阿里云 vDAS 部署实施指导书

深信服智安全
SANGFOR SECURITY

深信服科技股份有限公司

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

修订历史					
编号	**修订内容简述**	**修订日期**	**修订前版本号**	**修订后版本号**	**修订人**
1	阿里云 vDAS 部署实施指导书	20191031	1.0	1.0	Chenke
2					
3					

目录

第 1 章 需求背景

目前大量用户为了减轻运维和数据不落地的需求采用了公有云托管业务，但是一直以来公有云架构的安全防护方面一直处于劣势，需要借助第三方安全虚拟化组件来补齐短板。依托该需求深信服推出了基于阿里云的数据库审计解决方案，实现阿里云上数据库审计的场景需求，解决客户痛点。

第 2 章 部署概述

2.1 阿里云平台特性描述

- 底层架构为 KVM
- 能够自定义上传镜像格式包括 raw
- 能够自定义安全规则
- 支持绑定浮动 IP
- 支持添加 1-2 块网卡

2.2 镜像获取

vDAS 镜像已经上传阿里云镜像市场，用户直接在阿里云镜像市场搜索“深信服数据库安全审计”就可以获取相应镜像。

2.3 部署方式

vDAS 支持旁路部署（需要在数据库服务器上安装 agent），不支持镜像部署。

2.4 资源配置

规格	配置参数	吞吐量	磁盘
vDAS-200	2 CPU,4G RAM	200Mb/s	具体大小需要根据实际情况来配置，不少于 81G。
vDAS-400	4 CPU,8G RAM	400Mb/s	具体大小需要根据实际情况来配置，不少于 81G。
vDAS-600	8 CPU,16G RAM	600Mb/s	具体大小需要根据实际情况来配置，不少

			于 81G。

2.5 授权方式

1、 支持在线试用
2、 支持在线授权

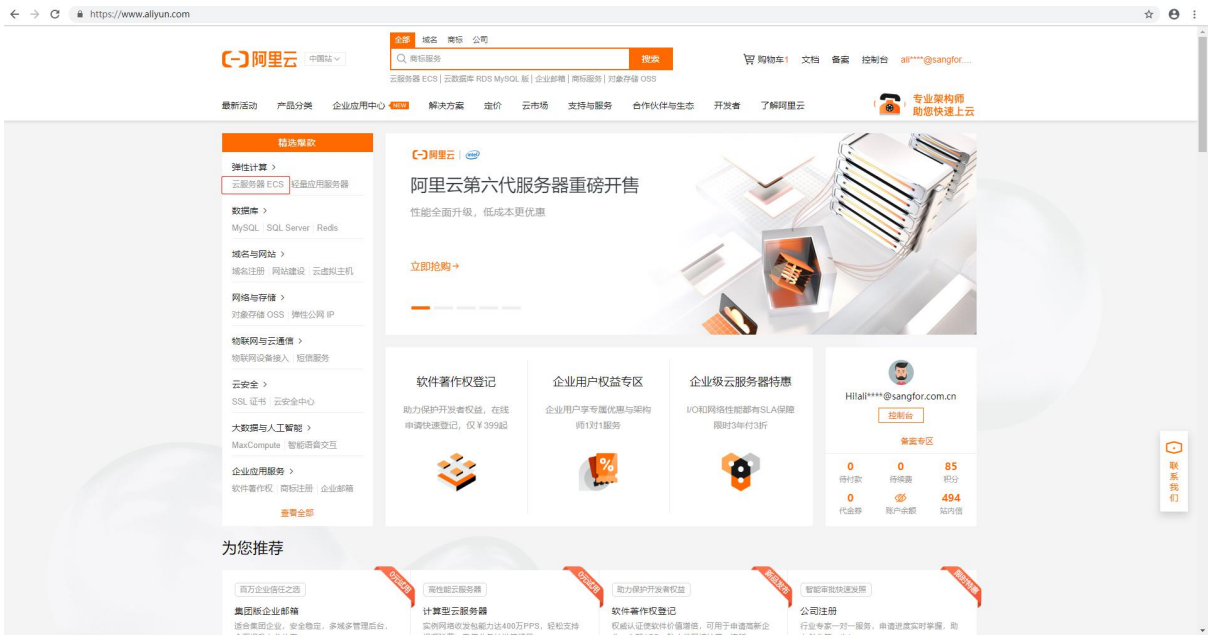
第 3 章　部署指导

3.1 云平台配置

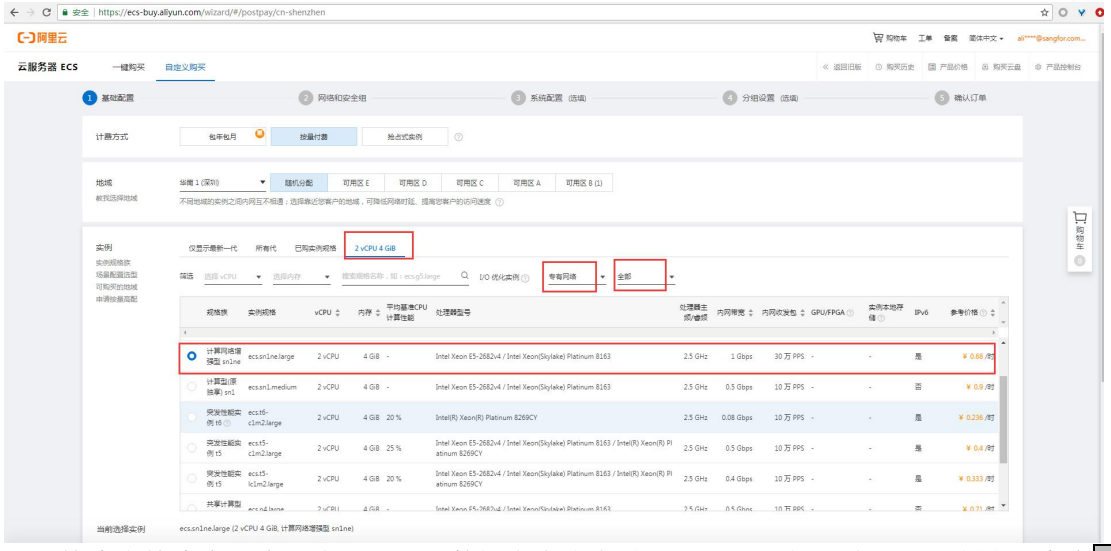
深信服 vDAS 是以系统镜像的方式提供的，部署深信服 vDAS 需要先提供一台独立的 ECS 主机来安装 vDAS 镜像。

3.1.1 创建 ECS 虚拟机

登录阿里云中国站，点击购买 ECS 云服务器。



出现以下选择页面，参考【2.4 资源配置】，按照实际需求选择对应的服务器，例如选择 2 核 CPU、4G 内存的云服务器。实例类型需要选择（计算网络增强型 sn1n）型号，其他型号的 cpu 可能会出现网卡适配不了网络配置无法生效的问题。

