

云盾·数据库审计 快速部署手册

二〇一九年一月

目 录

1. 产品初始化.....	3
1.1 添加被审计数据库实例	3
1.1.1 添加被保护数据库实例.....	3
1.2 部署 AGENT 程序.....	6
1.2.1 Agent 程序部署位置.....	6
1.2.2 Agent 程序自动部署（仅支持 linux 系统）	6
1.2.3 Agent 程序手动部署.....	8
1.2.4 Agent 程序部署注意事项.....	30
1.3 部署测试.....	32

1. 产品初始化

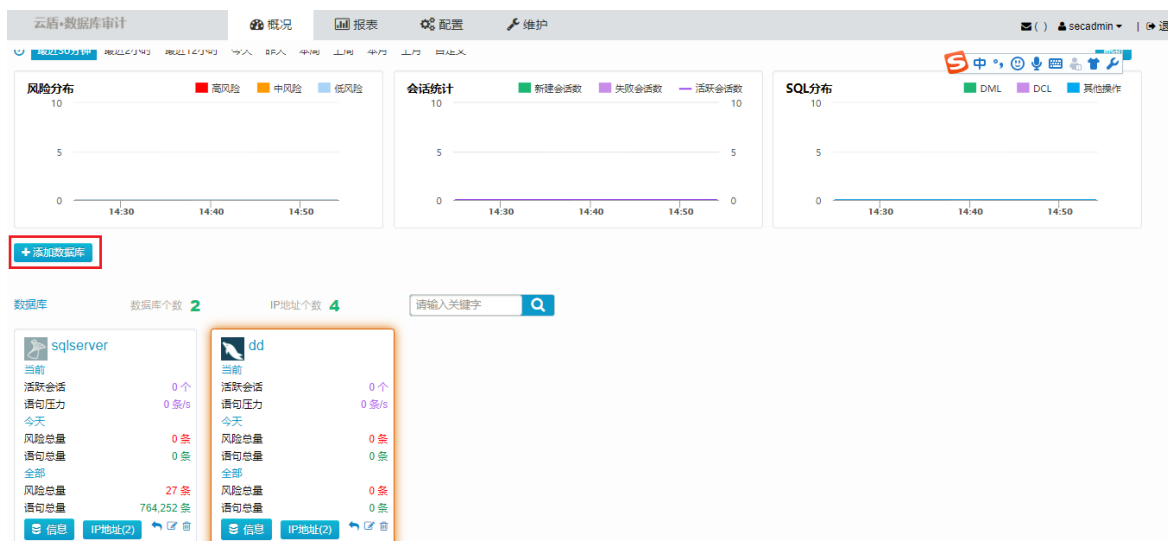
1.1 添加被审计数据库实例

1.1.1 添加被保护数据库实例

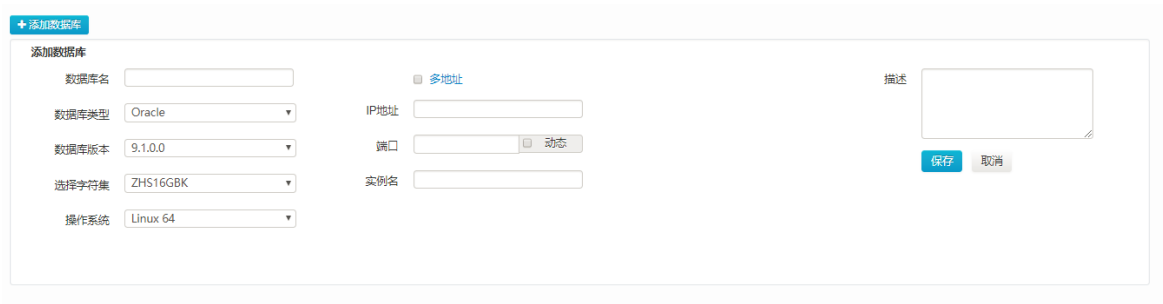
系统支持对云服务器自建数据库实例和云服务商提供的云数据库实例的审计。用户需根据自身云环境下数据库的实际部署方式进行添加。具体添加方式如下：

1.1.1.1 添加云服务器自建数据库实例

1、进入安全管理员界面后点击【概况】，点击【添加数据库】按钮，如下图：

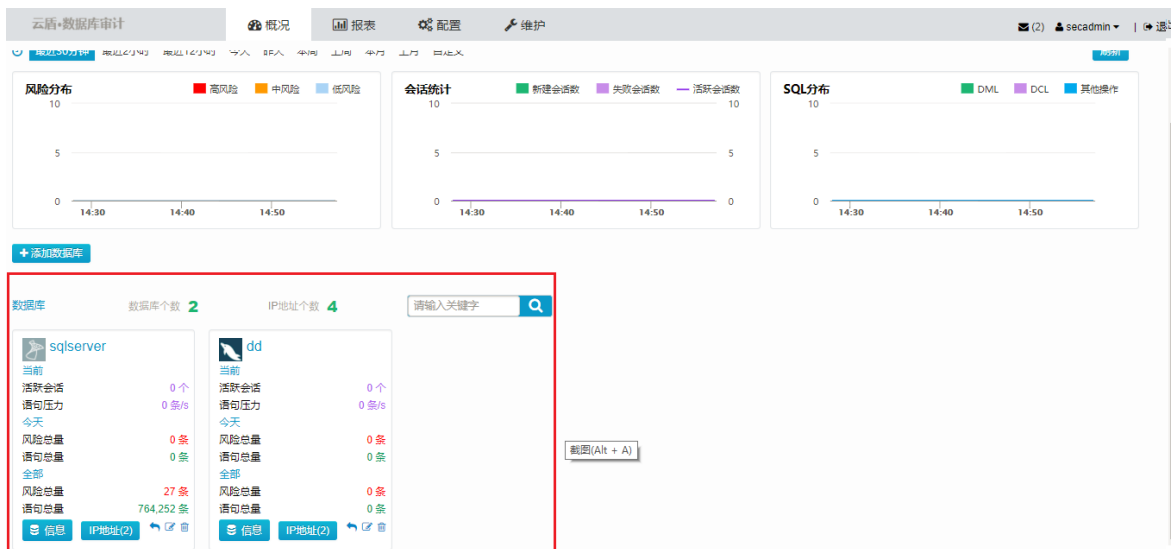


2、在弹出的【添加数据库】页面中填写要审计的数据库实例相关信息，然后点击【保存】按钮，如下图：

**注意事项：**

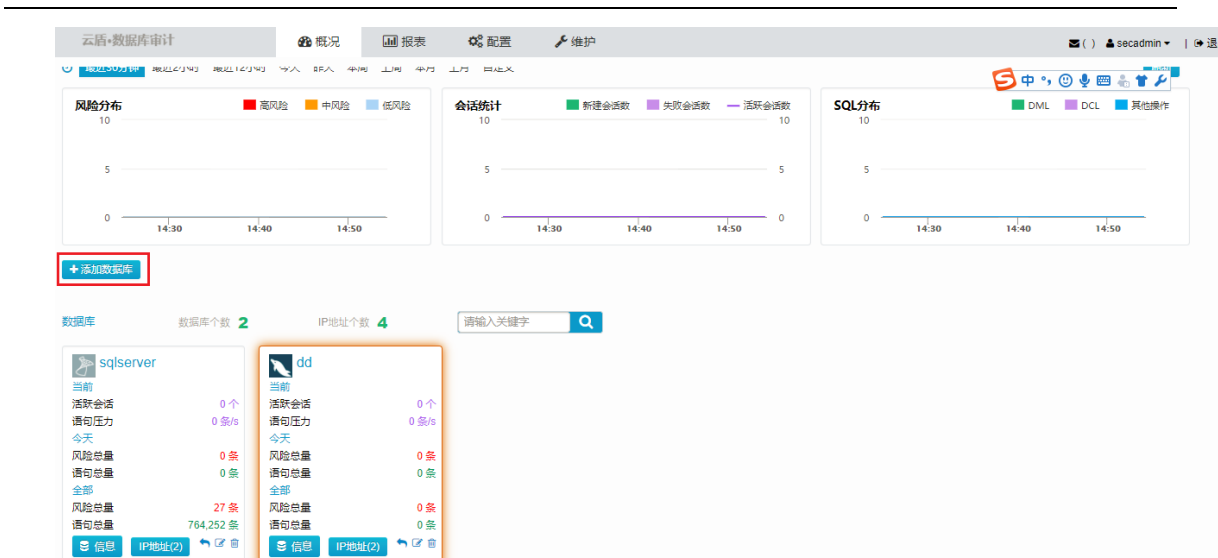
- 数据库名：为被审计数据库实例指定一个名字。
- 数据库类型：根据被审计数据库实例的类型选择。
- 数据库版本：根据实际情况选择对应数据库版本信息。
- IP 地址：被审计数据库实例的 IP 地址。
- 端口：被审计数据库实例的端口号。
- 描述：为被添加保护的数据库添加注释。

3、数据库添加成功后，可以在【概况】页下方的【数据库组】列表页处看到增加的数据库摘要信息，如下图：



1.1.1.2 添加 RDS 数据库

1、进入安全管理员界面后点击【概况】，点击【添加数据库】按钮，如下图：



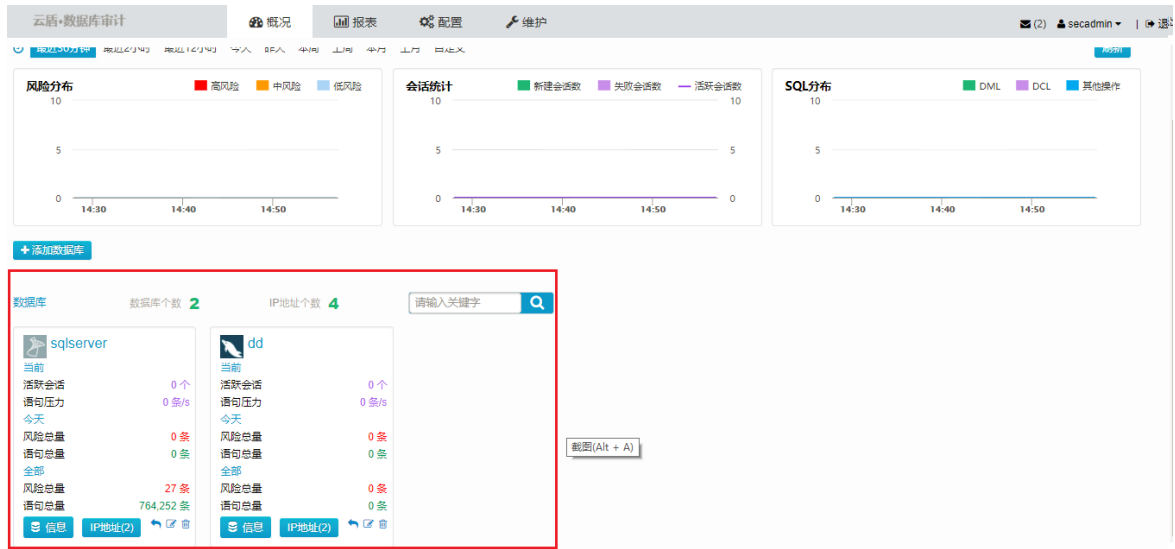
2、在弹出的【添加数据库】页面中填写要审计的数据库实例相关信息，然后点击【保存】按钮，如下图：

