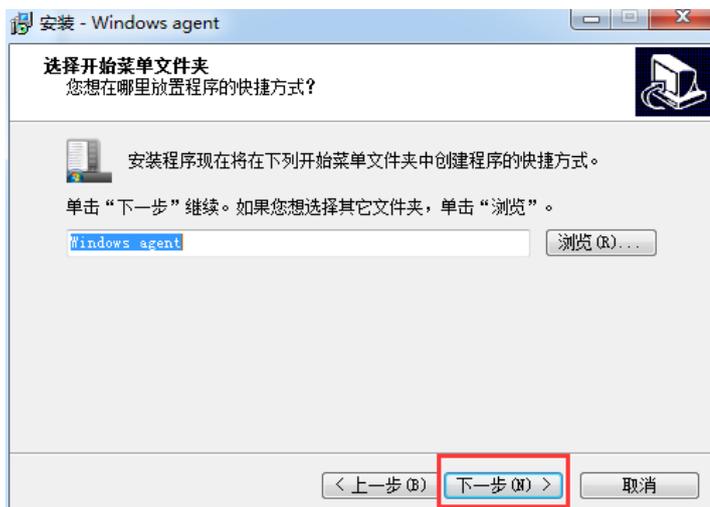


- (4) 单击“下一步”。

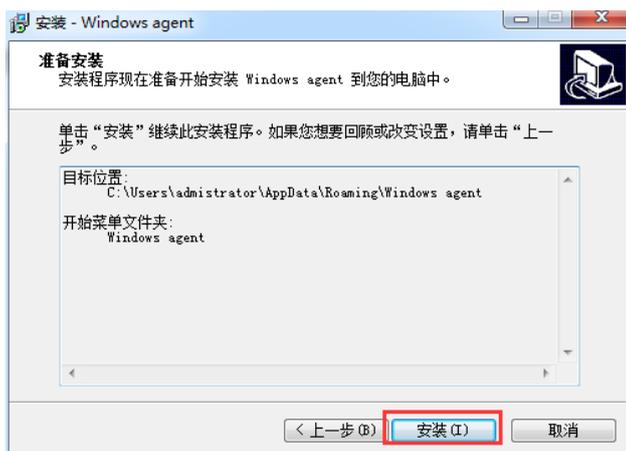


- (5) 选择安装位置，单击“下一步”。





(6) 单击“安装”。

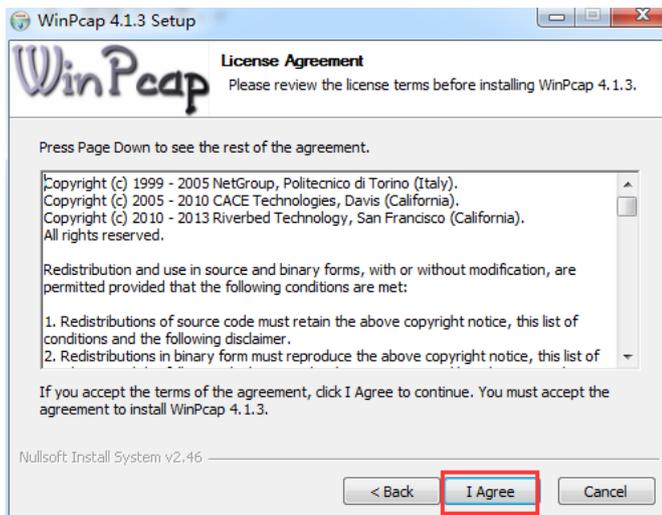
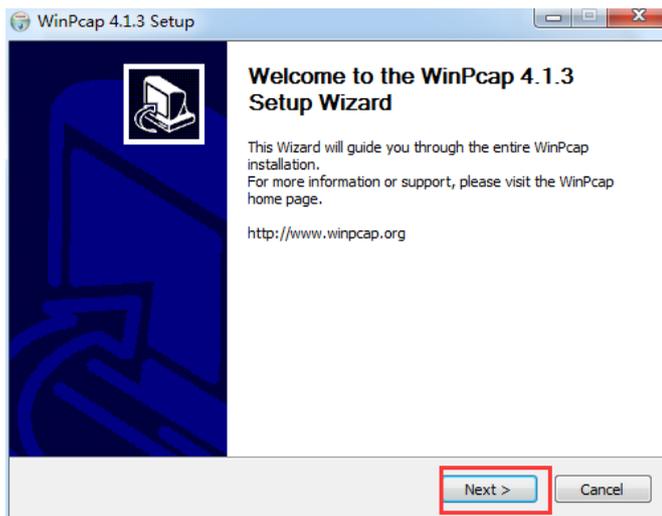