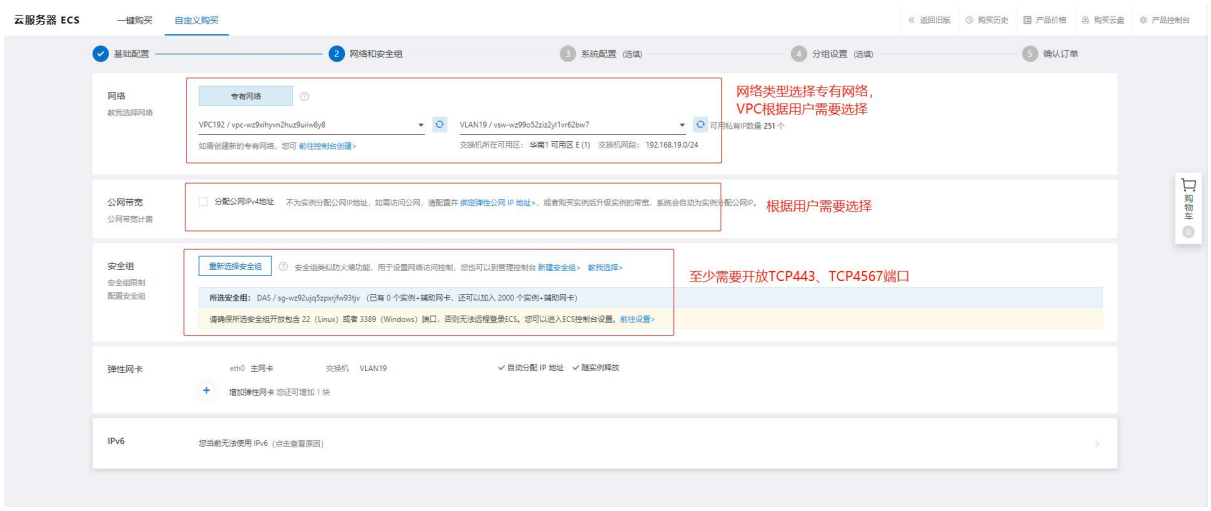


镜像在镜像市场中搜索“深信服数据库安全审计 ”即可看到，选择 2.0.2 版本，点击 使用 按钮。

【说明】国外阿里云市场没有深信服数据库审计镜像，需要联系深信服工程师通过共享镜像的方式来提供。

存储选择按照需求选择高效云盘或者 SSD 云盘，存储选择 81G 以上，不需要选择额外的数据盘。

3.1.2 配置网络和安全组



网络需要选择专有网络，需要选择业务虚拟机所在的 VPC，VLAN 可以是跟业务虚拟机同一个，也可以是独立的 VLAN；

公网带宽根据实际情况选择，如果需要从公网直接访问 DAS 的控制台，则需要分配公网带宽；

安全组未配置默认进方向都是拦截，出方向都是放行的，若未定义则会导致创建好云主机后无法访问的情况，所以需要在安全组中放通 TCP443 端口（控制台管理）、TCP4567 端口（agent 同步日志端口）。

点击 新建安全组 跳转到新窗口设置安全组；

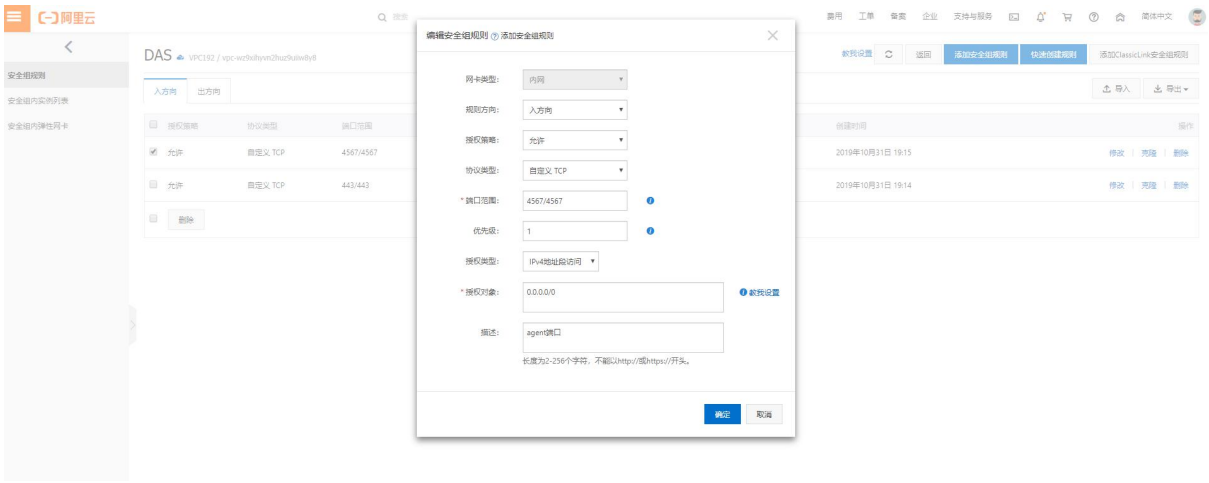
在新弹出的网页中点击 创建安全组 按钮；

模板选择自定义，名称按照实际情况填写，网络选择专有网络，最后点击 确定 按钮保存。

创建完成后，点击 配置规则 按钮添加规则；

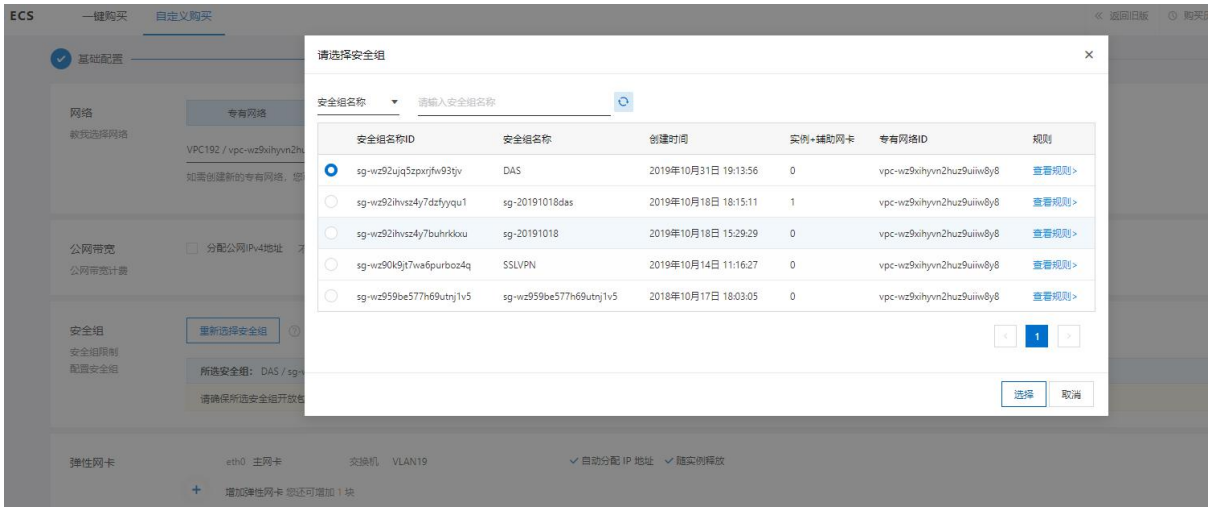
跳转到配置页面后，点击 添加安全组规则 按钮，然后在弹出的网页中逐个添加 TCP443、TCP4567 端口。

