安华金和云数据库防火墙
接入文档

北京安华金和科技有限公司

二〇一九年一月

版权申明

目　录

1. 产品部署 4

2. 产品初始化 9

2.1 导入 LICENSE 文件 9

2.1.1 登录系统管理员界面 9

2.1.2 导入 License 文件 10

2.2 设置代理端口 11

2.2.1 登录系统管理员界面 11

2.2.2 添加代理端口 11

2.3 配置集群 13

2.3.1 负载均衡配置 13

2.3.2 分区管理 14

2.3.3 节点管理 15

2.4 KERNEL 节点配置 16

2.5 添加被保护数据库实例 19

2.5.1 登录安全管理员界面 19

2.5.2 添加被保护数据库实例 19

2.6 设置虚拟补丁规则 24

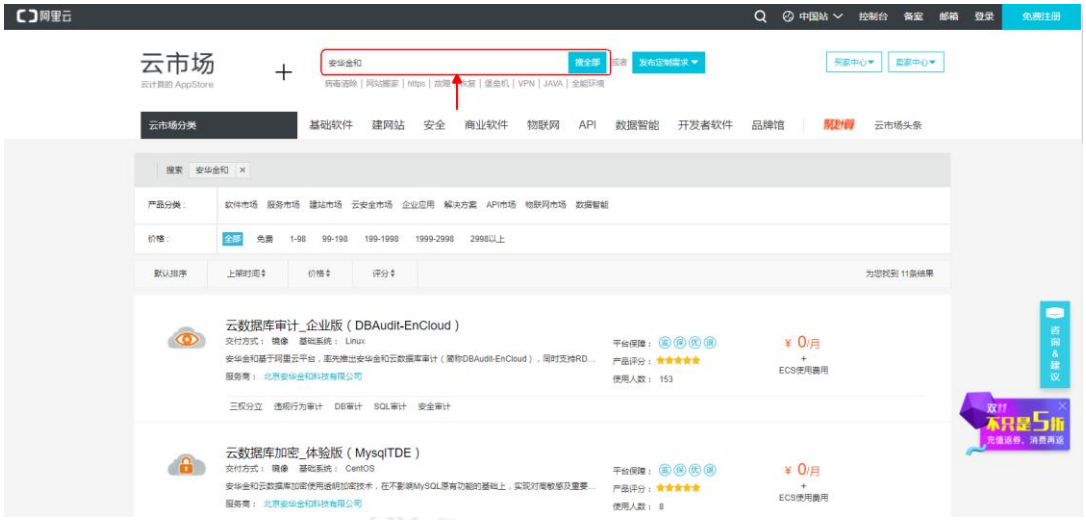
2.7 设置防火墙规则 26

2.8 配置负载均衡 28

2.9 部署测试 30

1.产品部署

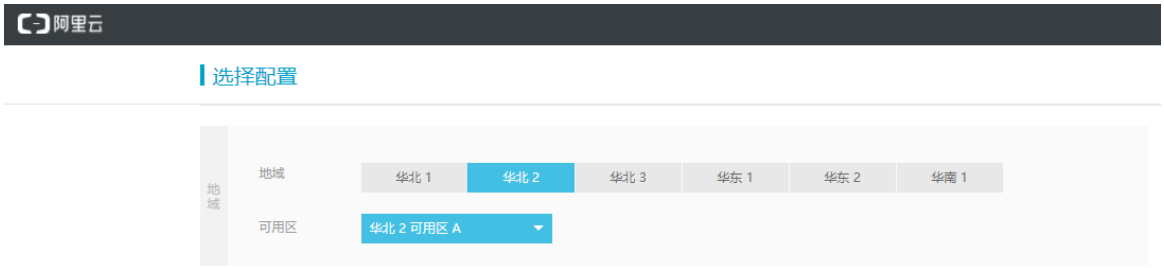
1、 打开阿里云云市场，搜索“安华金和”，如下图所示。



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

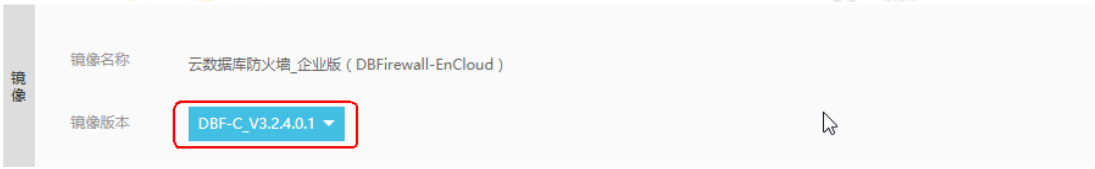
3、 在打开的产品详情页面中点击“立即购买”，如下图所示。

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，防火墙高可用版需要购买一个管理端和两个节点共三个实例，产品规格说明详见下方“说明”部分内容。此处以企业版中一台实例的购买为例，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	默认 1 年	CPU：4 核 内存：8G	云市场标示的价格

			数据盘：1T	
2	企业版	按年购买	CPU：8 核 内存：16G 数据盘：2T	咨询客服人员
3	专业版	按年购买	CPU：16 核 内存：32G 数据盘：4T	咨询客服人员
4	旗舰版	按年购买	CPU：16 核 内存：64G 数据盘：8T	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防火墙系统在同一个 VPC（专有网络）内，通过内网通信，且通过内网管理云数据库防火墙系统，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防火墙系统，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 2000G，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：云数据库防火墙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：云数据库防火墙标准版镜像内置 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。

节点	端口	备注
管理控制台（Manager）	443	Web控制台HTTPS服务通讯端口
管理控制台（Manager）、集群节点（Kernel）	22	Web控制台SSH服务通讯端口
集群节点（Kernel）	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。
管理控制台（Manager）	9901、9311、9207	应用服务器管理端和节点之前的通信端口
集群节点（Kernel）	9301	健康检查端口

2.1 导入 License 文件

2.1.1 登录系统管理员界面

1、打开 Google Chrome 或 Firefox 浏览器，在地址栏内输入 https://云数据库防火墙系统管理节点 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。

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

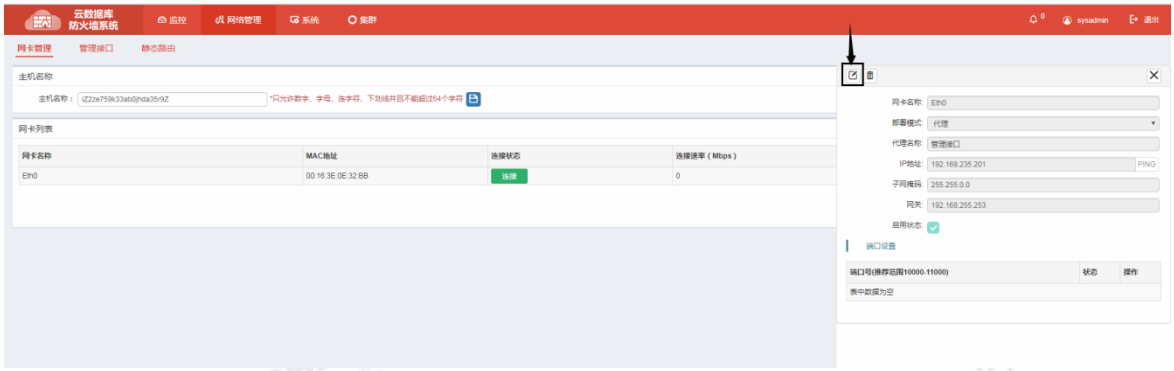
1、打开 Google Chrome 或 Firefox 浏览器，在地址栏内输入 https://云数据库防火墙系统管理节点 IP 地址。进入登录页面后，输入用户名：sysadmin 默认密码：sysadmin1234，点击【登录】进入系统管理员界面。