The screenshot shows the '添加数据库' (Add Database) form. The form has a title bar with a red box highlighting the '+ 添加数据库' button. Below the title bar, there are two columns of fields. The left column contains: '数据库名' (Database Name), '数据库类型' (Database Type) with a dropdown menu showing 'Oracle', '数据库版本' (Database Version) with a dropdown menu showing '9.1.0.0', '选择字符集' (Select Character Set) with a dropdown menu showing 'ZHS16GBK', and '操作系统' (Operating System) with a dropdown menu showing 'Linux 64'. The right column contains: 'IP地址' (IP Address), '端口' (Port) with a dropdown menu showing '动态' (Dynamic), and '实例名' (Instance Name). There is a '多地址' (Multiple Addresses) checkbox. To the right of the form is a '描述' (Description) text area. At the bottom right, there are '保存' (Save) and '取消' (Cancel) buttons.

注意事项：

- 数据库名：为被审计数据库实例指定一个名字。
- 数据库类型：根据被审计数据库实例的类型选择。
- 数据库版本、字符集、操作系统默认即可。
- IP地址：被审计数据库实例的URL连接串。
- 端口：被审计数据库实例的端口号。
- 描述：为被添加保护的数据库添加注释。

3、数据库添加成功后，可以在【概况】页下方的【数据库组】列表页处看到增加的数据库摘要信息，如下图：



1.2 部署 Agent 程序

1.2.1 Agent 程序部署位置

Agent 程序需要部署到数据库或应用服务器上来获取访问数据库的流量，审计系统对获取到的流量进行分析审计。

- 云服务器自建数据库实例 agent 部署位置：数据库所在的服务器上。
- 云服务商提供的 RDS 数据库 agent 部署位置：应用服务器上。

1.2.2 Agent 程序自动部署（仅支持 linux 系统）

1、打开浏览器，以安全管理员账户登录云盾·数据库审计，点击【维护】->【Agent 管理】->【Agent 自动部署】图标，如下图：



2、在弹出的【Agent 自动部署】页面填写需要部署 Agent 程序的服务器 IP 地址、ROOT 用户密

码和 SSH 端口号，然后点击“部署”，即可自动部署到相应的服务器中，如下图：



注意：

- Agent 部署服务器需要开通 ssh, 并且需要使用 root 密码。
- 如果应用系统与数据库部署在同一台服务器，在自动部署 Agent 程序时，需要勾选“本地回环”
- 审计服务器 IP: 添加数据库审计系统的 IP 地址(如果数据库审计系统与 agent 所在服务器在同一内网环境中, 就添加数据库审计的内网 IP, 如果不在同一内网中则添加数据库审计的外网 IP 地址, 数据审计的 IP 地址可在数据库审计的云盾入口处查询)
- 目标服务器: 为需要部署 agent 的服务器(格式如上图)

3、点击【维护】->【Agent 管理】->【Agent 部署配置】图标，如下图：



4、在弹出的【Agent 部署配置】窗口输入需要部署 Agent 程序的服务器 IP 地址，然后点击【添加】按钮，添加完成后，【点击关闭】按钮，如下图：

Agent部署配置

序号	IP地址	操作
1	172.17.71.212	
2	192.168.0.1	
3	192.168.0.111	

IP地址:

192.168.100.88
192.168.100.89

添加

关闭

注意：

- 如果需要部署 Agent 程序的服务器与云数据库审计系统在同一个内网，则添加内网地址即可，如果与云数据库审计系统不在同一个内网需要通过外网进行通信的，则添加该服务器的外网地址。
- 如果不添加部署 Agent 程序的服务器 IP 地址，审计系统将不会对抓取的该服务器数据进行审计。

1.2.3 Agent 程序手动部署

1.2.3.1 Windows 系统部署

1.2.3.1.1 应用系统与数据库部署在不同的服务器

1、打开浏览器，以安全管理员账号登录云盾·数据库审计系统，点击【维护】->【Agent 管理】->【下载 Agent】图标，如下图：



2、系统自动弹出【提示】窗口，且浏览器自动开始下载 Agent 程序（即 rmagent.tar.gz 文件）至本地。然后点击【确定】按钮，如下图：



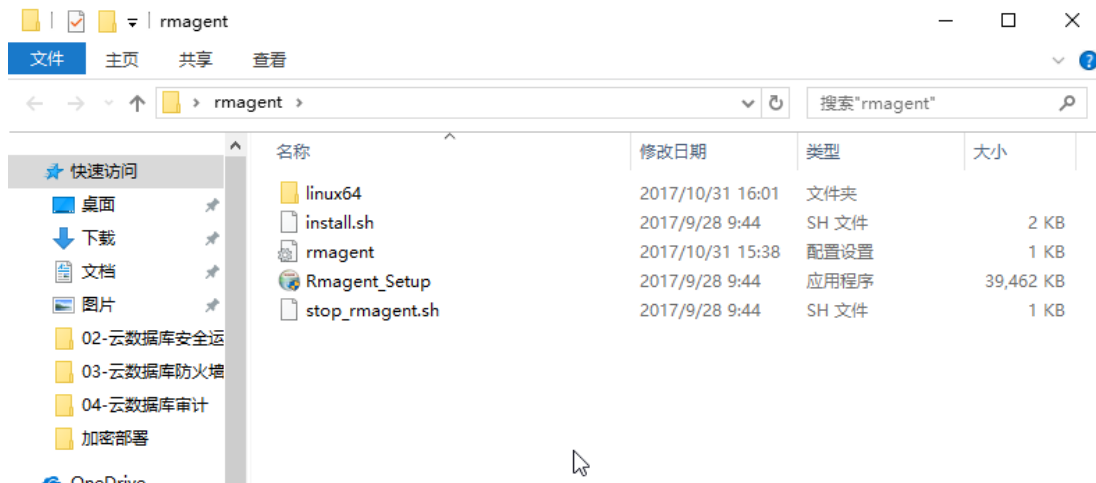
3、在弹出的【Agent 部署配置】窗口输入需要部署 Agent 程序的服务器 IP 地址，然后点击【添加】按钮，添加完成后，点击【关闭】按钮，如下图：



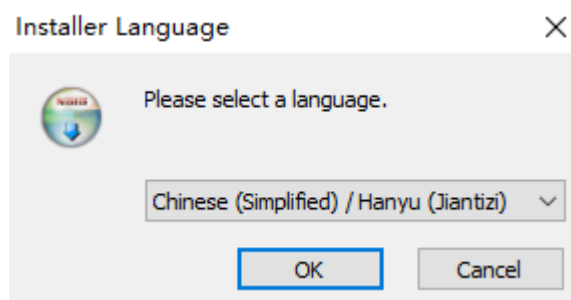
注意：

- 如果需要部署 Agent 程序的服务器与云数据库审计系统在同一个内网，则添加内网地址即可，如果与云数据库审计系统不在同一个内网需要通过外网进行通信的，则添加该服务器的外网地址。
- 如果不添加部署 Agent 程序的服务器 IP 地址，审计系统将不会对抓取的该服务器数据进行审计。

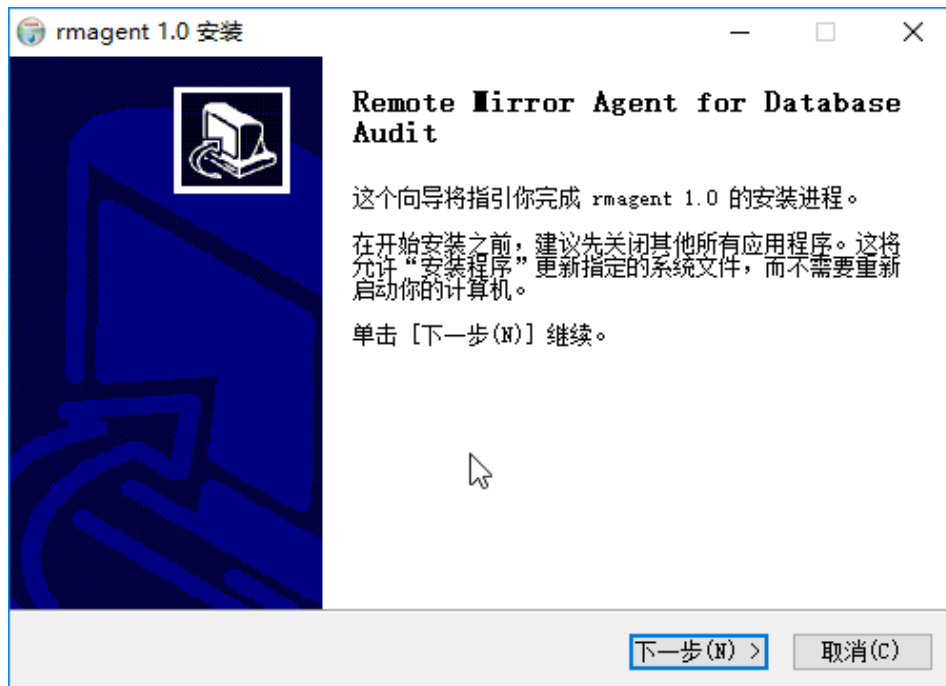
4、将 rmagent.tar.gz 文件上传到需要部署 Agent 程序的服务器，并将其解压缩，如下图：



