### **态势感知部署流程**

#### 前期准备

|  |  |
| --- | --- |
| **名称** | **说明** |
| **母盘一块** | **默认IP：192.168.10.110**  **ssh端口(hadoop用户)：13322**  **root用户密码： root bd@SSA@root**  **hadoop用户密码：hadoop bd@SSA@1234** |
| **笔记本一台** | **需要配置成192.168.10.88这个IP** |
| **客户系统硬盘一块** | **1T以上** |
| **软件** | **MobaXterm\_Personal\_11.0连接工具,用来打开虚拟机管理界面** |
| **配置信息Excel表格** | **态势感知各台虚拟机配置说明** |

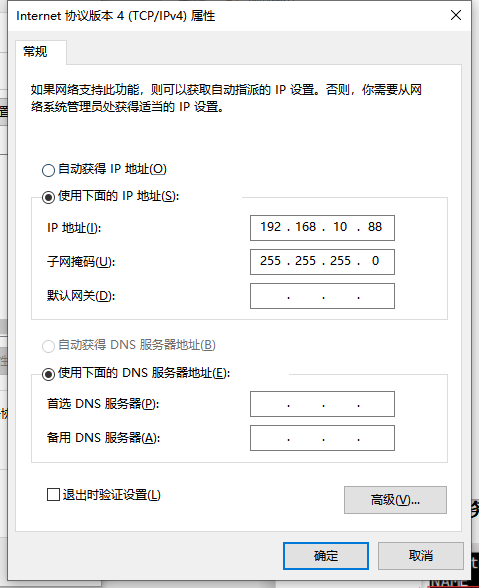
#### 笔记本和服务器直连

如果需要手动安装kvm，则参考如下：

https://github.com/chenyansong1/note/blob/master/kvm/CentOS7%E5%AE%89%E8%A3%85KVM%E8%99%9A%E6%8B%9F%E6%9C%BA%E8%AF%A6%E8%A7%A3.md