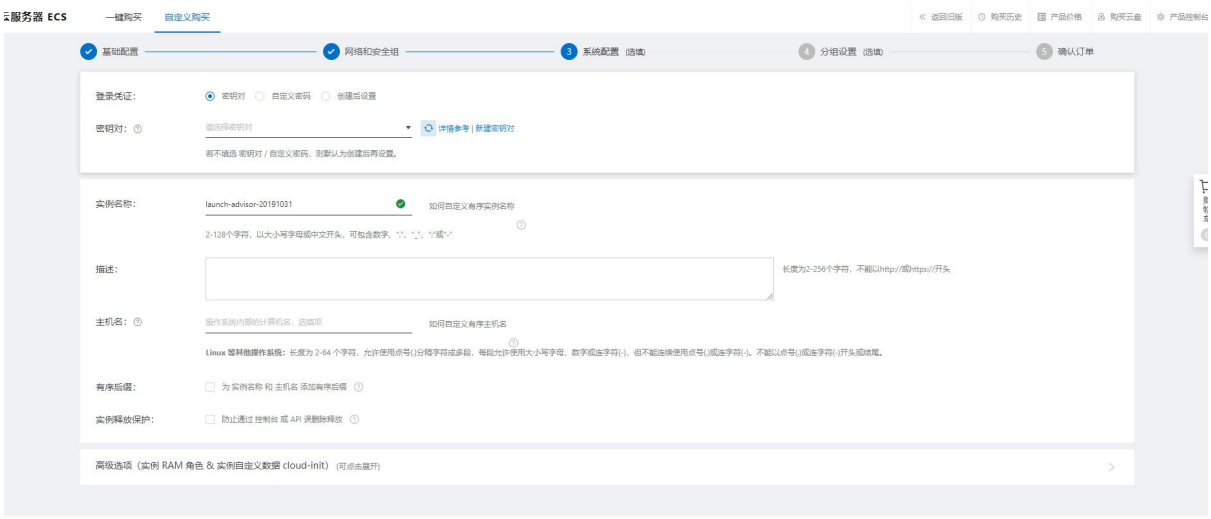
注：规则方向选择入方向；授权动作选择允许；授权对象填写 0.0.0.0/0（代表任意 IP，若有其他需求则按需填写）

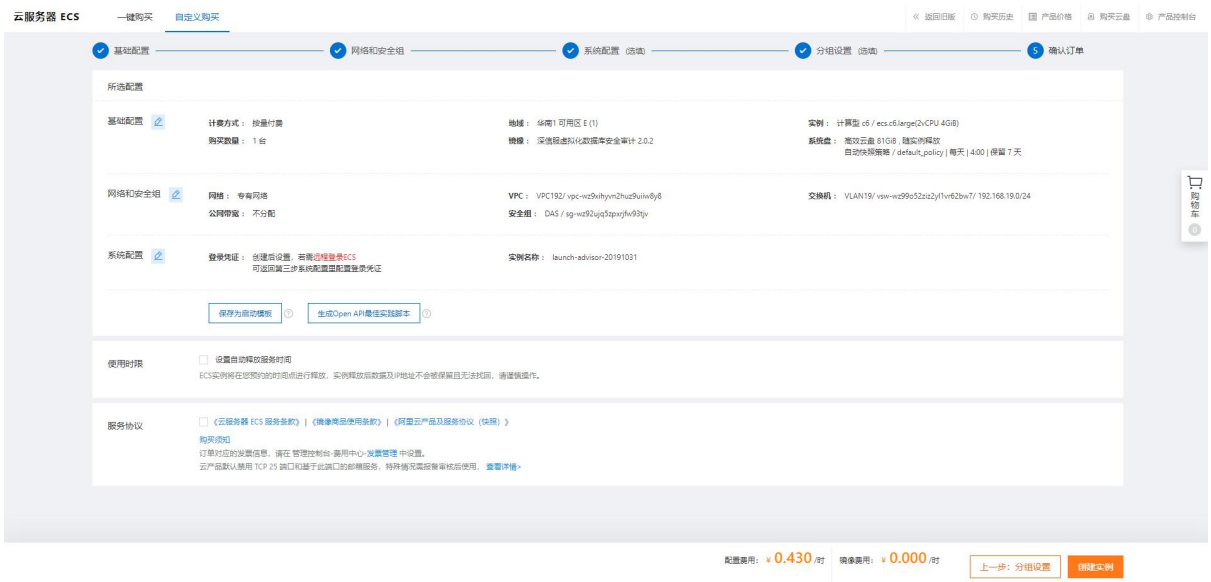


填写完成后回到配置云服务器的页面，点击 重新选择安全组 的按钮，选择刚刚创建的安全组，然后选择下一步；

后面的配置按照实际情况选择即可，一般情况下保持默认即可。







最后确认订单支付即可完成云主机的创建，创建完成后可以在实例列表里看到新建的 vDAS 主机的相关信息，包括运行状态、内网 IP 地址、EIP 地址、配置信息等。

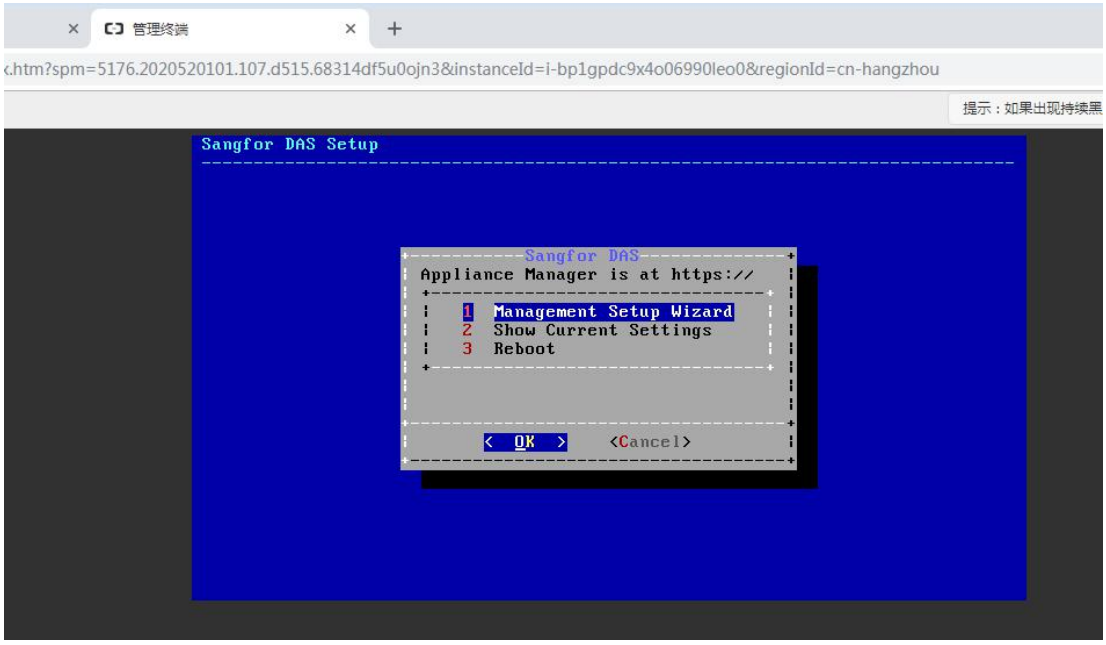
196424

3.2 网络配置

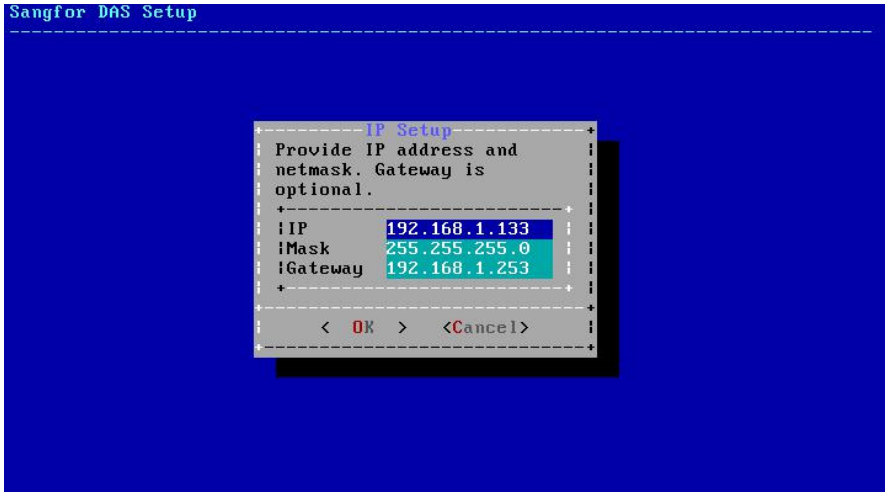
由于 DAS 不支持 DHCP，所以需要手工配置 DAS 的 IP 地址，具体配置方法如下：

