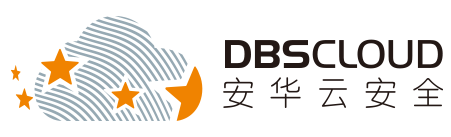
**安华金和云数据库审计**

**接入文档**



北京安华金和科技有限公司

二〇二〇年四月

**版权申明**

本文档包含了来自北京安华金和科技有限公司的技术和商业信息，提供给北京安华金和科技有限公司的客户或合作伙伴使用。接受本文档表示同意对其内容保密并且未经北京安华金和科技有限公司书面认可，不得复制、泄露或散布本文档的全部或部分内容。

本文档及其描述的产品受有关法律的版权保护，对本文档内容的任何形式的非法复制，泄露或散布，需承担相应的法律责任。

北京安华金和科技有限公司保留在不另行通知的情况下修改本文档的权利，并保留对本文档内容的解释权。

目 录

[1. 产品部署 4](#_Toc497825850)

[2. 产品初始化 13](#_Toc497825851)

[2.1 导入License文件 13](#_Toc497825852)

[2.1.1 登录系统管理员界面 13](#_Toc497825853)

[2.1.2 导入License文件 13](#_Toc497825854)

[2.2 添加被审计数据库实例 14](#_Toc497825855)

[2.2.1 登录安全管理员界面 14](#_Toc497825856)

[2.2.2 添加被保护数据库实例 15](#_Toc497825857)

[2.3 部署Agent程序 20](#_Toc497825858)

[2.3.1 Agent程序部署位置 20](#_Toc497825859)

[2.3.2 Agent程序自动部署（仅支持linux系统） 20](#_Toc497825860)

[2.3.3 Agent程序手动部署 22](#_Toc497825861)

[2.3.4 Agent程序部署注意事项 46](#_Toc497825862)

[2.4 部署测试 48](#_Toc497825863)

# 产品初始化

**说明**：本产品由Agent和Web控制台两部分组成，在系统使用之前需要打开以下端口：

|  |  |  |  |
| --- | --- | --- | --- |
| **源** | **目的** | **端口** | **备注** |
| 运维管理端 | Web控制台 | 443 | Web控制台HTTPS服务通讯端口 |
| 运维管理端 | Web控制台 | 22 | Web控制台SSH服务通讯端口 |
| Agent | Web控制台 | 9266 | Agent与Web控制台通讯端口 |

## 导入License文件

### 登录系统管理员界面

1、打开IE或其他浏览器，在地址栏内输入<https://云数据库审计系统IP地址>。进入登录页面后，输入用户名：sysadmin 默认密码：sysadmin1234，点击【登录】进入系统管理员界面。

**注意：**首次登录系统需要修改安全管理员默认密码。

### 导入License文件

1、进入系统管理员界面，点击“系统”，然后选择“证书管理”，如下图所示。



2、在打开的“证书管理”页面，点击“浏览”，选择获取到的License文件存放路径，然后点击“上传”，校验通过后系统方可正常使用。

## 添加被审计数据库实例

### 登录安全管理员界面

1、打开IE或其他浏览器，在地址栏内输入<https://云数据库审计系统IP地址>。进入登录页面后，输入用户名：secadmin 默认密码：secadmin1234，点击【登录】进入安全管理员界面。

