BEYOND
TECHNOLOGY

东软 NetEye 数据库审计系统快速向导

东软 NDBA7000 是综合型的数据库安全平台

目 录

一、 产品介绍

1.1 产品简介

东软 NetEye 数据库审计系统支持旁路部署、串联部署、探针部署等多种部署方式，实现对数据库操作和用户行为进行审计，对违规操作和风险操作进行阻断，并提供多种查询方式和报表，供数据管理者取证、查询、分析、决策，具有维护简易、稳定运行的特点。

系统具备超大容量的审计数据管理和分析能力，支持对 Oracle、SQL Server、Sybase、DB2、Mysql 等数据库进行审计与防护，适用于政府、公安、军队、医疗、航空航天、电信、金融、证券、保险、电力、教育等组织数据库审计与防护的安全需求。

1.2 管理操作方式

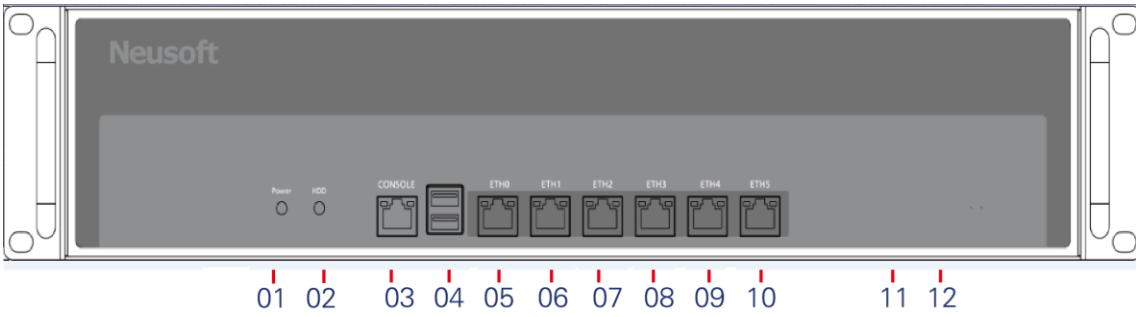
系统采用 B/S 管理方式，系统配置管理和审计数据查询/展示都可以通过 Web 来完成。

1.3 系统硬件介绍

产品系列分为高中低多款型号，能够满足不同网络环境的部署需求。

本手册以一款 2U 标准设备为例进行示意说明。

1.3.1 前面板

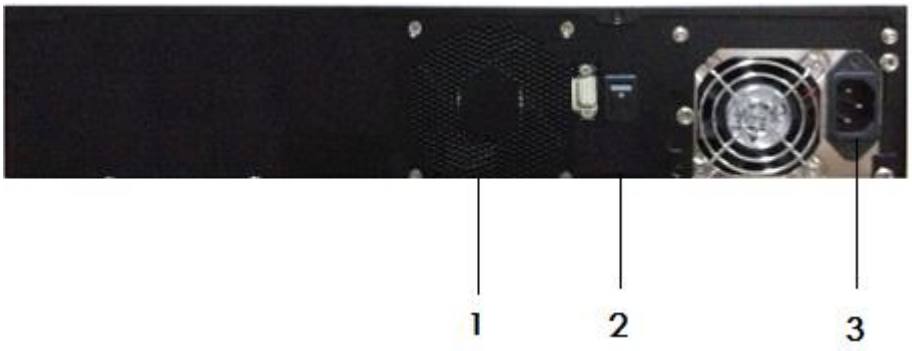


1:电源灯　2:状态灯　3:Console 口　4:USB 口　5~9: 镜像/桥接口

10: 管理口　11:扩展口　12:扩展口

注：桥接口是开启数据库防火墙功能需要用到的接口；镜像口是开启数据库审计需要用到的接口；管理口是对系统进行管理配置及展示查询所需要的接口。

1.3.2 后面板



1：风扇　2：电源开关　3：电源接口

1.3.3 指示灯

项目	说明
电源灯	灯亮表示电源接通并电源开关处于开通状态; 灯灭表示没有供电或电源故障。
状态灯	灯闪烁表示系统正在读写 CF 卡或者硬盘。

二、 安装准备

本章节介绍系统安装前的各项准备工作。

2.1 安装环境要求

本设备必须安装在室内环境，并具备以下条件。

2.1.1 温度及湿度要求

为保证系统正常工作并延长其使用寿命，安装环境要求维持一定的温度和湿度。

若安装环境内长期湿度过高，则容易造成绝缘材料绝缘不良，甚至漏电，还会发生材料机械性能变化，金属部件锈蚀等现象。若相对湿度过低绝缘垫片会干缩而引起紧固螺丝松动，在干燥的气候环境下还容易产生静电，从而危及系统电路。

温度过高危害更大，因为高温会加速绝缘材料的老化，使系统可靠性大大降低并严重影响其使用寿命。

环境要求如下:

温度：0°C～ 40°C

湿度：10%～ 70%（非凝结状态）

2.1.2 环境清洁度要求

尘埃对设备安全运行也是一个重要影响因素，因为空气中的灰尘的累积会造成静电吸附，使金属接插件或金属接点接触不良或电路短路。这一因素不但会影响设备的使用寿命，同时也容易造成通信故障。尤其是在室内相对湿度偏低时，更易产生这种静电吸附。

除尘埃外，设备对空气中所含的腐蚀性酸性气体也有严格的要求，因为这些有害气体在一定湿度环境下会加速对金属部分的腐蚀和某些部件的老化。

安装环境的要求为无爆炸性、导电性、导磁性及腐蚀性气体或尘埃。具体要求请参照下表的相关要求或规定。

项目	规格
尘埃粒子	不大于 3×10^4 个/立方米
二氧化硫气体（SO_2）	不大于 0.2 毫克/立方米
氯气（Cl_2）	不大于 0.006 毫克/立方米
硫化氢（H_2S）	不大于 0.05 毫克/立方米
氨气（NH_3）	不大于 0.01 毫克/立方米

2.1.3 静电要求

静电感应主要来自两个方面：一是高压输电线路、雷电等外界电场；二是环境建筑及装饰材料、整机结构等。

因此，为防止静电损害，应做到：

- ☑ 设备及地板有良好的接地连接；
- ☑ 环境防尘；
- ☑ 保持适当的环境温度与湿度；
- ☑ 接触电路板时应佩戴防静电手腕套或手套，穿防静电工作服；
- ☑ 拆卸下的电路板应板面朝上放置在具有抗静电作用的工作台上或防静电袋中；
- ☑ 观察或转移已拆卸的电路板时，应只接触电路板的外边缘，避免用手直接触摸电路板上的元器件。

2.1.4 雷电/电磁要求

强烈的电磁干扰源，无论是来自设备外部，还是来自内部，都是以电容耦合、电感耦合、电磁波辐射、公共阻抗包括接地系统耦合等传导方式对设备产生影响。为达到更好的防雷和抗干扰效果，应做到：

- ☑ 对供电系统采取有效的防电网干扰措施
- ☑ 设备安装环境最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些
- ☑ 远离强功率无线电发射台、雷达发射台、高频大电流设备等
- ☑ 必要时采取电磁屏蔽的方法
- ☑ 保证机箱的保护接地用保护地线与大地保持良好接触
- ☑ 保证电源插座的接地点与大地良好接触
- ☑ 为增强电源的防雷击效果，可以在电源的输入端安装电源避雷器，这样可大大增强电源的抗雷击能力

2.1.5 其他注意事项

- ☑ 确认设备通风口处留有足够的空间，以利于设备散热
- ☑ 确认安装环境自身有良好的通风散热系统
- ☑ 确认安装环境（机架等）足够牢固，能够支撑设备及其附件重量
- ☑ 确认安装环境有良好接地连接

注：设备与墙壁的距离应不小于 15 厘米

2.2 安装工具准备

2.2.1 设备清单检查

在确认安装环境符合要求后，打开设备包装箱并对照定货合同及装箱单仔细核对设备及附件是否齐全，如有疑问或差错请及时与设备销售商取得联系。

2.2.2 安装工具

- ☑ 十字镙丝刀
- ☑ 一字镙丝刀
- ☑ 防静电手腕套
- ☑ 防静电带

2.2.3 配套电缆

- ☑ 电源线

☑ 网线

☑ 串口线

2.2.4 安装设备及仪表

配置终端可以是普通的 PC 机。

注：本产品包装中不附带安装工具、安装设备及仪表。

2.3 部署规划

在正式安装前，建议提前了解应用业务系统及网络环境，只有这样才能够正确的规划部署方案。

注：请结合售前的解决方案文档。

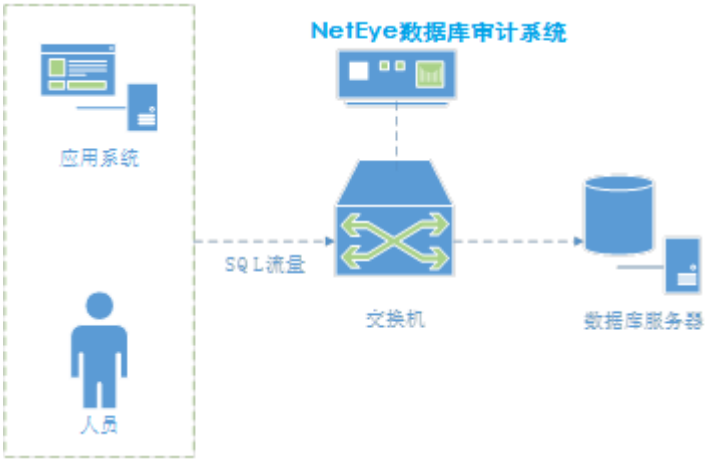
本部分介绍常见的几种部署方案。

2.3.1 旁路部署

产品在此部署模式下可以开启数据库审计功能，无法开启数据库防火墙功能。

设备通过旁路监听的方式接入网络，只要在交换机上设置端口镜像，不需要对现有的网络体系结构（包括：路由器、防火墙、应用层负载均衡设备、应用服务器等）进行调整。

支持多路采集数据的接入模式，一个审计引擎可以同时采集多个数据源的审计数据。这样的好处：一是降低审计系统部署成本；二是适合更多的应用环境的审计需求，比如审计数据源相对分散的环境（多个交换机镜像口）。



