

# 数据库审计产品快速购买配置指南

## 购买注意点

- 1.使用数据库审计之前，需要在访问数据库审计的客户端主机上先安装主机入侵检测（uhids），控制台页面有配置指导！
- 2.数据库审计与数据库必须在同一区，同一网络下才可以正常使用。
- 3、数据库审计不支持删除退费（季度/年付）
- 4、数据库审计各平台账号密码：

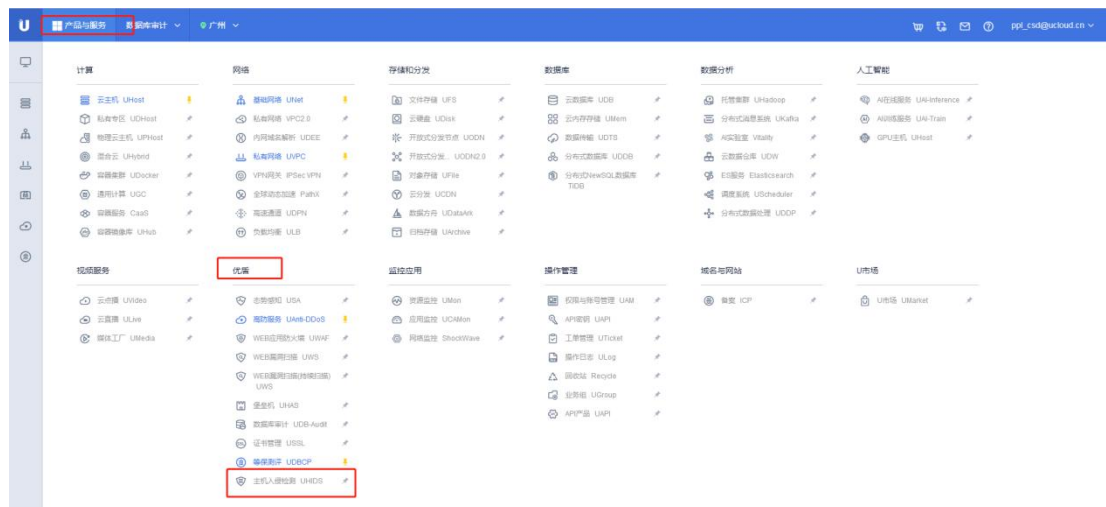
审计管理平台：auditadmin/!1fw@2soc#3vpn

规则管理平台：ruleadmin/!1fw@2soc#3vpn

系统管理平台：admin/!1fw@2soc#3vpn

## 第一部分部署 agent

在访问数据库的云主机上安装 uhids 指导如下：（数据库、数据库审计、云主机在同一，可用区，且网络可达）





## 第二部分 产品配置

### 数据库审计各平台账号：

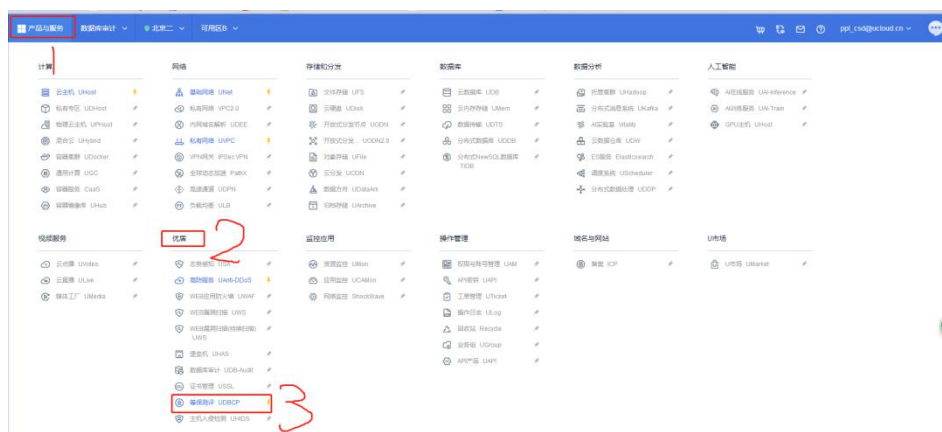
审计管理平台：auditadmin/!1fw@2soc#3vpn

规则管理平台：ruleadmin/!1fw@2soc#3vpn

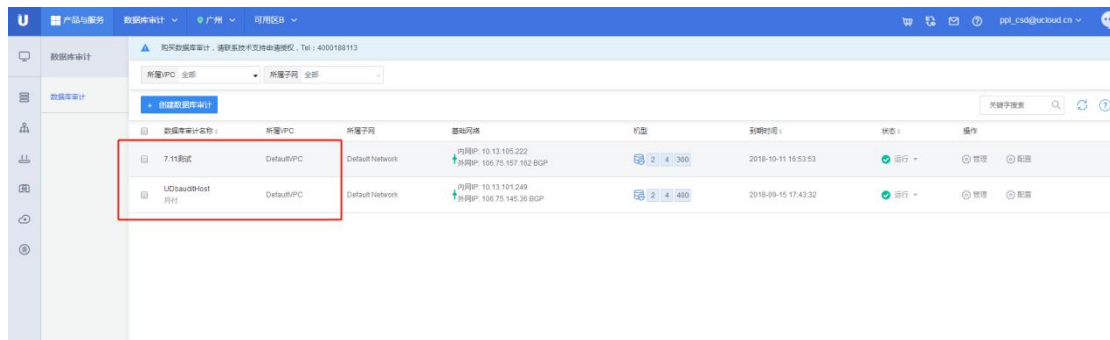
系统管理平台：admin/!1fw@2soc#3vpn

### 1、产品购买

登录控制台，选择左上角产品与服务，并找到优质下面对应的数据库审计一栏，进入并完成产品购买和安装页面