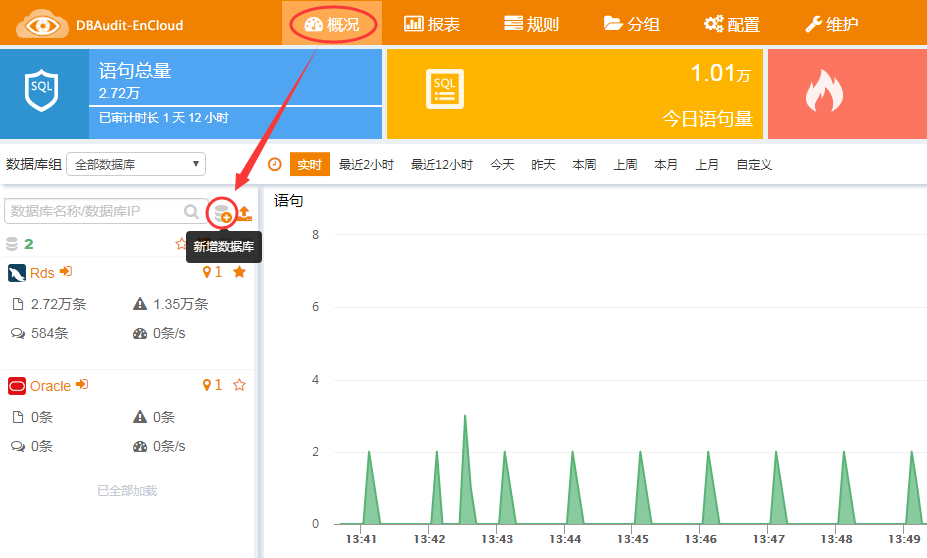
**注意：**首次登录系统需要修改安全管理员默认密码。

### 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：

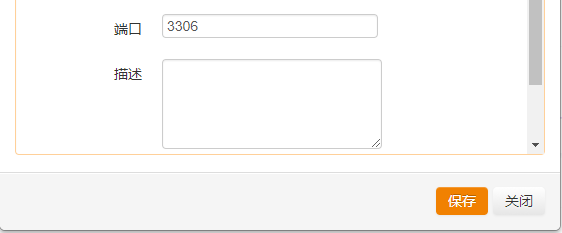
#### 添加云服务器自建数据库实例

1、进入安全管理员界面后点击【概况】，在页面左侧数据库组列表页中点击“新增数据库”图标，如下图所示：



2、在弹出的“新增数据库”页面中填写要审计的数据库实例相关信息，然后点击“保存”。如下图所示：

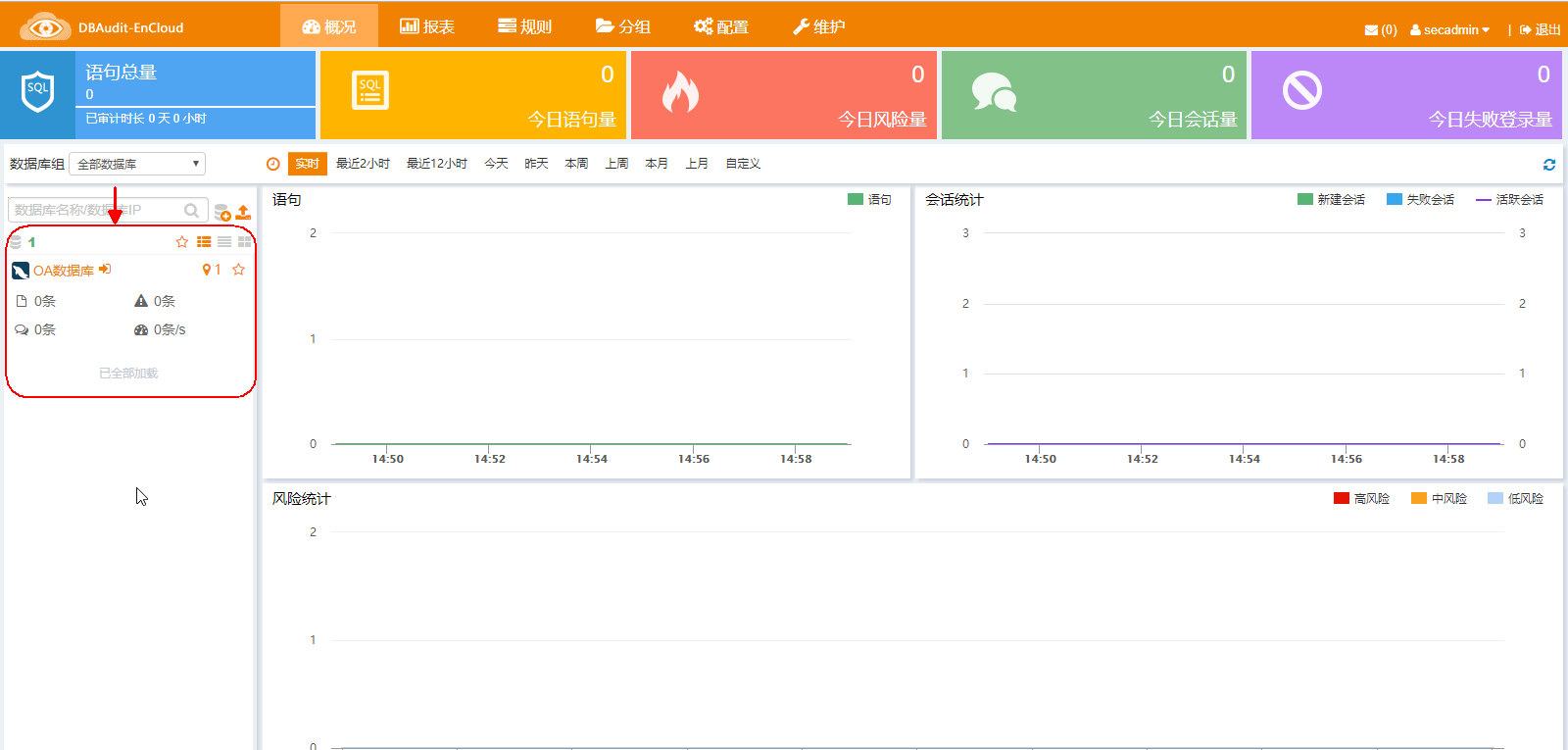




**注意事项：**

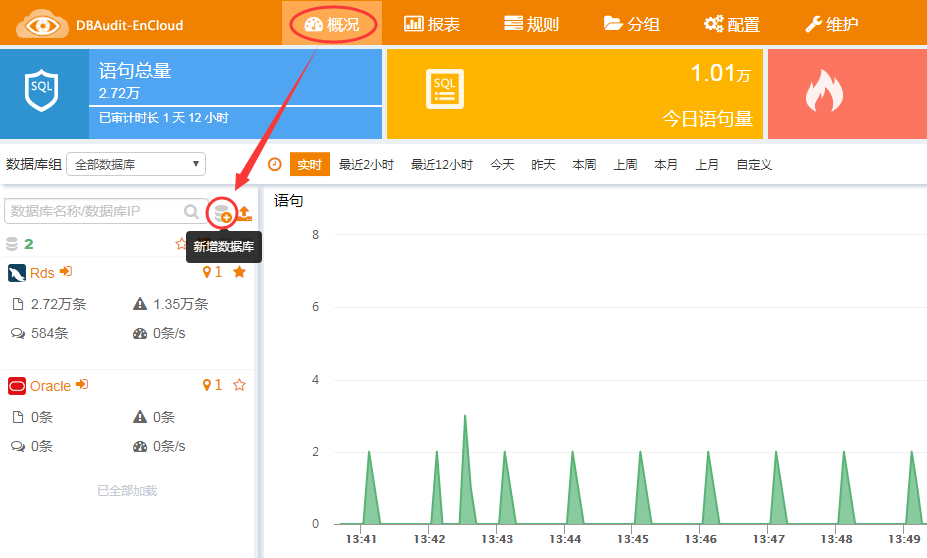
* 数据库名：为被审计数据库实例指定一个名字。
* 数据库类型：根据被审计数据库实例的类型选择。
* 数据库版本：可以手动选择或者点击【自动获取】输入数据库主机IP、数据库主机端口、数据库实例名、用户名、密码，单击“确认”按钮，可以自动获取数据库版本，Oracle数据库同时会获取到字符集。实例名：Oracle与Postgres需要填写，其他数据库可以留空。
* IP地址：被审计数据库实例的IP地址。
* 端口：被审计数据库实例的端口号。