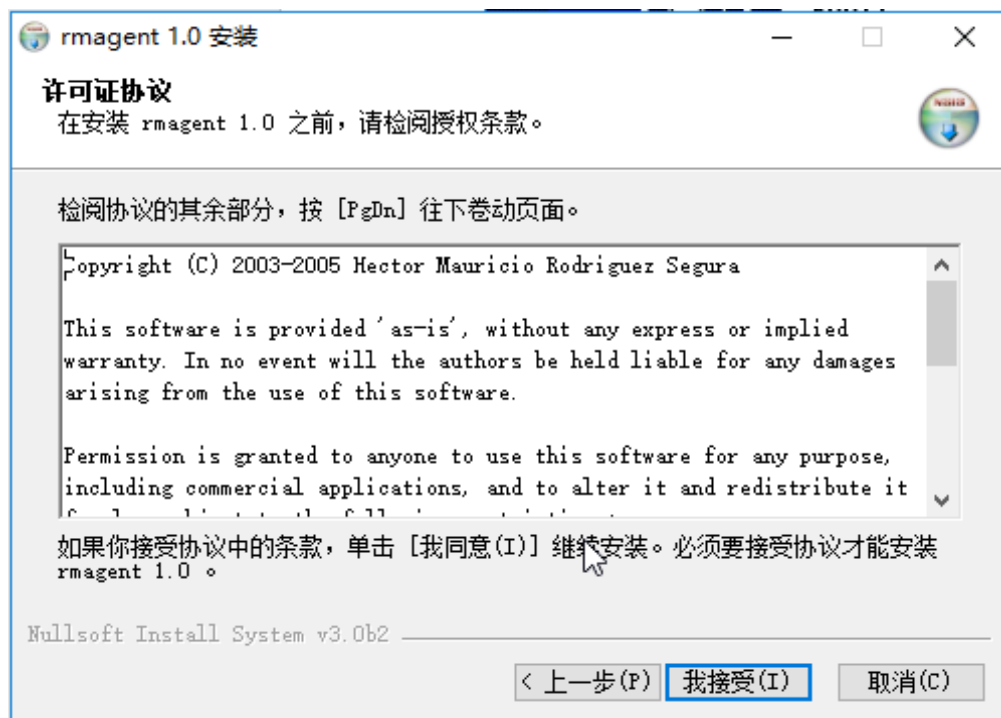
5、打开解压后的 Agent 程序文件夹，双击运行【Rmagent_Setup.exe】文件，在弹出的【Installer Language】窗口点击【OK】按钮，如下图：