2.2.2 添加代理端口

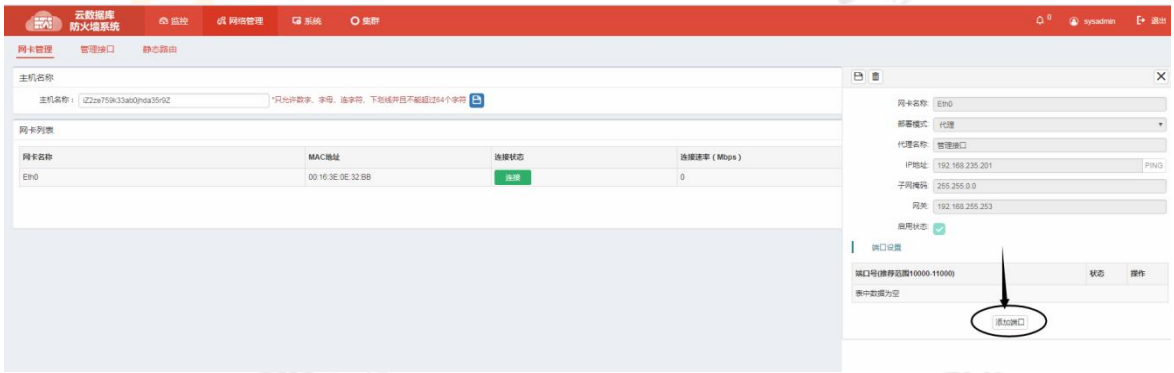
1、进入系统管理员界面后点击【网络管理】->【网卡管理】，进入网卡列表页，如下图所示。

