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

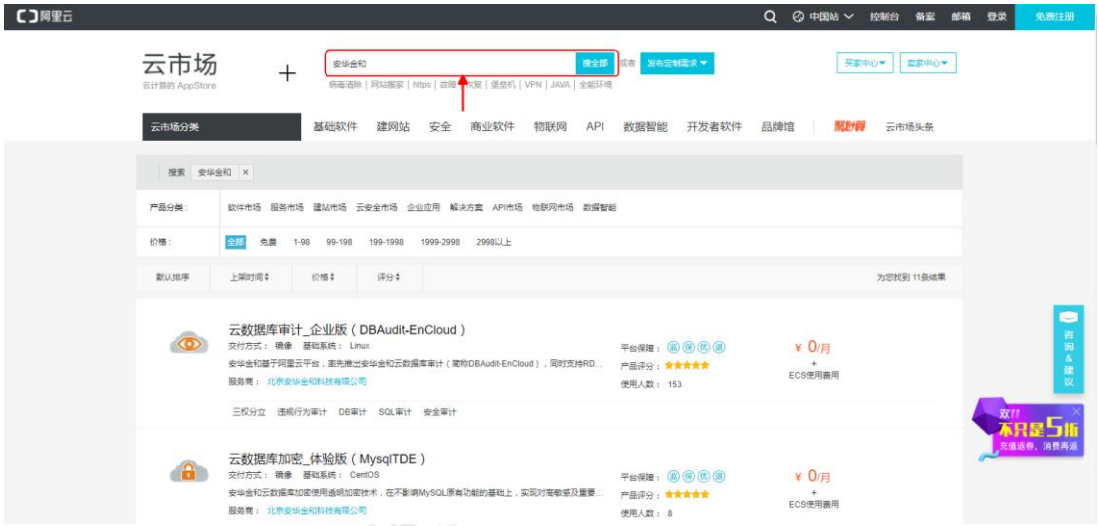
二〇一八年八月

版权申明

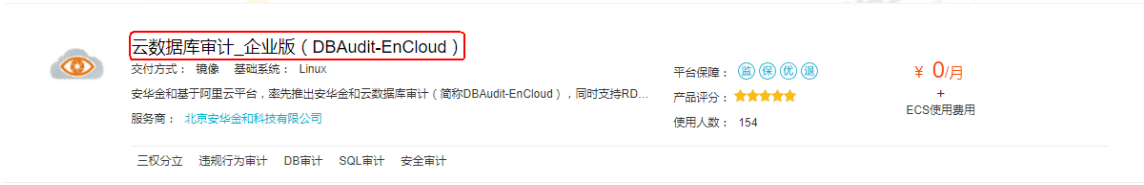
目　录

1.产品部署

1、 打开阿里云云市场，搜索“安华金和”，如下图所示。

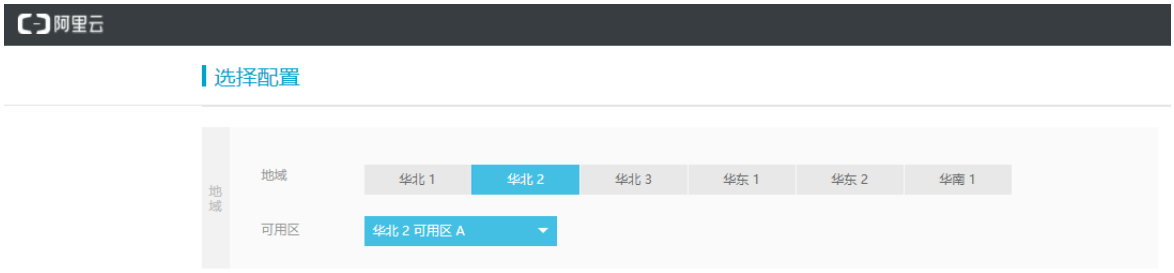


2、 在搜索结果中查找到需要购买的云数据库审计产品，然后点击该产品，如下图所示。



3、 在打开的产品详情页面中点击“立即购买”，如下图所示。

4、 在打开的 “选择配置”页面根据用户实际使用情况设置“地域”相关选项，如下图所示。



5、 在打开的“选择配置”页面选择需要购买的镜像版本，如下图所示。

说明：在选择镜像版本时需要与客服人员进行沟通，以确保所选择的版本是最新的。

6、 在打开的“选择配置”页面，设置云服务器相关配置。

第一步：设置网络类型，根据实际情况选择专有网络，如下图所示。

第二步：设置实例规格，根据所购买的产品规格选择相应的实例规格，产品规格说明详见下方“说明”部分内容。此处以企业版为例，选择 8 核 16G 的实例规格，如下图所示。