2.3.2 串联部署

产品在此部署模式下可以同时开启数据库防火墙与数据库审计功能。(需相应的授权许可支持)

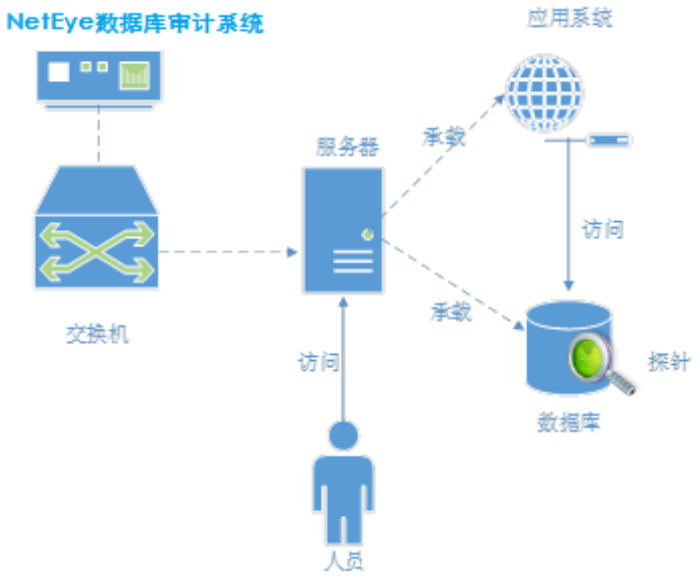
设备以串联的方式接入网络，部署在数据库服务器之前，并提供硬件 Bypass 功能以保证网络的可用性。此外，采用双机热备方式可进一步提高自身的可用性。

2.3.3 探针部署

探针部署方式只需要在管理系统中进行配置即可。

探针部署方式针对的主要有以下几种情况：

- ☑ 应用系统与数据库系统在同一台服务器上
- ☑ 人员进入机房直接在数据库服务器上操作数据库
- ☑ 人员通过远程桌面连接到数据库服务器，对数据库进行操作
- ☑ 虚拟化环境



三、 产品安装

本章节介绍设备安装过程。

在进行安装前请仔细阅读本手册的前文内容，并确认已经满足其要求。

3.1 硬件安装位置

本系统可以安装到以下两种环境中：

☑ 直接放置在稳定的水平平台上

☑ 与其它网络设备一起安装在标准机架上

3.1.1 安装到水平台面

这是一种最简便经济的安装方式，但安装操作过程中要注意以下事项：

☑ 保证水平平台的牢固性和稳定性，并保证有良好的接地连接

☑ 设备通风口与形成通风障碍的障碍物之间要留有至少 15 厘米的通风通道

☑ 设备上表面不要堆放重物

3.1.2 安装到标准机架

设备机箱设计是符合标准 19 英寸机架（以下称机架）安装要求。

以下为安装到机架上的具体说明：

1） 检查并确认机架的安装是否合格并符合其安装标准，并注意检查机架是否稳固并且有良好的接地连接；

2） 将挂耳用螺钉安装到设备前面板的两侧；

3） 确定安装位置，将本产品安放到预定位置的托盘上（建议用户提供与该机架配套的设备托盘），并注意设备与机架之间保持适当的间隙；

4） 用平头镙钉将设备固定到机架上。

3.2 旁路部署接线方式

硬件设备可以从交换机镜像口获取网络当中访问数据库的流量，只需要把设备的监听口与镜像口通过网线连接即可。

1）将设备的管理口连接到管理网络中；

2）将设备的监听口连接到交换机的镜像口；（交换机镜像口必须配置为双向镜像，审计模式下的部署）

3）将业务接口连接到环境中的交换机或数据库服务器上。

3.3 串联部署接线方式

硬件设备需要对数据库进行防护的时候，需要将数据库服务器和指向数据库的交换机分别与硬件设备的两个桥接口进行连接。

四、 加电与初始配置

本章介绍完成上架安装后的初次启动与系统基础配置。

4.1 产品通电启动

4.1.1 通电前检查

设备通电启动前需要进行如下检查：

☑ 供电电压是否与设备标定的额定电压相符

☑ 与配置终端连接的配置电缆是否连接妥当，配置终端是否已经启动并设置完成

注：通电启动前，一定要明确电源开关的位置，以便在通电启动时出现意外情况可以及时切断电源，最大限度减少意外发生时的损失，保证设备与工作人员的安全。

4.1.2 通电启动

☑ 接通供电电源为设备供电；

☑ 打开设备电源开关。

4.1.3 系统通电后的检查

☑ 确认设备冷却通风系统已经正常工作。

确认标准：系统上电后，可听见明显的风扇转动发出的噪音，说明冷却通风系统工作正常；另外，也可以用手背或软丝带放在靠近风扇的地方，如果系统正常冷却且通风系统工作正常，就可以明显感觉到有风吹动。

☑ 检查设备前面板上的各指示灯是否工作正常。

确认标准：各指示灯的确切含义，请参见本手册“硬件介绍-指示灯”部分。

4.1.4 连接到网络

1）将设备的管理口连接到管理网络中

2）将设备的监听口连接到交换机的镜像口。（交换机镜像口必须配置为双向镜像）

确认标准：可以 Ping 通设备的管理口地址。

4.2 初始配置

本章节介绍系统初始配置方法。

4.2.1 初始管理地址

初始管理口地址： 192.168.1.254。

4.2.2 Web 连接系统

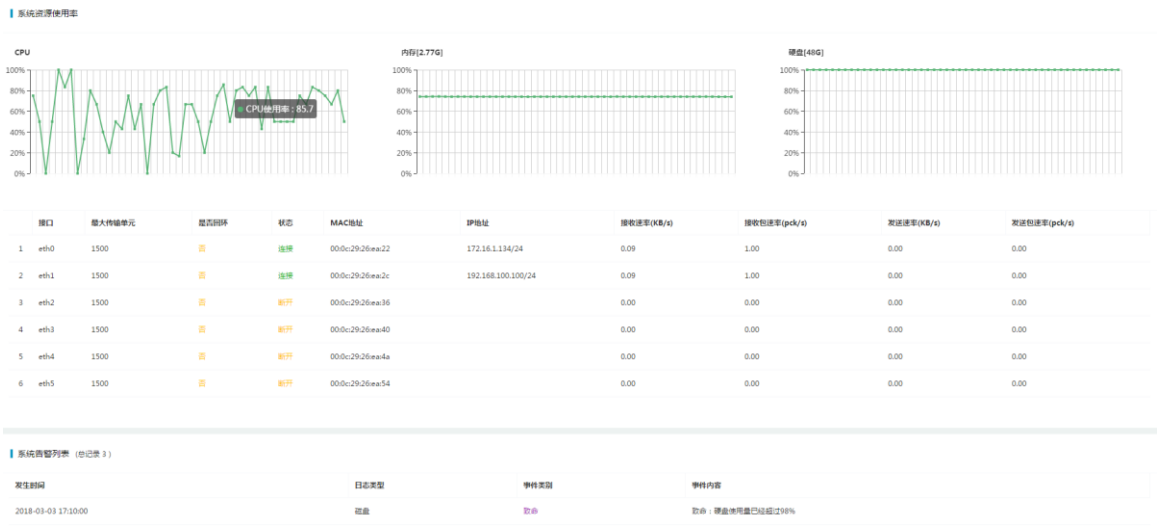
浏览器输入地址： https://192.168.1.254。

4.2.3 登录系统

选择系统管理员，并输入密码进行登录。

注：初始密码为： admin12345 。

输入用户名、密码（默认为：sysadmin/admin12345），点击“登录”，便可进入管理主页。



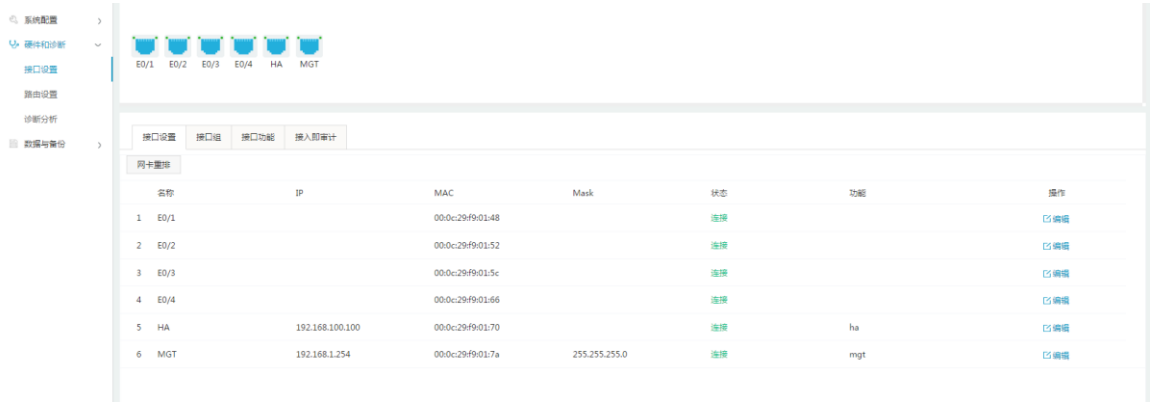
五、 Web 管理界面操作指引

成功登录 Web 管理界面之后，可按照以下步骤进行操作维护。

5.1 配置管理 IP

点击系统配置，页面如下图所示，在接口设置中可以看到配置口默认 IP 为 192.168.1.254，默认端口为 MGT，可以自行修改 IP 即可。

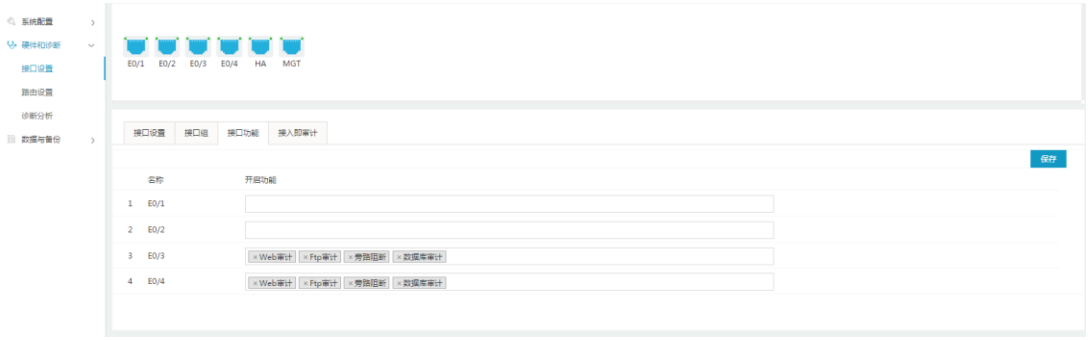
注：修改后需要重新在浏览器输入新 IP 登录。



5.2 数据库审计模式配置

5.2.1 开启接口审计功能

SysAdmin 登入，进入“系统配置”页面，点击“接口设置”，选中“接口功能”。界面如下图所示，默认接口 E0/3 和 E0/4 具有审计功能，点击右侧空白处，选取需要的审计功能，然后点击保存并生效。（注：agent 也需要开启接口审计功能）