2、然后点击“查看代理端口”图标，如下图所示。

3、进入代理组页面，点击“编辑”图标，如下图所示。

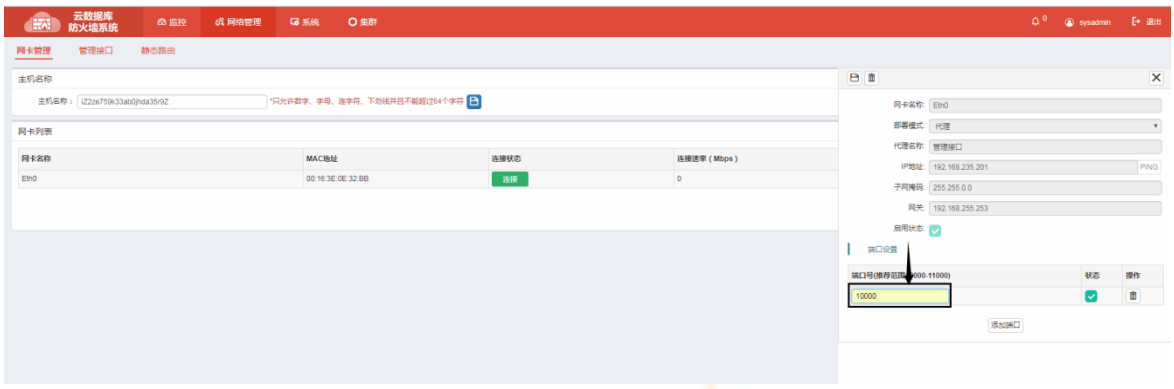


4、进入端口设置界面，点击“添加端口”图标，如下图所示。

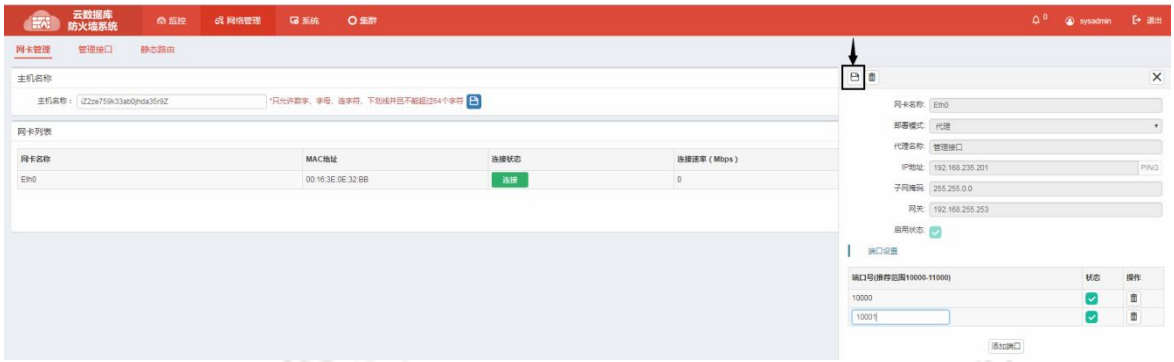


5、在“端口设置”页中输入可用的端口号，如下图所示。

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。



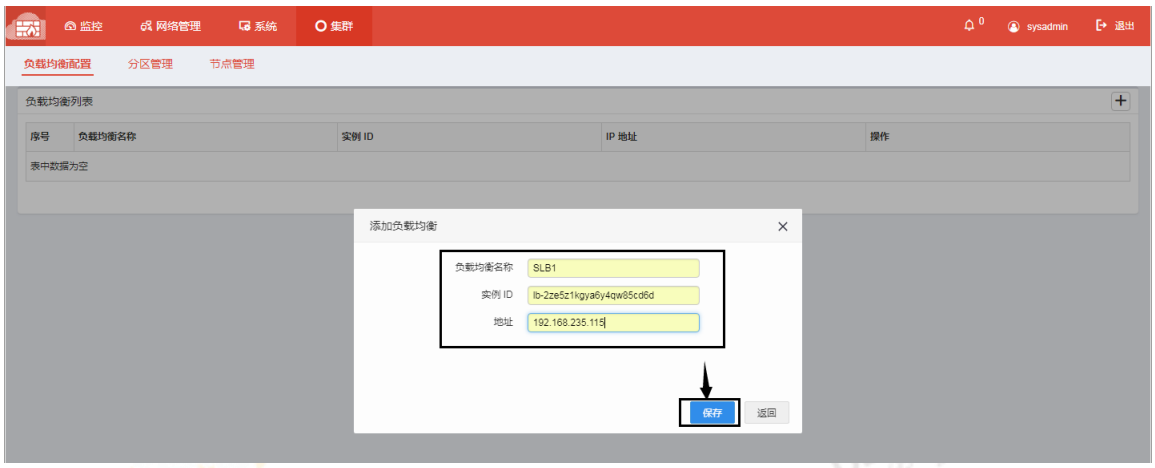
2.3 配置集群

2.3.1 负载均衡配置

1、进入系统管理员界面后点击【集群】->【负载均衡配置】，如下图所示。

2、点击“添加”按钮图标，如下图所示。

3、在弹出的“添加负载均衡”页，添加负载均衡相关信息，并保存，如下图所示。

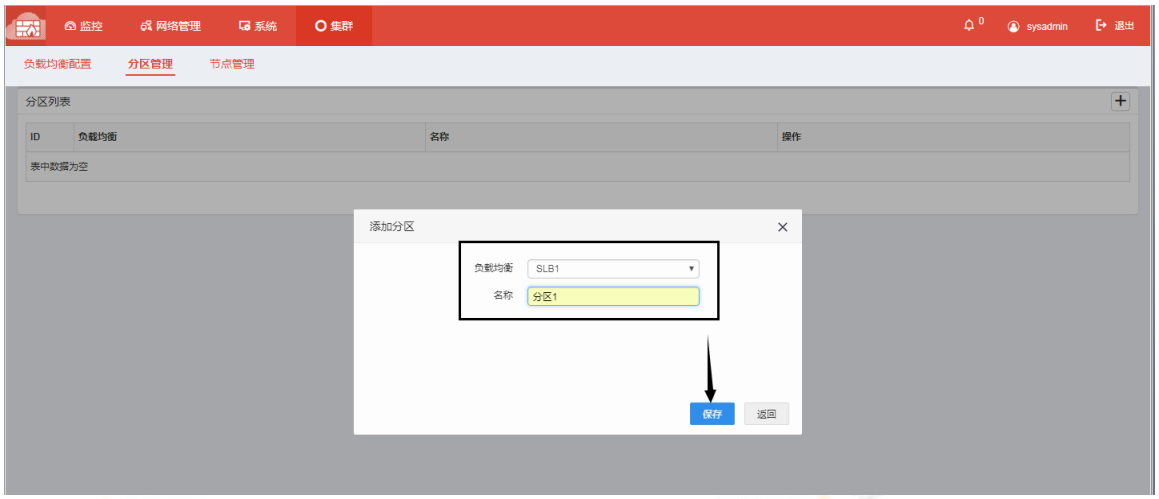


2.3.2 分区管理

1、进入系统管理员界面后点击【集群】->【分区管理】，如下图所示。

2、点击“添加”按钮图标，如下图所示。

3、在弹出的“添加分区”页，选择负载均衡，并输入分区名称，保存，如下图所示。



2.3.3 节点管理

1、进入系统管理员界面后点击【集群】->【节点管理】，如下图所示。

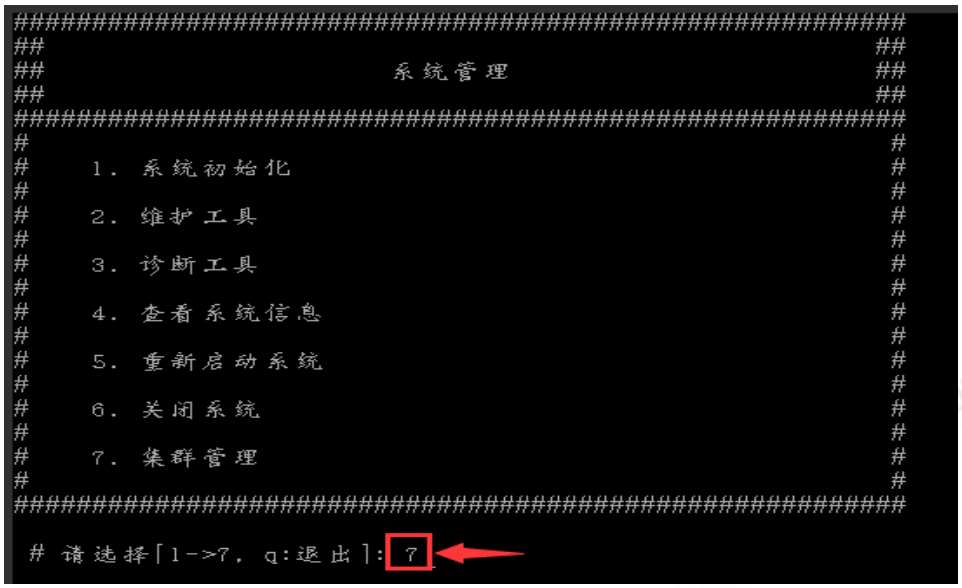
2、点击“添加”按钮图标，如下图所示。

3、在弹出的“添加节点”页，输入节点的实例 ID，选择负载均衡、分区，输入节点的 IP 地址，保存，如下图所示。

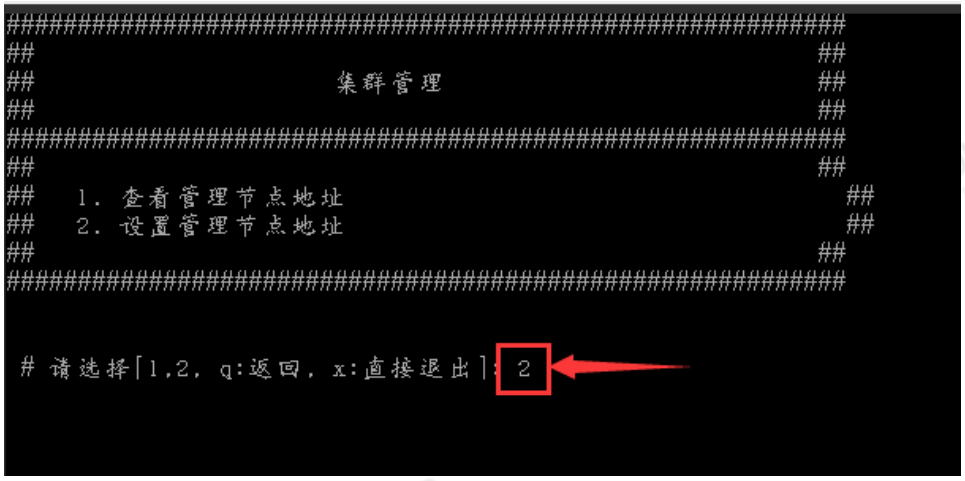
2.4 kernel 节点配置

1、通过阿里云控制台远程连接到 kernel 节点后台，输入后台用户名，密码，进入系统管理界面，如下图所示。