首先在实例列表里查看 vDAS 实例的私网 IP，如下例，阿里云平台给 DAS 分配的私网地址是 192.168.1.133。

然后点击远程连接，进入到以下界面。

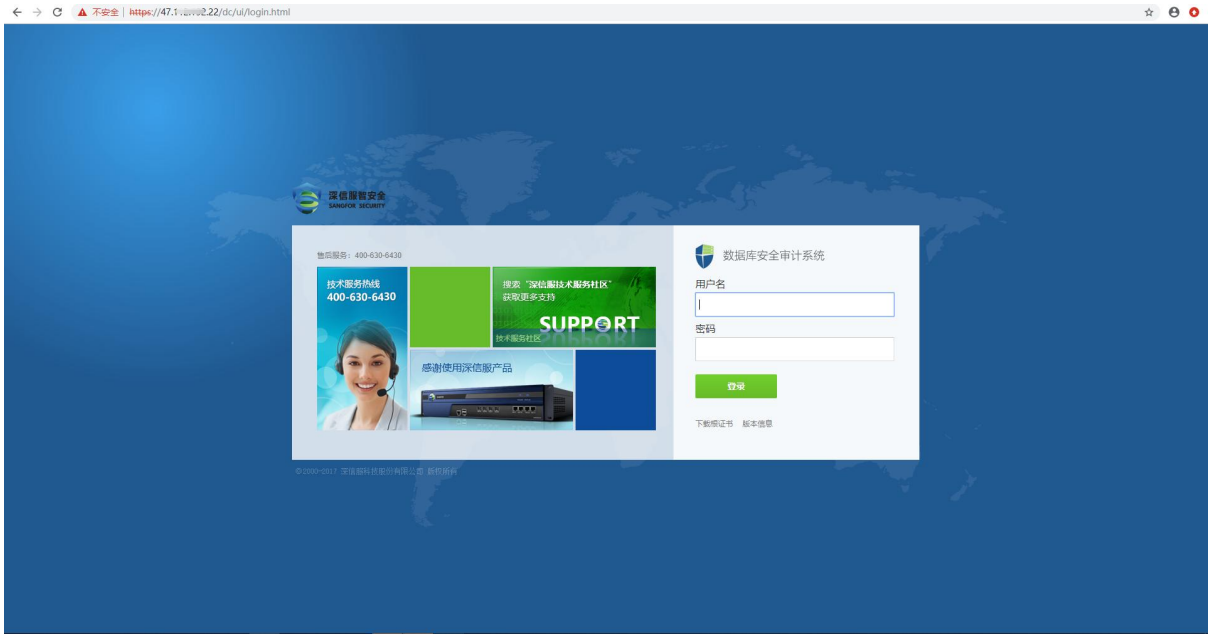


选择第一项 Management Setup Wizard，然后配置 DAS 的 IP、掩码和网关，其中 IP 配置成阿里云平台分配的私网 IP 地址，掩码配置成 VPC 设置的掩码，网关配置成 x.x.x.253，然后点击 OK 保存配置生效。



3.3 登陆控制台

IP 地址配置生效后，用户就可以通过私网 IP 或云平台给 DAS 分配的公网 IP（如果有）登陆 DAS 的 WEB 控制台页面了，登陆方式是 https://x.x.x.x。



默认的用户名和密码均为 admin，建议登录后及时修改密码。

3.4 云组件授权配置

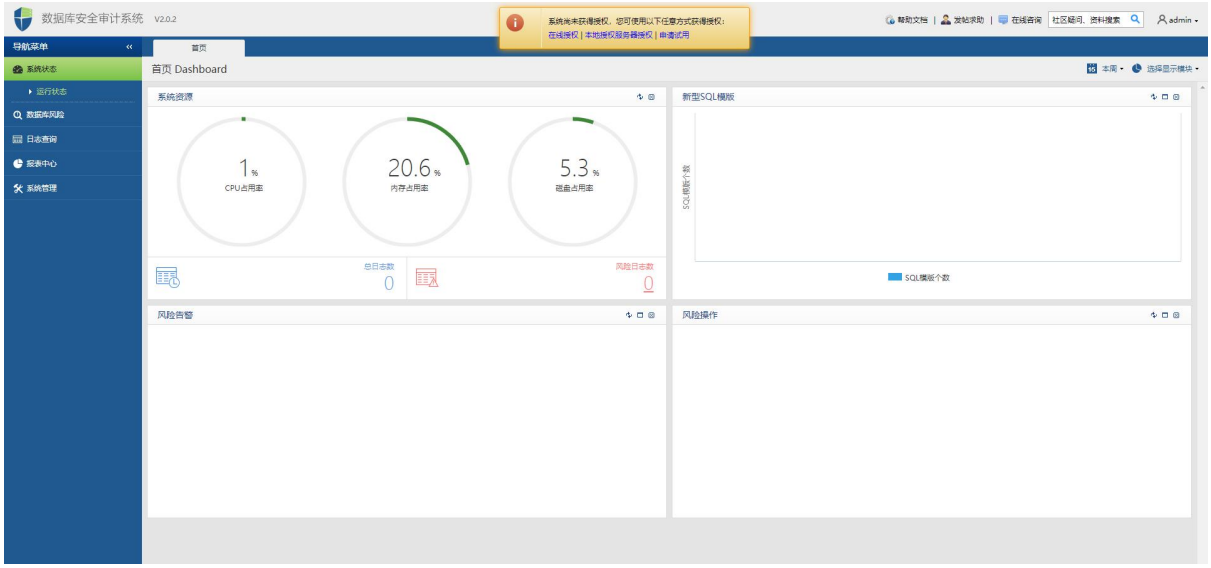
首次使用 vDAS 系统，需要先给 vDAS 授权。vDAS 授权分以下为三种，使用云主机只需关注“在线授权”和“申请试用”即可。