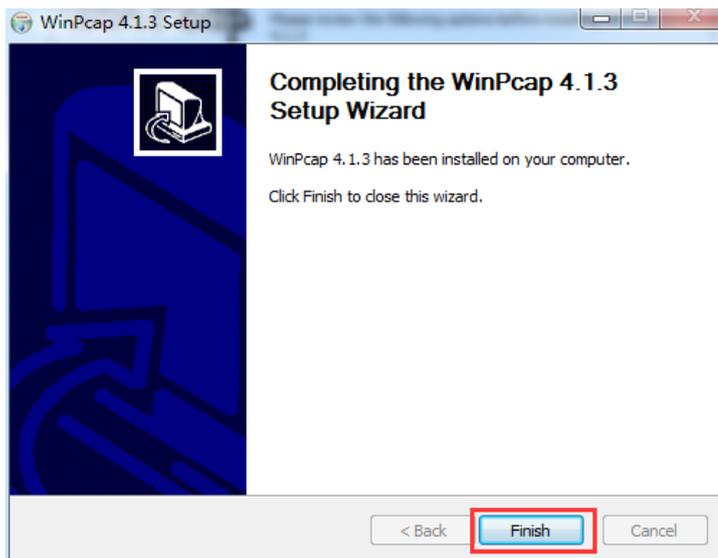
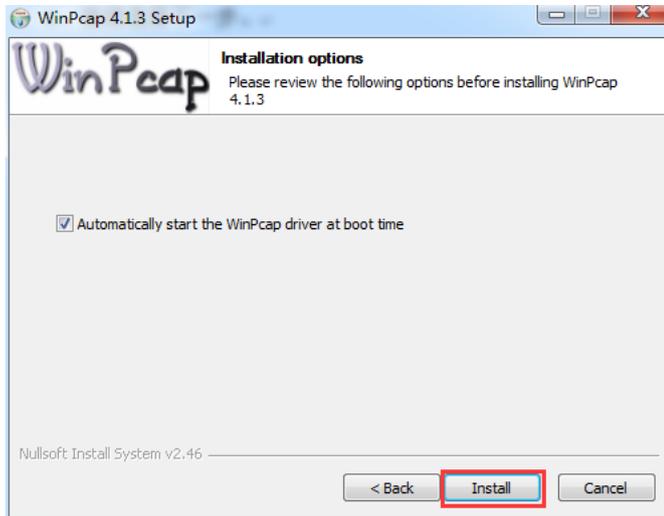
(7) 安装 WinPcap。

如果已经安装有 Winpcap 则会弹出如下提示是否重新安装，没有则点击下一步安装。（出现如下提示，选择确定接下一步操作，选择取消则表示不重新安装 winpcap 将会完成 Agent 安装）。



(8) 单击“Next > I Agree > Install > Finish”，完成 Winpcap 安装。

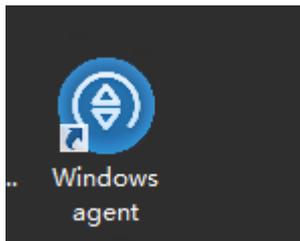




(9) 单击“完成”，完成 Agent 安装。



安装完成之后，在桌面会生成快捷方式。



3.3.3 Linux-agent 安装

- (1) 解压 Agent 包。
 - a. 将下载的 Linux 安装包上传到数据库所在的 linux 系统的根目录。
 - 32 位系统选择 linux_agent-32.tar.gz。
 - 64 位系统选择 linux_agent-64.tar.gz。
 - Arm 架构选择 linux_agent-arm.tar.gz。
 - b. 执行解压命令：tar -zxvf linux_agent64.tar.gz。

```
[root@localhost csm]# tar -zxvf linux_agent64.tar.gz
linux_agent/
linux_agent/watchAgent.sh
linux_agent/version.info
linux_agent/linux_agent.sh
linux_agent/queue.conf
linux_agent/stopAgent.sh
linux_agent/startAgent.sh
linux_agent/agent.conf
linux_agent/disable_agent_service.sh
linux_agent/audit_agent
linux_agent/enable_agent_service.sh
```