###### 用母盘启动服务器

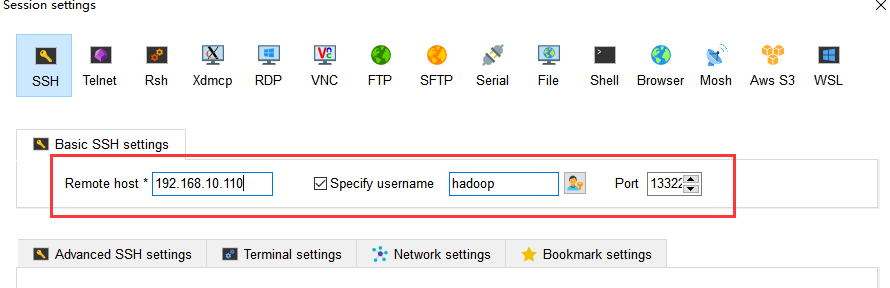
###### 2、配置笔记本IP，一定要192.168.10.88这个IP



###### 3、用网线连接服务器和笔记本

###### 4、使用笔记本ping 192.168.10.110，不通就换其他网口，直到网络通为止

###### 5、用**MobaXterm\_Personal\_11.0或者**shell相关工具连接服务器192.168.10.110，注意：只能使用hadoop用户连接,端口为13322



#### 烤盘(切换root用户)

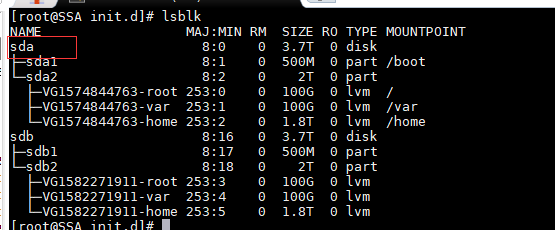
**注意：烤盘步骤需要使用root用户操作,敲su命令即可切换root用户**

**密码为bd@SSA@root**

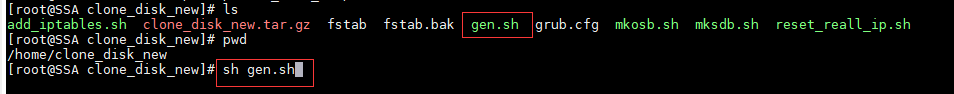


###### 如果服务器支持硬盘热拔插，直接插入客户硬盘即可，但是确保母盘在sda

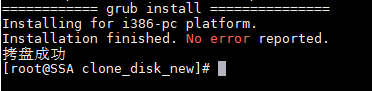
输入指令lsblk可以进行查看



###### 进入/home/clone\_disk\_new目录，执行gen.sh脚本进行烤盘



###### 等待几分钟，烤盘结束，关机拔下母盘，以新盘作为启动盘开机



#### 三、启动虚拟机

###### 拷贝4个镜像

**#创建目录**

**mkdir /home/img -p**

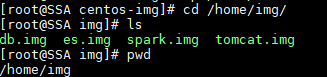
**#复制四个镜像出来（tomcat、spark、es、db）**

**cp /home/centos-img/backup.img /home/img/tomcat.img**

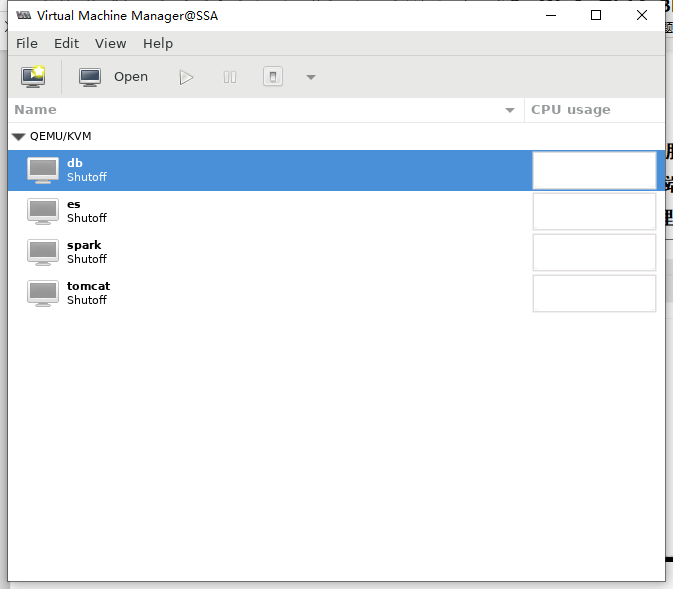
**cp /home/centos-img/backup.img /home/img/spark.img**

