安华金和云数据库安全运维
接入文档

北京安华金和科技有限公司

二〇一七年十二月

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。

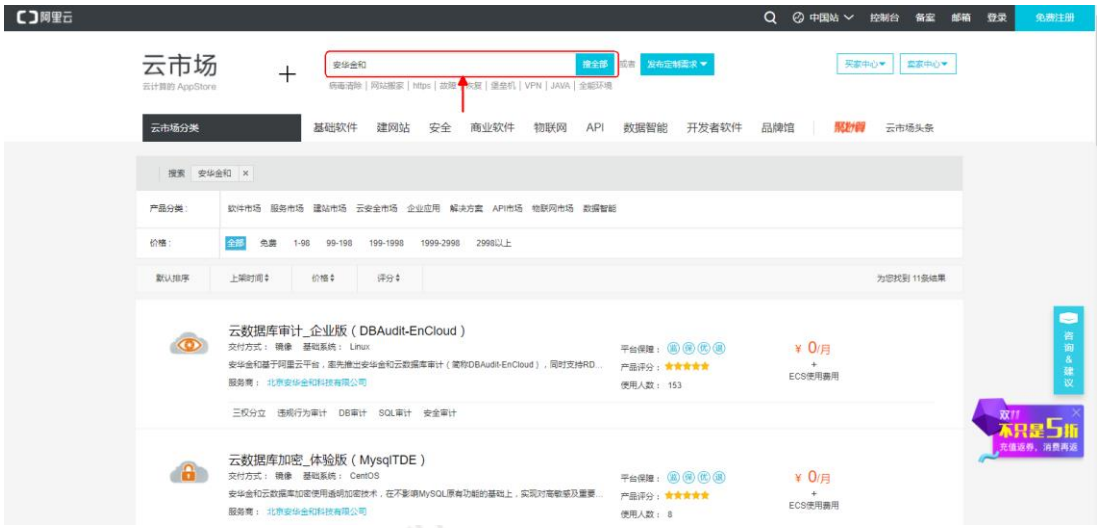
本文档及其描述的产品受有关法律的版权保护，对本文档内容的任何形式的非法复制，泄露或散布，需承担相应的法律责任。

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

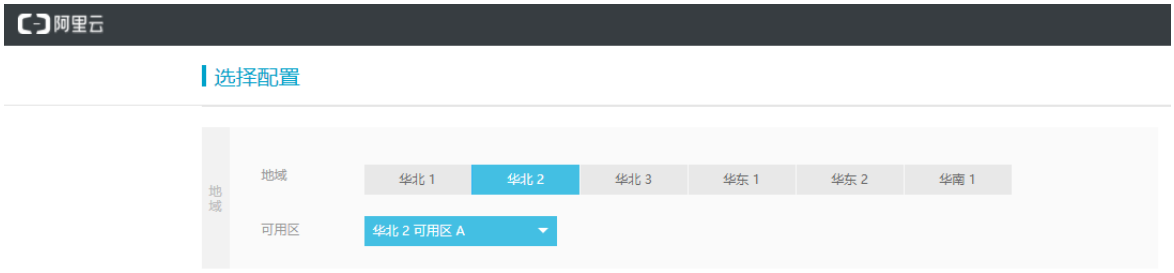
1、 打开阿里云云市场，搜索“安华金和”，如下图所示。



2、 在搜索结果中查找到需要购买的云数据库安全运维产品，然后点击该产品，如下图所示。

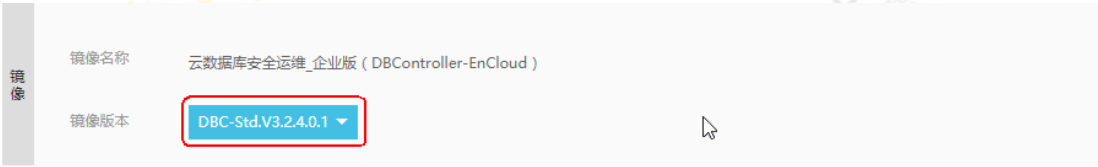
3、 在打开的产品详情页面中点击“立即购买”，如下图所示。

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	标准版	可按月或按年购买	CPU：4 核 内存：8G 数据盘：500G	云市场标示的价格

