

数据库审计快速购买配置指南【6.0】

购买注意点

1、云数据库环境配置，需要在 agent 的引流下完成审计的整个过程

云数据库：agent 部署在访问数据库的应用服务端（客户端）

自建数据库：agent 可部署在访问数据库的应用服务端（客户端）

agent 也可部署在自建数据库的底层操作系统上（服务端），但会占用底层主机的性能（CPU、内存阈值不超过主机整体的 5%），部署前需先评估业务流量大小机底层主机性能，

2、数据库审计、数据库、应用服务器建议在同一内网环境，不推荐外网访问（数据转发为明文传输）

3、数据库审计不支持到期前删除退费（季度/年付）

4、数据库审计 6.0 各平台默认账号密码：

系统管理员 sysadmin/3edc\$RFV

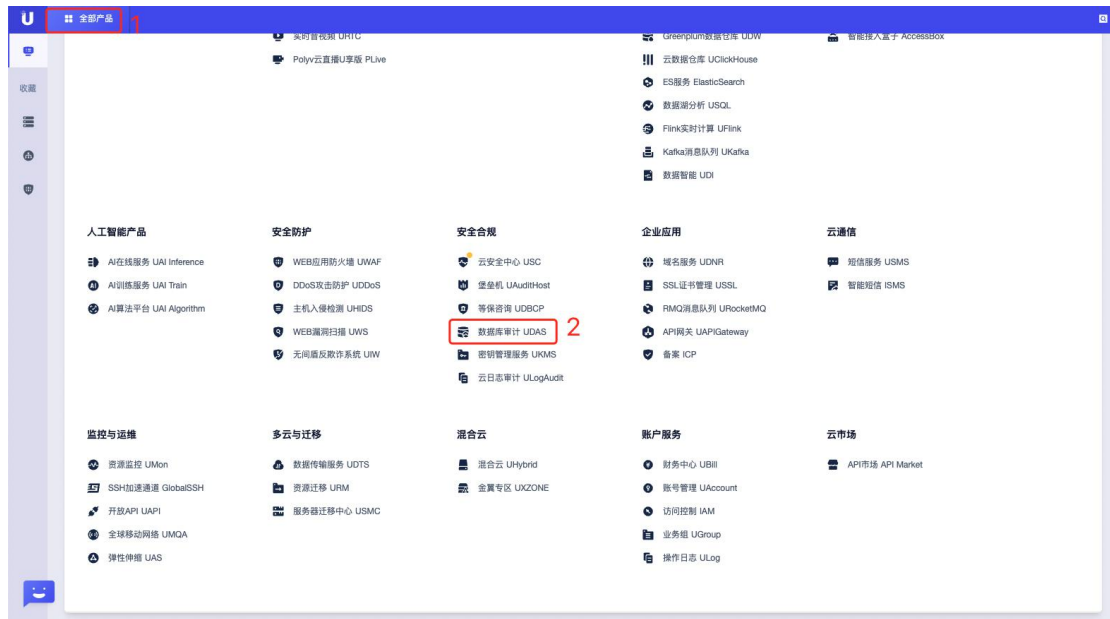
安全管理员 secadmin/3edc\$RFV

审计管理员 auditadmin/3edc\$RFV

第一部分、产品部署

1、产品购买

登录控制台，选择左上角产品与服务，并找到优盾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）



地域

地域可用区

华北（北京）

可用区B

配置选择

产品类型

数据库审计系统

数据库审计版本

高级版

企业版

旗舰版

CPU: 4核, 内存:8G, 系统盘:60G, 可审计数据库实例3个

峰值: 3600条SQL语句/秒级吞吐量, 300万/小时入库速度, 在线SQL语句存储8亿条（日志可实现网络转存）

磁盘

系统盘

60 GB

数据盘

300 GB

网络设置

所属VPC

DefaultVPC

所属子网

DefaultNetwork(10.9.0.0/16)