3、数据库添加成功后，可以在“概况”页左侧的“数据库组”列表页处看到增加的数据库摘要信息，如下图所示：

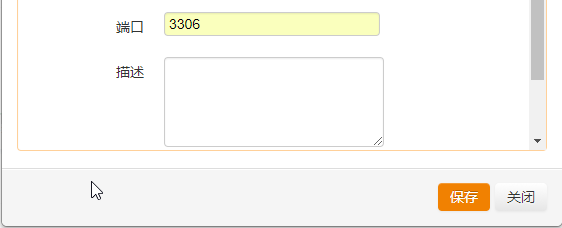


#### 添加云服务商提供的数据库服务实例（如RDS数据库）

1、进入安全管理员界面后点击【概况】，在页面左侧数据库组列表页中点击“新增数据库”图标，如下图所示：



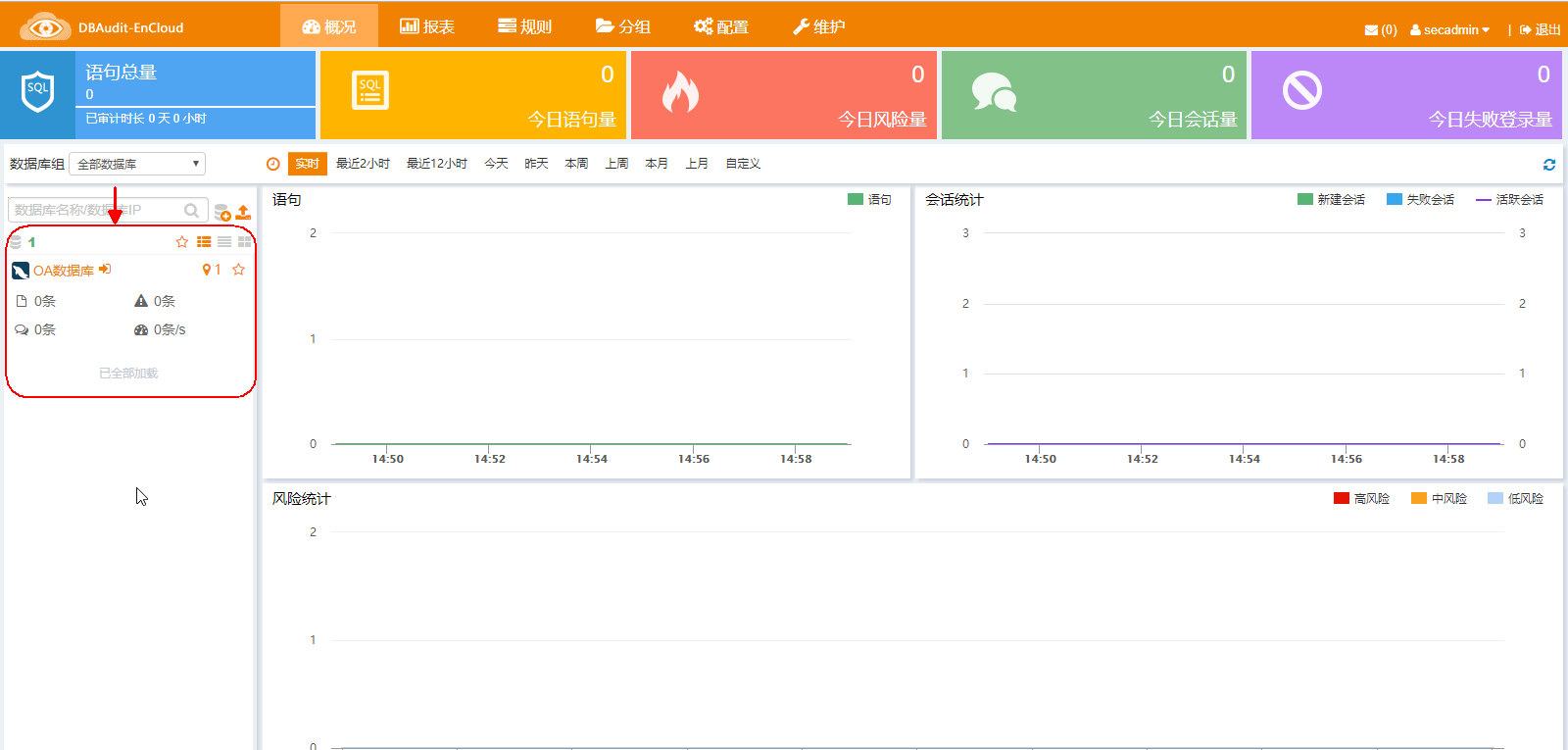
2、在弹出的“新增数据库”页面中填写要审计的数据库实例相关信息，然后点击“保存”。如下图所示：



**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：可以手动选择或者点击【自动获取】输入数据库主机IP、数据库主机端口、数据库实例名、用户名、密码，单击“确认”按钮，可以自动获取数据库版本，Oracle数据库同时会获取到字符集。实例名：Oracle与Postgres需要填写，其他数据库可以留空。
* 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。

3、数据库添加成功后，可以在“概况”页左侧的“数据库组”列表页处看到增加的数据库摘要信息，如下图所示。



## 部署Agent程序

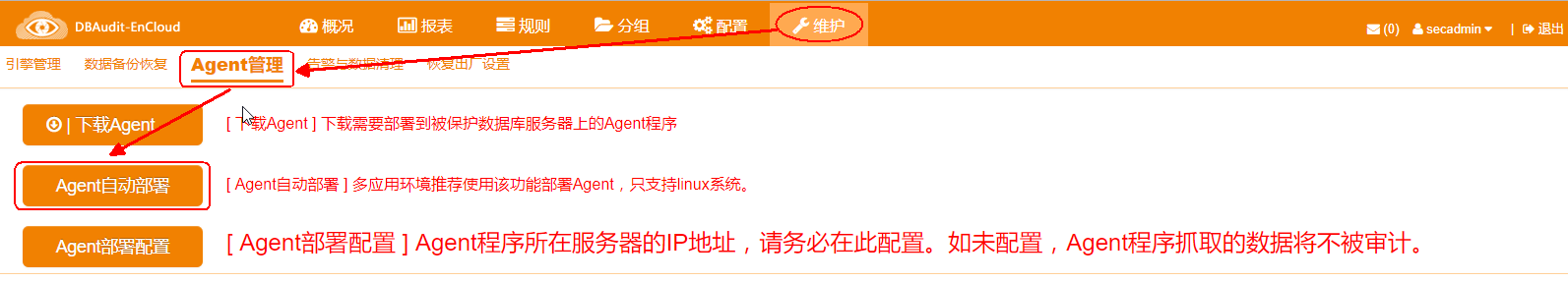
### Agent程序部署位置

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。
* 云服务商提供的数据库服务实例（如RDS数据库）agent部署位置：应用服务器上。

### 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数据库审计，点击“维护”，选择“Agent管理”，然后点击“Agent自动部署”图标，如下图所示。



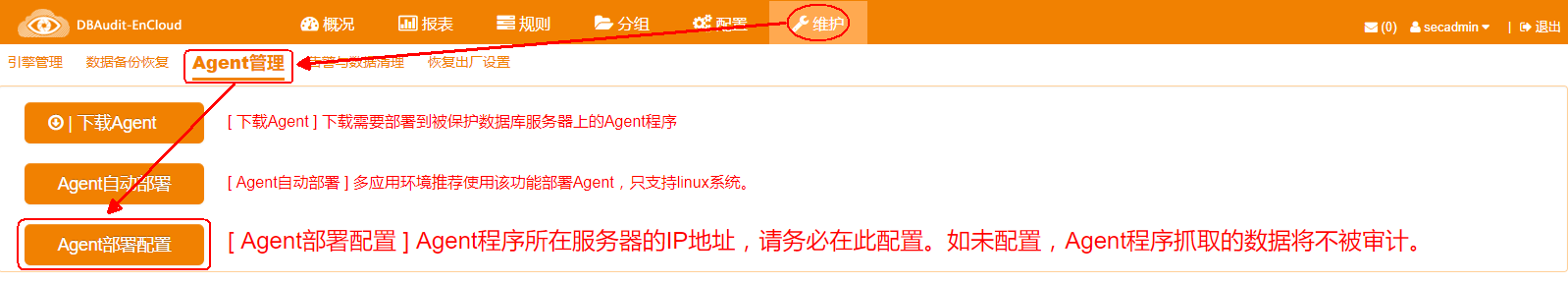
2、在弹出的“Agent自动部署”页面填写需要部署Agent程序的服务器IP地址、ROOT用户密码和SSH端口号，然后点击“部署”，即可自动部署到相应的服务器中。



