

**明御®综合日志审计平台**

**V3.0**

**华为云安恒明御综合日志审计平台购买指导说明**

**文档版本：01**

**发布日期：2020-11-13**

本文中出现的任何文字描述、文字格式、插图、照片、方法等内容，除另有特别注明，版权均属杭州安恒信息技术股份有限公司（简称“安恒信息”）所有，受到有关产权及版权法保护。任何个人、机构未经安恒信息的书面授权许可，不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的的单位或个人，应在授权范围内使用，并注明“来源：安恒信息”。违反上述声明者，安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外，本手册中出现的其他商标、产品标识及商品名称，由各自权利人拥有。

文档说明

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 | | 明御®综合日志审计平台 | |
| 适用平台/版本 | | V3.0 | |
| 拟制人 |  | **评审组** |  |
| 发布人 |  | **备注** | 受控 |

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 修改记录 | 修改人 |
| 2020-11-13 | 01 | 初次发布 |  |

目 录

1. 华为云安恒明御综合日志审计购买指导说明 1

1.1 说明 1

1.2 操作步骤 1

1.3 授权许可说明 5

2. 关于SSH登录华为云安恒综合日志审计系统后台的补充说明 6

2.1 说明 6

2.2 操作方法 6

1. 华为云安恒明御综合日志审计购买指导说明

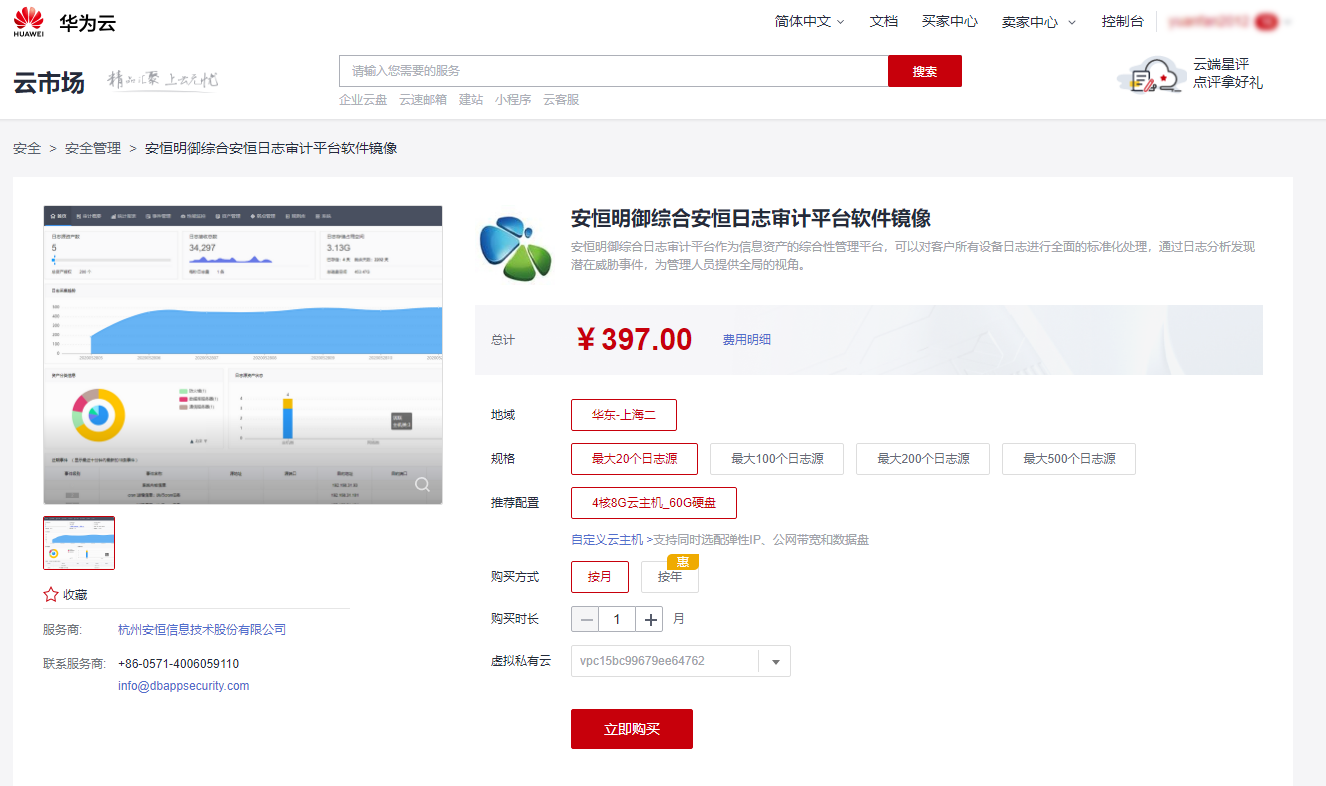
## 说明

明御®综合日志审计平台作为信息资产的综合性管理平台，通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件。为管理人员提供全局的视角，确保客户业务的不间断运营安全。通过采集网络资产设备上报的日志，实时监视网络各类操作行为及攻击信息。根据设置的规则，智能判断出各种风险行为，对风险行为进行报警。