说明：产品规格、购买时长和配置需按以下要求进行选择。

序号	产品规格	购买方式	云服务器最低配置	价格
1	企业版	按年购买	CPU：8 核 内存：16G 数据盘：8T（建议数	咨询客服人员

			据盘初期选择 1T）	
2	专业版	按年购买	CPU：8 核 内存：32G 数据盘：10T（建议数据盘初期选择 2T）	咨询客服人员
3	旗舰版	按年购买	CPU：16 核 内存：32G 数据盘：20T（建议数据盘初期选择 5T）	咨询客服人员

第三步：设置公网带宽，根据用户实际情况设置“带宽”，如下图所示。

说明：如果被保护数据库与云数据库审计系统在同一个 VPC（专有网络）内，通过内网通信，且通过内网管理云数据库审计系统，则可选择不使用外网流量，在“带宽”项中设置为 0Mbps 即可。如果需要通过外网访问或管理云数据库审计系统，则需要购买外网流量，带宽建议设置为 5Mbps。

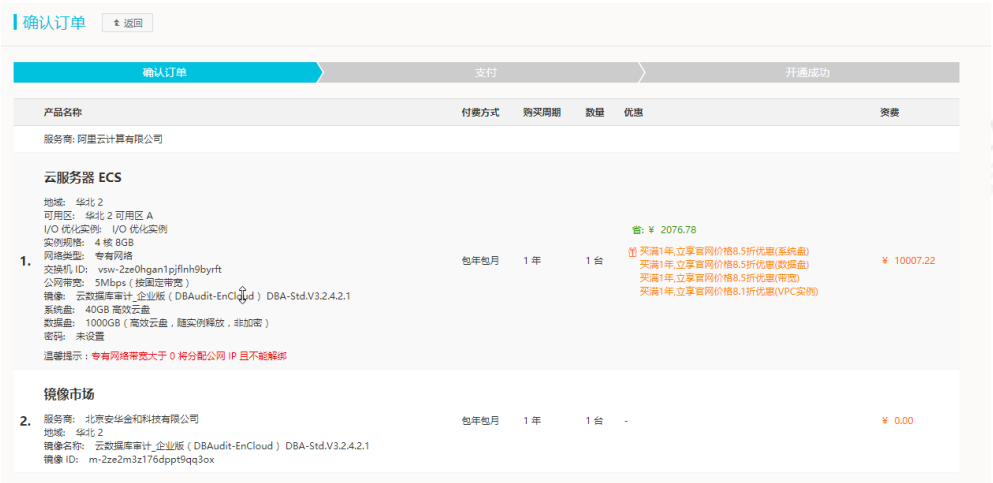
第四步：设置磁盘容量，系统盘默认即可，然后点击“增加一块”图标，添加一块类型为“高效云盘”的数据盘，根据所购买的产品规格设置相应的磁盘容量，产品规格相关内容详见第二步“说明”部分内容。此处以企业版为例，磁盘容量设置为 1000G，如下图所示。

7、 在打开的“选择配置”页面，设置购买量。根据所购买的产品规格，选择相应的付费方式和购买时长，产品规格相关内容详见第 6 步骤中的第二步“说明”部分内容。此处以企业版为例，选择付费方式为包月套餐，购买时长为 1 年，如下图所示。

说明：云数据库审计系统以提供镜像方式提供服务，镜像文件内部默认内置 7 天试用授权，用户可选择“按量”模式进行产品试用。

8、 在打开的“选择配置”页面右侧，勾选“同意《云服务器 ECS 服务条款》”，然后点击“立即购买”，如下图所示。

9、 在打开的“确认订单”页面，核对购买产品信息，如下图所示。



10、在打开的“确认订单”页面，设置云服务器 ECS 操作系统 root 账户的密码。然后点击“去下单”，如下图所示。

11、在打开的“支付”页面，选择支付方式，然后点击“确认支付”完成购买，如下图所示。

12、联系厂商客服人员获取 License 文件。

2.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
Agent	Web控制台	9266	Agent与Web控制台通讯端口
运维管理端	Web控制台	22	Web控制台SSH服务通讯端口