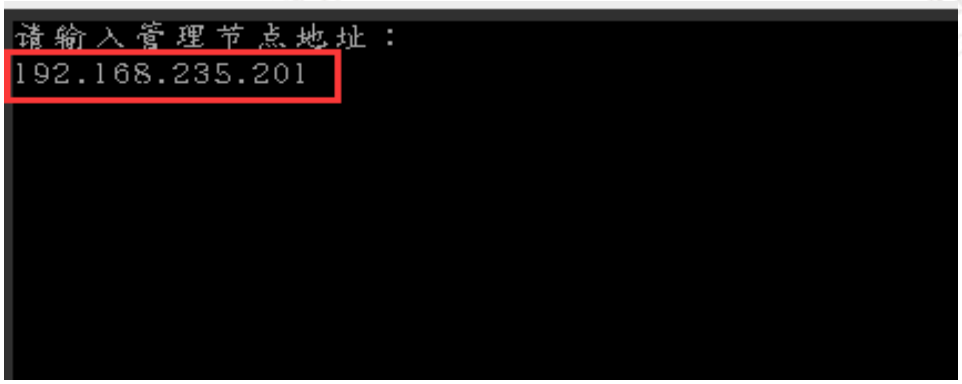
2、选择序号 7，并回车，进行集群管理配置，如下图所示。



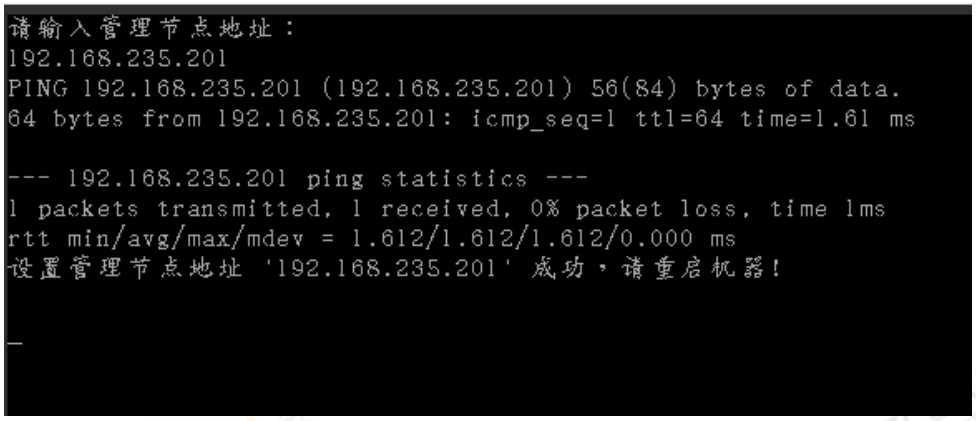
3、选择序号 2，并回车，设置管理节点地址，如下图所示



4、输入管理节点地址，如下图所示。

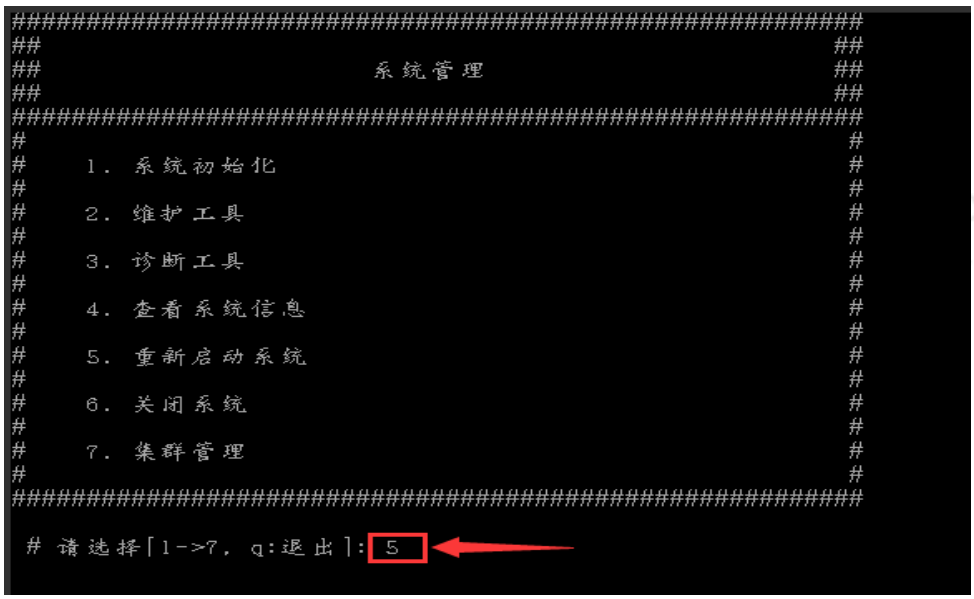


5、敲回车键，kernel 会去 ping 管理节点 IP，ping 通后，提示重启机器，如下图所示。

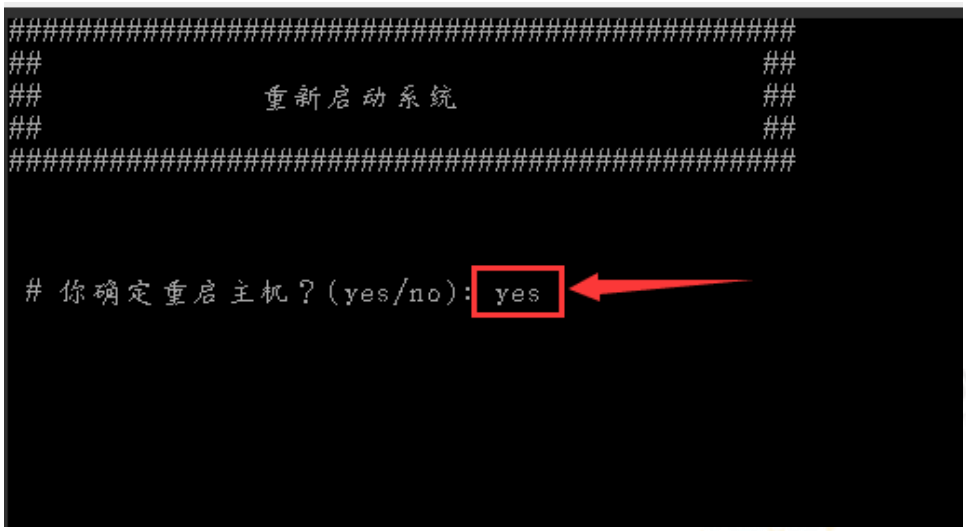


6、敲回车键，退回到集群管理界面，并输入 q，返回到系统管理界面，如下图所示。

7、退回到系统管理界面后，输入 5 重新重启系统，并回车，如下图所示。



8、在重新启动系统的提示中，输入 yes，并回车，如下图所示。



9、待 kernel 节点启动完成后，防火墙管理页面查看节点状态正常，如下图所示。

2.5 添加被保护数据库实例

2.5.1 登录安全管理员界面

1、打开 Google Chrome 或 Firefox 浏览器，在地址栏内输入 https://云数据库防火墙系统管理节点 IP 地址。进入登录页面后，输入用户名：secadmin 默认密码：secadmin1234。

注意：首次登录系统需要修改安全管理员默认密码。

2.5.2 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：

2.5.2.1 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：云数据库防火墙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。