c. 解压后，显示如下。

```
[root@localhost csm]# ll
总用量 728
drwxr-xr-x 2 root root  4096 12月 12 19:38 linux_agent
-rw-r--r-- 1 root root 741079 12月 12 19:38 linux_agent64.tar.gz
[root@localhost csm]# cd linux_agent/
[root@localhost linux_agent]# ll
总用量 1868
-rw-r--r-- 1 root root    89 12月 12 16:26 agent.conf
-rwxr-xr-x 1 root root 1873648 11月 20 15:22 audit_agent
-rw-r--r-- 1 root root   179 12月  2 15:46 disable_agent_service.sh
-rw-r--r-- 1 root root   780 12月  2 14:43 enable_agent_service.sh
-rwxr-xr-x 1 root root  1190 12月 12 19:38 linux_agent.sh
-rw-r--r-- 1 root root   332 11月 20 15:22 queue.conf
-rwxr-xr-x 1 root root   319 11月 20 15:22 startAgent.sh
-rwxr-xr-x 1 root root   455 11月 20 15:22 stopAgent.sh
-rw-r--r-- 1 root root   145 12月 12 16:59 version.info
-rwxr-xr-x 1 root root   598 12月 12 16:54 watchAgent.sh
```

(2) 设置开机启动。

为了能让 Agent 实现开机自启，需要执行以下命令：sh enable_agent_service.sh。

```
[root@localhost linux_agent]# sh enable_agent_service.sh
/root/lpyuan/linux_agent
/root/bxd/csm/linux_agent
/root/bxd/csm/linux_agent
start complete.
```

3.4 配置报文转发

3.4.1 Linux 配置报文转发

(1) 执行 vi agent.conf 配置 agent.conf 文件，按下图说明配置。

```
[root@localhost linux_agent]# cat agent.conf
receive_device=en0 数据库设备的网卡名称
send_device=en0
packet_filter=tcp port 3306 需要抓取的端口
dst_ip=172.24.1.21 审计设备IP
```

(2) 按需填好配置文件后，就可以启动 Agent。

若 agent 已启动则选择重启命令执行重启操作。

○ 启动命令：service linux_agent start 或者 sh startAgent.sh。

```
[root@localhost linux_agent]# service linux_agent start
start Agent...start audit_agent.
start audit_agent daemon.
start complete.
```

```
[root@localhost linux_agent]# sh startAgent.sh
start audit_agent.
start audit_agent daemon.
start complete.
```

- 重启命令: service linux_agent restart。

```
[root@localhost linux_agent]# service linux_agent restart
stop Agent...stop audit_agent.
stop audit_agent daemon.
stop complete.
start Agent...start audit_agent.
start audit_agent daemon.
start complete.
```

- 停止命令: service linux_agent stop 或者 sh stopAgent.sh。

```
[root@localhost linux_agent]# service linux_agent stop
stop Agent...stop audit_agent.
stop audit_agent daemon.
stop complete.
```

```
[root@localhost linux_agent]# sh stopAgent.sh
stop audit_agent.
stop audit_agent daemon.
stop complete.
```

- (3) 查看运行情况。

在任意路径下执行 `ps -ef|grep audit_agent` 查看 Agent 程序是否正在运行, 显示如下, 说明已经在运行。

```
[root@localhost linux_agent]# ps -ef|grep audit_agent
root    14905      1  0 11:44 pts/1    00:00:00 ./audit_agent
root    15303  4938  0 11:44 pts/1    00:00:00 grep --color=auto audit_agent
```