- 在线授权：需要先购买获得序列号，然后将序列号信息填写到对应的位置
- 本地授权服务器授权：需要在本地搭建一个授权服务器（VLS），使用授权服务器对 vDAS

来授权。

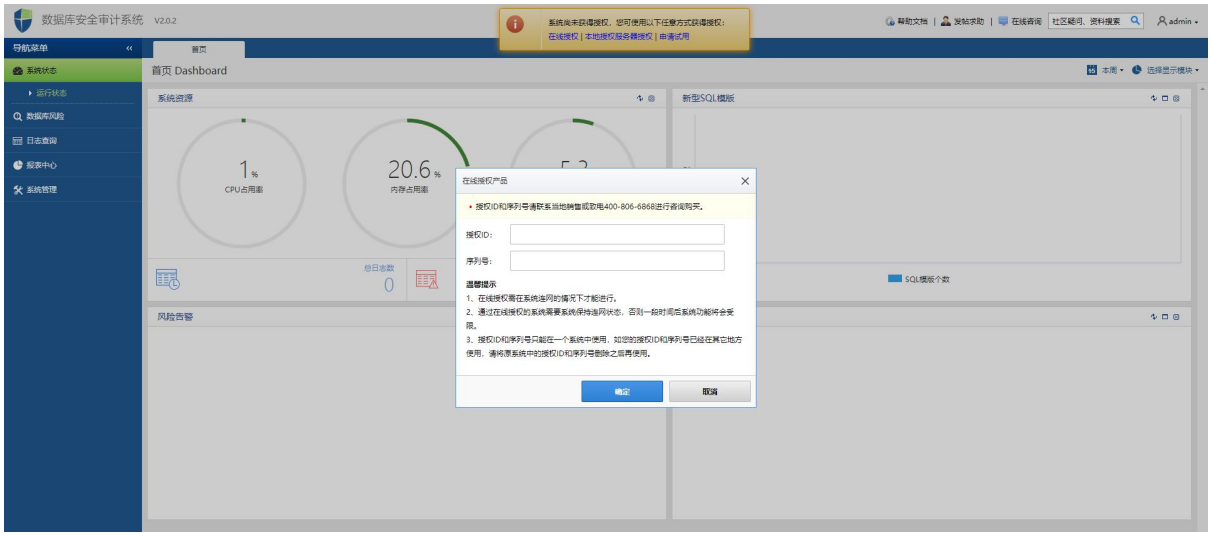
- 申请试用：只要填写申请信息即可通过短信方式获得授权序列号，把序列号填入【在线授权】即可，使用此序列号可以**免费试用 30 天**。

【在线授权】与【申请试用】都需要 vDAS 能够连接互联网，与 vls.sangfor.com.cn 的 443 端口保持通信。



3.4.1 在线授权

在线授权需要填写授权 ID 和序列号，请联系当地销售或致电 400-806-6868 进行咨询购买。
点击控制台的在线授权，将购买的授权序列号填写到对应位置，提交后等待设备进程重启后即可变为授权状态。



授权成功后在授权信息页面会有【更改授权】、【删除授权】和【授权服务器授权】三个选项。
【删除授权】和【授权服务器授权】都是删除掉当前的授权信息，使设备变为初始化状态；【更改授权】则是将新的序列号覆盖掉当前的，授权 ID 不会更改。

3.4.2 申请试用

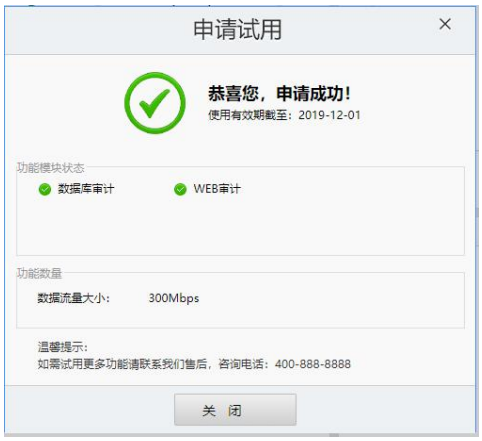
点击 申请试用， 填写对应信息。

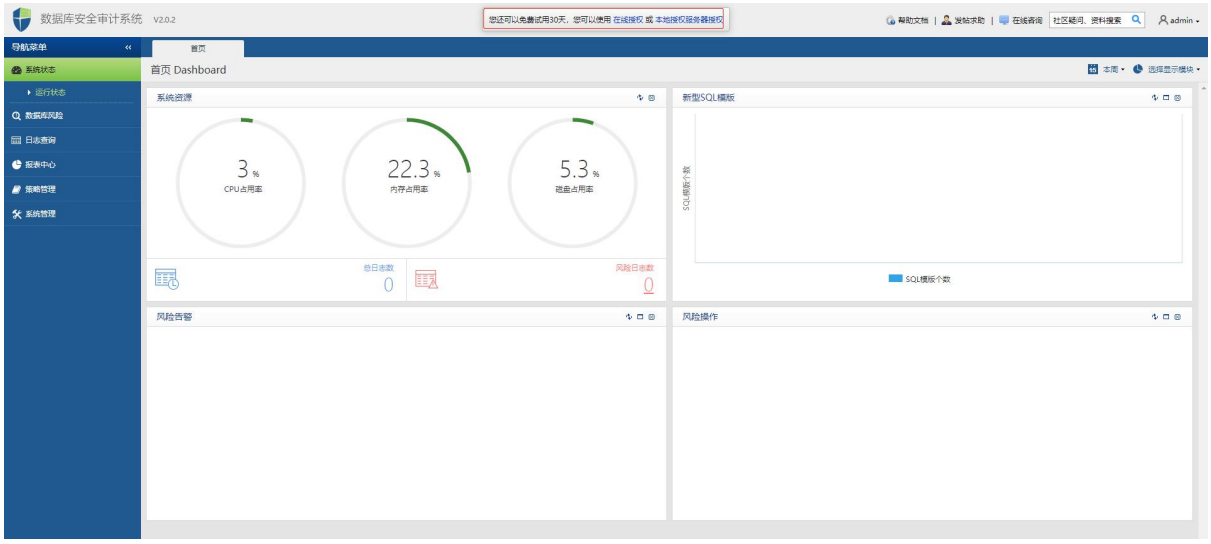
【姓名】、【手机号码】、【短信验证码】、【公司名称】和【产品用途】是必填项，提交申请后，会有审核人审批，审批完成后，会收到授权 ID 和授权序列号，把授权 ID 和授权序列号填入【在线授权】，填写成功后控制台会有提示：您还可以免费试用 30 天，您可以使用【在线授权】或【本地授权服务器授权】。

重新登录 vDAS 控制台，系统就会显示可以免费试用 30 天。

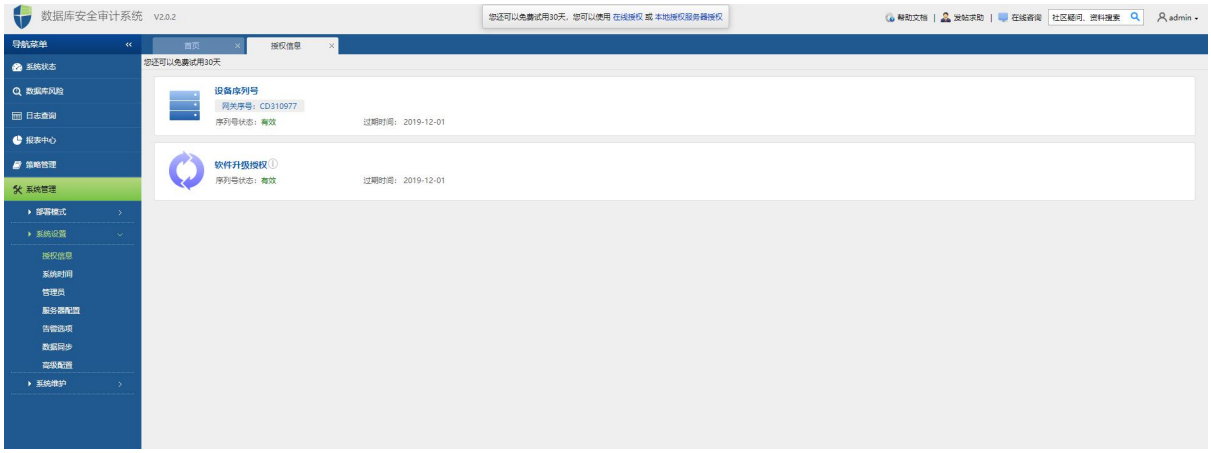
3.4.3 vDAS 授权说明

授权成功后，vDAS 控制台有授权客户和授权有效期的提示。





查看【系统管理】-【系统设置】页面，即可显示授权信息。



若因为某种原因（网络不可达等），连续 7 天未收到授权服务器的心跳信息，此时 vDAS 从授权切换到非法状态，非法状态时控制台不可配置业务，但原有的业务还可以继续使用。非法状态的设备登录后在首页头部有非法状态的提示。