**注意：**

* 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”
* 如果需要部署Agent程序的服务器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，则需要勾选“外网通讯”，并输入云数据库审计系统的外网IP地址。
* 如果需要将Agent程序自动部署至多台服务器时，可以点击“+”号进行添加。

3、点击“维护”，选择“Agent管理”，然后点击“Agent部署配置”图标，如下图所示。



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”，添加完成后，点击“关闭”。



**注意：**

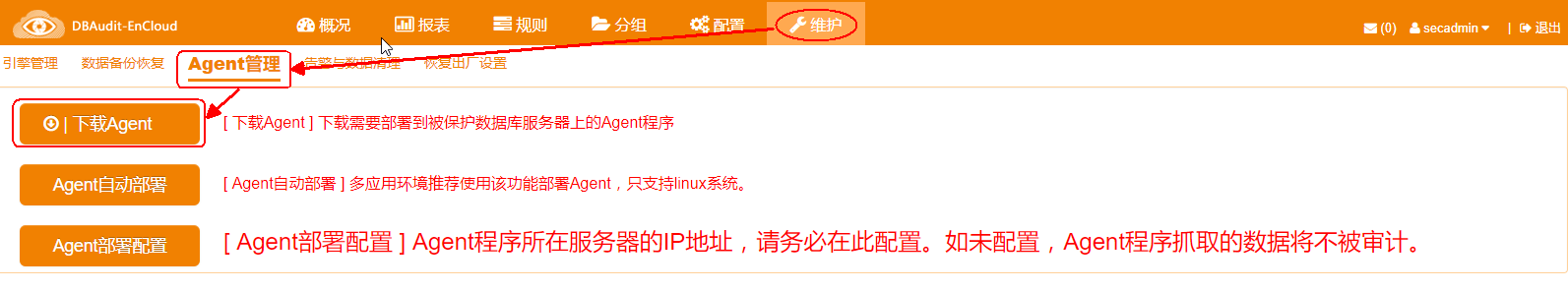
* 如果需要部署Agent程序的服务器与云数据库审计系统在同一个内网，则添加内网地址即可，如果与云数据库审计系统不在同一个内网需要通过外网进行通信的，则添加该服务器的外网地址。
* 如果不添加部署Agent程序的服务器IP地址，审计系统将不会对抓取的该服务器数据进行审计。

### Agent程序手动部署

#### Windows系统部署

##### 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数据库审计系统，点击“维护”，选择“Agent管理”，然后点击 “下载Agent”图标，如下图所示。



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”。如下图所示。



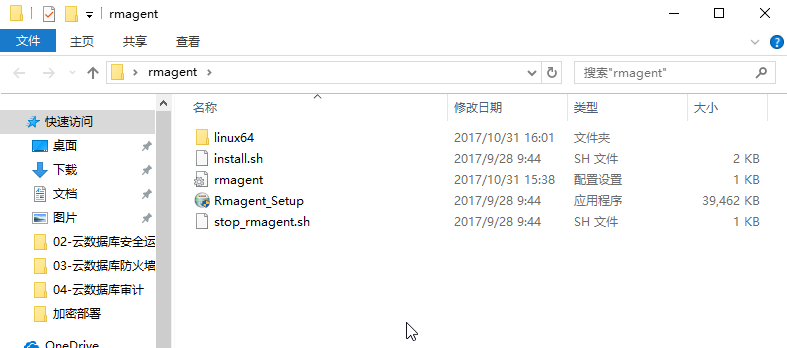
3、在弹出的“Agent部署配置”窗口输入需要部署Agent程序的服务器IP地址，然后点击“添加”，添加完成后，点击“关闭”。



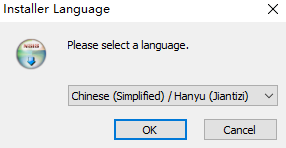
**注意：**

* 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。

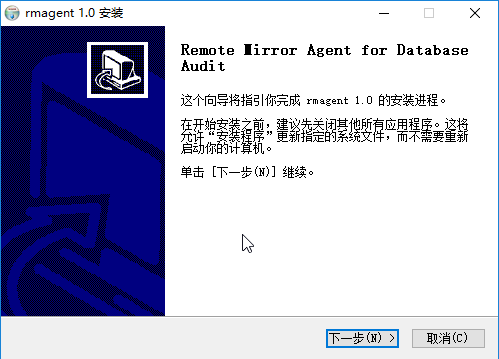
4、将rmagent.tar.gz文件上传到需要部署Agent程序的服务器，并将其解压缩。



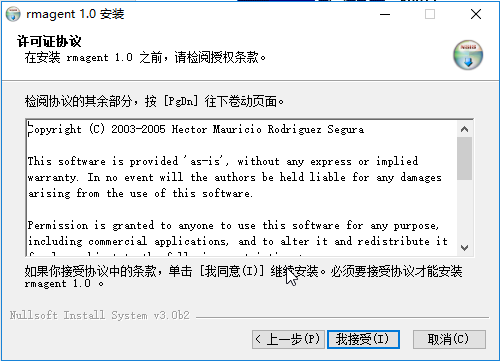
5、打开解压后的Agent程序文件夹，双击运行“Rmagent\_Setup.exe”文件，在弹出的“Installer Language”窗口点击“OK”，如下图所示。