2.1 导入 License 文件

2.1.1 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：首次登录系统需要修改安全管理员默认密码。

2.1.2 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。

2.2 添加被审计数据库实例

2.2.1 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（secadmin）界面。

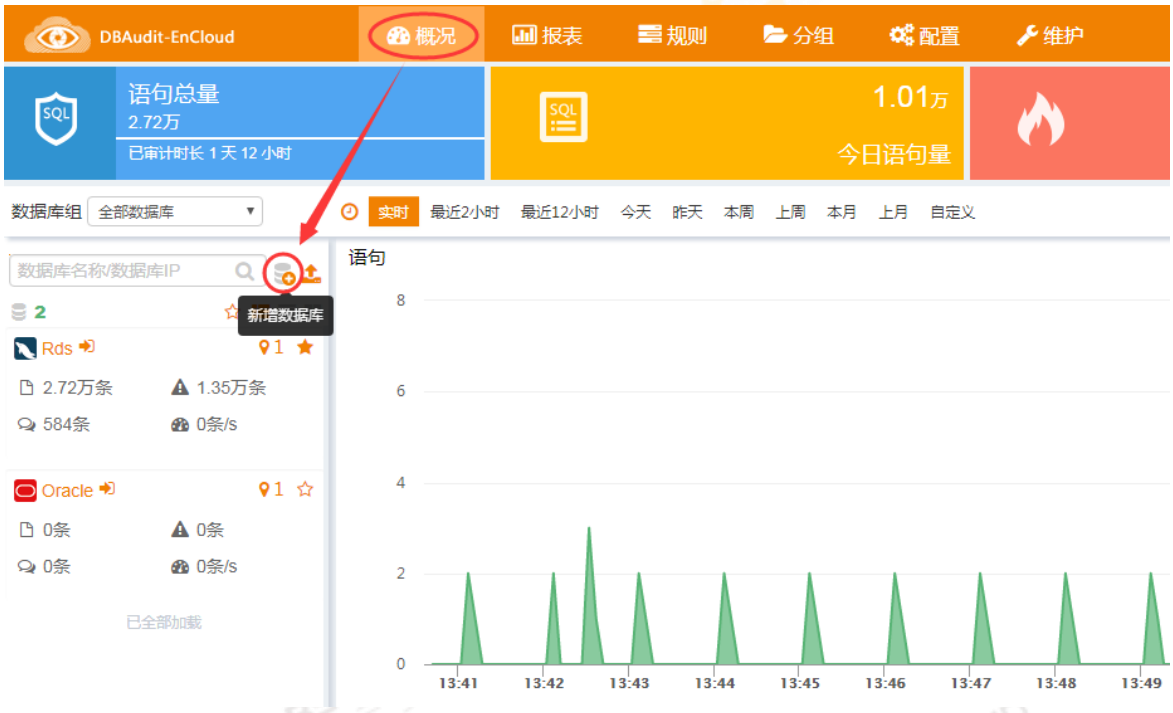
注意：首次登录系统需要修改安全管理员默认密码。

2.2.2 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：

2.2.2.1 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】，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：