导致非法状态的原因有序列号过期、授权资源与实际资源不匹配、序列号被禁用、序列号失效等，在控制台头部都会有对应的提示信息。

如果非法状态的设备经过 30 天还是没有收到正确的授权则都会变为初始化状态。由于设备是由已经授权过的设备转变为初始化状态，因此将不会再有免费试用的选项。

3.5 数据库审计功能配置

3.5.1 用户环境与需求

A 公司在阿里云上部署了若干数据库服务器，现在需要对所有访问数据库的行为进行记录。

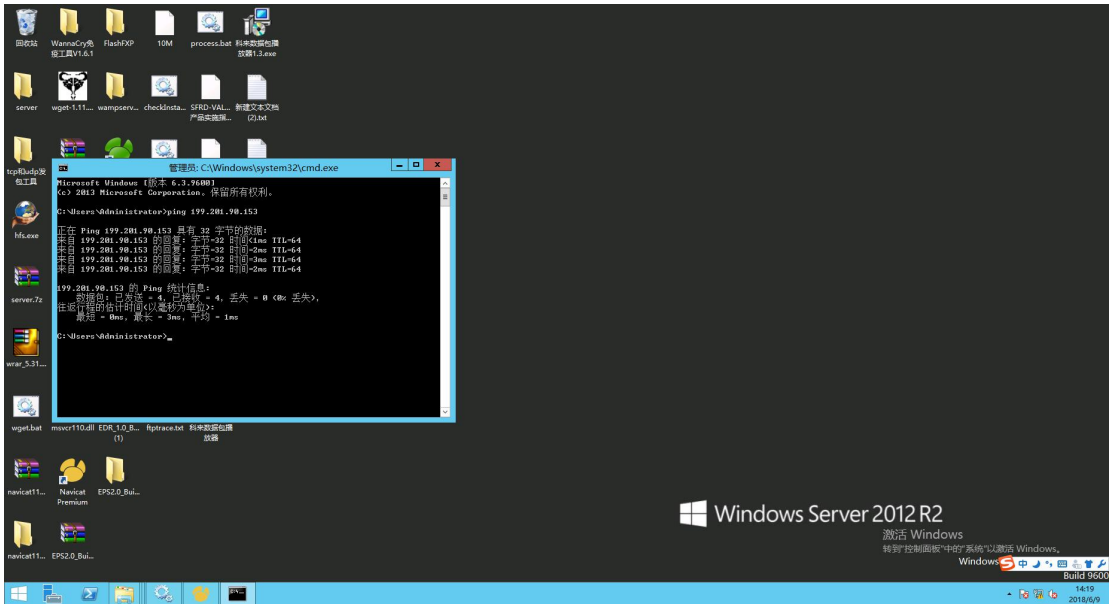
3.5.2 配置步骤

配置步骤如下：

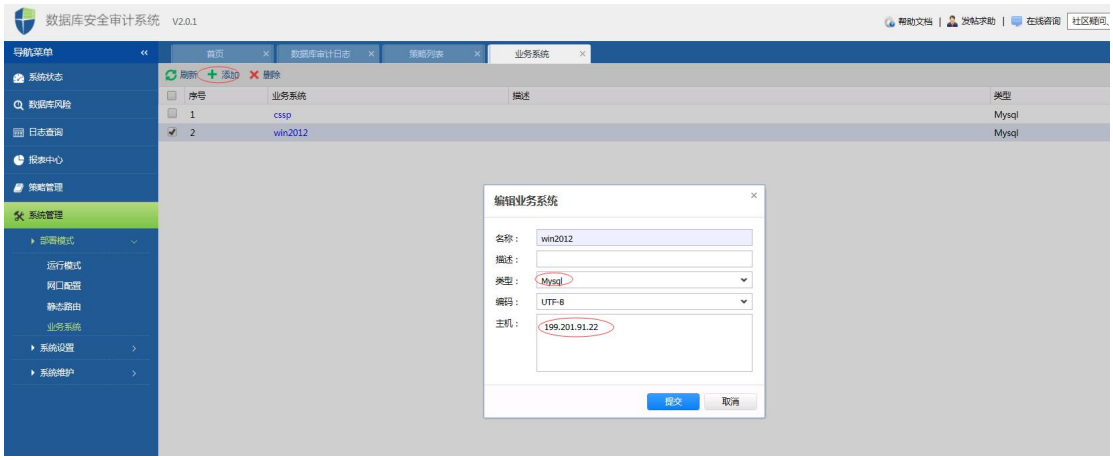
数据库审计可以记录常见的数据库操作日志，包括 Mysql、Oracle、SQL、DB2、Informix、KingBase、Dameng 等数据库的查询、修改、新增、删除等日志。

windows 主机数据库配置

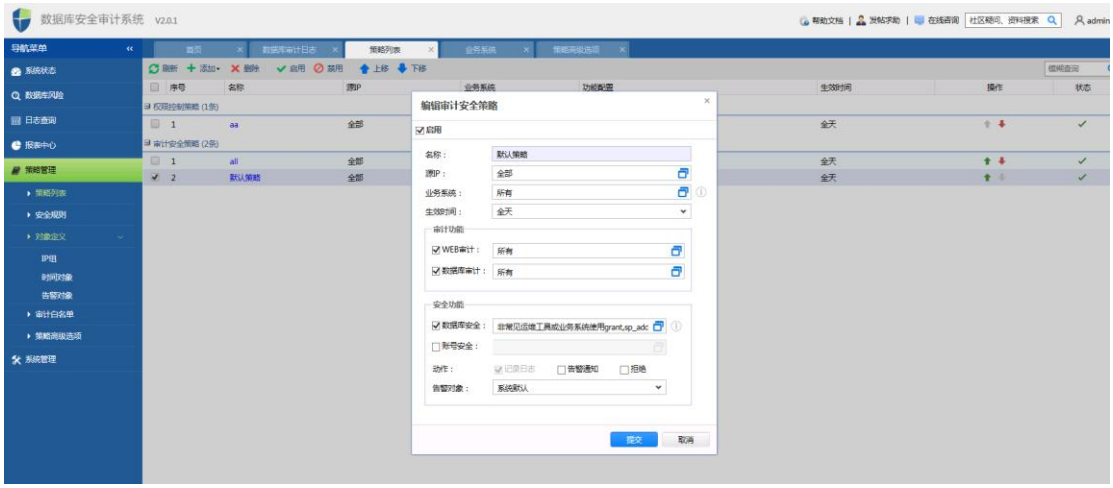
Windows 主机仅仅支持 64 位 Windows 2008 、64 位 Windows 2012。保证 windows 主机和数据库审计是可达的。