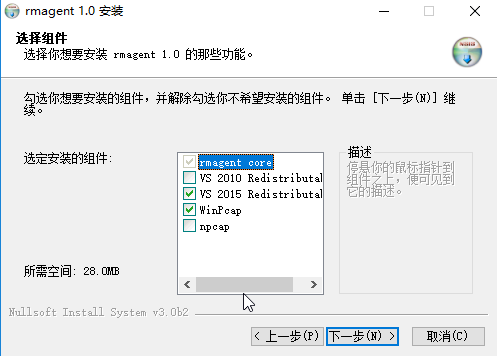
6、弹出“rmagent1.0安装”窗口，点击“下一步”，如下图所示。



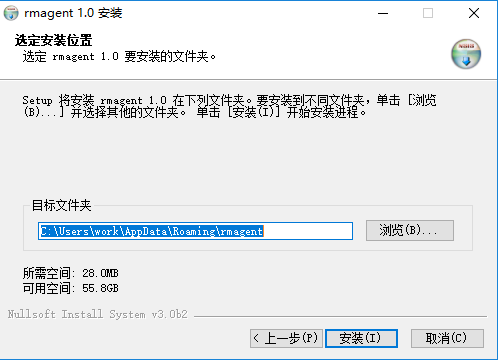
7、弹出“许可证协议”窗口，点击“我接受”，如下图所示。



8、弹出“选择组件”窗口，点击“下一步”



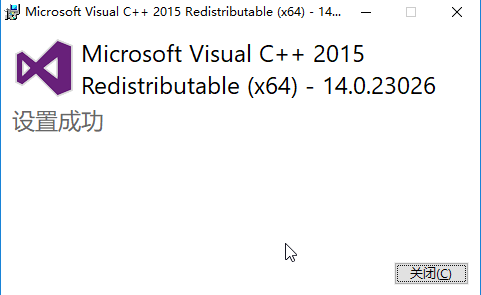
9、弹出“选定安装位置”窗口，默认即可，点击“安装”，如下图所示。



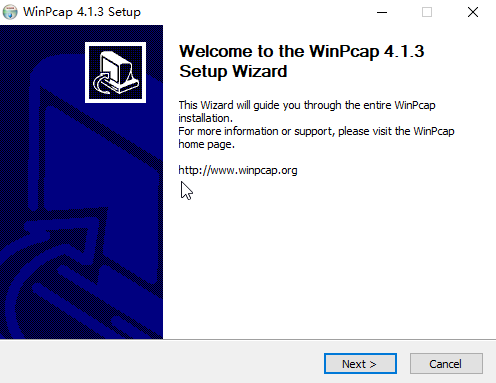
10、弹出“Microsoft Visual C++ 2015”安装窗口，勾选“我同意许可条款和条件”，然后点击“安装”，如下图所示。



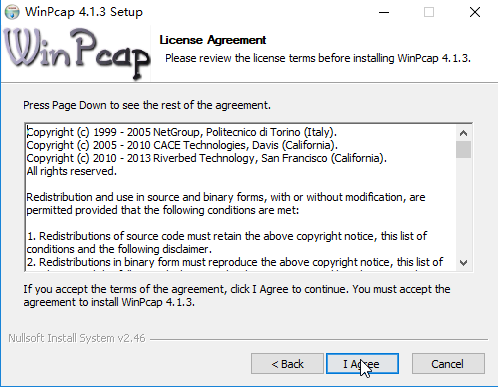
11、“Microsoft Visual C++ 2015”安装完成，点击“关闭”，如下图所示。



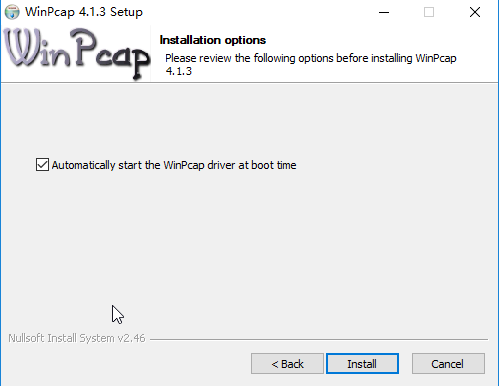
12、弹出“WinPcap”安装窗口，点击“Next”，如下图所示。



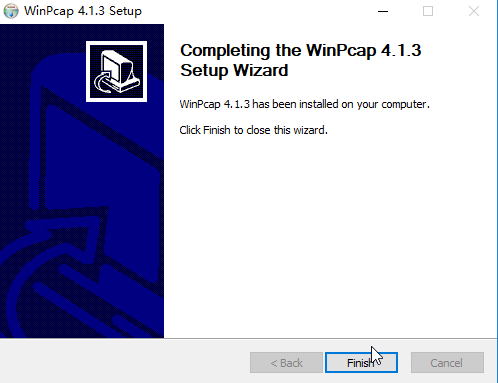
13、在弹出的窗口点击“I Agree”，如下图所示。



14、在弹出的窗口点击“Install”，如下图所示。



15、安装“WinPcap”程序完成，点击“Finish”。



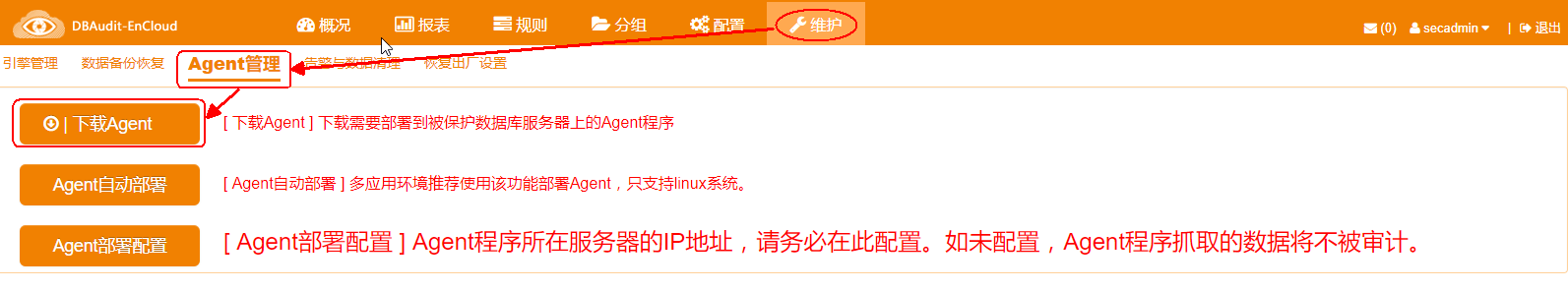
16、弹出“rmagent”安装完成窗口，点击“完成”，如下图所示。



17、重新启动操作系统。

##### 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数据库审计系统，点击“维护”，选择“Agent管理”，然后点击 “下载Agent”图标，如下图所示。



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”。如下图所示。



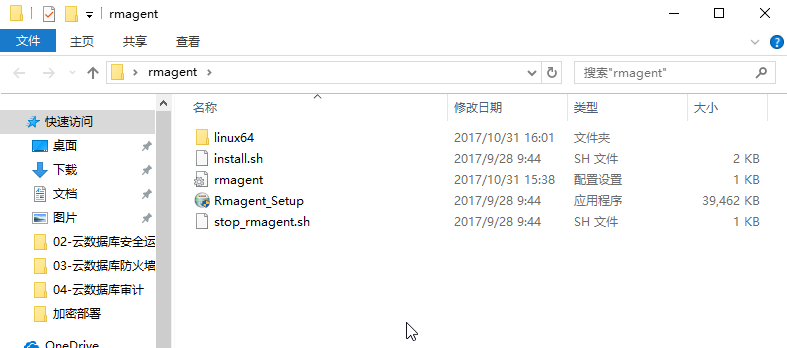
3、在弹出的“Agent部署配置”窗口输入需要部署Agent程序的服务器IP地址，然后点击“添加”，添加完成后，点击“关闭”。