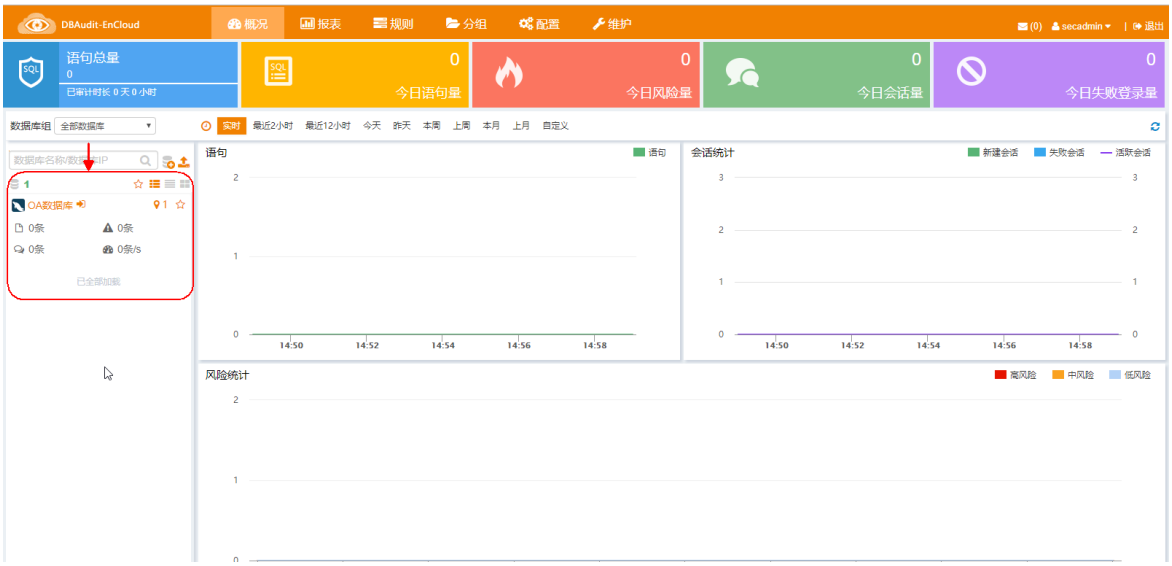


2、在弹出的“新增数据库”页面中填写要审计的数据库实例相关信息，然后点击“保存”。如下图所示：

注意事项：

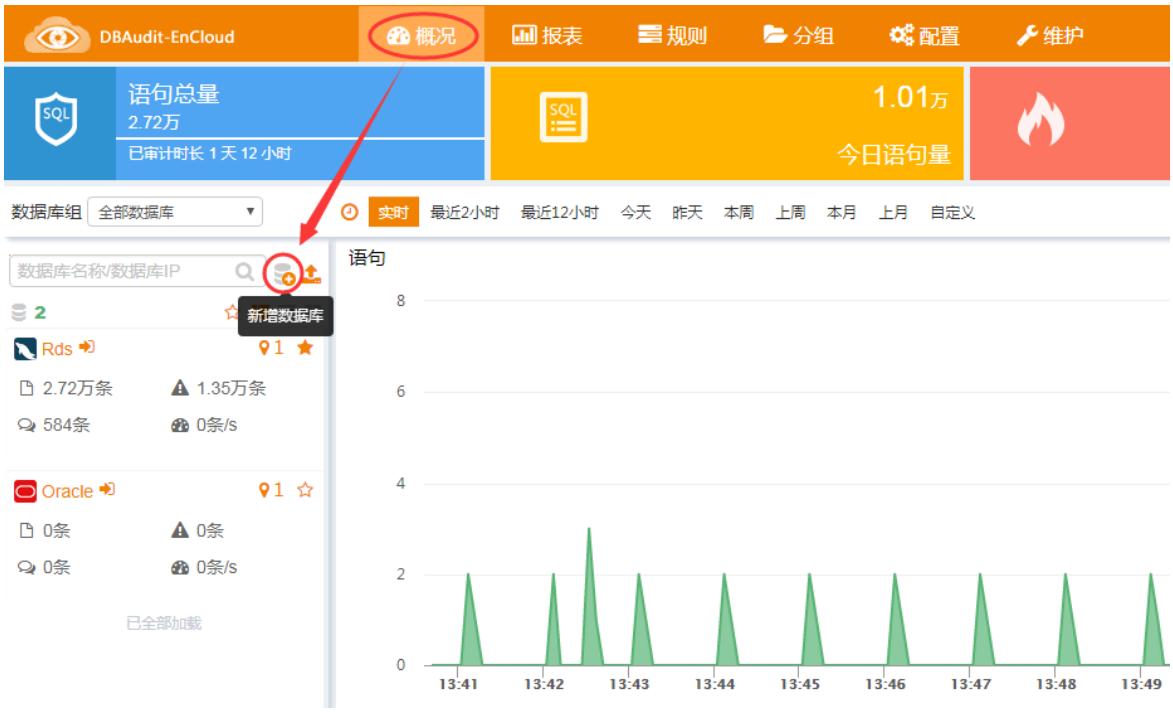
- 数据库名：为被审计数据库实例指定一个名字。
- 数据库类型：根据被审计数据库实例的类型选择。
- 数据库版本：可以手动选择或者点击【自动获取】输入数据库主机 IP、数据库主机端口、数据库实例名、用户名、密码，单击“确认”按钮，可以自动获取数据库版本，Oracle 数据库同时会获取到字符集。实例名：Oracle 与 Postgres 需要填写，其他数据库可以留空。
- IP 地址：被审计数据库实例的 IP 地址。
- 端口：被审计数据库实例的端口号。