**cp /home/centos-img/backup.img /home/img/es.img**

**cp /home/centos-img/backup.img /home/img/db.img**

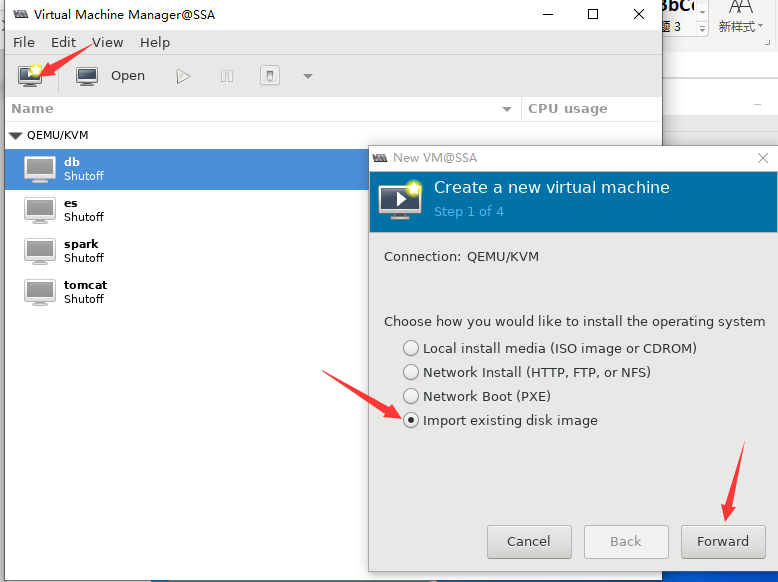


###### 使用MobaXterm\_Personal\_11.0工具软件连接到这台服务器(默认IP：192.168.10.110)，ssh连接只能使用hadoop用户连接(ssh端口13322)，连接后切换root用户执行virt-manager命令，会弹出虚拟机管理界面，如图所示