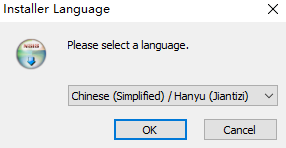
**注意：**

* 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。

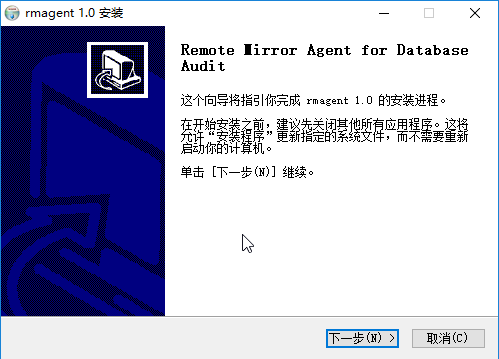
4、将rmagent.tar.gz文件上传到需要部署Agent程序的服务器，并将其解压缩。



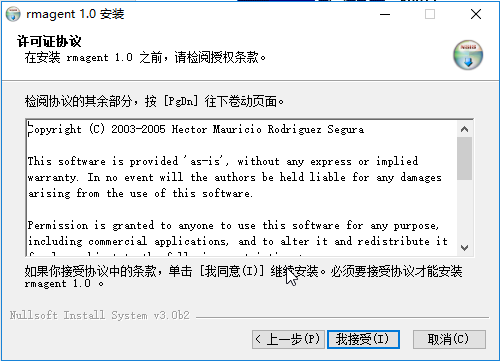
5、打开解压后的Agent程序文件夹，双击运行“Rmagent\_Setup.exe”文件，在弹出的“Installer Language”窗口点击“OK”，如下图所示。



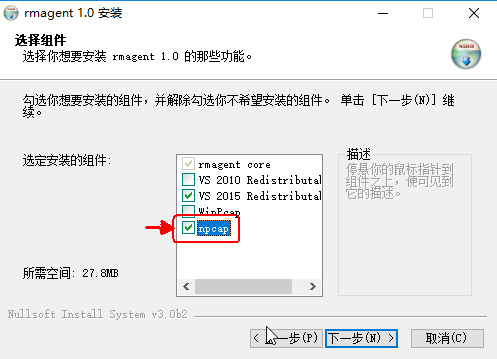
6、弹出“rmagent1.0安装”窗口，点击“下一步”，如下图所示。



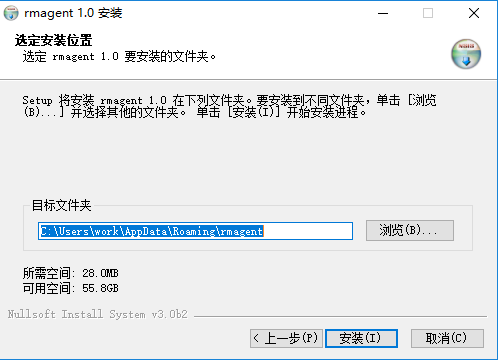
7、弹出“许可证协议”窗口，点击“我接受”，如下图所示。



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”，如下图所示。



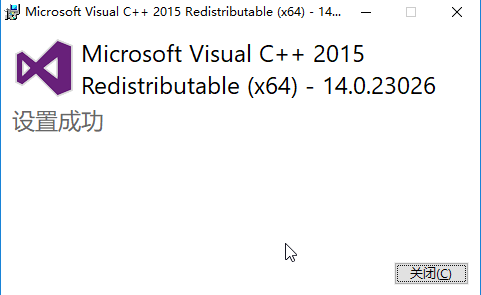
9、弹出“选定安装位置”窗口，默认即可，点击“安装”，如下图所示。



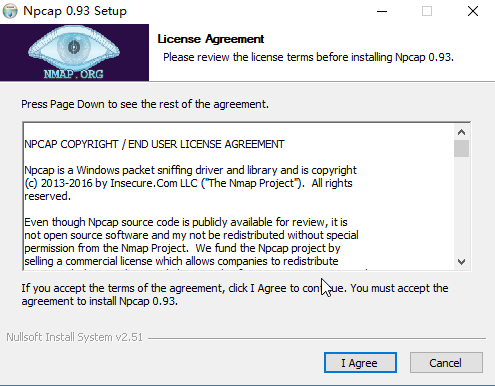
10、弹出“Microsoft Visual C++ 2015”安装窗口，勾选“我同意许可条款和条件”，然后点击“安装”，如下图所示。



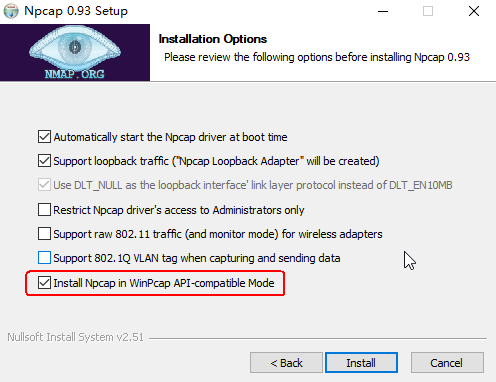
11、“Microsoft Visual C++ 2015”安装完成，点击“关闭”，如下图所示。