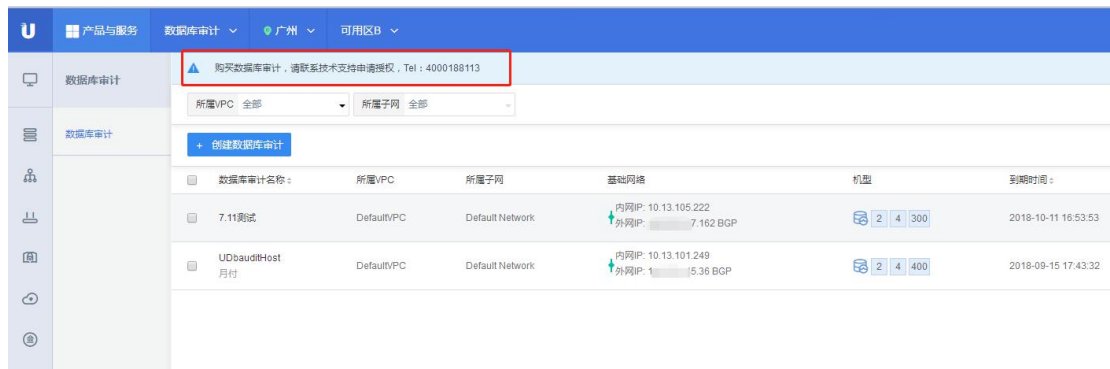


点击购买数据库审计，并选择相应的配置，完整支付及自动创建（大约 5 分钟）



## 2、申请并导入授权

默认创建的数据库审计是没有 license 授权的，需要联系技术支持，找到对应的负责人进行申请。



打开浏览器，在地址栏输入设备 https://EIP（建议使用 Google 浏览器），

登录系统管理员页面 admin/!1fw@2soc#3vpn ，下载注册信息文件，将授权给到申请人



拿到授权文件进行文件导入，导入之后就可以看到数据库审计具体的实例个数和有效时间

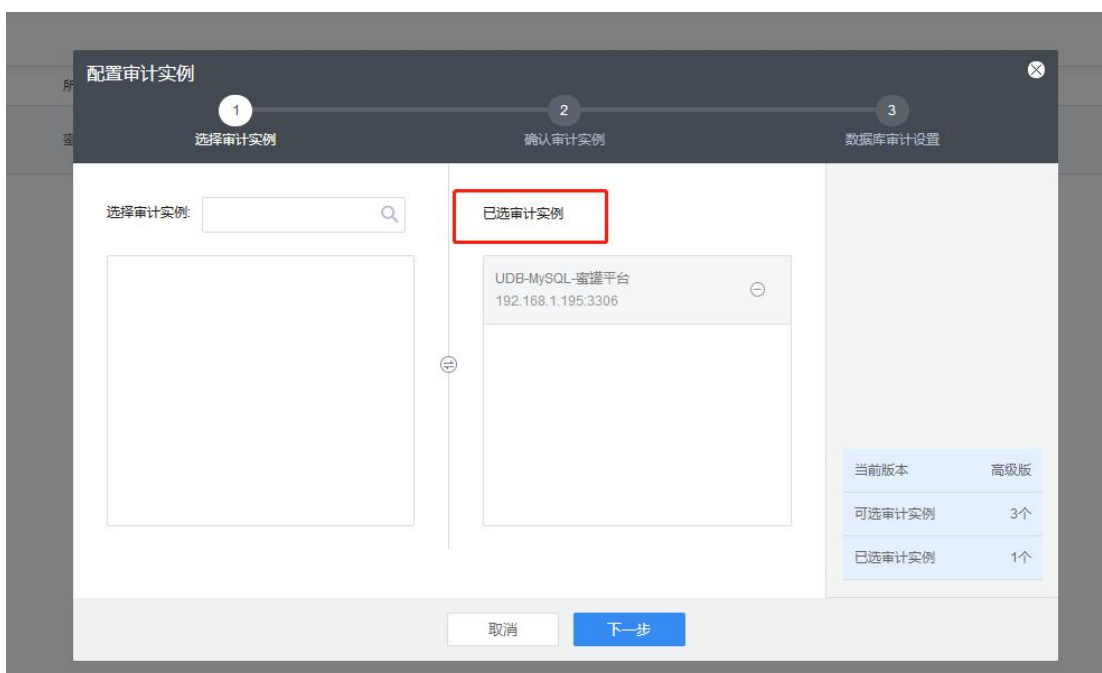


### 3、流量镜像策略

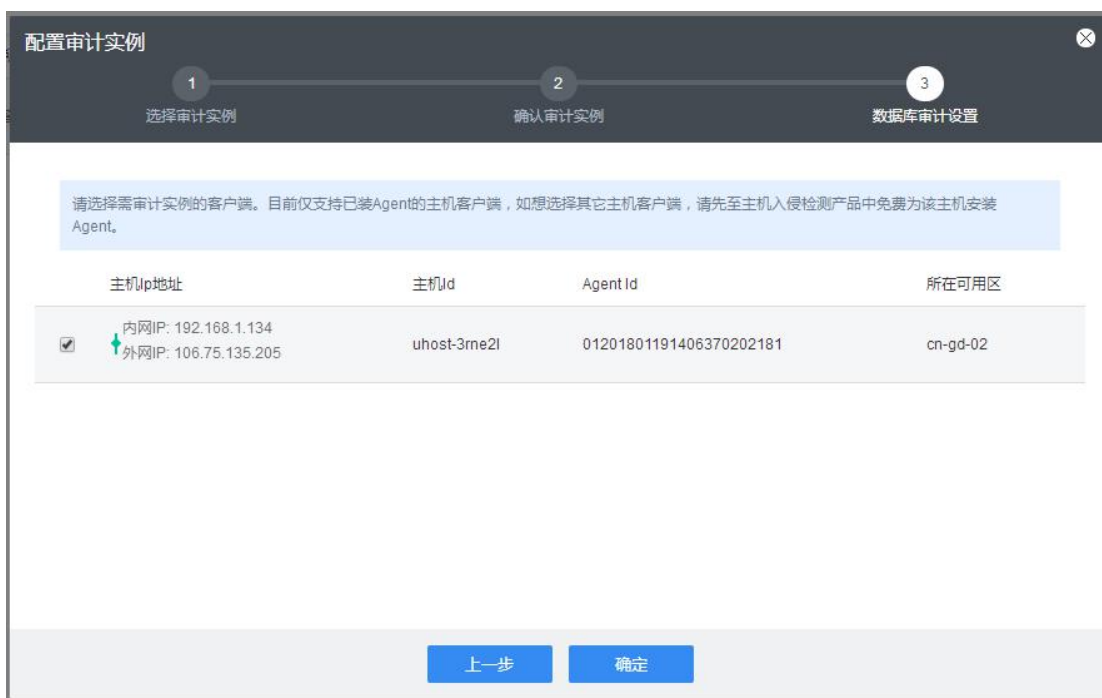
点击配置按钮



选择需要审计的数据库实例



选择访问数据库并部署 uhids 的云主机，并点击确认



## 4、审计规则配置

打开浏览器，在地址栏输入 https://EIP，在弹出的登陆页面输入规则用户名/密码：ruleadmin/!1fw@2soc#3vpn 后，进入规则配置平台。

点击对象设置-->审计对象，点击“添加”，输入需要被审计数据库服务器的相关信息，输入完成以后点击保存，（扩展配置可不填）如下图所示：