本文档主要介绍在华为云市场如何进行购买安恒明御综合日志审计指导说明

## 操作步骤

1. 在华为云市场搜索安恒明御综合安恒日志审计平台软件镜像，选择对应的规格和推荐配置，确认购买方式按月或按年进行购买

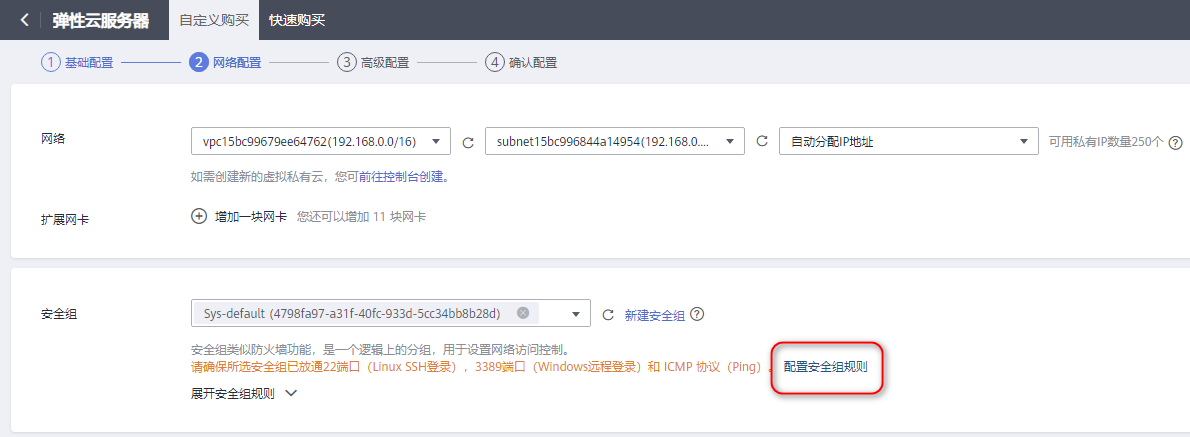


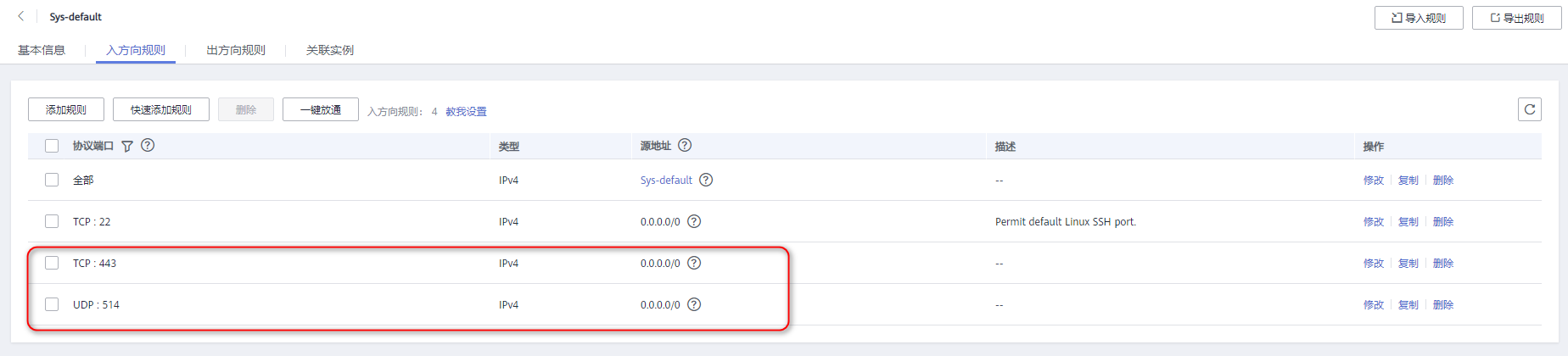
1. 在自定义购买界面添加一块数据不小于500G的数据盘



1. 自定义购买界面配置安全组规则

入方向规则中添加TCP 443和UDP 514端口的规则

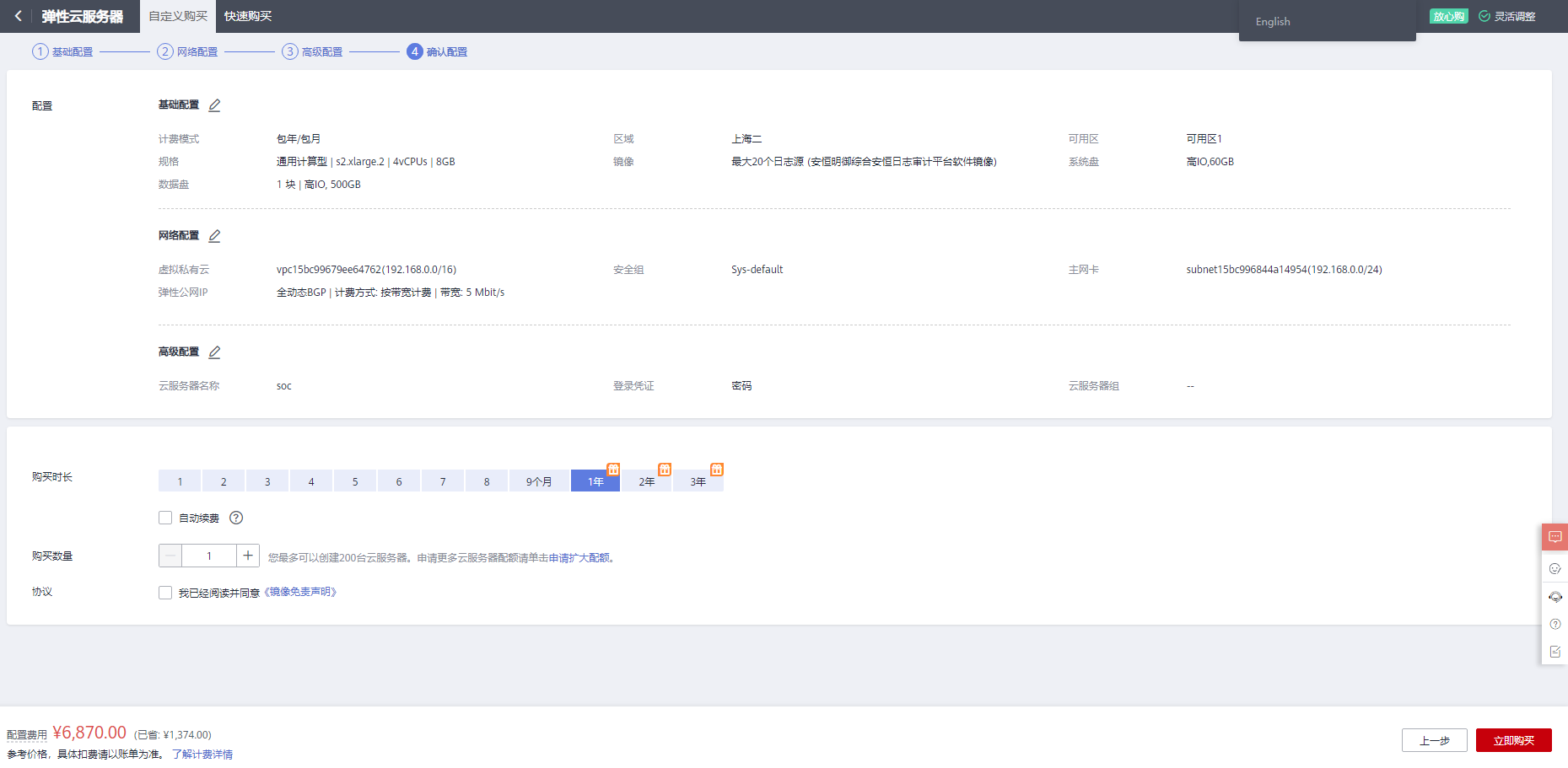




1. 设置root用户密码

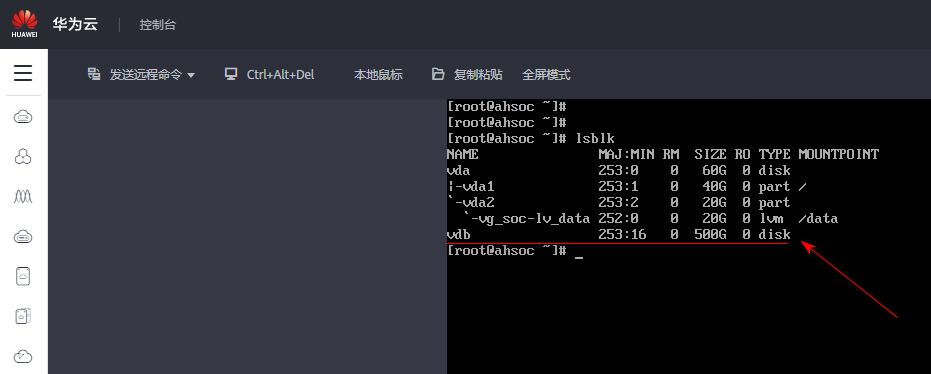