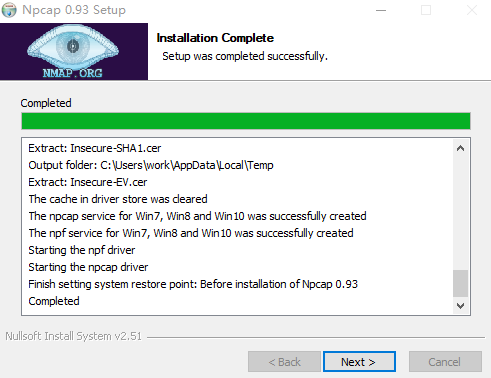
12、弹出“Npcap”安装窗口，点击“I Agree”，如下图所示。



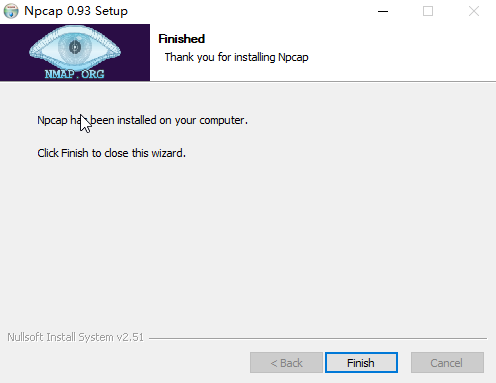
13、在弹出的窗口勾选“Install Npcap in WinPcap API-compatible Mode”，点击“Install”，如下图所示。



14、在弹出的窗口点击“Next”，如下图所示。



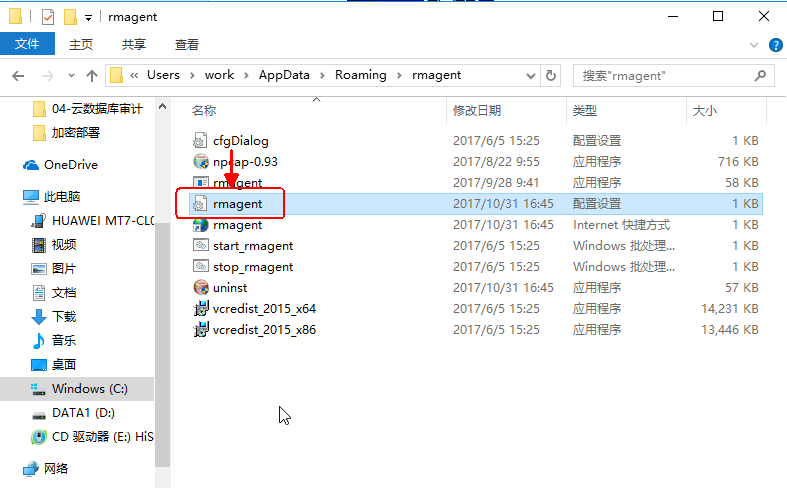
15、安装“Npcap”程序完成，点击“Finish”。

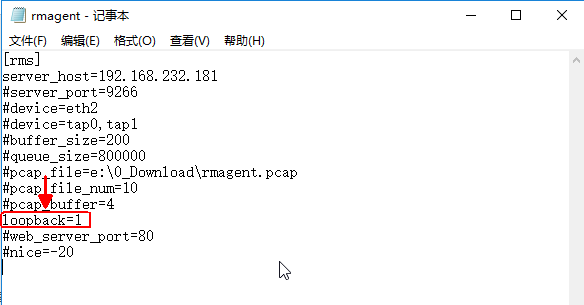


16、弹出“rmagent”安装完成窗口，点击“完成”，如下图所示。



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，如下图所示。



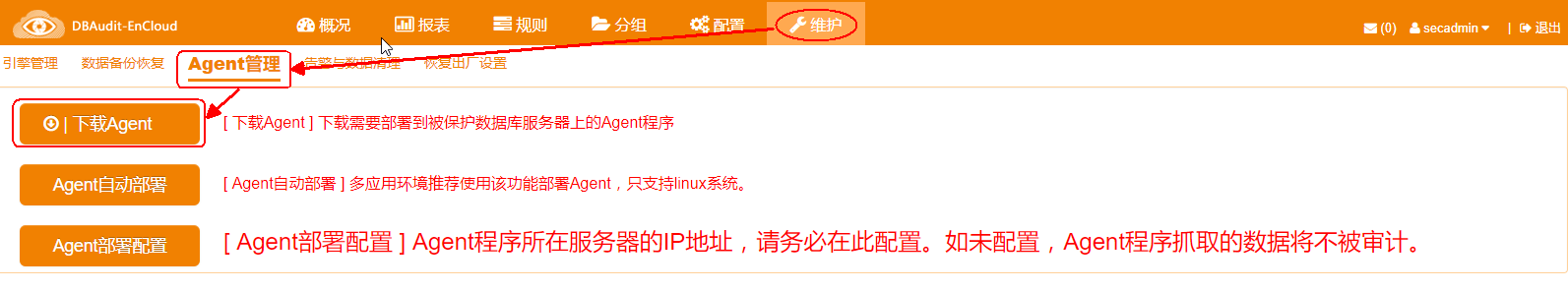


18、重新启动操作系统。

#### Linux系统部署

##### 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数据库审计系统，点击“维护”，选择“Agent管理”，然后点击 “下载Agent”图标，如下图所示。



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”。如下图所示。



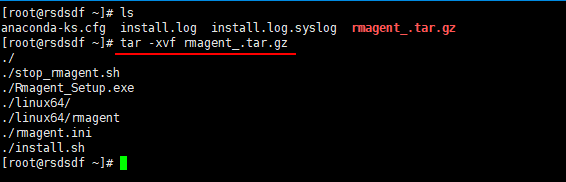
3、在弹出的“Agent部署配置”窗口输入需要部署Agent程序的服务器IP地址，然后点击“添加”，添加完成后，点击“关闭”。



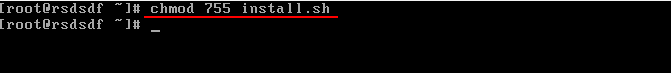
**注意：**

* 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。

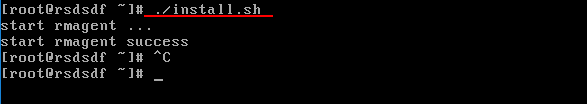
4、以root用户登录需要安装Agent程序的服务器，将rmagent.tar.gz文件上传到服务器，并将其解压缩。如下图所示。