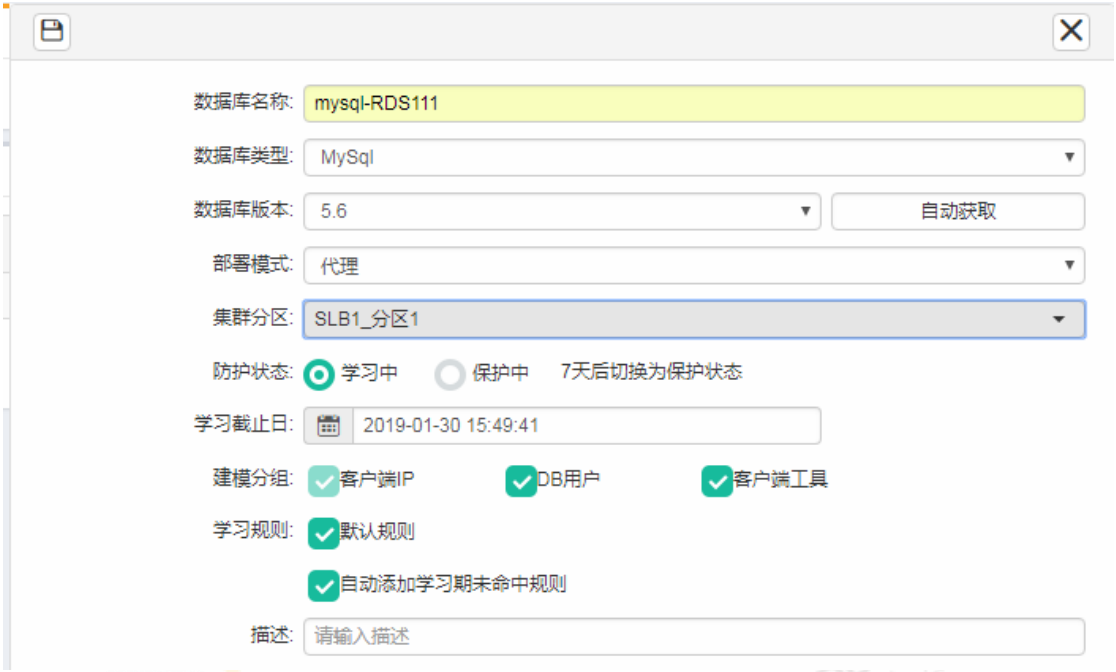
4、然后点击“操作”列中的“保存”图标，如下图所示。

5、点击“保存”图标，如下图所示。

2.5.2.2 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：云数据库防火墙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。

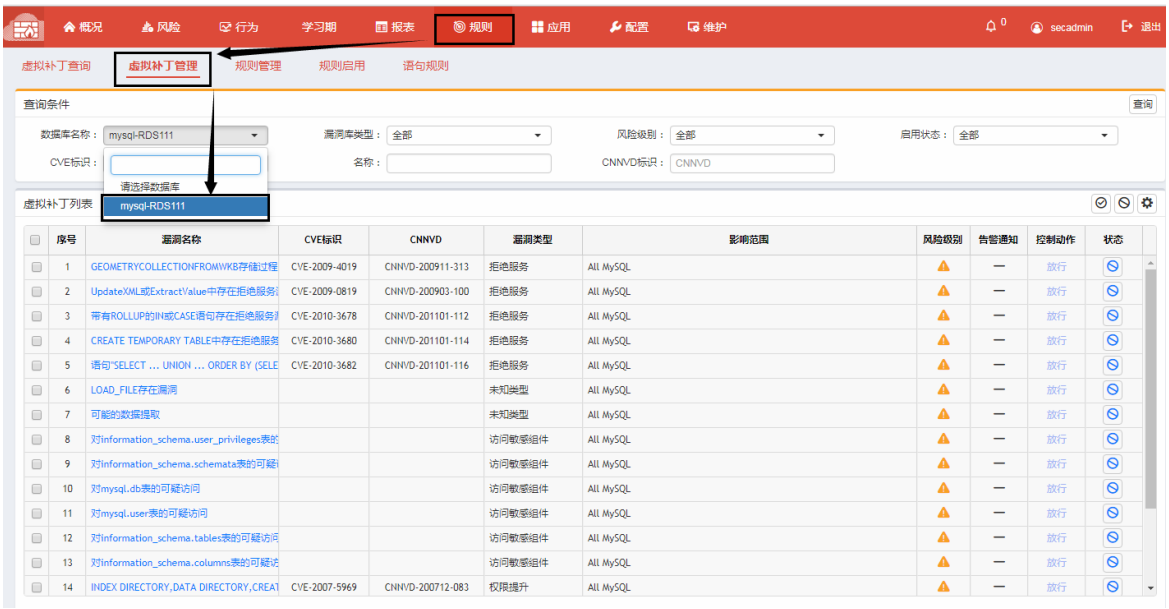
3、在“网络设置”页中的“地址：端口号（动态端口）”列中输入被保护云服务商提供的数据库服务（如 RDS 数据库）实例的连接字符串域名和端口号，“代理组”列中选择“管理接口”和“端口号”，如下图所示。

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。

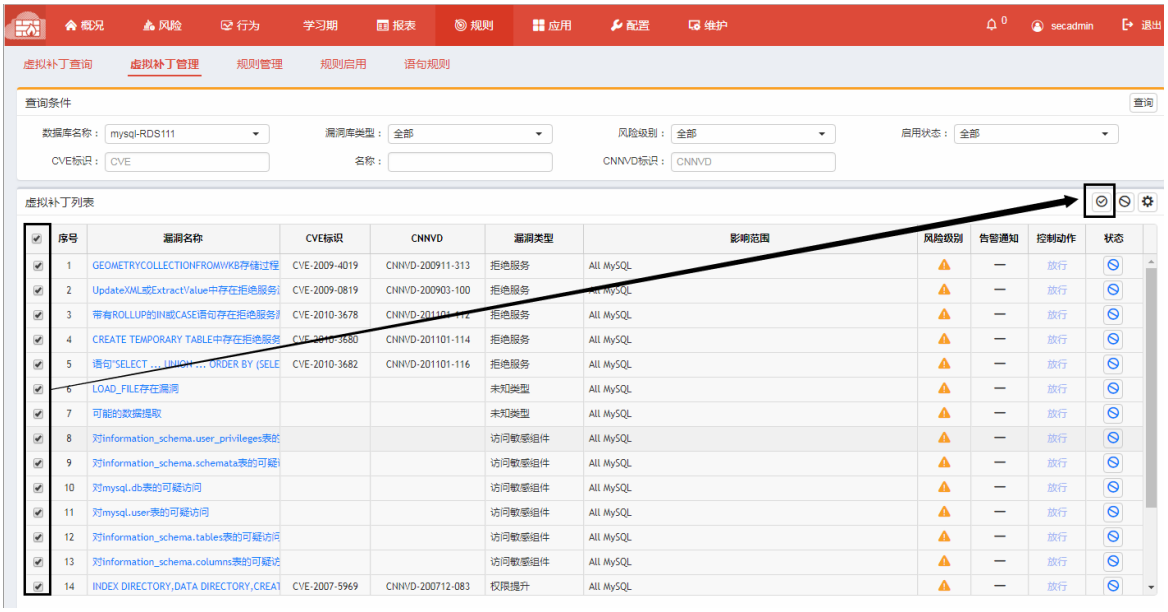
2.6 设置虚拟补丁规则

1、进入安全管理员界面，点击【规则】->【虚拟补丁管理】，进入虚拟补丁列表页，然后在“查询条件”项中的“数据库名称”下拉列表中选择被保护的数据库实例。如下图所示。