审计对象名:	某银行oracle数据库	状态:	启用
数据库类型:	Oracle	版本号:	Oracle 11g
服务地址:	172.30.112.151	端口:	1521
应用规则组:	某银行审计规则组	数据库编码:	GB2312
应用部门:	根部门	关联对象:	
HIS厂商:			
备注:			

☐ 扩展配置

保存

注：等保客户可直接勾选等级保护规则

## 第三部分 产品应用

打开浏览器，在地址栏输入 https://外网 IP，在弹出的登陆页面输入审计用户名/密码：auditadmin/!1fw@2soc#3vpn 后，进入审计管理平台。

### 1、日常行为查询

登陆审计管理平台，进入审计管理-->日常行为查询，输入或选择查询条件后，滚动鼠标到最下方，点击查询。（查询之前请先通过配置 uhids 的主机操作数据库并产生一定的流量）

审计对象:		风险级别:		操作类型:	
时间选择:	最近五分钟	开始时间:	先选择时间, 再选择日期	结束时间:	先选择时间, 再选择日期
客户端IP:		进程名:	等于	数据库账户:	等于
关键字一过滤:	等于	关键字二过滤:	等于		
不计算总数: <input checked="" type="checkbox"/> 勾选上之后可以增加查询的速度。					

注：查看能否审计到数据时，一般按照默认的选项进行查询就可以了。

## 2、审计结果显示

点击查询后出现下图的画面表示审计正常，设备基础配置到此完成。

查询结果

详细

导出报表菜单

文件导出

	发生时间	客户端IP	数据库账户	访问者	操作类型	表名	语句执行...	返回结果	风险...	处理...	操作语句
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input checked="" type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login
<input type="checkbox"/>	2019-07-15 15:...	10.13.173....	root		login(登...	/	失败	/	一般行为	已处理	login

1

第 1 页, 共 221 页

显示第1条到20条记录, 一共4410条

客户端信息

服务器端信息

操作语句

客户端IP及端口: 10.13.173.209:25570 发生时间: 2019-07-15 15:55:19 操作系统主机名: /  
操作系统用户名: / 源MAC地址: 52:54:00:06:E6:BD 客户端进程: / 应用账户: / 数据库账户: root

服务器端IP及端口: 10.13.113.63:3306 服务器端MAC地址: 52:54:00:75:6E:86

login

全屏查看