至此系统管理员配置部分完成，接下来进入安全管理员配置部分。

5.2.2 添加数据库引擎

我们所要审计保护的数据库被称为引擎。在使用数据库审计功能前，首先需要添加数据库引擎信息。包括数据库 IP、端口、类型、缺省数据库等。

SecAdmin 用户登入，进入“数据库概况”页面如下图所示:

点击“添加”按钮，提示是否使用配置向导进行数据库的添加与配置。

使用配置向导进行数据库添加与配置（带*必填），共分为三个步骤：

基本信息

名称：防护数据库自定义名称。

类型：系统所支持的所有数据库类型，根据情况选择所审计保护的数据库类型。

版本：所要审计保护的数据库版本

数据库（实例）：即数据库实例名，系统显示为各数据库默认实例名；根据实际情况填写数据库实际实例名。

端口：系统显示为各数据库默认端口号，在实际配置中请按照环境情况填写。

IP：所要审计保护的数据库 IP 地址。

备注：审计保护数据库的批注。

模式选择

模式：根据需求以及设备在网络环境中的连接情况，选择是审计模式或防火墙模式。

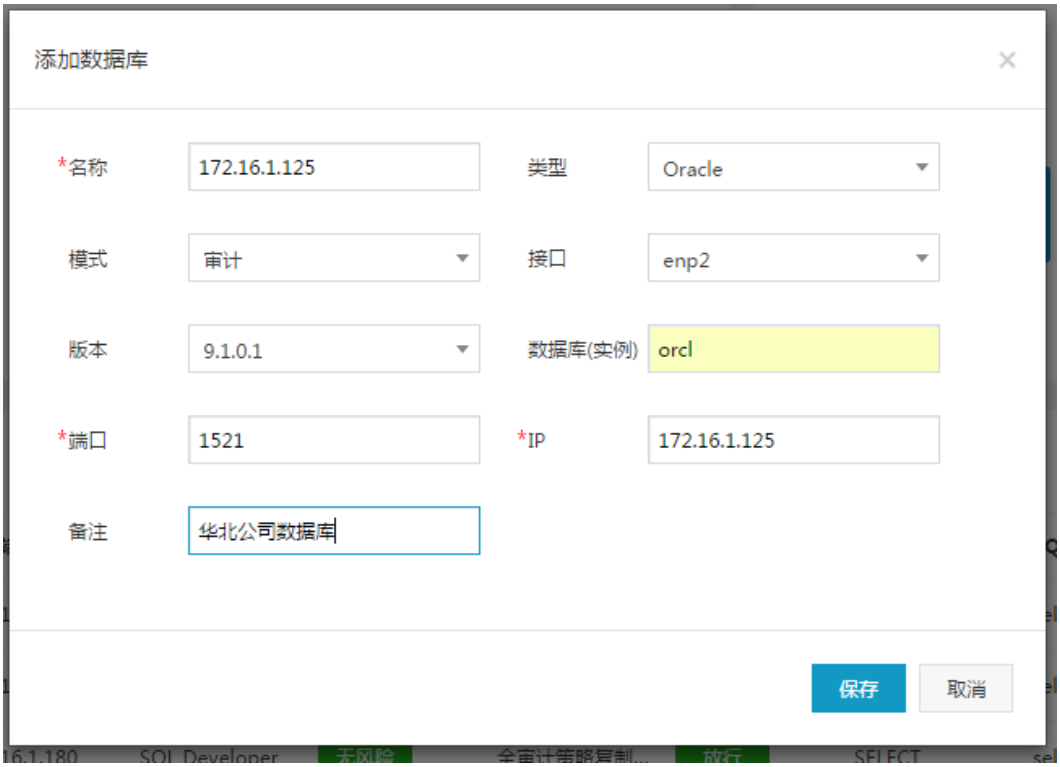
接口：审计数据的来源口。

策略配置

策略：根据需求配置。

最后点击保存并启用

不使用配置向导进行数据库添加与配置（带*必填）：



5.2.3 Agent 审计

使用 agent 功能审计时，需单独配置，如图所示；

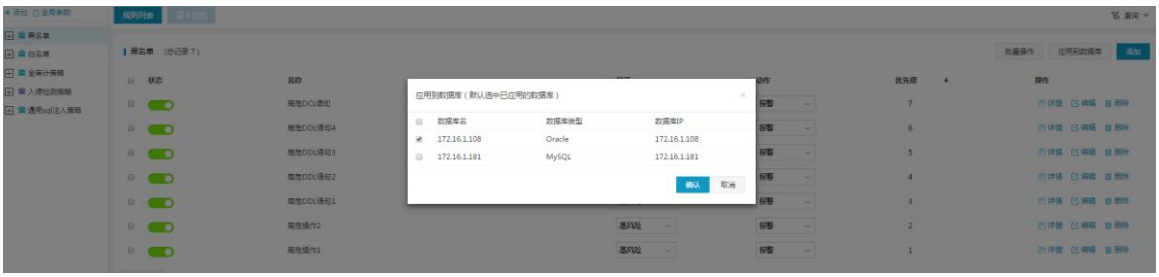
在页面上下载 agent 插件，并在数据库服务器上安装。

agent 插件在数据库服务器上安装并配置完成后，此页面的 cpu、内存以及审计接口会刷新出数据库服务器上的信息。此时添加审计 IP，以及在默认的接受端口被占用情况下，修改端口后，点击“启动”按钮，启动其审计功能。