2	企业版	可按月或按年购买	CPU：8 核 内存：16G 数据盘：1T	咨询客服人员
3	专业版	可按月或按年购买	CPU：8 核 内存：16G 数据盘：1T	咨询客服人员
4	旗舰版	可按月或按年购买	CPU：16 核 内存：32G 数据盘：3T	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安全运维系统在同一个 VPC（专有网络）内，通过内网通信，且通过内网管理云数据库安全运维系统，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安全运维系统，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：云数据库安全运维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。

说明：云数据库安全运维标准版镜像内置 1 年 License 授权，购买后即可正常使用，其他版本需与厂商客服人员联系获取 License 文件。

2.产品初始化

说明：在系统使用之前需要在安全组中开放以下端口：

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
运维人员终端	Web控制台	10000-11000	此处端口需根据2.2.2章节所设置的具体端口号开放。
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://云数据库安全运维系统 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系统管理员默认密码。

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”， 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 设置代理端口

2.2.1 登录系统管理员界面

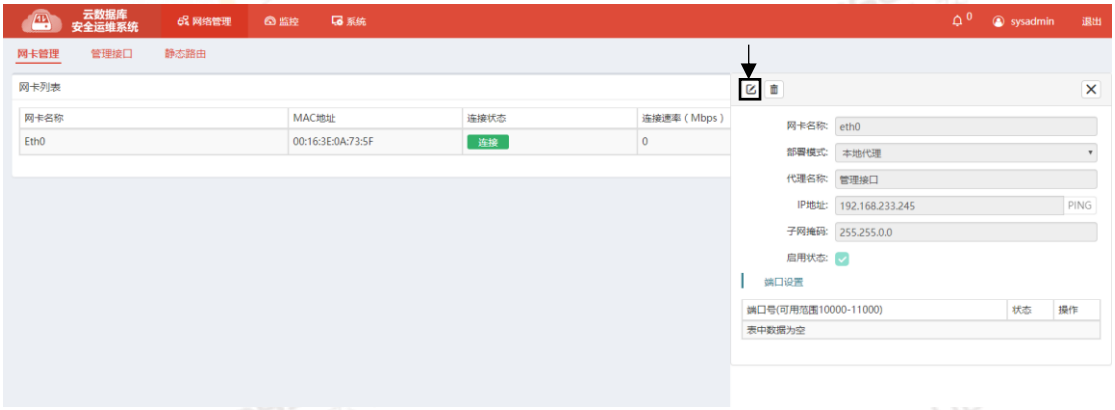
1、打开 IE 或其他浏览器，在地址栏内输入 https://云数据库安全运维系统 IP 地址。进入登录页面后，输入用户名：sysadmin 默认密码：sysadmin1234，点击【登录】进入系统管理员（sysadmin）界面。

2.2.2 添加代理端口

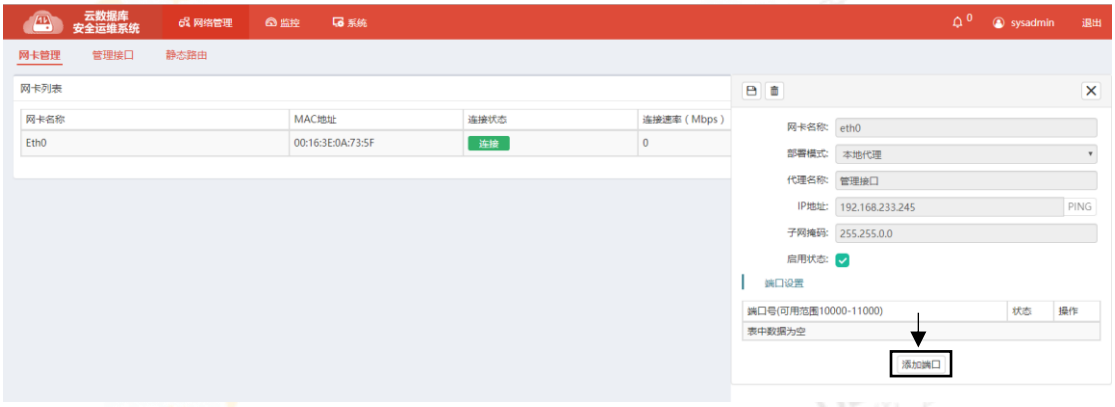
1、进入系统管理员界面后点击【网络管理】->【网卡管理】，进入网卡列表页，如下图所示。