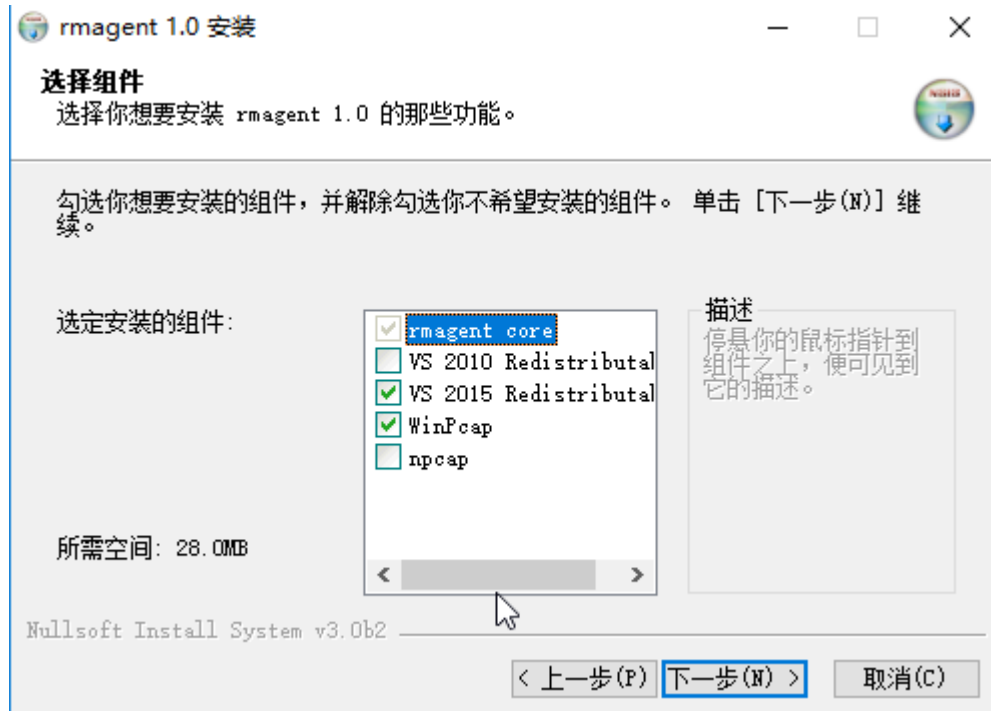
6、弹出【rmagent1.0 安装】窗口，点击【下一步】按钮，如下图：



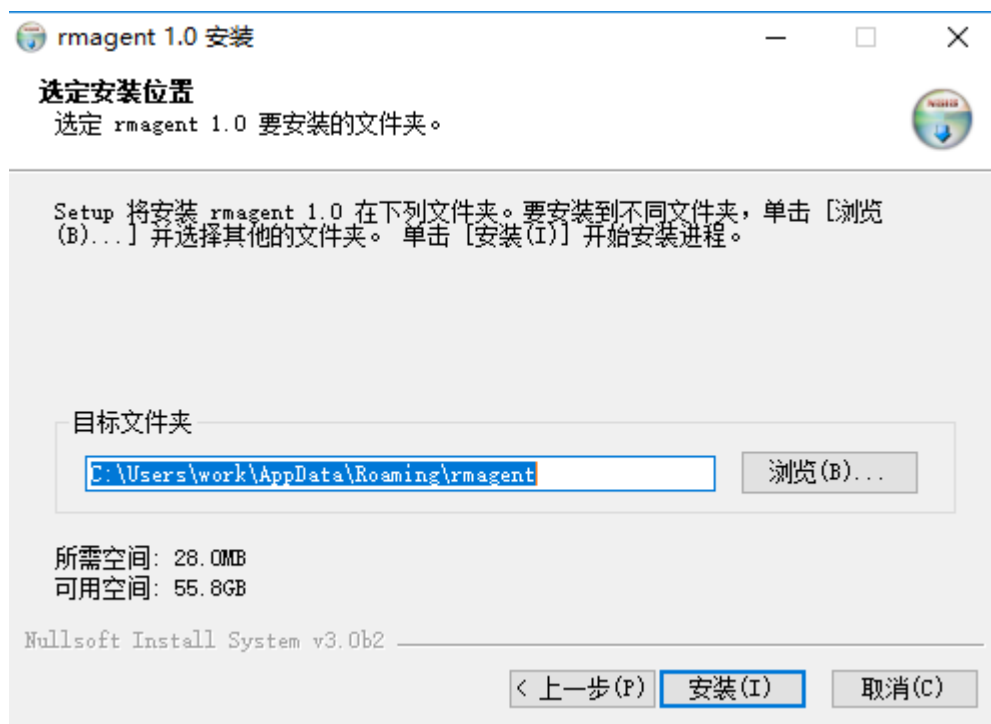
7、弹出【许可证协议】窗口，点击【我接受】按钮，如下图：



8、弹出【选择组件】窗口，点击【下一步】按钮，如下图：



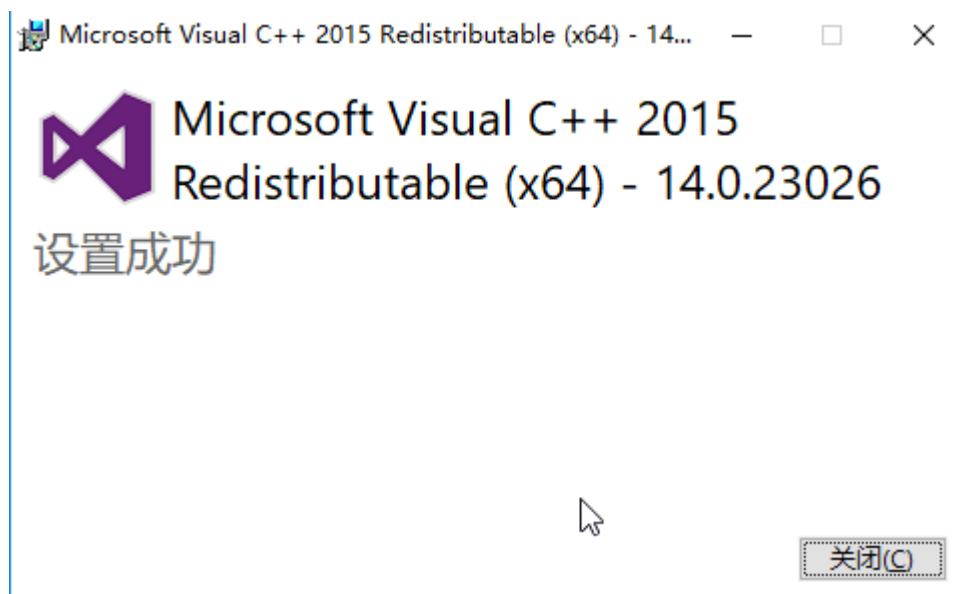
9、弹出【选定安装位置】窗口，默认即可，点击【安装】按钮，如下图：



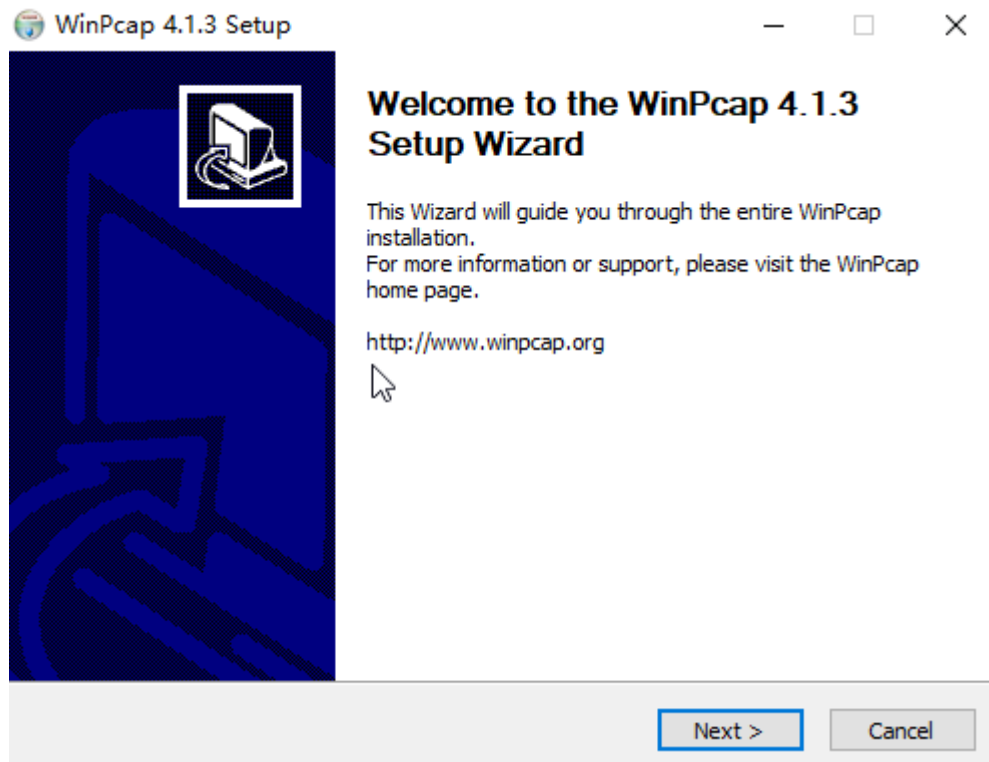
10、弹出【Microsoft Visual C++ 2015】安装窗口，勾选【我同意许可条款和条件】，然后点击【安装】按钮，如下图：



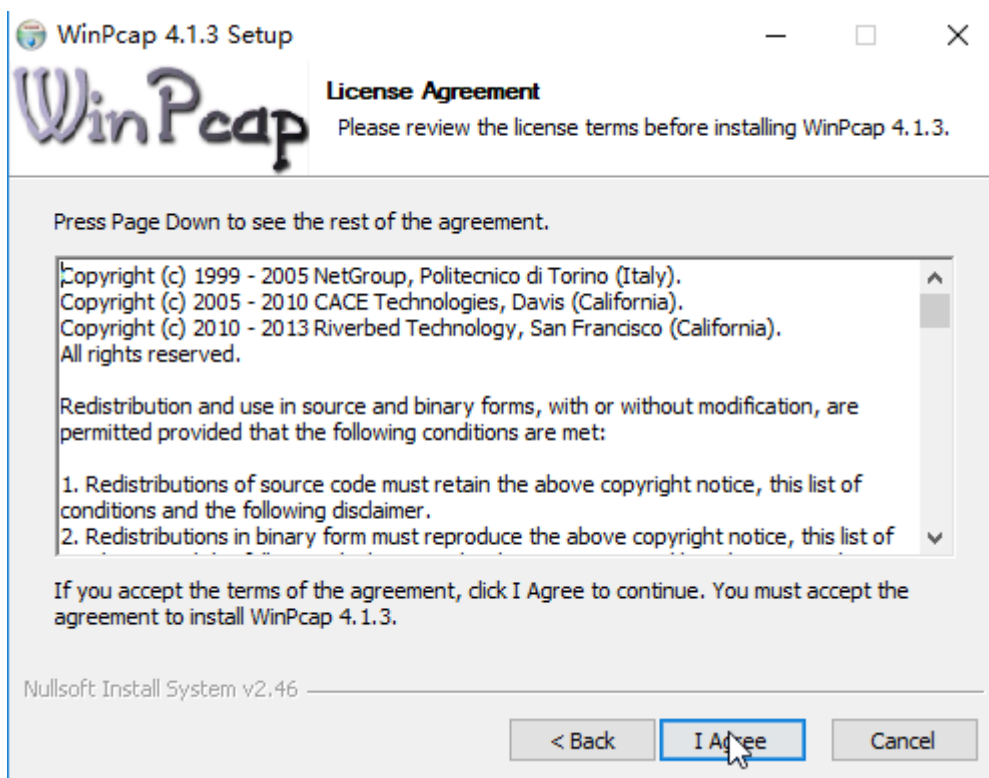
11、【Microsoft Visual C++ 2015】安装完成，点击【关闭】按钮，如下图：