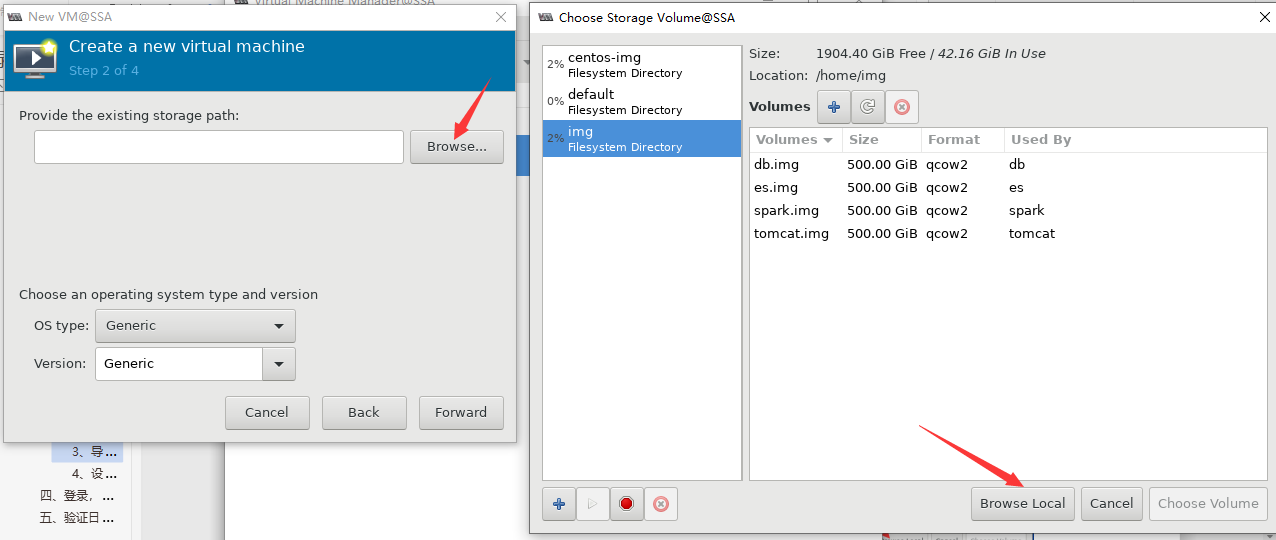


###### 导入镜像

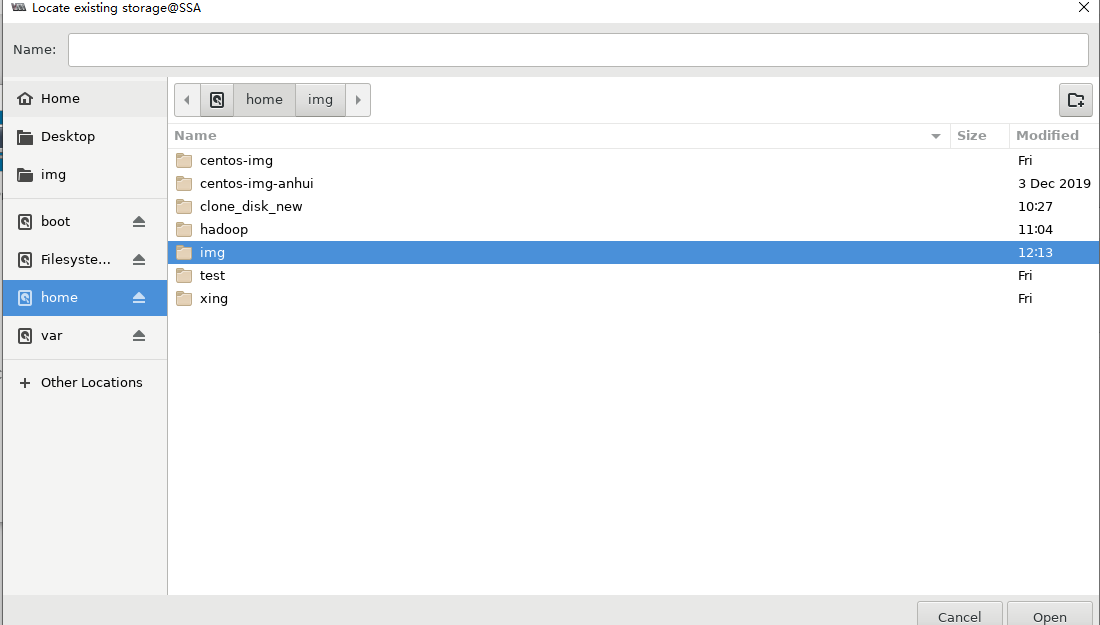
**点击左上角电脑图标，选择导入镜像**



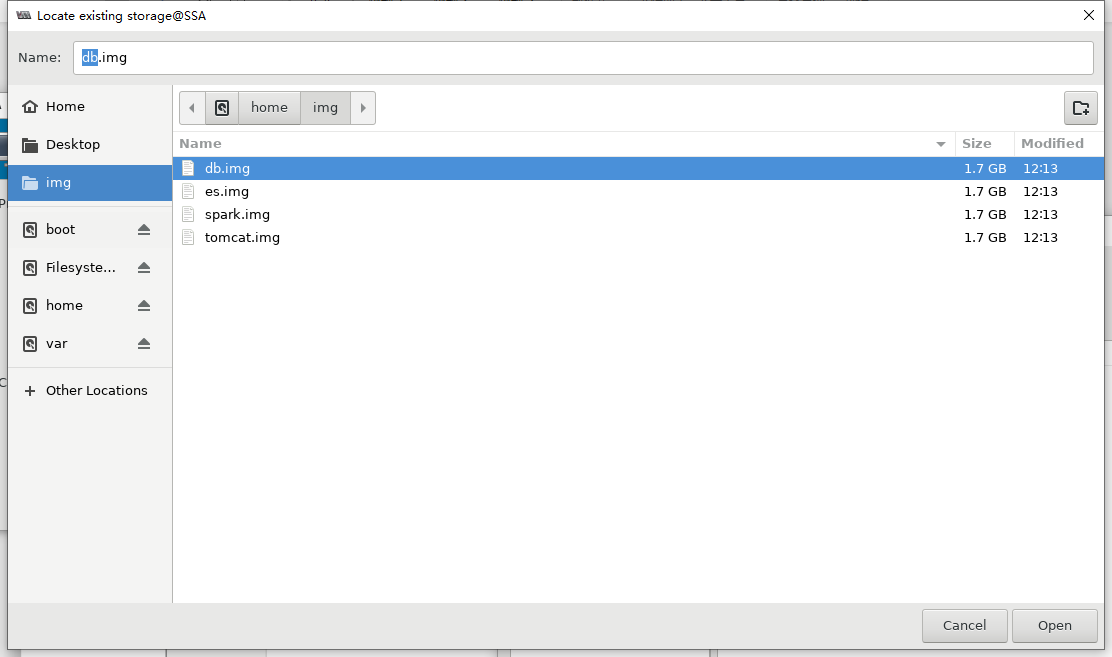
点击图所指按钮