2、在网卡列表中点击“查看代理端口”图标，如下图所示。

3、在打开的代理组页面，点击“编辑”图标，如下图所示。

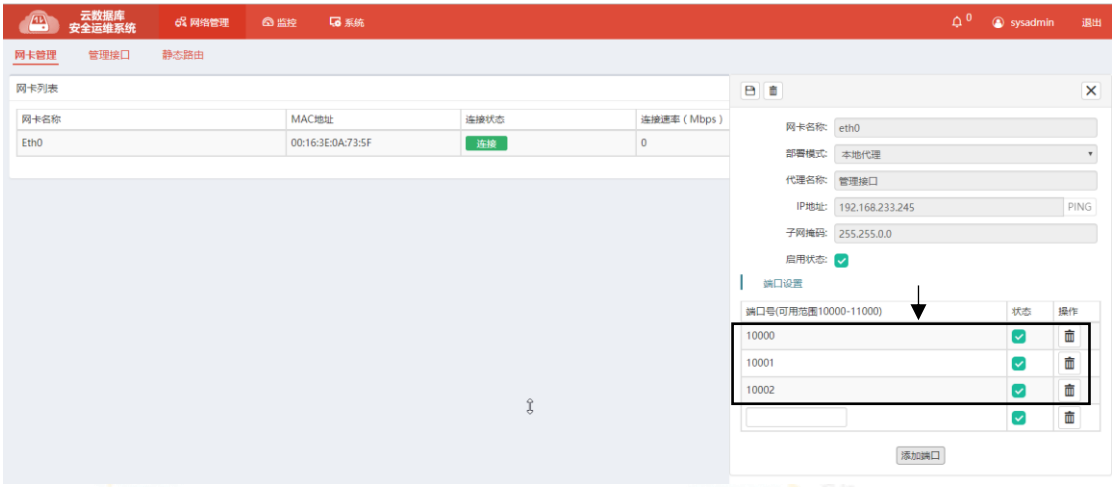


4、进入端口设置界面，点击“添加端口”图标，如下图所示。

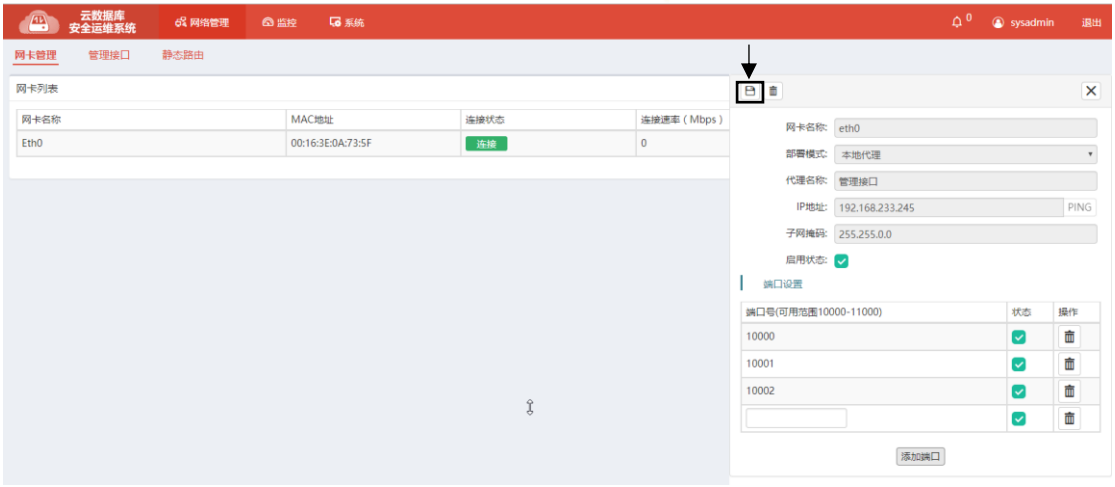


5、在“端口设置”页中输入可用的端口号，如下图所示。

注意：可以添加多个端口号，每个端口号对应一个被保护的数据库实例，端口号可用范围为：10000-11000



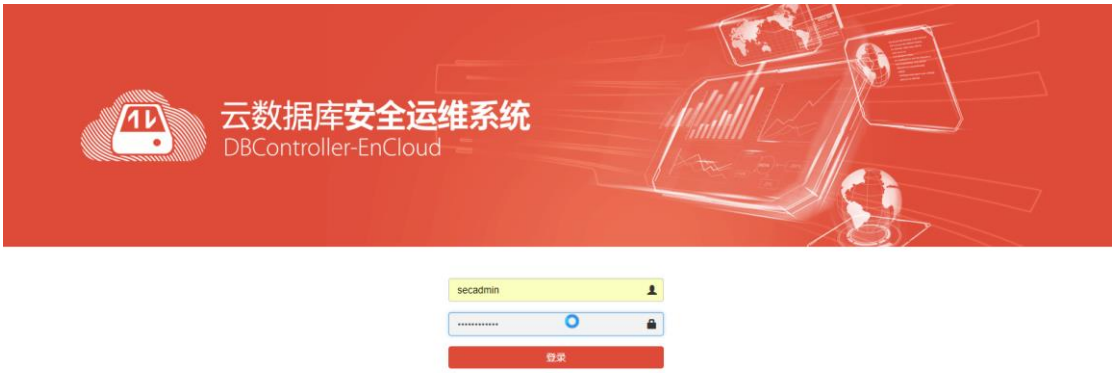
6、点击“保存”图标，完成添加代理端口，如下图所示。



2.3 添加被保护数据库实例

2.3.1 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://云数据库安全运维系统 IP 地址。进入登录页面后，输入用户名：secadmin 默认密码：secadmin1234，见下图所示：



注：首次登录系统需要修改安全管理员默认密码。

2.3.2 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防护。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：

2.3.2.1 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【配置】->【数据库】，进入数据库列表页，然后点击“增加数据库”图标，如下图所示。

2、在弹出“添加数据库”页面中填写被保护的数据库实例相关信息。如下图所示。

注意：

1、Oracle 数据库需要正确选择该数据库所使用的字符集，其他数据库不需要设置。

2、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。

3、防护状态：云数据库安全运维系统默认保护模式为学习模式，并且默认 7 天后自动切换为保护模式。学习模式下所有的数据库访问行为都将被放行。即使命中了规则，语句也不会被阻断，以保证业务系统的正常行为，但系统会记录下所有的 SQL 语句,同时也将记录下语句被哪些策略所命中。学习模式下脱敏规则仍会正常执行。系统默认 7 天为一个学期周期，学习期满自动切换至保护模式。也可在此直接设置为保护模式，但是不建议这样设置，因为直接进入保护模式系统就无法建立应用系统的特征模型，很可能使正常的应用系统行为被误判，导致被中断会话或拦截。建议按照应用系统使用的周期来设置学习模式的学习周期。

3、在“网络设置”页中输入被保护数据库实例 IP 址和端口号，“代理组”列中选择“管理接口”和“端口号”，如下图所示：

4、点击“操作”列中的“保存”图标，如下图所示：

5、点击“保存”图标，如下图所示：

2.3.2.2 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【配置】->【数据库】，进入数据库列表页，然后点击“增加数据库”图标，如下图所示。