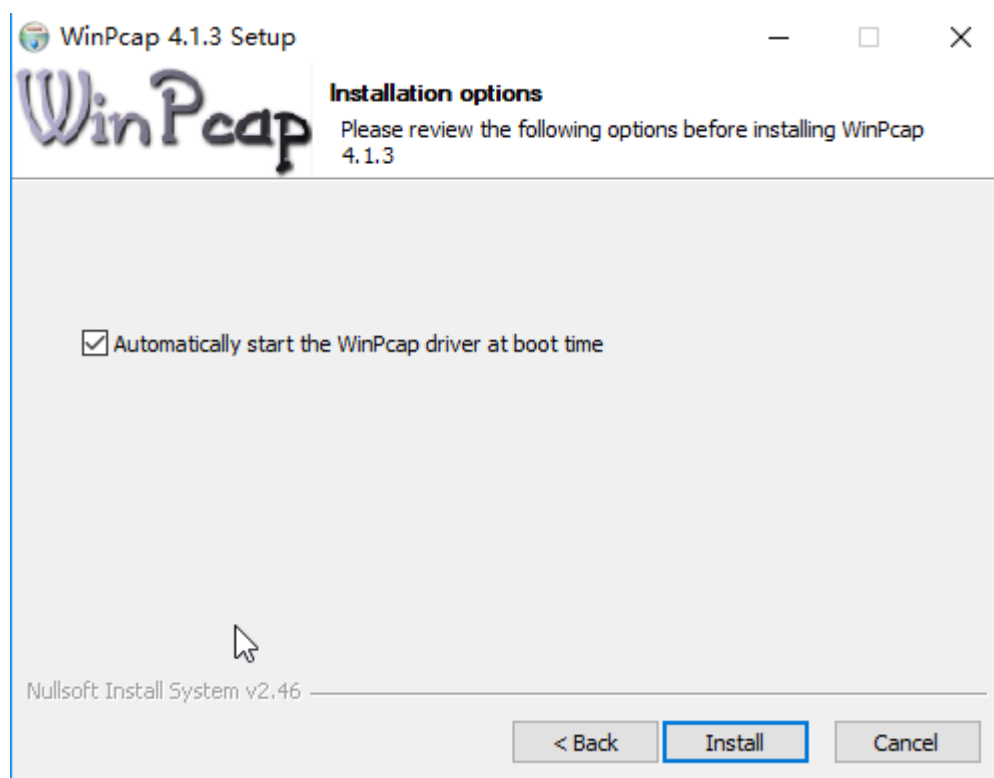
12、弹出【WinPcap】安装窗口，点击【Next】按钮，如下图：



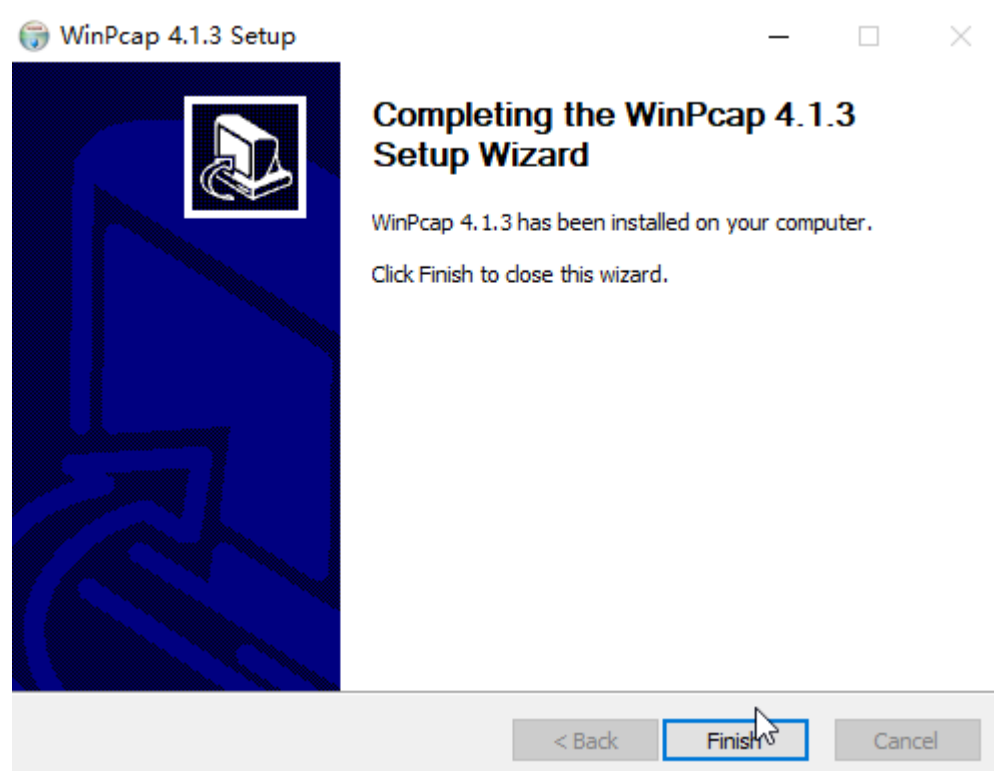
13、在弹出的窗口点击【I Agree】按钮，如下图：



14、在弹出的窗口点击【Install】按钮，如下图：



15、安装【WinPcap】程序完成，点击【Finish】按钮，如下图：



16、弹出【rmagent】安装完成窗口，点击【完成】按钮，如下图：



17、重新启动操作系统。

1.2.3.1.2 应用系统与数据库部署在同一台服务器

1、打开浏览器，以安全管理员账号登录云盾·数据库审计系统，点击【维护】->【Agent 管理】，->【下载 Agent】图标，如下图：



2、系统自动弹出【提示】窗口，且浏览器自动开始下载 Agent 程序（即 rmagent.tar.gz 文件）至本地。然后点击【确定】按钮，如下图：



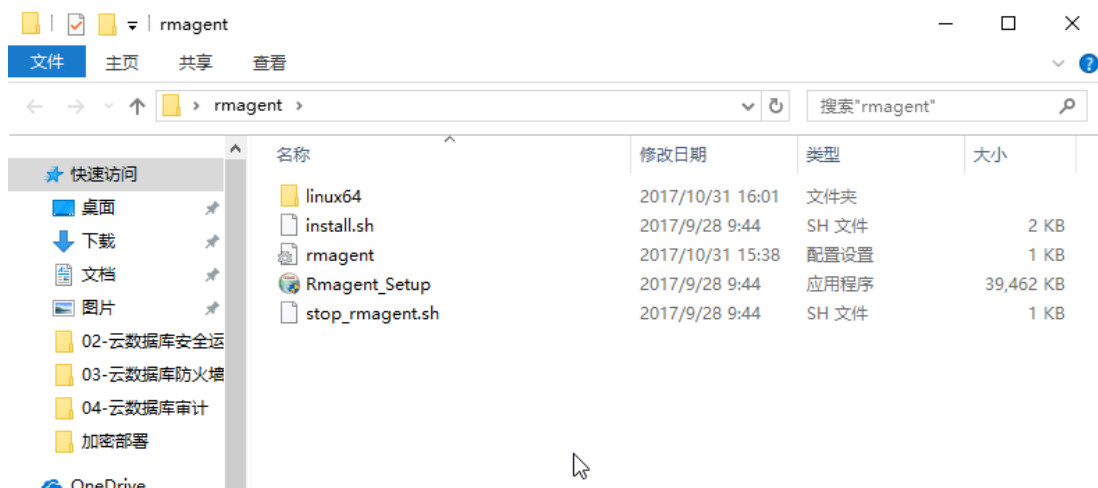
3、在弹出的【Agent 部署配置】窗口输入需要部署 Agent 程序的服务器 IP 地址，然后点击【添加】按钮，添加完成后，点击【关闭】按钮，如下图：



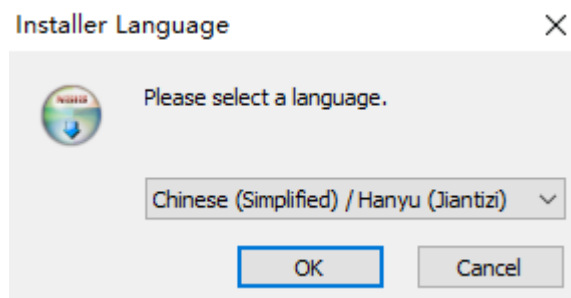
注意：

- 如果需要部署 Agent 程序的服务器与云数据库审计系统在同一个内网，则添加内网地址即可，如果与云数据库审计系统不在同一个内网需要通过外网进行通信的，则添加该服务器的外网地址。
- 如果不添加部署 Agent 程序的服务器 IP 地址，审计系统将不会对抓取的该服务器数据进行审计。

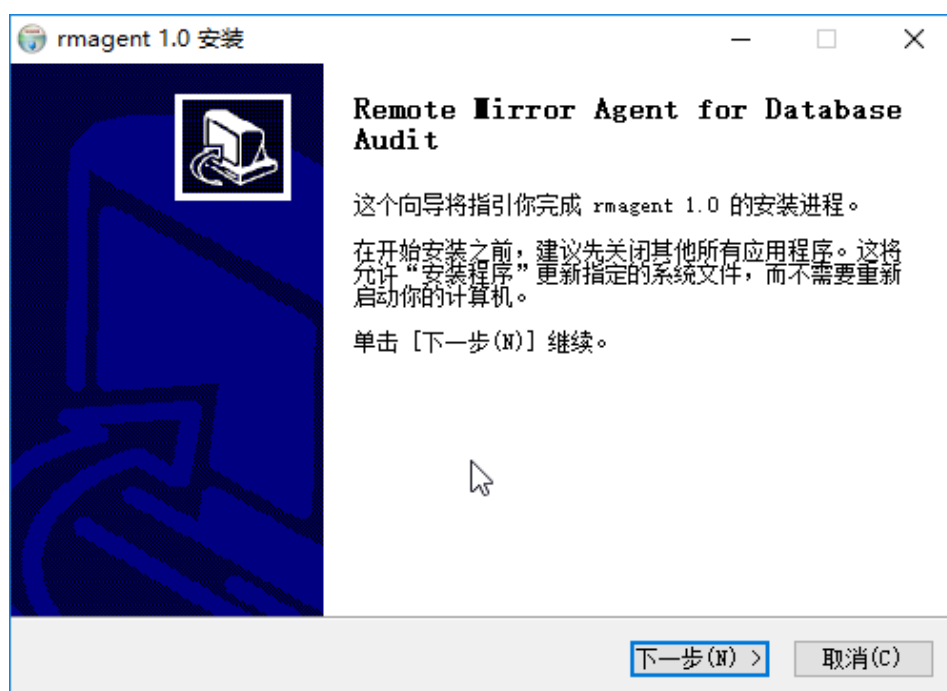
4、将 rmagent.tar.gz 文件上传到需要部署 Agent 程序的服务器，并将其解压缩，如下图：



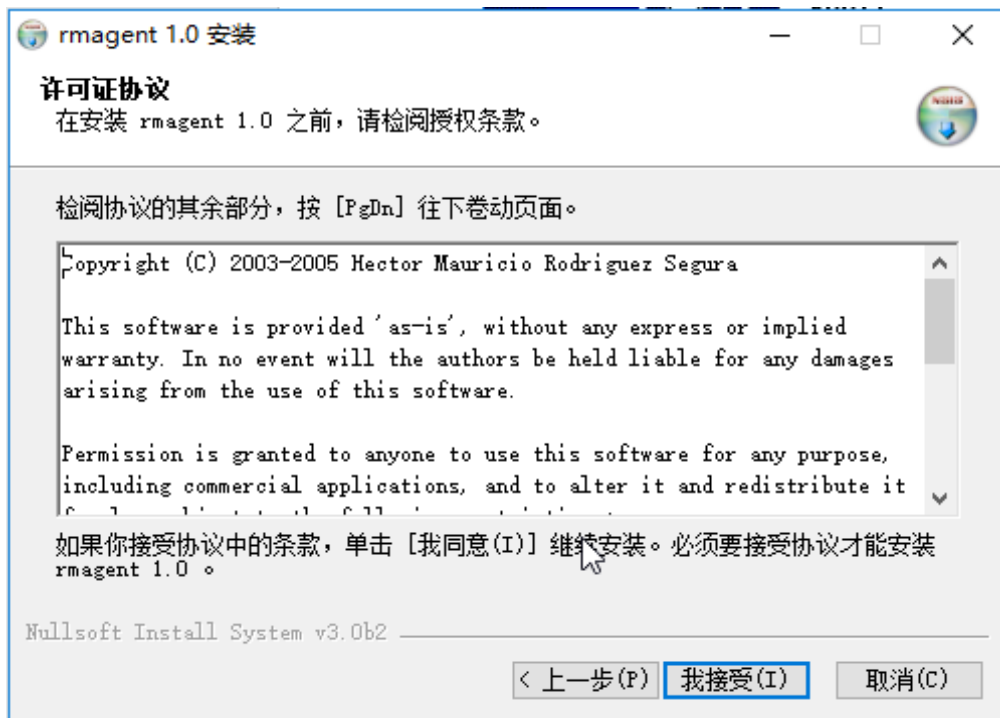
5、打开解压后的 Agent 程序文件夹，双击运行【Rmagent_Setup.exe】文件，在弹出的【Installer Language】窗口点击【OK】按钮，如下图：