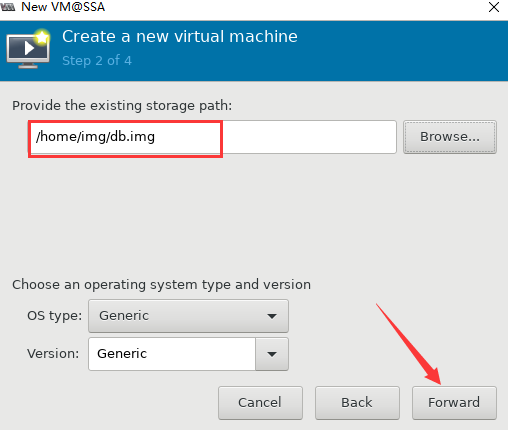


**选择本地/home/img/目录下对应的镜像**

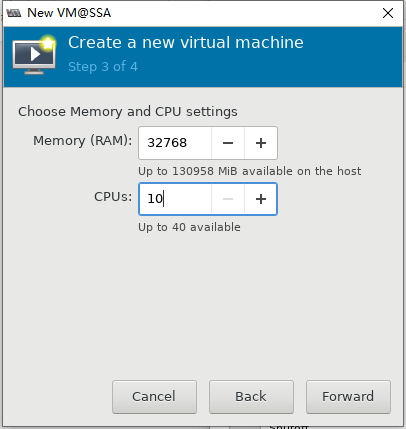


双击选中

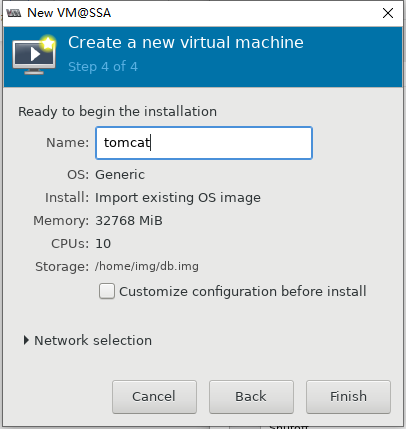