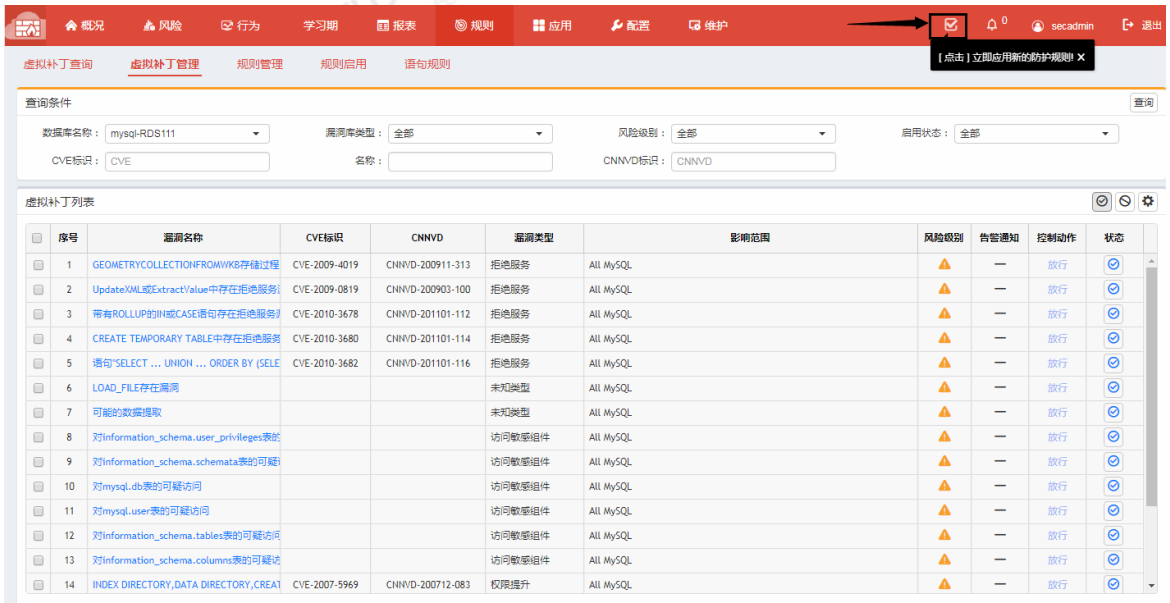


2、在“虚拟补丁列表”页中即会显示未启用的系统默认规则，然后选择需要启用的规则，点击

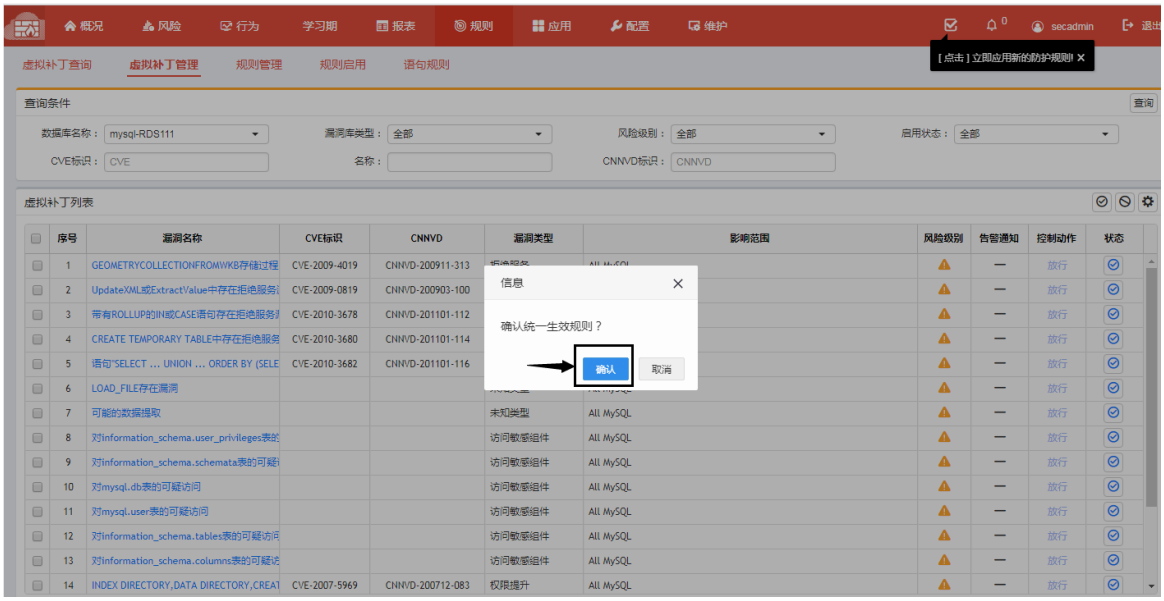
“启用”图标，如下图所示。



3、点击“立即应用新的防护规则”图标，如下图所示。



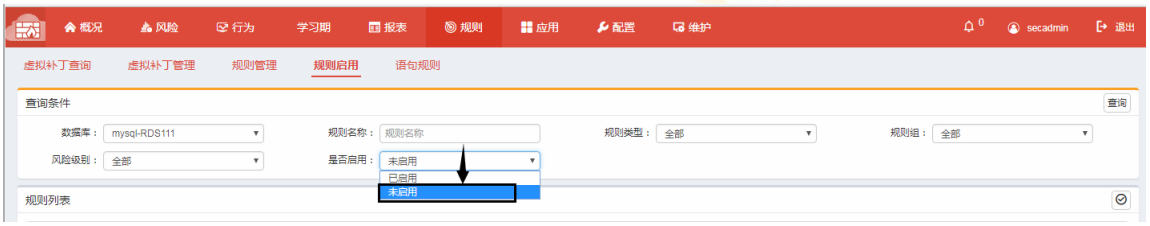
4、在弹出的窗口上点击“确定”，如下图所示。



2.7 设置防火墙规则

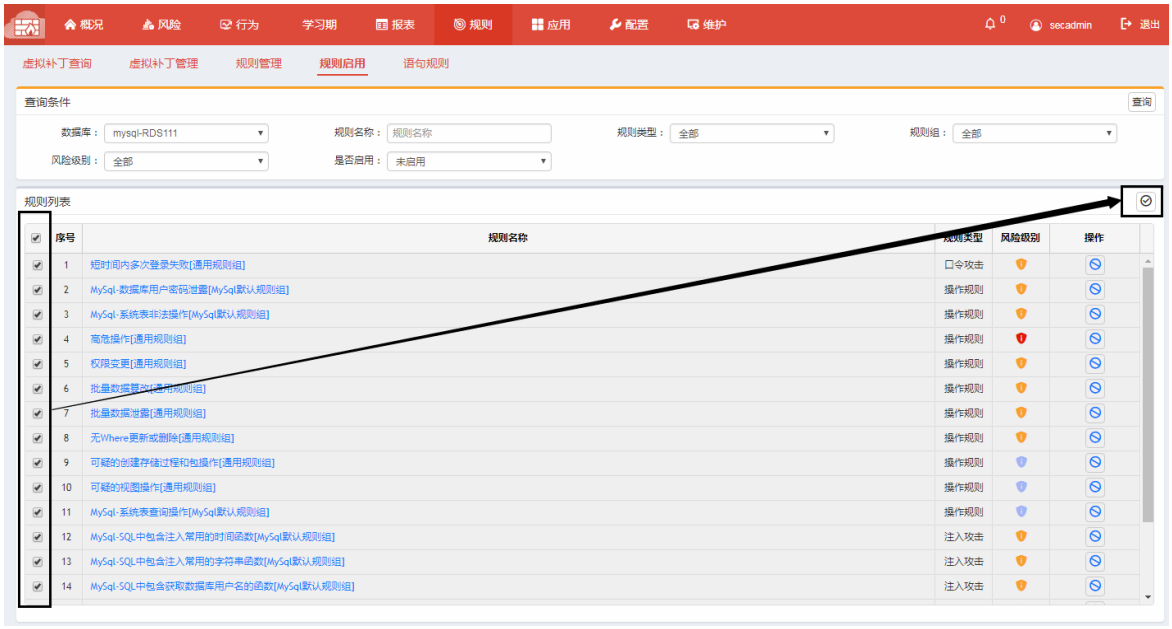
1、进入安全管理员界面，点击【规则】->【规则启用】，然后在“查询条件”页中的“数据库”下拉列表中选择被保护的数据库实例。如下图所示。