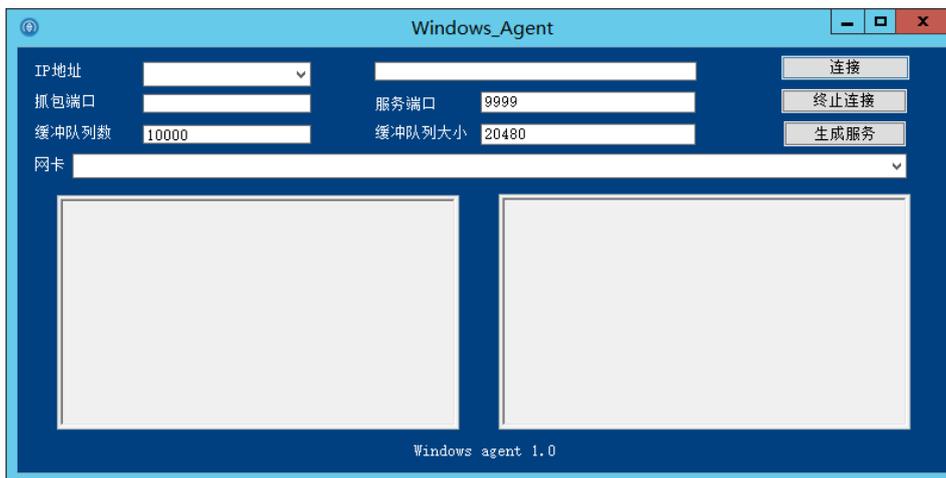
执行命令: `tail -f linux_agent.log` 查看 Agent 连接数据库审计设备是否正常, 正常连接显示。

```
[root@localhost linux_agent]# tail -f linux_agent.log
CACHE_NUM_MAX = [20000],CACHE_SIZE = [20480]
[2019-12-13 11:47:07]server resource is prepared already, connection OK, try to send answer 65535
[2019-12-13 11:47:07]success to send ack info
[2019-12-13 11:47:07]Connect AAS[172.24.1.21] OK!
[2019-12-13 11:47:07]Receive packet thread start work ...
```

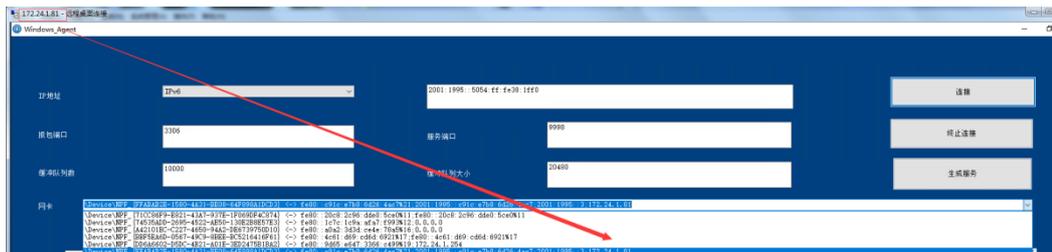
3.4.2 Windows 配置报文转发

1. 操作步骤

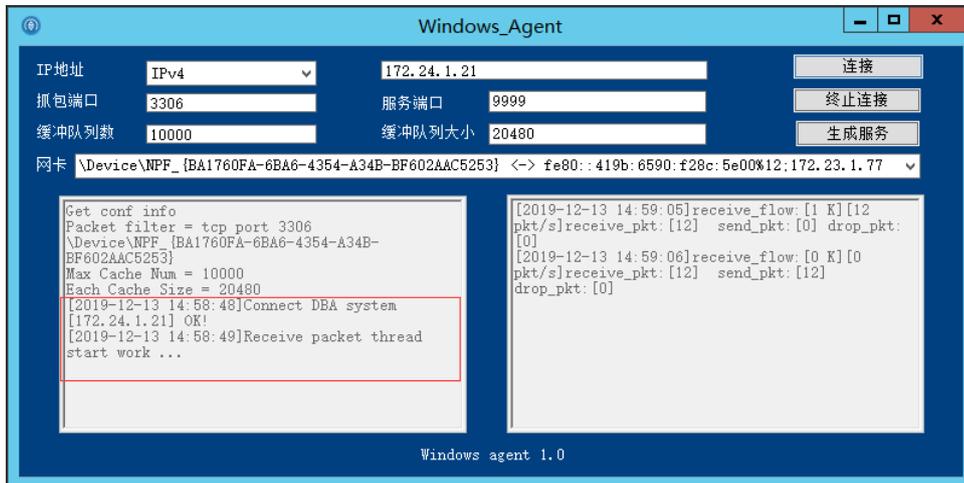
- (1) 双击快捷方式，启动 Windows Agent。
- (2) 按照如下参数说明，进行配置。