**设置内存和CPU，根据提供的服务器配置Excel表格的信息设置对应大小**



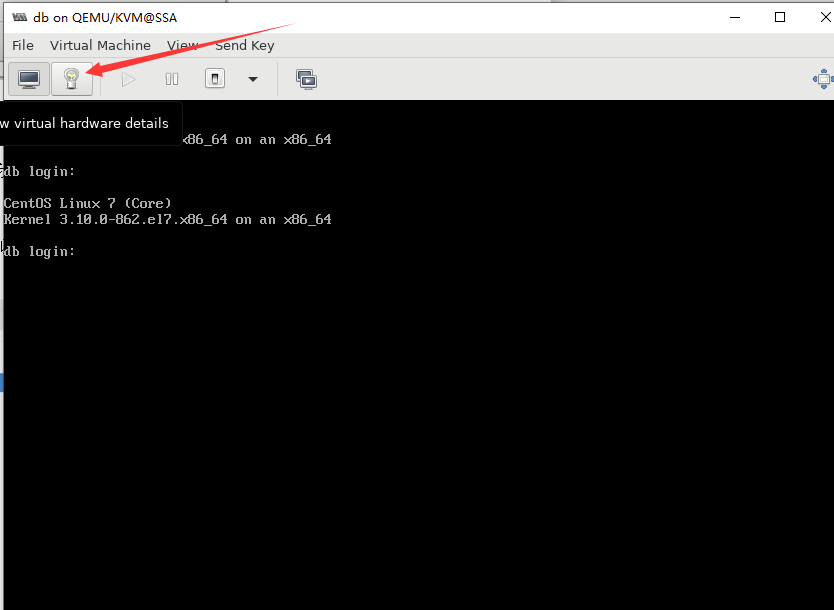
**设置名称，根据选择镜像分别为tomcat、spark、es、db**



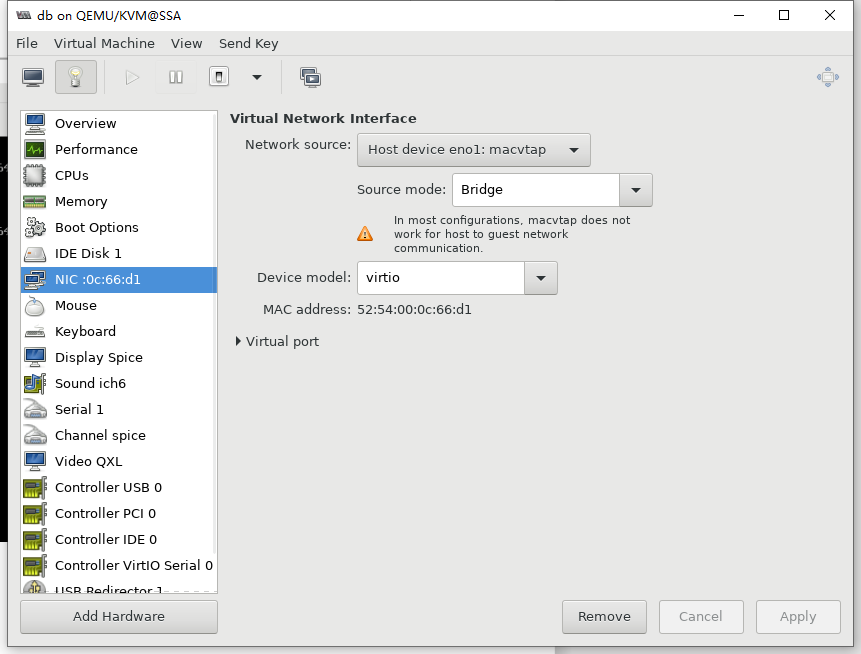
###### 4、设置网络

**四台虚拟机按以上步骤全部导入，我们还得设置桥接网络**