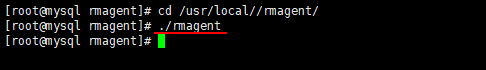
5、给install.sh文件增加权限。如下图所示。



6、安装Agent程序。如下图所示。

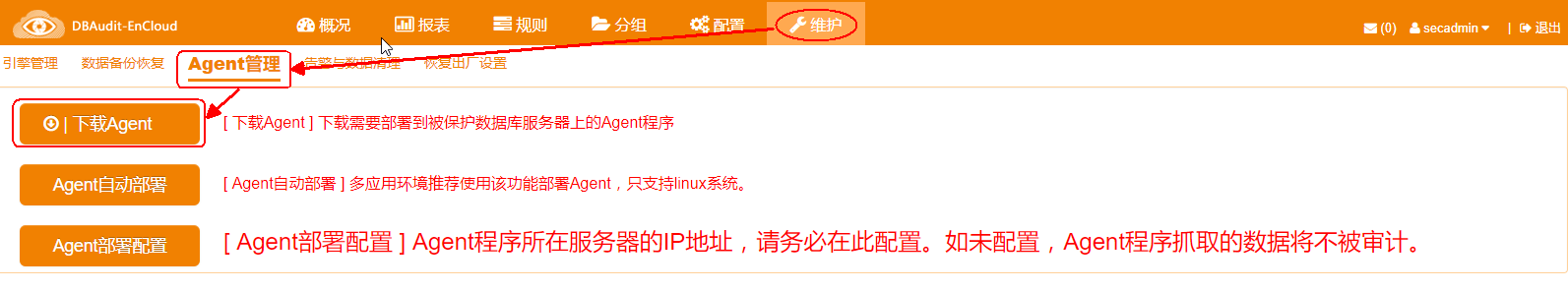


7、启动rmagent。



##### 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数据库审计系统，点击“维护”，选择“Agent管理”，然后点击 “下载Agent”图标，如下图所示。



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”。如下图所示。



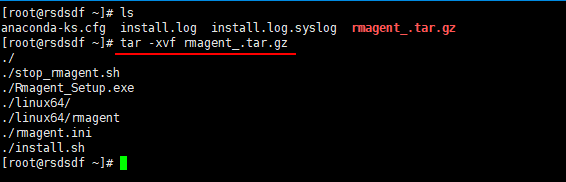
3、在弹出的“Agent部署配置”窗口输入需要部署Agent程序的服务器IP地址，然后点击“添加”，添加完成后，点击“关闭”。



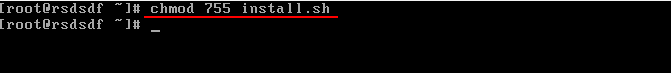
**注意：**

* 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。

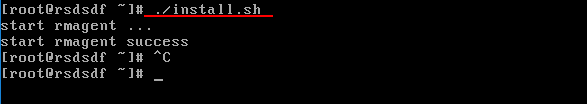
4、以root用户登录需要安装Agent程序的服务器，将rmagent.tar.gz文件上传到服务器，并将其解压缩。如下图所示。



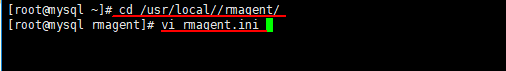
5、给install.sh文件增加权限。如下图所示。

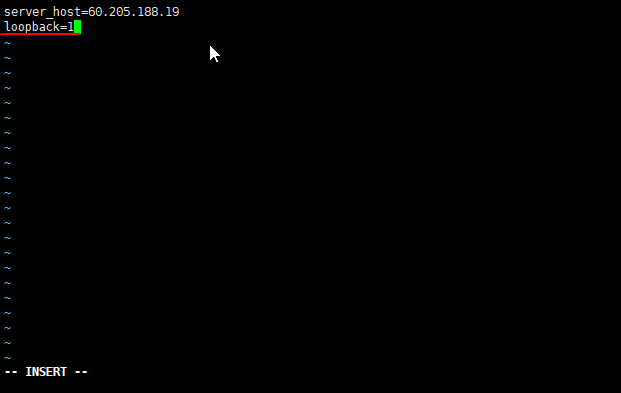


6、安装Agent程序。如下图所示。

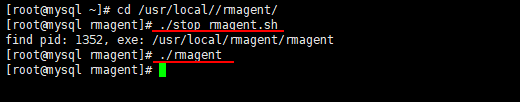


7、进入rmagent安装目录，使用VI编辑器修改rmagent.ini配置文件，如下图所示。



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

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。

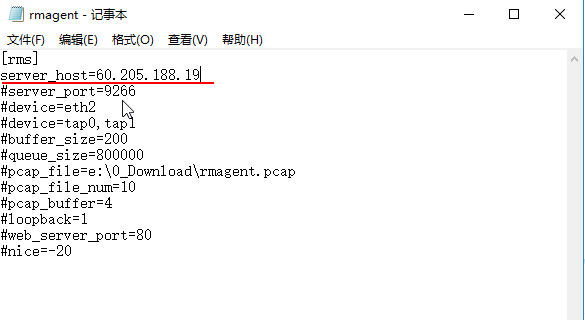


### Agent程序部署注意事项

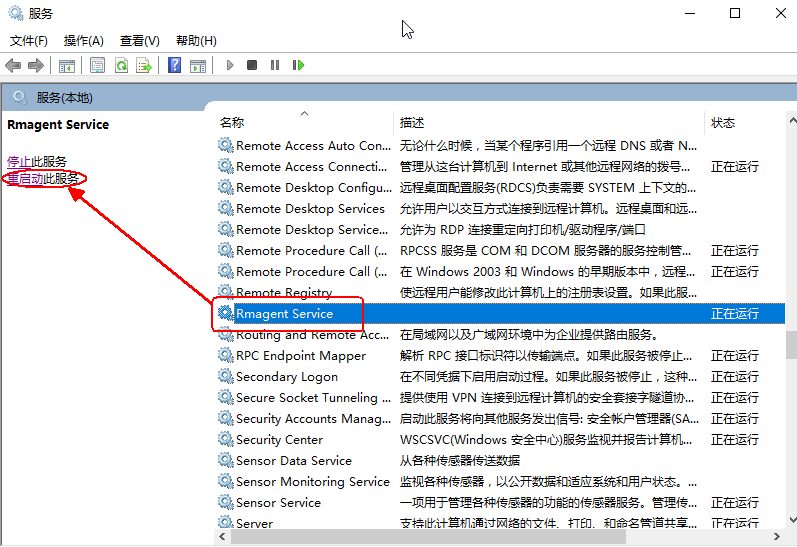
Agent程序默认连接云数据库审计系统的内网IP，如果部署Agent程序的服务器与云数据库审计系统通过外网连接则需要修改rmagent.ini中的IP地址。

#### 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，如下图所示。

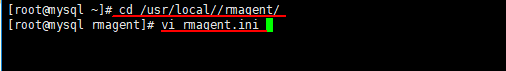


2、重新启动“rmagent”服务。打开“服务”管理器，选中“Rmagent Service”服务，然后点击左侧的“重启动此服务”，如下图所示。



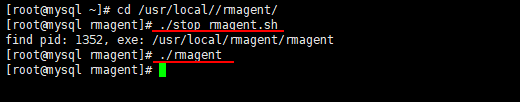
#### Linux系统

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



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。如下图所示。

3、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。



## 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。