2、在弹出“添加数据库”页面中填写被保护的数据库实例相关信息。如下图所示。

注意：

1、Oracle 数据库需要正确选择该数据库所使用的字符集，其他数据库不需要设置。

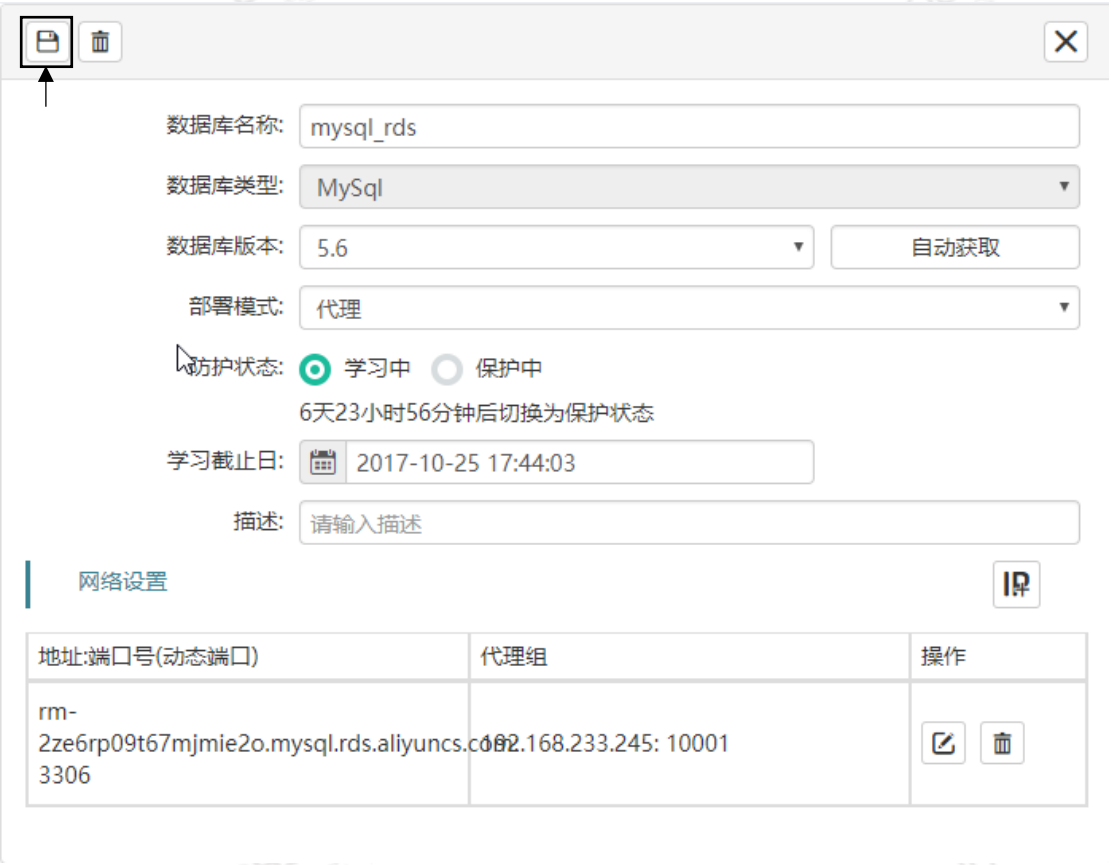
2、点击【自动获取】输入数据库主机 IP、数据库主机端口、数据库实例名、用户名、密码，单击“确认”按钮，可以自动获取数据库版本，Oracle 数据库同时会获取到字符集。

3、防护状态：云数据库安全运维系统默认保护模式为学习模式，并且默认 7 天后自动切换为保护模式。学习模式下所有的数据库访问行为都将被放行。即使命中了规则，语句也不会被阻断，以保证业务系统的正常行为，但系统会记录下所有的 SQL 语句,同时也将记录下语句被哪些策略所命中。学习模式下脱敏规则仍会正常执行。系统默认 7 天为一个学期周期，学习期满自动切换至保护模式。也可在此直接设置为保护模式，但是不建议这样设置，因为直接进入保护模式系统就无法建立应用系统的特征模型，很可能使正常的应用系统行为被误判，导致被中断会话或拦截。建议按照应用系统使用的周期来设置学习模式的学习周期。

3、在“网络设置”页中的“地址：端口号（动态端口）”列中输入被保护云服务商提供的数据库服务（如 RDS 数据库）实例的连接字符串域名和端口号，“代理组”列中选择“管理接口”和“端口号”，如下图所示。