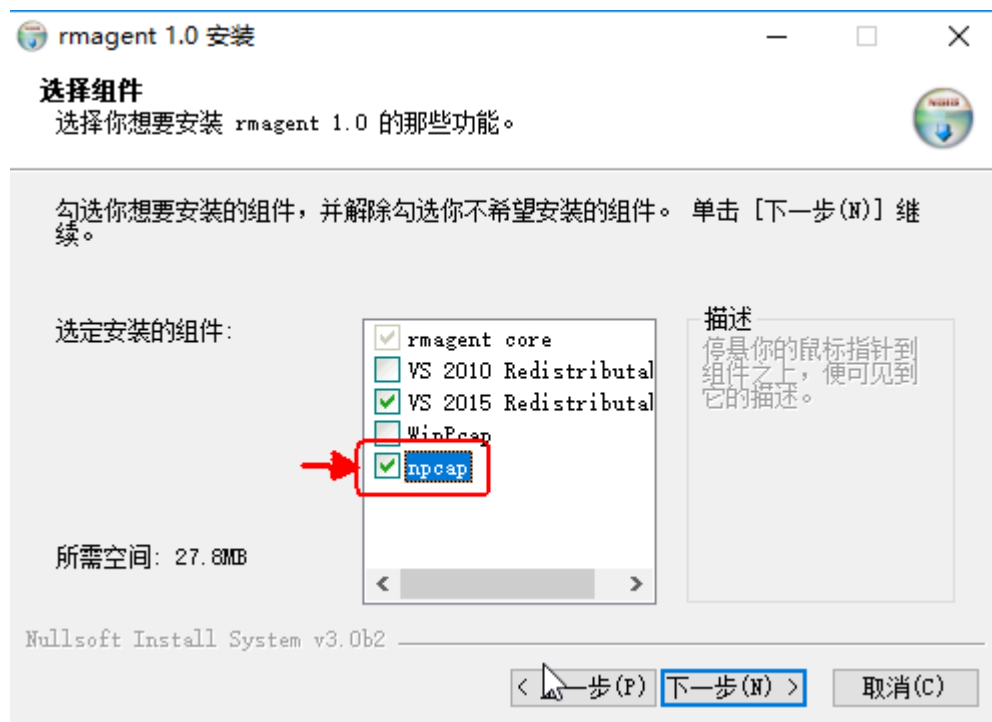
6、弹出【rmagent1.0 安装】窗口，点击【下一步】按钮，如下图：



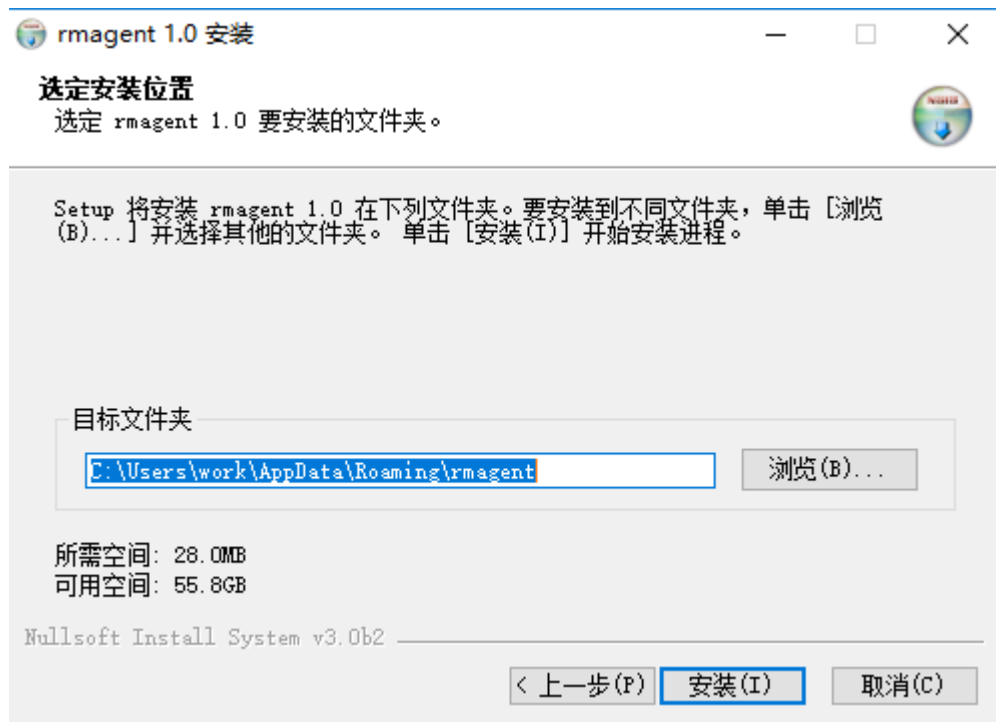
7、弹出【许可证协议】窗口，点击【我接受】按钮，如下图：



8、弹出【选择组件】窗口，选择【npcap】组件，不安装【WinPcap】组件，点击【下一步】按钮，如下图：



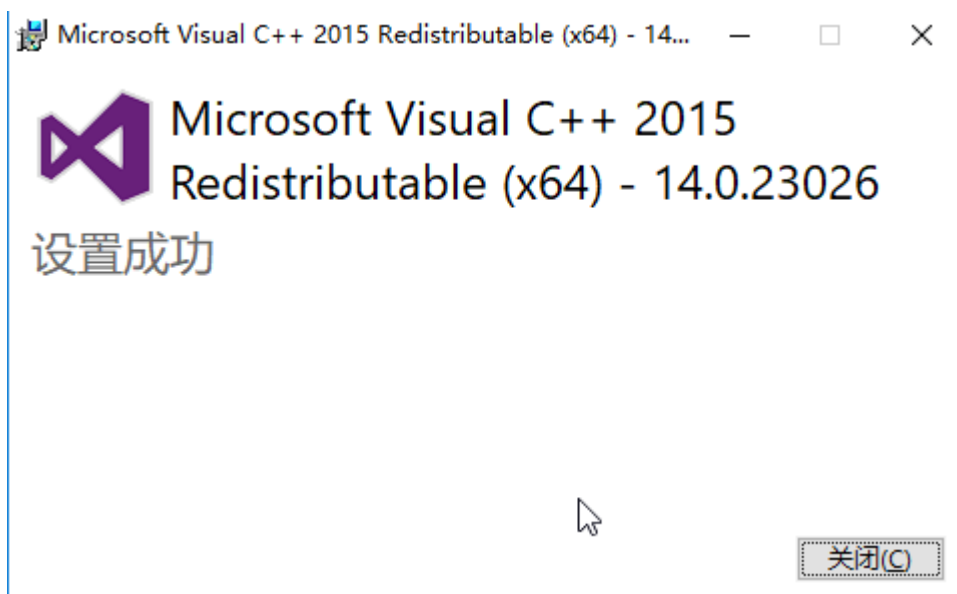
9、弹出【选定安装位置】窗口，默认即可，点击【安装】按钮，如下图：



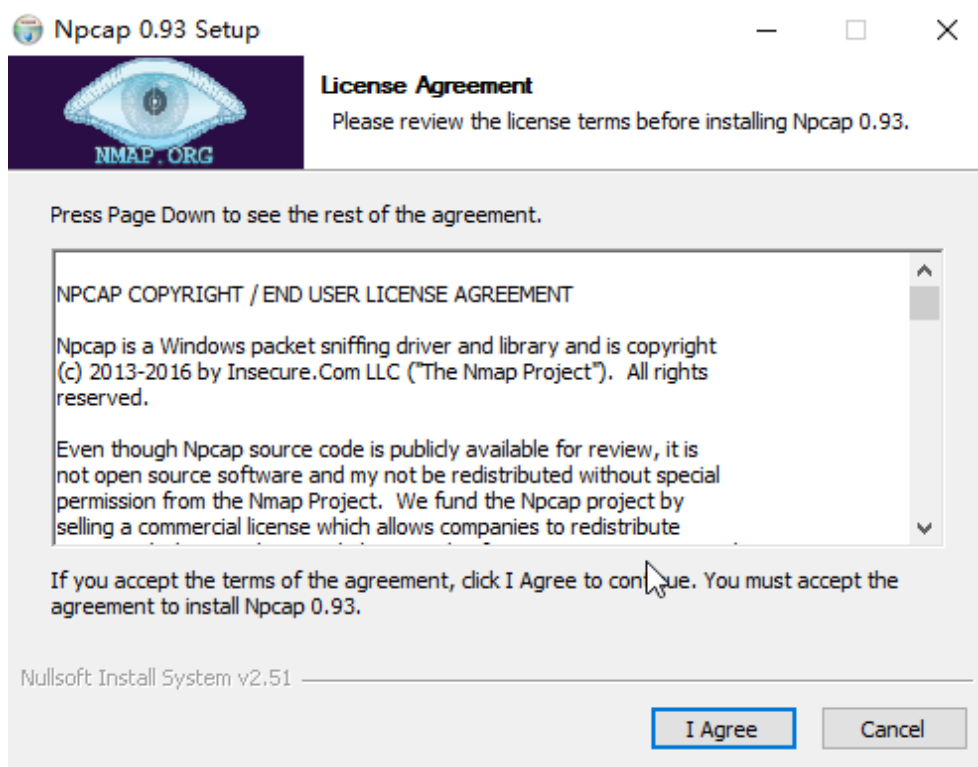
10、弹出【Microsoft Visual C++ 2015】安装窗口，勾选【我同意许可条款和条件】，然后点击【安装】按钮，如下图：



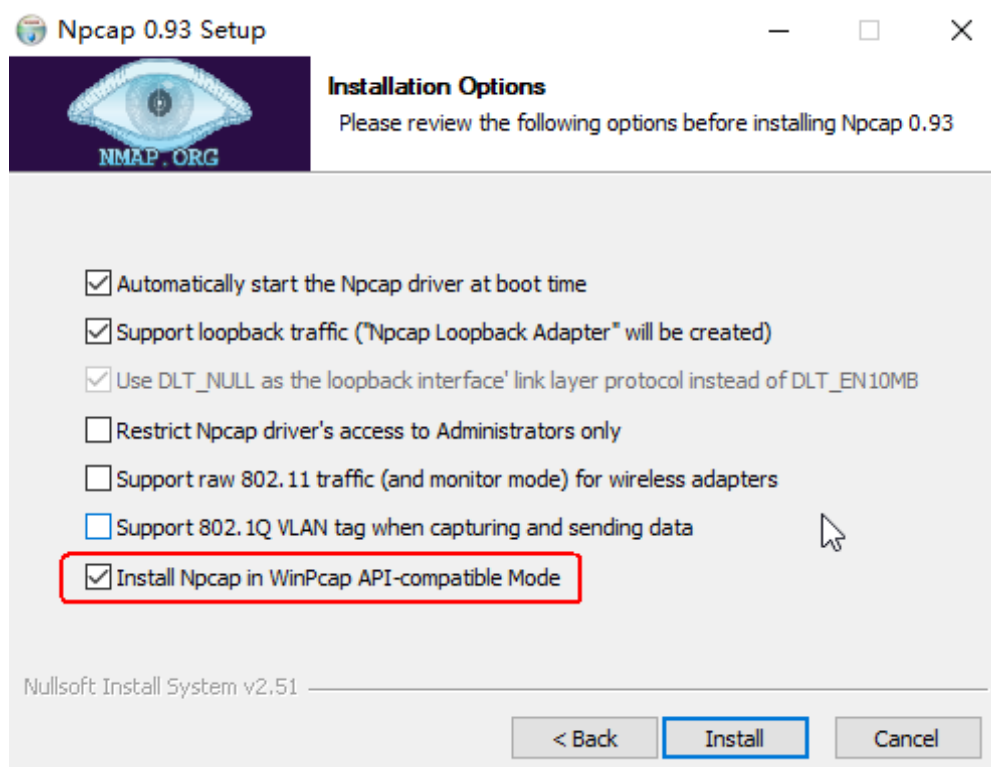
11、【Microsoft Visual C++ 2015】安装完成，点击【关闭】按钮，如下图：