1. 确认购买的配置无误后，点击立即购买



1. 购买后在华为云主机控制台使用控制台提供的VNC方式登录云主机后台，检查数据盘大小，数据盘用于存储日志审计数据

确认在云主机后台使用lsblk命令能看到新增的这块新增的大容量数据盘



联系安恒技术服务热线4006059110进行云主机数据盘磁盘在线扩容操作

服务方式：远程支持服务

客服电话：4006059110 转7

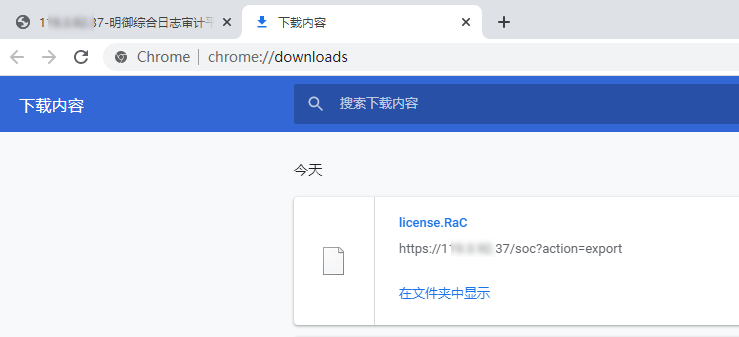
邮箱：400@dbappsecurity.com.cn

1. 在 华为云控制台，复制云主机的弹性公网 IP 地址，打开浏览器，输入 https:// 弹性公网 IP 地址 ，进入WEB 界面





点击许可导出，下载license.RaC