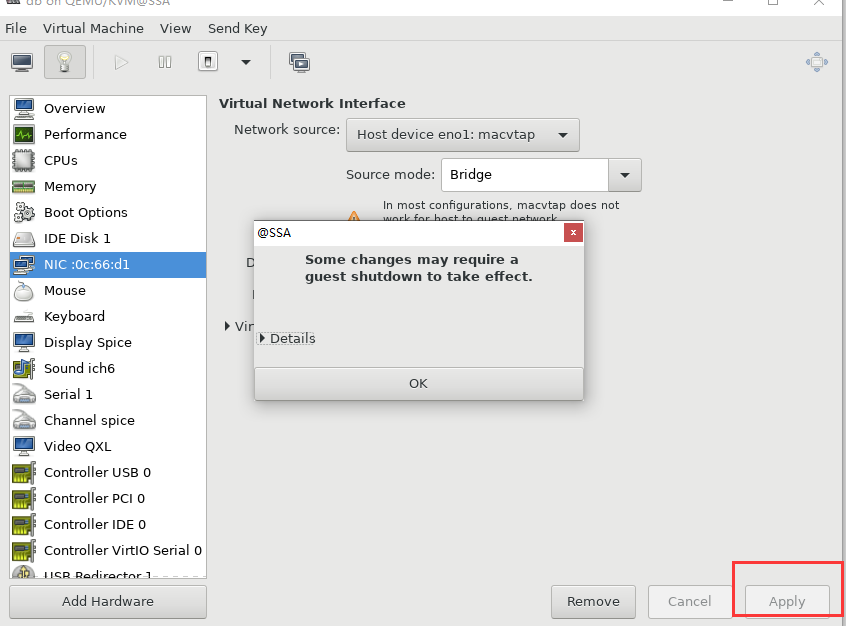
**点击灯泡图标，设置网络，四台同样操作**



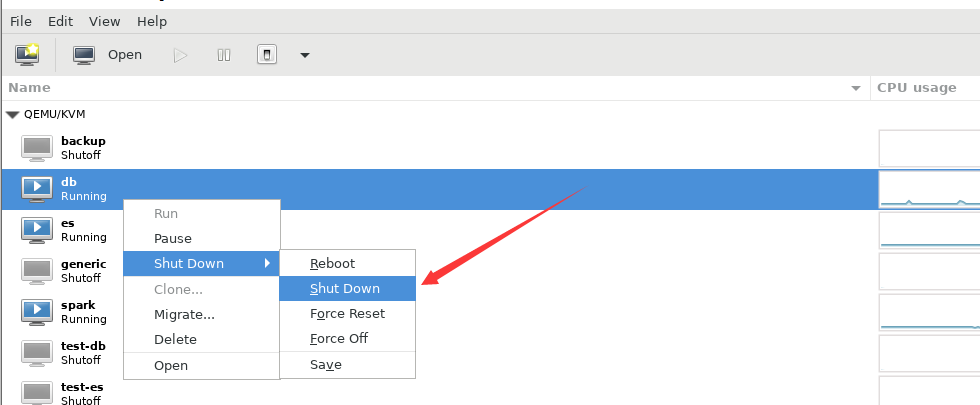
**设置如图所示（eno1为宿主机对应的网卡名称），选择Network source的时候要按着鼠标左键才能选择**