2、在“查询条件”页的“是否启用”下拉列表选项中选择“未启用”，如下图所示。



3、“规则列表”页中即会自动显示未启用的规则，然后选择需要启用的规则，点击“启用”图标，

如下图所示。



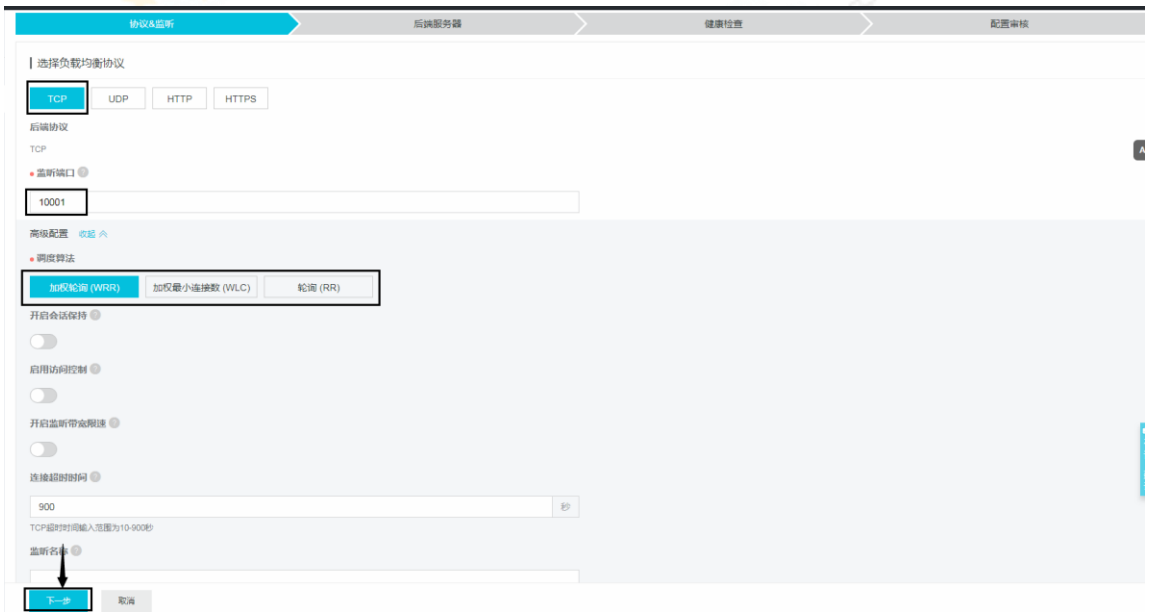
4、点击“立即应用新的防护规则”图标，如下图所示。

5、在弹出的窗口上点击“确定”，如下图所示。

2.8 配置负载均衡

1、创建一个负载均衡 SLB，创建完成后，点击“点我开始配置”，如下图所示。

2、选择负载均衡协议为 TCP，配置负载均衡对外服务提供的端口为 10001，高级配置中根据实际情况选择适当的调度算法，其他参数默认，，点击“下一步”，如下图所示。