4、点击“操作”列中的“保存”图标，如下图所示。

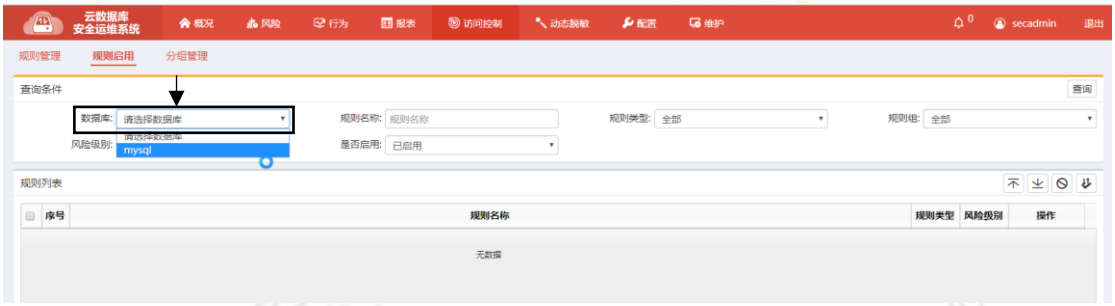
5、点击“保存”图标，如下图所示。



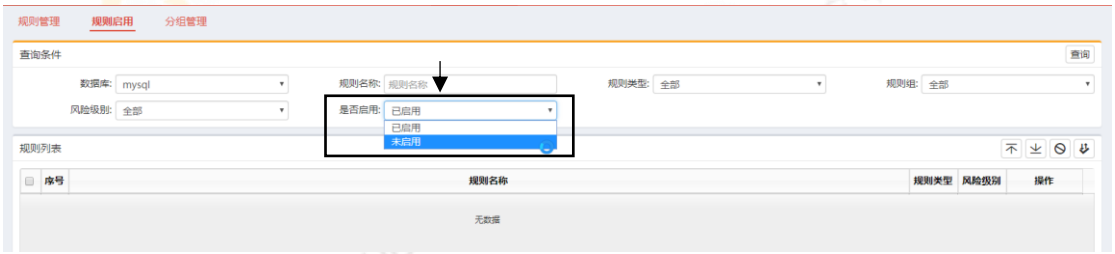
2.3.3 设置访问控制规则

1、点击【访问控制】->【规则启用】，进入规则列表页，如下图所示。

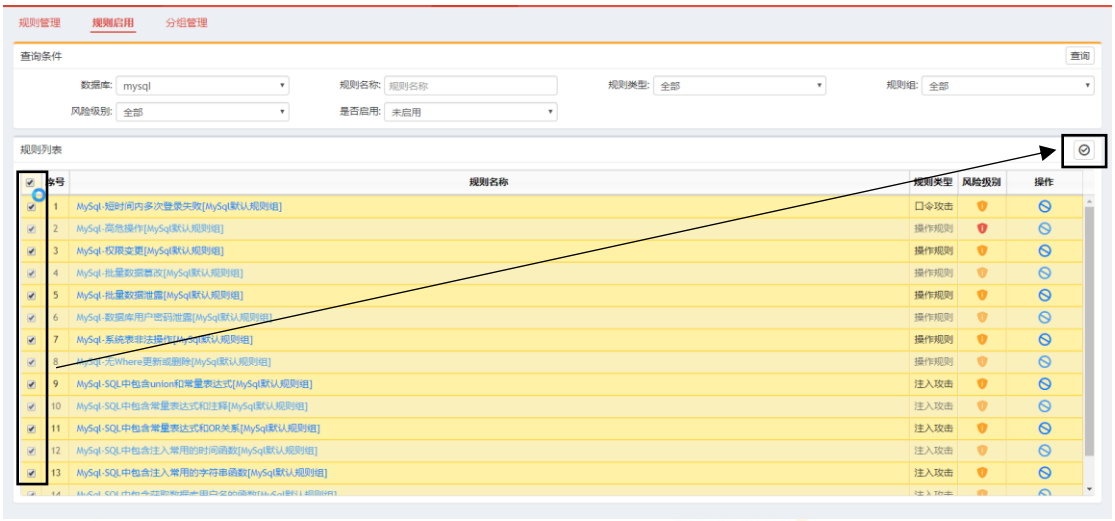