5.2.4 策略绑定

数据库引擎只有绑定了策略规则才能生效，匹配策略规则执行记录、告警或其它操作。

SecAdmin 用户登入安全管理系统，选中导航栏区的“全局配置”，点击策略管理，选中“应用到数据库”，界面如下所示：



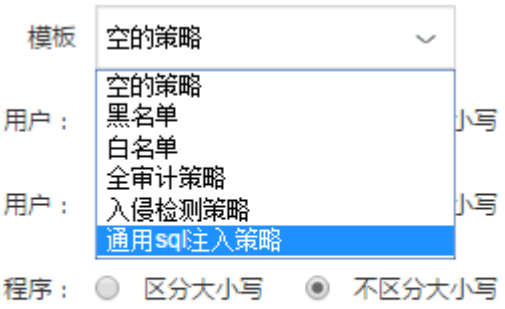
5.2.5 策略配置

在“策略管理”页面中，点击“添加”按钮，如下图所示。

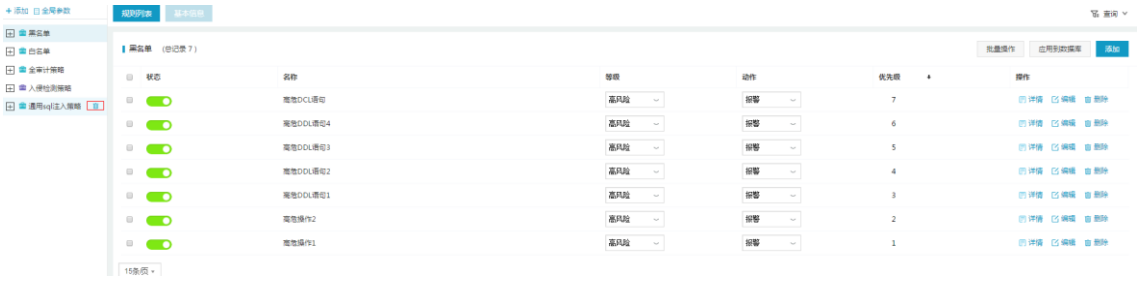
首先填写策略“名称”作为标识。

模板来源：可应用于全部数据库引擎，也可应用于单条数据库引擎。

模板：



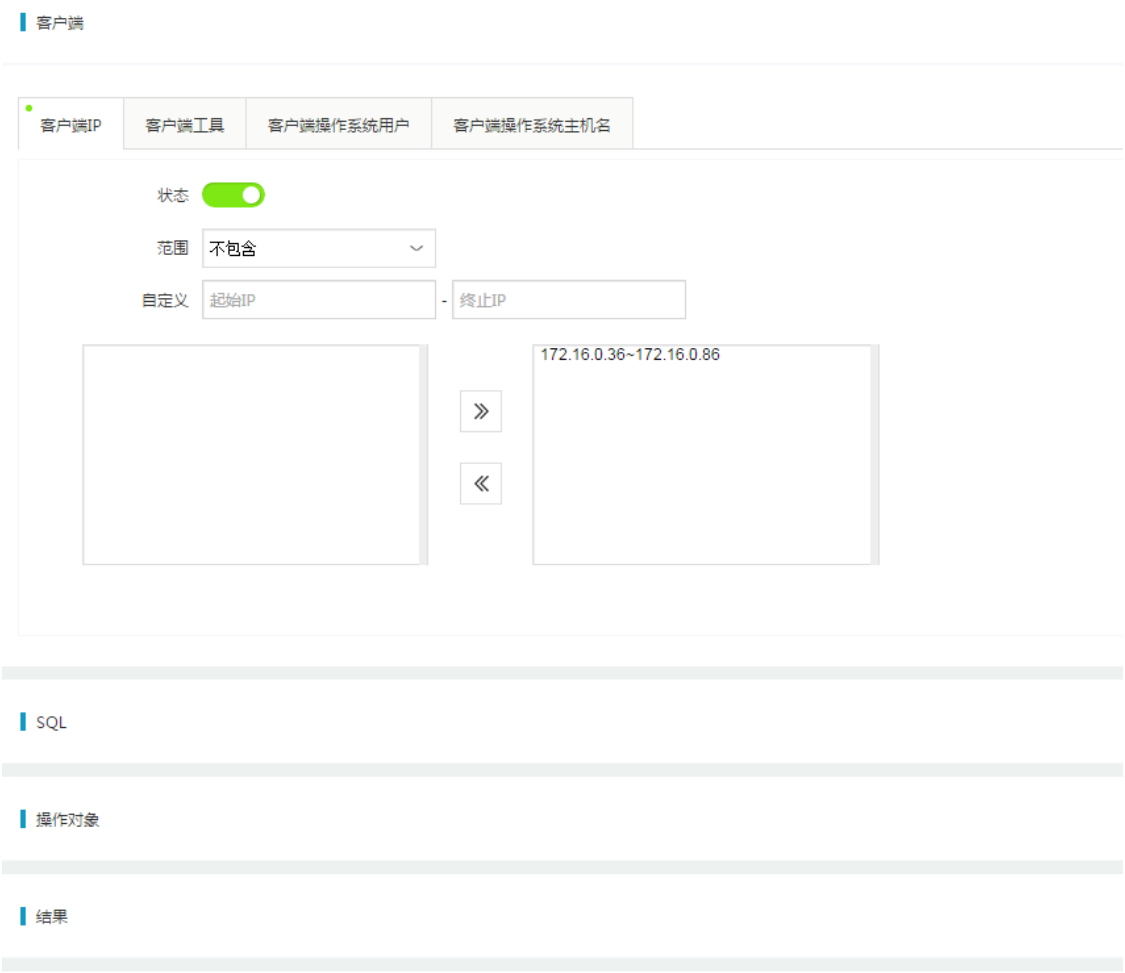
删除策略，点击策略后面的“删除”，页面会弹出提示框，点击“确定”，成功删除策略。



5.2.6 规则

规则的展开

要配置某个条件的具体内容，需要先把条件展开。如下图所示，点击“客户端”，会展开此条件的配置栏，配置好需要配的条件后，状态开启即可。



条件是否包括

每个条件后面都有“包含”、“不包含”的选项。举例，如下图所示，操作对象中的“目标表”已经展开，填写了表“help”，若默认选择“不包括”，则所有操作中未影响表“help”的都会匹配到此条件。

添加删除规则

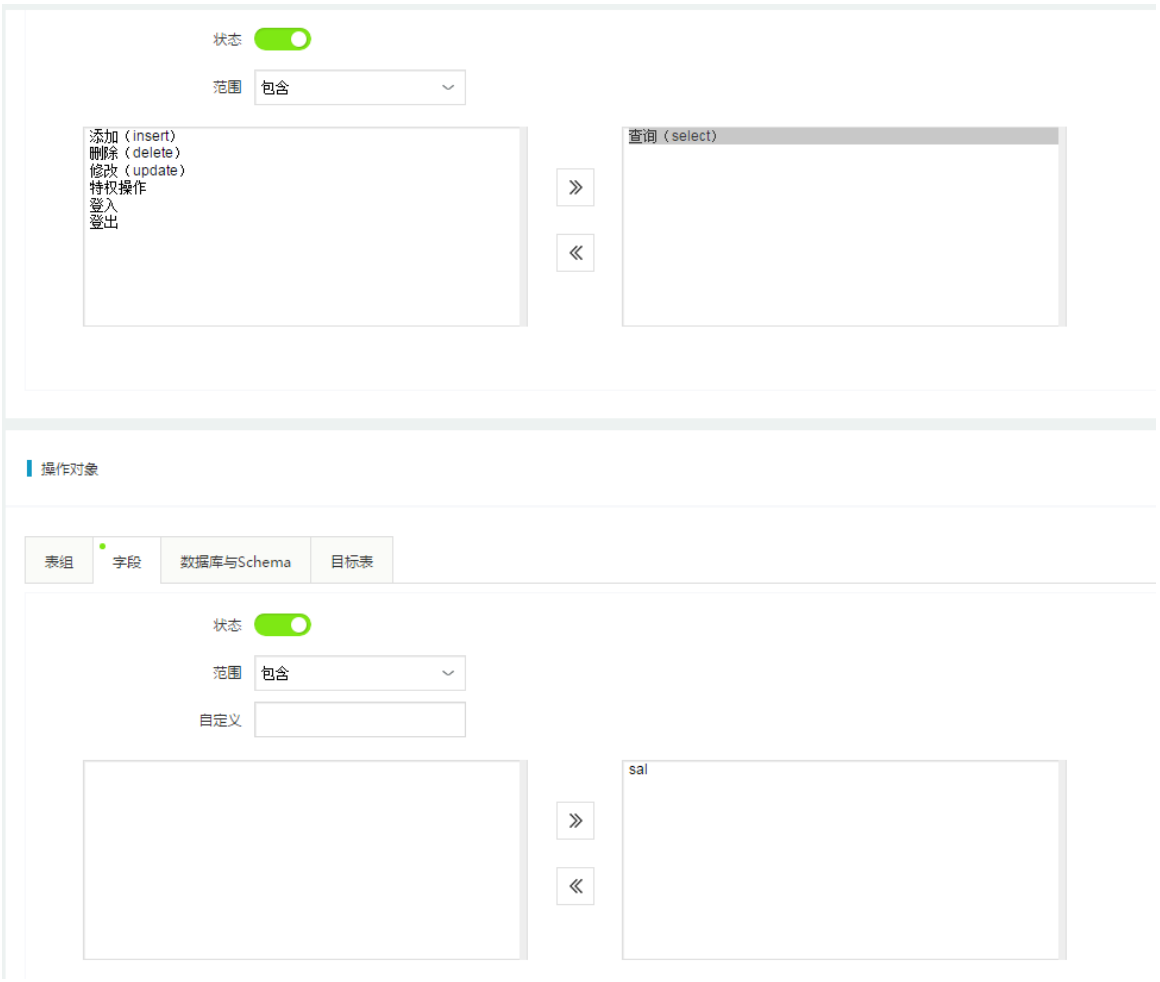
如下图，首先选中一条策略，点击图中的“添加规则”或策略后的“添加”，都会弹出添加规则框。