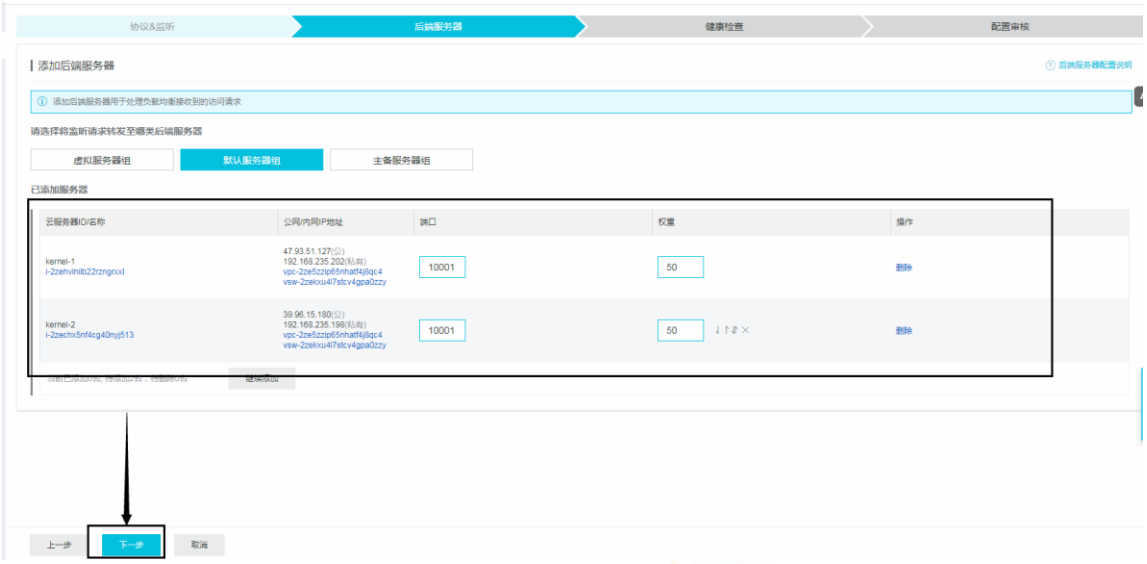
负载均衡支持如下三种调度算法如下，可以根据实际情况调整：

加权轮询：权重值越高的后端服务器，被轮询到的次数（概率）也越高；

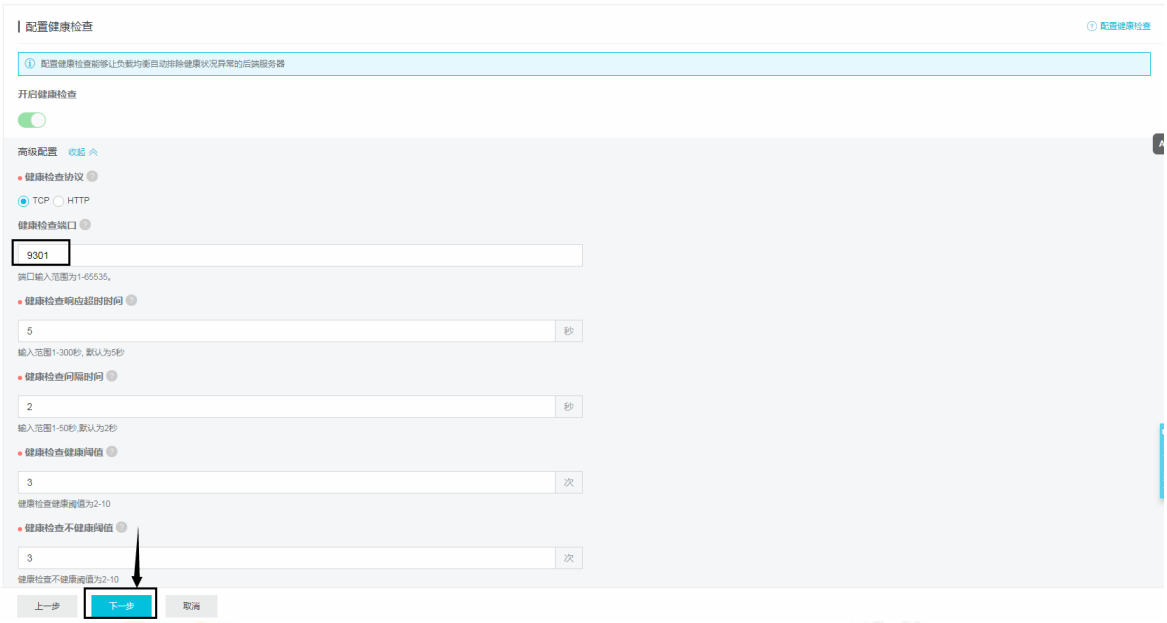
加权最小连接数（WLC）：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高；

轮询（RR）：按照访问顺序依次将外部请求依序分发到后端服务器。

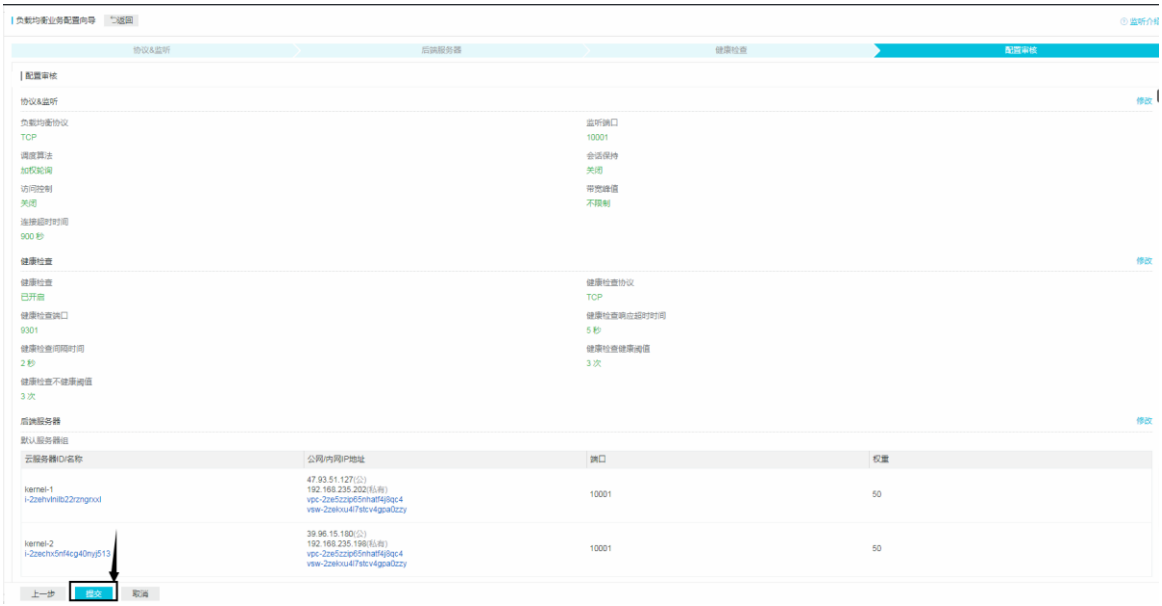
3、添加后端服务器用于处理负载均衡接收到的访问请求，选择默认服务器组，并将相应的 kernel 节点添加到该服务器组中，根据实际需要，配置每台 kernel 节点的端口和权重，点击“下一步”，如下图所示。



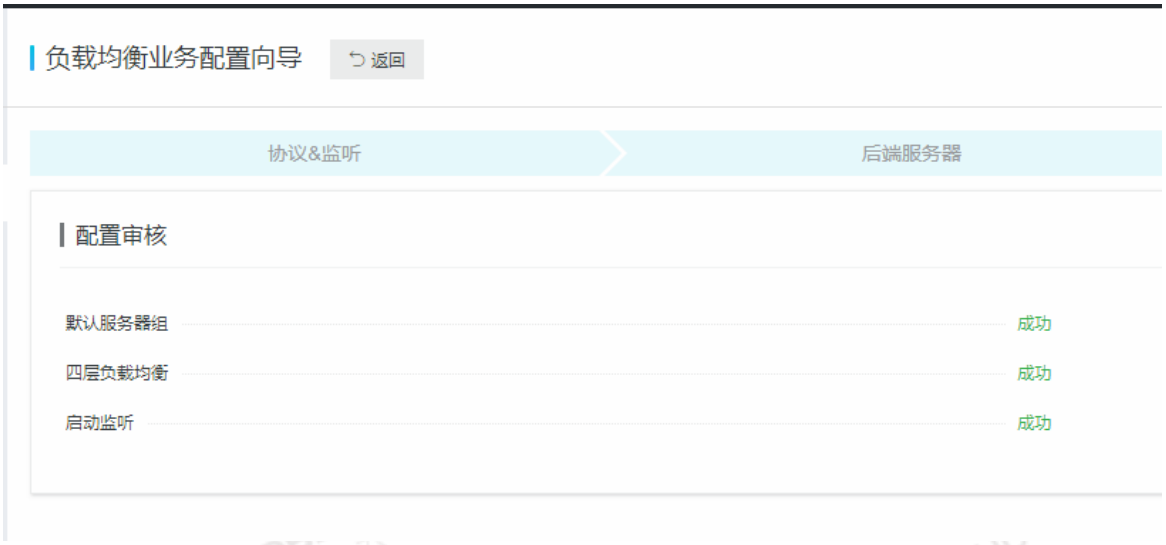
4、配置健康检查，健康检查端口配置为 9301，其他健康检查参数可以使用默认值，或者根据实际需要进行配置，点击“下一步”，如下图所示。



5、配置审核，所有配置信息审核通过后，点击‘提交’按钮，如下图所示。



6、负载均衡配置并启动监听成功后，如下图所示。



2.9 部署测试

修改应用或使用 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 SLB 的 ip 和代理端口，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：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。