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：

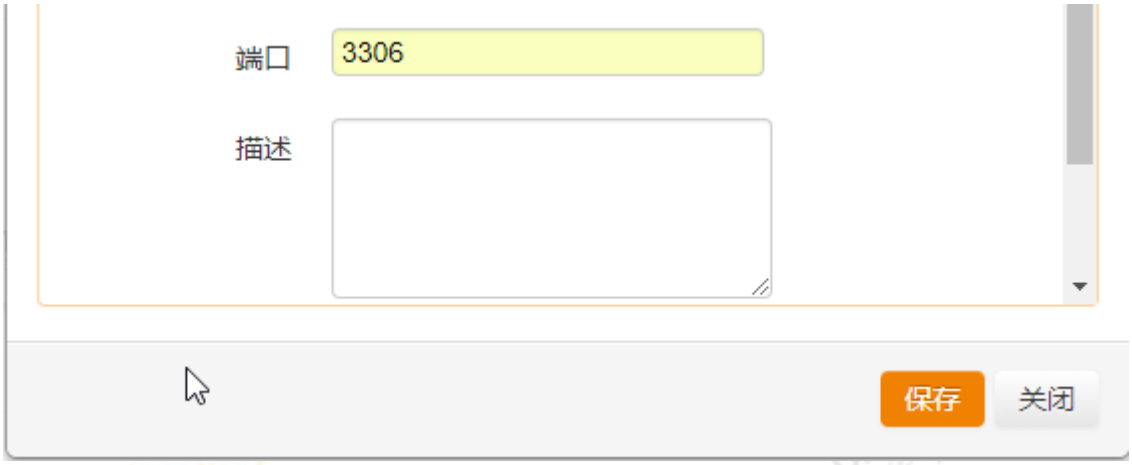


2.2.2.2 添加云服务商提供的数据库服务实例（如 RDS 数据库）

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：



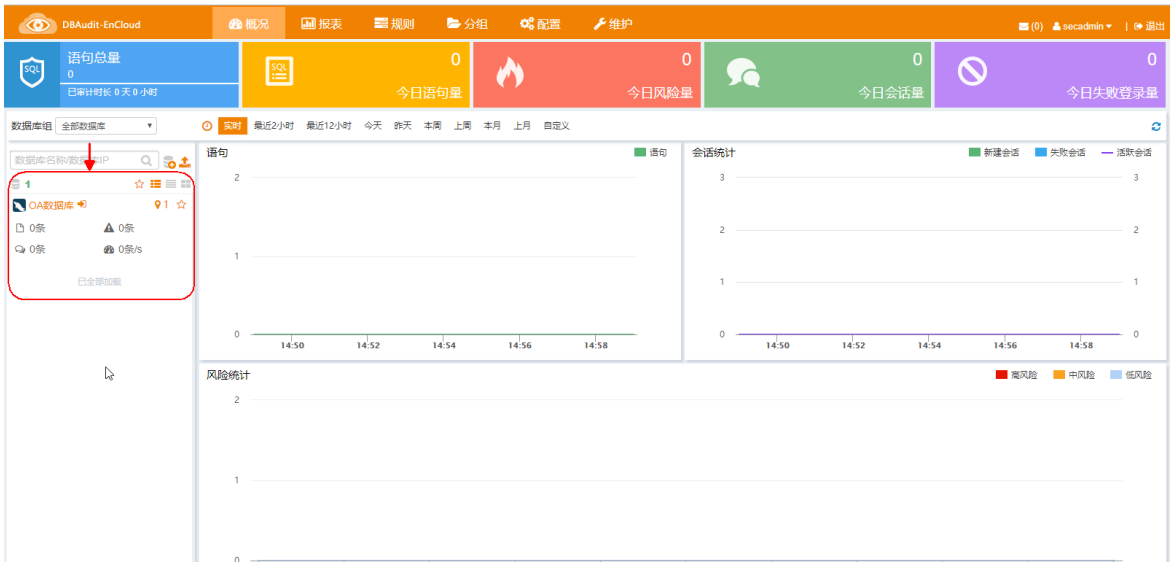
2、在弹出的“新增数据库”页面中填写要审计的数据库实例相关信息，然后点击“保存”。如下图所示：



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。



2.3 部署 Agent 程序

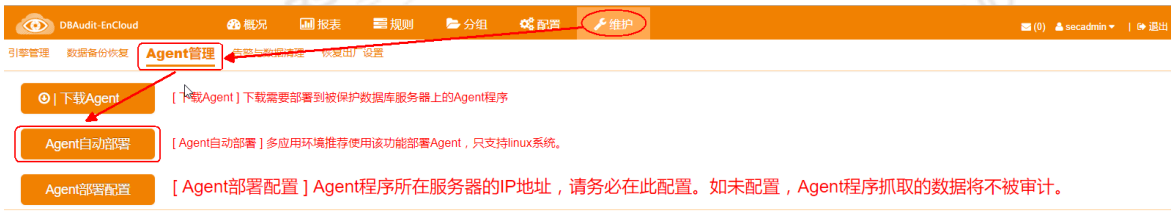
2.3.1 Agent 程序部署位置

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

2.3.2 Agent 程序自动部署（暂只支持 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。

2.3.3 Agent 程序手动部署

Window 平台，需要手动部署，Linux 平台，也可手动部署。操作细则另行提供。

2.4 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。