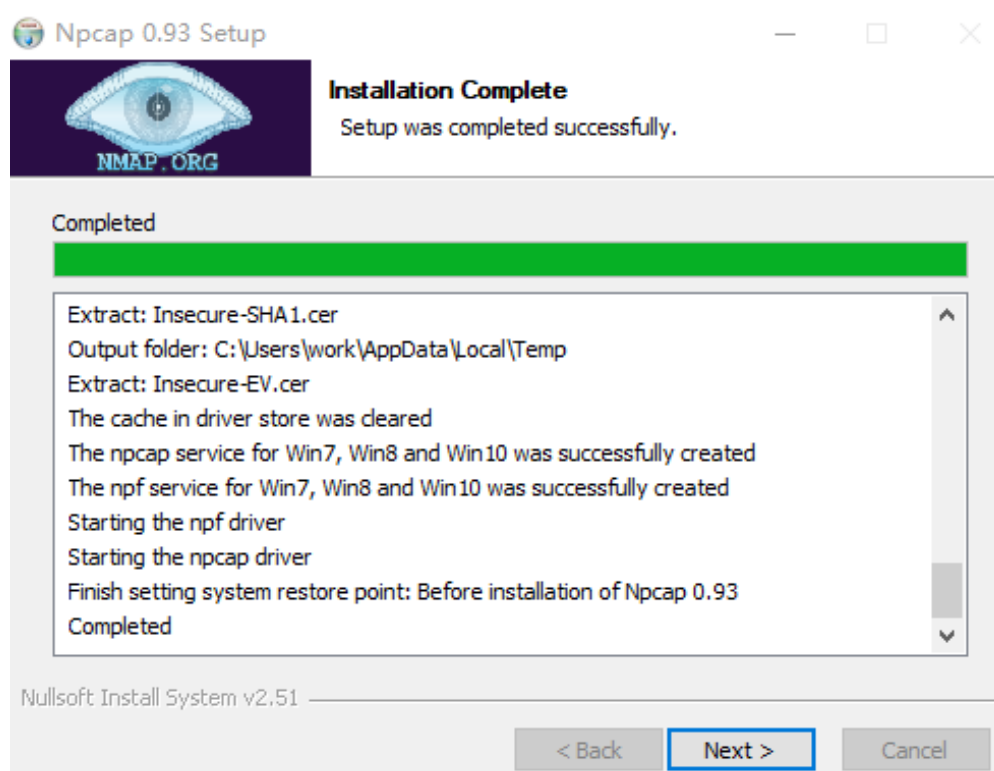
12、弹出【Npcap】安装窗口，点击【I Agree】按钮，如下图：



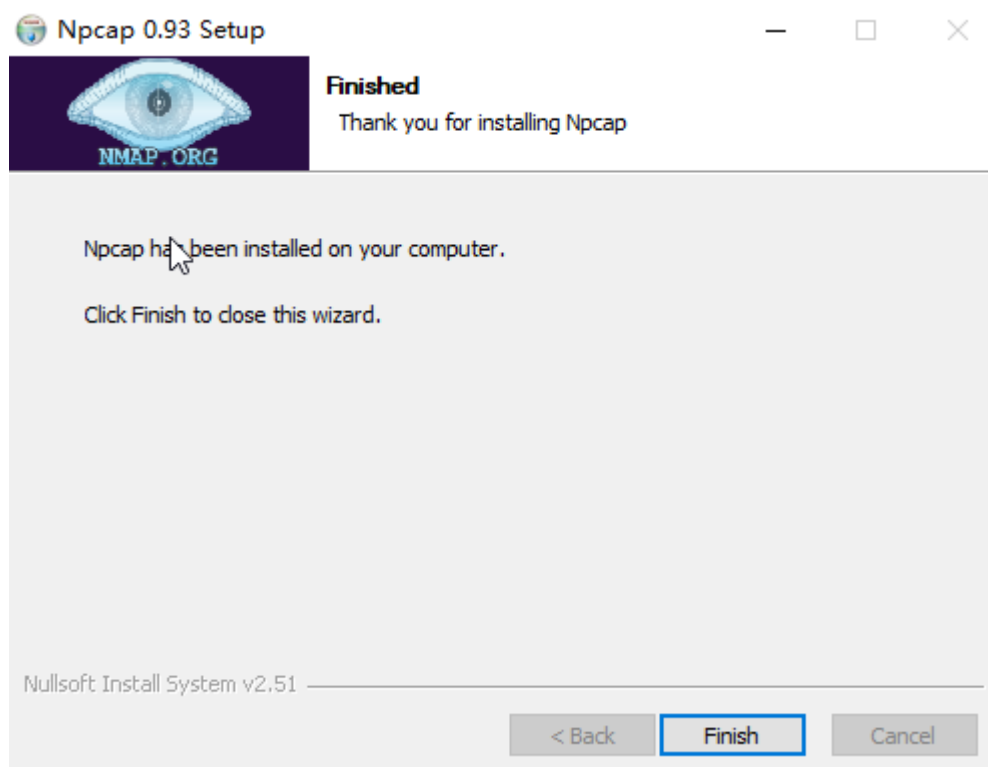
13、在弹出的窗口勾选【Install Npcap in WinPcap API-compatible Mode】，点击【Install】按钮，如下图：



14、在弹出的窗口点击【Next】按钮，如下图：



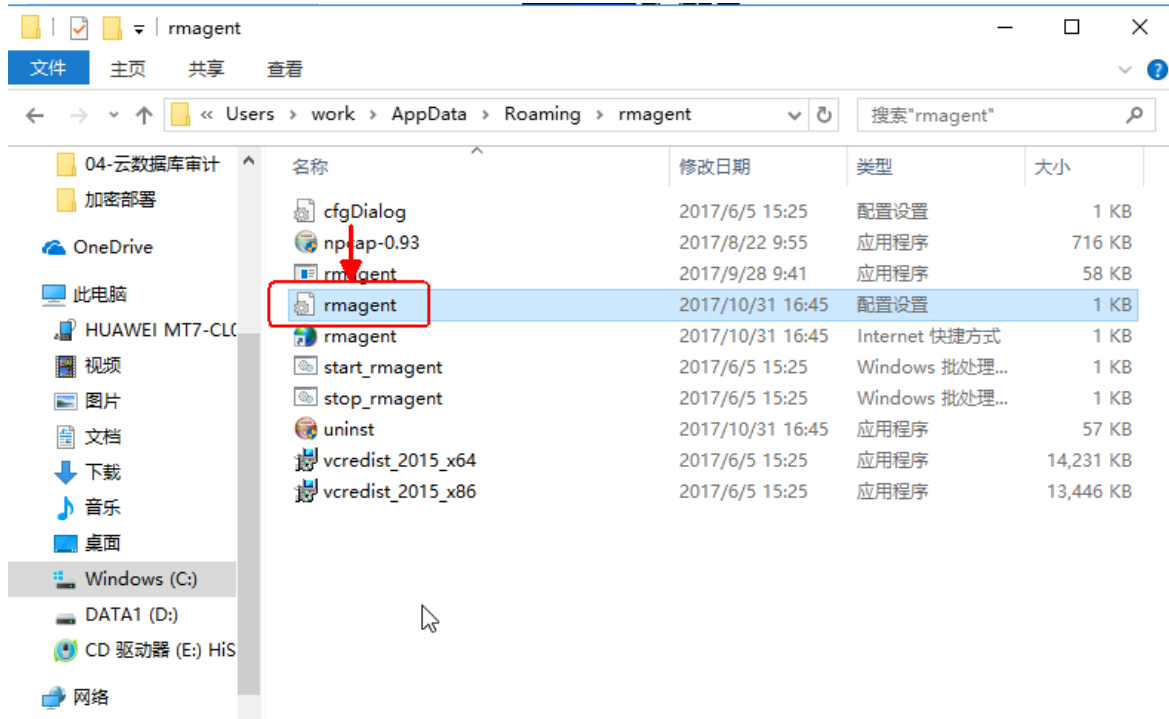
15、安装【Npcap】程序完成，点击【Finish】按钮，如下图：



16、弹出【rmagent】安装完成窗口，点击【完成】按钮，如下图：



17、修改【C:\Users\<用户名>\AppData\Roaming\rmagent\rmagent.ini】，将其中#loopback=1 一行中的“#”删除以解除注释，保存文件，如下图：



18、重新启动操作系统。

1.2.3.2 Linux 系统部署

1.2.3.2.1 应用系统与数据库部署在不同的服务器

1、打开浏览器，以安全管理员账号登录云盾·数据库审计系统，点击【维护】->【Agent 管理】，

-> 【下载 Agent】图标，如下图：



2、系统自动弹出【提示】窗口，且浏览器自动开始下载 Agent 程序（即 rmagent.tar.gz 文件）至本地。然后点击【确定】按钮，如下图：



3、在弹出的【Agent 部署配置】窗口输入需要部署 Agent 程序的服务器 IP 地址，然后点击【添加】按钮，添加完成后，点击【关闭】按钮，如下图：

Agent部署配置

序号	IP地址	操作
1	172.17.71.212	
2	192.168.0.1	
3	192.168.0.111	

IP地址:

192.168.100.88

192.168.100.89

添加

关闭

注意:

- 如果需要部署 Agent 程序的服务器与云数据库审计系统在同一个内网,则添加内网地址即可,如果与云数据库审计系统不在同一个内网需要通过外网进行通信的,则添加该服务器的外网地址。
- 如果不添加部署 Agent 程序的服务器 IP 地址,审计系统将不会对抓取的该服务器数据进行审计。

4、以 root 用户登录需要安装 Agent 程序的服务器,将 `rmagent.tar.gz` 文件上传到服务器,并将其解压缩,如下图:

```
[root@rsdsdf ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  rmagent_.tar.gz
[root@rsdsdf ~]# tar -xvf rmagent_.tar.gz
./
./stop_rmagent.sh
./Rmagent_Setup.exe
./linux64/
./linux64/rmagent
./rmagent.ini
./install.sh
[root@rsdsdf ~]#
```

5、给 install.sh 文件增加权限，如下图：

```
[root@rsdsdf ~]# chmod 755 install.sh  
[root@rsdsdf ~]# _
```