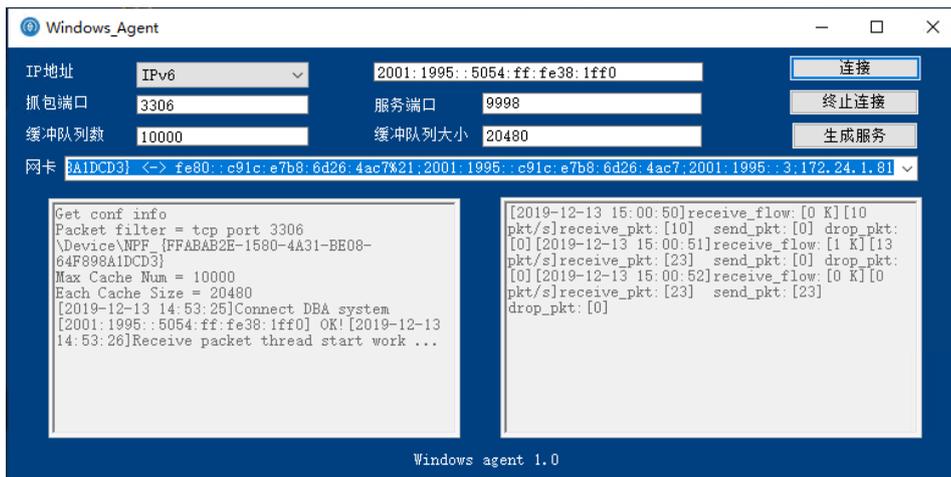
- IP 地址：可以选择 IP 格式为 IPV4 或者 IPV6，后续输入相应的 IP。
- 抓包端口：需要抓取的端口，多个端口之间用,号隔开，如 3306,1521。
- 服务端口：IPV4 连接则使用 9999，IPV6 连接则使用 9998。
- 缓冲队列数和缓冲队列大小可以直接使用默认值。
- 网卡：选择该设备 IP 的网卡,例如下图。