5.2.7 策略模版

示例 1：敏感数据查询

将对敏感数据的查询(如：手机号，工资等）视为高风险并报警，策略配置如下图：


基本信息
名称
敏感数据查询
描述
描述一下规则的基本信息
状态
等级
高风险
动作
报警
日志记录级别
总是记录



示例 2：不带条件删除语句

将不带条件的删除语句视为高风险并报警，策略配置如下图：

基本信息

名称 不带条件的删除规则

描述 描述一下规则的基本信息

状态

等级 高风险

动作 报警

日志记录级别 总是记录

SQL

SQL语句 SQL关键字 特权操作 操作类型

状态

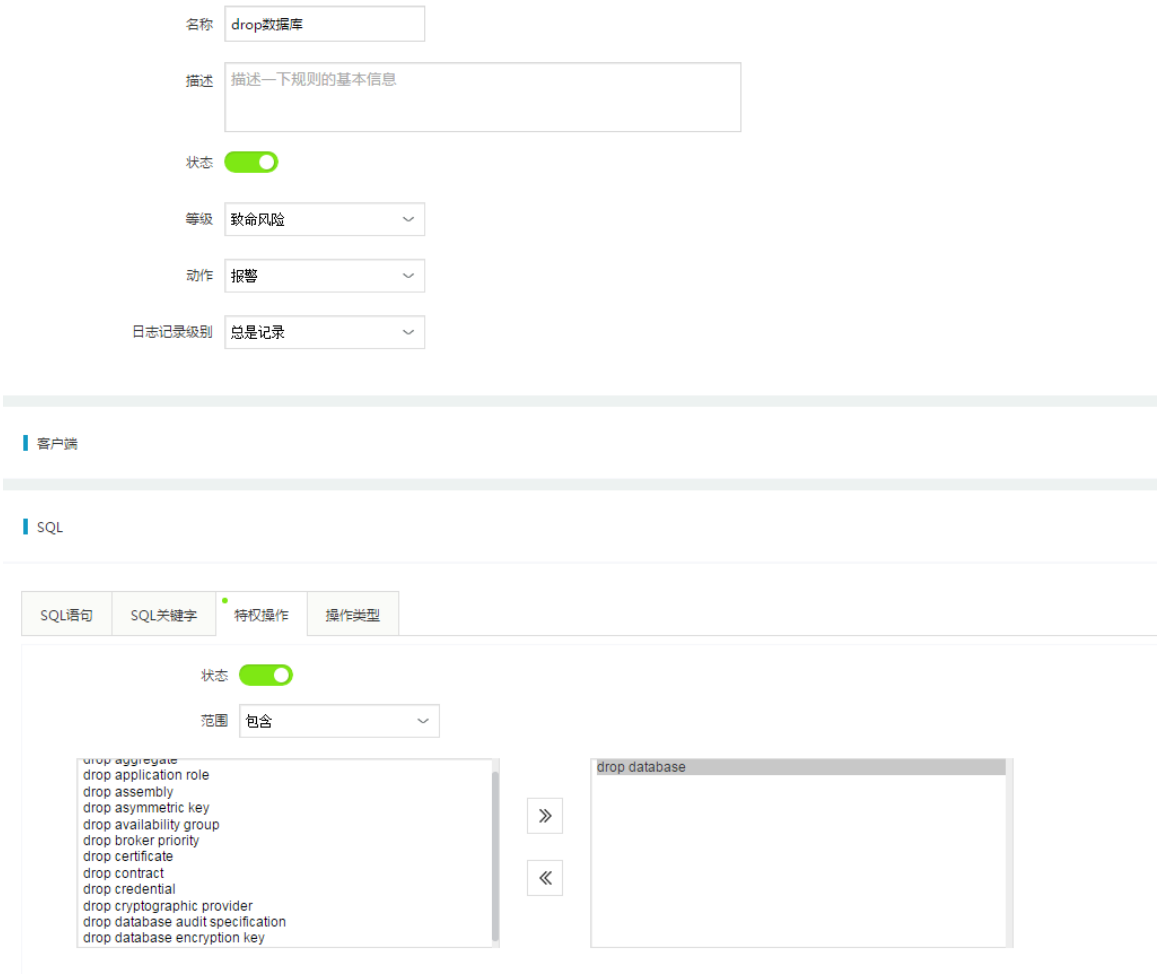
范围 包含

添加（insert）
查询（select）
修改（update）
特权操作
登入
登出

删除（delete）

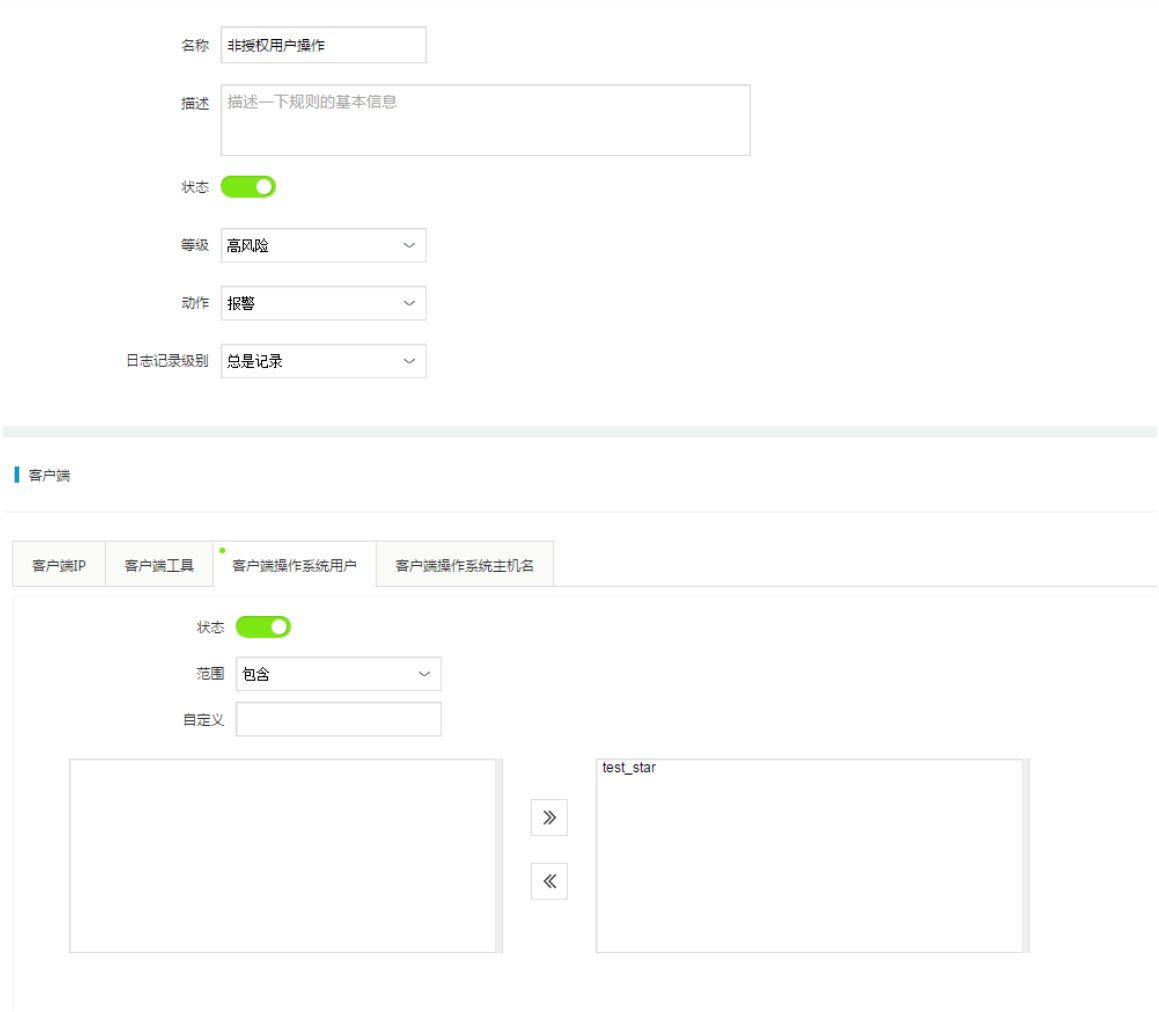
示例 3：删除数据表

将删除数据表视为致命等级并报警，策略配置如下图：



示例 4：非授权用户操作

将非授权用户操作数据库视为高风险并报警，策略配置如下图：



示例 5：非常规客户端

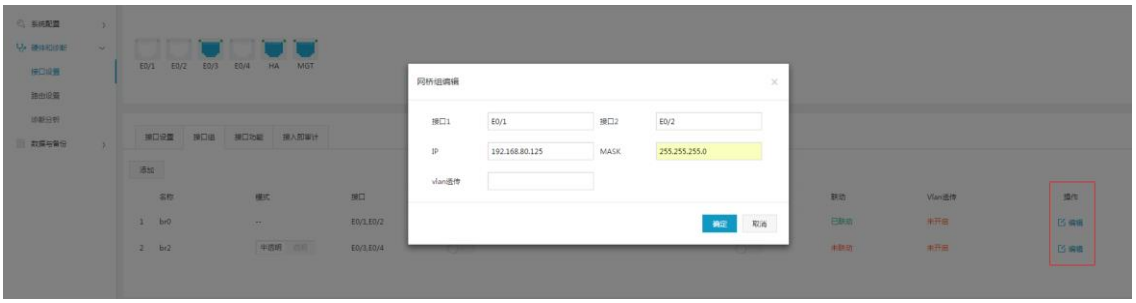
将非常规客户端操作数据库视为高风险并报警，策略配置如下图：

5.3 数据库防火墙模式配置

5.3.1 配置防火墙接口

1、配置网桥串联模式

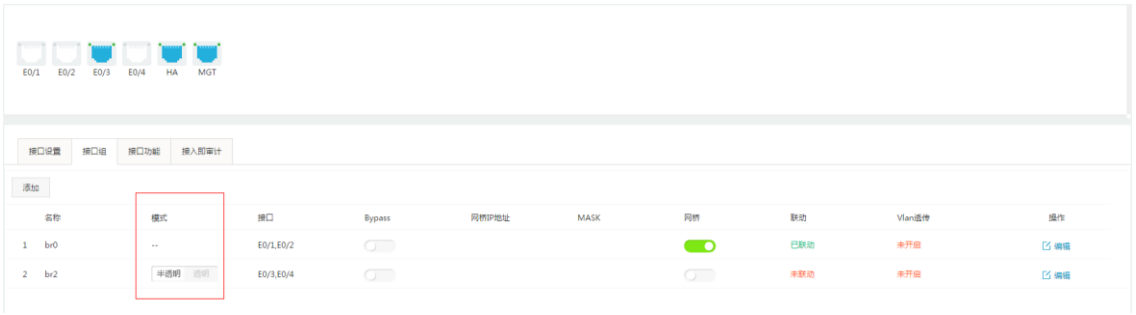
点击“编辑”按钮，填入网桥的 IP 地址和掩码。按提示添加相应信息，如下图所示：