2、在“查询条件”页的“数据库”选项中选择被保护的数据库实例，如下图所示。



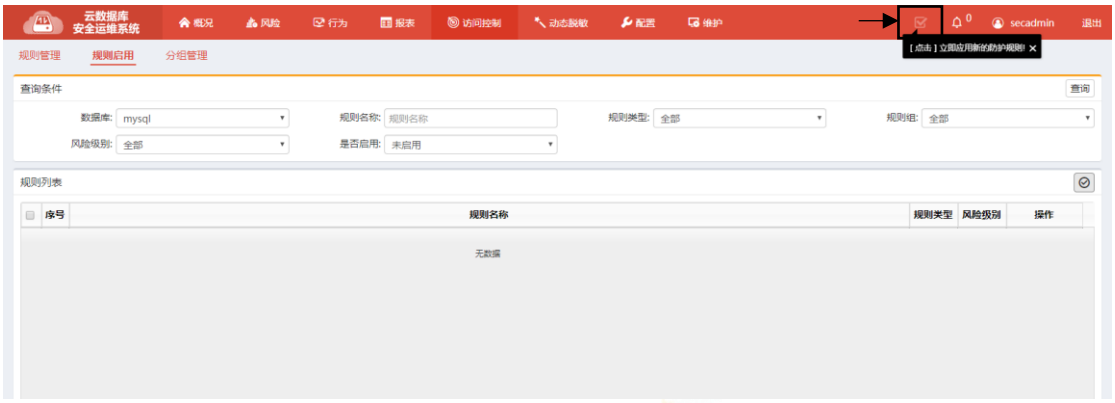
3、然后在“是否启用”选项中选择“未启用”，如下图所示。



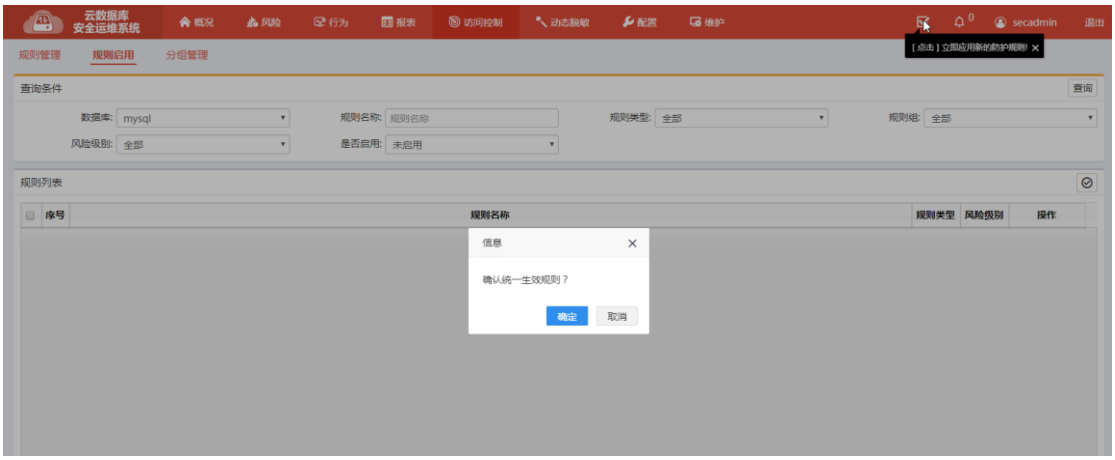
4、在“规则列表”页中即会显示未启用的系统默认规则，然后选择需要启用的规则，点击“启用”图标，如下图所示。