## 授权许可说明

购买完成后安恒明御综合安恒日志审计平台实例会自动运行，需要购买许可方能使用。

license 购买流程（购买前如有疑问请咨询客服 [客服电话：4006059110]）：

1、根据您单位情况，选择合适的最大资产数，并购买支付；

2、支付成功后联系客服核对信息，验证支付；

3、登录安恒明御综合安恒日志审计平台系统的web管理界面，点击“许可导出”按钮，会自动下载license.RaC文件；

4、在交付中心提交需求，上传license.RaC文件（由于上传不支持此后缀名，请先压缩为.zip或.rar文件上传） ；

5、服务商在交付中心提供许可文件，下载并解压出license.RaU文件；

6、在安恒明御综合安恒日志审计平台系统系统的web管理界面，点击“许可导入”按钮，上传license.RaU文件；

7、导入成功后可以看到相应的license注册信息，请核实，如果有问题请联系客服。

8、如果导入失败，请使用谷歌浏览器重新导入许可，如果有问题请联系客服。

\*\*注意\*\*：购买许可前，请先购买安恒明御综合安恒日志审计平台软件镜像

1. 关于SSH登录华为云安恒综合日志审计系统后台的补充说明

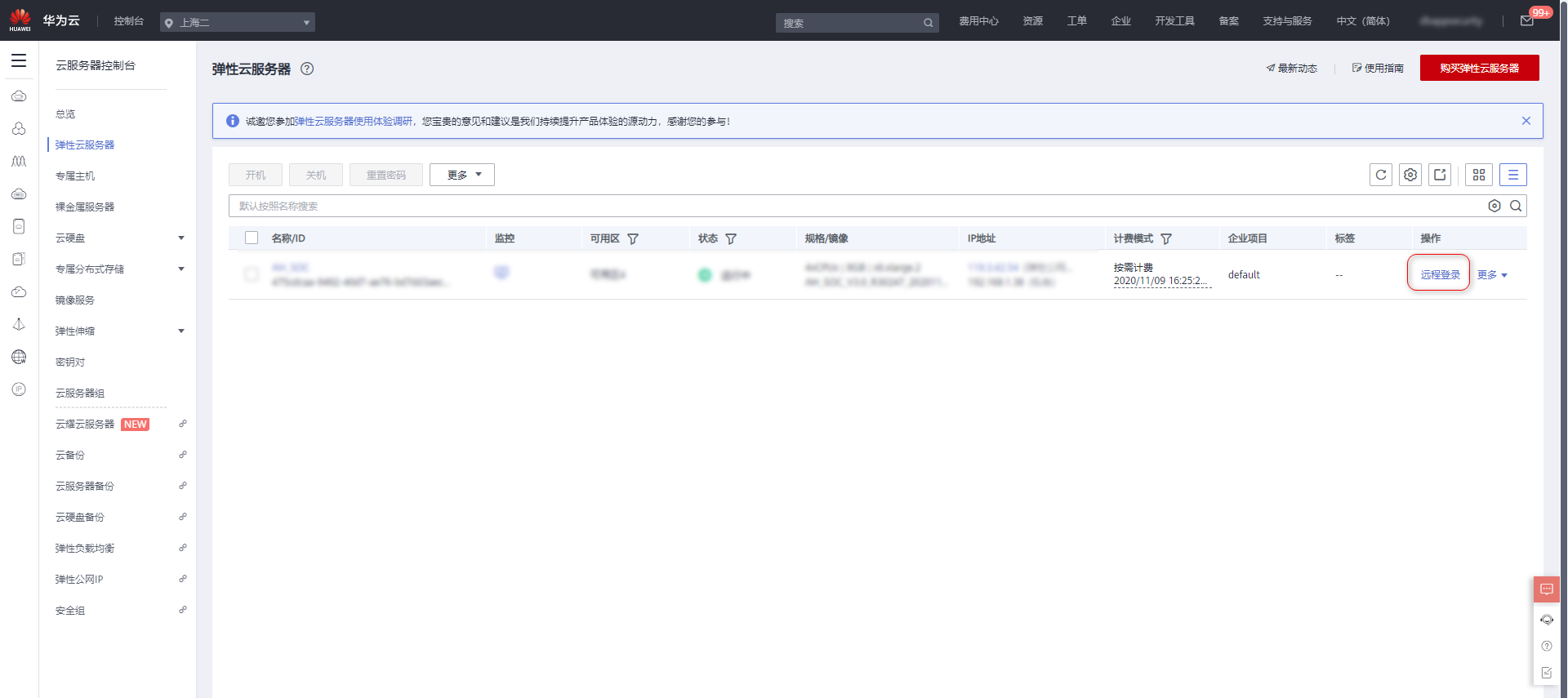
## 说明

由于安恒综合日志审计华为云镜像安全策略SSH服务设置了root用户不能直接SSH登录，必须需要先创建普通用户登录SSH后再su - root切成root用户

## 操作方法

1. 登录云服务器控制台, 使用控制台提供的VNC方式登录

登录华为云服务器控制台，在弹性云服务器界面选择对应的云主机，点击远程登录