网桥组接口设置：可以使用 VLAN 透传功能，输入相应的 VLAN ID 即可。

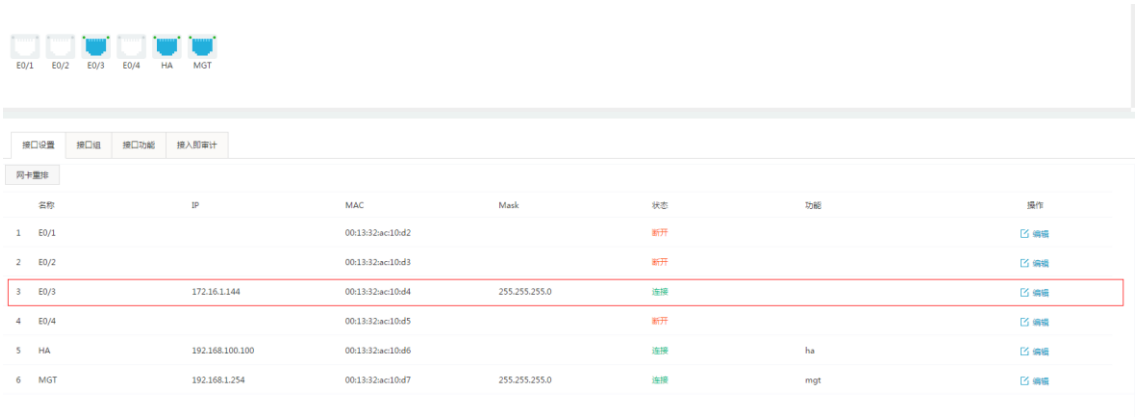
2、配置串联 DPDK 模式

点击切换成全透明模式，此模式下不需要配置地址、VLAN 透传以及路由等，如图所示。



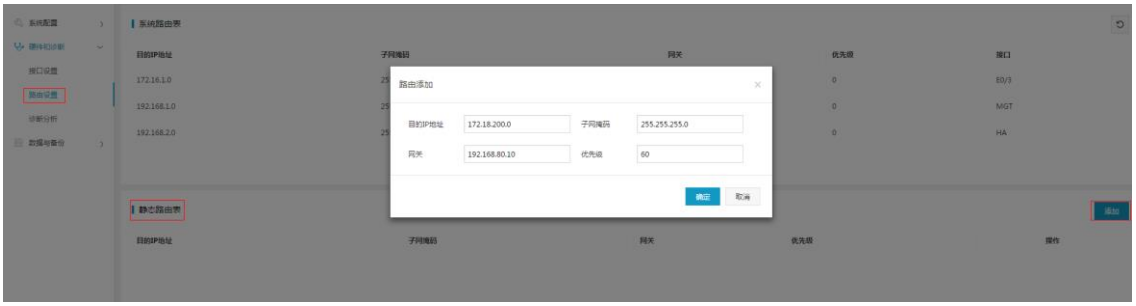
3、 旁路部署代理模式

旁路部署代理防火墙时，业务接口路由可达数据库服务器和应用端的地址，如图所示。



5.3.2 添加路由

针对跨网段的生产环境，系统提供配置静态路由的功能，可以根据实际情况配置到数据库或用户端的路由。按提示添加相应信息，如下图所示：



5.3.3 添加数据库引擎

我们所要审计保护的数据库被称为引擎。在使用数据库防火墙功能前，首先需要添加数据库引擎信息。包括数据库 IP、端口、类型、缺省数据库等。

SecAdmin 用户进入“主页”模块，进入“数据库概况”页面如下图所示：

点击“添加”按钮，按提示添加相应信息。

名称：防护数据库自定义名称。

类型：系统所支持的所有数据库类型，根据情况选择所防护的数据库类型。

模式：根据需求以及设备在网络环境中的连接情况，选择是审计模式还是防火墙模式。

接口：防护数据的接口组。

版本：所要防护的数据库版本

数据库（实例）：即数据库实例名，系统显示为各数据库默认实例名；根据实际情况填写数据库实际实例名。

端口：系统显示为各数据库默认端口号，在实际配置中请按照环境情况填写。

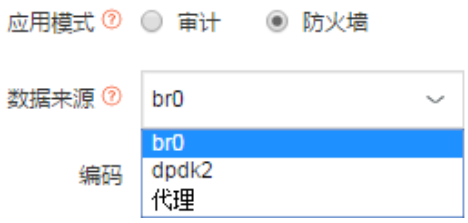
IP：所要防护的数据库 IP 地址。

备注：防护数据库的批注。

5.3.4 开启防火墙功能

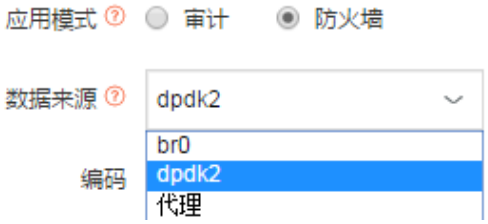
1、SecAdmin 用户进入“通用管理”模块，进入“数据库引擎”页面，点击对应数据库引擎的审计防火墙“添加”按钮，按提示添加相应信息。:

网桥串联部署模式，如图所示；



旁路代理模式，如图所示:

DPDK 透明模式（注：该模式不支持代理），如图所示:



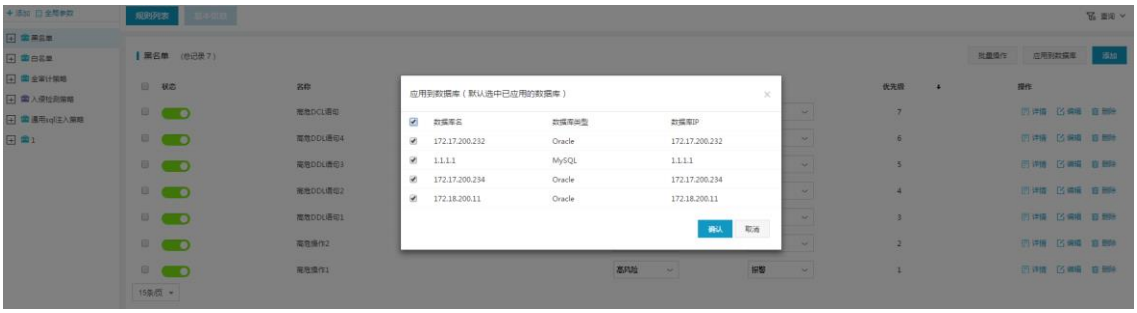
应用模式：根据需求以及设备在网络环境中的连接情况，选择是审计模式还是防火墙模式。

网口名称：网桥的接口编号

5.3.5 策略绑定

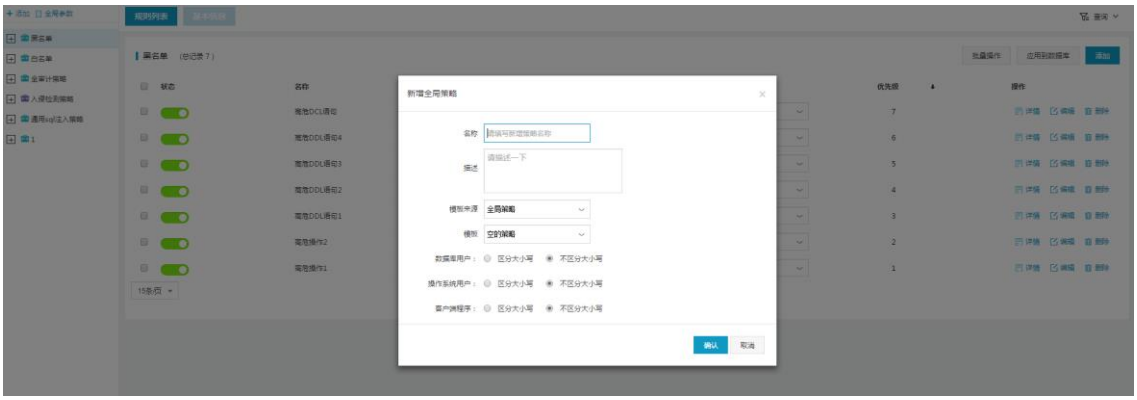
数据库引擎只有绑定了策略规则才能生效，匹配策略规则执行阻断、记录、告警或其它操作。

SecAdmin 用户进入主页，选择导航栏“全局配置”，点击策略管理，选中“应用到数据库”，界面如下所示：



5.3.6 配置策略

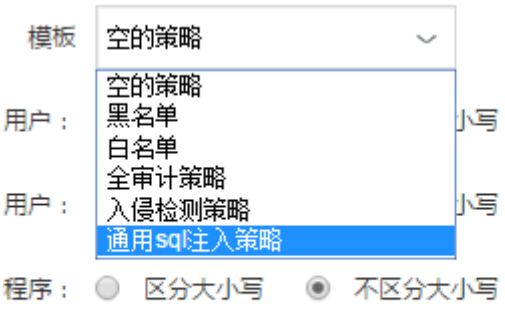
在“策略管理”页面中，点击“添加”按钮，如下图所示。



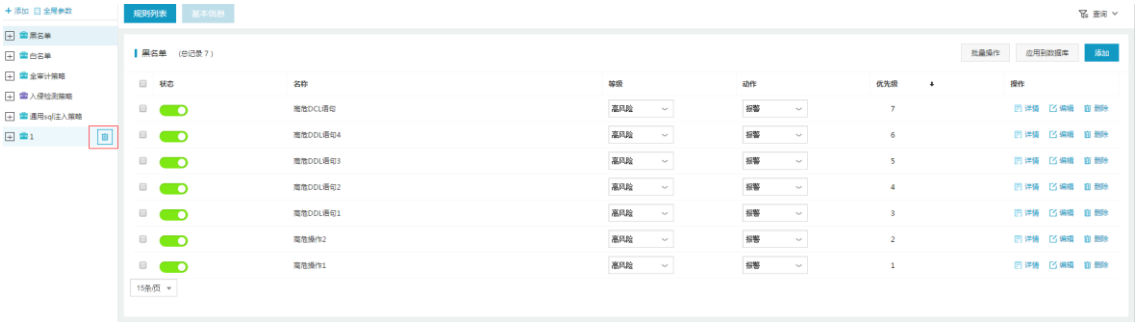
首先填写策略“名称”作为标识。

模板来源：可应用于全部数据库引擎，也可应用于单库引擎。

模板：



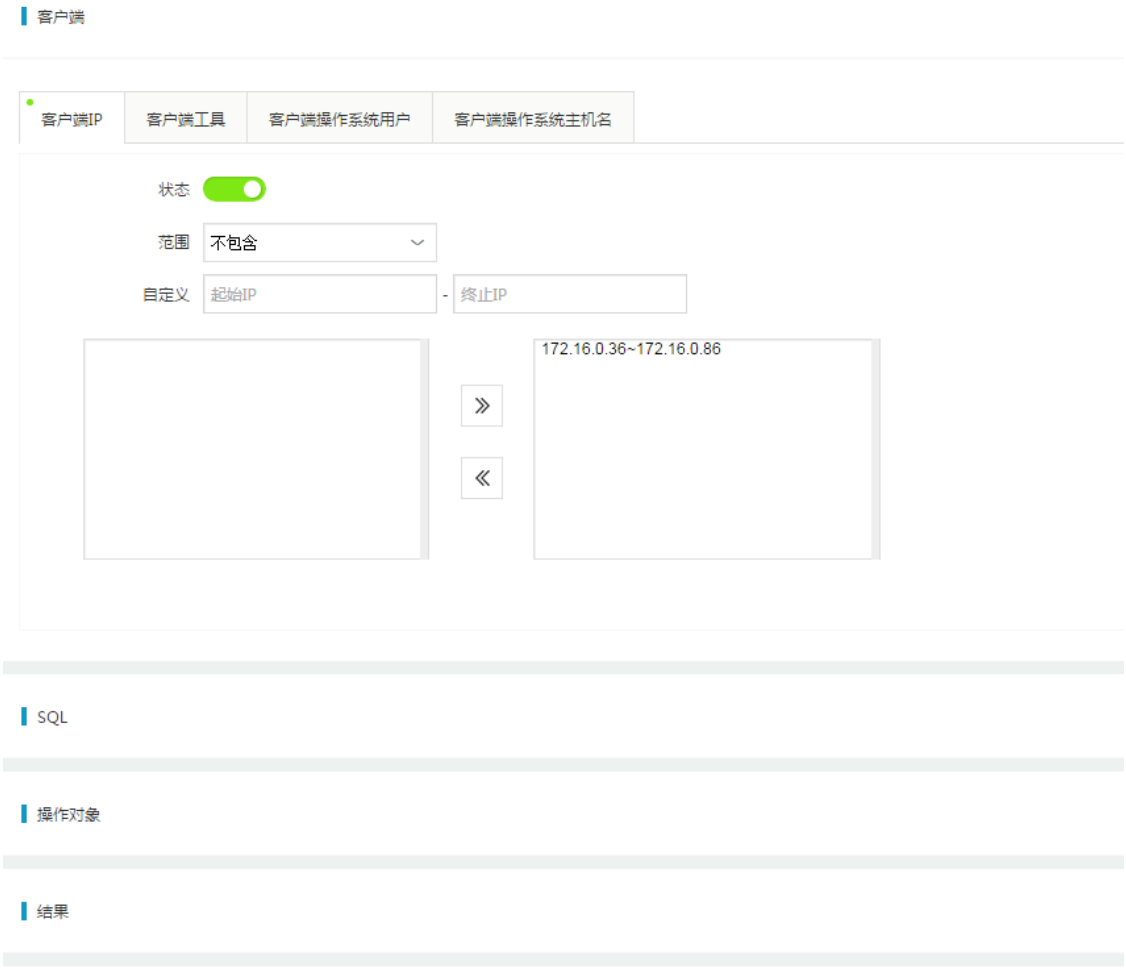
删除策略，点击策略后面的“删除”，页面会弹出提示框，点击“确定”，成功删除策略。