5、点击“立即应用新的防护规则”图标，如下图所示：

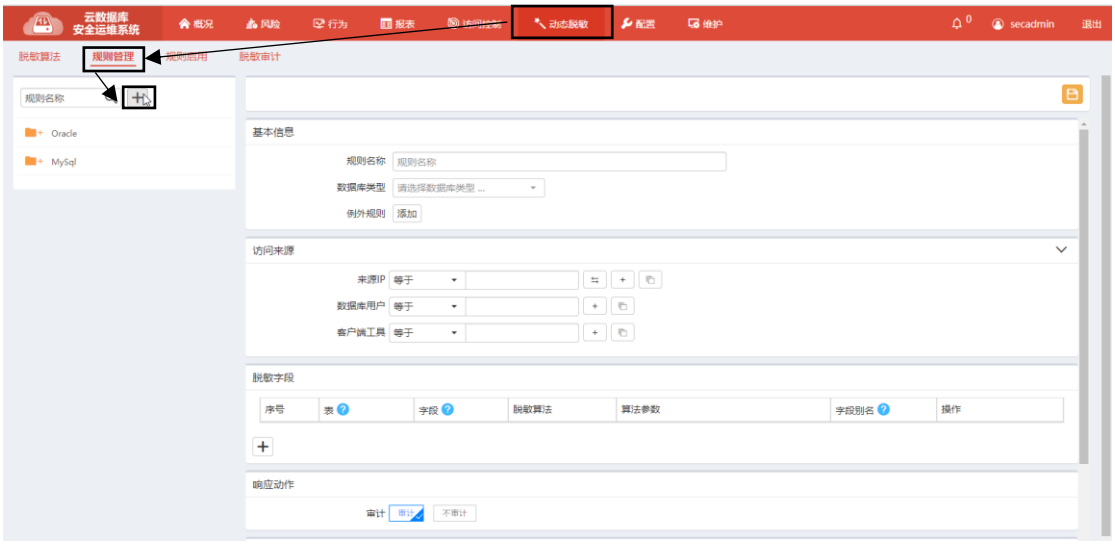


6、在弹出的窗口中点击“确定”，如下图所示。

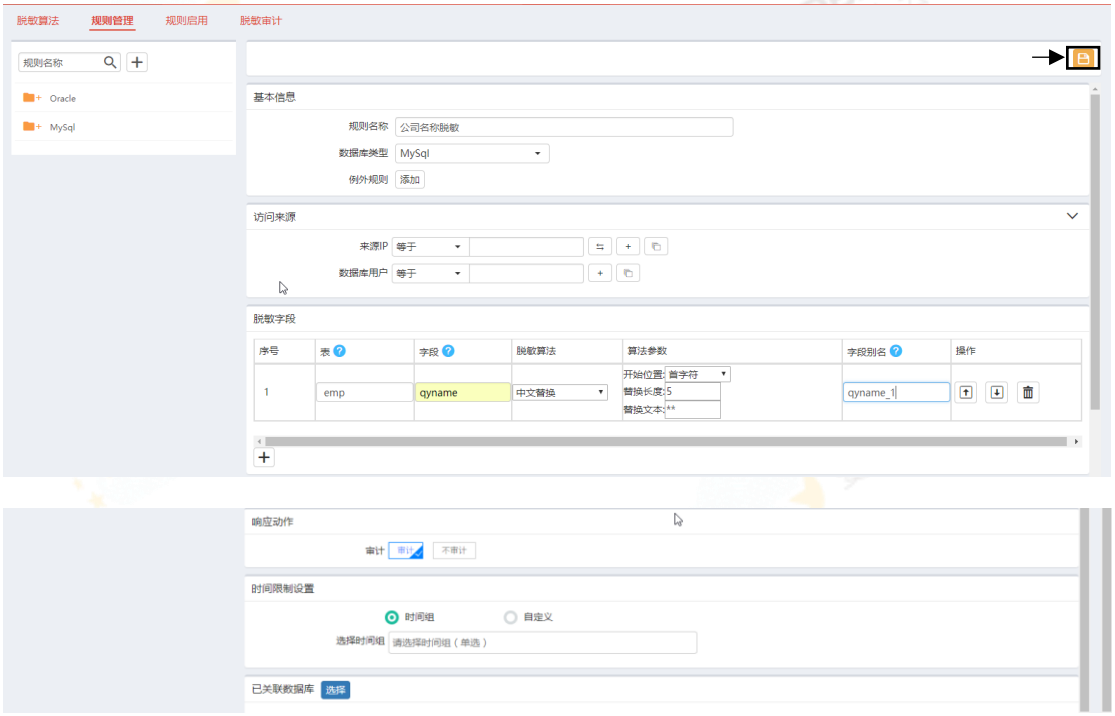


2.3.4 设置动态脱敏规则

1、点击【动态脱敏】->【规则管理】，点击“新建规则”图标，进入规则设置页面，如下图所示。



2、输入规则名称，选择数据库类型，设置访问来源，添加需要脱敏的数据库表字段并配置脱敏算法及算法参数。设置响应动作及时间限制。然后点击“保存”图标。如下图所示。

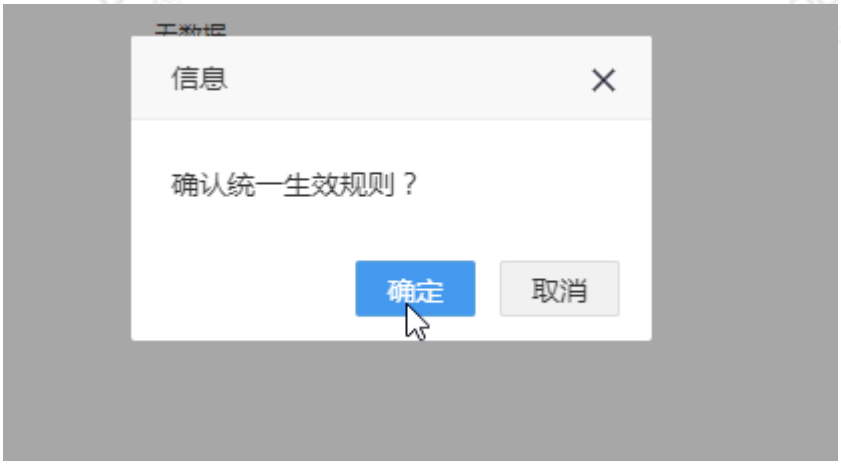


3、点击【动态脱敏】->【规则启用】，进入规则启用页面，如下图所示。

4、在“查询条件”项的“数据库”选项中选择被保护的数据库实例，在“是否启用”选项中选择“未启用”，然后在“规则列表”页中即会显示未启用的规则，然后选择需要启用的规则，点击“启用”图标，如下图所示。

5、点击“立即应用新的防护规则”图标，如下图所示。

6、在弹出的窗口上点击“确定”，如下图所示。



2.3.5 部署测试

使用 Navicat 等客户端工具，配置连接信息，将连接到数据库的 ip 和端口指定为代理组的 ip 和端口，通过代理转发的方式访问数据库。执行相关操作，查看防护效果。

注意：客户端工具必须连接代理服务器，而不是原数据库。原则上原数据库应该不允许代理服务器及应用系统之外的地址访问。