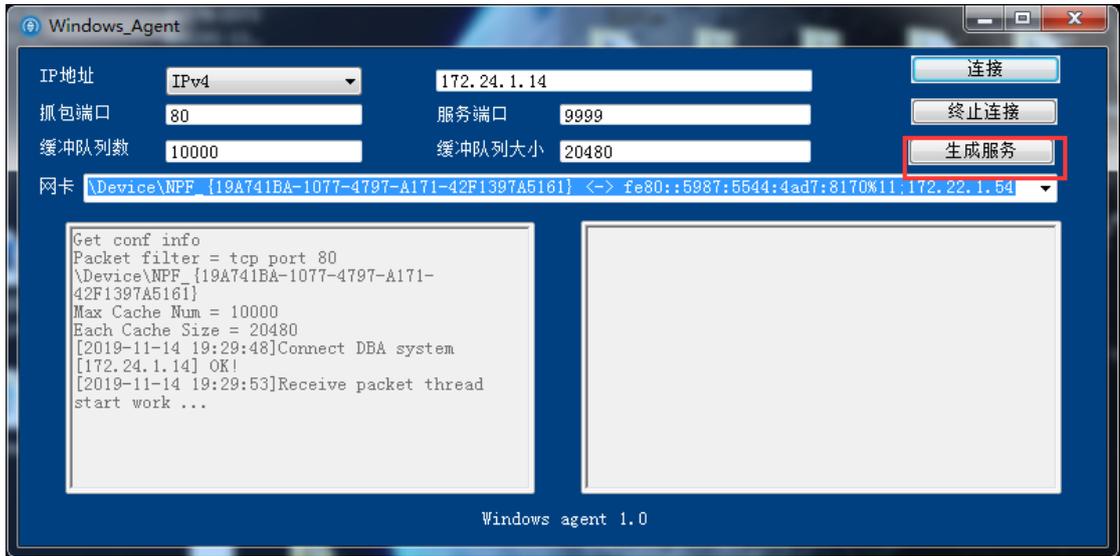
- (3) 配置完成后单击“连接”。
- IPV4 连接



o IPV6 连接

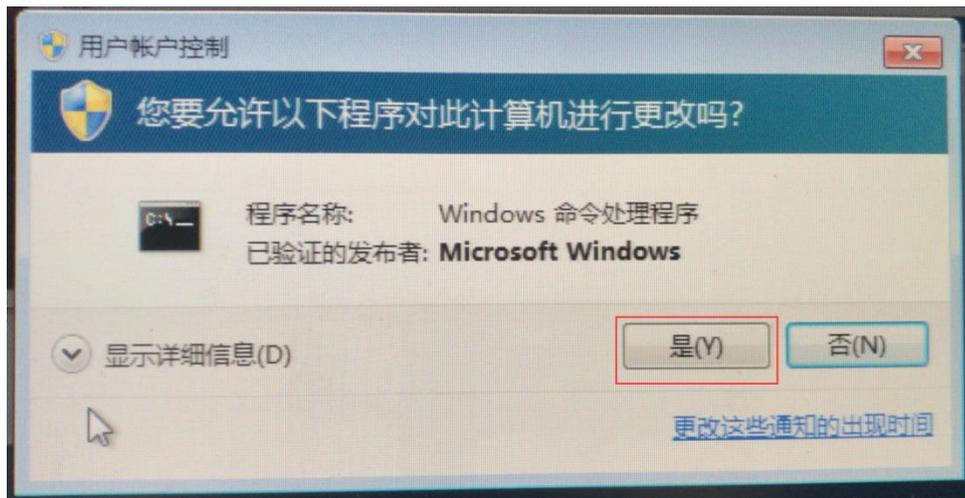


(4) 单击“生成服务”，自动配置数据库操作报文的转发服务。



a. 允许获取权限。

获取管理员权限运行的提示（可能有其他提示，比如 360 提示等需同意。）

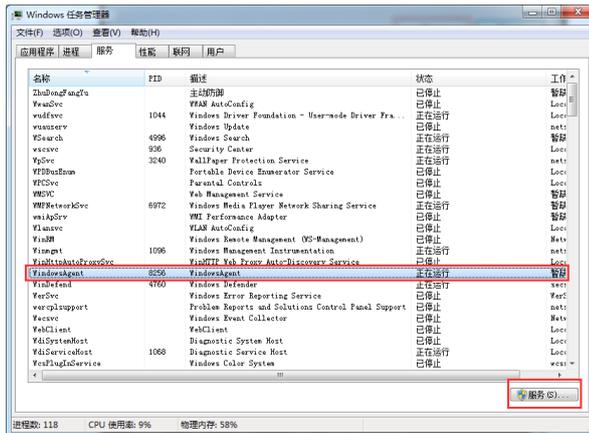


b. 服务成功启动。

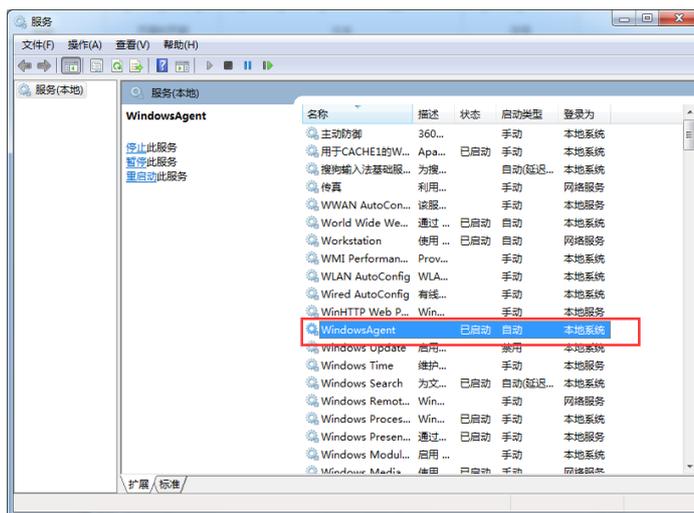


2. 相关注意事项

- (1) 如需要重新配置，则需要在任务管理器先停止服务。
 - 找到对应服务 WindowsAgent 右键停止服务。



- 若出现提示错误无法停止说明权限不够，需要点击右下角的管理员权限标志找到 WindowsAgent 服务进行停止。



(2) 停止服务之后，则可以双击桌面快捷方式重新配置，再选择需要的方式运行。

3.5 配置审计对象及规则

3.5.1 配置审计对象

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 单击目标实例操作列的“访问”，进入产品配置界面。
- (3) 单击“对象设置 > 审计对象”，进入“审计对象”配置界面。
- (4) 单击“添加”维护数据库实例信息。



(5) 根据下表中的参数说明配置参数信息，完成后单击“保存”。

名称	说明
审计对象名称	设置业务对象的名称，可以自定义，建议设置的名称最好体现该对象的特点。
状态	禁用还是启用。
数据库类型	选择数据库类型，如Oracle、Cache、SQL Server、Sybase等等。
版本号	选定数据库服务器类型后，这里选择数据库的版本号。
服务地址	数据库服务器所在的IP地址。
端口	数据库服务器设置的数据库的端口号，默认： <ul style="list-style-type: none"> • SQL Server: 1433 • HTTP: 80 • Oracle: 1521 • MySQL: 3306
应用规则组	规则组设置，根据实际情况选择
数据库编码	根据数据库服务器数据库设置的编码字符集选择。 <ul style="list-style-type: none"> • Oracle: GB2312 • SQLServer: 936 • 其他: UTF-8
应用部门	默认选择根部门。
关联对象	可将该审计对象与其他的审计对象进行关联。