5.3.7 规则

5.3.7.1 规则的展开

要配置某个条件的具体内容，需要先把条件展开。如下图所示，点击“客户端”，会展开此条件的配置栏，配置好需要配的条件后，状态开启即可。

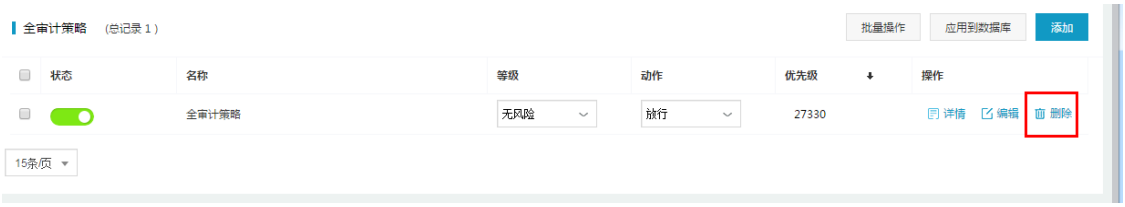


5.3.7.2 条件是否包括

每个条件后面都有“包含”、“不包含”的选项。举例，如下图所示，操作对象中的“目标表”已经展开，填写了表“help”，若默认选择“不包括”，则所有操作中未影响表“help”的都会匹配到此条件。

5.3.7.3 添加删除规则

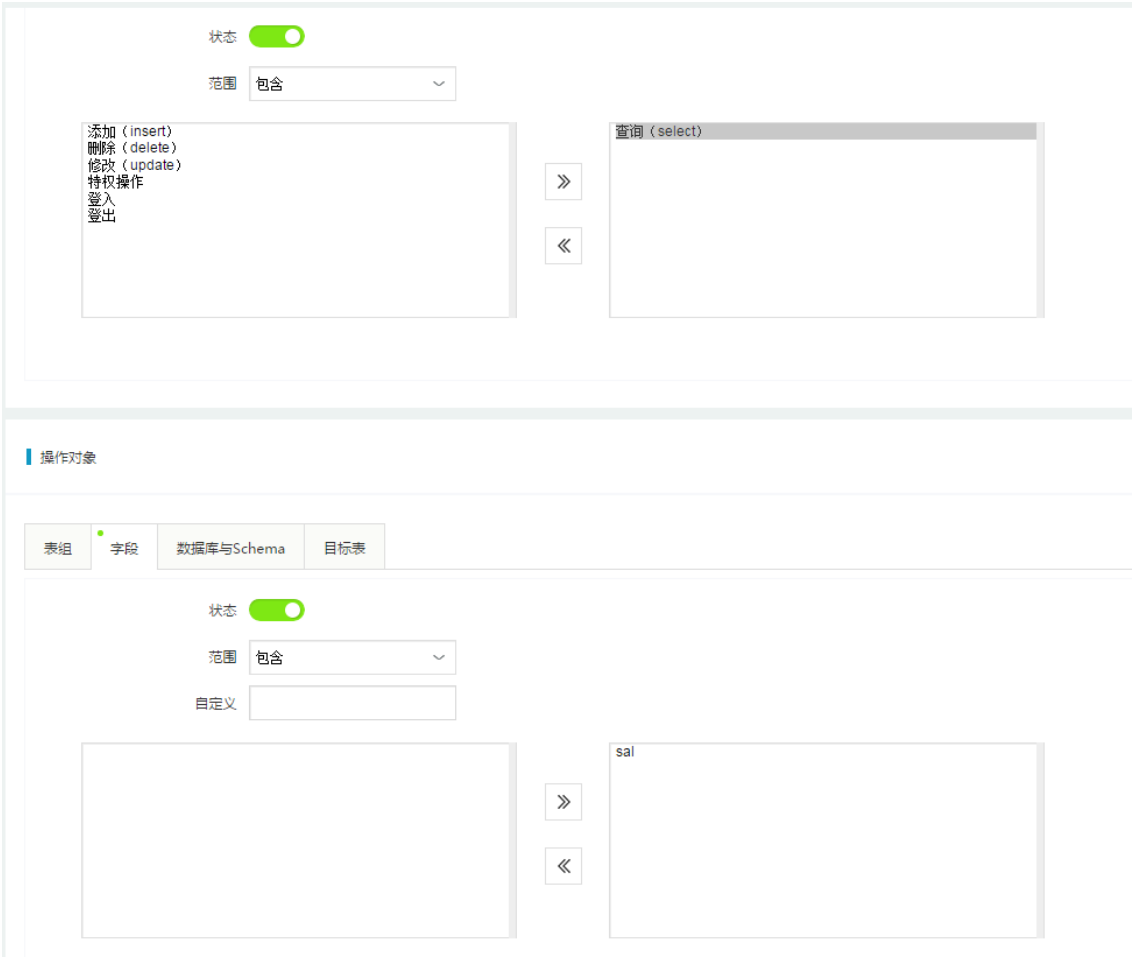
如下图，首先选中一条策略，点击图中的“添加规则”或策略后的“添加”，都会弹出添加规则框。