1) 新增一个业务系统，并配置对应的审计策略



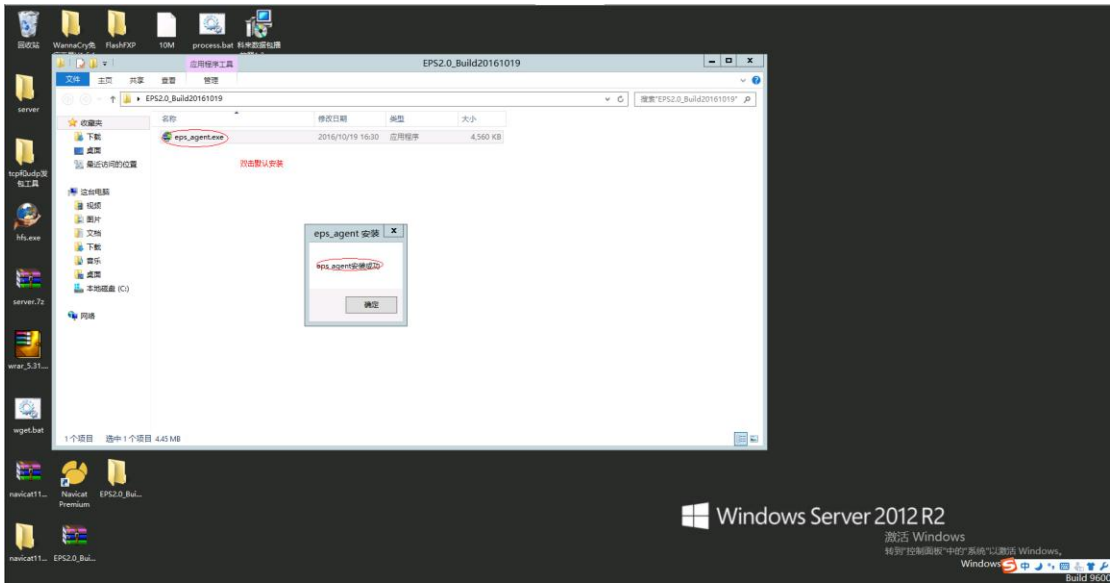
可以审计安全策略，审计功能和安全功能配置，同时还可以配置权限控制策略。



2) 通过下载 agent 安装文件

3) 进入到下载页面，支持 windows：64 位 Windows 2008 、64 位 Windows 2012；

4) 下载 windows 的 agent 安装文件到 windows，并安装成功；



默认安装路径 C:\Program Files\Sangfor\AC\EPS，需要改对应的配置文件；

C:\Program Files\Sangfor\AC\EPS\1.0.000000\config\das_agent.ini

[server]

#das_agent 连接服务端地址

host = 199.201.90.153

port = 4567

[capture]

#网卡配置(linux 下配置为网口名称，win 下面配置为本机网口 ip 地址)

dev = 199.201.91.22

#抓包过滤条件(配置为 shutdown 则停止抓包)

filter = tcp

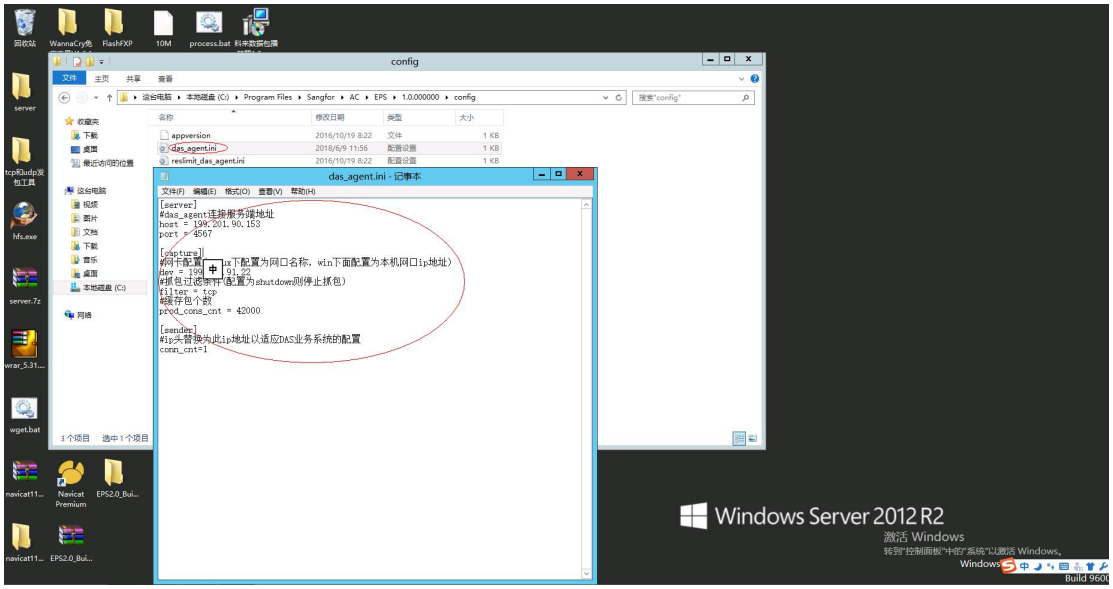
#缓存包个数

prod_cons_cnt = 42000

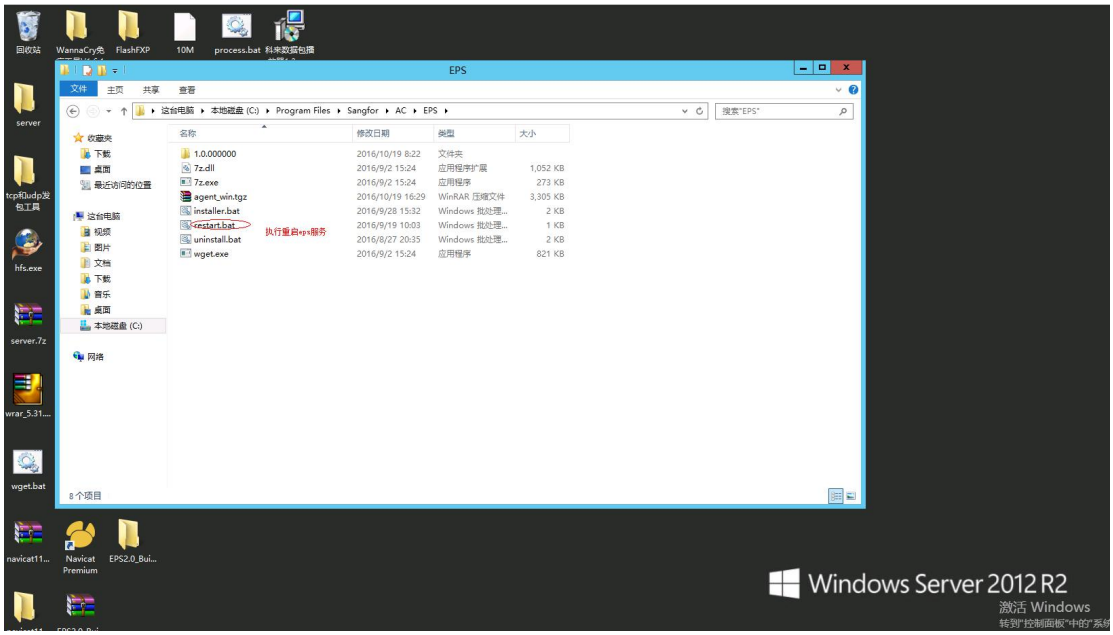
[sender]