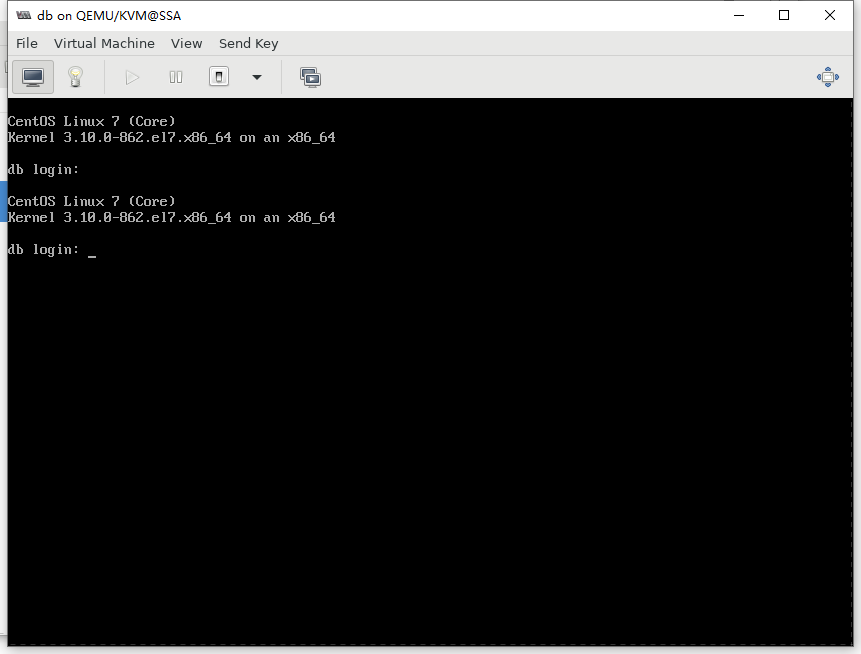
**点击左下角Apply按钮，会弹出提示，意思就是要关机才能生效**



**四台虚拟机网络全部设置完成后，关闭4台虚拟机，重启启动生效**



#### 四、登录，执行初始化脚本



登陆账号为root 密码为bd@SSA@root

**执行脚本，格式： sh 脚本名称 主机名**

**注意：要在对应主机名执行，否则会导致不属于该台服务器的程序运行起来**

**db服务器：**

**cd /home/vm\_init/**

**sh vm\_init\_script.sh db**

**tomcat服务器：**

**cd /home/vm\_init/**

**sh vm\_init\_script.sh tomcat**

**spark服务器：**

**cd /home/vm\_init/**

**sh vm\_init\_script.sh spark**

**es服务器：**

**cd /home/vm\_init/**

**sh vm\_init\_script.sh es**

#### 五、验证日志整体流程

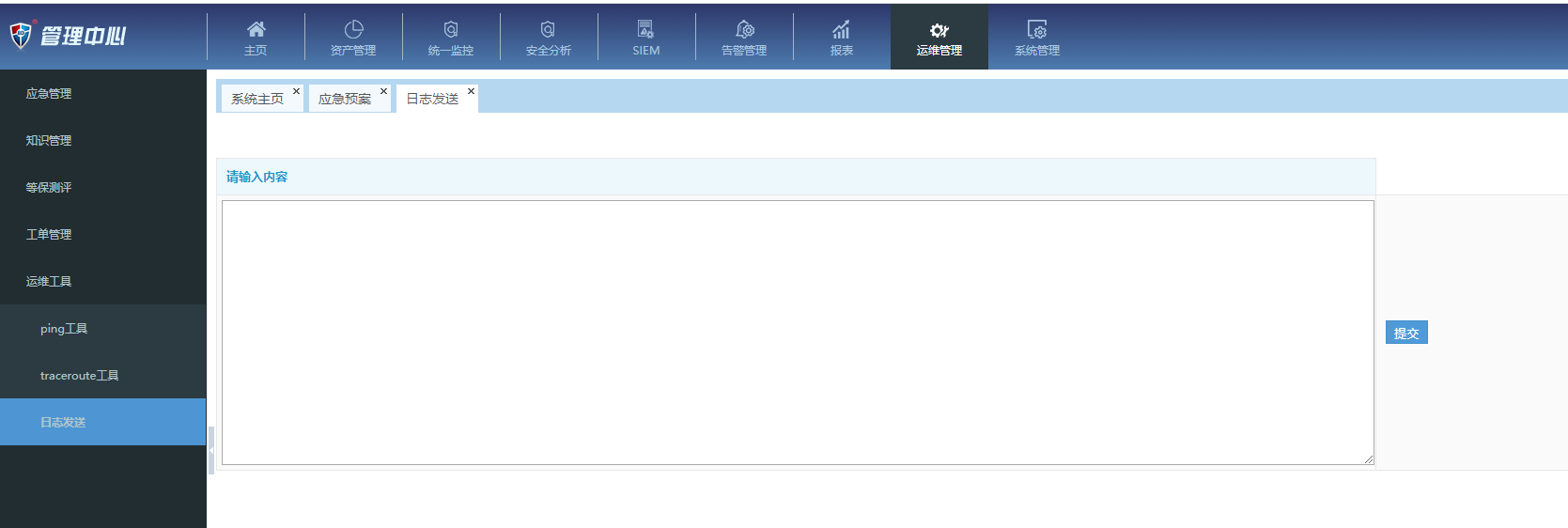
**态势感知大屏：<http://192.168.10.24>**

**态势感知后台：<http://192.168.10.24>/SOCWeb**

**账号：admin**

**密码：Admin\_1234**

1. **登录<http://192.168.10.24>/SOCWeb**
2. **进入运维管理---运维工具---日志发送模块**



1. **提交发送下面日志内容测试**

**<13>Jan 21 23:59:36 172.16.40.254/172.16.40.254 <13>Jan 21 23:57:58 localhost 1579622278 2020/01/21 Tue 23:57:58 ipt\_log=ACCEPT IN=vEth0 OUT=enp2s0 MAC=82:4b:ad:48:b6:0e:00:10:f3:71:9b:93:08:00 SRC=172.16.115.10 DST=192.168.0.102 LEN=96 TOS=0x00 PREC=0x00 TTL=124 ID=16580 PROTO=UDP SPT=61372 DPT=54544 LEN=76**

1. **等待两分钟，检查下面两个模块是否有原始日志和事件生成**

**SIEM-->日志管理-->原始日志查询**

**SIEM-->单事件查询-->安全设备上报事件**