5.3.8 策略模版

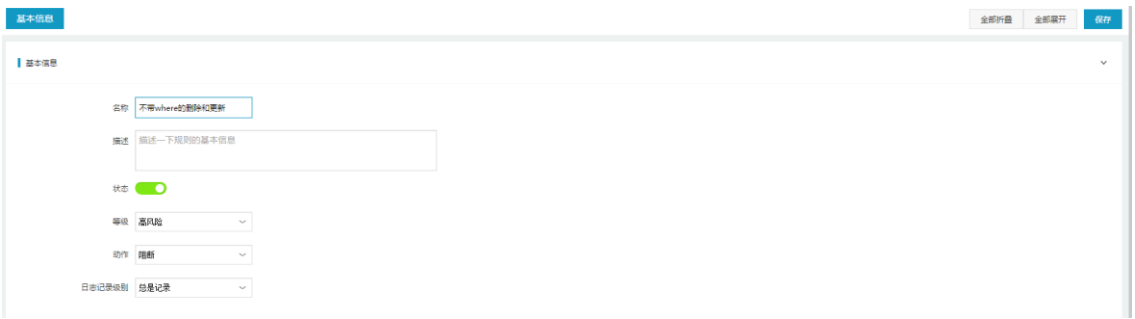
示例 1：敏感数据查询

将对敏感数据的查询(如：手机号，工资等）视为高风险并报警，策略配置如下图：



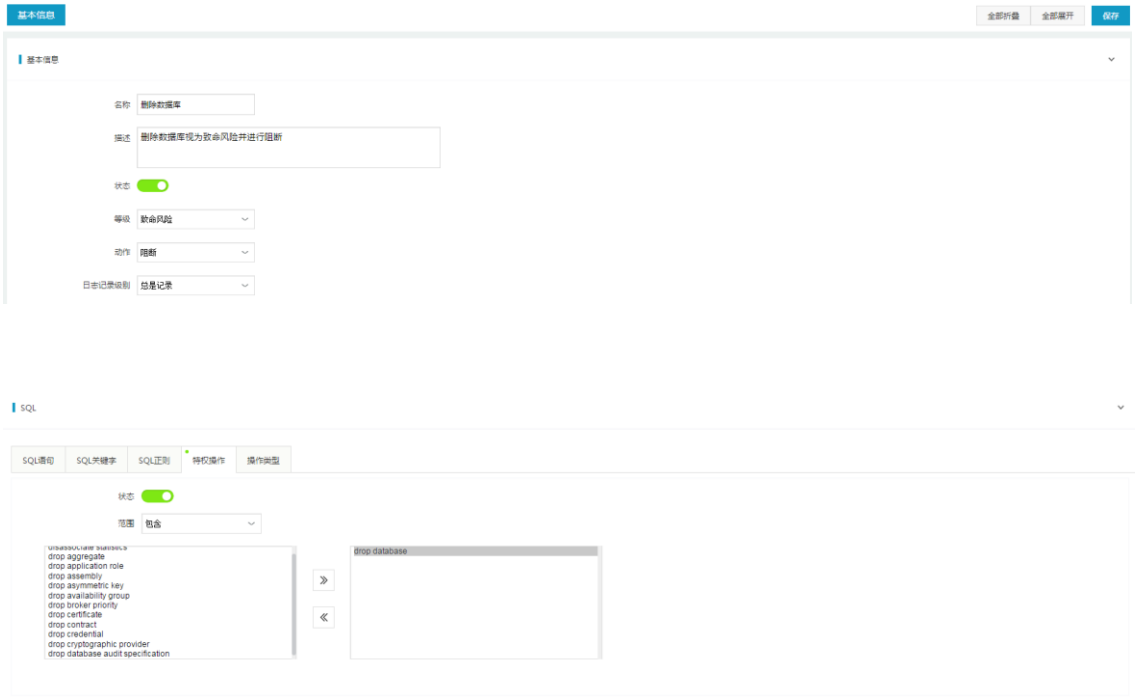
示例 2：No where 的 update 和 delete 高危操作阻断

将不带条件的删除语句视为高风险并阻断，策略配置如下图：



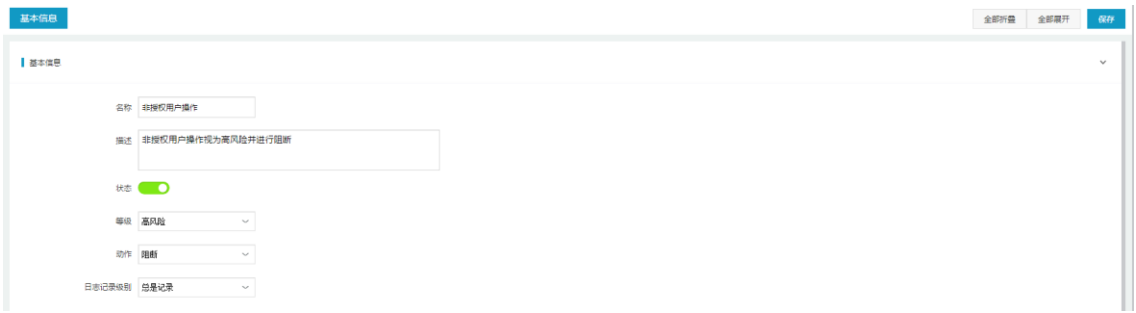
示例 3：删除数据库表

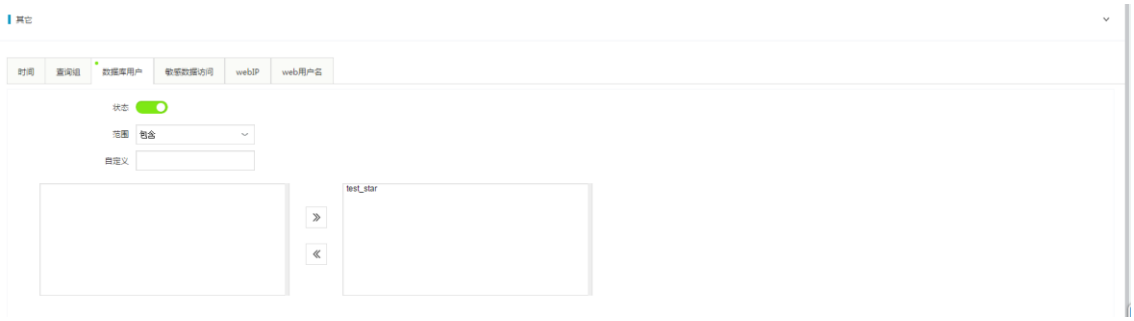
将删除数据库表视为致命等级并阻断，策略配置如下图：



示例 4：非授权用户操作

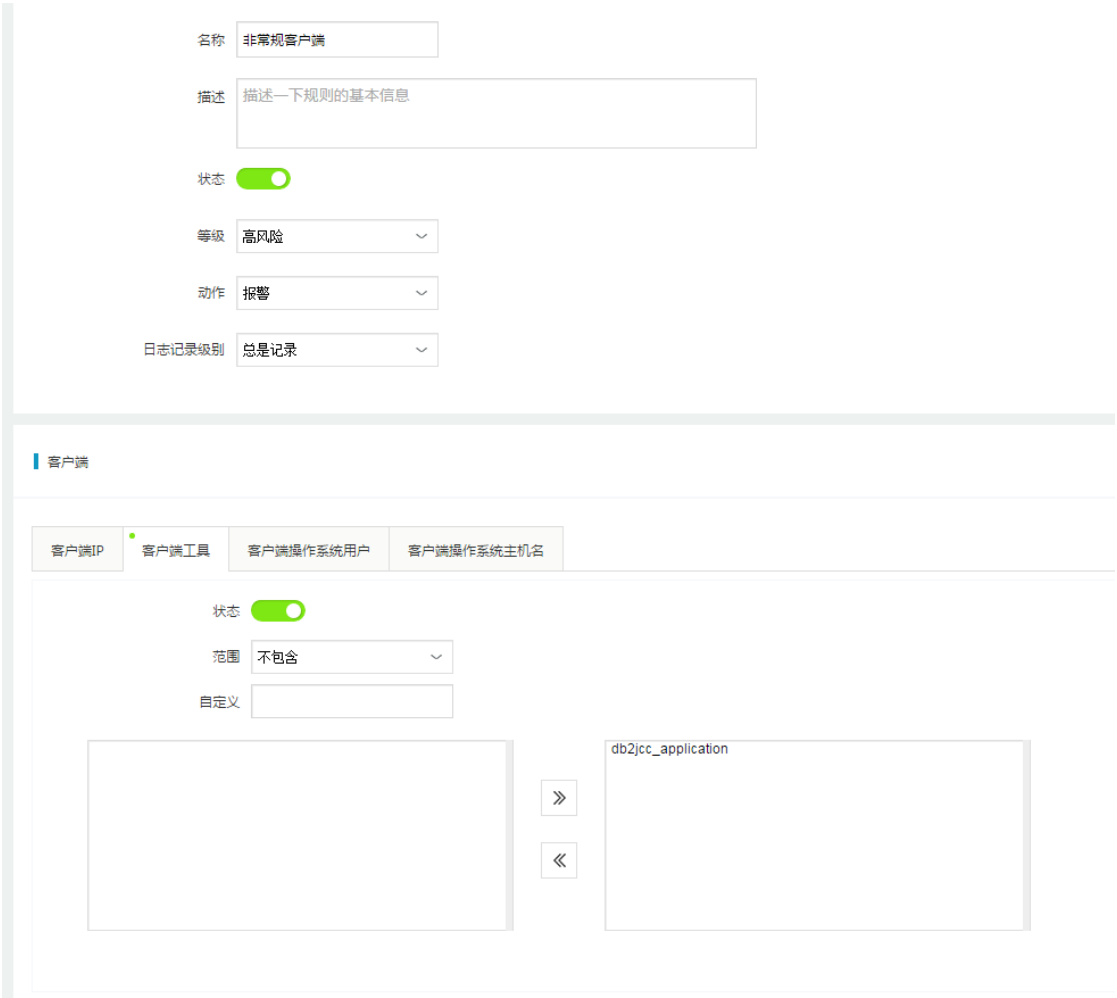
将非授权用户操作数据库视为高风险并阻断，策略配置如下图：





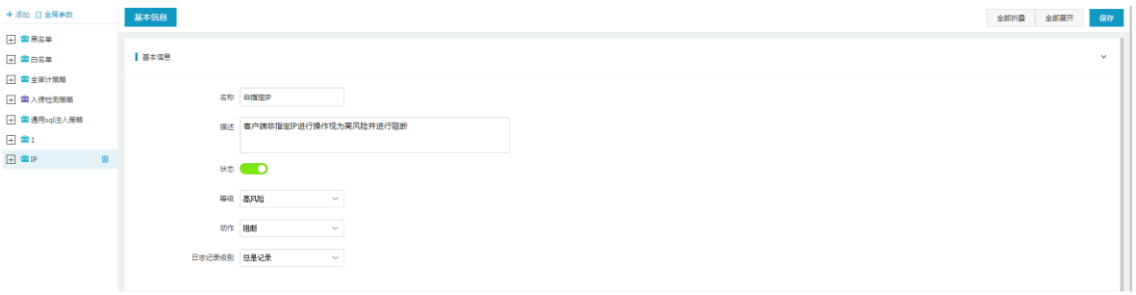
示例 5：非常规客户端

将非常规客户端操作数据库视为高风险并报警，策略配置如下图：



示例 6：IP 黑名单

将客户端非指定范围的 IP 地址设为黑名单，策略配置如下图：



六、 常发生的问题

6.1 浏览器无法登录系统

1. 修改管理口 IP 后未保存。

解决：后台查看 IP 登录后重新修改并保存。

2. Web 端口错误。

解决：在浏览器地址中，明确输入“https://”的 URL 起始头。

3. 网络故障。

解决：查看网络连接，修复响应故障。

6.2 未产生审计数据

1. 数据镜像问题。

解决：检查交换机的数据镜像配置，或抓包镜像数据核对数据正确性，若确定是镜像问题，协调用户修改镜像。

2. 数据库引擎未开启。

解决：点击审计防火墙中“启动”按钮。

3. 策略未应用到数据库引擎上。

解决：配置数据库引擎到相应的策略规则上。

4. “日志记录级别”为“不记录”。

解决：检查“日志记录级别”是否配置为“不记录”。修改规则日志记录级别。

6.3 审计日志记录中响应状态为“未知”

在数据库审计引擎上“设置”列表中开启“数据库应答监控”功能

6.4 添加状态监控，用户名/密码正确但始终添加失败

数据库用户不具备查询状态监控所需数据的查询的权限；

使用 DBA 或让 DBA 管理员授权此用户有查询对所有系统表的查询权限。

6.5 单库概况，报表预览页面无数据

单库概况，报表预览页面，为了缓解资源占用，点击进入，页面不会下发获取数据，即便时间范围显示 1 个小时，需要点击“刷新页面”才会下发。

6.6 SQLserver 审计日志中不记录数据库用户名

在数据库审计设置界面开启“数据库登录辅助”功能，输入正确的数据库用户名密码，确保系统与数据库路由可达。

随后，您可以按照《用户手册》进行其他系统管理配置工作。

欢迎使用东软 NetEye 数据库审计系统。