#ip 头替换为此 ip 地址以适应 DAS 业务系统的配置

conn_cnt=1



5) 然后重启一下 eps 服务，双击重启服务

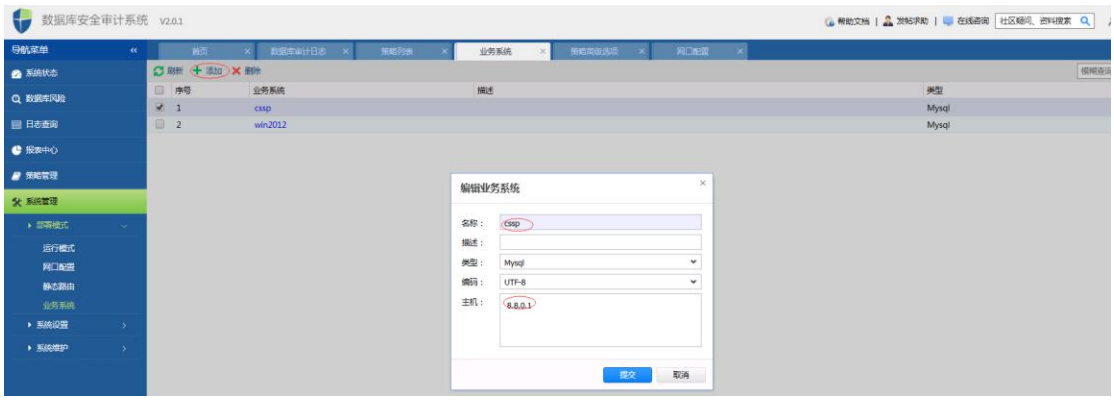


linux 主机数据库配置

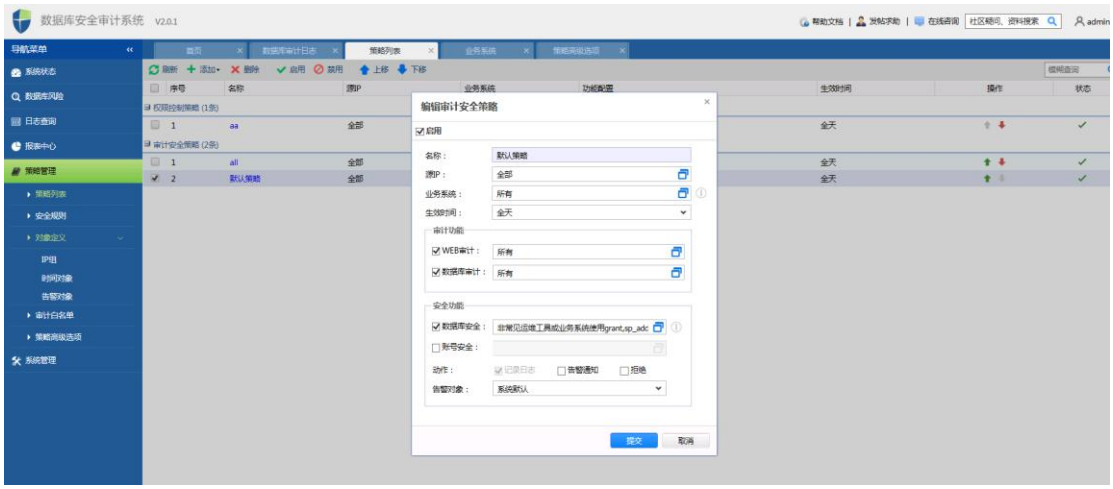
Linux 主机支持 linux：64 位的 CentOS 5/6/7、Debian 6/7、Ubuntu 10.04-14.4、RHEL 5/6/7。首先保证 Linux 可以与数据库审计可达；

```
root@CSSP4.0.3:~/vdas/bin$
root@CSSP4.0.3:~/vdas/bin$
root@CSSP4.0.3:~/vdas/bin$ping 8.8.0.23
PING 8.8.0.23 (8.8.0.23) 56(84) bytes of data.
64 bytes from 8.8.0.23: icmp_seq=1 ttl=63 time=2.88 ms
64 bytes from 8.8.0.23: icmp_seq=2 ttl=63 time=5.30 ms
64 bytes from 8.8.0.23: icmp_seq=3 ttl=63 time=11.4 ms
64 bytes from 8.8.0.23: icmp_seq=4 ttl=63 time=6.70 ms
^C
--- 8.8.0.23 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.885/6.578/11.425/3.114 ms
root@CSSP4.0.3:~/vdas/bin$
```

1) 新增一个业务系统，并配置对应的审计策略



可以审计安全策略，审计功能和安全功能配置，同时还可以配置权限控制策略。



2) 通过下载 agent 安装文件

3) 进入到下载页面，支持 linux：64 位的 CentOS 5/6/7、Debian 6/7、Ubuntu 10.04-14.4、RHEL 5/6/7。

4) 下载 Linux 的 agent 安装文件到 Linux，并安装成功；

```
root@CSSP4.0.3:~$./agent_installer.bin /root/vdas/
eps agent is installing on x86_64 machines
extract das_agent.tgz
extract eps_base.tgz
extract eps_packman.tgz
extract eps_sys.tgz
extract sfguard.tgz
/root/vdas/ install success
eps start success
root@CSSP4.0.3:~$
```

5) 给安装文件可执行权限 chmod +x agent_installer.bin

./agent_installer.bin /root/vdas （可选择需要安装路径）

```
root@CSSP4.0.3:~/vdas/config$pwd
/root/vdas/config
root@CSSP4.0.3:~/vdas/config$ls
5  aflog.proto  appversion  das_agent.ini  machineid  not5  reslimit_das_agent.ini  reslimit_logcli.ini  sfguardpath
```

[server]
#das_agent 连接服务端地址
host = 8.8.0.23
port = 4567
[capture]
#网卡配置(linux 下配置为网口名称，win 下面配置为本机网口 ip 地址)
dev = eth1
#抓包过滤条件(配置为 shutdown 则停止抓包)
filter = tcp
#缓存包个数
prod_cons_cnt = 42000
[sender]
#ip 头替换为此 ip 地址以适应 DAS 业务系统的配置
conn_cnt=1

```
root@CSSP4.0.3:~/vdas/config$cat das_agent.ini
[server]
#das_agent¿ ¿ ¿ ¿ ¿ ¿
host = 8.8.0.23
port = 4567

[capture]
#¿ ¿ ¿ ¿ (linux¿ ¿ ¿ ¿ ¿ ¿ ¿ ¿ ¿ win¿ ¿ ¿ ¿ ¿ ¿ ¿ ¿ ip¿ ¿ )
dev = eth1
#¿ ¿ ¿ ¿ ¿ ¿ (¿ ¿ ¿ shutdown¿ ¿ ¿ ¿ ¿ )
filter = tcp
#¿ ¿ ¿ ¿ ¿
prod_cons_cnt = 42000

[sender]
#ip¿ ¿ ¿ ¿ ¿ ip¿ ¿ ¿ ¿ ¿ DAS¿ ¿ ¿ ¿ ¿ ¿
conn_cnt=1
root@CSSP4.0.3:~/vdas/config$
```

6) 然后重启一下 eps 服务，双击重启服务

```
root@CSSP4.0.3:~/vdas/config$cd ../bin/
root@CSSP4.0.3:~/vdas/bin$ls
agent_list    cpulimit   enable_sshd_execmem  eps_monitor   eps_services_check.sh  epsxtest       ipc_probe    ipc_proxy  luadbg    resmon_export.sh  sfginject     sfglogs     sfgpromote.bashrc
agent_list.l  das_agent  eps_app              eps_services  eps_uninstall.sh       get_appversion  ipc_probe.l  lloader    patchelf  sfgconfig         sfginject.bin  sfgpromote  sfgpromote.l
root@CSSP4.0.3:~/vdas/bin$./eps_services restart
eps stop success
eps start success
root@CSSP4.0.3:~/vdas/bin$
```

7) 通过数据库审计日志查询对应的日志

第 4 章 常见问题

1、实例类型需要选择（计算网络增强型 sn1n）型号，其他型号的 cpu 可能会出现网卡适配不了网络配置无法生效的问题。