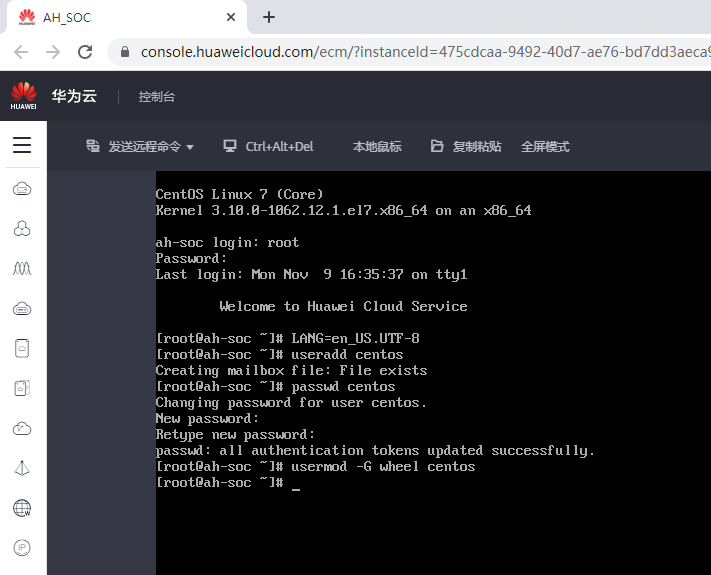


使用控制台提供的VNC方式登录





1. 输入云服务器的root账号和root密码登录



并输入如下命令

LANG=en\_US.UTF-8

useradd centos

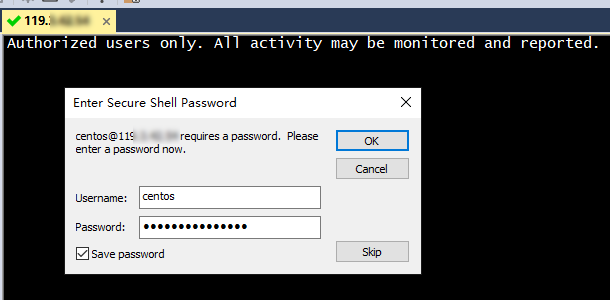
passwd centos

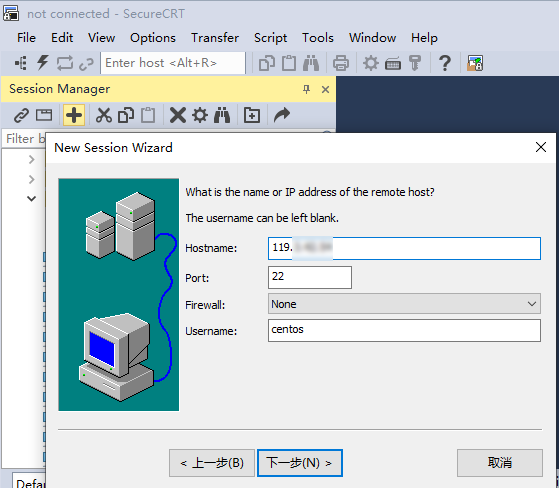
#给centos用户设置密码

usermod -G wheel centos

并将centos用户加到wheel组

1. 使用SSH登录工具例如SecureCRT通过centos用户登录云主机的SSH后台





1. 登录成功后使用sudo su – root命令切换成root用户