6、安装 Agent 程序，如下图：

```
[root@rsdsdf ~]# ./install.sh  
start rmagent ...  
start rmagent success  
[root@rsdsdf ~]# ^C  
[root@rsdsdf ~]# _
```

7、启动 rmagent，如下图：

```
[root@mysql rmagent]# cd /usr/local//rmagent/  
[root@mysql rmagent]# ./rmagent  
[root@mysql rmagent]# █
```

1.2.3.2.2 应用系统与数据库部署在同一台服务器

1、打开浏览器，以安全管理员账号登录云盾·数据库审计系统，点击【维护】->【Agent 管理】，->【下载 Agent】图标，如下图：



2、系统自动弹出【提示】窗口，且浏览器自动开始下载 Agent 程序（即 rmagent.tar.gz 文件）至本地。然后点击【确定】按钮，如下图：



3、在弹出的【Agent 部署配置】窗口输入需要部署 Agent 程序的服务器 IP 地址，然后点击【添加】按钮，添加完成后，点击【关闭】按钮，如下图：



注意：

- 如果需要部署 Agent 程序的服务器与云数据库审计系统在同一个内网，则添加内网地址即可，如果与云数据库审计系统不在同一个内网需要通过外网进行通信的，则添加该服务器的外网地址。
- 如果不添加部署 Agent 程序的服务器 IP 地址，审计系统将不会对抓取的该服务器数据进行审计。

4、以 root 用户登录需要安装 Agent 程序的服务器，将 rmagent.tar.gz 文件上传到服务器，并将其解压缩，如下图：

```
[root@rsdsdf ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  rmagent_.tar.gz
[root@rsdsdf ~]# tar -xvf rmagent_.tar.gz
./
./stop_rmagent.sh
./Rmagent_Setup.exe
./linux64/
./linux64/rmagent
./rmagent.ini
./install.sh
[root@rsdsdf ~]#
```

5、给 install.sh 文件增加权限，如下图：

```
root@rsdsdf ~]# chmod 755 install.sh
root@rsdsdf ~]# _
```

6、安装 Agent 程序，如下图：

```
[root@rsdsdf ~]# ./install.sh
start ragent ...
start ragent success
[root@rsdsdf ~]# ^C
[root@rsdsdf ~]# _
```

7、进入 rmagent 安装目录，使用 VI 编辑器修改 rmagent.ini 配置文件，如下图：

```
[root@mysql ~]# cd /usr/local//rmaagent/
[root@mysql rmaagent]# vi rmaagent.ini
```

8、打开有 `rmagent.ini` 文件，并在其最后加入一行 `loopback=1`，然后保存，如下图：

```
server_host=60.205.188.19
loopback=1
```

9、重启 rmagent。先执行 ./stop_rmagent.sh 将 rmagent 进程停止，然后再执行 ./rmagent 启动 rmagent 进程，如下图：

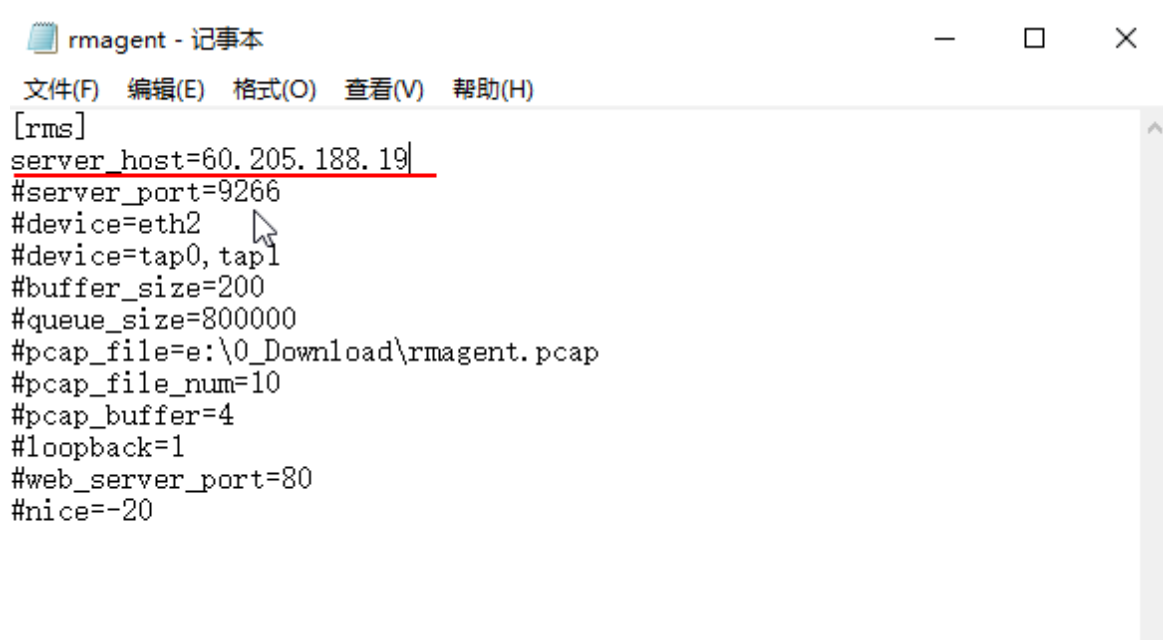
```
[root@mysql ~]# cd /usr/local//rmagent/  
[root@mysql rmagent]# ./stop_rmagent.sh  
find pid: 1352, exe: /usr/local/rmagent/rmagent  
[root@mysql rmagent]# ./rmagent  
[root@mysql rmagent]#
```

1.2.4 Agent 程序部署注意事项

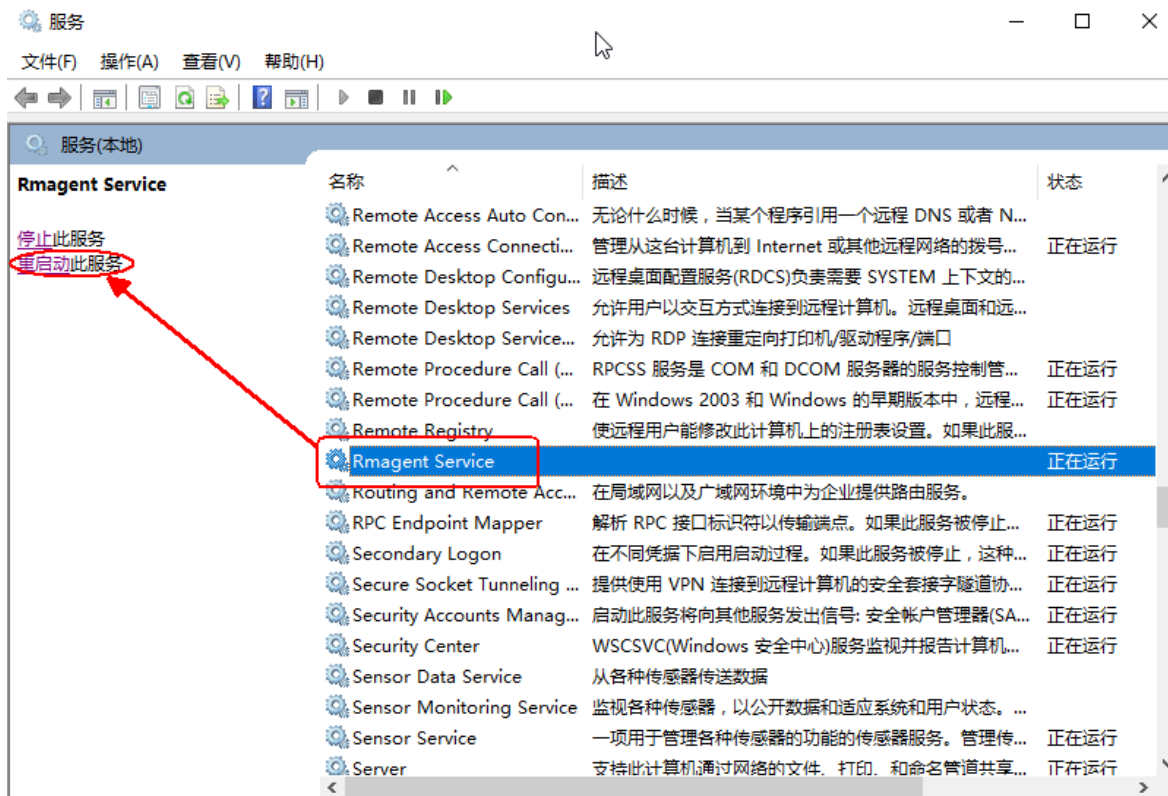
Agent 程序默认连接云数据库审计系统的内网 IP，如果部署 Agent 程序的服务器与云数据库审计系统通过外网连接则需要修改 rmagent.ini 中的 IP 地址。

1.2.4.1 Windows 系统

1、修改【C:\Users\<用户名>\AppData\Roaming\rmagent\rmagent.ini】，将其中 server_host 一行的 IP 地址修改为云数据库审计系统的外网 IP 地址，保存文件，如下图：



2、重新启动【rmagent】服务。打开【服务】管理器，选中【Rmagent Service】服务，然后点击左侧的【重新启动此服务】，如下图：



1.2.4.2 Linux 系统

1、进入 rmagent 安装目录，使用 VI 编辑器修改 rmagent.ini 配置文件，如下图：

```
[root@mysql ~]# cd /usr/local//rmagent/  
[root@mysql rmagent]# vi rmagent.ini
```

2、打开 rmagent.ini 文件，将 server_host 的值修改为云数据库审计系统的外网 IP 地址，然后保存，如下图：

```
server_host=60.205.188.19
```

```
-- INSERT --
```

3、重启 ragent。先执行 ./stop_ragent.sh 将 ragent 进程停止，然后再执行 ./rmagent 启动 ragent 进程，如下图：

```
[root@mysql ~]# cd /usr/local//rmagent/  
[root@mysql rmagent]# ./stop_ragent.sh  
find pid: 1352, exe: /usr/local/rmagent/rmagent  
[root@mysql rmagent]# ./rmagent  
[root@mysql rmagent]# █
```

1.3 部署测试

使用安装有 Agent 程序的服务器访问被审计数据库并执行 SQL 语句，并以安全管理员账号登录云数据库审计系统，查看是否有审计信息。