扩展配置	添加数据库账号、密码、数据库服务IP、数据库名（进行反查）。
HIS厂商	每个医院都会有一个HIS系统，用于管理医院信息，不涉及可不填。

3.5.2 配置审计规则

用户根据实际情况，数据库审计的规则和告警机制，具体操作请参见运营中心的《数据库审计 DAS 用户指南》中的规则配置章节。

4 实例管理

4.1 扩容数据库审计

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 单击目标数据库审计操作列的“扩容”，进入数据库审计扩容页面。
- (3) 设置扩容后的授权数，单击“下一步”，进入确认配置页面。
- (4) 确认变更后的授权数和变更后的费用无误后，单击“确定扩容”。

扩容成功后，系统自动返回至“实例管理”页面，实例显示为“运行中”。

4.2 续费数据库审计

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 单击目标数据库审计操作列的“续费”，进入产品续订页。
- (3) 确认产品实例信息，选择续费时长后，单击“确定续费”即可。

4.3 启动数据库审计

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 勾选目标数据库审计实例名称左侧的复选框。
- (3) 单击“启动”，启动该数据库审计实例。

4.4 关闭数据库审计

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 关闭操作有两种方式：
 - 单击目标数据库审计实例操作列的“更多 > 关闭”，关闭该数据库审计实例。
 - 勾选目标数据库审计实例名称前的复选框，单击“关闭”，关闭数据库审计实例。

4.5 退订数据库审计

- (1) 在数据库审计 DAS 控制台页面，单击左侧导航栏的“实例列表”，进入“实例列表”页面。
- (2) 单击目标数据库审计操作列的“更多 > 退订”，进入产品退订页。
- (3) 确认要退订的实例、退款金额等信息，单击“确定退订”，即可完成退订。

4.6 DAS实例到期/欠费

4.6.1 包周期计费模式下实例到期后状态变化

对于到期后没有及时续费的数据库审计实例，将开启回收机制，按时间期限划分为三个阶段，如下图所示。



- 宽限期：实例到期的 1~7 天内。此阶段的数据库审计可正常使用。
- 保留期：实例到期的 8~22 天内。此阶段的数据库审计停止提供服务。在保留期内结清欠款，数据库审计将恢复正常服务。
- 释放期：实例到期的第 23 天及以后。此阶段的数据库审计实例会被回收。在释放期内只能重新购买数据库审计实例提供服务，造成损失由客户自行负责。