剩余IP数: 49147

外网弹性IP

☒ 购买并绑定

计费方式

带宽计费

流量计费

共享带宽

带宽:

2 Mb

防火墙

非Web服务器推荐(22, 3389)

管理设置

数据库审计名称

udbaudit

购买数量

1 台

月付

3个月

月单价: 元/月

年付

1年

SALE

折价: 元/月

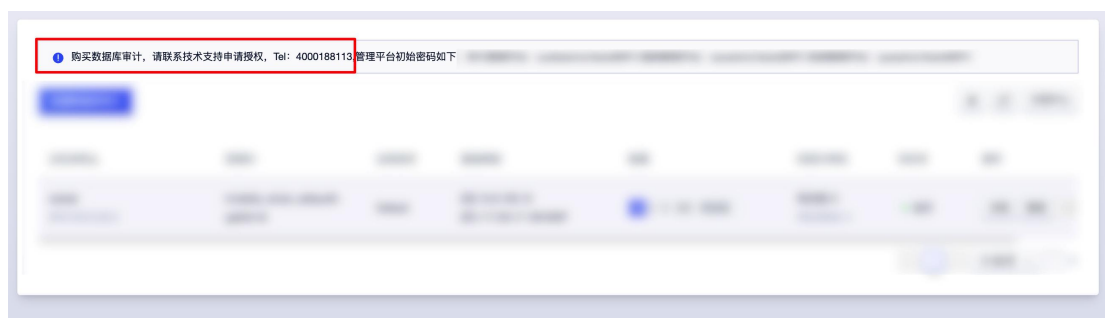
支付费用

元

立即购买

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），登录系统管理平台 `sysadmin/3edc$RFV`，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、下载 agent

系统管理平台-部署方式（支持 Linux 和 windows 版本的 agent），下载对应版本的 agent,



4、agent 部署

参考对应版本 agent 部署文档

《Linux_agent 部署指导-V6.0》

《windows_agent 部署指导-V6.0》

5、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：安全管理员 secadmin/3edc\$RFV 后，安全管理平台。

点击‘保护对象’，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，如下图所示：





注：操作日志全量审计，审计策略为触发对应规则的风险告警

第二部分 产品应用

1、日常行为审计查询

在目前的安全管理平台，检索模块，选择对应的检索条件，点击检索



注：查看能否审计到数据时，检索条件选择不选也可以。

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。

Ucloud

数据库审计系统UDAS - 安全管理平台

退出

监控墙

保护对象

风险

检索

报表

审计管理

策略管理

对象管理

告警

检索条件

时间: 不限 最近一分钟 最近五分钟 最近十分钟 最近半小时 最近一小时 最近十二小时 今天 本周 本月 自定义时间

风险级别: 高风险 中风险 低风险 关注行为 一般行为

保护对象: UDB-数据库审计测试 操作类型: 请选择

访问工具: 等于 请选择 数据库账户: 等于 多个数据库账户用,隔开

客户端IP: 等于 多个IP用,隔开

应用用户: 等于 请选择

关键字过滤: 等于 模糊匹配请使用*, 多个关键字请使用空格隔开

搜索 重置

检索结果

显示的列

| 时间 | 风险级别 | 客户端IP | 服务端IP | 操作类型 | 数据库账户 | 操作语句 | 回应 | 操作 |
|---------------------|------|---------------|--------------|--------|-------|---------------------|----|----|
| 2021-07-09 20:54:21 | 一般行为 | 10.13.167.121 | 10.13.42.201 | logout | | logout | 成功 | |
| 2021-07-09 20:54:21 | 一般行为 | 10.13.167.121 | 10.13.42.201 | logout | | logout | 成功 | |
| 2021-07-09 18:38:05 | 一般行为 | 10.13.167.121 | 10.13.42.201 | logout | | logout | 成功 | |
| 2021-07-09 18:38:05 | 一般行为 | 10.13.167.121 | 10.13.42.201 | logout | | logout | 成功 | |
| 2021-07-09 18:36:4 | | | | | | select @@character_ | | |