4.6.2 按需计费模式下账户欠费时实例变化

按需计费下，当您的账户欠费时，系统将会关闭实例，不允许开机，实例管理页面仅能执行释放实例操作。只有结清欠款后才允许开机及其他实例操作。



5 常见问题

1. 配置完 agent 后报错如何处理？

常见报错一：

```
[root@localhost linux_agent]# tail -f linux_agent.log
[2019-12-13 14:20:44]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:20:49]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:20:54]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:20:59]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:21:04]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:21:09]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:21:14]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:21:19]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:21:24]Connect AAS[172.24.1.14] error[110].
[2019-12-13 14:21:29]Connect AAS[172.24.1.14] error[110].
```

处理方式：

- 检查是否有证书、后台启动是否成功。在审计设备上运行 `netstat -anp|grep 9999` 命令，检查监听服务是否启动。

```
[root@localhost ~]# netstat -anp|grep 9999
tcp        0      0 0.0.0.0:9999          0.0.0.0:*            LISTEN     9074/audit_server
```

如有上图监听，则代表后台启动成功，如果没有监听那就很有可能是后台没有起来，去 `/home/audit/` 目录下执行 `sh audit.sh`，启动后台。再次查看监听，监听还未启动则需请开发排查。

- 相关防火墙没有开放 9999 或者 9998 端口。

常见报错二：

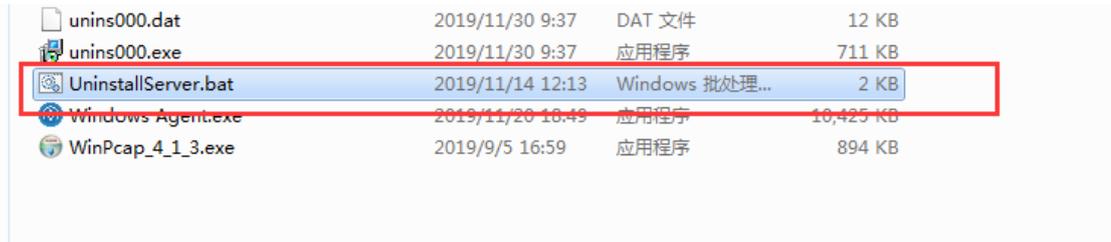
```
[root@localhost linux_agent]# tail -f linux_agent.log
[2019-12-13 14:24:42]Connect AAS[172.24.1.21] OK!
[2019-12-13 14:24:42]Get receive device[eth0] error!
[2019-12-13 14:24:42] thread quit ret[0]
[2019-12-13 14:24:52]backup thread quit for other thread quit.
[2019-12-13 14:24:52]Thread quit!
[2019-12-13 14:24:52]server resource is prepared already, connection OK, try to send answer 65535
[2019-12-13 14:24:52]success to send ack info
[2019-12-13 14:24:52]Connect AAS[172.24.1.21] OK!
[2019-12-13 14:24:52]Get receive device[eth0] error!
[2019-12-13 14:24:52] thread quit ret[0]
```

处理方式：`agent.conf` 配置文件里的网卡不对，需要换成当前设备网卡。

2. Windows-agent 如何删除卸载掉服务

（当前电脑不需要 agent 需要把服务卸载掉的情况），找到程序安装的位置（右键桌面快捷方式，打开文件所在位置），双击目录下的 UninstallServer.bat 脚本。

（可能有其他提示，比如 360 等防护软件警告信息提示，需同意）



文件名	日期	时间	文件类型	大小
unins000.dat	2019/11/30	9:37	DAT 文件	12 KB
unins000.exe	2019/11/30	9:37	应用程序	711 KB
UninstallServer.bat	2019/11/14	12:13	Windows 批处理...	2 KB
Windows Agent.exe	2019/11/20	16:49	应用程序	10,425 KB
WinPcap_4_1_3.exe	2019/9/5	16:59	应用程序	894 KB